Mikailalsys Journal of Advanced Engineering International

e-ISSN : 3046-9694
p-ISSN : 3046-8914

Index : Harvard, Boston, Sydney University, Dimensions, Lens, Scilit, Semantic, Google, etc

https://doi.org/10.58578/MJAEI.v2i3.7367

Enhancing TARIG Transform-Based Encryption Using Nonlinear Permutation Polynomial over Prime Fields

Domven Lohcwat, Daniel Danladi, Patrick Pam Peter, Abbas Saleh Bailey
Karl K*ü*mm University, Vom, Plateau State, Nigeria
lohcwatlar@gmail.com; danladid@kku.edu.ng

Article Info:

Submitted:	Revised:	Accepted:	Published:
Aug 25, 2025	Sep 16, 2025	Sep 28, 2025	Oct 3, 2025

Abstract

The Affine Cipher, when implemented via the Tarig Transform, provides a straightforward and efficient approach to data encryption but is constrained by a limited key space and susceptibility to known-plaintext attacks. To overcome these shortcomings, this study proposes an enhanced encryption scheme that incorporates polynomial-based transformations into the Affine-based Tarig Transform framework. By introducing nonlinear polynomial mappings, the proposed method significantly expands the key space, enhances diffusion properties, and strengthens resistance to cryptanalytic techniques. Experimental evaluations confirm that the polynomial-based approach offers improved security metrics, including greater statistical randomness, while preserving computational efficiency comparable to the original implementation. These findings indicate that the enhanced scheme presents a viable and more secure alternative to conventional Affine Cipher methods for robust data communication.

Keywords: Tarig Transform; Cryptography; Nonlinear Function; Encryption; Decryption

INTRODUCTION

Cryptography is the mathematical science of protecting information by concealing its content. It allows sensitive data to be stored or transmitted over insecure channels such as the internet so that only authorized recipients can access it. Encryption converts readable information, known as plaintext, into an unreadable format called ciphertext, while decryption reverses the process, restoring ciphertext back to plaintext. As a discipline, cryptography plays a crucial role in ensuring communication confidentiality and data protection historically serving to secure exchanges between individuals. Over the years, various encryption algorithms have been developed using mathematical tools such as the Laplace transform [1, 2] and other integral transforms, including the Mahgoub [3], Aboodh [4] and El-Zaki transforms [5]. Most cryptographic schemes based on integral transforms first convert plaintext into numerical form before applying transformations. Recently, [6] gave an encryption and decryption algorithm based on Tarig transformation and congruence modulo, though the Affine Cipher, when applied through the Tarig Transform, offers a simple and efficient means of encrypting data, yet suffers from limited key space and vulnerability to known-plaintext attacks. To address these limitations, this paper presents a polynomial-based encryption scheme as an enhancement to the traditional Affine-based Tarig Transform method.

Related Work

Information security comprises a set of practices designed to prevent unauthorized access or modification of data. When an attacker bypasses firewalls, passwords, and other preventive measures, cryptography becomes the final defense, ensuring that sensitive information remains unreadable. Thus, cryptography is essential for protecting both personal and organizational data. Two widely used cryptographic approaches are symmetric key and asymmetric key systems. Symmetric (private key) methods are generally more efficient for encrypting large data volumes and require less computational power than asymmetric techniques [7]. Within symmetric cryptography, block ciphers are fundamental, with the substitution permutation network (SPN) being one of the most popular structures [8, 9]. SPN-based ciphers transform plaintext into ciphertext through multiple rounds of substitution and permutation. The substitution step employs an **S-box** to replace bit blocks, providing *confusion*, while the permutation step rearranges bits or bytes, providing *diffusion*, as defined by Claude Shannon. Well-known block ciphers such as AES, SHARK, SQUARE, and DES employ this principle. The nonlinear nature of S-boxes significantly strengthens

cipher security [9], and SPN structures ensure that even minor key changes produce drastically different ciphertext [10]. [2] proposed a block cipher scheme based on the series expansion of $f(rt)$, where the plaintext letters (encoded as 1–26) are multiplied by the coefficients of the initial series terms. The Laplace transform of the resulting series is computed, and its coefficients reduced modulo 26 form the ciphertext, with the modular quotients serving as the secret key. Decryption uses the inverse Laplace transform. However, [11] and [12] identified the method as weak because it does not rely on the Laplace transform for security; the ciphertext can be decrypted using basic modular arithmetic. [13] modified the process by selecting coefficients from n random terms of the series for a plaintext of length n. Numerous Laplace transform-based encryption schemes have since been discussed in the literature [14, 6, 15, 16, 17]. More recently, [18] introduced a cryptosystem combining the Laplace transform with a substitution permutation network. The encryption process involves multiple cycles, adding the secret key in each round, and substituting Laplace transform outputs using S-box values determined by quotient and remainder operations on block lengths. Security and statistical analysis show that this method offers improved resistance against various cryptographic attacks.

MATERIALS AND METHODS

Cryptography, the science of secure communication, has become essential in addressing the growing challenges of data security. It employs mathematical methods to protect information [19, 20, 21]. Encryption transforms a readable message, or plaintext, into an unreadable form called ciphertext, while decryption reverses this process to restore the original data. Modern cryptographic systems rely on mathematical algorithms and secret keys for both encryption and decryption. In applied mathematics, integral transforms are widely used, and recent studies have explored their application in developing new cryptographic methods [2, 6, 20]. Among these, the Tarig Transform introduced by Tarig M. Elzaki has been examined for its properties and potential cryptographic uses [20].

Definition 1 (Affine Cipher)

Affine cipher is a substitution cipher, where each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. Each letter is encrypted using the formula:

$$E(x) = \alpha x^{\omega} + \beta \ (mod\ 29) \quad (1)$$

where α and β are keys of the cipher and ω is non-linear. The value α must be chosen such that α is coprime to 29. The decryption function is given by the formula:

$$D(y) = [\alpha^{-1}(x - \beta)]^{d} \quad (2)$$

where α^{-1} is the modular multiplicative inverse of α modulo 29 and d is the modular multiplicative inverse of ω modulo 29.

Definition 2. Tarig Transform [20]

Consider the functions f in S where the set S is defined as:

$$S = \left\{ f(t): \exists\, M, k_1, k_2 > 0, |f(t)| < Me^{\frac{|t|}{k_j}}, t \in (-1)^j * [0, \infty) \right\} \quad (3)$$

For a given function in the set $M > 0$ must be finite number and k_1, k_2 may be finite or infinite.

For a given function $f \in S$, the Tarig transform of $f(t)$ is defined as:

$$E(u) = T[f(t)] = \frac{1}{u}\int_0^{\infty} f(t)e^{-\frac{t}{u^2}}dt, u \neq 0 \quad (4)$$

Tarig Transform satisfies the linearity property (Shrinath & Bhadane, 2018).

1. $E(u) = T[1] = u$
2. $E(u) = T[t] = u^3$, when $f(t) = t$
3. In general, when $f(t) = t^n, E(u) = T[t^n] = n! \cdot u^{1+2n}$
4. $E^{-1}[u] = 1$
5. $E^{-1}(n! \cdot u^{1+2n}) = t^n$

RESULTS AND DISCUSSION

The following algorithm provides an insight into the proposed cryptographic scheme. The sender converts the original message or plaintext into ciphertext using the following steps.

Table1. Numerical values of Alphabets and some symbols used.

A 0	B 1	C 2	D 3	E 4	F 5	G 6	H 7	I 8	J 9
K 10	L 11	M 12	N 13	O 14	P 14	Q 16	R 17	S 18	T 19
U 20	V 21	W 22	X 23	Y 24	Z 25	@ 26	. 27	/ 28	

Encryption Algorithm

1. Every letter in the plaintext message is converted into a number as shown in table 1.
2. The plaintext message is organized as a finite sequence of numbers based on the above conversion
3. Use the encryption $E(x) = \alpha x^{\omega} + \beta \ (mod\ 29)$ ensuring that α and 29 are co-prime, that is $\gcd(\alpha, 29) = 1$ where x is an integer corresponding to the plaintext.
4. Let $n + 1$ be the number of terms in the sequence.
5. Consider a polynomial $P(t)$ of degree n with coefficients as the term of the given finite sequence.
6. Take the Tarig Transform $E(u)$ of the polynomial $P(t)$ and write $E(u) = \sum_{j=0}^{n} q_j u^{2j+1}$
7. Next, find the r_j such that $q_j \equiv r_j (mod\ 29)$ for each $j, 0 \leq j \leq n$.
8. Write $q_j = 29k_j + r_j$, get a key $k_j, for\ j = 0, 1\ 2, \ . \ . \ . \ , \ n$.
9. Now consider a new finite sequence $r_0, r_1, r_2, \ . \ . \ . \ , \ r_n$
10. Convert the finite sequence into alphabets to get the ciphertext.

Decryption Algorithm

1. Consider the ciphertext and key received from sender.
2. Convert the given ciphertext to corresponding the finite sequence $r_0, r_1, r_2, \ . \ . \ . \ , \ r_n$.
3. Let $q_j = 29k_j + r_j, for\ j = 0, 1\ 2, \ . \ . \ . \ , \ n$.
4. Let $E(u) = \sum_{j=0}^{n} q_j u^{2j+1}$
5. Take the inverse Tarig Transform of $E(u)$ and get the polynomial $P(t)$.

6. Consider the coefficients of the polynomial $P(t)$ as a finite sequence.
7. For each number y in the sequence, use the decryption function $[\alpha^{-1}(y-\beta)]^d \ (mod\ 29)$ where, α and β are affine cipher keys.

Illustration

Let's consider the message to be send through insecure channel as: **GAUSS@EDU.NG** using the encryption function $E(x) = 9x^3 + 12\ (mod\ 29)$. Find the ciphertext and decrypt it.

Using table 1 above, the message **GAUSS@EDU.NG** equivalent to the sequence:

6, 0, 20, 18, 18, 26, 4, 3, 20, 27, 13, 6.

Plain text	x	$9x^3 + 12\ (mod\ 29)$
G	6	13
A	0	12
U	20	5
S	18	10
S	18	10
@	26	1
E	4	8
D	3	23
U	20	5
.	27	27
N	13	7
G	6	13

Hence, we have a polynomial $P(t)$ of degree 11 which is:

$$P(t) = 13 + 12t + 5t^2 + 10t^3 + 10t^4 + t^5 + 8t^6 + 23t^7 + 5t^8 + 27t^9 + 7t^{10} + 13t^{11}\ .$$

We now take the Tarig Transform of the polynomial $P(t)$, that is;

$$E(u) = T[P(t)]$$
$$= E[13 + 12t + 5t^2 + 10t^3 + 10t^4 + t^5 + 8t^6 + 23t^7 + 5t^8 + 27t^9 + 7t^{10} + 13t^{11}]$$
$$= 13u + 12u^3 + 5(2!)u^5 + 10(3!)u^7 + 10(4!)u^9 + 1(5!)u^{11} + 8(6!)u^{13} + 23(7!)u^{15} + 5(8!)u^{17} + 27(9!)u^{19} + 7(10!)u^{21} + 13(11!)u^{23}$$
$$= 13u + 12u^3 + 10u^5 + 60u^7 + 240u^9 + 120u^{11} + 5760u^{13} + 115920u^{15} + 201600u^{17} + 9797760u^{19} + 25401600u^{21} + 518918400u^{23}$$
$$= \sum_{j=0}^{n} q_j u^{2j+1}$$

Next, we find r_j such that $q_j \equiv r_j \ (mod\ 29)$ for each $j, 0 \leq j \leq n$.

$q_0 = 13 \equiv 13\ (mod\ 29)$, $q_1 = 12 \equiv 12\ (mod\ 29)$, $q_2 = 10 \equiv 10\ (mod\ 29)$,

$q_3 = 60 \equiv 2\ (mod\ 29)$, $q_4 = 240 \equiv 8\ (mod\ 29)$, $q_5 = 120 \equiv 4\ (mod\ 29)$

$q_6 = 5760 \equiv 18\ (mod\ 29)$, $q_7 = 115920 \equiv 7\ (mod\ 29)$, $q_8 = 201600 \equiv 13\ (mod\ 29)$

$q_9 = 9797760 \equiv 23\ (mod\ 29)$, $q_{10} = 25401600 \equiv 13\ (mod\ 29)$,

$q_{11} = 518918400 \equiv 13\ (mod\ 29)$

Write $q_j = 29k_j + r_j$. Thus, we get a key $k_j\ for\ j = 0, 1\ 2, \ . \ . \ . \ , n$ as follows:

$k_0 = 0, k_1 = 0, k_2 = 0, k_3 = 2, k_4 = 8, k_5 = 4, k_6 = 198, k_7 = 3997, k_8 = 6951, k_9 = 337853,$

$k_{10} = 875917, k_{11} = 17893737$

We then consider a new finite sequence $r_0, r_1, r_2, \ . \ . \ . \ , \ r_n$. That is;

13, 12, 10, 2, 8, 4, 18, 7, 21, 23, 7, 27

The sequence is then converted into alphabets to get the ciphertext **NMKCIESHVXH.**

It is assumed here that the receiver knows the Affine cipher keys α and β. The multiplicative inverse of α and ω under modulo 29 is denoted by α^{-1} and ω^{-1} respectively. In the illustration,

$\alpha = 9\ and\ \beta = 12$ and so $\alpha^{-1} = 13$ and $\omega^{-1} = 19$

We now take the ciphertext and key received from the sender. As above, the ciphertext is **NMKCIESHVXH.** and the key is: 0, 0, 0, 2, 8, 4, 198, 3997, 6951, 337853, 875917, 17893737.

The ciphertext is then converted to corresponding finite sequence of numbers $r_0, r_1, r_2, \ . \ . \ . \ , \ r_n$. That is: **13, 12, 10, 2, 8, 4, 18, 7, 21, 23, 7, 27**

Let $q_j = 29k_j + r_j, \ \ for\ j = 0, 1\ 2, \ . \ . \ . \ , \ n$

Then,

$q_0 = 29(0) + 13 = 13, \ q_1 = 29(0) + 12 = 12, \ q_2 = 29(0) + 10 = 10,$

$q_3 = 29(2) + 2 = 60, \ q_4 = 29(8) + 8 = 240, \ q_5 = 29(4) + 4 = 120, \ q_6 = 29(198) + 18 = 5760, \ q_7 = 29(3997) + 7 = 115920, \ q_8 = 29(6951) + 21 = 201600,$

$q_9 = 29(337853) + 23 = 9797760, \ q_{10} = 29(875917) + 7 = 25401600,$

$q_{11} = 29(17893737) + 27 = 518918400$

Let $E(u) = \sum_{j=0}^{n} q_j u^{2j+1}$. Then,

$E(u) = 13u + 12u^3 + 5(2!)u^5 + 10(3!)u^7 + 10(4!)u^9 + 1(5!)u^{11} + 8(6!)u^{13} + 23(7!)u^{15} + 5(8!)u^{17} + 27(9!)u^{19} + 7(10!)u^{21} + 13(11!)u^{23}$

Taking the inverse Tarig Transform of $E(u)$ and obtain the polynomial $P(t)$. As above, we obtained:

$P(t) = 13 + 12t + 5t^2 + 10t^3 + 10t^4 + t^5 + 8t^6 + 23t^7 + 5t^8 + 27t^9 + 7t^{10} + 13t^{11}$.

Now considering the coefficients of the polynomial $P(t)$ as a finite sequence that is:

13, 12, 5, 10, 10, 1, 8, 23, 5, 27, 7, 13

For each number y in the sequence, use the decryption function $D(y) = [\alpha^{-1}(y - \beta)]^d \ (mod\ 29)$ where $\alpha\ and\ \beta$ are affine cipher keys, then we have:

y	$[13(y-12)]^{19} \pmod{29}$	plaintext
13	6	**G**
12	0	**A**
5	20	**U**
10	18	**S**
10	18	**S**
1	26	**@**
8	4	**E**
23	3	**D**
5	20	**U**
27	27	**.**
7	13	**N**
13	6	**G**

CONCLUSION

This work presented an enhancement of the Tarig Transform–based encryption scheme by incorporating nonlinear permutation polynomials over prime fields. Unlike the original affine-based approach, the use of nonlinear polynomials introduces stronger confusion and diffusion, thereby improving resistance against brute-force, statistical, and algebraic attacks. The integration of polynomial mappings with the Tarig Transform ensures higher key sensitivity, larger key space, and more secure ciphertext representation. Overall, the proposed scheme achieves a more robust cryptographic framework suitable for modern data security applications.

As an extension of this work, the Hybrid Approaches can be use by Combining nonlinear permutation polynomials with elliptic curve cryptography (ECC) or lattice-based schemes for post-quantum security with different types of ciphers available in the literature instead of affine cipher.

Conflict of Interest

The author declared that there is no conflict of interest.

Founding

The research is self-founded

REFERENCES

[1]. Nagalakshmi, G., Ravi, K. B and Chandra S. A **(**2011**).** A cryptographic scheme of Laplace transforms, International Journal of Mathematical Archive-2(12), 2515-2519.

[2]. Hiwarekar A.P. (2012). A new method of cryptography using Laplace transform, International Journal of Mathematical Archive, 3(3), 1193-1197.

[3]. Kumar P. Senthil, Vasuki S. (2018). An Application of MAHGOUB Transform in Cryptography, Advances in Theoretical and Applied Mathematics, ISSN 0973-4554, Volume 13, Number 2, pp. 91-99.

[4]. Abdelilah K. Hassan Sedeeg, Mohand M. Abdelrahim Mahgoub, Muneer A. Saif Saeed, (2016). An Application of the New Integral "Aboodh Transform" in Cryptography, Int J Pure Appl Math, 5 (5), 151-154

[5]. Uttam Dattu Kharde., (2017). An Application of the Elzaki Transform in Cryptography. Journal for Advanced Research in Applied Sciences, 4(5), pp. 86 – 89.

[6]. Bhuvaneswari, R and Bhuvaneswari, K (2020)**.** Application of yang transform in cryptography. *International Journal of Engineering, Science and Mathematics,* 9(3):41–45.

[7]. Ghanti, M. & Bandyopadhyay, S. K (2017)**.** A proposed method for cryptography using random key and rotation of text**.** *International Journal of Advanced Trends in Computer Science and Engineering,* Vol. 6, pp. 18-22.

[8]. Dragan Lambić and MiodragŽivković (2013)**.** Comparison of random s-box generation methods. *Publications de l'institutmathematique,* 93(107):109–115.

[9]. Mohamed, Kamsiah and Ali, Fakariah Hani HjMohd and Ariffin, Suriyani (2020). A New Design of Permutation Function Using Spiral Fibonacci in Block Cipher, *International Journal of Advanced Trends in Computer Science and Engineering,* Vol. 9(1.3), pp. 445-450.

[10]. Ammar S Alanazi (2021). A dual layer secure data encryption and hiding scheme for color images using the three-dimensional chaotic map and lah transformation. *IEEE Access,* 9:26583–26592.

[11]. Praneesh Gupta and Prasanna Raghaw Mishra (2014). Cryptanalysis of "a new method of cryptography using Laplace Transform". *In Proceedings of the Third International Conference on Soft Computing for Problem Solving*, pages 539–546. Springer.

[12]. Gençoğlu, M. Tuncay (2017). Cryptanalysis of a new method of cryptography using Laplace Transform hyperbolic functions**.** *Communications in Mathematics and Applications,* 8(2):183 189.

[13]. Roberto Pulmano Briones (2018). Modification of an encryption scheme based on the Laplace Transform. *International Journal of Current Research,* 10(7):71759–71763.

[14]. Muharrem, T. G. (2019)**.** Embedded image coding using laplace transform for turkish letters**.** *Multimedia Tools and Applications,* 78(13):17521–17534.

[15]. Nagalakshmi, G, Chandra, A. S, & Ravi, D. S (2020). Asymmetric key cryptography using Laplace Transform. *International Journal of Innovative Technology and Exploring Engineering.*

[16]. Binoy, J. and Bindhu, K.T. (2020). A new (k, n) secret sharing symmetric-key cryptographic method using ascii conversion and laplace transforms**.** *Malaya Journal of Matematik (MJM),* 8(3), pp.1203—1205.

[17]. Nagalakshmi. G, Chandra, A.S, Ravi, N. S, and Venkateswarlu, K (2019). Enhancing the data security by using rsa algorithm with application of laplace transform cryptosystem. *International Journal of Recent Technology and Engineering,* 8(2).

[18]. Abdoualwase M. Al-Azzani, Moammar. A. M. Rageh, Ghaleb H. Al-Gaphari, (2021). A New Cryptography Scheme Based on Laplace Transform and a Substitution-Permutation Network. *International Journal of Advanced Trends in Computer Science and Engineering, Vol. 10, No 4, pp. 2658 – 2663.*

[19]. Barr, T.H. (2002). Invitation to Cryptography. Prentice Hall.

[20]. Blakeley G.R. (1999). Twenty years of Cryptography in the open literature, Security and Privacy 1999, Proceedings of the IEEE Symposium, 9-12.

[21]. Johanees A. B. (2009). Introduction to Cryptography, Fourth Edn. Indian Reprint, Springer.

[22]. Shrinath, M., Bhadane, A.P (2018). Applications of Tarig Transformation to New Fractional Derivatives with Non-Singular Kernel. Journal of Fractional Calculus and Applications, Vol.9(1), pp.160-166.