International Journal of Mathematics and
Computer Science, **18**(2023), no. 2, 199–204

HUDTRU: An Enhanced NTRU for Data Security via Quintuple Algebra

Hassan Rashed Yassein[1], **Huda Abdulateef Ali**[2]

[1]Department of Mathematics
College of Education
University of Al-Qadisiyah
Al-Qadisiyah, Iraq

[2]Department of Mathematics
Faculty of Education for Girls
University of Kufa
Al Najaf, Iraq

email: hassan.yaseen@qu.edu.iq, hudaalrobayee75@gmail.com

(Received November 15, 2022, Accepted December 22, 2022,
Published January 23, 2023)

Abstract

NTRU is an alternative to those cryptosystems that were based on discrete logarithm problems or integer factorization. It delivers efficiency against many attacks and, as a result, is the perfect choice for many applications. In this paper, we introduce a new alternative to NTRU public key cryptosystem called HUDTRU which is built on Quintuple algebra, by changing the mathematical structure of keys to encrypt and decrypt the text to obtain a high level of security.

Keywords and phrases: NTRU, BCTRU, Quintuple algebra.
AMS (MOS) Subject Classifications: 94A60, 68P25.
ISSN 1814-0432, 2023, http://ijmcs.future-in-tech.net

1 Introduction

NTRU is one of the fastest public key cryptosystems and has much smaller keys based on the truncated polynomial ring $Z[X]/(X^N-1)$ [1]. Due to these advantages, several authors have made many improvements: In 2002, Gaborit et al. [2] prefaced an NTRU-like cryptosystem depending on a polynomial ring over a binary field called CTRU. Coglianese and Goi [3] introduced the MaTRU cryptosystem replacing the ring of polynomials of order N with a ring of square matrices $k \times k$ of polynomials $R = Z[X]/(X^N - 1)$. In 2016, Yassein and Al-Saidi [4] presented a new NTRU cryptosystem analog, called HXDTRU based on hexadecnion algebra, with high security. Also, Yassein et al. [5] introduced improvements to the NTRU cryptosystem by using a higher dimensional algebra, a new mathematical model, or both. In 2022, Ali and Yassein [6] introduced QTNTR, a commutative and associative multidimensional public key using Quintuple algebra. We propose a new multidimensional public key HUDTRU based on Quintuple algebra through a new mathematical structure.

2 HUDTRU cryptosystem

The underlying algebraic structure for the HUDTRU cryptosystem is the Quintuple algebra [6]. The parameters of the new HUDTRU are integers N, p and q such that $gcd(p, q) = 1$ as defined in NTRU. Consider the three truncated polynomial rings $\delta = Z[X]/(X^N - 1)$, $\delta_p = Z[X]/(X^N - 1)$, and $\delta_q = Z[X]/(X^N - 1)$ and Quintuple algebra

$\gamma = \{(\beta_1, \beta_2)(1,1) + (\beta_3, \beta_4)(1,i) + (\beta_5, \beta_6)(1,j)(\beta_7, \beta_8)(1,k)$
$+ (\beta_9, \beta_{10})(1,h)\} |\ \beta_i \in \delta\ ,\ i = 1, 2, \ldots\ldots, 10\}$,
$\gamma_p = \{(\beta_1, \beta_2)(1,1) + (\beta_3, \beta_4)(1,i) + (\beta_5, \beta_6)(1,j)(\beta_7, \beta_8)(1,k)$
$+ (\beta_9, \beta_{10})(1,h)\} |\ \beta_i \in \delta_p,\ i = 1, 2, \ldots\ldots, 10\}$,
$\gamma_q = \{(\beta_1, \beta_2)(1,1) + (\beta_3, \beta_4)(1,i) + (\beta_5, \beta_6)(1,j)(\beta_7, \beta_8)(1,k)$
$+ (\beta_9, \beta_{10})(1,h)\} |\ \beta_i \in \delta_q,\ i = 1, 2, \ldots\ldots, 10\}$.

Now, define subsets as follows:

$\mathcal{L}_\alpha = \Big\{(\alpha_1, \alpha_2)(1,1)+(\alpha_3, \alpha_4)(1,i)+(\alpha_5, \alpha_6)(1,j)+(\alpha_7, \alpha_8)(1,k)+(\alpha_9, \alpha_{10})(1,h) \in$
$\gamma : \ell(d_\alpha,\ d_\alpha - 1)\Big\}$,
$\mathcal{L}_u = \Big\{(u_1, u_2)(1,1)+(u_3, u_4)(1,i)+(u_5, u_6)(1,j)+(u_7, u_8)(1,k)+(u_9, u_{10})(1,h) \in$
$\gamma : \ell(d_u, d_u)\Big\}$,

$\mathcal{L}_\omega = \Big\{(\omega_1, \omega_2)\,(1,1)+(\omega_3, \omega_4)\,(1,i)+(\omega_5, \omega_6)\,(1,j)+(\omega_7, \omega_8)\,(1,k)+(\omega_9, \omega_{10})\,(1,h) \in \gamma : \ell(d_\omega,\ d_\omega - 1)\Big\}$,
$\mathcal{L}_\upsilon = \Big\{(\upsilon_1, \upsilon_2)\,(1,1)+(\upsilon_3, \upsilon_4)\,(1,i)+(\upsilon_5, \upsilon_6)\,(1,j)+(\upsilon_7, \upsilon_8)\,(1,k)+(\upsilon_9, \upsilon_{10})\,(1,h) \in \gamma : \ell(d_\upsilon,\ d_\upsilon - 1)\Big\}$,
$\mathcal{L}_\mathcal{M} = \Big\{(m_1, m_2)\,(1,1) + (m_3, m_4)\,(1,i) + (m_5, m_6)\,(1,j) + (m_7, m_8)\,(1,k) + (m_9, m_{10})\,(1,h) \in \gamma$ with coefficients of $\mathcal{M}$ chosen modulo p between $-p/2$ and $p/2$ $\Big\}$.
The subsets $\mathcal{L}_\tau, \mathcal{L}_\vartheta$ and $\mathcal{L}_\sigma$ are defined similar to $\mathcal{L}_u$.

The phases of the HUDTRU are as follows:
Phase 1. Key Generation. After randomly choosing four small Quintuple $\alpha\epsilon\ \mathcal{L}_\alpha,\ \tau\epsilon\mathcal{L}_\tau,\ \omega\,\epsilon\mathcal{L}_\omega$, and $\upsilon\epsilon\mathcal{L}_\upsilon$, such that $\alpha*\ \alpha^{-1} \equiv 1(mod\, p),\ \ \alpha *\ \alpha^{-1} \equiv 1(mod\, q), \omega*\omega^{-1} \equiv 1\,(mod\ q)\,,$ and $\upsilon * \upsilon^{-1} \equiv 1\,(mod\ p)$ the following pseudo code 1 is used to generate the keys.

Pseudo Code 1 Key generation

Input: $N, p, q, d_\alpha, d_\tau, d_\omega, d_\upsilon, d_u$
Output: public keys $\mathcal{H}, \mathcal{B}$
1: $\alpha_q^{-1} =$ inverse $\alpha\ mod\ q$
2: $\omega_q^{-1} =$ inverse $\ \omega\ mod\ q$
3: $\mathcal{H} = \alpha_q^{-1} * \tau * u\ mod\ q$
4: $\mathcal{B} = \upsilon * \omega_q^{-1} mod\ q$
5: end

Then, the private keys are $\alpha, \tau, \omega,\ \upsilon, u$, the process of generating keys of HUDTRU requires thirty convolution multiplication.
Phase 2. Encryption. First, we convert the message to the following form $\mathcal{M} = (m_1, m_2)\,(1,1)+(m_3, m_4)(1,i)+(m_5, m_6)(i,j)+(m_7, m_8)(1,k)+(m_9, m_{10})(1,h)$, then we choose $\vartheta \in \mathcal{L}_\vartheta$ and $\sigma \in \mathcal{L}_\sigma$ randomly. These values are known as ephemeral. The text $\mathcal{M}$ is encrypted according to the following pseudo code 2:

Pseudo Code 2 Encryption

Input: : $N, q,\ \vartheta, \sigma$, message $\mathcal{M}$, public keys $\mathcal{H}, \mathcal{B}$
Output: encryption message E

$E = p\left(\mathcal{H} * \vartheta + \sigma\right) + \mathcal{M} * \mathcal{B}\ (mod\ q)$
end

The encryption phase requires twenty convolution multiplications and twenty polynomial additions.

Phase 3. Decryption. To get the original text $\mathcal{M}$ from the ciphertext E, the recipient performs the steps shown in the pseudo code 3:

Pseudo Code 3 Decryption

Input: $N, p, q, E,\ \alpha, \omega, \alpha_p^{-1},\ \upsilon_p^{-1}$, public keys $\mathcal{H}, \mathcal{B}$
Output: $\mathcal{M}$

$A_1 = \alpha * E$
$A_2 = A_1 * \omega$
for $i = 1$ *to* 10 **do**
    for $j = 1$ *to* N **do**
        if $A_2(i,j) <= \frac{-q}{2}$ **then**
            $A_2\left(i,j\right) = A_2\left(i,j\right) + q$
        else if $A_2(i,j) > \frac{q}{2}$ **then**
            $A_2(i,j) = A_2(i,j) - q$
        end if
    end for
end for
$A_3 = A_2\ mod\ p$
$A_4 = \alpha_p^{-1} * A_3\ mod\ p$
$A_5 = A_4 * \upsilon_p^{-1}\ mod\ p$
for $i = 1$ *to* 10 **do**
    for $j = 1$ *to* N **do**
        if $A_5(i,j) <= \frac{-p}{2}$ **then**
            $A_5\left(i,j\right) = A_5\left(i,j\right) + p$
        else if $A_5(i,j) > \frac{p}{2}$ **then**
            $A_5\left(i,j\right) = A_5\left(i,j\right) - p$
        end if
    end for
end for
$\mathcal{M} = A_5$
end

The decryption phase needs seventy convolution multiplications and twenty polynomial additions.

3 Analysis of Security

In HUDTRU, an attacker who knows the public parameters in addition to the public keys $\mathcal{H}$ and $\mathcal{B}$ does a search in the subsets $\mathcal{L}_\tau, \mathcal{L}_u$, and $\mathcal{L}_\upsilon$ whose sizes are

$$\frac{(N!)^{10}}{(d_\tau!)^{20}(N-2d_\tau)!^{10}}, \frac{(N!)^{10}}{(d_u!)^{20}(N-2d_u)!^{10}}, \text{ and } \frac{(N!)^{10}}{(d_\upsilon!)^{20}(N-2d_\upsilon)!^{10}}$$

respectively for accessing the private keys τ, u, and υ for the public keys from which to get the original text, or can be made by searching the subsets $\mathcal{L}_\vartheta$ and $\mathcal{L}_\sigma$ whose sizes are

$$\frac{(N!)^{10}}{(d_\vartheta!)^{20}(N-2d_\vartheta)!^{10}} \text{ and } \frac{(N!)^{10}}{(d_\sigma!)^{20}(N-2d_\sigma)!^{10}}$$

respectively for accessing to the private keys ϑ and σ for the ciphertext.

4 Conclusions

We introduced the multidimensional cryptosystem HUDTRU that can encrypt ten messages in one round from one source or ten different sources. This feature yields the possibility to apply it in many areas that need multiple data sources with high security.

References

[1] J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A ring-based public key cryptosystem, Proceedings Third International Symposium in Algorithmic Number Theory, (1998), 267–288.

[2] P. Gaborit, J. Ohler, P. Solé, CTRU, a polynomial analogue of NTRU, Doctoral dissertation, Inria, (2002).

[3] M. Coglianese, B. M. Goi, MaTRU: A new NTRU-based cryptosystem, International conference on cryptology in India, (2005), 232–243.

[4] H. R. Yassein, N. M. Al-Saidi, HXDTRU Cryptosystem Based on Hexadecnion Algebra, Proceeding of the 5th International Cryptology and Information Security Conference, Malaysia, (2016).

[5] 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.

[6] H. A. Ali, H. R. Yassein, QTNTR: A New Secure NTRU Encrypt Alternative with a High Level of Security, Mathematical Statistician and Engineering Applications, **71,** no. 4, (2022), 5634–5639.