ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Cyclic groups of Elliptic curves-An Implementation to Cryptography

A.Chandra Sekhar*
Professor, Department of Mathematics
GIT,Gitam University, Visakhapatnam, India
acs@gitam.edu

G.Sivanagamalleswar Rao
Research Scholar, Department of Applied Mathematics
GIS,Gitam University, Visakhapatnam, India
gsiva357@gmail.com

G,Naga Lakshmi
Assistant Professor, Department of Mathematics
GIT,Gitam University, Visakhapatnam, India
nagalakshmi_g@gmail.com

B.Ravi Kumar
Assistant Professor, Department of Mathematics
GIT,Gitam University, Visakhapatnam, India
Ravikumarbrk6@gmail.com

Abstract: Cryptography is the process of sending the messages in unknown form so that the receiving party can remove the unknown part of the message and can read the original message. The study of cryptography extended to new concepts and techniques basically from the applications of Number theory.[2],[4], Up until the mid 1970's the study of the arithmetical properties of algebraic curves has been one of the most exciting areas of mathematical research. Among such curves one is an Elliptic curve. An elliptic curve over real numbers consists of the points which form a group together with a special point O called the point at infinity is the identity element in that group. Elliptic curve groups are additive groups; that is, their basic function is addition. In this paper we proved that these groups are cyclic groups and a cryptosystem is implemented.

Keywords: Groups, cyclic Groups, Generators.

I. INTRODUCTION

An elliptic curve over real numbers may be defined as the set of points (x, y) which satisfy an elliptic curve equation of the form: $y^2 = x^3 + ax + b$, where x, y, a and b are real numbers. Each choice of the numbers a and b yields a different elliptic curve. For example, a = 3 and b = 8 give the elliptic curve Example-2: Observed that (4, 7) a point on the elliptic curve $y^2 = x^3 - 5x + 5$ over real numbers?
Yes, since the equation holds true for =4andy=7:
$(7)^2 = (4)^3-5(4)+5$
49=64-20+5
49 = 49

A. Adding two distinct points P and Q:

Suppose that P and Q are two distinct points on an elliptic curve, and the P is not -Q. To add the points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve in exactly one more point, call -R. The point -R is reflected in the x-axis to the point R. The law for addition in an elliptic curve group is P + Q = R. Adding distinct points P and Q.

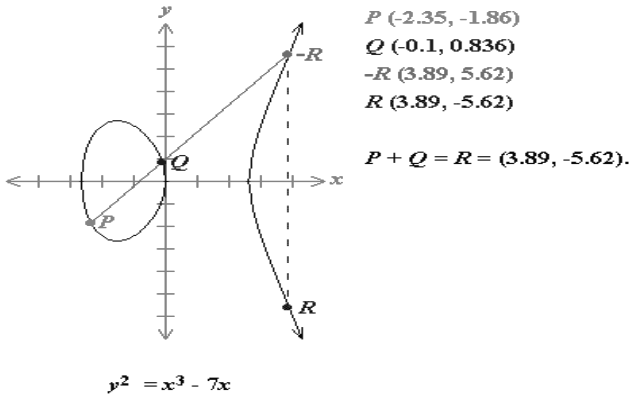

Figure – 1.1 adding two points

When $P = (x_p,y_p)$ and $Q = (x_q,y_q)$ are not negative of each other, $P + Q = R$ where $R = (x_r,y_r)$ and $s = (y_p - y_q) / (x_p - x_q)$. Then $x_r = s^2 - x_p - x_q$ and $y_r = -y_p + s(x_p - x_r)$.
If $x^3 + ax + b$ contains no repeated factors, or equivalently if $4a^3 + 27b^2$ is not 0, then the elliptic curve $y^2 = x^3 + ax + b$ is called non singular otherwise singular and the points on the elliptic curve forms an abelian group under the operation addition.
Example-1: The elliptic curve equation $y^2 = x^3 - 7x - 6$ over real numbers form a group.[12]
Since $4a^3+ 27b^2= 4(-7)^3+ 27(-6)^2= -400$.

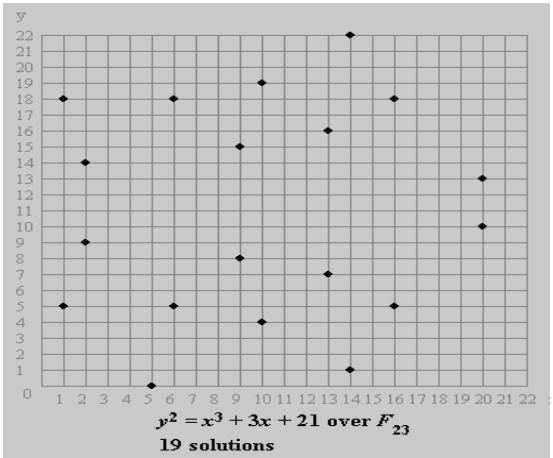

Figure - 1.4.Points on the Elliptic Curve

The elliptic curve $y^2 = x^3 + 3x + 21$ has 19 solutions .The set of points=(1,5),(1,18),(2,9),(2,14),(5,0),(6,5),(6,18),(9,8),(9,15),(10,1),(10,19),(13,7),(13,16),(14,1),(14,22),(16,5),(16,18),(20,10),(20,13).

© 2010, IJARCS All Rights Reserved

We observe that exactly 10 points below at y = 10 and 10 points above i.e., symmetric about y = 10. Also $4(3)^3 + 27(21)^2 \neq 0 \bmod 23$ and hence the elliptic curve is nonsingular and does not have a repeated root. Therefore the points on the elliptic curve form a group under addition. As the value of the prime increases the number of points also increases. Selection of largest prime plays critical role in cryptography. Other concepts in group theory like subgroups, cosets and normal subgroups holds well in these groups.

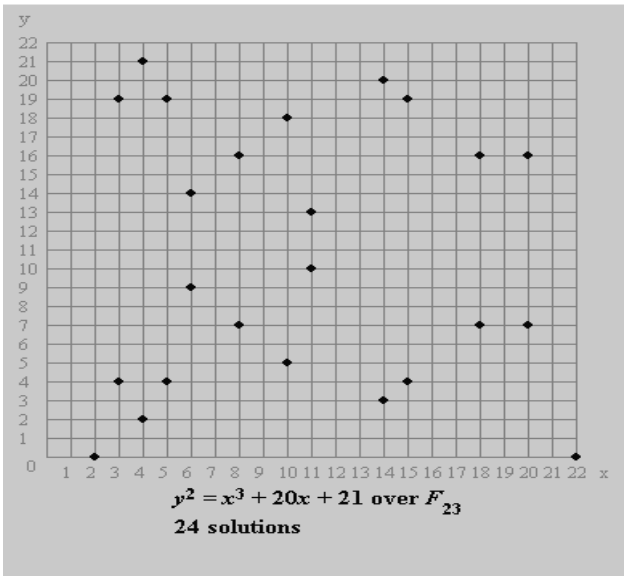

Figure - 1.5.Points on the Elliptic Curve

Consider the Elliptic curve $y^2 = x^3 + 20x + 21$ and p = 23.

By trial and error one root of right hand side equation is -1.By synthetic division the resultant equation is $x^2 - x + 21$.Clearly-1 ≡ 22 mod23 and 21≡21 mod23.Therefore the resultant polynomial is $x^2 + 22x + 21$ and whose roots are -1,-21 and hence $x^3 + 20x + 21 = (x+1)^2(x+21)$.Also observe that$(x+1)^2(x+21) = x^3 + 23x^2 + 43x + 21$---------- (1)

Clearly 1 ≡ 1 mod23,23 ≡ 23 mod23,43 ≡ 20 mod23 and hence (1) is same as $x^3 + 20x + 21$.Because x = -1 is a repeated root of $x^3 + 20x + 21$ the points on the elliptic curve does not form a group because the closure property is not satisfied

II. PROPOSED WORK

A group G under an operation * is called a cyclic group if $G = \{a^n : n \in Z\} = \langle a \rangle$ where a is the generator of the cyclic group. If * is multiplication then $\langle a \rangle = \{a^n : n \in Z\}$ and if * is addition then $\langle a \rangle = \{na : n \in Z\}$

Example: G={1,-1,i,-i} is a cyclic group under multiplication with i,-i as generators . Also Z is an infinite cyclic group with -1,1 as generators. In particular O(G)=n then the number generators of cyclic group is $\phi(n)$,where $\phi(n)$ is the Euler totient function ,defined as the number of positive integers less than n and relatively prime to n and O(G) is the order of G i.e., the number of elements in the group .In particular if the number of points in the cyclic group is a prime then every element in the cyclic group is a generator[1].

Lemma: If G is the additive group of an Elliptic curve E: $y^2=x^3+ax+b$ then G is cyclic group.

Proof: Let G = {(x,y) : (x,y) ∈E} be a finite group of an Elliptic curve E. With the point O at infinity as the identity. Such that O(G) = n. Now we prove that ∃ an element (x,y) ∈ G such that O(x,y) = n.

Suppose there is no element (x,y) ∈G such that n(x,y)≠ 0 then the number of points in G will be infinity. This contradicts the fact that G is finite ∴ There must exist at least one point (x,y) ∈G such that n(x,y) = 0. Therefore G must be cyclic.

Example: The Elliptic curve $y^2=x^3+5x+4$ over F_{23} has 19solutions Let G={O,(0,2),(0,21),(3,0),(5,4),(5,19), (8,2),(8,21),(13,19),(13,14),(14,9),(14,14),(15,2), (15,21), (19,9),(19,14),(20,10),(20,13),(21,3),(21,20)}

Clearly G is a cyclic group with P = (8, 2) is a generator. Because 1P=P,2P=(19,14),3P=(20,10),4P=(21,20), 5P= (0,2),6P=(15,21),7P=(13,14), 8P=(5,19), 9P=(14,9), 10P=(3,0),11P=(14,14),12P=(5,4),13P=(13,9),14P=(15,2), 15P=(0,21), 16P=(21,3), 17P=(20,13), 18P=(19,9), 19P=(8,21).

Now since O(G)=20 it follows that $\phi(20)=8$ where . Therefore there are 8 generators for this cyclic group. The other generators are (8,2),(8,21), (13,9), (13,14), (14,9), (14,14), (20,10), (20,13).

Implementation to Cryptography: Consider the Elliptic curve $E_{23}(5,4)$ over GF(23).[3],[5]

Encryption: Sender and receiver agree on the Elliptic curve. (E, e_1, e_2) ,.

where receiver selects e_1= (8,21) a generator of the cyclic group & d=4

calculates $e_2 = d \times e_1$= (21,3).

Sender wants to select the plain text P = (8, 2) to receiver. Sender selects r=3 as secret key.

In the encryption process [10], it is observed that e_1 must be a generator otherwise the process does not exist.

Sender calculate the point $C_1 = r \times e_1$ = (20, 13)

and also calculate

the point $C_2 = P + r \times e_2$ =(14,9).

The receiver receives C_1 and C_2.

Decryption:

Receiver calculates $P = C_2 - (d \times C_1)$

= (14, 9) – (5, 19)

= (14, 9) + (5, 4) where (5, 4) is the additive inverse of (5, 19).

Therefore P = (8, 2) as required.

III. CONCLUSIONS

The benefit of public key encryption is that if a system is reversible, meaning that decryption can be performed before encryption It is proved that the points on the Elliptic curve which form a group also forms a cyclic group and a cryptographic scheme is presented. Advantages of elliptic curve cryptography over standard public key cryptography: Known theoretical attacks much less effective, so requires much shorter keys for the same security, leading to reduced bandwidth and greater efficiency and lesser in cost.

However, the main disadvantage of elliptic curve cryptography is the algorithms are more complex, so it's harder to implement them correctly. In the recent research work Selection of large prime playing a major role in addition to this selection of generator also contribute a high level security.

© 2010, IJARCS All Rights Reserved

IV. REFERENCES

[1]. Guide to Elliptic Curve Cryptography-springer.

[2]. W. Diffie and M. E. Hellman. "New directions in cryptography. IEEE Transactions on Information Theory", 22 ,644-654,1976.

[3]. T. ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In Advances in Cryptology (CRYPTO 1984), Springer LNCS 196, 10–18, 1985.

[4]. N.Koblitz.. An elliptic curve implementation of the finite field digital signature algorithm. In Advances in Cryptology (CRYPTO 1998), Springer LNCS 1462, 327–337, 1998.

[5]. N. Koblitz. Elliptic Curve Cryptosystems. Mathematics of Computation, 48, 203–209, 1987.

[6]. N. Koblitz. Hyperelliptic Cryptosystems. In J. of Cryptology, 1, 139–150,1989.

[7]. A. J. Menezes, T. Okamoto and S. A. Vanstone. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions in Information Theory, 39, 1639–1646, 1993.

[8]. V. Miller. Uses of Elliptic Curves in Cryptography. In Advances in Cryptology (CRYPTO 1985), Springer LNCS 218, 417–426, 1985

[9]. A. M. Odlyzko. Discrete logarithms in finite fields and their cryptographic significance. In Advances in Cryptology (EUROCRYPT 1984), Springer LNCS 209, 224–314, 1985.

[10]. Qizhi Qiu and Qianxing Xiong Research on Elliptic Curve Cryptography The 8th International Conference on Computer Supported Cooperative Work in Design Proceedings ,698-701,2005

[11]. A text book of Cryptography and Network Security by Behrouz A. Forouzan.

[12]. http://www.certicom.com/index.php/ecc-tutorial

© 2010, IJARCS All Rights Reserved