Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 29 (2026), No. 5, pp. 2063–2068
DOI : 10.47974/JDMSC-2677

UQTRU cryptosystem via unit complex numbers

Fatima AbdAljwad Abdalla Alathari *
Intissar Abdulhur Kadum †
Department of Mathematics
Faculty of Education for Women
University of Kufa
Kufa
Iraq

Abstract

This work presents a novel cryptosystem, UQTRU, based on the QTRU cryptosystem, using truncated polynomial rings whose coefficients are roots of unity. This multidimensional public key cryptosystems be the base on a quaternion algebra of $W_n[z]/(z^N-1); n \in N$.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Quaternions algebra, NTRU, QTRU, UQTRU.*

1. Introduction

In recent years, wireless communications have developed and spread widely, and security has become a critical issue. Encryption has emerged as an optimal solutions to these problems, which has necessitated emergence for many public-key encryption system since the presentation of the fundamental Diffie and Hellman [1] paper In 2022, through the proposed NTRU public key by Hoffstein, Pipher, and Silverman [2] cryptosystem, which relied on the lattice problem rather than numbers, using truncated polynomials with integer coefficients. NTRU plays an important role because it offers high speed and requires less memory than public-key cryptosystems, making it a suitable choice for data transmission. In 2011, the author studied the QTRU cryptosystem based on quaternion algebra [3]. Many authors have studied different concepts in algebra and topology, see [4-10].

Definition 1: The rotation of the complex plane about the origin can be parametrized by the angle measure θ and identified with the imaginary line in the complex plane $\{\theta i : \theta \in \mathbb{R}\}$ The exponential map for this group is given by

* *E-mail:* fatimaa.alathari@student.uokufa.edu.iq (Corresponding Author)
† *E-mail:* intesara.kadhim@uokufa.edu.iq

© Taru Publications

$$\theta i \to \omega = e^{i\theta} = \cos(\theta) + isin(\theta)$$

For any $\in \mathbb{N}$, the unit circle $\omega = e^{\frac{2\pi}{n}i}$, the group of unit complex numbers is called a cyclic group and denoted by $\mathcal{W}_n$.

Definition 2: Let (, +′, .′) be a ring with $\mathcal{W}_n$ = {ω^0 = 1, ω^1, ω^2, …, ω^{n-1}} where $\omega = e^{\frac{2\pi}{n}i}$, n is an integer number, addition and multiplication are defined as:

$$\omega^{k_1} +' \omega^{k_2} = \omega^{k_1+k_2 mod\ n}; 0 \le k_1, k_2 \le n-1$$

and

$$\omega^{k_1} .' \omega^{k_2} = \omega^{k_1.k_2 mod\ n}; 0 \le k_1, k_2 \le n-1$$

The zero element $\omega^0 = 1$ does not have the multiplicative inverse.

In this ring ($\mathcal{W}_n$, +′, .′), the char($\mathcal{W}_n$) is the smallest positive number n such that:

$$\omega . \omega . \omega . \ldots = \omega^n = 1$$

when p is a prime number then ($\mathcal{W}_p$, +′, .′) is a field.

2. Main Results

Definition 2.1: Let $\mathbb{C}$ be a complex field. Then, the quaternion algebra $\mathcal{A}$ defined over $\mathbb{C}$ is illustrated in Tables 1 and 2:

$$\mathcal{A} = (\frac{2\pi,2\pi}{\mathbb{C}}) = \{q = \sigma + \rho i + \theta j + \mu k \backslash \sigma, \rho, \theta, \mu \in \mathbb{C}, i^2 = 2\pi, j^2 = 2\pi, ij = k = -ji\},$$

Table 1

Addition table of the elements 1, i, j, k in the quaternion algebra A

+	$1 = 2\pi$	$i = \frac{\pi}{2}$	$j = \pi$	$i = \frac{3\pi}{2}$
1	1	*k*	*j*	*i*
$i = \frac{\pi}{2}$	*k*	*j*	*i*	1
$j = \pi$	*j*	*i*	*1*	*k*
$k = \frac{3\pi}{2}$	*k*	*j*	*i*	*1*

Table 2

Addition table of elements 1, i, j, k (mod 2π)

.	$1 = 2\pi$	$i = \frac{\pi}{2}$	$j = \pi$	$k = \frac{3\pi}{2}$
1	1	*k*	*j*	*i*
$i = \frac{\pi}{2}$	*i*	*1*	*k*	*j*
$j = \pi$	*j*	*i*	*1*	*k*
$k = \frac{3\pi}{2}$	*k*	*j*	*i*	*1*

The set $\{1, i, j, k\}$ is basis for $\mathcal{A}$ (i.e. $\mathcal{A}$ is algebra of four dimensions).

Now, consider three quaternion algebra $\mathcal{A}$, $\mathcal{A}_p$ and $\mathcal{A}_q$ as follows:

$$\mathcal{A} = \{\alpha_0(z) + \alpha_1(z)i + \alpha_2(z)j + \alpha_3(z)k \,|\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathcal{W}_n[z]/(z^N - 1)\}$$

$$\mathcal{A}_p = \{\beta_0(z) + \beta_1(z)i + \beta_2(z)j + \beta_3(z)k \,|\beta_0, \beta_1, \beta_2, \beta_3 \in \mathcal{W}_p/(z^N - 1)\}$$

$$\mathcal{A}_q = \{\sigma_0(z) + \sigma_1(z)i + \sigma_2(z)j + \sigma_3(z)k \,|\sigma_0, \sigma_1, \sigma_2, \sigma_3 \in \mathcal{W}_q/(z^N - 1)\}.$$

Assume that

$q_1, q_2 \in \mathcal{A}_p$ or $\mathcal{A}_q$, $q_1 = \alpha_0(z) + \alpha_1(z)i + \alpha_2(z)j + \alpha_3(z)k$ and $q_2 = \beta_0(z) + \beta_1(z)i + \beta_2(z)j + \beta_3(z)k$, then the addition and multiplication of the two-quaternion defined as following:

$$q_1 \acute{+} q_2 = (\alpha_0(z) \acute{+} \beta_0(z)) + (\alpha_1(z) \acute{+} \beta_1(z))i + (\alpha_2(z) \acute{+} \beta_2(z))j + (\alpha_3(z) \acute{+} \beta_3(z))k.$$

$$q_1 \acute{\cdot} q_2 = (\alpha_0(z) \acute{*} \beta_0(z) \acute{-} \alpha_1(z) \acute{*} \beta_1(z) \acute{-} \alpha_2(z) \acute{*} \beta_2(z) \acute{-} \alpha_3(z) \acute{*} \beta_3(z)) +$$
$$(\alpha_0(z) \acute{*} \beta_1(z) \acute{+} \alpha_1(z) \acute{*} \beta_0(z) \acute{-} \alpha_3(z) \acute{*} \beta_2(z) \acute{+} \alpha_2(z \acute{*} \beta_3(z))i +$$
$$(\alpha_3(z) \acute{*} \beta_1(z) \acute{+} \alpha_2(z) \acute{*} \beta_0(z) \acute{+} \alpha_0(z) \acute{*} \beta_2(z) \acute{-} \alpha_1(z) \acute{*} \beta_3(z))j +$$
$$(\alpha_1(z) \acute{*} \beta_2(z) \acute{+} \alpha_0(z) \acute{*} \beta_3(z) \acute{-} \alpha_2(z) \acute{*} \beta_1(z) \acute{+} \alpha_3(z) \acute{+} \alpha_0\beta_0(z))k,$$

Where, $\acute{+}$, $\acute{\cdot}$ and $\acute{*}$ denotes the convolution product on $\mathcal{W}_n[z]$ as

$$\alpha_0(z) \acute{+} \beta_0(z) = \left(w_n^{a_0} +' w_n^{b_0}\right) + \cdots + \left(w_n^{N} +' w_n^{b_N}\right) z^n$$
$$= w_n^{a_0 + b_0} + \cdots + w_n^{a_{N-1} + b_{N-1}} z^{N-1}$$

when k^{th} coefficient w^{δ_k} is

$$\delta_k = \sum_{k=0}^{N-1} \sum_{j=k}^{N-1} a_j \,.\, b_{k-j}$$

$$\alpha_0(z) \acute{*} \beta_0(z) = \sum_{k=0}^{N-1} w_p^{\alpha k \,.\beta k \bmod n} z^k$$

so quaternion algebra be the alternative, associatives, but non-commutatives.

A conjugate $\overline{q_1}$ norm $N(q_1)$ and multiplicative inverse q_1^{-1} of q_1 are defined as follows:

$\overline{q_1} = \alpha_0(z) - \alpha_1(z)i - \alpha_2(z)j - \alpha_3(z)k$,

$N(q_1) = \alpha_0(z)^2 + \alpha_1(z)^2 + \alpha_2(z)^2 + \alpha_3(z)^2$,

$q_1^{-1} = \frac{\overline{q_1}}{N(q_1)} = (\alpha_0(z)^2 + \alpha_1(z)^2 + \alpha_2(z)^2 + \alpha_3(z)^2)^{-1}(\alpha_0(z) - \alpha_1(z)i - \alpha_2(z)j + \alpha_3(z)k$, where $N(q_1) \neq 0$.

Proposed Scheme of UQTRU 2.2:

The UQRTU public key cryptosystem depends on parameters N, p, q have the same properties in UNTRU and the subsets $l_{\mathcal{F}}, l_g, l_r, l_m \subset \mathcal{A}$ consists of all polynomials in the quaternion algebra that are described in the table 3:

Table 3

Polynomial subsets in the quaternion algebra used in the UQTRU cryptosystem

Notation	Definition
$l_{\mathcal{F}}$	$\{\mathcal{F}_0(z)+\mathcal{F}_1(z)i+\mathcal{F}_2(z)j+\mathcal{F}_3(z)k \in \mathcal{A} \mid \mathcal{F}_i \in \mathcal{W}_n[z]/(z^N-1); n>2$ has $d_{\mathcal{F}}$ coefficients equal to w^{+1}, $(d_{\mathcal{F}}-1)$ equal to w^{-1}, the rest $w^0=1\}$
$l_{\mathcal{g}}$	$\{\mathcal{g}_0(z)+\mathcal{g}_1(z)i+\mathcal{g}_2(z)j+\mathcal{g}_3(z)k \in \mathcal{A} \mid \mathcal{g}_i \in \mathcal{W}_n[z]/(z^N-1); n>2$ has $d_{\mathcal{g}}$ coefficients equal to w^{+1}, $d_{\mathcal{g}}$ equal to w^{-1}, the rest $w^0=1\}$
l_r	$\{r_0(z)+r_1(z)i+r_2(z)j+r_3(z)k \in \mathcal{A} \mid r_i \in \mathcal{W}_n[z]/(z^N-1); n>2$ has d_r coefficients equal to w^{+1}, d_r equal to w^{-1}, the rest $w^0=1\}$
l_m	$\{m_0(z)+m_1(z)i+m(z)j+m_3(z)k \in \mathcal{A} \mid$ coefficients of $m_i \in \mathcal{W}_n[z]/(z^N-1)\,; n>2$ is chosen modulo between $w^{-p/2} and\, , w^{p/2}\}$

UQTRU Phases 2.3:

The constructions for the UQTRU cryptosystems can describ as:

1) Key Generation:

key generated in the UQTRU by selecting a quaternions $\mathcal{F}$ & $\mathcal{g}$ s.t, $\mathcal{F}$ has inverses on $\mathcal{W}_p$ & $\mathcal{W}_q$ denoted by $\mathcal{F}_{w^p}^{-1}$ and $\mathcal{F}_{w^q}^{-1}$ and is calculated by the following:

$$\hbar = \mathcal{F}_{w^q}^{-1} * \mathcal{g} (mod\ w^q)$$

The quaternion $\mathcal{F}$, $\mathcal{F}_{w^q}^{-1}$and $\mathcal{F}_{w^p}^{-1}$ are the private keys.

2) Encryption:

Initially, a random quaternion $r \in l_r$ generated, which is called the blinding quaternion. The input message must be written quaternion form

$$m = m_0 + m_1 i + m_2 j + m_3 k \in l_m.$$

The ciphertext e is $e = w^p \hbar \circledast r \dot{+} m$.

Encryption needs one quaternion multiplication, including four polynomial additions with $\mathcal{O}(N)$ complexity, and sixteen convolution multiplications with $\mathcal{O}(N^2)$ complexity.

3) Decryption:

After receiving e, the quaternion $\mathcal{B}$ is calculated by:

$$\begin{aligned}\mathcal{B} = \mathcal{F} \circledast e &= \mathcal{F} \circledast (w^p \hbar \circledast r \dot{+} m)\ (mod w^q) \\ &= \mathcal{F} * (w^p\, \mathcal{F}_q^{-1} \circledast \mathcal{g}) * r \dot{+} m)\ (mod\ w^q)\end{aligned}$$

Where the coefficient of all polynomials in the last result lie in the interval $(w^{-q/2}, w^{q/2}\ ]$.

Let

$$\begin{aligned}\mathcal{D} = \mathcal{B}\ (mod\ w^p) &= w^p\, \mathcal{g} \circledast r \dot{+} \mathcal{F} \circledast m (mod\ w^q) \\ &= \mathcal{F} \circledast m\ (mod\ w^q)\end{aligned}$$

By left multiplication form by $\mathcal{F}_{w^p}^{-1}$, we get the original message m such that the resulting coefficients lie in the interval $(w^{-p/2}, w^{p/2}]$.

3. Conclusion

We present novel cryptosystems based on the QTRU cryptosystem, using truncated polynomial rings whose coefficients are roots of unity and are denoted by UQTRU.

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," in *Democratizing cryptography: the work of Whitfield Diffie and Martin Hellman*, pp. 365–390 (2022).

[2] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *International Algorithmic Number Theory Symposium,* Berlin, Heidelberg: Springer, pp. 267–288 (Jun. 1998).

[3] E. Malekian, A. Zakerolhosseini, and A. Mashatan, "QTRU: Quaternionic Version of the NTRU Public-key Cryptosystems,'' *ISC International Journal of Information Security*, vol. 3, no. 1, pp. 29-42 (2011).

[4] R. H. Hilal, N. A. Al-Karamy, and S. N. Jabair, "Derivation a New Numerical Methods to Calculate the Double Integration with Continuous Calls," *Annals of Pure and Applied Mathematics*, vol. 22, no. 2, pp. 125–135 (2020).

[5] A. S. Mohammed, I. S. Ahmed, and S. H. Asaad, "Study of the rings in which each element express as the sum of an idempotent and pure," *Int. J. Nonlinear Anal. Appl,* vol. 12, no. 2, pp. 1719-1724 (2021), doi: 10.22075/IJNAA.2021.5311.

[6] A. Al-Fayadh, A. J. Hussain, P. Lisboa, and D. Al-Jumeily, "Novel hybrid classified vector quantization using discrete cosine transform for image compression," *Journal of Electronic Imaging*, vol. 18, no. 2, pp. 023003–023003 (2009).

[7] Z. T. Abdulqader, S. H. Khalil, and M. H. Hadi, "Graph strongly by Qpre-closed set-in topological spaces," *Journal of Interdisciplinary Mathematics,* vol. 25, no. 6, pp. 1829–1834 (2022).

[8] I. A. Kadum, W. G. Atshan, and A. T. Hameed, "Sandwich theorems for a new class of complete homogeneous symmetric functions by using cyclic operator," *Symmetry,* vol. 14, no. 10, p. 2223 (2022), doi: 10.3390/sym14102223.

[9] S. H. Asaad, I. S. Ahmed, and H. H. Ebrahim, "On Finitely Null-additive and Finitely Weakly Null-additive Relative to the σ–ring," *Baghdad Sci. J,* vol. 19, no. 5, pp. 1148-1154 (2022).

[10] A. Mersin, "The comparative performance analysis of lattice based NTRU cryptosystem with other asymmetrical cryptosystems," MS thesis, Graduate School of Engineering and Science, Izmir Institute of Technology, Izmir, Turkey, pp. 1–60 (2007).

Received November, 2025