On a Novel Security Algorithm for the Encryption of 3×3 Fuzzy Matrices with Rational Entries Based on The Symbolic 2-Plithogenic Integers and El-Gamal Algorithm

Yaser Ahmad Alhasan[1,*], Abuobida Mohammed A. Alfahal[1], Raja Abdullah Abdulfatah[1], Rozina Ali[2], Mayas Aljibawi[3]

[1]Deanship of the Preparatory Year, Prince Sattam bin Abdulaziz University, Alkharj, Saudi Arabia
[2]Department of Mathematics, Faculty of Science, Cairo University, Cairo, Egypt
[3]Computer Techniques Engineering Department, Al-Mustaqbal University, Hillah 51001, Iraq

Emails: y.alhasan@psau.edu.sa; a.alfahal@psau.edu.sa; r.abdulfatah@psau.edu.sa ; rozyyy123n@gmail.com; mayas.mohammed@uomus.edu.iq
Corresponding author: y.alhasan@psau.edu.sa

Abstract

Mathematical cryptography applies special properties of integers and number theory in encrypting and decrypting messages in our world which is increasingly in demand for information security, especially for social media and multimedia. The objective of this work is to generalize El-Gamal crypto algorithm to be applied by using symbolic 2-plithogenic integers instead of classical integers. Also, we apply the novel algorithm to the encryption and the decryption of square 3×3 fuzzy matrices with rational entries, and fuzzy relations which can be represented as fuzzy matrices with rational entries. In addition, many examples with numerical data will be presented.

Keywords: Symbolic 2-plithogenic integer; fuzzy matrix; fuzzy relation; EL-Gamal crypto-algorithm

1. Introduction and Preliminaries

The concept of fuzzy logic and fuzzy set was presented by Zadeh [10]. If X is a non-empty set. A fuzzy set (subset) μ of the set X is defined as a function μ: X → [0, 1], and if μ is a fuzzy subset of a set X. For t ∈ [0, 1], the set $X_t = \{x \in X ; \mu(x) \geq t\}$, then μ is called a t-level subset of the fuzzy subset μ [3].

The encryption and decryption of fuzzy matrices with rational entries was studied in [18-19] by using neutrosophic and refined neutrosophic number theory to build more complex generalizations of some public key crypto algorithms.

In this paper, we give a push to the previous efforts for applying generalized versions of number theory in cryptology, where a symbolic 2-plitogenic version of El-Gamal algorithm. For more details about symbolic plithogenic algebra see [27-34]. We refer to that El-Gamal algorithm was extended to neutrosophic integer systems in [35].

Fuzzy matrices with rational entries have many applications in many scientific fields, from this point of view, the encryption and the decryption of these matrices is an important problem and will has a big effect on the evolution of intelligent systems and computer science.

DOI: https://doi.org/10.54216/IJNS.210108
Received: March 29 2023 Revised: April 21, 2023 Accepted: May 31, 2023

Definition:

Let R be a ring, the symbolic 2-plithogenic ring is defined as follows:
$2-SP_R=\{a_0+a_1P_1+a_2P_2;\ a_i\in R, {P_j}^2=P_j, P_1\times P_2=P_{max(1,2)}=P_2\}$.
Smarandache has defined algebraic operations on $2-SP_R$ as follows:
Addition:
$[a_0+a_1P_1+a_2P_2]+[b_0+b_1P_1+b_2P_2]=(a_0+b_0)+(a_1+b_1)P_1+(a_2+b_2)P_2$.
Multiplication:
$[a_0+a_1P_1+a_2P_2].[b_0+b_1P_1+b_2P_2]=a_0b_0+a_0b_1P_1+a_0b_2P_2+a_1b_0{P_1}^2+a_1b_2P_1P_2+a_2b_0P_2+a_2b_1P_1P_2+a_2b_2{P_2}^2+a_1b_1P_1P_1=a_0b_0+(a_0b_1+a_1b_0+a_1b_1)P_1+(a_0b_2+a_1b_2+a_2b_0+a_2b_1+a_2b_2)P_2$.
We say that $A\le B$ if $a_0\le b_0, a_0+a_1\le b_0+b_1, a_0+a_1+a_2\le b_0+b_1+b_2$.
Theorem:

$A\equiv B(mod\ C)$ if and only if:
$$\begin{cases} a_0\equiv b_0(mod\ c_0) \\ a_0+a_1\equiv b_0+b_1(mod\ c_0+c_1) \\ a_0+a_1+a_2\equiv b_0+b_1+b_2(mod\ c_0+c_1+c_2)\end{cases}.$$

2. Main Discussion

Symbolic 2-Plithogenic Version of EL-Gamal algorithm:
To build a symbolic 2-plithogenic version of EL-Gamal Algorithm, we substitute each integer t by a positive symbolic 2-plithogenic integer $t_0+t_1P_1+t_2P_2\ ;\ t_0>0\ , t_0+t_1, t_0+t_1+t_2>0$.
The recipient (B) picks a symbolic 2-plithogenic positive integer $p=p_0+p_1P_1+p_2P_2$, where $p_0, p_0+p_1, p_0+p_1+p_2$ are large primes.
(B) picks a generator $0<g=g_0+g_1P_1+g_2P_2<p=p_0+p_1P_1+p_2P_2-1$, i.e $g_0<p_0-1,\ g_0+g_1<p_0+p_1-1, g_0+g_1+g_2<p_0+p_1+p_2-1$.
(B) picks $0<x=x_0+x_1P_1+x_2P_2<p=p_0+p_1P_1+p_2P_2-2$, i.e $x_0<p_0-2,\ x_0+x_1<p_0+p_1-2, x_0+x_1+x_2<p_0+p_1+p_2-2$ and then computes $X=g^x(mod\ p)={g_0}^{x_0}(mod\ p_0)+P_1[(g_0+g_1)^{x_0+x_1}(mod\ p_0+p_1)-{g_0}^{x_0}(mod\ p_0)]+P_2[(g_0+g_1+g_2)^{x_0+x_1+x_2}(mod\ p_0+p_1+p_2)-(g_0+g_1)^{x_0+x_1}(mod(p_0+p_1)]$.
The publish key is (g,X).
Assume that (A) will send $m=m_0+m_1P_1+m_2P_2$ to (B).
(A) should pick $0<r=r_0+r_1P_1+r_2P_2<p=p_0+p_1P_1+p_2P_2-2$ and compute:
$R=g^r(mod\ p)={g_0}^{r_0}(mod\ p_0)+P_1[(g_0+g_1)^{r_0+r_1}(mod\ p_0+p_1)-{g_0}^{r_0}(mod\ p_0)]+P_2[(g_0+g_1+g_2)^{r_0+r_1+r_2}(mod\ p_0+p_1+p_2)-(g_0+g_1)^{r_0+r_1}(mod(p_0+p_1)].=t_0+t_1P_1+t_2P_2$.
The shared key
$K=X^r(mod\ p)={g_0}^{x_0r_0}(mod\ p_0)+P_1\left[(g_0+g_1)^{(x_0+x_1)(r_0+r_1)}(mod\ p_0+p_1)-{g_0}^{x_0r_0}(mod\ p_0)\right]+P_2[(g_0+g_1+g_2)^{(x_0+x_1+x_2)(r_0+r_1+r_2)}(mod\ p_0+p_1+p_2)-(g_0+g_1)^{(x_0+x_1)(r_0+r_1)}(mod(p_0+p_1)]=k_0+k_1P_1+k_2P_2$.
(A) encrypts its message as follows:
$S=m\times k=(m_0+m_1P_1+m_2P_2)(k_0+k_1P_1+k_2P_2)=m_0k_0+P(m_0k_1+m_1k_1+m_1k_0)+P_2(m_0k_2+m_1k_2+m_2k_2+m_2k_0+m_2k_1)$.
The other side (B)decrypts the message as follows:
$m=R^{-x}(mod\ p);\ R^{-1}={t_0}^{-1}(mod\ p_0)+P_1[(t_0+t_1)^{-1}(mod\ p_0+p_1)-{t_0}^{-1}(mod\ p_0)]+P_2[(t_0+t_1+t_2)^{-1}(mod\ p_0+p_1+p_2)-(t_0+t_1)^{-1}(mod(p_0+p_1)]$.
Example.
Consider that (B) has picked $p=5+6P_1+2P_2$, the generator $g=3+2P_1+P_2$, the secret key is $x=2+5P_1+P_2$.
$X=g^x(mod\ p)=3^2(mod\ 5)+P_1[(5)^7(mod\ 11)-\ 3^2(mod\ 5)]+P_2[(6)^8(mod\ 13)-\ (5)^7(mod\ 11)]=4-P_1$.
The public key is $(g,X)=(\ 3+2P_1+P_2, 4-P_1)$.
Assume that (A) has decided to send $m=4+7P_1-P_2$ to (B).
The first side (A) Picks $r=2+P_1+2P_2$, and computes
$R=g^r(mod\ p)=3^2(mod\ 5)+P_1[(5)^3(mod\ 11)-\ 3^2(mod\ 5)]+P_2[(6)^5(mod\ 13)-\ (5)^3(mod\ 11)]=4-2P_2$.
The shared key is:

DOI: https://doi.org/10.54216/IJNS.210108
Received: March 29 2023 Revised: April 21, 2023 Accepted: May 31, 2023

$K = X^r(mod\ p) = (4 - P_1)^{2+P_1+2P_2}(mod\ p) = 4^2(mod\ 5) + P_1[(3)^3(mod\ 11) - 4^2(mod\ 5)] + P_2[(3)^5(mod\ 13) - (3)^3(mod\ 11)] = 1 + 4P_1 + 4P_2.$
The encrypted message is
$S = mK = (4 + 7P_1 - P_2)(1 + 4P_1 + 4P_2) = 4 + 51P_1 + 35P_2.$
The second side (B) decrypts the message as follows:
$m = R^{-x}s(mod\ p) = (1 + 8P_1 - 6P_2)(4 + 51P_1 + 35P_2)(mod\ p) = (4 + 491P_1 - 225P_2)(mod\ 5 + 6P_1 + 2P_2) = 4 + 7P_1 - P_2.$

3. 3× 3 Fuzzy Matrices as symbolic 2-plithogenic points

Definition:

Let A be a fuzzy 3 × 3 matrix with rational entries:

$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, where $a_{ij} \in Q \cap [0,1]$.

Then A can be written in term of a 3-dimensional symbolic 2-plithogenic point as follows:

$A_P = (a_{11} + a_{12}P_1 + a_{13}P_2, a_{21} + a_{22}P_1 + a_{23}P_2, a_{31} + a_{32}P_1 + a_{33}P_2).$

Example:

Consider the following fuzzy matrix:

A=$\begin{pmatrix} 0,2 & 0,4 & 0,6 \\ 0,5 & 0,1 & 0,9 \\ 0,8 & 0,1 & 0,3 \end{pmatrix}$, then A can be written in the following form:

$A_P = (0,2 + 0,4P_1 + 0,6P_2, 0,5 + 0,1P_1 + 0,9P_2, 0,8 + 0,1P_1 + 0,3P_2).$

4. The encryption/decryption of a fuzzy 3 × 3 matrix:

Let A be a fuzzy 3 × 3 matrix with rational entries

A=$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, assume that the sender (X) has decided to send the matrix A to the recipient (Y) as a cipher text.

As a first step, (X) should transform the fuzzy matrix A to a 23-dimensional symbolic 2-plithogenic point as follows:

$A_P = (a_{11} + a_{12}P_1 + a_{13}P_2, a_{21} + a_{22}P_1 + a_{23}P_2, a_{31} + a_{32}P_1 + a_{33}P_2)$, then (X) picks a weight $w \in Z^+$ with the property: $wa_{ij} \in Z^+$. This implies that $w(a_{11} + a_{12}P_1 + a_{13}P_2), w(a_{21} + a_{22}P_1 + a_{23}P_2), w(a_{31} + a_{32}P_1 + a_{33}P_2) \in 2 - SP_Z$, and (X) should send w to (Y).

The recipient (Y) generates the public key as we explained above in symbolic 2-plithogenic El-Gamal algorithm and shares his/her key with (X).

(X) decrypts the $w(a_{11} + a_{12}P_1 + a_{13}P_2), w(a_{21} + a_{22}P_1 + a_{23}P_2), w(a_{31} + a_{32}P_1 + a_{33}P_2)$ by using the key, and sends the cipher neutrosophic point to (Y).

(Y) decrypts the message as we have shown previously, and divide it by the weight w. Then (Y) rearranges the values into matrix rows to get the plain text.

Example:

We explain the validity of the novel scheme by the following example.

Consider the following fuzzy matrix:

A=$\begin{pmatrix} 0,2 & 0,4 & 0,6 \\ 0,5 & 0,1 & 0,9 \\ 0,8 & 0,1 & 0,3 \end{pmatrix}$, then A can be written in the following form:

$A_P = (0,2 + 0,4P_1 + 0,6P_2, 0,5 + 0,1P_1 + 0,9P_2, 0,8 + 0,1P_1 + 0,3P_2).$

DOI: https://doi.org/10.54216/IJNS.210108

Received: March 29 2023 Revised: April 21, 2023 Accepted: May 31, 2023

(X) picks w=10 and computes the new point $wA_P = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2)$, then (X) shares w=10 with (Y).

Assume that the recipient (Y) has generated the public key as follows:

Consider the (Y)has picked $p = 5 + 6P_1 + 2P_2$, the generator $g = 3 + 2P_1 + P_2$, the secret key is $x = 2 + 5P_1 + P_2$.
$X = g^x(mod\ p) = 3^2(mod\ 5) + P_1[(5)^7(mod\ 11) - 3^2(mod\ 5)] + P_2[(6)^8(mod\ 13) - (5)^7(mod\ 11)] = 4 - P_1$.
The public key is $(g, X) = (3 + 2P_1 + P_2, 4 - P_1)$.
(X) will send $wA_P = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2)$ to (Y).
$r = 2 + P_1 + 2P_2$, and computes
$R = g^r(mod\ p) = 3^2(mod\ 5) + P_1[(5)^3(mod\ 11) - 3^2(mod\ 5)] + P_2[(6)^5(mod\ 13) - (5)^3(mod\ 11)] = 4 - 2P_2$.
The shared key is:
$K = X^r(mod\ p) = (4 - P_1)^{2+P_1+2P_2}(mod\ p) = 4^2(mod\ 5) + P_1[(3)^3(mod\ 11) - 4^2(mod\ 5)] + P_2[(3)^5(mod\ 13) - (3)^3(mod\ 11)] = 1 + 4P_1 + 4P_2$.
The encrypted message is:
$S = wA_P \times K = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2)(1 + 4P_1 + 4P_2) = (2 + 28P_1 + 78P_2, 5 + 25P_1 + 105P_2, 8 + 37P_1 + 63P_2)$.
(Y) decrypts the message as follows:
The plain text is $wA_P = R^{-x}s(mod\ p) = (1 + 8P_1 - 6P_2)(2 + 28P_1 + 78P_2, 5 + 25P_1 + 105P_2, 8 + 37P_1 + 63P_2) = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2)$.
Now, (Y) should divide the plain text by w=10, and rearrange it as rows of a matrix to get:

A=$\begin{pmatrix} 0{,}2 & 0{,}4 & 0{,}6 \\ 0{,}5 & 0{,}1 & 0{,}9 \\ 0{,}8 & 0{,}1 & 0{,}3 \end{pmatrix}$.

5. Applications to fuzzy relations

Let $X = \{x_1, x_2, x_3\}$,$Y = \{y_1, y_2, y_3\}$ be two sets with two elements, with a fuzzy relation R(X,Y) defined on X as follows:
$f_{ij}(x_i, y_j) = a_{ij} \in [0,1]$. Then this relation can be represented as a fuzzy 3×3 matrix

A=$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, , so that by using symbolic 2-plithogenic El-Gamal algorithm we can encrypt it as a secret message.

Example:
Assume that we have the following fuzzy relation,$f(x_1, y_1) = 0.2$,
$f(x_1, y_2) = 0.4, f(x_1, y_3) = 0.6, f(x_2, y_1) = 0.5, f(x_2, y_2) = 0.1, f(x_2, y_3) = 0.9, f(x_3, y_1) = 0{,}8, f(x_3, y_2) = 0.1, f(x_3, y_3) = 0.3$.
So, it can be described by the following fuzzy matrix with rational entries:

A=$\begin{pmatrix} 0{,}2 & 0{,}4 & 0{,}6 \\ 0{,}5 & 0{,}1 & 0{,}9 \\ 0{,}8 & 0{,}1 & 0{,}3 \end{pmatrix}$, then A can be written in the following form:

$A_P = (0{,}2 + 0{,}4P_1 + 0{,}6P_2, 0{,}5 + 0{,}1P_1 + 0{,}9P_2, 0{,}8 + 0{,}1P_1 + 0{,}3P_2)$.

(X) picks w=10 and computes the new point $wA_P = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2)$, then (X) shares w=10 with (Y).

Assume that the recipient (Y) has generated the public key as follows:

Consider the (Y)has picked $p = 5 + 6P_1 + 2P_2$, the generator $g = 3 + 2P_1 + P_2$, the secret key is $x = 2 + 5P_1 + P_2$.
$X = g^x(mod\ p) = 3^2(mod\ 5) + P_1[(5)^7(mod\ 11) - 3^2(mod\ 5)] + P_2[(6)^8(mod\ 13) - (5)^7(mod\ 11)] = 4 - P_1$.
The public key is $(g, X) = (3 + 2P_1 + P_2, 4 - P_1)$.
(X) will send $wA_P = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2)$ to (Y).
$r = 2 + P_1 + 2P_2$, and computes

DOI: https://doi.org/10.54216/IJNS.210108

Received: March 29 2023 Revised: April 21, 2023 Accepted: May 31, 2023

$R = g^r(mod\ p) = 3^2(mod\ 5) + P_1[(5)^3(mod\ 11) - 3^2(mod\ 5)] + P_2[(6)^5(mod\ 13) - (5)^3(mod\ 11)] = 4 - 2P_2.$
The shared key is:
$K = X^r(mod\ p) = (4 - P_1)^{2+P_1+2P_2}(mod\ p) = 4^2(mod\ 5) + P_1[(3)^3(mod\ 11) - 4^2(mod\ 5)] + P_2[(3)^5(mod\ 13) - (3)^3(mod\ 11)] = 1 + 4P_1 + 4P_2.$
The encrypted message is:
$S = wA_P \times K = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2)(1 + 4P_1 + 4P_2) = (2 + 28P_1 + 78P_2, 5 + 25P_1 + 105P_2, 8 + 37P_1 + 63P_2).$
(Y) decrypts the message as follows:
The plain text is $wA_P = R^{-x}s(mod\ p) = (1 + 8P_1 - 6P_2)(2 + 28P_1 + 78P_2, 5 + 25P_1 + 105P_2, 8 + 37P_1 + 63P_2) = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2).$
Now, (Y) should divide the plain text by w=10, and rearrange it as rows of a matrix to get:
A=$\begin{pmatrix} 0{,}2 & 0{,}4 & 0{,}6 \\ 0{,}5 & 0{,}1 & 0{,}9 \\ 0{,}8 & 0{,}1 & 0{,}3 \end{pmatrix}$.
Now, (Y) should divide the plain text by w=10, and rearrange it as rows of a matrix to get:
A=$\begin{pmatrix} 0{,}2 & 0{,}4 & 0{,}6 \\ 0{,}5 & 0{,}1 & 0{,}9 \\ 0{,}8 & 0{,}1 & 0{,}3 \end{pmatrix}$. This means that (Y) is able to reform the secret fuzzy relation in the original form
$f(x_1, y_1) = 0.2,$
$f(x_1, y_2) = 0.4, f(x_1, y_3) = 0.6, f(x_2, y_1) = 0.5, f(x_2, y_2) = 0.1, f(x_2, y_3) = 0.9, f(x_3, y_1) = 0.8, f(x_3, y_2) = 0.1, f(x_3, y_3) = 0.3.$
Example:
Assume that we have the following fuzzy relation, $f(x_1, y_1) = 0.1,$
$f(x_1, y_2) = 0.4, f(x_1, y_3) = 0.7, f(x_2, y_1) = 0.1, f(x_2, y_2) = 0.1, f(x_2, y_3) = 0.1, f(x_3, y_1) = 0.2, f(x_3, y_2) = 0.1, f(x_3, y_3) = 0.3.$
So, it can be described by the following fuzzy matrix with rational entries:
A=$\begin{pmatrix} 0{,}1 & 0{,}4 & 0{,}7 \\ 0{,}1 & 0{,}1 & 0{,}1 \\ 0{,}2 & 0{,}1 & 0{,}3 \end{pmatrix}$, then A can be written in the following form:

$A_P = (0{,}1 + 0{,}4P_1 + 0{,}7P_2, 0{,}1 + 0{,}1P_1 + 0{,}1P_2, 0{,}2 + 0{,}1P_1 + 0{,}3P_2).$

(X) picks w=10 and computes the new point $wA_P = (1 + 4P_1 + 7P_2, 1 + P_1 + P_2, 2 + P_1 + 3P_2)$, then (X) shares w=10 with (Y).

Assume that the recipient (Y) has generated the public key as follows:

Consider the (Y)has picked $p = 5 + 6P_1 + 2P_2$, the generator $g = 3 + 2P_1 + P_2$, the secret key is $x = 2 + 5P_1 + P_2$.
$X = g^x(mod\ p) = 3^2(mod\ 5) + P_1[(5)^7(mod\ 11) - 3^2(mod\ 5)] + P_2[(6)^8(mod\ 13) - (5)^7(mod\ 11)] = 4 - P_1.$
The public key is $(g, X) = (3 + 2P_1 + P_2, 4 - P_1).$
(X) will send $wA_P = (2 + 4P_1 + 6P_2, 5 + P_1 + 9P_2, 8 + P_1 + 3P_2)$ to (Y).
$r = 2 + P_1 + 2P_2$, and computes
$R = g^r(mod\ p) = 3^2(mod\ 5) + P_1[(5)^3(mod\ 11) - 3^2(mod\ 5)] + P_2[(6)^5(mod\ 13) - (5)^3(mod\ 11)] = 4 - 2P_2.$
The shared key is:
$K = X^r(mod\ p) = (4 - P_1)^{2+P_1+2P_2}(mod\ p) = 4^2(mod\ 5) + P_1[(3)^3(mod\ 11) - 4^2(mod\ 5)] + P_2[(3)^5(mod\ 13) - (3)^3(mod\ 11)] = 1 + 4P_1 + 4P_2.$
The encrypted message is:
$S = wA_P \times K = (1 + 4P_1 + 7P_2, 1 + P_1 + P_2, 2 + P_1 + 3P_2)(1 + 4P_1 + 4P_2) = (1 + 24P_1 + 83P_2, 1 + 9P_1 + 17P_2, 2 + 13P_1 + 39P_2).$
(Y) decrypts the message as follows:
The plain text is $wA_P = R^{-x}s(mod\ p) = (1 + 8P_1 - 6P_2)(1 + 24P_1 + 83P_2, 1 + 9P_1 + 17P_2, 2 + 13P_1 + 39P_2) = (1 + 4P_1 + 7P_2, 1 + P_1 + P_2, 2 + P_1 + 3P_2).$
Now, (Y) should divide the plain text by w=10, and rearrange it as rows of a matrix to get:
A=$\begin{pmatrix} 0{,}1 & 0{,}4 & 0{,}7 \\ 0{,}1 & 0{,}1 & 0{,}1 \\ 0{,}2 & 0{,}1 & 0{,}3 \end{pmatrix}$.
This means that (Y) is able to reform the secret fuzzy relation in the original form

DOI: https://doi.org/10.54216/IJNS.210108

Received: March 29 2023 Revised: April 21, 2023 Accepted: May 31, 2023

$f(x_1, y_1) = 0.1$,
$f(x_1, y_2) = 0.4, f(x_1, y_3) = 0.7, f(x_2, y_1) = 0.1, f(x_2, y_2) = 0.1, f(x_2, y_3) = 0.1, f(x_3, y_1) = 0.2, f(x_3, y_2) = 0.1, f(x_3, y_3) = 0.3$.
Now, we show a comparison of time duration between symbolic 2-plithogenic El-Gamal system, and classical system.
Table 1: A Comparison of time duration between symbolic 2-plithogenic El-Gamal system, and classical system.

Time Duration measured by m.sec	**El Gamal Crypto System**	**Symbolic 2-plithogenic system**
Around 1,0031 for classical system Around 1,04358787251 For the novel system	For $500000 < g < 1000000$	For $500000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 1000000$
Around 9,12001 for the classical system Around 767,533023 For the novel system	For $5000000 < g < 10000000$	For $5000000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 10000000$
Around 25,3241 for the classical system Around 16257,5906 for the novel system	For $10000000 < g < 30000000$	For $1000000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 30000000$
Around 223,1348 for the classical system Around 11329689.544475 for the novel system	For $100000000 < g < 300000000$	For $10000000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 300000000$

The previous table explains the complexity of the new algorithm compared to the classical algorithm.

Table 2: A Comparison between refined neutrosophic El-Gamal algorithm and symbolic 2-plithogenic system:

Time Duration measured by m.sec	**Symbolic 2-plithogenic system**	**Refined Neutrosophic El Gamal Crypto System**
Around 1,0031 for classical system Around 1,04358787251 For the refined neutrosophic system	For $500000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 1000000$	For $500000 < g_0, g_0 + g_2, g_0 + g_1 + g_2 < 1000000$
Around 9,12001 for the classical system Around 767,533023 For the refined neutrosophic system	For $5000000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 10000000$	For $5000000 < g_0, g_0 + g_2, g_0 + g_1 + g_2 < 10000000$
Around 25,3241 for the classical system Around 16257,5906 refined neutrosophic system	For $1000000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 30000000$	For $1000000 < g_0, g_0 + g_2, g_0 + g_1 + g_2 < 30000000$
Around 223,1348 for the classical system Around 11329689.544475 for the refined neutrosophic system	For $10000000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 300000000$	For $10000000 < g_0, g_0 + g_2, g_0 + g_1 + g_2 < 300000000$

6. Conclusion

In this paper, we have used the basics of symbolic 2-plithogenic number theory and classical El-Gamal crypto-system to present symbolic 2-plithogenic EL-Gamal algorithm. In addition, we use the novel algorithm to encrypt and decrypt messages that contain 3×3 fuzzy matrices with rational entries.

Acknowledgments " This study is supported via funding from Prince sattam bin Abdulaziz University project number (PSAU/2023/R/1444) ".

DOI: https://doi.org/10.54216/IJNS.210108

Received: March 29 2023 Revised: April 21, 2023 Accepted: May 31, 2023

References

[1] Abobala, M., (2021). Partial Foundation of Neutrosophic Number Theory. Neutrosophic Sets and Systems, Vol. 39..

[2] Abobala, M., and Ziena, M.B., (2023) . A Study Of Neutrosophic Real Analysis By Using One Dimensional Geometric AH-Isometry. Galoitica Journal Of Mathematical Structures and Applications, Vol 3.

[3] Akram, M.; Dudek, W.A. Regular bipolar fuzzy graphs. Neural Comput. Appl. **2012**, 21, 197–205.

[4] Cozzens, M. Miller, S.J. (2013). The Mathematics of Encryption: An Elementary Introduction, American Mathematical Society.

[5] D.S.Malik, J.N.Mordeson, Fuzzy Commutative Algebra, World Scientific Publishing, Singapore, 1998.

[6] G. Emam and M.Z. Ragab, The Determinant and Adjoint of a Square Fuzzy Matrix, Information Sciences, vol. 84 (New York, New York, 1995) pp. 209-220.

[7] HAO, Jiang, General theory on fuzzy subgroupoids with respect to a t-norm T1, Fuzzy Sets and Systems, **117**, 455-461 (2001).

[8] Ilanthenral, F. Smarandache, and W.B. Vasantha Kandasamy, Elementary Fuzzy Matrix215 Theory and Fuzzy Models for Social Scientists, (Los Angeles, California, 2007) p. 33.

[9] K.S. Krishnamohan and K. Muthugurupackiam, Generalisation of Idempotent Fuzzy Matrices, International Journal of Applied Engineering Research, vol. 13, no. 13 (2018) pp. 11087-11090.

[10] L.A.Zadeh, Fuzzy sets, Inform. Control 8(1965) 383-353.

[11] M.G. Thomason, Convergence of powers of a fuzzy matrix, Journal of Mathematical Analysis and Applications, vol. 57(2) (February 1977) pp. 476-480.

[12] Martin, N., Priya, R., & Smarandache, F. (2021). New Plithogenic sub cognitive maps approach with mediating effects of factors in COVID-19 diagnostic model. Journal of Fuzzy Extension and Applications, 2(1), 1-15. doi: 10.22105/jfea.2020.250164.1015

[13] P.W. Eklund, X. Sun, and D.A. Thomas, Fuzzy Matrices: An Application in Agriculture, Proc. IPMU, (September 1995) pp. 765-769.

[14] Polymenis, A. (2021). A neutrosophic Student's t –type of statistic for AR (1) random processes. Journal of Fuzzy Extension and Applications, 2(4), 388-393. doi: 10.22105/jfea.2021.287294.1149.

[15] Rivest, R. Shamir, Adleman, A. (1975). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM (21): 120-126.

[16] Smarandache, F. (1999). A Unifying Field in Logics. Neutrosophy: Neutrosophic Probability, Set and Logic. Rehoboth: American Research Press.

[17] X.Yuan, E.S.Lee,Fuzzy group based on fuzzy binary operation, Comput. Math. App. 47 (2004) 631-641.

[18] Merkepci, M., Abobala, M., and Allouf, A., " The Applications of Fusion Neutrosophic Number Theory in Public Key Cryptography and the Improvement of RSA Algorithm ", Fusion: Practice and Applications, 2023.

[19] Merkepci, M,; Sarkis, M. An Application of Pythagorean Circles in Cryptography and Some Ideas for Future Non Classical Systems. Galoitica Journal of Mathematical Structures and Applications **2022**.

[20] S.Barzut, M.Milosavljevic, S. Adamovic, M. Saračević, N. Macek, M.Gnjatovic (2021), A Novel Fingerprint Biometric Cryptosystem Based on Convolutional Neural Networks, Mathematics, 9(7), 730.

[21] Aroukatos, N.; Manes, K.; Zimeras, S.; Georgiakodis, F. Techniques in Image Steganography using Famous Number Sequences.Int. J. Comput. Technol. 2013, 11, 2321–2329.

[22] Merkepci, M., and Abobala, M., " Security Model for Encrypting Uncertain Rational Data Units Based on Refined Neutrosophic Integers Fusion and El Gamal Algorithm ", Fusion: Practice and Applications, 2023.

[23] Hatip, A., " On Intuitionistic Fuzzy Subgroups of (M-N) Type and Their Algebraic Properties", Galoitica Journal Of Mathematical Structures and Applications, Vol.4, 2023.

[24] Zayood, K., " On Novel Public-key Cryptosystem Using MDS Code", Neoma Journal Of Mathematics and Computer Science, 2023.

[25] Zayood, K., " On A Novel Generalization of The RSA Crypto-System", Neoma Journal Of Mathematics and Computer Science, 2023.

[26] Al Basheer, O., " On Some Novel Simplex Linear Codes Defined Over The Algebraic Ring $\boldsymbol{F2+vF2}$ ", Neoma Journal Of Mathematics and Computer Science, 2023.

[27] Nader Mahmoud Taffach , Ahmed Hatip., "A Review on Symbolic 2-Plithogenic Algebraic Structures " Galoitica Journal Of Mathematical Structures and Applications, Vol.5, 2023.

[28] Nader Mahmoud Taffach , Ahmed Hatip.," A Brief Review on The Symbolic 2-Plithogenic Number Theory and Algebraic Equations ", Galoitica Journal Of Mathematical Structures and Applications, Vol.5, 2023.

DOI: https://doi.org/10.54216/IJNS.210108

Received: March 29 2023 Revised: April 21, 2023 Accepted: May 31, 2023

[29] Merkepci, H., and Abobala, M., " On The Symbolic 2-Plithogenic Rings", International Journal of Neutrosophic Science, 2023.

[30] Smarandache, F., " Introduction to the Symbolic Plithogenic Algebraic Structures (revisited)", Neutrosophic Sets and Systems, vol. 53, 2023.
[31] Taffach, N., " An Introduction to Symbolic 2-Plithogenic Vector Spaces Generated from The Fusion of Symbolic Plithogenic Sets and Vector Spaces", Neutrosophic Sets and Systems, Vol 54, 2023.
[32] Taffach, N., and Ben Othman, K., " An Introduction to Symbolic 2-Plithogenic Modules Over Symbolic 2-Plithogenic Rings", Neutrosophic Sets and Systems, Vol 54, 2023.
[33] Merkepci, H., and Rawashdeh, A., " On The Symbolic 2-Plithogenic Number Theory and Integers ", Neutrosophic Sets and Systems, Vol 54, 2023.
[34] Albasheer, O., Hajjari., A., and Dalla., R., " On The Symbolic 3-Plithogenic Rings and TheirAlgebraic Properties", Neutrosophic Sets and Systems, Vol 54, 2023.
[35] Abobala, M., and Allouf, A., " On A Novel Security Scheme for The Encryption and Decryption Of 2×2 Fuzzy Matrices with Rational Entries Based on The Algebra of Neutrosophic Integers and El-Gamal Crypto-System", Neutrosophic Sets and Systems, vol.54, 2023.

DOI: https://doi.org/10.54216/IJNS.210108

Received: March 29 2023 Revised: April 21, 2023 Accepted: May 31, 2023