



# Elliptic Curve Cryptography, Part 1

Cryptography, Autumn 2021

---

Lecturers: J. Daemen, B. Mennink

November 30, 2021

Institute for Computing and Information Sciences  
Radboud University

Some motivation for ECC

Prime fields

Elliptic curve groups

## Some motivation for ECC

---

# Diffie-Hellman key exchange (1976)

$q = 1606938044258990275541962092341162602522202993782792835301301$

$g = 123456789$



$g^a \bmod q = 78467374529422653579754596319852702575499692980085777948593$

$560048104293218128667441021342483133802626271394299410128798 = g^b \bmod q$



$a =$   
685408003627063  
761059275919665  
781694368639459  
527871881531452

$b =$   
362059131912941  
987637880257325  
269696682836735  
524942246807440

$g^{ab} \bmod q = 437452857085801785219961443000845969831329749878767465041215$

Size of field prime  $p$  (called  $q$  in this figure) and  $\text{ord}(g)$  chosen to offer safety margin with respect to the best discrete log algorithms in 1976

# Diffie-Hellman key exchange (2021)

$$q =$$

$$g = 123456789$$

$$g^a \pmod{q}$$

9749664881271932862610481425597391097799762535760048014799487575456670542185781051331821479206905991067606799976  
 854666859540340934637356245103973929667618840424914816827503426022062467044507707726324368211747246128321956  
 5376315202786494366479736196739396739672818671783836042887358954210564305876614615372780217824375642623001423055196  
 9749646503202861861149557401474638545716624401013947442701505569477663721859303325537983917887502752814212655951639  
 605423241268749717778343860669272064707120665821062665886173047461661156530808488964787747266127073866961529476714559  
 3042221414714898256600612419571562251002200239142814878080117814763455044564728671394409401857871021855500379131

$$\equiv g^b \pmod{q}$$

$$q =$$

$$q^{ab} =$$

$$b =$$

Size of field prime  $p$  (called  $q$  in this figure) and  $\text{ord}(g)$  chosen to offer safety margin with respect to the best discrete log algorithms in 2021

Security degenerated due to Moore's law but mostly a DL solving method called *index calculus* (out of scope of this introductory course)

# Looking for alternatives

- ▶ For groups  $\langle g \rangle \subset (\mathbb{Z}/p\mathbb{Z})^*$  index calculus forced  $p$  to grow from hundreds to thousands of bits
  - ... and with it public keys, cryptograms and signatures
  - computational effort of  $g^a$  is quadratic in length of  $p$  for fixed  $a$
- ▶ Mid-eighties: effort to find other cyclic groups where DL is hard and
  - public keys, cryptograms and signatures are short
  - exponentiation (or equivalent) is much lighter
- ▶ Natural candidate: algebraic groups
  - elements: points in some space with coordinates in some *field*
  - group law: polynomial expression on the coordinates
  - finite: if the field is finite (see later)
- ▶ Simplest case, points  $(x, y)$  on a *curve*
  - degree 1:  $ax + by = c$ , ... too simple
  - degree 2:  $ax^2 + bxy + cy^2 + dx + ey + f = 0$ , ... too simple
  - degree 3: aha, here we have something: elliptic curves!

# ECDH: Elliptic Curve Diffie-Hellman (1999-now)

$$p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$$

$p = 115792089210356248762697446949407573530086143415290314195533631308867097853951$

$$E/\mathbb{F}_p: y^2 = x^3 - 3x + b$$

$\#E = 11579208921035624876269744694940757352999695522413576034242259061068512044369$

$P = (48439561293906451759052585252797914202762949526041747995844080717082404635286, 36134250956749795798585127919587881956611106672985015071877198253568414405109)$



$a =$

89130644591246033577639  
77064146285502314502849  
28352556031837219223173  
24614395

$[a]P = (84116208261315898167593067868200525612344221886333785331584793435449501658416, 102885655542185598026739250172885300109680266058548048621945393128043427650740)$

$[b]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383, 77887418190304022994116595034556257760807185615679689372138134363978498341594)$

$[ab]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383, 77887418190304022994116595034556257760807185615679689372138134363978498341594)$



$b =$

10095557463932786418806  
93831619070803277191091  
90584053916797810821934  
05190826

$\langle G \rangle \subset \mathcal{E}$  with elliptic curve group  $\mathcal{E}$  and  $\text{ord}(G)$  chosen to offer safety margin against best DL attacks in 1999 and actually still today

Neal Koblitz and Victor Miller each proposed EC crypto in 1985

EC crypto is the subject of this and next lecture

## Prime fields

---



- ▶ We consider a set and two operations: addition and multiplication
- ▶ For example  $(\mathbb{Z}, +, \times)$
- ▶  $(\mathbb{Z}, +)$  is a group
- ▶  $(\mathbb{Z}, \times)$  satisfies:
  - closed
  - associative
  - has neutral element: 1
- ▶ Additional property:  $\times$  is distributive with respect to  $+$   
 $\forall a, b, c \in A : \quad a(b + c) = ab + ac$   
 $(b + c)a = ba + ca$
- ▶ We call this a **ring**
- ▶ But we are interested in finite sets
- ▶  $(\mathbb{Z}/n\mathbb{Z}, +, \times)$  forms a ring with  $n$  elements

- ▶ Consider  $(\mathbb{Z}/p\mathbb{Z}, +, \times)$  with  $p$  a prime
  - $(\mathbb{Z}/p\mathbb{Z}, +)$  is a group
  - $((\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}, \times)$  is a group
  - $\times$  is distributive with respect to  $+$
- ▶ This is called a **finite field**, denoted as  $\mathbb{F}_p$  (or as  $\text{GF}(p)$ )
- ▶ Properties of  $\mathbb{F}_p$ 
  - additive group has order  $p$
  - multiplicative group has order  $p - 1$
  - there is exactly one finite field per prime
- ▶ For information: there is a field for every prime power  $p^n$  but we do not treat the case  $n > 1$  in this course

# Elliptic curve groups

---

*An elliptic curve is a set of points on a curve of genus 1 [for info only]*

- ▶ Coordinates are elements of a field, finite when used for crypto
- ▶ In this course, we limit to fields  $\mathbb{F}_p$  with  $p$  a large prime
- ▶ There are many ways to represent an elliptic curve
- ▶ The representation has an impact on the computation
- ▶ Some representations are restricted to certain classes of curves

Most widespread for curves over  $\mathbb{F}_p$ : set of points  $(x, y)$  that satisfy

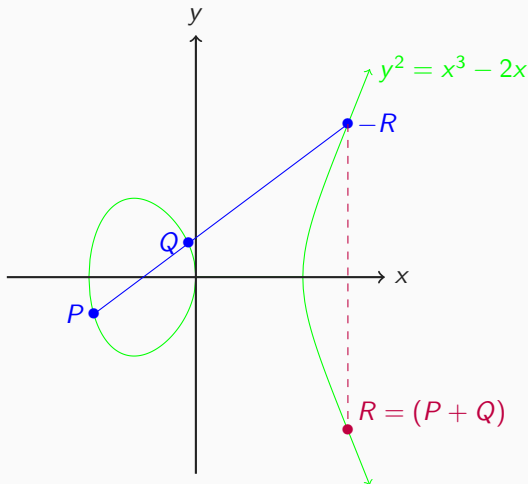
$$y^2 = x^3 + ax + b$$

for some fixed values of  $p, a, b$  (these are domain parameters)

- ▶ This is called the *(short) Weierstrass equation*
- ▶ All elliptic curves over  $\mathbb{F}_p$  can be represented this way
- ▶ Condition of *non-singularity*:  $4a^3 + 27b^2 \bmod p \neq 0$  [for info only]

## Elliptic curve group $\mathcal{E}$

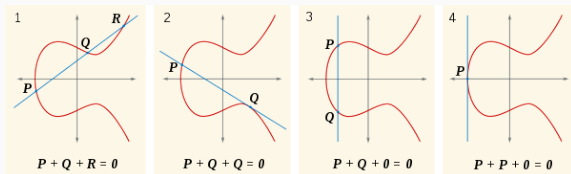
- Set: points  $(x, y)$  on the curve and the *point at infinity*,  $\mathcal{O}$
- Group law is *addition of points*, here illustrated for a curve over  $\mathbb{R}$



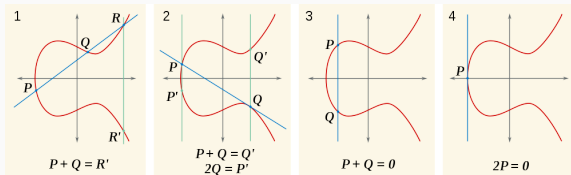
# Some intuition behind point addition

## Definition of the group law

Let  $P, Q, R \in \mathcal{E}$ :  $P + Q + R = \mathcal{O}$  iff they are on a straight line  
 $\mathcal{O}$  is at infinity in the direction of the  $y$ -axis



For point addition this implies:



- ▶ Closure: a straight line intersecting the curve in 2 points will intersect it in a 3rd point
  - if a third-degree equation has 2 roots, it has one more (taking into account multiplicity)
- ▶ Associativity holds but proof is non-trivial
- ▶ Identity: the point at infinity  $\mathcal{O}$
- ▶ Inverse: if  $P = (x, y)$ , then  $-P = (x, -y)$
- ▶ Commutative: roles of  $P$  and  $Q$  in  $P + Q$  are symmetric

It is an abelian group over any field

## Point addition, algebraically in $\mathbb{R}$ , or any field, including $\mathbb{F}_p$

Computing  $R = P + Q$  in  $\mathcal{E}$  with  $P = (x_p, y_p)$ ,  $Q = (x_q, y_q)$ ,  $R = (x_r, y_r)$

$x_p \neq x_q$  slope of line  $P$ - $Q$

$P = Q$ , slope of tangent

$$\lambda = \frac{y_p - y_q}{x_p - x_q}$$

$$\lambda = \frac{3x_p^2 + a}{2y_p}$$

Points on the line satisfy  $y = y_p + \lambda(x - x_p)$

Substituting  $y$  in Weierstrass  $(y_p + \lambda(x - x_p))^2 = x^3 + ax + b$

Fact: coefficient of  $x^{n-1}$  of degree- $n$  monic polynomial is minus sum of its roots

Coefficient of  $x^2$  in this equation is  $-\lambda^2$ , so  $x_p + x_q + x_r = \lambda^2$ , or

$$x_r = \lambda^2 - x_p - x_q$$

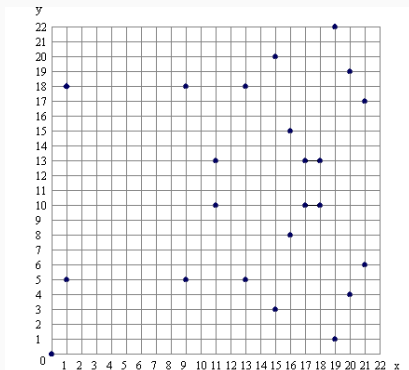
$$y_r = \lambda(x_p - x_r) - y_p$$

Note: addition, subtraction and multiplication are all modulo  $p$ . Division is multiplication by inverse, requiring ext. Euclidean or exponentiation



## Toy example in $\mathbb{F}_{23}$

$$\mathcal{E} : y^2 = x^3 + x \text{ over } \mathbb{F}_{23}$$



Verify the following:

- ▶  $(9, 5) \in \mathcal{E}$  and what is its inverse?
- ▶  $\#\mathcal{E} = 24$ : 23 points  $(x, y)$  that satisfy the equation, plus  $\mathcal{O}$

# Discrete log in the world of elliptic curves

- ▶ For  $G \in \mathcal{E}$ , consider the sequence:
  - $i = 1 : G$
  - $i = 2 : G + G$
  - $i = 3 : G + G + G$
  - ...
  - $i = n : [n]G$
- ▶ We call  $[n]G$  the **scalar multiplication** of point  $G$  by scalar  $n$
- ▶  $\text{ord}(G)$  is the smallest integer  $q > 0$  such that  $[q]G = \mathcal{O}$

## Discrete log (DL) problem in $\mathcal{E}$

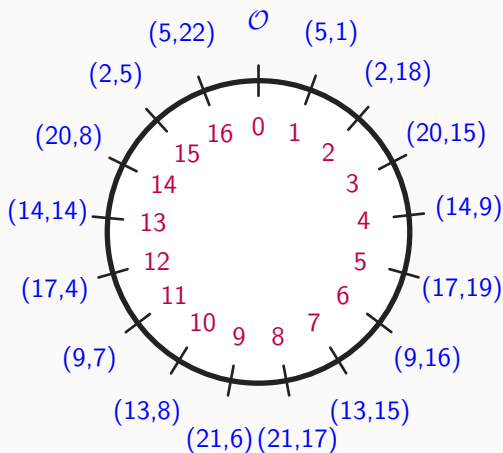
Let  $G \in \mathcal{E}$  have order  $q$ .

Let  $a \xleftarrow{\$} \mathbb{Z}/q\mathbb{Z}$  and  $A \leftarrow [a]G$

Given  $\langle G \rangle$  and  $A$ , determine  $a$

Note: similar to the discrete log problem in modular multiplicative groups, this has a certain hardness.

## Illustration with a cyclic subgroup of $\mathcal{E}(\mathbb{F}_{23}) : y^2 = x^3 - x - 4$



Here  $G = (5, 1) \in \mathcal{E}$  and  $\text{ord}(G) = 17$

For each  $i \in \mathbb{Z}/17\mathbb{Z}$  we have  $[i]G \in \mathcal{E}$

