P- ISSN 1991-8941 E-ISSN 2706-6703
2024,(18), (01):252– 256

Journal of University of Anbar for Pure Science (JUAPS)

Open Access

Perform The Complex EFG Transform in Cryptography

Emad A. Kuffi

Department of Mathematics, College of Basic Education, Mustansiriyah University, Baghdad-Iraq.

ARTICLE INFO

Received: 08 / 01 /2024
Accepted: 18 / 02 / 2024
Available online: 18 / 06 / 2024

DOI: 10.37652/juaps.2024.145931.1176

Keywords:
Complex EFG transform, Inverse of EFG transform, Encryption, Decryption, ASCII code.

ABSTRACT

The integral transforms in their various forms, the traditional and the complex forms, have proven their importance in many scientific fields, and mathematicians exploit them in these fields to the fullest. In addition to employing integral transforms in scientific fields, mathematicians study the different ways to improve these integral transforms in order to include as many applications as possible in each integral transform.

The complex EFG (Emad - Faruk - Ghaith) integral transformation is one of the novel transforms that has not been used in many fields; hence, the light has yet to be shown upon its full potential. Therefore, in this paper, we will show the success and ability of complex EFG (Emad - Faruk - Ghaith) transformation in the process of encryption and decryption algorithms. The potential of the complex EFG in the cryptographic field is proved through practical application, and the results from that application appeared to be very promising in that it adds a new field of application into integral transformation.

Introduction

The complex EFG integral transform has been used to find the exact solution of ordinary differential equations and some of application for differential equations in some of Science's sides [1, 6, 7]. It also comes out to be very effective tool to analyze the boundary value problems (B.V.P.s) in science which are generally solved by adopting different integral transformations, [2, 3, 4, 5] It comes out to be very effective tool to analyze the electrical network circuits and heat transfer with delta function. In this work, a novel integral transformation " complex EFG Transform " has been developed an algorithm for cryptography in which we proposed complex EFG integral transform for encrypting the plaintext and corresponding inverse complex EFG integral transform for decryption.

Definitions and Standard Results

Plaintext: The name of it indicates its meaning in that it is a text that is plainly structured and understandable by anyone who can see it [5].

*Corresponding author at :Department of Mathematics, College of Basic Education, Mustansiriyah University, Baghdad-Iraq
ORCID:https://;Tel,+9647713666167
Email: emad.kuffi@uomustansiriyah.edu.iq

Ciphertext: The resulting text from converting the clear text into unreadable or ununderstandable text is called ciphertext [5].

Encryption and Decryption: Converting plaintext into ciphertext is called the encryption process, while decryption is the inverse process [5].

Definition (1), [1]: " The complex EFG integral transform"

For the function of exponential order in set β , which defined as:

$$\beta\left\{\begin{array}{c} g(t):\ \exists\ , M, L_1\ , L_2\ > 0\ , |g(t)|\ < M\ e^{-il_j|t|}\ , \text{if} \\ t \in (-1\ )^j x\ [0, \infty)\ , \text{where}\ j = 1,2\ \text{and}\ \ i^2 =\ -1 \end{array}\right\}\ .\#(1)$$

The constant M must be a finite for a particular function in the set β , While the constant L_1 and, L_2 may be finite or infinite. The complex EFG transformation denoted by the operator $G^c\{.\}$ and defined as:

$$G^c\ \{g(t)\}\ = F^c(s) = \lim_{\square\to\infty} \int_{t=0}^{\square} g(t)\ e^{-ir(s)t}\ dt\ , \#(2)$$

where $t \geq 0$, and $L_1 \leq r(s)\ \leq L_2$, $r(s)$ is a complex function of the parameter s , $Im(r(s)) < 0, i \in \mathbb{C}$, and the $Im()$ represents the imaginary part of $r(s)$.

In the complex EFG transform, the s variable application's purpose is to factorize the t variable through the function g(t) argument.

The Complex EFG Integral transform And Its Inverse for several Functions [1]

In the following a list the complex EFG transform for some important functions, [1]:

A. $G^c\{k\} = \frac{-i\,k}{r(s)}$, where k is a constant value .

B. $G^c\{t^n\} = \frac{(-i)^{n+1}n!}{(r(s))^{n+1}}$, $r(s) \neq 0$, $Re(r(s)) > 0$, and n is a positive integer .

C. $G^c\{t^n\} = \frac{(-i)^{n+1}\Gamma(n+1)}{(r(s))^{n+1}}$ where $\Gamma(.) > 0$, is a gamma function and $n > -1$, $r(s) \neq 0$ and $\mathrm{Re}\,(r(s)) > 0$.

D. $G^c\{e^{at}\} = -\left[\frac{a}{a^2+(r(s))^2} + i\frac{1}{a^2+(r(s))^2}\right]$, $a + i\,r(s) \neq 0$, $\mathrm{Re}(a + r(s)) > 0$, and a is an arbitrary constant .

E. $G^c\{\sin(at)\} = \frac{-a}{(r(s))^2-a^2}$, $r(s) > |a|$.

F. $G^c\{\cos(at)\} = \frac{-i\,r(s)}{(r(s))^2-a^2}$, $r(s) > |a|$.

G. $G^c\{\sinh(at)\} = \frac{-a}{(r(s))^2+a^2}$, $r(s) > 0$.

H. $G^c\{\cosh(at)\} = \frac{-i\,r(s)}{(r(s))^2+a^2}$, $r(s) > 0$.

A list of the inverse of complex EFG transform for some important functions, [1].

A. $G^{c^1}\{\frac{-i\,k}{r(s)}\} = k$.

B. $G^{c^1}\{\frac{(-i)^{n+1}n!}{(r(s))^{n+1}}\} = t^n$.

C. $G^{c^{-1}}\{\frac{a}{a^2+(r(s))^2} + \frac{i}{a^2+(r(s))^2}\} = -e^{at}$.

D. $G^{c^{-1}}\{\frac{a}{(r(s))^2-a^2}\} = -\sinh(at)$.

E. $G^{c^{-1}}\{\frac{ir(s)}{(r(s))^2-a^2}\} = -\cos(at)$.

F. $G^{c^{-1}}\{\frac{ir(s)}{(r(s))^2+a^2}\} = -\cosh(at)$.

G. $G^{c^{-1}}\{\frac{a}{(r(s))^2+a^2}\} = -\sinh(at)$.

Practical Application of (The Complex EFG Transform) Proposed in Cryptography

The details of the proposed cryptography algorithms (including encryption and decryption) are explained in the following section.

Encryption Stage (Method of Encryption)

This method is implemented through the transmitter, encryption is used to the information to convert it from consistent to inconsistent information.

Step (1): Assuming the message M with length n is the plaintext meant to be sent, then the plaintext M is converted into its equivalent *ASCII* code.

Step (2): Suppose that the given plaintext is" *ACADEMICS* " Here the length of the message $n = 9$. Based on step (1); *ACSII* code of plaintext:

$A = 65$, $B = 67$, $A = 65$, $D = 68$, $E = 69$, $M = 77$, $I = 73$, $C = 67$, $S = 82$.

The finite sequence of the plaintext would be:

$F_0 = 65$, $F_1 = 67$, $F_2 = 65$, $F_3 = 68$, $F_4 = 69$, $F_5 = 77$, $F_6 = 73$, $F_7 = 67$, $F_8 = 83$, $F_n = 0$ .For every n is greater than or equal to 9.

Step (3): Now, writing the above numbers in step(2) as the coefficients $t\cosh(vt)$, v is a constant.

For the following standard series:

$$\cosh(vt) = 1 + \frac{v^2t^2}{2!} + \frac{v^4t^4}{4!} + \frac{v^6t^6}{6!} + \cdots + \frac{v^{2j}t^{2j}}{(2j)!} = \sum_{j=0}^{\infty}\frac{(vt)^{2j}}{(2j)!}.$$

Where $v \in N$, and the series of $t\cosh(vt)$ is:

$$t\cosh(vt) = t + \frac{v^2t^3}{2!} + \frac{v^4t^5}{4!} + \frac{v^6t^7}{6!} + \cdots + \frac{v^{2j}t^{2j+1}}{(2j)!} = \sum_{j=0}^{\infty}\frac{v^{2j}t^{2j+1}}{(2j)!}.$$

Consider the following:

$$g(t) = F\,t\cosh(2t)\,,(v=2) = t\left\{F_0 + F_1\frac{2^2t^2}{2!} + F_2\frac{2^4t^4}{4!} + F_3\frac{2^6t^6}{6!} + F_4\frac{2^8t^8}{8!} + F_5\frac{2^{10}t^{10}}{10!} + F_6\frac{2^{12}t^{12}}{12!} + F_7\frac{2^{14}t^{14}}{14!} + F_8\frac{2^{16}t^{16}}{16!}\right\}$$

$$= 65\,t + 67\frac{2^2t^3}{2!} + 65\frac{2^4t^5}{4!} + 68\frac{2^6t^7}{6!} + 69\frac{2^8t^9}{8!} + 77\frac{2^{10}t^{11}}{10!} + 73\frac{2^{12}t^{13}}{12!} + 67\frac{2^{14}t^{15}}{14!} + 83\frac{2^{16}t^{17}}{16!} = \sum_{j=0}^{\infty}\frac{F_j 2^{2j}t^{2j+1}}{(2j)!}.$$

Step (4): Now, by taking the complex EFG integral transform to the above equation, to get:

$$G^c\{g(t)\} = G^c\{ft\cosh(2t)\} = \frac{(-i)^2 65}{(r(s))^2} + \frac{(-i)^4 80}{(r(s))^4}\frac{(-i)^6 5200}{(r(s))^6} + \frac{(-i)^8 30464}{(r(s))^8} + \frac{(-i)^{10}158979}{(r(s))^{10}} + \frac{(-i)^{12}867328}{(r(s))^{12}} + \frac{(-i)^{14}3887104}{(r(s))^{14}} + \frac{(-i)^{16}16465920}{(r(s))^{16}} + \frac{(-i)^{18}92471296}{(r(s))^{18}}.$$

Step (5): Next evaluate v_p such $v_p = M_p \, mod\ 200$

Where $p = 0, 1, 2, \dots, n$

$v_0 = 65\ mod\ 200 = 200(0) + 65 = 65$,

$v_1 = 804\ mod\ 200 = 200(4) + 4 = 4$,

$v_2 = 5200\ mod\ 200 = 200(26) + 0 = 0$,

$v_3 = 30464\ mod\ 200 = 200(152) + 64 = 64$,

$v_4 = 158976\ mod\ 200 = 200(794) + 176 = 176$,

$v_5 = 867328\ mod\ 200 = 200(4336) + 128 = 128$,

$v_6 = 3887104\ mod\ 200 = 200(19435) + 104 = 104$,

$v_7 = 16465920\ mod\ 200 = 200(82329) + 120 = 120$,

$v_8 = 92471296\ mod\ 200 = 200(462356) + 96 = 96$,

The resulting $ASCII$ code represents the message after its encryption. Hence, A♦@ □hx´" is the message ACADEMICS encryption.

Step (6): Next its essential to find the key k_P, where $k_P = \frac{M_P - V_P}{200}$, $P = 0, 1, 2, \dots, n$. Moreover, the denominator's value can be chosen freely.

The values of k_P can be found as:

$k_0 = 0, k_1 = 4, k_2 = 26, k_3 = 152, k_4 = 794, k_5 = 4336, k_6 = 19435, k_7 = 82329, k_8 = 462356$.

The ciphertext and the key for converting it back have been concluded from the above steps.

Decryption Stage

To transform back the ciphertext into its equivalent message, the following steps are going to be followed:

Step (1): It is necessary to get the ciphertext and its related key from the sender. For the preceding example, the following ciphertext and key were received: cipher is $A♦@\,hx'$", and the key is 0,4,26,152, 794, 4336, 19435, 82329, and 462356.

Step (2): The received ciphertext is going to be transformed into its numerical finite sequence equivalent: 65, 4, 0, 64, 176, 128, 104, 120, 96.

Then it is possible to consider:

$F'_0 = 65, F'_1 = 4, F'_2 = 0, F'_3 = 64, F'_4 = 176, F'_5 = 128, F'_6 = 104, F'_7 = 120, and\ F'_8 = 96$.

Step (3): Given Key $k_P\ for\ P = 0,1,2,\dots,n$ as 0,4 ,26 ,152, 794, 4336, 19435, 82329, 462356 .

$M_P = 200k_P + F'_P$ for $P = 0,1,2,\dots,n$.

$M_0 = 200(0) + 65 = 65$,

$M_1 = 200(4) + 4 = 804$,

$M_2 = 200(26) + 0 = 5200$,

$M_3 = 200(152) + 64 = 30404$,

$M_4 = 200(794) + 176 = 158976$,

$M_5 = 200(4336) + 128 = 867328$,

$M_6 = 200(19435) + 104 = 3887104$,

$M_7 = 200(82329) + 120 = 16465920$,

$M_8 = 200(462356) + 96 = 92471296$.

Consider the following:

$$F\left\{\frac{-d}{ds}\right\}\frac{-i\,r(s)}{(r(s))^2+4} = \frac{(-i)^2 65}{(r(s))^2} + \frac{(-i)^4 804}{(r(s))^4} + \frac{(-i)^6 5200}{(r(s))^6} + \frac{(-i)^8 30464}{(r(s))^8} + \frac{(-i)^{10}158976}{(r(s))^{10}} + \frac{(-i)^{12}867328}{(r(s))^{12}} + \frac{(-i)^{14}3887104}{(r(s))^{14}} + \frac{(-i)^{16}16465920}{(r(s))^{16}} + \frac{(-i)^{18}92471296}{(r(s))^{18}} = \sum_{j=0}^{\infty}\frac{M_j(-i)^{2j+2}}{(r(s))^{2j+2}}.$$

Step (4): Take the inverse of the EFG transform of above equation (3.4), we get:

$$g(t) = Ft\cosh(2t)$$
$$= G^{C^{-1}}\left\{\frac{(-i)^2 65}{(r(s))^2} + \frac{(-i)^4 804}{(r(s))^4} + \frac{(-i)^6 5200}{(r(s))^6} + \frac{(-i)^8 30464}{(r(s))^8} + \frac{(-i)^{10} 158976}{(r(s))^{10}} + \frac{(-i)^{12} 867328}{(r(s))^{12}} + \frac{(-i)^{14} 3887104}{(r(s))^{14}} + \frac{(-i)^{16} 16465920}{(r(s))^{16}} + \frac{(-i)^{18} 92471296}{(r(s))^{18}}\right\}.$$
$$= 65t + 67\frac{2^2 t^3}{2!} + 65\frac{2^4 t^5}{4!} + 68\frac{2^6 t^7}{6!} + 69\frac{2^8 t^9}{8!} + 77\frac{2^{10} t^{11}}{10!} + 73\frac{2^{12} t^{13}}{12!} + 67\frac{2^{14} t^{15}}{14!} + 83\frac{2^{16} t^{17}}{16!}.$$

Then, we have:

$F_0 = 65, F_1 = 67, F_2 = 65, F_3 = 68, F_4 = 69, F_5 = 77, F_6 = 73, \quad F_7 = 67, F_8 = 83, F_n = 0 \ for\ all\ n \geq 9$.

Step (5): The final step in returning the original message from the received ciphertext is to transform the concluded infinite sequence into its equivalent alphabets (ASCII code values), resulting in the original message, which is ACADEMICS.

Illustrative Examples

1. The message that is "Academics" would be converted to:
   "Ao}♦┤gm-é" with key as:
   $0, 9, 131, 1735, 20371, 250072, 2521687, 24034419, 303694616$, for $v = 3$.
2. ACADEMICS would be converted into:
   A►`8┤ with key as:
   $0, 16, 416, 9748, 20348, 4440719, 79607889, 13888167, 30300994280$, for $v = 4$.
3. ACADEMICS would be converted into:
   " A↓}d≫d" with key as
   $0, 25, 1015, 37187, 1212890, 41357421, 1158447265, 30670166020, 1076507569000$, for $v = 5$.

Results and Discussion

This work represents the capability of using one of the integral transforms (the complex EFG integral transform) in the cryptography world. The complex EFG integral transform has been used to encrypt a message (plaintext). The message that has been discussed in the work is (ACADEMICS), and the ciphertext that has resulted from the encryption stage is (A♦@ ▒ □hx´") in the same stage, a decryption key is also concluded (0, 4, 26, 152,794, 4336, 19435, 82329, 462356). The resulting ciphertext and the concluded key will be transformed by the receiving party to be decrypted back into the original message through the received key (ACADEMICS).

The case study proved the effectiveness of using the complex EFG integral transform for such a task and opened the door to many other future applications in the cryptographic field.

References

[1] Kuffi, E. A., Karaaslan, F., & Sadkhan, G. S. (2022). The complex EFG Integral Transform and its Applications. International Journal of Health Sciences, 6(53), 537-547.

[2] Mansour, E. A., Kuffi, E. A., & Mehdi, S. A. (2022). The Solution of Faltung Type Volterra Integro-Differential Equation of First Kind using Complex SEE Transform. Journal of college of Education, Mustansiriyah University, 23(1),205-210.

[3] Mohammed, N. S., & Kuffi, E. A. (2023). Perform the CSI complex Sadik integral transform in cryptography. Journal of Interdisciplinary Mathematics, 26(6), 1303–1309. https://doi.org/10.47974/JIM-1628.

[4] Srinivas, V., & Jayanthi, C. H. (2020). Application of the New Integral "J-transform" in Cryptography. International Journal of Emerging Technologies, 11(2), 678-682.

[5] Mansour, E. A., & Meftin, N. K. (2021). Mathematical modeling for cryptography using Jafari transformation method. Periodicals of Engineering and Natural Sciences, 9(4), 892-897.

[6] Mohamad, H. A., & Mushtt, I. Z. (2018, December). Oscillatory and Asymptotic Behavior of Second Order Non-Linear Neutral Difference Equations. In Oscillatory and Asymptotic Behavior of Second

Order Non-Linear Neutral Difference Equations. Conference: The 23rd Specialized Scientific Conference of the Faculty of Education/At: Mustansiriya University-Iraq.

[7] Kuffi, E. A., & Mansour, E. A. (2015). On Hewit and Story Method for Construction Liapunov Function of Differential Algebraic Equations. Journal of College of Education, (5).

تطبيق تحويل EFG المعقد في التشفير

عماد عباس كوفي

قسم الرياضيات، كلية التربية الأساسية، الجامعة المستنصرية، بغداد، العراق
Email.emad.kuffi@uomustansiriyah.edu.iq

الخلاصة:

لقد أثبتت التحويلات التكاملية بأشكالها المختلفة، التقليدية والمعقدة، أهميتها في العديد من المجالات العلمية، وقام علماء الرياضيات باستغلالها في هذه المجالات على أكمل وجه. بالإضافة إلى توظيف التحويلات التكاملية في المجالات العلمية، يدرس علماء الرياضيات الطرق المختلفة لتحسين هذه التحويلات التكاملية من أجل تضمين أكبر عدد ممكن من التطبيقات في كل تحويل تكاملي.

يعتبر التحويل التكاملي المعقد **EFG** (عماد – فاروق – غيث) أحد التحويلات الجديدة التي لم يتم استخدامها في العديد من المجالات؛ حيث إن لم يظهر كامل إمكاناته بعد. لذلك سنعرض في هذا البحث نجاح وقدرة تحويلات **EFG** المعقدة (عماد – فاروق – غيث) في عملية خوارزميات التشفير وفك التشفير. تم إثبات إمكانات **EFG** المعقدة في مجال التشفير من خلال التطبيق العملي، وبدت نتائج هذا التطبيق واعدة للغاية من حيث إنها تضيف مجالًا جديدًا للتطبيق في التحويل المتكامل.

الكلمات المفتاحية: تحويل **EFG** المعقد، عكس تحويل **EFG**، التشفير، فك التشفير، كود **ASCII**.