Elliptic Curve Cryptography

28 November 2019 17:32

Can we find another cyclic group in which the DLP is difficult? Ideally more difficult than in $\mathbb{Z}_p^*$?

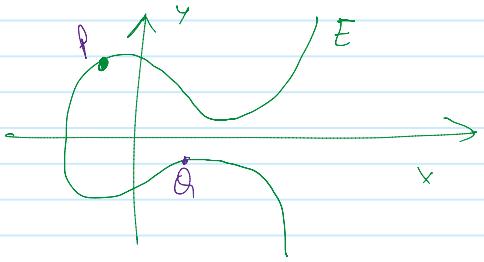
for use in crypto we need to consider polynomials over $\mathbb{Z}_p$.

DEFINITION → The EC over $\mathbb{Z}_p$, $p > 3$ is the set of all pairs $(x, y) \in \mathbb{Z}_p$:

$$y^2 = x^3 + ax + b \bmod p$$

together w/ an imaginary point at infinity $\mathcal{O}$, where $a, b \in \mathbb{Z}_p$ for $4a^3 + 27b^2 \neq 0 \bmod p$

eg: $y^2 = x^3 - 3x + 3$ over $\mathbb{R}$



Note: symmetry wrt to x axis

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

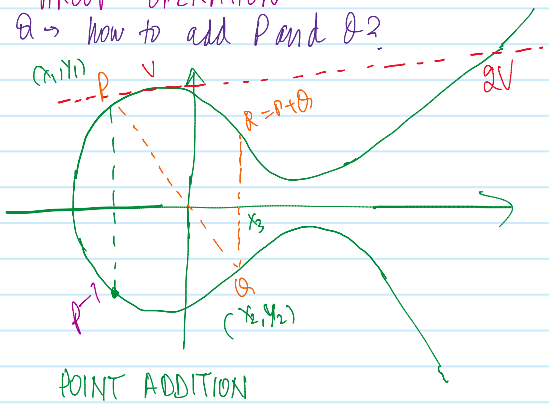
$$y = \pm\sqrt{x^3 + ax + b}$$

for a DLP we need a cyclic group. For a group we need

(a) a set of elements
(b) a group operation that fulfills the group laws

GROUP OPERATION

Q → how to add P and Q?



POINT ADDITION

$P + Q = R$

POINT DOUBLING ?

ELLIPTIC CURVE LOGARITHMIC PROBLEM

We obtain immediately a discrete logarithmic problem :-

Definition 9.2.1 Elliptic Curved Discrete Logarithm Problem (ECDLP)

Given is an elliptic curve E. We consider a primitive element P and another element T. The DL problem is finding the integer d, where $1 \leq d \leq \#E$, such that:

$$\underbrace{P + P + \cdots + P}_{d \text{ times}} = dP = T. \quad (9.2)$$

(no of hops I made on the curve to get from starting point P to end at T.)

eg: $P = (5,1)$ generator

$T = (16,4) = dP.$

i.e. $(16,4) = d(2,5)$ d ?

This is NOT EASY TO FIND.

Notes: (1) the ECDLP $d\ (= k_{pr})$ is an integer but $T = (k_{pub})$ is point on curve i.e. a group element.

Q: group cardinality of E ??

Theorem 9.2.2 Hasse's theorem

Given an elliptic curve E modulo p, the number of points on the curve is denoted by #E and is bounded by:

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

Finding exact #E is computationally difficult.

All EC protocols rely on the hardness of the ECDLP

If the EC is choosen carefully, the best known algorithm for computing the ECDLP requires $\approx \sqrt{p}$ steps.

EC DIFFIE-HELLMAN KEY EXCHANGE (ECDH)

→ straightforward application of DH in $\mathbb{Z}_p$.

I Phase set up :

E $y^2 \equiv x^3 + ax + b \bmod p$

primitive element $P = (x_p, y_p)$

II Phase - Protocol

ALICE $\xleftarrow{E, p}$ BOB

$a = k_{pr,A} \in \{2, 3, \ldots, \#E - 1\}$ $\quad b = k_{pr,B} \in \{2, 3, \ldots$

$P+Q=R$

POINT DOUBLING ?
i.e. what is $V+V=2V$

Q → Analytical expression for the group operation?

Idea: Given $E: y^2 \equiv x^3+ax+b$,
$P=(x_1,y_1)$, $Q=(x_2,y_2)$.

1) Find the line PQ:
let say $y = Sx + M$
then "$l = E$"
$(Sx+M)^2 = x^3+ax+b$
degree 3 ⇒ 3 solutions,
but we already have 2 solutions namely X_1, X_2.

Elliptic Curve Point Addition and Point Doubling

$$x_3 = s^2 - x_1 - x_2 \bmod p$$
$$y_3 = s(x_1 - x_3) - y_1 \bmod p$$

where $(y_2-y_1)(x_2-x_1)^{-1}$ ← from extended euclidean algorithm (!)

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

Q: as per the group laws, what is the NEUTRAL ELEMENT.
$P + Z = P \quad \forall P$

we define a "point at infinity" $\mathcal{O}$
property 3 of DEF 4.37
$P+Q = P \quad \forall P \in E$

property 4 → $P+(-P) = \mathcal{O}$
⇒ $-P$ of $P=(x,y)$ is by definition
$-P \equiv (x,-y)$
↙ the INVERSE wrt MINUS of group operation
↘ the MINUS we know (just mod p)

example:
$E: y^2 \equiv x^3+2x+2 \bmod 17$
we want to double $P=(5,1)$
$2P = P+P = (5,1)+(5,1) = (x_3,y_3)$
$S = \frac{3x_1^2+a}{2y_1} = (2\cdot 1)^{-1}(3\cdot 5^2+2) \pmod{17}$
$= 2^{-1}\cdot 9 \bmod 17$
$= 9\cdot 9 \bmod 17$
$= 13$
$x_3 = S^2 - x_1 - x_2 = 13^2 - 5 - 5 \bmod 17$
$= 159 \bmod 17$

ALICE $\quad a \in_R \{2,3,\dots,\#E-1\}$ $\quad A = K_{pubA} = a\cdot P = (x_A, y_A)$

BOB $\quad b = k_{PR,B} \in \{2,3,\dots,\#E-1\}$ $\quad B = K_{pubB} = bP = (x_B, y_B)$

A → $\quad aB = (x_{AB}, y_{AB})$ ← B $\quad bA = (x_{AB}, y_{AB})$

USECASE:
message M:
$AES_{x_{AB}}(M)$ —C→ $AES^{-1}_{x_{AB}}(C)$

proof of correctness:

Alice computes:
$a\cdot B = a(bP) = abP$
Bob computes:
$bA = b(aP) = abP$

Alice		Bob
choose $a = k_{prA} = 3$		choose $b = k_{prB} = 10$
$A = k_{pubA} = 3P = (10,6)$	A →	$B = k_{pubB} = 10P = (7,11)$
	← B	
$T_{AB} = aB = 3(7,11) = (13,10)$		$T_{AB} = bA = 10(10,6) = (13,10)$

Q → how to compute aP i.e. $P+P+P\dots+P$ (a times)

LEFT TO RIGHT →

eg: $26P = (11010)_2 P$
Step:

∅	$P = 1_2 P$		
1_A	$P+P = 2P = 10_2 P$	D	
1_B	$2P+P = 3P = 11_2 P$	A	
2_A	$3P+3P = 6P = 110_2 P$	D	
3_A	$6P+6P = 12P = 1100_2 P$	D	
3_B	$12P+P = 13P = 1101_2 P$	A	
4_A	$13P+13P = 11010_2 P$	D	

✓

$= 13$

$x_3 = s^2 - x_1 - x_2 = 13^2 - 5 - 5 \bmod 17$
$= 159 \bmod 17$
$= 6 \bmod 17$

$y_3 = s(x_1 - x_3) - y_1 = 13(5-6) - 1$
$= -14 \bmod 17$
$\equiv 3 \bmod 17$

check: $(6,3)$ lies on the curve

The points on an elliptic curve including $\mathcal{O}$, have CYCLIC SUBGROUPS. under certain conditions all points on EC form a CYCLIC GROUP.

Example 9.5. We want to find all points on the curve:

$$E : y^2 \equiv x^3 + 2 \cdot x + 2 \bmod 17.$$

this is a cyclic group. this is NOT ALWAYS TRUE

It happens that all points on the curve form a cyclic group and that the order is $\#E = 19$. For this specific curve the group order is a prime and, according to Theorem 8.2.4, every element is primitive.

As in the previous example we start with the primitive element $P = (5,1)$. We compute now all "powers" of P. More precisely, since the group operation is addition, we compute $P, 2P, \ldots, (\#E)P$. Here is a list of the elements that we obtain:

$2P = (5,1) + (5,1) = (6,3)$
$3P = 2P + P = (10,6)$
$4P = (3,1)$
$5P = (9,16)$
$6P = (16,13)$
$7P = (0,6)$
$8P = (13,7)$
$9P = (7,6)$
$10P = (7,11)$
$11P = (13,10)$
$12P = (0,11)$
$13P = (16,4)$
$14P = (9,1)$
$15P = (3,16)$
$16P = (10,11)$
$17P = (6,14)$
$18P = (5,16)$
$19P = \mathcal{O}$

the INFINITY POINT

From now on, the cyclic structure becomes visible since:

$$20P = 19P + P = \mathcal{O} + P = P$$
$$21P = 2P$$
$$\vdots$$

It is also instructive to look at the last computation above, which yielded:

$$18P + P = \mathcal{O}.$$