NTR<sub>SH</sub>: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra

S H shahhadi<sup>1</sup> , H R Yassein<sup>1</sup>

<sup>1</sup>University of Al-Qadisiyah, College of Education , Al-Diwaniyah, Iraq

hassan.yaseen@qu.edu.iq

Abstract. Since cryptography relied on mathematical theories and applications of computer science, mathematical algorithms are built with high difficulty. In this paper, we make an improvement and modification NTRU cryptosystem called NTR<sub>SH</sub> 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 more and higher security.

1. Introduction

With the development of life, the need arose to find a safe method for confidential information sent electronically to prevent unauthorized persons from accessing confidential and important data, and this is what was done through cryptography. Many cryptosystems appeared, one of the most important is NTRU which was founded in 1996 by Hoffstein et al. are founded a public key cryptosystem NTRU [1]. It is based on the convolution polynomials ring of the degree N – 1 denoted by Z[x] / (x<sup>N</sup> – 1). An overview of some of these studies is abstracted as follows.

In 2005, by replacing the ring of polynomials with the ring of k × k matrices of polynomials, Coglianese and Goi introduced the MaTRU cryptosystem [2]. In 2009, Nevins et al. [3] proposed a new variant, to NTRU by replacing the original NTRU ring with Einstein integers. Also, Malekian et al. [4] introduced a public key cryptosystem QTRU depends on the Quaternion. NTRU is less resistant to some attacks compared to QTRU. In 2010 Malekian et al. [5] proposed an alternative of NTRU which is called OTRU by replacing the origin 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 [6-9] introduced HXDTRU and BITRU depend on the hexadecnion and binary algebras respectively. In 2019, they also introduced another multidimensional analog NTRU called BCTRU using bicartesian algebra [10,11]. In 2020, Yassein et al. [12] introduced the QOB<sub>TRU</sub> cryptosystem is proposed based on carternion algebra. Also, Yassein et al. [13] introduced a new NTRU alternative cryptosystem called NTRTE that depends on a commutative quaternion algebra with a new structure, which is multi-dimensional. In 2021 Yassein et al. [13] design a new version of NTRU by improving QTRU based on a new mathematical structure called QMNTR.
In this paper, we used tripternion algebra and a change to the mathematical structure, to design a new alternative of NTRU cryptosystem called NTR\textsubscript{SH}. The rest of this paper is organized as follows: In Section 2, we shortly review the NTRU cryptosystem. In Section 3, tripternion algebra is presented, and the operations on this algebra are defined. In Section 4, a multi-dimensional cryptosystem was presented and explained the algorithm of each phase. We show performance analysis and comparison with NTRU in Section 5. Finally, we summarize our conclusions in Section 6.

2. NTRU CRYPTOSYSTEM

NTRU cryptosystem depends on a truncated polynomial ring of degree $N - 1$ denoted by $K = \mathbb{Z}[x] / (x^N - 1)$, such that $N$ is a prime number. The rings of truncated polynomial mod $p$ denoted it by a symbol $K_p = \mathbb{Z}_p[x] / (x^N - 1)$ and the rings of truncated polynomial mod $q$ denoted it by a symbol $K_q = \mathbb{Z}_q[x] / (x^N - 1)$, such that $p, q$ are integers number and gcd $(p, q) = 1$, where $p$ is smaller than $q$. The subset $L_f, L_g, L_r, L_m$ defines as follow:

$L_f = \{f \in K : f \text{ satisfy } \ell_{(d_x, d_y)}\}$

$L_g = \{g \in K : g \text{ satisfy } \ell_{(d_x, d_y)}\}$

$L_r = \{r \in K : r \text{ satisfy } \ell_{(d_x, d_y)}\}$

$L_m = \{m \in K : \text{ coefficients of } m \text{ are chosen mod } p \text{ between } -\frac{p}{2} \text{ and } \frac{p}{2}\}$

where $\ell_{(d_x, d_y)} = \{f \in K : f \text{ has } d_x \text{ coefficients equal } 1, d_y \text{ coefficients equal } -1, \text{the remaining equal } 0\}$

The NTRU Cryptosystem is passed three stages:

I. Key Generation

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

II. Encryption

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

$e = ph * r + m \text{ (mod } q\}.$

III. Decryption

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

$f * e \text{ (mod } q\} = (pf * h * r + f * m) \text{ (mod } q\}$

$f * e \text{ (mod } p\} = f * m \text{ (mod } p\}$

$f_p^{-1} * f * e \text{ (mod } p\} = f_p^{-1} * f * m \text{ (mod } p\}$

$= m \text{ (mod } p\}.$

3. TRIPTERNION ALGEBRA

In this section, we introduce a new multidimensional algebra over the field $F$ which called tripternion algebra $\mathbb{T}$ as follows:
Let $T = \{a + bx + cx^2 \mid a, b, c \in F\}$ 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:

\[
A = a_0 + a_1x + a_2x^2 \quad \text{and} \quad B = b_0 + b_1x + b_2x^2
\]

The addition, multiplication of two tripternions, scalar multiplication, and inverse multiplication are defined by:

\[
A + B = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2
\]

\[
A \cdot B = \beta a_0 + \beta a_1x + \beta a_2x^2, \quad \text{for any scalar } \beta
\]

\[
A^{-1} = \frac{1}{a_0 + \frac{1}{a_1}x + \frac{1}{a_2}x^2}, a_0, a_1, a_2 \neq 0
\]

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. NTR$_{SH}$ CRYPTOSYSTEM

NTR$_{SH}$ cryptosystem depends on tripternion algebra. The rings of truncated polynomial denoted it by a symbol $\mathbb{A} = \mathbb{Z}[x]/(x^N - 1)$, the rings of truncated polynomial mod $p$ and the rings of truncated polynomial mod $q$ denoted by a symbols $\mathbb{A}_p = \mathbb{Z}_p[x]/(x^N - 1)$ and $\mathbb{A}_q = \mathbb{Z}_q[x]/(x^N - 1)$, respectively, such that $p, q$ are integers number and gcd$(p, q) = 1$, where $p$ is smaller than $q$.

Let $d_f, d_j, d_v, d_u, d_g, d_r, d_s, d_c$ and $d_m$ be constant integers less than $N$. The subset $L_F, L_I, L_V, L_U, L_G, L_R, L_S, L_C$ and $L_M$ are define as follow:

\[
L_F = \{f_0 + f_1x + f_2x^2 \in \mathbb{A} \text{ satisfy } \ell(d_f, d_f - 1)\}
\]

\[
L_I = \{i_0 + i_1x + i_2x^2 \in \mathbb{A} \text{ satisfy } \ell(d_i, d_i - 1)\}
\]

\[
L_V = \{v_0 + v_1x + v_2x^2 \in \mathbb{A} \text{ satisfy } \ell(d_v, d_v - 1)\}
\]

\[
L_U = \{u_0 + u_1x + u_2x^2 \in \mathbb{A} \text{ satisfy } \ell(d_u, d_u)\}
\]

\[
L_G = \{g_0 + g_1x + g_2x^2 \in \mathbb{A} \text{ satisfy } \ell(d_g, d_g)\}
\]

\[
L_R = \{r_0 + r_1x + r_2x^2 \in \mathbb{A} \text{ satisfy } \ell(d_r, d_r)\}
\]

\[
L_S = \{s_0 + s_1x + s_2x^2 \in \mathbb{A} \text{ satisfy } \ell(d_s, d_s - 1)\}
\]

\[
L_C = \{c_0 + c_1x + c_2x^2 \in \mathbb{A} \text{ satisfy } \ell(d_c, d_c)\}
\]

\[
L_M = \{m_0 + m_1x + m_2x^2 \text{ coefficients of } m_i \text{ are chosen mod } p \text{ between } -\frac{p}{2} \text{ and } \frac{p}{2}\}
\]

where $\ell(d_x, d_y) = \{f \in \mathbb{A} \mid f \text{ has } d_x, d_y \text{ coefficients equal } 1, d_x, d_y \text{ coefficients equal } -1, \text{the remaining equal } 0\}$.

I. Key Generation phase

The keys are constructed as follows: we randomly choose six polynomials $F, G, U, S, V$, and $J$ from $L_F, L_G, L_U, L_S, L_V$ and $L_J$ respectively. The keys are generated according to the algorithm below.

**Algorithm keys generation**

Input: $N, p, q, F, G, U, S, V, J$

Output: public keys $H, K$

\[
F_q^{-1} = \text{inverse } F \mod q
\]

\[
J_q^{-1} = \text{inverse } J \mod q
\]

\[
H = F_q^{-1} * G \mod q
\]

\[
K = S * V * J_q^{-1} \mod q
\]
$F, G, U, S, V$ and $J$ are special keys that are known to the recipient only, while $H$ and $K$ are known to both the sender and the recipient.

II. Encryption phase

The message $M \in L_M$ is encryption after selecting random polynomial $R \in L_R$, and $C \in L_C$ text encryption is according to this algorithm.

*Algorithm Encryption*

Input: $N, p, q, R, C$, message $M$, public keys $H, K$

Output: encryption message $E$

$$E = p(H + R * C) + M * K \pmod q.$$  

III. Decryption phase

After receiving the encrypted text, we get the original text through the algorithm.

*Algorithm Decryption*

Input: $N, p, q, E, V_p^{-1}, S_p^{-1}, F_p^{-1}$

Output: $M$

$$Y_1 = F * E \pmod q$$

$$Y_2 = Y_1 * J \pmod q$$

for $i = 1$ to $3$

for $j = 1$ to $N$

if $Y_2(i, j) \leq -q/2$

$Y_2(i, j) = Y_2(i, j) + q$

else if $Y_2(i, j) > -q/2$

$Y_2(i, j) = Y_2(i, j) - q$

end if

end for

$Y_3 = Y_2 \pmod p$

$Y_4 = Y_3 * V_p^{-1} \pmod p$

$Y_5 = Y_4 * S_p^{-1} \pmod p$

$Y_6 = F_p^{-1} * Y_5 \pmod p$

for $i = 1$ to $3$

for $j = 1$ to $N$

if $Y_6(i, j) \leq -p/2$

$Y_6(i, j) = Y_5(i, j) + p$

else if $Y_6(i, j) > p/2$

$Y_6(i, j) = Y_5(i, j) - p$

end if

end for

end for

$M = Y_6.$
5. COMPARATIVE BETWEEN NTRU, NTR$_{Sh}$

5.1. Mathematical Operation

Depending on algorithms of the key generation, encryption, and decryption of NTRU and NTR$_{Sh}$ then the mathematical operations (convolution multiplications and addition) of key generation, encryption, and decryption between NTRU and NTR$_{Sh}$ show in Table 1.

|                 | NTRU                          | NTR$_{Sh}$                     |
|-----------------|-------------------------------|--------------------------------|
| Key Generate    | 1 convolution multiplications | 54 convolution multiplications |
|                 | 1 convolution multiplications  | 18 convolution multiplications  |
| Encryption      | 1 polynomial addition         | 6 polynomials addition         |
|                 | 2 convolution multiplications, |                                 |
|                 | 1 polynomial addition         |                                 |

Table 2 explain the speed of NTRU and NTR$_{Sh}$ based on table 1.

|                 | NTRU                          | NTR$_{Sh}$                     |
|-----------------|-------------------------------|--------------------------------|
| Speed           | $4t + 2t_1$                   | $261t + 12t_1$                 |

where $t$ denoted multiplication time, and $t_1$ denoted addition time. So NTR$_{Sh}$ is slower than NTRU but we can solve this problem by reduce value $N$.

5.2. Level of security

Depending on $d_g, d_u, d_s$ and $d_v$ the key security of NTR$_{Sh}$ is 12 times the key security of NTRU. Also, the message security of NTR$_{Sh}$ is 6 times the message security of NTRU according to $d_r$ and $d_c$. Table 3 shows the level of security comparison of key and message between NTRU and NTR$_{Sh}$.

|                 | NTR$_{Sh}$ | NTRU |
|-----------------|------------|------|
| Key security    | $\frac{N!}{(d_g)!^2(N-2d_g)!}$ | $\frac{N!}{d_r)!^2(N-2d_r)!$ |
|                | $\frac{N!}{(d_u)!^2(N-2d_u)!}$ | $\frac{N!}{d_c)!^2(N-2d_c)!$ |
|                | $\frac{N!}{(d_s)!^2(N-2d_s)!}$ | $\frac{N!}{d_v)!^2(N-2d_v)!$ |

| Message security | NTR$_{Sh}$ | NTRU |
|------------------|------------|------|
|                  | $\frac{N!}{(d_g)!^2(N-2d_g)!}$ | $\frac{N!}{d_r)!^2(N-2d_r)!$ |
|                  | $\frac{N!}{(d_u)!^2(N-2d_u)!}$ | $\frac{N!}{d_c)!^2(N-2d_c)!$ |
|                  | $\frac{N!}{(d_s)!^2(N-2d_s)!}$ | $\frac{N!}{d_v)!^2(N-2d_v)!$ |
6. Conclusion

NTR_{SH} a multidimensional public key cryptosystem via tripternion algebra is guaranteed high security against attacks, as brute force and good efficiency. Its speed is less than NTRU, with the possibility of solving this negativity by reducing the value of N while maintaining a high level of security. With these characteristics, NTR_{SH} is suitable for many applications that require more than one data source and even one source as electronic voting.

References

[1] Hoffstein J, Pipher J and Silverman J 1998 NTRU: A ring based public key cryptosystem, Proceeding of ANTS III LNCS Springer Verlag, 1423 267-288.
[2] Coglianese M and Goi B, MaTRU: A new NTRU based cryptosystem, Springer Verlag Berlin Heidelberg 3797 232-243.
[3] Nevins M, Pour C K and Miri A 2009 NTRU over rings beyond Z, Designs, Codes and Cryptography 56 65-78.
[4] Malecian E, Zakerholsooeini A and Mashatan A 2011 QTRU: a lattice attack resistant version of NTRU PCKS based on quaternion algebra, The ISC Int'l Journal of Information Security 3 29–42.
[5] Malecian E and Zakerholsooeini A 2010 OTRU: A non-associative and high speed public key cryptosystem, IEEE Computer Society 16 83-90.
[6] Yassein H R and Al-Saidi N M G 2016 HXDTRU Cryptosystem Based on Hexadecimal Algebra Proceeding of The 6th International Cryptology and Information Security Conf. Sabah, Malaysia 1-10.
[7] Al-Saidi N M G and Al-Saidi H R Yassein 2017 A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure. Malaysian Journal of Mathematical Sciences 11 29 – 43.
[8] Al-Saidi N M G and Yassein H R 2016 BITRU: Binary Version of the NTRU Public Key Cryptosystem via Binary Algebra International Journal of Advanced Computer Science and Applications 7 1-6.
[9] Yassein H R and Al-Saidi N M G 2017 A Comparative Performance Analysis of NTRU and Its Variant Cryptosystems Proceeding of International Conference on Current Research in Computer Science and Information Technology Slemani, Iraq 115-120.
[10] Yassein H R and Al-Saidi N M G 2018 BCTRU: A New Secure NTRU Crypt Public Key System Based on a Newly Multidimensional Algebra Proceeding of The 6th International Cryptology and Information Security Conf. Negeri Sembilan, Malaysia 1-11.
[11] Yassein H R and Al-Saidi N M G 2019 An Innovative Bi-Cartesian Algebra for Designing of Highly Performed NTRU Like Cryptosystem Malaysian Journal of Mathematical Sciences 13 77-91.
[12] Yassein H R, Al-Saidi N M G and Farhan A K 2020 A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure Journal of Discrete Mathematical Sciences and Cryptography 23 1-20.
[13] Yassein H R, Al-Saidi N M G and Almosawi A K 2020 A multi-dimensional algebra for designing an improved NTRU cryptosystem Eurasian journal of mathematical and computer applications. 8 97-107.
[14] Yassein H R, Abidahzahra A A and Al-Saidi N M G 2021 A New Design of NTRU Encryption with High Security and Performance Level AIP Conf. Proc. Istanbul Turkey 2334 080005- 1-080005- 4.