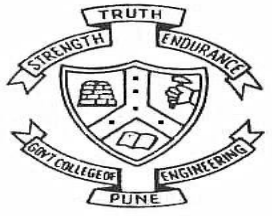

Greeting
COEP Technological University

Cryptography and Network Security

V. K. Pachghare



Elliptic Curve Groups over Fp

- An Essential property for cryptography is that a group has a finite number of points.
- Calculations over the real numbers are slow and inaccurate due to round-off error.
- 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, and computations end by taking the remainder on division by p. For example, in F_{23} the field is composed of integers from 0 to 22, and any operation within this field will result in an integer also between 0 and 22.

- An elliptic curve with the underlying field of Fp can formed by choosing the variables a and b within the field of F_p. The elliptic curve includes all points (x,y) which satisfy the elliptic curve equation modulo p (where x and y are numbers in F_p).

For example

$y^2 \bmod p = x^3 + ax + b \bmod p$ has an underlying field of Fp if a and b are in Fp.

If $x^3 + ax + b$ contains no repeating factors (or, equivalently, if $4a^3 + 27b^2 \bmod p$ is not 0), then the elliptic curve can be used to form a group. An elliptic curve group over Fp consists of the points on the corresponding elliptic curve, together with a special point O called the point at infinity. There are finitely many points on such an elliptic curve.

- As a very small example, consider an elliptic curve over the field F_{23}. With a = 1 and b = 0, the elliptic curve equation is $y^2 = x^3 + x$. The point (9,5) satisfies this equation since:
- $y^2 \bmod p = x^3 + x \bmod p$

  $25 \bmod 23 = 729 + 9 \bmod 23$

  $25 \bmod 23 = 738 \bmod 23$

  $2 = 2$

The 23 points which satisfy this equation are:

(0,0) (1,5) (1,18) (9,5) (9,18) (11,10) (11,13) (13,5) (13,18) (15,3) (15,20) (16,8)

(16,15) (17,10) (17,13) (18,10) (18,13) (19,1) (19,22) (20,4) (20,19) (21,6) (21,17)

- Note that there is two points for every x value. Even though the graph seems random, there is still symmetry about y = 11.5. Recall that elliptic curves over real numbers, there exists a negative point for each point which is reflected through the x-axis. Over the field of F_{23}, the negative components in the y-values are taken modulo 23, resulting in a positive number as a difference from 23. Here -P = (x_P, ($-y_P$ Mod 23))

Adding distinct points P and Q

The negative of the point $P = (x_P, y_P)$ is the point $-P = (x_P, -y_P \bmod p)$. If P and Q are distinct points such that P is not -Q, then

$P + Q = R$ where

$s = (y_P - y_Q) / (x_P - x_Q) \bmod p$

$x_R = s^2 - x_P - x_Q \bmod p$ and $y_R = -y_P + s(x_P - x_R) \bmod p$

Note that s is the slope of the line through P and Q.

Doubling the point P

- Provided that y_P is not 0,

  2P = R where

  $s = (3x_P^2 + a) / (2y_P) \bmod p$

  $x_R = s^2 - 2x_P \bmod p$ and $y_R = -y_P + s(x_P - x_R) \bmod p$

  Recall that a is one of the parameters chosen with the elliptic curve and that s is the slope of the line through P and Q

Models

1. Change the variables a and b to see the resulting number of points on the curve.
2. Select a point P on the curve, and then select a point Q. Add them together.
3. Select a point P on the curve and then double it.
4. Try doubling P when $y_P = 0$
5. Try adding two points with the same x-value.

Elliptic Curve Groups over F

1. Does the elliptic curve equation $y^2 = x^3 + 10x + 5$ define a group over F_{17}?
2. Do the points P(2,0) and Q(6,3) lie on the elliptic curve $y^2 = x^3 + x + 7$ over F_{17}?
3. What are the negatives of the following elliptic curve points over F_{17}? P(5,8) Q(3,0) R(0,6)

4. In the elliptic curve group defined by $y^2 = x^3 + x + 7$ over F_{17}, what is P + Q if P = (2,0) and Q = (1,3)?

5. In the elliptic curve group defined by $y^2 = x^3 + x + 7$ over F_{17}, what is 2P if P = (1, 3)?

Elliptic Curve Groups over Fp

1. Does the elliptic curve equation $y^2 = x^3 + 10x + 5$ define a group over F_{17}?

- No, since:

  $= 4(10)^3 + 27(5)^2 \bmod 17$

  $= 4675 \bmod 17$

  $= 0$

  Thus this elliptic curve does not define a group because

  $4a^3 + 27b^2 \bmod p$ is 0

2. Do the points P(2,0) and Q(6,3) lie on the elliptic curve $y^2 = x^3 + x + 7$ over F_{17}?

- The point P(2,0) is on the elliptic curve since both sides of the equation agree:

  (0)2 mod 17 = (2)3 + 2 + 7 mod 17

  0 mod 17 = 17 mod 17

  0 = 0.

  However, the point Q(6,3) is not on the elliptic curve since the equation is false:

  (3)2 mod 17 = (6)3 + 6 + 7 mod 17

  9 mod 17 = 229 mod 17

  9 = 8, does not agree.

What are the negatives of the following elliptic curve points over F_{17}?

- P(5,8) Q(3,0) R(0,6)

  The negative of a point P = (xP, yP) is the point -P = (xP, -yP mod p). Thus

  -P(5,9) -Q(3,0) -R(0,11)

4.In the elliptic curve group defined by $y^2 = x^3 + x + 7$ over F_{17}, what is P + Q if P = (2,0) and Q = (1,3)?

- s = (yP - yQ) / (xP - xQ) mod p = (-3) / 1 mod 17 = -3 mod 17 = 14
  xR = s2 - xP - xQ mod p = 196 - 2 - 1 mod 17 = 193 mod 17 = 6
- yR = -yP + s(xP - xR) mod p = 0 + 14*(2 - 6) mod 17 = -56 mod 17 = 12

Thus P + Q = (6,12)

5. In the elliptic curve group defined by$y^2 = x^3 + x + 7$ over F_{17}, what is 2P if P = (1, 3)?

$s = (3xP^2 + a) / (2yP) \bmod p = (3 + 1) * 6\text{-}1 \bmod 17 = 4 * 3 \bmod 17 = 12$
$xR = s^2 - 2xP \bmod p = 144 - 2 \bmod 17 = 142 \bmod 17 = 6$

$yR = -yP + s(xP - xR) \bmod p = -3 + 12 * (1 - 6) \bmod 17 = -63 \bmod 17 = 5$

Thus 2P = (6,5)

- There are finitely many points on a curve over F_2m .
- Elements of the field F_2m are m-bit strings. 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_2m 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.

- As a very small example, consider the field $F_2 4$, 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 over F_2m :

  $y^2 + xy = x^3 + g^4x^2 + 1$

  $(g^3)^2 + g^5g^3 = (g^5)^3 + g^4g^{10} + 1$

  $g^6 + g^8 = g^{15} + g^{14} + 1$

- $(1100) + (0101) = (0001) + (1001) + (0001)$

  $(1001) = (1001)$

  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) $(g^{12}, 0)$ $(0, 1)$ 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.

- **The following algebraic rules are applied for arithmetic over F_2m**

4.2.1 Adding distinct points P and Q

- The negative of the point P = (xP, yP) is the point -P = (xP, xP + yP). If P and Q are distinct points such that P is not -Q, then

  P + Q = R where

  s = (yP - yQ) / (xP + xQ)

  $xR = s^2 + s + xP + xQ + a$ and yR = s(xP + xR) + xR + yP

- As with elliptic curve groups over real numbers, P + (-P) = O, the point at infinity. Furthermore, P + O = P for all points P in the elliptic curve group.

4.2.2 Doubling the point P

- If xP = 0, then 2P = O
- Provided that xP is not 0,

  2P = R where

  s = xP + yP / xP

  xR = s^2+ s + a and yR = xP^2 + (s + 1) * xR

- Recall that a is one of the parameters chosen with the elliptic curve and that s is the slope of the line through P and Q
- The following model can be used to experiment with addition and doubling in a variety of elliptic curve groups over F24.

1. Change the variables a and b to see the resulting number of points on the curve.

2. Select a point P on the curve, and then select a point Q on the curve, and then add them together.

3. Select a point P on the curve and then double it.

4. Try doubling P for g^0

5. Try adding two points with the same x-value.

Elliptic Curve Groups Over

- For the following questions, assume the use of the field $F_2 3$. The field is described here using polynomial representation with the irreducible polynomial $x^3 + x + 1$. A generator for the field is g = (010), and the powers of g are:

$g^1 = (010)$ $g^2 = (100)$ $g^3 = (011)$ $g^4 = (110)$ $g^5 = (111)$ $g^6 = (101)$ $g^7 = (001) = 1$

1. Does the elliptic curve equation $y^2 + xy = x^3 + g^5x^2 + g^6$ define a group over $F_2 3$?
2. Do the points P(g3, g6) and Q(g5, g2) lie on the elliptic curve $y^2 + xy = x^3 + g^2x^2 + g^6$ over $F_2 3$?
3. What are the negatives of the following elliptic curve points over $F_2 3$? $P(g^3,g^6)$ $Q(g,0)$ $R(0,g^3)$
4. In the elliptic curve group defined by $y^2 + xy = x^3 + g^2x^2 + g^6$ over $F_2 3$, what is P + Q if $P = (g^2,g^6)$ and $Q = (g^5,g^5)$?
5. In the elliptic curve group defined by $y^2 + xy = x^3 + g^2x^2 + g^6$ over $F_2 3$, what is 2P if $P = (g^3, g^4)$?

1. Does the elliptic curve equation $y^2 + xy = x^3 + g^5x^2 + g^6$ define a group over $F_2 3$?

- Since the parameter b = 6 is not zero, the equation $y^2 + xy = x^3 + g^5x^2 + g^6$ does define an elliptic curve group over $F_2 3$.

Do the points $P(g^3, g^6)$ and $Q(g^5, g^2)$ lie on the elliptic curve $y^2 + xy = x^3 + g^2x^2 + g^6$ over F_23?

- The point $P(g^3,g^6)$ is on the elliptic curve $y^2 + xy = x^3 + g^2x^2 + g^6$ over F_23 since that equation holds true:

  $(g^6)^2 + (g^3)(g^6) = (g^3)^3 + g^2(g^3)^2 + g^6$

  $g^5 + g^2 = g^2 + g + g^6$

- $(111) + (100) = (100) + (010) + (101)$

  $(011) = (011)$

- $g^3 = g^3$

  However, the point $Q(g^5)(g^2)$ is not on the elliptic curve, since the equation

  disagrees:

  $(g^2)^2 + (g^5)(g^2) = (g^5)^3 + g^2(g^5)^2 + g^6$

- $g^4 + 1 = g + g^5 + g^6$

  $(110) + (001) = (001) + (111) + (101)$

  $(111) = (000)$

  $g^5 = 0$ which is false.

What are the negatives of the following elliptic curve points over $F_2 3$?

- $P(g^3, g^6)$ $Q(g,0)$ $R(0,g3)$

  The negatives of the points are defined by (xP, xP + yP)

  $-P = (g^3, g^3 + g^6) = (g^3, g^4)$

  $-Q = (g, g + 0) = (g, g)$

  $-R = (0, 0 + g^3) = (0, g^3)$

In the elliptic curve group defined by $y^2 + xy = x^3 + g^2x^2 + g^6$ over $F_2 3$, what is P + Q if $P = (g^2, g^6)$ and $Q = (g^5, g^5)$?

- P + Q = R where:

  $s = (y^P - y^Q) / (x^P + x^Q) = (g^6 + g^5) / (g^2 + g^5) = g / g^3 = g\text{-}2 = g^5$

  $x^R = s^2 + s + x^P + x^Q + a = g^3 + g^5 + g^2 + g^5 + g^2 = g^3$

  $y^R = s(x^P + x^R) + x^R + y^P = g^5 * (g^2 + g^3) + g^5 + g^6 = g^5 * g^5 + g^3 + g^6 = g^3 +$

  $g^3 + g^6 = g^6$

  Thus $P + Q = (g^3, g^6)$

5. In the elliptic curve group defined by $y^2 + xy = x^3 + g^2x^2 + g^6$ over $F_2 3$, what is 2P if $P = (g^3, g^4)$?

- 2P = R where:

  $s = x^P + y^P / 2x^P = g^3 + g^4 / g^3 = g^3 + g = 1$

  $x^R = s^2 + s + a = 1 + 1 + g^2 = g^2$

  $y^R = x^P + (s + 1) * x^R = g^3 + 0 * g^2 = g^3$

  Thus $2P = (g^2, g^3)$