Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/170420

TRUHSH: Developing NTRU Cryptosystem in Terms of Security and Performance

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

[1]Department of Mathematics, Faculty of Education for Girls, University of Kufa, Najaf, Iraq
[2]Department of Mathematics, College of Education, University of Al-Qadisiyah, Dewaniyah, Iraq

Received: 17 Mar. 2023, Revised: 1 May 2023, Accepted: 3 Jun. 2023
Published online: 1 Jul. 2023

Abstract: The rapid advancement of technology, the creation of new communication channels, the globalization of some aspects of society, and the reliance on networks for the distribution of different types of data have all increased the risk of information leakage and unauthorized access, making it urgent to maintain information security. In this work, we presented the improvement of the NTRU system, which is still effective, by introducing a new system called TRUHSH based on a new algebra called hexa$_t$, in addition to a new mathematical construction of the encryption stages, while giving high security and efficient performance.

Keywords: NTRU, hexa$_t$ algebra, Security of key, Security of message.

1 Introduction

The need for public key cryptography is growing as many people, organizations and countries use networks to exchange confidential information. Without an effective and secure public key cryptography system, many of these tasks would be impossible to perform. There have been numerous presented public-key cryptosystems based on discrete logarithm and factorization integers. In 1996, Hoffstein et al. introduced a public key cryptosystem NTRU based on rings $Z[x]/(x^N-1)$ [1]. It is quicker and uses considerably smaller keys than RSA and ECC. The possibility of decryption failure is one of NTRU's shortcomings; however, parameters can be selected to reduce or remove this issue. In 2015, AlSaidi et al. using commutative quaternion algebra to proposed the CQTRU multidimensional public key cryptosystem [2]. In 2016 HXDTRU and BITRU, which are defined by the hexadecnion and binary algebras as analogs to the NTRU cryptosystem, were introduced by Yassein and Al-Saidi [3,4,5,6]. BCTRU, an NTRU-like multidimensional cryptosystem based on bi-cartesian algebra, was developed by Yassein and Al-Saidi in 2018 [7,8]. In 2020, Yassein et al. [9] proposed a multi-dimensional algebra for designing an improved NTRU cryptosystem. In 2021, Yassein et al. designed a new copy of NTRU with high security and performance levels [10]. In 2021, Shihadi and Yassein introduced a newly designing for NTRU with increased security and improved performance using algebra of tripternion [11]. Also, Abo-Alsood and Yassein design an alternative NTRU called BOTRU depend on bi-octonion subalgebra with high secure [12]. Yassein et al. introduced QMNTR by building a new mathematical key [13].

2 hexa$_t$ Algebra

Assuming that $\mathcal{R}$ be an arbitrary finite ring with $Char(\mathcal{R}) \neq 2$, the algebra $\mathcal{S}$ defined over $\mathcal{R}$ is as follows: $\mathcal{S} = \{(c_1,\ c_2)(1,1) + (c_3,c_4)(x,i) + (c_5,c_6)(y,j)c_i \in \mathcal{R} \ni i = 1,2,...,6\}$ where this algebra's basis is $(1,1)$, $(x,\ i)$, $(y,\ j)$. Now, suppose have three rings of truncated polynomials $W = Z[\varkappa]/(x^N-1)$, $W_p = Z_p[\varkappa]/(x^N-1)$, $W_q = Z_q[\varkappa]/(x^N-1)$, following is a demonstration of three algebraic symbols: A, A_p, and A_q

$A = \{(\alpha_1,\alpha_2)(1,1) + (\alpha_3,\alpha_4)(x,\ i) + (\alpha_5,\alpha_6)(y,\ j)$ $\alpha_1,\ldots,\ \alpha_6 \in W\}$

$A_p = \{(\alpha_1,\alpha_2)(1,1) + (\alpha_3,\alpha_4)(x,\ i) + (\alpha_5,\alpha_6)(y,\ j)$ $\alpha_1,\ldots,\ \alpha_6 \in W_p\}$

$A_q = \{(\alpha_1,\alpha_2)(1,1) + (\alpha_3,\alpha_4)(x,\ i) + (\alpha_5,\alpha_6)(y,\ j)$ $\alpha_1,\ldots,\ \alpha_6 \in W_q\}$.

Let $\eta_1,\eta_2 \in A_p,A_q$ such that

$\eta_1 = (\mathfrak{y}_1,\mathfrak{y}_2)(1,1)+(\mathfrak{y}_3,\mathfrak{y}_4)(x,i)+(\mathfrak{y}_5,\mathfrak{y}_6)(y,j)$ and

* Corresponding author e-mail: hassan.yaseen@qu.edu.iq

$\eta_2 = (\mathscr{o}_1, \mathscr{o}_2)(1,1) + (\mathscr{o}_3, \mathscr{o}_4)(x,\ i) + (\mathscr{o}_5, \mathscr{o}_6)(y,\ j)$ be two elements belong to A_p *or* A_q. The operation of adding comparable coefficients results in the addition $\eta_1 + \eta_2$. It is possible to calculate the multiplication.
$\eta_1 * \eta_2 = (\gamma_1\mathscr{o}_1 + \gamma_3\mathscr{o}_5 + \gamma_5\mathscr{o}_3, \gamma_2\mathscr{o}_2 + \gamma_4\mathscr{o}_6 + \gamma_6\mathscr{o}_4)$ $(1,1)$ + $(\gamma_3\mathscr{o}_3$ + $\gamma_1\mathscr{o}_5$ + $\gamma_5\mathscr{o}_1, \gamma_4\mathscr{o}_4$ + $\gamma_2\mathscr{o}_6$ + $\gamma_6\mathscr{o}_2)(x,i)$ + $(\gamma_5\mathscr{o}_5$ + $\gamma_1\mathscr{o}_3$ + $\gamma_3\mathscr{o}_1, \gamma_6\mathscr{o}_6$ + $\gamma_2\mathscr{o}_4 + \gamma_4\mathscr{o}_2)(y,j)$, this multiplication is commutative. Inverse multiplication of $\eta = (k_1,k_2)(1,1) + (k_3,k_4)(x,i) + (k_5,k_6)(y,j)$ is represented as follows: $h^{-1} = (h_1,h_2)(1,1) + (h_3,h_4)(x,i) + (h_5,h_6)(y,j)$ such that

$$h_1 = \frac{k_3k_5 - (k_1)^2}{3k_1k_3k_5 - (k_1)^3 - (k_3)^3 - (k_5)^3},$$

$$h_2 = \frac{k_4k_6 - (k_2)^2}{3k_2k_4k_6 - (k_2)^3 - (k_4)^3 - (k_6)^3},$$

$$h_3 = \frac{k_1k_5 - (k_5)^2}{3k_1k_3k_5 - (k_1)^3 - (k_3)^3 - (k_5)^3}$$

$$h_4 = \frac{k_2k_6 - (k_6)^2}{3k_2k_4k_6 - (k_2)^3 - (k_4)^3 - (k_6)^3}$$

$$h_5 = \frac{k_1k_5 - (k_3)^2}{3k_1k_3k_5 - (k_1)^3 - (k_3)^3 - (k_5)^3}$$

$$h_6 = \frac{k_2k_4 - (k_4)^2}{3k_2k_4k_6 - (k_2)^3 - (k_4)^3 - (k_6)^3}$$

The identity multiplication is $I = (1,1)(1,1) + (0,0)$ $(x,i) + (0,0)(y,j)$.

3 TRUHSH Cryptosystem

In addition to the general parameters in NTRU, the TRUHSH cryptosystem relies on the subsets $\mathfrak{T}_\mathcal{F}, \mathfrak{T}_\mathcal{L}, \mathfrak{T}_\mathcal{V}, \mathfrak{T}_\mathcal{S}$ and $\mathfrak{T}_\mathrm{M} \subset A$ satisfying the condition for the existence of the inverse for $\mathcal{F} \in \mathfrak{T}_\mathcal{F}$.
The numbers $d_\mathfrak{f}$, d_ℓ , d_v, $d_\mathfrak{s}$ and d_m are describe a like way as in NTRU. The TRUHSH cryptosystem can be represented through the three steps that follow:

3.1 Key Creation

We will select three polynomials $\mathcal{F} \in \mathfrak{T}_\mathcal{F}, \mathcal{L} \in \mathfrak{T}_\mathcal{L}, V$ $\in \mathfrak{T}_V$ to generate key $\mathbb{H}$, such that $\mathcal{F}$ should be invertible mod p and q, the public keys are generated by the equation $\mathbb{H} = \mathcal{F}_q^{-1} * (\mathcal{L} * V)\,(mod\ q)$. Consequently, the private keys are $\{\mathcal{F}, \mathcal{L}, \mathcal{N}\}$.

3.2 Encryption

We select random polynomial $\mathcal{S} \in T_\mathcal{S}$, after converting the original message M to hexa$_\mathfrak{t}$ algebra . Calculate ciphertext E by equation $E = p\ \mathbb{H} * \mathcal{S} + \mathrm{M}\ (mod\ q)$.

3.3 Decryption

After getting the ciphertext E, the recipient gets the original message by using the following steps: Compute $C_1 = \mathcal{F} * E\ mod\ q$, convert A_2 from *mod* q to *mod* p, i.e. $C_2 = C_1\ mod\ p$ and the coefficients are adjusted to fall in the interval $(\frac{-p}{2}, \frac{p}{2}]$. Now, multiply C_2 by $\mathcal{F}_p^{-1}$ from the left, i.e. $C_3 = \mathcal{F}_p^{-1} * C_2\ mod\ p$, and $\mathrm{M} = C_3$.

4 Security Analysis

An attacker has public parameters and the public keys $\mathbb{H} = \mathcal{F}_q^{-1} * (\mathcal{L} * V)(mod\ q)$ and must search in $\mathfrak{T}_\mathcal{L}$ in order to locate the private keys $\mathcal{L}$ and in $\mathfrak{T}_V$ to find the private keys $\mathcal{V}$ until a decryption key is found. The total space for the three subsets $\mathfrak{T}_\mathcal{L}, \mathfrak{T}_\mathcal{V}$, and $\mathfrak{T}_\mathcal{F}$ are computed using a brute force assault as follows:
$| \mathfrak{T}_\mathcal{L} | = \left(\frac{N!}{(d_{\ell!})^2 (N-2d_\ell)!}\right)^6$, and $| \mathfrak{T}_V | = \left(\frac{N!}{(d_{v!})^2\ (N-2d_v)!}\right)^6$.
As a result, the key security is equal to the following:

$$\frac{(N!)^6}{(d_{v!}d_{\ell!})^6\ ((N-2d_\ell)!\,(N-2d_v)!)^3}.$$

Similarly, an attacker must also seek in order to discover the original message in $\mathfrak{T}_\mathcal{S}$ such that

$$| \mathfrak{T}_\mathcal{S} | = \left(\frac{N!}{(d_{\mathcal{S}!})^2\,(N-2d_\mathcal{S})!}\right)^6.$$

As a result, the security of message security is equal to the following:

$$\frac{(N!)^3}{(d_{\mathcal{S}!}\ )^6\,((N-2d_\mathcal{S})!)^3}.$$

5 Conclusions

Due to the multiple dimensions of the TRUHSH cryptosystem and its mathematical structure, it gave higher security compared to the original NTRU cryptosystem (six times as much because there are six polynomials in one element), in addition to the ability to send different messages at the same time, but it is slower than NTRU for the presence of a large number of mathematical calculations however, this problem can be mitigated by decreasing the value of N without affecting the safety level. That qualities make TRUHSH suited for a variety of applications that call for multiple data sources, With the possibility of applying it in one source by zeroing all coefficients except for one coefficient, like electronic voting.

Acknowledgement

Authors of this article wish to extend their cordial thanks to professor Nadia M. G. Al-Saidi, department of applied sciences University of Technology for her generous guidance in preparing this paper.

References

[1] J. Hoffstein, J. Pipher , J. Silverman, NTRU: a ring based public key cryptosystem, Int. Algorithmic Number Theory Symp **1423**, 267-288 (1998).
[2] N M. AlSaidi, M. Said,A T. Sadiq, A A. Majeed A A. An improved NTRU cryptosystem via commutative quaternions algebra, Int. Conf. Security and Management SAM, 198 (2015).
[3] H R. Yassein, N M. Al-Saidi, HXDTRU cryptosystem based on hexadecnion algebra, Proc. 5th Int. Cryptology and Information Security Conf. **5**:1-14 (2016a).
[4] N M. Al-Saidi, H R. Yassein, A new alternative to NTRU cryptosystem based on highly dimensional algebra with dense lattice structure, Malaysian J. Mathematical Sci.**11**, 29-43 (2017).
[5] H. R. Yassein, N. M. Al-Saidi, BITRU: binary version of the NTRU public key cryptosystem via binary algebra, Int. J. Advanced Computer Sci. and Applications **7**,1-6 (2016b).
[6] H. R. Yassein, N. M. G. Al-Saidi, A Comparative Performance Analysis of NTRU and Its Variant Cryptosystems, In 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), 115–120 (2017).
[7] H. R. Yassein, N. M. Al-Saidi, BCTRU: a new secure NTRUcrypt public key system based on a newly multidimensional algebra, proc. 6th Int. Cryptology and Information Security conf. **6**,1-11 (2018).
[8] H. R. Yassein, N. M. Al-Saidi, An Innovative Bi-Cartesian Algebra for Designing of Highly Performed NTRU Like Cryptosystem, Malaysian Journal of Mathematical Sciences **13**, 29–43 (2019)
[9] H. R. Yassein, N. M. Al-Saidi, A. K. Farhan, A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure, J. Discrete Mathematical Sci. and Cryptography **23**, 1-20 (2020).
[10] H. R. Yassein, N. M. Al-Saidi, A. K. Jabber, A multi-dimensional algebra for designing an improved NTRU cryptosystem Eurasian, J. Mathematical and Computer Applications **8**, 97-107 (2020).
[11] 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**, 1515-1522 (2021).
[12] H. H. Abo-Alsood and H. R. Yassein, Design of an Alternative NTRU Encryption with High Secure and Efficient, International Journal of Mathematics and Computer Science, **16**, 1469-1477 (2021).
[13] H. R. Yassein, A. A. Abidalzahra and N. M. G. Al-Saidi, A new design of NTRU encryption with high security and performance level, AIP Conference Proceedings **2334**, 080005-1-080005-4 (2021).

Hiba Shakir Salman
Completed the B.Sc. degree in mathematics from college of education, university of Al-Qadisiyah in 2005. She completed his master in algebraic topology at the faculty of education for girls university of Kufa, Iraq in 2020. Now a Ph.D. student specializing in mathematical cryptography.

Hassan Rashed Yassein
Completed his doctorate in cryptography at the college of the science university of Baghdad, Iraq in 2017. His research interests include algebra, security, representation theory, cryptography, applied mathematics, fuzzy algebra, and abstract algebra. In 2017 he has been elected as Secretary of the Administrative Board of the Iraqi Mathematical Society. He supervised many postgraduate students, masters, and doctorates.