Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/170414

Structure a Public-Key Cryptosystem Based on HSS Algebra

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: 5 Mar. 2023, Revised: 12 Apr. 2023, Accepted: 5 May 2023
Published online: 1 Jul. 2023

Abstract: NTRU (Number theory research unit) is a public key cryptosystem that uses lattice-based cryptography. It is more resistant to assaults than other commonly used public-key cryptosystems, and its performance has been proven to be much better. This study introduces TRUHIB, a commutative variation of the NTRU, as a novel multidimensional public-key cryptosystem. It operates using a novel mathematical structure that consists of two public keys and five private keys. in a algebra called HSS algebra. This new structure has improved the security and sophistication of the public key cryptosystem.

Keywords: NTRU, key security, message security, HSS Algebra.

1 Introduction

As more people utilize computer networks to transmit confidential documents, several of these duties would be impossible to complete without the availability of an efficient and safe cryptosystem. Many public-key cryptosystems depend on factorization and discrete algorithm issues, such as RSA and El- Gamal have been presented [1,2]. In 1996, Hoffstein et al. proposed NTRU a public key based on rings $Z[x]\backslash(x^N-1)$ [3]. Due to the effectiveness of NTRU, many improvements have been made to it.

In 2019, Yassein and Al-Saidi studied an innovative bi-cartesian algebra for designing highly performed NTRU- like [4]. In 2020,Yassein et al. proposed a new NTRU public key through an innovational algebraic structure [5]. In the same year, Yassein et al. proposed a multi-dimensional algebra for designing an improved NTRU [6]. In 2021, Yassein et al. proposed an improvement of QTRU called QMNTR depending on a new mathematical structure [7]. In the same year, Abo-Alsood and Yassein proposed a new like-NTRU called BOTRU and QOTRU depending on bi-octonion subalgebra and Qu-octonion subalgebra respectively [8, 9]. Shahhadi and Yassein introduce two cryptosystem variant NTRU called NTRS and NTRSH via tripternion algebra [10,11]. In 2022, Abo-Alsood and Yassein used octonion algebra to build an alternative to the NTRU called TOTRU [12]. Also, Shahhadi and Yassein introduce a new method analog NTRU called NTRTRN via tripternion algebra [13]. In 2023, Yassein at el. proposed NTRU-like which called QuiTRU with high security [14] . In this study, TRUHIB a new NTRU alternative is provided with a new mathematical structure that is based on the HSS algebra.

2 HSS Algebra

Let F be a field such that $Char(F) \neq 2$, then the HSS algebra defined as following [15]:
$HSS = \{(\tau_1,\tau_2,\tau_3)(1,1,1) + (\tau_4,\tau_5,\tau_6)(x,x,x) + (\tau_7,\tau_8,\tau_9)(y,y,y)\backslash\tau_i \in F, i = 1,2,\ldots,9\}$ such that $\{(1,1,1),(x,x,x),(y,y,y)\}$ is basis of Ď. Suppose have three rings of truncated polynomials:
$K = Z[\varkappa]\backslash(x^N-1), K_p = Z_p[\varkappa]\backslash(x^N-1), K_q = Z_q[\varkappa]\backslash(x^N-1)$.
The three algebra V,V_p,and V_q are demonstrated as follows:
$V = \{(\mu_1,\mu_2,\mu_3)(1,1,1) + (\mu_4,\mu_5,\mu_6)(x,x,x) + (\mu_7,\mu_8,\mu_9)(y,y,y)\backslash\mu_i \in K\}$
$V_p = \{(\mu_1,\mu_2,\mu_3)(1,1,1) + (\mu_4,\mu_5,\mu_6)(x,x,x) +$

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

$(\mu_7,\mu_8,\mu_9)(y,y,y)\backslash\mu_i \in K_p\}$
$V_q = \{(\mu_1,\mu_2,\mu_3)(1,1,1) + (\mu_4,\mu_5,\mu_6)(x,x,x) + (\mu_7,\mu_8,\mu_9)(y,y,y)\backslash\mu_i \in K_q\}$
Let $E_1, E_2 \in V_p, V_q$ such that
$E_1 = (\gamma_1,\gamma_2,\gamma_3)(1,1,1) + (\gamma_4,\gamma_5,\gamma_6)(x,x,x) + (\gamma_7,\gamma_8,\gamma_9)(y,y,y)$ and $E_2 = (\eta_1,\eta_2,\eta_3)(1,1,1) + (\eta_4,\eta_5,\eta_6)(x,x,x) + (\eta_7,\eta_8,\eta_9)(y,y,y)$
Corresponding coefficients are added to complete the addition E_1+E_2.
The multiplication $E_1 * E_2$ can be determined $E_1 * E_2 = (\gamma_1\eta_1 + \gamma_4\eta_7 + \gamma_7\eta_4, \gamma_2\eta_2 + \gamma_5\eta_8 + \gamma_8\eta_5, \gamma_3\eta_3 + \gamma_6\eta_9 + \gamma_9\eta_6)(1,1,1) + (\gamma_4\eta_4 + \gamma_1\eta_7 + \gamma_7\eta_1, \gamma_5\eta_5 + \gamma_2\eta_8 + \gamma_8\eta_2, \gamma_6\eta_6 + \gamma_3\eta_9 + \gamma_9\eta_3)(x,x,x) + (\gamma_7\eta_7 + \gamma_1\eta_4 + \gamma_4\eta_1, \gamma_8\eta_8 + \gamma_5\eta_2 + \gamma_2\eta_5, \gamma_9\eta_9 + \gamma_3\eta_6 + \gamma_6\eta_3)(y,y,y)$. The multiplication $E_1 * E_2$ commutative, identity element of multiplication equal to $\omega = (1,1,1)(1,1,1) + (0,0,0)(x,x,x) + (0,0,0)(y,y,y)$, and inverse element multiplication is defined as following

$$\begin{aligned} E^{-1} =& (\iota_1,\iota_2,\iota_3)(1,1,1) + (\iota_4,\iota_5,\iota_6)(x,x,x) \\ &+ (\iota_7,\iota_8,\iota_9)(y,y,y), \end{aligned}$$

where

$$\iota_1 = \frac{\beth_4\beth_7 - (\beth_1)^2}{3\beth_1\beth_4\beth_7 - (\beth_1)^3 - (\beth_4)^3 - (\beth_7)^3},$$

$$\iota_2 = \frac{\beth_5\beth_8 - (\beth_2)^2}{3\beth_2\beth_5\beth_8 - (\beth_2)^3 - (\beth_5)^3 - (\beth_8)^3},$$

$$\iota_3 = \frac{\beth_6\beth_9 - (\beth_3)^2}{3\beth_3\beth_6\beth_9 - (\beth_3)^3 - (\beth_6)^3 - (\beth_9)^3},$$

$$\iota_4 = \frac{\beth_1\beth_4 - (\beth_7)^2}{3\beth_1\beth_4\beth_7 - (\beth_1)^3 - (\beth_4)^3 - (\beth_7)^3},$$

$$\iota_5 = \frac{\beth_2\beth_5 - (\beth_8)^2}{3\beth_2\beth_5\beth_8 - (\beth_2)^3 - (\beth_5)^3 - (\beth_8)^3},$$

$$\iota_6 = \frac{\beth_3\beth_6 - (\beth_9)^2}{3\beth_3\beth_6\beth_9 - (\beth_3)^3 - (\beth_6)^3 - (\beth_9)^3},$$

$$\iota_7 = \frac{\beth_1\beth_7 - (\beth_4)^2}{3\beth_1\beth_4\beth_7 - (\beth_1)^3 - (\beth_4)^3 - (\beth_7)^3},$$

$$\iota_8 = \frac{\beth_2\beth_8 - (\beth_5)^2}{3\beth_2\beth_5\beth_8 - (\beth_2)^3 - (\beth_5)^3 - (\beth_8)^3},$$

and

$$\iota_9 = \frac{\beth_3\beth_9 - (\beth_6)^2}{3\beth_3\beth_6\beth_9 - (\beth_3)^3 - (\beth_6)^3 - (\beth_9)^3}.$$

3 TRUHIB Cryptosystem

TRUHIB cryptosystem depends on parameters N, p, q similar to NTRU as well as subsets $I_\varsigma, I_\mathcal{U}, I_\mathcal{G}, I_\mathcal{W}, I_\mathcal{Y}, I_\Psi, I_\phi$ and $I_\mathrm{M} \subset V$ such $I_\mathcal{G}$ has inverse mod p and q. The following three stages can be used to describe the TRUHIB cryptosystem.

3.1 Key Creation

Use five polynomials $\varsigma \in I_\varsigma, \mathcal{U} \in I_\mathcal{U}, \mathcal{G} \in I_\mathcal{G}, \mathcal{W} \in I_\mathcal{W}$ and $\mathcal{Y} \in I_\mathcal{Y}$ to create keys $\mathcal{H}$ and $\mathcal{K}$, such that ς and $\mathcal{Y}$ should be invertible modulo p and q and $\mathcal{W}$ invertible modulo p. The public keys are generated as follows: $K = \varsigma * (\mathcal{G} * \mathcal{U}) \, mod \, q$ and $H = \mathcal{W} * \mathcal{Y}_q^{-1} \, mod \, q$.

3.2 Encryption

Random polynomials $\Psi \in I_\Psi$ are picked after translating the original message M to HSS algebra. Compute ciphertext E by formula: $E = p(\mathcal{K} * \Psi + H) + \mathrm{M} \, (mod \, q)$.

3.3 Decryption

After getting the ciphertext E, the recipient gets the original message by using the following steps:
First, compute $B_1 = E * \mathcal{Y} \, mod \, q$, second, covert to $mod \, p$ i.e. $B_2 = B_1 \, mod \, p$, the coefficients are adjusted to lie in the interval $(\frac{-p}{2}, \frac{p}{2}]$ and multiplying B_2 from the right by $\mathcal{Y}_p^{-1}$ denoted by $B_3 = B_2 * \mathcal{Y}_p^{-1} \, mod \, p = \mathrm{M}$.

4 Security analysis

An attacker who has general parameters and the public keys $\mathcal{H}$ and $\mathcal{K}$ must search in $I_\mathcal{G}$, $I_\mathcal{U}$, and $I_\mathcal{W}$ get private keys $\mathcal{G}, \mathcal{U}$, and $\mathcal{W}$ until a decryption key is found. The size of space for the three subsets $I_\mathcal{G}$, $I_\mathcal{U}$, and $I_\mathcal{W}$ are computed using a brute force assault as follows: $|I_\mathcal{G}| = \binom{N}{d_\mathcal{G}}^9 \binom{N-d_\mathcal{G}}{d_\mathcal{G}}^9$, $|I_\mathcal{U}| = \binom{N}{d_\mathcal{U}}^9 \binom{N-d_\mathcal{U}}{d_\mathcal{U}}^9$ and $|I_\mathcal{W}| = \binom{N}{d_\mathcal{W}}^9 \binom{N-d_\mathcal{W}}{d_\mathcal{W}}^9$ As a result, the key security is equal to: $\left(\binom{N}{d_\mathcal{G}}^9 \binom{N-d_\mathcal{G}}{d_\mathcal{G}}^9 \binom{N}{d_\mathcal{U}}^9 \binom{N-d_\mathcal{U}}{d_\mathcal{U}}^9 \binom{N}{d_\mathcal{W}}^9 \binom{N-d_\mathcal{W}}{d_\mathcal{W}}^9\right)^{\frac{1}{2}}$ Similarly, an attacker must also seek in order to discover the original message in I_Ψ such that $|I_\Psi| = \binom{N}{d_\Psi}^9 \binom{N-d_\Psi}{d_\Psi}^9$, As a result, the message security is equal to: $\left(\binom{N}{d_\Psi}^9 \binom{N-d_\Psi}{d_\Psi}^9\right)^{\frac{1}{2}}$.

5 Conclusions

TRUHIB cryptosystem is based on commutative HSS algebra. Security of TRUHIB is more than NTRU, QMNTR, BOTRU, QOTRU, NTRS, NTRSH, TOTRU, NTRTRN, and QuiTRU but it speed faster than TOTRU and slower than NTRU, QMNTR, BOTRU, NTRS, NTRSH, TOTRU, NTRTRN, and QuiTRU. TRUHIB is multidimensional and can encrypt nine messages in one round nine different sources or from a single source. This feature may be important in some applications that need multiple sources.

References

[1] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, **21**, 120-126 (1978).

[2] T. El- Gamal, A public key cryptosystem and a signature scheme based on discrete logarithm, *IEEE Transactions on Information Theory*, **31**, 469-472 (1985).

[3] J. Hoffstein, J. Pipher and J. Silverman, NTRU: a ring based public key cryptosystem, *Int. Algorithmic Number Theory Symp*, **1423**, 267-288 (1998).

[4] H. R. Yassein and N. M. Al-Saidi, An Innovative Bi-Cartesian Algebra for Designing of Highly Performed NTRU Like Cryptosystem, *Malaysian Journal of Mathematical Sciences*, **13**, 77–91 (2019).

[5] H. R. Yassein, N. M. Al-Saidi and 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**, 1–20 (2020).

[6] H. R. Yassein, N. M. Al-Saidi and A. K. Jabber, A multi-dimensional algebra for designing an improved NTRU cryptosystem Eurasian, *J. Mathematical and Computer Applications*, **8**, 97-107 (2020).

[7] H. R. Yassein and A. A. Abidalzahra and N. M. G. Al-Saidi, *A new design of NTRU encryption with high security and performance level*, AIP Conference Proceedings, 080005-1-080005-4 (2021).

[8] 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).

[9] H. H. Abo-Alsood and H. R. Yassein, QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra, *Journal of Physics: Conference Series*, **1999**, 1-6 (2021).

[10] S. H. Shahhadi and H. R. Yassein, A New Design of NTRUEncrypt-analog Cryptosystem with High Security and Performance Level via Tripternion Algebra, *International Journal of Mathematics and Computer Science*, **16**, 1515-1522 (2021).

[11] S. H. Shahhadi and H. R. Yassein, NTRsh: A New Secure Variant of NTRUEncrypt Based on Tripternion Algebra, *Journal of Physics: Conference Series*, **1999**, 1-6 (2021).

[12] H. H. Abo-Alsood and H. R. Yassein, *Analogue to NTRU Public Key Cryptosystem by Multi-Dimensional Algebra with High Security*, AIP Conference Proceedings, 060009-1 - 060009-6, (2022).

[13] S. H. Shahhadi and H. R. Yassein, *An Innovative Tripternion Algebra for Designing NTRU - Like Cryptosystem with High security*, AIP Conference Proceedings, 060009-1-060009-6, (2022).

[14] H. R. Yassein, H. N. Zaky, H. H. Abo-Alsood, I. A. Mageed and W. I. El-Sobky, QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra, *Applied Mathematics & Information Sciences*, **17**, 1-5 (2023).

[15] H. S. Salman and H. R. Yassein, An Innovative HSS Algebra for Designing a Secure Like-NTRU Encryption, *Mathematical Statistician and Engineering Applications*, **71**, 6098-6113 (2022).

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.