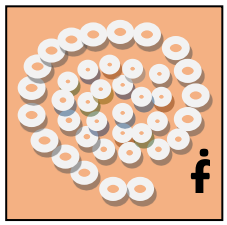

International Journal of Mathematical Analysis and Modelling

(Formerly Journal of the Nigerian Society for Mathematical Biology)

Volume 8 Issue 1, 2025

ISSN (Print): 2682 - 5694
ISSN (Online): 2682 – 5708
www.tnsmb.org

Effect of self-invertible rhotrix on cipher pentagraphic polyfunction

I.J. Ugbene[*†] and **S.C. Obukadata**[†‡]

Abstract

Traditional cryptography has long relied on matrices for encryption transformations, our work takes a different path by exploring the use of *rhotrix*, an extension of matrices that offers extra structural flexibility. Recent research has shown vulnerabilities in some self-invertible matrices, particularly those of dimensions 4×4 and 6×6. To enhance the security of systems such as the Cipher Tetragraphic Trifunction and Cipher Hexagraphic Polyfunction, these matrices should be strictly avoided. Building on this knowledge, our study seeks to identify patterns in self-invertible, rhotrix-based encryption keys and evaluate their impact on the security of Cipher Pentagraphic Polyfunction transformations. To this end, we derive solutions for self-invertible rhotrix keys that satisfy transformation conditions analogous to $L^2_{5\times5} \equiv A_{5\times5} \pmod N$, where $A_{5\times5}$ are diagonal and symmetric rhotrices. By implementing these rhotrix keys, we analyze their structural influence on the security of Cipher Pentagraphic Polyfunction transformations, aiming to contribute a new perspective to cryptographic design that is both theoretically sound and practically robust.

Keywords and phrases: cipher pentagraphic polyfunction; rhotrix; encryption keys; self invertible rhotrix; diagonal and symmetric rhotrices

1 Introduction

Cryptography is the art and science of safeguarding our communications. It takes clear, understandable information, what we call plaintext and scrambles it into a chaotic, unreadable form known as ciphertext, which can later be converted back into the original message when needed [1]. It is indeed fascinating as it's where the elegance of mathematics, the ingenuity of computer science, and the depth of information theory converge to form the very foundation of the digital security systems that keep our online lives safe every day.

Before the breakthrough of asymmetric cryptography, almost every encryption method relied on a single, secret key to both encrypt and decrypt information, a practice that, while effective in its day, limited flexibility and scalability. Everything changed in the 1970s. It was during this transformative period that researchers began developing asymmetric cryptosystems, where two distinct keys are employed: one for encrypting the data and a completely separate one for decrypting it. One of the most thrilling innovations from that era was the introduction of the RSA cryptosystem in 1978 by Ron Rivest, Adi Shamir, and Leonard Adleman [2, 3]. Imagine the excitement, finally, a system emerged that made secure, public-key communication a reality. RSA not only provided a practical solution for asymmetric encryption but also laid the cornerstone for the modern digital security landscape we depend on today.

In this paper, we explore the use of an asymmetric cryptosystem based on Rhotrix, an entirely new approach to encryption and decryption. Rhotrix explores the principles of Cipher Pentagraphic Polyfunction to provide robust security for communication. Our goal in using Rhotrix is to keep your

[*]Corresponding Author; E-mail: ugbene.ifeanyi@fupre.edu.ng
[†]Department of Mathematics, Federal University of Petroleum Resources, Effurun, Nigeria.
[‡]E-mail: obukadatastanley23@gmail.com

data safe and private. We want to create a system where your information is locked away, so that only the people who are meant to see it can get access, ensuring that your sensitive data remains truly secure.

1.1 Preliminaries

A rhotrix is a special type of numerical array arranged in a rhomboidal shape. The concept of forming arrays that lie between two-dimensional vectors and 2×2 matrices was first explored by [4] in their work on matrix-tertions and noitrets. Building on this idea, Ajibade [5] introduced a new mathematical structure that extends beyond 2×2 matrices but remains distinct from traditional 3×3 matrices. He named this structure a rhotrix. Specifically, he defined a three-dimensional rhotrix as:

$$R = \left\{ \left\langle \begin{array}{ccc} & a & \\ b & c & d \\ & e & \end{array} \right\rangle : a, b, c, d, e \in R \right\} \tag{1}$$

In this special kind of matrix called a rhotrix R. Right in its center is an element called the "heart" of the rhotrix. We denote this central element as c, and because it is so crucial, we often represent it as $h(R)$. It has been observed that rhotrices structured around this central heart always have an odd dimension. For a rhotrix of dimension n, the total number of elements is given by

$$|R_n| = \frac{1}{2}(n^2 + 1).$$

where n is a odd number. It's quite interesting to note that the basic algebra behind these rhotrices, along with the whole analytical setup, was first introduced by Ajibade back in 2003. His groundbreaking work really paved the way for exploring this area. In that paper, the addition and multiplication operations for what are called "heart-based" rhotrices were clearly defined, offering us a straightforward way to grasp how these special matrices operate.

$$R + Q = \left\langle \begin{array}{ccc} & a & \\ b & h(R) & d \\ & e & \end{array} \right\rangle + \left\langle \begin{array}{ccc} & f & \\ g & h(Q) & j \\ & k & \end{array} \right\rangle = \left\langle \begin{array}{ccc} & a+f & \\ b+g & h(R)+h(Q) & d+j \\ & e+k & \end{array} \right\rangle \tag{2}$$

and

$$R \circ Q = \left\langle \begin{array}{ccc} & ah(Q)+fh(R) & \\ bh(Q)+gh(R) & h(R)h(Q) & dh(Q)+jh(R) \\ & eh(Q)+kh(R) & \end{array} \right\rangle \tag{3}$$

[6] and [7] demonstrate a generalization of this robust multiplication. [8] developed a heart-based rhotrices row-column multiplication as follows:

$$R \circ Q = \left\langle \begin{array}{ccc} & af+dg & \\ bf+eg & h(R)h(Q) & aj+dk \\ & bj+ek & \end{array} \right\rangle \tag{4}$$

This row-column multiplication was further generalized as follows by Sani (2007):

$$R_n \circ Q_n = \langle a_{i_1 j_1}, c_{i_2 j_2} \rangle \circ \langle b_{i_2 j_2}, d_{l_2 k_2} \rangle = \left\langle \sum_{i_2 j_1 = 1}^{t} (a_{i_1 j_1} b_{i_2 j_2}) \quad , \quad \sum_{l_2 k_1 = 1}^{t-1} (c_{l_1 k_1} d_{l_2 k_2}) \right\rangle, \quad t = \frac{n+1}{2} \tag{5}$$

$n-$dimensional rhotrices (with n rows and n columns) are represented by R_n and Q_n. In this work, R will be used to represent any rhotrix, whereas R_n is a n-dimensional rhotrix.

Given a n-dimensional rhotrix $R_n = \langle a_{ij}, c_{lk} \rangle$, the determinant of R_n may be found using the formula $\det(R_n) = \det(A_t)\det(C_{t-1})$, where $t = \frac{n+1}{2}$ and $n \in 2\mathbb{Z}^+ + 1$ are the rhotrix R_n, which is composed of two square matrices of dimension $(t \times t)$ and $(t-1) \times (t-1)$, respectively, A_t and C_{t-1}.

Definition 1.1: The inverse of a rhotrix $R_n = (a_{ij}, c_{lk})$ is denoted as $R_n^{-1} = \langle q_{ij}, r_{lk} \rangle$, where it satisfies the condition

$$R_n \circ R_n^{-1} = \langle a_{ij}, c_{lk} \rangle \circ \langle q_{ij}, r_{lk} \rangle = \langle I_{ij}, I_{lk} \rangle$$

Here, the matrices $[q_{ij}]_{t\times t}$ and $[r_{lk}]_{t-1\times t-1}$ represent the inverses of the two square matrices $[a_{ij}]_{t\times t}$ and $[c_{lk}]_{t-1\times t-1}$, respectively, which constitute the rhotrix R_n. The parameter t is given by

$$t = \frac{n+1}{2}, \quad \text{where} \quad n \in 2\mathbb{Z}^+ + 1.$$

An $n \times n$ rhotrix R_n with integer entries is termed *self-invertible modulo* N if it satisfies

$$R_n \equiv R_n^{-1} \pmod{N}.$$

That is, if there exists a matrix R_n^{-1} such that

$$R_n R_n^{-1} = R_n^{-1} R_n \equiv I \pmod{N},$$

where I denotes the identity rhotrix of order n, then R_n^{-1} is the inverse of R_n modulo N. In particular, when R_n equals its own inverse modulo N, it is called self-invertible. For $R = \left\langle \begin{matrix} & a & \\ b & h(R) & d \\ & e & \end{matrix} \right\rangle$ be any rhotrix of size 3, then for any integer m, $R^m = (h(R))^{m-1} \left\langle \begin{matrix} & ma & \\ mb & h(R) & md \\ & me & \end{matrix} \right\rangle$. In particular, R^0 and R^{-1} are the identity and inverse of R respectively, provided $h(R)$ is non-zero.

Definition 1.2: Let $R_n(F)$ be a set of all rhotrices of size n with entries from an arbitrary field F. For $A_n, B_n \in R_n(F)$, define a binary operation $\circ$ on $R_n(F)$ by the rule:

$$A_n \circ B_n = (a_{i_1 j_1}, c_{l_1 k_1}) \circ (b_{i_2 j_2}, d_{l_2 k_2}) = \left\langle \sum_{i_2 j_1 = 1}^{t} (a_{i_1 j_1} b_{i_2 j_2}), \sum_{l_2 k_1 = 1}^{t-1} (c_{l_1 k_1} d_{l_2 k_2}) \right\rangle, \; t = \frac{n+1}{2}$$

$a_{ij} \in M_t(F)$ and $c_{lk} \in M_{t-1}(F)$. Then $S = (R_n(F), \circ)$ is a rhotrix type A semigroup [9]. Conversely, every rhotrix type A semigroup is isomorphic to one of such construction.

Suppose $A_n = \langle a_{i_1 j_1}, c_{l_1 k_1} \rangle$, $B_n = \langle b_{i_2 j_2}, d_{l_2 k_2} \rangle$, $C_n = \langle u_{i_3 j_3}, v_{l_3 k_3} \rangle$, then we have that

$$A_n \circ (B_n \circ C_n) = \langle a_{i_1 j_1}, c_{l_1 k_1} \rangle \circ (\langle b_{i_2 j_2}, d_{l_2 k_2} \rangle \circ \langle u_{i_3 j_3}, v_{l_3 k_3} \rangle)$$

$$= \langle a_{i_1 j_1}, c_{l_1 k_1} \rangle \circ \left\langle \sum_{i_3 j_2 = 1}^{t} (b_{i_2 j_2} u_{i_3 j_3}), \sum_{l_3 k_2 = 1}^{t-1} (d_{l_2 k_2} v_{l_3 k_3}) \right\rangle$$

$$= \left\langle \sum_{i_2 j_1 = 1}^{t} a_{i_1 j_1} \left[\sum_{i_3 j_2 = 1}^{t} (b_{i_2 j_2} u_{i_3 j_3}) \right], \sum_{l_2 k_1 = 1}^{t-1} c_{l_1 k_1} \left[\sum_{l_3 k_2 = 1}^{t-1} (d_{l_2 k_2} v_{l_3 k_3}) \right] \right\rangle$$

$$= \left\langle \sum_{i_2 j_1 = 1}^{t} \sum_{i_3 j_2 = 1}^{t} a_{i_1 j_1} (b_{i_2 j_2} u_{i_3 j_3}), \sum_{l_2 k_1 = 1}^{t-1} \sum_{l_3 k_2 = 1}^{t-1} c_{l_1 k_1} (d_{l_2 k_2} v_{l_3 k_3}) \right\rangle$$

$$= \left\langle \sum_{i_2 j_1 = 1}^{t} \sum_{i_3 j_2 = 1}^{t} a_{i_1 j_1} b_{i_2 j_2} u_{i_3 j_3}, \sum_{l_2 k_1 = 1}^{t-1} \sum_{l_3 k_2 = 1}^{t-1} c_{l_1 k_1} d_{l_2 k_2} v_{l_3 k_3} \right\rangle$$

.

Similarly, we have that

$$(A_n \circ B_n) \circ C_n = (\langle a_{i_1 j_1}, c_{l_1 k_1} \rangle \circ \langle b_{i_2 j_2}, d_{l_2 k_2} \rangle) \circ \langle u_{i_3 j_3}, v_{l_3 k_3} \rangle$$

$$= \left\langle \sum_{i_2j_1=1}^{t} a_{i_1j_1}b_{i_2j_2}, \sum_{l_2k_1=1}^{t-1} c_{l_1k_1}d_{l_2k_2} \right\rangle \circ \langle u_{i_3j_3}, v_{l_3k_3} \rangle$$

$$= \left\langle \sum_{i_3j_2=1}^{t} u_{i_3j_3} \left[\sum_{i_2j_1=1}^{t} a_{i_1j_1}b_{i_2j_2} \right], \sum_{l_3k_2=1}^{t-1} v_{l_3k_3} \left[\sum_{l_2k_1=1}^{t-1} c_{l_1k_1}d_{l_2k_2} \right] \right\rangle$$

$$= \left\langle \sum_{i_3j_2=1}^{t} \sum_{i_2j_1=1}^{t} (a_{i_1j_1}b_{i_2j_2})u_{i_3j_3}, \sum_{l_3k_2=1}^{t-1} \sum_{l_2k_1=1}^{t-1} (c_{l_1k_1}d_{l_2k_2})v_{l_3k_3} \right\rangle$$

$$= \left\langle \sum_{i_3j_2=1}^{t} \sum_{i_2j_1=1}^{t} a_{i_1j_1}b_{i_2j_2}u_{i_3j_3}, \sum_{l_3k_2=1}^{t-1} \sum_{l_2k_1=1}^{t-1} c_{l_1k_1}d_{l_2k_2}v_{l_3k_3} \right\rangle$$

Consequently,
$A_n \circ (B_n \circ C_n) = (A_n \circ B_n) \circ C_n$.

Let S be a rhotrix type A semigroup. Define a map $\theta : S \to R_n(F)$ by the rule that

$$s\theta = \left\langle \begin{array}{ccccc} & & a_{11} & & \\ & a_{21} & c_{11} & a_{12} & \\ & \cdots & \cdots & \cdots & \\ a_{t1} & \cdots & \cdots & \cdots & a_{1t} \\ & \cdots & \cdots & \cdots & \\ & a_{t(t-1)} & c_{(t-1)(t-1)} & a_{(t-1)t} & \\ & & a_{tt} & & \end{array} \right\rangle \theta$$

$$= \left\langle \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1t} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t1} & a_{t2} & \cdots & a_{tt} \end{bmatrix}, \begin{bmatrix} c_{11} & \cdots & c_{1(t-1)} \\ \vdots & \ddots & \vdots \\ c_{(t-1)1} & \cdots & c_{(t-1)(t-1)} \end{bmatrix} \right\rangle$$

$$\implies s\theta \to R_n(F)\theta \to \langle M_t(F), M_{t-1}(F) \rangle$$

where $t = \frac{n+1}{2}, n \in 2\mathbb{Z}^+ + 1, a_{tt} \in M_t(F)$ and $c_{(t-1)(t-1)} \in M_{t-1}(F)$ and θ maps each element of S to its corresponding $t \times t$ matrix and $(t-1)(t-1)$ matrix in $R_n(F)$ with the usual matrix, the matrix $M_t(F)$ and $M_{t-1}(F)$ are often referred to as coupled matrix of the rhotrix $R_n(F)$. Since a rhotrix can be viewed as a coupled matrix, the decryption process in such systems depends on computing the inverse of the matrix key. Unfortunately, a matrix inverse does not always exist; when the key is non-invertible, it becomes impossible to recover the original message. To address this issue, researchers have developed techniques based on modular arithmetic that generate self-invertible matrices. This approach ensures that the encryption key can always be inverted, thus guaranteeing that the ciphertext can be decrypted. Their work specifically focuses on constructing self-invertible matrices of various dimensions, such as 2×2, 3×3, 4×4, and even larger even-order matrices. By employing these techniques, the computational burden of finding an inverse during decryption is effectively eliminated. In particular, a method for generating a self-invertible 4×4 matrix is proposed as follows:

Let $M_4(F) = \begin{bmatrix} M_{4_{11}}(F) & M_{4_{12}}(F) \\ M_{4_{21}}(F) & M_{4_{22}}(F) \end{bmatrix}$ be self-invertible matrix where $M_{4_{11}}(F) = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, $M_{4_{12}}(F) = \begin{bmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{bmatrix}$, $M_{4_{21}}(F) = \begin{bmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{bmatrix}$, and $M_{4_{22}}(F) = \begin{bmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{bmatrix}$. Then from $R_n \cdot R_n^{-1} = I$, the system of equations is $M_{4_{12}}(F)M_{4_{21}}(F) = I - M_{4_{11}}(F)^2$, $M_{4_{11}}(F)M_{4_{12}}(F) + M_{4_{12}}(F)M_{4_{22}}(F) = 0$, $M_{4_{21}}(F)M_{4_{11}}(F) + M_{4_{22}}(F)M_{4_{21}}(F) = 0$ and $M_{4_{21}}(F)M_{4_{12}}(F) = I - M_{4_{22}}(F)^2$.

Hence, the solution for $M_4(F)$ is $\begin{bmatrix} M_{4_{11}}(F) & (I - M_{4_{11}}(F))k \\ (I + M_{4_{11}}(F))k^{-1} & -M_{4_{11}}(F) \end{bmatrix}$ where $k \in \mathbb{Z}$. Within this scheme, every matrix is evaluated modulo N, and to guarantee invertibility, the requirement $(k, N) = 1$ is imposed.

1.2 Generation of self-invertible 5×5 rhotrix

Let $R_5 = \left\langle \begin{array}{ccccc} & & a & & \\ & f & d & b & \\ k & i & g & e & c \\ & l & j & h & \\ & & m & & \end{array} \right\rangle = \left\langle \begin{bmatrix} a & b & c \\ f & g & h \\ k & l & m \end{bmatrix}, \begin{bmatrix} d & e \\ i & j \end{bmatrix} \right\rangle$

Let $M_{2\times 2} = \begin{bmatrix} d & e \\ i & j \end{bmatrix}$, then,

$$M_{2\times 2}^{-1} = \frac{adj(M_{2\times 2})}{\det(M_{2\times 2})} = \frac{(Cofac(M_{2\times 2}))^T}{\det(M_{2\times 2})}$$

$$\therefore M_{2\times 2}^{-1} = \frac{1}{\det M_{2\times 2}} \begin{bmatrix} j & -e \\ -i & d \end{bmatrix}$$

$M_{2\times 2}$ is said to be self-invertible if $M_{2\times 2} = M_{2\times 2}^{-1}$

So, $e = -e \,/\, \det(M_{2\times 2})$ & $i = -i \,/\, \det(M_{2\times 2})$

$\therefore \det(M_{2\times 2}) = -1$ and $d = -j \implies d + j = 0$

Consider the matrix

$$\left[\begin{array}{c|cc} a & b & c \\ \hline f & g & h \\ k & l & m \end{array}\right] = \begin{bmatrix} M_{11} & M_{12} \\ M_{21} & M_{22} \end{bmatrix},$$

where M_{11} is a 1×1 matrix $[a]$, M_{12} is a 1×2 matrix $\begin{bmatrix} b & c \end{bmatrix}$, M_{21} is a 2×1 matrix $\begin{bmatrix} f \\ k \end{bmatrix}$, and M_{22} is a 2×2 matrix $\begin{bmatrix} g & h \\ l & m \end{bmatrix}$. If the 3×3 matrix is self-inverting, the following conditions must be satisfied:

$$\begin{aligned} M_{11}^2 + M_{12}M_{21} &= I, \\ M_{11}M_{12} + M_{12}M_{22} &= 0, \\ M_{21}M_{11} + M_{22}M_{21} &= 0, \\ M_{21}M_{12} + M_{22}^2 &= I. \end{aligned}$$

Since M_{11} is simply $[a]$, we have

$$M_{21}(aI + M_{22}) = 0.$$

For a non-trivial solution to exist, it is necessary that

$$aI + M_{22} = 0,$$

which implies that a must be equal to the negative of one of the eigenvalues of M_{22}. Moreover, the product $M_{21}M_{12}$ can be expressed as

$$M_{21}M_{12} = \begin{bmatrix} f \\ k \end{bmatrix} \begin{bmatrix} 0 & b & c \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} fb & fc \\ kb & kc \end{bmatrix}.$$

This result shows that $M_{21}M_{12}$ is singular, and we have the relation

$$M_{21}M_{12} = I - M_{22}^2.$$

Therefore, M_{22} must have an eigenvalue of ± 1. It can also be demonstrated that

$$\text{Trace}(M_{21}M_{12}) = M_{12}M_{21}.$$

Finally, if we set $M_{11} = a = -\lambda$ (where λ is one of the eigenvalues of M_{22}), then any non-trivial solution of the equation

$$M_{21}M_{12} = I - M_{22}^2$$

will also satisfy

$$M_{12}M_{21} = 1 - a^2.$$

1.3 A general method of generating self-invertible rhotrix

Let $A = \left\langle \begin{matrix} & & a_{11} & & \\ & a_{21} & c_{11} & a_{12} & \\ & \cdots & \cdots & \cdots & \\ a_{t1} & \cdots & \cdots & \cdots & a_{1t} \\ & \cdots & \cdots & \cdots & \\ & a_{t(t-1)} & c_{(t-1)(t-1)} & a_{(t-1)t} & \\ & & a_{tt} & & \end{matrix} \right\rangle$

$= \left\langle \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1t} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t1} & a_{t2} & \cdots & a_{tt} \end{bmatrix}, \begin{bmatrix} c_{11} & \cdots & c_{1(t-1)} \\ \vdots & \ddots & \vdots \\ c_{(t-1)1} & \cdots & c_{(t-1)(t-1)} \end{bmatrix} \right\rangle$ be an $n \times n$ self-invertible rhotrix, it's coupled matrix can be partitioned in such a way that $M_t(F) = \begin{bmatrix} M_{t_{11}}(F) & M_{t_{12}}(F) \\ M_{t_{21}}(F) & M_{t_{22}}(F) \end{bmatrix}$

$M_{t_{11}}(F)$, a 1×1 matrix, written as $[a_{11}]$. $M_{t_{12}}(F)$ is a $1 \times (n-1)$ matrix given by $\begin{bmatrix} a_{12} & \dots & a_{1t} \end{bmatrix}$. Similarly, $M_{t_{21}}(F)$ is an $(n-1) \times 1$ matrix represented as $\begin{bmatrix} a_{21} \\ \vdots \\ a_{t1} \end{bmatrix}$, and $M_{t_{22}}(F)$ is an $(n-1) \times (n-1)$ matrix arranged as

$$\begin{bmatrix} a_{22} & a_{23} & \dots & a_{2t} \\ a_{32} & a_{33} & \dots & a_{3t} \\ \vdots & \vdots & \ddots & \vdots \\ a_{t2} & a_{t3} & \dots & a_{tt} \end{bmatrix}.$$

So,

$$M_{t_{12}}(F)M_{t_{21}}(F) = I - M_{t_{11}}(F)^2 = 1 - a_{11}^2 \tag{6}$$

and

$$M_{t_{12}}(F)(a_{11}I + M_{t_{22}}(F)) = 0$$

Also, $a_{11} =$ (one of the Eigen values of $M_{t_{22}}(F)$ other than 1) Since $M_{t_{21}}(F)M_{t_{12}}(F)$ is a singular matrix having the rank 1 and

$$M_{t_{21}}(F)M_{t_{12}}(F) = I - M_{t_{22}}(F)^2 \tag{7}$$

So, $M_{t_{22}}(F)^2$ must have rank of $(n-2)$ with Eigen values $+1$ of $(n-2)$ multiplicity. Therefore, $M_{t_{22}}(F)$ must have Eigen values ± 1. It can also be proved that the consistent solution obtained for elements $M_{t_{21}}(F)$ & $M_{t_{12}}(F)$ by solving the equation (7) term by term will also satisfy the equation (6) and same idea goes for the matrix $M_{(t-1)}(F)$. Several notations to be utilized during the encryption phase of the Cipher Pentagraphic Polyfunction are detailed below:

- In this context, P represents the numerical value assigned to an element in the plaintext. For example, if the letter B corresponds to the number 50, then $P = 50$.
- $P_{i\times i} = \begin{cases} P^1_{x\times x|y\times y} \\ \vdots \\ P^n_{x\times x|y\times y} \end{cases} = \langle\langle p^1_{xx}, p^1_{yy}\rangle \dots \langle p^n_{xx}, p^n_{yy}\rangle\rangle = \sum_{j=1}^{n} \left\langle p^j_{xx}, p^j_{yy} \right\rangle$ is a corresponding numbers sequence with a plain text, that is $p^1_{xx}, p^1_{yy} \dots p^n_{xx}, p^n_{yy}$ For every x satisfying $x \leq \frac{i+1}{2}$, and every y satisfying $y \leq \frac{i+1}{2} - 1$, where these values are arranged according to the rows and columns of a coupled matrix, and letting n denote the number of times the plaintext is divided, we obtain the following mapping. For instance, consider the plaintext "PLEASE". When processed using this scheme, the corresponding numerical sequence is $80,\ 76,\ 69,\ 65,\ 83,\ 69$, the text is divided

into equal halves corresponding to the dimension of the rhotrix, suppose the dimension of the key rhotrix is 5, we get $P_{i\times i} = P_{5\times 5}$, use $x = \frac{i+1}{2} = \frac{6}{2} = 3$ and $y = \frac{i+1}{2} = \frac{6}{2} - 1 = 2$, but the split is solely dependent on x, since $x > y$. So, we split into |80 76 69| 65 83 69| corresponding to |PLE|ASE| and add arbitrary "special character" from ASCII code to fill out the last pair if the plaintext has an odd number of letters, and use a constant number to represent the rest, such that

$$P_5 = \begin{cases} P^1_{3\times 3|2\times 2} = \left\langle \begin{matrix} & & 80 & & \\ & 45 & 45 & 76 & \\ 45 & 45 & 45 & 45 & 69 \\ & 45 & 45 & 45 & \\ & & 45 & & \end{matrix} \right\rangle = \left\langle \begin{bmatrix} 80 & 76 & 69 \\ 45 & 45 & 45 \\ 45 & 45 & 45 \end{bmatrix}, \begin{bmatrix} 45 & 45 \\ 45 & 45 \end{bmatrix} \right\rangle \\ P^2_{3\times 3|2\times 2} = \left\langle \begin{matrix} & & 65 & & \\ & 45 & 45 & 83 & \\ 45 & 45 & 45 & 45 & 69 \\ & 45 & 45 & 45 & \\ & & 45 & & \end{matrix} \right\rangle = \left\langle \begin{bmatrix} 65 & 83 & 69 \\ 45 & 45 & 45 \\ 45 & 45 & 45 \end{bmatrix}, \begin{bmatrix} 45 & 45 \\ 45 & 45 \end{bmatrix} \right\rangle \end{cases}$$

- Let C denote the numerical value corresponding to a ciphertext produced by a monofunction transformation. For example, if the ciphertext "AB" is mapped to the number 7686, then this transformation yields $C = 7686$. In other words, the monofunction transformation converts the ciphertext "AB" into its numerical representation 7686, which is used in subsequent cryptographic processing.
- $C_{i\times i} = \begin{cases} C^1_{x\times x|y\times y} \\ \vdots \\ C^n_{x\times x|y\times y} \end{cases} = \langle\langle c^1_{xx}, c^1_{yy}\rangle \dots \langle c^n_{xx}, c^n_{yy}\rangle\rangle = \sum_{j=1}^{n} \left\langle c^j_{xx}, c^j_{yy} \right\rangle$ is a corresponding numbers sequence with a cipher text $c^1_{xx}, c^1_{yy} \dots c^n_{xx}, c^n_{yy}$ for every $x \le \frac{i+1}{2}$ and $y \le \frac{i+1}{2} - 1$, Consider the ciphertext "ABCDEF" produced by a monofunction transformation, where each character is converted to its corresponding ASCII value. This yields the sequence: 65, 66, 67, 68, 69, 70. These numbers are then arranged into a coupled matrix based on the row and column structure derived from the transformation. For instance, the sequence can be organized into a 5×5 rhotrix as follows:

$$C_5 = \begin{cases} C^1_{3\times 3|2\times 2} = \left\langle \begin{matrix} & & 65 & & \\ & 45 & 45 & 66 & \\ 45 & 45 & 45 & 45 & 67 \\ & 45 & 45 & 45 & \\ & & 45 & & \end{matrix} \right\rangle = \left\langle \begin{bmatrix} 65 & 66 & 67 \\ 45 & 45 & 45 \\ 45 & 45 & 45 \end{bmatrix}, \begin{bmatrix} 45 & 45 \\ 45 & 45 \end{bmatrix} \right\rangle \\ C^2_{3\times 3|2\times 2} = \left\langle \begin{matrix} & & 68 & & \\ & 45 & 45 & 69 & \\ 45 & 45 & 45 & 45 & 70 \\ & 45 & 45 & 45 & \\ & & 45 & & \end{matrix} \right\rangle = \left\langle \begin{bmatrix} 68 & 69 & 70 \\ 45 & 45 & 45 \\ 45 & 45 & 45 \end{bmatrix}, \begin{bmatrix} 45 & 45 \\ 45 & 45 \end{bmatrix} \right\rangle \end{cases}$$

Consider the numerical sequence corresponding to a ciphertext obtained via a monofunction transformation. For each transformation t, we define, $C^{(t)}_{i\times i} = \left[\sum_{j=1}^{n} \langle c^j_{xx}, c^j_{yy}\rangle\right]^{(t)}$, which represents

the sequence associated with the ciphertext, $\sum_{j=1}^{n}\langle c_{xx}^{j}, c_{yy}^{j}\rangle$, where the indices x and y satisfy, $x \leq \frac{i+1}{2}$ and $y \leq \frac{i+1}{2} - 1$. These values are arranged according to the rows and columns of a coupled matrix derived from the transformation process at the t^{th} stage (with $t = 1, 2, 3, \ldots$). When $t = 1$, we denote the ciphertext sequence as

$$C_{i\times i} = \left\langle \langle c_{xx}^{1}, c_{yy}^{1}\rangle, \langle c_{xx}^{2}, c_{yy}^{2}\rangle, \ldots, \langle c_{xx}^{n}, c_{yy}^{n}\rangle \right\rangle.$$

For example, if the ciphertext is "MZWAD" and, under the third transformation, the corresponding numerical sequence produced is $78 \quad 90 \quad 87 \quad 86 \quad 65 \quad 68$, then these numbers are arranged according to the coupled matrix structure as specified.

$$\begin{cases} {C^{1}_{3\times3|2\times2}}^{(3)} = \left\langle \begin{matrix} & & 78 & & \\ & 70 & 70 & 90 & \\ 70 & 70 & 70 & 70 & 87 \\ & 70 & 70 & 70 & \\ & & 70 & & \end{matrix} \right\rangle = \left\langle \begin{bmatrix} 78 & 90 & 87 \\ 70 & 70 & 70 \\ 70 & 70 & 70 \end{bmatrix}, \begin{bmatrix} 70 & 70 \\ 70 & 70 \end{bmatrix} \right\rangle \\ {C^{2}_{3\times3|2\times2}}^{(3)} = \left\langle \begin{matrix} & & 86 & & \\ & 70 & 70 & 65 & \\ 70 & 70 & 70 & 70 & 68 \\ & 70 & 70 & 70 & \\ & & 70 & & \end{matrix} \right\rangle = \left\langle \begin{bmatrix} 86 & 65 & 68 \\ 70 & 70 & 70 \\ 70 & 70 & 70 \end{bmatrix}, \begin{bmatrix} 70 & 70 \\ 70 & 70 \end{bmatrix} \right\rangle \end{cases}$$

Encryption key $L_{i\times i} = \langle l_{xx}, l_{yy}\rangle$ is an integer sequence l_{xx}, l_{yy} arranged based on the row and column of a coupled matrix while $L_{k}^{-1} = \langle q_{xx}, q_{yy}\rangle$ is the inverse rhotrix for $L_{i\times i}$ such that $|L_{i\times i}| \neq 0$.

Several key definitions that are crucial for this work have been established in earlier studies [10–14], but not in the terms of rhotrix. In this paper, we adopt the following definitions:

Definition 1.3: Let N be any positive integer. We define the numerical representations corresponding to the plaintext and ciphertext as *rhotrices* with i rows and i columns.

$$P_{i\times i} \equiv \sum_{j=1}^{n} \langle p_{xx}^{j}, p_{yy}^{j}\rangle \mod N,$$

and

$$C_{i\times i}^{(t)} \equiv \left[\sum_{j=1}^{n} \langle c_{xx}^{j}, c_{yy}^{j}\rangle\right]^{(t)} \mod N$$

for every $x \leq \frac{i+1}{2}$ and $y \leq \frac{i+1}{2} - 1$.

Let the encryption key be an $i \times i$ rhotrix:

$$L_{i\times i}^{(t)} \equiv \langle l_{xx}, l_{yy}\rangle \mod N$$

Assume the plaintext is represented by an $i \times i$ rhotrix defined as, $P_{i\times i} \equiv \sum\limits_{j=1}^{n} \langle p_{xx}^{j}, p_{yy}^{j}\rangle \pmod N$, where the paired elements $\langle p_{xx}^{j}, p_{yy}^{j}\rangle$ are arranged into the rhotrix based on their row and column positions. For the first transformation, the encryption process produces a ciphertext rhotrix given by, $C_{i\times i}^{(1)} \equiv \left[\sum\limits_{j=1}^{n} \langle c_{xx}^{j}, c_{yy}^{j}\rangle\right]^{(1)} \pmod N$. This result is obtained by mapping each plaintext component $\langle p_{xx}^{j}, p_{yy}^{j}\rangle$ to its corresponding ciphertext component $\langle c_{xx}^{j}, c_{yy}^{j}\rangle$ through the monofunction transformation. The subsequent arrangement into a coupled matrix structure ensures that the transformation

adheres to the row and column ordering, and the modulo N operation confines the result within the appropriate finite field, such that

$$C_{i\times i}^{(1)} \equiv L_{i\times i}^{(1)} P_{i\times i} \mod N$$

with $C_{i\times i}^{(1)} \equiv \langle l_{xx}, l_{yy}\rangle^{(1)} \circ \sum_{j=1}^{n} \left\langle p_{xx}^{j}, p_{yy}^{j} \right\rangle \mod N = \sum_{j=1}^{n} \left\langle l_{xx}^{(1)} p_{xx}^{j}, l_{yy}^{(1)} p_{yy}^{j} \right\rangle \mod N$ which is called a Polygraphic cipher of a Monofunction Transformation.

Next, the cipher text $C_{i\times i}^{(1)} \equiv \left[\sum_{j=1}^{n} \left\langle c_{xx}^{j}, c_{yy}^{j} \right\rangle\right]^{(1)} \mod N$ was translated into a cipher text $C_{i\times i}^{(2)} \equiv \left[\sum_{j=1}^{n} \left\langle c_{xx}^{j}, c_{yy}^{j} \right\rangle\right]^{(2)} \mod N$at the second transformation through

$$C_{i\times i}^{(2)} \equiv L_{i\times i}^{(2)} C_{i\times i}^{(1)} \mod N$$

with $C_{i\times i}^{(2)} \equiv \langle l_{xx}, l_{yy}\rangle^{(2)} \circ \sum_{j=1}^{n} \left\langle l_{xx}^{(1)} p_{xx}^{j}, l_{yy}^{(1)} p_{yy}^{j} \right\rangle \mod N \equiv \sum_{j=1}^{n} \left\langle l_{xx}^{(2)} (l_{xx}^{(1)} p_{xx}^{j}), l_{yy}^{(2)} (l_{yy}^{(1)} p_{yy}^{j}) \right\rangle \mod N$ which is called Polygraphic cipher of a Difunction Transformation.

Moreover, the cipher text $C_{i\times i}^{(2)} \equiv \left[\sum_{j=1}^{n} \left\langle c_{xx}^{j}, c_{yy}^{j} \right\rangle\right]^{(2)} \mod N$ was translated into a cipher text $C_{i\times i}^{(3)} \equiv \left[\sum_{j=1}^{n} \left\langle c_{xx}^{j}, c_{yy}^{j} \right\rangle\right]^{(3)} \mod N$ at the third transformation through

$$C_{i\times i}^{(3)} \equiv L_{i\times i}^{(3)} C_{i\times i}^{(2)} \mod N$$

with $C_{i\times i}^{(3)} \equiv \langle l_{xx}, l_{yy}\rangle^{(3)} \sum_{j=1}^{n} \left\langle l_{xx}^{(2)} (l_{xx}^{(1)} p_{xx}^{j}), l_{yy}^{(2)} (l_{yy}^{(1)} p_{yy}^{j}) \right\rangle \mod N$ which is called Polygraphic cipher of a Trifunction Transformation.

Further, the equation of Cipher Polygraphic Polyfunction Transformation is

$$C_{i\times i}^{(t)} \equiv L_{i\times i}^{(t)} C_{i\times i}^{(t-1)} \mod N$$

with $C_{i\times i}^{(t)} \equiv \sum_{j=1}^{n} \sum_{k=1}^{n} \left\langle l_{xx}^{(k)} p_{xx}^{j}, l_{yy}^{(k)} p_{yy}^{j} \right\rangle \mod N$.

The encryption transformation can be expressed more simply as

$$C_{i\times i}^{(t)} \equiv L_{i\times i}^{t} P_{i\times i} \pmod N,$$

assuming that all secret keys $L_{i\times i}^{(t)}$ are the same. In our work, we set $i = 5$ and term this method the Cipher Pentagraphic Polyfunction. Thus, with uniform secret keys $L_{5\times 5}^{(t)}$, the transformation becomes

$$C_{5\times 5}^{(t)} \equiv L_{5\times 5}^{t} P_{5\times 5} \pmod N.$$

2 Literature Review

Hill Ciphers, introduced by [15], utilize linear algebra in cryptography, relying heavily on matrix operations for encryption and decryption. The fundamental principle of the Hill Cipher is based on polygraphic substitution, where blocks of plaintext characters are transformed into ciphertext through

matrix multiplication. Let P be the plaintext vector and K the encryption key matrix. The corresponding ciphertext C is then calculated by performing the matrix multiplication of K with P, followed by taking the result modulo 26:

$$C \equiv KP \pmod{26}.$$

In this context, both C and P are column vectors of length m, and K is an $m \times m$ matrix. The decryption process involves computing the modular inverse of K, satisfying $KK^{-1} \equiv I \pmod{26}$, where I is the identity matrix. This dependency on matrix inversion presents a notable limitation, as not all matrices are invertible, leading to potential decryption failures.

Several researchers have worked on improving the Hill Cipher's security and versatility [16]. In recent studies, number theory has been leveraged to enhance encryption methods, offering new insights into strengthening cryptographic techniques [17]. Modulo arithmetic concepts have been extended to Cipher Digraphic Polyfunction transformations, such as:

$$C_{2\times j} \equiv A_{2\times 2}P_{2\times j} \pmod{N}$$

where the determinant conditions $(|A_{2\times 2}|, N) = 1$ and $|A_{2\times 2}| \neq 0$ ensure the invertibility of the encryption matrix. These extensions address some weaknesses in the original Hill Cipher, particularly the issue of non-invertibility. Moreover, iterative encryption schemes have been explored, defining transformations such as:

$$C_{2\times j} \equiv \prod_{u=0}^{t-1} A_{2\times 2}^{(t-u)} P_{2\times j} \pmod{N}$$

to increase security through multiple transformations. Additionally, researchers have proposed self-invertible matrix generation techniques, ensuring that decryption is always feasible without requiring explicit matrix inversion. Furthermore, self-repetitive matrices, where $A^n \equiv I \pmod{N}$, have been suggested as an alternative to conventional Hill Cipher keys, increasing complexity for potential attackers [18].

Despite the widespread use of matrices in cryptography, an emerging alternative, **rhotrix**, provides additional security advantages. Introduced as an extension of matrices, rhotrix structures retain matrix-like properties while incorporating additional elements that increase their flexibility and security. Unlike traditional square matrices, rhotrix structures offer more complex transformations that are not easily susceptible to conventional matrix-based cryptanalysis.

According to recent studies [19–22], rhotrix-based encryption keys introduce new algebraic properties that improve cryptographic strength. Given these advantages, this study proposes the integration of self-invertible rhotrix keys into Cipher Pentagraphic Polyfunction transformations, an extension of previous digraphic and trigraphic encryption methods. To evaluate their effectiveness, solutions for self-invertible rhotrix keys satisfying transformation conditions analogous to:

$$L_{5\times 5}^2 \equiv A_{5\times 5} \pmod{N}$$

where $A_{5\times 5}$ are diagonal and symmetric rhotrices, will be derived and analyzed. The impact of these rhotrix-based keys on the security of Cipher Pentagraphic Polyfunction transformations will be assessed, highlighting their potential superiority over traditional matrix-based encryption techniques.

Earlier studies have investigated the role of self-inverting matrices in Cipher Tetragraphic Trifunction transformations. [23], explored $L_{2\times 2}$ matrices that fulfill the following condition:

$$L_{2\times 2}^3 \equiv A_{2\times 2} \pmod{N}$$

where $A_{2\times 2}$ varies between zero matrices, identity matrices, lower and upper triangular matrices, and general non-singular forms. The obtained solutions for $L_{2\times 2}$ include:

- When $A_{2\times 2} = 0$, possible solutions include matrices of the form:

$$L_{2\times 2} = \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & b \\ -b^{-1} & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & b \\ -b^{-1} & 1 \end{bmatrix}.$$

- When $A_{2\times2} = I$, valid choices for $L_{2\times2}$ include:

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} -2^{-1} & -3(4c)^{-1} \\ c & -2^{-1} \end{bmatrix}.$$

For other matrix forms of $A_{2\times2}$, solutions involve complex transformations, ensuring that $L_{2\times2}$ avoids singularities and enhances security. To improve Cipher Tetragraphic Trifunction transformations, it was recommended avoiding secret keys of the form:

$$L_{4\times4} \equiv \begin{bmatrix} L_{2\times2} & I - L_{2\times2} \\ I + L_{2\times2} & -L_{2\times2} \end{bmatrix} \pmod{N}$$

to prevent predictable patterns that could compromise encryption security. The encryption process follows:

$$C_{4\times4}^{(t)} \equiv L_{4\times4}^{t} P_{4\times4} \pmod{N}, \quad t \in \{1, 2, 3, \dots\}.$$

[24], expanded upon this scheme by deriving nine distinct solutions for self-invertible $L_{3\times3}$ matrices. These solutions were obtained from the equation

$$L_{3\times3}^{2} \equiv A_{3\times3} \pmod{N},$$

where $A_{3\times3}$ is defined as a diagonal and symmetric matrix. This extension not only reinforces the applicability of self-invertible matrices in cryptographic schemes but also broadens the scope of design options available for secure key generation. However, such keys introduce repetition in Cipher Hexagraphic Polyfunction transformations, potentially allowing plaintext recovery by third parties. This led to an updated prerequisite for choosing secret keys in Cipher Polygraphic Polyfunction systems involving $A_{6\times6}$ matrices.

While these studies focused solely on matrix-based cryptographic systems, matrices are not the only structures capable of encryption transformations. **Rhotrix**, an extension of matrices, provides greater structural flexibility, allowing for enhanced encryption schemes with improved security features. Unlike matrices, rhotrices can accommodate additional elements that disrupt linear predictability, thereby reducing vulnerability to known cryptographic attacks. Drawing inspiration from the nonlinear dynamics of biological Boolean networks [25–31] and the algebraic structure of transformation semigroups [32–36], this paper extends the concept of self-invertible encryption keys beyond traditional matrices to rhotrix structures, introducing rhotrix-based cryptographic transformations that exploit richer transformation behavior and enhanced state complexity. By leveraging rhotrix for Cipher Pentagraphic Polyfunction transformations, we aim to establish a more secure encryption framework that mitigates the weaknesses identified in matrix-based systems.

3 Result & Discussion

3.1 Solutions for $L_{5\times5}$ for a Diagonal Rhotrix $L_{5\times5}^{2} \equiv A_{5\times5} \pmod{N}$

We assume the encryption key $A_{5\times5} = \left\langle \begin{array}{ccccc} & & a_{11} & & \\ & a_{21} & c_{11} & a_{12} & \\ a_{31} & c_{21} & a_{22} & c_{12} & a_{13} \\ & a_{32} & c_{22} & a_{23} & \\ & & a_{33} & & \end{array} \right\rangle \pmod{N}$ and let

$L_{5\times5} = \left\langle \begin{array}{ccccc} & & a & & \\ & f & d & b & \\ k & i & g & e & c \\ & l & j & h & \\ & & m & & \end{array} \right\rangle \pmod{N}$, such that $L_{5\times5}^{2} \equiv A_{5\times5} \pmod{N}$. To get $L_{5\times5}$, we need to solve simultaneous equations as shown below.

$$a^2 + bf + ck \equiv a_{11} \pmod{N} \tag{8}$$

$$ab + bg + cl \equiv a_{12} \pmod{N} \tag{9}$$

$$ac + bh + cm \equiv a_{13} \pmod{N} \tag{10}$$

$$d^2 + ei \equiv c_{11} \pmod{N} \tag{11}$$

$$de + ej \equiv c_{12} \pmod{N} \tag{12}$$

$$fa + gf + hk \equiv a_{21} \pmod{N} \tag{13}$$

$$fb + g^2 + hl \equiv a_{22} \pmod{N} \tag{14}$$

$$fc + gh + hm \equiv a_{23} \pmod{N} \tag{15}$$

$$id + ji \equiv c_{21} \pmod{N} \tag{16}$$

$$ie + j^2 \equiv c_{22} \pmod{N} \tag{17}$$

$$ka + lf + mk \equiv a_{31} \pmod{N} \tag{18}$$

$$kb + lg + ml \equiv a_{32} \pmod{N} \tag{19}$$

$$kc + lh + m^2 \equiv a_{33} \pmod{N} \tag{20}$$

Proposition 3.1. *Let* $L_{5\times5} = \left\langle \begin{array}{ccccc} & & a & & \\ & f & d & b & \\ k & i & g & e & c \\ & l & j & h & \\ & & m & & \end{array} \right\rangle \pmod{N}$, *assuming that* b, c, f, h, k, *and* l *are all coprime with* N, *the solution for the diagonal rhotrix* $L^2_{3\times3} \pmod{N}$ *is given by:*

$$L_{5\times5} = \left\langle \begin{array}{ccccc} & & 2^{-1}\left(l^{-1}kb - lfk^{-1} - f^{-1}hk\right) & & \\ & f & -j & b & \\ k & i & g & e & c \\ & l & d & h & \\ & & m & & \end{array} \right\rangle \pmod{N}, \tag{21}$$

where $c \equiv l^{-1}f^{-1}hkb \pmod{N}$, $g \equiv 2^{-1}\left(-l^{-1}kb + lfk^{-1} - f^{-1}hk\right) \pmod{N}$, $d \equiv -j$ *and* $m \equiv 2^{-1}\left(-l^{-1}kb - lfk^{-1} + f^{-1}hk\right) \pmod{N}$.

Proof. Let $\left\langle \begin{array}{ccccc} & & a & & \\ & f & d & b & \\ k & i & g & e & c \\ & l & j & h & \\ & & m & & \end{array} \right\rangle^2 = \left\langle \begin{array}{ccccc} & & a^2+bf+ck & & \\ & 0 & d^2+ei & 0 & \\ 0 & 0 & fb+g^2+hl & 0 & 0 \\ & 0 & ie+j^2 & 0 & \\ & & kc+lh+m^2 & & \end{array} \right\rangle \pmod N$. Substituting $a_{12}=a_{13}=c_{12}=a_{21}=a_{23}=c_{21}=a_{31}=a_{32}=0$ into Equations (8)-(20).
From Equation (9),

$$b(a+g)+cl\equiv 0 \implies cl\equiv -b(a+g) \implies -b^{-1}cl\equiv a+g \mod N \ for\ b(N,1)=1 \quad (22)$$

from equation (10)

$$c(a+m)+bh\equiv 0 \implies bh\equiv -c(a+m) \implies -c^{-1}bh\equiv a+m \mod N \ for\ c(N,1)=1 \quad (23)$$

from equation (12)

$$de+ej\equiv 0 \implies e(d+j)\equiv 0 \implies d+j\equiv 0 \mod N \quad (24)$$

from equation (13)

$$f(a+g)+hk\equiv 0 \implies hk\equiv -f(a+g) \implies -f^{-1}hk\equiv a+g \mod N \ for\ f(N,1)=1 \quad (25)$$

from equation (15),

$$fc+h(g+m)\equiv 0 \implies fc\equiv -h(g+m) \implies -h^{-1}fc\equiv g+m \mod N \ for\ h(N,1)=1 \quad (26)$$

from equation (16)

$$id+ji\equiv 0 \implies i(d+j)\equiv 0 \implies d+j\equiv 0 \mod N \quad (27)$$

from equation (18)

$$k(a+m)+lf\equiv 0 \implies lf\equiv -k(a+m) \implies -k^{-1}lf\equiv a+m \mod N \ for\ k(N,1)=1 \quad (28)$$

from equation (19)

$$kb+l(g+m)\equiv 0 \implies kb\equiv -l(g+m) \implies -kbl^{-1}\equiv g+m \mod N \ for\ l(N,1)=1 \quad (29)$$

Equating equation (22) and equation (25)

$$b^{-1}cl\equiv f^{-1}hk \mod N \quad (30)$$

Equating equation (23) and equation (28)

$$c^{-1}bh\equiv k^{-1}lf \mod N \quad (31)$$

Equating equation (26) and equation (29)

$$h^{-1}fc\equiv kbl^{-1} \mod N \quad (32)$$

From equation (24) and (27)

$$d\equiv -j \quad \text{and} \quad e\equiv i\equiv 0 \mod N \quad (33)$$

Now from equation (30) − (32), we get;

$$c\equiv l^{-1}f^{-1}hkb \mod N \quad (34)$$

So substituting equation (34) into equation (22), gives

$$-f^{-1}hk \equiv a+g \implies a \equiv -g - f^{-1}hk \mod N \tag{35}$$

Substituting equation (34) into equation (26)

$$-l^{-1}kb \equiv g+m \implies g \equiv -l^{-1}kb - m \mod N \tag{36}$$

Substituting equation (34) into equation (23)

$$m \equiv -lfk^{-1} - a \mod N \tag{37}$$

So

$$a \equiv 2^{-1}\left(l^{-1}kb - lfk^{-1} - f^{-1}hk\right) \mod N \tag{38}$$

Then substituting equation (38) into equation (37)

$$m \equiv 2^{-1}\left(-l^{-1}kb - lfk^{-1} + f^{-1}hk\right) \mod N \tag{39}$$

Substituting equation (39) into equation (36)

$$g \equiv 2^{-1}\left(-l^{-1}kb + lfk^{-1} - f^{-1}hk\right) \mod N \tag{40}$$

□

3.2 Some Solutions $L_{5\times5}$ for a Symmetric Rhotrix $L_{5\times5}^2 \equiv A_{5\times5} \pmod N$

We investigate the properties of the key rhotrix $L_{5\times5}$ in our Cipher Pentagraphic Polyfunction system by examining the condition

$$L_{5\times5}^2 \equiv A_{5\times5} \pmod N,$$

where $A_{5\times5}$ is a symmetric rhotrix. This requirement ensures that the key exhibits self-invertible behavior, which is crucial for the decryption process. By ensuring the symmetry of $A_{5\times5}$ and the congruence relation modulo N, we establish a robust algebraic scheme that enhances the security of the encryption scheme.

Proposition 3.2. *Let* $L_{5\times5} = \left\langle \begin{array}{ccccc} & & a & & \\ & f & d & b & \\ k & i & g & e & c \\ & l & j & h & \\ & & m & & \end{array} \right\rangle \pmod N$ *and* $(b-f,N) = (c-k,N) = (h-l,N) = 1$. *Then* $L_{5\times5}$ *with* $a \equiv 2^{-1}\left((b-f)^{-1}(hk-cl) - (h-l)^{-1}(kb-fc) + (c-k)^{-1}(lf-bh)\right) \pmod N$, $g \equiv 2^{-1}\left((b-f)^{-1}(hk-cl) - (c-k)^{-1}(lf-bh) + (h-l)^{-1}(kb-fc)\right) \pmod N$, $d \equiv -j$ *and* $m \equiv 2^{-1}\left((c-k)^{-1}(lf-bh) - (b-f)^{-1}(hk-cl) + (h-l)^{-1}(kb-fc)\right) \pmod N$ *are solutions to a symmetric rhotrix* $L_{5\times5}^2 \pmod N$.

Proof. Let $\left\langle \begin{array}{ccccc} & & a & & \\ & f & d & b & \\ k & i & g & e & c \\ & l & j & h & \\ & & m & & \end{array} \right\rangle^2 = \left\langle \begin{array}{ccccc} & & a^2+bf+ck & & \\ & r & d^2+ei & r & \\ s & y & fb+g^2+hl & y & s \\ & t & ie+j^2 & t & \\ & & kc+lh+m^2 & & \end{array} \right\rangle \pmod N$. Where, $a_{12} = a_{21} = r$, $c_{12} = c_{21} = y$, $a_{13} = a_{31} = s$ and $a_{23} = a_{32} = t$, this gives;

$$ab + bg + cl \equiv r \pmod N \tag{41}$$

$$ac + bh + cm \equiv s \pmod{N} \tag{42}$$

$$de + ej \equiv y \pmod{N} \tag{43}$$

$$fa + gf + hk \equiv r \pmod{N} \tag{44}$$

$$fc + gh + hm \equiv t \pmod{N} \tag{45}$$

$$id + ji \equiv y \pmod{N} \tag{46}$$

$$ka + lf + mk \equiv s \pmod{N} \tag{47}$$

$$kb + lg + ml \equiv t \pmod{N} \tag{48}$$

Equating, Equation (41) and Equation (44), we get

$$b(a+g) + cl \equiv f(a+g) + hk \implies (b-f)(a+g) \equiv hk - cl \pmod{N} \tag{49}$$

Equating, Equation (42) and Equation (47),

$$c(a+m) + bh \equiv k(a+m) + lf \implies (c-k)(a+m) \equiv lf - bh \pmod{N} \tag{50}$$

Equating, Equation (43) and Equation (46),

$$e(d+j) \equiv i(d+j) \implies (e-i)(d+j) \equiv 0 \pmod{N} \tag{51}$$

Equating, Equation (45) and Equation (48),

$$h(g+m) + fc \equiv l(g+m) + kb \implies (h-l)(g+m) \equiv kb - fc \pmod{N} \tag{52}$$

From equation (49), we get;

$$a \equiv (b-f)^{-1}(hk - cl) - g \mod N \text{ for } (b-f, N) = 1 \tag{53}$$

From equation (50), we get;

$$m \equiv (c-k)^{-1}(lf - bh) - a \mod N \text{ for } (c-k, N) = 1 \tag{54}$$

From equation (51), we get;

$$\begin{aligned} d &\equiv -j \quad \text{and} \\ e &\equiv i \end{aligned} \tag{55}$$

From equation (52), we get;

$$g \equiv (h-l)^{-1}(kb - fc) - m \mod N \text{ for } (h-l, N) = 1 \tag{56}$$

Therefore;

$$a \equiv 2^{-1}\left((b-f)^{-1}(hk - cl) - (h-l)^{-1}(kb - fc) + (c-k)^{-1}(lf - bh)\right) \mod N \tag{57}$$

$$m \equiv 2^{-1}\left((c-k)^{-1}(lf - bh) - (b-f)^{-1}(hk - cl) + (h-l)^{-1}(kb - fc)\right) \mod N \tag{58}$$

$$g \equiv 2^{-1}\left((b-f)^{-1}(hk - cl) - (c-k)^{-1}(lf - bh) + (h-l)^{-1}(kb - fc)\right) \mod N \tag{59}$$

Case 1

From Equations (57)-(59), we impose the conditions, $b-f=1, \quad h-l=1, \quad c-k=1$. This immediately gives us, $b=1+f, \quad h=1+l, \quad c=1+k$. Under these constraints, the system simplifies considerably. For this particular case, the resulting expression becomes
For $a \equiv 2^{-1}\left((b-f)^{-1}(hk-cl)-(h-l)^{-1}(kb-fc)+(c-k)^{-1}(lf-bh)\right)$ given $b-f=1, h-l=1$, and $c-k=1$. This simplifies the equation to:

$$a \equiv 2^{-1}(hk-cl-kb+fc+lf-bh)$$

Express b, h, and c in terms of f, l, and k respectively: $b=f+1$, $h=l+1$, $c=k+1$
Substitute these expressions into the equation:

$$a \equiv 2^{-1}\left((l+1)k-(k+1)l-k(f+1)+f(k+1)+lf-(f+1)(l+1)\right)$$

Expand the terms:

$$a \equiv 2^{-1}(lk+k-kl-l-kf-k+fk+f+lf-(fl+f+l+1))$$

Simplify by canceling terms:

$$a \equiv 2^{-1}(lk-kl+k-k-l-l-kf+fk+f-f+lf-fl-1)$$

Notice that $lk-kl=0$, $k-k=0$, $f-f=0$, and $lf-fl=0$. This simplifies to:

$$a \equiv 2^{-1}(-2l-kf+fk-1)$$

Since $-kf+fk=0$, the expression further simplifies to:

$$a \equiv \frac{1}{2}(-2l-1)$$

Distribute the $\frac{1}{2}$:

$$a \equiv -l-2^{-1}$$

Similarly simplification would also give;

$$g \equiv k+2^{-1}$$

and

$$m \equiv -f-2^{-1}$$

Corollary 3.3. *Let* $(2,N)=(4,N)=1$. *If* $L_{5\times 5}=\left\langle \begin{array}{ccccc} & & -l-2^{-1} & & \\ & f & -j & 1+f & \\ k & i & k+2^{-1} & i & 1+k \\ & l & -j & 1+l & \\ & & -f-2^{-1} & & \end{array} \right\rangle \pmod N$,

then $L_{5\times 5}^2=\left\langle \begin{array}{ccccc} & & a_{11} & & \\ & a_{12} & c_{11} & a_{12} & \\ -a_{12} & c_{12} & a_{11} & c_{12} & -a_{12} \\ & a_{12} & c_{11} & a_{12} & \\ & & a_{11} & & \end{array} \right\rangle \pmod N$ *is symmetric where* $a_{11} \equiv l^2+f^2+k^2+l+f+k+4^{-1} \pmod N$
and $a_{12} \equiv k(1+f+l)-lf \pmod N$.

Proof.

Let $L_{5\times5} = \left\langle \begin{array}{ccccc} & & -l-2^{-1} & & \\ & f & -j & 1+f & \\ k & i & k+2^{-1} & i & 1+k \\ & l & -j & 1+l & \\ & & -f-2^{-1} & & \end{array} \right\rangle$ and $L^2_{5\times5} = \left\langle \begin{array}{ccccc} & & a_{11} & & \\ & a_{21} & c_{11} & a_{12} & \\ a_{31} & c_{21} & a_{22} & c_{12} & a_{13} \\ & a_{32} & c_{22} & a_{23} & \\ & & a_{33} & & \end{array} \right\rangle$ (mod N). We need to compute $L^2_{5\times5}$:

$$L^2_{5\times5} = L_{5\times5} \cdot L_{5\times5}$$

With step-by-step rhotrix Multiplication:

$$a_{11} \equiv (-l-2^{-1})(-l-2^{-1}) + (1+f)(f) + (1+k)(k) = l^2 + l + \frac{1}{4} + f^2 + f + k^2 + k$$

$$a_{11} \equiv l^2 + f^2 + k^2 + l + f + k + 4^{-1} \mod N$$

$$\begin{aligned} a_{12} &\equiv (-l-2^{-1})(1+f) + (1+f)(k+2^{-1}) + (1+k)(l) \\ &= -l - lf - \frac{1}{2} - \frac{f}{2} + k + kf + \frac{1}{2} + \frac{f}{2} + l + kl \\ &= kf + kl - lf + k \end{aligned}$$

$$a_{12} \equiv k(1+f+l) - lf \mod N$$

$$\begin{aligned} a_{13} &\equiv (-l-2^{-1})(1+k) + (1+f)(1+l) + (1+k)(-f-2^{-1}) \\ &= -l - lk - \frac{1}{2} - \frac{k}{2} + 1 + f + l + lf - f - kf - \frac{1}{2} - \frac{k}{2} \\ &= lf - lk - kf - k \end{aligned}$$

$$a_{13} \equiv lf - lk - kf - k \mod N$$

$$c_{11} \equiv j^2 + i^2 \mod N$$

$$c_{12} \equiv -2ji \mod N$$

$$\begin{aligned} a_{21} &\equiv (f)(-l-2^{-1}) + (k+2^{-1})(f) + (1+l)(k) \\ &= -lf - \frac{f}{2} + kf + \frac{f}{2} + k + kl = kf - lf + k + kl \end{aligned}$$

$$a_{21} \equiv k(1+f+l) - lf \mod N \quad (\text{Notice } a_{21} \equiv a_{12})$$

$$\begin{aligned} a_{22} &\equiv (f)(1+f) + (k+2^{-1})(k+2^{-1}) + (1+l)(l) \\ &= f + f^2 + k^2 + k + \frac{1}{4} + l + l^2 = f^2 + k^2 + l^2 + f + k + l + 4^{-1} \end{aligned}$$

$$a_{22} \equiv f^2 + k^2 + l^2 + f + k + l + 4^{-1} \mod N \quad (\text{Notice } a_{22} \equiv a_{11})$$

$$\begin{aligned} a_{23} &\equiv (f)(1+k) + (k+2^{-1})(1+l) + (1+l)(-f-2^{-1}) \\ &= f + fk + k + kl + \frac{1}{2} + \frac{l}{2} - f - lf - \frac{1}{2} - \frac{l}{2} = fk + k + kl - lf \end{aligned}$$

$$a_{23} \equiv fk + k + kl - lf \mod N$$

$$c_{21} \equiv i^2 + j^2 \mod N \quad (\text{Notice } c_{21} \equiv c_{12})$$

$$c_{22} \equiv -2ij \mod N \quad (\text{Notice } c_{22} \equiv c_{11})$$

$$a_{31} \equiv (k)(-l-2^{-1}) + (l)(f) + (-f-2^{-1})(k)$$
$$= -kl - \frac{k}{2} + lf - fk - \frac{k}{2} = lf - kl - fk - k$$
$$a_{31} \equiv lf - kl - fk - k \mod N \quad (\text{Notice } a_{31} \equiv a_{13})$$

$$a_{32} \equiv (k)(1+f) + (l)(k+2^{-1}) + (-f-2^{-1})(l)$$
$$= k + kf + kl + \frac{l}{2} - fl - \frac{l}{2} = k + kf + kl - fl$$
$$a_{32} \equiv k + kf + kl - fl \mod N \quad (\text{Notice } a_{32} \equiv a_{23})$$

$$a_{33} \equiv (k)(1+k) + (l)(1+l) + (-f-2^{-1})(-f-2^{-1})$$
$$= k + k^2 + l + l^2 + f^2 + f + \frac{1}{4}$$
$$a_{33} \equiv k^2 + l^2 + f^2 + k + l + f + 4^{-1} \mod N \quad (\text{Notice } a_{33} \equiv a_{11})$$

Case 2

From Equations (57)–(59), we impose the conditions $b - f = 1, \quad h - l = -1, \quad c - k = -1$. These yield, $b = 1 + f, \quad h = -1 + l, \quad c = -1 + k$. Under these constraints, the system simplifies, we reach the following conclusion:

Corollary 3.4. *Assume* $(2, N) = (4, N) = 1$, *meaning that both 2 and 4 are relatively prime to* N. *If*

$$L_{5\times5} = \left\langle \begin{array}{ccccc} & & l-2^{-1} & & \\ & f & -j & 1+f & \\ k & i & 2^{-1}-k & i & k-1 \\ & l & -j & l-1 & \\ & & -f-2^{-1} & & \end{array} \right\rangle \pmod N, \text{ then } L_{5\times5}^2 = \left\langle \begin{array}{ccccc} & & a_{11} & & \\ & a_{12} & c_{11} & a_{12} & \\ a_{12} & c_{12} & a_{11} & c_{12} & a_{12} \\ & -a_{12} & c_{11} & -a_{12} & \\ & & a_{11} & & \end{array} \right\rangle$$

$\pmod N$ *where* $a_{11} \equiv l^2 + f^2 + k^2 - l + f - k + 4^{-1} \pmod N$
and $a_{12} \equiv k(l - f - 1) + lf \pmod N$.

Proof. The technique of proofing this is similar to that of Corollary 1

Case 3

From Equations (57)–(59), we impose the conditions, $b - f = -1, \quad h - l = -1, \quad c - k = 1$. These conditions immediately imply that, $b = f - 1, \quad h = l - 1, \quad c = 1 + k$. Under these constraints, the system simplifies, and we obtain the following result:

Corollary 3.5. *Let* $(2, N) = (4, N) = 1$. *If* $L_{5\times5} = \left\langle \begin{array}{ccccc} & & l-2^{-1} & & \\ & f & -j & f-1 & \\ k & i & 2^{-1}+k & i & 1+k \\ & l & -j & l-1 & \\ & & f-2^{-1} & & \end{array} \right\rangle \pmod N$,

then $L_{5\times5}^2 = \left\langle \begin{array}{ccccc} & & a_{11} & & \\ & a_{12} & c_{11} & a_{12} & \\ a_{12} & c_{12} & a_{11} & c_{12} & a_{12} \\ & a_{12} & c_{11} & a_{12} & \\ & & a_{11} & & \end{array} \right\rangle \pmod N$ *where* $a_{11} \equiv l^2 + f^2 + k^2 - l - f + k + 4^{-1}$

$(\text{mod } N)$
and $a_{12} \equiv k(l+f-1)+lf \pmod N$.

Proof. The technique of proofing this is similar to that of Corollary 1

Case 4

Based on Equations (57)–(59), we impose the conditions $b-f=-1$, $h-l=1$, and $c-k=-1$. These lead directly to the relationships, $b=f-1, \quad h=l+1, \quad c=k-1$. Under these specific constraints, the system simplifies considerably. In this case, we arrive at the following conclusion:

Corollary 3.6. *Assume* $(2,N)=(4,N)=1$, *meaning that both 2 and 4 are relatively prime to* N. *If*
$L_{5\times5}=\left\langle \begin{array}{ccccc} & & -l-2^{-1} & & \\ & f & -j & f-1 & \\ k & i & 2^{-1}-k & i & k-1 \\ & l & -j & 1+l & \\ & & f-2^{-1} & & \end{array} \right\rangle \pmod N$, *then* $L_{5\times5}^2=\left\langle \begin{array}{ccccc} & & a_{11} & & \\ & a_{12} & c_{11} & a_{12} & \\ -a_{12} & c_{12} & a_{11} & c_{12} & -a_{12} \\ & -a_{12} & c_{11} & -a_{12} & \\ & & a_{11} & & \end{array} \right\rangle$
$(\text{mod } N)$ *where* $a_{11} \equiv l^2+f^2+k^2+l-f-k+4^{-1} \pmod N$
and $a_{12} \equiv k(l+f-1)+lf \pmod N$.

Proof. The technique of proofing this is similar to that of Corollary 1 □
We now examine the defining characteristics of the rhotrix $L_{5\times5}$, which satisfies the condition $L_{5\times5}^2 \equiv A_{5\times5} \pmod N$, where $A_{5\times5}$ is a symmetric rhotrix. By substituting the values $d=j=1$ and $c=h=e=i=0$ into Equations (57)–(59), we derive the following outcome.

Corollary 3.7. *Let* $(2,N)=(4,N)=(l,N)=(k,N)=1$. *If* $L_{5\times5}=\left\langle \begin{array}{ccccc} & & 2^{-1}(kbl^{-1}-lfk^{-1}) & & \\ & f & 1 & & b \\ k & 0 & -2^{-1}(kbl^{-1}-lfk^{-1}) & 0 & 0 \\ & l & 1 & & 0 \\ & & 2^{-1}(-lfk^{-1}-kbl^{-1}) & & \end{array} \right\rangle$
$(\text{mod } N)$ *then,* $L_{5\times5}^2 \equiv (4^{-1}(k^2b^2l^{-2}+l^2f^2k^{-2})+2^{-1}bf)I_{5\times5} \pmod N$, *where* $I_{5\times5} \equiv \left\langle \begin{array}{ccccc} & & 1 & & \\ & 0 & 1 & 0 & \\ 0 & 0 & 1 & 0 & 0 \\ & 0 & 1 & 0 & \\ & & 1 & & \end{array} \right\rangle$

Proof.
Let $L_{5\times5}=\left\langle \begin{array}{ccccc} & & 2^{-1}(kbl^{-1}-lfk^{-1}) & & \\ & f & 1 & & b \\ k & 0 & -2^{-1}(kbl^{-1}-lfk^{-1}) & 0 & 0 \\ & l & 1 & & 0 \\ & & 2^{-1}(-lfk^{-1}-kbl^{-1}) & & \end{array} \right\rangle \pmod N$. Then, $L_{5\times5}^2=\left\langle \begin{array}{ccccc} & & a_{11} & & \\ & a_{21} & c_{11} & a_{12} & \\ a_{31} & c_{21} & a_{22} & c_{12} & a_{13} \\ & a_{32} & c_{22} & a_{23} & \\ & & a_{33} & & \end{array} \right\rangle$
$(\text{mod } N)$, where

$$\begin{aligned} a_{11} \equiv 4^{-1}(kbl^{-1}-lfk^{-1})^2+bf \pmod N &\equiv 4^{-1}(k^2b^2l^{-2}+l^2f^2k^{-2})-2^{-1}bf+bf \pmod N \\ &\equiv 4^{-1}(k^2b^2l^{-2}+l^2f^2k^{-2})+2^{-1}bf \pmod N, \\ a_{12} \equiv 2^{-1}b(kbl^{-1}-lfk^{-1})+2^{-1}b(lfk^{-1}-kbl^{-1}) \equiv 0 \pmod N, \\ a_{13} \equiv 0 \pmod N, \end{aligned}$$

$$\begin{aligned} c_{11} &\equiv 1 \pmod N, \\ c_{12} &\equiv 0 \pmod N, \end{aligned}$$

$$a_{21} \equiv 2^{-1}f(kbl^{-1} - lfk^{-1}) + 2^{-1}(lfk^{-1} - kbl^{-1})f \equiv 0 \pmod{N},$$

$$a_{22} \equiv 4^{-1}(lfk^{-1} - kbl^{-1})^2 + bf \equiv a_{11} \pmod{N},$$
$$a_{23} \equiv 0 \pmod{N},$$

$$c_{21} \equiv 0 \pmod{N},$$
$$c_{22} \equiv 1 \pmod{N},$$

$$a_{31} \equiv 2^{-1}k(kbl^{-1} - lfk^{-1}) + lf + 2^{-1}(-lfk^{-1} - kbl^{-1})k \equiv 0 \pmod{N},$$

$$a_{32} \equiv kb + 2^{-1}l(lfk^{-1} - kbl^{-1}) + 2^{-1}(-lfk^{-1} - kbl^{-1})l \equiv 0 \pmod{N}$$

and

$$a_{33} \equiv 4^{-1}(-lfk^{-1} - kbl^{-1})^2 \pmod{N}$$
$$\equiv 4^{-1}(k^2b^2l^{-2} + 2bf + l^2f^2k^{-2}) \pmod{N} \equiv 4^{-1}(k^2b^2l^{-2} + l^2f^2k^{-2}) + 2^{-1}bf \equiv a_{11} \pmod{N}.$$

We can clearly see that $L_{5\times5}^2 \equiv (4^{-1}(k^2b^2l^{-2} + l^2f^2k^{-2}) + 2^{-1}bf)I_{5\times5} \pmod{N}$. □ Next, we explore the defining properties of the matrix $L_{5\times5}$, which satisfies the condition $L_{5\times5}^2 \equiv A_{5\times5} \pmod{N}$, where $A_{5\times5}$ is a symmetric rhotrix. By substituting the values $d = j = 1$ and $b = c = h = e = i = 0$ into Equations (57)–(59), we obtain the following result.

Corollary 3.8. *Let* $(2, N) = (k, N) = 1$. *If* $L_{5\times5} = \left\langle \begin{matrix} & & -2^{-1}lfk^{-1} & & \\ & f & 1 & 0 & \\ k & 0 & 2^{-1}lfk^{-1} & 0 & 0 \\ & l & 1 & 0 & \\ & & -2^{-1}lfk^{-1} & & \end{matrix} \right\rangle \pmod{N}$ *then,*

$L_{5\times5}^2 \equiv 4^{-1}l^2f^2k^{-2}I_{5\times5} \pmod{N}$, *where* $I_{5\times5} \equiv \left\langle \begin{matrix} & & 1 & & \\ & 0 & 1 & 0 & \\ 0 & 0 & 1 & 0 & 0 \\ & 0 & 1 & 0 & \\ & & 1 & & \end{matrix} \right\rangle$

Proof. The method used to prove this result is analogous to the one applied in Corollary 5. □
Finally, analyze the essential properties of the matrix $L_{5\times5}$, which satisfies the condition $L_{5\times5}^2 \equiv A_{5\times5} \pmod{N}$, where $A_{5\times5}$ is a symmetric rhotrix. By substituting the values $d = j = 1$ and $f = k = l = e = i = 0$ into Equations (57)–(59), we arrive at the following result.

Corollary 3.9. *Let* $(c, m) = (2, N) = 1$. *If* $L_{5\times5} = \left\langle \begin{matrix} & & -2^{-1}bhc^{-1} & & \\ & 0 & 1 & b & \\ 0 & 0 & 2^{-1}bhc^{-1} & 0 & c \\ & 0 & 1 & h & \\ & & -2^{-1}bhc^{-1} & & \end{matrix} \right\rangle \pmod{N}$ *then,*

$L_{5\times5}^2 \equiv 4^{-1}b^2h^2c^{-2}I_{5\times5} \pmod{N}$, *where* $I_{5\times5} \equiv \left\langle \begin{matrix} & & 1 & & \\ & 0 & 1 & 0 & \\ 0 & 0 & 1 & 0 & 0 \\ & 0 & 1 & 0 & \\ & & 1 & & \end{matrix} \right\rangle$

Proof. The method used to prove this result is analogous to the one applied in Corollary 5. □

3.3 Effect of the Self-Invertible Rhotrix Key on the Cipher Pentgraphic Polyfunction

The Cipher Pentagraphic Polyfunction Transformation is developed from the theorem outlined below.

Theorem 3.10. *Consider the transformation as defined in Definition 1. If the* 5×5 *rhotrix* $A_{5\times5}$ *has a nonzero determinant and meets the condition* $\gcd(|A_{5\times5}|, N) = 1$*, then the system* $P_{5\times5}$ *yields a unique solution. The decryption algorithms are detailed below:*

$$\begin{aligned}
C_{5\times5}^{(t-1)} &\equiv A_{5\times5}^{-1} C_{5\times5}^{(t)} \pmod N,\\
C_{5\times5}^{(t-2)} &\equiv A_{5\times5}^{-1} C_{5\times5}^{(t-1)} \pmod N,\\
&\vdots\\
C_{5\times5}^{(2)} &\equiv A_{5\times5}^{-1} C_{5\times5}^{(3)} \pmod N,\\
C_{5\times5}^{(1)} &\equiv A_{5\times5}^{-1} C_{5\times5}^{(2)} \pmod N,\\
P_{5\times5} &\equiv A_{5\times5}^{-1} C_{5\times5}^{(1)} \pmod N
\end{aligned}$$

Here, $A_{5\times5}^{-1}$ *represents the inverse rhotrix of* $A_{5\times5}$*, which serves as the key for decryption.*

Proof. Examine the Cipher Pentagraphic Polyfunction transformations as outlined below:

$$\begin{aligned}
C_{5\times5}^{(1)} &\equiv A_{5\times5} P_{5\times5} \pmod N,\\
C_{5\times5}^{(2)} &\equiv A_{5\times5} C_{5\times5}^{(1)} \pmod N,\\
C_{5\times5}^{(3)} &\equiv A_{5\times5} C_{5\times5}^{(2)} \pmod N,\\
&\vdots\\
C_{5\times5}^{(t-1)} &\equiv A_{5\times5} C_{5\times5}^{(t-2)} \pmod N,\\
C_{5\times5}^{(t)} &\equiv A_{5\times5} C_{5\times5}^{(t-1)} \pmod N.
\end{aligned}$$

There exist the inverse of $A_{5\times5}$ such that $A_{5\times5}A_{5\times5}^{-1} \equiv I \pmod N$, when $|A_{5\times5}| \neq 0$. So

$$A_{5\times5}^{-1} C_{5\times5}^{(t)} \equiv A_{5\times5}^{-1} A_{5\times5} C_{5\times5}^{(t-1)} \equiv C_{5\times5}^{(t-1)} \pmod N, \tag{60}$$
$$A_{5\times5}^{-1} C_{5\times5}^{(t-1)} \equiv A_{5\times5}^{-1} A_{5\times5} C_{5\times5}^{(t-2)} \equiv C_{5\times5}^{(t-2)} \pmod N, \tag{61}$$
$$\vdots$$
$$A_{5\times5}^{-1} C_{5\times5}^{(3)} \equiv A_{5\times5}^{-1} A_{5\times5} C_{5\times5}^{(2)} \equiv C_{5\times5}^{(2)} \pmod N, \tag{62}$$
$$A_{5\times5}^{-1} C_{5\times5}^{(2)} \equiv A_{5\times5}^{-1} A_{5\times5} C_{5\times5}^{(1)} \equiv C_{5\times5}^{(1)} \pmod N, \tag{63}$$
$$A_{5\times5}^{-1} C_{5\times5}^{(1)} \equiv A_{5\times5}^{-1} A_{5\times5} P_{5\times5} \equiv P_{5\times5} \pmod N, \tag{64}$$

and

$$(adj A_{5\times5}) C_{5\times5}^{(t)} \equiv |A_{5\times5}| C_{5\times5}^{(t-1)} \pmod N, \tag{65}$$
$$(adj A_{5\times5}) C_{5\times5}^{(t-1)} \equiv |A_{5\times5}| C_{5\times5}^{(t-2)} \pmod N. \tag{66}$$

$$(adj A_{5\times5}) C_{5\times5}^{(3)} \equiv |A_{5\times5}| C_{5\times5}^{(2)} \pmod N, \tag{67}$$
$$(adj A_{5\times5}) C_{5\times5}^{(2)} \equiv |A_{5\times5}| C_{5\times5}^{(1)} \pmod N, \tag{68}$$
$$(adj A_{5\times5}) C_{5\times5}^{(1)} \equiv |A_{5\times5}| P_{5\times5} \pmod N. \tag{69}$$

From Equations (60)–(64), we get the decryption algorithm as follows:

$$\begin{aligned}
C_{5\times5}^{(t-1)} &\equiv A_{5\times5}^{-1}C_{5\times5}^{(t)} \pmod N,\\
C_{5\times5}^{(t-2)} &\equiv A_{5\times5}^{-1}C_{5\times5}^{(t-1)} \pmod N,\\
&\vdots\\
C_{5\times5}^{(2)} &\equiv A_{5\times5}^{-1}C_{5\times5}^{(3)} \pmod N,\\
C_{5\times5}^{(1)} &\equiv A_{5\times5}^{-1}C_{5\times5}^{(2)} \pmod N,\\
P_{5\times5} &\equiv A_{5\times5}^{-1}C_{5\times5}^{(1)} \pmod N.
\end{aligned}$$

From Equations (65)–(69), if the condition $\gcd(|A_{5\times5}|, N) = 1$ holds, then the system $P_{5\times5}$ admits unique solutions. This completes the proof.

In Theorem 1, a cyclic process emerges (specifically, $C_{5\times5}^{(t)} \equiv P_{5\times5} \pmod N$) when $A_{5\times5}^{t} \equiv I \pmod N$, where I represents the identity rhotrix. The sender can continue to encrypt the plaintext up to the $(t-1)^{\text{th}}$ transformation to ensure the confidentiality of the message. This differs in effect when we consider

$$A_{5\times5} = \left\langle \begin{bmatrix} L_{3\times3} & (I - L_{3\times3})k \\ (I + L_{3\times3})k^{-1} & -L_{3\times3} \end{bmatrix}, \begin{bmatrix} L_{2\times2} & (I - L_{2\times2})k \\ (I + L_{2\times2})k^{-1} & -L_{2\times2} \end{bmatrix} \right\rangle.$$

The following demonstrates the application of this key. Naturally, cryptographic applications benefit from longer transformations that map plaintext to ciphertext, as they enhance security. We begin by exploring the ciphertext patterns that emerge after applying only a few transformations. Assume that the plaintext values are organized in a 5×5 rhotrix, $P_{5\times5}$. We select any generated self-invertible rhotrix $L_{5\times5}$. Before proceeding with the encryption process, it is essential to ensure that the chosen secret key meets the criteria outlined in Theorem 1, specifically that $|L_{5\times5}| \equiv 1 \pmod N$. Thus, we have $(|L_{5\times5}|, N) = 1$. The encryption process then follows:

$$\begin{aligned}
C_{5\times5}^{(1)} &\equiv L_{5\times5}P_{5\times5} \pmod N,\\
C_{5\times5}^{(2)} &\equiv L_{5\times5}C_{5\times5}^{(1)} \equiv P_{5\times5} \pmod N,\\
C_{5\times5}^{(3)} &\equiv L_{5\times5}C_{5\times5}^{(2)} \equiv C_{5\times5}^{(1)} \pmod N,\\
C_{5\times5}^{(4)} &\equiv L_{5\times5}C_{5\times5}^{(3)} \equiv P_{5\times5} \pmod N,\\
&\vdots
\end{aligned}$$

The process continues such that $C_{5\times5}^{(2z)} \equiv P_{5\times5} \pmod N$ and $C_{5\times5}^{(2z-1)} \equiv P_{5\times5} \pmod N$ for $z \in \mathbb{Z}^+$. This occurs due to the fact that $L_{5\times5}^{2} \equiv I \pmod N$. Consequently, the transformation following $C_{5\times5}^{(1)}$ is unnecessary.

We now explore the conditions that $A_{5\times5}$ must satisfy in Theorem 1. For the third transformation to effectively convert plaintext into ciphertext, it is essential to ensure that the condition $A_{5\times5}A_{5\times5}A_{5\times5} \not\equiv I \pmod N$ holds, where I represents the identity rhotrix. Consequently, all configurations of self-invertible rhotrices $(L_{5\times5})$ discussed in Sections 3.1 and 3.2 should be excluded from the Cipher Pentagraphic Polyfunction system prior to the implementation of $L_{5\times5}$. This measure can significantly enhance the security of the ciphered message.

4 Conclusion

This study has successfully extended the conventional matrix-based cryptographic techniques to a more robust scheme using rhotrix structures. By employing self-invertible rhotrix keys, we have addressed key limitations of matrix-based encryption, such as predictable transformations and vulnerability to

known attacks. In Sections 3.1 and 3.2, we rigorously analyzed the structural properties of self-invertible rhotrices, utilizing **two propositions and seven corollaries** to determine distinct patterns of self-invertible rhotrix keys from the equation:

$$L_{5\times5}^2 \equiv A_{5\times5} \pmod{N}$$

where $A_{5\times5}$ is a diagonal and symmetric rhotrix. Our findings demonstrate that rhotrix-based cryptographic transformations introduce greater complexity, reducing the risk of key predictability and enhancing overall security. Compared to conventional matrix encryption, rhotrix-based transformations offer improved key diversity, making decryption by unauthorized parties more computationally challenging. The application of these self-invertible rhotrix keys to **Cipher Pentagraphic Polyfunction transformations** establishes a novel approach to polygraphic encryption, ensuring greater resistance to cryptanalysis techniques that exploit algebraic vulnerabilities in matrix systems.

Future work may explore extending rhotrix-based cryptography to higher-dimensional structures and integrating it with modern cryptographic algorithms to further strengthen data security in digital communications.

References

[1] Panigrahy, K., Acharya, B., and Jena, D. (2008). Image encryption using self-invertible key matrix of hill cipher algorithm. pages 1–4.

[2] Asbullah, M. and Ariffin, M. (2019). Another proof of wiener's short secret exponent. *Malaysian Journal of Science*, pages 67–73.

[3] Rivest, R., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126.

[4] Atanassov, K. T. and Shannon, A. G. (1998). Matrix-tertions and matrix-noitrets: Exercise for mathematical enrichment. *International Education in Science and Technology*, 29(6):898–903.

[5] Ajibade, A. O. (2003). The concept of rhotrix in mathematical enrichment. *International Journal of Mathematical Education in Science and Technology*, 34:175–179.

[6] Mohammed, A. (2011). *Theoretical Development and Application of Rhotrices*. PhD thesis, University of Ilorin, Ilorin, Kwara State, Nigeria.

[7] Ezugwu, E. A., Sani, B., and Junaidu, B. S. (2011). The concept of heart-oriented rhotrix multiplication. *Global Journal of Science Frontier Research*, 11(2):35–46.

[8] Sani, B. (2004). An alternative method for multiplication of rhotrices. *International Journal of Mathematical Education in Science and Technology*, 35:777–781.

[9] Ndubuisi, R. U., Abubakar, R. B., Araka, N. N., and Ugbene, I. J. (2022). The concept of rhotrix type a semigroups. *Journal of Mathematics and Computer Science*, 12. Article ID.

[10] Yunos, F. (2001). *Beberapa Penggunaan Teori Nombor Dalam Kriptografi*. PhD thesis, University Putra Malaysia, Serdang, Malaysia.

[11] Yunos, F., Said, M. R. M., and Atan, K. A. M. (2001). Transformasi polifungsi saifer digrafik bermodulo n1 dalam sistem kriptografi. In *Proceeding Simposium Kebangsaan Sains Matematik ke-9*, pages 88–95, Selangor, Malaysia. Persatuan Sains Matematik Malaysia and Institut Statistik Malaysia and Pusat Pengajian Sains Matematik, Universiti Kebangsaan Malaysia.

[12] Yunos, F., Atan, K. A. M., and Said, M. R. M. (2002). Transformasi polifungsi luc dalam sistem kriptografi. *J. Teknol.*, 37:21–38.

[13] Reddy, L. S. (2012). A new modal of hill cipher using non–quadratic residues. *International Journal of Soft Computing and Engineering*, 10:73–74.

[14] Acharya, B., Rath, G. S., Patra, S. K., and Panigrahy, S. K. (2007). Novel methods of generating self-invertible matrix for hill cipher algorithm. *International Journal of Security*, 1:14–21.

[15] Hill, L. S. (1929). Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, 36(6).

[16] Rosen, K. H. (1987). *Elementary Number Theory and Its Applications (Sixth Edition)*. Addison-Wesley, Boston, MA, USA.

[17] Overbey, J., Traves, W., and Wojdylo, J. (2005). On the keyspace of the hill cipher. *Cryptologia*, 29(1):59–72.

[18] Mahapatra, A. and Dash, R. (2007). Data encryption and decryption by using hill cipher technique and self repetitive matrix.

[19] Lohcwat, D., Suleiman, E., Markus, S., and Yakubu, D. G. (2023). Construction of cryptographic scheme of finite field using logical operators on rhotrices. In *Science Forum (Journal of Pure and Applied Sciences)*, volume 23, pages 12–20.

[20] Yakubu, D. G., Mathias, L. B., Lucy, B. G., and Lohcwat, D. (2022). A secured cryptographic technique using rhotrices in polygraphic cipher systems. *Science Forum: Journal of Pure and Applied Sciences*, 22(1):35–42.

[21] Yakubu, D. G., Mathias, L. B., Lucy, B. G., and Lohcwat, D. (2018). Extension of affine hill cipher using rhotrices in the polyalphabetic cipher systems. *Abacus: Journal of Mathematics Association of Nigeria*, 45(1):273–284.

[22] Tudunkaya, S. M., Usaini, S., Yakubu, D. G., Mathias, L. B., Lucy, B. G., and Lohcwat, D. (2020). Rhotrix-modules and the multi-cipher hill ciphers. *Nigerian Mathematical Society Journal*, 39(2):269–285.

[23] Yunos, F., Chin, L. S., and Said, M. R. M. (2016). Effect of self-invertible matrix on cipher tetragraphic trifunction. In *AIP Proceeding SKSM25*, Melville, NY, USA. Persatuan Sains Matematik Malaysia and AIP Publishing.

[24] Ching, S. L. P. and Yunos, F. (2019). Effect of self-invertible matrix on cipher hexagraphic polyfunction. *Cryptography*, 3(2):15.

[25] Emunefe, F. G., & Ugbene, I. J. (2024). Jukes-Cantor correction for phylogenetic tree reconstruction. *bioRxiv*. https://doi.org/10.1101/2024.07.30.605767

[26] Osanakpa, R. O., & Ugbene, I. J. (2025). Modeling meiotic rearrangements: Using dynamic programming to elucidate the role of DNA alignments in ciliate reproduction. *FUPRE Journal of Scientific and Industrial Research*, 9(1), 01-13.

[27] Kayoh, C. O., & Ugbene, I. J. (2023). Towards mechanism-based interventions for auxin signaling: Application of algebraic edge control to a Boolean network model. *International Journal of Mathematical Analysis and Modelling*, 6(2).

[28] Ugbene, J. I., & Utoyo, T. O. (2024). Switching stomatal aperture dynamics through computationally algebraic node control. *FUPRE Journal of Scientific and Industrial Research*, 8(1), 136-144.

[29] Ugbene, I. J., & Agwemuria, R. O. (2024). Identifying control targets for regulating mild cognitive impairment using reduced computational models of a life kinetic network. *FUPRE Journal of Scientific and Industrial Research*, 8(1), 23-38.

[30] Ugbene, I. J., & Utoyo, T. O. (2024). Determining synchronously updated fixed points and attractors in a prototype Boolean gene regulation model of diphtheria pathogenesis. *Open Journal of Mathematical Sciences*, 8, 167-184. https://doi.org/10.30538/oms2024.0234

[31] Ugbene, I. J., & Ajuremisan, I. S. (2025). State space analysis of diphtheria pathogenesis using semi-tensor products and permutation methods. *Network Biology*, 15(4), 123-149.

[32] Ugbene, I. J., & Makanjuola, S. O. (2012). On the number of conjugacy classes in the injective order-preserving transformation semigroup. *Icastor Journal of Mathematical Sciences*, 6(1).

[33] Ugbene, I. J., Makanjuola, S. O., & Eze, E. O. (2013). On the number of conjugacy classes in the injective order-decreasing transformation semigroup. *Image*, 1.

[34] Ugbene, I. J., & Mbah, M. A. (2015). On the combinatorial properties of nilpotent and idempotent conjugacy classes of the injective order-decreasing transformation semigroup. *FULafia Journal of Science and Technology*, 1(1), 91-94.

[35] Ugbene, I. J., Bakare, G. N., & Ibrahim, G. R. (2019). Conjugacy classes of the order-preserving and order-decreasing partial one-to-one transformation semigroups. *FUTMINA*.

[36] Ugbene, I. J., Ogundele, S. O., & Ndubuisi, R. U. (2022). Digraph of the full transformation semigroup. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(8), 2457-2465.