Bol. Soc. Paran. Mat.
©SPM – E-ISSN-2175-1188
SPM: www.spm.uem.br/bspm

(3s.) **v. 2025 (43)** : 1–4.
ISSN-0037-8712
doi:10.5269/bspm.77183

Comparative Analysis between Some Cryptosystems based on Truncated Polynomials Ring and DNA

Fatimah H. Albakaa and Hassan Rashed Yassein*

ABSTRACT: DNA encryption is currently an effective method due to its numerous advantages in terms of security, randomness, and multiple text representation options. Numerous developments and improvements have emerged in DNA encryption methods to counter various attack methods that attempt to access the original data. In this paper, we present a comparison of encryption systems primarily based on DNA encryption PDNA, PODNA, and FDNA in terms of security and speed, making it easier for users to choose the appropriate method based on the nature of the transmitted data.

Key Words: PODNA, FDNA, PODNA, Security Space, Execution time.

Contents

1. Introduction

One of the properties of DNA is its tremendous capacity to store information and the large randomness of its components, which exceeds all known methods. Therefore, Gehani et al. exploited this ability by applying it to encrypting information and storing it in a system called DNA cryptosystem in 1999 [6]. In 2010, the $OTRU$ cryptosystem was introduced by Malekian and Zakerolhosseini, which is a non-associative system based on NTRU encryption with octonion algebra [7]. In 2011 Yunpeng et al. proposed a symmetric cryptosystem scheme based on DNA cryptosystem [10]. In 2018, Nafea and et al. proposed a new algorithm called the OTP-DNA cryptosystem scheme [8]. In 2022, Abo-Alsood and Yassein proposed a two public-key octonion algebra cryptosystem called $TOTRU$ [3]. In 2023, Yassein and Abo-Alsood proposed compression the NTRU and $OTRU$ encryption systems with some other system in terms of algebraic construction, speed, and security [9]. In 2024, the TPRSA encryption system was introduced by Abass and Yassein via polynomials and Tri-Cartesian algebra [1]. In 2024, a new DNA cipher is presented by Abidulzahra based on combining the idea to use the DNA based on codons and truncated polynomials ring [2]. In 2025, Albakaa and Yassein introduced a new cryptosystem via algebra polynomials with DNA called $FDNA$ [4]. Also, they proposed $PODNA$ depends on polynomials and DNA octonion DNA [5].

2. Size of Space Security

The security level of the PDNA depends on two keys $\mathcal{G}$ of length n which represents a specific DNA sequence and $\mathcal{F}$ which is a polynomial belonging to truncated polynomials ring of degree N.

While in the FDNA, the private keys, which are $\mathcal{X}$ represented by random codes of length n and polynomials $\mathcal{F}$ and $\mathcal{G}$, are what determine the level of security.

As for the PODNA, the three polynomial keys $\mathcal{F}, \mathcal{G}$, and $\mathcal{W}$ for the public key $\mathcal{K}$ and one key $\mathcal{H}$ whose security depends on the number of possibilities of length n are what determine the security level of the method.

* Corresponding author

Submitted June 04, 2025. Published July 11, 2025
2010 *Mathematics Subject Classification:* 94A60. 68P25.

Therefore, the number of attempts that represent the safety level of the three methods is:

Table 1: Size of key space for $PDNA, FDNA$, and $PODNA$

Methods	Size of space
$PDNA$	$4^{\tau}\frac{N!}{d_f!\ (d_f-1)!\ (N-2d_f+1)!}$
FDNA	$4^{\tau}\frac{N!}{d_f!(d_f-1)!(N-2d_f+1)!}$ or $4^{\tau}\frac{N!}{d_g!(d_g-1)!(N-2d_g+1)!}$
PODNA	$4^{\tau}\left(\frac{N!}{d_f!(d_f-1)!(N-2d_f+1)!}\right)^8 \left(\frac{N!}{d_g!(d_g-1)!(N-2d_g+1)!}\right)^8$

Where τ represents the length of the DNA sequence, d_f is the number of coefficients of the polynomial, d_g is the number of coefficients of the polynomial, and N represents the degree of the polynomial.

According the values of public parameters in Table 2, the level of security show in Figure 1.

Table 2: Values of public parameters

N	d_f	d_g
107	12	5
107	20	10
149	12	10
149	25	20
167	18	18
167	27	22
211	20	18
211	34	22
257	20	18
257	24	24

Now, in Table 3 show the compared of key space between $PDNA$, $FDNA$, and $PODNA$ based on values of the variables in Table 2.

Table 3: Key space security for $FDNA$, $PODNA$, and $PDNA$

Key Space of $PDNA$	Key Space of $FDNA$	Key Space of $PODNA$
2.1678×10^{31}	3.0968×10^{30}	3.1514×10^{235}
9.0907×10^{41}	2.6737×10^{41}	9.7297×10^{322}
2.2573×10^{36}	2.1498×10^{35}	6.3321×10^{265}
4.3426×10^{56}	1.0856×10^{56}	2.6780×10^{431}
1.7736×10^{50}	2.4185×10^{49}	6.0516×10^{369}
2.3281×10^{63}	5.5138×10^{62}	4.4168×10^{476}
1.9921×10^{59}	2.3164×10^{58}	1.5966×10^{433}
4.3557×10^{80}	1.0284×10^{80}	2.4103×10^{606}
1.7961×10^{64}	1.6478×10^{63}	3.8999×10^{463}
1.1917×10^{72}	1.3619×10^{71}	8.4911×10^{526}

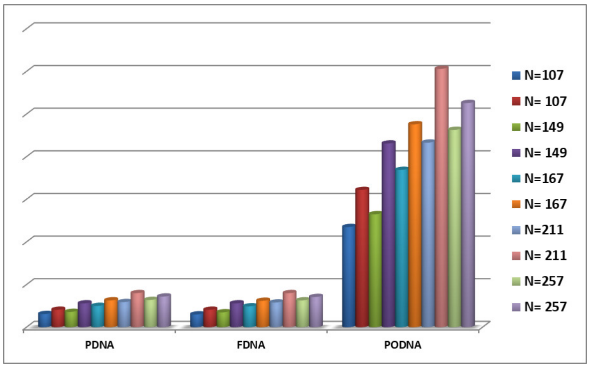

Figure 1: Comparison size of key space of $PDNA$, $FDNA$, and $PODNA$

It is clear that $PODNA$ is much more security then $FDNA$, then $PDNA$ ($FDNA$ is more security than $PDNA$ because there are two ways to reach the key).

3. Execution Time

The execution time of the three operations depends on the time required to perform polynomial operations (addition and multiplication) and codon combination operations in the three stages of key generation, encryption, and decryption, which can be illustrated in the following Table 4.

Table 4: Execution Time for $FDNA, PODNA$, and $PDNA$

Cryptosystem	$FDNA$	$PODNA$	$PDNA$
Execution Total Time	$4t_0 + 2t_1$	$4672t_0 + 2t_1$	$2t_0 + 2t_1$

Where t_0 represent the time of multiplication polynomials, t_1 represent the time of merge the codons Therefore, the execution time of $FDNA$ is faster than $PODNA$ and slower than $PDNA$.

Figure 2 shows the compared of execution Time for $PDNA, FDNA$, and $PODNA$.

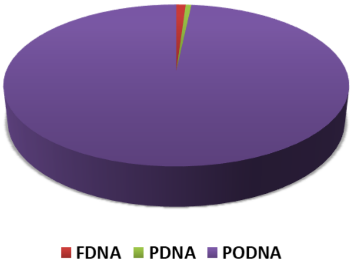

Figure 2: Execution Time for $FDNA, PODNA$, and $PDNA$

4. Conclusion

In this research paper, we compare three encryption schemes: PDNA, FDNA, and PODNA, which all share a common mathematical structure, such as DNA structure and polynomials, in terms of security, speed, and selection based on the nature of the transmission data. It turns out that PODNA is more secure than FDNA, and that FDNA is more secure than PDNA. Therefore, PODNA is the most secure of the three methods mentioned. In terms of speed, PDNA is the fastest. Therefore, if the user needs a method with high security at the expense of time, we choose PODNA, while if the user needs speed with acceptable security, we choose FDNA.

References

1. B. N. Abass and H. R. Yassein. Design of an alternative to polynomial modified rsa algorithm. *Computer Science*, 19(3):693–696, 2024.
2. A. A. Abidulzahra. *Designing Secure Public Key Cryptosystems Based on NTRU and DNA*. M.sc. thesis, University of Al-Qadisiyah, 2024.
3. H. H. Abo-Alsood and H. R. Yassein. Analogue to ntru public key cryptosystem by multi-dimensional algebra with high security. *AIP Conference Proceedings*, 2386(1):060006, 2022.
4. F. H. Albakaa and H. R. Yassein. A new encryption scheme based on dna and polynomials with more security. *International Journal of Mathematics and Computer Science*, 20:383–386, 2025.
5. F.H. Albakaa and H.R. Yassein. A new method of encryption based on octonion algebra and dna. *AIP Conference Proceedings*, 2025. Accepted for publication.
6. A. Gehani, T. H. LaBean, and J. H. Reif. Dna-based cryptography. In *5th DIMACS Workshop on DNA Based Computers*, MIT, 1999.
7. E. Malekian and A. Zakerolhosseini. OTRU: A non-associative and high speed public key cryptosystem. In *2010 15th CSI International Symposium on Computer Architecture and Digital Systems*, pages 83–90, Tehran, Iran, 2010. IEEE.
8. S. S. Nafea and M. K. Ibrahem. Cryptographic algorithm based on dna and rna properties. *Int. J. Adv. Res. Comput. Eng. Technol.*, 7:804–811, 2018.
9. H. R. Yassein and H. H. Abo-Alsood. Performance analysis of some analog NTRU public key. *AIP Conference Proceedings*, 2845(1):050038, September 2023.
10. Z. Yunpeng, Z. Yu, W. Zhong, and R. O. Sinnott. Index-based symmetric dna encryption algorithm. In *2011 4th International Congress on Image and Signal Processing*, volume 5, pages 2290–2294, Shanghai, China, 2011. IEEE.

Fatimah H. Albakaa,
Department of Mathematics,
College of Education of Women, University of Kufa,
Iraq.
E-mail address: fatema.albakaa@atu.edu.iq

and

Hassan Rashed Yassein,
Department of Mathematics,
College of Education, University of Al-Qadisiyah,
Iraq.
E-mail address: hassan.yaseen@qu.edu.iq