Applied Mathematics and Computational Intelligence
Volume 12, No. 1, Apr 2023 [70 − 86]

Solution of $L^2 = A$ Matrix to Generate Involutory Matrices for Cipher Trigraphic Polyfunction

Faridah Yunos[1], Asmaa Zafirah Kamaluzaman[2*], Mohd Syafiq Jamaludin[3], Witriany Basri[4]

[1,2,3,4]Department of Mathematics and Statistics, Faculty of Science, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.
[1]Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.

* Corresponding author: asmaazafirah@gmail.com

Received: 20 September 2022
Accepted: 25 January 2023

ABSTRACT

Cipher Trigraphic Polyfunction (CTriPoly) developed by previous researchers is a modification of the Hill Cipher technique in modern cryptography. It was built on the system using three symbols or letters and more than one transformation of the original message. The modular arithmetic of a key matrix plays an important role in the encryption and decryption processes. A crucial aspect of the decryption process is to get the inverse matrix for involutory matrices. The objective of this paper is to obtain some solution of $L^2_{2\times2} \equiv A_{2\times2} \pmod{N}$ and subsequently generate suitable involutory matrices which will be used as an encryption key in CTriPoly. This definitely reduces the computational time of finding the decryption key.

Keywords: Cryptography, Encryption, decryption, involutory matrices, secret key

1 INTRODUCTION

Cryptography comes from two Greek words, which are 'Kryptos' and 'Graphein'. 'Kryptos' means hidden while 'Graphein' means writing [1]. Basically, the meaning itself encounter us what cryptography is all about. Cryptography started in the year 1400, and for the next 450 years, this field was dominated by the *nomenclator* in which each letter is replaced by a different letter (called cipher) according to a fixed table of substitute letter [2]. Many decades ago proved that cryptography has been widely used to secure communication. Normally, it is used to protect corporate secrets, secure classified information and protect personal information from identity theft.

There are two classifications of cryptography which are symmetric key cryptography and asymmetric key cryptography. Symmetric key cryptography was then divided into classical and modern cryptography. Under classical cryptography, we have transposition cipher and substitution cipher. On the other hand, the modern cipher is divided into stream cipher and block cipher. Symmetric key cryptography uses the same secret key for both encryptions of plaintext and decryption of ciphertext. The keys may be identical, but there may be some simple transformation to go between the two keys. For example, Hill Cipher is a well-known symmetric key scheme which is, in effect, a linear transformation on a message space, consisting of m-dimensional vectors of integers [3]. That is, a plaintext string over an alphabet of order m is rewritten as a vector over Z_m using a natural correspondence [4].

Based on [5], the numerical form of plaintext in Hill Cipher usually will be written as matrix P with d rows, where d is an arbitrarily chosen positive integer. A matrix K is chosen to be the key matrix, and C is the ciphertext after performing the encryption process to the plaintext as follows:

$C \equiv KP \ (mod\ N)$,

where N is a positive integer, rewriting the resulting matrix as a string over the same alphabet. Meanwhile, decryption is performed as follows:

$P \equiv K^{-1}C \ (mod\ N)$,

where K^{-1} is the inverse of L in modulo N.

If the key matrix is invertible, the process of decrypting the ciphertext would be harder because the inverse of the key matrix should be found first. Normally, we use the elementary row operations method and modular multiplicative inverse concept in modular arithmetic to get the inverse of a square matrix [6],[7]. By using involutory matrices as a secret key of Hill Cipher, the process of finding the inverse of the key in the decryption process can be eliminated because the inverse of such a key is itself. [8] have unfolded some methods of generating any dimension of an involutory matrix to be used in Hill Cipher. This method was also implemented in modified Hill Cipher systems such as in [9],[10],[11],[12],[13],[14],[15].

Here, [10] proposed an involutory, permuted and reiterative key matrix generation method for the Hill Cipher system to enhance the security of Hill Cipher as this scheme can generate different patterns of key for each block of data encryption.

Apart from that, [11] proposed a technique for securing biometric traits using the modified Hill Cipher with an involutory key and a robust cryptosystem. They used the Modified Hill Cipher proposed by [16] to solve the drawbacks of conventional Hill ciphers using iteration and interlacing.

Meanwhile, [12] proposed SD-AEI for image encryption, which applies an extended Hill Cipher technique using an involutory matrix. This matrix was generated by the same passwords used in previous encryption to make it more secure. He also mentioned that this technique could be further extended by adding bit manipulation to the extended Hill Cipher to strengthen the encryption algorithm.

On the other hand, [13] proposed a two-stage Hill Cipher, which includes selecting square blocks to manipulate the involutory matrix. This proposition aimed to control the amount of encryption of pixel changing rate. They used Latin Square Image Cipher technique to generate a basic block of the involutory matrix. They also compared the amount of information encrypted between two-stage and four-stage Hill cipher to enhance the smartness of the camera and increase the application fields.

Elliptic Curve Cryptography (ECC) is a complex asymmetric key encryption, while Hill Cipher uses simple symmetrical encryption. An image encryption technique that combines ECC with Hill Cipher (ECCHC) has been proposed in [17] to convert Hill Cipher from symmetrical techniques to asymmetry and improve its security and efficiency to counter hackers. The self-invertible key matrix comes from the elliptical curve parameter $E_p : y^2 \equiv x^3 + ax + b \ (mod\ p)$ over a prime field

F_p used to generate secret encryption and decryption keys. Therefore, finding the inverse matrix during the decryption process is unnecessary. Entropy, Peak Signal to Noise Ratio (PSNR), and Unified Average Changing Intensity (UACI) have been used to assess the efficiency of the proposed encryption technique for the grayscale image. Through these measurements, ECCHC proved to be better than the previous cryptosystem developed by [13]. Furthermore, [14] found some solutions for $L^3_{2\times2} \equiv A_{2\times2}\ (mod\ N)$, where $L_{2\times2}$ act as a generator key for involutory encryption key $L_{4\times4}$ in the form of

$$L_{4\times4} \equiv \begin{bmatrix} L_{2\times2} & (I - L_{2\times2})k \\ (I + L_{2\times2})k^{-1} & -L_{2\times2} \end{bmatrix}\ (mod\ N).$$

To enhance the security of Cipher Tetragraphic Trifunction (CTetraTri), some patterns of $L_{2\times2}$ as generator key should be avoided before implementing CTetraTri since there are easy to be attacked by a third party. Meanwhile, [15] also faced the same effects on Cipher Hexagraphic Polyfuntion (CHexaPoly) while they implemented some involutory encryption key in the form of

$$L_{6\times6} \equiv \begin{bmatrix} L_{3\text{x}3} & (I - L_{3\text{x}3})k \\ (I + L_{3\text{x}3})k^{-1} & -L_{3\text{x}3} \end{bmatrix}\ (mod\ N),$$

where $L_{3\times3}$ (such that $L^2_{3\text{x}3} = A_{3\times3}$) act as a generator key of $L_{6\times6}$.

To protect a grayscale image, [18] modified the ECCHC system and named as MECCHC. Hill Cipher in ECCHC requires the original image to be mapped to a numerical value before implementing encryption. Still, for the case of image encryption in MECCHC, the plaintext is an image pixel that is already in numerical form and does not require a mapping function. The analysis proved that the calculation time for image encryption and decryption is faster than the ECCHC method. Efficiency assessments using Entropy, PSNR and UACI showed equivalent effects such as ECCHC.

The highlights of the above study focused on the use of involutory keys for the purpose of reducing the time to obtain inverse keys and improving the security system in Hill Cipher and its extension. In this paper, we have re-examined the evidence arguments in finding the solution of $L^2_{2\times2} \equiv A_{2\times2}\ (mod\ N)$ from [14]. The problem arises is that if there are any more generators that can be implemented before performing involutory matrices of $L_{3\times3}$ as an encryption key in Cipher Trigraphic Polyfunction (CTriPoly)? Therefore, this paper is intended to obtain as many patterns of $L_{2\times2}$ as possible by involving six categories of $A_{2\times2}$.

The organization of this paper is as follows. Section 1 describes the implementation of the involutory matrix in Hill cipher and its variant with some advantages. In Section 2, the preliminaries of this study are presented. Meanwhile, Section 3 gives some solution for $L^2_{2\times2} \equiv A_{2\times2}\ (mod\ N)$. Followed by a discussion on how to generate an involutory matrix from $L_{2\times2}$ in Section 4. The effect of using this new involutory matrix as an encryption key in CTriPoly is discussed in Section 5. The concluding section contains a summary of the paper.

2 PRELIMINARIES

The following are some notations considered in this paper.

Plaintext is the ordinary message that will be delivered to the receiver [19]. P is the corresponding number in the plaintext, such as $A = 0$, $B = 1$, $C = 2$,..., $Z = 25$. The plaintext would be arranged in matrix form $P_{i\times j}$. For example, the corresponding number sequence of plaintext $T\ R\ I\ G\ O\ N\ O\ M\ E\ T\ R\ Y$ is 19 17 08 06 14 13 14 12 04 19 17 24 are arranged by matrix 3 by 4 such as $P_{3\times 4} = \begin{bmatrix} 19 & 17 & 08 & 06 \\ 14 & 13 & 14 & 12 \\ 04 & 19 & 17 & 24 \end{bmatrix}$.

Ciphertext is the encrypted message sent to the recipient [20]. $C^{(t)}_{i\times j}$ is equivalent numbers sequence with ciphertext based on i^{th} row and j^{th} column matrix at t - transformation for $t = 1, 2, 3, \ldots$. Let $C^{(1)}_{i\times j} = C_{i\times j}$ [14],[15]. For example, the corresponding number of ciphertext $G\ U\ T\ V\ K\ D$ produced by the third transformation is 06 20 19 21 10 03 arranged by matrix 3 rows and 2 columns such that $C^{(3)}_{3\times 2} = \begin{bmatrix} 06 & 20 \\ 19 & 21 \\ 10 & 03 \end{bmatrix}$.

Encryption is the process of performing necessary changes to the text to create the ciphertext according to the cipher and the key chosen. Encryption key $E_{i\times i}$ is arranged based on matrix i^{th} row and i^{th} column while $E^{-1}_{i\times i}$ is the inverse matrix for $E_{i\times i}$ such that $|E_{i\times i}| \neq 0$ [14], [15]. On the other hand, decryption is the process on how to revert the ciphertext back into the plaintext using the ciphertext and key [20]. Here, a public key is used to encrypt plaintext into ciphertext, while a secret key is a special key that is needed to revert the process, which is to decrypt the ciphertext into plaintext [19].

CTriPoly, which we will focus on this research, is constructed based on Cipher Polygraphic Polyfuntion as follows:

Theorem 1. *[15], [21] Let Cipher Polygraphic Polyfunction Transformation be defined as:*

$C^{(t)}_{i\times j} \equiv E^{t}_{i\times i} P_{i\times j}\ (mod\ N)$ *where* $t \in \mathsf{Z}^{+}$,

where $E_{i\times i}$ *act as an encryption key. Provided that the determinant for* $E_{i\times i}$ *is not zero,* $(|E_{i\times i}|, N) = 1$*, so* $P_{i\times j}$ *have a unique solution, in which the decryption algorithm is as follows:*

$P_{i\times j} \equiv (E^{-1}_{i\times i})^{t} C^{(t)}_{i\times j}\ (mod\ N)$.

Here, the decryption key $E^{-1}_{i\times i}$ *is the inverse matrix of* $E_{i\times i}$.

Remark:
If $i = 3$, $i = 4$, $i = 5$, and $i = 6$, then the above system refers to Cipher Trigraphic Polyfunction (CTriPoly), Cipher Tetragraphic Polyfunction (CTetraPoly), Cipher Pentagraphic Polyfunction (CPentaPoly) and Cipher Hexagraphic Polyfunction (CHexaPoly), respectively.

If $E_{i\times i} \equiv E^{-1}_{i\times i}\ (mod\ N)$, then $E_{i\times i}$ is an involutory matrix, where $E^{-1}_{i\times i}$ is an inverse of $E_{i\times i}\ (mod\ N)$ [14], [15].

The following concept of modular arithmetic in Number Theory [22], [23], [24], [25] plays an important role in solving linear and quadratic congruences equations in Section 3.

Linear Congruence is when $ax \equiv b \ (mod\ N)$, where a, b and N are positive integers and x is a variable. One of its properties is as follows:

Theorem 2. *[23] If $(a, N) = 1$, then $ax \equiv b \ (mod\ N)$ has exactly one solution in modulo N.*

An integer a is called a quadratic residue modulo N if $x^2 \equiv a \ (mod\ N)$, where a and N are positive integers and x is a variable. Otherwise, a is called a quadratic non-residue modulo N. There are some ways to determine whether an integer a is a quadratic residue modulo N, given as follows:

Theorem 3. *[24] If a is a positive integer, then (a,N) = 1 and the congruence $x^2 \equiv a \ (mod\ N)$ has a solution. Hence, integer a is a quadratic residue modulo N.*

The following lemma is an Euler's Criterion which is suitable to be used to determine whether $x^2 \equiv a \ (mod\ N)$ has a solution or not.

Lemma 1. *[22] If N is an odd prime and $N \nmid a$, then equation $x^2 \equiv a \ (mod\ N)$,*

1. *has a solution if $a^{\frac{N-1}{2}} \equiv 1 \ (mod\ N)$,*
2. *has no solution if $a^{\frac{N-1}{2}} \equiv -1 \ (mod\ N)$.*

Since Euler's Criterion is unsuitable if a and N are in a large size, then we can use Legendre's symbol to check whether the integer is a quadratic residue modulo prime.

Lemma 2. *[25] Let $N \neq 2$ be a prime and a be an integer such that $N \nmid a$. The Legendre symbol $\left(\dfrac{a}{N}\right)$ is defined by*

1. *a is quadratic residue modulo N if $\left(\frac{a}{N}\right) = 1$ if $a^{\frac{N-1}{2}} \equiv 1 \ (mod\ N)$,*
2. *a is quadratic non-residue modulo N if $\left(\frac{a}{N}\right) = -1$ if $a^{\frac{N-1}{2}} \equiv -1 \ (mod\ N)$.*

3 SOME SOLUTIONS FOR $L^2_{2\times 2} \equiv A_{2\times 2} \ (mod\ N)$

In this section, we give some solution for $L^2_{2\times 2} \equiv A_{2\times 2} \ (mod\ N)$, where matrix $A_{2\times 2}$ act as public key have six categories. There are zero matrices given by $\begin{bmatrix} e & f \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & f \\ 0 & h \end{bmatrix}$, $\begin{bmatrix} e & 0 \\ 0 & 0 \end{bmatrix}$, $\begin{bmatrix} 0 & 0 \\ 0 & h \end{bmatrix}$ and $\begin{bmatrix} e & f \\ 0 & h \end{bmatrix}$ mod N. We assume $A_{2\times 2} = \begin{bmatrix} e & f \\ g & h \end{bmatrix}$ and $L_{2\times 2} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ with a, b, c, d are integers such that $L^2_{2\times 2} \equiv A_{2\times 2} \ (mod\ N)$ and have simultaneous equations as follows:

$$a^2 + bc \equiv e \ (mod\ N), \tag{1}$$
$$ab + bd \equiv f \ (mod\ N), \tag{2}$$
$$ac + cd \equiv g \ (mod\ N), \tag{3}$$
$$bc + d^2 \equiv h \ (mod\ N). \tag{4}$$

Using the concept in Number Theory, we produced the following propositions, which discussed how to find all solutions of the above equations involving six categories of $A_{2\times2}$. The cases we consider in each of the proof arguments are based on the following: $c = 0$ and $a + d \neq 0; c \neq 0$ and $a + d = 0; c = 0$ and $a + d = 0$.

Proposition 1. *Let* $L_{2\times2} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $(mod\ N)$ *where* $a = -d$. *The solution to* $L^2_{2\times2} \equiv \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ $(mod\ N)$ *is* $\begin{bmatrix} (-bc)^{\frac{1}{2}} & b \\ c & -(-bc)^{\frac{1}{2}} \end{bmatrix}$.

Proof. Let $e = f = g = h = 0$ and substitute it into (1)-(4). From (3), we have $c\,(a + d) \equiv 0\ (mod\ N)$. Now, we consider three cases as follows:

Case 1 : For $c = 0$ and $a + d \neq 0$.

Substituting $c = 0$ into (1) and (4), we have $a \equiv d \equiv 0\ (mod\ N)$. This is contradicted because of $a \neq -d$.

Case 2 : For $c \neq 0$ and $a + d = 0$.

Substituting $c \neq 0$ in (1), we have

$$a \equiv (-bc)^{\frac{1}{2}}\ (mod\ N) \text{ for } \left(\frac{-bc}{N}\right) = 1, \text{ and } (bc, N) = 1. \tag{5}$$

Substituting $a = -d$ into (5), we have

$$d \equiv -(-bc)^{\frac{1}{2}}\ (mod\ N). \tag{6}$$

Since $c \neq 0$, and $(bc, N) = 1$, then

$$b \not\equiv 0\ (mod\ N). \tag{7}$$

Hence, from (5), (6), and (7), we get $L_{2\times2} \equiv \begin{bmatrix} (-bc)^{\frac{1}{2}} & b \\ c & -(-bc)^{\frac{1}{2}} \end{bmatrix}$ $(mod\ N)$.

Case 3 : For $c = 0$ and $a + d = 0$.

Substituting $c = 0$ in (1), we have

$$a \equiv 0\ (mod\ N). \tag{8}$$

Since $a = -d$, we have

$$d \equiv 0\ (mod\ N). \tag{9}$$

Hence, from (8) and (9), we get $L_{2\times2} \equiv \begin{bmatrix} 0 & b \\ 0 & 0 \end{bmatrix}$ $(mod\ N)$.

For this proposition, we take results from Cases 2 and 3 and conclude that

$$L_{2\times2} \equiv \begin{bmatrix} (-bc)^{\frac{1}{2}} & b \\ c & -(-bc)^{\frac{1}{2}} \end{bmatrix}\ (mod\ N). \qquad \square$$

Proposition 2. *Let* $L_{2\times 2} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *(mod N) where* $a \neq -d$*. The solution to* $L^2_{2\times 2} \equiv \begin{bmatrix} e & 0 \\ 0 & 0 \end{bmatrix}$ *(mod N) is* $\begin{bmatrix} e^{\frac{1}{2}} & 0 \\ 0 & 0 \end{bmatrix}$ *where* $(e^{\frac{1}{2}}, N) = 1$*, and* $\left(\frac{e}{N}\right) = 1$*.*

Proof. Let $g = f = h = 0$ and substitute it into (2)-(4), we now have $c(a + d) \equiv 0$ $(mod\ N)$. Now, we consider three cases as follows:

Case 1 : For $c = 0$ and $a + d \neq 0$.

Substituting $c = 0$ into (1), we have

$$a \equiv e^{\frac{1}{2}}\ (mod\ N),\ \text{for}\ \left(\frac{e}{N}\right) = 1,\ \text{and}\ (e, N) = 1. \tag{10}$$

Substituting $c = 0$ into (4), we have

$$d \equiv 0\ (mod\ N). \tag{11}$$

Substituting (10) and (11) into (2), we have

$$b\,(a + d) \equiv b\left(e^{\frac{1}{2}}\right) \equiv 0\ (mod\ N). \tag{12}$$

From (12), since $e \neq 0$, then

$$b \equiv 0\ (mod\ N). \tag{13}$$

Hence, from (10), (11) and (13), we get $L_{2\times 2} \equiv \begin{bmatrix} e^{\frac{1}{2}} & 0 \\ 0 & 0 \end{bmatrix}$ $(mod\ N)$.

Case 2 : For $c \neq 0$ and $a + d = 0$.

The result from this case is similar to Proposition 1.

Case 3 : For $c = 0$ and $a + d = 0$.

Substituting $c = 0$ in (1), we have $a \equiv e^{\frac{1}{2}} \mod N$ for $\left(\frac{e}{N}\right) = 1$, and $(e, N) = 1$.
Since $a = -d$, then $d \equiv -\left(e^{\frac{1}{2}}\right)$ $(mod\ N)$.
From (2), since $a + d = 0$, we have $b(a + d) \equiv b(0) \equiv 0$ $(mod\ N)$.
Substituting $c = 0$ into (4), we have $e \equiv 0$ $(mod\ N)$. This contradicts with $e \neq 0$.

For this proposition, we just consider Case 1 for the conclusion. □

Proposition 3. *Let* $L_{2\times 2} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *(mod N). The solution to* $L^2_{2\times 2} \equiv \begin{bmatrix} 0 & 0 \\ 0 & h \end{bmatrix}$ *(mod N) is* $\begin{bmatrix} 0 & 0 \\ 0 & h^{\frac{1}{2}} \end{bmatrix}$ *where* $(h^{\frac{1}{2}}, N) = 1$ *and* $\left(\frac{h}{N}\right) = 1$*.*

Proof. Upon substituting $e = f = g = 0$ into (1)-(3), we obtain $c(a + d) \equiv 0$ $(mod\ N)$ from (3). Therefore, three cases are considered as follows:

Case 1: For $c = 0$ and $a + d \neq 0$.

Substituting $c = 0$ into (1), we have

$$a \equiv 0 \mod N. \tag{14}$$

Since $a \neq -d$ and $d \neq 0$, then from (2), we have

$$b \equiv 0 \; (mod \; N). \tag{15}$$

Substituting (15) into (4), we have

$$d \equiv h^{\frac{1}{2}} \; (mod \; N), \text{ where } \left(\frac{h}{N}\right) = 1. \tag{16}$$

Hence, from (14), (15) and (16), we get $L_{2\times2} \equiv \begin{bmatrix} 0 & 0 \\ 0 & h^{\frac{1}{2}} \end{bmatrix} \; (mod \; N)$.

Case 2 : For $c \neq 0$ and $a + d = 0$.

The result from this case is similar to Proposition 1.
Case 3 : For $c = 0$ and $a + d = 0$

The result from this case is similar to Proposition 1.
For this proposition, we take the result from Case 1 as a conclusion. □

Proposition 4. *Let* $L_{2\times2} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \; (mod \; N)$, $\left(\frac{e}{N}\right) = 1$, $(e, N) = 1$, *and* $(e^{\frac{1}{2}}, N) = 1$.*The solution to* $L^2_{2\times2} \equiv \begin{bmatrix} e & f \\ 0 & 0 \end{bmatrix} \; (mod \; N)$ *are* $\begin{bmatrix} e^{\frac{1}{2}} & (e^{-\frac{1}{2}})f \\ 0 & 0 \end{bmatrix}$ *if* $c = 0$ *and* $a \neq -d$.

Proof. Let $g = h = 0$ and substitute it into (3) and (4). From (3), we have $c(a + d) \equiv 0 \; (mod \; N)$. Now, we consider three cases as follows:

Case 1 : For $c = 0$ and $a + d \neq 0$

Substituting $c = 0$ into (1), we have

$$a \equiv e^{\frac{1}{2}} \; (mod \; N) \text{ for } \left(\frac{e}{N}\right) = 1, \text{ and } (e, N) = 1. \tag{17}$$

Substituting $c = 0$ into (4), we have

$$d \equiv 0 \; (mod \; N). \tag{18}$$

Substituting (17) and (18) into (2), we have

$$b \equiv e^{-\frac{1}{2}} f \; (mod \; N) \text{ where } \left(e^{\frac{1}{2}}, N\right) = 1. \tag{19}$$

Hence, from (17), (18) and (19), we get $L_{2\times2} \equiv \begin{bmatrix} e^{\frac{1}{2}} & e^{-\frac{1}{2}} f \\ 0 & 0 \end{bmatrix} \; (mod \; N)$.

Case 2 : For $c \neq 0$ and $a + d = 0$

The result from this case is similar to Proposition 1.

Case 3 : For $c = 0$ and $a + d = 0$

Substituting $c = 0$ in (1), we have

$$a \equiv e^{\frac{1}{2}}\ (mod\ N) \text{ for } \left(\frac{e}{N}\right) = 1, \text{ and } (e, N) = 1. \tag{20}$$

Since $a = -d$, we then have

$$d \equiv -e^{\frac{1}{2}}\ (mod\ N) \tag{21}$$

Since $a + d = 0$, from (2), we get

$$f \equiv b\,(a + d) \equiv b\,(0) \equiv 0\ (mod\ N). \tag{22}$$

Hence, from (20) and (21), we get

$$L_{2\times 2} \equiv \begin{bmatrix} e^{\frac{1}{2}} & b \\ 0 & -e^{\frac{1}{2}} \end{bmatrix}\ (mod\ N). \tag{23}$$

However, $L^2_{2\times 2} \equiv \begin{bmatrix} e & 0 \\ 0 & e \end{bmatrix}\ (mod\ N)$.
This contradicts our assumption that $h = 0$ and $(e, N) = 1$. Thus, (23) is not the solution for $L^2_{2\times 2} \equiv \begin{bmatrix} e & f \\ 0 & 0 \end{bmatrix}\ (mod\ N)$.
For this proposition, we take the result for Case 1 as a conclusion. □

Proposition 5. *Let* $L_{2\times 2} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *(mod N) where* $c = 0$ *and* $a \neq -d$. *The solution to* $L^2_{2\times 2} \equiv \begin{bmatrix} 0 & f \\ 0 & h \end{bmatrix}$ *(mod N) is* $\begin{bmatrix} 0 & fh^{-\frac{1}{2}} \\ 0 & h^{\frac{1}{2}} \end{bmatrix}$ *where* $(h^{\frac{1}{2}}, N)$, $\left(\frac{h}{N}\right) = 1$, *and* $(h, N) = 1$.

Proof. Substituting $g = e = 0$ into (1) and (3), we have $c(a + d) \equiv 0\ (mod\ N)$.
Now, we consider three cases as follows:

Case 1 : For $c = 0$ and $a + d \neq 0$

Substituting $c = 0$ into (1), we have

$$a \equiv 0\ (mod\ N). \tag{24}$$

Substituting $c = 0$ into (4), we obtain

$$d \equiv h^{\frac{1}{2}}\ (mod\ N) \text{ where } \left(\frac{h}{N}\right) = 1, \text{ and } (h, N)\,. \tag{25}$$

Substituting (24) and (25) into (2), we have

$$b \equiv fh^{-\frac{1}{2}}\ (mod\ N) \text{ where } \left(h^{\frac{1}{2}}, N\right) = 1. \tag{26}$$

Hence, from (24), (25) and (26), we get $L_{2\times 2} \equiv \begin{bmatrix} 0 & fh^{-\frac{1}{2}} \\ 0 & h^{\frac{1}{2}} \end{bmatrix}$ $(mod\ N)$.

Case 2 : For $c \neq 0$ and $a + d = 0$.

The result from this case is similar to Proposition 1.

Case 3 : For $c = 0$ and $a + d = 0$.

The result from this case is similar to Proposition 1.
For this proposition, we take the result for Case 1 as a conclusion. □

Proposition 6. *Let* $L_{2\times 2} \equiv \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *(mod N). The solution to* $L^2_{2\times 2} \equiv \begin{bmatrix} e & f \\ 0 & h \end{bmatrix}$ *(mod N) are*

1. $\begin{bmatrix} e^{\frac{1}{2}} & f(e^{\frac{1}{2}} + h^{\frac{1}{2}})^{-1} \\ 0 & h^{\frac{1}{2}} \end{bmatrix}$ *where* $a \neq -d, (e^{\frac{1}{2}} + h^{\frac{1}{2}}, N) = 1, \left(\frac{e}{N}\right) = 1$ *and* $\left(\frac{h}{N}\right) = 1$.

2. $\begin{bmatrix} (e - bc)^{\frac{1}{2}} & b \\ c & -(e - bc)^{\frac{1}{2}} \end{bmatrix}$ *where* $a = -d$, $e = h$, $f = 0$, $\left(\frac{e-bc}{N}\right) = 1$ *and* $(e - bc, N) = 1$.

Proof. Substituting $g = 0$ into (3), we have $c(a + d) \equiv 0$ $(mod\ N)$. Now, we consider three cases as given below:
Case 1 : For $c = 0$ and $a + d \neq 0$

Substituting $c = 0$ into (1), we have

$$a \equiv e^{\frac{1}{2}}\ (mod\ N) \text{ where } (\frac{e}{N}) = 1, \text{ and } (e, N) = 1. \tag{27}$$

Substituting $c = 0$ into (4), we obtain

$$d \equiv h^{\frac{1}{2}} \mod N \text{ where } (\frac{h}{N}) = 1, \text{and}(h, N) = 1. \tag{28}$$

Substituting $a + d \neq 0$ into (2), we have

$$b \equiv f(e^{\frac{1}{2}} + h^{\frac{1}{2}})^{-1} \mod N\text{where} \left(e^{\frac{1}{2}} + h^{\frac{1}{2}}, N\right) = 1. \tag{29}$$

Hence, from (27), (28) and (29), we get $L_{2\times 2} \equiv \begin{bmatrix} e^{\frac{1}{2}} & f(e^{\frac{1}{2}} + h^{\frac{1}{2}})^{-1} \\ 0 & h^{\frac{1}{2}} \end{bmatrix}$ $(mod\ N)$.
This is the proof for Proposition 6 Part 1.

Case 2: For $c \neq 0$ and $a + d = 0$

Substituting $c \neq 0$ in (1), we have

$$a \equiv (e - bc)^{\frac{1}{2}}\ (mod\ N) \text{ for } \left(\frac{e - bc}{N}\right) = 1, \text{ and } (e - bc, N) = 1. \tag{30}$$

Substituting $a = -d$ into (30), we have

$$d \equiv -(e - bc)^{\frac{1}{2}}\ (mod\ N). \tag{31}$$

Substituting $a + d = 0$ in (2), we get

$$f \equiv b\,(a + d) \equiv b\,(0) \equiv 0\ (mod\ N). \tag{32}$$

Substituting (31) in (4), we have

$$e \equiv h\ (mod\ N). \tag{33}$$

Hence, from (30) and (31), we get $L_{2\times 2} \equiv \begin{bmatrix} (e-bc)^{\frac{1}{2}} & b \\ c & -(e-bc)^{\frac{1}{2}} \end{bmatrix}\ (mod\ N)$.
This is the proof for Proposition 6 Part 2.

Case 3: For $c = 0$ and $a + d = 0$

Substituting $c = 0$ in (1), we have

$$a \equiv e^{\frac{1}{2}}\ (mod\ N) \text{ where } (\frac{e}{N}) = 1, \text{ and } (e, N) = 1. \tag{34}$$

Since $a = -d$, we then obtain

$$d \equiv -e^{\frac{1}{2}}\ (mod\ N). \tag{35}$$

Substituting (34) and (34) into (2), we get

$$f \equiv b(a + d) \equiv b(0) \equiv 0\ (mod\ N). \tag{36}$$

Substituting $c = 0$ in (4), we have

$$e \equiv h\ (mod\ N). \tag{37}$$

Hence, from (34) and (35), we get $L_{2\times 2} \equiv \begin{bmatrix} e^{\frac{1}{2}} & b \\ 0 & -e^{\frac{1}{2}} \end{bmatrix}\ (mod\ N)$.
This is the proof for Proposition 6 Part 2.

□

4 GENERATION OF INVOLUTORY MATRIX

In this section, we recall the method for generating an involutory matrix that was presented in [8] as follows:

Let $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$ be an $n\times n$ involutory matrix partitioned to $A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$,

where $A_{11} = [a_{11}]$ is a 1×1 matrix, $A_{12} = \begin{bmatrix} a_{12} & a_{13} & \cdots & a_{1n} \end{bmatrix}$ is a $1 \times (n - 1)$ matrix,

$A_{21} = \begin{bmatrix} a_{21} \\ a_{31} \\ \cdots \\ a_{n1} \end{bmatrix}$ is a $(n-1) \times 1$ matrix, $A_{22} = \begin{bmatrix} a_{22} & a_{23} & \cdots & a_{2n} \\ a_{32} & a_{33} & \cdots & a_{3n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{n2} & a_{n3} & \cdots & a_{nn} \end{bmatrix}$ is a $(n-1) \times (n-1)$ matrix.

Since A is involutory, it satisfies $A^2 = I$. Therefore

$$A_{12}A_{21} = 1 - A_{11}^2 = 1 - a_{11}^2, \tag{38}$$

and

$$A_{12}(a_{11}I + A_{22}) = 0. \tag{39}$$

Also, $a_{11} = -$(one of the eigenvalues of A_{22} other than 1). Since $A_{21}A_{12}$ is a singular matrix having the rank 1 and

$$A_{21}A_{12} = I - A_{22}^2, \tag{40}$$

then A_{22} must have eigenvalues ± 1. It can also be proved that the consistent solution obtained for matrix A_{21} and A_{12} by solving (40) term by term will also satisfy (38).

Algorithm 1 has been introduced in [8] to give general steps in order to generate an involutory matrix.

Algorithm 1.

1. *Select A_{22}, a non-singular $(n-1) \times (n-1)$ matrix which has $(n-2)$ number of eigenvalue of either $+1$ or -1 or both. The method for calculating an eigenvalue from $|\lambda I - A_{22}| = 0$ can be referred to [26].*
2. *Determine the other eigenvalue λ of A_{22}.*
3. *Set $a_{11} = -\lambda$.*
4. *Obtain the consistent solution of all elements of A_{21} and A_{12} by using (40).*
5. *Formulate the matrix A.*

To align with our study, we take $A_{11} = L_{1\times1}$, $A_{22} = L_{2\times2}$, $A_{12} = L_{1\times2}$, $A_{21} = L_{2\times1}$ to formulate A, which is $L_{3\times3}$. The first step in Algorithm 1 requires a non-singular $L_{2\times2}$ matrix. Therefore, we only consider $L_{2\times2}$ from Proposition 6. The steps below were employed to generate involutory matrix $L_{3\times3}$ from Proposition 6 Part 1.

Step 1: Let $L_{2\times2} = \begin{bmatrix} e^{\frac{1}{2}} & f(e^{\frac{1}{2}} + h^{\frac{1}{2}})^{-1} \\ 0 & h^{\frac{1}{2}}, \end{bmatrix}$ which has eigenvalues $\lambda_1 = h^{\frac{1}{2}}$ and $\lambda_2 = e^{\frac{1}{2}}$. We assume that $\lambda_1 \equiv 1 \ (mod\ N)$.

Step 2: Therefore, we can choose any $\lambda_2 \neq 1$.

Step 3: Set $a_{11} \equiv -\lambda_2 \ (mod\ N)$.

Step 4: Obtain the consistent solution of all elements of $L_{1\times 2}$ and $L_{2\times 1}$ by using (40) as follows:

$$L_{2\times 1}L_{1\times 2} = I - L_{2\times 2}^2 = \begin{bmatrix} 1-e & -f \\ 0 & 0 \end{bmatrix}. \tag{41}$$

This matrix is proven to be singular such that $L_{2\times 2}$ has an eigenvalue 1 or −1. All consistent solutions is $L_{2\times 1} = \begin{bmatrix} k \\ 0 \end{bmatrix}$ and $L_{1\times 2} = \begin{bmatrix} (1-e)k^{-1} & -fk^{-1} \end{bmatrix}$, where $(k, N) = 1$.

Step 5: Thus, we get

$$L_{3\times 3} \equiv \begin{bmatrix} -e^{\frac{1}{2}} & (1-e)k^{-1} & -fk^{-1} \\ k & e^{\frac{1}{2}} & (e^{\frac{1}{2}}+1)^{-1}f \\ 0 & 0 & 1 \end{bmatrix} \ (mod\ N). \tag{42}$$

Meanwhile, we can find another involutory matrix when $\lambda_1 \neq 1$ and $\lambda_2 = 1$ i.e.

$$L_{3\times 3} \equiv \begin{bmatrix} -h^{\frac{1}{2}} & 0 & k \\ -fk^{-1} & 1 & (h^{\frac{1}{2}}+1)^{-1}f \\ (1-h)k^{-1} & 0 & h^{\frac{1}{2}} \end{bmatrix} \ (mod\ N). \tag{43}$$

On the other hand, the following are several reasons why we are unable to generate an involutory matrix from $L_{2\times 2}$ in Proposition 6 Part 2: Let $L_{2\times 2} = \begin{bmatrix} (e-bc)^{\frac{1}{2}} & b \\ c & -(e-bc)^{\frac{1}{2}} \end{bmatrix}$ which has repeated eigenvalue $\lambda_1 = \lambda_2 = e^{\frac{1}{2}}$. Now, if we consider $\lambda_1 = 1$, then $L_{2\times 1}L_{1\times 2}$ is singular. However, we need to setup $L_{1\times 1} = -\lambda_2$ for $\lambda_2 \neq 1$. This contradicts since $\lambda_1 = \lambda_2$. Furthermore, if we take $\lambda_1 = -1$, then $L_{2\times 1}L_{1\times 2}$ is non singular.

5 EFFECT OF INVOLUTORY KEY IN CTRIPOLY

In this section, we show the effect of applying the involutory matrix, $L_{3\times 3}$ $(mod\ N)$ as a secret key in CTriPoly as follows:

Example 1.

Let $L_{2\times 2} = \begin{bmatrix} 2 & 5 \\ 0 & 1 \end{bmatrix}$ act as secret key is solution of $L_{2\times 2}^2 \equiv \begin{bmatrix} 4 & 2 \\ 0 & 1 \end{bmatrix}$ $(mod\ 13)$ by applying Proposition 6 Part 1. This is followed by generating $L_{3\times 3} \equiv \begin{bmatrix} 11 & 10 & 11 \\ 1 & 2 & 5 \\ 0 & 0 & 1 \end{bmatrix}$ $(mod\ 13)$ using formula (42) when $e = 4, f = 2, h = 1$ and $k = 1$. Let $L_{3\times 3}$ act as an encryption key while encrypting a plaintext to ciphertext. The message "ALGORITHM" will be used as plaintext and can be written as

$$P_{3\times 3} \equiv \begin{bmatrix} A & L & G \\ O & R & I \\ T & H & M \end{bmatrix} \equiv \begin{bmatrix} 0 & 11 & 6 \\ 1 & 4 & 8 \\ 6 & 7 & 12 \end{bmatrix} (mod\ 13).$$

Since $\gcd(|L_{3\times3}|, 13) = 1$, then there exist a unique solution for plaintext, $P_{3\times3}$. Now, we are using algorithm for encryption from $P_{3\times3}$ to $C^{(4)}_{3\times3}$ that was mentioned in Theorem 1 as follows:

$$C^{(1)}_{3\times3} \equiv L_{3\times3}P_{3\times3} \equiv \begin{bmatrix} 11 & 4 & 5 \\ 6 & 2 & 4 \\ 6 & 7 & 12 \end{bmatrix} (mod\, 13).$$

$$C^{(2)}_{3\times3} \equiv L_{3\times3}C^{(1)}_{3\times3} \equiv \begin{bmatrix} 0 & 11 & 6 \\ 1 & 4 & 8 \\ 6 & 7 & 12 \end{bmatrix} (mod\, 13).$$

$$C^{(3)}_{3\times3} \equiv L_{3\times3}C^{(2)}_{3\times3} \equiv \begin{bmatrix} 11 & 4 & 5 \\ 6 & 2 & 4 \\ 6 & 7 & 12 \end{bmatrix} (mod\, 13).$$

$$C^{(4)}_{3\times3} \equiv L_{3\times3}C^{(3)}_{3\times3} \equiv \begin{bmatrix} 0 & 11 & 6 \\ 1 & 4 & 8 \\ 6 & 7 & 12 \end{bmatrix} (mod\, 13).$$

From the algorithm above, the odd-th and even-th transformations result will produce the secret message "LEFGCEGHM" and plaintext "ALGORITHM", respectively. Since $L_{3\times3}$ is self-invertible, the receiver easily gets the original text via the decryption process as follows:

$$C^{(3)}_{3\times3} \equiv L_{3\times3}C^{(4)}_{3\times3} \equiv \begin{bmatrix} 11 & 4 & 5 \\ 6 & 2 & 4 \\ 6 & 7 & 12 \end{bmatrix} (mod\, 13).$$

$$C^{(2)}_{3\times3} \equiv L_{3\times3}C^{(3)}_{3\times3} \equiv \begin{bmatrix} 0 & 11 & 6 \\ 1 & 4 & 8 \\ 6 & 7 & 12 \end{bmatrix} (mod\, 13).$$

$$C^{(1)}_{3\times3} \equiv L_{3\times3}C^{(2)}_{3\times3} \equiv \begin{bmatrix} 11 & 4 & 5 \\ 6 & 2 & 4 \\ 6 & 7 & 12 \end{bmatrix} (mod\, 13).$$

$$P_{3\times3} \equiv L_{3\times3}C^{(1)}_{3\times3} \equiv \begin{bmatrix} 0 & 11 & 6 \\ 1 & 4 & 8 \\ 6 & 7 & 12 \end{bmatrix} (mod\, 13).$$

From the encryption algorithm in the example above, the result for the second and fourth transformations are similar to plaintext. In contrast, the result from the third transformation is the same as the first transformation. Generally, for $n \in \mathbb{Z}^+$,

$$C^{2n}_{3\times3} \equiv L^{2n}_{3\times3}P_{3\times3} \equiv (L^2_{3\times3})^n P_{3\times3} \equiv I^n P_{3\times3} \equiv P_{3\times3}\, (mod\, N) \tag{44}$$

whereas

$$C^{2n+1}_{3\times3} \equiv L^{2n+1}_{3\times3}P_{3\times3} \equiv L_{3\times3}(L^2_{3\times3})^n P_{3\times3} \equiv L_{3\times3}I^n P_{3\times3} \equiv L_{3\times3}P_{3\times3} \equiv C^{(1)}_{3\times3}\, (mod\, N). \tag{45}$$

Therefore, the result of the odd-th and even-th transformations will produce the secret message and plaintext, respectively. In other words, the sender of the original message should only send a message until the second transformation if the encryption key is involutory. Thus, Theorem 1 is only used for $t = 1, 2$ with the involutory $E_{i\times i}$ key. However, future studies can be further expanded using different $E_{i\times i}$, which is involutory for each transformation.

From Section 3, we have obtained one pattern of $L_{2\times 2}$ (i.e. from Proposition (6) Part 1.) matrix that can be fulfilled all criteria to generate the involutory $L_{3\times 3}$ matrices as in (42) and (43). However, the third parties can analyze the ciphertext using the patterns of involutory matrices mentioned above even though they do not know the decryption keys. There are about $2N^3$ combinations of (42) and (43) that need to be tested before deriving the actual value of the plaintext. Nevertheless, it is possible to get it so fast with the appropriate algorithm and high-performance computer.

6 CONCLUSION

In conclusion, we obtained some solutions of $L^2_{2\times 2} \equiv A_{2\times 2}\,(mod\ N)$ with six criteria of $A_{2\times 2}$. As a result, we choose one pattern of $L_{2\times 2}$ that was produced by Proposition (6) Part 1. This will generate two type of involutory matrices $L_{3\times 3}$ in the form of (42) and (43). Its use in the CTriPoly's system can solve the problem of obtaining the inverse of the encryption key. In addition, the benefits of this pattern can also be further refined because the third party's ability to find the right key may be limited as the matrix dimensions increase.

REFERENCES

[1] M. Rathidevi, R. Yaminipriya, and S. Sudha, "Trends of cryptography stepping from ancient to modern," in *International Conference on Innovations in Green Energy and Healthcare Technologies (IGEHT).* IEEE, 2017, pp. 1–9.

[2] D. Davies, "A brief history of cryptography," *Information Security Technical Report*, vol. 2, no. 2, pp. 14–17, 1997.

[3] L. S. Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306–312, 1929. [Online]. Available: https://doi.org/10.1080/00029890.1929.11986963

[4] J. Overbey, W. Traves, and J. Wojdylo, "On the keyspace of the hill cipher," *Cryptologia*, vol. 29, no. 1, pp. 59–72, 2005.

[5] C. Christensen, "Cryptography of the vigenère cipher," in *Proceedings of Computer Sciences Corporation*, 2006, pp. 1–18.

[6] R. Bronson and G. B. Costa, *Linear algebra: An introduction.* Academic Press, 2007.

[7] R. A. Mollin, *An introduction to cryptography.* Chapman and Hall/CRC, 2006.

[8] B. Acharya, G. Rath, S. Patra, and S. K. Panigrahy, "Novel methods of generating self-

invertible matrix for hill cipher algorithm," *International Journal of Security*, vol. 1, no. 1, pp. 14–21, 2007.

[9] S. K. Panigrahy, B. Acharya, and D. Jena, "Image encryption using self-invertible key matrix of hill cipher algorithm," in *Proceedings of the 1st International Conference on Advances in Computing*, February 2008.

[10] B. Acharya, S. K. Patra, and G. Panda, "Involutory, permuted and reiterative key matrix generation methods for hill cipher system," *International Journal of Recent Trends in Engineering*, vol. 1, no. 4, p. 106, 2009.

[11] B. Acharya, M. D. Sharma, S. Tiwari, and V. K. Minz, "Privacy protection of biometric traits using modified hill cipher with involutory key and robust cryptosystem," *Procedia Computer Science*, vol. 2, pp. 242–247, 2010. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050910003613

[12] S. Dey, "Sd-aei: An advanced encryption technique for images," in *2012 Second International Conference on Digital Information Processing and Communications (ICDIPC)*. IEEE, 2012, pp. 68–73.

[13] S. Naveenkumar, H. Panduranga *et al.*, "Partial image encryption for smart camera," in *Proceedings of the 2013 IEEE International Conference on Recent Trends in Information Technology (ICRTIT)*, 2013, pp. 126–132.

[14] F. Yunos, S. Ling, and M. R. Md Said, "Effect of self invertible matrix on cipher tetragraphic trifunction," in *Proceeding of the 25th National Symposium On Mathematical Science (SKSM25)*, June 2018.

[15] P. C. Sally Lin and F. Yunos, "Effect of self-invertible matrix on cipher hexagraphic polyfunction," *Cryptography*, vol. 3, no. 2, 2019. [Online]. Available: https://www.mdpi.com/2410-387X/3/2/15

[16] V. Sastry and N. R. Shankar, "Modified hill cipher for a large block of plaintext with interlacing and iteration," *Journal of Computer Science*, vol. 4, no. 1, pp. 15–20, 2008.

[17] Z. E. Dawahdeh, N. Y. Shahrul, and R. R. Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *Journal of King Saud University – Computer and Information Sciences*, vol. 30, pp. 349–35, 2018.

[18] S. Satapathy and S. Rajkumar, "Image encryption using modified elliptic curve cryptography and hill cipher," *Smart Intelligent Computing and Applications*, pp. 675–683, 2020.

[19] O. G. Abood and S. K. Guirguis, "A survey on cryptography algorithms," *International Journal of Scientific and Research Publications*, vol. 8, no. 7, pp. 495–516, 2018.

[20] D. R. Clark, "Crypto corner," https://crypto.interactive-maths.com/glossary.html/, 2019.

[21] F. Yunos, *Beberapa penggunaan teori nombor dalam kriptografi.* Master Thesis, Universiti

Putra Malaysia, Serdang, 2001.

[22] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An introduction to the theory of numbers.* John Wiley & Sons, 1991.

[23] K. H. Rosen, *Elementary Number Theory and Its Application (Six Edition).* Addison-Wesley : Boston, MA, USA, 1987.

[24] L. S. Reddy, "A new modal of hill cipher using non–quadratic residues," *Integers*, vol. 1, no. 2, p. 1, 2012.

[25] W. Raji, "Legendre symbol," https://math.libretexts.org/Bookshelves/Combinatorics_and_Discrete_Mathematics/Elementary_Number_Theory_(Raji)/05%3A_Primitive_Roots_and_Quadratic_Residues/5.05%3A_Legendre_Symbol, July 2021.

[26] Q. Kong, T. Siauw, and A. Bayen, *Python Programming and Numerical Methods: A Guide for Engineers and Scientists.* Academic Press, 2020.