International Journal of Mathematics and
Computer Science, **19**(2024), no. 1, 37–40

A High-Security Encryption Based on Hexadecnion Polynomials

Baneen Najah Abbas[1], **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
Al-Qadisiyah, Iraq

email: Najahbanen2@gmail.com, hassan.yaseen@qu.edu.iq

(Received May 2, 2023, Accepted June 24, 2023,
Published August 31, 2023)

Abstract

With technological development, hackers are possible to access the transmitted data, so we need to constantly develop encryption methods to increase security. In this paper, we have introduced a new cryptosystem hexadecnion polynomial RSA (PH-RSA) by mixing NTRU and polynomial RSA based on a hexadecnion polynomial instead of polynomial RSA with a high level of security.

1 Introduction

Communication networks are expanding at a rapid pace due to the increasing use of the Internet. As a result, the need to constantly need to develop data encryption and increase its security appears.

Keywords and phrases: Polynomial RSA, Hexadecnion algebra, Security of key.
AMS (MOS) Subject Classifications: 94A60, 68P25.
ISSN 1814-0432, 2024, http://ijmcs.future-in-tech.net

In 1978, Rivest et al. proposed a public-key cryptosystem RSA depends on factoring problem, it is a relatively slow algorithm [1]. This is where the NTRU cryptosystem plays a leading role since it is capable of providing adequate levels of security at an extremely low cost. In 1996, Hoffstein et al. presented NTRU public key cryptosystem, which uses the ring of truncated polynomials $Z[x]/\left(x^N - 1\right)$ [2]. In 2015, Gafitoiu proposed a polynomial RSA by using polynomials instead of integers [3]. In 2016, Yassein and Al-Saidi, introduced HXDTRU cryptosystem based on hexadecnion algebra [4]. In this paper, we propose a new cryptosystem known as the PH-RSA based on hexadecnion polynomial and discuss security analysis.

2 PH-RSA cryptosystem

A public key hexadecnion polynomial RSA which is denoted by PH-RSA is determined by the same parameters as polynomial RSA, but the polynomial ring $Z_p[x]$ is replaced by hexadecnion algebra $HD = \{w|w = r_0 + \sum_{i=1}^{15} r_i x_i$ $|r_0, r_1, \ldots, r_{15} \in R\}$ [4], and the subsets L_F and L_G are defines as follows:
$L_F = \{f_0(x) + \sum_{i=1}^{15} f_i(x)x_i \in HD$ satisfy $\tau(d_f, d_{f-1})\}$,
$L_G = \{g_0(x) + \sum_{i=1}^{15} g_i(x)x_i \in HD$ satisfy $\tau(d_g, d_g)\}$,
where $\tau(d_x, d_y) = \{f$ has d_x coefficients equal 1, d_y coefficients equal -1 and the rest 0 $\}$.

The cryptosystem phases of PH-RSA are as follows:

I. **Key Generation** In this way, we construct the key as follows:

(a) Choose two irreducible polynomials $P(x), Q(x) \in HD$ as:
$P(x) = f_0(x) + \sum_{i=1}^{15} f_i(x)x_i$ and $Q(x) = g_0(x) + \sum_{i=1}^{15} g_i(x)x_i$ such that $P(x)Q(x) = N(x)$

(b) Take $R = HD/ < N(x) > = \{$ all possible remainders when each polynomial in HD is divided by $N(x)\}$,

(c) Choose $e \in Z_s = \{0, 1, 2, \ldots, s-1\}$ such that $gcd(e,\ s) = 1$.

(d) Find $d \in Z_s$ such that $ed = 1\ mod\ s$ ($d = e^{-1}\ mod\ s$ multiplication inverse).

II. **Encryption**
The primary message $M(x) = m_0(x) + \sum_{i=1}^{15} m_i(x)x_i$ is encrypted in accordance with the following formula:

$$C(x) = \left[m_0(x) + \sum_{i=1}^{15} m_i(x)x_i\right]^e\ mod\ N(x).$$

III. **Decryption**

After received the ciphertext $C\left(x\right) = C_0\left(x\right) + \sum_{i=1}^{15} C_i(x)x_i$, by the receiver take the following steps to restore the original text:

$$\begin{aligned} C[x]^d &= \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} \ mod\ N\left(x\right) \\ &= \left[\left(m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right)^s\right]^k \cdot \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] mod\ N\left(x\right) \\ &= \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] mod\ N\left(x\right). \end{aligned}$$

If $M(x)$ does not have an inverse modulo $N(x)$, then $P(x)$ and $Q(x)$ can be substituted for s, respectively, as congruence modulo,
$\left[\left(m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right)^{(p^m-1)(p^n-1)}\right]^k \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] \equiv$
$\left[\left(m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right)^{(p^n-1)}\right]^{k(p^m-1)}.$
$\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] mod\ P(x),$
$\left[\left(m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right)^{(p^m-1)(p^n-1)}\right]^k \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] \equiv$
$\left[\left(m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right)^{(p^m-1)}\right]^{k(p^n-1)}$
$\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] mod\ Q(x),$
$\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} \equiv 1^{k(p^m-1)} \left[\ m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] mod\ P(x)$
$\equiv \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] mod\ P(x)$
$\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} \equiv 1^{k\ (p^n-1)} \left[\ m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] mod\ Q(x)$
$\equiv \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] mod\ Q(x).$
Therefore, $\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} - \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]$
$\equiv 0\ mod\ P\left(x\right),$
$\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} - \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] \equiv 0\ mod\ Q\left(x\right).$
$Hence$ $\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} - \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\ \right]$ divisible by $P(x)$ and $Q(x)$. Because $P\left(x\right)$, $Q(x)$ are irreducible and not associated, then $\left[\ m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} - \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]$ is divisible by $P\left(x\right)\ Q(x)$. Therefore,
$\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} - \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right] \equiv o\ mod\ P\left(x\right)$
$Q\left(x\right).$ Hence $\left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]^{ed} \equiv \left[m_0\left(x\right) + \sum_{i=1}^{15} m_i\left(x\right)x_i\right]$

$mod\ N(x)$. As a consequence, the decryption formula returns the original message $M(x)$.

3 Security Analysis for PH-RSA

In a brute-force assault, the attacker uses public parameters and $N(x) = a_0(x) + \sum_{i=1}^{n-1} a_i x^i$ to search the sets L_F and L_G for the private key $P(x)$ or $Q(x)$. As a result, the security key for PH-RSA is

$$\left(\frac{n_1!}{(d_f!)^2 (n_1 - 2d_f)!}\right)^{16} 1 \leq n_1 < n-1 \text{ or } \left(\frac{n_2!}{(d_g!)^2 (n_2 - 2d_g)!}\right)^{16} 1 \leq n_2 < n-1.$$

4 Conclusion

Hexadecnion polynomial RSA is an improvement of polynomial RSA by replacing each polynomial in polynomial RSA with sixteen polynomials which is an element in hexadecnion algebra HD making it more secure, in addition to the possibility of encrypting multiple messages at a round.

References

[1] R. Rivest, A. Shamir, L. Adleman, A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, Communications of the ACM, **21,** no. 4, (1978), 120–126.

[2] J. Hoffstein, J. Pipher, J. H. Silverman, NTRU: A ring-based public key cryptosystem, in Algorithmic Number Theory, Proceedings of the Third International Symposium, (1998), 267–288.

[3] I. B. Gafitoiu, Polynomial based RSA, Bachelor Thesis, Linnaeus University, Sweden, (2015).

[4] H. R. Yassein, N. M. Al-saidi, HXDTRU cryptosystem based on hexadecnion algebra, Proceedings of the 5th International Cryptology and Information Security Conference, Kota Kinabalu, Malaysia, (2016), 1–14.