Security Model for Encrypting Uncertain Rational Data Units Based on Refined Neutrosophic Integers Fusion and El Gamal Algorithm

Article · March 2023

DOI: 10.54216/FPA.100203

CITATIONS
0

READS
2

2 authors, including:

Mohammad Abobala
Tishreen University
62 PUBLICATIONS **1,845** CITATIONS

SEE PROFILE

Security Model for Encrypting Uncertain Rational Data Units Based on Refined Neutrosophic Integers Fusion and El Gamal Algorithm

Mehmet Merkepci[1], Mohammad Abobala[2]

[1]Department of Computer Engineering, Gaziantep University, Gaziantep, Turkey
[2] Tishreen University, Department of Mathematics, Latakia, Syria

Emails: mehmet.merkepci@gmail.com; Mohammadabobala777@gmail.com

Abstract

The objective of this paper is to introduce a novel security model for the encryption of uncertain rational data units represented as single-valued rational neutrosophic numbers by combining refined neutrosophic number theoretical concepts with the El Gamal public key crypto scheme. In addition, some applications on uncertain data units will be shown and illustrated.

Keywords: El Gamal crypto scheme; neutrosophic integer Fusion; uncertain rational data unit; neutrosophic number; indeterminacy

1. Introduction and preliminaries

Uncertainty arises in many real-life problems, especially in statistics and physics [3-4]. For uncertain data, mathematicians have improved many models to deal with these kinds of data, such as fuzzy sets [10], intuitionistic fuzzy sets [2], and neutrosophic sets [8].

Single-valued neutrosophic logic deals with data by providing three logical values, the truth (T), the falsity (F), and the indeterminacy (I) [9]. This idea has a generalized fuzzy logic approach, which was dependent on truth and falsity values only.

In the literature, we find many applications of number theory in public key cryptography, where RSA and El Gamal algorithms were built over the ideas of number theory [5,7]. The main goal of cryptography is to keep data and messages secret. From this point of view, we apply refined neutrosophic number theory to encrypt uncertain data units represented as single-valued rational neutrosophic numbers with a novel algorithm depending on the EL Gamal crypto scheme. The application of neutrosophic number theory in cryptography was first supposed in [11].

We define an uncertain data unit as a single-valued neutrosophic number (x_T, y_F, z_I), where $x_T, y_F, z_I \in]0^-, 1^+[$.

The triple (x_T, y_F, z_I) denotes truth, falsity, and uncertainty (indeterminacy) logical values, respectively.

For example, consider that we have measured the ability of 7 players in team X, and we have found that they can score a goal or two goals from 4 possible chances, then the truth value for those players is 0.25 or 0.5.

Doi: https://doi.org/10.54216/FPA.100203
Received: November 09, 2022 Accepted: March 19, 2023

Since we have not checked the other four players, then we can say that the truth value for the team is around 0.25, the indeterminacy is about 0.25, and the falsity is about 0.5. This experiment represents an uncertain data unit (0.25,0.5,0.25).

An uncertain data unit is called rational if and only if $x_T, y_F, z_I \in Q$, i.e. $x_T = \frac{a}{b}, y_F = \frac{c}{d}, z_I = t/m$, where $a, b, c, d, t, m \in Z^+$. For example, (0.25,0.5,0.25) is considered a rational uncertain data unit.

The description of El Gamal crypto-scheme:

Assume that we have two sides A and B, the first side A wants to send an encrypted message to B.

The recipient B picks a large prime number p and a generator $1 < g < p - 1$, then B picks x that $0 < x < p - 2$ and computes $X = g^x (mod\ p)$. The number x is kept as the secret key, suppose that A wants to send (m) as a message to B.

A should pick $0 < r < p - 2$and compute $R = g^r (mod\ p)$, the shared key K is computed as follows $K = X^r (mod\ p)$.

A encrypts the message as follows $S = m \times k$ and sends the encrypted message to B as a duplet (R, S).

The second side B decrypts the message by using her/his secret key x as follows $m = R^{-x} \times S$.

For example:

Consider that (B) picked $p = 7, g = 4, x = 4$, then $\mathrm{X} \equiv 4^4 (\mathrm{mod}\ 7) = 4$.

Assume that A picked $r = 2, \mathrm{R} \equiv 4^2 (\mathrm{mod}\ 7) = 2$.

The shared key $\mathrm{K} \equiv X^r (\mathrm{mod}\ 7) \equiv 4^2 (\mathrm{mod}\ 7) = 2$.

A encrypts the message as follows $S = m \times k = 5 \times 2 = 10 \equiv 3 (\mathrm{mod}\ 7)$, where $m = 5$.

B encrypts the message as follows:

$R^{-x} \times S = 2^{-4} \times 3 \equiv (2^{-1})^4 \times 3 (\mathrm{mod}\ 7) \equiv 4^4 \times 3 (\mathrm{mod}\ 7) \equiv 12\ (\mathrm{mod}\ 7) = 5$.

Definition: [1]

Let R be any ring, the corresponding refined neutrosophic ring is defined as follows:

$R(I_1, I_2) = \{(a, bI_1, cI_2); a, b, c \in R\}$.

Definition : [1]

The addition is defined as follows:

$(x, yI_1, zI_2) + (a, bI_1, cI_2) = (x + a, [y + b]I_1, [z + c]I_2)$.

Multiplication is defined as follows:

$(x, yI_1, zI_2).(a, bI_1, cI_2) = (x.a, [x.b + y.a + y.b + y.c + z.b]I_1, [x.c + z.a + z.c]I_2)$.

Theorem : [6]

Let $x = (x_0, x_1I_1, x_2I_2), y = (y_0, y_1I_1, y_2I_2), z = (z_0, z_1I_1, z_2I_2)$ be three elements in $Z(I_1, I_2)$. Then $x \equiv y(modz)$ if and only if

$x_0 \equiv y_0 (mod\ z_0), x_0 + x_2 \equiv y_0 + y_2 (mod\ z_0 + z_2), x_0 + x_1 + x_2 \equiv y_0 + y_1 + y_2 (mod\ z_0 + z_1 + z_2)$.

Definition : [6]

Let $\mathrm{Z}(I_1, I_2) = \{(a\ bI_1, cI_2);\ a, b, c \in Z\}$ be the refined neutrosophic ring of integers, we say that $(a\ bI_1, cI_2) \leq (x, yI_1, zI_2)$ if and only if $a \leq x\ and\ a + c \leq x + z, a + b + c \leq x + y + z$.

Which is a partial order relation on $Z(I_1, I_2)$.

Doi: https://doi.org/10.54216/FPA.100203
Received: November 09, 2022 Accepted: March 19, 2023

Remark:

Refined neutrosophic numbers can be written as $x + yI_1 + zI_2$ instead of (x, yI_1, zI_2).

For definitions and theorems about refined neutrosophic integers and numbers, theory check [6].

Theorem : [6]

Let $x = (x_0, x_1I_1, x_2I_2) \in Z(I_1, I_2)$, let n be any positive integer, hence $x^n = (x_0^n, I_1[(x_0 + x_1 + x_2)^n - (x_0 + x_2)^n], I_2[(x_0 + x_2)^n - x_0^n])$.

Main discussion

In the following, we establish the mathematical foundation of the refined neutrosophic EL Gamal crypto-scheme.

Refined neutrosophic EL-Gamal algorithm:
Assume that we have two sides $(A)(\ and\ B)$. The first side (A) has decided to send an encrypted message to (B).
The recipient (B) picks a large refined positive number $p = p_0 + p_1I_1 + p_2I_2$(it is preferred that $p_0, p_0 + p_2, p_0 + p_1 + p_2$ are large primes), and a generator $g = g_0 + g_1I_1 + g_2I_2$such that $1 < g < p - 1$, i.e, $g_0 + g_2 < p_0 + p_2 - 1$, $g_0 + g_1 + g_2 < p_0 + p_1 + p_2 - 1$.
(B) should pick $x_0 + x_1I_1 + x_2I_2$ such that $0 < x < p - 2$, i.e $x_0 < p_0 - 2$, $x_0 + x_2 < p_0 + p_2 - 2$, $x_0 + x_1 + x_2 < p_0 + p_1 + p_2 - 2$.
Then (B) computes $X = g^r(mod\ p)$, where:
$g^x = {g_0}^{x_0}(mod\ p_0) + I_1\left[(g_0 + g_1 + g_2)^{(x_0+x_1+x_2)}(mod\ p_0 + p_1 + p_2) - (g_0 + g_2)^{x_0+x_2}(mod\ p_0 + p_2)\right] + I_2\left[(g_0 + g_2)^{(x_0+x_2)}(mod\ p_0 + p_2) - {g_0}^{x_0}(mod\ p_0)\right]$,
$X = {g_0}^{x_0}(mod\ p_0) + I_1\left[(g_0 + g_1 + g_2)^{(x_0+x_1+x_2)}(mod\ p_0 + p_1 + p_2) - (g_0 + g_2)^{x_0+x_2}(mod\ p_0 + p_2)\right] + I_2\left[(g_0 + g_2)^{(x_0+x_2)}(mod\ p_0 + p_2) - {g_0}^{x_0}(mod\ p_0)\right]$,
The refined neutrosophic number x is kept as a secret key. The public key is (g, X).
Suppose that (A) has decided to send $m = m_0 + m_1I_1 + m_2I_2$ as a message to (B).
(A) should pick $0 < r = r_0 + r_1I_1 + r_2I_2 < p - 2$ and compute $R = g^r(mod\ p)$, where:
$g^r = {g_0}^{r_0} + I_1\left[(g_0 + g_1 + g_2)^{(r_0+r_1+r_2)} - (g_0 + g_2)^{r_0+r_2}\right] + I_2[(g_0 + g_1 + g_2)^{r_0+r_2} - {g_0}^{r_0}]$
The shared key K is computed s follows:
$K = X^r(mod\ p)$, where:
$X^r = {x_0}^{r_0} + I_1\left[(x_0 + x_1 + x_2)^{(r_0+r_1+r_2)} - (x_0 + x_2)^{r_0+r_2}\right] + I_2[(x_0 + x_2)^{r_0+r_2} - {x_0}^{r_0}]$
(A) encrypts the message as follows $S = m \times k$
(B) decrypts the message as follows $m = R^{-x} \times S$, where
$R^{-1} = {r_0}^{-1}(mod\ p_0) + I_1[(r_0 + r_1 + r_2)^{-1}(mod\ p_0 + p_1 + p_2) - (r_0 + r_2)^{-1}(mod\ p_0 + p_2)] + I_2[(r_0 + r_2)^{-1}(mod\ p_0 + p_2) - {r_0}^{-1}(mod\ p_0)]$

Example.
Consider that (B)picked $p = 7 + 2I_1 + 4I_2$, $1 < g = 3 + I_1 + 2I_2 < p - 1$, $1 < x = 2 + 3I_1 + I_2 < p - 2$
$g^x = 3^2 + I_1[6^6 - 5^3] + I_2[5^3 - 3^2]$
$X^r \equiv g^x(mod\ p) = 3^2(mod\ 7) + I_1[6^6(mod\ 13) - 5^3(mod\ 11)] + I_2[5^3(mod\ 11) - 3^2(mod\ 7)] = 2 + I_1[12 - 4] + I_2[4 - 2] = 2 + 8I_1 + 2I_2$.
The public key is $(3 + I_1 + 2I_2, 2 + 8I_1 + 2I_2)$.
Assume that (A) has picked $0 < r = 1 + 3I_1 + 3I_2 < p - 2$
$g^r = 3^1 + I_1[6^7 - 5^4] + I_2[5^4 - 3^1]$
$R \equiv g^r(mod\ p) = 3(mod\ 7) + I_1[6^7(mod\ 13) - 5^4(mod\ 11)] + I_2[5^4(mod\ 11) - 3(mod\ 7)] = 3 + I_1[7 - 9] + I_2[9 - 3] = 3 - 2I_1 + 6I_2$,
$X^r = 2^1 + I_1[12^7 - 4^4] + I_2[4^4 - 2^1]$
The shared key is:
$K \equiv X^r(mod\ p) = 2(mod\ 7) + I_1[12^7(mod\ 13) - 4^4(mod\ 11)] + I_2[4^4(mod\ 11) - 2(mod\ 7)] = 2 + I_1[12 - 4] + I_2[3 - 2] = 2 + 9I_1 + I_2$.
Suppose that (A) has decided to send $m = 4 + 5I_1 + 2I_2$ to (B).
(A) encrypts the message as follows:
$S = m \times k = (4 + 5I_1 + 2I_2)(2 + 9I_1 + I_2) = 8 + 36I_1 + 4I_2 + 10I_1 + 45I_1 + 5I_1 + 4I_2 + 18I_1 + 2I_2 = 8 + 114I_1 + 10I_2$.
(B) encrypts the message as follows:

Doi: https://doi.org/10.54216/FPA.100203
Received: November 09, 2022 Accepted: March 19, 2023

$R^{-1} = 3^{-1}(mod\ 7) + I_1[7^{-1}(mod\ 13) - 9^{-1}(mod\ 11)] + I_2[9^{-1}(mod\ 11) - 3^{-1}(mod\ 7)] = 5 + I_1[2-5] + I_2[5-5] = 5 - 3I_1.$
$R^{-x} = (R^{-1})^x = 5^2 + I_1[2^6 - 5^3] + I_2[5^3 - 5^2] = 25 - 61I_1 + 100I_2,$
$R^{-x} \times S = (25 - 61I_1 + 100I_2)(8 + 114I_1 + 10I_2) = 200 + 2850I_1 + 250I_2 - 488I_1 - 6954I_1 - 610I_1 + 800I_2 + 11400I_1 + 1000I_2 = 200 + 6198I_1 + 2050I_2.$
$R^{-x} \times S(mod\ p) = 200(mod\ 7) + I_1[8448(mod\ 13) - 2250(mod\ 11)] + I_2[2250(mod\ 11) - 200(mod\ 7)] = 4 + I_1[11-6] + I_2[6-4] = 4 + 5I_1 + 2I_2.$
Which is plain text.

Encrypting rational uncertain data units:

Suppose that we have an uncertain rational unit of data with the first side (A) who wants to share it with the second side (B) secretly.

The first side (A) should transform the uncertain data unit into a refined neutrosophic integer, for this goal (A) chooses a positive integer w such that $wx_T, wy_F, wz_I \in Z^+$, then (A) sends (w) to (B).

The second side generates the public key in the same way we have described in the refined neutrosophic El Gamal algorithm.

The first side (A) forms his message as follows:

$m = wx_T + wy_F I_1 + wz_I I_2 = m_0 + m_1 I_1 + m_2 I_2.$

Then (A) continues the steps of the refined EL Gamal algorithm that have been explained before to send the text m to (B).

(B) decrypts the message normally, then (B) computes the logical values of the uncertain data unit as follows:

$x_T = \frac{m_0}{w}, y_F = \frac{m_1}{w}, z_I = \frac{m_2}{w}.$

Example:

Suppose that we have two sides (X) and (Y) involved in a war between their country (A) and another country (B).

(X) has some information about the nuclear weapons of (B). According to the estimations of military data scientists in the country (A), they ensure that (B) is ready to use 0.3 of its weapons in the first month, and 0.4 of its weapons can not be used, and there is uncertainty about the other weapons if they are ready to be used or not, this uncertainty has been estimated as 0.6. This means that (X) has rational uncertain data, which can be represented as follows: $(0.3, 0.4, 0.6)$.

(X) has decided to share information and statistics with (Y) through an insecure channel. For this goal, (X) picks $w = 10$, and forms his message as a refined neutrosophic integer as follows:

$m = 10(0.3) + 10(0.4)I_1 + (10)(0.6)I_2 = 3 + 4I_1 + 6I_2.$

(X) sends $w = 10$ to (Y) as a first step.

(Y) picks $p = 7 + 2I_1 + 4I_2, 1 < g = 3 + I_1 + 2I_2 < p - 1, 1 < x = 2 + 3I_1 + I_2 < p - 2$
$g^x = 3^2 + I_1[6^6 - 5^3] + I_2[5^3 - 3^2]$
$X^r \equiv g^x(mod\ p) = 3^2(mod\ 7) + I_1[6^6(mod\ 13) - 5^3(mod\ 11)] + I_2[5^3(mod\ 11) - 3^2(mod\ 7)] = 2 + I_1[12-4] + I_2[4-2] = 2 + 8I_1 + 2I_2.$
The public key is $(3 + I_1 + 2I_2, 2 + 8I_1 + 2I_2)$.
Now, (X) picks $0 < r = 1 + 3I_1 + 3I_2 < p - 2$
$g^r = 3^1 + I_1[6^7 - 5^4] + I_2[5^4 - 3^1]$
$R \equiv g^r(mod\ p) = 3(mod\ 7) + I_1[6^7(mod\ 13) - 5^4(mod\ 11)] + I_2[5^4(mod\ 11) - 3(mod\ 7)] = 3 + I_1[7-9] + I_2[9-3] = 3 - 2I_1 + 6I_2.$
$X^r = 2^1 + I_1[12^7 - 4^4] + I_2[4^4 - 2^1]$
The shared key is:
$K \equiv X^r(mod\ p) = 2(mod\ 7) + I_1[12^7(mod\ 13) - 4^4(mod\ 11)] + I_2[4^4(mod\ 11) - 2(mod\ 7)] = 2 + I_1[12-4] + I_2[3-2] = 2 + 9I_1 + I_2.$
(X) encrypts the message as follows:

Doi: https://doi.org/10.54216/FPA.100203
Received: November 09, 2022 Accepted: March 19, 2023

$S = m \times k = (3 + 4I_1 + 6I_2)(2 + 9I_1 + I_2) = 6 + 27I_1 + 3I_2 + 8I_1 + 36I_1 + 4I_1 + 12I_2 + 54I_1 + 6I_2 = 6 + 129I_1 + 21I_2$. Then sends the previous cipher data to (Y).

Now, (Y) decrypts the message as follows:

$R^{-x} \times S = (25 - 61I_1 + 100I_2)(6 + 129I_1 + 21I_2) = 150 + 3225I_1 + 525I_2 - 366I_1 - 7869I_1 - 1281I_1 + 600I_2 + 12900I_1 + 2100I_2 = 150 + 6609I_1 + 3225I_2$.

$R^{-x} \times S(mod\ p) = 150(mod\ 7) + I_1[9984(mod\ 13) - 3375\ (mod\ 11)] + I_2[3375(mod\ 11) - 150(mod\ 7)] = 3 + I_1[13 - 9] + I_2[9 - 3] = 3 + 4I_1 + 6I_2$, which is the plain text.

Now, (Y) computes the logical values as follows:

$\frac{3}{10} = 0.3, \frac{4}{10} = 0.4, \frac{6}{10} = 0.6$. This means that (Y) has got the following statement: (B) is ready to use 0.3 of its weapons in the first month, and 0.4 of its weapons can not be used, and there is uncertainty about the other weapons if they are ready to be used or not, this uncertainty has been estimated as 0.6.

Remark that if the message has been attacked, then the attacker will see $150 + 6609I_1 + 3225I_2$, which is meaningless with respect to the original data.

Example:

We assume that we have confidential information about the effectiveness of a drug for covid-19 cases in the hospital (A), this information should be sent confidentially to the government health officer (B) through an insecure messaging channel that is vulnerable to hacking and cyber-attack.

Suppose that the considered drug has contributed to the cure of 20% of cases and negatively affected 30% of cases, while the effect is still unknown for the remaining 50% of patients. This means that (A) has an uncertain unit of rational data represented as (0.2,0,3,0,5).

The sender (A) picks $w = 10$ and forms his message as follows:

$m = 10(0.2) + 10(0.3)I_1 + 10(0.5)I_2 = 2 + 3I_1 + 5I_2$, then (A) sends w=10 to (B).

(B) generates the public key as follows: (we will use the same numbers in the previous example):

(B) picks $p = 7 + 2I_1 + 4I_2$, $1 < g = 3 + I_1 + 2I_2 < p - 1$, $1 < x = 2 + 3I_1 + I_2 < p - 2$

$g^x = 3^2 + I_1[6^6 - 5^3] + I_2[5^3 - 3^2]$

$X^r \equiv g^x(mod\ p) = 3^2(mod\ 7) + I_1[6^6(mod\ 13) - 5^3(mod\ 11)] + I_2[5^3(mod\ 11) - 3^2(mod\ 7)] = 2 + I_1[12 - 4] + I_2[4 - 2] = 2 + 8I_1 + 2I_2$.

The public key is $(3 + I_1 + 2I_2, 2 + 8I_1 + 2I_2)$.

Now, (A) picks $0 < r = 1 + 3I_1 + 3I_2 < p - 2$

$g^r = 3^1 + I_1[6^7 - 5^4] + I_2[5^4 - 3^1]$

$R \equiv g^r(mod\ p) = 3(mod\ 7) + I_1[6^7(mod\ 13) - 5^4(mod\ 11)] + I_2[5^4(mod\ 11) - 3(mod\ 7)] = 3 + I_1[7 - 9] + I_2[9 - 3] = 3 - 2I_1 + 6I_2$.

$X^r = 2^1 + I_1[12^7 - 4^4] + I_2[4^4 - 2^1]$

The shared key is:

$K \equiv X^r(mod\ p) = 2(mod\ 7) + I_1[12^7(mod\ 13) - 4^4(mod\ 11)] + I_2[4^4(mod\ 11) - 2(mod\ 7)] = 2 + I_1[12 - 4] + I_2[3 - 2] = 2 + 9I_1 + I_2$.

(A) encrypts the message as follows:

$S = m \times k = (2 + 3I_1 + 5I_2)(2 + 9I_1 + I_2) = 4 + 18I_1 + 2I_2 + 6I_1 + 27I_1 + 3I_1 + 10I_2 + 45I_1 + 5I_2 = 4 + 99I_1 + 17I_2$. Then sends the previous cipher data to (B).

Now, (B) decrypts the message as follows:

$R^{-x} \times S = (25 - 61I_1 + 100I_2)(4 + 99I_1 + 17I_2) = 100 + 2475I_1 + 425I_2 - 244I_1 - 6039I_1 - 1037I_1 + 400I_2 + 9900I_1 + 1700I_2 = 100 + 5055I_1 + 2525I_2$.

$R^{-x} \times S(mod\ p) = 100(mod\ 7) + I_1[7680(mod\ 13) - 2625\ (mod\ 11)] + I_2[2625(mod\ 11) - 100(mod\ 7)] = 2 + I_1[10 - 7] + I_2[7 - 2] = 2 + 3I_1 + 5I_2$, which is the plain text.

Now, (B) computes the logical values as follows:

$\frac{2}{10} = 0.2, \frac{3}{10} = 0.3, \frac{5}{10} = 0.5$. This means that (B) has the following statement: the considered drug has contributed to the cure of 20% of cases and negatively affected 30% of cases, while the effect is still unknown for the remaining 50% of patients

Remark that if the message has been attacked, then the attacker will see $4 + 99I_1 + 17I_2$, which is meaningless with respect to the original data.

A Comparison between El-Gamal System and Refined Neutrosophic El-Gamal System (Complexity analysis):

The following table clarifies the experimental results of the duration of breaking each code by using Brute-Force, where it shows clearly that the refined neutrosophic El-Gamal system is stronger than the classical one and its complexity is around t^3, while t is the duration of the classical code.

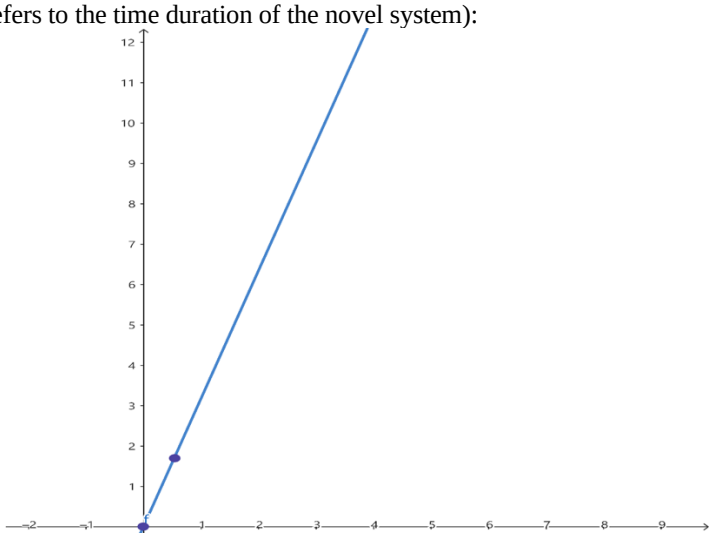
Table (1)

Time Duration measured by sec	El Gamal Crypto System	Refined Neutrosophic El Gamal

Doi: https://doi.org/10.54216/FPA.100203
Received: November 09, 2022 Accepted: March 19, 2023

		Crypto System
Around 0,002 for the classical system Around 0,006 For the novel system	For $g\ of\ size\ 7$	Same size
Around 0,002 for the classical system Around 0,007 For the novel system	For $g\ of\ size\ 8$	Same size
Around 0,55 for the classical system Around 1,7 for the novel system	For $g\ of\ size\ 9$	Same size
Around 4,2 for the classical system Around 13,1 for the novel system	For $g\ of\ size\ 10$	Same size

The previous table shows that the refined neutrosophic El-Gamal algorithm has a complexity of around$3t$, where t is the time needed to break the classical El-Gamal System.
A graph of the previous table can be illustrated as follows (The x-axis refers to the time duration of the classical system and the y-axis refers to the time duration of the novel system):



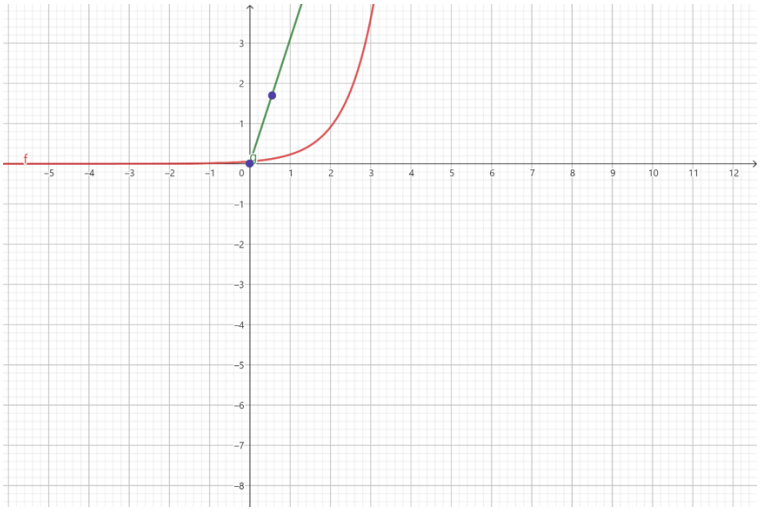
A Comparison between Refined Neutrosophic El-Gamal algorithm and RSA algorithm

The following table compares the duration of breaking RSA and refined neutrosophic Eh-Gamal algorithm by using brute force measured by seconds.

Time Duration measured by sec	**RSA Crypto System**	**Refined Neutrosophic El Gamal Crypto System**
Around 0,002 for the classical system Around 0,006 For the novel system	For $n\ of\ size\ 7$	Same size
Around 0,002 for the classical system Around 0,007 For the novel system	For $n\ of\ size\ 8$	Same size
Around 0,56 for the classical system Around 1,7 for the novel system	For $n\ of\ size\ 9$	Same size
Around 4,2 for the classical system Around 13,1 for the novel system	For $n\ of\ size\ 10$	Same size

We can illustrate the following graph to explain the previous comparison.

Doi: https://doi.org/10.54216/FPA.100203
Received: November 09, 2022 Accepted: March 19, 2023



Conclusion

In this paper, we have used refined neutrosophic number theory and the El Gamal algorithm to introduce a novel crypto-scheme for the encryption of rational uncertain data units represented by single-valued neutrosophic numbers. On the other hand, we have illustrated some examples to clarify the validity of the new algorithm and its applicability to real-life problems.

As a future research direction, we aim to find some additional applications of neutrosophic structures in cryptography, especially in generalizing the RSA algorithm.

References

[1] Adeleke, E.O, Agboola, A.A.A, and Smarandache, F. (2020). Refined Neutrosophic Rings I. International Journal of Neutrosophic Science. 2(2): 77-81,.

[2] Atanassov, K., (1986). Intuitionistic fuzzy sets. Fuzzy Sets and Systems. 20: 87-96.

[3] Bhowmik, M., and Pal, M. (2009). Intuitionistic neutrosophic set, Journal of Information and Computing Science 2(4): 142-152.

[4] Broumi, S., and Smarandache, F. (2014). On Neutrosophic Implications. Neutrosophic Sets and Systems. 2: 9-17.

[5] Disheng Zheng , Kai Liang, Chaotic Butterfly Optimization with Optimal Multi-key Image Encryption Technique for Wireless Sensor Networks, Journal of Intelligent Systems and Internet of Things, Vol. 1 , No. 2 , (2020) : 80-92

[6] Ibrahim, M. and Abobala, M. (2021). An Introduction To Refined Neutrosophic Number Theory. Neutrosophic Sets and Systems. (45).

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

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

[9] Smarandache, F., (2005). Neutrosophic set, a generalization of the intuitionistic fuzzy sets. International Journal of Pure and Applied Mathematics. (24): 287–297.

[10] Zadeh, L. A., (1965), Fuzzy sets. Inform. and Control. (8): 338-353.

[11] Merkepci, M., and 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.

Doi: https://doi.org/10.54216/FPA.100203
Received: November 09, 2022 Accepted: March 19, 2023