Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
2025, Volume 31, Number 3, 588-606
DOI: 10.7546/nntdm.2025.31.3.588-606

Affine–Hill cipher from Hadamard-type Fibonacci–Mersenne and Fibonacci-balancing p-sequences

Elahe Mehraban[1,2,*], **T. Aaron Gulliver**[3] **and Evren Hincal**[1,2,4]

[1] Mathematics Research Center, Near East University TRNC
Mersin 10, 99138 Nicosia, Turkey

[2] Department of Mathematics, Near East University TRNC
Mersin 10, 99138 Nicosia, Turkey
e-mail: `e.mehraban.math@gmail.com`

[3] Department of Electrical and Computer Engineering, University of Victoria
Victoria, BC V8W 2Y2, Canada
e-mail: `agullive@ece.uvic.ca`

[4] Research Center of Applied Mathematics, Khazar University
Baku, Azerbaijan
e-mail: `evren.hincal@neu.edu.tr`

* *Corresponding author*

Received: 9 December 2024 **Revised:** 5 September 2025
Accepted: 7 September 2025 **Online First:** 10 September 2025

Abstract: In this paper, we define two new sequences using the generalized Mersenne numbers, Fibonacci p-numbers, and m-balancing numbers. These sequences are constructed using the Hadamard-type product of their characteristic polynomials. The determinants and combinatorial and exponential representations of these new sequences are given. As an application, they are with used to generate keys for encryption for the Affine–Hill cipher using an elliptic curve and self-invertible matrix.

Keywords: Mersenne numbers, Fibonacci p-numbers, Elliptic curve, Self-invertible matrix, Affine–Hill cipher.
2020 Mathematics Subject Classification: 11K31, 11C20, 68P25, 68R01, 68P30, 15A15.

1 Introduction

For $k \geq 3$ a fixed integer, the generalized Mersenne numbers, denoted by $\{M(k,n)\}_{n=0}^{\infty}$, are defined as

$$M(k,n) = kM(k,n-1) - (k-1)M(k,n-2),\ n \geq 2,$$

with initial conditions $M(k,0) = 0$ and $M(k,1) = 1$ [17].

Definition 1.1. *([22]) For integer $p \geq 0$, the Fibonacci $p-$numbers, denoted by $\{F_p(n)\}_0^{\infty}$, are defined as*

$$F_p(n) = F_p(n-1) + F_p(n-p-1),\ n \geq 1,$$

with initial conditions $F_p(0) = 0$ and $F_p(1) = F_p(2) = \cdots = F_{p+1}(p) = 1$.

For example, if $p = 2$ we have

$$F_2(n) = F_2(n-1) + F_2(n-3),\ n \geq 1,$$

so the sequence is $\{F_2(n)\}_0^{\infty} = \{0, 1, 1, 1, 2, 3, \cdots\}$.

Definition 1.2. *([18, 19]) For $m \geq 1$, the m-balancing numbers, denoted by $\{B_{m,n}\}_0^{\infty}$, are defined as*

$$B_{m,n+1} = 6mB_{m,n} - B_{m,n-1},\ n \geq 1,$$

with initial conditions $B_{m,0} = 0$ and $B_{m,1} = 1$.

For example, if $m = 1$ we have

$$B_{1,n+1} = 6B_{1,n} - B_{1,n-1}, n \geq 1,$$

so the sequence is $\{B_{m,n}\}_0^{\infty} = \{0, 1, 6, 35, \ldots\}$. The characteristic polynomials of the generalized Mersenne numbers, m-balancing numbers, and Fibonacci p-numbers are $x^2 - kx + k - 1$, $x^2 - 6mx + 1$, and $x^{p+1} - x^p - 1$, respectively.

Definition 1.3. *([8, 13]) An elliptic curve E over a prime field F_q is defined by*

$$E : y^2 \equiv x^3 + ax + b \pmod{q},$$

where $a, b \in F_q, q \neq 2, 3$ and satisfy the condition $4a^3 + 27b^2 \neq 0(\bmod\ q)$. The elliptic curve group $E(F_q)$ consists of all points (x, y) that satisfy E and the point at infinity 0 .

Definition 1.4. *([1]) A matrix M is called self-invertible matrix if $M = M^{-1}$.*

The Hadamard-type product of polynomials f and g is defined as follows [2].

Definition 1.5. *The Hadamard-type product of polynomials f and g is $f * g = \sum_{i=0}^{\infty}(a_i * b_i)x^i$ where*

$$a_i * b_i = \begin{cases} a_ib_i, & \text{if } a_ib_i \neq 0, \\ a_i + b_i, & \text{if } a_ib_i = 0, \end{cases}$$

and $f(x) = a_mx^m + \cdots + a_1x + a_0$ and $g(x) = b_nx^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0$.

In [21, 23], some linear recurrence sequences were defined and their properties examined using matrix methods. The Hill cipher was invented in 1929 [11]. It is a polygraphic block cipher. The Affine cipher was introduced in [23]. It is an application of linear algebra and can be described as follows.

Encryption:

$$C_i \equiv P_iK + B \pmod{m},$$

where K is an $n \times n$ key matrix, and P_i, C_i and B are $1 \times n$ matrices over Z_m. It should satisfy

$$\gcd(\det K (\operatorname{mod} m)), m) = 1.$$

Decryption:

$$P_i \equiv (C_i - B)K^{-1} \pmod{m}.$$

In 2016, a key matrix of order 3 that reflects an arbitrary line $y = ax + b$ was used to overcome the noninvertible matrix problem in the Affine–Hill cipher modulo a prime number [21]. In [20], a public key cipher was obtained using the generalized Fibonacci matrices with the Affine–Hill cipher. In [3], the authors used the Affine ciphers with the modulo 257 and showed that this cipher looked like a permutation cipher. In [4], the authors constructed a relation between Tribonacci numbers and generalized Tribonacci numbers and offered a public key cryptosystem by using k-generalized Fibonacci sequences. In [7], a new pseudo-random sequence was offered based on two chaotic systems, a logistic map and a seven-dimensional (7D) hyperchaotic system. In [16], it was proposed to assign them to secure images. For this, the authors used data (which is defined from the logistics map) to generate a super-increasing sequence which canattributed as a weight of the synapses. Also, they were inspired to encrypt the images by the Merkel–Hellman algorithm. Here, the generalized Mersenne numbers, Fibonacci p-numbers, and m-balancing numbers are used to obtain new sequences. Then, an elliptic curve and self-invertible matrix are employed to obtain a public key for the Affine–Hill cipher.

The General Linear group, denoted by $GL_\lambda(F_q)$ (q is a prime), consists of all invertible matrices of order $\lambda \times \lambda$ over F_q [14]. This group has order

$$\mid GL_\lambda(F_q) \mid = (q^\lambda - q^{\lambda-1})(q^\lambda - q^{\lambda-2}) \cdots (q^\lambda - 1).$$

The remainder of this paper is organized as follows. In Sections 2 and 3, we present the Fibonacci–Mersenne p-sequences and the Hadamard-type Fibonacci-balancing p-sequences, respectively. The Fibonacci–Mersenne p-matrix and Hadamard-type Fibonacci-balancing p-matrix are used in Section 4 as a key in the Affine–Hill cipher. Note that in this paper p denotes an integer.

2 The Hadamard-type Fibonacci–Mersenne p-sequences

In this section, we define new sequences using the Hadamard-type product of the characteristic polynomials of the Fibonacci p-numbers and Mersenne numbers.

Definition 2.1. *For integers $k \geq 3$ and $p \geq 3$, the Hadamard-type Fibonacci–Mersenne p-sequences, denoted by $\{HM_n(k,p)\}_0^\infty$, are defined as*

$$HM_{n+p+1}(k,p) = HM_{n+p}(k,p) - HM_{n+2}(k,p) + kHM_{n+1}(k,p) + (k-1)HM_n(k,p),\ n \geq 0, \quad (1)$$

with initial conditions $HM_0(k,p) = HM_1(k,p) = \cdots = HM_{p-1}(k,p) = 0$ and $HM_p(k,p) = 1$.

For example, $p = 3$ and $k = 3$ give

$$HM_{n+4}(3,3) = HM_{n+3}(3,3) - HM_{n+2}(3,3) + 3HM_{n+1}(3,3) + 2HM_n(3,3),\ n \geq 0,$$
$$\{HM_n(3,3)\}_0^\infty = \{0,0,0,1,0,2,7,7,6,24,\ldots\},$$

and $p = 4$ and $k = 3$ give

$$HM_{n+5}(4,3) = HM_{n+4}(4,3) - HM_{n+2}(4,3) + 3HM_{n+1}(4,3) + 2HM_n(4,3),\ n \geq 0,$$
$$\{HM_n(4,3)\}_0^\infty = \{0,0,0,0,1,1,0,2,6,11,11,11,22,\ldots\}.$$

From the recurrence relation (1), we have

$$\begin{bmatrix} HM_{n+p+1}(k,p) \\ HM_{n+p}(k,p) \\ HM_{n+p-1}(k,p) \\ \vdots \\ HM_{n+2}(k,p) \\ HM_{n+1}(k,p) \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots & 0 & -1 & k & k-1 \\ 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} HM_{n+p}(k,p) \\ HM_{n+p-1}(k,p) \\ HM_{n+p-2}(k,p) \\ \vdots \\ HM_{n+1}(k,p) \\ HM_n(k,p) \end{bmatrix}.$$

The Hadamard-type Fibonacci–Mersenne p-sequences have the following companion matrix, denoted $M_p(k)$,

$$M_p(k) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & -1 & k & k-1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}_{(p+1)\times(p+1)},$$

and is called the Hadamard-type Fibonacci–Mersenne p-matrix.

Theorem 2.1. *For $p = 3, k = 3$ and $n \geq 4$, we have*

$$(M_3(3))^n = \begin{bmatrix} HM_{n+3}(3,3) & HM_{n+4}(3,3) - HM_{n+3}(k,3) & a_1 & 2HM_{n+2}(3,3) \\ HM_{n+2}(3,3) & HM_{n+3}(3,3) - HM_{n+2}(3,3) & a_2 & 2HM_{n+1}(k,3) \\ HM_{n+1}(3,3) & HM_{n+2}(3,3) - HM_{n+1}(3,3) & a_3 & 2HM_n(3,3) \\ HM_n(3,3) & HM_{n+1}(3,3) - HM_n(3,3) & a_4 & 2HM_{n-1}(3,3) \end{bmatrix}_{(4)\times(4)},$$

$$a_1 = HM_{n+5}(3,3) - HM_{n+4}(3,3) + HM_{n+3}(3,3),$$
$$a_2 = HM_{n+4}(3,3) - HM_{n+3}(3,3) + HM_{n+2}(3,3),$$
$$a_3 = HM_{n+3}(3,3) - HM_{n+2}(3,3) + HM_{n+1}(3,3),$$

$$a_4 = HM_{n+2}(3,3) - HM_{n+1}(3,3) + HM_n(3,3),$$

where

$$M_3(3) = \begin{bmatrix} 1 & -1 & 3 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{(4)\times(4)}.$$

Proof. We use induction on n. For $n = 4$ we have

$$(M_3(3))^4 = \begin{bmatrix} 1 & -1 & 3 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}^4 = \begin{bmatrix} 7 & 0 & 6 & 4 \\ 2 & 5 & 2 & 0 \\ 0 & 2 & 5 & 2 \\ 1 & -1 & 3 & 2 \end{bmatrix}$$

$$= \left[\begin{matrix} HM_7(3,3) & HM_8(3,3) - HM_7(3,3) & HM_9(3,3) - HM_8(3,3) + HM_7(3,3) \\ HM_6(3,3) & HM_7(3,3) - HM_6(3,3) & HM_8(3,3) - HM_7(3,3) + HM_6(3,3) \\ HM_5(3,3) & HM_6(3,3) - HM_5(3,3) & HM_7(3,3) - HM_6(3,3) + HM_5(3,3) \\ HM_4(3,3) & HM_5(3,3) - HM_4(3,3) & HM_6(3,3) - HM_6(3,3) + HM_4(3,3) \end{matrix} \right.$$

$$\left. \begin{matrix} 2HM_6(3,3) \\ 2HM_5(3,3) \\ 2HM_4(3,3) \\ 2HM_3(3,3) \end{matrix} \right].$$

so the statement holds. Now, assume that the statement holds for $n = t$. Therefore, for $n = t + 1$ we have

$$(M_3(k))^{t+1} = \begin{bmatrix} 1 & -1 & 3 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \left[\begin{matrix} HM_{t+3}(3,3) & HM_{t+4}(3,3) - HM_{t+3}(3,3) \\ HM_{t+2}(3,3) & HM_{t+3}(3,3) - HM_{t+2}(3,3) \\ HM_{t+1}(3,3) & HM_{t+2}(3,3) - HM_{t+1}(3,3) \\ HM_t(3,3) & HM_{t+1}(3,3) - HM_t(3,3) \end{matrix} \right.$$

$$\left. \begin{matrix} HM_{t+5}(3,3) - HM_{t+4}(3,3) + HM_{t+3}(3,3) & 2HM_{t+2}(3,3) \\ HM_{t+4}(3,3) - HM_{t+3}(3,3) + HM_{t+2}(3,3) & 2HM_{t+1}(3,3) \\ HM_{t+3}(3,3) - HM_{t+2}(3,3) + HM_{t+1}(3,3) & 2HM_t(3,3) \\ HM_{t+2}(3,3) - HM_{t+1}(3,3) + HM_t(3,3) & 2HM_{t-1}(3,3) \end{matrix} \right]$$

$$= \left[\begin{matrix} HM_{t+4}(3,3) & HM_{t+5}(3,3) - HM_{t+4}(3,3) \\ HM_{t+3}(3,3) & HM_{t+4}(3,3) - HM_{t+3}(3,3) \\ HM_{t+2}(3,3) & HM_{t+3}(3,3) - HM_{t+2}(3,3) \\ HM_{t+1}(3,3) & HM_{t+2}(3,3) - HM_{t+1}(3,3) \end{matrix} \right.$$

$$\left. \begin{matrix} HM_{t+6}(3,3) - HM_{t+5}(3,3) + HM_{t+4}(3,3) & 2HM_{t+3}(3,3) \\ HM_{t+5}(3,3) - HM_{t+4}(3,3) + HM_{t+3}(3,3) & 2HM_{t+2}(3,3) \\ HM_{t+4}(3,3) - HM_{t+3}(3,3) + HM_{t+2}(3,3) & 2HM_{t+1}(3,3) \\ HM_{t+3}(3,3) - HM_{t+2}(3,3) + HM_{t+1}(3,3) & 2HM_t(3,3) \end{matrix} \right],$$

which completes the proof. □

Similar to Theorem 2.1, we can obtain the following result.

Corollary 2.1. *For $p = 3, k \geq 4$ and $n \geq 4$, we have*

$$(M_3(k))^n = \begin{bmatrix} HM_{n+p}(k,3) & HM_{n+p+1}(k,3) - HM_{n+p}(k,3) & a & (k-1) \times HM_{n+p-1}(k,3) \\ HM_{n+p-1}(k,3) & HM_{n+p}(k,3) - HM_{n+p-1}(k,3) & b & (k-1) \times HM_{n+p-2}(k,3) \\ HM_{n+p-2}(k,3) & HM_{n+p-1}(k,3) - HM_{n+p-2}(k,3) & c & (k-1) \times HM_{n+p-3}(k,3) \\ HM_{n+p-3}(k,3) & HM_{n+p-2}(k,3) - HM_{n+p-3}(k,3) & d & (k-1) \times HM_{n+p-4}(k,3) \end{bmatrix},$$

where

$$\begin{aligned} a &= HM_{n+p+2}(k,3) - HM_{n+p+1}(k,3) + HM_{n+p}(k,3), \\ b &= HM_{n+p+1}(k,3) - HM_{n+p}(k,3) + HM_{n+p-1}(k,3), \\ c &= HM_{n+p}(k,3) - HM_{n+p-1}(k,3) + HM_{n+p-2}(k,3), \\ d &= HM_{n+p-1}(k,3) - HM_{n+p-2}(k,3) + HM_{n+p-3}(k,3), \end{aligned}$$

and

$$M_3(k) = \begin{bmatrix} 1 & -1 & k & k-1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{(4)\times(4)}.$$

It can be readily established by induction that for $p \geq 4$ and $n \geq p+1$

$$(M_p(k))^n = \begin{bmatrix} HM_{n+p}(k,p) & HM_{n+p+1}(k,p) - HM_{n+p}(k,p) & \cdots & (k-1)HM_{n+p-1}(k,p) \\ HM_{n+p-1}(k,p) & HM_{n+p}(k,p) - HB_{n+p-1}(k,p) & \cdots & (k-1)HB_{n+p-2}(k,p) \\ \vdots & \vdots & M_p^* & \vdots \\ HM_{n+1}(k,p) & HM_{n+2}(k,p) - HM_{n+1}(k,p) & \cdots & (k-1)HM_n(k,p) \\ HM_n(k,p) & HM_{n+1}(k,p) - HM_n(k,p) & \cdots & (k-1)HM_{n-1}(k,p) \end{bmatrix},$$

where M_p^* is the following $(p-2) \times (p-2)$ matrix

$$M_p^* = \begin{bmatrix} HM_{n+p+2}(k,p) - HM_{n+p+1}(k,p) & \dots & HM_{n+2p-2}(k,p) - HM_{n+2p-3}(k,p) & b_1 \\ HM_{n+p+1}(k,p) - HM_{n+p}(k,p) & \dots & HM_{n+2p-3}(k,p) - HM_{n+2p-4}(k,p) & b_2 \\ \vdots & \ddots & \vdots & \vdots \\ HM_{n+3}(k,p) - HM_{n+2}(k,p) & \dots & HM_{n+p-1}(k,p) - HM_{n+p-2}(k,p) & b_3 \\ HM_{n+2}(k,p) - HM_{n+1}(k,p) & \dots & HM_{n+p-2}(k,p) - HM_{n+p-3}(k,p) & b_4 \end{bmatrix},$$

$$\begin{aligned} b_1 &= (HM_{n+2p-1}(k,p) - HM_{n+2p-2}(k,p)) + HM_{n+p}(k,p), \\ b_2 &= (HM_{n+2p-2}(k,p) - HM_{n+2p-3}(k,p)) + HM_{n+p-1}(k,p), \\ b_3 &= (HM_{n+p}(k,p) - HM_{n+p-1}(k,p)) + HM_{n+1}(k,p), \\ b_4 &= (HM_{n+p-1}(k,p) - HM_{n+p-2}(k,p)) + HM_n(k,p). \end{aligned}$$

It can be easily determined that

$$M_p(k) = \begin{cases} -(k-1), & \text{if } p \text{ is odd,} \\ k-1, & \text{if } p \text{ is even,} \end{cases}$$

so therefore

$$(M_p(k))^n = \begin{cases} -(k-1)^n, & \text{if } p \text{ is odd and } n \text{ is odd,} \\ (k-1)^n, & \text{otherwise.} \end{cases}$$

Lemma 2.1. *Let $g(x)$ be the generating function of the Hadamard-type Fibonacci–Mersenne p-sequences. Then*

$$g(x) = \frac{x^p}{1 - x + x^{p-1} - kx^p - (k-1)x^{p+1}}. \tag{2}$$

Proof. We have

$$\begin{aligned} g(x) &= \sum_{n=1}^{\infty} HM_n(k,p)x^n \\ &= HM_1(k,p)x^1 + HM_2(k,p)x^2 + \cdots + HM_{p-1}(k,p)x^{p-1} + HM_p(k,p)x^p \\ &\quad + \sum_{n=p+1}^{\infty} HM_n(k,p)x^n \\ &= x^p + \sum_{n=p+1}^{\infty} [HM_{n+p}(k,p) - HM_{n+2}(k,p) + kHM_{n+1}(k,p) + (k-1)HM_n(k,p)]x^n \\ &= x^p + \sum_{n=p+1}^{\infty} HM_{n+p}(k,p)x^n - \sum_{n=p+1}^{\infty} HM_{n+2}(k,p)x^n + k\sum_{n=p+1}^{\infty} HM_{n+1}(k,p)x^n \\ &\quad + (k-1)\sum_{n=p+1}^{\infty} HM_n(k,p)x^n \\ &= x^p + x\sum_{n=1}^{\infty} HM_n(k,p)x^n - x^2\sum_{n=1}^{\infty} HM_n(k,p)x^n + kx^p\sum_{n=1}^{\infty} HM_n(k,p)x^n \\ &\quad + (k-1)x^{p+1}\sum_{n=1}^{\infty} HM_n(k,p)x^n \\ &= x^p + xg(x) - x^{p-1}g(x) + kx^pg(x) + (k-1)x^{p+1}g(x). \end{aligned}$$

□

Theorem 2.2. *The Hadamard-type Fibonacci–Mersenne p-sequences $\{HM_n(k,p)\}$ have the following exponential representation*

$$g(x) = x^p \exp\sum_{i=1}^{\infty} \frac{(x)^i}{i}(1 - x^{p-2} + kx^{p-1} + (k-1)x^p)^i,$$

where $p \geq 5$.

Proof. Using (2), we have

$$\ln g(x) = \ln x^p - \ln(1 - x + x^{p-1} - kx^p - (k-1)x^{p+1}).$$

Since

$$\begin{aligned}
-\ln\left(1-x+x^{p-1}-kx^{p}-(k-1)x^{p+1}\right) &= -[-x(1-x^{p-2}+kx^{p-1}+(k-1)x^{p}) \\
&\quad -\frac{1}{2}x^{2}(1-x^{p-2}+kx^{p-1}+(k-1)x^{p})^{2}-\cdots \\
&\quad -\frac{1}{i}x^{i}(1-x^{p-2}+kx^{p-1}+(k-1)x^{p})^{i}-\cdots] \\
&= \sum_{i=1}^{\infty}\frac{(x)^{i}}{i}(1-x^{p-2}+kx^{p-1}+(k-1)x^{p})^{i},
\end{aligned}$$

the result follows. □

3 The Hadamard-type Fibonacci-balancing p-sequences

In this section, we define new sequences using the Hadamard-type product of the characteristic polynomials of the Fibonacci p-numbers and m-balancing numbers.

Definition 3.1. *For $m \geq 1$ and $p \geq 3$, the Hadamard-type Fibonacci-balancing p-sequences, denoted by $\{HB_n^m\}_0^\infty$, are defined as*

$$HB_{n+p+1}^{m} = HB_{n+p}^{m} - HB_{n+2}^{m} + 6mHB_{n+1}^{m} + HB_{n}^{m},\ n \geq 0, \tag{3}$$

with initial conditions $HB_0^m = HB_1^m = \cdots = HB_{p-1}^m = 0$ and $HB_p^m = 1$.

For example $m = 1$ and $p = 3$ give

$$HB_{n+4}^{m} = HB_{n+3}^{m} - HB_{n+2}^{m} + 6HB_{n+1}^{m} + HB_{n}^{m},\ n \geq 0,$$

and $\{HB_n^1\}_0^\infty = \{0,0,0,1,\ldots\}$. From the recurrence relation (3), we have

$$\begin{bmatrix} HB_{n+p+1}^{m} \\ HB_{n+p}^{m} \\ HB_{n+p-1}^{m} \\ \vdots \\ HB_{n+2}^{m} \\ HB_{n+1}^{m} \end{bmatrix} = \begin{bmatrix} 1 & 0 & \cdots & 0 & -1 & 6m & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 0 & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} HB_{n+p}^{m} \\ HB_{n+p-1}^{m} \\ HB_{n+p-2}^{m} \\ \vdots \\ HB_{n+1}^{m} \\ HB_{n}^{m} \end{bmatrix}.$$

The Hadamard-type Fibonacci-balancing p-sequences have the following companion matrix, $B_p(m)$,

$$B_p(m) = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & -1 & 6m & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}_{(p+1)\times(p+1)},$$

and is called the Hadamard-type Fibonacci-balancing p-matrix.

Theorem 3.1. *For $p \geq 3$, $m \geq 1$ and $n \geq p+1$, we have*

$$(B_p(m))^n = \begin{bmatrix} HB^m_{n+p} & HB^m_{n+p+1} - HB^m_{n+p} & \cdots & HB^m_{n+p-1} \\ HB^m_{n+p-1} & HB^m_{n+p} - HB^m_{n+p-1} & \cdots & HB^m_{n+p-2} \\ \vdots & \vdots & B^*_p & \vdots \\ HB^m_{n+1} & HB^m_{n+2} - HB^m_{n+1} & \cdots & HB^m_n \\ HB^m_n & HB^m_{n+1} - HB^m_n & \cdots & HB^m_{n-1} \end{bmatrix},$$

where B^*_p is the following $(p-2) \times (p-2)$ matrix

$$B^*_p =$$

$$\begin{bmatrix} HB^m_{n+p+2} - HB^m_{n+p+1} & \cdots & HB^m_{n+2p-2} - HB^m_{n+2p-3} & (HB^m_{n+p} - HB^m_{n+2p-2}) + HB^m_{n+2p-1} \\ HB^m_{n+p+1} - HB^m_{n+p} & \cdots & HB^m_{n+2p-3} - HB^m_{n+2p-4} & (HB^m_{n+p-1} - HB^m_{n+2p-3}) + HB^m_{n+2p-2} \\ \vdots & \ddots & \vdots & \vdots \\ HB^m_{n+3} - HB^m_{n+2} & \cdots & HB^m_{n+p-1} - HB^m_{n+p-2} & (HB^m_{n+1} - HB^m_{n+p-1}) + HB^m_{n+p} \\ HB^m_{n+2} - HB^m_{n+1} & \cdots & HB^m_{n+p-2} - HB^m_{n+p-3} & (HB^m_n - HB^m_{n+p-2}) + HB^m_{n+p-1} \end{bmatrix}.$$

Proof. The proof is similar to that of Theorem 2.1 and so is omitted. □

It can be easily determined that $\det B_p(m) = (-1)^p$ so $\det(B_p(m))^n = (-1)^{np}$.

Lemma 3.1. *Let $w(x)$ be the generating function of the Hadamard-type Fibonacci-balancing p-sequences. Then*

$$w(x) = \frac{x^p}{1 - x + x^{p-1} - 6mx^p - x^{p+1}}. \tag{4}$$

Proof. We have

$$\begin{aligned} w(x) &= \sum_{n=1}^{\infty} HB^m_n x^n \\ &= HB^m_1 x^1 + HB^m_2 x^2 + \cdots + HB^m_{p-1} x^{p-1} + HB^m_p x^p + \sum_{n=p+1}^{\infty} HB^m_n x^n \\ &= x^p + \sum_{n=p+1}^{\infty} [HB^m_{n+p} - HB^m_{n+2} + 6mHB^m_{n+1} + HB^m_n] x^n \\ &= x^p + \sum_{n=p+1}^{\infty} HB^m_{n+p} x^n - \sum_{n=p+1}^{\infty} HB_{n+2} x^n + 6m \sum_{n=p+1}^{\infty} HB^m_{n+1} x^n + \sum_{n=p+1}^{\infty} HB^m_n x^n \\ &= x^p + x \sum_{n=1}^{\infty} HB^m_n x^n - x^{p-1} \sum_{n=1}^{\infty} HB_n x^n + 6mx^p \sum_{n=1}^{\infty} HB^m_n x^n + x^{p+1} \sum_{n=1}^{\infty} HB^m_n x^n \\ &= x^p + xw(x) - x^{p-1} w(x) + 6mx^p w(x) + x^{p+1} w(x). \end{aligned}$$

□

Theorem 3.2. *The Fibonacci-balancing p-sequences $\{FB_n(k,p)\}$ have the following exponential representation*

$$w(x) = x^p \exp \sum_{i=1}^{\infty} \frac{(x)^i}{i} (1 - x^{p-2} + 6mx^{p-1} + x^p)^i,$$

where $p \geq 3$.

Proof. Using (4), we have

$$\ln w(x) = \ln x^p - \ln(1 - x + x^{p-1} - 6mx^p - x^{p+1}).$$

Since

$$\begin{aligned}
-\ln\left(1 - x + x^{p-1} - 6mx^p - x^{p+1}\right) &= -[-x(1 - x^{p-2} + 6mx^{p-1} + x^p) \\
&\qquad - \frac{1}{2}x^2(1 - x^{p-2} + 6mx^{p-1} + x^p)^2 - \cdots \\
&\qquad - \frac{1}{i}x^i(1 - x^{p-2} + 6mx^{p-1} + x^p)^i - \cdots] \\
&= \sum_{i=1}^{\infty} \frac{(x)^i}{i}(1 - x^{p-2} + 6mx^{p-1} - x^p)^i.
\end{aligned}$$

the result follows. □

4 A public key cipher using Fibonacci-balancing p-sequences and Hadamard-type Fibonacci–Mersenne p-sequences

In this section, a public key for the Affine–Hill cipher is obtained by considering the Hadamard-type Fibonacci–Mersenne p-sequences The key matrix has a large space so it can provide sufficient security. The algorithm is given below. For illustration purposes, an alphabet of 37 symbols is considered which contains the letters $A - Z$ with numerical equivalents $0 - 25$, the numbers $0 - 9$ with numerical equivalents $26 - 35$, and space with numerical equivalent 36 as shown in Table 1.

Table 1. A 37 symbol alphabet

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

First, we consider the Hadamard-type Fibonacci–Mersenne p-sequences and an elliptic curve $E(F_q)$, and introduce Algorithm 1.

Algorithm 1

Bob has the elliptic group $E(F_q)$ and using (a, b, q) chooses an arbitrary element of the group (x, y). Then he sends $n :=\mid x - y \mid$, k and p to Alice where k and p are defined as follows

$$k := \begin{cases} \gcd(x, y), & \text{if } \gcd(x, y) \geq 3, \\ 3, & \text{if } \gcd(x, y) < 3, \end{cases}$$

where $\gcd(x, y)$ is the greatest common divisor x and y, and

$$p := \begin{cases} \mid a - b \mid, & \text{if } \mid a - b \mid \geq 3, \\ 4, & \text{if } \mid a - b \mid < 3. \end{cases}$$

Then, Alice employs the encryption algorithm to get the ciphertext.

Encryption:

Step 1. Divide the plaintext into blocks of size $1 \times (p + 1)$.

Step 2. Construct a key matrix $K := (M_p(k))^n$ and

$$B := [MB_{n+p}(k, p), MB_{n+p+1}(k, p), \ldots, MB_{n+2p}(k, p)].$$

We have that $K \equiv K (\bmod 37)$ and $B \equiv B \pmod{37}$.

Step 3. Calculate $C_i \equiv (P_i K + B) \pmod{37}$.

Step 4. Obtain the ciphertext.

Bob receives the ciphertext and employs the decryption algorithm to get the plaintext.

Decryption:

Step 1. Using K and B, calculate $P \equiv (C - B)K^{-1} \pmod{37}$.

Step 2. Using Table 1, obtain the plaintext.

This algorithm is illustrated in the following example.

Example 4.1. Bob chooses $a = 3$, $b = 1$, and $q = 31$ and gets

$$y^2 \equiv x^3 + 3x + 1 \pmod{31}.$$

Since $4(3)^3 + 27 \times 1 = 135 \equiv 11 \neq 0 \pmod{31}$, Bob obtains the elliptic curve group $E(F_{31})$. Then he chooses $(1, 6)$ which is an element of $E(F_{31})$. Bob then obtains $n :=\mid 1 - 6 \mid= 5$, $k = 3$, and $p = 4$, and sends them to Alice. Then, Alice creates the ciphertext for the plaintext

```
MATHEMATICS IS INTERESTING
```

Applying the Fibonacci–Mersenne p-sequence gives

$$(M_4(3))^5 = \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & -1 & 2 & 5 & 2 \\ 1 & 0 & -1 & 3 & 2 \end{bmatrix} \equiv \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix} \pmod{37},$$

$$\begin{aligned} B &= [MH_9(3,4), MH_{10}(3,4)], MH_{11}(3,4), MH_{12}(3,4), MH_{13}(3,4)] \\ &= [6, 11, 11, 11, 22] \equiv [6, 11, 11, 11, 22] \pmod{37}. \end{aligned}$$

Now, calculate $C_i \equiv (P_iK + B)(\text{mod } 37)$ and

$$\begin{aligned} P_1 &= [\texttt{M}, \texttt{A}, \texttt{T}, \texttt{H}, \texttt{E}], \\ P_2 &= [\texttt{M}, \texttt{A}, \texttt{T}, \texttt{I}, \texttt{C}], \\ P_3 &= [\texttt{S}, \textvisiblespace, \texttt{I}, \texttt{S}, \textvisiblespace], \\ P_4 &= [\texttt{I}, \texttt{N}, \texttt{T}, \texttt{E}, \texttt{R}], \\ P_5 &= [\texttt{E}, \texttt{S}, \texttt{T}, \texttt{I}, \texttt{N}], \\ P_6 &= [\texttt{G}, \textvisiblespace, \textvisiblespace, \textvisiblespace, \textvisiblespace], \end{aligned}$$

so then

$$\begin{aligned} C_1 &= \begin{bmatrix} 12 & 0 & 19 & 7 & 4 \end{bmatrix} \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix} + \begin{bmatrix} 6 & 11 & 11 & 11 & 22 \end{bmatrix} \\ &\equiv \begin{bmatrix} 15 & 28 & 23 & 3 & 19 \end{bmatrix} \pmod{37}, \end{aligned}$$

$$\begin{aligned} C_2 &= \begin{bmatrix} 12 & 0 & 19 & 8 & 2 \end{bmatrix} \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix} + \begin{bmatrix} 6 & 11 & 11 & 11 & 22 \end{bmatrix} \\ &\equiv \begin{bmatrix} 13 & 34 & 27 & 2 & 17 \end{bmatrix} \pmod{37}, \end{aligned}$$

$$\begin{aligned} C_3 &= \begin{bmatrix} 18 & 36 & 8 & 18 & 36 \end{bmatrix} \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix} + \begin{bmatrix} 6 & 11 & 11 & 11 & 22 \end{bmatrix} \\ &\equiv \begin{bmatrix} 18 & 21 & 1 & 22 & 33 \end{bmatrix} \pmod{37}, \end{aligned}$$

$$\begin{aligned} C_4 &= \begin{bmatrix} 8 & 13 & 19 & 4 & 17 \end{bmatrix} \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix} + \begin{bmatrix} 6 & 11 & 11 & 11 & 22 \end{bmatrix} \\ &\equiv \begin{bmatrix} 27 & 26 & 26 & 29 & 23 \end{bmatrix} \pmod{37}, \end{aligned}$$

$$\begin{aligned} C_5 &= \begin{bmatrix} 4 & 18 & 19 & 8 & 13 \end{bmatrix} \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix} + \begin{bmatrix} 6 & 11 & 11 & 11 & 22 \end{bmatrix} \\ &\equiv \begin{bmatrix} 13 & 22 & 27 & 23 & 7 \end{bmatrix} \pmod{37}, \end{aligned}$$

$$\begin{aligned} C_6 &= \begin{bmatrix} 6 & 36 & 36 & 36 & 36 \end{bmatrix} \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix} + \begin{bmatrix} 6 & 11 & 11 & 11 & 22 \end{bmatrix} \\ &\equiv \begin{bmatrix} 1 & 36 & 1 & 27 & 2 \end{bmatrix} \pmod{37}. \end{aligned}$$

Therefore, the ciphertext is

`P2XDTN81CRSVBW71003XNW1XHB␣B1C`

For decryption, we require

$$(M_4(3))^{-5} = \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix}^{-5}.$$

Using $K^{-1} := (M_4(3))^{(-5)}$ and B, calculate $P \equiv (C-B)K^{-1} \pmod{37}$

$$\begin{aligned} P_1 = (C_1 - B)K^{-1} &= \left(\begin{bmatrix} 15 & 28 & 23 & 3 & 19 \end{bmatrix} - \begin{bmatrix} 6 & 11 & 11 & 11 & 22 \end{bmatrix}\right) \times \begin{bmatrix} 6 & 5 & 0 & 6 & 4 \\ 2 & 4 & 5 & 2 & 0 \\ 0 & 2 & 4 & 5 & 2 \\ 1 & 36 & 2 & 5 & 2 \\ 1 & 0 & 36 & 3 & 2 \end{bmatrix}^{-5} \\ &\equiv \begin{bmatrix} 12 & 0 & 19 & 7 & 4 \end{bmatrix} \pmod{37}, \end{aligned}$$

$$P_2 = (C_2 - B)K^{-1} = (\begin{bmatrix}13 & 34 & 27 & 2 & 17\end{bmatrix} - \begin{bmatrix}6 & 11 & 11 & 11 & 22\end{bmatrix}) \times \begin{bmatrix}6 & 5 & 0 & 6 & 4\\ 2 & 4 & 5 & 2 & 0\\ 0 & 2 & 4 & 5 & 2\\ 1 & 36 & 2 & 5 & 2\\ 1 & 0 & 36 & 3 & 2\end{bmatrix}^{-5}$$

$$\equiv \begin{bmatrix}12 & 0 & 19 & 8 & 2\end{bmatrix} \pmod{37},$$

$$P_3 = (C_3 - B)K^{-1} = (\begin{bmatrix}18 & 21 & 1 & 22 & 33\end{bmatrix} - \begin{bmatrix}6 & 11 & 11 & 11 & 22\end{bmatrix}) \times \begin{bmatrix}6 & 5 & 0 & 6 & 4\\ 2 & 4 & 5 & 2 & 0\\ 0 & 2 & 4 & 5 & 2\\ 1 & 36 & 2 & 5 & 2\\ 1 & 0 & 36 & 3 & 2\end{bmatrix}^{-5}$$

$$\equiv \begin{bmatrix}18 & 36 & 8 & 18 & 36\end{bmatrix} \pmod{37},$$

$$P_4 = (C_4 - B)K^{-1} = (\begin{bmatrix}27 & 26 & 26 & 29 & 23\end{bmatrix} - \begin{bmatrix}6 & 11 & 11 & 11 & 22\end{bmatrix}) \times \begin{bmatrix}6 & 5 & 0 & 6 & 4\\ 2 & 4 & 5 & 2 & 0\\ 0 & 2 & 4 & 5 & 2\\ 1 & 36 & 2 & 5 & 2\\ 1 & 0 & 36 & 3 & 2\end{bmatrix}^{-5}$$

$$\equiv \begin{bmatrix}8 & 13 & 19 & 4 & 17\end{bmatrix} \pmod{37},$$

$$P_5 = (C_5 - B)K^{-1} = (\begin{bmatrix}13 & 22 & 27 & 23 & 7\end{bmatrix} - \begin{bmatrix}6 & 11 & 11 & 11 & 22\end{bmatrix}) \times \begin{bmatrix}6 & 5 & 0 & 6 & 4\\ 2 & 4 & 5 & 2 & 0\\ 0 & 2 & 4 & 5 & 2\\ 1 & 36 & 2 & 5 & 2\\ 1 & 0 & 36 & 3 & 2\end{bmatrix}^{-5}$$

$$\equiv \begin{bmatrix}4 & 18 & 19 & 8 & 13\end{bmatrix} \pmod{37},$$

$$P_6 = (C_6 - B)K^{-1} = (\begin{bmatrix}1 & 36 & 1 & 27 & 2\end{bmatrix} - \begin{bmatrix}6 & 11 & 11 & 11 & 22\end{bmatrix}) \times \begin{bmatrix}6 & 5 & 0 & 6 & 4\\ 2 & 4 & 5 & 2 & 0\\ 0 & 2 & 4 & 5 & 2\\ 1 & 36 & 2 & 5 & 2\\ 1 & 0 & 36 & 3 & 2\end{bmatrix}^{-5}$$

$$\equiv \begin{bmatrix}6 & 36 & 36 & 36 & 36\end{bmatrix} \pmod{37}.$$

Then the plaintext is obtained as

```
MATHEMATICS IS INTERESTING
```

Algorithm 2 uses the Fibonacci-balancing p-sequences.

Algorithm 2

First, Bob calculates n and p as in Algorithm 1, and he obtains i and m as follows:

$$i = \begin{cases} \mid a-b \mid, & \text{if } \mid a-b \mid \geq 4, \\ 3, & \text{if } \mid a-b \mid \leq 3, \end{cases}$$

$$m := \begin{cases} \gcd(x,y), & \text{if } \gcd(x,y) \geq 3, \\ 3, & \text{if } \gcd(x,y) < 3, \end{cases}$$

He sends these to Alice. Then, Alice employs the encryption algorithm to get the ciphertext.

Encryption:

Step 1. Divide the plaintext into blocks of size $1 \times (i+1)$.

Step 2. Construct a self-invertible matrix M using $HB^m_{n+p}, HB^m_{n+p+1}, \ldots, HB^m_{n+p+i}$ and get key matrix $K := M$ [1]. Put $B := [HB^m_{n+p}, HB^m_{n+p+1}, \ldots, HB^m_{n+p+i}]$. We have that $K \equiv K \pmod{37}$ and $B \equiv B (\bmod 37)$.

Step 3. Calculate $C_i \equiv (P_i K + B) \pmod{37}$.

Step 4. Obtain the ciphertext.

Decryption:

Step 1. Using K (K is self-invertible, so $K = K^{-1}$) and B, calculate $P \equiv (C-B)K^{-1} (\bmod 37)$.

Step 2. Using Table 1, obtain the plaintext.

Example 4.2. Bob sends $p = 4$, $n = 4$, $m = 3$ and $i = 3$ to Alice. Using the plaintext in Example 4.1, we obtain

$$B = [HB^3_8, HB^3_9, HB^3_{10}, HB^3_{11}] = [17, 35, 54, 38] \equiv [17, 35, 17, 1] \pmod{37},$$

and using $[HB^3_8, HB^3_9, HB^3_{10}, HB^3_{11}] \equiv [17, 35, 17, 1] \pmod{37}$ obtains the self-invertiable matrix

$$M = \begin{bmatrix} HB^3_8 & HB^3_9 & 1-HB^3_8 & -HB^3_9 \\ HB^3_{10} & HB^3_{11} & -HB^3_{10} & 1-HB^3_{11} \\ 1+HB^3_8 & HB^3_9 & -HB^3_8 & -HB^3_9 \\ HB^3_{10} & 1+HB^3_{11} & -HB^3_{10} & -HB^3_{11} \end{bmatrix},$$

$$= \begin{bmatrix} 17 & 35 & 16 & -35 \\ 17 & 1 & -17 & 0 \\ 18 & 35 & -17 & -35 \\ 17 & 2 & -17 & -1 \end{bmatrix} \equiv \begin{bmatrix} 17 & 35 & 16 & 2 \\ 17 & 1 & 20 & 0 \\ 18 & 35 & 20 & 2 \\ 17 & 2 & 20 & 36 \end{bmatrix} \pmod{37}.$$

Now, calculate $C_i \equiv (P_i K + B)(\bmod 37)$.

$$\begin{aligned}
P_1 &= [\texttt{M}, \texttt{A}, \texttt{T}, \texttt{H}],\\
P_2 &= [\texttt{E}, \texttt{M}, \texttt{A}, \texttt{T}],\\
P_3 &= [\texttt{I}, \texttt{C}, \texttt{S}, \textvisiblespace],\\
P_4 &= [\texttt{I}, \texttt{S}, \textvisiblespace, \texttt{I}],\\
P_5 &= [\texttt{N}, \texttt{T}, \texttt{E}, \texttt{R}],\\
P_6 &= [\texttt{E}, \texttt{S}, \texttt{T}, \texttt{I}],\\
P_7 &= [\texttt{N}, \texttt{G}, \textvisiblespace, \textvisiblespace],
\end{aligned}$$

so then

$$C_1 = \begin{bmatrix} 12 & 0 & 19 & 7 \end{bmatrix} \begin{bmatrix} 17 & 35 & 16 & 2 \\ 17 & 1 & 20 & 0 \\ 18 & 35 & 20 & 2 \\ 17 & 2 & 20 & 36 \end{bmatrix} + \begin{bmatrix} 17 & 35 & 17 & 1 \end{bmatrix} \equiv \begin{bmatrix} 16 & 24 & 36 & 19 \end{bmatrix} \pmod{37},$$

$$C_2 = \begin{bmatrix} 4 & 12 & 0 & 19 \end{bmatrix} \begin{bmatrix} 17 & 35 & 16 & 2 \\ 17 & 1 & 20 & 0 \\ 18 & 35 & 20 & 2 \\ 17 & 2 & 20 & 36 \end{bmatrix} + \begin{bmatrix} 17 & 35 & 17 & 1 \end{bmatrix} \equiv \begin{bmatrix} 20 & 3 & 35 & 27 \end{bmatrix} \pmod{37},$$

$$C_3 = \begin{bmatrix} 8 & 2 & 18 & 36 \end{bmatrix} \begin{bmatrix} 17 & 35 & 16 & 2 \\ 17 & 1 & 20 & 0 \\ 18 & 35 & 20 & 2 \\ 17 & 2 & 20 & 36 \end{bmatrix} + \begin{bmatrix} 17 & 35 & 17 & 1 \end{bmatrix} \equiv \begin{bmatrix} 13 & 20 & 7 & 8 \end{bmatrix} \pmod{37},$$

$$C_4 = \begin{bmatrix} 8 & 18 & 36 & 8 \end{bmatrix} \begin{bmatrix} 17 & 35 & 16 & 2 \\ 17 & 1 & 20 & 0 \\ 18 & 35 & 20 & 2 \\ 17 & 2 & 20 & 36 \end{bmatrix} + \begin{bmatrix} 17 & 35 & 17 & 1 \end{bmatrix} \equiv \begin{bmatrix} 22 & 18 & 16 & 7 \end{bmatrix} \pmod{37},$$

$$C_5 = \begin{bmatrix} 13 & 19 & 4 & 17 \end{bmatrix} \begin{bmatrix} 17 & 35 & 16 & 2 \\ 17 & 1 & 20 & 0 \\ 18 & 35 & 20 & 2 \\ 17 & 2 & 20 & 36 \end{bmatrix} + \begin{bmatrix} 17 & 35 & 17 & 1 \end{bmatrix} \equiv \begin{bmatrix} 34 & 17 & 26 & 28 \end{bmatrix} \pmod{37},$$

$$C_6 = \begin{bmatrix} 4 & 8 & 19 & 8 \end{bmatrix} \begin{bmatrix} 17 & 35 & 16 & 2 \\ 17 & 1 & 20 & 0 \\ 18 & 35 & 20 & 2 \\ 17 & 2 & 20 & 36 \end{bmatrix} + \begin{bmatrix} 17 & 35 & 17 & 1 \end{bmatrix} \equiv \begin{bmatrix} 14 & 13 & 4 & 2 \end{bmatrix} \pmod{37},$$

$$C_7 = \begin{bmatrix} 13 & 6 & 36 & 36 \end{bmatrix} \begin{bmatrix} 17 & 35 & 16 & 2 \\ 17 & 1 & 20 & 0 \\ 18 & 35 & 20 & 2 \\ 17 & 2 & 20 & 36 \end{bmatrix} + \begin{bmatrix} 17 & 35 & 17 & 1 \end{bmatrix} \equiv \begin{bmatrix} 9 & 15 & 9 & 26 \end{bmatrix} \pmod{37}.$$

The resulting ciphertext is

```
QY␣TUD91NUHIW31H8R02ONECJPJ0
```

Now, Bob receives the ciphertext and using k, n, and p calculates $K^{-1} = K$.

$$P_1 = (\begin{bmatrix}16 & 24 & 36 & 19\end{bmatrix} - \begin{bmatrix}17 & 35 & 17 & 1\end{bmatrix})\begin{bmatrix}17 & 35 & 16 & 2\\17 & 1 & 20 & 0\\18 & 35 & 20 & 2\\17 & 2 & 20 & 36\end{bmatrix} \equiv \begin{bmatrix}12 & 0 & 19 & 7\end{bmatrix} \pmod{37},$$

$$P_2 = (\begin{bmatrix}20 & 3 & 35 & 27\end{bmatrix} - \begin{bmatrix}17 & 35 & 17 & 1\end{bmatrix})\begin{bmatrix}17 & 35 & 16 & 2\\17 & 1 & 20 & 0\\18 & 35 & 20 & 2\\17 & 2 & 20 & 36\end{bmatrix} \equiv \begin{bmatrix}4 & 12 & 0 & 19\end{bmatrix} \pmod{37},$$

$$P_3 = (\begin{bmatrix}13 & 20 & 7 & 8\end{bmatrix} - \begin{bmatrix}17 & 35 & 17 & 1\end{bmatrix})\begin{bmatrix}17 & 35 & 16 & 2\\17 & 1 & 20 & 0\\18 & 35 & 20 & 2\\17 & 2 & 20 & 36\end{bmatrix} \equiv \begin{bmatrix}8 & 2 & 18 & 36\end{bmatrix} \pmod{37},$$

$$P_4 = (\begin{bmatrix}22 & 18 & 16 & 7\end{bmatrix} - \begin{bmatrix}17 & 35 & 17 & 1\end{bmatrix})\begin{bmatrix}17 & 35 & 16 & 2\\17 & 1 & 20 & 0\\18 & 35 & 20 & 2\\17 & 2 & 20 & 36\end{bmatrix} \equiv \begin{bmatrix}8 & 18 & 36 & 8\end{bmatrix} \pmod{37},$$

$$P_5 = (\begin{bmatrix}34 & 17 & 26 & 28\end{bmatrix} - \begin{bmatrix}17 & 35 & 17 & 1\end{bmatrix})\begin{bmatrix}17 & 35 & 16 & 2\\17 & 1 & 20 & 0\\18 & 35 & 20 & 2\\17 & 2 & 20 & 36\end{bmatrix} \equiv \begin{bmatrix}13 & 19 & 4 & 17\end{bmatrix} \pmod{37},$$

$$P_6 = (\begin{bmatrix}14 & 13 & 4 & 2\end{bmatrix} - \begin{bmatrix}17 & 35 & 17 & 1\end{bmatrix})\begin{bmatrix}17 & 35 & 16 & 2\\17 & 1 & 20 & 0\\18 & 35 & 20 & 2\\17 & 2 & 20 & 36\end{bmatrix} \equiv \begin{bmatrix}4 & 8 & 19 & 8\end{bmatrix} \pmod{37},$$

$$P_7 = (\begin{bmatrix}9 & 15 & 9 & 26\end{bmatrix} - \begin{bmatrix}17 & 35 & 17 & 1\end{bmatrix})\begin{bmatrix}17 & 35 & 16 & 2\\17 & 1 & 20 & 0\\18 & 35 & 20 & 2\\17 & 2 & 20 & 36\end{bmatrix} \equiv \begin{bmatrix}13 & 6 & 36 & 36\end{bmatrix} \pmod{37},$$

and the plaintext is obtained.

4.1 Security analysis

In the proposed method, matrices M_p^n and B_p^n are used to construct the Affine–Hill cipher encryption key. Note that these matrices are over F_{37}. Therefore, M_p^n and B_p^n are required by an attacker to obtain the key, and

$$\begin{aligned}\mid GL_{p+1}(F_{37}) \mid &= (37^{p+1} - 37^{p})(37^{p+1} - 37^{p-1}) \cdots (37^{p+1} - 1),\\ \mid GL_{i+1}(F_{37}) \mid &= (37^{i+1} - 37^{i})(37^{i+1} - 37^{i-1}) \cdots (37^{i+1} - 1).\end{aligned}$$

Thus, to obtain the key an attacker needs to check a large number of matrices which confirms that the key is strong.

For example, if $p = 49$, we have:

$$| GL_{50}(F_{37}) |= (37^{50} - 37^{49})(37^{50} - 37^{48}) \cdots (37^{50} - 1) = 3.1 \times 10^{3920}.$$

Therefore, an attacker needs to check 10^{3920} matrices which is intractable.

5 Conclusion

In this paper, two new sequences were defined using the generalized Mersenne numbers, Fibonacci p-numbers and m-balancing numbers. Using these sequences, a Hadamard-type Fibonacci–Mersenne p-matrix with determinant equal to $k - 1$ or $-(k - 1)$ and a Hadamard-type Fibonacci-balancing p-matrix with determinant equal to 1 and -1, were obtained. A public key cipher was developed which use the parameters $k, n, p, i,$ and m which are known only to Alice and Bob. It was shown that breaking this system is intractable if suitable parameters are chosen which ensures the security of the data. As future work, other sequences can be used to build these algorithms (see [5, 6, 9, 10, 12, 15]).

References

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

[2] Aküzüm, Y., & Deveci, Ö. (2020). The Hadamard-type k-step Fibonacci sequences in groups. *Communications in Algebra*, 48(7), 2844–2856.

[3] Ali-Pacha, H., Hadj-Said, N., Ali-Pacha, A., & Özer, Ö. (2020). Significant role of the specific prime number $p = 257$ in the improvement of cryptosystems. *Notes on Number Theory and Discrete Mathematics*, 26(4), 213–222.

[4] Badidja, S., Mokhtar, A. A., & Özer, Ö. (2021). Representation of integers by k-generalized Fibonacci sequences and applications in cryptography. *Asian-European Journal of Mathematics*, 14(9), Article ID 2150157.

[5] Deveci, Ö. (2019). The Jacobsthal–Padovan p-sequences and their applications. *Proceedings of the Romanian Academy, Series A*, 20(3), 215–224.

[6] Deveci, Ö., & Shannon, A. G. (2018). The quaternion-Pell sequence. *Communications in Algebra*, 46(12), 5403–5409.

[7] Hadj Brahim, A., Ali-Pacha, H., Naim, M., & Ali-Pacha, A. (2024). A new pseudo-random generator based on two chaotic systems. *Journal of Systems Science and Information*, 12(6), 775–789.

[8] Hankerson, D., Vanstone, S., & Menezes, A. (2004). *Guide to Elliptic Curve Cryptography*. Springer-Verlag, New York.

[9] Hashemi, M., & Mehraban, E. (2021). The generalized order k-Pell sequences in some special groups of nilpotency class 2. *Communications in Algebra*, 50(4), 1768–1784.

[10] Hashemi, M., & Mehraban, E. (2022). An application of the t-extension of the p-Fibonacci Pascal matrix in coding theory. *Advances in Mathematical Physics*, 2022, Article ID 4619136.

[11] Hill, L. S. (1929). Cryptography in an algebraic alphabet. *The American Mathematical Monthly*, 36(6), 306–312.

[12] Hiller, J., Aküzüm, Y., & Deveci, Ö. (2018). The adjacency-Pell-Hurwitz numbers. *Integers*, 18, Article ID #A83.

[13] Hoffstein, J. (2008). Elliptic Curves and Cryptography (Chapter 5). In: *An Introduction to Mathematical Cryptography.* (Silverman, J. H., & Pipher, J., Eds.), 299–371. Springer, New York.

[14] Grillet, P. A. (2007). *Abstract Algebra* (2nd ed.). Graduate Texts in Mathematics, Vol. 242, Springer, Berlin.

[15] Mehraban, E., & Hashemi, M. (2023). Fibonacci length and the generalized order k-Pell sequences of the 2-generator p-groups of nilpotency class 2. *Journal of Algebra and Its Applications*, 22(3), Article ID 2350061.

[16] Merzoug, A., Ali-Pacha, H., Ali-Pacha, A., & Özer, Ö. (2025). Neuronal crypto system based on chaotic super-increasing sequence. *Journal of Discrete Mathematical Sciences and Cryptography*, 28(3), 733–751.

[17] Ochalik, P., & Włoch, A. (2018). On generalized Mersenne numbers, their interpretations and matrix generators. *Annales Universitatis Mariae Curie-Skłodowska. Sectio A-Mathematica*, 72(1), 69–76.

[18] Özkoç, A. (2015). Tridiagonal matrices via k-balancing number. *British Journal of Mathematics and Computer Science*, 10(4), 1–11.

[19] Özkoç, A., & Tekcan, A. (2017). On k-balancing numbers. *Notes on Number Theory and Discrete Mathematics*, 23(3), 38–52.

[20] Prasad, K., & Mahato, H. (2022). Cryptography using generalized Fibonacci matrices with Affine-Hill cipher. *Journal of Discrete Mathematical Sciences and Cryptography*, 25(8), 2341–2352.

[21] Prasad, M. G. V., Chari, P. P. P., & Satyam, K. P. (2016). Affine Hill cipher key generation matrix of order 3 by using reflects in an arbitrary line $y = ax + b$. *International Journal of Science Technology and Management*, 5(8), 268–272.

[22] Stakhov, A. P. (2006). Fibonacci matrices, a generalization of the "Cassini formula", and new coding theory. *Chaos, Solitons & Fractals*, 30(1), 56–66.

[23] Stinson, D. R. (2005). *Cryptography: Theory and Practice* (3rd ed.). Chapman and Hall/CRC, Boca Raton, FL.