International Journal of Mathematics and
Computer Science, **19**(2024), no. 1, 1–4

HAQTR: NTRU-Like Public Key

Abbas Chichan Fadeel, Hassan Rashed Yassein

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

email: edu-math.post34@qu.edu.iq, hassan.yaseen@qu.edu.iq

(Received April 7, 2023, Accepted May 11, 2023,
Published August 31, 2023)

Abstract

Due to the importance of the NTRU public key cryptosystem, many improvements have been made to it by increasing security or speed to keep pace with the process of technological development in exchanging various data. In this paper, we construct a public key cryptosystem called HAQTR using non-commutative quaternion algebra with the change of the mathematical structure.

1 Introduction

In 1996, Hoffstein et al. proposed NTRU based on a truncated polynomial ring [1] and worked on developing the NTRU cryptosystem. Afterwards, many versions of NTRU appeared and we briefly mention some of them: In 2021, Shahhadi and Yassein [2, 3] proposed a new design of NTRU called NTRS and they proposed NTRSH. In the same year, Abo-alsood and Yassein [4] proposed a QOTRU cryptosystem depending on bi-octonion algebra. In 2023, Yassein and Ali [5] enhanced the security of NTRU based on quintuple algebra and they called it HUDTRU. In this paper, we construct a new development of NTRU based on a new mathematical structure called

Keywords and phrases: NTRU, Quaternion algebra, Key space, Message space.
AMS (MOS) Subject Classifications: 94A60, 68P25.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

HAQTR. Our work goes through three main phases which are key generation, encryption, and decryption. As expected, HAQTR provides more security than NTRU.

2 HAQTR Cryptosystem

HAQTR is based on quaternion algebra [6]. HAQTR depends on the same parameters in NTRU. Let $\wp = Z[x]\backslash(x^N - 1)$, $\wp_p = Z_p[x]\backslash(x^N - 1)$ and $\wp_q = Z_q[x]\backslash x^N - 1$ and three algebra $\mho = \{f_0(x)+f_1(x)i+f_2(x)j+f_3(x)k \mid f_\alpha(x) \in \wp\}, \mho_p = \{f_0(x)+f_1(x)i+f_2(x)j+f_3(x)k \mid f_\alpha(x) \in \wp_p\}, \mho_q = \{f_0(x)+f_1(x)i+f_2(x)j + f_3(x)k \mid f_\alpha(x) \in \wp_q\}$ with seven subsets $L_f, L_\varphi, L_\alpha, L_w, L_r$, and L_g of the quaternion algebra $\mho$ which are defined as follows:
$L_f = \big\{f_0(x) + f_1(x)i + f_2(x)j + f_3(x)k \in \mho \mid f_\alpha(x) \in \wp$, where f_α has d_f coefficient equal to $+1, (d_f - 1)$ equal -1, the rest $0\big\}$,
$L_\varphi = \big\{\varphi_0(x) + \varphi_1(x)i + \varphi_2(x)j + \varphi_3(x)k \in \mho \mid \varphi_\alpha(x) \in \wp,\ \varphi_\alpha$ has d_φ coefficients equal to $+1, d_\varphi$ equal to -1 , the rest $0\big\}$,
$L_m = \big\{m_0(x) + m_1(x)i + m_2(x)j + m_3(x)k \in \mho \mid$ coefficients of m are chosen modulo p , between $-p/2$ and $p/2\big\}$. The subsets L_φ and L_w are defined as L_f, and the subsets L_α, L_r, and L_g are defined as L_φ.
HAQTR is designed through three main phases as follows:

2.1 Key generation Phase

The recipient should create the public keys by choosing four polynomials, $g \in L_g,\ w \in L_w,\ \varphi \in L_\varphi$ and, $f \in L_f$. The public keys h and k compute by the formulas $h = {f^{-1}}_q * g(mod\ q)$ and $k = w * {\varphi^{-1}}_q(mod\ q)$.

2.2 Encryption Phase

In this phase, the sender converts a message from plaintext to ciphertext by using quaternion algebra form and the following encrypt equation $e = p(h * r + \alpha) + m * k(mod\ q)$ where $r \in L_r$ and $\alpha \in L_\alpha$.

2.3 Decryption Phase

The recipient should find

$$\begin{aligned} a &= f * e * \phi \ (mod\ q) \\ &= p(f * {f^{-1}}_q * g * r * \phi + f * \alpha * \phi) + f * m * w(mod\ q) \\ &= p(g * r * \phi + f * \alpha * \phi) + f * m * w(mod\ q). \end{aligned}$$

When we replace $(mod\ q)$ to $(mod\ p)$, we obtain

$$\begin{aligned} b = a(mod\ p) = f * m * w(mod\ p) \\ {f^{-1}}_p * b * {w^{-1}}_p = m(mod\ p). \end{aligned}$$

The resulting coefficients are adjusted to lie in the interval $(-p/2,\ p/2]$.

3 Analysis of HAQTR

The security of HAQTR relies on the size of the space of the subsets L_g and L_w. The larger the size of the set, the more attempts to uncover the key, where the size of the space of keys g and w is equal to $\left(\frac{(N!)^2}{(d_g!d_w!)^2(N-2d_g)!(N-2d_w)!}\right)^4$, and the size of the space of message is equal to $\left(\frac{(N!)^2}{(d_r!d_\alpha!)^2(N-2d_r)!(N-2d_\alpha)!}\right)^4$. The execution time of HAQTR depends on the number of operations in the three phases key generation, encryption and decryption which are equal to $448t + 16t_1$ where t is the multiplication times and t_1 is the addition times.

4 Conclusion

In this work, we proposed a HAQTR multidimensional cryptosystem which was more secure than NTRU but slower than it. When the public key $k = 1$, the private key $\alpha = 0$, and the coefficients of $i,\ j,\ k = 0$, we get NTRU. This means that NTRU public key cryptosystem is a special case of HAQTR which can be used to encrypt multiple messages at the same time.

References

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

[2] S. H. Shihadi, H. R. Yassein, A New Design of NTRU Encrypt-analog Cryptosystem with High Security and Performance Level via Tripternion Algebra, International Journal of Mathematics and Computer Science, **16,** no. 4, (2021), 1515–1522.

[3] S. H. Shahhadi, H. R. Yassein, NTRsh: A New Secure Variant of NTRU-Encrypt Based on Tripternion Algebra, Journal of Physics: Conference Series, **1999,** (2021), 1–6.

[4] H. H. Abo-Alsood, H. R. Yassien, Design of an Alternative NTRU Encryption with High Secure and Efficient, International Journal of Mathematics and Computer Science, **16,** no. 4, (2021), 1469–1477.

[5] H. R. Yassein, H. A. Ali, HUDTRU: An Enhanced NTRU for Data Security via Quintuple Algebra, International Journal of Mathematical and Computer Science, **18,** no. 2, (2023), 199–204.

[6] J. H. Conway, D. A. Smith, On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry, A. K. Peters, Ltd., 2003.