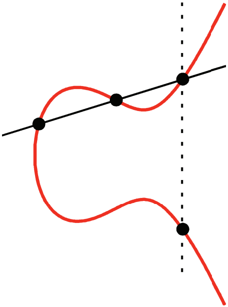
Elliptic Curve Cryptography

Çetin Kaya Koç

http://cs.ucsb.edu/~koc
koc@cs.ucsb.edu



Groups in Cryptography

- The security of the Diffie-Hellman key exchange, ElGamal public-key encryption algorithm, ElGamal signature scheme, and Digital Signature Algorithm depends on the difficulty of the DLP in $\mathcal{Z}_p^*$
- Another type of group for which the DLP is difficult is the elliptic curve group over a finite field
- In fact, the Elliptic Curve Discrete Logarithm Problem (ECDLP) seems to be a much more difficult problem than the DLP
- There is no subexponential algorithm for the ECDLP as of yet
- Furthermore, the elliptic curve variants of the Diffie-Hellman and the DSA require significantly smaller group size for the same amount of security, as compared to that of $\mathcal{Z}_p^*$ groups

Elliptic Curves

- An elliptic curve is the solution set of a nonsingular cubic polynomial equation in two unknowns over a field $\mathcal{F}$

$$\mathcal{E} = \{(x, y) \in \mathcal{F} \times \mathcal{F} \mid f(x, y) = 0\}$$

- The general equation of a cubic in two variables is given by

$$ax^3 + by^3 + cx^2y + dxy^2 + ex^2 + fy^2 + gxy + hx + iy + j = 0$$

- When $\text{char}(\mathcal{F}) \neq \{2, 3\}$, we can convert the above equation to the Weierstrass form

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

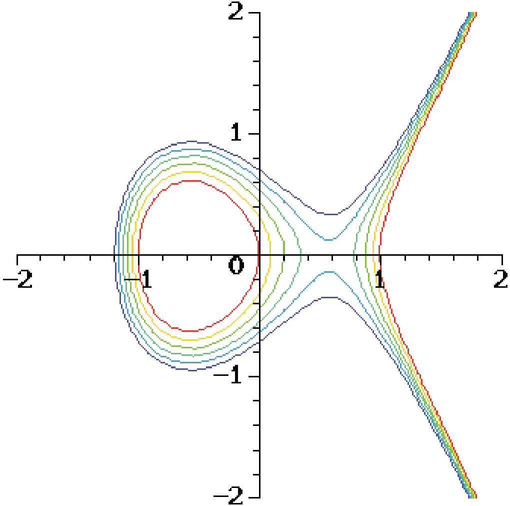
Elliptic Curves over $\mathcal{R}$

- The field in which this equation solved can be an infinite field, such as $\mathcal{C}$ (complex numbers), $\mathcal{R}$ (real numbers), or $\mathcal{Q}$ (rational numbers)
- The point at infinity, represented by $\mathcal{O}$, is also considered a solution of the equation
- The discriminant is defined as

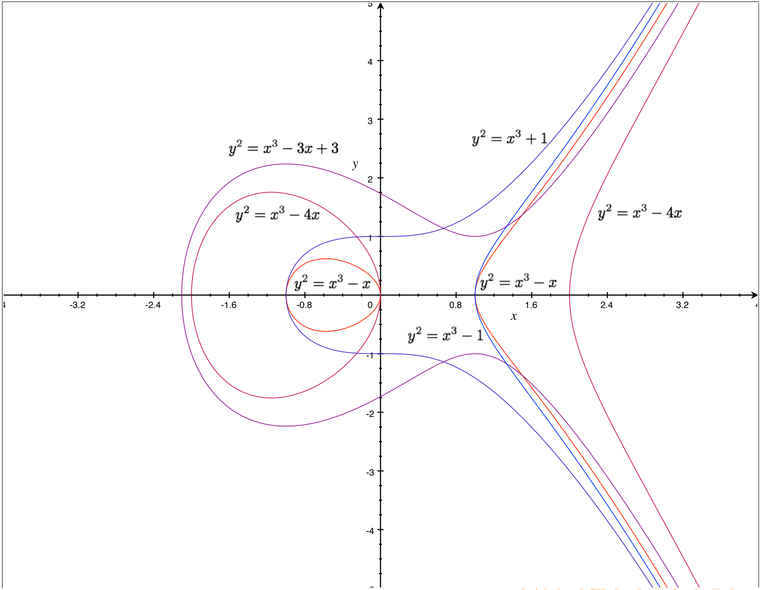
  $$\Delta = 4a^3 + 27b^2$$

  which is nonzero for nonsingular curves
- The elliptic curves over $\mathcal{R}$ for different values of a and b make continuous curves on the plane, which have either one or two parts

Elliptic Curves over $\mathcal{R}$



Elliptic Curves over $\mathcal{R}$



Bezout Theorem

Theorem

A linear line that intersects an elliptic curve at 2 points also crosses at a third point.

- Consider the elliptic curve and the linear equation together:

$$\begin{aligned} y^2 &= x^3 + ax + b \\ y &= cx + d \end{aligned}$$

- Substituting either y or x from the second equation to the first one, we obtain one of the following cubic equations

$$\begin{aligned} (cx+d)^2 &= x^3 + ax + b \\ y^2 &= (y-d)^3/c^3 + a(y-d)/c + b \end{aligned}$$

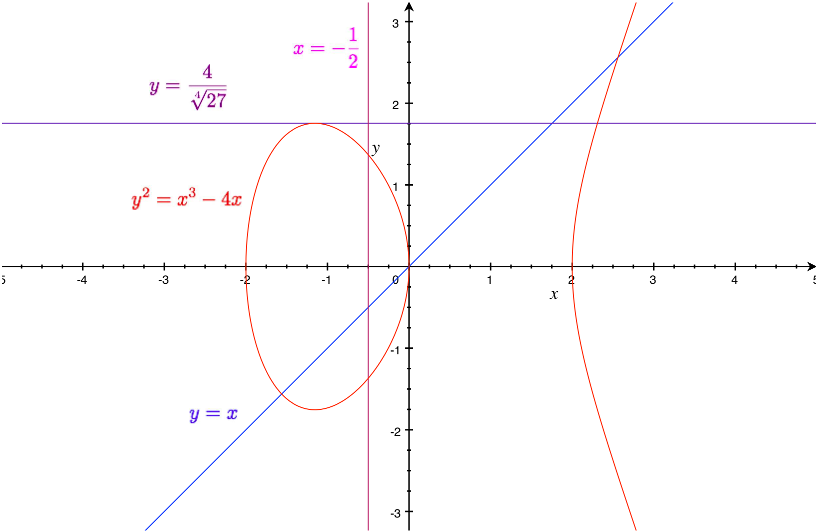
- A cubic equation has either 1 or 3 real roots; since we already have two points on the curve (2 real roots), the third one must be real

Elliptic Curve Chord and Tangent

- For example, by solving $y^2 = x^3 - 4x$ with three different linear equations, as given below, we find the following points on the curve:

$y = x$	$y = \frac{4}{\sqrt[4]{27}}$	$x = -\frac{1}{2}$
$(0, 0)$	$(-\frac{2}{\sqrt{3}}, \frac{4}{\sqrt[4]{27}})$	$(-\frac{1}{2}, \frac{\sqrt{15}}{2\sqrt{2}})$
$(\frac{1-\sqrt{17}}{2}, -\sqrt{\frac{9}{2} + \frac{\sqrt{17}}{2}})$	$(-\frac{2}{\sqrt{3}}, \frac{4}{\sqrt[4]{27}})$	$(-\frac{1}{2}, -\frac{\sqrt{15}}{2\sqrt{2}})$
$(\frac{1+\sqrt{17}}{2}, \sqrt{\frac{9}{2} + \frac{\sqrt{17}}{2}})$	$(\frac{4}{\sqrt{3}}, \frac{4}{\sqrt[4]{27}})$	

Elliptic Curve Chord and Tangent



Elliptic Curve Chord and Tangent

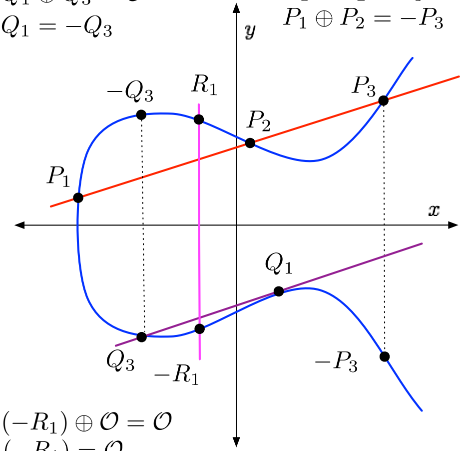
- In the first case we have (x_1, y_1), (x_2, y_2), (x_3, y_3), where all three coordinates are different
- In the second case, we have (x_1, y_1), (x_1, y_1), (x_3, y_3), where the first two coordinates are same, but the third one different
- Finally, in the third case we have (x_1, y_1), $(x_1, -y_1)$, where the x coordinates are equal and the y coordinates are equal with different sign
- By including the point at infinity $\mathcal{O}$ as one of points (neutral element) of the curve, we can introduce an operation $\oplus$ which "adds" three points P_1, P_2, and P_3 to get neutral element $\mathcal{O}$

$$P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$$

Elliptic Curve Point Addition

$$Q_1 \oplus Q_1 \oplus Q_3 = \mathcal{O}$$
$$Q_1 \oplus Q_1 = -Q_3$$

$$P_1 \oplus P_2 \oplus P_3 = \mathcal{O}$$
$$P_1 \oplus P_2 = -P_3$$



$$R_1 \oplus (-R_1) \oplus \mathcal{O} = \mathcal{O}$$
$$R_1 \oplus (-R_1) = \mathcal{O}$$
$$R_1 \oplus \mathcal{O} = R_1$$

Elliptic Curve Point Addition

- The “point addition” is a geometric operation: a linear line that connects P_1 and P_2 also crosses the elliptic curve at a third point, which we will name as P_3
- The new “sum” point $-P_3 = P_1 \oplus P_2$ is the mirror image of P_3 with respect to the x axis:

$$\text{if} \quad P_3 = (x_3, y_3) \quad \text{then} \quad -P_3 = (x_3, -y_3)$$

- The point at infinity $\mathcal{O}$ acts as the neutral (zero) element

$$\begin{aligned} P \oplus \mathcal{O} &= \mathcal{O} \oplus P = P \\ P \oplus (-P) &= (-P) \oplus P = \mathcal{O} \end{aligned}$$

Elliptic Curve Groups

- The set of points (x, y) on elliptic curve together with the point at infinity $\mathcal{O}$

$$\mathcal{E} = \{(x, y) \mid (x, y) \in \mathcal{F}^2 \text{ and } y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

  forms an Abelian group with respect to the addition operation $\oplus$

- The addition operation computes the coordinates (x_3, y_3) of $-P_3$ for $-P_3 = P_1 \oplus P_2 = (x_1, y_1) \oplus (x_2, y_2)$
- The addition rule for $-P_3 = P_1 \oplus P_2$ can be algebraically obtained by first computing the slope m of the straight line that connects $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ using

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

Elliptic Curve Addition and Doubling Rule

- Then, the linear equation $y - y_1 = m(x - x_1)$ is solved together with the elliptic curve equation $y^2 = x^3 + ax + b$ to obtain the coordinates of the third point $-P_3 = (x_3, y_3)$
- In the case of doubling

  $$-Q_3 = Q_1 \oplus Q_1 = (x_1, y_1) \oplus (x_1, y_1)$$

  the slope m of the linear line is equal to the derivative of the elliptic curve equation $y^2 = x^3 + ax + b$ evaluated at point x_1 as

  $$2yy' = 3x^2 + a \quad \rightarrow \quad y' = \frac{3x^2 + a}{2y}$$

- Once the slope m is obtained, the linear equation can be written, and solved together with the elliptic curve equation to find x_3 and y_3

Elliptic Curve Addition and Doubling over GF(p)

Given $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, the computation of $-P_3 = (x_3, y_3)$:

- If $(x_1, y_1) = \mathcal{O}$, then $(x_3, y_3) = (x_2, y_2)$ since $-P_3 = \mathcal{O} + P_2 = P_2$
- If $(x_2, y_2) = \mathcal{O}$, then $(x_3, y_3) = (x_1, y_1)$ since $-P_3 = P_1 + \mathcal{O} = P_1$
- If $x_2 = x_1$ & $y_2 = -y_1$, then $(x_3, y_3) = \mathcal{O}$ since $-P_3 = -P_1 + P_1 = \mathcal{O}$
- Otherwise, first compute the slope using

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{for} \quad x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{for} \quad x_1 = x_2 \text{ and } y_1 = y_2 \end{cases}$$

- Then, (x_3, y_3) is computed using

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m\,(x_1 - x_3) - y_1 \end{aligned}$$

Elliptic Curves over Finite Fields

- The field in which the Weierstrass equation solved can also be a finite field, which is of interest in cryptography
- Most common cases of finite fields are:
    - Characteristic p: GF(p), where p is a large prime
    - Characteristic 2: GF(2^k), where k is a small prime
    - Characteristic p: GF(p^k), where p and k are small primes
- In GF(p) for a prime $p \neq 2, 3$, we can use the Weierstrass equation

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

  with the understanding that the solution of this equation and all field operations are performed in the finite field GF(p)
- We will denote this group by $\mathcal{E}(a, b, p)$

An Elliptic Curve over GF(23)

- Consider the elliptic curve group $\mathcal{E}(1,1,23)$: The solutions of the equation with $a=1$ and $b=1$

  $$y^2 = x^3 + x + 1$$

  over the finite field GF(23)
- We obtain the elements of the group by solving this equation in GF(23) for all values of $x \in \mathcal{Z}_{23}^*$
- As we give a particular value for x, we obtain a quadratic equation in y modulo 23, whose solution will depend on whether the right hand side is a QR mod 23
- Note that if (x,y) is a solution, so is $(x,-y)$ because $y^2 = (-y)^2$, i.e., the elliptic curve is symmetric with respect to the x axis

An Elliptic Curve over GF(23)

- Starting with $x = 0$, we get $y^2 = 1 \pmod{23}$ which immediately gives two solutions as $(0, 1)$ and $(0, -1) = (0, 22)$
- Similarly, for $x = 1$, we obtain $y^2 = 3 \pmod{23}$
- This is a quadratic equation, the solution will depend on whether 3 is QR, which turns out to be:

$$3^{(p-1)/2} = 3^{11} = 1 \pmod{23}$$

The solution for y is

$$y = 3^{(p+1)/4} = 3^6 = 16 \pmod{23}$$

and thus, we find a pair of coordinates: $(1, 16)$, $(1, -16) = (1, 7)$

An Elliptic Curve over GF(23)

- Now, taking $x = 2$, we have $y^2 = 2^3 + 2 + 1 = 11 \pmod{23}$, however, 11 is a QNR since

  $$11^{(p-1)/2} = 11^{11} = -1$$

  therefore, there is no solution for $y^2 = 11 \pmod{23}$, and this elliptic curve does not have any points whose x coordinate is 2
- On the other hand, for $x = 3$, we have $y^2 = 3^3 + 3 + 1 = 31 = 8 \pmod{23}$, and 8 is a QR since

  $$8^{(p-1)/2} = 8^{11} = 1 \pmod{23}$$

- We solve for $y^2 = 8 \pmod{23}$ using

  $$y = 8^{(p+1)/4} = 8^6 = 13 \pmod{23}$$

  thus, obtain the pair of coordinates: $(3, 13)$, $(3, -13) = (3, 10)$

An Elliptic Curve over GF(23)

- Proceeding for the other values of $x \in \mathcal{Z}_{23}^{*}$, we find 27 solutions:

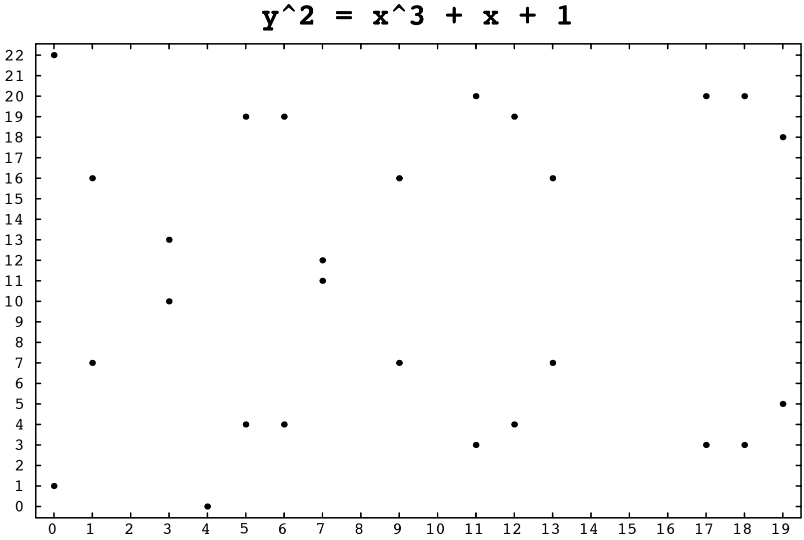
$$\begin{array}{ccccccc}
(0,1) & (0,22) & (1,7) & (1,16) & (3,10) & (3,13) & (4,0) \\
(5,4) & (5,19) & (6,4) & (6,19) & (7,11) & (7,12) & \\
(9,7) & (9,16) & (11,3) & (11,20) & (12,4) & (12,19) & \\
(13,7) & (13,16) & (17,3) & (17,20) & (18,3) & (18,20) & \\
(19,5) & (19,18) & & & & &
\end{array}$$

- Note that the solutions come in pairs except one of them: $(4,0)$, since for $x = 4$, we have

$$y^2 = 4^3 + 4 + 1 = 69 = 0 \pmod{23}$$

which has only one solution $y = 0$ and thus one point $(4,0)$

An Elliptic Curve over GF(23)



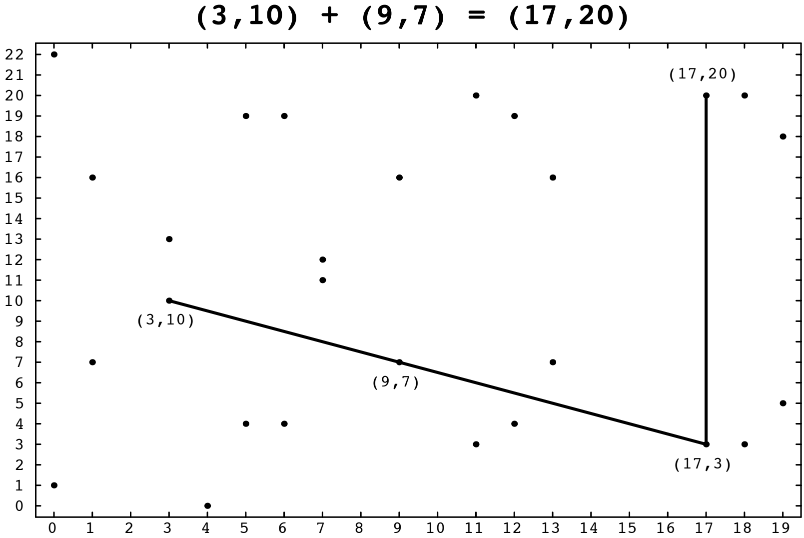
Elliptic Curve Point Addition over GF(23)

- Given $P_1 = (3, 10)$ and $P_2 = (9, 7)$, compute $P_1 \oplus P_2 = P_3$
- Since $x_1 \neq x_2$, we have

$$\begin{aligned}
m &= (y_2 - y_1) \cdot (x_2 - x_1)^{-1} \pmod{23} \\
&= (7 - 10) \cdot (9 - 3)^{-1} = (-3) \cdot 6^{-1} = 11 \pmod{23} \\
x_3 &= m^2 - x_1 - x_2 \pmod{23} \\
&= 11^2 - 3 - 9 \;=\; 17 \pmod{23} \\
y_3 &= m\,(x_1 - x_3) - y_1 \pmod{23} \\
&= 11 \cdot (3 - 17) - 10 \;=\; 20 \pmod{23}
\end{aligned}$$

- Thus, we have $(x_3, y_3) = (3, 10) \oplus (9, 7) = (17, 20)$
- Question: Is the geometry of point addition still valid?

Elliptic Curve Point Addition over GF(23)



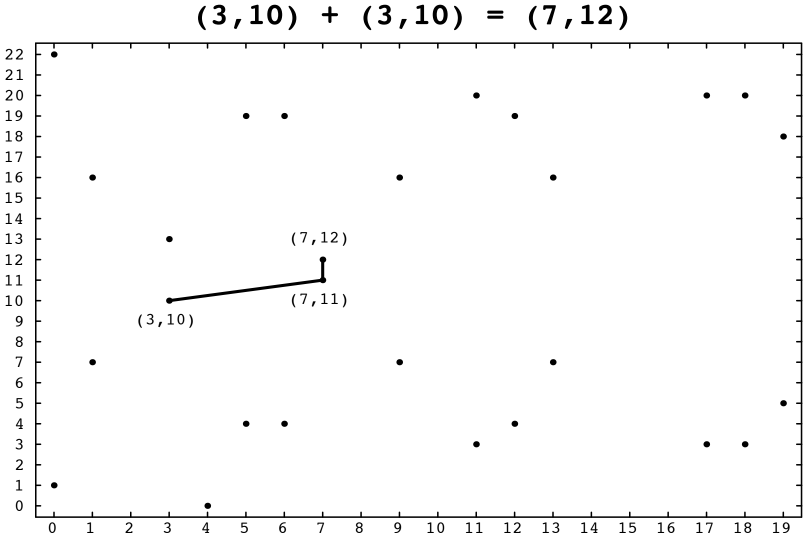
Elliptic Curve Point Doubling over GF(23)

- Given $P_1 = (3, 10)$, compute $P_1 \oplus P_1 = P_3$
- Since $x_1 = x_2$ and $y_1 = y_2$, we have

$$\begin{aligned}
m &= (3x_1^2 + a) \cdot (2y_1)^{-1} \pmod{23} \\
&= (3 \cdot 3^2 + 1) \cdot (20)^{-1} = 6 \pmod{23} \\
x_3 &= m^2 - x_1 - x_2 \pmod{23} \\
&= 6^2 - 3 - 3 = 7 \pmod{23} \\
y_3 &= m\,(x_1 - x_3) - y_1 \pmod{23} \\
&= 6 \cdot (3 - 7) - 10 = 12 \pmod{23}
\end{aligned}$$

- Thus, we have $(x_3, y_3) = (3, 10) \oplus (3, 10) = (7, 12)$
- Question: Is the geometry of point addition still valid?

Elliptic Curve Point Doubling over GF(23)



Elliptic Curves over GF(2^k)

- The Weierstrass form of an elliptic curve over GF(2^k) is given as

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

  with parameters $a, b \in$ GF(2^k) and $b \neq 0$, whose solutions are found in the field GF(2^k)
- The addition law is based on this equation, and therefore, the rules of addition and doubling formulae are different
- The elements of the field GF(2^k) can be represented in several ways
- We studied the polynomial representation, where $a(x) \in$ GF(2^k)

  $$a(x) = a_{k-1}x^k + \cdots + a_1x + a_0$$

  is a polynomial of degree at most k, with coefficients in GF(2)

Elliptic Curve Addition and Doubling over GF(2^k)

Given $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$, the computation of $P_3 = (x_3, y_3)$:

- If $(x_1, y_1) = \mathcal{O}$, then $(x_3, y_3) = (x_2, y_2)$ since $P_3 = \mathcal{O} + P_2 = P_2$
- If $(x_2, y_2) = \mathcal{O}$, then $(x_3, y_3) = (x_1, y_1)$ since $P_3 = P_1 + \mathcal{O} = P_1$
- If $x_2 = x_1$ and $y_2 = x_1 + y_1$, then $(x_3, y_3) = \mathcal{O}$ since $P_3 = -P_1 + P_1 = \mathcal{O}$
  ******
- Otherwise, (x_3, y_3) is computed using

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2 \\ y_3 &= m\,(x_1 - x_3) - y_1 \end{aligned}$$

where the slope is defined as

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{for} \quad x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1} & \text{for} \quad x_1 = x_2 \text{ and } y_1 = y_2 \end{cases}$$

****

Elliptic Curve Point Multiplication

- The elliptic curve point multiplication operation takes an integer k and a point on the curve P, and computes

$$[k]P = \overbrace{P \oplus P \oplus \cdots \oplus P}^{k \text{ times}}$$

- This can be accomplished with the binary method, using the binary expansion of the integer $k = (k_{m-1} \cdots k_1 k_0)_2$
- For example $[17]P$ is computed using the addition chain

$$P \xrightarrow{d} [2]P \xrightarrow{d} [4]P \xrightarrow{d} [8]P \xrightarrow{d} [16]P \xrightarrow{a} [17]P$$

- The symbol $\xrightarrow{d}$ stands for doubling, such as $[2]P \oplus [2]P = [4]P$
- The symbol $\xrightarrow{a}$ stands for addition, such as $P \oplus [16]P = [17]P$

Number of Points on an Elliptic Curve

- The elliptic curve group $\mathcal{E}(1,1,23)$ had the following elements:

$$\begin{array}{ccccccc}
(0,1) & (0,22) & (1,7) & (1,16) & (3,10) & (3,13) & (4,0) \\
(5,4) & (5,19) & (6,4) & (6,19) & (7,11) & (7,12) & \\
(9,7) & (9,16) & (11,3) & (11,20) & (12,4) & (12,19) & \\
(13,7) & (13,16) & (17,3) & (17,20) & (18,3) & (18,20) & \\
(19,5) & (19,18) & & & & &
\end{array}$$

- There are 27 points in the above list
- Including the point at infinity $\mathcal{O}$, the elliptic curve group $\mathcal{E}(1,1,23)$ has $27 + 1 = 28$ elements
- In other words, the order of the group $\mathcal{E}(1,1,23)$ is 28

Order of Elliptic Curve Groups

- In order to use an elliptic curve group $\mathcal{E}$ in cryptography, we need to know the order of the group, denoted as order($\mathcal{E}$)
- The order of $\mathcal{E}(a, b, p)$ is always less than $2p + 1$
- The finite field has p elements, and we solve the equation

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

  for values of $x = 0, 1, \ldots, p - 1$, and obtain a pair of solutions (x, y) and $(x, -y)$ for every x, we can have no more than $2p$ points
- Including the point at infinity, the order is bounded as

  $$\text{order}(\mathcal{E}(a, b, p)) \leq 2p + 1$$

- The order of $\mathcal{E}(1, 1, 23)$ is 28 which is less than $2 \cdot 23 + 1 = 47$

Order of Elliptic Curve Groups

- However, this bound is not very precise
- As we discovered in finding the elements of $\mathcal{E}(1,1,23)$, not every x value yields a solution of the quadratic equation $y^2 = x^3 + x + 1$
- For a solution to exists, $u = x^3 + ax + b$ needs to be a QR mod p
- Only half of the elements in GF(p) are QRs
- As x takes values in GF(p), depending on whether

  $$u = x^3 + ax + b$$

  is a QR or QNR, we will have a solution for $y^2 = u \pmod p$ or not, respectively
- Therefore, the number of solutions will be less than $2p$

Order of Elliptic Curve Groups

- If we define $\chi(u)$ as

$$\chi(u) = \begin{cases} +1 & \text{if } u \text{ is QR} \\ -1 & \text{if } u \text{ is QNR} \end{cases}$$

we can write the number of solutions to $y^2 = u \pmod{p}$ as $1 + \chi(u)$

- Therefore, we find the size of the group including $\mathcal{O}$ as

$$\begin{aligned} \text{order}(\mathcal{E}) &= 1 + \sum_{x \in \mathrm{GF}(p)} (1 + \chi(x^3 + ax + b)) \\ &= p + 1 + \sum_{x \in \mathrm{GF}(p)} \chi(x^3 + ax + b) \end{aligned}$$

which is a function of $\chi(x^3 + ax + b)$ as x takes values in $\mathrm{GF}(p)$

Hasse Theorem

- As x takes values in GF(p), the value of $\chi(x^3 + ax + b)$ will be equally likely as $+1$ and -1
- This is a random walk where we toss a coin p times, and take either a forward and backward step
- According to the probability theory, the sum $\sum \chi(x^3 + ax + b)$ is of order $\sqrt{p}$
- More precisely, this sum is bounded by $2\sqrt{p}$
- Thus, we have a bound on the order of $\mathcal{E}(a, b, p)$, due to Hasse:

Theorem

The order of an elliptic curve group over GF(p) is bounded by

$$p + 1 - 2\sqrt{p} \leq order(\mathcal{E}) \leq p + 1 + 2\sqrt{p}$$

Order of Elements

- The order of an element P is the smallest integer k such that

$$[k]P = \overbrace{P \oplus P \oplus \cdots \oplus P}^{k \text{ times}} = \mathcal{O}$$

- According to the Lagrange Theorem, the order of any point divides the order of the group
- The primitive element is defined as the element $P \in \mathcal{E}$ whose order $n = \text{order}(P)$ is equal to the group order

$$n = \text{order}(P) = \text{order}(\mathcal{E})$$

- According to the Hasse Theorem, we have

$$p + 1 - 2\sqrt{p} \leq \text{order}(\mathcal{E}(a, b, p)) \leq p + 1 + 2\sqrt{p}$$

Order of Elements

- For the group $\mathcal{E}(1,1,23)$, we have $\lceil\sqrt{23}\rceil = 5$, and the bounds are

  $$14 \leq \text{order}(\mathcal{E}(1,1,23)) \leq 34$$

  Indeed, we found it as $\text{order}(\mathcal{E}(1,1,23)) = 28$
- According to the Lagrange Theorem, the element orders in $\mathcal{E}(1,1,23)$ can only be the divisors of 28 which are $1, 2, 4, 7, 14, 28$
- The order of a primitive element is 28
- The order of $\mathcal{O}$ is 1 since $[1]\mathcal{O} = \mathcal{O}$
- The order $(4,0)$ is 2 since $[2](4,0) = (4,0) \oplus (4,0) = \mathcal{O}$

Order of Elements

- Compute the order of the point $P = (11, 3)$ in $\mathcal{E}(1, 1, 23)$

$$\begin{array}{rcccl} [2]P & = & (11,3) \oplus (11,3) & = & (4,0) \\ [3]P & = & (11,3) \oplus (4,0) & = & (11,20) \quad \leftarrow \end{array}$$

- Note that

$$[3]P = (11, 20) = (11, -3) = -P$$

- This gives

$$[4]P = [3]P \oplus P = (-P) \oplus P = \mathcal{O}$$

- Therefore, the order of $(11, 3)$ is 4

Order of Elements

- Compute the order of the point $P = (1,7)$ in $\mathcal{E}(1,1,23)$

$$\begin{array}{rclcll}
[2]P & = & (1,7) \oplus (1,7) & = & (7,11) & \\
[3]P & = & (1,7) \oplus (7,11) & = & (18,20) & \\
[4]P & = & (7,11) \oplus (7,11) & = & (17,20) & \\
[7]P & = & (18,20) \oplus (17,20) & = & (11,3) & \leftarrow \\
[14]P & = & (11,3) \oplus (11,3) & = & (4,0) & \\
[21]P & = & (11,3) \oplus (4,0) & = & (11,20) & \leftarrow
\end{array}$$

- Since the order of $(1,7)$ is not 2, or 7, or 14, it must be 28
- Indeed $(11,20)$ and $(11,3)$ are negatives of one another

$$[28]P = [7]P \oplus [21]P = (11,3) \oplus (11,-3) = \mathcal{O}$$

- Therefore, the order of $P = (1,7)$ is 28 and $(1,7)$ is primitive

Elliptic Curve Group Order

- One remarkable property of the elliptic curve groups is that the order n can be a prime number, while the multiplicative group $\mathcal{Z}_p^*$ order is always even: $p - 1$
- When the group order is a prime, all elements of the group are primitive elements (except the neutral element $\mathcal{O}$ whose order is 1)
- As a small example, consider $\mathcal{E}(2, 1, 5)$: The equation

  $$y^2 = x^3 + 2x + 1 \pmod{5}$$

  has 6 finite solutions $(0, 1)$, $(0, 4)$, $(1, 2)$, $(1, 3)$, $(3, 2)$, and $(3, 3)$
- Including $\mathcal{O}$, this group has 7 elements, and thus, its order is a prime number and all elements (except $\mathcal{O}$) are primitive

Elliptic Curve Point Multiplication

- The elliptic curve point multiplication operation is the computation of the point $Q = [k]P$ given an integer k and a point on the curve P

$$Q = [k]P = \overbrace{P \oplus P \oplus \cdots \oplus P}^{k \text{ times}}$$

- If the order of the point P is n, we have $[n]P = \mathcal{O}$
- Thus, the computation of $[k]P$ effectively gives

$$[k]P = [k \bmod n]P$$

- Similarly, we have

$$\begin{aligned} [a]P \oplus [b]P &= [a + b \bmod n]P \\ [a][b]P &= [a \cdot b \bmod n]P \end{aligned}$$

Elliptic Curve DLP

- Once we have a primitive element $P \in \mathcal{E}$ whose order n equal to the group order, we can execute the steps of the Diffie-Hellman key exchange algorithm using the elliptic curve group $\mathcal{E}$
- Diffie-Hellman works over any group as long as the DLP in that group is a difficult problem
- The Elliptic Curve DLP is defined as the computation of the integer k given P and Q such that

$$Q = [k]P = \overbrace{P \oplus P \oplus \cdots \oplus P}^{k \text{ times}}$$

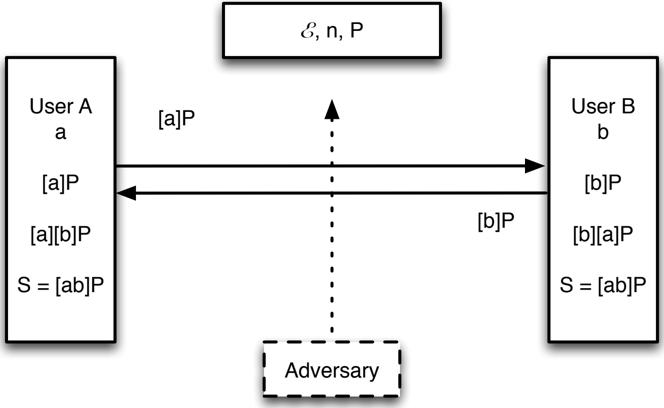
- The ECDLP requires an exhaustive search on the integer k
- No subexponential algorithm for the ECDLP exists as of yet

Elliptic Curve Diffie-Hellman

- A and B agree on the elliptic curve group $\mathcal{E}$ of order n and a primitive element $P \in \mathcal{E}$ (whose order is also n)
- This is done in public: $\mathcal{E}$, n, and P are known to the adversary
- A selects integer $a \in [2, n-1]$, computes $Q = [a]P$, and sends Q to B
- B selects integer $b \in [2, n-1]$, computes $R = [b]P$, and sends R to A
- A receives R, and computes $S = [a]R$
- B receives Q, and computes $S = [b]Q$

$$S = [a]R = [a][b]P = [a \cdot b \bmod n]P$$
$$S = [b]Q = [b][a]P = [b \cdot a \bmod n]P$$

Elliptic Curve Diffie-Hellman



$\mathscr{E}$, n, P

User A
a

[a]P

[a][b]P

S = [ab]P

[a]P

[b]P

User B
b

[b]P

[b][a]P

S = [ab]P

Adversary

DSA vs ECDSA

- The ECDSA is the elliptic curve analogue of the DSA
- The SHA is used to compute the hash of the message: $H(m)$
- Instead of working in a subgroup of order q in $\mathcal{Z}_p^*$, we work in an elliptic curve group $\mathcal{E}(a, b, p)$ which is of order n
- The subgroup order q corresponds to $\mathcal{E}(a, b, p)$ of order n
- The qth root of 1 denoted by g corresponds to the primitive element P of order n in the elliptic curve group
- The private key in DSA is an integer $x < q$ while the private key in ECDSA is also an integer $d < n$
- The public key in DSA is an integer $y < p$ while the public key in ECDSA is Q which is a point on the curve $\mathcal{E}$

DSA vs ECDSA

The correspondence of the variables and operations

Group	$\mathcal{Z}_p^*$	$\mathcal{E}(a,b,p)$
Elements	Integers: $\{1,2,\ldots,p-1\}$	Points $(x,y)\in\mathcal{E}(a,b,p)$
Operation	Multiplication mod p	Point addition $\oplus$ in $\mathcal{E}$
Notation	Elements: g and h Multiplication: $g\cdot h$ Inverse: g^{-1} Division: $g\cdot h^{-1}$ Exponentiation g^a	Elements: P and Q Addition: $P\oplus Q$ Negative: $-P$ Subtraction: $P-Q$ Point multiplication: $[a]P$
DLP	Given $g\in\mathcal{Z}_p^*$ and $h=g^a \pmod{p}$, find a	Given $P\in\mathcal{E}(a,b,p)$ and $Q=[a]P$, find a

ECDSA Setup

- The elliptic curve group $\mathcal{E}(a, b, p)$ with parameters a, b, p
- The order of $\mathcal{E}(a, b, p)$ is either prime n or divisible by prime n
- The primitive element $P \in \mathcal{E}$, which is of order n
- The size of the prime p is 160 or larger
- The size of n is similar to that of p (due to Hasse theorem)
- The private key is a random integer $d \in [2, n-2]$
- The public key is a point on the curve $Q = [d]P$

ECDSA Signing

1. Generate a random integer $r \in [2, n-2]$
2. Compute $[r]P = (x_1, y_1)$
3. Compute the integer $s_1 = x_1 \pmod{n}$
4. If $s_1 = 0$, stop and go to Step 1
5. Compute $r^{-1} \pmod{n}$
6. Compute $s_2 = r^{-1}(H(m) + d \cdot s_1) \pmod{n}$
7. If $s_2 = 0$, stop and go to Step 1
8. The signature on the message m is the pair of integers (s_1, s_2)

ECDSA Verification

1. The verifier receives the message and the signature: $[m, s_1, s_2]$
2. The verifier knows the system parameters and the public key Q
3. The integers s_1, s_2 are in the range $[1, n-1]$
4. Compute $w = s_2^{-1} \pmod{n}$
5. Compute $u_1 = H(m) \cdot w \pmod{n}$
6. Compute $u_2 = s_1 \cdot w \pmod{n}$
7. Compute $[u_1]P \oplus [u_2]Q = (x_2, y_2)$
8. Compute the integer $v = x_2 \pmod{n}$
9. The signature is valid if $v = s_1$

ECDSA Correctness

- The signer computes $s_2 = r^{-1}(H(m) + d \cdot s_1) \pmod{n}$, which gives

$$
\begin{aligned}
r &= s_2^{-1} \cdot (H(m) + d \cdot s_1) \pmod{n} \\
&= H(m) \cdot s_2^{-1} + d \cdot s_1 \cdot s_2^{-1} \pmod{n} \\
&= H(m) \cdot w + d \cdot s_1 \cdot w \pmod{n} \\
r[P] &= [H(m) \cdot w + d \cdot s_1 \cdot w]P \\
&= [H(m) \cdot w]P \oplus [s_1 \cdot w][d]P \\
&= [u_1]P \oplus [u_2]Q \\
&= (x_2, y_2) \\
v &= x_2 \pmod{n}
\end{aligned}
$$

- The signer computes $r[P] = (x_1, y_1)$, which gives $s_1 = x_1 \pmod{n}$
- The equality of $v = s_1$ indeed verifies the signature

ECIES: Elliptic Curve Integrated Encryption Scheme

- The standard ECC encryption algorithm
- It works like the static Diffie-Hellman algorithm
- It employs a block cipher

ECIES Setup

- A block cipher $E_k(\cdot)$ and $D_k(\cdot)$
- Key space K_1

- A MAC function MAC_k
- Key space K_2

- A key derivation function V will map group elements to the key spaces K_1 and K_2

ECIES Key Generation

- $d \in \{1, 2, \ldots p - 1\}$
- $Q = [d]P$

- d is the private key of the User
- P is the generator of the elliptic curve group
- Q is the public key of the User

ECIES Encryption

- Generate a random number $r \in \{1, 2, \ldots p-1\}$
- $U = [r]P$
- $T = [r]Q$
- $(k_1, k_2) = V(T)$
- $C = E_{k_1}(M)$
- $D = MAC_{k_2}(C)$
- Send $U \mid\mid C \mid\mid D$

- The ciphertext: U, C, D
- U is used for key agreement
- C is the actual encrypted text

ECIES Decryption

- Receive and parse $U \mid\mid C \mid\mid D$ to obtain U, C, and D
- $T = [d]U$
- $(k_1, k_2) = V(T)$
- If $D \neq MAC_{k_2}(C)$ then return Invalid
- $M = D_{k_1}(C)$
- Return M

- ECIES makes it easy to encrypt long messages
- Standardized by several institutions: ANSI X9.63, IEEE P1363