Palestine Journal of Mathematics

Vol 15(1)(2026) , 129–138

Cryptography using generalized Pell $(k, i)-$ numbers with Diffie-Hellman and Elliptic Curve

R. Mohanty and H. Mahato

Communicated by: Manoj Patel

MSC 2010 Classifications: 11T71, 11B39, 14G50, 94A60.

Keywords and phrases: Diffie-Hellman Key Exchange, Elliptic Curve, Generalized Pell Sequence & Matrix.

The authors would like to thank the reviewers and editor for their constructive comments and valuable suggestions that improved the quality of our paper.

Abstract In this article, we have proposed a new public key cryptography using Diffie-Hellman and Elliptic curve cryptography with generalized Pell matrix. The key establishment (exchange of key matrix P_k^n for encryption-decryption) scheme with the help of generalized Pell sequences has been proposed. In this scheme, instead of exchanging key matrix, we need to exchange only pair of numbers (k, n), which reduces the time complexity as well as space complexity and build up a large key-space.

1 Introduction

Cryptography is a method of protecting messages and secure transmission through the use of encrypted message, so that only the intended recipient can read and process it. In 1976 Whitfield Diffie and Martin Hellman purposed the concept of Diffie-Hellman key exchange protocol, which is the most primitive thought behind public key cryptography [4], [10] .
Nihal Tas et.al [16] introduced a new coding and decoding (encryption and decryption) method using the generalized Pell (k, i)- numbers. The relations among the code matrix elements error detection and correction have been established for this coding theory and also gives two new block algorithms using Pell numbers and generalized Pell (k, i)- numbers.
In [14] B.Ravi Kumar presented Cryptographic model using Diffie-Hellman encryption which uses points on elliptic curve and as an additional security the Fibonacci-Q matrix is introduced.
In this article, we investigate a public key cryptosystem using Diffie-Hellman Elliptic curve cryptography with generalized Pell (k, i)- matrix as key matrix. Our algorithm is quite reliable.

2 Preliminaries

In this section, we have described some preliminary concepts and definitions related to our main results.

2.1 Discrete Logarithmic Problem(DLP)

The discrete logarithmic problem for a finite cyclic group M with respect to a given generator m and an element y find an $x \in \mathbb{Z}$ such that $y = m^x$. Such an x is defined modulo $|M|$. We call the smallest such non-negative integer x the discrete logarithm of y with respect to the base m [5], [12].

2.2 Diffie-Hellman(DH) key exchange scheme

Using DLP the DH key exchange scheme may be described on a finite cyclic group M. Consider a generator m of M. Alice and Bob choose their own private keys 'a' and 'b' from the set

$\{2, 3, \ldots, |M|-1\}$ respectively and compute m^a and m^b. After exchanging their public keys m^a and m^b to each other the encryption and decryption keys are computed as $m^{ab} = (m^a)^b = (m^b)^a$ [4], [12].

2.3 Elliptic Curve

The elliptic curve over $\mathbb{Z}_p,\ p > 3$, is the set of all pairs $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ which satisfies

$$y^2 = x^3 + ux + v \pmod{p} \tag{2.1}$$

together with an imaginary point 0 at infinity, which is treated as an identity i.e. $P + 0 = P$, where $u,\ v \in \mathbb{Z}_p$ with condition $4u^3 + 27v^2 \neq 0 \pmod{p}$ [8], [9].

Let $P = (x_1,\ y_1)$ and $Q = (x_2,\ y_2)$ be two points on the elliptic curve then $P + Q = R = (x_3,\ y_3)$ in the elliptic curve is defined as follows:-

$$x_3 = s^2 - x_1 - x_2 \pmod{p} \tag{2.2}$$

$$y_3 = s(x_1 - x_3) - y_1 \pmod{p} \tag{2.3}$$

where

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \pmod{p},\ if P \neq Q\ (point\ addition) \\ \dfrac{3{x_1}^2 + u}{2y_1} \pmod{p},\ if P = Q\ (point\ doubling) \end{cases}$$

It may be noted that the elliptic curve forms a cyclic group when p is prime [8], [9].

2.4 Pell sequence and Pell P^n- matrix

In [7], [15] and [16] Pell number was discovered by John Pell. The recurrence relation for Pell number is defined as

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

with initial values $P_0 = 0,\ P_1 = 1$. Then the characteristic equation of the Pell recurrence relation is

$$t^2 - 2t - 1 = 0$$

with the roots $\gamma = 1 + \sqrt{2}\ and\ \delta = 1 - \sqrt{2}$. Using the roots Binet formula for the Pell number is given by

$$P_n = \frac{\gamma^n - \delta^n}{\gamma - \delta}$$

and

$$\lim_{n\to\infty} \frac{P_{n+1}}{P_n} = \gamma.$$

The Pell $P - matrix$ of order 2 is of the form:

$$P = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}.$$

and observed that the n-th power of the P-matrix and its determinant are given by

$$P^n = \begin{pmatrix} p_{n+1} & p_n \\ p_n & p_{n-1} \end{pmatrix}$$

and

$$\det P^n = p_{n+1}p_{n-1} - p_n^2 = (-1)^n.$$

3 Generalized Pell (k,i)-numbers and Pell-matrix (p_k^n):

In [7], [15], the generalized $Pell\ (k,i)-$ numbers are defined by the recurrence relations

$$P_k^{(i)}(n) = 2P_k^{(i)}(n-1) + P_k^{(i)}(n-k-1),\ 0 \le i \le k,\ n > k+1,\ k = 1,2,3,... \tag{3.1}$$

with initial values $P_k^{(i)}(1) = \cdots = P_k^{(i)}(i) = 0,\ P_k^{(i)}(i+1) = \cdots = P_k^{(i)}(k+1) = 1$.

The sequence of generalized Pell (k,i)-numbers can be extended in negative direction also using the recurrence relation equation (3.1) rewritten as

$$P_k^{(i)}(n-k-1) = P_k^{(i)}(n) - 2P_k^{(i)}(n-1),$$

i.e.

$$P_k^{(i)}(r) = P_k^{(i)}(r+k+1) - 2P_k^{(i)}(r+k), r \le 0. \tag{3.2}$$

In [7], [15], the generalized Pell matrix P_k^n has been defined as follows for $i = k$,

$$P_k^n = \begin{pmatrix} P_k^k(n+k+1) & P_k^k(n+1) & P_k^k(n+2) & \dots & P_k^k(n+k) \\ P_k^k(n+k) & P_k^k(n) & P_k^k(n+1) & \dots & P_k^k(n+k-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ P_k^k(n+2) & P_k^k(n-k+2) & P_k^k(n-k+3) & \dots & P_k^k(n+1) \\ P_k^k(n+1) & P_k^k(n-k+1) & P_k^k(n-k+2) & \dots & P_k^k(n) \end{pmatrix}_{(k+1)\times(k+1)}. \tag{3.3}$$

for all $n \in \mathbb{Z}$. It also denoted by $A^{(n)}$ and in particular, we have

$$A^{(1)} = A = \begin{pmatrix} 2 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}_{(k+1)\times(k+1)}. \tag{3.4}$$

and

$$A^{(-1)} = A^{-1} = \begin{pmatrix} 0 & 1 & \dots & 0 & 0 \\ 0 & 0 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 1 \\ 1 & -2 & \dots & 0 & 0 \end{pmatrix}_{(k+1)\times(k+1)}. \tag{3.5}$$

Also

$$\det A^{(n)} = (-1)^{n(k+2)},\ \forall\ n \in \mathbb{Z}. \tag{3.6}$$

It can be observed that $P_k^0 = A^{(0)} = I$ and $P_k^n = A^{(n)}$ is n time multiple of A, so we have the following statement.

Theorem 3.1. *For A, defined in equation (3.4) $A^{(n)} = A^n$, the nth power of A, $\forall\ n \in \mathbb{Z}^+$.*

Proof. It is clear that, for $n = 1$ as $A^1 = A$. Assume that the statement holds for n, which satisfies equation (3.4).

Now

$$A^{n+1} = A^n \times A = A^{(n)} \times A$$

$$= \begin{pmatrix} P_k^k(n+k+1) & P_k^k(n+1) & P_k^k(n+2) & \dots & P_k^k(n+k) \\ P_k^k(n+k) & P_k^k(n) & P_k^k(n+1) & \dots & P_k^k(n+k-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ P_k^k(n+2) & P_k^k(n-k+2) & P_k^k(n-k+3) & \dots & P_k^k(n+1) \\ P_k^k(n+1) & P_k^k(n-k+1) & P_k^k(n-k+2) & \dots & P_k^k(n) \end{pmatrix}_{(k+1)\times(k+1)}$$

$$\times \begin{pmatrix} 2 & 0 & \dots & 0 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}_{(k+1)\times(k+1)}$$

$$= \begin{pmatrix} 2P_k^k(n+k+1) + P_k^k(n+1) & P_k^k(n+2) & \dots & P_k^k(n+k+1) \\ 2P_k^k(n+k) + P_k^k(n) & P_k^k(n+1) & \dots & P_k^k(n+k) \\ \vdots & \vdots & \vdots & \vdots \\ 2P_k^k(n+2) + P_k^k(n-k+2) & P_k^k(n-k+3) & \dots & P_k^k(n+2) \\ 2P_k^k(n+1) + P_k^k(n-k+1) & P_k^k(n-k+2) & \dots & P_k^k(n+1) \end{pmatrix}_{(k+1)\times(k+1)}$$

$$= A^{(n+1)}.$$

Replacing n by $n+k+2,\ n+k+1, \dots\ n+3, n+2$ successively in equation (3.1), we get

$$P_k^k(n+k+2) = 2P_k^k(n+k+1) + P_k^k(n+1),$$
$$P_k^k(n+k+1) = 2P_k^k(n+k) + P_k^k(n),$$
$$P_k^k(n+3) = 2P_k^k(n+2) + P_k^k(n-k+2), \text{ and}$$
$$P_k^k(n+2) = 2P_k^k(n+1) + P_k^k(n-k+1).$$

Therefore, $A^{n+1} = A^{(n+1)}$. This completes the proof. □

Theorem 3.2. *$A^{(-n)} = (A^{-1})^n = A^{-n}$, when A^{-1} defined in equation (3.5).*

Proof. The proof is similar to Theorem 3.1. □

3.1 Inverse of Pell-matrix (p_k^{-n}):

From equation (3.6), it is clear thatP_k^n is invertible, $\forall\ n \in \mathbb{Z}$.

Theorem 3.3. *Inverse of P_k^n is P_k^{-n}, $\forall\ n \in \mathbb{Z}$.*

Proof. From Theorem 3.1 and 3.2 with equation (3.3), we have $P_k^n = A^n$ and $P_k^{(-n)} = A^{(-n)}$. It can be easily verified from equations (3.4) and (3.5) that, $A^1 \times A^{-1} = I$, also assume that $P_k^{n-1} \times P_k^{-(n-1)} = I$. Now by using Theorem 3.1 and 3.2, we get

$$P_k^n \times P_k^{-n} = A^{(n)} \times A^{(-n)}$$
$$= A^{n-1} \times A^1 \times A^{-1} \times A^{-(n-1)}$$
$$= A^{n-1} \times I \times A^{-(n-1)}$$
$$= I.$$

Therefore the inverse of P_k^n is P_k^{-n} and vice versa $\forall n \in \mathbb{Z}$. □

4 Results

Theorem 4.1. $P^n_{k,i} = (P_{k,k})^n (P_{k,i})^0, n > 0,\ for\ 0 \le i \le k.$

Proof. By using mathematical induction on n, clearly it holds for $n = 1$.

$$
\begin{aligned}
P^1_{k,i} &= (P_{k,k})^1 (P_{k,i})^0 \\
&= \begin{pmatrix} 2 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \begin{pmatrix} p^i_k(k+1) & p^i_k(1) & p^i_k(2) & \cdots & p^i_k(k) \\ p^i_k(k) & p^i_k(0) & p^i_k(1) & \cdots & p^i_k(k-1) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p^i_k(2) & p^i_k(-k+2) & p^i_k(-k+3) & \cdots & p^i_k(1) \\ p^i_k(1) & p^i_k(-k+1) & p^i_k(-k+2) & \cdots & p^i_k(0) \end{pmatrix} \\
&= \begin{pmatrix} 2p^i_k(k+1) + p^i_k(1) & 2p^i_k(1) + p^i_k(-k+1) & \cdots & 2p^i_k(k) + p^i_k(0) \\ p^i_k(k+1) & p^i_k(1) & \cdots & p^i_k(k) \\ \vdots & \vdots & \vdots & \vdots \\ p^i_k(3) & p^i_k(-k+3) & \cdots & p^i_k(2) \\ p^i_k(2) & p^i_k(-k+2) & \cdots & p^i_k(1) \end{pmatrix} \\
&= \begin{pmatrix} p^i_k(k+2) & p^i_k(2) & \cdots & p^i_k(k+1) \\ p^i_k(k+1) & p^i_k(1) & \cdots & p^i_k(k) \\ \vdots & \vdots & \vdots & \vdots \\ p^i_k(3) & p^i_k(-k+3) & \cdots & p^i_k(2) \\ p^i_k(2) & p^i_k(-k+2) & \cdots & p^i_k(1) \end{pmatrix} \\
&= p^{(1)}_{k,i}.
\end{aligned}
$$

Now, we assume that this is true for n. So

$$p^{(n)}_{k,i} = (p^{(n)}_{k,k})(p^{(0)}_{k,i}). \tag{4.1}$$

Then we have to show that it holds for $n+1$. That is to show,

$$p^{(n+1)}_{k,i} = (p^{(n+1)}_{k,k})(p^{(0)}_{k,i}). \tag{4.2}$$

Multiplying both sides of (4.1) by $p^{(1)}_{k,k}$, we obtain

$$
\begin{aligned}
(p^{(1)}_{k,k})(p^{(n)}_{k,i}) &= (p^{(1)}_{k,k})(p^{(n)}_{k,k})(p^{(0)}_{k,i}) \\
&= (p^{(n+1)}_{k,k})(p^{(0)}_{k,i}) \\
&= p^{(n+1)}_{k,i}.
\end{aligned} \tag{4.3}
$$

Therefore, the result is true by the method of induction. □

Theorem 4.2. *For $n > 0$, we have $p^{(-n)}_{k,i} = (p^{(-n)}_{k,k})(p^{(0)}_{k,i})$. Another way $p^{(-n)}_{k,i} = (p^{(-1)}_{k,k})^n (p^{(0)}_{k,i})$.*

Proof. The proof is same as Theorem 4.1. □

Theorem 4.3. *Prove that*

$$\det(P^n_{k+2,i}) = \det(P^n_{k,i}) = \begin{cases} -1, & if\ k\ odd \\ 2, & if\ k\ even \end{cases}, \forall\ k \geqslant 1\ with\ fixed\ value\ of\ n,\ i = 1.$$

Proof. (Induction on k) We will use the method of induction on odd k and even k separately. Let k be an odd integer. The case for $k = 1$ is clear. That is $\det(P^1_{1+2,1}) = \det(P^1_{1,1}) = -1$. By

using row column reduction, we have

$$(P^1_{3,1}) = \begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & -1 & 0 & 1 \\ 1 & -1 & -1 & 0 \end{pmatrix}_{(4\times4)} \quad C_4 \leftrightarrow C_4 - C_3 \quad \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & -1 & 0 & 1 \\ 1 & -1 & -1 & 1 \end{pmatrix}_{(4\times4)}$$

$$R_4 \leftrightarrow R_4 - R_3 \quad \begin{pmatrix} 2 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}_{(4\times4)} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}_{(2\times2)} = (P^1_{1,1})$$

or,

$$\det(P^1_{3,1}) = \det(P^1_{1,1}) = -1.$$

Now we suppose that it is correct for odd k positive integer. So $\det(P^1_{k+2,1}) = \det(P^1_{k,1}) = -1$. Then we have to show that it is correct for $k+2$ that is

$$\det(P^1_{k+4,1}) = \det(P^1_{k+2,1}) = -1.$$

Again using row column reduction, we have

$$(P^1_{k+4,1}) = \begin{pmatrix} 2 & 1 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 & 1 & 1 \\ 1 & -1 & 0 & 1 & \dots & 1 & 1 & 1 \\ 1 & -1 & -1 & 0 & \dots & 1 & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \\ 1 & -1 & -1 & -1 & \dots & 0 & 1 & 1 \\ 1 & -1 & -1 & -1 & \dots & -1 & 0 & 1 \\ 1 & -1 & -1 & -1 & \dots & -1 & -1 & 0 \end{pmatrix}_{(k+5)\times(k+5)} \quad C_{k+5} \leftrightarrow C_{k+5} - C_{k+4}$$

$$\begin{pmatrix} 2 & 1 & 1 & 1 & \dots & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & \dots & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 & \dots & 1 & 1 & 0 \\ 1 & -1 & -1 & 0 & \dots & 1 & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \\ 1 & -1 & -1 & -1 & \dots & 0 & 1 & 0 \\ 1 & -1 & -1 & -1 & \dots & -1 & 0 & 1 \\ 1 & -1 & -1 & -1 & \dots & -1 & -1 & 1 \end{pmatrix}_{(k+5)\times(k+5)} \quad R_{k+5} \leftrightarrow R_{k+5} - R_{k+4}$$

$$\begin{pmatrix} 2 & 1 & 1 & 1 & \dots & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & \dots & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 & \dots & 1 & 1 & 0 \\ 1 & -1 & -1 & 0 & \dots & 1 & 1 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \\ 1 & -1 & -1 & -1 & \dots & 0 & 1 & 0 \\ 1 & -1 & -1 & -1 & \dots & -1 & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & -1 & 0 \end{pmatrix}_{(k+5)\times(k+5)} = \begin{pmatrix} 2 & 1 & 1 & 1 & \dots & 1 \\ 1 & 0 & 1 & 1 & \dots & 1 \\ 1 & -1 & 0 & 1 & \dots & 1 \\ 1 & -1 & -1 & 0 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \\ 1 & -1 & -1 & -1 & \dots & 0 \end{pmatrix}_{(k+3)\times(k+3)}$$

$$= (P^1_{k+2,1})$$

or,

$$\det(P^1_{k+4,1}) = \det(P^1_{k+2,1}) = -1.$$

Thus, this part of the assertion for all odd positive integers k is to be true. Now let k be an even positive integer. Then the case for $k = 2$ is clear. So $\det(P^1_{4,1}) = \det(P^1_{2,1}) = 2$.

$$(P^1_{4,1}) = \begin{pmatrix} 2 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & -1 & 0 & 1 & 1 \\ 1 & -1 & -1 & 0 & 1 \\ 1 & -1 & -1 & -1 & 0 \end{pmatrix}_{(5\times5)} \quad C_5 \leftrightarrow C_5 - C_4 \quad \begin{pmatrix} 2 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 0 & 1 \\ 1 & -1 & -1 & -1 & 1 \end{pmatrix}_{(5\times5)}$$

$$R_5 \leftrightarrow R_5 - R_4 \quad \begin{pmatrix} 2 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & -1 & 0 & 1 & 0 \\ 1 & -1 & -1 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{pmatrix}_{(5\times5)} = \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & -1 & 0 \end{pmatrix}_{(3\times3)} = (P^1_{2,1})$$

or,

$$\det(P^1_{4,1}) = \det(P^1_{2,1}) = 2.$$

We assume that it is correct for even positive integer k. So $\det(P^1_{k+2,1}) = \det(P^1_{k,1}) = 2$. Now we show that it holds for $k+2$ that is $\det(P^1_{k+4,1}) = \det(P^1_{k+2,1}) = 2$. By proceeding in the same way as for k odd, we get the statement is true for all even positive integer k. Which completes the proof. □

Theorem 4.4. $\det(P^0_{k,i}) = \begin{cases} 1, & if\ k\ odd \\ 2, & if\ k\ even \end{cases}, \forall\ k \geqslant 1\ with\ fixed\ value\ of\ n,\ i = 1.$

Proof. From (4.1),$P^n_{k,i} = (P_{k,k})^n (P_{k,i})^0, n > 0$. For particular case that is for $n,\ i = 1$, we have $P^1_{k,1} = (P_{k,k})^1 (P_{k,1})^0$. Now by operating determinant on both sides

$$\det(P^1_{k,1}) = \det((P_{k,k})^1 (P_{k,1})^0)$$

or,

$$\det(P^1_{k,1}) = \det(P_{k,k})^1\ \det(P_{k,1})^0 = (-1)^{(k+2)}\ \det(P_{k,1})^0$$

As $\det(P^n_{k,i}) = \begin{cases} -1, & if\ k\ odd \\ 2, & if\ k\ even \end{cases}, \forall\ k \geqslant 1\ with\ fixed\ value\ of\ n,\ i = 1$. So it has two cases. For odd k,

$$-1 = (-1)\det(P_{k,1})^0 \tag{4.4}$$

and when k is even,

$$2 = \det(P_{k,1})^0. \tag{4.5}$$

So we have $\det(P^0_{k,i}) = \begin{cases} 1, & if\ k\ odd \\ 2, & if\ k\ even \end{cases}, \forall\ k \geqslant 1\ with\ fixed\ value\ of\ n,\ i = 1$. This completes the proof. □

5 Diffie-Hellman Elliptic Curve Cryptography with generalized Pell P^n_k matrix

In context of our proposed encryption scheme, both encryption and decryption keys are the generalized Pell P^n_k matrices and it's inverse respectively. To develop the keys, the required parameters k and n are exchanged using Diffie-Hellman Elliptic curve cryptography.
Alice wants to send a message to Bob using Diffie-Hellman Elliptic Curve Cryptography. Alice chooses an Elliptic curve $y^2 = x^3 + ux + v$ over the field $\mathbb{Z}_p$. Choose the point G on the elliptic curve. Alice selects a private key 'a' and generates the public key $A = aG$ and Bob selects the private key 'b' and generates the public key $B = bG$, where $a, b \in \{2, 3, \ldots, \#E - 1\}$,(# E= number of points in the elliptic curve).

5.1 Encryption Algorithm

- **Step 1.** Alice selects Bob's public key $B = bG$.
- **Step 2.** Computes $abG = (n, k)$ with her own private key.
- **Step 3.** Now he wants to send the message 'M', obtained by forming the corresponding ASCII characters of the original message to a square matrix of order $(k + 1)$.
- **Step 4.** Alice developed the encryption key (P_k^n), obtained from the generalized Pell $(k,\ i)$-numbers using equation (3.1).
- **Step 5.** Compute $C = {P_k}^n \times M$.
- **Step 6.** Send $[c_{11}, c_{12}, \cdots, c_{1,k+1}, c_{k+1,1}, \cdots, c_{k+1,k+1}]$ to Bob. Which is the encrypted message or ciphertext.

5.2 Decryption Algorithm

- **Step 1.** Bob selects Alice's public key $B = aG$.
- **Step 2.** Computes $baG = (n, k)$, with her own private key.
- **Step 3.** Bob generates the decryption key (P_k^{-n}) which is inverse of generalized Pell P_k^n matrix obtained from equation (3.2), where $-n$ is additive inverse of n in $\mathbb{Z}$.
- **Step 5.** Now Bob computes $M = {P_k}^{-n} \times C$.
- **Step 6.** Which is the original message.

Example

Consider the Elliptic curve

$$y^2 = x^3 + x + 6 \pmod{11}, \tag{5.1}$$

here $u = 1,\ v = 6\ and\ p = 11$. Now the points on the elliptic curve are:
$E = 0,\ (2,4),\ (2,7),\ (3,5),\ (3,6),\ (5,2),\ (5,9), (7,2),\ (7,9),\ (8,3),\ (8,8),\ (10,2),\ (10,9)$.
So $\#E = 13$. A point G chosen from the elliptic curve, let $G = (2,4)$. Alice selects her private key $a = 6$ and Bob selects his private key $b = 8$. Then Alice computes public key $aG = 6(2,4) = (7,2)$ and Bob also generates own public key $bG = 8(2,4) = (3,6)$.

Encryption Algorithm

- **Step 1.** Alice selects Bob's public key $B = bG = (3,6)$.
- **Step 2.** He computes $abG = (n,k) = 6(3,6) = (10,2)$ with the help of her own private key.
- **Step 3.** He wants to send the message $M =$ "$COVAXIN$" to Bob, by using ASCII characters of order $(k + 1) \times (k + 1)$.
- **Step 4.** Then selects P_k^n i.e P_2^{10} as private key.
- **Step 5.** Compute $C = P_k^n \times M = P_2^{10} \times M$

$$= \begin{pmatrix} 2296 & 472 & 1041 \\ 1041 & 214 & 472 \\ 472 & 97 & 214 \end{pmatrix} \times \begin{pmatrix} 67 & 79 & 86 \\ 65 & 88 & 73 \\ 78 & 32 & 32 \end{pmatrix} = \begin{pmatrix} 110 & 104 & 8 \\ 25 & 79 & 60 \\ 93 & 64 & 121 \end{pmatrix} = \begin{pmatrix} n & h & \lhd \\ \downarrow & O & < \\ ] & @ & y \end{pmatrix}.$$

- **Step 6.** Now Alice sends
  110, 104, 8, 25, 79, 60, 93, 64, 121.
  Which is the ciphertext. By converting these numerical values to corresponding ASCII characters the ciphertext becomes

  "$nh\lhd \downarrow O <]@y$".

Decryption Algorithm

To recuperate the plaintext from the ciphertext Bob will follow the procedure:

- **Step 1.** Bob selects Alice's public key $A = aG = (7,2)$.
- **Step 2.** Compute $baG = (n,k) = 8(7,2) = (10,2)$ using his own private key.
- **Step 3.** For $n = 10,\ k = 2$ Bob find the inverse of generalized Pell (k,i)- matrix i.e.$P_k^{-n} = P_2^{-10} = \begin{pmatrix} p_2^2(-7) & p_2^2(-9) & p_2^2(-8) \\ p_2^2(-8) & p_2^2(-10) & p_2^2(-9) \\ p_2^2(-9) & p_2^2(-11) & p_2^2(-10) \end{pmatrix} = \begin{pmatrix} 12 & -31 & 10 \\ 10 & -8 & 31 \\ -31 & 72 & -8 \end{pmatrix}$.
- **Step 4.** Bob computes $M = P_k^{-n} \times C = P_2^{-10} \times C$
$= \begin{pmatrix} 12 & -31 & 10 \\ 10 & -8 & 31 \\ -31 & 72 & -8 \end{pmatrix} \times \begin{pmatrix} 110 & 104 & 8 \\ 25 & 79 & 60 \\ 93 & 64 & 121 \end{pmatrix} = \begin{pmatrix} 67 & 79 & 86 \\ 65 & 88 & 73 \\ 78 & 32 & 32 \end{pmatrix} = \begin{pmatrix} C & O & V \\ A & X & I \\ N & & \end{pmatrix}$.
- **Step 5.** Which is the original message

  "COVAXIN".
- **Step 6.** End of algorithm.

6 Complexity Analysis

Discrete logarithmic problem plays a vital role in Cryptographic protocols and computational number theory. An efficient algorithm for discrete logarithms would make several authentication and key-exchange systems insecure. However the discrete logarithm problem and the Diffie-Hellman problm are hard. For instance , let 64-bits is the most significant bits are used as a secret key for a block cipher. In this case the eavesdropper who cannot compute the Diffie-Hellman function, but can compute the 64 most significant bits can still crack the session. Thus it becomes important to study the security of small substrings of the key. Both Alice and Bob is enable to compute g^{ab} but an adversary, who knows $G,\ g^a\ and\ g^b$ is unable to compute g^{ab}. Basically it is intended that 128 most significant bits key, for a common block cipher, then it should be difficult to compute the Diffie- Hellman function [4], [12].

The problem is intimately connected with the Discrete logarithm problem i.e. if one is able to break DL then he can break DH protocol also. The DL problem is at least as hard as the DH problem. The complexity of the problems is shown to be the lower bounded by $\Omega(\sqrt{p})$, where p is the largest prime divisor of the group order. Also it is hard to compute[4], [5].

ECC is an efficient public key cryptosystem, which has wide range of uses in recent years. It uses short encryption key. ECC is faster and requires less computation power and less time consuming. ECC algorithm is more complex and increases the size of the encrypted message.Due to high complexity of the algorithm, it increases security of the algorithm. Also ECC required short key size as compared to others i.e. only 224 bits where RSA and DSA require 2048 bits. ECC is more secure and fast[4], [8] and [9].

To calculate the time complexity for both the multiplication and inversion of matrix, we use Gauss-Jordan elimination, Strassen algorithm, Coppersmith-winograd algorithm and Optimized CW-like algorithm with time complexity $O(n)^3$, $O(n)^{2.807}$, $O(n)^{2.376}$ and $O(n)^{2.373}$ respectively. Optimized CW-like algorithm is asymptotically the fastest known algorithm to date for both matrix multiplication and inversion with time complexity $O(n)^{2.373}$ with input two $n \times n$ matrices and output one $n \times n$ matrix for multiplication also one $n \times n$ matrix for input, one $n \times n$ matrix as output for inversion. In the context of Brute - force attack the time complexity increases for large number of repetition in multiplication and inversion method. So it is hard to compute the keys of our proposed algorithm. However for Alice and Bob it is quite easy as the keys are nothing but the matrix made by the entries of generalized Pell (k,i)-numbers [2], [3].

7 Conclusion

In this article the inverse of generalized Pell matrix P_k^n has been formulated and a new encryption scheme has been proposed in which both the encryption and decryption keys are P_k^n and P_k^{-n} (inverse of P_k^n) respectively. The parameters n and k are exchanged using Diffie-Hellman

Elliptic Curve key exchange scheme. It is very difficult to recover these parameters by intruder and the calculation of inverse of a matrix enhance the difficulty level to obtain the decryption key. However it is quiet easy to construct the both the encryption and decryption keys for sender and receiver as these may be obtained from the generalized Pell numbers directly.

References

[1] I. F. Blake and T. Garefalakis, *On the complexity of the discrete logarithm and Diffie-Hellman problems*, Journal of Complexity, **20**, 148–170, (2004).

[2] D. Coppersmith and S. Winograd, *On the asymptotic complexity of matrix multiplication*, In Proc. SFCS, 82–90, (1981).

[3] D. Coppersmith and S. Winograd, *Matrix multiplication via arithmetic progressions*, J. Symb. Compu., **9(3)**, 251–280, (1990).

[4] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Trans. Inform. Theory, **22**, 644–654, (1976).

[5] T. Elgamal, *A public key Cryptosystem and a signature scheme based on discrete logarithms*, IEEE transactions on information theory, **31**, 469–472, (1985).

[6] P. A. Grillet, *Abstract algebra*, Springer Science and Business Media, **242**, (2007).

[7] E. Kilic, *The generalized Pell (p, i)-numbers and their Binet formulas. combinatorial representation, sums*, chaos Solitons Fractals, **40**, 2047–2063, (2009).

[8] N. Koblitz, *Elliptic curve cryptosystem*, International Journal of Cryptography, **1**, 139–150, (1989).

[9] N. Koblitz, *Hyper Elliptic cryptosystems*, Mathematics of computation, **48**, 203–209, (1987).

[10] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer.

[11] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, Newyork, NY: John Wiley and Sons, (2001).

[12] U. M. Maurer and S. WolF, *The relationship between breaking the Diffie-Hellman protocol and computing discrete logarithms*, SIAM J.Comput., **28**, 1689–1721, (1999).

[13] K. Prasad and H. Mahato, *Cryptography using generalized Fibonacci matrices with Affine-Hill cipher*, Discrete mathematics and computation, (2020).

[14] B. Ravi Kumar, A. Chandra Sekhar and G. Appala Naidu, *Diffie-Hellman key exchange for self-Encryption over points on the Elliptic Curve Cryptography*, Journal of Information and Computing Science, **12**, 083–087, (2017).

[15] P. Sundarayya and M. G. Vara Prasad, *Coadingtheory on Pell-Lucas P numbers*, Journal of Physics: Conf. Series, **1344**, 012–017, (2019).

[16] S. Ucar, N. Tas and N. Y. Ozgur, *Pell Coding and Decoding Methods with Some Applications*, arXiv:1706.04377vl [math.NT], (2017).

Author information

R. Mohanty, Department of Mathematics, Central University of Jharkhand, India.
E-mail: ritanjalipoonam6@gmail.com

H. Mahato, Department of Mathematics, Central University of Jharkhand, India.
E-mail: hrishikesh.mahato@cuj.ac.in

Received: 2025-01-01
Accepted: 2025-09-24