Unit-3 - CCS

Elliptic Curve Arithmetic

Abelian Group

set of elements with a binary operation, denoted by $\cdot$, that associates to each ordered pair (a, b) of elements in G an element $(a \cdot b)$ in G, such that the following axioms are obeyed:[3]

(A1) Closure: If a and b belong to G, then $a \cdot b$ is also in G.

(A2) Associative: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all a, b, c in G.

(A3) Identity element: There is an element e in G such that $a \cdot \mathrm{e} = \mathrm{e} \cdot a = a$ for all a in G.

(A4) Inverse element: For each a in G there is an element a' in G such that $a \cdot a' = a' \cdot a = \mathrm{e}$.

(A5) Commutative: $a \cdot b = b \cdot a$ for all a, b in G.

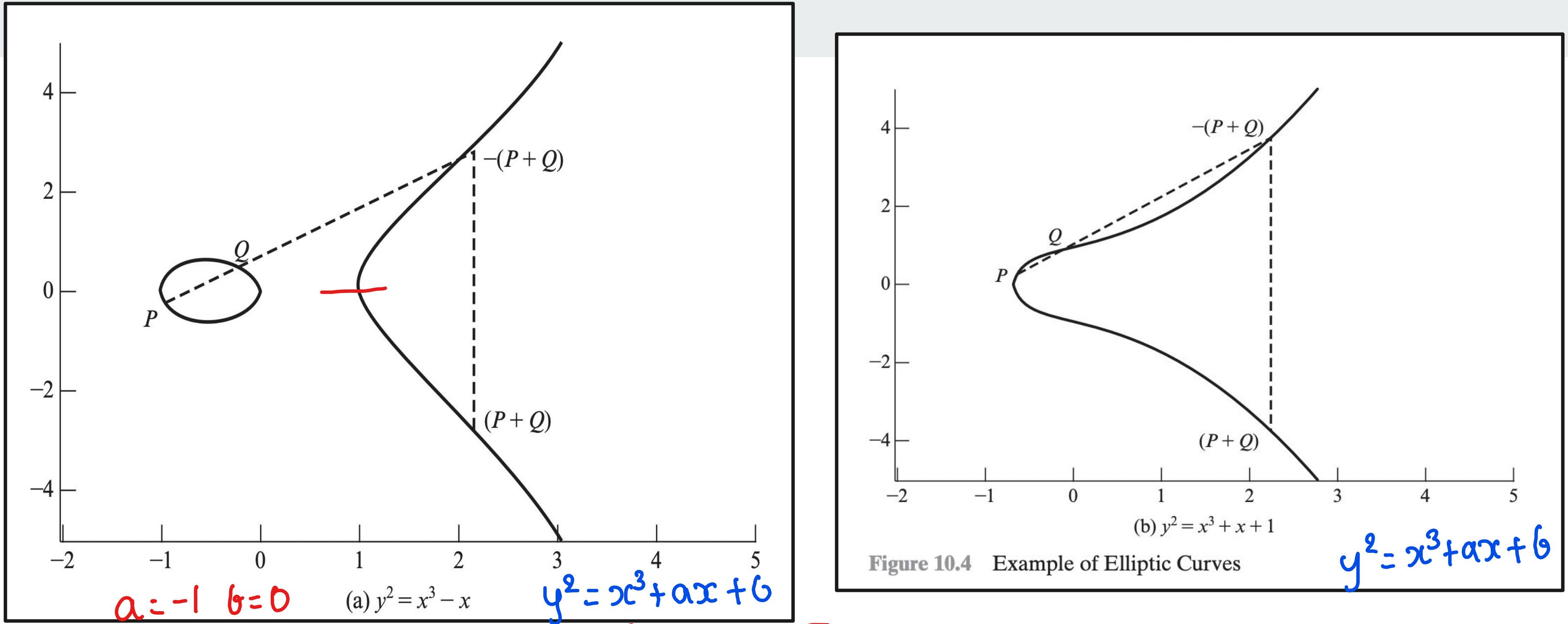
What is Elliptic Curve?

- An elliptic curve is defined by an equation in two variables with coefficients. For cryptography, the variables and coefficients are restricted to elements in a finite field, which results in the definition of a finite abelian group

Elliptic Curves over Real Numbers

$$\boxed{y^2 = x^3 + ax + b}$$

- Such equations are said to be cubic, or of degree 3, because the highest exponent they contain is a 3.
- Single element denoted O and called the point at infinity or the zero point. If three points on an elliptic curve lie on a straight line, their sum is O.
- For given values of a and b, the plot consists of positive and negative values of y for each value of x. Thus, each curve is symmetric about y = 0



(a) $y^2 = x^3 - x$

(b) $y^2 = x^3 + x + 1$

Figure 10.4 Example of Elliptic Curves

$y^2 = 27 - 3$ $y^2 = 24$ $y = \sqrt{24}$

Geometric Description of Addition It can be shown that a group can be defined based on the set E(*a*, *b*) for specific values of *a* and *b* in Equation (10.1), provided the following condition is met:

$$4a^3 + 27b^2 \neq 0 \tag{10.2}$$

Rules of Addition over Elliptic Curve

1. O serves as the additive identity.
   a. Thus **O = -O**; for any point P on the elliptic curve, **P + O = P**. In what follows, we assume P ≠ O and Q ≠ O.
2. The negative of a point P is the point with the same x coordinate but the negative of the y coordinate; that is,
   a. if **P = (x, y), then -P = (x, -y).** Note that these two points can be joined by a vertical line.
   b. Note that **P + (-P) = P - P = O.**
3. To add two points P and Q with different x coordinates, draw a straight line between them and find the third point of intersection R.
   a. To form a group structure, we need to define addition on these three points: P + Q = -R. That is, we define P + Q to be the mirror image (with respect to the x axis) of the third point of intersection.
4. The geometric interpretation of the preceding item also applies to two points, P and -P, with the same x coordinate. The points are joined by a vertical line, which can be viewed as also intersecting the curve at the infinity point. We therefore have **P + (-P) = O**, which is consistent with item (2).
5. To double a point Q, draw the tangent line and find the other point of intersection S.

Then Q + Q = 2Q = -S.

P(4,8)
-P(4,-8)

Algebraic Description of Addition

$R(x_R, y_R)$

ALGEBRAIC DESCRIPTION OF ADDITION In this subsection, we present some results that enable calculation of additions over elliptic curves.[5] For two distinct points, $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, that are not negatives of each other, the slope of the line l that joins them is $\Delta = (y_Q - y_P)/(x_Q - x_P)$. There is exactly one other point where l intersects the elliptic curve, and that is the negative of the sum of P and Q. After some algebraic manipulation, we can express the sum $R = P + Q$ as

$P+Q$

$$\begin{cases} x_R = \Delta^2 - x_P - x_Q \\ y_R = -y_P + \Delta(x_P - x_R) \end{cases} \tag{10.3}$$

We also need to be able to add a point to itself: $P + P = 2P = R$. When $y_P \neq 0$, the expressions are

$P+P$

$$\begin{cases} x_R = \left(\dfrac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P \\ y_R = \left(\dfrac{3x_P^2 + a}{2y_P}\right)(x_P - x_R) - y_P \end{cases} \tag{10.4}$$


thank you


LIKE
COMMENT
SHARE
SUBSCRIBE

Elliptic Curves over Z^p

$$y^2 \bmod p = (x^3 + ax + b) \bmod p \tag{10.5}$$

For example, Equation (10.5) is satisfied for $a = 1, b = 1, x = 9, y = 7, p = 23$:

$$\begin{aligned} 7^2 \bmod 23 &= (9^3 + 9 + 1) \bmod 23 \\ 49 \bmod 23 &= 739 \bmod 23 \\ 3 &= 3 \end{aligned}$$

let $p = 23$ and consider the elliptic curve $y^2 = x^3 + x + 1$.

a=1 b=1

1. P + O = P.

2. If P = (x_p, y_p) then -P = $(x_p, -y_p)$ implies P+(-P) =O

3. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ with $P \neq -Q$, then $R = P + Q = (x_R, y_R)$ is determined by the following rules:

$$x_R = (\lambda^2 - x_P - x_Q) \bmod p$$
$$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$$

where

$$\lambda = \begin{cases} \left(\frac{y_Q - y_P}{x_Q - x_P}\right) \bmod p & \text{if } P \neq Q \\ \left(\frac{3x_P^2 + a}{2y_P}\right) \bmod p & \text{if } P = Q \end{cases}$$

For example, let $P = (3, 10)$ and $Q = (9, 7)$ in $E_{23}(1, 1)$. Then

$$\lambda = \left(\frac{7 - 10}{9 - 3}\right) \bmod 23 = \left(\frac{-3}{6}\right) \bmod 23 = \left(\frac{-1}{2}\right) \bmod 23 = 11$$
$$x_R = (11^2 - 3 - 9) \bmod 23 = 109 \bmod 23 = 17$$
$$y_R = (11(3 - 17) - 10) \bmod 23 = -164 \bmod 23 = 20$$

So $P + Q = (17, 20)$. To find $2P$,

2) P+P

$$\lambda = \left(\frac{3(3^2) + 1}{2 \times 10}\right) \bmod 23 = \left(\frac{5}{20}\right) \bmod 23 = \left(\frac{1}{4}\right) \bmod 23 = 6$$

$$x_R = (6^2 - 3 - 3) \bmod 23 = 30 \bmod 23 = 7$$
$$y_R = (6(3 - 7) - 10) \bmod 23 = (-34) \bmod 23 = 12$$

and $2P = (7, 12)$.

4. Multiplication is defined as repeated addition; for example, $4P =$
4P= $P + P + P + P$.

Elliptic Curves over GF(2^m)

1. $P + O = P$.
2. If $P = (x_P, y_P)$, then $P + (x_P, x_P + y_P) = O$. The point $(x_P, x_P + y_P)$ is the negative of P, which is denoted as $-P$.

   $x_P, -y_P$
3. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ with $P \neq -Q$ and $P \neq Q$, then $R = P + Q = (x_R, y_R)$ is determined by the following rules:

$$x_R = \lambda^2 + \lambda + x_P + x_Q + a$$
$$y_R = \lambda(x_P + x_R) + x_R + y_P$$

where

$$\lambda = \frac{y_Q + y_P}{x_Q + x_P}$$

4. If $P = (x_P, y_P)$ then $R = 2P = (x_R, y_R)$ is determined by the following rules:

$$x_R = \lambda^2 + \lambda + a$$
$$y_R = x_P^2 + (\lambda + 1)x_R$$

where

$$\lambda = x_P + \frac{y_P}{x_P}$$


thank you


LIKE
COMMENT
SHARE
SUBSCRIBE

ECC- Diffie Hellman

Global Public Elements	
$E_q(a, b)$	elliptic curve with parameters a, b, 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

User A Key Generation	
Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$

User B Key Generation	
Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$

Calculation of Secret Key by User A

$K = n_A \times P_B$

Calculation of Secret Key by User B

$K = n_B \times P_A$

Figure 10.7 ECC Diffie–Hellman Key Exchange

Encryption and Decryption

To encrypt and send a message P_m to B, A chooses a random positive integer k and produces the ciphertext C_m consisting of the pair of points:

$$C_m = \{kG, P_m + kP_B\}$$

Note that A has used B's public key P_B. To decrypt the ciphertext, B multiplies the first point in the pair by B's private key and subtracts the result from the second point:

$$P_m + kP_B - n_B(kG) = P_m + k(n_BG) - n_B(kG) = P_m$$

Security in ECC

The security of ECC depends on how difficult it is to determine k given kP and P. This is referred to as the elliptic curve logarithm problem. The fastest known technique for taking the elliptic curve logarithm is known as the Pollard rho method.

Table 10.3 Comparable Key Sizes in Terms of Computational Effort for Cryptanalysis (NIST SP-800-57)

Symmetric Key Algorithms	Diffie–Hellman, Digital Signature Algorithm	RSA (size of n in bits)	ECC (modulus size in bits)
80	$L = 1024$ $N = 160$	1024	160–223
112	$L = 2048$ $N = 224$	2048	224–255
128	$L = 3072$ $N = 256$	3072	256–383
192	$L = 7680$ $N = 384$	7680	384–511
256	$L = 15{,}360$ $N = 512$	15,360	512+

Note: L = size of public key, N = size of private key.

Elliptic Curve Cryptography - Key Points

Analog of Diffie Hellman

1. Key exchange using elliptic curves can be done in the following manner. First pick a large integer q, which is either a prime number p or an integer of the form 2^m and elliptic curve parameters a and b. This defines the elliptic group of points $E^q(a, b)$.
2. Next, pick a base point $G = (x_1, y_1)$ in $E_p(a, b)$ whose order is a very large value n.
3. The order n of a point G on an elliptic curve is the smallest positive integer n such that nG = 0 and G are parameters of the cryptosystem known to all participants.

A key exchange between users A and B can be accomplished as follows (Figure 10.7).

1. A selects an integer n_A less than n. This is A's private key. A then generates a public key $P_A = n_A \times G$; the public key is a point in $E_q(a, b)$.
2. B similarly selects a private key n_B and computes a public key P_B.
3. A generates the secret key $k = n_A \times P_B$. B generates the secret key $k = n_B \times P_A$.

The two calculations in step 3 produce the same result because

$$n_A \times P_B = n_A \times (n_B \times G) = n_B \times (n_A \times G) = n_B \times P_A$$

Example - Using Properties of Addition in ECC

As an example,[6] take $p = 211$; $E_p(0, -4)$, which is equivalent to the curve $y^2 = x^3 - 4$; and $G = (2, 2)$. One can calculate that $240G = O$. A's private key is $n_A = 121$, so A's public key is $P_A = 121(2, 2) = (115, 48)$. B's private key is $n_B = 203$, so B's public key is $203(2, 3) = (130, 203)$. The shared secret key is $121(130, 203) = 203(115, 48) = (161, 69)$.


thank you


LIKE
COMMENT
SHARE
SUBSCRIBE