Asymmetric key crypto: ECC

2019. 3. 25

Contents

Generalized Discrete Logarithm Problem

Def:
Given a finite cyclic group G and group operator ☺ and cardinality n, the DL problem is to find the integer x such that

$$a^x = \underbrace{a ☺ a ☺ a ☺ a ☺ \ldots ☺ a}_{x \text{ times}} = b$$

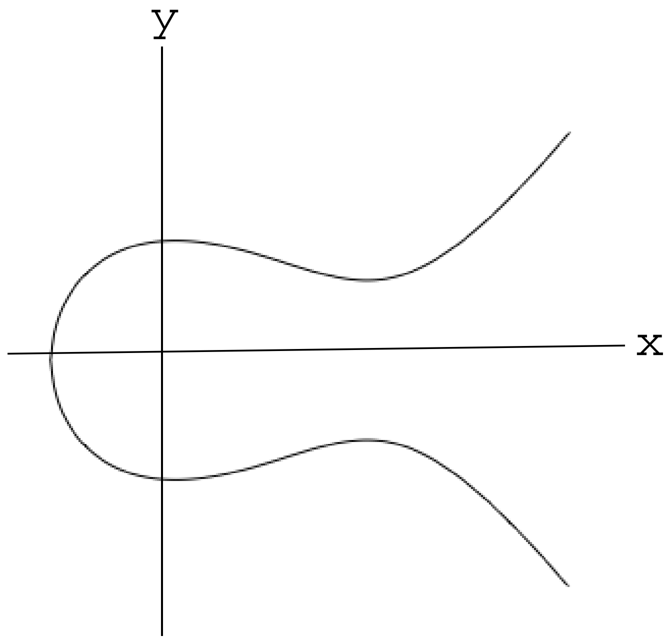
where a∈G is a primitive element and b∈G, 1 ≤x≤n.

What is an Elliptic Curve?

- An elliptic curve E is the graph of an equation of the form

  $y^2 = x^3 + ax + b$ where $a, b \in Z_p$
- Also includes a “(imaginary) point at infinity”
- And the condition $4a^3 + 27b^2 \neq 0 \mod p$
- What do elliptic curves look like?

Examples of EC graphs



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

Operations on EC

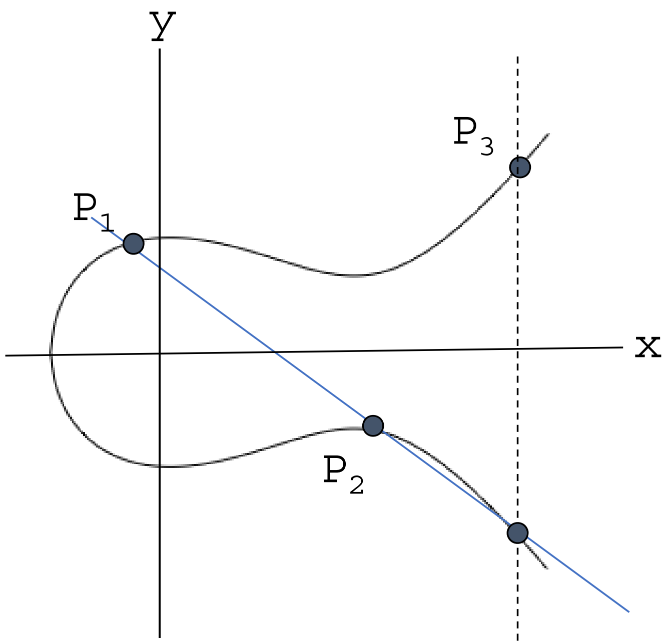
Define the Point Addition operation such that

$$P_3 \equiv P_1 + P_2$$
$$(x_3,y_3) \equiv (x_1,y_1) + (x_2, y_2)$$

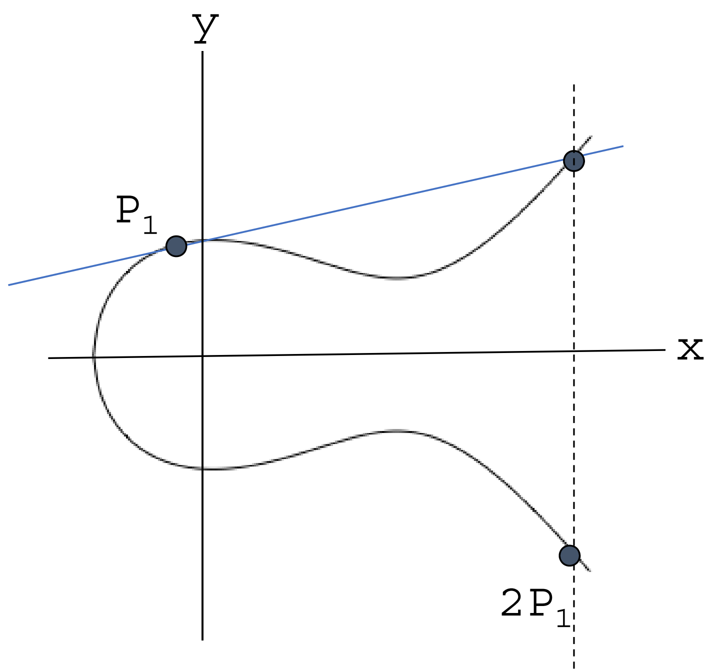
(note: point addition operation in not a vector operation)

Geometric interpretation of operation

$P_3 \equiv P_1 + P_2$



$2P_1 \equiv P_1 + P_1$



Analytical expression for operation

Given a EC, $y^2 = x^3+ax+b$, $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_3=(x_3, y_3)$=?

Assume that the equation of a line passing through P_1 and P_2,

$$y = mx+c$$

Then, $(mx+c)^2 = x^3+ax+b \rightarrow$ 3 solutions: P_1 , P_2, and $P_3=(x_3, y_3)$

$$x_3 = m^2 - x_1 - x_2 \bmod p,$$

$$y_3 = m(x_1 - x_3) - y_1 \bmod p$$

$$\text{where } m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \bmod p & \text{; if } P \neq Q \text{ (point addition)} \\ \dfrac{3x_1^2 + a}{2y_1} \bmod p & \text{; if } P = Q \text{ (point doubling)} \end{cases}$$

Identity element

We define a "point of infinity", **∞** as

$P + \infty = P$ for all P on EC

We define the inverse –P as

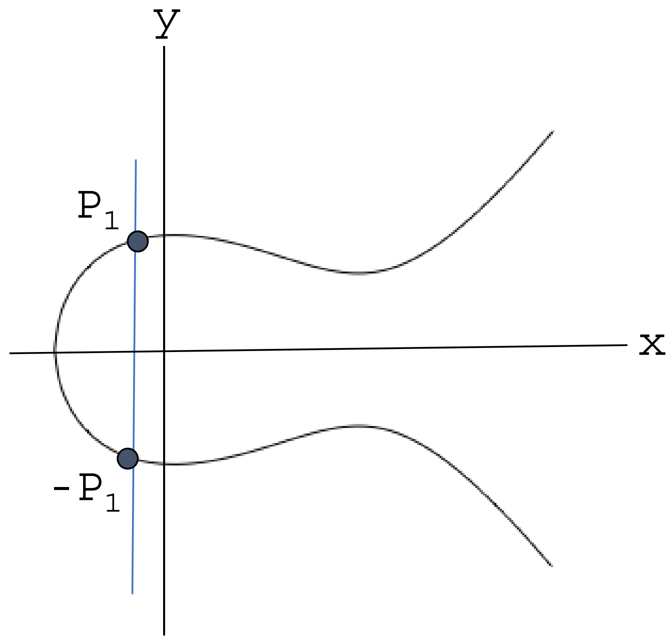
$P + (-P) = \infty$ for all p on EC

What is the graphic interpretation of **∞?**

How do we find –P?

-P of P=(x, y) is (x,-y).

-P of $P=(x_p, x_p) = (x_p, p-x_p)$ on EC over prime field



Example

Given a EC, $y^2 = x^3+2x+2 \bmod 7$, and $P=(5,1)$

Cyclic Group

Suppose the following EC: $y^2 = x^3+2x+2 \mod 17$, and a primitive point(generator) P=(5,1)

2P = P + P = (5,1) + (5,1) = (6,3)
3p = 2p + P = (10,6)
4p = (3,1)
5P = (9,16)
6P = (16,13)
7P = (0,6)
8P = (13,7)
9P = (7,6)
10P = (7,11)
11P = (13,10)
12p = (0,11)
13p = (16,4)
14P = (9,1)
15P = (3,16)
16P = (10,11)
17P = (6,14)
18P = (5,16)
19P = ∞
20P = (5,1)=P

These points on EC has the cyclic group of the order |E|=19.

(source: Understanding Cryptography)

EC Discrete Logarithm Problem

- Given an EC, we consider a primitive element P and another point Q on the curve. The EC DL problem is to find the integer x, where $1 \leq x \leq |E|$, such that

$$\underbrace{P + P + P + \ldots + P}_{x \text{ times}} = x \cdot P = Q$$

Complexity of computation: # of points on and EC

- How can many points be on an arbitrary EC?
- Hasse's Theorem
  - Given an elliptic curve modulo *p*, the number of points on the curve is bounded by

$$p+1-2\sqrt{p} \leq |E| \leq p+1+2\sqrt{p}$$

So, the number of point is close to *p*.
To generate a curve with about 2^{160} points, a prime number with a length of about 160 bits is required.

EC DH Key Exchange and Encryption

Alice 

$E: y^2 = x^3+ax+b \bmod p$, $G= (x_p, y_p)$

Bob 

Select $a \in \{2,3,\ldots,|E|\}$
(private to Alice)
Compute $A= aG =(x_A, y_A)$

Select $b \in \{2,3,\ldots,|E|\}$
(private to Bob)
Compute $B= bG =(x_B, y_B)$

A →

← B

$K_{AB}= aB = abG = (x_{AB}, y_{AB})$

$K_{AB} = bA=abG =(x_{AB}, y_{AB})$

Message m
Encrypt: $x=E_{K_{AB}}(m)$

x →

Decrypt: $m=D_{K_{AB}}(x)$

Example

Alice 

$E: y^2 = x^3+2x+2 \mod 17$, $G= (5, 1)$

Bob 

Select $3 \in \{2,3,\ldots,19\}$
(private to Alice)
Compute $A= 3G =(10, 6)$

Select $10 \in \{2,3,\ldots,19\}$
(private to Bob)
Compute $B= 10G =(7, 11)$

(10,6) →

← (7,11)

$K_{AB} = 3(7,11) = (13, 10)$

$K_{AB} = 10(10,6)=(13, 10)$

Message m
Encrypt: $x=E_{K_{AB}}(m)$

x →

Decrypt: $m=D_{K_{AB}}(x)$

ECC security

- ECDLP is considerably strong against the attacks which work to DLP or the factoring algorithm.
- The currently known attack requires the step of roughly square root of the group cardinality.
- So, by Hasse's theorem, p should be chosen with 160 bits (roughly 2^{160} points on the curve). Then 2^{80} steps are required by an attacker.
- This security can be achieved only if cryptographically strong ECs are used.
- There are the standardized curves by the government organizations.

ECC usefulness

- ECC is not restricted to be used for DH key exchange.
- Almost all other discrete logarithm protocols, such as digital signature, encryption, can utilize ECC.
- ECC slowly becomes popular on many applications, especially on embedded platforms such as mobile devices.

Comparison of security level

Algorithm family	crypto	Security level(bits)			
Integer factoring	RSA	1024	3072	7680	15360
Discrete logarithm	DH, DSA, Elgamal	1024	3072	7680	15360
Elliptic curve	ECDH, ECDSA	160	256	384	512
Symm key	AES, 3DES	80	128	192	256