RESEARCH PAPER | Mathematics | Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

Elliptic Curve Cryptosystems

KEYWORDS: Cryptography, RSA, Elliptic Curve.

S.Vasundhara
Asst Prof of Mathematics, GNITS Shaikpet hyderabad-500008

Dr.K.V.Durgaprasad
Professor of Mathematics(Rtd), osmania University, Hyderabad.

ABSTRACT *This paper deals with an implementation of Elliptic Curve Cryptosystem. Cryptography (or cryptology) from Greek word kryptos, "hidden, secret"; and graph, "writing" is the practice and study of hiding information. Modern cryptography intersects the disciplines of mathematics, computer science, and engineering. Applications of cryptography include ATM cards, computer passwords, RFID and electronic commerce. Cryptology is prior to the modern age was almost synonymous with encryption, the conversion of information from a readable state to nonsense. The sender retained the ability to decrypt the information and therefore avoid unwanted persons being able to read it. The secret key cryptography and public key cryptography are the two main types of cryptography. RSA is the most prominent algorithm used in public key cryptography techniques for encryption and digital signatures. Over the years, the key lengths for RSA have been increasing. This puts considerable burden on RSA. Another public key cryptography technique is gaining popularity in the last few years. It is called as Elliptic Curve Cryptography (ECC). The main difference between RSA and Elliptic Curve Cryptography is that unlike RSA, Elliptic Curve Cryptography offers the same level of security for smaller key sizes. Elliptic Curve Cryptography is highly mathematical in nature. While conventional public-key cryptosystems (RSA, Diffie - Hellman and DSA) operate directly on large integers, an Elliptic Curve Cryptography operates over points on an elliptic curve.*

Introduction:

Since a lot of sensitive data such as credit card numbers and social security numbers are transmitted over the Internet during transactions. Securing electronic transaction becomes a very important issue. An efficient way to protect and secure the information is by using cryptography which can be used to provide and assure confidentiality and integrity of the transactions (Mackenzie, et al. 1996). The history of cryptography is long and interesting. It had a very considerable turning point when two researchers from Stanford, Whitfield Diffie and Martin Hellman, published the paper "New Directions in Cryptography" in 1976. They preface the new idea of public key cryptography in the paper.

Public-key cryptography and symmetric-key cryptography are two main categories of cryptography. The Well-known public-key cryptography algorithms are RSA (Rivest, et al. 1978), El-Gamal and Elliptic Curve Cryptography. Presently, there are only three problems of public key cryptosystems that are considered to be both secure and effective (Certicom, 2001). Table 1.1 shows these mathematical problems and the cryptosystems that rely on such problems.

	Mathematical problem	Detail	Cryptosystem
1	Integer Factorization problem (IFP)	Given an integer n find its prime factorization	RSA
2	Discrete Logarithm problem(DLS)	Given integer g and h find x' such that =g^{x}mod n	Diffie-Hellman(DH)
3	Elliptic curve discrete logarithmic problem(ECDLP)	Given points P and Q on the curve find 'x' such that Q=xP	Diffie-Hellman(DH)

Providing an equivalent level of security with smaller key size is an advantage of ECC compared to RSA. It is very efficient to implement ECC.ECC obtains lower power consumption, and faster computation. It also gains small memory and bandwidth because of its key size length (Dormale, Bulens and Quisquater 2004), (Huang 2007). Such attributes are mainly fascinating in security applications in which calculative power and integrated circuit space are limited. Wireless devices and smart cards present a good example for the constrained devices with limited resources. Cryptography companies such as Certicom Corporation have already implemented ECC in their products for some commercial purposes which are RFID and Zigbee.

TABLE:2.2 ECC and RSA Key Comparison.

ECC Key Size	RSA Key Size	Key-Size Ratio	AES Key Size
163	1,024	1:6	n/a
256	3,072	1:12	128
384	7,680	1:20	192
512	15,360	1:30	256
Key sizes in bits.		Source: Certicom, NIST	

II. Elliptic Curve Cryptography: The use of elliptic curves in cryptography was first proposed by Neil Koblitz [16]and Victor Miller [20] in 1985. Koblitz and Miller did not invent a new cryptographic algorithm but they implemented certain existing algorithms using elliptic curve arithmetic. Since its founding elliptic curve cryptography has been studied a lot in the academic world. The use of elliptic curves in cryptography is very inviting because shorter key lengths can be used than in the case of conventional cryptography e.g. RSA. Elliptic curves have been studied by mathematicians for more than a century. An extremely rich theory has been developed around them, and in turn they have been the basis of numerous new developments in mathematics. As far as cryptography is concerned, elliptic curves have been used for factoring and primality proving. The idea of using elliptic curves for public-key cryptosystems is due to Victor Miller [Miller85] and Neal Koblitz [Koblitz87] in the mid-eighties. As with all cryptosystems, and especially with public-key cryptosystems, it takes years of public evaluation before a reasonable level of confidence in a new system is established. The elliptic curve public-key cryptosystems (ECPKCs) seem to have reached that level now. In the last couple of years, the first commercial applications have appeared(email security, web security, smart cards, etc.). Before we look at how the ECPKC s work, we will give a short introduction to elliptic curves

Definition of elliptic curves: Elliptic curves are not ellipses. They are called this because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse. In general, an elliptic curve is the set of solutions of an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_5 \quad \ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

Where the coefficients ai are elements of some field (R, Z or Zp) which satisfy some Simple conditions in order to avoid singularities. Such an equation is said to be Cubic,or of degree 3, because the highest exponent it contains is 3. The Eq.1 is Called Weierstrass equation. Also included in the definition of any elliptic curve is a single element denoted O and called point of infinity or the zero point .

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 =1 and b =1 gives the elliptic curve with equation $y^2 = x^3 + x + 1$; the graph of this curve is shown below: If $x^3 + ax + b$ contains no repeated factors, or equivalently if $4a^3 + 27b^2$ is not 0, then the elliptic curve $y^2 = x^3 + ax + b$ can be used to form a group. An elliptic curve group over real numbers consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity. Elliptic Curve (y2 = x3+x +1)represents the elliptiuc curve over real numbers With a=1 and b=1 with the condition that $4a^3 + 27b^2$ is not 0.The figure is given below.

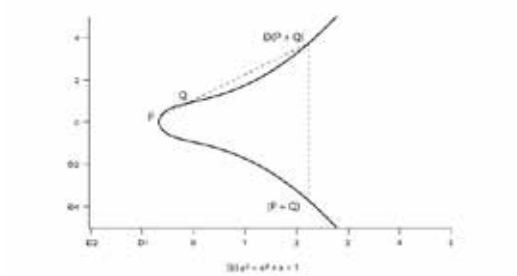
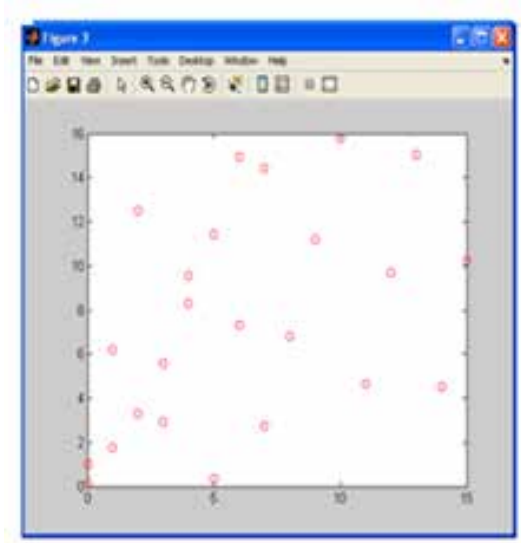


Figure 1

Elliptic curves over Finite fields F_p :
All elliptic curve operations mentioned earlier are based on real numbers. However, operations over the real numbers are inaccurate and slow, whereas cryptographic operations need to be accurate and fast. Therefore, the curve cryptography can be defined over finite fields to operate EC efficiently and accurately. A finite field is a set of a finite number of elements. Cryptographic applications require fast and precise arithmetic; thus elliptic curve groups over the finite fields of F_p and F_2m are used in practice. Recall that the field Fp uses the numbers from 0 to p – 1

$y^2=x^3+ax+b$ with finite field over mod 23. Figure 2



Elliptic curves over binary field over 2^n:
The rules for arithmetic in F_2m can be defined by either polynomial representation or by optimal normal basis representation. Since F_2m operates on bit strings, computers can perform arithmetic in this field very efficiently. An elliptic curve with the underlying field F_2^m is formed by choosing the elements a and b within F_2m (the only condition is that b is not 0). As a result of the field F_2m having a characteristic 2, the elliptic curve equation is slightly adjusted for binary representation

$y^2 + xy = x^3 + ax^2 + b$

The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation over F_2m (where x and y are elements of F_2m). An elliptic curve group over F_2m consists of the points on

the corresponding elliptic curve, together with a point at infinity, O. There are finitely many points on such an elliptic curve.

Example of Elliptic curve over F_2^n:
As a very small example, consider the field F_24, defined by using polynomial representation with the irreducible polynomial $f(x) = x^4 + x + 1$.

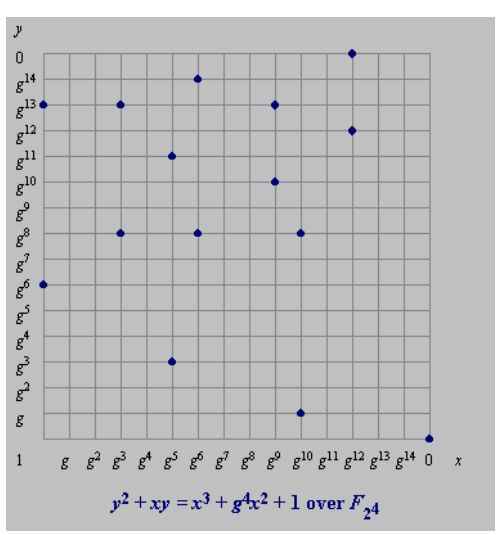
The element g = (0010) is a generator for the field . The powers of g are:

g^0=(0001)g^1=(0010)g^2=(0100)g^3=(1000)g^4=(0011)g^5=(0110)
g^6=(1100)g^7=(1011)g^8=(0101)g^9=(1010)g^{10}=(0111)g^{11}=(1110)
g^{12} = (1111) g^{13} =(1101) g^{14} =(1001) g^{15} = (0001)

In a true cryptographic application, the parameter m must be large enough to preclude the efficient generation of such a table otherwise the cryptosystem can be broken. In today's practice, m = 160 is a suitable choice. The table allows the use of generator notation (g^e) rather than bit string notation, as used in the following example. Also, using generator notation allows multiplication without reference to the irreducible polynomial $f(x) = x^4 + x + 1$.

Consider the elliptic curve $y^2 + xy = x^3 + g^4x^2 + 1$. Here $a = g^4$ and $b = g^0 = 1$. The point (g^5, g^3) satisfies this equation overF_2^m :

$y^2 + xy = x^3 + g^4x^2 + 1$
$(g^3)^2 + g^5g^3 = (g^5)^3 + g^4g^{10} + 1$
$g^6 + g^8 = g^{15} + g^{14} + 1$
(1100) + (0101) = (0001) + (1001) + (0001)
(1001) = (1001) The fifteen points which satisfy this equation are: (1, g^{13}) (g^3, g^{13}) (g^5, g^{11}) (g^6, g^{14}) (g^9, g^{13}) (g^{10}, g^8) (g^{12}, g^{12}) (1, g^6) (g^3, g^8) (g^5, g^3) (g^6, g^8) (g^9, g^{10}) (g^{10}, g) (g^{12}, 0) (0, 1) These points are graphed below: figure 3.



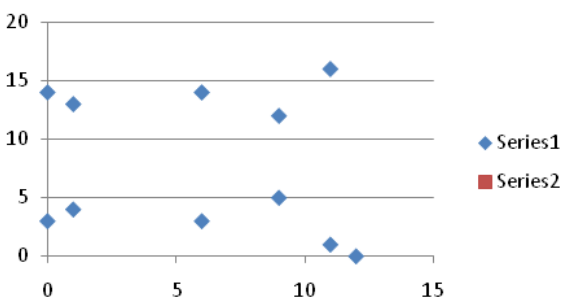
Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

Elliptic curve groups over F_2m have a finite number of points, and their arithmetic involves no round off error. This combined with the binary nature of the field, F_2m arithmetic can be performed very efficiently by a computer. Similarly consider the

Elliptic curve +10x+5 here a=3,b=5 and p=17 the points are given by

0	3
0	14
1	4
1	13
6	3
6	14
9	12
9	5
11	1
11	16
12	0

Table:3 the graph is given by



To find the cryptosystem in the finite field of order GF(2^8) with the irreducible polynomial

Consider the Elliptic curve $E_2^8(a,b)$
$Y^2+xy=x^3+ax^2+b$
Let a=1,b=1 $4a^3+27b^20$
Hence $E_2^8(1,1)$ exists.
$Y^2+xy=x^3+g^{17}x^2+1$ . . . . . .(I)
Put x=0 $y^2=1$
Y=1
i.e. (0,1) is a point on the curve (I)
$Y^2+xy=x^3+ax^2+b$
$Y^2=x^3+ax^2+b-xy$
$Y^2=x^3+x^2+xy+1$

Put $x=a^{17}$
$Y^2=a^{51}+a^{34}+a^{17}y+1$
(00001010)+(01001110)+(a^{17}y)+(00000000)
=(01000101)+a^{17}y
$a^{102}+a^{17}y$
$y^2=a^{102}+ya$

$a^{238}y^2=(a^{85}+y)$
L.H.S=$a^{238}a^{34}=a^{17}$
R=a^{34}
$a^{238}a^{68}=a^{85}+a^{34}$
$=a^{51}$
$x^{-1}y^2=x^2+x+x^{-1})+y$
$a^{238}y^2=(a^{34}+a^{119})+y$ $=a^{170}+y$
$Y^2=a^{187}+a^{17}y$
$Y^2=a^{187}+a^{17}y$
$y^2+xy=x^3+a^{51}x^2+1$
$y^2=x^3+a^{51}x^2+xy+1$
$y^2=a^{51}+a^{51}a^{34}+a^{17}y+1$
$=a^{51}(1+a^{34})+a^{17}y+1$
$=a^{51}.a^{136}+a^{17}y+1$
$=a^{204}+a1^7y$
$a^{34}=x^3+a^{51}x^2+a^{17}x+1$
$a^{34}+1=x^2(x+a^{51})+(a^{17}x+1)$
$(x+1)(x^2+x+1)+a^{17}x(a^{34}x+1)$
$Xy+y^2=x^3+Ax^2+B$
$Xy+y^2=x^{51}+Ax^{34}+B$
Put B=1
$a^{17}y+y^2=a^{51}+Ax^{34}+1$=(00001010)+$Aa^{34}+1$
put $A=a^{51}$ xy=(00001010)+$a^{85}+1$
(00001010)+(11010110)+(00000001)
=(11011101)=a^{204}
$a^{51}+a^{153}=a^{17}$
$y^2+a^{17}y+a^{204}=0$
$y^2+(a^{51}+a^{13})+a^{51}a^{103}=0$
$(y+a^{50})(y+a^{153})=0$
Put $x=a^{68}$
$X^3+a^{51}x^2+1=a^{204}+a^{51}a^{136}+1$
$=a^{204}+a^{187}+1$
$Y^2+xy=0$ $y^2+a^{68}y=0$

Global public key elements:
$E_2^8(a^{51},1)$ Elliptic curve with parameters $P(a^{51},1)$,$Q=2^8$.
Let G=point on the Elliptic curve whose order is large let (a^{17},a^{51}) $y^2+xy=x^3+a^{51}x^2+1$.
$P((x_p,y_p)$ then R=2P,$a=a^{51}$
P=Q $x_R=\lambda^2+\lambda+a$
$Y_R=x_P^2+(\lambda+1)x_R$
$\lambda=a^{17}+a^{51}/a^{17}=a^{17}+a^{34}$
$x_R=(a^{17}+a^{34})^2+(a^{17}+a^{34})+a^{51}$
$(a^{17}+a^{34})(a^{17}+a^{34}+1)+a^{51}$
$=a^{85}(a^{85}+1)+a^{51}$
$a^{170}+a^{85}+a^{51}$
$=a^{238.}$
$Y_R=a^{34}+(a^{17}+a^{34}+1)a238$
$=a^{34}+(a^{85}+1)a^{238}$
$=a^{34}+a^{323}+a^{238}$
$=a^{34}+a^{68}+a^{238}$
$=a^{34}+a^{153}$
$=a^{1877}$
2P=(a^{238},a^{187}).
3P=P+2P $(a^{17},a^{51})+(a^{238},a^{187})$
P≠Q
$X_R=\lambda^2+\lambda+x_P+x_Q+a$
$Y_R=\lambda(x_P+x_R)+x_R+y_P$
$=a^{187}+a^{51}/a^{238}+a^{17}$
a^{85}/a^{119} $=a^{221}$
$x_R=a^{442}+a^{221}+a^{17}+a^{238}+a^{51}$
$=a^{187}+^{221}+a^{17}+a^{238}+a^{51}$
$a^{51}+a^{51}=0$
$y_R=a^{221}(a^{17}+0)+0+a^{17}$
$a^{238}+a^{17}=a^{119}$
3P=($0,a^{119}$)
4P=2P+2P
=(a^{238},a^{187})+(a^{238},a^{187})
$=\lambda=x_P+y_P/x_P=a^{238}+a^{187}/a^{238}=a^{238}+a^{204}=a^{85}$
$X_R=\lambda^2+\lambda+a=a^{51}$
$Y_R=x_P^2+(\lambda+1)x_R$
$a^{221}+a^{136}+a^{51}=0$
i.e 4P=(a^{51},0)
5P=4P+P
P
$X_R=\lambda^2+\lambda+x_P+x_Q+a$
$Y_R=\lambda(x_P+x_R)+x_R+y_P$
$X_R=a^{306}+a^{153}+a^{51}+a^{17}+a^{51}=a^{17}+a^{17}=0$
$Y_R=a^{153}(a^{51}+0)+0+0=a^{136}$
5P=(0,a^{136})
6P=5P+P=(0,a^{136})+($a^{17}+a^{51}$) =(∞,∞) The points on the curve are
P=(a^{17},a^{51})
2P=(a^{238},a^{187})

Volume : 4 | Issue : 3 | Mar 2014 | ISSN - 2249-555X

$3P=(0,a^{119})$
$4P=(a^{51},0)$
$5P=(0,a^{136})$
$6P=(\infty,\infty)$
Points are
$P=(a^{17},a^{51})$
$2P=(a^{238},a^{187})$
$3P=(0,a^{119})$
$4P=(a^{51},0)$
$5P=(0,a^{136})$
$6P=(\infty,\infty)$

Cryptosystem of order 2^8 :
$E_q(a,b)$ elliptic curve with parameters a and q where q is a prime or an integer of the form 2^m

G point on elliptic curve whose order is large value n let $G=(a^{17},a^{51})$ n=6

User A key generation: Select private n_A $n_a<n$

i.e $n_A=2$
calculate public key $P_A=n_AXG$
$2(a^{17},a^{51})$
$=(a^{238},a^{187})$

User B key generation:
Select private key n_B $n_B<n$
i.e $n_B=1$
calculate public key P_B i.e $P_B=n_BXG=1(a^{17},a^{51})$

calculation of secret key by user A
$K=n_AXP_B=2(a^{17},a^{51})$
$=(a^{238},a^{187})$

Calculation of secret key by user B:
$K=n_BXP_A$
$=1(a^{238},a^{187})$
$=(a^{238},a^{187})$
The two calculations in this produce the same result, because
$n_AX\ P_B=n_AX(n_BXG)=n_BX(n_AXG)=n_BXP_A$
$n_AXP_B=n_BXP_A$.

REFERENCE
1. Certicom, "standards for Efficient Cryptography,SEC 1:Elliptic curve | 2. Cole, Eric, Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials with CISSP CBK, Version 2.1.USA: SANS Press, 2003. | 3.J.Edge,an introduction to elliptic curve ,cryptography, http://Iwn.net/Articles/174127/.2006. | 4.N.Koblitz,A course in Number theory and cryptography,2nd ed.,brookes/Cole,1997. | 5.J.H.Silverman,The Arithmetic of Elliptic curves, Springer –Verlag,1986. | 6.RSA" Wikipedia.wikipedia,n.d.web.09 feb 2011.Stalings,William. Cryptography and network security.fourth,pearson,2009.print. | 7.Alfredj Menezes, paul c,vanoorschot and scott A.vanstone,guide to Elliptic curve Cryptography ,1996. | 8.N.Koblitz.CM-curves with good cryptographic properties. In Advances in Cryptology: Crypto 91' volume 576 of in computer science, pages 279-287,springer-verlag,1992. Notes | 9.The Thesis of on 2-Spreads in PG(5,3) by K. Hanumanthu under the super vision of Prof.K.Satyanarayana. | 10.Thesis of Dr. K .V. Durga Prasad : "Construction ofTranslation planes and Determinition of their translation complements",Ph.D Thesis,Osmania University | 11.Diffie, W., and M. E. Hellman. "New directions in cryptography." IEEE Transactions on Information Theory,, 1976: 644- 654. | 12. A Scalar Multiplication in Elliptic Curve Cryptography with Binary Polynomial Operations in Galois Field Hero Modares(thesis of master science. |