Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

Cryptographic Application of Elliptic Curve generated through the formation of Diophantine triples using Hex Numbers and Pronic Numbers

[1] T. Anupreethi , [2]Vinmol. K. Jesudas, [3]Manju Somanath, [4*] V. Sangeetha, [5]J. Kannan and **[6]P. Vijaya Shanthi**

[1] Ph. D. Research Scholar, PG and Research Department of Mathematics, National College (Autonomous, affiliated to Bharathidasan University), Trichy - 620 001, Tamil Nadu, India.

[2] Assistant Professor, Department of Mathematics, Rajagiri School of Engineering and Technology, Kerala. (Research Scholar, PG and Research Department of Mathematics, National College (Autonomous, affiliated to Bharathidasan University), Trichy - 620 001, Tamil Nadu, India.).

[3]Associate Professor, PG and Research Department of Mathematics, National College (Autonomous, affiliated to Bharathidasan University), Trichy - 620 001, Tamil Nadu, India.

[4]Assistant Professor, PG and Research Department of Mathematics, National College (Autonomous, affiliated to Bharathidasan University), Trichy - 620 001, Tamil Nadu, India.

[5]Assistant Professor, Department of Mathematics, Ayya Nadar Janaki Ammal College (Autonomous, affiliated to Madurai Kamaraj University), Sivakasi – 626 124, Tamil Nadu, India.

[6]Assistant Professor, PG and Research Department of Mathematics, A.P.C. Mahalaxmi College for Women (Affiliated to Manonmaniam Sundaranar University), Thoothukudi – 628 002, Tamil Nadu, India.

Email id: (anupreethitamil@gmail.com, vinmolk@rajagiritech.edu.in, manjuajil@yahoo.com,

* prasansangee@gmail.com, jayram.kannan@gmail.com, vijayashanthi26892@gmail.com)

Article History:

Received: 12-11-2024

Revised: 22-12-2024

Accepted: 18-01-2025

Abstract:

A public-key encryption technique akin to RSA can be referred to as elliptic curve cryptography (ECC). While RSA's security relies on huge prime numbers, ECC leverages the mathematical idea of elliptic curves to offer the same level of security with much smaller keys. In this paper, we will discuss elliptic curves and examine their applications in cryptography. A Diophantine pair of Hex numbers and Pronic numbers is extended to a Diophantine triple with appropriate property, that generates the elliptic curve and perform the encryption-decryption process.

Keywords: Elliptic Curve Cryptography, Hex numbers, Pronic numbers, Diophantine triples, Encryption, Decryption.

1. Introduction

ECC is a public-key cryptographic system that utilizes the algebraic structure of elliptic curves over finite fields. Its primary advantage lies in achieving comparable security to traditional systems like RSA but with significantly smaller key sizes, leading to efficiency in computation and storage. The

security of ECC is based on the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP) . Elliptic curve cryptography algorithms entered wide use in 2004 to 2005[1-5].

This research paper delves into the innovative construction of elliptic curves for cryptographic applications by leveraging Diophantine triples derived from specific polynomial sequences, notably Hex [A003215]and Pronic numbers[A002378] [6].This approach is part of a broader exploration into the intersection of number theory and cryptography, aiming to enhance security mechanisms through mathematical rigor.

A Diophantine triple consists of three positive integers (a, b, c) such that the product of any two, increased by one, yields a perfect square:

$$ab + 1 = x^2, bc + 1 = y^2, ca + 1 = z^2$$

These triples can be utilized to construct elliptic curves with specific properties. For instance, research has demonstrated that certain Diophantine triples can induce elliptic curves with high ranks, which are beneficial for cryptographic applications.

The choice of specific elliptic curves, especially those derived from Diophantine triples of Hex and Pronic numbers, can influence the security and efficiency of these cryptographic operations.

Recent researchers work on transforming a Diophantine equation to an elliptic curve and frame the algorithm for encryption-decryption process [7, 8]. As a part of recent research, we form an elliptic curve using Diophantine triples which were extended from a pair of polynomials namely Hex number and Pronic number with suitable property [9-12].

2. Methods

Let $H_N = 3n^2 + 3n + 1$ and $P_N = n^2 + n$ be Hex number and Pronic number respectively, so that $H_N P_N + (n^4 - 2n^3 + n^2 + n + 1)$ is a perfect square,

that is $\alpha^2 = (2n^2 + n + 1)^2$.

Let A_N be any non-zero integer such that it satisfies the following conditions:

$$H_N A_N + (n^4 - 2n^3 + n^2 + n + 1) = \beta^2$$

$$P_N A_N + (n^4 - 2n^3 + n^2 + n + 1) = \gamma^2.$$

By using the linear transformations $\beta = X + H_N y;\ \gamma = X + P_N y$, these equations can be reduced to a Pellian equation $X^2 - H_N P_N y^2 = n^4 - 2n^3 + n^2 + n + 1$,with a basic solution $\big((2n^2 + n + 1), 1\big)$.

Therefore, from the infinite number of solutions to the aforementioned Pell's equation, a Diophantine triple $(H_N, P_N, A_N) = (3n^2 + 3n + 1, n^2 + n, 8n^2 + 6n + 3)$ can be produced. Our goal in this paper is to find Diophantine triples (H_N, P_N, A_N) and to illustrate them. Firstly, let us look at the fundamental formulae: $H_N = 3n^2 + 3n + 1$, $P_N = n^2 + n$ and $A_N = 8n^2 + 6n + 3$. A recurrent pattern emerges as we begin to solve these equations. Going ahead, the idea is that the existence of Diophantine 3-tuples and the characteristics of the elliptic curves associated with them are closely

related. With respect to the Diophantine triple (H_N, P_N, A_N) , let us consider its property $D(n)$.For all non-negative integer numbers Δ , ψ and Γ, there exist the formulas $(H_N A_N + x) = \Delta^2$, $(P_N A_N + x) = \psi^2$, $(H_N P_N + x) = \Gamma^2$.When $\Delta\psi\Gamma = y$,then $(H_N A_N + x)(P_N A_N + x)(H_N P_N + x) = (\Delta\psi\Gamma)^2$ .When we substitute

$H_N = 19$,$P_N = 6$ and $A_N = 47$,which are obtained from the choice $n = 2$, we get an elliptic curve

$$(114 + x)(893 + x)(282 + x) = y^2$$

Simplifying the expression further yields the following:

$$x^3 + 1289x^2 + 385776x + 28708164 = y^2 \text{ …….(1)}$$

Cubic equations for elliptic curves typically take the form of Weierstrass equations, which are expressed as $y^2 + axy + by = x^3 + cx^2 + dx + e$ where a, b, c, d, e are real numbers and x and y take values in the real numbers. We only need to consider equations of the type $y^2 = x^3 + ax + b$. for our purposes. Reducing (1) over E_p for $p = 1289$ yields an elliptic curve in Weierstrass form

$E_p(a, b) = E_{1289}(365,845)$. Therefore,

$$(x^3 + 365x + 845)(mod\ 1289) = y^2(mod\ 1289) \text{ ……..(2)}$$

when congruence is taken modulo 1289. If $(x^3 + ax + b)\ mod\ p$ has repeated factors, then the set $E_p(a, b)$ can be used to define a finite abelian group over $E_p(a, b)$.This can be expressed as follows: $(4a^3 + 27b^2)\ mod\ p \neq 0(mod\ p)$. $4a^3 + 27b^2 \neq 0$ since $a = 365$, $b = 845$ and $p = 1289$.Thus,elliptic curve cryptography can be implemented using equation (2).

3. Algorithm for elliptic curve cryptography

(I) $E_p(a, b) : (x^3 + 365x + 845) = y^2$ is the equation for an elliptic curve, where E_p is an elliptic curve defined over the finite field E_p for a prime p .

(II) Key Generating:

The message will be encrypted by the sender using the recipient's public key and the recipient will use his private key to decrypt it.

(i) Let "M" be the point on the elliptic curve.

(ii) Select "M" as the point from$E_p(a, b)$.

(iii) Choose generator point G in $E_p(a, b)$.

(iv) Select a private key n from the interval $1 \leq n \leq p - 1$ and utilize it to compute

$P_U = n * G$ the public key.

(v) Choose a number k that falls between $1 \leq k \leq p - 1$ at this point .

(III) Encryption:

$C_1$and C_2 are the two cipher texts that will be generated. $C_1 = k * G$,$C_2 = M + k * P_U$. These C_1 and C_2will be given to the recipient.

(IV) Decryption:

The original point that we have sent, point "M", needs to be decrypted using the formula

$M = C_2 - n * C_1$, as it was sent to the recipient.

4. An example demonstrating the encryption and decryption of an elliptic curve:

Examine the following Elliptic curve $E_{1289}(365,845)$: $y^2 = x^3 + 365x + 845$.

(I)A simple text message can be encoded as a point on the elliptic curve $E_{1289}(365,845)$.

We obtain $M = (188,1000) \in E_{1289}(365,845)$ from the solution of (2).This study will use encryption to protect the point (188,1000).

(II) A generator point $G = (8,446) \in E_{1289}(365,845)$ should be selected. Afterwards, choose a private key $n = 5$ that falls between $1 \leq n \leq 1288$ and calculate $P_U = 5 * G$.

The algebraic method for elliptic curves defined over real numbers is corresponding to the addition rules over $E_p(a,b)$.

$$5 * G = 5(8,446)$$
$$= (8,446) + (8,446) + (8,446) + (8,446) + (8,446)$$

When we first compute $5 * G = (1079,185)$, we obtain $P_U = 5 * G = (1079,185)$

(III) For $p = 1289$, take a random number k such that $1 \leq k \leq p - 1$.Select $k = 3$

$$C_1 = k * G$$
$$= (868,435)$$
$$C_2 = M + k * P_U$$
$$= (188,1000) + 3 * (1079,185)$$
$$C_2 = (1110,1232).$$

As a result, the cipher text or encrypted message is (C_1, C_2), where $C_1 = (868,435)$ and $C_2 = (1110,1232)$.

(IV) To obtain the elliptic point, the decryption process is used in accordance with the algorithm, $M = (188,1000)$

$$M = C_2 - n * C_1$$
$$= (1110,1232) - 5 * (868,435)$$
$$= (1110,1232) - (5,305)$$
$$= (1110,1232) + (5, -305(mod\ 1289))$$
$$= (1110,1232) + (5,984)$$
$$M = (188,1000)$$

This verifies the process for generating an elliptic curve for cryptography.

5. Conclusion

In summary, this research paper contributes to the ongoing efforts to explore novel mathematical constructs in the design of secure and efficient cryptographic systems. By harnessing the properties of Diophantine triples and special polynomial sequences, it's possible to develop elliptic curves that offer robust security features for modern cryptographic applications

References

[1] Dickson, L.E.(1952). History of Theory of Numbers, Chelsea Publishing Company, New York.
[2] Miret, J.M., Sadornil, D., and Tena, J.G. (2018). Pairing-Based Cryptography on Elliptic Curves. Math. Comput. Sci. 12, 309-318.
[3] Kannan, J., Manju, S.(2023). Fundamental Perceptions in Contemporary Number Theory, Nova Science Publisher, Inc,Ny,11788 USA.ISBN:979-8-88697-794-3.
[4] Richard Michael Hill,(2020).Introduction to Number Theory, World Scientific, Publishing Company.
[5] Sangeetha, V., Anupreethi, T., and Manju, S.(2023). Construction of special dio-triples. Indian Journal of Science and Technology.16(39),3440-3442.
[6] https://oeis.org
[7] Somanath, M., Das, R., and Bindu, V.A. (2024).Solution of Negative Pell's Equation Using Self Primes, Palestine Journal of mathematics,13(4),1005-1008.
[8] Somanath, M., Kannan, J., and Raja, K.(2019).On a class of solutions for the Hyperbolic Diophantine equation. International journal of Applied Mathematics,32(3),443-449.
[9] Somanath, M., Gopalan, M.A., Sangeetha, V.(2014).Construction of strong and almost strong rational Diophantine quadruples.JP Journal of Algebra, Number Theory and Applications,35(1),35-48.
[10] William Stallings,(2023).Cryptography and Network Security: Principles and Practice, Pearson Education Inc., London, 8th Edition.
[11] Yuhan Yan,(2022).The Overview of Elliptic Curve Cryptography (ECC),Journal of Physics: Conference Series.
[12] https://www.researchgate.net/publication/343211676_High_rank_elliptic_curves_induced_by_rational_Diophantine_triples