**Prime Field over Elliptic Curve Cryptography for security**

S.Vasundhara.

Asst Professor of Mathematics

G.Narayanamma Institute of Technology& Science(Women)

Shaikpet Hyderabad

Abstract:

Elliptical curve cryptography (ECC) is based on a public key cryptosystem based system that is an elliptic curve theory. Elliptic curve cryptography can be used to create smaller faster and more efficient cryptography keys. Elliptic-curve cryptography (ECC) is an approach to [public-key cryptography](https://en.wikipedia.org/wiki/Public-key_cryptography) based on the [algebraic structure](https://en.wikipedia.org/wiki/Algebraic_structure) of [elliptic curves](https://en.wikipedia.org/wiki/Elliptic_curve) over [finite fields](https://en.wikipedia.org/wiki/Finite_field). ECC requires smaller keys compared to non-EC cryptography (based on plain [Galois fields](https://en.wikipedia.org/wiki/Galois_field)) to provide equivalent security. Elliptic curves are applicable for [key agreement](https://en.wikipedia.org/wiki/Key_agreement), [digital signatures](https://en.wikipedia.org/wiki/Digital_signature), [pseudo-random generators](https://en.wikipedia.org/wiki/CPRNG) and other tasks. Indirectly, they can be used for [encryption](https://en.wikipedia.org/wiki/Encryption) by combining the key agreement with a [symmetric encryption](https://en.wikipedia.org/wiki/Symmetric-key_algorithm) scheme. They are also used in several [integer factorization](https://en.wikipedia.org/wiki/Integer_factorization) [algorithms](https://en.wikipedia.org/wiki/Algorithm) based on elliptic curves that have applications in cryptography, such as [Lenstra elliptic-curve factorization](https://en.wikipedia.org/wiki/Lenstra_elliptic-curve_factorization" \o "Lenstra elliptic-curve factorization).

Key words: Cryptography, Finite fields, Elliptic curves

**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 =gxmod 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) |

**Table 1.1**-**Mathematical Problem**

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. This company has an agreement with NSA on a set of cryptographic algorithms called suite B. This suite uses Elliptic curves and works over the prime field.

**1. Elliptic Curves over Real Numbers**

First elliptic curves over real numbers are considered, because it is easier to get an insight of addition and multiplication over an elliptic curve when they are explained with more familiar real number curves.

An interesting feature of elliptic curve theory is that an algebra can be created over an elliptic curve. Having two points on an elliptic curve and adding them together, a third point, which is also on the curve, is produced as the result. Importantly for cryptography, it is very difficult to say which two points were added. In fact the difficulty of this problem grows exponentially with the key length . *The Weierstrass equation*2 is defined as

*E* : *y*2+*a*1*xy*+*a*3*y* = *x*3 +*a*2*x*2 +*a*4*x*+*a*6;

where *x* and *y* are variables covering a plane. In future this is simply called *an elliptic curve*. Notice that *x* and *y* can be complex, real, integers or any kind of field elements . An elliptic curve *ER* : *y*2 = *x*3 +5*x*2 +4 over reals is presented in Figure 1. This curve will be later used for demonstrating elliptic curve algebra.

To create an algebra over an elliptic curve, addition must be defined and an *identity element* must be found. The identity element *O*¥ is the point that added to any point on a curve produces the same point as the result:

*P*+*O*= *P*: When elliptic curves are discussed the identity element is usually called *the point at infinity*. That is because if elliptic curves over real numbers are considered, this point can be thought of as lying infinitely far up the *y*-axis . Equation can also be presented in the following form:

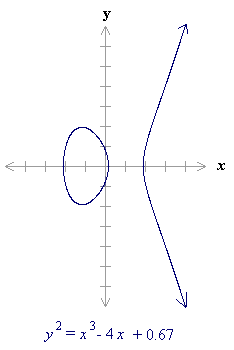
*PP*+(-*P*) = *O*: An elliptic curve over real numbers may be defined as the set of points (x,y) which satisfy an elliptic curve equation of the form:

y2 = x3 + 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 = -4 and b = 0.67 gives the elliptic curve with equation y2 = x3 - 4x + 0.67; the graph of this curve is shown below:

If x3 + ax + b contains no repeated factors, or equivalently if 4a3 + 27b2 is not 0, then the elliptic curve

y2 = x3 + 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.



**2.Elliptic Curve Groups over F2m**: The number of points on E(F2m)() is denoted by #*E*(F2m). The Hasse Theorem states that:

2m+1-22m#*E*(F2m) 2m+1+22m:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| There are finitely many points on a curve over F2m .   Elements of the field F2m are m-bit strings. The rules for arithmetic in F2m can be defined by either polynomial representation or by optimal normal basis representation. Since F2m operates on bit strings, computers can perform arithmetic in this field very efficiently.   An elliptic curve with the underlying field F2m is formed by choosing the elements a and b within F2m (the only condition is that b is not 0). As a result of the field F2m having a characteristic 2, the elliptic curve equation is slightly adjusted for binary representation:  y2 + xy = x3 + ax2 + b  The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation over F2m (where x and y are elements of F2m ). An elliptic curve group over F2m 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.   |  |  |  |  | | --- | --- | --- | --- | | An Example of an Elliptic Curve Group over F2m: |  |  |  |  |  | | --- | | As a very small example, consider the field F*2*4, defined by using polynomial representation with the irreducible polynomial f(x) = x4 + x + 1.  The element g = (0010) is a generator for the field . The powers of g are:  g0 = (0001) g1 = (0010) g2 = (0100) g3 = (1000) g4 = (0011) g5 = (0110)  g6 = (1100) g7 = (1011) g8 = (0101) g9 = (1010) g10 = (0111) g11 = (1110)  g12 = (1111) g13 =(1101) g14 =(1001) g15 = (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 (ge) 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) = x4 + x + 1.  Consider the elliptic curve y2 + xy = x3 + g4x2 + 1. Here a = g4 and b = g0 =1. The point (g5, g3) satisfies this equation overF2m :  y2 + xy = x3 + g4x2 + 1   (g3)2 + g5g3 = (g5)3 + g4g10 + 1   g6 + g8 = g15 + g14 + 1   (1100) + (0101) = (0001) + (1001) + (0001)   38(1001) = (1001)   The fifteen points which satisfy this equation are:   (1, g13) (g3, g13) (g5, g11) (g6, g14) (g9, g13) (g10, g8) (g12, g12)   (1, g6) (g3, g8) (g5, g3) (g6, g8) (g9, g10) (g10, g) (g12, 0) (0, 1) | |

**3.Construction of finite field of order 28 table for GF(28):**

Construction of finite field of order 28 (GF(28)with the irreducible polynomial(x)=x8+x4+x2+x+1.Let a be a point in this polynomial then a8=a4+a3+a2+1.

As α is a primitive element of GF(28),every element x of GF(28) may be expressed as a0+a1α+a2α2+a3α3+a4α4+a5α5+a6α6+a7α7 aiGF(28),0i.It is represented as 8-tuple (a0,a1,a2,a3,a4,a5,a6, a7).By this terminology we have α0=(1,0,0,0,0,0,0,0),α1=(0,1,0,0,0,0,0,0)α2=(0,0,1,0,0,0),α3=(0,0,0,1,0,0,0,0),α4=(0,0,0,0,1,0) α5=(0,0,0,0,0,10,0,) α6=(0,0,0,0,0,0,1,0),α7=(0,0,0,0,0,0,0,1)

And α8=α 4+α3 +α2+1=(10,1,1,1,0,0,0,0),we get α9= α5+α4+α3+α=(0,1,0,1,1,1,0,0)The other powers of α are computed similarly with the following table.

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| i | ai | 42 | 10101101 | 85 | 01101011 | 128 | 10100001 | 171 | 11001101 | 214 | 10011111 |
| i | ai | 42 | 10101101 | 85 | 01101011 | 128 | 10100001 | 171 | 11001101 | 214 | 10011111 |
| 0 | 10000000 | 43 | 11101110 | 86 | 10001101 | 129 | 11101000 | 172 | 11011110 | 215 | 11110111 |
| 1 | 01000000 | 44 | 01110111 | 87 | 11111110 | 130 | 01110100 | 173 | 01101111 | 216 | 11000011 |
| 2 | 00100000 | 45 | 10000011 | 88 | 01111111 | 131 | 00111010 | 174 | 10001111 | 217 | 11011001 |
| 3 | 00010000 | 46 | 11111001 | 89 | 10000111 | 132 | 00011101 | 175 | 11111111 | 218 | 11010100 |
| 4 | 00001000 | 47 | 11000100 | 90 | 11111011 | 133 | 10110110 | 176 | 11000111 | 219 | 01101010 |
| 5 | 00000100 | 48 | 01100010 | 91 | 11000101 | 134 | 01011011 | 177 | 11011011 | 220 | 00110101 |
| 6 | 00000010 | 49 | 00110001 | 92 | 11011010 | 135 | 10010101 | 178 | 11010101 | 221 | 10100010 |
| 7 | 00000001 | 50 | 10100000 | 93 | 01101101 | 136 | 11110010 | 179 | 11010010 | 222 | 01010001 |
| 8 | 10111000 | 51 | 01010000 | 94 | 10001110 | 137 | 01111001 | 180 | 01101001 | 223 | 10010000 |
| 9 | 01011100 | 52 | 00101000 | 95 | 01000111 | 138 | 10000100 | 181 | 10001100 | 224 | 01001000 |
| 10 | 00101110 | 53 | 00010100 | 96 | 10011011 | 139 | 01000010 | 182 | 01000110 | 225 | 00100100 |
| 11 | 00010111 | 54 | 00001010 | 97 | 11110101 | 140 | 00100001 | 183 | 00100011 | 226 | 00010010 |
| 12 | 10110011 | 55 | 00000101 | 98 | 11000010 | 141 | 10101000 | 184 | 10101001 | 227 | 00001001 |
| 13 | 11100001 | 56 | 10111010 | 99 | 01100001 | 142 | 01010100 | 185 | 11101100 | 228 | 10111100 |
| 14 | 11001000 | 57 | 01011101 | 100 | 10001000 | 143 | 00101010 | 186 | 01110110 | 229 | 01011110 |
| 15 | 01100100 | 58 | 10010110 | 101 | 01000100 | 144 | 00010101 | 187 | 00111011 | 230 | 00101111 |
| 16 | 00110010 | 59 | 01001011 | 102 | 00100010 | 145 | 10110010 | 188 | 10100101 | 231 | 10101111 |
| 17 | 00011001 | 60 | 10011101 | 103 | 00010001 | 146 | 1011001 | 189 | 11101010 | 232 | 11101111 |
| 18 | 10110100 | 61 | 11110110 | 104 | 10110000 | 147 | 10010100 | 190 | 01110101 | 233 | 11001111 |
| 19 | 01011010 | 62 | 01111011 | 105 | 01011000 | 148 | 01001010 | 191 | 10000010 | 234 | 11011111 |
| 20 | 00101101 | 63 | 10000101 | 106 | 00101100 | 149 | 00100101 | 192 | 01000001 | 235 | 11010111 |
| 21 | 10101110 | 64 | 11111010 | 107 | 00010110 | 150 | 10101010 | 193 | 10011000 | 236 | 11010011 |
| 22 | 01010111 | 65 | 01111101 | 108 | 00001011 | 151 | 01010101 | 194 | 01001100 | 237 | 11010001 |
| 23 | 10010011 | 66 | 10000110 | 109 | 10111101 | 152 | 10010010 | 195 | 00100110 | 238 | 11010000 |
| 24 | 11110001 | 67 | 01000011 | 110 | 11100110 | 153 | 01001001 | 196 | 00010011 | 239 | 01101000 |
| 25 | 11000000 | 68 | 10011001 | 111 | 01110011 | 154 | 10011100 | 197 | 10110001 | 240 | 00110100 |
| 26 | 01100000 | 69 | 11110100 | 112 | 10000001 | 155 | 01001110 | 198 | 11100000 | 241 | 00011010 |
| 27 | 00110000 | 70 | 01111010 | 113 | 11111000 | 156 | 00100111 | 199 | 01110000 | 242 | 00001101 |
| 28 | 00011000 | 71 | 00111101 | 114 | 01111100 | 157 | 10101011 | 200 | 00111000 | 243 | 10111110 |
| 29 | 00001100 | 72 | 10100110 | 115 | 00111110 | 158 | 11101101 | 201 | 00011100 | 244 | 01011111 |
| 30 | 00000110 | 73 | 01010011 | 116 | 00011111 | 159 | 11001110 | 202 | 00001110 | 245 | 10010111 |
| 31 | 00000011 | 74 | 10010001 | 117 | 10110111 | 160 | 01100111 | 203 | 00000111 | 246 | 11110011 |
| 32 | 10111001 | 75 | 11110000 | 118 | 11100011 | 161 | 10001011 | 204 | 10111011 | 247 | 11000001 |
| 33 | 11100100 | 76 | 01111000 | 119 | 11001001 | 162 | 11111101 | 205 | 11100101 | 248 | 11011000 |
| 34 | 01110010 | 77 | 00111100 | 120 | 11011100 | 163 | 11000110 | 206 | 11001010 | 249 | 01101100 |
| 35 | 00111001 | 78 | 00011110 | 121 | 01101110 | 164 | 01100011 | 207 | 01100101 | 250 | 00110110 |
| 36 | 10100100 | 79 | 00001111 | 122 | 00110111 | 165 | 10001001 | 208 | 10001010 | 251 | 00011011 |
| 37 | 01010010 | 80 | 10111111 | 123 | 10100011 | 166 | 11111100 | 209 | 01000101 | 252 | 10110101 |
| 38 | 00101001 | 81 | 11100111 | 124 | 11101001 | 167 | 01111110 | 210 | 10011010 | 253 | 11100010 |
| 39 | 10101100 | 82 | 11001011 | 125 | 11001100 | 168 | 00111111 | 211 | 01001101 | 254 | 01110001 |
| 40 | 01010110 | 83 | 11011101 | 126 | 01100110 | 169 | 10100111 | 212 | 10011110 | 255 | 10000000 |
| 41 | 00101011 | 84 | 11010110 | 127 | 00110011 | 170 | 11101011 | 213 | 01001111 |

A finite field of order 24it is also a subfield of order 28

Table:

|  |  |
| --- | --- |
| I | ai |
| 0 | 00000000 |
| 17 | 10011000 |
| 34 | 01001110 |
| 51 | 00001010 |
| 68 | 10011001 |
| 85 | 11010110 |
| 102 | 01000100 |
| 119 | 10010011 |
| 136 | 01001111 |
| 153 | 10010010 |
| 170 | 11010111 |
| 187 | 11011100 |
| 204 | 11011101 |
| 221 | 01000101 |
| 238 | 00001011 |
| 255 | 00000001 |

Similarly the multiplication table for the GF(28) with the irreducible polynomial

Consider the Elliptic curve E28(a,b)

Y2+xy=x3+ax2+b

Let a=1,b=1 4a3+27b20

Hence E28(1,1) exists.

Y2+xy=x3+g17x2+1 . . . . . .. . . .(I)

Put x=0 y2=1

Y=1

i.e. (0,1) is a point on the curve (I)

Y2+xy=x3+ax2+b

Y2=x3+ax2+b-xy

Y2=x3+x2+xy+1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Put x=a17

Y2=a51+a34+a17y+1

(00001010)+(01001110)+(a17y)+(00000000)

=(01000101)+a17y

a102+a17y

y2=a102+ya

\_\_\_\_\_\_\_\_\_\_\_\_\_-

a238y2=(a85+y)

L.H.S=a238a34=a17

R=a34

a238a68=a85+a34

=a51

x-1y2=x2+x+x-1)+y

a238y2=(a34+a119)+y =a170+y

Y2=a187+a17y

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Y2=a187+a17y

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

y2+xy=x3+a51x2+1

y2=x3+a51x2+xy+1

y2=a51+a51a34+a17y+1

=a51(1+a34)+a17y+1

=a51.a136+a17y+1

=a204+a17y

a34=x3+a51x2+a17x+1

a34+1=x2(x+a51)+(a17x+1)

(x+1)(x2+x+1)+a17x(a34x+1)

Xy+y2=x3+Ax2+B

Xy+y2=x51+Ax34+B

Put B=1

a17y+y2=a51+Ax34+1=(00001010)+Aa34+1

put A=a51 xy=(00001010)+a85+1

(00001010)+(11010110)+(00000001)

=(11011101)=a204

a51+a153=a17

y2+a17y+a204=0

y2+(a51+a13)+a51a103=0

(y+a5()(y+a153)=0

Put x=a68

X3+a51x2+1=a204+a51a136+1

=a204+a187+1

Y2+xy=0 y2+a68y=0

**Global public key elements:**

E28(a51,1) Elliptic curve with parameters P(a51,1),Q=28.

Let G=point on the Elliptic curve whose order is large let (a17,a51) y2+xy=x3+a51x2+1.

**P**((xp,yp) then **R=2P**,a=a51

**P=Q** xR=λ2+λ+a

YR=xP2+(λ+1)xR

λ=a17+a51/a17=a17+a34

xR=(a17+a34)2+(a17+a34)+a51

(a17+a34)(a17+a34+1)+a51

=a85(a85+1)+a51

a170+a85+a51

=a238.

YR=a34+(a17+a34+1)a238

=a34+(a85+1)a238

=a34+a323+a238

=a34+a68+a238

=a34+a153

=a1877

**2P**=(a238,a187).

**3P=P+2P** (a17,a51)+(a238,a187)

**P≠Q**

XR=λ2 +λ+xP+xQ+a

YR=λ(xP+xR)+xR+yP

=a187+a51/a238+a17

a85/a119 =a221

xR=a442+a221+a17+a238+a51

=a187+221+a17+a238+a51

a51+a51=0

yR=a221(a17+0)+0+a17

a238+a17=a119

**3P**=(0,a119)

**4P=2P+2P**

=(a238,a187)+(a238,a187)

=λ=xP+yP/xP=a238+a187/a238=a238+a204=a85

XR=λ2+λ+a=a51

YR=xP2+(λ+1)xR

a221+a136+a51=0

i.e 4P=(a51,0)

**5P=4P+P**

**P**

XR=λ2 +λ+xP+xQ+a

YR=λ(xP+xR)+xR+yP

XR=a306+a153+a51+a17+a51=a17+a17=0

YR=a153(a51+0)+0+0=a136

**5P**=(0,a136)

**6P=5P+P**=(0,a136)+(a17+a51) =(∞,∞) The points on the curve are

**P**=(a17,a51)

**2P**=(a238,a187)

**3P**=(0,a119)

**4P**=(a51,0)

**5P**=(0,a136)

**6P**=(∞,∞)

Points are

**P**=(a17,a51)

**2P**=(a238,a187)

**3P**=(0,a119)

**4P=**(a51,0)

**5P**=(0,a136)

**6P**=(∞,∞)

**Cryptosystem:**

Eq(a,b) elliptic curve with parameters a and q where q is a prime or an integer of the form 2m

G point on elliptic curve whose order is large value n let G=(a17,a51) n=6

**User A key generation:** Select private nA na<n

i.e nA=2

calculate public key PA=nAXG

2(a17,a51)

=(a238,a187)

**User B key generation:**

Select private key nB nB<n

i.e nB=1

calculate public key PB i.e PB=nBXG=1(a17,a51)

**calculation of secret key by user A**

K=nAXPB=2(a17,a51)

=(a238,a187)

**Calculation of secret key by user B**:

K=nBXPA

=1(a238,a187)

=(a238,a187)

The two calculations in this produce the same result, because

nAX PB=nAX(nBXG)=nBX(nAXG)=nBXPA

nAXPB=nBXPA.

E28(a34,a187) elliptic curve with parameters P(a34,a187) G is point on the elliptic curve whose order is very large

Let (a34,a187)

Y2+xy=x3+a51x2+1

L.H.S=A374+A221

=a85

R.H.S= a102+a51+68+1

=a 85

L.H.S=R.H.S

P=Q

P(xP,yP) then R=2P

XR=λ2+λ+a

YR=xP2+(λ+1)

λ=a187

XR=a221

YR=a34

**2P=(a221,a34)**

**3P**=2P+P= a221,a34)+(a34,a187)

PQ here

XR=λ2+λ+xP+xQ+a , YR=λ(xP+xR)+xR+yP

λ=a170

xR=0

yR=1

**3P=(0,1)**

**4P**=2P+2P

(a221,a34)+(a221,a34)

λ=a187

xR=a221

yR=a238

**4P=(a221,a238)**

**5P**=4P+P=(a221,a238)+(a34,a187)

λ=a187

xR=a34

yR=a153

**5P**=(a34,a153)

**6P**=2(3P)=3P+3P=(0,1)+(0,1)

λ=

xR=∞

yR=∞

Similarly another cryptosystem is given with the following points on the curve

Y2+xy=x3+ax2+b

a=a51

P=(a34,a187)

2P=(a221,a34)

3P=(0,1)

4P=(a221,a238)

5P=(a34,a153)

6P=(∞,∞)

Cryptosystem:

Let n=6

G=(a34,a187)

User A key generation: select private key nA nA<n

i.e nA=4

calculate public key PA=nAXG=4(a34,a187)

=(a221,a238)

User B key generation:

Select private key nB nB<n

nB<n

i.e nB=5

calculate public key PBi.e PB=nBXG=5(a34,a187)=(a34,a153)

calculate of secret key by user A:

k=nAXPB=4(a34,a187)

=(a221,a34)

Calculation of secret key by user B:

K=nBXPA=5(a221,a238)

=(a221,a34)

The two calculations in this produce the same result,

because nAX PB=nAX(nBXG)=nBX(nAXG)=nBXPA

nAXPB=nBXPA. In this paper, an introduction of ECC operations over binary field, prime field and their mathematical operations is explained. With clear examples, how the field operation level work over both fields (Binary, Prime) are shown. Then, higher level operations (ECC operations) are discussed. The process of adding point to another point and point doubling in order to produce a new point is explained .We explained the construction of finite field of order2 8  .This paper gives the cryptosystem over the binary field of order 28

References: 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.