INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Cryptographic Application of Elliptic Curve Generated through Centered Hexadecagonal Numbers

V Sangeetha[1]*, T Anupreethi[2], Manju Somanath[3]

1 Assistant Professor, PG and Research Department of Mathematics, National College (Autonomous) (Affiliated to Bharathidasan University), Trichy, 620 001, Tamil Nadu, India
2 Research Scholar, PG and Research Department of Mathematics, National College (Autonomous) (Affiliated to Bharathidasan University), Trichy , 620 001, Tamil Nadu, India
3 Associate Professor and Research Advisor, PG and Research Department of Mathematics, National College (Autonomous) (Affiliated to Bharathidasan University), Trichy, 620 001, Tamil Nadu, India

OPEN ACCESS

Received: 10-04-2024

Accepted: 28-04-2024

Published: 14-05-2024

Citation: Sangeetha V, Anupreethi T, Somanath M (2024) Cryptographic Application of Elliptic Curve Generated through Centered Hexadecagonal Numbers. Indian Journal of Science and Technology 17(20): 2074-2078. https://doi.org/10.17485/IJST/v17i20.1183

* **Corresponding author**.

prasansangee@gmail.com

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Background/Objectives: Elliptic Curve Cryptography (ECC) is a public-key encryption method that is similar to RSA. ECC uses the mathematical concept of elliptic curves to achieve the same level of security with significantly smaller keys, whereas RSA's security depends on large prime numbers. Elliptic curves and their applications in cryptography will be discussed in this paper. The elliptic curve is formed by the extension of a Diophantine pair of Centered Hexadecagonal numbers to a Diophantine triple with property D(8). **Method:** The Diffie–Hellman key exchange, named for Whitfield Diffie and Martin Hellman, was developed by Ralph Merkle and is a mathematical technique for safely transferring cryptographic keys over a public channel. Based on the Diffie–Hellman key exchange, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography. The generation of keys, encryption and decryption are the three main operations of the ElGamal cryptosystem. **Findings:** Given the relative modesty of our objectives, the fundamental algebraic and geometric characteristics of elliptic curves shall be delineated. Then the behaviour of elliptic curves modulo p: ultimately, there is a fairly strong analogy between the structure of the points on an elliptic curve modulo p and the integers modulo *n* will be studied. In the end, elliptic curve ElGamal encryption analogues of Diffie–Hellman key exchange will be created. **Novelty:** Elliptic curves are encountered in a multitude of mathematical contexts and have a varied and fascinating history. Elliptic curves are very significant in number theory and are a focus of much recent work. The earlier research works in Elliptic Curve Cryptography has concentrated on computer algorithms and pairing – based algorithms. In this paper, the concept of polygonal numbers and its extension from Diophantine pair to triples is encountered, thus forming an elliptic curve and perform the encryption-decryption process.

MSC Classification Number: 11D09, 11D99,11T71,11G05.

Keywords: Elliptic curves; Cryptography; Encryption; Decryption; Centered polygonal numbers

1 Introduction

A Centered Hexadecagonal number represents a dot in the center and other dots around it in successive hexadecagonal (16-sided polygon) layers. A set of positive integers $(a_1, a_2, \ldots a_m)$ is said to have the property $D(\lambda)$, $\lambda \in Z - \{0\}$ if $a_i a_j + \lambda$ is a perfect square for all $1 \leq i < j \leq m$ and such a set is called a Diophantine m-tuple with property D(λ) [1,2].

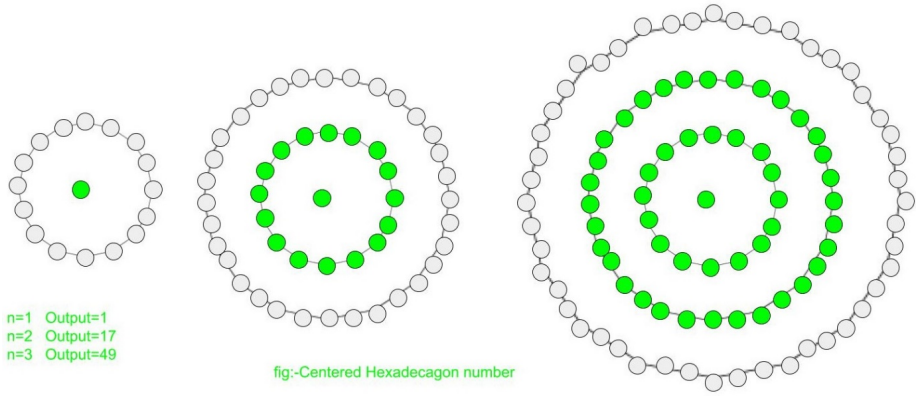

Fig 1. Centered Hexadecagon

Elliptic curves have been studied using components from most of the major fields of Mathematics, including topology, algebra, geometry, analysis, number theory and even logic. Elliptic curves can be found in the proofs of numerous complex Mathematical concepts. Andrew Wiles used them to prove Fermat's Last Theorem, for instance. Additionally, they find applications in integer factorization and elliptic curve cryptography (ECC). An elliptic curve is defined as a smooth, projective, algebraic curve of genus one with a given point O on it in Mathematics. Points in K2, which is the Cartesian product of K and itself, are described by an elliptic curve that is defined over a field K. The curve can be characterized as a plane algebraic curve consisting of solutions (x, y) for the equation $y^3 = ax + by$ for certain coefficients a and b in K, if the field's characteristic differs between 2 and 3. It is necessary for the curve to not be solitary, meaning that it cannot have any cusps or self-intersections. (This is the same as $4a^3 + 27b^2 \neq 0$, which means that x is square-free). It is widely accepted that the curve actually exists in the projective plane, and that the unique point at infinity is point O. According to several definitions, an elliptic curve is just a curve that has this kind of equation. [3,4]

One of the first public-key protocols, the Diffie–Hellman key exchange was devised by Ralph Merkle and named after Whitfield Diffie and Martin Hellman. It is a mathematical technique for safely transferring cryptographic keys over a public channel [5]. One of the first useful instances of public key exchange in cryptography was distributed hashing (DH). The concept of a private key and matching public key was first introduced in a study that was published in 1976 by Diffie and Hellman. Based on the Diffie–Hellman key exchange, the ElGamal encryption system is an asymmetric key encryption algorithm for public-key cryptography. ElGamal encryption is present in several cryptosystems, including the latest iterations of PGP and the free GNU Privacy Guard program. ElGamal encryption should not be confused with the Digital

Signature Algorithm (DSA), which is a variation of the ElGamal signature technique. ElGamal encryption can be defined over any cyclic group G, such as the multiplicative group of integers modulo n. The degree of complexity of a particular discrete logarithm computation task in G determines the security of the system [6,7].

2 Methodology

Consider Centered hexadecagonal numbers $\alpha = 8n^2 + 8n + 1$ and $\beta = 8n^2 + 24n + 17$ of rank n and $n+1$ respectively such that $\alpha\beta + 8$ is a perfect square, say $\gamma^2 = \left(8n^2 + 16n + 5\right)^2$.

Let μ be any non-zero integer such that the conditions $\alpha\mu + 8 = A^2$, $\beta\mu + 8 = B^2$ are satisfied. These equations can be reduced to a Pellian equation $X^2 - \alpha\beta y^2 = 8$ with basic solution $\left(\left(8n^2 + 16n + 5\right), 1\right)$ by applying the linear transformations $A = X + \alpha y, B = X + \beta y$.

Thus, a Diophantine triple $(\alpha, \beta, \mu) = \left(8n^2 + 8n + 1, 8n^2 + 24n + 17, 32n^2 + 64n + 28\right)$ can be generated from the infinite number of solutions of the above mentioned Pell's equation.

This study focuses on finding diophantine triples (α, β, μ) and its depiction. To start with, consider the basic equations, $\alpha = 8n^2 + 8n + 1, \beta = 8n^2 + 24n + 17$ and $\mu = 32n^2 + 64n + 28$. Obtaining solutions of these equations, a recurring pattern develops. Moving forward, the hypothesis is that the properties of the elliptic curves associated with diophantine 3-tuples are intimately related to the problem of their existence. Consider the rational Diophantine triple (α, β, μ), which has property $D(x)$. This indicates that $(\alpha\mu + x) = \Delta^2$, $(\beta\mu + x) = \Psi^2$ and $(\alpha\beta + x) = \Gamma^2$ exists for all non-negative rational numbers Δ, Ψ, and Γ.

Then $(\alpha\mu + x)(\beta\mu + x)(\alpha\beta + x) = (\Delta\Psi\Gamma)^2$, where $(\Delta\Psi\Gamma) = y$.

The choice $n = 1$, gives $\alpha = 17$, $\beta = 49$ and $\mu = 124$, when substituted gives us an elliptic curve,

$$(833 + x)(2108 + x)(6076 + x) = y^2$$

On simplification, the above expression takes the form

$$x^3 + 9017x^2 + 19625480x + 10669237264 = y^2 \tag{1}$$

In general, cubic equations for elliptic curves assumes the form known as Weierstrass equations $y^2 + axy + by = x^3 + cx^2 + dx + e$ where a, b, c, d, e are real numbers and x and y take as values in the real numbers. For the purpose of researchers, it is sufficient to restrict to equations of the form $y^2 = x^3 + ax + b$.

Thus, an elliptic curve in Weierstrass form $E_p(a, b) = E_{127}(43, 30)$ is obtained by reducing Equation (1) over E_p for $p = 127$. Hence, on taking congruence modulo 127,

$$\left(x^3 + 43x + 30\right)(mod\ 127) = y^2\,(mod\ 127) \tag{2}$$

A finite abelian group over $E_p(a, b)$ can be defined based on the set $E_p(a, b)$ provided $\left(x^3 + ax + b\right)\ mod\ p$ has repeated factors. This is equivalent to the condition $\left(4a^3 + 27b^2\right)\ mod\ p \neq 0\,(mod\ p)$. Therefore, $a = 43, b = 30$ and $p = 127, 4a^3 + 27b^2 \neq 0$. Hence, Equation (2) can be used for elliptic curve cryptography.

3 Results and Discussion

- **Elliptic curve cryptography-Algorithm**

(I). The equation for an elliptic curve is given by $E_p(a, b) : \left(x^3 + 43x + 30\right) = y^2$, where E_p represents an elliptic curve defined over the finite field E_p for a prime p.

(II). Key Generation:

Using the recipient's public key, the sender will encrypt the message, which the recipient will then decrypt using his private key.

(i). Pick a point "M" from $E_p(a, b)$.

(ii). Let "M" be the elliptic curve's point.

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

(iv). Choose a private key n from the range $1 \leq n \leq p - 1$ and use it to calculate the public key $P_U = n * G$.

(v). Now select a number k within the range of $1 \leq k \leq p - 1$.

(III). Encryption:

There will be two cipher texts produced, denoted as C_1 and C_2.

$C_1 = k * G$,$C_2 = M + k * P_U$ The recipient will receive these C_1 and C_2.

(IV). Decryption:

The point "M", which was sent to the recipient, needs to be decrypted using the formula $M = C_2 - n * C_1$, is the original point that has been sent.

- **Illustrative example for the Elliptic curve encryption/decryption**

Consider the Elliptic curve $E_{127}(43,30) : y^2 = x^3 + 43x + 30$.

(I). Encode a plain text message as a point on the elliptic curve $E_{127}(43,30)$. From the solution of Equation (2), it is obtained that $M = (1,70) \in E_{127}(43,30)$. The point (1,70) will be encrypted in this research.

(II). Choose a generator point $G = (93,44) \in E_{127}(43,30)$. Then select a private key n=7 which is selected from the range $1 \leq n \leq 126$ and compute $P_U = 7 * G$.

The rules for addition over $E_p(a,b)$ correspond to the algebraic technique described for elliptic curves defined over real numbers.

$7 * G = 7(93,44)$

$= (93,44) + (93,44) + (93,44) + (93,44) + (93,44) + (93,44) + (93,44)$

Initially it has been calculated $7 * G = (8,88)$and have $P_U = 7 * G = (8,88)$.

(III). Consider a random number k such that $1 \leq k \leq p-1$,, for p=127. Choose $k = 3$.

$C_1 = k * G$

$= 3 * (93,44)$

$= (67,12)$

$C_2 = M + k * P_U$

$= (1,70) + 3 * (8,88)$

$= (1,70) + (81,86)$

$C_2 = (106,36)$.

Thus, the encrypted message or cipher text is $(C_1,\ C_2)$ where $C_1 = (67,12)$ and $C_2 = (106,\ 36)$.

(IV). The process of decryption is employed as per the algorithm to acquire the elliptic point

$M = (1,70)$.

$M = C_2 - n * C_1$

$= (106,36) - 7 * (67,12)$

$= (106,36) - (81,86)$

$= (106,36) + (81, -86\,(mod\ 127))$

$= (106,36) + (81,41)$

$M = (1,70)$

This confirms designing an elliptic curve for cryptography.

4 Conclusion

Research on the formation of triples and quadruples using a variety of features and relations has proven quite interesting. For Gaussian integers and other rational and irrational numbers, triples and quadruples can be produced. The particular dio-triples involving Centered Polygonal numbers are built in this study. This concept is incorporated with Elliptic curve cryptography and perform the encryption decryption process. Several methods of ECC can be implemented and execute the cryptosystem for the same.

References

1) Somanath M, Kannan J, Shanthi PV, and MM. Contemporary Research Trends in Mathematics. 1st ed. Multi Spectrum Publications. 2023. Available from: https://www.researchgate.net/publication/371904519_CONTEMPORARY_RESEARCH_TRENDS_IN_MATHEMATICS.
2) Sangeetha V, Anupreethi T, Somanath M. Construction of Special dio — triples. *Indian Journal Of Science And Technology*. 2023;16(39):3440–3442. Available from: https://dx.doi.org/10.17485/ijst/v16i39.1735.
3) Yan Y. The Overview of Elliptic Curve Cryptography (ECC). In: The International Conference on Computing Innovation and Applied Physics (CONF-CIAP 2022);vol. 2386 of Journal of Physics: Conference Series. IOP Publishing. 2022;p. 1–8. Available from: https://dx.doi.org/10.1088/1742-6596/2386/1/012019.
4) Stallings W. Cryptography and Network Security: Principles and Practice. 8th ed. London. Pearson Education Inc. 2023. Available from: https://www.cs.vsb.cz/ochodkova/courses/kpb/cryptography-and-network-security_-principles-and-practice-7th-global-edition.pdf.
5) Somanath M, Kannan J, Raja K. Encryption Decryption Algorithm Using Solutions of Pell equation. *Int J Math And Appl*. 2022;10(1):1–8.

6) Miret JM, Sadornil D, Tena JG. Pairing-Based Cryptography on Elliptic Curves. *Mathematics in Computer Science*. 2018;12(3):309–318. Available from: https://dx.doi.org/10.1007/s11786-018-0347-3.
7) Ullah S, Zheng J, Din N, Hussain MT, Ullah F, Yousaf M. Elliptic Curve Cryptography; Applications, challenges, recent advances, and future trends: A comprehensive survey. *Computer Science Review*. 2023;47. Available from: https://dx.doi.org/10.1016/j.cosrev.2022.100530.