Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 9(5): 13537–13552.
DOI: 10.3934/math.2024660
Received: 20 January 2024
Revised: 29 March 2024
Accepted: 03 April 2024
Published: 12 April 2024

Research article

New sequences from the generalized Pell $p-$numbers and mersenne numbers and their application in cryptography

Elahe Mehraban[1,2,3,*], **T. Aaron Gulliver**[4], **Salah Mahmoud Boulaaras**[5,*], **Kamyar Hosseini**[1,6] **and Evren Hincal** [1,2,3]

[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

[3] Faculty of Art and Science, University of Kyrenia, TRNC, Mersin 10, 99320 Kyrenia, Turkey

[4] Department of Electrical and Computer Engineering, University of Victoria, Victoria, BC, V8W 2Y2, Canada

[5] Department of Mathematics, College of Science, Qassim University, Buraydah 51452, Saudi Arabia

[6] Department of Computer Science and Mathematics, Lebanese American University, Beirut, Lebanon

* **Correspondence:** Email: e.mehraban.math@gmail.com, s.boularas@qu.edu.sa; Tel: +90-5338203378, +96-6559618327; Fax: +90-3922236461, +96-613803070.

Abstract: This paper presents the generalized Pell $p-$numbers and provides some related results. A new sequence is defined using the characteristic polynomial of the Pell $p-$numbers and generalized Mersenne numbers. Two algorithms for Diffie-Hellman key exchange are given as an application of these sequences. They are illustrated via numerical examples and shown to be secure against attacks. Thus, these new sequences are practical for encryption and constructing private keys.

Keywords: Mersenne numbers; Pell $p-$numbers; Diffie-Hellman key exchange; public key; private key; sequence analysis
Mathematics Subject Classification: 11K31, 11C20, 68P25, 68R01, 68P30, 15A15

1. Introduction

The Fibonacci sequence $\{F_n\}$ is defined as

$$F_n = F_{n-1} + F_{n-2}, \ n \geq 0,$$

with initial conditions $F_0 = 0$ and $F_1 = 1$. This sequence and its generalizations (e.g. k-Fibonacci sequences and k-Pell sequences), have been investigated extensively and there are applications in many diverse fields [1–3].

The Pell sequence $\{P_n\}$ is defined as

$$P_n = 2P_{n-1} + P_{n-2},\ n \geq 2,$$

with initial conditions $P_0 = 0$ and $P_1 = 1$. This sequence and its generalizations have also been studied extensively [4–7]. The Pell $p-$numbers are defined as follows.

Definition 1.1 ([8]). *For an integer p, the Pell p−numbers, denoted by* $\{P(n, p)\}$, *are*

$$P(n + p + 1) = 2P(n + p) + P(n),\ n \geq 0,$$

where $P(0) = P(1) = P(2) = \cdots = P(p) = 0$, $P(p) = 1$ *and* $P(p + 1) = 0$.

Example 1.1. *(i) The Pell p−numbers for* $p = 2$ *are given by*

$$P(n + 3) = 2P(n + 2) + P(n),\ n \geq 0,$$

so the sequence is $\{P(n, 2)\}_0^\infty = \{0, 1, 0, 0, 1, 2, 4, 9, 20, \dots\}$.

(ii) The Pell p−numbers for $p = 3$ *are given by*

$$P(n + 4) = 2P(n + 3) + P(n),\ n \geq 0,$$

so, the sequence is $\{P(n, 3)\}_0^\infty = \{0, 0, 1, 0, 0, 0, 1, 2, 4, 8, 17, 36, 76, 160, \dots\}$.

The generalized order k-Pell sequences were defined in [9] as the semi-direct product of finite cyclic groups. In [10], the quaternion-Pell sequence was introduced and extended to finite cyclic groups. The generalized order k-Pell sequences for special groups of nilpotency class 2 were given in [11]. Two new identities involving generalized Fibonacci and generalized Lucas numbers were introduced in [12]. In [13], a Horadam-type of generalization was provided which involves the generalized Fibonacci, generalized Lucas, Fibonacci, Lucas, Pell, Pell-Lucas, Fermat, Fermat-Lucas, Jacobsthal, Jacobsthal-Lucas, balancing, and co-balancing numbers. Expressions connecting two generalized classes of Fibonacci and Lucas polynomials were given in [14]. A class of polynomials known as convolved Pell polynomials was investigated in [15].

Another important sequence is the Mersenne numbers. The nth Mersenne number has the form $M_n = 2^n - 1$ where n is a nonnegative integer. A generalization of these numbers is as follows:

Definition 1.2 ([16]). *For* $k \geq 3$ *an integer, the generalized Mersenne numbers, denoted by* $\{M(k, n)\}_0^\infty$, *are*

$$M(k, n) = kM(k, n - 1) - (k - 1)M(k, n - 2),\ n \geq 0,$$

with initial conditions $M(k, 0) = 0$ *and* $M(k, 1) = 1$.

For $k = 3$, we have

$$M(3, n) = 3M(3, n - 1) - 2M(3, n - 2),\ n \geq 0,$$

which gives the sequence $\{M(3, n)\}_0^\infty = \{0, 1, 3, 7, \cdots\}$. The Mersenne numbers and their generalizations and properties have been studied extensively [17–21]. The characteristic polynomials of the Pell $p-$numbers and generalized Mersenne numbers are $x^{p+1} - 2x^p - 1$ and $x^2 - kx + k - 1$, respectively.

The Hadamard-type product of polynomials f and g is defined as follows:

Definition 1.3 ([22]). *The Hadamard-type product of polynomials f and g is $f * g = \sum_{i=0}^{\infty}(a_i * b_i)x^i$ where*

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

and $f(x) = a_m x^m + \cdots + a_1 x + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0$.

Diffie-Hellman key exchange is one of the earliest and most widely used public-key cryptographic primitives [23–26]. It allows two parties who have never met to exchange a secret key over an open channel. In [27], the Diffie-Hellman key exchange protocol was studied using matrices over noncommutative rings. A universal algebraic generalization of the Diffie-Hellman scheme was proposed in [28].

Motivated by the above results and the practical importance of Diffie-Hellman key exchange, we first generalize the Pell numbers and study their combinatorial representations. Then the characteristic polynomials of the Pell $p-$numbers and generalized Mersenne numbers are used to obtain new sequences. As an application, these sequences are employed to obtain a new Diffie-Hellman key exchange. This is the first algorithm that uses sequences and matrices to obtain a key.

The remainder of this paper is organized as follows: Section 2 presents the Pell $(p, t)-$numbers and their combinatorial representation and matrices are given. In Section 3, the Hadamard-type product of Pell $p-$number polynomials and generalized Mersenne numbers are considered. Section 4 provides a Diffie-Hellman key exchange using the Pell $(p, t)-$numbers and the Hadamard-type Pell-Mersenne $p-$numbers. Finally, some concluding remarks are given in Section 5.

2. The Pell $(p, t)-$numbers

In this section, we define the Pell $(p, t)-$numbers and obtain new sequences. Then their structure is investigated. The Pell $(p, t)-$numbers, p an integer, are defined as follows.

Definition 2.1. *For integers p and t, the Pell $(p, t)-$numbers, denoted by $\{P_n(p, t)\}$, are*

$$P_n(p, t) = 2P_{n-1}(p, t) + P_{n-p-1}(p, t) + \cdots + P_{n-p-t-1}(p, t),\ n \geq p + t + 1, \tag{2.1}$$

where $P_0(p, t) = P_1(p, t) = \cdots = P_{p+t-1}(p, t) = 0$, $P_{p+t}(p, t) = 1$.

Example 2.1. *(i) The Pell $(p, t)-$numbers for $p = 2$ and $t = 1$ are given by*

$$P_n(2, 1) = 2P_{n-1}(2, 1) + P_{n-3}(2, 1) + P_{n-4}(2, 1),\ n \geq 4,$$

so the sequence is $\{P_n(2, 1)\}_0^{\infty} = \{0, 0, 0, 1, 2, 4, 9, 21, 48, 109, 248, 565, \ldots\}$.

(ii) The Pell $(p, t)-$numbers for $p = 3$ and $t = 1$ are given by

$$P_n(3, 1) = 2P_{n-1}(3, 1) + P_{n-4}(3, 1) + P_{n-5}(3, 1),\ n \geq 5,$$

so the sequence is $\{P_n(3, 1)\}_0^{\infty} = \{0, 0, 0, 1, 2, 4, 8, 17, 37, 80, 172, \ldots\}$.

Lemma 2.1. *Let $u(x)$ be the generating function of the Pell $(p, t)-$numbers. Then*

$$u(x) = \frac{x^{p+t}}{1 - 2x - x^{p+1} - x^{p+2} - \cdots - x^{p+t+1}}. \tag{2.2}$$

Proof. We have

$$\begin{aligned}
u(x) &= \sum_{n=1}^{\infty} P_n(p,t)x^n \\
&= P_1(p,t)x + P_2(p,t)x^2 + \cdots + P_{p+t}(p,t)x^{p+t} + \sum_{n=p+t+1}^{\infty} P_n(p,t)x^n \\
&= x^{p+t} + \sum_{n=p+t+1}^{\infty} [2P_{n-1}(p,t) + P_{n-p-1}(p,t) + \cdots + P_{n-p-t-1}(p,t)]x^n \\
&= x^{p+t} + \sum_{n=p+t+1}^{\infty} 2P_{n-1}(p,t)x^n + \sum_{n=p+t+1}^{\infty} P_{n-p-1}(p,t)x^n + \cdots + \sum_{n=p+t+1}^{\infty} P_{n-p-t-1}(p,t)x^n \\
&= x^{p+t} + 2x\sum_{n=1}^{\infty} P_n(p,t)x^n + x^{p+1}\sum_{n=1}^{\infty} P_n(p,t)x^n + \cdots + x^{p+t+1}\sum_{n=1}^{\infty} P_n(p,t)x^n \\
&= x^{p+t} + 2xu(x) + x^{p+1}u(x) + \cdots + x^{p+t+1}u(x).
\end{aligned}$$

□

Theorem 2.1. *The Pell (p,t)−numbers $\{P_n(p,t)\}$ have the following exponential representation*

$$t(x) = x^{p+t} \exp \sum_{i=1}^{\infty} \frac{(x)^i}{i}(2 + x^p + x^{p+1} + \cdots + x^{p+t})^i, \; p \geq 2.$$

Proof. Using (2.2), we have

$$\ln u(x) = \ln x^{p+t} - \ln(1 - 2x - x^{p+1} - x^{p+2} - \cdots - x^{p+t+1}).$$

Since

$$\begin{aligned}
-\ln(1 - 2x - x^{p+1} - x^{p+2} - \cdots - x^{p+t+1}) = -[&-x(2 + x^p + x^{p+1} \\
&+ \cdots + x^{p+t}) - \frac{1}{2}x^2(2 + x^p + x^{p+1} + \cdots + x^{p+t})^2 \\
&- \cdots - \frac{1}{n}x^n(2 + x^p + x^{p+1} + \cdots + x^{p+t})^n - \ldots],
\end{aligned}$$

the result follows. □

Let $t = 1$. Then the recurrence relation (2.1) gives

$$\begin{bmatrix} P_n(p,1) \\ P_{n-1}(p,1) \\ \vdots \\ P_{n-p-t+1}(p,1) \\ P_{n-p-t}(p,1) \end{bmatrix} = \begin{bmatrix} 2 & 0 & \cdots & 0 & 1 & 1 \\ 1 & 0 & \cdots & 0 & 1 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} P_{n-1}(p,1) \\ P_{n-2}(p,1) \\ \vdots \\ P_{n-p-t}(p,1) \\ P_{n-p-t-1}(p,1) \end{bmatrix}.$$

Lemma 2.2. *For $p = 2$, $t = 1$, and $n \geq 4$, we have*

$$(M_2(1))^n = \begin{bmatrix} P_{n+3}(2,1) & P_{n+1}(2,1) + P_n(2,1) & P_{n+2}(2,1) + P_{n+1}(2,1) & P_{n+2}(2,1) \\ P_{n+2}(2,1) & P_n(2,1) + P_{n-1}(2,1) & P_{n+1}(2,1) + P_n(2,1) & P_{n+1}(2,1) \\ P_{n+1}(2,1) & P_{n-1}(2,1) + P_{n-2}(2,1) & P_n(2,1) + P_{n-1}(2,1) & P_n(2,1) \\ P_n(2,1) & P_{n-2}(2,1) + P_{n-3}(2,1) & P_{n-1}(2,1) + P_{n-2}(2,1) & P_{n-1}(2,1) \end{bmatrix}_{4\times 4}$$

where

$$M_2(1) = \begin{bmatrix} 2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}.$$

Proof. By induction on n. For $p = 2$, $t = 1$, and $n = 4$, we have

$$(M_2(1))^4 = \begin{bmatrix} 21 & 6 & 13 & 9 \\ 9 & 3 & 6 & 4 \\ 4 & 1 & 3 & 2 \\ 2 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} P_7(2,1) & P_5(2,1) + P_4(2,1) & P_5(2,1) + P_6(2,1) & P_6(2,1) \\ P_6(2,1) & P_4(2,1) + P_3(2,1) & P_4(2,1) + P_5(2,1) & P_5(2,1) \\ P_5(2,1) & P_3(2,1) + P_2(2,1) & P_3(2,1) + P_4(2,1) & P_4(2,1) \\ P_4(2,1) & P_2(2,1) + P_1(2,1) & P_2(2,1) + P_3(2,1) & P_3(2,1) \end{bmatrix}.$$

Now, assume that the statement holds for $n = s$. Then for $n = s + 1$

$$\begin{aligned} &(M_2(1))^{s+1} \\ &= \begin{bmatrix} 2 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} P_{s+3}(2,1) & P_{s+1}(2,1) + P_s(2,1) & P_{s+2}(2,1) + P_{s+1}(2,1) & P_{s+2}(2,1) \\ P_{s+2}(2,1) & P_s(2,1) + P_{s-1}(2,1) & P_{s+1}(2,1) + P_s(2,1) & P_{s+1}(2,1) \\ P_{s+1}(2,1) & P_{s-1}(2,1) + P_{s-2}(2,1) & P_s(2,1) + P_{s-1}(2,1) & P_s(2,1) \\ P_s(2,1) & P_{s-2}(2,1) + P_{s-3}(2,1) & P_{s-1}(2,1) + P_{s-2}(2,1) & P_{s-1}(2,1) \end{bmatrix} \\ &= \begin{bmatrix} P_{s+4}(2,1) & P_{s+2}(2,1) + P_{s+1}(2,1) & P_{s+3}(2,1) + P_{s+2}(2,1) & P_{s+3}(2,1) \\ P_{s+3}(2,1) & P_{s+1}(2,1) + P_s(2,1) & P_{s+2}(2,1) + P_{s+1}(2,1) & P_{s+2}(2,1) \\ P_{s+2}(2,1) & P_s(2,1) + P_{s-1}(2,1) & P_{s+1}(2,1) + P_s(2,1) & P_{s+1}(2,1) \\ P_{s+1}(2,1) & P_{s-1}(2,1) + P_{s-2}(2,1) & P_s(2,1) + P_{s-1}(2,1) & P_s(2,1) \end{bmatrix}, \end{aligned}$$

which completes the proof. □

Let $M_p(1) = [m_{i,j}]_{(p+2)\times(p+2)}$ be the companion matrix for the Pell $(p, 1)-$numbers. It can be readily established by mathematical induction on n that for $p \geq 3$ and $n \geq p + 2$

$$\begin{aligned} &(M_p(1))^n = \\ &\begin{bmatrix} P_{n+p+1}(p,1) & P_n(p,1) + P_{n+1}(p,1) & \cdots & P_{n+p}(p,1) + P_{n+p-1}(p,1) & P_{n+p}(p,1) \\ P_{n+p}(p,1) & P_{n-1}(p,1) + P_n(p,1) & \cdots & P_{n+p-1}(p,1) + P_{n+p-2}(p,1) & P_{n+p-1}(p,1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ P_{n+1}(p,1) & P_{n-p+1}(p,1) + P_{n-p}(p,1) & \cdots & P_n(p,1) + P_{n-1}(p,1) & P_n(p,1) \\ P_n(p,1) & P_{n-p}(p,1) + P_{n-p-1}(p,1) & \cdots & P_{n-1}(p,1) + P_{n-2}(p,1) & P_{n-1}(p,1) \end{bmatrix}. \end{aligned}$$

Theorem 2.2. *For $u \in \mathbb{N}$, $p \geq 2$ and $n \geq p + 2$, we have*

(i) $(M_p(1))^n (M_p(1))^u = (M_p(1))^{n+u}$.

(ii) $(M_p(1))^n(M_p(1))^u = (M_p(1))^u(M_p(1))^n$.

Proof. By induction on u. For $u = 1$ we have

$$\begin{aligned}
&(M_p(1))^n M_p(1) = \\
&\begin{bmatrix}
P_{n+p+1}(p,1) & P_n(p,1)+P_{n+1}(p,1) & \cdots & P_{n+p}(p,1)+P_{n+p-1}(p,1) & P_{n+p}(p,1) \\
P_{n+p+}(p,1) & P_{n-1}(p,1)+P_n(p,1) & \cdots & P_{n+p-1}(p,1)+P_{n+p-2}(p,1) & P_{n+p-1}(p,1) \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
P_{n+1}(p,1) & P_{n-p+1}(p,1)+P_{n-p}(p,1) & \cdots & P_n(p,1)+P_{n-1}(p,1) & P_n(p,1) \\
P_n(p,1) & P_{n-p}(p,1)+P_{n-p-1}(p,1) & \cdots & P_{n-1}(p,1)+P_{n-2}(p,1) & P_{n-1}(p,1)
\end{bmatrix} \\
&\times \begin{bmatrix}
2 & 0 & 0 & \cdots & 0 & 1 & 1 \\
1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & 0
\end{bmatrix} \\
&= \begin{bmatrix}
P_{n+p+2}(p,1) & P_{n+1}(p,1)+P_{n+2}(p,1) & \cdots & P_{n+p+1}(p,1)+P_{n+p}(p,1) & P_{n+p+1}(p,1) \\
P_{n+p+1}(p,1) & P_n(p,1)+P_{n+1}(p,1) & \cdots & P_{n+p}(p,1)+P_{n+p-1}(p,1) & P_{n+p}(p,1) \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
P_{n+2}(p,1) & P_{n-p+2}(p,1)+P_{n-p+1}(p,1) & \cdots & P_{n+1}(p,1)+P_n(p,1) & P_{n+1}(p,1) \\
P_{n+1}(p,1) & P_{n-p+1}(p,1)+P_{n-p}(p,1) & \cdots & P_n(p,1)+P_{n-1}(p,1) & P_n(p,1)
\end{bmatrix} \\
&= (M_p(1))^{n+1}.
\end{aligned}$$

Now suppose it is true for $u = s$. Then for $u = s + 1$

$$\begin{aligned}
&(M_p(1))^n M_p(1)^{s+1} = M_p(1)^{n+s} M_p(1) = \\
&\begin{bmatrix}
P_{n+s+p+1}(p,1) & P_{n+s}(p,1)+P_{n+s+1}(p,1) & \cdots & P_{n+s+p}(p,1)+P_{n+s+p-1}(p,1) & P_{n+s+p}(p,1) \\
P_{n+s+p+}(p,1) & P_{n+s-1}(p,1)+P_{n+s}(p,1) & \cdots & P_{n+s+p-1}(p,1)+P_{n+s+p-2}(p,1) & P_{n+s+p-1}(p,1) \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
P_{n+s+1}(p,1) & P_{n+s-p+1}(p,1)+P_{n+s-p}(p,1) & \cdots & P_{n+s}(p,1)+P_{n+s-1}(p,1) & P_{n+s}(p,1) \\
P_{n+s}(p,1) & P_{n+s-p}(p,1)+P_{n+s-p-1}(p,1) & \cdots & P_{n+s-1}(p,1)+P_{n+s-2}(p,1) & P_{n+s-1}(p,1)
\end{bmatrix} \\
&\times \begin{bmatrix}
2 & 0 & 0 & \cdots & 0 & 1 & 1 \\
1 & 0 & 0 & \cdots & 0 & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 1 & 0 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 & 0
\end{bmatrix} = M_p(1)^{n+s+1},
\end{aligned}$$

which completes the proof of (i). For (ii), using (i) we have

$$(M_p(1))^n(M_p(1))^u = (M_p(1))^{n+u} = (M_p(1))^{u+n} = (M_p(1))^u(M_p(1))^n.$$

□

For $n < 0$, the Pell $(p, t)-$numbers are defined as

$$P_{-n}(p,t) = P_{-n+p+t+1}(p,t) - 2P_{-n+p+t}(p,t) + P_{-n+t}(p,t) + \cdots + P_{-n}(p,t),\ n \geq 0.$$

For $n < 0$, the companion matrix of the Pell $(p, 1)-$numbers are defined as follows. For $n = -1$ we have

$$(M_p(1))_{-1} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & -2 & 0 & \cdots & 0 & -1 & -1 \end{bmatrix}$$

and by induction on n, we obtain

$$(M_p(1))_{-n} = \begin{bmatrix} P_{-n+p+1}(p,1) & P_{-n}(p,1)+P_{-n+1}(p,1) & \cdots & P_{-n+p}(p,1)+P_{-n+p-1}(p,1) & P_{-n+p}(p,1) \\ P_{-n+p}(p,1) & P_{-n-1}(p,1)+P_{-n}(p,1) & \cdots & P_{-n+p-1}(p,1)+P_{-n+p-2}(p,1) & P_{-n+p-1}(p,1) \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ P_{-n+1}(p,1) & P_{-n-p+1}(p,1)+P_{-n-p}(p,1) & \cdots & P_{-n}(p,1)+P_{-n-1}(p,1) & P_{-n}(p,1) \\ P_{-n}(p,1) & P_{-n-p}(p,1)+P_{-n-p-1}(p,1) & \cdots & P_{-n-1}(p,1)+P_{-n-2}(p,1) & P_{-n-1}(p,1) \end{bmatrix}.$$

Theorem 2.3. *For $u \in \mathbb{N}$, $p \geq 2$, and $n \geq p + 2$, we have*

(i) $(M_p(1))_{-n}(M_p(1))_{-u} = (M_p(1))_{-(n+u)}$.

(ii) $(M_p(1))_{-n}(M_p(1))_{-u} = (M_p(1))_{-u}(M_p(1))_{-n}$.

Proof. The proof is similar to that of Theorem 2.2 and so is omitted. □

3. The Hadamard-type Pell-Mersenne $p-$numbers

In this section, new sequences are obtained using the Hadamard-type product of the Pell $p-$numbers and Mersenne numbers. Then, some results on their structure are obtained. First, we give the new Hadamard-type Pell-Mersenne $p-$sequences.

Definition 3.1. *For integers $k \geq 3$ and $p \geq 3$, the Hadamard-type Pell-Mersenne $p-$sequences, denoted by $\{MP_n(k, p)\}_0^\infty$, are*

$$MP_{n+p+1}(k,p) = 2MP_{n+p}(k,p) - MP_{n+2}(k,p) + kMP_{n+1}(k,p) + (k-1)MP_n(k,p),\ n \geq 0, \tag{3.1}$$

with initial conditions $MP_0(k, p) = MP_1(k, p) = \cdots = MP_{p-1}(k, p) = 0$ and $MP_p(k, p) = 1$.

For example, the Hadamard-type Pell-Mersenne $p-$sequence for $p = 3$ and $k = 3$ is given by

$$MP_{n+4}(3,3) = 2MP_{n+3}(3,3) - MP_{n+2}(3,3) + 3MP_{n+1}(3,3) + 2MP_n(3,3),\ n \geq 0,$$

so $\{MP_n(3, 3)\}_0^\infty = \{0, 0, 0, 1, 2, 3, 7, 19, 44, 96, \cdots\}$, and for $p = 4$ and $k = 3$ is given by

$$MP_{n+5}(4,3) = 2MP_{n+4}(4,3) - MP_{n+2}(4,3) + 3MP_{n+1}(4,3) + 2MP_n(4,3),\ n \geq 0,$$

so $\{MP_n(4,3)\}_0^\infty = \{0,0,0,0,1,2,3,8,24,58,133,\dots\}$.

From the recurrence relation (3.1), we have

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

The Hadamard-type Pell-Mersenne $p-$numbers have the following companion matrix

$$N_p(k) = \begin{bmatrix} 2 & 0 & 0 & \cdots & 0 & -1 & k & k-1 \\ 1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 & 1 & 0 \end{bmatrix}_{(p+1)\times(p+1)},$$

and is called the Hadamard-type Pell-Mersenne $p-$matrix.

Theorem 3.1. *For $p = 3, k = 3$, and $n \geq 4$, we have*

$$(N_3(3))^n = \begin{bmatrix} MP_{n+3}(3,3) & -MP_{n+2}(3,3) + (3MP_{n+1}(3,3) + 2MP_n(3,3)) & 3MP_{n+2}(3,3) + 2MP_{n+1}(3,3) & 3MP_{n+2}(3,3) \\ MP_{n+2}(3,3) & -MP_{n+1}(3,3) + (3MP_n(3,3) + 2MP_{n-1}(3,3)) & 3MP_{n+1}(3,3) + 2MP_n(3,3) & 3MP_{n+1}(3,3) \\ MP_{n+1}(3,3) & -MP_n(3,3) + (3MP_{n-1}(3,3) + 2MP_{n-2}(3,3)) & 3MP_n(3,3) + 2MP_{n-1}(3,3) & 3MP_n(3,3) \\ MP_n(3,3) & -MP_{n-1}(3,3) + (3MP_{n-2}(3,3) + 2MP_{n-3}(3,3)) & 3MP_{n-1}(3,3) + 2MP_{n-2}(3,3) & 3MP_{n-1}(3,3) \end{bmatrix} := U_n(3)$$

where

$$N_3(3) = \begin{bmatrix} 2 & -1 & 3 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{4\times4}.$$

Proof. By induction on n. For $n = 4$ we have

$$(N_3(3))^4 = \begin{bmatrix} 1 & -1 & 3 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{4\times4}^4 = \begin{bmatrix} 19 & 6 & 27 & 14 \\ 7 & 5 & 13 & 6 \\ 3 & 1 & 8 & 4 \\ 2 & -1 & 3 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} MP_7(3,3) & -MP_6(3,3)+(3MP_5(3,3)+2MP_4(3,3)) & 3MP_6(3,3)+2MP_5(3,3) & 3MP_6(3,3) \\ MP_6(3,3) & -MP_5(3,3)+(3MP_4(3,3)+2MP_3(3,3)) & 3MP_5(3,3)+2MP_4(3,3) & 3MP_5(3,3) \\ MP_5(3,3) & -MP_4(3,3)+(3MP_3(3,3)+2MP_2(3,3)) & 3MP_4(3,3)+2MP_3(3,3) & 3MP_4(3,3) \\ MP_4(3,3) & -MP_3(3,3)+(3MP_2(3,3)+2MP_1(3,3)) & 3MP_3(3,3)+2MP_2(3,3) & 3MP_3(3,3) \end{bmatrix},$$

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

$$(N_3(3))^{t+1} = \begin{bmatrix} 2 & -1 & 3 & 2 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \times \begin{bmatrix} MP_{t+3}(3,3) & -MP_{t+2}(3,3)+(3MP_{t+1}(3,3)+2MP_t(3,3)) \\ MP_{t+2}(3,3) & -MP_{t+1}(3,3)+(3MP_t(3,3)+2MP_{t-1}(3,3)) \\ MP_{t+1}(3,3) & -MP_t(3,3)+(3MP_{t-1}(3,3)+2MP_{t-2}(3,3)) \\ MP_t(3,3) & -MP_{t-1}(3,3)+(3MP_{t-2}(3,3)+2MP_{t-3}(3,3)) \end{bmatrix}$$

$$\begin{matrix} 3MP_{t+2}(3,3)+2MP_{t+1}(3,3) & 3MP_{t+2}(3,3) \\ 3MP_{t+1}(3,3)+2MP_t(3,3) & 3MP_{t+1}(3,3) \\ 3MP_t(3,3)+2MP_{t-1}(3,3) & 3MP_t(3,3) \\ 3MP_{t-1}(3,3)+2MP_{t-2}(3,3) & 3MP_{t-1}(3,3) \end{matrix} \Bigg] := U_{t+1}(3),$$

which completes the proof. □

Corollary 3.1. *For $p = 3, k \geq 4$, and $n \geq 4$, we have*

$$(N_3(k))^n = \begin{bmatrix} MP_{n+3}(k,3) & -MP_{n+2}(k,3)+(kMP_{n+1}(k,3)+(k-1)MP_n(k,3)) \\ MP_{n+2}(k,3) & -MP_{n+1}(k,3)+(kMP_n(k,3)+(k-1)MP_{n-1}(k,3)) \\ MP_{n+1}(k,3) & -MP_n(k,3)+(kMP_{n-1}(k,3)+(k-1)MP_{n-2}(k,3)) \\ MP_n(k,3) & -MP_{n-1}(k,3)+(kMP_{n-2}(k,3)+(k-1)MP_{n-3}(k,3)) \end{bmatrix}$$

$$\begin{matrix} kMP_{n+2}(k,3)+(k-1)MP_{n+1}(k,3) & kMP_{n+2}(k,3) \\ kMP_{n+1}(k,3)+(k-1)MP_n(k,3) & kMP_{n+1}(k,3) \\ kMP_n(k,3)+(k-1)MP_{n-1}(k,3) & kMP_n(k,3) \\ kMP_{n-1}(k,3)+(k-1)MP_{n-2}(k,3) & kMP_{n-1}(k,3) \end{matrix} \Bigg],$$

where

$$N_3(k) = \begin{bmatrix} 2 & -1 & k & k-1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{4\times 4}.$$

Using induction on $p \geq 4$ and $n \geq p + 1$ gives

$$(N_3(3))^n = \begin{bmatrix} MP_{n+p}(k,p) & & kMP_{n+p-1}(k,p)+(k-1)MP_{n+p-2}(k,p) & (k-1)MP_{n+p-1}(k,p) \\ MP_{n+p-1}(k,p) & & kMP_{n+p-2}(k,p)+(k-1)MP_{n+p-3}(k,p) & (k-1)MP_{n+p-2}(k,p) \\ \vdots & N_3^* & \vdots & \vdots \\ MP_{n+1}(k,p) & & kMP_n(k,p)+(k-1)MP_{n-1}(k,p) & (k-1)MP_n(k,p) \\ MP_n(k,p) & & kMP_{n-1}(k,p)+(k-1)MP_{n-2}(k,p) & (k-1)MP_{n-1}(k,p) \end{bmatrix}$$

$$N_3^* = \begin{bmatrix} -MP_{n+2}(k,p)+(kMP_{n+1}(k,p)+(k-1)MP_n(k,p)) & \cdots \\ -MP_{n+1}(k,p)+(kMP_n(k,p)+(k-1)MP_{n-1}(k,p)) & \cdots \\ \vdots & \vdots \\ -MP_{n-(p-3)}(k,p)+(kMP_{n(p-2)}(k,p)+(k-1)MP_{n-(p-1)}(k,p)) & \cdots \\ -MP_{n-(p-2)}(k,p)+(kMP_{n(p-1)}(k,p)+(k-1)MP_{n-p}(k,p)) & \cdots \end{bmatrix}$$

$$\left.\begin{matrix} -MP_{n+p-1}(k,p)+(kMP_{n+p-2}(k,p)+(k-1)MP_{n+p-3}(k,p)) \\ -MP_{n+p-2}(k,p)+(kMP_{n+p-3}(k,p)+(k-1)MP_{n+p-4}(k,p)) \\ \vdots \\ -MP_{n}(k,p)+(kMP_{n-1}(k,p)+(k-1)MP_{n-2}(k,p)) \\ -MP_{n-1}(k,p)+(kMP_{n-2}(k,p)+(k-1)MP_{n-3}(k,p)) \end{matrix}\right] .$$

Lemma 3.1. *Let $y(x)$ be the Hadamard-type Pell-Mersenne $p-$numbers. Then*

$$y(x)=\frac{x^p}{1-2x+x^{p-1}-kx^p-(k-1)x^{p+1}}. \tag{3.2}$$

Proof. We have

$$\begin{aligned} y(x)&=\sum_{n=1}^{\infty}MP_n(k,p)x^n \\ &=MP_1(k,p)x^1+MP_2(k,p)(k,p)x^2+\cdots+MP_{p-1}(k,p)x^{p-1}+MP_p(k,p)x^p+\sum_{n=p+1}^{\infty}MP_n(k,p)x^n \\ &=x^p+\sum_{n=p+1}^{\infty}[2MP_{n+p}(k,p)-MP_{n+2}(k,p)+kMP_{n+1}(k,p)+(k-1)MP_n(k,p)]x^n \\ &=x^p+\sum_{n=p+1}^{\infty}2MP_{n+p}(k,p)x^n-\sum_{n=p+1}^{\infty}MP_{n+2}(k,p)x^n+k\sum_{n=p+1}^{\infty}MP_{n+1}(k,p)x^n \\ &\quad+(k-1)\sum_{n=p+1}^{\infty}MP_n(k,p)x^n \\ &=x^p+2x\sum_{n=1}^{\infty}MP_n(k,p)x^n-x^2\sum_{n=1}^{\infty}MP_n(k,p)x^n+kx^p\sum_{n=1}^{\infty}MP_n(k,p)x^n \\ &\quad+(k-1)x^{p+1}\sum_{n=1}^{\infty}MP_n(k,p)x^n \\ &=x^p+2xy(x)-x^{p-1}y(x)+kx^py(x)+(k-1)x^{p+1}y(x). \end{aligned}$$

□

Theorem 3.2. *The Hadamard-type Pell-Mersenne $p-$numbers sequences $\{MP_n(k,p)\}$ have the following exponential representation*

$$y(x)=x^p\exp\sum_{i=1}^{\infty}\frac{(x)^i}{i}(2-x^{p-2}+kx^{p-1}+(k-1)x^p)^i,\ p\geq 5.$$

Proof. Using (3.2), we have

$$\ln(y(x))=\ln x^p-\ln(1-2x+x^{p-1}-kx^p-(k-1)x^{p+1}).$$

Since

$$-\ln(1-2x+x^{p-1}-kx^p-(k-1)x^{p+1})=-[-x(2-x^{p-2}+kx^{p-1}+(k-1)x^p)$$

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

the result follows. □

4. Diffie-Hellman Key Exchange Using the Pell $(p, 1)-$numbers and the Hadamard-type Pell-Mersenne $p-$numbers

In this section, we present a new Diffie-Hellman key exchange using the Pell $(p, t)-$numbers and Hadamard-type Pell-Mersenne $p-$numbers matrices. Then, a security analysis is given. Two algorithms are given below.

Algorithm 1. *Alice and Bob want to establish a secret key. They select a Pell $(p, t)-$numbers matrix and q a prime number over an insecure channel. Alice chooses a random number $a \geq 4$ and sends $M_p(1)^a \pmod q$ to Bob. Bob chooses a random number $b \geq 4$ and sends $M_p(1)^b \pmod q$ to Alice. Alice and Bob both compute $M_p(1)^{ab} \pmod q$ and use this as their private key. The algorithm steps are given below and illustrated in Figure 1.*
Step 1. The prime number q and generator $M_p(1)$ are public (assume all users have agreed on the general linear group over a finite field F_q and $M_p(1)$ as the Pell $(p, 1)-$matrix).
Step 2. Alice chooses a random number $a \geq 4$ and sends $M_p(1)^a \pmod q$ to Bob.
Step 3. Bob chooses a random number $b \geq 4$ and sends $M_p(1)^b \pmod q$ to Alice.
Step 4. Alice and Bob both compute $M_p(1)^{ab} \pmod q$ and use this as the private key for future communications.

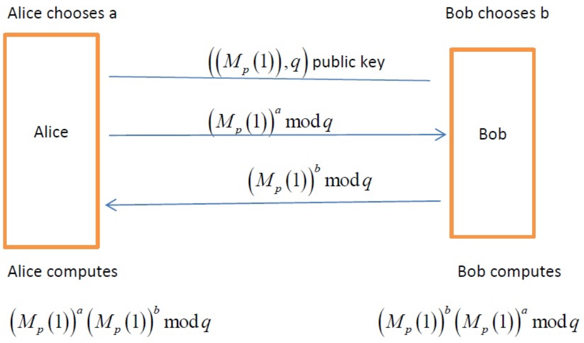

Figure 1. Algorithm 1.

Example 4.1. *Let $(M_2(1), 13)$ be the public key. Alice chooses $a = 4$ and using Lemma 2.2 computes* $M_2(1)^4 \pmod{13}$

$$(M_2(1))^4 = \begin{bmatrix} 21 & 6 & 13 & 9 \\ 9 & 3 & 6 & 4 \\ 4 & 1 & 3 & 2 \\ 2 & 0 & 1 & 1 \end{bmatrix} \equiv \begin{bmatrix} 8 & 6 & 0 & 9 \\ 9 & 3 & 6 & 4 \\ 4 & 1 & 3 & 2 \\ 2 & 0 & 1 & 1 \end{bmatrix} \pmod{13},$$

and sends this to Bob. Bob chooses $b = 7$ and obtains $M_2(1)^7$ (mod 13)

$$(M_2(1))^7 = \begin{bmatrix} 248 & 69 & 157 & 109 \\ 109 & 30 & 69 & 48 \\ 48 & 13 & 30 & 21 \\ 21 & 6 & 13 & 9 \end{bmatrix} \equiv \begin{bmatrix} 1 & 4 & 1 & 5 \\ 5 & 4 & 4 & 9 \\ 9 & 0 & 4 & 8 \\ 8 & 6 & 0 & 9 \end{bmatrix} \pmod{13},$$

and sends this to Alice. From Theorem 2.2, we have $M_2(1)^4 M_2(1)^7 = M_2(1)^7 M_2(1)^4$, so Alice and Bob both compute

$$(M_2(1))^7(M_2(1))^4 = \begin{bmatrix} 248 & 69 & 157 & 109 \\ 109 & 30 & 69 & 48 \\ 48 & 13 & 30 & 21 \\ 21 & 6 & 13 & 9 \end{bmatrix} \begin{bmatrix} 8 & 6 & 0 & 9 \\ 9 & 3 & 6 & 4 \\ 4 & 1 & 3 & 2 \\ 2 & 0 & 1 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 4 & 1 & 5 \\ 5 & 4 & 4 & 9 \\ 9 & 0 & 4 & 8 \\ 8 & 6 & 0 & 9 \end{bmatrix} \begin{bmatrix} 21 & 6 & 13 & 9 \\ 9 & 3 & 6 & 4 \\ 4 & 1 & 3 & 2 \\ 2 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 6 & 6 & 6 & 6 \\ 6 & 7 & 6 & 0 \\ 0 & 6 & 7 & 6 \\ 6 & 1 & 6 & 2 \end{bmatrix} \pmod{13}.$$

This is used as the private key for future communications.

Algorithm 2. *This algorithm is the same as Algorithm 1 but in Step 1 $N_p(k)$ is used.*

Example 4.2. *Let $(N_3(3), 11)$ be the public key. Alice chooses $a = 5$ and using Lemma 2.2 computes $N_3(3)^5$ (mod 11)*

$$(N_3(3))^5 = \begin{bmatrix} 44 & 8 & 71 & 38 \\ 19 & 6 & 27 & 14 \\ 7 & 5 & 13 & 6 \\ 3 & 1 & 8 & 4 \end{bmatrix} \equiv \begin{bmatrix} 0 & 8 & 5 & 5 \\ 8 & 6 & 5 & 3 \\ 7 & 5 & 2 & 6 \\ 3 & 1 & 8 & 4 \end{bmatrix} \pmod{11},$$

and sends this to Bob. Bob chooses $b = 6$ and obtains $N_3(3)^6$ (mod 11)

$$(N_3(3))^6 = \begin{bmatrix} 96 & 27 & 170 & 88 \\ 44 & 8 & 71 & 38 \\ 19 & 6 & 27 & 14 \\ 7 & 5 & 13 & 6 \end{bmatrix} \equiv \begin{bmatrix} 8 & 5 & 5 & 0 \\ 0 & 8 & 5 & 5 \\ 8 & 6 & 5 & 3 \\ 7 & 5 & 2 & 6 \end{bmatrix} \pmod{11},$$

and sends this to Alice. From Theorem 2.2, we have $N_3(3)^5 N_3(3)^6 = N_3(3)^6 N_3(3)^5$, so Alice and Bob both compute

$$(N_3(3))^5(N_3(3))^6 = \begin{bmatrix} 0 & 8 & 5 & 5 \\ 8 & 6 & 5 & 3 \\ 7 & 5 & 2 & 6 \\ 3 & 1 & 8 & 4 \end{bmatrix} \begin{bmatrix} 8 & 5 & 5 & 0 \\ 0 & 8 & 5 & 5 \\ 8 & 6 & 5 & 3 \\ 7 & 5 & 2 & 6 \end{bmatrix} \equiv \begin{bmatrix} 9 & 9 & 9 & 8 \\ 4 & 1 & 2 & 8 \\ 4 & 7 & 5 & 1 \\ 6 & 3 & 2 & 9 \end{bmatrix} \pmod{11}.$$

This is used as the private key for future communications.

One way for an adversary to obtain the key is to generate all possible matrices. Since q can be a very large prime number, it is intractable to check all q^{m^2} matrices where m is the matrix size. Because the matrices used to make the key are invertible, it is possible to check only the order of the general linear group $GL_m(F_q)$ which also can be made intractable by choosing q a very large prime number and m large.

$GL_m(F_q)$, q a prime number, consists of all invertible matrices of order $m \times m$ over F_q [29]. This group has order

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

Consider $M_p(1)$. Since $M_p(1)$ is a $(p+2) \times (p+2)$ matrix, we must check

$$\mid GL_{p+2}(F_q) \mid = (q^{p+2} - q^{p+1})(q^{p+2} - q^{p}) \cdots (q^{p+2} - q)(q^{p+2} - 1), \tag{4.1}$$

matrices. For example, for $M_{48}(1)$ over F_{37}, we have

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

and for the key $N_p(k)$

$$\mid GL_{p+1}(F_q) \mid = (q^{p+1} - q^{p})(q^{p+1} - q^{p-1}) \cdots (q^{p+1} - q)(q^{p+1} - 1). \tag{4.2}$$

Table 1 gives $N_p(k)$, q, and $\mid GL_p(F_q) \mid$ for $2 \leq p \leq 4$ and $2 \leq q \leq 11$. This shows that as p and q increase, the number of matrices grows significantly. Thus, it can be made intractable to break the protocol. From (4.1) and (4.2), it is clear that the key size increases with p, i.e. $\mid GL_p(F_q) \mid \to \infty$. Therefore, if the key space is large it is not practical to break the system via a brute-force attack [30].

Table 1. $N_p(k)$, q, and $\mid GL_p(F_q) \mid$ for $2 \leq p \leq 4$ and $2 \leq q \leq 11$.

$N_p(k)$	q	$\mid GL_p(F_q) \mid$
$N_2(k)$	2	$\mid GL_3(F_2) \mid = (2^3 - 2^2)(2^3 - 2)(2^3 - 1) = 168$
	3	$\mid GL_3(F_3) \mid = (3^3 - 3^2)(3^3 - 3)(3^3 - 1) = 11232$
	5	$\mid GL_3(F_5) \mid = (5^3 - 5^2)(5^3 - 5)(5^3 - 1) = 1488000$
	7	$\mid GL_3(F_7) \mid = (7^3 - 7^2)(7^3 - 7)(7^3 - 1) = 28613088$
	11	$\mid GL_3(F_{11}) \mid = (11^3 - 11^2)(11^3 - 11)(11^3 - 1) = 2124276000$
$N_3(k)$	2	$\mid GL_4(F_2) \mid = (2^4 - 2^3)(2^4 - 2^2)(2^4 - 2)(2^3 - 1) = 20160$
	3	$\mid GL_4(F_3) \mid = (3^4 - 3^3)(3^4 - 3^2)(3^4 - 3)(3^3 - 1) = 24261120$
	5	$\mid GL_4(F_5) \mid = (5^4 - 5^3)(5^4 - 5^2)(5^4 - 5)(5^4 - 1) = 116064000000$
	7	$\mid GL_4(F_7) \mid = (7^4 - 7^3)(7^4 - 7^2)(7^4 - 7)(7^4 - 1) = 27811094169600$
	11	$\mid GL_4(F_{11}) \mid = (11^4 - 11^3)(11^4 - 11^2)(11^4 - 11)(11^4 - 1) = 4.13 \times 10^{16}$
$N_4(k)$	2	$\mid GL_5(F_2) \mid = (2^5 - 2^4)(2^5 - 2^3)(2^5 - 2^2)(2^5 - 2)(2^5 - 1) = 9999360$
	3	$\mid GL_5(F_3) \mid = 475566474240$
	5	$\mid GL_5(F_5) \mid = 2.26 \times 10^{17}$
	7	$\mid GL_5(F_7) \mid = 1.8 \times 10^{25}$
	11	$\mid GL_5(F_{11}) \mid = 9.7 \times 10^{24}$

5. Conclusions

In this paper, two new sequences were defined using the Pell and Mersenne sequences. Their structures were examined and some results obtained using them. Then, they were used to develop a new Diffie-Hellman key exchange protocol that provides high security. The matrices $M_P(1)$ and $N_P(k)$ are constructed using these sequences so calculations are fast when a and b are very large, but it is intractable for an adversary to determine the key. This is the first algorithm that uses sequences and matrices to obtain a key. The sequences presented are suitable for constructing private keys. Note that other sequences such as Fibonacci and Pell sequences can be used with the proposed approach to construct keys. In general, any matrix sequence that has the commutative property for multiplication is suitable for use with this algorithm. As future work, the new sequences presented in this paper can be used in other private or public key encryption algorithms.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

Researchers would like to thank the Deanship of Scientific Research, Qassim University, for funding the publication of this paper.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. N. Jiang, W. Y. Wu, L. Wang, The quantum realization of Arnold and Fibonacci image scrambling, *Quantum Inf. Process.*, **13** (2014), 1223–1236. https://doi.org/10.1007/s11128-013-0721-7
2. B. Prased, Coding theory on Lucas p numbers, *Discrete Math. Algorithms Appl.*, **8** (2016), 1650074. https://doi.org/10.1142/S1793830916500749
3. T. Zhang, S. Li, R. Ge, M. Yuan, Y. Ma, A novel 1D hybrid chaotic map-based image compression and encryption using compressed sensing and Fibonacci-Lucas transform, *Math. Probl. Eng.*, **2016** (2016), 7683687. https://doi.org/10.1155/2016/7683687
4. S. Halici, S. Oz, On Gaussian Pell polynomials and their some properties, *Palest. J. Math.*, **7** (2018), 251–256.
5. M. Hashemi, E. Mehraban, Fibonacci length and the generalized order k-Pell sequences of the 2-generator p-groups of nilpotency class 2, *J. Algebra Appl.*, **22** (2023), 2350061. https://doi.org/10.1142/S0219498823500615
6. J. Hiller, Y. Aküzüm, Ö. Deveci, The adjacency-Pell-Hurwitz numbers, *Integers*, **18** (2018), A83. https://doi.org/10.5281/zenodo.10682656

7. E. Kilic, The generalized order-k Fibonacci-Pell sequence by matrix methods, *J. Comput. Appl. Math.*, **209** (2007), 133–145. https://doi.org/10.1016/j.cam.2006.10.071

8. E. Kilic, The generalized Pell (p, i)-numbers and their Binet formulas, combinatorial representations, sums, *Chaos Solit. Fractals*, **40** (2009), 2047–2063. https://doi.org/10.1016/j.chaos.2007.09.081

9. Ö. Deveci, The k-nacci sequences and the generalized order k-Pell sequences in the semi-direct product of finite cyclic groups, *Chiang Mai J. Sci.*, **40** (2013), 89–98.

10. Ö. Deveci, A. G. Shannon, The quaternion-Pell sequence, *Commun. Algebra*, **46** (2018), 5403–5409. https://doi.org/10.1080/00927872.2018.1468906

11. M. Hashemi, E. Mehraban, The generalized order k-Pell sequences in some special groups of nilpotency class 2, *Commun. Algebra*, **50** (2021), 1768–1784. https://doi.org/10.1080/00927872.2021.1988959

12. W. M. Abd-Elhameed, N. A. Zeyada, New identities involving generalized Fibonacci and generalized Lucas numbers, *Indian J. Pure Appl. Math.*, **49** (2018), 527–537. https://doi.org/10.1007/s13226-018-0282-7

13. A. K. Amin, N. A. Zeyada, Some new identities of a type of generalized numbers involving four parameters, *AIMS Math.*, **7** (2021), 12962–12980. https://doi.org/10.3934/math.2022718

14. W. M. Abd-Elhameed, A. N. Philippou, N. A. Zeyada, Novel results for two generalized classes of Fibonacci and Lucas polynomials and their uses in the reduction of some radicals, *Mathematics*, **10** (2022), 2342. https://doi.org/10.3390/math10132342

15. W. M. Abd-Elhameed, A. Napoli, New formulas of convolved Pell polynomials, *AIMS Math.*, **9** (2024), 565–593. https://doi.org/10.3934/math.2024030

16. P. Ochalik, A. Wloch, On generalized Mersenne numbers, their interpretations and matrix generators, *Ann. Univ. Mariae Curie-Skłodowska, Sect. A*, **72** (2018), 69–76. http://dx.doi.org/10.17951/a.2018.72.1.69-76

17. P. Catarino, H. Campos, P. Vasco, On the Mersenne sequence, *Ann. Math. Inform.*, **46** (2016), 37–53.

18. M. Chelgham, A. Boussayoud, On the k-Mersenne-Lucas numbers, *Notes Number Theory Discrete Math.*, **27** (2021), 7–13. https://doi.org/10.7546/nntdm.2021.27.1.7-13

19. A. M. Sergeer, Generalized Mersenne matrices and Balonin's conjecture, *Aut. Control Comp. Sci.*, **48** (2014), 214–220. https://doi.org/10.3103/S0146411614040063

20. Y. Soykan, On generalized p-Mersenne numbers, *Earthline J. Math. Sci.*, **8** (2022), 83–120. https://doi.org/10.34198/ejms.8122.83120

21. Y. Zheng, S. Shon, Exact inverse matrices of Fermat and Mersenne circulant matrix, *Abstr. Appl. Anal.*, **2015** (2015), 760823. https://doi.org/10.1155/2015/760823

22. Y. Akuzum, Ö. Deveci, The Hadamard-type k-step Fibonacci sequences in groups, *Commun. Algebra*, **48** (2020), 2844–2856. https://doi.org/10.1080/00927872.2020.1723609

23. L. Chen, Y. Chen, The n-Diffie-Hellman problem and multiple-key encryption, *Int. J. Inf. Secur.*, **11** (2012), 305–320. https://doi.org/10.1007/s10207-012-0171-8

24. H. Chien, Provably secure authenticated Diffie-Hellman key exchange for resource-limited smart card, *J. Shanghai Jiaotong Univ. (Sci.)*, **19** (2014), 436–439. https://doi.org/10.1007/s12204-014-1521-7

25. D. Coppersmith, A. M. Odlzyko, R. Schroeppel, Discrete logarithms in $GF(p)$, *Algorithmica*, **1** (1986), 1–15. https://doi.org/10.1137/0406010

26. L. Harn, C. Lin, Efficient group Diffie-Hellman key agreement protocols, *Comput. Electr. Eng.*, **40** (2014), 1972–1980. https://doi.org/10.1016/j.compeleceng.2013.12.018

27. M. Eftekhari, A Diffie-Hellman key exchange protocol using matrices over noncommutative rings, *Groups Complex. Cryptol.*, **4** (2012), 167–176. https://doi.org/10.1515/gcc-2012-0001

28. J. Partala, Algebraic generalization of Diffie-Hellman key exchange, *J. Math. Cryptol.*, **12** (2018), 1–21. https://doi.org/10.1515/jmc-2017-0015

29. P. A. Grillet, *Abstract Algebra*, 2 Eds., Berlin: Springer, 2007.

30. W. Stallings, *Cryptography and Network Security: Principles and Practice*, 7 Eds., Harlow: Pearson, 2017.

AIMS Press

©2024 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)