Determinants and Permanents of Hessenberg Matrices with Perrin's Bivariate Complex Polynomials and Its Application

JIRAWAT KANTALO
Department of Mathematics and Statistics,
Sakon Nakhon Rajabhat University,
Sakon Nakhon 47000,
THAILAND

Abstract: - In this paper, we define some $n \times n$ Hessenberg matrices and then we obtain determinants and permanents of their matrices that give the odd and even terms of bivariate complex Perrin polynomials. Moreover, we use our results to apply the application cryptology area. We discuss the Affine-Hill method over complex numbers by improving our matrix as the key matrix and present an experimental example to show that our method can work for cryptography.

Key-Words: Perrin Complex Bivariate Polynomials, Determinant, Permanent, Hessenberg Matrix, Cryptography

Received: September 19, 2022. Revised: April 9, 2023. Accepted: May 2, 2023. Published: May 17, 2023.

1 Introduction

Perrin's complex bivariate polynomials $\{\mathrm{P}_n(x,y)\}$ have been introduced by [1], and are defined by the recurrence relation, for $n \geq 3$,

$$\mathrm{P}_n(x,y) = ix^2\mathrm{P}_{n-2}(x,y) + y^2\mathrm{P}_{n-3}(x,y), \qquad (1)$$

where initial conditions $\mathrm{P}_0(x,y)=3,\ \mathrm{P}_1(x,y)=0,$ $\mathrm{P}_2(x,y)=2$ and $i^2=-1$. The first terms of the above sequences are presented in Table 1.

In recent years, the determinants and permanents of one type of Hessenberg matrices representation of many sequences. For example, [2], introduced determinants and permanents of Hessenberg matrices as the generalized Fibonacci and Pell sequences. In 2014, [3], presented some determinantal and permanental representations of associated polynomials of Perrin and Cordonnier numbers. In 2020, [4], defined tridiagonal matrices whose permanent is equal to the k-Jacobsthal sequence. See more examples in [5], [6], [7], [8].

In addition, the applications of number theory have been widely studied. One of the most interesting applications is cryptography. Several authors used the methods for encryption using their obtained results as a key such as in 2017, [9], presented a coding and decoding method using the generalized Pell numbers. In 2019, [10], proposed a new coding and decoding algorithm using Padovan Q-matrices and Maxrizal, [11], showing the Hill Cipher method can be generalized to key matrices over complex numbers.

Table 1. The first terms of Perrin's complex bivariate polynomials.

n	$\mathrm{P}_n(x,y)$
1	0
2	2
3	$3y^2$
4	$2ix^2$
5	$2y^2+3ix^2y^2$
6	$3y^4-2x^4$
7	$-3x^4y^2+4ix^2y^2$
8	$6ix^2y^4-2ix^6+2y^4$
9	$-3ix^6y^2-6x^4y^2+3y^6$
10	$-9x^4y^4+6ix^2y^4+2x^8$

In 2021, [12], defined some third-order Bronze Fibonacci sequences and developed the obtained results in encryption theory. Moreover, the anti-orthogonal and H-anti-orthogonal of type I matrices were firstly defined by [13], and they applied these matrices in cryptology.

In this paper, we consider the bivariate Perrin's complex polynomials and then define new $n \times n$ Hessenberg matrices which have determinants and permanents related to these polynomials. In addition, we consider an application in cryptology based on the Affine-Hill chipher which was introduced by [14]. We improve and modify the public key over complex numbers by using our obtained matrix which is a non-singular matrix. Finally, a numerical example of an encryption and decryption algorithm is given.

2 Preliminaries

In this section, the following definitions and lemmas for determinants and permanents of the Hessenberg matrix are given.

Definition 2.1 *[15], An $n\times n$ matrix $A_n=\lfloor a_{r,s}\rfloor$ is called a lower Hessenberg matrix if $a_{r,s}=0$ when $s-r>1$, i.e.,*

$$A_n=\begin{bmatrix} a_{1,1} & a_{1,2} & 0 & \cdots & 0 \\ a_{2,1} & a_{2,2} & a_{2,3} & \cdots & 0 \\ a_{3,1} & a_{3,2} & a_{3,3} & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ a_{n-1,1} & a_{n-1,2} & a_{n-1,3} & \cdots & a_{n-1,n} \\ a_{n,1} & a_{n,2} & a_{n,3} & \cdots & a_{n,n} \end{bmatrix}. \qquad (2)$$

Lemma 2.2 *[16], Let A_n be a lower Hessenberg matrix. The following determinant formula for A_n is given by*

$$\det A_n = a_{n,n}\det A_{n-1}+\sum_{t=1}^{n-1}\left(\left(-1\right)^{n-t}a_{n,t}\left[\prod_{j=t}^{n-1}a_{j,j+1}\right]\det A_{t-1}\right),$$

for $n\geq 2$, where $\det A_0=1$, and $\det A_1=a_{1,1}$.

Definition 2.3 *Let A_n be $n\times n$ a matrix, the permanent of A_n is defined by*

$$\operatorname{per} A_n=\sum_{\sigma\in S_n}\prod_{i=1}^{n}a_{i,\sigma(i)}, \qquad (3)$$

where S_n denotes the set of permutations of $\{1,2,\ldots,n\}$.

Lemma 2.4 *[17], Let A_n be a lower Hessenberg matrix. The following permanent formula for A_n is given by*

$$\operatorname{per} A_n = a_{n,n}\operatorname{per} A_{n-1}+\sum_{t=1}^{n-1}\left(a_{n,t}\left[\prod_{j=t}^{n-1}a_{j,j+1}\right]\operatorname{per} A_{t-1}\right),$$

for $n\geq 2$, where $\operatorname{per} A_0=1$, and $\operatorname{per} A_1=a_{1,1}$.

3 Main Results

In this section, we will define new $n\times n$ lower Hessenberg matrices and present the determinants and permanents of their matrices which are bivariate Perrin's complex polynomials, respectively.

Theorem 3.1 *Let $B_n=\lfloor b_{r,s}\rfloor$ be a $n\times n$ lower Hessenberg matrix, is defined by*

$$b_{r,s}=\begin{cases} 3y^2 & \text{if } r=s=1 \\ ix^2 & \text{if } r=s \text{ for } r,s\geq 2 \\ 2y^2 & \text{if } s-r=1 \\ (-i)^r\left(\dfrac{x^2}{2y^2}\right)^{r-2} & \text{if } r\geq 2, s=1 \\ \dfrac{1}{4}\left(\dfrac{-x^2 i}{2y^2}\right)^{r-s-2} & \text{if } r-s\geq 2 \text{ for } r\geq 4, s\geq 2 \\ 0 & \text{otherwise} \end{cases}. \qquad (4)$$

Then

$$\det B_n=P_{2n+1}\left(x,y\right),\ \textit{for } n\geq 1. \qquad (5)$$

Proof. We proved this by mathematical induction on n. By hypothesis, the result holds for all $n\leq 4$. Then, we suppose that the result is true for all positive integer k such that $k\geq 5$. We will prove it for $k+1$.

Firstly, we use elementary row operations on the matrix B_{k+1}. We multiply the $(k-1)^{\text{th}}$ row by $\dfrac{x^4}{4y^4}$ then add to $(k+1)^{\text{th}}$ row. So, we get the $(k+1)^{\text{th}}$ row as

$$\left\lfloor \underbrace{0\ \ 0\ \ \cdots\ \ 0}_{(k-3)^{\text{th}}}\ \ -\frac{ix^2}{8y^2}\ \ \frac{ix^6+y^4}{4y^4}\ \ \frac{x^4}{2y^2}\ \ ix^2 \right\rfloor.$$

That is

$$B_{k+1}=\begin{bmatrix} 3y^2 & 2y^2 & 0 & \cdots & & & \cdots & 0 \\ -1 & ix^2 & \ddots & 0 & & & \cdots & 0 \\ \dfrac{ix^2}{2y^2} & 0 & \ddots & \ddots & \ddots & & & \vdots \\ \dfrac{x^4}{4y^4} & \dfrac{1}{4} & \ddots & \ddots & \ddots & \ddots & & \vdots \\ -\dfrac{ix^6}{8y^6} & -\dfrac{ix^2}{8y^2} & \ddots & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ \vdots & & & \ddots & \dfrac{1}{4} & 0 & \ddots & 2y^2 \\ 0 & 0 & \cdots & 0 & -\dfrac{ix^2}{8y^2} & \dfrac{ix^6+y^4}{4y^4} & \dfrac{x^4}{2y^2} & ix^2 \end{bmatrix}.$$

Now, using Lemma 2.2, we have

$$\det B_{k+1} = ix^2 \det B_k + \sum_{t=1}^{k}\left((-1)^{k+1-t} b_{k+1,t}\left[\prod_{j=t}^{k} b_{j,j+1}\right]\det B_{t-1}\right)$$

$$= ix^2 \det B_k + \sum_{t=1}^{k-3}\left((-1)^{k+1-t} b_{k+1,t}\left[\prod_{j=t}^{k} b_{j,j+1}\right]\det B_{t-1}\right)$$

$$+ \sum_{t=k-2}^{k}\left((-1)^{k+1-t} b_{k+1,t}\left[\prod_{j=t}^{k} b_{j,j+1}\right]\det B_{t-1}\right).$$

Since $b_{k+1,t}=0$ for $1\le t\le k-3$, then

$$\det B_{k+1} = i\,x^2 \mathrm{P}_{2k+1}(x,y) + \sum_{t=k-2}^{k}\left((-1)^{k+1-t} b_{k+1,t}\left[\prod_{j=t}^{k} b_{j,j+1}\right]\det B_{t-1}\right)$$

$$= ix^2\,\mathrm{P}_{2k+1}(x,y) + ix^2y^4\,\mathrm{P}_{2k-5}(x,y) + \left(ix^6+y^4\right)\mathrm{P}_{2k-3}(x,y) - x^4\,\mathrm{P}_{2k-1}(x,y)$$

$$= ix^2\,\mathrm{P}_{2k+1}(x,y) + ix^2y^2\left(\mathrm{P}_{2k-2}(x,y) - ix^2\,\mathrm{P}_{2k-4}(x,y)\right) + ix^6\,\mathrm{P}_{2k-3}(x,y) + y^4\,\mathrm{P}_{2k-3}(x,y) - x^4\,\mathrm{P}_{2k-1}(x,y)$$

$$= ix^2\,\mathrm{P}_{2k+1}(x,y) + x^4\left(ix^2\,\mathrm{P}_{2k-3}(x,y) + y^2\,\mathrm{P}_{2k-4}(x,y)\right) + y^2\left(ix^2\,\mathrm{P}_{2k-2}(x,y) + y^2\mathrm{P}_{2k-3}(x,y)\right) - x^4\,\mathrm{P}_{2k-1}(x,y)$$

$$= ix^2\,\mathrm{P}_{2k+1}(x,y) + y^2\,\mathrm{P}_{2k}(x,y)$$

$$= \mathrm{P}_{2k+3}(x,y)$$

$$= \mathrm{P}_{2(k+1)+1}(x,y).$$

Then, $\det B_n = \mathrm{P}_{2n+1}(x,y)$ for all $n\ge 1$. □

Example 3.2 *Let B_6 is defined by (4). So, the determinant of B_6 which is as follows:*

$$\det B_6 = \begin{vmatrix} 3y^2 & 2y^2 & 0 & 0 & 0 & 0 \\ -1 & ix^2 & 2y^2 & 0 & 0 & 0 \\ \frac{ix^2}{2y^2} & 0 & ix^2 & 2y^2 & 0 & 0 \\ \frac{x^4}{4y^4} & \frac{1}{4} & 0 & ix^2 & 2y^2 & 0 \\ -\frac{ix^6}{8y^6} & \frac{-ix^2}{8y^2} & \frac{1}{4} & 0 & ix^2 & 2y^2 \\ -\frac{x^8}{16y^8} & \frac{-x^4}{16y^4} & \frac{-ix^2}{8y^2} & \frac{1}{4} & 0 & ix^2 \end{vmatrix}$$

$$= 3ix^{10}y^2 + 10x^8y^2 - 18x^4y^6 + 8ix^2y^6$$

$$= \mathrm{P}_{13}(x,y)$$

$$= \mathrm{P}_{2(6)+1}(x,y).$$

Theorem 3.3 *Let $D_n = \lfloor d_{r,s} \rfloor$ be a $n\times n$ lower Hessenberg matrix, is defined by $d_{1,1}=y^2$, $d_{1,2}=ix^2, d_{2,1}=-2ix^2, d_{2,2}=3y^2, d_{3,1}=\frac{3y^2}{2}$, $d_{3,2}=-1$ and*

$$d_{r,s} = \begin{cases} ix^2 & \text{if } r=s \text{ for } r,s\ge 3 \\ 2y^2 & \text{if } s-r=1 \text{ for } s\ge 3 \\ (-i)^{r-1}\left(\frac{x^2}{2y^2}\right)^{r-3} & \text{if } r\ge 3, s=2 \\ \frac{1}{4}\left(\frac{-ix^2}{2y^2}\right)^{r-s-2} & \text{if } r-s\ge 2 \\ & \text{for } r\ge 5, s\ge 3 \\ \frac{(-i)^{r-2}}{4}\left(\frac{x^2}{2y^2}\right)^{r-4}\left(2+3ix^2\right) & \text{if } r\ge 4, s=1 \\ 0 & \text{otherwise} \end{cases} . \quad (6)$$

Then

$$\det D_n = \mathrm{P}_{2n+2}(x,y), \quad \textit{for } n\ge 2. \quad (7)$$

Proof. We proved this by mathematical induction on n. By hypothesis, the result holds for all $2\le n\le 5$. Then, we suppose that the result is true for all positive integer k such that $k\ge 6$. We will prove it for $k+1$.

We use elementary row operations on the matrix D_{k+1}. We multiply the $(k-1)^{\text{th}}$ row by $\frac{x^4}{4y^4}$ then add to $(k+1)^{\text{th}}$ th row. So, we get the $(k+1)^{\text{th}}$ row as

$$\left\lfloor \underbrace{0 \quad 0 \quad \cdots \quad 0}_{(k-3)^{\text{th}}} \quad -\frac{ix^2}{8y^2} \quad \frac{y^4+ix^6}{4y^4} \quad \frac{x^4}{2y^2} \quad ix^2 \right\rfloor.$$

That is

$$D_{k+1} = \begin{bmatrix} y^2 & ix^2 & 0 & \cdots & & & \cdots & 0 \\ -2ix^2 & 3y^2 & 2y^2 & 0 & & & \cdots & 0 \\ \frac{3y^2}{2} & -1 & ix^2 & \ddots & \ddots & & & \vdots \\ \frac{-2-3ix^2}{4} & \frac{ix^2}{2y^2} & 0 & \ddots & \ddots & \ddots & & \vdots \\ \frac{-3x^4+2x^2}{8y^2} & \frac{x^4}{4y^4} & \frac{1}{4} & \ddots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \vdots & & \ddots & \ddots & & \ddots & 0 \\ \vdots & \vdots & & & \frac{1}{4} & 0 & \ddots & 2y^2 \\ 0 & 0 & \cdots & 0 & -\frac{ix^2}{8y^2} & \frac{y^4+ix^6}{4y^4} & \frac{x^4}{2y^2} & ix^2 \end{bmatrix}$$

Now, using Lemma 2.2, we have

$$\det D_{k+1} = ix^2 \det D_k + \sum_{t=1}^{k}\left((-1)^{k+1-t} d_{k+1,t}\left[\prod_{j=t}^{k} d_{j,j+1}\right]\det D_{t-1}\right)$$

$$= ix^2 \det D_k + \sum_{t=1}^{k-3}\left((-1)^{k+1-t} d_{k+1,t}\left[\prod_{j=t}^{k} d_{j,j+1}\right]\det D_{t-1}\right)$$

$$+ \sum_{t=k-2}^{k}\left((-1)^{k+1-t} d_{k+1,t}\left[\prod_{j=t}^{k} d_{j,j+1}\right]\det D_{t-1}\right).$$

Since $d_{k+1,t} = 0$ for $1 \le t \le k-3$, then

$$\det D_{k+1} = i\,x^2 \mathrm{P}_{2k+2}(x,y) + \sum_{t=k-2}^{k}\left((-1)^{k+1-t} d_{k+1,t}\left[\prod_{j=t}^{k} d_{j,j+1}\right]\det D_{t-1}\right)$$

$$= ix^2 \mathrm{P}_{2k+2}(x,y) + ix^2y^4 \mathrm{P}_{2k-4}(x,y) + \left(ix^6 + y^4\right)\mathrm{P}_{2k-2}(x,y) - x^4 \mathrm{P}_{2k}(x,y)$$

$$= ix^2 \mathrm{P}_{2k+2}(x,y) + ix^2y^2\left(\mathrm{P}_{2k-1}(x,y) - ix^2 \mathrm{P}_{2k-3}(x,y)\right) + ix^6 \mathrm{P}_{2k-2}(x,y) + y^4 \mathrm{P}_{2k-2}(x,y) - x^4 \mathrm{P}_{2k}(x,y)$$

$$= ix^2 \mathrm{P}_{2k+2}(x,y) + x^4\left(ix^2 \mathrm{P}_{2k-2}(x,y) + y^2 \mathrm{P}_{2k-3}(x,y)\right) + y^2\left(ix^2 \mathrm{P}_{2k-1}(x,y) + y^2 \mathrm{P}_{2k-2}(x,y)\right) - x^4 \mathrm{P}_{2k}(x,y)$$

$$= ix^2 \mathrm{P}_{2k+2}(x,y) + y^2 \mathrm{P}_{2k+1}(x,y)$$

$$= \mathrm{P}_{2k+4}(x,y)$$

$$= \mathrm{P}_{2(k+1)+2}(x,y).$$

Therefore, $\det D_n = \mathrm{P}_{2n+2}(x,y)$ for all $n \ge 2$.

Example 3.4 *Let D_6 is defined by (6). So, the determinant of D_6 which is as follows:*

$$\det D_6 = \begin{vmatrix} y^2 & ix^2 & 0 & 0 & 0 & 0 \\ -2ix^2 & 3y^2 & 2y^2 & 0 & 0 & 0 \\ \frac{3y^2}{2} & -1 & ix^2 & 2y^2 & 0 & 0 \\ \frac{-2-3ix^2}{4} & \frac{ix^2}{2y^2} & 0 & ix^2 & 2y^2 & 0 \\ \frac{-3x^4+2ix^2}{8y^2} & \frac{x^4}{4y^4} & \frac{1}{4} & 0 & ix^2 & 2y^2 \\ \frac{2x^4+3ix^6}{16y^4} & -\frac{ix^6}{8y^6} & -\frac{ix^2}{8y^2} & \frac{1}{4} & 0 & ix^2 \end{vmatrix}$$

$$= -2x^{12} + 15y^4x^8 - 20iy^4x^6 + 12iy^8x^2 + 2y^8$$

$$= \mathrm{P}_{14}(x,y)$$

$$= \mathrm{P}_{2(6)+2}(x,y).$$

Now, we will present the permanents of matrices that are bivariate complex Perrin polynomials. In [18], this study gave the relationship between the determinant and the permanent of a Hessenberg matrix by using Lemmas 2.2 and 2.4.

Then, let A_n be $n \times n$ lower Hessenberg matrix $A = \lfloor a_{r,s} \rfloor$ is given in (2) and also E_n be $n \times n$ a lower Hessenberg matrix which is defined by $e_{r,r+1} = -a_{r,r+1}$ for all r, $e_{r,s} = a_{r,s}$ for $r \ge s$ and 0 otherwise. So, we have $\det E_n = A_n$ or $\det A_n = \operatorname{per} E_n$. Then, we have the following Corollary without proof.

Let H_n be $n \times n$ matrix, is defined by

$$H_n = \begin{bmatrix} 1 & -1 & 1 & \cdots & 1 \\ 1 & 1 & -1 & \ddots & 1 \\ 1 & 1 & 1 & \ddots & 1 \\ \vdots & \vdots & \ddots & \ddots & -1 \\ 1 & 1 & \cdots & 1 & 1 \end{bmatrix}. \qquad (8)$$

Corollary 3.5 *Let V_n and W_n be $n \times n$ matrices and define $V_n = H_n \circ B_n$ and $W_n = H_n \circ C_n$ where $\circ$ denotes the operator of Hadamard product of matrix. Then,*

$$\operatorname{per} V_n = \mathrm{P}_{2n+1}(x,y), \qquad (9)$$

$$\operatorname{per} W_n = \mathrm{P}_{2n+2}(x,y). \qquad (10)$$

4 Applications in Cryptography

In this section, we present new encoding and decoding algorithms over complex numbers based on the Affine-Hill cipher method for encryption. We give some obtained results as a key matrix.

Let $p_1, p_2, p_3, \ldots, p_n$ be the plain text with numerical characters. We consider the plain text with complex number form, i.e.,

$$p_1 + p_2 i, p_3 + p_4 i, \ldots, p_{n-1} + p_n i. \qquad (11)$$

Define P_j as the j^{th} plain text in 2×2 matrix form, for $1 \le j \le l$ where $l = \left\lceil \frac{n}{8} \right\rceil$, is the smallest integer which is greater than or equal to the length of plain text divided by 8. If the plain text matrix

P_j is not suitable, a zero will be added to complete the matrix P_j.

Let us consider 37-characters with the numerical values in Table 2.

Table 2. The 37-characters with the numerical values

A	B	C	D	E	F	G	H	I	J
1	2	3	4	5	6	7	8	9	10
K	L	M	N	O	P	Q	R	S	T
11	12	13	14	15	16	17	18	19	20
U	V	W	X	Y	Z	0	1	2	3
21	22	23	24	25	26	27	28	29	30
4	5	6	7	8	9	blank			
31	32	33	34	35	36	37			

Example 4. 1 *Suppose the plain text with the characters "CHOOSE HAPPY" . In Table 2, we have the corresponding numerical characters as 3, 8, 15, 15, 19, 5, 37, 8, 1, 16, 16, and 25. Then, the length of plain text is 12. So, we have* $l=\left\lceil \frac{12}{8} \right\rceil = 2.$ *Finally, plain text with complex number forms become*

$3+8i, 15+15i, 19+5i, 37+8i, 1+16i, 16+25i,$

and then

$$P_1 = \begin{bmatrix} 3+8i & 15+15i \\ 19+5i & 37+8i \end{bmatrix},$$

and

$$P_2 = \begin{bmatrix} 1+16i & 16+25i \\ 0+0i & 0+0i \end{bmatrix}.$$

4.1 Encryption and Decryption Algorithms

We will explain the following new coding and decoding algorithms.

Firstly, we let ρ be a prime number and choose a private key G such that $1 < G < \phi(\rho)$ where $\phi(\rho)$ is the Euler's phi function. Then, we select δ_1 that is the primitive root of ρ and calculate δ_2 that $\delta_2 \equiv \delta_1^G \pmod{\rho}$. Finally, we have a public key, denoted $(\rho, \delta_1, \delta_2)$ and G as the private key.

Encryption Algorithm

Step 1: The sender chooses a secret number ς such that $1 < \varsigma < \phi(\rho)$.

Step 2: The sender calculates the signature α such that $\alpha \equiv \delta_1^{\varsigma} \pmod{\rho}$.

Step 3: The sender calculates the secret key λ such that $\lambda \equiv \delta_2^{\varsigma} \pmod{\rho}$.

Step 4: The sender constructs K as the key matrix of size 2×2 which is obtained in our results for $x=\alpha$ and $y=\lambda$.

Step 5: The sender constructs S as the shifting matrix of size 2×2.

Step 6: The sender calculates

$$C_j \equiv P_j K + S \pmod{\rho},$$

where P_j and C_j are j^{th} of 2×2 matrix of plain text and cipher text, respectively, for $1 \le j \le l$.

Finally, the sender will send (α, C) to the recipient for decoding the cipher text.

Decryption Algorithm

After receiving (α, C) , the recipient decrypts the cipher text with the following steps.

Step 1: The recipient calculates the secret key λ such that $\lambda \equiv \alpha^G \pmod{\rho}$.

Step 2: The recipient receives K as the key matrix with $x=\alpha,\ y=\lambda$ and calculates K^{-1}.

Step 3: The recipient receives S as the shifting matrix.

Step 4: The recipient calculates

$$P_j \equiv (C_j - S) K^{-1} \pmod{\rho}.$$

Note that: The prime number ρ shall be at least the number of different characters used in plain text and $\gcd(\det K, \rho) = 1$.

4.2 Numerical Example

We suppose the key matrix K is defined by B_2 that given in (4) and the shifting matrix S is defined by D_2 that given in (6), respectively. So, we have

$$K=\begin{bmatrix}3y^2 & 2y^2\\ -1 & ix^2\end{bmatrix} \text{ and } S=\begin{bmatrix}y^2 & ix^2\\ -2ix^2 & 3y^2\end{bmatrix}.$$

Example 4.2 *Assume that* $\rho=37$, *the key matrix* $K=B_n$, *private key* G *is* 11 *and primitive the root of* ρ, $\delta_1=5$. *Then we calculate* δ_2 *such that*
$\delta_2\equiv 5^{11} \equiv 2(mod 37)$. *So, the public key is* $(\rho,\delta_1,\delta_2)=(37,5,2)$.

We consider the plain text to be "STAY AT HOME" in encryption and decryption algorithms. Therefore, we obtain the plain text with numerical characters 19, 20, 1, 25, 0, 1, 20, 0, 8, 15, 13, 5 and $l=\lceil\frac{12}{8}\rceil=2$.

Then, the plain text matrix P_j for $1\le j\le 2$ become

$$P_1\equiv\begin{bmatrix}19+20i & 1+25i\\ 0+i & 20+0i\end{bmatrix}(\text{mod}\,37),$$

and

$$P_2\equiv\begin{bmatrix}8+15i & 13+5i\\ 0+0i & 0+0i\end{bmatrix}(\text{mod}\,37).$$

Encryption Algorithm:
Step 1: Choosing a secret number $\varsigma=32$.
Step 2: Calculating the signature :

$$\alpha\equiv 5^{32}\equiv 9\,(\text{mod}37).$$

Step 3: Calculating the secret key :

$$\lambda\equiv 2^{32}\equiv 7\,(\text{mod}37).$$

Step 4: We have K as the key matrix for $x=9$, $y=7$, is defined by

$$K=\begin{bmatrix}147 & 98\\ -1 & 81i\end{bmatrix}\equiv\begin{bmatrix}36 & 24\\ 36 & 7i\end{bmatrix}(\text{mod}\,37).$$

Step 5: We have S as shifting matrix for $x=9$, $y=7$, is defined by

$$S=\begin{bmatrix}49 & 81i\\ -162i & 147\end{bmatrix}\equiv\begin{bmatrix}12 & 7i\\ 23i & 36\end{bmatrix}(\text{mod}37).$$

Step 6: So, we have C_j cipher text for $j=1,2$, as follows:

$$C_1=\begin{bmatrix}19+20i & 1+25i\\ 0+i & 20+0i\end{bmatrix}\begin{bmatrix}36 & 24\\ 36 & 7i\end{bmatrix}+\begin{bmatrix}12 & 7i\\ 23i & 36\end{bmatrix}$$
$$\equiv\begin{bmatrix}29+29i & 22+13i\\ 17+22i & 36+16i\end{bmatrix}(\text{mod}\,37).$$

$$C_2=\begin{bmatrix}8+15i & 13+5i\\ 0+0i & 0+0i\end{bmatrix}\begin{bmatrix}36 & 24\\ 36 & 7i\end{bmatrix}+\begin{bmatrix}12 & 7i\\ 23i & 36\end{bmatrix}$$
$$\equiv\begin{bmatrix}28+17i & 9+14i\\ 0+23i & 36+0i\end{bmatrix}(\text{mod}\,37).$$

So, we have cipher text with numerical numbers as 29, 29, 22, 13, 17, 22, 36, 16, 28, 17, 9, 14, 0, 23, 36, 0 and sent the cipher text "22VMQV9P1QIN W9 " and signature $\alpha=9$ to the recipient.

Decryption Algorithm :
Step 1: Firstly, calculating the secret key from $\lambda\equiv 9^{11}(\text{mod}\,37)$. So, we have $\lambda=7$.

Step 2: Calculating K^{-1}. By Theorem 3.1, we obtain

$$\begin{aligned}\det K^{-1}&=p_5^{-1}(9,7)\\ &\equiv(24+30i)^{-1}(\text{mod}\,37)\\ &\equiv\frac{1}{1476}(24-30i)\;(\text{mod}\,37)\\ &\equiv 9(24+7i)\;(\text{mod}\,37)\\ &\equiv 31+26i\;(\text{mod}\,37).\end{aligned}$$

Then, we have

$$K^{-1}\equiv(31+26i)\begin{bmatrix}7i & 13\\ 1 & 36\end{bmatrix}(\text{mod}\,37)$$
$$\equiv\begin{bmatrix}3+32i & 33+5i\\ 31+26i & 6+11i\end{bmatrix}(\text{mod}\,37).$$

Step 3: Calculating the shifting matrix for $\lambda=7$, then

$$S\equiv\begin{bmatrix}12 & 7i\\ 23i & 36\end{bmatrix}(\text{mod}\,37).$$

Step 4: Finally, we decrypt the cipher text as follows.

$$P_1=\left(\begin{bmatrix}29+29i & 22+13i\\ 17+22i & 36+16i\end{bmatrix}-\begin{bmatrix}12 & 7i\\ 23i & 36\end{bmatrix}\right)\times\begin{bmatrix}3+32i & 33+5i\\ 31+26i & 6+11i\end{bmatrix}$$
$$\equiv\begin{bmatrix}19+20i & 1+25i\\ 0+i & 20+0i\end{bmatrix}(\text{mod}\,37).$$

$$P_2=\left(\begin{bmatrix}28+17i & 9+14i\\ 0+23i & 36+0i\end{bmatrix}-\begin{bmatrix}12 & 7i\\ 23i & 36\end{bmatrix}\right)$$

$$\times\begin{bmatrix}3+32i & 33+5i\\ 31+26i & 6+11i\end{bmatrix}$$
$$\equiv\begin{bmatrix}8+15i & 13+5i\\ 0+0i & 0+0i\end{bmatrix}\pmod{37}.$$

First, we receive the plain text with numerical characters after decrypting the cipher text, and then we decrypt it again to obtain "STAY AT HOME".

5 Discussion and Conclusion

In this paper, we have obtained the $n\times n$ Hessenberg matrices whose determinants and permanents are the odd and even terms of bivariate Perrin's complex polynomial. Moreover, we demonstrate the significance of these in the field of mathematics and cryptography and provide experimental evidence of their usefulness in cryptography applications. We have developed a method over complex numbers based on the Affine-Hill cipher method that requires an invertible key matrix. We have shown that our matrices can be used as the key matrix for encryption and decryption algorithms. In future work, these matrices may be applied in steganography. Finally, we hope that this will inspire further research in this area and provide a new algorithm for more secure encryption in the future.

Acknowledgment:
The author would like to sincerely appreciate the referees for their valuable comments and suggestions on the manuscript. This work is supported by Research and Development Institute, Sakon Nakhon Rajabhat University under Grant No.1/2022.

References:

[1] R. P. M. Vieira, M. C. dos Santos Mangueira, F. R. V. Alves and P. M. M. C. Catarino, Perrin's bivariate and complex polynomials, Notes on Number Theory and Discrete Mathematics, Vol.27, 2021, pp.70–78.

[2] E. Kilic and D. Tasci, On the generalized Fibonacci and Pell sequences by Hessenberg matrices, *Ars Combin*, Vol.94, 2010, pp.161–174.

[3] K. Kaygısız and A. Sahin, Calculating terms of associated polynomials of Perrin and Cordonnier numbers, *Notes on Number Theory and Discrete Mathematics*, Vol.20, 2014, pp.10–18.

[4] P. Kasempin, W. Vipismakul and A. Kaewsuy, Tridiagonal Matrices with Permanent Values Equal to k-Jacobsthal Sequence, *Asian Journal of Applied Sciences*, Vol.8, 2020, pp.269–274.

[5] F. Yilmaz and D. Bozkurt, Hessenberg matrices and the Pell and Perrin numbers, *Journal of Number Theory*, Vol.131, 2011, pp.1390–1396.

[6] K. Kaygısız and A. Sahin, Determinant and permanent of Hessenberg matrix and Fibonacci type numbers, *Gen*, Vo.9, 2012, pp.32–41.

[7] J. L. Cereceda, Determinantal representations for generalized Fibonacci and Tribonacci numbers, *Int. J. Contemp. Math. Sci*, Vol.9, 2014, pp.269–285.

[8] İ. Aktaş and H. Köse, On Special Number Sequences via Hessenberg Matrices, *Palestine Journal of Mathematics*, Vol.6, 2017, pp.94–100.

[9] N. Taş, S. Uçar and N. Y. Özgür, Pell coding and pell decoding methods with some applications, *Contributions to Discrete Mathematics*, Vol.15, 2020, pp.52–66.

[10] J. Shtayat and A. Al-Kateeb, An Encoding-Decoding algorithm based on Padovan numbers, 2019, arXiv preprint arXiv:1907.02007.

[11] M. Maxrizal, Hill Cipher Cryptosystem over Complex Numbers, *Indonesian Journal of Mathematics Education*, Vol.2, 2019, pp.9–13.

[12] M. Akbiyik and J. Alo, On Third-Order Bronze Fibonacci Numbers, *Mathematics*, Vol.9, 2021, 2606.

[13] N. Kamyun, K. Pingyot and S. Sompong, Encryption Schemes Using Anti-Orthogonal of Type I Matrices, *Thai Journal of Mathematics*, Vol.19, 2021, pp.1671–1683.

[14] D. R. Stinson, *Cryptography: theory and practice*, Chapman and Hall/CRC, 2005.

[15] M. Esmaeili, More on the Fibonacci sequence and Hessenberg matrices, *Integers*, Vol.6, 2006, A32.

[16] N. D. Cahill and D. Narayan, Fibonacci and Lucas numbers as tridiagonal matrix

determinants, *The Fibonacci Quarterly*, Vol.42, 2004, pp.216–285.

[17] A. A. Öcal, N. Tuglu and E. Altinişik, On the representation of k-generalized Fibonacci and Lucas numbers, *Applied mathematics and computation*, Vol.170, 2005, pp.584–596.

[18] K. Kaygısız and A. Sahin, Determinant and permanent of Hessenberg matrix and generalized Lucas polynomials, *Bulletin of the Iranian Mathematical Society*, Vol.39, 2013, pp.1065–1078.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The author equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

The research was financially supported by the Research and Development Institute, Sakon Nakhon Rajabhat University under Grant No.1/2022.

Conflict of Interest

The author has no conflict of interest to declare.