

A new designing of MaTRU cryptosystem

Asia Aqeel Abidalzahra [†]

Hassan Rashed Yassein ^{*}

Department of Mathematics

University of Al-Qadisiyah

Al-Diwaniya 58003

Iraq

Abstract

A multidimensional public-key MaTRU cryptosystem improves NTRU works under the same generic parameters as NTRU, except for a different ring with a different mathematical structure. In this paper, a new multidimensional public key encryption scheme is presented called AmTRU. It works under the same general principle as MaTRU but with a different mathematical structure. This change has made this public-key system stronger and more secure.

Subject Classification: 94A60, 68P25.

Keywords: NTRU, MaTRU, AmTRU.

1. Introduction

The transmission of confidential information over open networks has become a difficult undertaking in many business sectors. Therefore, the creation and development of cryptosystems with high levels of security have gained great acceptance among many researchers. Hoffstein et al. [9] introduced the NTRU cryptosystem in 1996, which is built on a truncated polynomial. In 2005, Coglianesi and Goi [7] proposed a MaTRU cryptosystem that operates over the ring $M_k[Z][X]/(X^n - 1)$ of $k \times k$ matrices of polynomials in $Z[X]/(X^n - 1)$. In 2019, Verma et al. proposed a new cryptosystem by using an alternate superior dynamic lookup table [18]. In 2020, a number of researchers have

[†] ORCID-ID: 0009-0004-8004-1626

^{*} ORCID-ID: 0000-0002-6788-0247

[†] E-mail: asialasia21998@gmail.com

^{*} E-mail: hassan.yaseen@qu.edu.iq (Corresponding Author)

presented public key methods based on different algebraic structures [6, 22]. In 2021, Yassein et al. [20] established QMNTR, relying on new mathematical structures as an improvement for QTRU. In the same year, Yassein and Shahhadi proposed two improvements for NTRU based on tripternion algebra, called NTRS and NTR_{SH} [15, 16]. Abo-Alsood and Yassein [2, 3] introduce BOTRN and QOTRU with two new algebras called the qu-octonion subalgebra and bi-octonion subalgebra, respectively. Imine et al. introduced a new cryptosystem via non-permutation equivalent polar [10]. In 2022, Yassein et al. presented some new methods analogous to NTRU by adopting different algebraic structures with a new mathematical structure [4, 8, 11, 17, 19]. Also, Benamara and Merazka presented two versions of the Boneh-Goh-Nissim cryptosystem [5]. In 2023, Yassein et al. proposed a QuiTRU based on an HH-real algebra with a new mathematical structure [21, 23-26]. Also, Salman and Yassein presented three new cryptosystems, TRUFT, TRUHIB, TRUHSH, by relying on multidimensional algebras to ensure a high level of security [12-14]. In 2024, Yassein and Abidalzahra [1] presented an ASTRU built on a new AS algebra with a new mathematical structure. In this paper, we present another variant of NTRU, named AmTRU. It operates in the matrices ring of size $k \times k$ where elements of matrices are from ring $Z[X]/X^N - 1$. The mathematical construction of AmTRU, consisting of five private keys and two public keys, makes it enjoy a high level of security.

2. The Proposed AmTRU Cryptosystem

Let $\mathbb{M} = \{[a_{ij}]_{k \times k} \mid a_{ij} \in \varphi = Z[X]/(X^n - 1)\}$ be a noncommutative matrix ring where the ring φ is truncated polynomials of degree $n - 1$ having integer coefficients.

The width of $f \in \mathbb{M}$ is defined by: $\|f\|_\infty = \text{Max}(\text{coefficients in polys. } m \in f) - \text{Min}(\text{coefficients in polys. } m \in f)$. The definition for width is similar to a polynomial in φ .

A matrix $f \in \mathbb{M}$ is said to be short if $\|f\|_\infty \leq p$.

The size of an element $f \in \mathbb{M}$ equal to

$$|f| = \sqrt{\sum_{poly.m \in f} \sum (coeff.in m)^2}.$$

AmTRU uses the parameters $(n, k, p, q), p, q \in \mathbb{N}$. The numbers p and q are relatively prime and q is much larger than p .

The AmTRU cryptosystem relies on parameters (n, k, p, q) and six subsets $\ell_{\mathcal{A}}, \ell_F, \ell_R, \ell_S, \ell_V, \ell_M \subseteq \mathbb{M}$.

The following notation below is used to define the sets of short matrices.

$\ell(d) = \{M \in \mathbb{M} \mid \text{for } [-(p-1)/2] \dots [p-1/2], i \neq 0, \text{ every polynomial in } M \text{ has on average } d \text{ coefficients equal } i, \text{ the rest } 0\}$.

Now, we define the subsets $\mathcal{L}_A, \mathcal{L}_F, \mathcal{L}_R, \mathcal{L}_V, \mathcal{L}_S, \mathcal{L}_M$ as follows: $\ell_{\mathcal{A}} = \{\mathcal{A} \in \mathbb{M} \mid \mathcal{A} \text{ is permutation matrices and } \mathcal{A}^i, i = 0, 1, \dots, k-1 \text{ are linearly independent modulo } q \text{ and for short } a_i \in \varphi, \sum_{i=0}^{k-1} a_i \mathcal{A}^i \text{ is short}\}$

$$\begin{aligned}\ell_F &= \{F \in \mathbb{M} \mid F = \sum_{i=0}^{k-1} c_i C^i, \text{ such that } c_0, \dots, c_{k-1} \in \\ &\quad \varphi \text{ is a short polynomial and } C \in \ell_{\mathcal{A}}\}, \\ \ell_R &= \{R \in \mathbb{M} \mid R = \sum_{i=0}^{k-1} c_i C^i, \text{ such that } c_0, \dots, c_{k-1} \\ &\quad \in \varphi \text{ is a short polynomial and } C \in \ell_{\mathcal{A}}\}, \\ \ell_V &= \{V \in \mathbb{M} \mid V \text{ is random matrix of size } k \times k\},\end{aligned}$$

$$\ell_S = \{S \in \mathbb{M} \mid S \text{ is random matrix of size } k \times k \text{ has inverse mod } p\},$$

$$\ell_M = \{M \in \mathbb{M} \mid \text{polynomials in } M \text{ have coefficients between } [-(p-1)/2] \text{ and } [p-1/2]\}.$$

In addition, the elements in ℓ_F satisfy the condition that they have the inverse of modulo p and q .

Since the matrices A and B are public keys, the security of F, G, R, W is contingent upon the difficulty of identifying the short polynomials a_i, b_i, r_i, w_i , $i = 0, 1, \dots, k-1$, so we wish to increase the number of options available polynomials. We therefore commonly choose $d_F \approx \frac{n}{p}, d_R \approx \frac{n}{p}$.

Now, we describe the phases of the AmTRU cryptosystem as follows:

2.1 Key Generation

To obtain the public keys, the recipient chooses the private keys as follows. In the first step, he/she selects two matrices $\mathcal{A}, \mathcal{B} \in \ell_{\mathcal{A}}$ of size $k \times k$ and randomly selects short polynomials $a_i, b_i \in \varphi, i = 0, 1, \dots, k-1$. Now, compute $F, G \in \ell_F$ as follows:

$F = \sum_{i=0}^{k-1} a_i \mathcal{A}^i$ and $G = \sum_{i=0}^{k-1} b_i \mathcal{B}^i$, the matrices F and G have multiplication inverse modulo p denoted by F_p^{-1}, G_p^{-1} respectively and modulo q denoted by F_q^{-1}, G_q^{-1} , respectively.

In the second step, he/she will choose three matrices $V, T \in \ell_V, S \in \ell_S$ of size $k \times k$. Now, the public keys are calculated by

$$H = F_q^{-1} * V * T \pmod{q}, K = S * G_q^{-1} \pmod{q}.$$

2.2 Encryption

To send ciphertext, the sender selects a message $M \in \ell_M$ and it is creating matrices $\mathcal{R}, \mathcal{W} \in \ell_R$ by taking:

$$\mathcal{R} = \sum_{i=0}^{k-1} r_i A^i \text{ and } \mathcal{W} = \sum_{i=0}^{k-1} w_i B^i$$

such that $r_i, w_i \in \psi, i = 0, 1, \dots, k-1$ are random short polynomials. Now, the ciphertext is calculated by:

$$E = p(\mathcal{R} * H * \mathcal{W}) + M * K \pmod{q}.$$

2.3 Decryption

The recipient decrypts the cipher text as follows:

$$\begin{aligned}D &= F * E * G \pmod{q} = F * (p(\mathcal{R} * H * \mathcal{W}) + M * K) * G \pmod{q} \\ &= F * \left(p(\mathcal{R} * (F_q^{-1} * V * T) * \mathcal{W}) + M * (S * G_q^{-1}) \right) * G \pmod{q}\end{aligned}$$

$$= p(F * \mathcal{R} * (F_q^{-1} * V * T) * \mathcal{W} * G) + F * M * (S * G_q^{-1}) * G \pmod{q}$$

Since

$$\begin{aligned} F * \mathcal{R} &= \left(\sum_{i=0}^{k-1} a_i A^i \right) * \left(\sum_{i=0}^{k-1} r_i A^i \right) \pmod{q} \\ &= \sum_{i=0}^{k-1} \sum_{s+t \pmod{k}} a_s A^s r_t A^t \pmod{q} \\ &= \sum_{i=0}^{k-1} \sum_{s+t \pmod{k}} r_t A^{s+t} a_s \pmod{q} \\ &= \sum_{i=0}^{k-1} \sum_{s+t \pmod{k}} r_t A^t a_s A^s \pmod{q} \\ &= \left(\sum_{i=0}^{k-1} r_i A^i \right) * \left(\sum_{i=0}^{k-1} a_i A^i \right) = \mathcal{R} * F \pmod{q}, \end{aligned}$$

then

$$D = p(\mathcal{R} * V * T * W) * G + F * M * S \pmod{q}$$

The coefficients in the last equation must be modified to lie in the interval $(-\frac{q}{2}, \frac{q}{2}]$.

Now, take $Y = D \pmod{p} = F * M * S \pmod{p}$, then

$$M \pmod{p} = F_p^{-1} * Y * S_p^{-1} \pmod{p}.$$

3. Security Analysis

Through a brute force attack, the attacker accesses the plaintext in one of two ways.

1. Search for the private keys used in constructing public keys (that is, the attacker must search for all possible short matrices $F \in \mathcal{L}_F$ and $T \in \mathcal{L}_V$ or $F \in \mathcal{L}_F$ and $V \in \mathcal{L}_V$ in the public key H and also look for $G \in \mathcal{L}_G$ in the public key K). Because the matrices A and B are generic, the security of F and G depends on $2k$ polynomials having degree $n - 1$. So the number of possible of F, G and T are

$$\left(\frac{n!}{(n-(p-1)!d_F!d_F^{(p-1)})} \right)^k, \left(\frac{n!}{(n-(p-1)!d_G!d_G^{(p-1)})} \right)^k \left(\frac{n!}{(n-(p-1)!d_V!d_V^{(p-1)})} \right)^{k^2},$$

respectively.

2. Search for the message keys (that is, the attacker must search for all possible short matrices $\mathcal{R} \in \mathcal{L}_R, \mathcal{W} \in \mathcal{L}_V$). The security of $\mathcal{R}$ and $\mathcal{W}$ necessarily depends on $2k$ polynomials $r_i, w_i, i = 0, 1, \dots, k - 1$. The number of possible $\mathcal{R}$ and $\mathcal{W}$ equal to $\left(\frac{n!}{(n-(p-1)!d_R!d_R^{(p-1)})} \right)^{2k}$,

$$\left(\frac{n!}{(n-(p-1)!d_W!d_W^{(p-1)})} \right)^{k^2}.$$

4. Conclusions

We introduced the AmTRU cryptosystem that is based on a non-commutative ring $\mathbb{M} = M_k[Z][X]/(X^n - 1)$. The hard mathematical structure of this improvement, consisting of two public and five private keys, gives it a high level of security against many known attacks compared to NTRU and MaTRU, which is a good choice for many electronic transactions.

References

- [1] A. A. Abidalzahra and H. R. Yassein, "Proposed development of NTRU encryption," *Int. J. Math. Comput. Sci.*, vol. 19, no. 3, pp. 715-719 (2024).
- [2] H. H. Abo-Alsood and H. R. Yassein, "Design of an alternative NTRU encryption with high secure and efficient," *Int. J. Math. Comput. Sci.*, vol. 16, no. 4, pp. 1469-1477 (2021).
- [3] H. H. Abo-Alsood and H. R. Yassein, "Analogue to NTRU public key cryptosystem by multi-dimensional algebra with high security," *AIP Conf. Proc.*, vol. 2386, no. 1, p. 060006 (2022). [Online]. Available: <http://dx.doi.org/10.1063/5.0067033>.
- [4] H. A. Ali and H. R. Yassein, "QTNTR: A new secure NTRUEncrypt alternative with a high level of security," *Math. Statist. Eng. Appl.*, vol. 71, no. 4, pp. 5634-5639 (2022).
- [5] O. Benamara and F. Merazka, "A new distribution version of Boneh-Goh-Nissim cryptosystem: Security and performance analysis," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 6, pp. 1633-1647 (2022). [Online]. Available: <https://doi.org/10.1080/09720529.2020.1782570>.
- [6] A. Chillali and M. Sahmoudi, "SCC-Cryptosystem on an algebraic closure ring," *J. Discrete Math. Sci. Cryptogr.*, vol. 23, no. 8, pp. 1475-1485 (2020). [Online]. Available: <https://doi.org/10.1080/09720529.2019.1624338>.
- [7] M. Coglianesi and B.-M. Goi, "MaTRU: A new NTRU-based cryptosystem," in *Progress in Cryptology - INDOCRYPT 2005*, S. Maitra, C. E. Veni Madhavan, and R. Venkatesan, Eds., Berlin, Heidelberg: Springer, pp. 232-243 (2005).
- [8] E. N. Hameed and H. R. Yassein, "QOCNTR: Improved NTRU public key based on a new algebraic structure," *Math. Statist. Eng. Appl.*, vol. 71, no. 4, pp. 5627-5633 (2022).
- [9] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Algorithmic Number Theory*, J. P. Buhler, Ed., Berlin, Heidelberg: Springer, pp. 267-288 (1998). [Online]. Available: <https://doi.org/10.1007/BFb0054868>.
- [10] B. Imine, N. Hadj-Said, and A. Ali-Pacha, "New McEliece cryptosystem based on non-permutation equivalent polar codes," *J. Discrete Math. Sci. Cryptogr.*, vol. 26, no. 1, pp. 103-114 (2023). [Online]. Available: <https://doi.org/10.1080/09720529.2021.1933706>.

- [11] H. S. Salman and H. R. Yassein, "An innovative HSS algebra for designing a secure like-NTRU encryption," *Math. Statist. Eng. Appl.*, vol. 71, no. 4, pp. 6098-6113 (2022).
- [12] H. S. Salman and H. R. Yassein, "Structure a public-key cryptosystem based on HSS algebra," *Appl. Math. Inf. Sci.*, vol. 17, no. 4, pp. 659-661 (2023). [Online]. Available: <http://dx.doi.org/10.18576/amis/170414>.
- [13] H. S. Salman and H. R. Yassein, "TRUFT: A new public key cryptosystem based on novel FTH algebra," *Int. J. Math. Comput. Sci.*, vol. 18, no. 4, pp. 589-593 (2023).
- [14] H. S. Salman and H. R. Yassein, "TRUHSH: Developing NTRU cryptosystem in terms of security and performance," *Appl. Math. Inf. Sci.*, vol. 17, no. 4, pp. 723-725 (2023). [Online]. Available: <http://dx.doi.org/10.18576/amis/170420>.
- [15] S. H. Shahhadi and H. R. Yassein, "A new design of NTRU encrypt-analog cryptosystem with high security and performance level via tripternion algebra," *Int. J. Math. Comput. Sci.*, vol. 16, no. 4, pp. 1515-1522 (2021).
- [16] S. H. Shahhadi and H. R. Yassein, "NTRsh: A new secure variant of NTRUEncrypt based on tripternion algebra," *J. Phys.: Conf. Ser.*, vol. 1999, no. 1, p. 012092 (2021). [Online]. Available: <http://dx.doi.org/10.1088/1742-6596/1999/1/012092>.
- [17] S. H. Shahhadi and H. R. Yassein, "An innovative tripternion algebra for designing NTRU-like cryptosystem with high security," *AIP Conf. Proc.*, vol. 2386, no. 1 (2022). [Online]. Available: <http://dx.doi.org/10.1063/5.0067023>.
- [18] D. K. Verma, M. Rani, R. K. Tyagi, and B. B. Sagar, "Baptista chaotic cryptosystem based on alternate superior dynamic lookup table," *J. Discrete Math. Sci. Cryptogr.*, vol. 22, no. 8, pp. 1383-1392 (2019). [Online]. Available: <https://doi.org/10.1080/09720529.2019.1692446>.
- [19] H. Yassein, A. Reshan, and N. Al-Saidi, "AHQTR: A new NTRU variant based on quaternion algebra," in *Proc. 8th Int. Cryptol. Inf. Security Conf.*, Port Dickson, Negeri Sembilan, pp. 100-108 (2022).
- [20] H. R. Yassein, A. A. Abidalzahra, and N. M. Al-Saidi, "A new design of NTRU encryption with high security and performance level," *AIP Conf. Proc.*, vol. 2334, no. 1, p. 080005 (2021). [Online]. Available: <https://doi.org/10.1063/5.0042312>.

- [21] H. R. Yassein, H. N. Zaky, H. H. Abo-Alsoo, I. A. Mageed, and W. I. El-Sobky, "QuiTRU: Design secure variant of NtruEncrypt via a new multi-dimensional algebra," *Appl. Math. Inf. Sci.*, vol. 17, no. 1, pp. 49-53 (2023). [Online]. Available: <http://dx.doi.org/10.18576/amis/paper>.
- [22] H. R. Yassein, N. M. G. Al-Saidi, and A. K. Farhan, "A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 2, pp. 523-542 (2020). [Online]. Available: <https://doi.org/10.1080/09720529.2020.1741218>.
- [23] A. H. Alwan, "Small intersection graph of subsemimodules of a semi-module," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2022, no. 1, pp. 15-22 (2022).
- [24] S. Ediza, M. Cancana, and M. R. Farahani, "Eccentric connectivity and connective eccentricity indices of generalized Petersen graphs," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2021, no. 1, pp. 1-6 (2021).
- [25] R. Ponraj, S. Prabhu, and M. Sivakumar, "Pair mean cordial labeling of total graph of some graphs and prism related graphs," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2024, no. 2, pp. 181-192 (2024).
- [26] F. O. Oduol and I. O. Okoth, "Counting vertices among all noncrossing trees by levels and degrees," *Commun. Combinatorics Cryptogr. Comput. Sci.*, vol. 2024, no. 2, pp. 193-212 (2024).

Received May, 2024