Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/170321

PMRSA: Designing an Efficient and Secure Public-Key Similar to RSA Based on Polynomial Ring

Fatima Rheem Atea[1] *and Hassan Rashed Yassein*[2,*]

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

Received: 3 Jan. 2023, Revised: 12 Feb. 2023, Accepted: 25 Feb. 2023
Published online: 1 May 2023

Abstract: RSA and NTRU encryption methods it is the still used nowadays and they constantly evolving simultaneously, thus paper proposed an encryption method based on linking the concepts of NTRU and modified RSA by using polynomials ring $Z_{\mathfrak{p}}[\varkappa]/<\mathscr{N}(\varkappa)>$ through generate two public keys, consisting four polynomials private key, this increase increases the complexity algorithm, in spite of this method is slows although this method is slow, it gives a high efficiency of security.

Keywords: RSA, NTRU, modified RSA, Polynomials ring.

1 Introduction

Because the case with the development in information technology and the increase in electronic transactions, where the information of individuals and companies is all in the cloud of the internet, information and data become more and more at risk of being hacked so the world constantly needs to develop known encryption methods. Among the public-key encryption methods, the RSA encryption algorithm, which was created by Rivest et al. in 1979, relies on the use of parameters from prime numbers mainly [1]. Also, the NTRU encryption algorithm, which was established in 1996 by Hoffstein et al. and relies on its work on truncated polynomials known as the ring $Z[\varkappa]/(\varkappa^{N-1})$ [2]. The researchers presented many studies on the development of RSA, including: In 2012, Ivy et al. used a modified algorithm of the RSA cipher system to handle prime numbers and provide security by using a prime number that cannot be broken easily [3]. In 2015, Gafitoiu introduced the polynomial RSA encryption system, which gave complex mathematical operations in encryption and decryption, which increased its security [4]. The researchers also gave lots of studies on the improvement of NTRU, including: In 2016, HXDTRU and BITRU, which are used algebra of hexadecnion and binary as analogs of the NTRU cipher system, were presented by Yassein and Al-Saidi [5,6,7]. BCTRU, an NTRU-like multidimensional cipher system based on Cartesian binary algebra, was developed by Yassin and Al-Saidi in 2018 [8,9]. In 2020, Yassein et al. proposed a multidimensional algebra to design an improved cipher scheme for NTRU [10,11]. In 2021, many researchers. prepared a new NTRU versions with good levels of performance and security [12,13,14,15, 16]. In 2022, Al-Awadi proposed a public key QP-RSA that depends on quaternion algebra to get high security [17]. In the same year, QOBTRU, NTRU-like cryptosystem relies on carternion algebra, suggested by Yassein et al. [18]. In 2023, through a novel mathematical structure, Yassein et al. presented a brand-new multidimensional asymmetric, called HUDTRU, used quintuple algebra [19]. In addition to this section, the next section, we describe our submitted PMRSA cryptosystem in detail. Finally, in section 3, we present our conclusions.

2 PMRSA Cryptosystem

PMRSA (Polynomial modified RSA) depend on the polynomial ring $Z_{\mathfrak{p}}[\varkappa]=\{z_0+z_1\varkappa+z_2\varkappa^2+\ldots+z_k\varkappa^k \mid k\geq 0,\ z_i\in Z_{\mathfrak{p}}\}$, addition and multiplication are performed as modulo a polynomial, and $\mathfrak{p}$ is a prime number. Let $\omega=Z_{\mathfrak{p}}[\varkappa]/<\mathscr{N}(\varkappa)>$ ={all possible remainders when any polynomial in $Z_{\mathfrak{p}}[\varkappa]$ is divided by $\mathscr{N}(\varkappa)$}. This cryptosystem consists of the following steps:

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

2.1 Key generation

To configure the key we have to follow the following steps:

– Choose four irreducible polynomials not associated $\mathrm{A}(\varkappa), \mathrm{B}(\varkappa), \mathrm{C}(\varkappa)$ and $\mathfrak{D}(\varkappa) \in Z_{\mathfrak{p}}[\varkappa]$ such that:

$$\mathrm{A}(\varkappa) = \sum_{i=0}^{m} a_i\varkappa^i, \mathrm{B}(\varkappa) = \sum_{i=0}^{n} b_i\varkappa^i, \mathrm{C}(\varkappa) = \sum_{i=0}^{r} c_i\varkappa^i, \mathfrak{D}(\varkappa) = \sum_{i=0}^{t} a_i\varkappa^i$$

– Calculate $\mathcal{N}_1(\varkappa) = \mathrm{A}(\varkappa)\mathrm{B}(\varkappa)$ and $\mathcal{N}_2(\varkappa) = \mathrm{C}(\varkappa)\,\mathfrak{D}(\varkappa)$ such that $s_1 = (\mathfrak{p}^m - 1)(\mathfrak{p}^n - 1)$ number of invariable elements in ω modulo $\mathcal{N}_1(\varkappa)$ and $s_2 = (\mathfrak{p}^r - 1)(\mathfrak{p}^t - 1)$ number of invariable elements in ω modulo $\mathcal{N}_2(\varkappa)$.
– Compute $\mathcal{N}(\varkappa) = \mathrm{A}(\varkappa)\mathrm{B}(\varkappa)\mathrm{C}(\varkappa)\,\mathfrak{D}(\varkappa)$ in which $s = (\mathfrak{p}^m - 1)(\mathfrak{p}^n - 1)(\mathfrak{p}^r - 1)(\mathfrak{p}^t - 1)$ number of invariable elements in ω modulo $\mathcal{N}_1(\varkappa)$.
– Choose $0 \le e_1 < s_1$, $0 \le e_2 < s_2$ such that gcd $(e_1, s_1) = 1$ and gcd $(e_2, s_2) = 1$.
– Find d such that $de_1 = 1 \mod s(d = {e_1}^{-1} \mod s$ multiplication inverse), $e_1 d = k_1 s + 1$ and g such that $ge_2 = 1 \mod s$ $(g = {e_2}^{-1} \mod s$ multiplication inverse) $e_2 g = k_2 s + 1$.

2.2 Encryption

The original message $M(\varkappa)$ is converted to ciphertext by applying the formula:

$$\mathrm{C}(\varkappa) = \left([\mathtt{M}\ (\varkappa)]^{e_1} \bmod \mathcal{N}(\varkappa)\right)^{e_2} \bmod \mathcal{N}(\varkappa).$$

2.3 Decryption

To decrypt the encrypted message $C(\varkappa)$ to find the plaintext $M(\varkappa)$, the recipient performs the following steps:

$$\begin{aligned}
(C(\varkappa))^{gd} \bmod \mathcal{N}(\varkappa) &\equiv \left([\mathtt{M}\ (\varkappa)]^{e_1 e_2}\right)^{gd} \bmod \mathcal{N}(\varkappa)\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{e_1 d e_2}\right)^{g} \bmod \mathcal{N}(\varkappa)\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{(k_1 s+1)e_2}\right)^{g} \bmod \mathcal{N}(\varkappa)\\
&\equiv \left((\mathtt{M}\ (\varkappa))^{(k_1 e_2)}(\mathtt{M}\ (\varkappa))^{e_2}\right)^{g} \bmod \mathcal{N}(\varkappa)\\
&\equiv (\mathtt{M}\ (\varkappa))^{e_2 g} \bmod \mathcal{N}(\varkappa)\\
&\equiv (\mathtt{M}\ (\varkappa))^{sk_2+1} \bmod \mathcal{N}(\varkappa)\\
&\equiv (\mathtt{M}\ (\varkappa))^{sk_2}\mathtt{M}\ (\varkappa) \bmod \mathcal{N}(\varkappa)\\
&\equiv \mathtt{M}\ (\varkappa) \bmod \mathcal{N}(\varkappa).
\end{aligned}$$

If the message $\mathtt{M}\ (\varkappa)$ is first encrypted as an integer in $\mathrm{Z}_n[\varkappa]$, $gcd\mathtt{M}\ (\varkappa)\ \mathcal{N}(\varkappa)$; We write the decryption formula as before, but this time modulo $\mathrm{A}(\varkappa)$, $\mathrm{B}(\varkappa)$, $\mathrm{C}(\varkappa)$ and $\mathfrak{D}(\varkappa)$ respectively

$$\begin{aligned}
(\mathrm{C}(\varkappa))^{gd} \, mod\, \mathcal{N}(\varkappa) &\equiv \left([\mathtt{M}\ (\varkappa)]^{e_1 e_2}\right)^{gd} \bmod \mathrm{A}(\varkappa)\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{e_1 e_2}\right)^{gd} \bmod \mathrm{B}(\varkappa)\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{e_1 e_2}\right)^{gd} \bmod \mathrm{C}(\varkappa)\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{e_1 e_2}\right)^{gd} \bmod \mathfrak{D}(\varkappa)
\end{aligned}$$

By Substitute for s in the previously defined formula

$$\begin{aligned}
&(\mathrm{C}(\varkappa))^{gd} \bmod \mathcal{N}(\varkappa) \equiv \left([\mathtt{M}\ (\varkappa)]^{(sk_1+1)e_2}\right)^{g}\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{(((\mathfrak{p}^m-1)(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1))k_1+1)e_2}\right)^{g} \bmod \mathrm{A}(\varkappa)\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{(\mathfrak{p}^m-1)(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_1 e_2}\right)^{g}\\
&\quad [\mathtt{M}\ (\varkappa)]^{e_2 g} \bmod \mathrm{A}(\varkappa)\\
&\equiv \left([\mathtt{M}\ (\varkappa)^{(\mathfrak{p}^m-1)}]^{(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_1 e_2}\right)^{g}\\
&\quad [\mathtt{M}\ (\varkappa)]^{e_2 g} \mathrm{mod} \mathrm{A}(\varkappa)\\
&\equiv (1)^{(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_1 e_2 g}[\mathtt{M}\ (\varkappa)]^{e_2 g} \bmod \mathrm{A}(\varkappa)\\
&\equiv [\mathtt{M}\ (\varkappa)]^{e_2 g} \bmod \mathrm{A}(\varkappa) \equiv [\mathtt{M}\ (\varkappa)]^{sk_2+1} \bmod \mathrm{A}(\varkappa)\\
&\equiv [\mathtt{M}\ (\varkappa)]^{sk_2 sk_2}\mathtt{M}\ (\varkappa) \bmod \mathrm{A}(\varkappa)\\
&\equiv [\mathtt{M}\ (\varkappa)]^{(\mathfrak{p}^m-1)(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_2}\mathtt{M}\ (\varkappa) \bmod \mathrm{A}(\varkappa)\\
&\equiv [\mathtt{M}\ (\varkappa)^{(p^m-1)}]^{(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_2}\mathtt{M}\ (\varkappa) \bmod \mathrm{A}(\varkappa)\\
&\equiv [1]^{(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_2}\mathtt{M}\ (\varkappa) \bmod \mathrm{A}(\varkappa)\\
&\equiv \mathtt{M}\ (\varkappa) \bmod \mathrm{A}(\varkappa)
\end{aligned}$$

In the same way,

$$\begin{aligned}
&(\mathrm{C}(\varkappa))^{gd} \bmod \mathcal{N}(\varkappa) \equiv \left([\mathtt{M}\ (\varkappa)]^{(sk_1+1)e_1}\right)^{g}\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{(((\mathfrak{p}^m-1)(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1))k_1+1)e_2}\right)^{g} \bmod \mathrm{B}(\varkappa)\\
&\equiv [1]^{(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_2}\mathtt{M}\ (\varkappa) \bmod \mathrm{B}(\varkappa)\\
&\equiv \mathtt{M}\ (\varkappa) \bmod \mathrm{B}(\varkappa)
\end{aligned}$$

$$\begin{aligned}
&(\mathrm{C}(\varkappa))^{gd} \bmod \mathcal{N}(\varkappa) \equiv \left([\mathtt{M}\ (\varkappa)]^{(sk_1+1)e_1}\right)^{g}\\
&\equiv \left([\mathtt{M}\ (\varkappa)]^{(((\mathfrak{p}^m-1)(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1))k_1+1)e_2}\right)^{g} \bmod \mathrm{C}(\varkappa)\\
&\equiv [1]^{(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_2}\mathtt{M}\ (\varkappa) \bmod \mathrm{C}(\varkappa)\\
&\equiv \mathtt{M}\ (\varkappa) \bmod \mathrm{C}(\varkappa)
\end{aligned}$$

$$(\mathrm{C}(\varkappa))^{gd} \bmod \mathscr{N}(\varkappa) \equiv \left([\mathtt{M}\ (\varkappa)]^{(sk_1+1)e_1}\right)^g$$
$$\equiv \left([\mathtt{M}\ (\varkappa)]^{(((\mathfrak{p}^m-1)(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1))k_1+1)e_2}\right)^g \bmod \mathfrak{D}(\varkappa)$$
$$\equiv [1]^{(\mathfrak{p}^n-1)(\mathfrak{p}^r-1)(\mathfrak{p}^t-1)k_2} M(\varkappa) \bmod \mathfrak{D}(\varkappa)$$
$$\equiv \mathtt{M}\ (\varkappa) \bmod \mathfrak{D}(\varkappa)$$

3 Conclusions

This paper introduces an encryption algorithm called PMRSA. It works on the product of four polynomials $\mathrm{A}(\varkappa), \mathrm{B}(\varkappa), \mathrm{C}(\varkappa)$ and $\mathfrak{D}(\varkappa) \in Z_{\mathfrak{p}}[\varkappa]$ which using in NTRU instead of two polynomials as is the case with the polynomial RSA algorithm. This technology provides more efficiency and reliability across networks, and also, increases security by the difficulty of breaking the key which increases the time required for that due to the increase to the number of keys, the attacker requires to know, because the attacker in PMRSA searches the sample space for four private keys instead of two in polynomial RSA.

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] J. Hoffstein, J. Pipher and J. Silverman, NTRU: a ring based public key cryptosystem, *Int. Algorithmic Number Theory Symp*, **1423**, 267-288 (1998).
[3] B. Persis Urbana Ivy, P. Mandiwa and M. Kumar, A modified RSA cryptosystem based on 'n' prime numbers, *International Journal of Engineering and Computer Science*, **1**, 63-66 (2012).
[4] I. B. Gafitoiu, *Polynomial based RSA*, B.Sc Thesis, Linnaeus University, Sweden, (2015).
[5] H R. Yassein and N M. Al-Saidi, *HXDTRU cryptosystem based on hexadecnion algebra*, Proc. 5th Int. Cryptology and Information Security Conf., 1-14, (2016a).
[6] N M. Al-Saidi and 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).
[7] H. R. Yassein and 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 (2016a).
[8] H. R. Yassein and N. M. Al-Saidi, *BCTRU: a new secure NTRUcrypt public key system based on a newly multidimensional algebra*, In proc. 6th Int. Cryptology and Information Security conf., **6**, 1-11, (2018).
[9] 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).
[10] H. R. Yassein, N. M. Al-Saidi and 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).
[11] 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).
[12] 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, 080005-1-080005-4, (2021).
[13] S. H. Shihadi and 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).
[14] S. H. Shahhadi and H. R. Yassein, NTRsh: A New Secure Variant of NTRU Encrypt Based on Tripternion Algebra, *Journal of physics conference series*, **1999**, 2-6 (2021).
[15] H. H. Abo-Alsood and H. R. Yassein, QOTRU: A New Design of NTRU Public Key Encryption Via Qu-Octonion Subalgebra, *In Journal of Physics: Conference Series*, 1-7 (2021).
[16] 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).
[17] M. H. Al-Awadi, *Designing an Efficient and Secure Cryptosystems Similar to MaTRU and RSA*, M. Sc. Thesis, University of Al-Qadisiyah, Iraq, (2022).
[18] H. R. Yassein, N. M. Al-Saidi and A. K. Farhan, A new NTRU cryptosystem outperforms three highly secured NTRU-analog systems through an innovational algebraic structure, *Journal of Discrete Mathematical Sciences and Cryptography*, **25**, 523-542 (2022).
[19] H. R. Yassein and H. A. Ali, HUDTRU: An Enhanced NTRU for Data Security via Quintuple Algebra, *International Journal of Mathematics and Computer Science*, **2**, 199–204 (2023).

Fatima Rheem Atea Completed the B.Sc. in mathematics from the college of education for pure science Al-Muthanna University in 2018. Now a master's student at the faculty of education for girls university of Kufa 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.