International Journal of Mathematics and
Computer Science, **18**(2023), no. 3, 381–385

SQNTRU: New Public Key Encryption

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 December 21, 2022, Accepted January 21, 2023,
Published March 31, 2023)

Abstract

In this paper, we present a new multidimensional public-key cryptosystem that is commutative and associative based on the subalgebra of Quintuple algebra called S_{QN} which utilizes a novel mathematical structure of two public keys and four private keys. This new structure has made the public key system more secure.

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

1 Introduction

Unlike public-key cryptosystems which are based on the difficulty of integer factorization or the discrete logarithm, NTRU is a public key cryptosystem in the ring of truncated polynomials $Z[x](x^N-1)$ which is one of the public key encryption systems that are capable of providing adequate levels of security at an extremely low cost [1]. Since NTRU was proposed, the original design has undergone numerous improvements. In 2020, Yassein et al. [2] offered a new NTRU-analog cryptosystem based on a new Carternion algebra called QOBTRU. In the same year, Yassein et al. [3] designed a a new multidimensional cryptosystem, called NTRTE, as an alternative to the NTRU cryptosystem. In 2021, Yassein et al. [4] introduced QMTRU which is a new multidimensional public-key cryptosystem with a high-security level. In 2021, Shihadi and Yassein [5] offered a multidimensional public key cryptosystem NTRS using Tripternion algebra. In 2022, Ali and Yassein introduced QTNTR, the multidimensional public key with high security and high speed based on Quintuple algebra [6]. In this paper, we design a new variant of NTRU, called SQNTRU, which is dependent on the subalgebra of Quintuple algebra, which is namely S_{QN} with a new mathematical structure.

2 S_{QN} Subalgebra

Let QU be the real Quintuple algebra
$QU = \{(a_1,b_1)(1,1)+(a_2,b_2)(1,\ i)+(a_3,b_3)(1,j)+(a_4,b_4)(1,k)+(a_5,b_5)(1,h)/a_\delta,b_\delta \in R,\ \delta=1,\ldots,5\}$,
where $\{(1,1),(1,\ i),(1,j),(1,k),(1,h)\}$ forms a basis of this algebra QU.
Consider the subalgebra S_{QN} of QU as a vector space of dimension three over the real numbers R :
$S_{QN} = \{(a_1,b_1)(1,1)+(a_2,b_2)(1,\ i)+(a_3,b_3)(1,j)/a_\delta,b_\delta \in R,\ \delta=1,2,3\}$,
where $\{(1,1),(1,\ i),(1,j)\}$ forms a basis of this subalgebra.

Assume that $\mathcal{F}$ is any finite ring with $\mathrm{char}(\mathcal{F}) \neq 2$. The S_{QN} subalgebra over $\mathcal{F}$ is defined as follows:

$$S_{QN_{\mathcal{F}}} = \{(a_1,b_1)(1,1)+(a_2,b_2)(1,\ i)+(a_3,b_3)(1,j)/a_\delta,b_\delta \in \mathcal{F},\ \delta=1,2,3\}$$

The definitions of addition, multiplication, and inverse multiplication are the same as in the Quintuple algebra [6]. Consider the three truncated polynomial rings $\mathfrak{I} = Z[x]/(x^N-1), \mathfrak{I}_p = Z_p[x]/(x^N-1), \mathfrak{I}_q = Z_q[x]/(x^N-1)$. We can define the S_{QN} subalgebras $\mho$, $\mho_p$, and $\mho_q$ as follows:

$\mho = \{(f_1, f_2)(1,1) + (f_3, f_4)(1,i) + (f_5, f_6)(1,j) / f_\delta \in \Im, \delta = 1, \ldots, 6\}$,
$\mho_p = \{(f_1, f_2)(1,1) + (f_3, f_4)(1,i) + (f_5, f_6)(1,j) / f_\delta \in \Im_p, \delta = 1, \ldots, 6\}$,
$\mho_q = \{(f_1, f_2)(1,1) + (f_3, f_4)(1,i) + (f_5, f_6)(1,j) / f_\delta \in \Im_q, \delta = 1, \ldots, 6\}$.

3 The Proposed SQNTRU Cryptosystem

Depending on the subsets $\mathcal{L}_\mathcal{F}, \mathcal{L}_G, \mathcal{L}_\mathcal{V}, \mathcal{L}_\Upsilon, \mathcal{L}_\vartheta$, and $\mathcal{L}_\mathcal{M} \subset \mho$ such that $\mathcal{L}_\mathcal{F}$ has inverse mod p and q, $\mathcal{L}_G$ has inverse mod q, and $\mathcal{L}_\mathcal{V}$ has an inverse mod p in addition to the parameters adopted in the NTRU and the SQNTRU cryptosystems consisting of the following phases:

Phase 1. Key Generation

To create the public key and the private key, first the receiver chooses randomly four polynomails with small coefficients $\mathcal{F}\epsilon\ \mathcal{L}_\mathcal{F}\ , G\epsilon\mathcal{L}_G, \Upsilon \in \mathcal{L}_\Upsilon$, and $\upsilon\epsilon\mathcal{L}_\upsilon$. The keys are created using the following formulas:
$k_1 = V * G^{-1}\ (mod\ q)$
and $k_2 = \mathcal{F}^{-1} * \Upsilon (mod\ q)$.
The process of creating keys requires twelve convolution multiplications.

Phase 2. Encryption

Initially, the message $\mathcal{M}$ is transformed into a polynomial in $\mathcal{L}_\mathcal{M}$. Thereafter, a blinding polynomial $\vartheta \in \mathcal{L}_\vartheta$ is selected at random. $\mathcal{M}$ is encrypted according to the following formula:
$E = pk_2 * \vartheta + \mathcal{M} * k_1\ (mod\ q)$.
The Encryption phase requires twelve convolution multiplications and six polynomial additions.

Phase 3. Decryption

Once the ciphertext is obtained, the following steps are performed to obtain the original text:
Compute $A_1 = \mathcal{F} * E\ (mod\ q), A_2 = A_1 * G\ (mod\ q)$. Convert A_2 from *mod* q to *mod* p; i.e., $A_3 = A_2 (mod\ p)$ and the coefficients are adjusted to lie in the interval $(\frac{-p}{2}, \frac{p}{2}]$. Now, multiply $A_3$by $\mathcal{F}^{-1}$ from the left; i.e., $A_4 = \mathcal{F}^{-1} * A_3\ (mod\ p)$, and $A_5 = A_1 * V^{-1}\ (mod\ p) = \mathcal{M}$.

The Decryption phase requires eighteen convolution multiplications and six polynomial additions.

4 Security Analysis

The SQNTRU attacker searches the subsets $\mathcal{L}_V$ and $\mathcal{L}_\Upsilon$ to get thr private keys V and Υ in order to retrieve the original message. The size of the subsets $\mathcal{L}_V$ and $\mathcal{L}_\Upsilon$ are $|\mathcal{L}_V| = \binom{N}{d_V}^6 \binom{N-d_V}{d_V}^6$ and $|\mathcal{L}_\Upsilon| = \binom{N}{d_\Upsilon}^6 \binom{N-d_\Upsilon}{d_\Upsilon}^6$. Consequently, the security of the message is equal to $\binom{N}{d_V}^3 \binom{N-d_V}{d_V}^3$, $\binom{N}{d_\Upsilon}^3 \binom{N-d_\Upsilon}{d_\Upsilon}^3$, or it can be searched in the subset for accessing the private key from ciphertext to get the original message. The size of the subsets $\mathcal{L}_\vartheta$ is $|\mathcal{L}_\vartheta| = \binom{N}{d_\vartheta}^6 \binom{N-d_\vartheta}{d_\vartheta}^6$. The security of the message is equal to $\binom{N}{d_\vartheta}^3 \binom{N-d_\vartheta}{d_\vartheta}^3$.

5 Conclusions

In this paper, we detailed a new variant of NTRU called SQNTRU that has some significant advantages in terms of both performance and security when compared to the standard version cryptosystem. SQNTRU is a public key cryptosystem that depends on newly generated triple algebra, which is commutative and associative. The speed of SQNTRU is slower than NTRU but the security of SQNTRU is better than that of NTRU. It is a multi-dimensional cryptosystem that can encrypt six messages from a single source or six different sources. This property is very important for some applications, such as electronic voting or financial transactions.

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] 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.

[3] 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.

[4] 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.

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