



Paper Type: Research Paper

## On Novel Security Systems Based on the 2-Cyclic Refined Integers and the Foundations of 2-Cyclic Refined Number Theory

Mohammad Abobala<sup>1\*</sup>, Hasan Sankari<sup>1</sup>, Mohamed Bisher Zeina<sup>2</sup>

<sup>1</sup> Tishreen University, Faculty of Science, Department of Mathematics, Syria; mohammadabobala777@gmail.com; hasansankari2@gmail.com.

<sup>2</sup> Department of Mathematical Statistics, Faculty of Science, University of Aleppo, Aleppo, Syria; bisher.zeina@gmail.com.

### Citation:

Received: 04 November 2023

Revised: 08 December 2023

Accepted: 21 January 2024

Abobala, M., Sankari, H., & Bisher Zeina, M. (2024). On novel security systems based on the 2-cyclic refined integers and the foundations of 2-cyclic refined number theory. *Journal of fuzzy extension and applications*, 5(1), 69-85.

### Abstract


Integers play a basic role in the structures of asymmetric crypto-algorithms. Many famous public key crypto-schemes use the basics of number theory to share keys and decrypt and encrypt messages and multimedia. As a novel trend in the world of cryptography, non-classical integer systems, such as neutrosophic or plithogenic integers, are used for encryption and decryption. The objective of this paper is to provide the basic foundations of 2-cyclic refined number theory and linear Diophantine equations in two variables by building suitable algebraic isomorphism between the 2-cyclic refined integer ring and a subring of the direct product of  $\mathbb{Z}$  with itself three times. Also, this work presents two novel crypto schemes for the encryption and decryption of data and information based on the algebraic properties of 2-cyclic refined integers, where improved versions of the El-Gamal crypto-scheme and RSA algorithm will be established through the view of the algebra and number theory of 2-cyclic refined integers. On the other hand, we illustrate some examples and tables to show the validity and complexity of the novel algorithms.

**Keywords:** 2-cyclic refined integers, RSA, EL-Gamal, Security system.

## 1 | Introduction

The concept of  $n$ -cyclic refined neutrosophic rings was proposed in [1] as a novel generalization of classic rings using logical generators and indices. The idea behind 2-cyclic refined rings is to use literal neutrosophic elements in building algebraic extensions of rings, as suggested for the first time in [2].

 Corresponding Author: mohammadabobala777@gmail.com

 <https://doi.org/10.22105/jfea.2024.423818.1321>



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

In [3]–[9], many special cases of  $n$ -cyclic refined neutrosophic algebraic structures were handled, such as 2-cyclic group of units, 2-cyclic Diophantine equations, and 2-cyclic refined neutrosophic matrices.

Theoretical mathematics is an important resource of cryptography, as the most famous cryptographic algorithms with their symmetric and asymmetric types follow generalized problems in traditional number theory and the theory of functions.

Concepts such as congruencies, Euler's function, and elliptic curves have been used in the construction and exchange of secret keys for the encryption and decryption process; perhaps the most prominent examples of this are asymmetric public-key encryption algorithms such as the RSA algorithm and the El-Gamal algorithm.

Proceeding from this point, it can be said that by generalizing and expanding the integers used in the encryption and decryption process, it is possible to build encryption systems that generalize classical systems and are characterized by a higher degree of complexity and greater difficulty for attackers to obtain secret keys.

So far, based on the latest published articles, three types of new numerical systems that expand integers in the construction of new encryption algorithms based on previously known algorithms have been used.

Neutrosophic integers, for example, are essentially an extended numerical system of partially ordered integers possessing many characteristic properties in two dimensions.

These numbers were used in the generalization of the RSA algorithm and El-Gamal algorithm and have given good results in terms of the resulting complexity in the difficulty of breaking and the flow ability of the approval calculations.

On the other hand, refined neutrosophic integers and symbolic 2-plithogenic integers are essentially extended numerical systems of partially ordered integers, possessing many characteristic properties in three dimensions.

The usage of non-classical integer systems in cryptography was proposed first in [10], and then many applications of neutrosophic of previous efforts to apply non-classical integer systems in cryptography. We can see generalized versions of RSA and El-Gamal algorithms were built by using neutrosophic integers, refined neutrosophic integers, and symbolic  $n$ -plithogenic numbers [11]–[15]; many other extensions and algorithms in cryptography were presented in [16], [17].

Through this paper, we depend on the algebraic properties of 2-cyclic refined integers and the foundational concepts in 2-cyclic refined number theory to present a novel generalized form of the El-Gamal crypto scheme and a novel generalization of the RSA algorithm, with many examples and tables that explain the complexity of the novel algorithm. On the other hand, we present valid and strong mathematical proofs for building the mathematical basis of 2-cyclic refined number theory and for solving 2-cyclic refined Diophantine equations in two variables.

## 2 | The Idea Behind Using Integers in Cryptography

Encryption using algebraic properties of integers is beneficial because it reduces the problem of breaking the code to an unsolvable problem in ordinary linear time.

For example, the RSA algorithm is based on answering the problem of code-breaking to the problem of finding a very large integer analysis of its prime factors.

The El-Gamal algorithm is based on answering the problem of breaking the cipher to the problem of calculating the natural logarithm mod  $n$ .

All of the above methods create a kind of bridge between complex problems in number theory and the disclosure of the secrecy of messages. Hence, discovering the Secret Key becomes a counter to solving a problem that is still impossible on the best computers nowadays.

We can easily say that when modern mathematics succeeds in solving these problems and finds effective and applicable algorithms for solving them, breaking encryption and discovering secret keys will become real achievements, which is still not possible today.

Non-classical extensions of integers for modern crypto-systems. So far, based on the latest published articles, three types of new numerical systems that expand integers in the construction of new encryption algorithms based on previously known algorithms have been used.

Initially, the use of such numbers was proposed in [9]. Neutrosophic integers, for example, are essentially an extended numerical system of partially ordered integers possessing many characteristic properties in two dimensions.

These numbers were used in the generalization of the RSA algorithm and El-Gamal algorithm and have given good results in terms of the resulting complexity in the difficulty of breaking and the flow ability of the approval calculations.

On the other hand, refined neutrosophic integers and symbolic 2-plithogenic integers are essentially extended numerical systems of partially ordered integers, possessing many characteristic properties in three dimensions.

These two novel sets provided good generalizations of classical RSA and El-Gamal Systems, and these generalizations are more complex than classical algorithms, which implies more security for sharing information and data through the internet and unsafe channels.



Fig. 1. Cryptography Process.

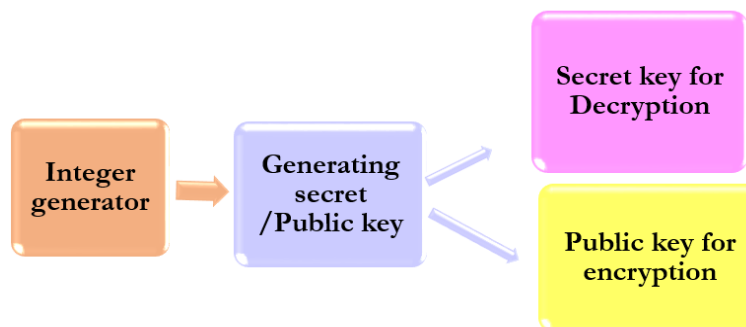


Fig. 2. Integers in constructing cryptography.

### 3 | The Mathematical Foundations of 2-Cyclic Refined Number Theory

**Definition 1.** The 2-cyclic refined integer is defined  $x + yI_1 + zI_2; x, y, z \in \mathbb{Z}$ . It is denoted by  $Z_2(I)$ .

Addition:

$$(x + yI_1 + zI_2) + (m + nI_1 + tI_2) = (x + m) + (y + n)I_1 + (z + t)I_2.$$

Multiplication:

$$(x + yI_1 + zI_2) \times (m + nI_1 + tI_2) = xm + (xn + ym + yt + zn)I_1 + (xt + yn + zm + zt)I_2.$$

**Theorem 1.** Let  $K = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$  be the direct product of three copies of  $\mathbb{Z}$ , then  $S = \{(a, b, c) \in K; b - c \in 2\mathbb{Z}\}$  is a subring of  $K$ .

Proof:  $S \neq \emptyset$ , that is because  $(0,0,0) \in S$ .

Let  $X = (a, b, c)$ ,  $Y = (m, n, t)$  be two arbitrary elements in  $S$ , then  $X + Y = (a + m, b + n, c + t)$ ,  $X.Y = (am, bn, ct)$ ,  $(b + n) - (c + t) = (b - c) + (n - t) \in 2\mathbb{Z}$ , thus  $X + Y \in S$ . On the other hand

$$\begin{cases} b - c = 2k_1, \\ n - t = 2k_2 \quad ; k_1, k_2 \in \mathbb{Z}. \end{cases}$$

Hence,  $bn - ct = (c + 2k_1)n - c(t + 2k_2) = 2(k_1n - ck_2) + c(n - t)$ , so that  $bn - ct \in 2\mathbb{Z}$ , and  $X.Y \in S$ . It is clear that  $-X = (-a, -b, -c) \in S$ , thus our proof is complete.

**Theorem 2.** Let  $Z_2(I)$  be the 2-cyclic refined ring, then  $Z_2(I) \cong S$ .

Proof: Define the mapping:  $f: Z_2(I) \rightarrow S$  such that

$$f(a + bI_1 + cI_2) = (a, a + b + c, a - b + c).$$

According to [18], the mapping  $f$  is a ring homomorphism.

Let  $X = a + bI_1 + cI_2 \in \ker(f)$ , then  $\begin{cases} a = 0 \\ b + c = 0 \\ -b + c = 0 \end{cases}$ . Thus,  $X=0$ , and  $(f)$  is injective.

Let  $Y = (a, b, c) \in S$ ;  $b - c \in 2\mathbb{Z}$ , there exists  $X = a + \frac{1}{2}(b - c)I_1 + (\frac{b+c}{2} - a)I_2 \in S$ , such that  $f(X) = Y$ , so that  $(f)$  is surjective, and then a ring isomorphism.

**Definition 2.** Let  $X = t_0 + t_1I_1 + t_2I_2, Y = s_0 + s_1I_1 + s_2I_2 \in Z_2(I)$ , then

I.  $X|Y$  if and only if  $f(X)|f(Y)$ , i.e.

$$\begin{cases} t_0|s_0, \\ t_0 + t_1 + t_2|s_0 + s_1 + s_2, \\ t_0 - t_1 + t_2|s_0 - s_1 + s_2. \end{cases}$$

II.  $\gcd(X, Y) = Z$  if and only if  $\gcd(f(X), f(Y)) = f(Z)$ , where  $Z = z_0 + z_1I_1 + z_2I_2 \in Z_2(I)$ , i.e.

$$\gcd(X, Y) = \gcd(t_0, s_0) + \frac{1}{2}I_1[\gcd(t_0 + t_1 + t_2, s_0 + s_1 + s_2) - \gcd(t_0 - t_1 + t_2, s_0 - s_1 + s_2)] + \frac{1}{2}I_2[\gcd(t_0 + t_1 + t_2, s_0 + s_1 + s_2) + \gcd(t_0 - t_1 + t_2, s_0 - s_1 + s_2) - 2\gcd(t_0, s_0)].$$

III.  $f(X) \equiv f(Y) \pmod{f(Z)}$  if and only if  $X \equiv Y \pmod{Z}$ , i.e.

$$\begin{cases} t_0 \equiv s_0 \pmod{z_0}, \\ t_0 + t_1 + t_2 \equiv s_0 + s_1 + s_2 \pmod{z_0 + z_1 + z_2}, \\ t_0 - t_1 + t_2 \equiv s_0 - s_1 + s_2 \pmod{z_0 - z_1 + z_2}. \end{cases}$$

IV.  $x^y = f^{-1}[f(x)]^{f(y)}$ , i.e.

$$x^y = t_0^{s_0} + \frac{1}{2}I_1[(t_0 + t_1 + t_2)^{s_0+s_1+s_2} - (t_0 - t_1 + t_2)^{s_0-s_1+s_2}] + \frac{1}{2}I_2[(t_0 + t_1 + t_2)^{s_0+s_1+s_2} + (t_0 - t_1 + t_2)^{s_0-s_1+s_2} - 2t_0^{s_0}].$$

Remark 1:

$$X \leq Y \Leftrightarrow \begin{cases} t_0 \leq s_0, \\ t_0 + t_1 + t_2 \leq s_0 + s_1 + s_2, \\ t_0 - t_1 + t_2 \leq s_0 - s_1 + s_2, \end{cases}$$

$(\leq)$  is a partial order relation clearly.

**Example 1.** Take  $X = 3 + I_1 + I_2, Y = 2 + 2I_1 + I_2, Z = 1 + I_1 + I_2$ , we have

$$\begin{cases} X > 0: (3 > 0, 5 > 0, 3 > 0), \\ Y > 0: (2 > 0, 5 > 0, 1 > 0), \\ Z > 0: (1 > 0, 3 > 0, 1 > 0). \end{cases}$$

Also

$$\begin{cases} 3 \equiv 2 \pmod{1}, \\ 5 \equiv 5 \pmod{3}, \\ 3 \equiv 1 \pmod{1}. \end{cases}$$

Hence,  $X \equiv Y \pmod{Z}$ .

Remark 2: If  $X \equiv Y \pmod{Z}$ , then  $Z|X - Y$ , and if  $\gcd(X, Y) = 1$ , then  $X$  and  $Y$  are called relatively prime.

**Example 2.** Let  $X = 10 + I_1 + 5I_2$ ,  $Y = 4 + 2I_1 + 3I_2$ , hence

$$\begin{cases} \gcd(4, 10) = 2, \\ \gcd(9, 16) = 1, \\ \gcd(14, 5) = 1. \end{cases}$$

Thus,  $\gcd(X, Y) = 2 + \frac{1}{2}I_1[1 - 1] + \frac{1}{2}I_2[1 + 1 - 2(2)] = 2 - I_2$ .

Remark 3: According to the partial order relation ( $\leq$ ) defined on  $Z_2(I)$ , we can see easily that  $\gcd(X, Y) > 0$  for every  $X, Y \in Z_2(I)$ .

**Definition 3.** Let  $0 < X = x_0 + x_1I_1 + x_2I_2 \in Z_2(I)$ , we define  $\varphi^*: Z_2(I) \rightarrow \mathbb{Z}$ , such that

$$\varphi^*(X) = |\{0 < Y = y_0 + y_1I_1 + y_2I_2 \leq X; \gcd(X, Y) = 1\}|.$$

**Theorem 3.** Let  $0 < X = x_0 + x_1I_1 + x_2I_2 \in Z_2(I)$ , then

$$\begin{aligned} \varphi^*(X) &= \begin{cases} \varphi(x_0) \times \varphi(x_0 + x_1 + x_2) \times \varphi(x_0 - x_1 + x_2); & x_0 + x_1 + x_2, x_0 - x_1 + x_2 \text{ are even,} \\ \frac{1}{2} \varphi(x_0) \times \varphi(x_0 + x_1 + x_2) \times \varphi(x_0 - x_1 + x_2); & x_0 + x_1 + x_2, x_0 - x_1 + x_2 \text{ are odd,} \end{cases} \end{aligned}$$

where  $\varphi$  is the classical phi-Euler's function.

Proof: Assume that  $x_0 + x_1 + x_2, x_0 - x_1 + x_2 \in 2\mathbb{Z}$ , hence if  $0 < Y = y_0 + y_1I_1 + y_2I_2 \leq X$  with  $\gcd(X, Y) = 1$ , we get

$$\begin{cases} y_0 - y_1 + y_2 \leq x_0 - x_1 + x_2 \\ y_0 + y_1 + y_2 \leq x_0 + x_1 + x_2 \end{cases} \text{ and } \begin{cases} \gcd(x_0 - x_1 + x_2, y_0 - y_1 + y_2) = 1 \\ \gcd(x_0 + x_1 + x_2, y_0 + y_1 + y_2) = 1 \end{cases}$$

According to the assumption,  $\begin{cases} x_0 + x_1 + x_2 \\ x_0 - x_1 + x_2 \end{cases}$  are even numbers; hence, all possible values of  $y_0 + y_1 + y_2, y_0 - y_1 + y_2$  are odd numbers, so that we have

$$\begin{cases} \varphi(x_0) \text{ different Value of } y_0, \\ \varphi(x_0 + x_1 + x_2) \text{ different Value of } y_0 + y_1 + y_2, \\ \varphi(x_0 - x_1 + x_2) \text{ different Value of } y_0 - y_1 + y_2. \end{cases}$$

Thus  $\varphi^*(X) = \varphi(x_0) \times \varphi(x_0 + x_1 + x_2) \times \varphi(x_0 - x_1 + x_2)$ .

Assume that  $\begin{cases} x_0 + x_1 + x_2 \\ x_0 - x_1 + x_2 \end{cases}$  are odd numbers, hence for  $0 < Y = y_0 + y_1I_1 + y_2I_2 \leq X$  with  $\gcd(X, Y) = 1$ , we have  $\frac{1}{2}\varphi(x_0 + x_1 + x_2)$  different odd values of  $y_0 + y_1 + y_2$ , and  $\frac{1}{2}\varphi(x_0 - x_1 + x_2)$  different even values of  $y_0 - y_1 + y_2$ .

Also, we have  $\frac{1}{2}\varphi(x_0 - x_1 + x_2)$  different even values of  $y_0 - y_1 + y_2$ , and  $\frac{1}{2}\varphi(x_0 + x_1 + x_2)$  different odd values of  $y_0 + y_1 + y_2$ , so that  $Y \in Z_2(I)$  if and only if  $\begin{cases} y_0 + y_1 + y_2 \\ y_0 - y_1 + y_2 \end{cases}$  are both odd or both even, hence

$$\begin{aligned} \varphi^*(X) &= \varphi(x_0) \times \left(\frac{1}{2}\varphi(x_0 + x_1 + x_2)\right) \times \left(\frac{1}{2}\varphi(x_0 - x_1 + x_2)\right) + \varphi(x_0) \times \left(\frac{1}{2}\varphi(x_0 - x_1 + x_2)\right) \\ &\quad \times \left(\frac{1}{2}\varphi(x_0 + x_1 + x_2)\right) = \frac{1}{2}\varphi(x_0) \times \varphi(x_0 + x_1 + x_2) \times \varphi(x_0 - x_1 + x_2). \end{aligned}$$

**Example 3.** Take:  $X = 4 + 5I_1 + 7I_2 \in Z_2(I)$ , then

$$\begin{cases} x_0 = 4, \\ x_0 + x_1 + x_2 = 16, \\ x_0 - x_1 + x_2 = 6. \end{cases}$$

So that  $\varphi^*(X) = \varphi(4) \times \varphi(16) \times \varphi(6) = 2 \times 8 \times 2 = 32$ . Take  $X = 4 + 3I_1 + 2I_2$ , then

$$\begin{cases} x_0 = 4, \\ x_0 + x_1 + x_2 = 9, \\ x_0 - x_1 + x_2 = 3. \end{cases}$$

So that  $\varphi^*(X) = \frac{1}{2} \varphi(4) \varphi(9) \varphi(3) = \frac{1}{2} (2)(6)(2) = 12$ .

**Theorem 4.** Let  $Y = y_0 + y_1I_1 + y_2I_2, X = x_0 + x_1I_1 + x_2I_2 \in Z_2(I)$ , such that  $X, Y > 0$ , and  $\gcd(X, Y) = 1$ , hence  $X^{\varphi^*(Y)} \equiv 1 \pmod{Y}$ .

Proof: According to the assumption,  $\gcd(X, Y) = 1$ , hence

$$\begin{cases} \gcd(x_0, y_0) = 1, \\ \gcd(x_0 + x_1 + x_2, y_0 + y_1 + y_2) = 1, \\ \gcd(x_0 - x_1 + x_2, y_0 - y_1 + y_2) = 1. \end{cases}$$

Case 1: If  $y_0 + y_1 + y_2, y_0 - y_1 + y_2$  are even numbers, then  $X^{\varphi^*(Y)} = L_0 + L_1I_1 + L_2I_2$ , where  $L_0 = x_0^\mu$ ;  $\mu = \varphi^*(Y) = \varphi(x_0)\varphi(x_0 + x_1 + x_2)\varphi(x_0 - x_1 + x_2)$ ,  $L_1 = \frac{1}{2} [(x_0 + x_1 + x_2)^\mu - (x_0 - x_1 + x_2)^\mu]$ ,  $L_2 = \frac{1}{2} [(x_0 + x_1 + x_2)^\mu + (x_0 - x_1 + x_2)^\mu - 2x_0^\mu]$ .

By classical Euler's theorem, we can write

$$\begin{cases} x_0^{\varphi(y_0)} \equiv 1 \pmod{y_0}, \\ (x_0 + x_1 + x_2)^{\varphi(y_0+y_1+y_2)} \equiv 1 \pmod{y_0 + y_1 + y_2}, \\ (x_0 - x_1 + x_2)^{\varphi(y_0-y_1+y_2)} \equiv 1 \pmod{y_0 - y_1 + y_2}. \end{cases}$$

Hence

$$\begin{cases} x_0^\mu \equiv 1 \pmod{y_0}, \\ (x_0 + x_1 + x_2)^\mu \equiv 1 \pmod{y_0 + y_1 + y_2}, \\ (x_0 - x_1 + x_2)^\mu \equiv 1 \pmod{y_0 - y_1 + y_2}. \end{cases}$$

Thus

$$\begin{cases} L_0 \equiv 1 \pmod{y_0}, \\ L_0 + L_1 + L_2 \equiv 1 \pmod{y_0 + y_1 + y_2}, \\ L_0 - L_1 + L_2 \equiv 1 \pmod{y_0 - y_1 + y_2}. \end{cases}$$

Hence  $X^{\varphi^*(Y)} \equiv 1 \pmod{y}$ .

Case 2: If  $y_0 + y_1 + y_2, y_0 - y_1 + y_2$  are odd numbers, then  $\mu = \varphi^*(Y) = \frac{1}{2} \varphi(y_0) \varphi(y_0 + y_1 + y_2) \varphi(y_0 - y_1 + y_2)$ , so that

$$\begin{aligned} L_0 &= x_0^\mu = [x_0^{\varphi(y_0)}]^{\frac{1}{2} \varphi(y_0+y_1+y_2) \varphi(y_0-y_1+y_2)} \equiv 1 \pmod{y_0}, \\ L_0 + L_1 + L_2 &= [(x_0 + x_1 + x_2)^{\varphi(y_0+y_1+y_2)}]^{\frac{1}{2} \varphi(y_0) \varphi(y_0-y_1+y_2)} \equiv 1 \pmod{y_0 + y_1 + y_2}, \\ L_0 - L_1 + L_2 &= [(x_0 - x_1 + x_2)^{\varphi(y_0-y_1+y_2)}]^{\frac{1}{2} \varphi(y_0) \varphi(y_0+y_1+y_2)} \equiv 1 \pmod{y_0 - y_1 + y_2}. \end{aligned}$$

Hence  $X^{\varphi^*(Y)} \equiv 1 \pmod{y}$ .

## 4 | Applications to Linear 2-Cyclic Refined Diophantine Equations in Two Variables

**Definition 4.** Let

$$(a_0 + a_1I_1 + a_2I_2)X + (b_0 + b_1I_1 + b_2I_2)Y = c_0 + c_1I_1 + c_2I_2. \quad (1)$$

Such that

$$\begin{cases} a_i, b_i, c_i, x_i, y_i \in \mathbb{Z}, \\ X = x_0 + x_1I_1 + x_2I_2, Y = y_0 + y_1I_1 + y_2I_2. \end{cases}$$

Then, it is called a linear 2-cyclic refined Diophantine equation in two Variables X,Y.

Remark 4: The Eq. (1) is equivalent to the following system of linear Diophantine equations:

$$a_0x_0 + b_0y_0 = c_0. \quad (2)$$

$$(a_0 + a_1 + a_2)(x_0 + x_1 + x_2) + (b_0 + b_1 + b_2)(y_0 + y_1 + y_2) = c_0 + c_1 + c_2. \quad (3)$$

$$(a_0 - a_1 + a_2)(x_0 - x_1 + x_2) + (b_0 - b_1 + b_2)(y_0 - y_1 + y_2) = c_0 - c_1 + c_2. \quad (4)$$

It holds directly by taking the direct image of Eq. (1) by the isomorphism f.

If any Eqs. (2)-(4) is not solvable, then Eq. (1) is not solvable, and this is equivalent to

$\gcd(a_0, b_0)$  does not divide  $c_0$ ,

or

$\gcd(a_0 + a_1 + a_2, b_0 + b_1 + b_2)$  does not divide  $c_0 + c_1 + c_2$ ,

or

$\gcd(a_0 - a_1 + a_2, b_0 - b_1 + b_2)$  does not divide  $c_0 - c_1 + c_2$ .

So, we must suppose that Eqs. (2)-(4) are solvable.

Assume that  $\begin{cases} (x_0, y_0) \text{ is a solution to Eq. (1)} \\ (x'_1, y'_1) \text{ is a solution to Eq. (2)} \\ (x'_2, y'_2) \text{ is a solution to Eq. (3)} \end{cases}$ . Hence  $\begin{cases} x'_1 = x_0 + x_1 + x_2 \\ y'_1 = y_0 + y_1 + y_2 \end{cases}$  and  $\begin{cases} x'_2 = x_0 - x_1 + x_2 \\ y'_2 = y_0 - y_1 + y_2 \end{cases}$ .

So that  $(x_0, x'_1, x'_2), (y_0, y'_1, y'_2)$  is a solution to the system  $f(*)$  in ring S if and only if

$$\begin{cases} x'_1, x'_2 \text{ are both even numbers or odd numbers,} \\ y'_1, y'_2 \text{ are both even numbers or odd numbers.} \end{cases}$$

In these cases, the solutions of Eq. (1) are exactly the inverse image of the solutions  $(y_0, y'_1, y'_2), (x_0, x'_1, x'_2)$  as follows:

$$X = x_0 + \frac{1}{2}I_1[x'_1 - x'_2] + \frac{1}{2}I_2[x'_1 + x'_2 - 2x_0].$$

$$Y = y_0 + \frac{1}{2}I_1[y'_1 - y'_2] + \frac{1}{2}I_2[y'_1 + y'_2 - 2y_0].$$

**Example 4.** Consider the following 2-cyclic refined Diophantine equation:

$$(2 + I_1 + 2I_2)X + (1 + I_1 + I_2)Y = 3 + 2I_2.$$

The equivalent system is

$$2x_0 + y_0 = 3. \quad (5)$$

$$5(x_0 + x_1 + x_2) + 3(y_0 + y_1 + y_2) = 5. \quad (6)$$

$$3(x_0 - x_1 + x_2) + (y_0 - y_1 + y_2) = 5. \quad (7)$$

$\gcd(3,1) = 1|5$ ,  $\gcd(5,3) = 1|5$ ,  $\gcd(2,1) = 1|3$ , hence Eqs. (5)-(7) are solvable in  $\mathbb{Z}$ .

The solutions of Eq. (5) are  $\begin{cases} x_0 = 1 + k_0 \\ y_0 = 1 - 2k_0 \end{cases}; k_0 \in \mathbb{Z}$ .

The solutions of Eq. (6) are:  $\begin{cases} x'_1 = 1 + 3k_1 \\ y'_1 = -5k_1 \end{cases}; k_1 \in \mathbb{Z}$ .

The solutions of Eq. (7) are:  $\begin{cases} x'_2 = 1 + k_2 \\ y'_2 = 2 - 3k_2 \end{cases}; k_2 \in \mathbb{Z}$ .

$x_1', x_2'$  are both even numbers if and only if  $k_1, k_2$  are odd.

$x_1', x_2'$  are both odd numbers if and only if  $k_1, k_2$  are even.

$y_1', y_2'$  are both even numbers if and only if  $k_1, k_2$  are even.

$y_1', y_2'$  are both odd numbers if and only if  $k_1, k_2$  are odd.

We discuss the possible Cases.

Case 3: If  $k_1, k_2$  are both odd numbers, then  $x_1', x_2'$  are even, and  $y_1', y_2'$  are odd. Hence

$$X = (1 + k_0) + \frac{1}{2}I_1(3k_1 - k_2) + \frac{1}{2}I_2(3k_1 + k_2 - 2k_0).$$

$$Y = (1 - 2k_0) + \frac{1}{2}I_1(-5k_1 + 3k_2 - 2) + \frac{1}{2}I_2(-5k_1 - 3k_2 + 4k_0).$$

Case 4: If ( $k_1$  is odd and  $k_2$  is even) or ( $k_1$  is even and  $k_2$  is odd), then  $(x_1', x_2')$  or  $(y_1', y_2')$  are not both odd or even numbers; hence, they will not generate any solution to the original equation.

Case 5: If  $k_1, k_2$  are both even, then  $(x_1', x_2')$  are both odd and  $(y_1', y_2')$  are both even, then

$$X = (1 + k_0) + \frac{1}{2}I_1(3k_1 - k_2) + \frac{1}{2}I_2(3k_1 + k_2 - 2k_0),$$

$$Y = (1 - 2k_0) + \frac{1}{2}I_1(-5k_1 + 3k_2 - 2) + \frac{1}{2}I_2(-5k_1 - 3k_2 + 4k_0),$$

is a solution of the original equation.

For example, take  $k_0 = 1, k_1 = 3, k_2 = 1$ , hence  $X = 2 + 4I_1 + 4I_2, Y = -1 - 7I_1 - 7I_2$ .

## 5 | The Description of the Novel Generalized El-Gamal Algorithm

Since 2-cyclic refined integers have three parts, we can use them to decrypt and encrypt data with three components, such as dimensional points or neutrosophic data units.

Consider that we have two sides (F) and (E). The first side decides to send a letter formed as a 2-cyclic refined integer as a cipher text to the second side (E). The recipient (E) picks a large 2-cyclic refined integer  $P = p_0 + p_1I_1 + p_2I_2$  with  $p_0, p_0 + p_1 + p_2, p_0 - p_1 + p_2$  are primes. Also, (E) picks a generator  $g = g_0 + g_1I_1 + g_2I_2$  such that

$$\begin{cases} 1 < g_0 < p_0 - 1, \\ 1 < g_0 + g_1 + g_2 < p_0 + p_1 + p_2 - 1, \\ 1 < g_0 - g_1 + g_2 < p_0 - p_1 + p_2 - 1. \end{cases}$$

Then (E) picks  $x = x_0 + x_1I_1 + x_2I_2$  such that

$$\begin{cases} 0 < x_0 < p_0 - 2, \\ 0 < x_0 + x_1 + x_2 < p_0 + p_1 + p_2 - 2, \\ 1 < x_0 - x_1 + x_2 < p_0 - p_1 + p_2 - 2. \end{cases}$$

(E) computes

$$X \equiv g^x \pmod{P} = g_0^{x_0} \pmod{p_0} + \frac{1}{2}I_1[(g_0 + g_1 + g_2)^{x_0+x_1+x_2} \pmod{(p_0 + p_1 + p_2)} - (g_0 - g_1 + g_2)^{x_0-x_1+x_2} \pmod{(p_0 - p_1 + p_2)}] + \frac{1}{2}I_2[(g_0 + g_1 + g_2)^{x_0+x_1+x_2} \pmod{(p_0 + p_1 + p_2)} - (g_0 - g_1 + g_2)^{x_0-x_1+x_2} \pmod{(p_0 - p_1 + p_2)}] - 2g_0^{x_0} \pmod{p_0}.$$

The 2-cyclic refined integer (x) is kept as the secret key.

Assume that (F) wants to send  $m = m_0 + m_1I_1 + m_2I_2$  as a message to (E). For this goal, (F) picks  $r = r_0 + r_1I_1 + r_2I_2$  such that such that



$$\begin{cases} 0 < r_0 < p_0 - 2, \\ 0 < r_0 + r_1 + r_2 < p_0 + p_1 + p_2 - 2, \\ 1 < r_0 - r_1 + r_2 < p_0 - p_1 + p_2 - 2. \end{cases}$$

Then, (F) computes

$$R \equiv g^r \pmod{P} = g_0^{r_0} \pmod{p_0} + \frac{1}{2} I_1 [(g_0 + g_1 + g_2)^{r_0+r_1+r_2} \pmod{(p_0 + p_1 + p_2)} - (g_0 - g_1 + g_2)^{r_0-r_1+r_2} \pmod{(p_0 - p_1 + p_2)}] + \frac{1}{2} I_2 [(g_0 + g_1 + g_2)^{r_0+r_1+r_2} \pmod{(p_0 + p_1 + p_2)} - (g_0 - g_1 + g_2)^{r_0-r_1+r_2} \pmod{(p_0 - p_1 + p_2)}] - 2g_0^{r_0} \pmod{p_0}.$$

The shared key  $k$  is computed as follows  $k \equiv X^r \pmod{P}$ .

(F) encrypts the message as  $S \equiv m \times k$ , and sends the ciphertext to (E) as a duplet  $(R, S)$ .

(E) decrypts the message as follows  $m \equiv R^{-x} \times S$ , where

$$R^{-1} \pmod{P} = r_0^{-1} \pmod{p_0} + \frac{1}{2} I_1 [(r_0 + r_1 + r_2)^{-1} \pmod{(p_0 + p_1 + p_2)} - (r_0 - r_1 + r_2)^{-1} \pmod{(p_0 - p_1 + p_2)}] + \frac{1}{2} I_2 [(r_0 + r_1 + r_2)^{-1} \pmod{(p_0 + p_1 + p_2)} - (r_0 - r_1 + r_2)^{-1} \pmod{(p_0 - p_1 + p_2)}] - 2r_0^{-1} \pmod{p_0}.$$

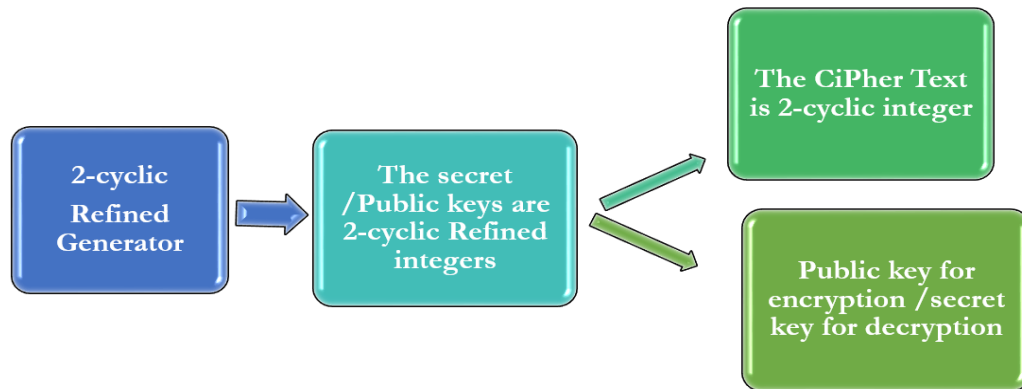


Fig. 3. The process 2-cyclic refined generator.

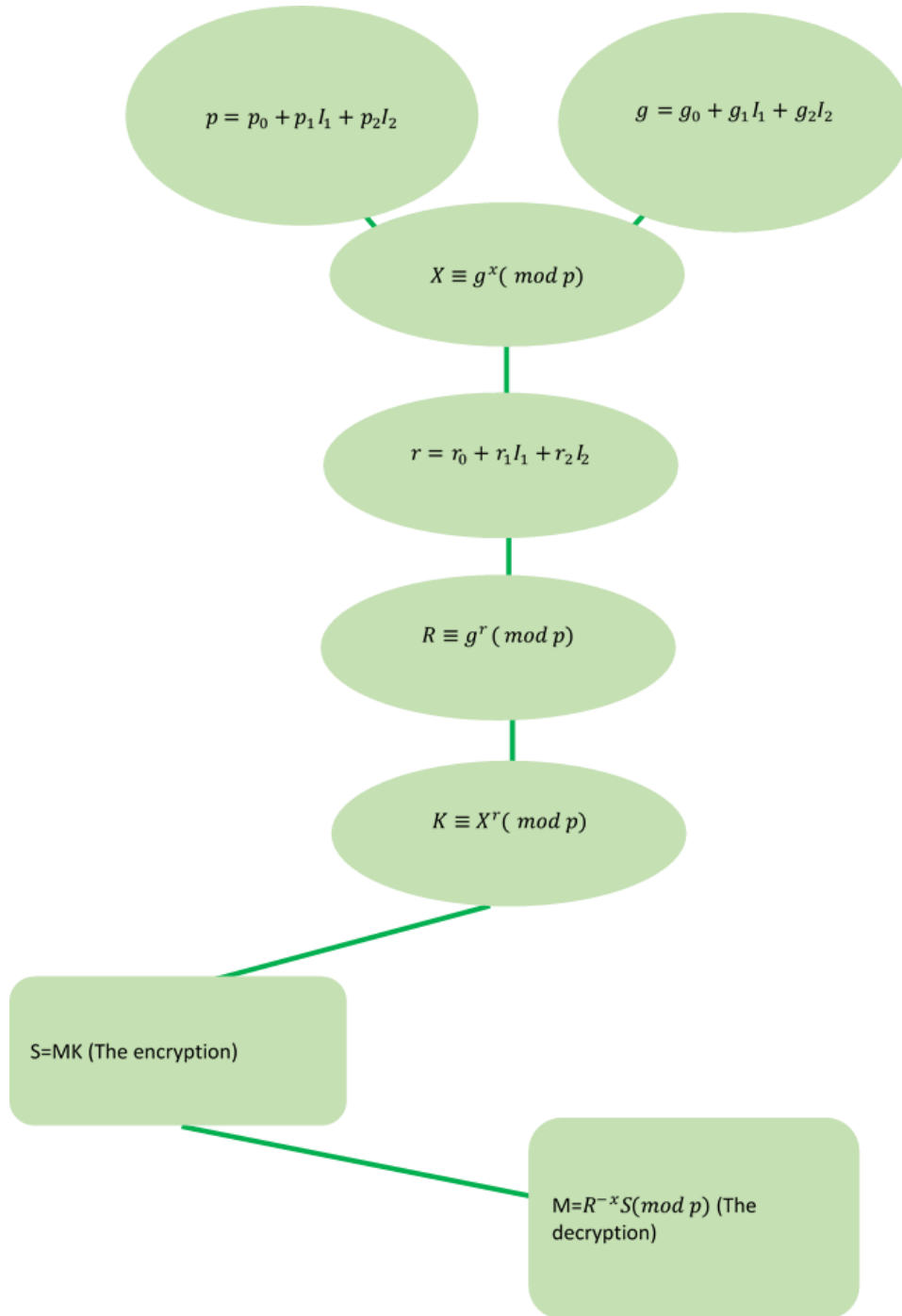


Fig. 4. The novel generalized El-Gamal algorithm.

**Example 5.** Consider that the second side picked  $P = 5 - 2I_1 + 4I_2$ , where  $5, 5 - 2 + 4 = 7, 5 - (-2) + 4 = 11$  are primes. The generator  $g = 3 + 2I_1 + I_2$ , where

$$\begin{cases} 0 < 3 < 5 - 1 = 4, \\ 0 < 3 + 1 + 1 = 5 < 7 - 1 = 6, \\ 1 < 3 - 1 + 1 = 3 < 11 - 1 = 10. \end{cases}$$

Now, the second side picks  $x = 2 + I_1 + I_2$ , where

$$\begin{cases} 0 < 2 < 5 - 2 = 3, \\ 0 < 2 + 1 + 1 = 4 < 7 - 2 = 5, \\ 1 < 2 - 1 + 1 = 2 < 11 - 2 = 9. \end{cases}$$

And computes

$$X \equiv g^x(\text{mod } P) = 3^2(\text{mod } 5) + \frac{1}{2}I_1[5^4(\text{mod } 7) - 3^2(\text{mod } 11)] + \frac{1}{2}I_2[5^4(\text{mod } 7) - 3^2(\text{mod } 11) - 2 \times 3^2(\text{mod } 5)].$$

$$X \equiv 4 + I_1 \left[ \frac{1}{2} \times 5^4(\text{mod } 7) - \frac{1}{2} \times 3^2(\text{mod } 11) \right] + I_2 \left[ \frac{1}{2} \times 5^4(\text{mod } 7) - \frac{1}{2} \times 3^2(\text{mod } 11) - 3^2(\text{mod } 5) \right] = 4 - 9I_1 + 2I_2.$$

Remark that we chose  $3^2(\text{mod } 11) \equiv 20(\text{mod } 11)$  to get an even integer so that we can divide it by 2.

Suppose that the first side decides to send  $m = 3 - I_1 + I_2$  to the second one.

The first side picks  $r = 1 + 2I_1 + I_2$ , where

$$\begin{cases} 0 < 1 < 5 - 2 = 3, \\ 0 < 1 + 1 + 1 = 3 < 7 - 2 = 5, \\ 1 < 1 - 1 + 1 = 1 < 11 - 2 = 9. \end{cases}$$

He computes

$$R \equiv g^r(\text{mod } P) = 3^1(\text{mod } 5) + \frac{1}{2}I_1[5^3(\text{mod } 7) - 3^1(\text{mod } 11)] + \frac{1}{2}I_2[5^3(\text{mod } 7) - 3^1(\text{mod } 11) - 2 \times 3^1(\text{mod } 5)] = 3 + I_1 \left[ \frac{1}{2} \times (6) - \frac{1}{2} \times (14) \right] + I_2 \left[ \frac{1}{2} \times (6) - \frac{1}{2} \times (14) - 3 \right] = 3 - 4I_1 + 7I_2.$$

The shared key (K) is

$$K = X^r(\text{mod } P) = (4 - 9I_1 + 7I_2)^{1+I_1+I_2} = 4^1(\text{mod } 5) + \frac{1}{2}I_1[2^3(\text{mod } 7) - 20^1(\text{mod } 11)] + \frac{1}{2}I_2[2^3(\text{mod } 7) + 20(\text{mod } 11) - 2 \times 4^1(\text{mod } 5)] = 4 + I_1[4 - 10] + I_2[4 + 10 - 4] = 4 - 6I_1 + 10I_2.$$

The encrypted message is

$$S = m \times k = (3 - I_1 + I_2)(4 - 6I_1 + 10I_2) = 12 + I_1[-18 - 4 - 10 - 6] + I_2[4 + 30 + 6 + 10] = 12 - 38I_1 + 50I_2.$$

$$R^{-1} = 3^{-1}(\text{mod } 5) + \frac{1}{2}I_1[6^{-1}(\text{mod } 7) - 14^{-1}(\text{mod } 11)] + \frac{1}{2}I_2[6^{-1}(\text{mod } 7) + 14^{-1}(\text{mod } 11) - 2 \times 3^{-1}(\text{mod } 5)] = 2 + I_1 + 3I_2.$$

$$R^{-x} = (R^{-1})^x = (2 + I_1 + 3I_2)^{2+I_1+I_2} = 4 + \frac{1}{2}I_1[6^4 - 4^2] + \frac{1}{2}I_2[6^4 - 4^2 - 8] = 4 + 640I_1 + 652I_2.$$

The second side decrypts the message

$$m = R^{-x} \times S = (4 + 640I_1 + 652I_2) \times (12 - 38I_1 + 50I_2) = 1248 + 14752I_1 + 16304I_2.$$

$$R^{-x} \times S(\text{mod } P) = 48(\text{mod } 5) + \frac{1}{2}I_1[31104(\text{mod } 7) - 1600(\text{mod } 11)] + \frac{1}{2}I_2[31104(\text{mod } 7) + 1600(\text{mod } 11) - 2 \times 48(\text{mod } 5)] = 3 + \frac{1}{2}I_1(3 - 5) + \frac{1}{2}I_2(3 + 5 - 6) = 4 - I_1 + I_2.$$

which is the plain text.

## 6 | The Description of the 2-Cyclic Refined RSA Algorithm

Suppose that we have two sides: a sender (F) and a recipient (E). Suppose that  $M = m_0 + m_1I_1 + m_2I_2$  is the message that (F) decided to send it to (E). (E) picks two positive 2-cyclic refined integers  $P = p_0 + p_1I_1 + p_2I_2$ ,  $Q = q_0 + q_1I_1 + q_2I_2$ , with  $p_0, q_0, p_0 + p_1 + p_2, q_0 + q_1 + q_2, p_0 - p_1 + p_2, q_0 - q_1 + q_2$  are large odd primes and then computes

$$N = PQ = p_0q_0 + I_1(p_0q_1 + p_1q_0 + p_1q_2 + p_2q_1) + I_1(p_0q_2 + p_2q_0 + p_2q_2 + p_2q_1) = n_0 + n_1I_1 + n_2I_2.$$

$$\emptyset^*(N) = \emptyset^*(P) \cdot \emptyset^*(Q) = \emptyset(p_0) * \emptyset(p_0 + p_1 + p_2) * \emptyset(p_0 - p_1 + p_2)\emptyset(q_0) * \emptyset(q_0 + q_1 + q_2) * \emptyset(q_0 - q_1 + q_2) = (p_0 - 1)(p_0 + p_1 + p_2 - 1)(p_0 - p_1 + p_2 - 1)(q_0 - 1)(q_0 + q_1 + q_2 - 1)(q_0 - q_1 + q_2 - 1).$$

Then (E) picks  $E = e_0 + e_1I_1 + e_2I_2$  with

$$\begin{cases} 1 < e_0 < \emptyset^*(N), \gcd(e_0, \emptyset^*(N)) = 1, \\ 1 < e_0 + e_1 + e_2 < \emptyset^*(N), \gcd(e_0 + e_1 + e_2, \emptyset^*(N)) = 1, \\ 1 < e_0 - e_1 + e_2 < \emptyset^*(N), \gcd(e_0 - e_1 + e_2, \emptyset^*(N)) = 1. \end{cases}$$

The public key is  $(E, N)$ . Now, (F) encrypts the message  $M$  as follows:

$$C \equiv M^E \pmod{N} = m_0^{e_0} \pmod{n_0} + \frac{1}{2}I_1[(m_0 + m_1 + m_2)^{e_0+e_1+e_2} \pmod{n_0 + n_1 + n_2} - (m_0 - m_1 + m_2)^{e_0-e_1+e_2} \pmod{n_0 - n_1 + n_2}] + \frac{1}{2}I_1[(m_0 + m_1 + m_2)^{e_0+e_1+e_2} \pmod{n_0 + n_1 + n_2} + (m_0 - m_1 + m_2)^{e_0-e_1+e_2} \pmod{n_0 - n_1 + n_2} - 2m_0^{e_0} \pmod{n_0}].$$

The secret key is

$$E^{-1} = e_0^{-1} \pmod{\emptyset^*(N)} + \frac{1}{2}I_1[(e_0 + e_1 + e_2)^{-1} \pmod{\emptyset^*(N)} - (e_0 - e_1 + e_2)^{-1} \pmod{\emptyset^*(N)}] + \frac{1}{2}I_1[(e_0 + e_1 + e_2)^{-1} \pmod{\emptyset^*(N)} - (e_0 - e_1 + e_2)^{-1} \pmod{\emptyset^*(N)} - e_0^{-1} \pmod{\emptyset^*(N)}].$$

The recipient (E) decrypts the message by  $M \equiv C^{E^{-1}} \pmod{N}$ .

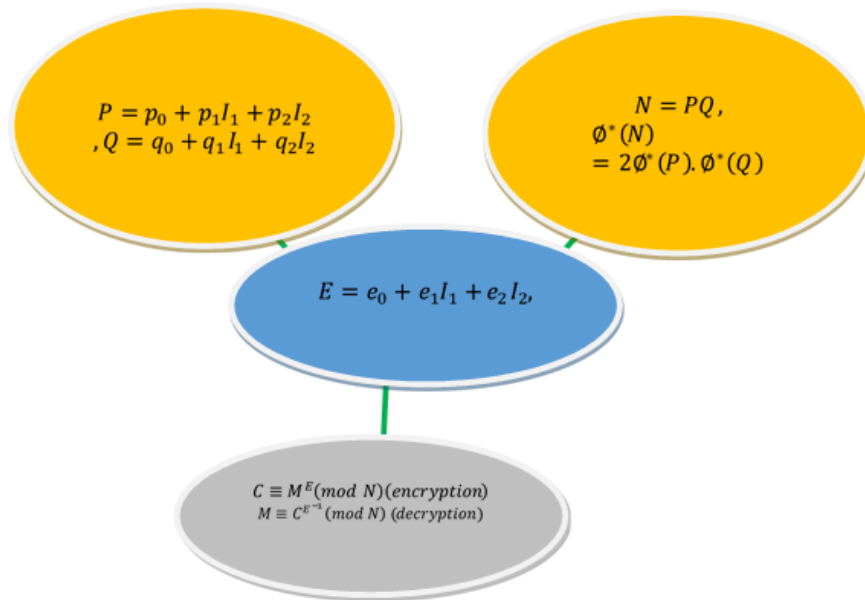


Fig. 5. The 2-cyclic refined RSA Algorithm.

**Example 6.** Suppose that (F) decides to send  $M = 3 + 4I_1 + 2I_2$  to (E).

(E) picks  $P = 13 + 2I_1 + 8I_2, Q = 7 + 4I_1, PQ = 91 + 52I_1 + 14I_1 + 18I_2 + 56I_2 + 32I_1 = 91 + 98I_1 + 64I_2. \emptyset^*(N) = \emptyset(13) \times \emptyset(23) \times \emptyset(19) \times \emptyset(7) \times \emptyset(11) \times \emptyset(3) = 12 \times 22 \times 18 \times 6 \times 10 \times 2 = 2. (285120).$

(E) picks  $E = 7 + 3I_1 + 3I_2$  it is clear that

$$\begin{cases} 0 < 7 < 285120, \gcd(7, 285120) = 1, \\ 0 < 7 + 3 + 3 = 13 < 285120, \gcd(13, 285120) = 1, \\ 0 < 7 - 3 + 3 = 7 < 285120, \gcd(7, 285120) = 1. \end{cases}$$

The public key is  $(7 + 3I_1 + 3I_2, 91 + 98I_1 + 64I_2)$ .

The encrypted message is

$$M \equiv C^{E^{-1}}(\text{mod } N) = 3^7(\text{mod } 91) + \frac{1}{2}I_1[9^{13}(\text{mod } 253) - 1^7(\text{mod } 57)] + \frac{1}{2}I_1[9^{13}(\text{mod } 253) + 1^7(\text{mod } 57) - 2 \times 3^7(\text{mod } 91)] = 3 + \frac{1}{2}I_1[269 - 1] + \frac{1}{2}I_1[269 + 1 - 6] = 3 + 134I_1 + 132I_2.$$

The second side (E) decrypts the message as follows:

$$e_0^{-1}(\text{mod } \emptyset^*(N)) = 7^{-1}(\text{mod } 285120) = 81463.$$

$$(e_0 + e_1 + e_2)^{-1}(\text{mod } \emptyset^*(N)) = 13^{-1}(\text{mod } 285120) = 65797.$$

$$(e_0 - e_1 + e_2)^{-1}(\text{mod } \emptyset^*(N)) = 7^{-1}(\text{mod } 285120) = 81463.$$

The plain text is

$$M \equiv C^{E^{-1}}(\text{mod } N) = 3^{81463}(\text{mod } 91) + \frac{1}{2}I_1[16^{228725}(\text{mod } 253) - 1^{97129}(\text{mod } 57)] + \frac{1}{2}I_1[16^{228725}(\text{mod } 253) + 1^{97129}(\text{mod } 57) - 2 \times 3^{81463}(\text{mod } 91)] = 3 + \frac{1}{2}I_1[9 - 1] + \frac{1}{2}I_1[9 + 1 - 6] = 3 + 4I_1 + 2I_2.$$

### Why 2-cyclic refined integers?

This numerical system is a powerful expansion of integers built on solid algebraic and logical rules.

These numbers have three dimensions, as they have a base of three independent generators, in addition to many algebraic properties that distinguish them from refined neutrosophic integers or symbolic 2-plithogenic integers.

For example, the ring of 2-cyclic refined integers is not isomorphic to the direct product of  $Z$  with itself; it has zero divisors and exactly 8 units.

In addition, congruencies are defined on them, with a partial order relation and the ability to compute natural powers and exponents.

2-cyclic refined integers are very useful in encrypting data in three dimensions, such as matrices with dimension 3, or data units with three pieces of information, such as neutrosophic data units or fuzzy relations and graphs.

These numbers are technically better because if we want to encrypt information consisting of three parts or three partial information, we need to apply the classical algorithm three times with three different keys to ensure security and not discover the secret key.

If the partial information is the same or all or some of it is the same, this will make it very easy for an attacker to discover the secret key and then steal information that is supposed to remain secret, in case it is of military, medical, or even logistical nature.

Whereas by using 2-cyclic refined numbers, it is enough to use only one secret key to encrypt the three parts together, and the difficulty of finding this secret key exceeds the difficulty of finding the three classic keys together.

The following table compares classical El-Gamal cryptosystems and a 2-cyclic refined system through the time needed to break the code, measured in milliseconds.

We can see from this table that the duration of the novel system is around three times compared to the classical system, and that can be explained algebraically by the existence of the isomorphism between a 2-cyclic refined integer ring and a subring of the three times direct product of  $Z$  with itself.

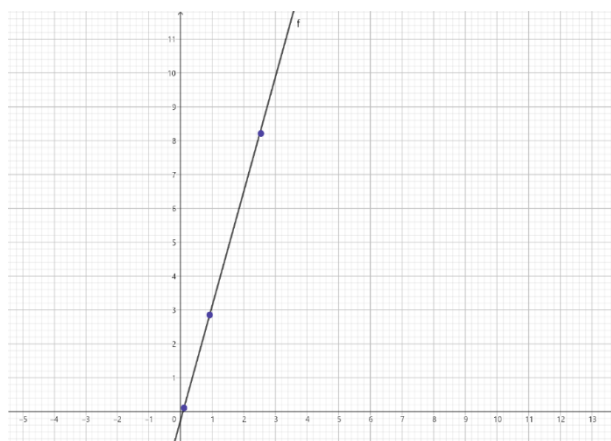
**Table 1. Comparing classical El-Gamal cryptosystems and the 2-cyclic refined system (El Gamal Crypto System).**

Time Duration Measured by M.Sec	El Gamal Crypto System	2-Cyclic Refined System
Around 1,0031 for a classical system	For	For
Around 1,07723787251	$500000 < g < 1000000$	$500000 < g_0, g_0 + g_1, g_0 - g_1 + g_2 < 1000000$
For the novel system		
Around 9,12001 for the classical system	For	For
Around 28,5433223 for the novel system	$5000000 < g < 10000000$	$5000000 < g_0, g_0 + g_1, g_0 - g_1 + g_2 < 10000000$
Around 25,3241 for the classical system	For	For
Around 82,1233678 for the novel system	$10000000 < g < 30000000$	$1000000 < g_0, g_0 + g_1, g_0 - g_1 + g_2 < 30000000$
Around 223,1348 for the classical system	For	For
Around 712.21445675 for the novel system	$100000000 < g < 300000000$	$10000000 < g_0, g_0 + g_1, g_0 - g_1 + g_2 < 300000000$

**Table 2. Comparing classical El-Gamal cryptosystems and the 2-cyclic refined system (2-Plithogenic El Gamal Crypto System).**

Time Duration Measured by M.Sec	2-Plithogenic El Gamal Crypto System	2-Cyclic Refined System
Around 1,04358787251 for 2-plithogenic	For	For
Around 1,07723787251 for the novel system	$500000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 1000000$	$500000 < g_0, g_0 + g_1, g_0 - g_1 + g_2 < 1000000$
Around 27,533023 for 2-plithogenic	For	For
Around 28,5433223 for the novel system	$5000000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 10000000$	$5000000 < g_0, g_0 + g_1, g_0 - g_1 + g_2 < 10000000$
Around 80,5906 for 2-plithogenic	For	For
Around 82,1233678 for the novel system	$1000000 < g_0, g_0 + g_1, g_0 + g_1 + g_2 < 30000000$	$1000000 < g_0, g_0 + g_1, g_0 - g_1 + g_2 < 30000000$

We can illustrate the following graph that explains the previous relationship between the complexity of the classical algorithm concerning the novel one.



**Fig. 6. Comparing the complexity of the classical and the novel algorithm.**

**Why should we use new algorithms?**

In cryptography, it is important to maintain confidentiality and security, whether it is digital data, text, or even information of a military or medical nature.

Therefore, we must use high-efficiency and high-complexity encryption systems, as increased secrecy is closely related to the increased complexity of the algorithm and the difficulty of attacking it.

Since the number system used in our new algorithm is three-dimensional, or in other words, described by three different components, this gives the process of exchanging keys or confidential data more security and reliability than using classical one-dimensional methods.

An attacker may be able to detect one of the components used. Still, it will be very far from detecting the remaining two components that enter into the formation of the algebraic key structure.

The main difficulties facing these new algorithms are the following points:

- I. Until now, computers do not recognize these numerical systems because they are new, which presents a challenge for programmers to introduce them into programming languages, making it easier for a computer to deal with them.
- II. Also, using these expanded numbers may result in greater consumption of computer resources, which significantly affects the ability of the computer to deal with them within a useful and logical time.

These theses remain as challenges to the possible development of the theory of cryptography and its various applications in this time when the movement of interest in cyber-security and its applications is accelerating.

The following figure shows a comparison between using integers and 2-cyclic refined integers in cryptography.

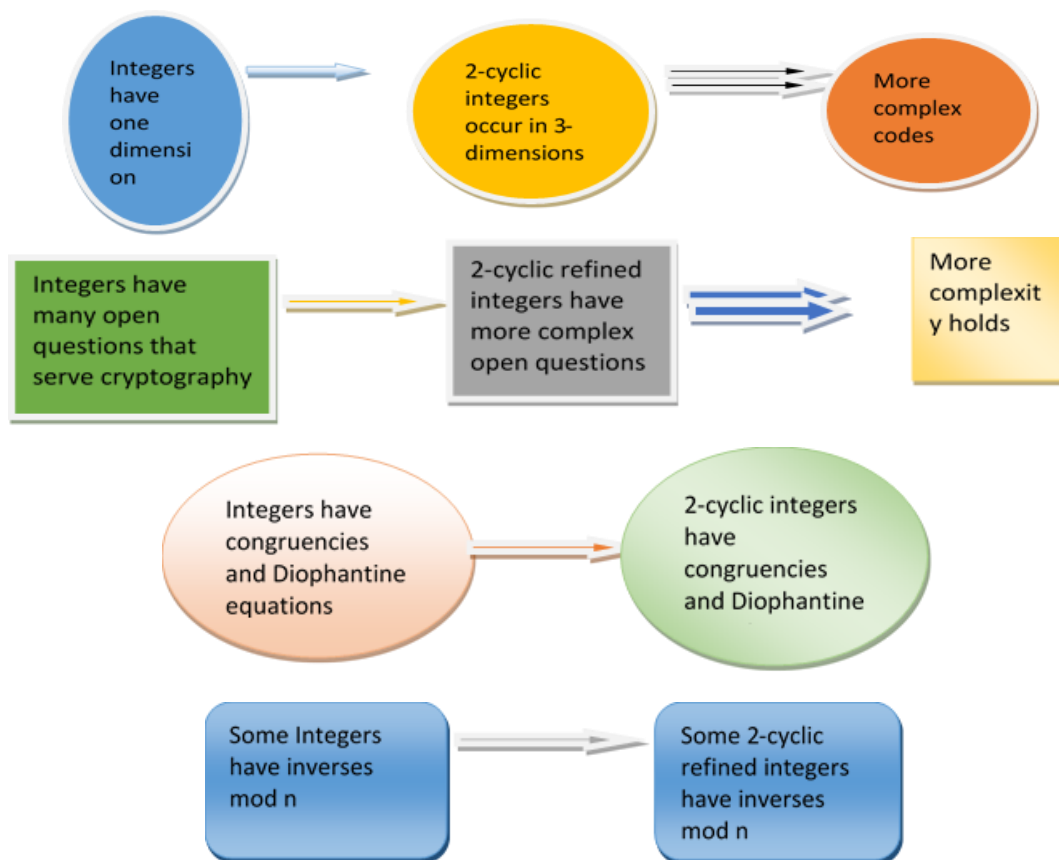


Fig. 7. Comparing integers and 2-cyclic refined integers in cryptography.

## 7 | Conclusion

This paper presents two novel algorithms for the encryption and decryption of data and information based on the El-Gamal algorithm, the RSA algorithm, and the algebra of 2-cyclic refined integers. In addition, we have discussed the possible future applications of the novel algorithms with many examples to clarify their

validity. Also, many figures and tables were provided to explain the new algorithms concerning the classical ones.

We recommend researchers continue our efforts and use the 3-cyclic refined integers to find novel generalizations of classical, well-known crypto-algorithms and study their properties and complexity.

## Author Contributions

Mohammad Abobala has suggested the main crypto-algorithms with the examples they presented. Hasan Sankari has provided mathematical proofs for the foundations of 2-cyclic refined number theory and Diophantine equations. Mohammad Bisher Ziena has analyzed the efficiency of the suggested algorithms, drawn figures, and written the text with language revision.

## Funding

This section indicates any support not included in the Author Contribution or Funding sections.

## Data Availability

All data generated during the study are included in the text.

## Conflicts of Interest

The authors declare no conflict of interest.

## References

- [1] Abobala, M. (2020). N-cyclic refined neutrosophic algebraic systems of sub-indeterminacies, an application to rings and modules. *International journal of neutrosophic science*, 12(2), 81–95. DOI:10.5281/zenodo.4278999
- [2] Smarandache, F. (2015). *Symbolic neutrosophic theory*. Infinite Study.
- [3] Al Rida Sadiq, B. A. (2022). A contribution to the group of units' problem in some 2-cyclic refined neutrosophic rings. *International journal of neutrosophic science*, 18(3), 48–58. DOI:10.54216/IJNS.180304
- [4] Von Shtawzen, O. (2022). Conjectures for invertible diophantine equations of 3-cyclic and 4-cyclic refined integers. *Journal of neutrosophic and fuzzy systems*, 3, 32–36.
- [5] Basheer, A. A., Ahmad, K. D., & Ali, R. (2022). On some open problems about n-cyclic refined neutrosophic rings and number theory. *Journal of neutrosophic and fuzzy systems*, 3(2), 37–42.
- [6] Shtawzen, O. V. (2022). On a novel group derived from a generalization of integer exponents and open problems. *Galoitica: journal of mathematical structures and applications*, 1(1), 12–35. DOI:10.54216/gjmsa.010102
- [7] Othman, K. Ben, Von Shtawzen, O., Khaldi, A., & Ali, R. (2023). *On the concept of symbolic 7-plithogenic real matrices*. Infinite Study.
- [8] Zayood, K. (2023). On novel public-key cryptosystem using MDS code. *CERN European organization for nuclear research*, 1. <https://doi.org/10.5281/zenodo.7882491>
- [9] Zayood, K. (2023). On a novel generalization of the RSA crypto-system. *Neoma journal of mathematics and computer science (NJMCS)*, 1. <https://zenodo.org/records/7882515>
- [10] Merkepci, M., & Sarkis, M. (2022). An application of pythagorean circles in cryptography and some ideas for future non classical systems. *Galoitica: journal of mathematical structures and applications*, 2(2), 28–30. DOI:10.54216/gjmsa.020205
- [11] Abobala, M., & Allouf, A. (2023). On a novel security scheme for the encryption and decryption Of  $2\tilde{A}-2$  fuzzy matrices with rational entries based on the algebra of neutrosophic integers and El-Gamal crypto-system. *Neutrosophic sets and systems*, 54, 19–32.
- [12] Merkepci, M., Abobala, M., & Allouf, A. (2023). *The applications of fusion neutrosophic number theory in public key cryptography and the improvement of RSA algorithm*. Infinite Study.
- [13] Merkepci, M., & Abobala, M. (2023). *Security model for encrypting uncertain rational data units based on refined neutrosophic integers fusion and El-Gamal algorithm*. Infinite Study.



- [14] Alhasan, Y. A., Alfahal, A. M. A., Abdulfatah, R. A., Ali, R., & Aljibawi, M. (2023). On a novel security algorithm for the encryption of  $3 \times 3$  fuzzy matrices with rational entries based on the symbolic 2-plithogenic integers and El-Gamal algorithm. *International journal of neutrosophic science*, 21(1), 88–95. DOI:10.54216/IJNS.210108
- [15] Taffach, N. M., & Hatip, A. (2023). A brief review on the symbolic 2-plithogenic number theory and algebraic equations. *Galoitica: journal of mathematical structures and applications*, 5(1), 36–44. DOI:10.54216/gjmsa.050103
- [16] Martin, N., & Edalatpanah, S. A. (2023). Application of extended fuzzy ISOCOV methodology in nanomaterial selection based on performance measures. *Journal of operational and strategic analytics*, 1(2), 55–61. DOI:10.56578/josa010202
- [17] Babazadeh, Y., Farahmand, N. F., Pasebani, M., & Matin, Y. A. (2022). Identifying key indicators for developing the use of blockchain technology in financial systems. *International journal of research in industrial engineering (2783-1337)*, 11(3), 244–257.
- [18] Sankari, H., & Abobala, M. (2023). On the classification of the group of units of rational and real 2-cyclic refined neutrosophic rings. *Neutrosophic sets and systems*, 54, 89–100. DOI:10.5281/zenodo.7817657