International Journal of Mathematics and
Computer Science, **18**(2023), no. 4, 589–593

TRUFT: A New Public Key Cryptosystem Based on Novel FTH Algebra

Hiba Shakir Salman[1], **Hassan Rashed Yassein**[2]

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

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

email: hibas.alwadi@student.uokufa.edu.iq, hassan.yaseen@qu.edu.iq

(Received January 2, 2023, Accepted February 23, 2023,
Published May 31, 2023)

Abstract

Given the increase in the various types of transactions over the Internet and to ensure the confidentiality of the transmitted data, there is need for encryption with the continued development of cryptosystems. In this paper, we offer TRUFT, a multi-dimensional public key cryptosystem, as a replacement for the NTRU encryption with a new structure that increases complexity and security.

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

1 Introduction

The Nth degree truncated polynomial ring unit (NTRU) public key cryptosystem was established in 1996 by Hoffstein et al. [1]. In 2010, Malekian and Zakerolhsooeini [2] presented a cryptosystem called OTRU, based on octonions algebra. In 2016, Yassein and Al-Saidi [3] introduced HXDTRU that depends on the hexadecnion algebras. In 2018, they also presented another multidimensional analog to NTRU, called BCTRU, using Bicartesian algebra [4]. In 2020, Yassein et al. [5] offered a Carternion algebra to build a new cryptosystem which was named QMN$_{\text{TRU}}$. In the same year, Yassein et al. [6] introduced a new NTRU alternative cryptosystem called NTRTE that depends on a commutative quaternion algebra with a new multi-dimensional structure. In 2021, Yassein et al. [7] designed a new version of NTRU by improving QTRU based on a new mathematical structure called QMNTR. In 2021, Shihadi and Yassein [8] introduced a new analog NTRU that uses Tripternion algebra and has good security and performance levels.

2 FTH Algebra

If FTH $= \{(h_1, h_2)(1,1) + (h_3, h_4)(\propto, \propto) | h_i \in F, \forall i = 1,2,3,4\}$ is defined over F such that F is a field with $Char(F) \neq 2$, then its algebra is called the FTH algebra, where $\{(1,1), (\propto, \propto)\}$ is a basis with the operations addition, multiplication, and scalar multiplication defined as follows:
Let $D_1, D_2 \in$ FTH such that
$D_1 = \{(k_1, k_2)\,(1,1) + (k_3, k_4)\,(\propto, \propto) | k_1, \ \ldots, k_4 \in F\}$ and
$D_2 = \{(t_1, t_2)\,(1,1) + (t_3, t_4)\,(\propto, \propto)\,| t_{1,} \ldots, t_4 \in F\}$,
$D_1 + D_2 = \ (\ k_1 + t_1, k_2 + t_2)\,(1,1) + (k_3 + t_3, k_4 + t_4)\,(\propto, \ \propto)$,
$D_1 * D_2 = (k_1\ t_1 + k_4 t_4\ , k_2\ t_2 + k_3 t_3)\,(1,1) + (k_2\ t_3 + k_3 t_2\ , k_1 t_4 + k_4 t_1)(\propto\ , \propto)$,
(this multiplication is associative and commutative),
$\alpha D_1 = (\alpha k_0, \alpha k_1)(1,1) + (\alpha k_2, \alpha k_3)(\propto, \propto)$
$D_1^{-1} = (\frac{k_1}{k_1^2 - k_4^2}, \frac{k_2}{k_2^2 - \ k_3^2})\,(1,1) + (\frac{k_3}{k_3^2 - \ k_2^2}\ , \frac{k_4}{k_4^2 - \ k_1^2})\,(\propto, \ \propto)$,
where the identity multiplication is known by $\mathrm{I} = (1,1)\,(1,1) + (0,0)\,(\propto\ , \propto)$.

3 TRUFT Cryptosystem

Suppose $\varphi = Z[x]/(x^N - 1), \varphi_p = Z_p[x]/(x^N - 1)$, and $\varphi_q = Z_q[x]/(x^N - 1)$ are three truncated polynomial rings relying on the TRUFT cryptosystem. Subsequently, three FTH algebras ß, ß$_p$ and ß$_q$ are defined as follows:

$\text{ß} = \{(\mho_1, \mho_2)\,(1,1) + (\mho_3, \mho_4)\;(\propto, \propto)\,|\mho_1, \ldots, \mho_4 \in \varphi\}$,
$\text{ß}_p = (\mho_1, \mho_2)\,(1,1) + (\mho_3, \mho_4)\,(\propto, \propto)\,|\mho_1, \ldots, \mho_4 \in \varphi_p\}$ and
$\text{ß}_q = \{(\mho_1, \mho_2)\,(1,1) + (\mho_3, \mho_4)\,(\propto, \propto)\,|\mho_1, \ldots, \mho_4 \in \varphi_q\}\,.$

3.1 Public Parameters

The parameters of the TRUFT cryptosystem consist of integers N, p, and q, similar to those of NTRU and the subsets $T_{\mathfrak{F}}, T_{\mathfrak{G}}, T_{\mathcal{Q}}\;, T_{\mathfrak{U}}, T_{\mathcal{J}}, T_{\mathfrak{D}}, T_{\mathfrak{R}}$ and $T_{\mathfrak{M}}$ such that:
$T_{\mathfrak{F}} = \{\mathfrak{F} = (\mathfrak{f}_1, \mathfrak{f}_2)(1,1) + (\mathfrak{f}_3, \mathfrak{f}_4)(\propto, \propto) \in \text{ß}|\mathfrak{f}_i \in \varphi,\ i = 1,2,3,4\,\text{satisfy}\,\ell(d_{\mathfrak{f}},\ d_{\mathfrak{f}} - 1)\}$,
$T_{\mathfrak{G}} = \big\{\mathfrak{G} = (\mathfrak{g}_1, \mathfrak{g}_2)\,(1,1) + (\mathfrak{g}_3, \mathfrak{g}_4)\,(\propto, \propto) \in \text{ß}|\mathfrak{g}_i \in \varphi, i = 1,2,3,4\ \text{satisfy}\ \ell\,(d_{\mathfrak{g}},\ d_{\mathfrak{g}})\,\big\}$,
$T_{\mathcal{J}}, T_{\mathfrak{U}}$, and $T_{\mathcal{O}}$ are defined similar to $T_{\mathfrak{F}}$ and
$T_{\mathfrak{G}}, T_{\mathcal{Q}}, T_{\mathfrak{D}}, T_{\mathfrak{R}}$ are defined similar to $T_{\mathfrak{G}}$.
In addition, $T_{\mathfrak{M}} = \big\{\mathfrak{M} = (\mathfrak{m}_1, \mathfrak{m}_2)(1,1) + (\mathfrak{m}_3, \mathfrak{m}_4)(\propto, \propto) \in \varphi|$ with coefficients of $\mathfrak{m}_i \in \varphi, i = 1,2,3,4$, $\mathfrak{m}_i$ are chosen modulo between $-p/2$ and $p/2\big\}$ with $\ell(d_x, d_y) = \big\{\mathfrak{F} \in \varphi :\ \mathfrak{F}$ has d_x with coefficients equal 1, d_y coefficients equal -1, and the remaining equal $0\big\}$.

3.2 TRUFT Phases

This cryptosystem consists of the following phase:

I. **Key Creation**
Here, we will choose six polynomials $\mathfrak{F} \in T_{\mathfrak{F}},\ \mathfrak{G} \in T_{\mathfrak{G}},\ \mathcal{Q} \in T_{\mathcal{Q}}\ ,\ \mathcal{O} \in T_{\mathcal{O}}\ ,\ \mathfrak{U} \in T_{\mathfrak{U}}$, and $\mathcal{J} \in T_{\mathcal{J}}$ to construct the keys $\mathcal{B}$ and $\mathcal{H}$ by the following formula:
$\mathcal{B}\ = \mathfrak{F}_q^{-1} * \mathfrak{G} * \mathcal{Q}\,(mod\ q)\,, \mathcal{H} = \mathcal{O} * \mathfrak{U} *\ \mathcal{J}_q^{-1}\ (mod\ q)\,.$

II. **Encryption**
Once the original message $\mathfrak{M}$ has been converted to FTH algebra, we choose two random polynomials $\mathfrak{D} \in T_{\mathfrak{D}}$ and $\mathfrak{R} \in T_{\mathfrak{R}}$ and calculate E by the formula:
$E = p\,(\mathcal{B} * \mathfrak{D} + \mathfrak{R}) + \mathfrak{M} * \mathcal{H}\,(mod\ q)\,.$

III. **Decryption**
After receiving the ciphertext, the recipient can get the original message through the following process:
$\mathcal{X} = \mathfrak{F}\ * E * \mathcal{J}\,mod\,q = \mathfrak{F} * (p\,(\mathcal{B} *\ \mathfrak{D} + \mathfrak{R}) + \mathfrak{M} * \mathcal{H}) * \mathcal{J}\ (mod\ q)$ such that the coefficient lies in the interval $(-q/2,\ q/2]$.

Converting $\mathcal{X} = p\,(\mathfrak{S} * \mathcal{Q} * \mathfrak{D} * \mathcal{J}) + (p\mathfrak{F} * \mathfrak{R} * \mathcal{J}) + \mathfrak{F} * (\mathfrak{M} * (\mathcal{O} * \mathfrak{U} * \ \mathcal{J}_q^{-1})) * \mathcal{J} \ \ (mod\ q)$ modulo $p:$
$\mathcal{X}$ (mod p) $= p\,(\mathfrak{S} * \mathcal{Q} \ * \mathfrak{D} * \mathcal{J}) + (p\mathfrak{F} * \mathfrak{R} * \mathcal{J}) + \mathfrak{F} * \mathfrak{M} * \mathcal{O} * \mathfrak{U}$ (mod p) $= \mathfrak{F} * \mathfrak{M} * \mathcal{O} * \mathfrak{U}$ (mod p). Hence ${\mathfrak{F}_p}^{-1} * \mathcal{X} * \mathfrak{U}_p^{-1} * \mathcal{O}_p^{-1} = \mathfrak{M}$ (mod p) and the resulting coefficients are adjusted to lie in the interval $(-p/2, p/2]$.

4 Security Analysis

An attacker will search for the private keys $\mathfrak{S}, \mathcal{Q}, \mathfrak{U}$, and $\mathcal{O}$ from the sets $T_{\mathfrak{S}}, T_{\mathcal{Q}}, T_{\mathfrak{U}}$, and $T_{\mathcal{O}}$, respectively. The sizes of the subsets $T_{\mathfrak{S}}, T_{\mathcal{Q}},\ T_{\mathfrak{U}}$, and $T_{\mathcal{O}}$ are equal to:
$|T_{\mathfrak{S}}| = \left(\frac{N!}{\left(d_{\mathfrak{g}!}\right)^2 (N-2d_{\mathfrak{g}})!}\right)^4, |T_{\mathcal{Q}}| = \left(\frac{N!}{(d_{\mathrm{II}!})^2 (N-2d_{\mathrm{II}})!}\right)^4,$
$|T_{\mathfrak{U}}| = \left(\frac{N!}{(d_{\mathfrak{u}!})^2 (N-2d_{\mathfrak{u}})!}\right)^4$, and $|T_{\mathcal{O}}| = \left(\frac{N!}{\left(d_{\wr!}\right)^2 \left(N-2d_{\wr}\right)!}\right)^4.$
Consequently, the key security is $\left(\frac{(N!)^{16}}{\left(d_{\mathrm{II}}!\ d_{\mathfrak{u}!} d_{\wr!} d_{\mathfrak{g}!}\right)^8 \left((N-2d_{\mathrm{II}})!(N-2d_{\mathfrak{u}})!\ \left(N-2d_{\wr}\right)!(N-2d_{\mathfrak{g}})!\right)^4}\right)^{\frac{1}{2}}.$
An attacker can get the original text from the ciphertext by searching for $\mathfrak{D} \in T_{\mathfrak{D}}$ and $\mathfrak{R} \in T_{\mathfrak{R}}$. The sizes of the subsets $T_{\mathfrak{D}}$ and $T_{\mathfrak{R}}$ are equal to:
$|T_{\mathfrak{D}}| = \left(\frac{N!}{\left(d_{\lceil!}\right)^2 \left(N-2d_{\lceil}\right)!}\right)^4, |T_{\mathfrak{R}}| = \left(\frac{N!}{(d_{\mathfrak{r}!})^2 (N-2d_{\mathfrak{r}})!}\right)^4.$

Consequently, the size of the security message is $\left(\frac{(N!)^8}{\left(d_{\lceil}!d_{\mathfrak{r}}!\right)^8 \left(\left(N-2d_{\lceil}\right)!(N-2d_{\mathfrak{r}})\right)^4}\right)^{\frac{1}{2}}.$

5 Conclusion

TRUFT is based on a new commutative and associative FTH algebra, with good security and speed when compared to some of NTRU advancements. This functionality can be very helpful in creating protocols or other applications of this type because it can encrypt four different messages from one source or from many sources.

References

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

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

[3] 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).

[4] H. R. Yassein, N. M. G. Al-Saidi, BCTRU: A New Secure NTRUCrypt Public Key System Based on a Newly multidimensional Algebra, Proceedings of the 6th International Cryptology and Information Security Conference, Malaysia, (2018).

[5] H. R. Yassein, N. M. Al-Saidi, A. K. Farhan, A New NTRU Cryptosystem Outperforms Three Highly Secured NTRU-Analog Systems through an Innovation Algebraic Structure, Journal of Discrete Mathematical Sciences and Cryptography, **23**, no. 2, (2020), 1–20.

[6] 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.

[7] H. R. Yassein, A. A. Abidalzahra, N. M. G. Al-Saidi, A New Design of NTRU Encryption with High Security and Performance Level, AIP Conference Proceedings, (2021), 080005-1 - 080005-4.

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