Chapter- 16

Cryptographic Applications of Pell-Like Equation

Hiba Nasrin P.C, Shaharban T.H, Girish K.P*
Centre for Research in Higher Mathematics, MES Kalladi College,
Mannarkkad,-678583, Kerala, India,
Affiliated to Calicut University
*Corresponding Author : Ph.: 9447524960,
Email id: girikalam@gmail.com

Abstract

This project investigates Pell's Equation and its generalization, the Pell-like Equation, highlighting their roles in cryptography. These equations form the basis for defining L-Groups, which are specialized cryptographic groups used to develop secure protocols such as the Diffie-Hellman key exchange and the ElGamal cryptosystem. By leveraging the mathematical properties of L-Groups, these protocols enable two parties to create a shared secret key or encrypt messages without directly sharing sensitive data, relying instead on the difficulty of the discrete logarithm problem for security. Through structured analysis, the project demonstrates how these cryptographic applications protect data confidentiality and integrity by translating complex mathematical problems into practical security tools. The work illustrates the deep connections between number theory and cryptography, showcasing Pell's Equation as a valuable framework for building secure communication protocols and encouraging further research in mathematically grounded cryptographic methods.

Keywords: Pell-like equations, L-Groups, Diffie-Hellman Key Exchange, Elgamal Cryptosystem

Introduction

This project explores Pell's Equation and its cryptographic applications, highlighting its role as a fundamental problem in number theory with significant uses in secure communications. Pell's Equation,

ISBN: 9789348505767

defined as $X^2 - P.Y^2 = 1$, where P is a square-free positive integer, has intrigued mathematicians since antiquity, including through **Bhaskara's** solution to $X^2 - 61.Y^2 = 1$ and further work by **Wallis** and **Brouncker**. A broader form, the **Pell-Like Equation** $X^2 - P.Y^2 = k$ (with k as any integer), has extended these applications, contributing to cryptographic methods that utilize the equation's properties. The project is structured into key sections: An introduction to Pell's Equation and its properties; a definition of **L-Groups**, cryptographic groups derived from Pell-like equations; and finally, practical applications of LGroups in cryptography, demonstrating how mathematical principles support secure key exchanges and encryption.

Pell's Equation

In number theory, a Diophantine equation is one for which integer solutions are sought (or, sometimes,solutions in rational numbers). Typically, the number of variables is greater than the number of equations, allowing for the possibility of infinitely many solutions. The task of finding these solutions can sometimes be very challenging. A very famous quadratic Diophantine equation is Pell's equation.

Definition

Let P be a positive integer which is not a perfect square. The equation

$$x^2 - Py^2 = 1 \qquad (1)$$

is called Pell's equation.

Definition

A Pell-like equation is a generalization of Pell's equation, taking the form;

$$x^2 - Py^2 = k \qquad (2)$$

where P is a positive integer that is not a perfect square and k is an integer.

Note: Solutions to Pell's equation can be found using continued fraction expansion of $\sqrt{P}$.

ISBN: 9789348505767

Theorem: If p, q is a positive solution of $x^2 - Py^2 = 1$, then $\frac{p}{q}$ is a convergent of the continued fraction expansion of $\sqrt{P}$.

Example

Let $P = 7$, then $x^2 - 7y^2 = 1$

Using the continued fraction expansion of $\sqrt{7}$,we find that $x = 8, y = 3$ satisfies the equation $8^2 - 7.3^2 = 1$

Note:

The fundamental solution of the equation $x^2 - Py^2 = 1$ to be its smallest positive solution.

Theorem: Let x_1, y_1 be the fundamental solution of the equation $x^2 - Py^2 = 1$. Then every positive solution of the equation can be represented as pair of integers (x_n,y_n), where x_n and y_n defined by

$$x_n + y_n\sqrt{p} = (x_1 + y_1\sqrt{p})^n, \qquad n = 1,2,3, \ldots$$

Thus, every positive solution is generated from the powers of the fundamental solution (x_1, y_1)

Example

For $x^2 - 35y^2 = 1$, the fundamental solution is $x = 6, y = 1$. Using this, a second solution is $x_2 = 71, y_2 = 12$, which satisfies $71^2 - 35 \cdot 12^2 = 5041 - 5040 = 1$.

A third positive solution is $x_3 = 846, y_3 = 143$, satisfying $846^2 - 35 \cdot 143^2 = 1$

L-Groups

Let P, q be odd primes and $G = \{(x, y) \in \mathbb{Z}_q^2 : x^2 - Py^2 = k\}$, where $(k/P) = (k/q) = 1$. We can define a binary operation on G as follows. Since $(k/q) = 1$ we know there is $a \in \mathbb{Z}$ such that $a^2 \equiv k \bmod q$. Thus, for $(x,y),(z,w) \in G$, we may define $(x, y) \cdot (z, w) = \left(\frac{xz+Pyw}{a}, \frac{xw+yz}{a}\right)$

Then G is a group under this operation.

Note: The order of group G is

$$|G| = q - \left(\frac{P}{q}\right)$$

ISBN: 9789348505767

Application of L-Groups

The Diffie-Hellman Key Exchange

Symmetric key cryptography relies on a shared secret key for both encryption and decryption, posing a challenge in securely distributing this key between communicating parties. The Diffie-Hellman key exchange protocol addresses this issue by allowing two parties to establish a shared secret key over an insecure channel without directly sharing the key. This is achieved through the use of a public prime number p and a base g, where each party selects a private key, computes a public key, and exchanges these public keys. Both parties can then compute the same shared secret key based on their private key and the other party's public key. The security of this method is grounded in the computational difficulty of the discrete logarithm problem, making it infeasible for an attacker to derive the private keys from the exchanged public information.

Note: Let G be an L-Group and $g \in G$. Choose $x \in \mathbb{N}$ and compute $b = x \cdot g$. Make g and b public. The discrete log problem is the problem of finding x.

Example

Suppose that Alice and Bob want to communicate securely using a symmetric key cryptosystem. To implement the Diffie-Hellman Key exchange they do the following:

1. **Initialization**

Publicly agree on a large prime number q and a generator g of the multiplicative group Z^*_q of integers modulo q.

2. **Key generation**

Alice generates a private key x (a random integer such that $1 \leq x \leq p - 2$)

Bob generates a private key y (a random integer such that $1 \leq y \leq p-2$)

3. **Compute public values**

Alice computes her public value, $u=g^x \bmod q$,Bob computes his public value, $v=g^y \bmod q$

4. **Exchange public values**

Alice sends her public values u to Bob, Bob sends his public values v to Alice.

ISBN: 9789348505767

5. **Compute shared secret**

Alice computes the shared secret $K_a=v^x \bmod q$,Bob computes the shared secret $K_b=u^y \bmod q$.

Example

Let q = 23, g=5

Choose x=6 and y=15

Alice's public value u,

$$u = g^x mod\ q$$
$$= 5^6\ mod\ 23 = 8$$

Bob's public value v,

$$u = g^y mod\ q$$
$$= 5^{15}\ mod\ 23 = 19$$

Alice sends u=8 to Bob and Bob sends v=19 to Alice.

$$K_a = v^x mod\ q$$
$$= 19^6\ mod\ 23 = 2$$
$$K_b = u^y mod\ q$$
$$= 8^5\ mod\ 23 = 2$$

Now, both Alice and Bob share the secret value $K=K_a=K_b=2$, which they can use for further secure communication.

Using L-Group:

We will now implement the Diffie-Hellman key exchange protocol in L-Groups.

1. They agree on a public L-Group, G and $g \in G$.
2. Alice and Bob choose random natural numbers x and y (respectively) and compute
   $u = x \cdot g$, $v = y \cdot g$ (respectively).
3. Alice publicly sends u to Bob and Bob publicly sends v to Alice.
4. Alice then computes $K_a = x \cdot v$ and Bob computes $K_b = y \cdot u$.

Example

Let P = 3, q = 7, and k = 1, $G = \{(x, y) \in \mathbb{Z}_7^2 : x^2 - 3y^2 = 1\}$with the binary operation defined as:

ISBN: 9789348505767

$$(x,y)\cdot(z,w)=\left(\frac{xz+3yw}{a},\frac{xw+yz}{a}\right)$$

where a is such that $a^2 \equiv 1 \bmod 7$.

step 1: Alice and Bob agree on the public group

$$G = \{(1,0),(6,0),(2,1),(5,1),(0,3),(0,4),(2,6),(5,6)\}$$

and the element $g = (2,1)$.

step 2: Alice chooses $x = 4$ and computes: $u = 4 \cdot (2,1)$

Let's compute u:

$$(2,1)\cdot(2,1)=\left(\frac{2\cdot 2+3\cdot 1\cdot 1}{1},\frac{2\cdot 1+2\cdot 1}{1}\right)=\left(\frac{4+3}{1},\frac{2+2}{1}\right)$$

$$=(7,4)\equiv(0,4)\mod 7$$

$$(0,4)\cdot(2,1)=\left(\frac{0\cdot 2+3\cdot 4\cdot 1}{1},\frac{0\cdot 1+4\cdot 2}{1}\right)=\left(\frac{0+12}{1},\frac{0+8}{1}\right)$$

$$=(12,8)\equiv(5,1)\mod 7$$

$$(5,1)\cdot(2,1)=\left(\frac{5\cdot 2+3\cdot 1\cdot 1}{1},\frac{5\cdot 1+1\cdot 2}{1}\right)=\left(\frac{10+3}{1},\frac{5+2}{1}\right)$$

$$=(13,7)\equiv(6,0)\mod 7$$

So, $u = (6,0)$.

Bob chooses $y = 5$ and computes: $y = 5 \cdot (2,1)$

Let's compute v:

$$(2,1)\cdot(2,1)=(0,4)$$

$$(0,4)\cdot(2,1)=(5,1)$$

$$(5,1)\cdot(2,1)=(6,0)$$

$$(6,0)\cdot(2,1)=\left(\frac{6\cdot 2+3\cdot 0\cdot 1}{1},\frac{6\cdot 1+0\cdot 2}{1}\right)=(12,6)\equiv(5,6)\mod 7$$

So, $v = (5,6)$.

step 3: Alice sends $u = (6,0)$ to Bob and Bob sends $v = (5,6)$ to Alice.

step 4: Alice computes:

$K_a = 4 \cdot (5,6)$ Let's compute K_a:

$$(5,6)\cdot(5,6)=\left(\frac{5\cdot 5+3\cdot 6\cdot 6}{1},\frac{5\cdot 6+6\cdot 5}{1}\right)=\left(\frac{25+108}{1},\frac{30+30}{1}\right)$$

$$=(133,60)\equiv(0,4)\pmod 7$$

$$(0,4)\cdot(5,6)=\left(\frac{0\cdot 5+3\cdot 4\cdot 6}{1},\frac{0\cdot 6+4\cdot 5}{1}\right)=\left(\frac{0+72}{1},\frac{0+20}{1}\right)$$

$$=(72,20)\equiv(2,6)\pmod 7$$

ISBN: 9789348505767

$$(2,6)\cdot(5,6) = \left(\frac{2\cdot 5+3\cdot 6\cdot 6}{1}, \frac{2\cdot 6+6\cdot 5}{1}\right) = \left(\frac{10+108}{1}, \frac{12+30}{1}\right)$$

$$= (118,42) \equiv (6,0) \pmod 7$$

Thus, $K_a = (6,0)$.

Bob computes:

$K_b = 5 \cdot (6,0)$ Let's compute K_b:

$$(6,0)\cdot(6,0) = \left(\frac{6\cdot 6+3\cdot 0\cdot 0}{1}, \frac{6\cdot 0+0\cdot 6}{1}\right) = \left(\frac{36+0}{1}, \frac{0+0}{1}\right) = (36,0) \equiv (1,0) \pmod 7$$

$$(1,0)\cdot(6,0) = \left(\frac{1\cdot 6+3\cdot 0\cdot 0}{1}, \frac{1\cdot 0+0\cdot 6}{1}\right) = \left(\frac{6+0}{1}, \frac{0+0}{1}\right) = (6,0) \equiv (6,0) \pmod 7$$

Therefore, both Alice and Bob compute the same shared secret key:

$K_a = K_b = (6,0)$

ElGamal Cryptosystem

ElGamal cryptosystem is a public-key cryptosystem named after its inventor, Taher ElGamal.

The security of an ElGamal system relies on the computational infeasibility of the discrete log problem.

Algorithm:

1. Key generation: Bob uses the following steps to create his public and private key.
   (a) Select a large prime number q.
   (b) Select a generator g of the multiplicative group Z^*_q of integers modulo q.
   (c) Select a private key x,a random integer such that $1 \le x \le p - 2$.
   (d) Compute $b=g^x \bmod q$.
   (e) The public key is (q,g,b).
   Bob encrypts a message m for Alice which Alice decrypts.
2. Encryption: Bob should do the following.
   (a) Obtain Alice's public key (q,g,b).
   (b) Represent the plaintext message m as an integer such that $0 \le m \le p$.
   (c) Select a random integer r such that $1 \le r \le p - 2$.
   (d) Compute $y=g^r \bmod q$.

ISBN: 9789348505767

(e) Compute $e = m \cdot b^r \bmod q$.

(f) The ciphertext is the pair $C=(y,e)$.

3. Decryption: To recover plaintext m from C, Alice should do the following.
   (a) Obtain the shared secret d, $d=y^x \bmod q$.
   (b) Compute the modular inverse of d,denoted as d^{-1}.
   (c) Recover the plaintext message m, $m = e \cdot d^{-1} \bmod q$.

Example

Let q=23, g=5 key generation: choose private key x=6

compute, $b = gx \bmod q$

$= 5^6 \bmod 23 = 8$

public key is $(q, g, b) = (23,5,8)$.

private key is x=6.

Encryption: Let m=15, choose r=3

$$y = g^r \bmod q$$
$$= 5^3 \bmod 23 = 10$$
$$e = m \cdot b^r$$
$$= 15 \cdot 8^3 \bmod 23 = 21$$

Ciphertext is $(y, e) = (10,21)$

Decryption: Shared secret d,$d = y^x \ mod \ q$

$$= 10^6 mod\ 23 = 6$$
$$d^{-1} = 6^{-1} \bmod 23$$

Using the extended Euclidean algorithm,

$$6^{-1} \ mod\ 23 \ = \ 4$$

so, $m = e \cdot d^{-1} = 21 \cdot 4 \bmod 23 = 15$

The decrypted plaintext m=15 matches the original plaintext.

Using L-Group:

We will now implement the ElGamal Cryptosystem protocol in L-Groups. Suppose that Alice wishes to receive a secret message from Bob. She must first create a public key so that Bob can encrypt a message for her:

1. She chooses an L-Group, say G, $g \in G$, and a random $x \in$ N.
2. She then computes $b = g^x$.
3. Her public key is (g,b,G).

ISBN: 9789348505767

4. She also needs to create a private key to be able to decrypt the ciphertext after recieving it. Let x be Alice's private key.

Let m be the message Bob wants to send to Alice. We assume that, through a prescribed standard protocol, m has been converted, by Bob, into

$M \in G$. We call this embedding m in the group, G.

Bob uses Alice's public key to encrypt M as follows:

1. Bob chooses a random $r \in \mathrm{N}$.
2. Bob computes, in G,$y = g^r$,$s = b^r$, and then $e = s \cdot m$.
3. Bob's encrypted message is the pair (y,e).
4. Bob sends (y,e) to Alice.

To decrypt (y,e), Alice does the following:

1. She computes $d = y^x$ and then $C = d^{-1} \cdot e$.
2. She then unembeds C from G to get M.

Example

Let $P = 5$, $q = 11$, and $k = 1$, the group G is defined as: $G = \{(x, y) \in \mathbb{Z}_{11}^2 : x^2 - 5y^2 = 1\}$

and its elements are

$G = \{(1,0),(10,0),(2,4),(9,4),(4,5),(7,5),(4,6),(7,6),(2,7),(9,7)\}$

The operation on G is defined as: $(x,y) \cdot (z,w) = (xz + 5yw, xw + yz)$

***Key Generation**:* Alice chooses $g = (1,0)$ and a random private key $x = 3$.

Alice computes $b = g^x = (1,0)^3 = (1,0)$.

Alice's public key is $(g,b,G) = ((1,0),(1,0),G)$. Alice's private key is $x = 3$.

Encryption: Bob wants to send the message $m = (2,4)$.

Bob chooses a random $r = 2$.

Bob computes $y = g^r = (1,0)^2 = (1,0)$.

Bob computes $s = b^r = (1,0)^2 = (1,0)$.

Bob computes $e = s \cdot m = (1,0) \cdot (2,4) = (2,4)$.

Bob's encrypted message is $(y,e) = ((1,0),(2,4)$.

Decryption: Alice receives $(y,e) = ((1,0),(2,4))$.

Alice computes $d = y^x = (1,0)^3 = (1,0)$.

The inverse of $d = (1,0)$ is $d^{-1} = (1,0)$.

Alice computes $C = d^{-1} \cdot e = (1,0) \cdot (2,4) = (2,4)$.

Alice retrieves the original message (2,4).

ISBN: 9789348505767

Conclusion

This project on Pell's Equation and its applications in cryptography provides a link between mathematical exploration and practical implications. In the context of cryptography, Pell's Equation emerges as a powerful tool for ensuring the confidentiality, integrity, and authenticity of transmitted information. By understanding the principles of Pell's Equation and quadratic irrationalities, cryptographic systems can be fortified to withstand adversarial threats and safeguard sensitive data. This project reveals the importance of mathematics in Designing Secure Communication Protocols. Overall, This Project Serves As A Valuable resource for individuals seeking to deepen their understanding of Pell's Equation and its implications in cryptography. By bridging the gap between theoretical concepts in number theory and practical applications in cryptography, this project offers a new perspective on the intricate relation between mathematics and information security. Through its exploration of Pell's Equation and cryptographic principles, this project paves the way for further research and innovation in the field of secure communication systems.

References

1. Jason Smith. Solvability characterization of Pell-Like equations. BostonUniversity, 2009.
2. Douglas R. Stinson,Maura B. Paterson.Cryptography Theory and Practice,fourth edition, CRC Press, Taylor and Francis Group, 2018.
3. Ravi M. The Role of Group Theory in Modern Cryptography, JETIR, 2023.
4. David M. Burton. Elementary Number Theory,seventh edition, McGrawHill, 2011.
5. Walter Feit. Some Diophantine Equations of the Form $X^2 - PY^2 = Z$, Proceedings of the American Mathematical Society, 2000.
6. A.J. Menezes, P.C. Van Oorshot, S.A. Vanstone. The Handbook of Applied Cryptography. CRC Press, 1996.

ISBN: 9789348505767