Int. J. Nonlinear Anal. Appl. In Press, 1–9
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2023.29918.4295

Cryptography using multinacci block matrices

Munesh Kumari[a,*], Jagmohan Tanti[b]

[a]Department of Mathematics, Central University of Jharkhand, Ranchi, India

[b]Department of Mathematics, Babasaheb Bhimrao Ambedkar University, Lucknow, India

(Communicated by Mohammad Resoul Velayati)

Abstract

In this paper, we propose public key cryptography using recursive block matrices involving generalized Fibonacci numbers over a finite field $\mathbb{Z}_p$. For this, we define multinacci block matrices, a kind of upper triangular matrix involving multinacci matrices at diagonal places and give some of its algebraic properties. Moreover, we set up a method for key element agreement at end users, which makes cryptography more efficient. The proposed cryptography comes with a large key space and its security relies on the Discrete Logarithm Problem (DLP).

Keywords: Fibonacci matrix, Block Matrix, Cryptography, Keyspace
2020 MSC: 11T71, 94A60

1 Introduction

Information is one of the most valuable assets since the dawn of civilizations. The secured transmission of information is of prime importance. Cryptography is the science of study about the security, privacy, and confidentiality of information transmitted over a secured channel. The problem concerned with the topic is to study public key cryptography with the reduction in complexity for key generation without compromising security. As an example, for the same level of security, the RSA cryptosystem uses a bigger key size than the key size of Elliptic curve cryptography.

In 1976, Diffie and Hellman [2] provided a solution to the long-standing problem of key exchange and pointed the way to a digital signature. In 1978 Rivest, Shamir and Adleman [11] proposed a public key cryptosystem which is famed as RSA cryptosystem. The security of RSA cryptosystem depends on the difficulty level of factoring large integers.

Alvareza et al. [1] proposed a public key cryptosystem based on the generalization of the discrete logarithm problem for block matrices over the field $\mathbb{Z}_p$ with the reduced key length for a given level of security. Kuppuswamy et al. [7] have given two different types of encryption algorithms, one of them is public key cryptography based on a linear block cipher and the other one is private key cryptography based on a simple symmetric algorithm. Viswanath and Kumar [16] proposed a public key cryptosystem using Hill's cipher, in which the security of the system depends on the involvement of two digital signatures. To reduce complexity and enhance the processing of key in cryptography K. Prasad and H. Mahato [9] have proposed public key cryptography using generalized Fibonacci matrices in which one has to send numbers instead of matrices for the key. Zeriouh et al. [17], proposed the concept of key exchange

*Corresponding author
Email addresses: muneshnasir94@gmail.com (Munesh Kumari), jagmohan.t@gmail.com (Jagmohan Tanti)

Received: February 2023 *Accepted:* April 2023

between Alice and Bob using specially designed matrices. In this key exchange scheme, each of the sender and receiver first chooses a square matrix of suitable order and then both publish their corresponding set of matrices that commute with their corresponding chosen matrices. Some recent work on the study of cryptography using number sequences, associated matrices and classical cryptography can be seen in [3, 5, 6, 8, 10, 12, 13, 15].

This paper is organized as follows. In section 2, we have first defined the multinacci block matrices and obtained its some properties then we have proposed public key cryptography using extended Hill's cipher and give a key agreement method for end users. In section 3, we have illustrated the scheme with a numerical example. And lastly in section 4, we have analyzed the keyspace and mathematical strength of the scheme followed by the conclusion in section 5.

1.1 Multinacci sequences and matrices

Here, we revisit the generalized Fibonacci sequences, associated matrices and some of their properties [9] which we use further in our work.

Definition 1.1. [9] For $n \in \mathbb{N}$ such that $n \geq 2$, the generalized Fibonacci sequence $\{t_k\}_{k\geq 0}$ of order n is given by

$$t_{k+n} = t_k + t_{k+1} + t_{k+2} + ... + t_{k+n-1}, \tag{1.1}$$

where $t_0 = t_1 = ... = t_{n-2} = 0$ and $t_{n-1} = 1$. The generalized Fibonacci sequence $\{t_k\}_{k\geq 0}$ is called the multinacci sequence.

Throughout the paper, we use the notation $t_{n,k}$ to represent the k^{th} term of the Multinacci sequence (generalized Fibonacci sequence) of order n.

The k^{th} generalized Fibonacci matrix Q_n^k (also known as Multinacci matrix) of order n associated with the sequence $\{t_{n,k}\}$ is given by

$$Q_n^k = \begin{bmatrix} t_{n,k+n-1} & t_{n,k+n-2} + t_{n,k+n-3} + ... + t_{n,k} & \cdots & t_{n,k+n-2} \\ t_{n,k+n-2} & t_{n,k+n-3} + t_{n,k+n-4} + ... + t_{n,k-1} & \cdots & t_{n,k+n-3} \\ \vdots & \vdots & \ddots & \vdots \\ t_{n,k+1} & t_{n,k} + t_{n,k-1} + ... + t_{n,k-n+2} & \cdots & t_{n,k} \\ t_{n,k} & t_{n,k-1} + t_{n,k-2} + ... + t_{n,k-n+1} & \cdots & t_{n,k-1} \end{bmatrix}, \text{for } k = 0, \pm 1, \pm 2, ... \tag{1.2}$$

with

$$Q_n = \begin{bmatrix} 1 & 1 & 1 & ... & 1 & 1 \\ 1 & 0 & 0 & ... & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & ... & 0 & 0 \\ 0 & 0 & 0 & ... & 1 & 0 \end{bmatrix}.$$

For $n = 2, 3$ in Eqn. (1.1), we get the Fibonacci and Tribonacci sequences and the associated matrices are known as Fibonacci and Tribonacci matrices, respectively. The following lemma lists some properties of the Multinacci matrices Q_n^k, which we use to establish some results.

Lemma 1.2. [9] Let $n \in \mathbb{N}$ such that $n \geq 2$ and $k, l \in \mathbb{Z}$. Then for Multinacci matrices Q_n^k, we have

1. $Q_n^0 = I_n$, where I_n is the identity matrix of order n.
2. $(Q_n^1)^k = Q_n^k$ and $(Q_n^{-1})^k = Q_n^{-k}$.
3. $Q_n^k Q_n^l = Q_n^{k+l}$ and $Q_n^k Q_n^{-k} = I_n$.
4. $\det(Q_n^k) = (-1)^{(n-1)k}$.

Inverse of Multinacci matrices:. From (4) of Lemma 1.2, it is worth to note that the determinant of Q_n^k never vanishes for any n and k, hence Q_n^k is always non-singular. And the inverse of the multinacci matrix Q_n^k is given by Q_n^{-k} which can be achieved by replacing k by $-k$ in (1.2).

Commutative nature:. From (3) of Lemma 1.2, it is clear that Multinacci matrices are commutative with respect to usual matrix multiplication.

2 Multinacci block matrices

In this section, we first define multinacci block matrices, investigate some algebraic properties of them and use these matrices in cryptography.

Definition 2.1 (Multinacci block matrix). Let $Q_n^{m_1}, Q_n^{m_2}$ be any two multinacci matrices of order n and C be any square matrix of same order, then the multinacci block matrix A (in short MBM) is defined as

$$A = \begin{bmatrix} Q_n^{m_1} & C \\ 0 & Q_n^{m_2} \end{bmatrix}_{2n\times 2n}.$$

The following theorem deals with the powers of A involving multinacci matrices, which follows a certain pattern.

Theorem 2.2. For $j \in \mathbb{N} \cup \{0\}$, we have

$$A^j = \begin{bmatrix} Q_n^{jm_1} & C^{(j)} \\ 0 & Q_n^{jm_2} \end{bmatrix}, \quad \text{where} \quad C^{(j)} = \begin{cases} 0 & : j = 0, \\ \sum_{r=0}^{j-1} (Q_n^{m_1})^{j-1-r} C (Q_n^{m_2})^r & : j \geq 1. \end{cases}$$

Proof . We prove it by inductive hypothesis on j. For $j = 1$, we have $A^1 = \begin{bmatrix} Q_n^{m_1} & C^{(1)} \\ 0 & Q_n^{m_2} \end{bmatrix} = A$ and $C^{(1)} = C$, satisfied. Now assuming the statement is true for j, we prove it for $j+1$. Here, we have

$$A^{j+1} = A^j A^1 = \begin{bmatrix} Q_n^{jm_1} & C^{(j)} \\ 0 & Q_n^{jm_2} \end{bmatrix} \begin{bmatrix} Q_n^{m_1} & C \\ 0 & Q_n^{m_2} \end{bmatrix} = \begin{bmatrix} Q_n^{jm_1} Q_n^{m_1} & Q_n^{jm_1} C + C^{(j)} Q_n^{m_2} \\ 0 & Q_n^{jm_2} Q_n^{m_2} \end{bmatrix}.$$

Since,

$$\begin{aligned} Q_n^{jm_1} C + C^{(j)} Q_n^{m_2} &= Q_n^{jm_1} C + \left[\sum_{r=0}^{j-1} (Q_n^{m_1})^{j-1-r} C (Q_n^{m_2})^r \right] Q_n^{m_2} \\ &= Q_n^{jm_1} C + \left[(Q_n^{m_1})^{j-1} C (Q_n^{m_2}) + (Q_n^{m_1})^{j-2} C (Q_n^{m_2})^2 + \ldots + C (Q_n^{m_2})^j \right] \\ &= \sum_{r=0}^{j} (Q_n^{m_1})^{j-r} C (Q_n^{m_2})^r = C^{(j+1)}, \end{aligned}$$

we have

$$A^{j+1} = \begin{bmatrix} Q_n^{(j+1)m_1} & C^{(j+1)} \\ 0 & Q_n^{(j+1)m_2} \end{bmatrix}, \text{ where } C^{(j+1)} = \sum_{r=0}^{j} (Q_n^{m_1})^{j-r} C (Q_n^{m_2})^r.$$

□

In order to use a matrix as a key element in cryptography, it should be necessarily invertible. In our case, we use an encryption method analogs to extended Hill cipher under the prime residue and a part of Multinacci block matrix as key element. To show that MBM is nonsingular, it is sufficient to prove that the determinant of MBM is non zero, which has been proven in the following theorem.

Theorem 2.3. Let $Q_n^{m_1}, Q_n^{m_2}$ be any two multinacci matrices of order n then the determinant of Multinacci block matrix is $\det(A) = (-1)^{(n-1)(m_1+m_2)}$.

Proof . To prove the statement, we use the fact that determinant of a block matrix $\begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix}$ is given by

$$\det\left(\begin{bmatrix} X & Y \\ 0 & Z \end{bmatrix} \right) = \det(X) \det(Z).$$

So, using (4) of Lemma 1.2, we have

$$\det\left(\begin{bmatrix} Q_n^{m_1} & C \\ 0 & Q_n^{m_2} \end{bmatrix} \right) = \det(Q_n^{m_1}) \det(Q_n^{m_2}) = (-1)^{(n-1)m_1} (-1)^{(n-1)m_2} = (-1)^{(n-1)(m_1+m_2)}.$$

□

Thus, MBM is non singular and therefore inverse of MBM exist. The following theorem gives the inverse of MBM.

Theorem 2.4. The inverse of Multinacci block matrix Q_n^k is given by

$$\begin{bmatrix} Q_n^{m_1} & C \\ 0 & Q_n^{m_2} \end{bmatrix}^{-1} = \begin{bmatrix} Q_n^{-m_1} & -Q_n^{-m_1} C Q_n^{-m_2} \\ 0 & Q_n^{-m_2} \end{bmatrix}.$$

Proof . It can be easily proved by using the fact that if B is inverse of A then $AB = BA = I$. □

Now, for both the parties (sender and receiver) to be agree on the same key element (matrix), we have to prove $[C^{(i)}]^{(j)} = [C^{(j)}]^{(i)}$, for which we need the following lemma.

Lemma 2.5. For $i, j \in \mathbb{N}$, we have

$$\begin{bmatrix} Q_n^{m_3} & C^{(j)} \\ 0 & Q_n^{m_4} \end{bmatrix}^i = \begin{bmatrix} Q_n^{im_3} & [C^{(j)}]^{(i)} \\ 0 & Q_n^{im_4} \end{bmatrix}, \text{ where } [C^{(j)}]^{(i)} = \sum_{s=0}^{i-1} (Q_n^{m_3})^{i-1-s} C^{(j)} (Q_n^{m_4})^s,$$

$$\text{and } \begin{bmatrix} Q_n^{m_1} & C^{(i)} \\ 0 & Q_n^{m_2} \end{bmatrix}^j = \begin{bmatrix} Q_n^{jm_1} & [C^{(i)}]^j \\ 0 & Q_n^{jm_2} \end{bmatrix}, \text{ where } [C^{(i)}]^{(j)} = \sum_{r=0}^{j-1} (Q_n^{m_1})^{j-1-r} C^{(i)} (Q_n^{m_2})^r.$$

Proof . The proof follows from Theorem 2.2. □

Theorem 2.6. For all $i, j \in \mathbb{N}$, we have

$$[C^{(i)}]^{(j)} = [C^{(j)}]^{(i)}.$$

Proof . By using the property of commutativity of the multinacci matrices, we have

$$\begin{aligned}
[C^{(i)}]^{(j)} &= \sum_{r=0}^{j-1} (Q_n^{m_1})^{j-1-r} C^{(i)} (Q_n^{m_2})^r \\
&= \sum_{r=0}^{j-1} (Q_n^{m_1})^{j-1-r} \left[\sum_{s=0}^{i-1} (Q_n^{m_3})^{i-1-s} C (Q_n^{m_4})^s \right] (Q_n^{m_2})^r \\
&= \sum_{r=0}^{j-1} \sum_{s=0}^{i-1} (Q_n^{m_1})^{j-1-r} (Q_n^{m_3})^{i-1-s} C (Q_n^{m_4})^s (Q_n^{m_2})^r \\
&= \sum_{r=0}^{j-1} \sum_{s=0}^{i-1} (Q_n^{m_3})^{i-1-s} (Q_n^{m_1})^{j-1-r} C (Q_n^{m_2})^r (Q_n^{m_4})^s \\
&= \sum_{s=0}^{i-1} (Q_n^{m_3})^{i-1-s} \left[\sum_{r=0}^{j-1} (Q_n^{m_1})^{j-1-r} C (Q_n^{m_2})^r \right] (Q_n^{m_4})^s \\
&= \sum_{s=0}^{i-1} (Q_n^{m_3})^{i-1-s} C^{(j)} (Q_n^{m_4})^s \\
&= [C^{(j)}]^{(i)}.
\end{aligned}$$

□

2.1 Key generation algorithm

In cryptography, elements of key component plays a crucial role for efficient encryption and better security. We are using Fibonacci block matrices for key composition and encryption and vice-versa. It has been discussed below in the steps followed by encryption algorithm.

Let us consider $S = \left\{ \begin{bmatrix} Q_n^{m_1}(\mathbb{Z}_p) & K \\ 0 & Q_n^{m_2}(\mathbb{Z}_p) \end{bmatrix} : K \in M_n(\mathbb{Z}_p) \right\}$, where we used the notation $Q_n^k(\mathbb{Z}_p)$ for Multinacci matrices over $\mathbb{Z}_p$ and $M_n(\mathbb{Z}_p)$ for matrices over $\mathbb{Z}_p$.

2.2 Construction of public key

Let us assume that the communication is being made between two parties, Alice and Bob. So, for public key setup, Alice do the following steps.

1. Alice chooses a prime number p, $l \in \mathbb{N}$ and matrix $A = \begin{bmatrix} G & K \\ 0 & H \end{bmatrix} \in S$ with $G = Q_n^{m_1}(\mathbb{Z}_p)$ and $H = Q_n^{m_2}(\mathbb{Z}_p)$.
2. Calculate key element $K^{(l)}$ as
$$K^{(l)} = \sum_{r=0}^{l-1} (G)^{l-1-r} K (H)^r \pmod{p}.$$
Now, Alice makes $(p, K, K^{(l)})$ as public key and keep (l, G, H) as her secret key.

2.3 Key generation and encryption

Let P represent the plaintext partitioned as $P = (P_1 P_2 ... P_n)$ and C is the corresponding ciphertext $C = (C_1 C_2 ... C_n)$. Now, using Alice's public key $(p, K, K^{(l)})$, Bob generates his encryption key and then encrypts his plaintext as follows:

1. Bob chooses a secret key, say $j \in \mathbb{N}$ and $B = \begin{bmatrix} M & K \\ 0 & N \end{bmatrix} \in S$ with $M = Q_n^{m_3}(\mathbb{Z}_p)$ and $N = Q_n^{m_4}(\mathbb{Z}_p)$.
2. Calculate, $K^{(j)} = \sum_{s=0}^{j-1} (M)^{j-1-s} K (N)^s \pmod{p}$.
3. Calculate encryption key as
$$[K^{(l)}]^{(j)} = \sum_{s=0}^{j-1} (M)^{j-1-s} K^{(l)} (N)^s \pmod{p}.$$
Thus, his encryption key (say E_k) is $[K^{(l)}]^{(j)}$.
4. Now, Bob construct a row vector E of size n over field $\mathbb{Z}_p$ whose i^{th} column is the sum of elements of i^{th} column of E_K .
5. Encryption method: $C_i \equiv (P_i E_K + E) \pmod{p}$, where $C = (C_1 C_2 ... C_n)$.
6. Finally, Bob sends $(K^{(j)}, C)$ to Alice.

2.4 Decryption

On the other side, after receiving $(K^{(j)}, C)$ from Bob, Alice perform following operations to recover the plaintext:

1. Alice first calculate key matrix E_k as,
$$E_k = [K^{(j)}]^{(l)} = \sum_{r=0}^{l-1} (G)^{l-1-r} * K^{(j)} * (H)^r \pmod{p}.$$
2. Thus, decryption key (say D_K) $= (E_k)^{-1}$.
3. Decryption of ciphertext: $P_i \equiv (C_i - E) D_K \pmod{p}$ where E is a row vector over $\mathbb{Z}_p$ whose i^{th} column is the sum of elements of i^{th} column of $[K^{(j)}]^{(l)}$ over $\mathbb{Z}_p$.

The above methodology is illustrated by an example in the following section.

3 Numerical example

Example 3.1. Consider $p = 47$ and $S = \left\{ \begin{bmatrix} Q_3^{m_1}(\mathbb{Z}_p) & K \\ 0 & Q_3^{m_2}(\mathbb{Z}_p) \end{bmatrix} : K \in M_3(\mathbb{Z}_p) \right\}$. Encrypt the plaintext **HEY** using proposed method.

Proof . Assume, Bob wish to send a plaintext **HEY** to Alice. So for encryption, Bob need public key of Alice.

Construction of Alice's Public Key:.

1. Alice chooses a random number, say $l = 5$ and $A = \begin{bmatrix} G & K \\ 0 & H \end{bmatrix} \in S$, where

$$G = Q_3^9 = \begin{bmatrix} 8 & 31 & 34 \\ 34 & 21 & 44 \\ 44 & 37 & 24 \end{bmatrix}, H = Q_3^{13} \begin{bmatrix} 13 & 21 & 34 \\ 34 & 26 & 34 \\ 34 & 0 & 9 \end{bmatrix} \text{ and } K = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

2. Construction of public key,

$$K^{(5)} = \sum_{r=0}^{4} (G)^{4-r} K (H)^r \pmod{47} \equiv \begin{bmatrix} 42 & 25 & 5 \\ 5 & 37 & 20 \\ 20 & 32 & 17 \end{bmatrix}.$$

Thus, Alice's public key is $\left(47, \begin{bmatrix} 2 & 3 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 42 & 25 & 5 \\ 5 & 37 & 20 \\ 20 & 32 & 17 \end{bmatrix} \right)$ and her secret key is

$$\left(5, \begin{bmatrix} 8 & 31 & 34 \\ 34 & 21 & 44 \\ 44 & 37 & 24 \end{bmatrix}, \begin{bmatrix} 13 & 21 & 34 \\ 34 & 26 & 34 \\ 34 & 0 & 9 \end{bmatrix} \right).$$

Key Generation and Encryption (Bob side). Now, Bob construct his encryption key using Alice's public key $\left(47, \begin{bmatrix} 2 & 3 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 42 & 25 & 5 \\ 5 & 37 & 20 \\ 20 & 32 & 17 \end{bmatrix} \right)$, and encrypt his plaintext as follows:

1. Row vector of plaintext: $P \leftarrow [07, 04, 24]$ $\quad (Here, [H, E, Y] = [07, 04, 24])$.
2. Bob chooses his secret number, say $m = 3$ and matrix $B \in S$ with

$$M = Q_3^7 = \begin{bmatrix} 44 & 37 & 24 \\ 24 & 20 & 13 \\ 13 & 11 & 7 \end{bmatrix} \text{ and } N = Q_3^{15} = \begin{bmatrix} 34 & 0 & 34 \\ 34 & 0 & 13 \\ 13 & 21 & 34 \end{bmatrix}.$$

3. Calculate

$$K^{(3)} = \sum_{s=0}^{2} (M)^{2-s} * K * (N)^s \pmod{47} = \begin{bmatrix} 24 & 4 & 19 \\ 19 & 5 & 32 \\ 32 & 34 & 20 \end{bmatrix}.$$

4. Calculation of encryption key,

$$[K^{(5)}]^{(3)} = \sum_{s=0}^{2} (M)^{2-s} K^{(5)} (N)^s \pmod{47} = \begin{bmatrix} 34 & 19 & 5 \\ 5 & 29 & 14 \\ 14 & 38 & 15 \end{bmatrix}.$$

Thus, encryption key $E_K = [K^{(5)}]^{(3)}$.

5. Bob's row vector E over $\mathbb{Z}_{47}$ is $E = \begin{bmatrix} 6 & 39 & 34 \end{bmatrix}$.
6. Encryption: $C \equiv (PE_K + E) \pmod{47}$.

$$\begin{aligned} C &\equiv \left(\begin{bmatrix} 7 & 4 & 24 \end{bmatrix} * \begin{bmatrix} 34 & 19 & 5 \\ 5 & 29 & 14 \\ 14 & 38 & 15 \end{bmatrix} + \begin{bmatrix} 6 & 39 & 34 \end{bmatrix} \right) \pmod{47} \\ &\equiv \begin{bmatrix} 36 & 25 & 15 \end{bmatrix} \rightarrow [> \quad Z \quad P]. \end{aligned}$$

Here, plaintext $[HEY]$ encrypted as $[> \ Z \ P]$.

7. Bob sends $\left(C, K^{(3)}\right) = \left([> \ Z \ P], \begin{bmatrix} 24 & 4 & 19 \\ 19 & 5 & 32 \\ 32 & 34 & 20 \end{bmatrix} \right)$ to Alice.

Decryption (Alice side). After receiving $\left(C, K^{(3)}\right) = \left(> ZP, \begin{bmatrix} 24 & 4 & 19 \\ 19 & 5 & 32 \\ 32 & 34 & 20 \end{bmatrix} \right)$ from Bob, Alice performs the following steps to recover the plaintext.

1. Alice calculates key matrix as
$$E_K = [K^{(3)}]^{(5)} \pmod{47} = \sum_{r=0}^{4} (G)^{4-r} * K^3 * (H)^r \pmod{47} = \begin{bmatrix} 34 & 19 & 5 \\ 5 & 29 & 14 \\ 14 & 38 & 15 \end{bmatrix}.$$
2. Decryption key D_K over $\mathbb{Z}_{47}$ is $(E_K)^{-1} = \begin{bmatrix} 43 & 30 & 36 \\ 36 & 7 & 41 \\ 41 & 42 & 13 \end{bmatrix}$.
3. Decryption method: $P \equiv (C - E)D_K \pmod{47}$.
Here, $C = [>, Z, P] \to [36 \;\; 25 \;\; 15]$ and row vector $E = \begin{bmatrix} 6 & 39 & 34 \end{bmatrix}$. Thus, Alice recovers the plaintext as
$$\begin{aligned} P &\equiv \left(\left(\begin{bmatrix} 36 & 25 & 15 \end{bmatrix} - \begin{bmatrix} 6 & 39 & 34 \end{bmatrix} \right) * \begin{bmatrix} 43 & 30 & 36 \\ 36 & 7 & 41 \\ 41 & 42 & 13 \end{bmatrix} \right) \pmod{47} \\ &\equiv \begin{bmatrix} 7 & 4 & 24 \end{bmatrix} \to [H \;\; E \;\; Y]. \end{aligned}$$

Thus, the message **HEY** successfully reached to Alice. □

4 Key space and mathematical strength

Security strength of our proposed scheme depends on the computational power require to achieve the private key (j, M, N) of sender and private key (l, G, H) of receiver. Our, encryption key is formulated as

$$[K^{(l)}]^{(j)} = \sum_{s=0}^{j-1} (M)^{j-1-s} * K^{(l)} * (N)^s$$

and after encryption Bob transmits $(K^{(j)}, C)$ to Alice through a unsecure channel. So, we assume that intruder may know $(K^{(j)}, C)$ by unfair means but after knowing $(K^{(j)}, C)$, intruder needs matrices M, N to calculate encryption key $[K^{(l)}]^{(j)}$. Since there is no any deterministic polynomial time algorithm (Discrete logarithm problem [4, 14]) to calculate M, N from $[K^{(l)}]^{(j)}$, so it is almost impossible to recover encryption key from given information on large primes.

Keyspace based on assumed parameters follows from matrix theory. In matrix theory $GL_n(\mathbb{Z}_p)$ represents the set of invertible matrices of order $n \times n$ over finite field $\mathbb{Z}_p$, where p is an odd prime. The order of General Linear group (GL_n) over finite field $\mathbb{Z}_p$ is given by

$$|GL_n(\mathbb{Z}_p)| = (p^n - p^{n-1})(p^n - p^{n-2}) \cdots (p^n - p^1)(p^n - 1). \tag{4.1}$$

To examine strength of our key space, we are presenting a table of possible key spaces over $\mathbb{Z}_p$ based on General Linear group. For simplicity, considering matrices of order 3 × 3 and 4 × 4.

Prime(p)	Possible Key spaces on $GL_3(\mathbb{Z}_p)$	Possible Key spaces on $GL_4(\mathbb{Z}_p)$
3	1.1232×10^{4}	2.4261×10^{7}
5	1.4880×10^{6}	1.1606×10^{11}
7	3.3784×10^{14}	2.7811×10^{13}
11	3.1920×10^{9}	6.2166×10^{25}
13	9.7264×10^{9}	6.1029×10^{18}
17	1.0948×10^{11}	4.5630×10^{19}
19	3.0481×10^{11}	2.7246×10^{20}
23	1.7194×10^{12}	5.8543×10^{21}
29	1.1499×10^{16}	3.6139×10^{28}
⋮	⋮	⋮

From the above table, we should note that the growth rate of key space is very high when $p \to \infty$. Thus, we conclude that if size of key matrix is increasing along with prime, then it forms a very large key space which can be easily done with Fibonacci matrices.

5 Conclusion

We have proposed multinacci block matrices, a kind of upper triangular matrix involving multinacci matrices at diagonal places. Moreover, we have obtained some algebraic properties of these block matrices and proposed a public key cryptography using it. Our proposed cryptography is based on the key element from block matrices over a finite field $\mathbb{Z}_p$. Here, we have used the multiplicative commutativity of the multinacci matrices for agreement of end users on the same key.

Here, the set $S = \left\{ \begin{bmatrix} Q_n^{m_1}(\mathbb{Z}_p) & K \\ 0 & Q_n^{m_2}(\mathbb{Z}_p) \end{bmatrix} : K \in M_n(\mathbb{Z}_p) \right\}$ is a global element i.e. known to everyone, a sender can choose any matrix from the set S to construct the key matrix. So, in the above-proposed scheme, neither sender nor receiver needs to publish their corresponding set of matrices that commute with a chosen matrix of sender and receiver, respectively. Our proposed scheme has a large key space and its security relies on discrete logarithm problem.

Acknowledgment

The authors are grateful to the anonymous reviewers for their insightful comments and suggestions to improve the article. The first author would like to thank the University Grant Commission (UGC), India for the research fellowship.

References

[1] R. Alvarez, F.-M. Martinez, J.-F. Vicent, and A. Zamora, *A new public key cryptosystem based on matrices*, 6th WSEAS Int. Conf. Inf. Secur. Privacy Tenerife, Spain, December 14-16, 2007, pp. 36–39.

[2] W. Diffie and M. Hellman, *New directions in cryptography*, IEEE Trans. Inf. Theory **22** (1976), no. 6, 644–654.

[3] O. Diskaya, E. Avaroglu, and H. Menken, *The classical AES-like cryptology via the Fibonacci polynomial matrix*, Turk. J. Eng. **4** (2020), no. 3, 123–128.

[4] J. Hoffstein, J. Pipher, J.H. Silverman, and J.H. Silverman, *An introduction to mathematical cryptography*, vol. 1, Springer, 2008.

[5] J. Kannan, M. Somanath, M. Mahalakshmi, and K. Raja, *Encryption decryption algorithm using solutions of Pell equation*, Int. J. Math. Appl. **10** (2022), no. 1, 1–8.

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

[7] P. Kuppuswamy and S.Q.Y. Al-Khalidi, *Hybrid encryption/decryption technique using new public key and symmetric key algorithm*, MIS Review: Int. J. **19** (2014), no. 2, 1–13.

[8] M. Mohan, M.K. Kavithadevi, and V.J. Prakash, *Improved classical cipher for healthcare applications*, Procedia Comput. Sci. **93** (2016), 742–750.

[9] 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.

[10] K. Prasad, H. Mahato, and M. Kumari, *A novel public key cryptography based on generalized Lucas matrices*, arXiv preprint arXiv:2202.08156 (2022).

[11] R.L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM **21** (1978), no. 2, 120–126.

[12] J. Shtayat and A. Al-Kateeb, *The perrin r-matrix and more properties with an application*, J. Discrete Math. Sci. Cryptogr. **25** (2022), no. 1, 41–52.

[13] Y. Soykan, E. Taşdemir, and İ. Vedat, *On matrix sequence of modified Tribonacci-Lucas numbers*, MANAS J. Eng. **10** (2022), no. 2, 211–221.

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

[15] 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.

[16] M.K. Viswanath and M.R. Kumar, *A public key cryptosystem using Hiil's cipher*, J. Discrete Math. Sci. Cryptogr. **18** (2015), no. 1-2, 129–138.

[17] M. Zeriouh, A. Chillali, and A. Boua, *Cryptography based on the matrices*, Bol. Soc. Parana. Mat. **37** (2019), no. 3, 75–83.