

A new multi-dimensional public key cryptosystem via KAH-Octo algebra

Kawthar Abdulabbas Hassoon *

*Department of Mathematics
Faculty of Education for Girls
University of Kufa
Kufa
Al Najaf 540011
Iraq*

Hassan Rashed Yassein [†]

*Department of Mathematics
Faculty of Education
University of Al-Qadisiyah
Al-Diwaniya 58003
Iraq*

Abstract

The security of information must be maintained is necessary to be maintained because different data is distributed via networks that raises the possibility of data loss. In this paper, is concerned with establishing a new public key cryptosystem called KAOTR using KAH-Octo algebra, which consists of two public keys and four private keys by submitting a high speed and acceptable security.

Subject Classification (2020): 11T71, 08C10, 12Lxx, 13L05.

Keywords: KAH-Octo Algebra, KAOTR, Key security, Message security.

* ORCID-ID: 0009-0004-4168-4952

[†] ORCID-ID: 0000-0002-6788-0247

* E-mail: kawthara.alshammari@student.uokufa.edu.iq (Corresponding Author)

[†] E-mail: hassan.yaseen@qu.edu.iq

1. Introduction

When the goal is to enhance the security of information transmission, exploring different encryption techniques can do that. Among them are OTRU introduced by Malekian and Zakerolhosseini in 2010 [4], QOBTRU introduced by Yassein et al. in 2020 [8], NTRsh introduced by Shahhadi and Yassein in 2021 [13], NTRS introduced by Shahhadi and Yassein in 2021 [11], QOTRU introduced by Abo-Alsood and Yassein in 2021 [7], BOTRU introduced by Abo-Alsood and Yassein in 2021 [6], NTRTRN introduced by Shahhadi and Yassein in 2022 [12], and TOTRU introduced by Abo-Alsood and Yassein in 2022 [5]. Several researchers have presented different cryptosystems based on some hard problems by [1-3] and [10, 14-17]. In this paper, we introduce a new KAOTR based on KAH-Octo algebra [9] and discuss its security and speed.

2. Proposed kaotr cryptosystem

Take into consideration the truncated polynomial rings $K = Z[x]/(x^N - 1)$, $K_p = Z_p[x]/(x^N - 1)$, $K_q = Z_q[x]/(x^N - 1)$ where generic parameters (N, p, q) are the same in OTRU.

Three KAH-Octo algebras are defined as follows:

$$KO = \{f_0(x) + \sum_{i=1}^7 f_i(x) \cdot \beta_i, f_i(x) \in K, i = 0, \dots, 7\},$$

$$KO_p = \{f_0(x) + \sum_{i=1}^7 f_i(x) \cdot \beta_i, f_i(x) \in k_p\},$$

and

$$KO_q = \{f_0(x) + \sum_{i=1}^7 f_i(x) \cdot \beta_i, f_i(x) \in k_q\},$$

and six subsets L_F, L_T, L_G, L_S, L_M and $L_\phi \subset KO$ as follows:

$$L_F = \{f_0(x) + \sum_{i=1}^7 f_i(x) \cdot \beta_i; f_i(x) \in K, \ell_{(d_f, d_{f-1})}\}$$

$$L_T = \{t_0(x) + \sum_{i=1}^7 t_i(x) \cdot \beta_i; t_i(x) \in K, \ell_{(d_t, d_{t-1})}\}$$

$$L_G = \{g_0(x) + \sum_{i=1}^7 g_i(x) \cdot \beta_i; g_i(x) \in K, \ell_{(d_g, d_g)}\}$$

$$L_S = \{s_0(x) + \sum_{i=0}^7 s_i(x) \cdot \beta_i; s_i(x) \in K, \ell_{(d_s, d_{s-1})}\}$$

$$L_M = \{m_0(x) + \sum_{i=1}^7 m_i(x) \cdot \beta_i; m_i(x) \in K \text{ chosen modulo during } \left(\frac{-p}{2}, \frac{p}{2}\right)\}$$

$$L_\phi = \{\sum_{i=0}^7 \phi_i(x) \cdot \beta_i; \phi_i(x) \in K, \ell_{(d_\phi, d_\phi)}\}$$

$$\text{Formula } \ell_{(d_x, d_y)} = \left\{ \begin{array}{l} f \in K; f \text{ has } d_x \text{ coefficients equal } 1, \\ d_y \text{ coefficients equal } -1, \text{ and the remaining equal } 0 \end{array} \right\}$$

The three phases of KAOTR are outlined below:

I. Key generation

The process for generating the keys needs the recipient to select randomly F, T, G , and S from the sets L_F, L_T, L_G , and L_S , such that $F = f_0(x) + \sum_{i=1}^7 f_i(x) \beta_i$, $T = t_0(x) + \sum_{i=1}^7 t_i(x) \beta_i$, $G = g_0(x) + \sum_{i=1}^7 g_i(x) \beta_i$ and $S =$

$s_0(x) + \sum_{i=1}^7 s_i(x)\beta_i$. T must be invertible $\text{mod } q$ referred to as T_q^{-1} and F must be invertible $\text{mod } p$ and $\text{mod } q$ referred to as F_p^{-1}, F_q^{-1} , respectively S must be invertible $\text{mod } p$ referred to as S_p^{-1} . The public keys are generated as $H = F_q^{-1} * G(\text{mod } q)$ and $K = S * T_q^{-1}(\text{mod } q)$, where F, T, G , and S are private keys, the key generation phase demands 16 convolution multiplications.

II. The encryption

The encryption process begins by writing the message $M \in L_M$ in the form of $M = m_0(x) + \sum_{j=1}^7 m_j(x)\beta_j$ then choose $\phi \in L_\phi$, which is known as an ephemeral value, after that the ciphertext is calculated using the formula $E = p(H * \phi) + M * K(\text{mod } q)$. The Encryption phase needs 16 convolution multiplications and eight additions of polynomials.

III. Decryption

After the receiving of E , the steps below can be used by the recipient to obtain the original message:

$$\begin{aligned} D &= F * E * T(\text{mod } q) \\ &= (pF * (H * \phi) + F * M * K) * T(\text{mod } q) \\ &= (pF * (F_q^{-1} * G * \phi) + F * M * S * T_q^{-1}) * T(\text{mod } q) \\ &= pG * \phi * T + F * M * S(\text{mod } q) \end{aligned}$$

Where the coefficients lie in the interval $(-q/2, q/2]$, let $B = D(\text{mod } p)$ so $M = F_p^{-1} * B * S_p^{-1}$ and the coefficients lie in the interval $(-p/2, p/2]$, the decryption phase needs 32 convolution multiplications and eight additions of polynomials.

3. Security analysis

Due to the public key and generic parameters being known to the KAOTR attacker, and thus he can apply a brute force attack, all potential $G \in L_G$ and $S \in L_S$ are attempting to obtain private keys G, S , assuming that the spaces L_G and L_S are smaller than L_F and L_T , respectively. The subsets L_G, L_S have sizes equal to

$$\begin{aligned} |L_G| &= \left(\binom{N}{d_g} \binom{N-d_g}{d_g} \right)^8 = \left(\frac{N!}{d_g!(N-d_g)!} \cdot \frac{(N-d_g)!}{d_g!(N-2d_g)!} \right)^8 = \left(\frac{N!}{(d_g!)^2 (N-2d_g)!} \right)^8, \\ |L_S| &= \left(\binom{N}{d_s} \binom{N-d_s}{d_s-1} \right)^8 = \left(\frac{N!}{d_s!(d_s-1)!(N-2d_s+1)!} \right)^8, \end{aligned}$$

respectively. Thus, the space of key security is equal to $|L_G| \times |L_S| = \frac{(N!)^{16}}{(d_g!)^{16} ((N-2d_g)! d_s! (d_s-1)! (N-2d_s+1)!)^8}$. Similarly, the attacker can search in the space L_ϕ to get the original message from the ciphertext, where the size of the

set L_ϕ is equal to $|L_\phi| = \left(\binom{N}{d_\phi} \binom{N-d_\phi}{d_\phi-1} \right)^8 = \left(\frac{N!}{(d_\phi!)^2 (N-2d_\phi)!} \right)^8$ which equals the space of message security.

4. Conclusion

The KAOTR is a cryptosystem that has a very high level of key security and message security compared to the NTR_{TRN} , NTRS, NTR_{SH} , and BOTRU. It is equal in terms of the key security of TOTRU and the message security of OTRU and QOTRU; it is also, less than the message security of TOTRU. As for speed, it is faster than OTRU, NTR_{TRN} , NTRS, NTR_{SH} , TOTRU, and QOTRU, and slower than BOTRU. This cryptosystem can be used in many contexts, depending on the importance of security, speed, or both, depending on the nature of the transmitted data.

References

- [1] M. Chillali and M. Sahmoudi, "SCC-Cryptosystem on an algebraic closure ring," *J. Discrete Math. Sci. Cryptography*, vol. 23, no. 8, pp. 1475-1485 (2020). [Online]. Available: <https://doi.org/10.1080/09720529.2019.1624338>.
- [2] N. Imine, N. Hadj-Said, and A. Ali-Pacha, "New McEliece cryptosystem based on non-permutation equivalent polar codes," *J. Discrete Math. Sci. Cryptography*, 2 Aug. (2021). [Online]. Available: <https://doi.org/10.1080/09720529.2021.1933706>.
- [3] 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. Cryptography*, vol. 22, no. 8, pp. 1383-1392 (2019). [Online]. Available: <https://doi.org/10.1080/09720529.2019.169244>.
- [4] A. Malekian and A. Zakerolhosseini, "OTRU: A non-associative and high speed public key cryptosystem," in *Proc. 15th CSI Int. Symp. on Computer Architecture and Digital Systems*, pp. 83-90 (2010). [Online]. Available: <https://doi.org/10.1109/CADS.2010.5623536>.
- [5] 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, pp. 1-6 (2022). [Online]. Available: <https://doi.org/10.1063/5.0067033>.

- [6] 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).
- [7] H. H. Abo-Alsood and H. R. Yassein, "QOTRU: A new design of NTRU public key encryption via Qu-Octonion subalgebra," *J. Phys.: Conf. Ser.*, vol. 1999, no. 1, pp. 1-7 (2021). [Online]. Available: <https://doi.org/10.1088/1742-6596/1999/1/012097>.
- [8] 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. Cryptography*, vol. 25, no. 2, pp. 523-542 (2020). [Online]. Available: <https://doi.org/10.1080/09720529.2020.1741218>.
- [9] K. A. Hassoon and H. R. Yassein, "Proposed multi-dimensional algebra," *Int. J. Math. Comput. Sci.*, vol. 19, no. 3, pp. 765-770 (2024).
- [10] O. Benamara and F. Merazka, "A new distribution version of Boneh-Goh-Nissim cryptosystem: Security and performance analysis," *J. Discrete Math. Sci. Cryptography*, vol. 25, no. 6, pp. 1633-1647 (2022). [Online]. Available: <https://doi.org/10.1080/09720529.2020.1782570>.
- [11] 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).
- [12] 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, pp. 1-6 (2022). [Online]. Available: <https://doi.org/10.1063/5.0067023>.
- [13] 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, pp. 1-6 (2021). [Online]. Available: <https://doi.org/10.1088/1742-6596/1999/1/012092>.
- [14] 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).

- [15] 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).
- [16] 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).
- [17] 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