International Journal of Mathematics and
Computer Science, **19**(2024), no. 3, 715–719

Proposed Development of NTRU Encryption

Asia Aqeel Abidalzahra, Hassan Rashed Yassein

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

email: asia1asia21998@gmail.com, hassan.yaseen@qu.edu.iq

(Received December 1, 2023, Accepted January 9, 2024,
Published February 12, 2024)

Abstract

In this work, we present an improvement to NTRU called ASTRU which is based on a new algebra called AS and a new mathematical structure. It was created in a way to increase the security of keys and it outperforms NTRU, QTRU, and QMNTR.

1 Introduction

In 1996, Hoffstein et al. presented a public key cryptosystem called NTRU with effective performance [1]. This feature has encouraged researchers to improve it. In 2009, Malekian et al. introduced a cryptosystem called QTRU which depends on the quaternion algebra [2]. In 2018, Yassein and Al-saidi presented BCTRU based on the bi-cartesisn algebra [3]. In 2021, by creating a novel mathematical structure, Yassein et al. established an analog QTRU cryptosystem, known as QMNTR [4]. In 2021, Yassein et al. presented NTRS and BOTR via tripternion algebra and bi-octonion subalgebra [5, 6]. In this paper, we introduce the ASTRU multidimensional public key cryptosystem. We demonstrate that ASTRU outperforms NTRU, QTRU, and QMNTR in terms of security.

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

2 AS Algebra

In this section, we introduce AS algebra. Let $\mathbb{F}$ be a field. Define AS algebra as follows:
$AS = \left\{\sum_{i=0}^{6} a_i\beta_i | a_i \in \mathbb{F}, i = 0, 1, \ldots, 6\right\}$, where $\{1, \beta_1, \beta_2, \beta_3, \beta_4, \beta_5, \beta_6\}$ is basis. Assume that $\mathcal{A}, \mathcal{B} \in AS$ such that $\mathcal{A} = a_0 + \sum_{i=1}^{6} a_i\beta_i, \mathcal{B} = b_0 + \sum_{i=1}^{6} b_i\beta_i$. We define addition, multiplication, scalar multiplication, identity, and inverse of a non-zero element by:
$\mathcal{A} + \mathcal{B} = (a_0 + b_0) + \sum_{i=1}^{6} (a_i + b_i)\beta_i, \mathcal{A} \circledast \mathcal{B} = (a_0 \circledast b_0) + \sum_{i=1}^{6} (a_i \circledast b_i)\beta_i$, $\lambda\mathcal{A} = \lambda a_0 + \sum_{i=1}^{6} (\lambda a_i)\beta_i; \lambda \in \mathbb{F}, I = 1 + \beta_1 + \beta_2 + \beta_3 + \beta_4 + \beta_5 + \beta_6$, and $\mathcal{A}^{-1} = a_0^{-1} + \sum_{i=0}^{6} a_i^{-1}\beta_i$, respectively.
It is clear that AS is associative and commutative.

3 Proposed ASTRU Cryptosystem

Let $\mathfrak{R} = Z[x]/(x^N - 1)$, $\mathfrak{R}_p = Z_p[x]/(x^N - 1)$, and let $\mathfrak{R}_q = Z_q[x]/(x^N - 1)$ be truncated polynomials rings, where p and q are relatively prime and N is positive integer number. Now, we define three algebras $\vartheta = \left\{\sum_{i=0}^{6} f_i\beta_i; f_i \in \mathfrak{R}\right\}$, $\vartheta_p = \left\{\sum_{i=0}^{6} f_i\beta_i; f_i \in \mathfrak{R}_p\right\}, \vartheta_q = \left\{\sum_{i=0}^{6} f_i\beta_i; f_i \in \mathfrak{R}_q\right\}$ and six subsets $\mathcal{L}_\mathcal{F}, \mathcal{L}_\mathcal{G}$, $\mathcal{L}_\mathcal{S}, \mathcal{L}_\mathcal{U}, \mathcal{L}_\mathcal{V}, \mathcal{L}_\mathcal{M} \subset \vartheta$ such that $\mathcal{L}_\mathcal{F} = \{\mathcal{F} \in Q | \mathcal{F}$ has $d_\mathcal{F}$ coefficients equal 1, $(d_\mathcal{F} - 1)$ equal -1, and 0 for the other values $\}$, $\mathcal{L}_\mathcal{G} = \{\mathcal{G} \in \vartheta | \mathcal{G}$ has $d_\mathcal{G}$ coefficients equal 1, $d_\mathcal{G}$ equal -1, and 0 for the other values$\}$. The subset $\mathcal{L}_\mathcal{S}$ is defined similar to $\mathcal{L}_\mathcal{F}$ and the subsets $\mathcal{L}_\mathcal{U}, \mathcal{L}_\mathcal{V}$ are defined similar to $\mathcal{L}_\mathcal{G}, \mathcal{L}_\mathcal{M} = \{\mathcal{M} \in \vartheta|$ with the coefficients of $\mathcal{M}$ are chosen modulo between-$\frac{p}{2}$ and $\frac{p}{2}\}$.

ASTRU can now be described in the following phases:

I. **Key Generation:** To generate the public key, the recipient selects three polynomials $\mathcal{F}, \mathcal{G}$ and $\mathcal{S}$ where $\mathcal{F}$ and $\mathcal{S}$ are both invertible in ϑ_p and ϑ_q. Now, the public key is calculated as follows:
$H = \mathcal{F}_q^{-1} \circledast \mathcal{G} \circledast \mathcal{S}\ mod\ q$. $\mathcal{F}, \mathcal{G}, \mathcal{S}$ is a private key set.

II. **Encryption:** The sender encrypts a message with the following steps: Convert the message to AS algebra form such that $\mathcal{M} = m_0 + \sum_{i=1}^{6} m_i\beta_i$. Two polynomials $\mathcal{U} \in \mathcal{L}_\mathcal{U}$ and $\mathcal{V} \in \mathcal{L}_\mathcal{V}$ are randomly selected. The ciphertext is calculated with the following formula:
$E = p(H \circledast \mathcal{U} + \mathcal{V}) + \mathcal{M}\ mod\ q$.

III. **Decryption:** The recipient will get the original text with the following steps:

Multiply E by $\mathcal{F}$

$$\mathcal{K} = \mathcal{F} \divideontimes E \ mod\ q = p\,(\mathcal{F} \divideontimes (H \divideontimes \mathcal{U} + \mathcal{V})) + \mathcal{F} \divideontimes \mathcal{M} \ mod\ q$$

$$= p\,\big(\ \mathcal{F} \divideontimes ((\mathcal{F}_q^{-1} \divideontimes \mathcal{G} \divideontimes \mathcal{S}) \divideontimes \mathcal{U} + \mathcal{V})\big) + \mathcal{F} \divideontimes \mathcal{M} \ mod\ q$$

$$= p\,((\mathcal{G} \divideontimes \mathcal{S}) \divideontimes \mathcal{U} + \mathcal{F} \divideontimes \mathcal{V}) + \mathcal{F} \divideontimes \mathcal{M} \ mod\ q.$$

All the coefficients in $\mathcal{K}$ should be reduced $mod\ p$. Thus we have $\mathcal{K} = \mathcal{F} \divideontimes \mathcal{M}\ mod\ p$. Therefore, $\mathcal{F}_p^{-1} \divideontimes \mathcal{K} = \mathcal{M}\ mod\ p$. Adjust the resulting coefficients within the interval $(-\frac{p}{2}, \frac{p}{2}]$.

4 Performance Analysis

An attacker can access the original text by knowing two private keys in addition to the known public parameters. If we assume that the size of the subsets $\mathcal{L}_{\mathcal{G}}$ and $\mathcal{L}_{\mathcal{S}}$ are smaller than $\mathcal{L}_{\mathcal{F}}$, then the sizes of the subsets $\mathcal{L}_{\mathcal{G}}$ and $\mathcal{L}_{\mathcal{S}}$ are equal to $|\mathcal{L}_{\mathcal{G}}| = (\frac{N!}{(d_{\mathcal{G}}!)^2(N-2d_{\mathcal{G}})!})^7, |\mathcal{L}_{\mathcal{S}}| = (\frac{N!}{(d_{\mathcal{S}}!)^2(N-2d_{\mathcal{S}})!})^7$. Hence the size of the private key is equal to $\frac{N!}{\big(d_{\mathcal{G}}!d_{\mathcal{S}}!\big)^2\big(N-2d_{\mathcal{G}}\big)!(N-2d_{\mathcal{S}})!})^{14}$.
It is also possible to access the original text through the ciphertext E knowing $\mathcal{U}, \mathcal{V}$. Therefore, the size of the message is equal to $(\frac{N!}{(d_{\mathcal{U}}!d_{\mathcal{V}}!)^2(N-2d_{\mathcal{U}})!(N-2d_{\mathcal{V}})!})^{14}$.

Table 1 shows the comparison among ASTRU and NTRU, QTRU and QMNTR in terms of the sizes of space for the private keys that constitute the public key and the ciphertext which determine the security level of the key and the message, respectively.

Table 1: Key and message space

	Key space	Message space
NTRU	$\frac{N!}{(d_g!)^2(N-2d_g)!}$	$\frac{N!}{(d_{\mathcal{U}}!)^2(N-2d_{\mathcal{U}})!}$
QTRU	$(\frac{N!}{(d_g!)^2(N-2d_g)!})^4$	$(\frac{N!}{(d_{\mathcal{U}}!)^2(N-2d_{\mathcal{U}})!})^4$
QMNTR	$(\frac{N!}{(d_g!d_u!d_s!)^2(N-2d_g)!(N-2d_u)!(N-2d_s)!})^{12}$	$(\frac{N!}{(d_{\mathcal{U}}!d_{\mathcal{V}}!)^2(N-2d_{\mathcal{U}})!(N-2d_{\mathcal{U}}d_{\mathcal{V}})!})^8$
ASTRU	$\frac{N!}{\big(d_{\mathcal{G}}!d_{\mathcal{S}}!\big)^2\big(N-2d_{\mathcal{G}}\big)!(N-2d_{\mathcal{S}})!})^{14}$	$\frac{N!}{(d_{\mathcal{U}}!d_{\mathcal{V}}!)^2(N-2d_{\mathcal{U}})!(N-2d_{\mathcal{V}})!})^{14}$

Table 2 shows the comparison in terms of the time of multiplication convolution and addition in all phases.

Table 2: Time of operations

Cryptosystem	NTRU	QTRU	QMNTR	ASTRU
Time	$4\mathcal{T} + 2\mathcal{T}_1$	$64\mathcal{T} + 8\mathcal{T}_1$	$1248\mathcal{T} + 8\mathcal{T}_1$	$49\mathcal{T} + 28\mathcal{T}_1$,

where $\mathcal{T}$ is the time of convolution multiplication while $\mathcal{T}_1$ is the time of polynomial addition.

5 Conclusion

ASTRU has proven to offer a high level of security when compared to the NTRU, QTRU and QMNTR encryption systems. ASTRU is slower than NTRU and QTRU but the effect of this problem can be reduced by lowering the value of N. However, it is faster than QMNTR with the same parameters.

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, A. Mashatan, QTRU: a lattice attack resistant version of NTRU PCKS based on quaternion algebra, The ISC International Journal of Information Security, **3,** no. 1, (2011), 29–42.

[3] H. R. Yassein, N. M. G. Al-Saidi, BCTRU: A New Secure NTRUCrypt Public Key System Based on a Newly multidimensional Algebra, Proceeding of the 6th International Cryptology and Information Security Conference, Malaysia, (2018), 1–11.

[4] H. R. Yassein, A. A. Abidalzahra, N. M. Al-Saidi, A new Design of NTRU Encryption with High Security and Performance Level, AIP Conference Proceedings, **2334,** no. 1, (2021), pp 080005_1-080005_4.

[5] S. H. Shahhadi, 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.

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