Cryptography

Lecture 4: Elliptic Curves I

Dr. Muhammad Hataba
Muhammad.Hataba@giu-uni.de

References and Legalities

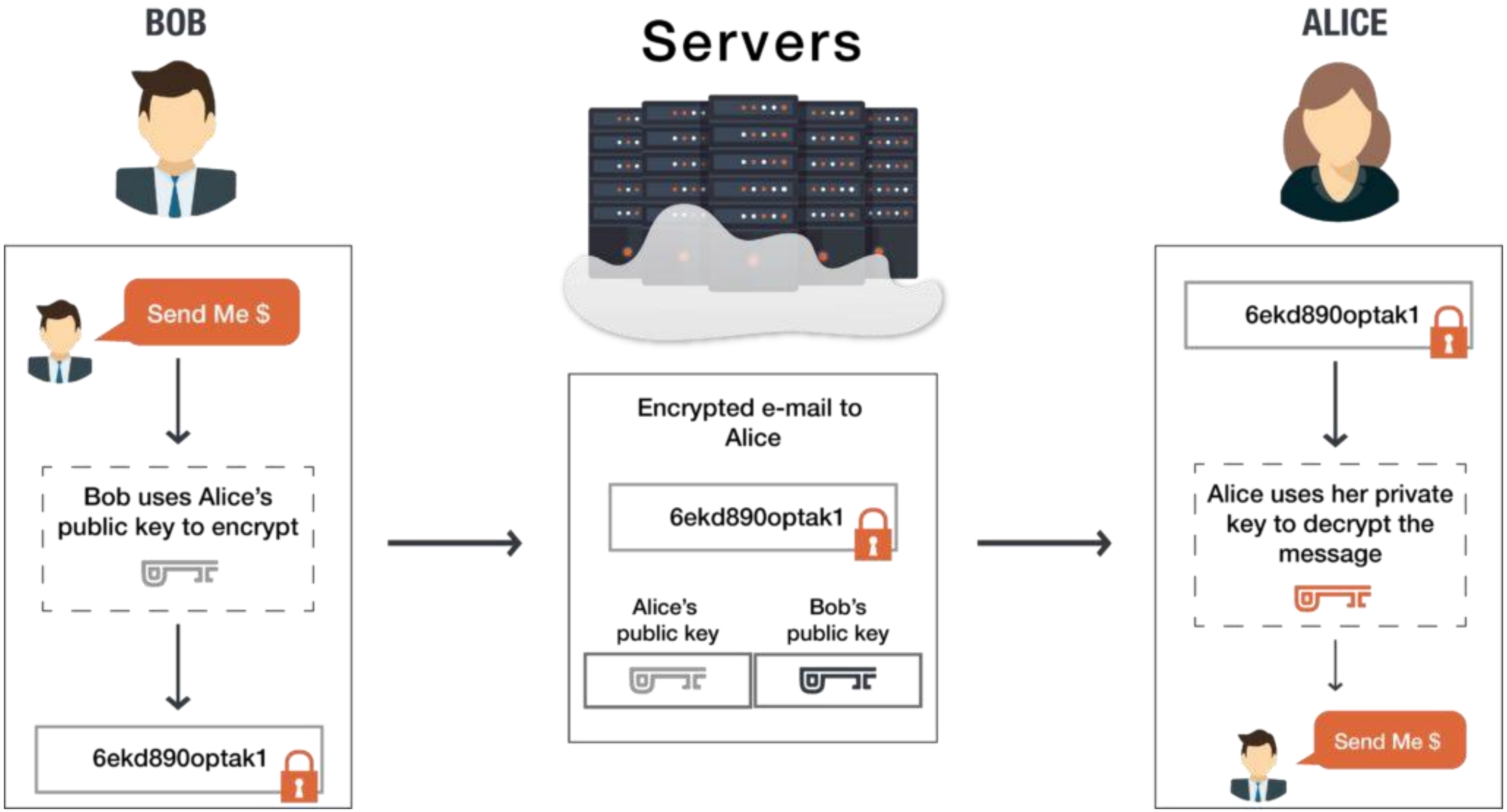
This lecture makes use of the following resources:

- Understanding Cryptography Chapter 9
- https://www.youtube.com/watch?v=F3zzNa42-tQ
- Information Security Course, German International University, Amr ElMougy
- Cryptography Course, German International University, *Alia El Bolock*

Outline of Today's Lecture

- Public Key Cryptography
- From Modular Arithmetic to Elliptic Curves
- Elliptic Curves Intro
- Computations on Elliptic Curves
- Elliptic Curve Cryptography
- Elliptic Curve Diffie-Hellman Protocol
- Security Aspects
- Implementation in Software and Hardware

Public-key Algorithms



Categories of PKC

- RSA (**Rivest–Shamir–Adleman**)
- Diffie-Hellman
- Elliptic Curve Cryptography

All built on the concept of trapdoor functions

https://www.twilio.com/blog/what-is-public-key-cryptography

Trapdoor Functions

- Example 1:
  - Mixing colors together is easy
  - Separating them from each other is hard (computationally “infeasible”)
- Example 2:
  - Multiplying large prime numbers together is easy
  - Factorising them is hard (computationally “infeasible”)
- Trapdoor functions are functions that are easy to compute one way, but difficult the other, i.e.,

$A \longrightarrow B$ ✅

$A \longleftarrow B$ ❌

RSA (Rivest–Shamir–Adleman)

- Private and public key pairs (based on the factoring problem of large primes)

RSA Algorithm

Key Generation

Select p, q	p and q both prime; $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$de \bmod \phi(n) = 1$
Public key	$KU = \{e, n\}$
Private key	$KR = \{d, n\}$

Encryption

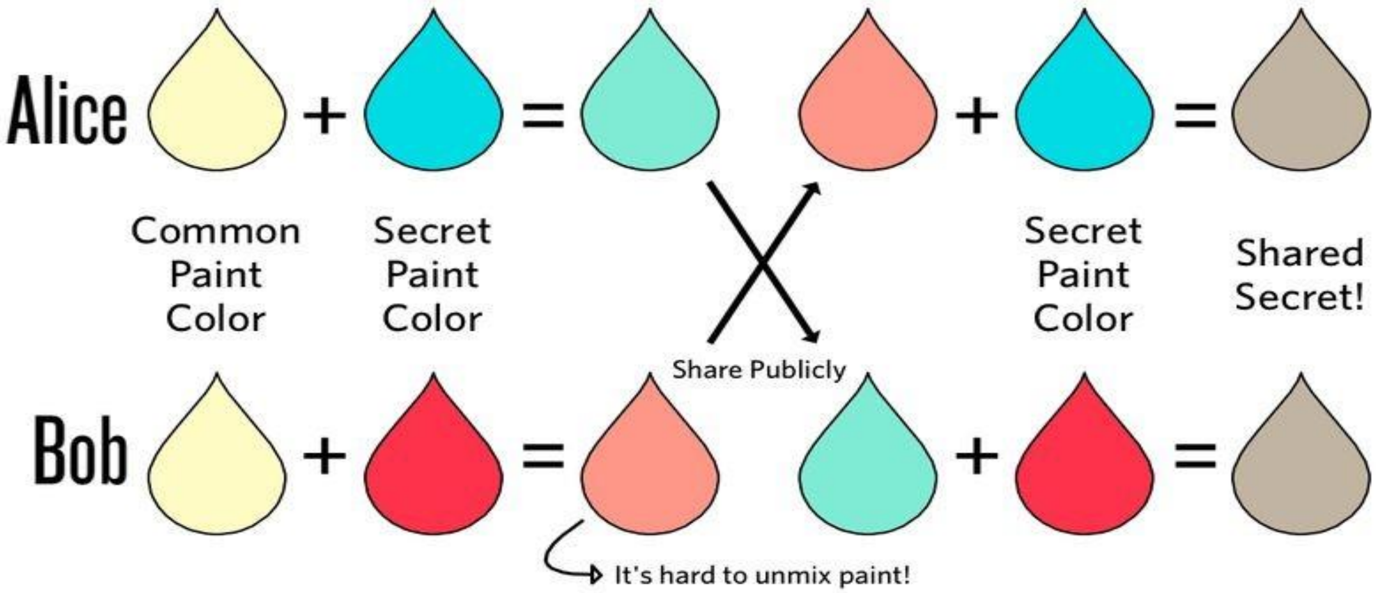
Plaintext:	$M < n$
Ciphertext:	$C = M^e \pmod{n}$

Decryption

Plaintext:	C
Ciphertext:	$M = C^d \pmod{n}$

Diffie-Hellman Key Exchange

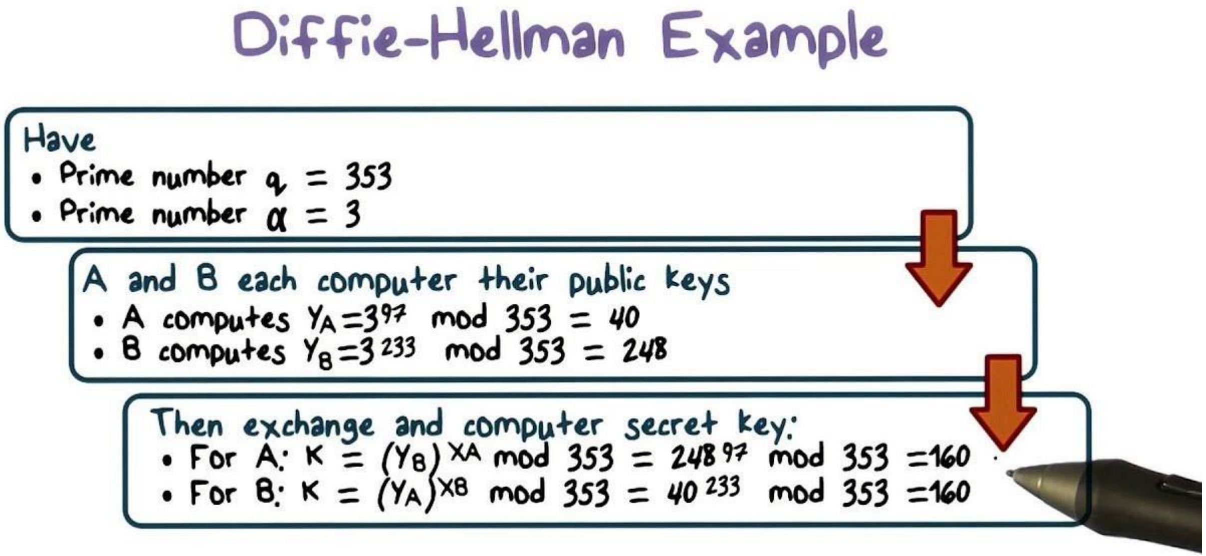
- Two parties build a shared key together ([Public key cryptography - Diffie-Hellman Key Exchange (full version)])
- Based on Discrete Logarithm Problem in $\mathbb{Z}^*_p$



Diffie-Hellman Key Exchange

- Two parties build a shared key together (based on modular arithmetic)

(Public key cryptography - Diffie-Hellman Key Exchange (full version))



From Modular Arithmetic to Elliptic Curves

- RSA (**Rivest–Shamir–Adleman**)
- Diffie-Hellman (and ElGamal)

Modular Arithmetic

- Elliptic Curve Cryptography

Elliptic Curves

All built on the concept of trapdoor functions

https://www.twilio.com/blog/what-is-public-key-cryptography

Why ECC?

- Problem:
  Asymmetric schemes like RSA and Elgamal require exponentiations in integer rings and fields with parameters of more than 1000 bits.
  - High computational effort on CPUs with 32-bit or 64-bit arithmetic
  - Large parameter sizes critical for storage on small and embedded
- Motivation:
  Smaller field sizes providing equivalent security are desirable
- Solution:
  Elliptic Curve Cryptography uses a group of points (instead of integers) for cryptographic schemes with coefficient sizes of 160-256 bits, reducing significantly the computational effort.

What’s wrong with RSA?

- RSA is based upon the ‘belief’ that factoring is ‘difficult’ – never been proven (NP complete)
- Prime numbers are getting too large
- Amount of research currently devoted to factoring algorithms
- Quantum computing will make RSA obsolete overnight

ECC vs RSA in a Nutshell

ECC Key Size (bits)	RSA Key Size(bits)	Key Size Ratio	Cost Ratio
160	1024	1:7	1:3
224	2048	1:10	1:6
256	3072	1:12	1:10
384	7680	1:20	1:32
521	15360	1:30	1:64

That covers why ECC

What is an Elliptic Curve?

Elliptic Curves

Let K be a field and $a \in K, b \in K$ constants such that

$$4a^3 + 27b^2 \neq 0$$

A non-singular elliptic curve is the set points E defined by the

solutions $(x,y) \in K \times K$ to the equation

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

together with a special point O called the point at infinity.

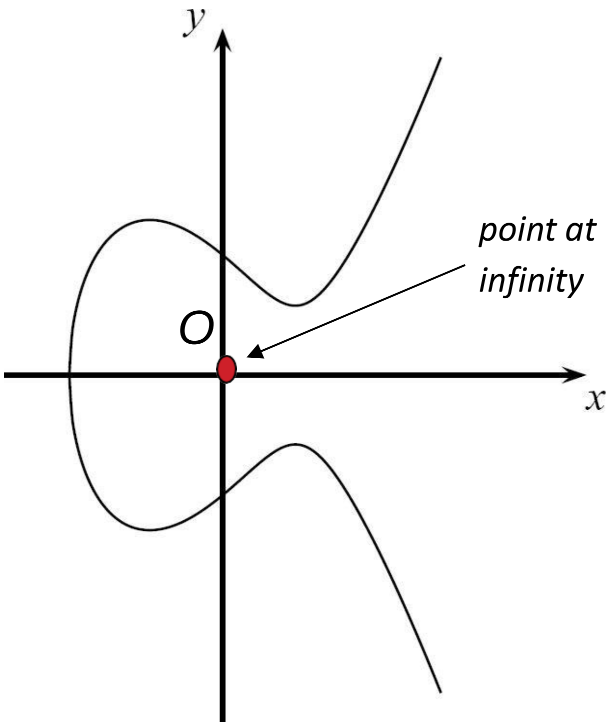
What is an Elliptic Curve?

- Elliptic curves are polynomials that define points based on the (simplified) Weierstraß equation:

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

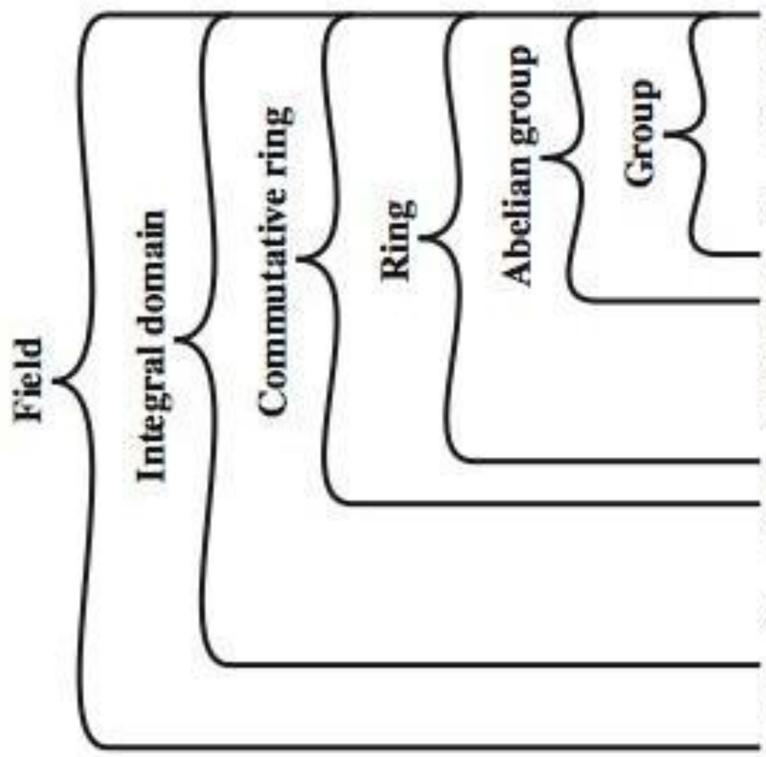
  for parameters a,b that specify the exact shape of the curve

- On the real numbers and with parameters $a, b \in \mathbb{R}$, an elliptic curve looks like this >>
- Elliptic curves can not just be defined over the real numbers $\mathbb{R}$ but over many other types of finite fields.



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

Recall

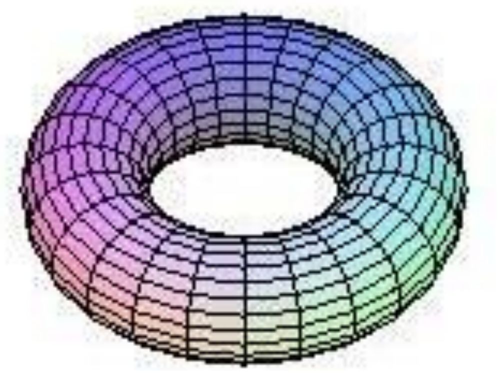


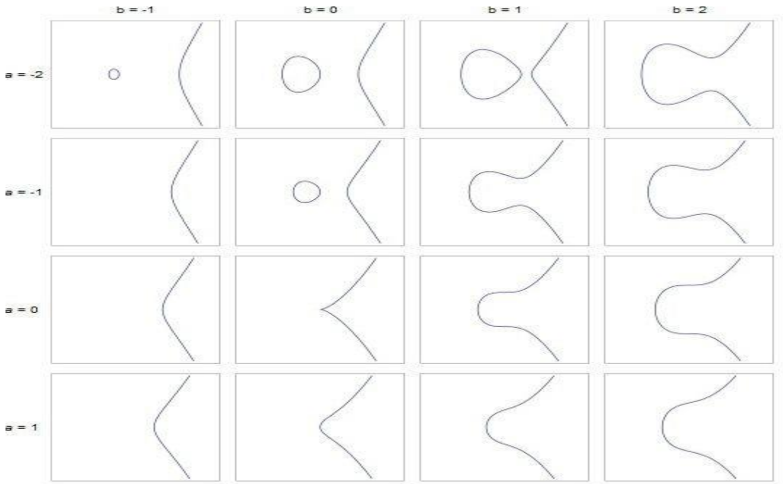
(A1) Closure under addition:
(A2) Associativity of addition:
(A3) Additive identity:
(A4) Additive inverse:
(A5) Commutativity of addition:
(M1) Closure under multiplication:
(M2) Associativity of multiplication:
(M3) Distributive laws:
(M4) Commutativity of multiplication:
(M5) Multiplicative identity:
(M6) No zero divisors:
(M7) Multiplicative inverse:

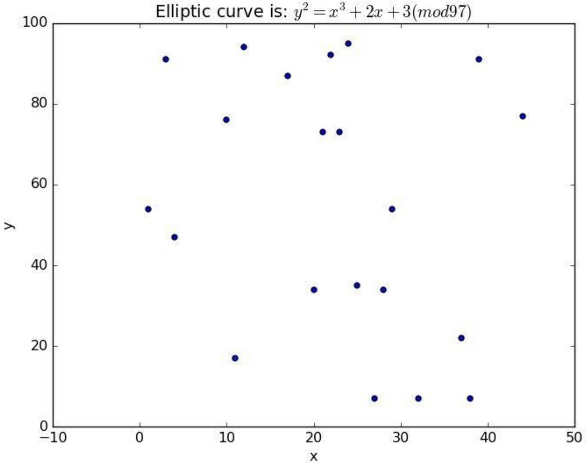
Fields of Elliptic Curve

K can be:

- $\mathbb{R}$
- $\mathbb{Q}$
- $\mathbb{C}$
- $\mathbb{Z}/p\mathbb{Z}$







Singular Elliptic Curve

- If $4a^3 + 27b^2 = 0$, then we have a singular elliptic curve
- This could potentially lead to not having 3 distinct roots
- Therefore, we must deal with non-singular elliptic curves with the condition $4a^3 + 27b^2 \neq 0$, in order to assure that we have 3 distinct roots
- This will allow us to establish the fact that the solution set E forms an Abelian group

Recall: Abelian Group

Given two points P, Q in $E(F_p)$, there is a third point, denoted by $P+Q$ on $E(F_p)$, and the following relations hold for all P, Q, R in $E(F_p)$

- $P+Q=Q+P$ (commutativity)
- $(P+Q)+R=P+(Q+R)$ (associativity)
- $P+O=O+P=P$ (existence of an identity element)
- there exists $(-P)$ such that $-P+P=P+(-P)=O$ (existence of inverses)

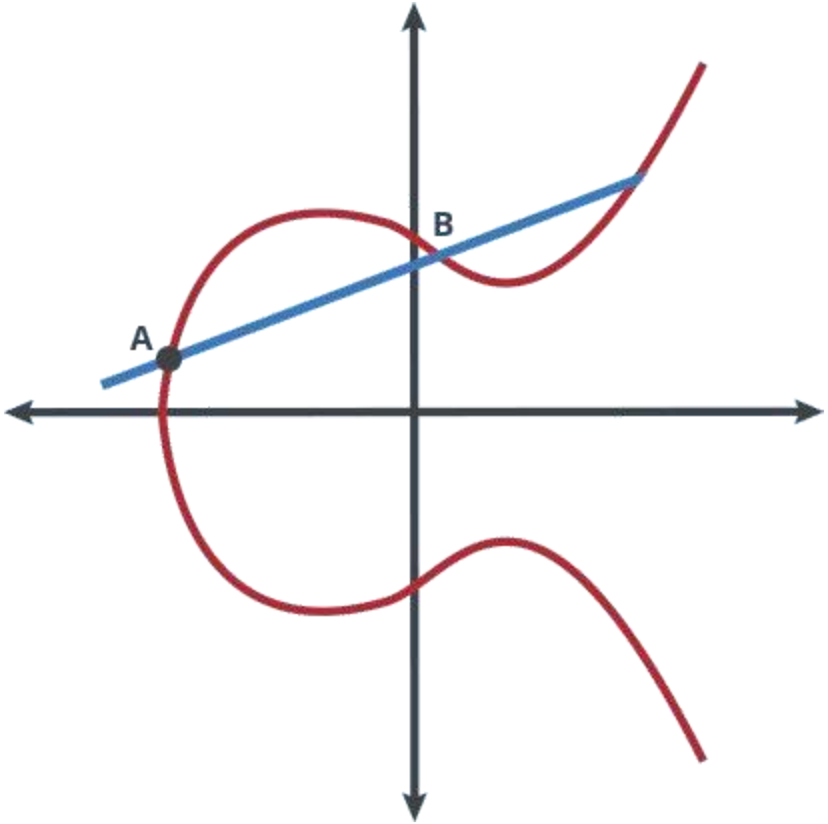
Elliptic Curve Groups

O: the point at ∞

We can define an (abelian) group over elliptic curves with O

- the elements of the group are the points of an elliptic curve
- the identity element is the point O
- the inverse of a point P is the one symmetric about the x-axis
- addition is given by the following rule: given 3 aligned, non-zero points P, Q and R, their sum P+Q+R=0.

Computations on Elliptic Curves



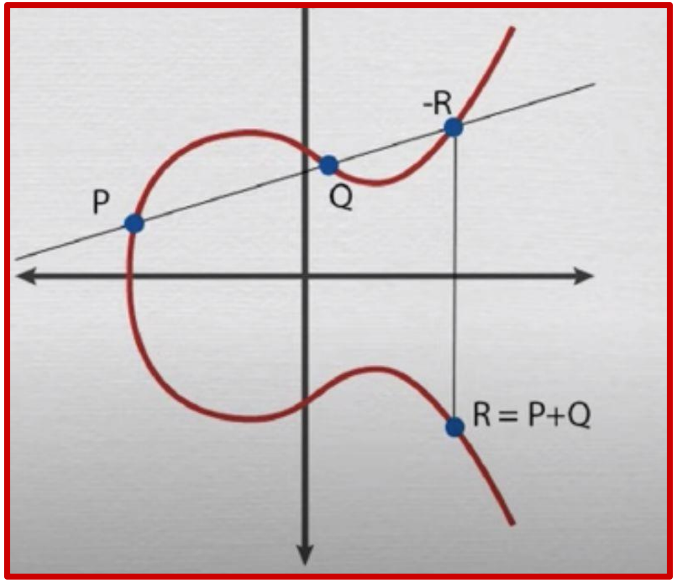
A (Relatively Easy To Understand) Primer on Elliptic Curve Cryptography

Point Addition - Geometrically

Given two points P, Q on the elliptic curve, i.e., in the set

$$E = \{(x,y) \mid y^2 = x^3 + ax + b\} \cup \{O\}$$

$P+Q=R$



Point Addition - Algebraically

Given two points P, Q on the elliptic curve, i.e., in the set

$$E = \{(x, y) \mid y^2 = x^3 + ax + b\} \cup \{O\}$$

$P + Q = R$

$$s = \frac{y_P - y_Q}{x_P - x_Q}$$

$$x_R = s^2 - (x_P + x_Q)$$

$$y_R = s(x_P - x_R) - y_P$$

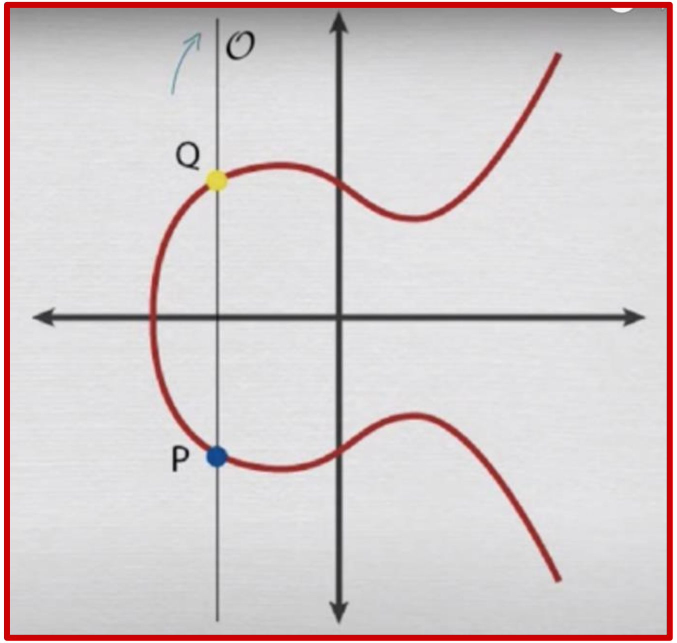
Adding Vertical Points

Given two points P, Q on the elliptic curve, i.e., in the set

$E = \{(x, y) \mid y^2 = x^3 + ax + b\} \cup \{O\}$

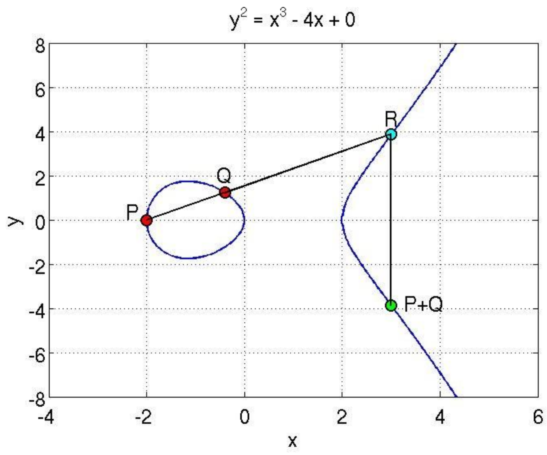
$P + Q = O$, if $x_p = x_q$, i.e., $Q = -P$ $P + P = O$, if

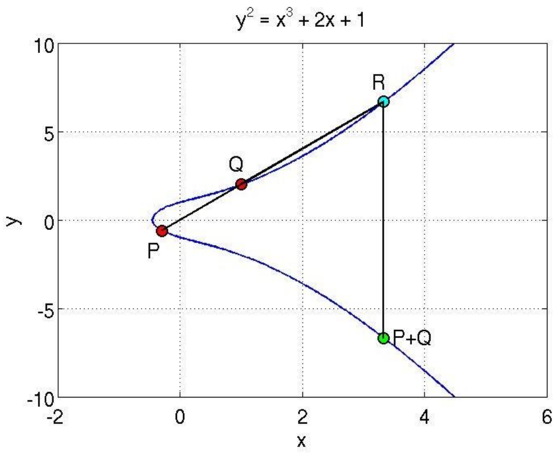
$x_p = O$



O serves as the identity

Point Addition





Adding two points on the curve

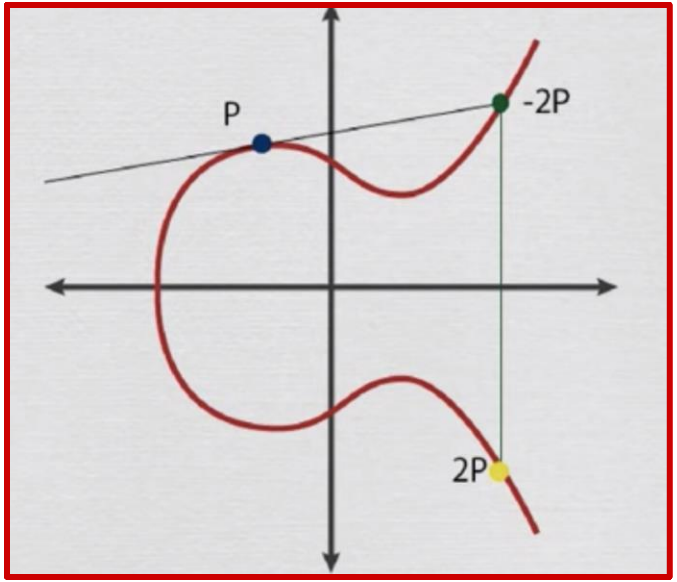
P and Q are added to obtain P+Q which is a reflection of R along the X-axis

Point Doubling - Geometrically

Given two points P, Q on the elliptic curve, i.e., in the set

$$E = \{(x, y) \mid y^2 = x^3 + ax + b\} \cup \{O\}$$

$P + P = R = 2P$



Point Doubling - Algebraically

Given two points P,Q on the elliptic curve, i.e., in the set

$E = \{(x,y) \mid y^2 = x^3 + ax + b\} \cup \{O\}$

$P + P = R = 2P$

$$s = \frac{3x_P^2 + a}{2y_P}$$

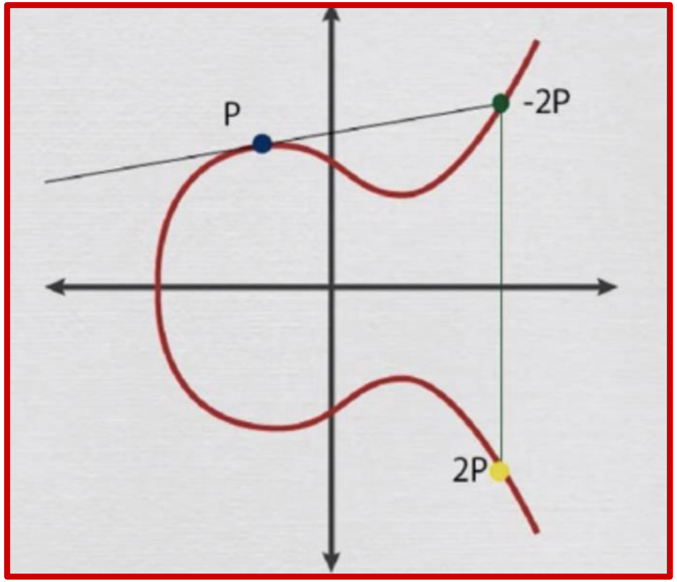
$$x_R = s^2 - 2x_P$$

$$y_R = s(x_P - x_R) - y_P$$

Scalar Multiplication

Given, $P \in E$ and $k \in \mathbb{Z}$

$$Q = kP = \underbrace{P + P + \ldots + P}_{k\ \text{times}}$$

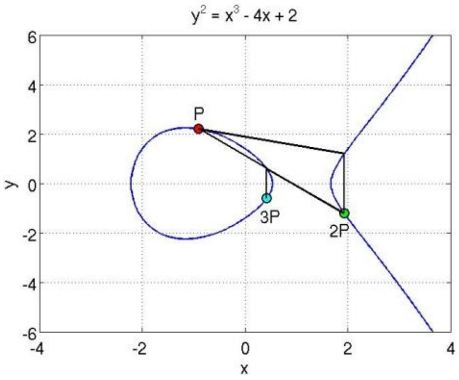


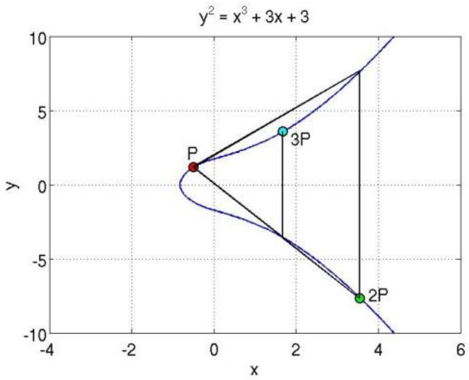
Elliptic curves: scalar multiplication

Point Operations Summary

A tangent at P is extended to cut the curve at a point; its reflection is 2P

- Adding P and 2P gives 3P
- Similarly, such operations can be performed as many times as desired to obtain Q=kP





Elliptic curves: scalar multiplication

Summary of Group Operations

- Main operations: point addition and point multiplication
- Adding two points that lie on an Elliptic Curve – results in a third point on the curve
- Point multiplication is repeated addition