Palestine Journal of Mathematics

Vol 14 (Special Issue IV), (2025) , 216–223

CRYPTOGRAPHY BASED ON SAWI-ELZAKI TRANSFORM

A. Patwa, H. Chandra and L. Soni

2010 Mathematics Subject Classification: 94A60, 68P25.

Keywords and phrases: Encryption, Decryption, Cryptography, Sawi transform, Elzaki transform.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Abstract Cryptography is the science of secure communication and continues to evolve to meet the growing demands of modern information security. In this paper, we propose a new encryption technique based on the Sawi and Elzaki integral transforms. These transforms, rooted in mathematical theory, have unique properties that make them suitable for cryptographic use. Our method uses the Sawi and Elzaki transforms to encrypt messages and their inverse transforms for decryption, offering strong resistance to common cryptographic attacks. We also provide a security analysis of the proposed method and evaluate its computational performance using JavaScript. The results show that our approach is both secure and efficient, with a total execution cost of 18.930 milliseconds (ms), making it a promising tool for secure data communication.

1 Introduction

Cryptography stands as a cornerstone in the realm of information security, playing a critical role in safeguarding sensitive data from unauthorized access or manipulation. Over the years, cryptographic techniques have evolved significantly to address the ever-growing challenges posed by cyber threats and advancements in computing technologies such as IoT [13, 14]. In this study, we have focused on secret-key cryptography, also known as symmetric key cryptography. This encryption method uses the same key to encrypt and decrypt the data. To communicate securely, both the sender and the recipient must share a secret key. However, the two parties must exchange this key through specific channels to ensure its confidentiality. Key exchange protocols are well-known and widely used cryptographic tools for this purpose [12, 15].

In recent years, there has been a increasing interest in exploring new ways for encrypting and decrypting data in a secure and efficient manner. Use of mathematical transforms has became a promising technique for developing robust cryptographic schemes [11, 16]. Among the integral transforms commonly used in cryptanalysis for encryption and decryption are Laplace, Elzaki, and Natural.

In this study, we explore the field of cryptographic innovation by using the Sawi and Elzaki integral transforms [1, 10]. We use these transforms to develop a new cryptographic technique that increases data security and resilience. In addition, we presented a new cryptographic scheme that combines these transforms with a meticulously designed encryption key to increase security measures and deter malicious adversaries. As we explore the intersection of mathematics and cryptography, we aim to highlight the potential of the Sawi and Elzaki integral transforms to revolutionize data protection paradigms and find the way for a new era of enhanced security in digital communications and information systems.

1.1 Previous Work

Data security and privacy have always been the top priorities for any system regarding safe communication. Numerous cryptographic-based mathematical security techniques have been suggested previously. In 2004, Buchanan et al. [4] introduced the basics of cryptography. In

2011, Elzaki et al. [1] developed a novel integral transform, the Elzaki transform, which has been used to solve linear ordinary differential equations with constant coefficients. In 2021, Jafari et al. [2] introduced a general integral transform in the class of Laplace transform. Meftin et al. [3], Huma et al. [5], and Hiwarekar et al. [8] gave a cryptographical model based on combining two different mathematical transforms. Aggarwal et al. [9] explained dualities between some useful integral transforms and the Sawi transform. In 2023, Kumar et al. [11] also gave a new encryption scheme based on Legendre's transform.

In subsequent works, Gupta et al. [15] developed an encryption–decryption technique based on planar graphs and self-invertible matrices, offering structural advantages in key generation. Panchal et al. [16] presented a public key scheme leveraging generalized Fibonacci matrices, introducing algebraic strength and efficiency. Khalat et al. [17] contributed a method utilizing matrix decomposition and the Abaoub Shkheam transform, where encryption and decryption are performed using hyperbolic functions and triangular matrices. More recently, Thakur et al. [18] introduced a robust encryption framework combining the Anuj Transform with the congruence modulo operator, demonstrating enhanced computational efficiency, encryption accuracy, and resistance to cryptanalytic attacks.

1.2 Road map of paper

The remaining part of the work is structured as follows: We will discuss both transform preliminaries in section 2. The encryption and decryption method will be explained in section 3. To give a better understanding, a numerical example has been provided in section 4. Furthermore, the proposed scheme has been generalized in section 5. The security analysis and experimental setup with source code are presented in sections 6 and 7, respectively. Finally, the paper concludes in section 8.

2 Preliminary

2.1 Sawi Integral Transform

M. Mohand [10] presented the Sawi transform to ease the process of solving partial and ordinary differential equations. For functions of exponential order, we discuss a transform known as the Sawi transform, which is applied on a functions in the set A defined by:

$$A = \left\{ f(t) : \exists\, M, K_1, K_2 \geq |f(t)|e^{\frac{t}{k_j}}, if \;\; t \in (-1)^j \times [0, \infty) \right\} \tag{2.1}$$

The constant M for any function in the set A must be a finite number, but K_1 and K_2 may be infinite or finite. Sawi transform, denoted by the operator S and is defined by the integral equations,

$$S\{F(t)\} = f(s) = \frac{1}{s^2} \int_0^\infty F(t) \exp^{\frac{-t}{s}} dt. \tag{2.2}$$

We have,

$$S\left[t^n\right] = n! s^{n-1},\; S\left[e^{at}\right] = \frac{1}{s(1-as)} \text{ and } S^{-1}\left[s^n\right] = \frac{t^{n+1}}{(n+1)!},\; S^{-1}\left[\frac{1}{s(1-as)}\right] = e^{at}.$$

2.2 Elzaki Integral Transform

The Elzaki transform was presented by Tarig Elzaki [1] as a way to address ordinary and partial differential equations in the given time domain. It comes from the traditional Fourier integral and is defined for functions of exponential order in the set A.

$$A = \left\{ f(t) : \exists M, K_1, K_2 \geq |f(t)|e^{\frac{t}{k_j}}, if \;\; t \in (-1)^j \times [0, \infty) \right\}. \tag{2.3}$$

For a function belonging to the set A, the constant M must be a finite number, but K_1 and K_2 may be finite or infinite. The Elzaki transform denoted by the operator E defined by the integral equation,

$$E\{F(t)\} = f(v) = v \int_0^\infty F(t) \exp^{\frac{-t}{v}} dt. \tag{2.4}$$

We have,

$$E\left[t^n\right] = n!v^{n+2}, \quad E\left[e^{at}\right] = \frac{v^2}{1-av} \text{ and } E^{-1}\left[v^n\right] = \frac{t^{n-2}}{(n-2)!}, \quad E^{-1}\left[\frac{v^2}{1-av}\right] = e^{at}.$$

3 Proposed Cryptographic Scheme

3.1 Encryption Scheme

(i) A shared key $\{R_n\}$ must be established between sender and recipient before encryption can begin.

(ii) Plain text is encoded as a defined series of numbers, that is, *A = 0, B = 1, C = 2, ... and Z = 25*.

(iii) Let F(t) be a polynomial of degree n, evaluated at a term from a specified sequence.

(iv) Determine the Elzaki Integral transform for the polynomial given above.

(v) Proceed by taking the Sawi Integral transform of the resulting polynomial from the prior step.

(vi) Compute the remainders $\left\{F_n^{'}\right\}$ such that $F_n^{'} = P_n \ mod\ (26)$. The values of remainder $\left\{F_n^{'}\right\}$ will give the encrypted message.

(vii) Compute the keys $\{R_n\}$ such that

$$\frac{P_n - F_n^{'}}{26} = R_n. \tag{3.1}$$

3.2 Decryption Scheme

(i) Consider the encrypted data along with the key R_n transmitted by the sender.

(ii) Map the cipher text to it's associated finite sequence of numbers using the equation (3.1) and given key R_n.

(iii) Find the inverse Sawi transform of the given function.

(iv) Then, the inverse Elzaki transform is applied on the resultant polynomial obtained from the previous step.

(v) By mapping the numbers in the given finite sequence to letters,the original plaintext is revealed.

4 Numerical Examples

In this technique, the message to be encrypted is represented as a coefficient of $F(t)$, numbered from 0 to 25 in alphabetical order: *A=0, B=1, C=2, D=3, E=4,...,Z=25*.

Let $F(t) = F_n \dfrac{t}{1-t}$ and plain text be ***W O R L D***. Hence, $F_0 = 22, F_1 = 14, F_2 = 17, F_3 = 11, F_4 = 3$. Now $F(t) = F_n \dfrac{t}{1-t} = \sum_0^n F_n t^{n+1}$. Then $F(t) = 22t + 14t^2 + 17t^3 + 11t^4 + 3t^5$, F_n = 0, $\forall\ n \geq 5$.

4.1 Encryption Process

(a) First Iteration

We have $E\{F(t)\} = E\left\{F_n t^{n+1}\right\}$, where F_n = 0, $\forall\ n \geq 5$. Hence, $E\{F(t)\} = 22 \times 1! \times u^3 + 14 \times 2! \times u^4 + 17 \times 3! \times u^5 + 11 \times 4! \times u^6 + 3 \times 5! \times u^7$.

(b) Second Iteration

Apply Sawi transform on $E\{F(t)\}$, we get:

$$S\{E\{F(t)\}\} = 22\times1!\times3!\times s^2+14\times2!\times4!\times s^3+17\times3!\times5!\times s^4+11\times4!\times6!\times s^5+3\times5!\times7!\times s^6.$$

Now the coefficients P_n, where n = 0 to 4 are given by P_n : 132, 672, 12240, 190080, 1814400. If $F_n^{'} \equiv P_n$ mod(26), then

$$F_0^{'} \equiv 132 = 2\ (mod26), F_1^{'} \equiv 672 = 22\ (mod26), F_2^{'} \equiv 12240 = 20\ (mod26),$$

$$F_3^{'} \equiv 190080 = 20\ (mod26),\ \text{ and } F_4^{'} \equiv 1814400 = 16\ (mod26).$$

Hence, the encrypted message or cipher text is ***C W U U Q*** with key R_n: 5, 25, 470, 7310, 69784, where $R_n = \dfrac{P_n - F_n^{'}}{26}$. The encryption process with code show in Figure 1.

main.js

```
console.time("Execution Time");
function fact(n) {
    if(n===0 || n===1) {
        return 1;
    } else {
        return n* fact(n-1);
    }
}
let s = "WORLD";
let v = [];
let key = [];
let f0;
let ft1;
let rem;
let quot;
let depth = s.length;
for(let i=0;i<depth;i++) {
    let temp = s.charCodeAt(i) - 65;
    f0 = (fact(i+1)*temp);
    rem = f0*fact(i+3)%26;
    quot = f0*fact(i+3)/26;
    key.push(quot.toString().split(".")[0]);
    v.push(rem);
}
let ans = "";
for(let i of v){
    ans+=String.fromCharCode(i+65);
}
console.log(ans);
console.log("Key : ",key);
console.timeEnd("Execution Time");
```

Figure 1. Encryption Code

4.2 Decryption Process

The encrypted data is received through a non-secure channel from the sender [19]. In this case, the encrypted text is ***CWUUQ***, and the key is R_n: 5, 25, 470, 7310, 69784. According to the key, the received cipher text is converted into its equivalent finite numerical sequence for further processing.
$\{C\ W\ U\ U\ Q\}$ = $\{2, 22, 20, 20, 16\}$ = $F_n^{'}$. Now, $P_n = 26R_n + F_n^{'}$, $n = 0$ to 4 and $P_n = 0$ for $n \geq 5$. So we have,

$$P_0 = 26\times5+2 = 132, P_1 = 26\times25+22 = 672, P_2 = 26\times470+20 = 12240,$$

$$P_3 = 26\times7310+20 = 190080, P_4 = 26\times69784+16 = 1814400.$$

We have

$$\sum_{0}^{4} P_n \times s^{n+2} = P_0\times s^2 + P_1\times s^3 + P_2\times s^4 + P_3\times s^5 + P_4\times s^6;$$

or

$$\sum_{0}^{4} P_n \times s^{n+2} = 132s^2 + 672s^3 + 12240s^4 + 190080s^5 + 1814400s^6,$$

where $P_n = 0$ for $n \geq 5$.

(a) First Iteration

Taking Inverse Sawi transform of the above equation, we get:

$$S^{-1}\left\{\sum_{0}^{4} P_n \times s^{n+2}\right\} = 132\frac{u^3}{3!} + 672\frac{u^4}{4!} + 12240\frac{u^5}{5!} + 190080\frac{u^6}{6!} + 1814400\frac{u^7}{7!},$$

or

$$S^{-1}\left\{\sum_{0}^{4} P_n \times s^{n+2}\right\} = 22u^3 + 28u^4 + 102u^5 + 264u^6 + 360u^7.$$

(b) Second Iteration

Taking the Inverse Elzaki transform of the equation obtained from first iteration:

$$E^{-1}\left\{S^{-1}\left\{\sum_{0}^{4} P_n \times s^{n+2}\right\}\right\} = E^{-1}\left\{22u^3 + 28u^4 + 102u^5 + 264u^6 + 360u^7\right\}$$

or

$$E^{-1}\left\{S^{-1}\left\{\sum_{0}^{4} P_n \times s^{n+2}\right\}\right\} = 22t + 14t^2 + 17t^3 + 11t^4 + 3t^5.$$

Upon closely examining the polynomial coefficients, we observe that they correspond to the F_n and $f(t) = \sum_{n=0}^{4} F_n t^{n+1} = F_n \frac{t}{1-t}$, where $F_n = 0 \; \forall \; n \geq 5$.

The numbers in the bounded sequence can be translated into their corresponding characters to reveal the original transmitted message ***W O R L D***. The decryption process with code show in Figure 2.

main.js

```
console.time("Execution Time");
function fact(n) {
    if(n===0 || n===1) {
        return 1;
    } else {
        return n* fact(n-1);
    }
}
let s = "CWUUQ";
let v = [];
let key = ['5','25','470','7310','69784'];
let f0;
let ft1
let ft2
let rem;
let depth = s.length;
for(let i=0;i<depth;i++) {
    let temp = s.charCodeAt(i) - 65;
    f0=key[i]*26+temp;
    ft1=f0/fact(i+3);
    ft2=ft1/fact(i+1);

    v.push(ft2);
}
let ans = "";
for(let i of v){
    ans+=String.fromCharCode(i+65);
}
console.log(ans);
console.timeEnd("Execution Time");
```

Figure 2. Decryption Code

5 Generalization

We generalize our result on $F_n \frac{t}{1-t}$ to $F_n \frac{t^j}{1-t}$ where $j \in N$.

• **Encryption Process**

Taking Elzaki transform in first iteration we have coefficient $q_n = F_n(n+j)!$. In the second iteration, we take Sawi transform, and then we get the coefficient as $P_n = F_n(n+j)!(n+j+2)!$. Now convert given plaintext F_n into $F_n^{'}$ with

$$F_n^{'} = F_n(n+j)!(n+j+2)! = P_n \text{ (mod } 26) \text{ and key } R_n = \frac{P_n - F_n^{'}}{26}.$$

• **Decryption Process**

We have received encrypted message $F_n^{'}$ and key R_n.
Consider the function

$$\sum_{n=0}^{n} P_n s^{n+2+j}, \text{where } P_n = 26R_n + F_n^{'}.$$

On taking the inverse Sawi Transform of the above function, we get:

$$\text{G(u)} = \sum_{n=0}^{n} \frac{P_n u^{(n+3+j)}}{(n+3+j)!}.$$

On taking the Elzaki Transform of above function, we get:

$$\text{G(t)} = \sum_{n=0}^{n} \frac{P_n t^{(n+1+j)}}{(n+3+j)!(n+1+j)!}.$$

The plaintext F_n is given by

$$F_n = \frac{P_n t^{(n+1+j)}}{(n+3+j)!(n+1+j)!}.$$

6 Security Analysis

This section uses the following attacks to examine the security of our suggested encryption and decryption strategy. We know that achieving CIA, where C stands for confidentiality, I for Integrity, and A for authentication, is the basic security objective for any cryptographic system. We demonstrate that our scheme is secure against the following attacks and meets the security objectives of CIA using the following attacks.

- ***Man In Middle Attack:*** In this attack, the attacker intercepts the message or key passed between two parties through a secured channel. In our approach, the sender encrypts the content and includes an enhanced key, R_n. Our plain text is encrypted using the Sawi and Elzaki Transform in stacked phases, and the key is strengthened with modular property, making it hard for an attacker to guess the key and defeat the method. As a result, our proposed scheme is protected from Man in the Middle assaults.
- ***Known Plaintext Attack :*** The attacker can access the encrypted text and its equivalent plaintext to perform known plaintext attacks. He aims to figure out the secret key (or keys) or develop an algorithm to let him. While the Sawi and Elzaki transform-based cryptographic scheme presents an innovative approach to encryption, its resistance to known-plaintext attacks is contingent upon the secrecy and complexity of the key, as well as the unpredictability of the encryption process. Enhancements in randomness, key variability, and cryptographic strength are essential to fortify the scheme against such attacks.

7 Experimental Setup

We selected the plaintext [WORLD] to evaluate the proposed encryption algorithm. The implementation was carried out in JavaScript on an HP desktop running Windows 11 (version 23H2),

equipped with an AMD Ryzen 5 5500U processor (with Radeon Graphics, 2.10 GHz) and 8.00 GB RAM (7.33 GB usable). The experiment was conducted using a fixed plaintext of length 5 to analyze the performance and correctness of the algorithm. The execution cost incurred by the program is illustrated in Figures 3 and 4. The overall computation cost for the proposed scheme is summarized in Table 1.

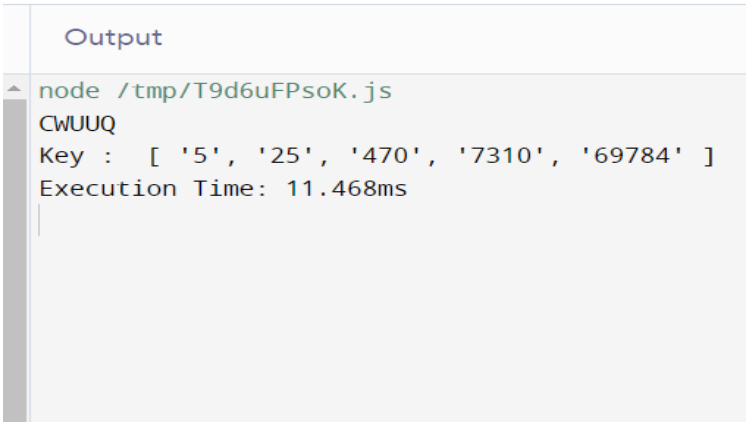

Figure 3. Encrypted message and Key with execution cost in milliseconds (ms)

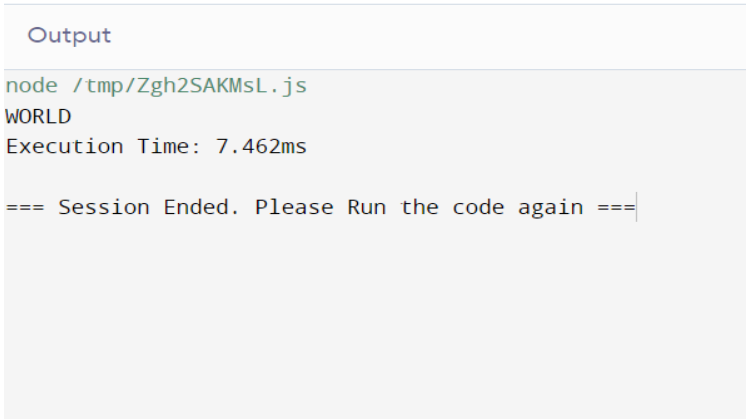

Figure 4. Decrypted message with execution cost in milliseconds (ms)

Encryption Time(ms)	Decryption Time(ms)	Total time(ms)
11.468	7.462	18.930

Table 1. Total computation cost for the proposed scheme in milliseconds (ms)

8 Conclusion

This study demonstrates the effectiveness and advantages of using Sawi and Elzaki integral transforms in cryptographic applications. These mathematical transforms have shown strong potential for securely converting plaintext into ciphertext, thereby enhancing data confidentiality and integrity. The proposed method introduces a novel cryptographic strategy that utilizes the structural properties of these transforms to perform secure encryption and decryption operations. One of the key strengths of the scheme is its use of a highly complex and dynamic key structure, which significantly increases its resistance to cryptanalysis, brute-force attacks, and tracing attempts. Furthermore, the algorithm maintains a balance between security and efficiency, making

it suitable for real-time secure communication. The implementation and performance analysis of the scheme, demonstrated using JavaScript, further validate its practicality in modern data protection scenarios.

References

[1] T. M. Elzaki, *The new integral transform Elzaki transform*, Global J. Pure Appl. Math. **7** (2011), no. 1, 57–64.

[2] H. Jafari, *A new general integral transform for solving integral equations*, J. Adv. Res. **32** (2021), 133–138.

[3] N. K. Meftin, *Elzaki-Rohit cryptographical model*, AIP Conf. Proc. **2834** (2023), no. 1, AIP Publishing.

[4] J. Buchmann, *Introduction to cryptography*, vol. 335, Springer, New York, 2004.

[5] Z. E. Huma, et al., *Cryptographic method based on Natural-Elzaki transform*, i-Manager's J. Math. **11** (2022), no. 1, 39.

[6] A. P. Hiwarekar, *Application of Laplace transform for cryptographic scheme*, Proceedings of the World Congress on Engineering, vol. 1, 2013.

[7] P. P. Raut and A. P. Hiwarekar, *New method of cryptography with Python code using Elzaki transform and linear combination of function*, Commun. Math. Appl. **14** (2023), no. 3, 1245.

[8] J. S. Shivaji, S. Jadhav, and A. P. Hiwarekar, *New method for cryptography using Laplace-Elzaki transform*, Psychology and Education Journal **58** (2021), no. 5.

[9] S. Aggarwal and A. R. Gupta, *Dualities between some useful integral transforms and Sawi transform*, Int. J. Recent Technol. Eng. **8** (2019), no. 3, 5978–5982.

[10] M. M. Abdelrahim Mahgoub and M. Mohand, *The new integral transform "Sawi Transform"*, Adv. Theor. Appl. Math. **14** (2019), no. 1, 81–87.

[11] A. Kumar, et al., *A new encryption scheme based on Legendre's transform*, Mathematics in Engineering, Science and Aerospace (MESA) **14** (2023), no. 4.

[12] L. Soni, et al., *Quantum-resistant public-key encryption and signature schemes with smaller key sizes*, Cluster Computing (2022), 1–13.

[13] D. S. Gupta, L. Soni, and H. Chandra, *Quantum-defended digital signature on lattice for IoT-enabled systems*, in International Conference on Internet of Things and Connected Technologies, Springer Nature Singapore, Singapore, 2022.

[14] A. Singh, et al., *Blockchain based authentication and access control protocol for IoT*, Multimedia Tools Appl. (2023), 1–23.

[15] D. Gupta, H. Chandra, and L. Soni, *An encryption and decryption technique using planar graph with self-invertible matrix*, Math. Eng. Sci. Aerospace (MESA), **15**(4) (2024).

[16] J. Panchal, H. Chandra, and A. Singh, *A new public key cryptography using generalized Fibonacci matrices*, Surv. Math. Appl., **19** (2024), 301–316.

[17] A. Omar, *A new cryptographic scheme using integral transform and matrix decomposition*, Libyan J. Sci., **27**(2) (2024).

[18] P.C. Thakur, D. Thakur, T. Gunasekar, P. Raghavendran, and S. Gochhait, *Application of integral transform algorithms for augmenting cryptographic security and performance analysis*, in AI-Driven Healthcare Cybersecurity and Privacy, IGI Global Sci. Publ., (2025), 187–204.

[19] E.A. Mansour, E.A. Kuffi, and S.A. Mehdi, *Applying SEE integral transform in cryptography*, in Samarra Journal of Pure and Applied Science, 2022.

Author information

A. Patwa, Department of Mathematics and Scientific Computing, Madan Mohan Malaviya University of Technology, India.
E-mail: 2022113003@mmmut.ac.in

H. Chandra, Department of Mathematics and Scientific Computing, Madan Mohan Malaviya University of Technology, India.
E-mail: hcmsc@mmmut.ac.in

L. Soni, Department of Mathematics and Scientific Computing, Madan Mohan Malaviya University of Technology, India.
E-mail: lacchitammmut22@gmail.com