Radboud University

Elliptic Curve Cryptography, Part 1

Cryptography, Spring 2020

L. Batina, J. Daemen

May 13, 2020

Institute for Computing and Information Sciences
Radboud University

Outline

Some motivation for ECC

Prime fields

Elliptic curve groups

Some motivation for ECC

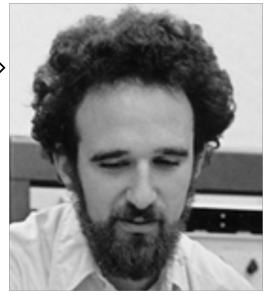
Diffie-Hellman key exchange (1976)

$q = 160693804425899027554196209234116260252220299378279283530130 1$

$g = 123456789$

$g^a \bmod q = 784673745294226535797545963198527025754996929800857779485 93$

$5600481042932181286674410213424831338026262713942994101287 98 = g^b \bmod q$



$a =$
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 $\mathrm{ord}(g)$ chosen to offer safety margin with respect to the best discrete log algorithms in 1976

Diffie-Hellman key exchange (2020)

Size of field prime p (called q in this figure) and $\mathrm{ord}(g)$ chosen to offer safety margin with respect to the best discrete log algorithms in 2020

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

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

$\#E$ = 115792089210356248762697446949407573529996955224135760342422259061068512044369

P = (48439561293906451759052585252797914202762949526041747995844080717082404635286,
36134250956749795798585127919587881956611106672985015071877198253568414405109)

a = 8913064459124603357763977064146285502314502849283525560318372192231732461439 5

[a]P = (84116208261315898167593067868200525612344221886333785331584793435449501658416,
102885655542185598026739250172885300109680266058548048621945393128043427650740)

[b]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383,
77887418190304022994116595034556257760807185615679689372138134363978498341594)

[ab]P = (101228882920057626679704131545407930245895491542090988999577542687271695288383,
77887418190304022994116595034556257760807185615679689372138134363978498341594)

b = 100955574639327864188069383161907080327719109190584053916797810821934 05190826

$\langle G \rangle \subset \mathcal{E}$ with elliptic curve group $\mathcal{E}$ and $\mathrm{ord}(G)$ 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

Rings and finite rings

- We consider a set and two operations: addition and multiplication
- For example $(\mathbb{Z}, +, \cdot)$
- $(\mathbb{Z}, +)$ is a group
- $(\mathbb{Z}, \cdot)$ satisfies:
  - closed
  - associative
  - has neutral element: 1
- Additional property: $\cdot$ 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

Prime fields

- 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 $\mathrm{GF}(p)$)
- 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

Elliptic curves over $\mathbb{F}_p$

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

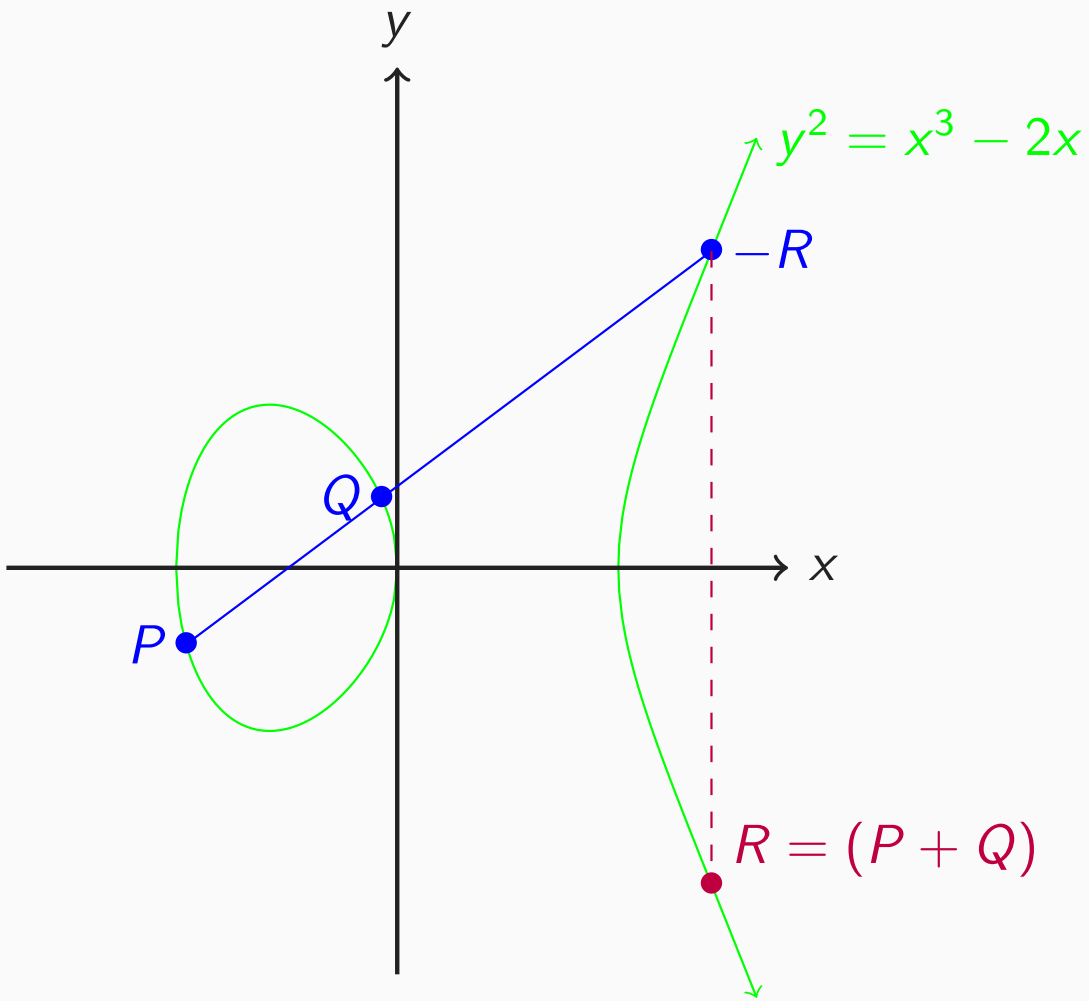
$$y^2 = x^3 + ax + b$$

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 $\mathbb{R}$

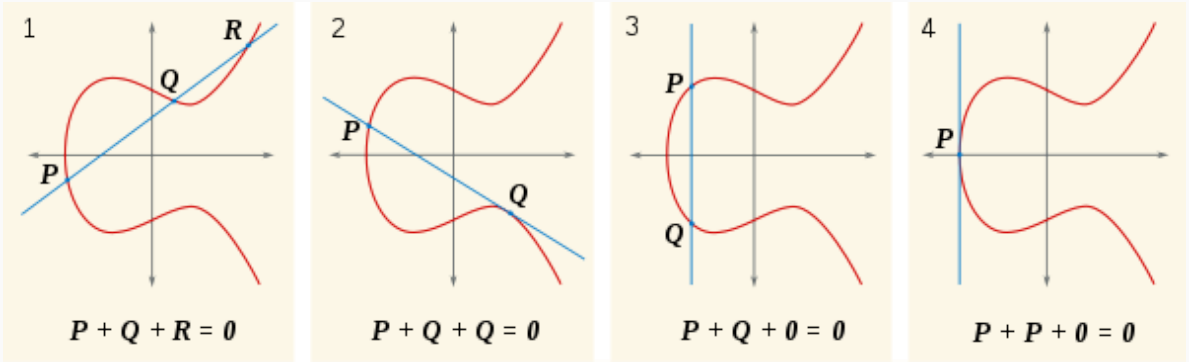


Some intuition behind point addition

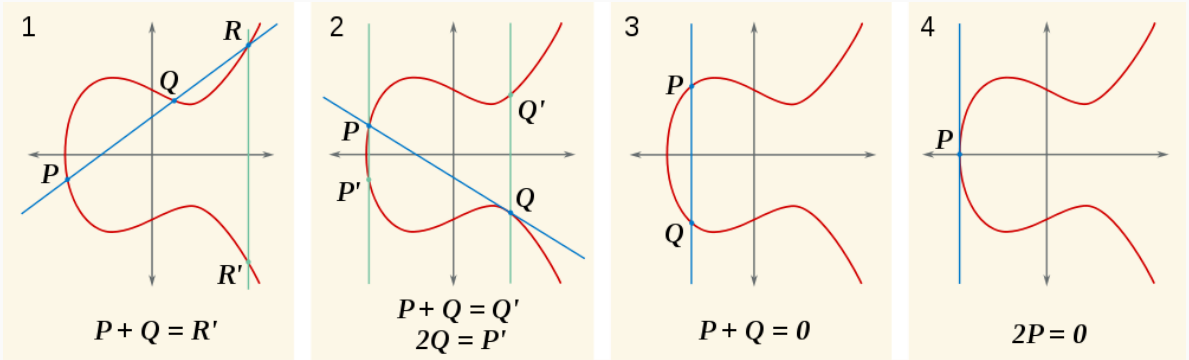
Definition of the group law

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:



$\mathcal{E}$ is an abelian group

- 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

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

$P = Q$, slope of tangent

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

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

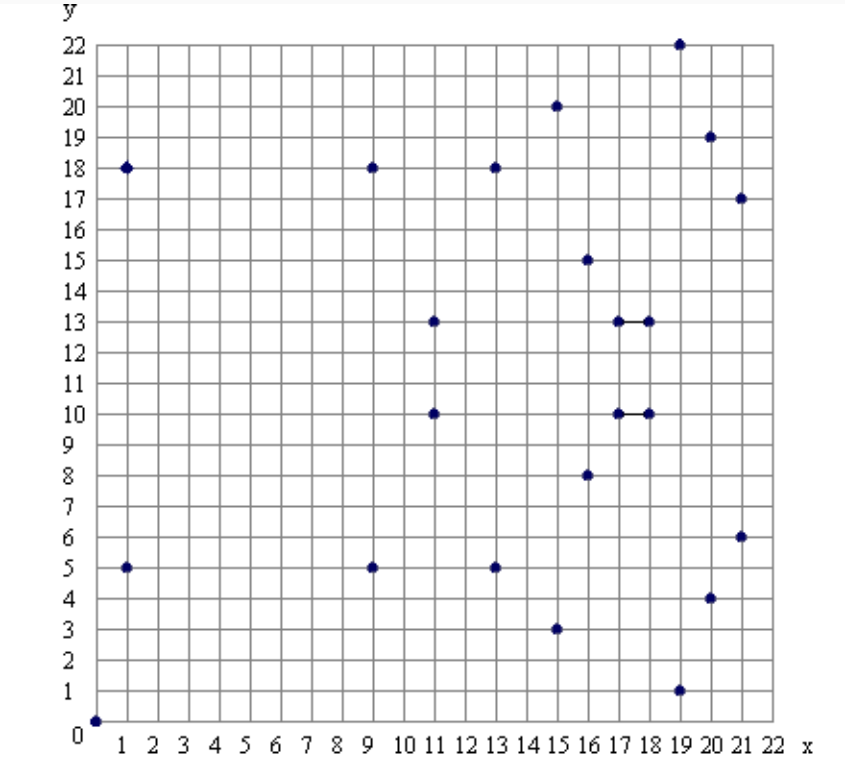
Coefficient of x^2 in this equation is $-\lambda^2$, so $x_p + x_q + x_r = \lambda^2$, or

$$x_r = \lambda^2 - x_p - x_q$$
$$y_r = \lambda(x_p - x_r) - y_p$$

Note: division is multiplication by inverse and inverse is expensive

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

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



Verify the following:

- $(9, 5) \in E$ 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

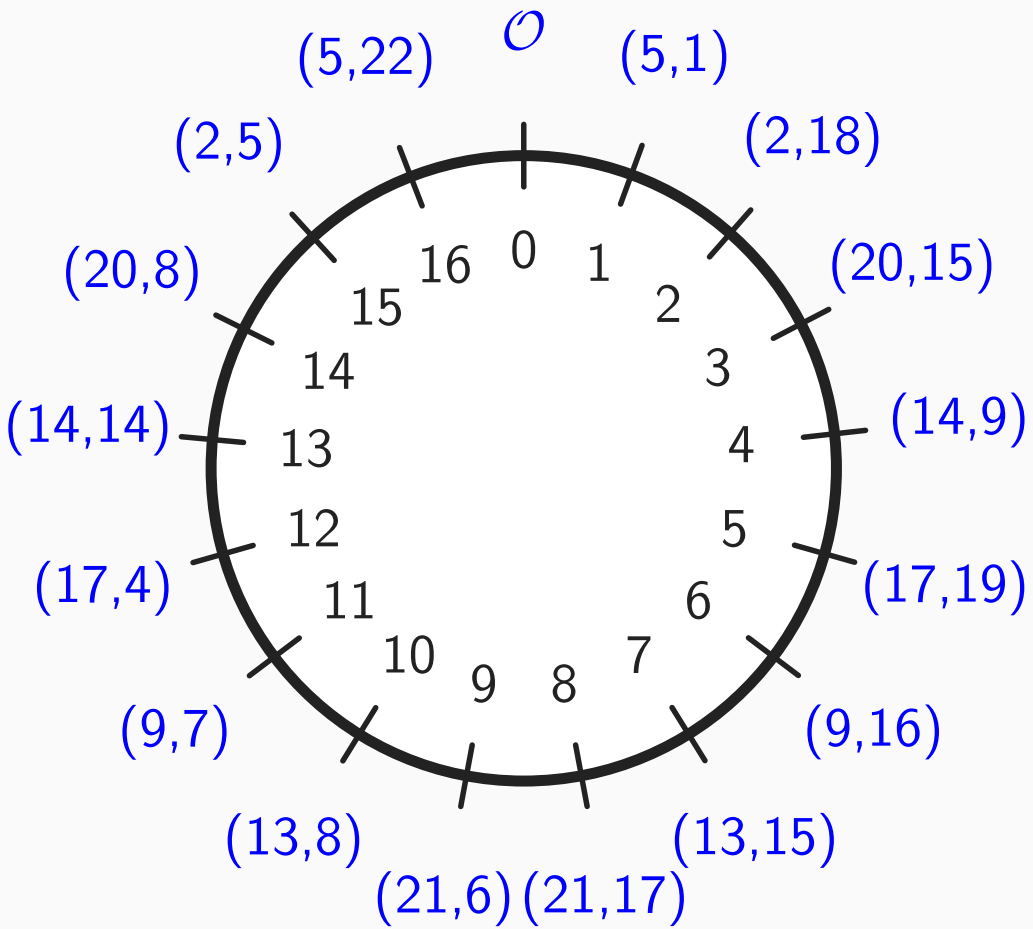
- For $G \in \mathcal{E}$, consider the sequence:
  - $i = 1 : G$
  - $i = 2 : G + G$
  - $i = 3 : G + G + G$
  - ...
  - $i = n : [n]G$
- we call $[n]G$ the **scalar multiplication** of point G by scalar n
- $\text{ord}(G)$ is the smallest integer $q > 0$ such that $[q]G = \mathcal{O}$

Discrete log hardness in $\mathcal{E}$

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

Given $\langle G \rangle$ and A, the success probability to determine a is negligible

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 $\mathrm{ord}(G) = 17$

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

End of ECC, part 1