Communications in Combinatorics and Optimization
Vol. xx, No. xx (xxxx), pp. 1-15
https://doi.org/10.22049/cco.2024.28022.1419

CCO
Commun. Comb. Optim.

Research Article

A modified public key cryptography based on generalized Lucas matrices

Kalika Prasad[1,2], Munesh Kumari[1,2,†] and Hrishikesh Mahato[1,*]

[1]Department of Mathematics, Central University of Jharkhand, India
klkaprsd@gmail.com
[†]muneshnasir94@gmail.com
[*]hrishikesh.mahato@cuj.ac.in

[2]Department of Mathematics, Government Engineering College, Bhojpur, Bihar, India

Received: 2 October 2022; Accepted: 14 January 2024
Published Online: 25 January 2024

Abstract: In this paper, we propose a generalized Lucas matrix (a recursive matrix of higher order) obtained from the generalized Fibonacci sequences. We obtain their algebraic properties such as direct inverse calculation, recursive nature, etc. Then, we propose a modified public key cryptography using the generalized Lucas matrices as a key element that optimizes the keyspace construction complexity. Furthermore, we establish a key agreement for encryption-decryption with a combination of the terms of generalized Lucas sequences under the residue operation.

Keywords: affine Hill cipher, cryptography, Fibonacci sequence, Lucas sequence, Lucas matrix.

AMS Subject classification: 11T71, 11B39, 94A60.

1. Introduction

Matrix theory is rich in special properties, some of such properties are based on its construction, interrelations in eigenvalues and structure of its invertibility. Based on its construction, matrices are used in different branches of science as well as in engineering and technologies. One of such area is cryptography [19, 21], where matrix theory plays a vital role in storing data, efficiency of encryption-decryption and enlarging the key-spaces. Some recent developments on application of special matrices in cryptography can be seen in [6, 11, 16, 22, 24].

* *Corresponding Author*

© 2024 Azarbaijan Shahid Madani University

It is well known that recursive sequences are defined in the terms of sum, difference or product (elementary operations) on preceding terms of corresponding sequences. Nowadays a lot of research work is going on in the direction of generalizing the existing sequences for higher order as well as generalizing for arbitrary initial values. While some of the authors made generalizations by considering the same relation but with different multipliers (constant/arbitrary functions as coefficients), some of such recent developments and their applications can be seen in [1, 3, 12, 13, 23].
Cerda-Morales [2] defined a new generalized Lucas $V(p,q)$-matrix similar to the generalized Fibonacci $U(1,-1)$-matrix which is different from the Fibonacci $U(p,q)$-matrix and further, they established some well-known equalities and a Binet-like formula by matrix method for both generalized sequences. Halici et al. [7], discussed the Fibonacci quaternion matrix by considering entries as n-th Fibonacci quaternion number and derived some identities like Cassini's identity, Binet formula, etc. In [20] Stanimirovic et al. defined a generalization of Fibonacci and Lucas matrices whose elements are defined by the general second-order non-degenerated sequence and in some cases, they also obtained inverse for those matrices. Özkan et al. [15] obtained the terms of n-step Lucas polynomials by using matrices and generalizing the concept and then establishing the relationship between Lucas polynomials and Fibonacci polynomials. In [18], the authors discussed r-circulant matrices that are special recursive matrices and these matrices can also be considered in the study of formation of key elements for cryptography.
We know that the well-known sequences Fibonacci and Lucas sequence [9] are given by recurrence relation $f_{k+2} = f_k + f_{k+1},\ (k \geq 0)$ with initial values $0, 1$ and $2, 1$, respectively. Similarly, Tribonacci and Lucas sequences of order three are given by recurrence relation $f_{k+3} = f_k + f_{k+1} + f_{k+2},\ (k \geq 0)$ with initial values $0, 0, 1$ [A000073] and $3, 1, 3$ [A001644], respectively. Matrix representations [9] corresponding to the above recursive sequences of order two and three have been obtained as follow, where $f_{k,n}$ represents nth term of the sequence of order k:

$$\begin{bmatrix} f_{2,n+1} & f_{2,n} \\ f_{2,n} & f_{2,n-1} \end{bmatrix}, \quad \begin{bmatrix} f_{3,n+2} & f_{3,n+1} + f_{3,n} & f_{3,n+1} \\ f_{3,n+1} & f_{3,n} + f_{3,n-1} & f_{3,n} \\ f_{3,n} & f_{3,n-1} + f_{3,n-2} & f_{3,n-1} \end{bmatrix}.$$

These matrices are recursive in nature consisting of many properties based on initial values of corresponding sequences. For example, let us assume that Q_k^n be the matrix of order k representing multiplication of Q_k to n times. If we consider initial values $0, 1$ for order two and $0, 0, 1$ for order three then $(Q_k^1)^n = Q_k^n$ holds but for other initial values, it does not hold, some of such observations has been found in [8, 10, 14, 16, 25].
In this paper, we are working on generalizing the Lucas sequences to higher order preserving the Fibonacci trace properties (the terms of Lucas sequence are the trace of the corresponding Fibonacci matrices). Further, we implement these matrices in the Affine-Hill technique and examine its behavior and strength.
This paper is organized as follows. In Section 2, preliminaries on the cryptographic scheme, signature scheme and their mathematical formulation are discussed. In Sec-

tion 3, we establish the generalized Lucas sequence and associated matrix form from the generalized Fibonacci matrices and discuss some remarkable properties. In Section 4, we propose a new algorithm for key exchange and an encryption-decryption scheme with a numerical example. Finally, in Section 5 we discuss the complexity and strength of the proposed scheme followed by a conclusion in Section 6.

2. Encryption Scheme and Mathematical Flow

Let us assume that P be the plaintext $(p_1, p_2, ..., p_r)$, K be key matrix (simply key) and $C = (c_1, c_2, ..., c_r)$ be corresponding ciphertext of sizes $1 \times rn$, $r \times r$ and $1 \times rn$, respectively, where p_i and c_i are block vectors of size $1 \times n$. A polygraphic block cipher equivalent to Hill Cipher [19, 21] refer as Affine-Hill Cipher is described as:

$$\begin{aligned} Enc(P): \quad & c_i \equiv (p_i K + B) \pmod{p}, \\ Dec(C): \quad & p_i \equiv (c_i - B)K^{-1} \pmod{p}, \end{aligned}$$

with $(|K|, p) = 1$, where B is a $1 \times n$ row vector, p is a prime number and $Enc(P)$ represents encryption of P and $Dec(C)$ represents decryption of C.

2.1. ElGamal and Signature Scheme

Elgamal cryptosystem [19, 21], proposed by T. Elgamal [5] in 1984 is a public-key scheme with digital signature whose strength is based on discrete logarithms (closely related to Deffie-Hellman technique). One of such similar digital signatures is 'Schnorr signature scheme' [19] which minimizes the message based computation required to generate a signature. Usually, the digital signature scheme involves the use of a private key for the generation of the digital signature and a public key for its verification purpose. The design of the Elgamal technique is as encryption is done by user's public key while decryption using user's private key.

2.1.1. Primitive root

Primitive roots [19] play a crucial role in securing strength of cryptographic schemes. Let n be any positive integer, an integer α is called primitive root of n if $\alpha^k \equiv 1 \pmod{n}$ where $k = \phi(n)$ is least positive integer, i.e. there does not exists any $r, 1 \leq r < k$ such that $\alpha^r \equiv 1 \pmod{n}$. Further, when α is primitive root of n, the powers of α, $\alpha, \alpha^2, \alpha^3, ..., \alpha^{\phi(n)}$ are distinct $\pmod{n}$ and also co-prime to n. Note that not all integers have primitive roots, in fact integers of the form $2, 4, p^k$ *or* $2p^k$, where p is a odd prime and $k \in \mathbb{N}$, have primitive roots.
Similar to the Diffie-Hellman scheme, in the Elgamal technique, the global elements are the prime p and a primitive root of p. Steps of the Elgamal scheme are discussed in the following subsubsections.

2.1.2. Public key setup

Let us assume that p be any odd prime number, α be a primitive root of p and an integer D is chosen such that $1 < D < \phi(p)$. Now, assign $E_1 = \alpha$ and $E_2 = E_1^D \pmod{p}$. Then $pk(p, E_1, E_2)$ will be made as a public key and chosen D is kept as a secret key. Elgamal technique can be understood as follows. Suppose two parties Alice and Bob want to communicate with each other, then they go through the following path:

2.1.3. Key exchanging

Alice (who wish to send a message to Bob) first choose a random integer e such that $1 < e < \phi(p)$ and then generates a signature key (say s) using public key $pk(p, E_1, E_2)$ where $s = E_1^e \pmod{p}$. Now she computes her secret key λ for encryption as $\lambda = E_2^e \pmod{p}$. Thus, Alice generates the parameters (λ, s) of an encryption key using Bob's public key (p, E_1, E_2), then encrypt the plaintext with the encryption key and send (λ, C) to Bob, where C is the corresponding ciphertext.

2.1.4. Key recover by Bob

On the other side Bob after receiving (s, C) from Alice, recover the same parameters (λ, s) of encryption key using his secret key $sk(D)$ as:

$$\begin{aligned} s^D \pmod{p} &\equiv (E_1^e)^D \pmod{p} \\ &\equiv (E_1^D)^e \pmod{p} \equiv (E_2)^e \pmod{p} = \lambda. \end{aligned} \tag{2.1}$$

Thus, Bob and Alice agree on the same parameters (λ, s) of encryption key, i.e. the parameters (λ, s) of encryption key exchanged securely and using these parameters, Bob can decrypt the ciphertext C and recover the original plaintext P.

3. Generalized Lucas Sequences and Matrix Construction

In this section, we discuss about the construction of the generalized Lucas sequences and matrices. Then, we present some algebraic properties for generalized Lucas matrices and connection with the generalized Fibonacci matrices.

3.1. Generalized Fibonacci matrices (GFM)

For $n \in \mathbb{Z}$, the generalized Fibonacci sequences $\{f_{k,n}\}$ of order $k \geq 2$ is defined as

$$f_{k,k+n} = f_{k,k+n-1} + f_{k,k+n-2} + f_{k,k+n-3} + \cdots + f_{k,n+1} + f_{k,n}, \tag{3.1}$$

where $f_{k,0} = f_{k,1} = f_{k,2} = \cdots = f_{k,k-2} = 0$ and $f_{k,k-1} = 1$.
The corresponding generalized Fibonacci matrix of order k [16] is denoted by Q_k^n and

defined as

$$Q_k^n = \begin{bmatrix} f_{k,k+n-1} & f_{k,k+n-2}+f_{k,k+n-3}+\cdots+f_{k,n} & \cdots & f_{k,k+n-2} \\ f_{k,k+n-2} & f_{k,k+n-3}+f_{k,k+n-4}+\cdots+f_{k,n-1} & \cdots & f_{k,k+n-3} \\ \vdots & \vdots & \ddots & \vdots \\ f_{k,k+n-(k-1)} & f_{k,n}+f_{k,n-1}+\cdots+f_{k,-k+n+2} & \cdots & f_{k,n} \\ f_{k,n} & f_{k,n-1}+f_{k,n-2}+\cdots+f_{k,-k+n+1} & \cdots & f_{k,n-1} \end{bmatrix},$$

where initial matrices are given by

$$Q_k = Q_k^1 = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \quad \text{and} \quad Q_k^{-1} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & -1 & -1 & \cdots & -1 & -1 \end{bmatrix}_{k\times k}.$$

Theorem 1. *[16] Let $2 \le k \in \mathbb{N}$, $n \in \mathbb{Z}$, Q_k^n be the generalized Fibonacci matrix and I_k is the identity matrix of order k then following properties hold true.*

1. $(Q_k^1)^n = Q_k^n$ *and* $(Q_k^{-1})^n = Q_k^{-n}$.
2. $Q_k^n Q_k^l = Q_k^{n+l} = Q_k^l Q_k^n$.
3. $Q_k^n Q_k^{-n} = Q_k^0 = I_k$.
4. $\det(Q_k^n) = [(-1)^{k-1}]^n = (-1)^{(k-1)n}$.

By virtue of [17], we use the following lemma to prove new results.

Lemma 1. *Let Q_k^1 be the first Fibonacci matrix of order k and $A = (a_{ij})$ be any square matrix of same size, then on multiplication with Q_k^1 to A, the first row of $Q_k^1 A$ will be the sum of corresponding columns of A and second row to k^{th}-row of $Q_k^1 A$ becomes first to $(k-1)^{kth}$ rows of A, respectively.*

Proof. It can be easily proved by usual matrix multiplication of Q_k^1 and A. □

3.2. Generalized Lucas Matrices (GLM)

A study on construction of generalized Lucas matrices from k-step Fibonacci sequence has been presented in [17]. Now, we investigate the generalized Lucas matrices (abbr. as GLM) analogous to generalized Fibonacci matrices and then we give their algebraic properties.

Definition 1. The generalized Lucas sequence $\{l_{k,n}\}_{n\ge 0}$ of order $k \ge 2$ is defined as

$$l_{k,k+n} = l_{k,k+n-1} + l_{k,k+n-2} + l_{k,k+n-3} + \cdots + l_{k,n+2} + l_{k,n+1} + l_{k,n}, \qquad (3.2)$$
$$\text{where } l_{k,r} = trace(Q_k^r),\ 0 \le r < k.$$

The initial values for the above Lucas sequence is obtained by taking trace of the first k generalized Fibonacci matrices. From equation (3.2) and by the definition of Q_k^n, we have

$$\begin{aligned} l_{k,n} &= trace(Q_k^n) \\ &= f_{k,k+n-1} + 1f_{k,k+n-3} + 2f_{k,k+n-4} + 3f_{k,k+n-5} + ... + (k-3)f_{k,n+1} \\ &\quad +(k-2)f_{k,n} + (k-1)f_{k,n-1} \\ &= f_{k,k+n-1} + \sum_{i=n-1}^{k+n-3} f_{k,i} + \sum_{i=n-1}^{k+n-4} f_{k,i} + ... + \sum_{i=n-1}^{n-2} f_{k,i} + \sum_{i=n-1}^{n-1} f_{k,i} \end{aligned} \tag{3.3}$$

which yields $k, 1, 3, 7, 15, 31, 63, 127, 255, 511, ..., 2^{k-1} - 1$ as initial values of $l_{k,n}$. Since the generalized Fibonacci sequences $\{f_{k,n}\}$ and generalized Fibonacci matrices $\{Q_k^n\}$ are both two ended sequences, so the new sequence $\{l_{k,n}\}$ can also be extended in negative direction. In particular, for $k = 2$ it gives the standard Lucas sequence and for $k = 3$, the Tribonacci-Lucas sequence.

A recursive matrix $L_k^{(n)}$ corresponding to the above generalized Lucas sequence is given [17] as

$$L_k^{(n)} = \begin{bmatrix} l_{k,k+n-1} & l_{k,k+n-2} + \cdots + l_{k,n} & l_{k,k+n-2} + \cdots + l_{k,n+1} & \cdots & l_{k,k+n-2} \\ l_{k,k+n-2} & l_{k,k+n-3} + \cdots + l_{k,n-1} & l_{k,k+n-3} + \cdots + l_{k,n} & \cdots & l_{k,k+n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ l_{k,k+n-(k-1)} & l_{k,n} + \cdots + l_{k,-k+n+2} & l_{k,n} + \cdots + l_{k,-k+n+3} & \cdots & l_{k,n} \\ l_{k,k+n-k} & l_{k,n-1} + \cdots + l_{k,-k+n+1} & l_{k,n-1} + \cdots + l_{k,-k+n+2} & \cdots & l_{k,n-1} \end{bmatrix}. \tag{3.4}$$

The matrix $L_k^{(n)}$ refers to the generalized Lucas matrix of order k, thus the initial Lucas matrix $L_k^{(0)}$ is

$$L_k^{(0)} = \begin{bmatrix} 2^{k-1}-1 & 2^{k-1} & 2^{k-1}-k & \cdots & 7(2^{k-4}) & 3(2^{k-3}) & 2^{k-2}-1 \\ 2^{k-2}-1 & 2^{k-2} & 2^{k-2}+1 & \cdots & 7(2^{k-5}) & 3(2^{k-4}) & 2^{k-3}-1 \\ 2^{k-3}-1 & 2^{k-3} & 2^{k-3}+1 & \cdots & 7(2^{k-6}) & 3(2^{k-5}) & 2^{k-4}-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \\ 1 & 2 & 3 & \cdots & k-2 & k-1 & k \\ k & 1-k & 2-k & \cdots & -3 & -2 & -1 \end{bmatrix}. \tag{3.5}$$

Example 1. Initial Lucas matrices of orders two, three, four and five are

$$\begin{bmatrix} 1 & 2 \\ 2 & -1 \end{bmatrix}, \begin{bmatrix} 3 & 4 & 1 \\ 1 & 2 & 3 \\ 3 & -2 & -1 \end{bmatrix}, \begin{bmatrix} 7 & 8 & 4 & 3 \\ 3 & 4 & 5 & 1 \\ 1 & 2 & 3 & 4 \\ 4 & -3 & -2 & -1 \end{bmatrix} \text{ and } \begin{bmatrix} 15 & 16 & 11 & 10 & 7 \\ 7 & 8 & 9 & 4 & 3 \\ 3 & 4 & 5 & 6 & 1 \\ 1 & 2 & 3 & 4 & 5 \\ 5 & -4 & -3 & -2 & -1 \end{bmatrix}, \text{ respectively.}$$

Theorem 2. *Let $n \in \mathbb{Z}$ and $L_k^{(n)}$ be the generalized Lucas matrix. Suppose $L_k^{(0)}$ be the initial Lucas matrix as defined in equation (3.5). Then we have*

$$L_k^{(n)} = Q_k^n L_k^{(0)} = L_k^{(0)} Q_k^n. \tag{3.6}$$

Proof. We prove it using mathematical induction on n for $n \geq 1$. For $n = 0$, the result holds obviously. For $n = 1$, we have

$$Q_k^1 L_k^{(0)} = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{bmatrix} \begin{bmatrix} 2^{k-1}-1 & 2^{k-1} & 2^{k-1}-k & \cdots & 7(2^{k-4}) & 3(2^{k-3}) & 2^{k-2}-1 \\ 2^{k-2}-1 & 2^{k-2} & 2^{k-2}+1 & \cdots & 7(2^{k-5}) & 3(2^{k-4}) & 2^{k-3}-1 \\ 2^{k-3}-1 & 2^{k-3} & 2^{k-3}+1 & \cdots & 7(2^{k-6}) & 3(2^{k-5}) & 2^{k-4}-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \\ 1 & 2 & 3 & \cdots & k-2 & k-1 & k \\ k & 1-k & 2-k & \cdots & -3 & -2 & -1 \end{bmatrix}$$

Now using Lemma 1, we can write

$$Q_k^1 L_k^{(0)} = \begin{bmatrix} 2^k-1 & 2^k-k-1 & 2^k-2-k & \cdots & 7(2^{k-3}) & 3(2^{k-2}) & 2^{k-1}-1 \\ 2^{k-1}-1 & 2^{k-1} & 2^{k-1}-k & \cdots & 7(2^{k-4}) & 3(2^{k-3}) & 2^{k-2}-1 \\ 2^{k-2}-1 & 2^{k-2} & 2^{k-2}+1 & \cdots & 7(2^{k-5}) & 3(2^{k-4}) & 2^{k-3}-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & & \\ 1 & 2 & 3 & \cdots & k-2 & k-1 & k \end{bmatrix} = L_k^{(1)}$$

Now, we assume that the result is true for $n = r$, i.e. $Q_k^r L_k^{(0)} = L_k^{(r)}$ and show that the given statement holds valid for $n = r + 1$. Using Lemma 1, we have,

$$\begin{aligned} Q_k^{r+1} L_k^{(0)} &= Q_k^1 Q_k^r L_k^{(0)} = Q_k^1 L_k^{(r)} \\ &= Q_k^1 \begin{bmatrix} l_{k,k+r-1} & l_{k,k+r-2}+l_{k,k+r-3}+\cdots+l_{k,r} & \cdots & l_{k,k+r-2} \\ l_{k,k+r-2} & l_{k,k+r-3}+l_{k,k+r-4}+\cdots+l_{k,r-1} & \cdots & l_{k,k+r-3} \\ \vdots & \vdots & \ddots & \vdots \\ l_{k,k+r-(k-1)} & l_{k,r}+l_{k,r-1}+\cdots+l_{k,-k+r+2} & \cdots & l_{k,r} \\ l_{k,k+r-k} & l_{k,r-1}+l_{k,r-2}+\cdots+l_{k,-k+r+1} & \cdots & l_{k,r-1} \end{bmatrix} \\ &= \begin{bmatrix} l_{k,k+r} & l_{k,k+r-1}+l_{k,k+r-2}+\cdots+l_{k,r+1} & \cdots & l_{k,k+r-1} \\ l_{k,k+r-1} & l_{k,k+r-2}+l_{k,k+r-3}+\cdots+l_{k,r} & \cdots & l_{k,k+r-2} \\ l_{k,k+r-2} & l_{k,k+r-3}+l_{k,k+r-4}+\cdots+l_{k,r-1} & \cdots & l_{k,k+r-3} \\ \vdots & \vdots & \ddots & \vdots \\ l_{k,k+r-(k-1)} & l_{k,r}+l_{k,r-1}+\cdots+l_{k,-k+r+2} & \cdots & l_{k,r} \end{bmatrix} \\ &= L_k^{(r+1)}. \end{aligned}$$

For negative direction, consider $n = -r$, where $r \geq 0$. Then by mathematical induction on r, it can be easily proved for negative direction with a similar argument. Combining both the cases, the result holds for all $n \in \mathbb{Z}$. The second equality can be proved in a similar way. □

Corollary 1. *For $k, n \in \mathbb{N}$,, we have* $L_k^{(-n)} = Q_k^{-n} L_k^{(0)}$.

Theorem 3. *Let $n \in \mathbb{N}$, then we have* $(L_k^{(1)})^n = (L_k^{(n)})(L_k^{(0)})^{n-1}$.

Proof. Using Theorem 2, we write

$$\begin{aligned}(L_k^{(1)})^n &= (Q_k^1 L_k^{(0)})^n = \underbrace{Q_k^1 L_k^{(0)} Q_k^1 L_k^{(0)} \cdots Q_k^1 L_k^{(0)}}_{\text{n-times}} = (Q_k^1)^n (L_k^{(0)})^n \\ &= (Q_k^n)(L_k^{(0)})^n = (Q_k^n L_k^{(0)})(L_k^{(0)})^{n-1} = (L_k^{(n)})(L_k^{(0)})^{n-1}.\end{aligned}$$

□

Theorem 4. *The determinant of the generalized Lucas matrices are given by*

$$\det(L_k^{(n)}) = \begin{cases} \det(L_k^{(0)}) & \text{if } k \text{ is odd,} \\ (-1)^n \det(L_k^{(0)}) & \text{if } k \text{ is even.} \end{cases}$$

Proof. We have

$$\begin{aligned}\det(L_k^{(n)}) &= \det(Q_k^{(n)} L_k^{(0)}) = \det(Q_k^n) \det(L_k^{(0)}) = (-1)^{(k-1)n} \det(L_k^{(0)}) \\ &= \begin{cases} \det(L_k^{(0)}) & \text{if } k \text{ is odd,} \\ (-1)^n \det(L_k^{(0)}) & \text{if } k \text{ is even.} \end{cases}\end{aligned}$$

□

Theorem 5. *For $m, n \in \mathbb{Z},\ 2 \le k \in \mathbb{N}$, we have*

$$L_k^{(m)} L_k^{(n)} = L_k^{(m+n)} L_k^{(0)} = L_k^{(n)} L_k^{(m)}. \tag{3.7}$$

Proof. From Theorem 2 and Theorem 1, we have

$$\begin{aligned} L_k^{(m)} L_k^{(n)} &= Q_k^{(m)} L_k^{(0)} Q_k^{(n)} L_k^{(0)} = Q_k^{(m)} Q_k^{(n)} L_k^{(0)} L_k^{(0)} = Q_k^{(m+n)} L_k^{(0)} L_k^{(0)} \\ &= L_k^{(m+n)} L_k^{(0)}, \\ \text{and} \quad L_k^{(n)} L_k^{(m)} &= Q_k^{(n)} L_k^{(0)} Q_k^{(m)} L_k^{(0)} = Q_k^{(n)} Q_k^{(m)} L_k^{(0)} L_k^{(0)} = Q_k^{(m+n)} L_k^{(0)} L_k^{(0)} \\ &= L_k^{(m+n)} L_k^{(0)}. \end{aligned}$$

Thus, this completes the proof. □

Corollary 2. *For $2 \le k \in \mathbb{N},\ n \in \mathbb{Z}$, we have* $L_k^{(n)} L_k^{(0)} = L_k^{(0)} L_k^{(n)}$.

Theorem 6. *Let $L_k^{(n)}$ be the generalized Lucas matrix and Q_k^n be the generalized Fibonacci matrix. Then*

$$\forall\ n \in \mathbb{Z}, \quad L_k^{(n)} L_k^{(-n)} = H, \text{ where } H = (L_k^{(0)})^2.$$

Proof. For $n \in \mathbb{N}$, we have

$$L_k^{(n)} L_k^{(-n)} = Q_k^n L_k^{(0)} Q_k^{-n} L_k^{(0)} = Q_k^n Q_k^{-n} L_k^{(0)} L_k^{(0)} = I_k H = H.$$

□

Theorem 7. *Suppose $L_k^{(n)}$ be the generalized Lucas matrix and $H = (L_k^{(0)})^2$ is invertible. Then*

$$(L_k^{(n)})^{-1} = L_k^{(-n)} H^{-1}.$$

Proof. Since $L_k^{(n)} L_k^{(-n)} = H$ and $(L_k^{(0)})$ is an invertible matrix, H is invertible. Now, we get

$$L_k^{(n)}(L_k^{(-n)} H^{-1}) = I_k; \qquad I_k \text{ is identity matrix.}$$

Thus for every generalized Lucas matrix $L_k^{(n)}$, there is an unique matrix $L_k^{(-n)} H^{-1}$ such that their product is an identity matrix. Hence

$$(L_k^{(n)})^{-1} = L_k^{(-n)} H^{-1}. \qquad \square$$

Lemma 2. *Let p be a prime number. Then for a generalized Lucas matrix L, we have*

$$\det(L) \pmod p = \det(L \pmod p). \tag{3.8}$$

Theorem 8. *[19] Let $A = (a_{ij})$ be any matrix. Then*

$$A \pmod p = [a_{ij} \pmod p].$$

4. Encryption Scheme and Algorithm

Let us assume that the receiver's public key is $pk(p, E_1, E_2)$ whose components are constructed by receiver (Bob) as discussed in Subsection (2.1.2). Now, a sender (Alice) constructs a secret key (say λ) with this public key by choosing a restricted integer and form an encryption matrix with their signature. Further, after receiving the encrypted message with the signature from Alice, Bob retrieve the secret key (λ) and after some calculation recover the plain text (see Section 2.1). In the following algorithm, we summarizes the methodology.

4.1. Algorithm

Encryption algorithm (sender have access to $pk(p, E_1, E_2)$):

1. Sender (Alice) first chooses a secret number e, such that $1 < e < \phi(p)$.
2. **Signature:** $s \leftarrow E_1^e \pmod p$.
3. **Secret key:** $\lambda \leftarrow E_2^e \pmod p$.
4. Initiate Lucas sequence $\{l_{\lambda,s}\}$ of order λ.
5. **Key matrix:** $K \leftarrow L_\lambda^{(s)} \pmod p$, where $L_\lambda^{(s)}$ may be obtained from Step-4 and equation (3.4).

6. **Shift vector:** $B \leftarrow [l_{\lambda,\lambda}, l_{\lambda,\lambda+1}, ..., l_{\lambda,2\lambda-1}]$ of size $1 \times \lambda$ (using Step-4).
7. **Encryption:** $C = Enc(P): \quad c_i \leftarrow (p_i K + B) \pmod{p}$.
8. transmit (C, s) to Bob.

Decryption algorithm: After receiving (C, s) from sender.

1. **Secret key:** $\lambda \leftarrow s^D \pmod{p}$, where D is Bob's chosen secret key.
2. Initiate Lucas sequence $\{l_{\lambda,s}\}$.
3. **Key matrix:** $K^* \leftarrow L_\lambda^{(-s)} H^{-1} \pmod{p}$, where both $L_\lambda^{(-s)}$ and $H = (L_\lambda^{(0)})^2$ may be obtained from Step-2 using equations (3.4) and (3.5), respectively.
4. **Shift vector:** $B \leftarrow [l_{\lambda,\lambda}, l_{\lambda,\lambda+1}, \ldots, l_{\lambda,2\lambda-1}]$ of size $1 \times \lambda$ (using step-2).
5. **Decryption:** $P = Dec(C): \quad p_i \leftarrow (c_i - B)K^* \pmod{p}$.
6. Plaintext (P) is recovered.

4.2. Example

Example 2. Let us assume that Alice (sender) wish to send a message to Bob (receiver). Consider the prime number $p = 37$. Establish the public key and secret key of communication for Bob.

Solution. Bob first chooses an integer D such that $1 < D < \phi(37) = 36$, say $D = 10$. The set of primitive roots of 37 is given as X= {2, 5, 13, 15, 17, 18, 19, 20, 22, 24, 32, 35 }. Now, Bob selects a primitive root say $\alpha = 17$ of p from X. According to public key setup (2.1.2), Bob assigns $E_1 = 17, E_2 = E_1^D \pmod{p} \equiv 17^{10} \pmod{37} \equiv 28$. Thus the public key $pk(p, E_1, E_2)$ for Bob is $pk(37, 17, 28)$ and secret key is $sk(10)$. Now using $pk(37, 17, 28)$ anyone can send message to Bob (explained in next example). □

Example 3 (Encryption-decryption). Using $pk(37, 17, 28)$, construct the key matrix and shift vector and encrypt the plaintext **NOBLE2022**.

Solution. Here, the numerical values equivalent to **NOBLE2022** is $[13, 14, 01, 11, 04, 28, 26, 28, 28]$. Let us consider the alphabets $\Sigma = \mathbb{Z}_{37}$ defined as: the letters A - Z equivalent to 00 - 25, digits 0 - 9 are equivalent to 26 - 35 and 36 for the blank/white space. Now, according Algorithm 4.1,

- Alice first choose an integer e such that $1 < e < \phi(37)$, say $e = 23$.
- Then, Alice makes signature (s) as $s = E_1^e = 17^{23} \pmod{37} \equiv 18$.
- Thus secret key for Alice is $\lambda = E_2^e = 28^{23} \pmod{37} \equiv 3$ and the key matrix is $K = L_\lambda^{(s)} \pmod{p}$.

Hence $K = L_3^{(18)} \pmod{37}$ is

$$\begin{aligned} K &= \begin{bmatrix} l_{3,20} & l_{3,19}+l_{3,18} & l_{3,19} \\ l_{3,19} & l_{3,18}+l_{3,17} & l_{3,18} \\ l_{3,18} & l_{3,17}+l_{3,16} & l_{3,17} \end{bmatrix} \pmod{37} \\ &= \begin{bmatrix} 196331 & 164778 & 106743 \\ 106743 & 89588 & 58035 \\ 58035 & 48708 & 31553 \end{bmatrix} \pmod{37} = \begin{bmatrix} 9 & 17 & 35 \\ 35 & 11 & 19 \\ 19 & 16 & 29 \end{bmatrix} \end{aligned}$$

which is obtained by substituting the values of the corresponding terms of the generalized Lucas sequence for $\lambda = 3$ (it is given in the following table).

index (n)	$\cdots$	-1	0	1	2	3	4	5	6	$\cdots$	15	16	17	18	19	20	$\cdots$
Lucas Seq.($l_{3,n}$)	$\cdots$	-1	**3**	**1**	**3**	7	11	21	39	$\cdots$	9327	17155	31553	58035	106743	196331	$\cdots$

Table 1. **Lucas sequence of order 3**

Then, shift vector is B, where $\mathrm{B} = [l_{3,3}, l_{3,4}, l_{3,5}] = [07, 11, 21]$. Now divide the plaintext **NOBLE2022** in blocks of size $1 \times \lambda$ as follows:

$P_1 = [\ N\ O\ B] = [13\ \ 14\ \ 01], P_2 = [L\ E\ 2] = [11\ 04\ 28]$ and $P_3 = [0\ 2\ 2] = [26\ 28\ 28]$.

Encryption takes places as: $C_i \leftarrow (P_iK + B) \pmod{37}$.

$$\begin{aligned} C_1 &= (P_1K + B) \equiv \left(\begin{bmatrix} 13 & 14 & 01 \end{bmatrix} \begin{bmatrix} 9 & 17 & 35 \\ 35 & 11 & 19 \\ 19 & 16 & 29 \end{bmatrix} + \begin{bmatrix} 07 & 11 & 21 \end{bmatrix} \right) \pmod{37} \\ &\equiv (04\ \ 32\ \ 31) \sim (E\ 7\ 6) \\ C_2 &= (P_2K + B) \equiv \left(\begin{bmatrix} 11 & 04 & 28 \end{bmatrix} \begin{bmatrix} 9 & 17 & 35 \\ 35 & 11 & 19 \\ 19 & 16 & 29 \end{bmatrix} + \begin{bmatrix} 07 & 11 & 21 \end{bmatrix} \right) \pmod{37} \\ &\equiv (01\ \ 24\ \ 36) \sim (B\ Y\ \square) \\ C_3 &= (P_3K + B) \equiv \left(\begin{bmatrix} 26 & 28 & 28 \end{bmatrix} \begin{bmatrix} 9 & 17 & 35 \\ 35 & 11 & 19 \\ 19 & 16 & 29 \end{bmatrix} + \begin{bmatrix} 07 & 11 & 21 \end{bmatrix} \right) \pmod{37} \\ &\equiv (14\ \ 25\ \ 18) \sim (O\ Z\ S). \end{aligned}$$

Thus, Alice encrypted the plaintext **NOBLE2022** to **E76BY□OZS**, and send it to Bob along with her signature, i.e Alice sends $\{s = 18, C = C_1C_2C_3\}$ to Bob.

Decryption: On the other side, Bob receives (C, s) from Alice. To construct

the decryption key K^*, Bob first recovers λ. It can be obtained using their secret key D as follow:

$$\lambda = s^D \pmod{37} = 18^{10} \pmod{37} \equiv 3.$$

Thus $K^* = L_3^{(-s)} H^{-1} \pmod{p}$, where $H = (L_3^{(0)})^2 = \begin{bmatrix} 16 & 18 & 14 \\ 14 & 2 & 4 \\ 4 & 10 & -2 \end{bmatrix}$ is given as

$$\begin{aligned} K^* &= L_3^{(-18)} H^{-1} \pmod{37} \\ &= \begin{bmatrix} l_{3,-16} & l_{3,-17}+l_{3,-18} & l_{3,-17} \\ l_{3,-17} & l_{3,-18}+l_{3,-19} & l_{3,-18} \\ l_{3,-18} & l_{3,-19}+l_{3,-20} & l_{3,-19} \end{bmatrix} \frac{1}{44} \begin{bmatrix} -1 & 4 & 1 \\ 1 & -2 & 3 \\ 3 & -2 & -5 \end{bmatrix} \pmod{37} \\ &= \frac{1}{44} \begin{bmatrix} -253 & 318 & 271 \\ 271 & -524 & 47 \\ 47 & -224 & -571 \end{bmatrix} \begin{bmatrix} -1 & 4 & 1 \\ 1 & -2 & 3 \\ 3 & -2 & -5 \end{bmatrix} \pmod{37} \\ &= \begin{bmatrix} 18 & 36 & 7 \\ 7 & 11 & 29 \\ 29 & 15 & 19 \end{bmatrix}. \end{aligned}$$

Clearly, $KK^* = I \pmod{37}$ (by Theorem 7). The shift vector B is recovered by λ as $B = [l_{3,3}, l_{3,4}, l_{3,5}] = [07, 11, 21]$. Note that entries of both L_3^{-18} and H may be obtained from Table 1. Here, the plaintext can be obtained by $P_i \leftarrow (C_i - B)K^* \pmod{37}$ as follows:

$$\begin{aligned} P_1 &= (C_1 - B)K^* \equiv \left(\begin{bmatrix} 04 & 32 & 31 \end{bmatrix} - \begin{bmatrix} 07 & 11 & 21 \end{bmatrix}\right) \begin{bmatrix} 18 & 36 & 7 \\ 7 & 11 & 29 \\ 29 & 15 & 19 \end{bmatrix} \pmod{37} \\ &\equiv (13 \;\; 14 \;\; 01) \sim (N \; O \; B) \\ P_2 &= (C_2 - B)K^* \equiv \left(\begin{bmatrix} 01 & 24 & 36 \end{bmatrix} - \begin{bmatrix} 07 & 11 & 21 \end{bmatrix}\right) \begin{bmatrix} 18 & 36 & 7 \\ 7 & 11 & 29 \\ 29 & 15 & 19 \end{bmatrix} \pmod{37} \\ &\equiv (11 \;\; 04 \;\; 28) \sim (L \; E \; 2) \\ P_3 &= (C_3 - B)K^* \equiv \left(\begin{bmatrix} 14 & 25 & 18 \end{bmatrix} - \begin{bmatrix} 07 & 11 & 21 \end{bmatrix}\right) \begin{bmatrix} 18 & 36 & 7 \\ 7 & 11 & 29 \\ 29 & 15 & 19 \end{bmatrix} \pmod{37} \\ &\equiv (26 \;\; 28 \;\; 28) \sim (0 \; 2 \; 2). \end{aligned}$$

Thus, the plaintext **NOBLE2022** successfully received by Bob. □

5. Strength Analysis

In the above proposed scheme, the generalized Lucas matrix and Elgamal technique have been considered as a key element of the system and decryption matrix is set up as $L_\lambda^{(-s)}H^{-1}$ constructed with combinations of terms of generalized Lucas sequence. The construction of key matrices is quite easy for authorized parties as λ are known for both of them but it is very difficult for an adversary to obtain λ, as the adversary needs to solve a discrete logarithm problem [5]. Further, matrix construction is based on only two elements (λ, s), so it reduces time complexity as well as space complexity of key formation and calculation of its inverse. In context of attacks based on public data, one of the popular attacks is brute force attack [19, 21]. In case of brute force attack, the adversary needs to calculate λ which is almost impossible (discrete logarithm problem), and the next challenge for the adversary is to identify the correct key matrix out of $|GL(\lambda)|$ matrices, where $GL(\lambda)$ represents the general linear group [4] of order λ and is given by

$$|GL_\lambda(F_p)| = (p^\lambda - p^{\lambda-1})(p^\lambda - p^{\lambda-2})\cdots(p^\lambda - p^1)(p^\lambda - 1) \tag{5.1}$$

From equation (5.1), it is clear that security for the generalized Lucas matrices $L_\lambda^{(s)}$ depends on λ only, not on signature s. So s does not compromise the security even though it is known to the adversary. For example, consider $p = 37$ and $\lambda = 50$, then by equation (5.1) total number of possible key space over $\mathbb{F}_{37}$ is approximately 3.105×10^{3920} which is too large. And in case of λ and/or prime p increasing, then the key space grows exponentially.

6. Conclusion

Here, we studied the generalized Lucas matrices that is constructed with a linear combinations of the generalized Fibonacci sequences. We studied their algebraic properties such as direct calculation of its inverse, recursive nature, product of two matrices, etc. We observed that the generalized Lucas matrices $GLM(\lambda, s)$ do not form a multiplicative group but there exists unique inverse (matrix) for each $GLM(\lambda, s)$, i.e. for every integer s, we have matrix $K^* = L_\lambda^{(-s)}H^{-1}$ such that $L_\lambda^s K^* = K^* L_\lambda^s = I_\lambda$, and it plays an important role in construction of keyspace for a cryptography.
Later, we proposed a modified public key cryptography using Affine-Hill cipher and Elgamal signature scheme with generalized Lucas matrices as a key element. The generalized Lucas matrices as key component in cryptosystem enlarges the keyspace, reduces the time complexity as well as the space complexity of key formation. The proposed method is based on construction with two parameters and has three digital signatures (λ, s and shift vector(B)) that strengthen the security of the modified cryptography. Since λ is known only to both the end parties (Alice and Bob), so shift vector B constructed with λ is also known only to Alice and Bob. Thus it is practically impossible to recover λ by anyone else as it is based on discrete logarithm

problem. Hence, the proposed method is mathematically simple for authorized party and tedious for an intruder, mathematically strong and have a large keyspace.

Acknowledgment. The authors are very grateful to the anonymous reviewers for carefully reading the manuscript and giving insightful comments. The first and second authors would like to thank the University Grant Commission (UGC), India for the Senior research fellowship.

Conflict of interest. The authors declare that they have no conflict of interest.

Data Availability. Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

References

[1] G. Bilgici, *Two generalizations of Lucas sequence*, Appl. Math. Comput. **245** (2014), 526–538.
https://doi.org/10.1016/j.amc.2014.07.111.

[2] G. Cerda-Morales, *On generalized Fibonacci and Lucas numbers by matrix methods*, Hacet. J. Math. Stat. **42** (2013), no. 2, 173–179.

[3] A. Demir, N. Omur, and Y.T. Ulutas, *Optimization by k-Lucas numbers*, Appl. Math. Comput. **197** (2008), no. 1, 366–371.
https://doi.org/10.1016/j.amc.2007.07.045.

[4] D.S. Dummit and R.M. Foote, *Abstract Algebra*, Wiley Hoboken, 2004.

[5] T. ElGamal, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Inf. Theory **31** (1985), no. 4, 469–472.
https://doi.org/10.1109/TIT.1985.1057074.

[6] I. Gupta, J. Singh, and R. Chaudhary, *Cryptanalysis of an extension of the Hill cipher*, Cryptologia **31** (2007), no. 3, 246–253.
https://doi.org/10.1080/01611190701202465.

[7] S. Halici and Ö. Deveci, *On Fibonacci quaternion matrix*, Notes Number Theory Discrete Math. **27** (2021), no. 4, 236–244.
https://doi.org/10.7546/nntdm.2021.27.4.236-244.

[8] C.H. King, *Some further properties of the Fibonacci numbers*, Master's thesis, San Jose State, San Jose, CA, 1960.

[9] T. Koshy, *Fibonacci and Lucas Numbers with Applications, Volume 2*, John Wiley & Sons, 2019.

[10] M. Kumari, K. Prasad, B. Kuloğlu, and E. Özkan, *The k-Fibonacci group and periods of the k-step Fibonacci sequences*, WSEAS Trans. Math. **21** (2022), 838–843.
http://doi.org/10.37394/23206.2022.21.95.

[11] M. Kumari, K. Prasad, and J. Tanti, *A note on linear codes with generalized Fibonacci matrices*, Jñānābha **52** (2022), no. 2, 77–81.

https://doi.org/10.58250/jnanabha.2022.52209.

[12] M. Kumari and J. Tanti, *On the role of the Fibonacci matrix as key in modified ECC*, arXiv preprint arXiv:2112.11013 (2021).

[13] ———, *Cryptography using multinacci block matrices*, International Journal of Nonlinear Analysis and Applications **14** (2023), no. 10, 57–65. https://doi.org/10.22075/ijnaa.2023.29918.4295.

[14] E.P. Miles, *Generalized Fibonacci numbers and associated matrices*, Amer. Math. Monthly **67** (1960), no. 8, 745–752. https://doi.org/10.1080/00029890.1960.11989593.

[15] E. Özkan and İ. Altun, *Generalized Lucas polynomials and relationships between the Fibonacci polynomials and Lucas polynomials*, Commun. Algebra **47** (2019), no. 10, 4020–4030. https://doi.org/10.1080/00927872.2019.1576186.

[16] K. Prasad and H. Mahato, *Cryptography using generalized Fibonacci matrices with Affine-Hill cipher*, J. Discrete Math. Sci. Cryptogr. **25** (2022), no. 8, 2341–2352. https://doi.org/10.1080/09720529.2020.1838744.

[17] ———, *On some new identities of Lucas numbers and generalization of Fibonacci trace sequences*, Palest. J. Math. **12** (2023), no. 2, 329–340.

[18] K. Prasad, H. Mahato, and M. Kumari, *Some properties of r-circulant matrices with k-balancing and k-Lucas balancing numbers*, Bol. Soc. Mat. Mex. **29** (2023), no. 2, Artical ID: 44. https://doi.org/10.1007/s40590-023-00510-6.

[19] W. Stallings, *Cryptography and network security - principles and practice, 7th edition*, Pearson Education India, 2017.

[20] P. Stanimirović, J. Nikolov, and I. Stanimirović, *A generalization of Fibonacci and Lucas matrices*, Discrete Appl. Math. **156** (2008), no. 14, 2606–2619. https://doi.org/10.1016/j.dam.2007.09.028.

[21] D.R. Stinson, *Cryptography: Theory and Practice*, Chapman and Hall/CRC., New York, 2005.

[22] P. Sundarayya and G.V. Prasad, *A public key cryptosystem using affine hill cipher under modulation of prime number*, J. Inf. Optim. Sci. **40** (2019), no. 4, 919–930. https://doi.org/10.1080/02522667.2018.1470751.

[23] D. Tasci and E. Kilic, *On the order-k generalized Lucas numbers*, Appl. Math. Comput. **155** (2004), no. 3, 637–641. https://doi.org/10.1016/S0096-3003(03)00804-X.

[24] B. Thilaka and K. Rajalakshmi, *An extension of Hill cipher using generalised inverses and mth residue modulo n*, Cryptologia **29** (2005), no. 4, 367–376. https://doi.org/10.1080/0161-110591893933.

[25] H.E. Tianxiao, H.C. Jeff, and J.S. Peter, *Matrix representation of recursive sequences of order 3 and its applications*, J. Math. Res. Appl. **38** (2018), no. 3, 221–235. https://doi.org/10.3770/j.issn:2095-2651.2018.03.001.