Lecture 8 – Group theory, Diffie-Hellman key exchange

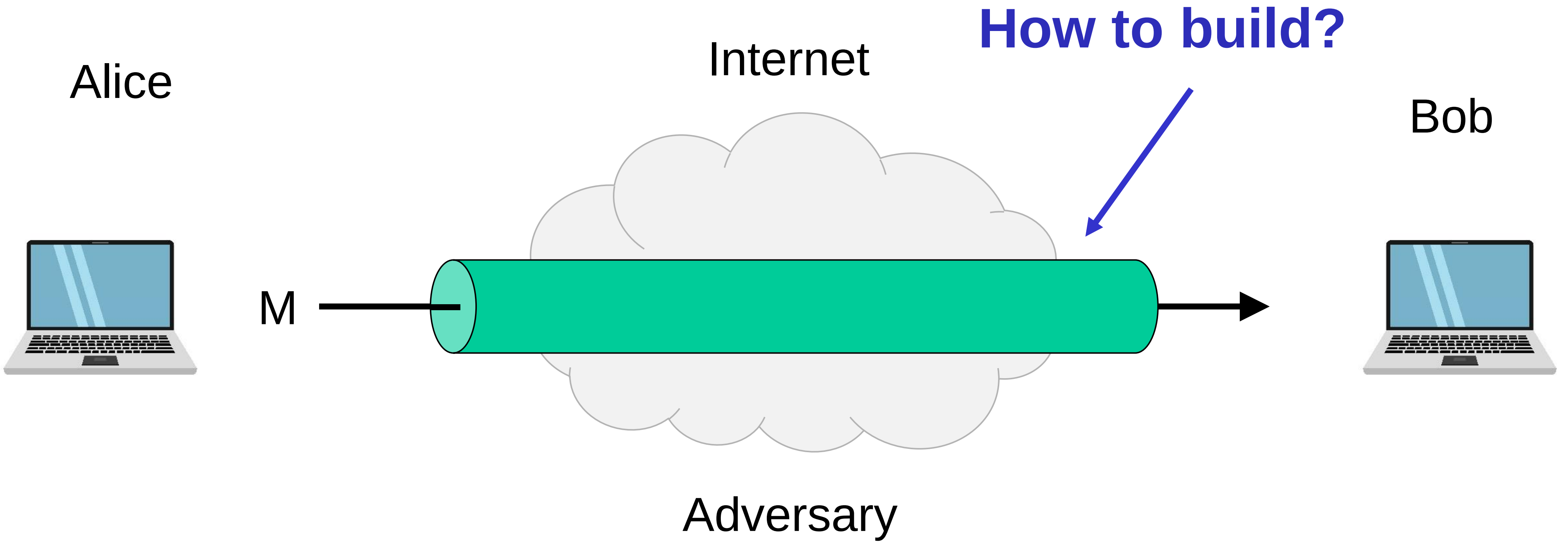
TEK4500

13.10.2020

Håkon Jacobsen

hakon.jacobsen@its.uio.no

Ideal solution: secure channels



Alice

Internet

How to build?

Bob

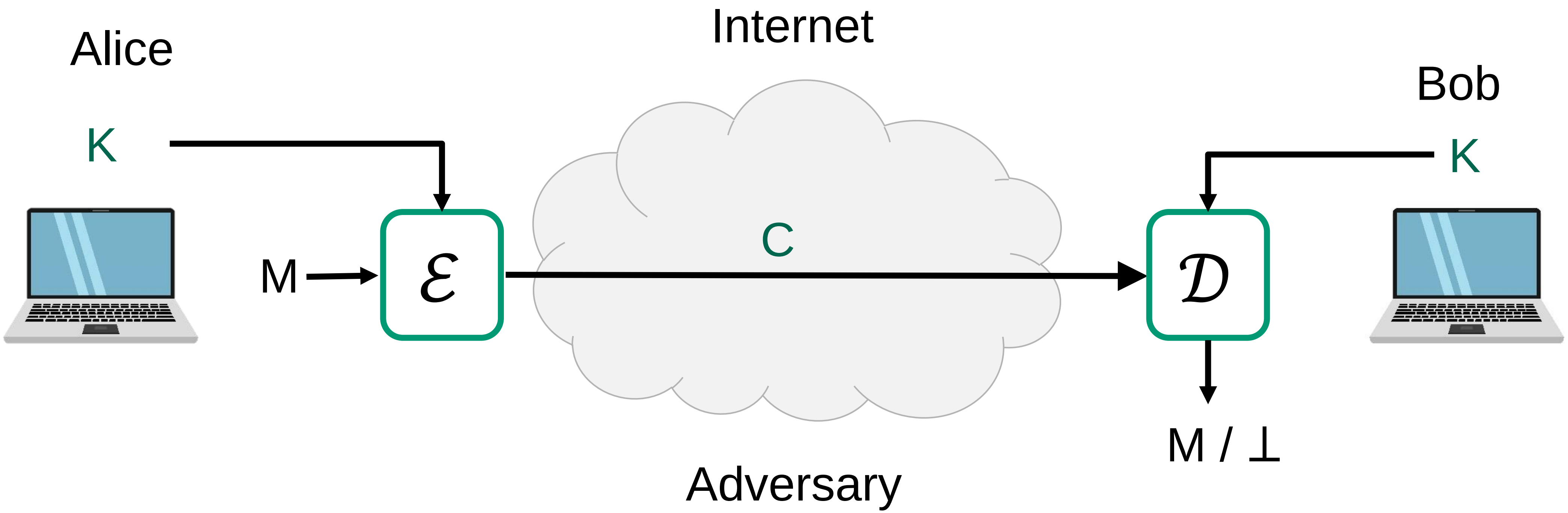
M

Adversary

Security goals:

- **Data privacy:** adversary should not be able to read message M ✓
- **Data integrity:** adversary should not be able to modify message M ✓
- **Data authenticity:** message M really originated from Alice ✓

Creating secure channels: encryption schemes



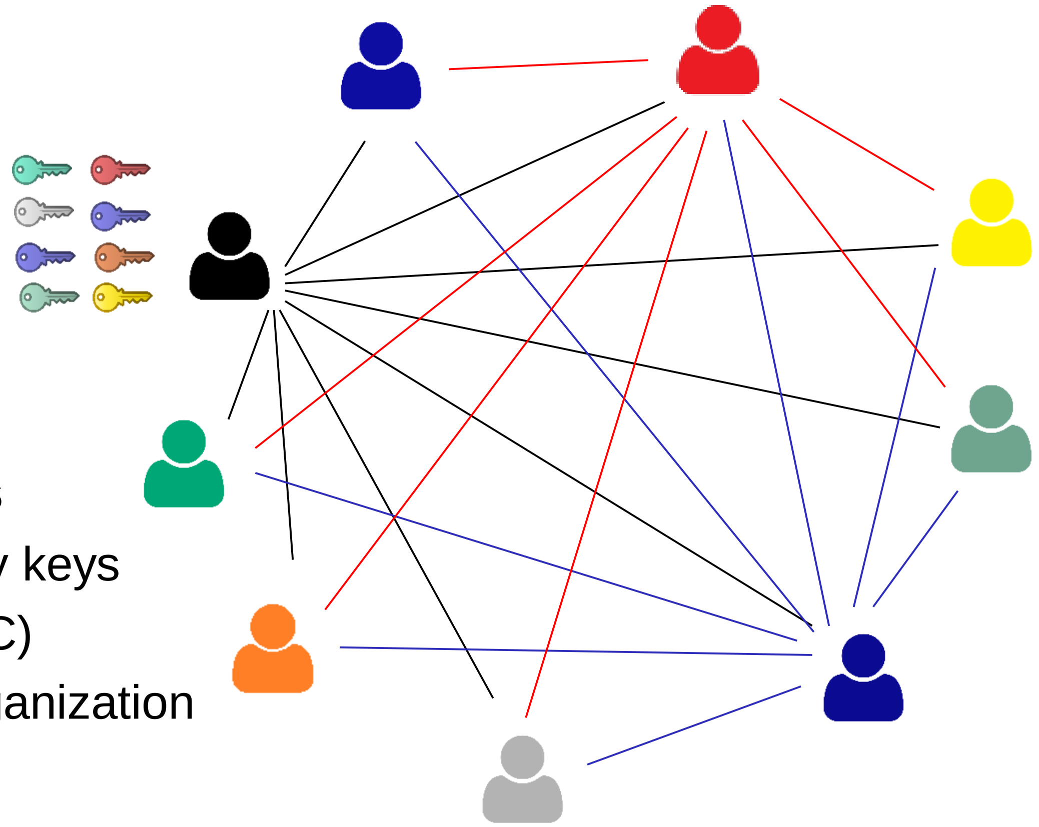
$\mathcal{E}$: encryption algorithm (public)

K : encryption / decryption key (secret)

$\mathcal{D}$: decryption algorithm (public)

Symmetric key distribution problem

- One user needs to store N symmetric keys when communicating with N other users
- $\frac{N(N-1)}{2} = \mathcal{O}(N^2)$ keys in total
- Difficult to store and manage so many keys securely
- Partial solution: **key distribution centers**
  - One central authority hands out temporary keys
  - $\mathcal{O}(N)$ (long-term) keys needed (to the KDC)
  - Might be a feasible solution in a single organization
  - Single point of failure
  - **What about the internet?**



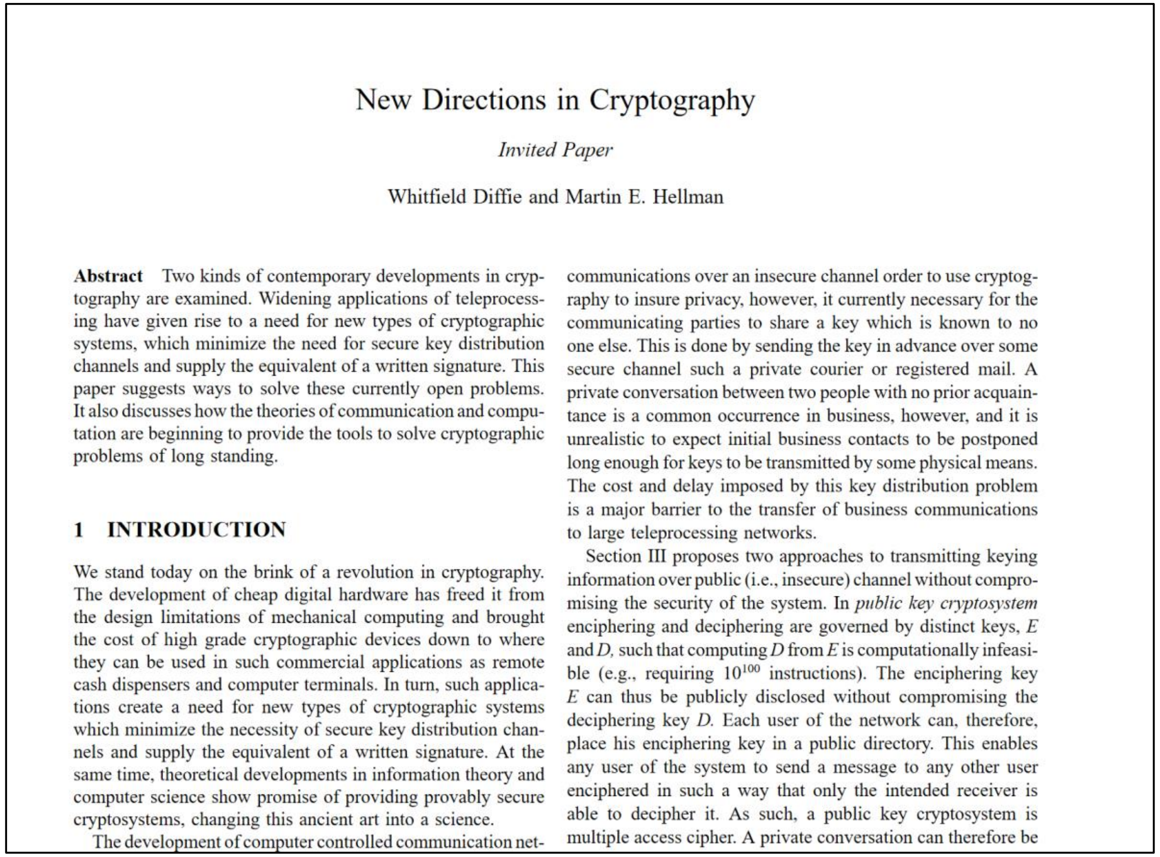
The public-key revolution

Diffie-Hellman key exchange

- Discovered in the 1970's
- Allows two parties to establish a shared secret without ever having met
- Diffie & Hellman paper also introduced:
  - Public-key encryption
  - Digital signatures

Ralph Merkle Whitfield Diffie

Martin Hellman



New Directions in Cryptography

Invited Paper

Whitfield Diffie and Martin E. Hellman

Abstract Two kinds of contemporary developments in cryptography are examined. Widening applications of teleprocessing have given rise to a need for new types of cryptographic systems, which minimize the need for secure key distribution channels and supply the equivalent of a written signature. This paper suggests ways to solve these currently open problems. It also discusses how the theories of communication and computation are beginning to provide the tools to solve cryptographic problems of long standing.

1 INTRODUCTION

We stand today on the brink of a revolution in cryptography. The development of cheap digital hardware has freed it from the design limitations of mechanical computing and brought the cost of high grade cryptographic devices down to where they can be used in such commercial applications as remote cash dispensers and computer terminals. In turn, such applications create a need for new types of cryptographic systems which minimize the necessity of secure key distribution channels and supply the equivalent of a written signature. At the same time, theoretical developments in information theory and computer science show promise of providing provably secure cryptosystems, changing this ancient art into a science.

The development of computer controlled communication net- communications over an insecure channel order to use cryptography to insure privacy, however, it currently necessary for the communicating parties to share a key which is known to no one else. This is done by sending the key in advance over some secure channel such a private courier or registered mail. A private conversation between two people with no prior acquaintance is a common occurrence in business, however, and it is unrealistic to expect initial business contacts to be postponed long enough for keys to be transmitted by some physical means. The cost and delay imposed by this key distribution problem is a major barrier to the transfer of business communications to large teleprocessing networks.

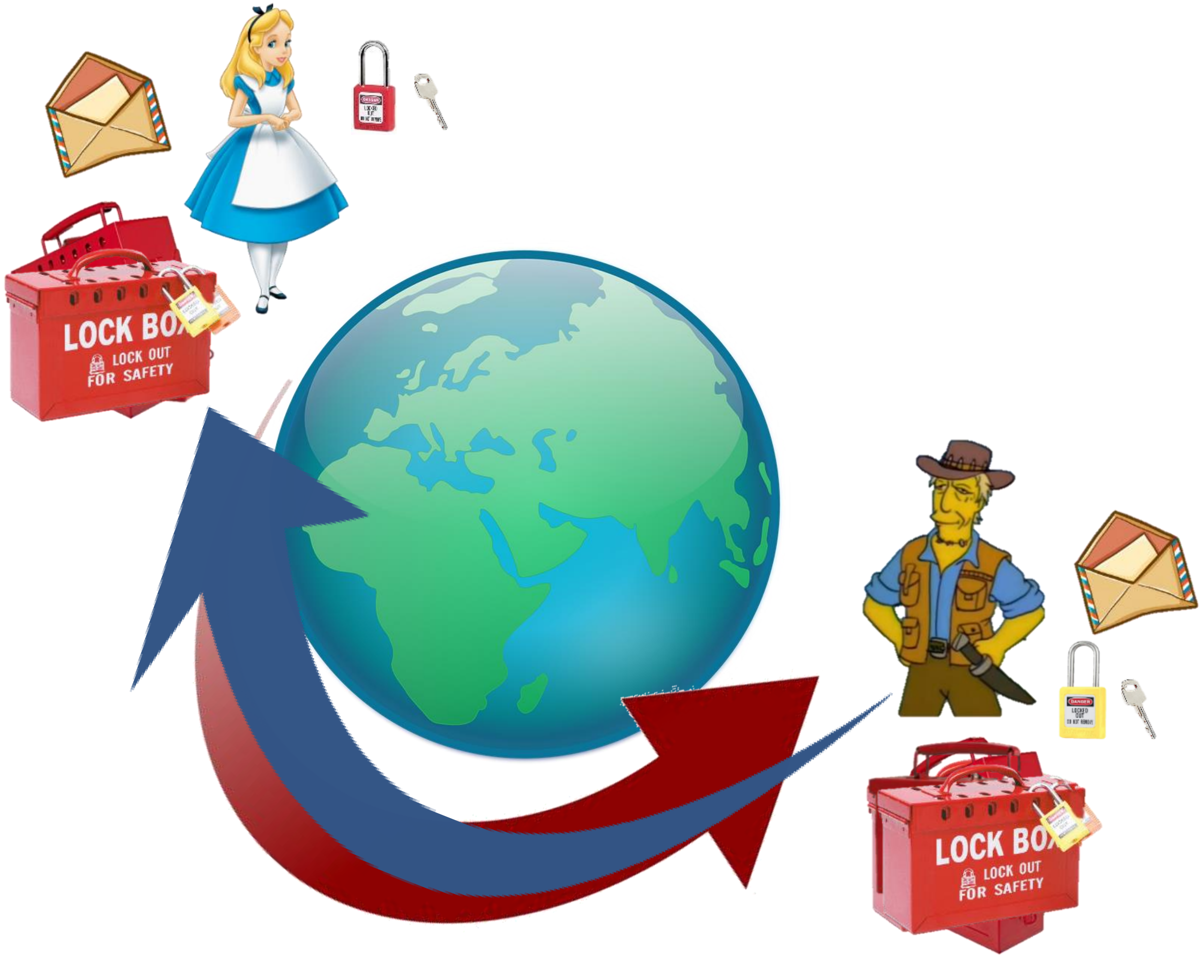
Section III proposes two approaches to transmitting keying information over public (i.e., insecure) channel without compromising the security of the system. In *public key cryptosystem* enciphering and deciphering are governed by distinct keys, *E* and *D*, such that computing *D* from *E* is computationally infeasible (e.g., requiring 10^{100} instructions). The enciphering key *E* can thus be publicly disclosed without compromising the deciphering key *D*. Each user of the network can, therefore, place his enciphering key in a public directory. This enables any user of the system to send a message to any other user enciphered in such a way that only the intended receiver is able to decipher it. As such, a public key cryptosystem is multiple access cipher. A private conversation can therefore be

Basic goals of cryptography

	Message privacy	**Message integrity / authentication**
Symmetric keys	Symmetric encryption	Message authentication codes (MAC)
Asymmetric keys	Asymmetric encryption (a.k.a. public-key encryption)	Digital signatures

(Key exchange)

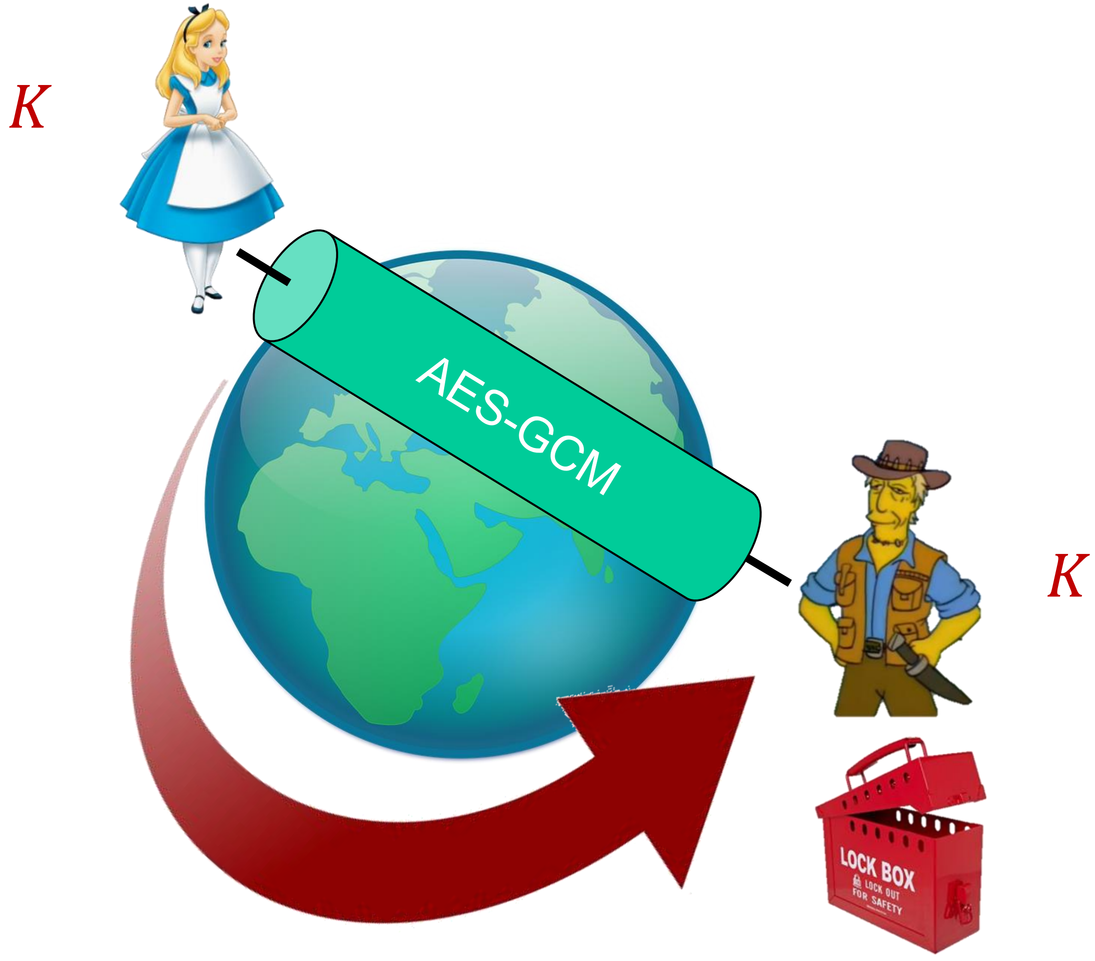
Diffie-Hellman key exchange – idea



Diffie-Hellman key exchange – idea

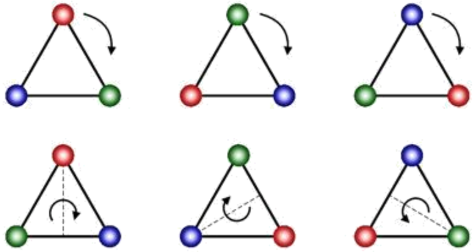
K
K
LOCK BOX
LOCK OUT
FOR SAFETY

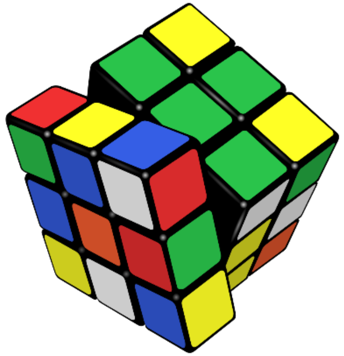
Diffie-Hellman key exchange + authenticated encryption

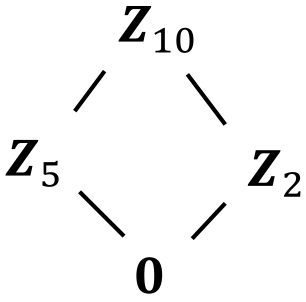


Public-key encryption

LOCK BOX
LOCK OUT
FOR SAFETY
LOCK BOX
LOCK OUT
FOR SAFETY







$\boldsymbol{Z}_{10}$

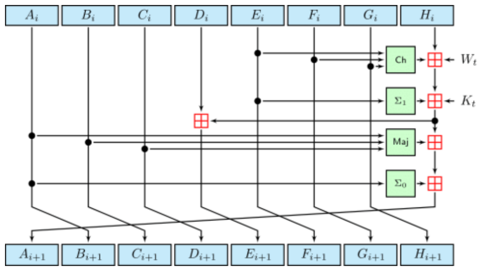
$\boldsymbol{Z}_{5}$ $\boldsymbol{Z}_{2}$

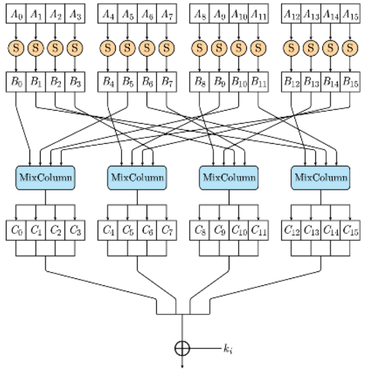
$\mathbf{0}$

Constructing asymmetric cryptography:
group theory + number theory

A different kind of primitives

- Symmetric crypto boils down to the security of a few *primitives*
  - Block ciphers, PRFs, hash functions
  - Good candidates: AES-256, SHA2-256
  - Why are these considered secure?
    - Answer: lots and lots of cryptanalysis
  - However, they are artificial and man-made



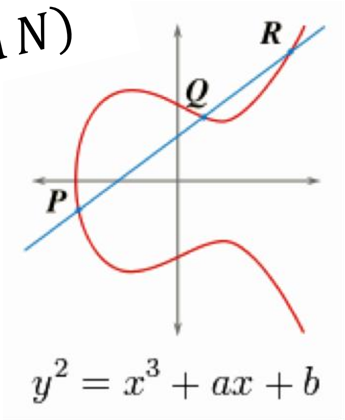

A_0 A_1 A_2 A_3 A_4 A_5 A_6 A_7 A_8 A_9 A_{10} A_{11} A_{12} A_{13} A_{14} A_{15}
S
B_0 B_1 B_2 B_3 B_4 B_5 B_6 B_7 B_8 B_9 B_{10} B_{11} B_{12} B_{13} B_{14} B_{15}
MixColumn
C_0 C_1 C_2 C_3 C_4 C_5 C_6 C_7 C_8 C_9 C_{10} C_{11} C_{12} C_{13} C_{14} C_{15}
k_i

- Want asymmetric crypto to be based on a few well-studied primitives too
  - Candidates now come from a different place:
    - *hard mathematical problems*
  - Good candidates: discrete logarithm problem, factoring
  - Much more algebraic structure

$$\boldsymbol{Z}_n^* \simeq \boldsymbol{Z}_{p_1}^* \times \boldsymbol{Z}_{p_2}^* \times \cdots \times \boldsymbol{Z}_{p_t}^*$$

$$C \leftarrow M^e \pmod N$$

$$e : G_1 \times G_2 \rightarrow G_T$$



Preliminaries

(integers)	$\boldsymbol{Z} = \{\dots, -2, -1, 0, 1, 2, 3, \dots\}$	
(reals)	$\boldsymbol{R}$ = the real numbers	$\boldsymbol{R}^* = \boldsymbol{R} \setminus \{0\}$
(integers “mod n”)	$\boldsymbol{Z}_n = \{0, 1, 2, \dots, n-1\}$	
(integers “mod p”)	$\boldsymbol{Z}_p = \{0, 1, 2, \dots, p-1\}$	$\boldsymbol{Z}_p^* = \boldsymbol{Z}_p \setminus \{0\}$

Examples:

$$\boldsymbol{Z}_{11} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\boldsymbol{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

Group – definition

Definition: A **group** $(G,\circ)$ is a set G together with a binary operation $\circ$ satisfying the following axioms.

$\mathcal{G}1$: $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c, \in G$ (associativity)

$\mathcal{G}2$: $\exists e \in G$ such that $e \circ a = a \circ e = a$ for all $a \in G$ (identity)

$\mathcal{G}3$: $\forall a \in G$ there exists $a^{-1} \in G$ such that $a \circ a^{-1} = a^{-1} \circ a = e$ (inverse)

A group is **abelian/commutative** if: $a \circ b = b \circ a$ for all $a, b \in G$

The **order** of a group is the number of elements in G, denoted $|G|$

Groups – examples

Definition: A **group** $(G,\circ)$ …

$\mathcal{G}1$: $(a \circ b) \circ c = a \circ (b \circ c)$ (associativity)
$\mathcal{G}2$: $\exists e \in G$: $e \circ a = a \circ e = a$ (identity)
$\mathcal{G}3$: $\exists a^{-1} \in G$: $a \circ a^{-1} = a^{-1} \circ a = e$ (inverse)

Groups

$(\boldsymbol{Z}, +)$ $e = 0$ $"3^{-1}" = -3$

$(\boldsymbol{R}, +)$ $e = 0$ $"(9/7)^{-1}" = -9/7$

$(\boldsymbol{R}^*, \cdot)$ $e = 1$ $(9/7)^{-1} = 7/9$

$(\boldsymbol{Z}_n, +_n)$ $e = 0$ $"3^{-1}" = x$: $3 + x \equiv 0 \bmod n$

$(\boldsymbol{Z}_p^*, \cdot_p)$ $e = 1$

$"3^{-1}" = x$: $3 \cdot x \equiv 1 \bmod p$

Not groups

$(\boldsymbol{Z}, \cdot)$ $2^{-1} = ?$

$(\boldsymbol{Z}, -)$ $(1-2)-3 \neq 1-(2-3)$

$(\boldsymbol{R}, \cdot)$ $0 \cdot x = 1?$

$(\boldsymbol{Z}_n, \cdot_n)$ $2x = 1 \pmod 4$?

$(\boldsymbol{Z}_p, \cdot_p)$

$(\boldsymbol{G}, \circ)$

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

$(\boldsymbol{Z}_3, +_3)$

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$(\boldsymbol{G}, \circ)$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

$(\boldsymbol{Z}_4, +_4)$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$(\boldsymbol{G}, \star)$

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Group arithmetic

$$g^0 \overset{\text{def}}{=} e$$

$$g^n \overset{\text{def}}{=} \overbrace{g \circ g \circ \cdots \circ g}^{n}$$

$$g^{-n} \overset{\text{def}}{=} (g^{-1})^n$$

Fact: $g^n g^m = \underbrace{\overbrace{g \circ \cdots \circ g}^{n} \circ \overbrace{g \circ \cdots \circ g}^{m}}_{n+m} = g^{n+m}$

Fact: $(g^n)^m = g^{nm} = (g^m)^n$

$(\boldsymbol{Z}, +)$: $\text{"}3^{15}\text{"} = \overbrace{3 + 3 + 3 + \cdots + 3}^{15} = 15 \cdot 3$

Cyclic groups

Definition: A **group** $(G,\circ)$ is **cyclic** if there exists $g \in G$ such that

$$G = \left\{ g^i \mid i \in \boldsymbol{Z} \right\} = \{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, g^3, \dots\}$$

Element g is called a **generator** for G and we write $(G,\circ) = \langle g \rangle$

Examples:

$$(\boldsymbol{Z}, +) = \langle 1 \rangle$$

$$(\boldsymbol{Z}_n, +_n) = \langle 1 \rangle$$

$$\left(\boldsymbol{Z}_p^*, \cdot\right) = \langle a \rangle$$

$$\begin{aligned}(\boldsymbol{Z}_7^*, \cdot) &= \langle 3 \rangle = \{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} \\ &= \langle 5 \rangle = \{5^0, 5^1, 5^2, 5^3, 5^4, 5^5\} = \{1, 5, 4, 6, 2, 3\} \\ &\neq \langle 2 \rangle = \{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4, 1, 2, 4\} = \{1, 2, 4\}\end{aligned}$$

Not cyclic groups:

$$(\boldsymbol{R}, +) \quad (\boldsymbol{R}^*, \cdot)$$

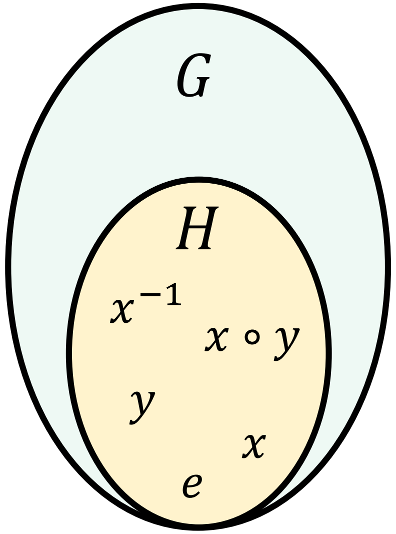
$(\boldsymbol{G}, \star)$

$\star$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Subgroups

Definition: A set $H \subseteq G$ is a **subgroup,** written $H < G$, if

$$\forall a, b \in H: \quad a \circ b \in H$$



Fact: a subgroup H is a group

Examples:

$\{e\} < G$ (for all groups)

$G < G$ (for all groups)

$2\boldsymbol{Z} = \{\dots, -2, 0, 2, 4, 6, \dots\} < (\boldsymbol{Z}, +)$

$3\boldsymbol{Z} = \{\dots, -3, 0, 3, 6, 9, \dots\} < (\boldsymbol{Z}, +)$

positive real numbers

$\boldsymbol{R}_+ < (\boldsymbol{R}^*, \cdot)$

$\{1, -1\} < (\boldsymbol{R}^*, \cdot)$

$\langle 20 \rangle < \langle 10 \rangle < \langle 5 \rangle < (\boldsymbol{Z}_{40}, +)$

$\langle 5 \rangle = \{0, 5, 10, \dots, 35\}$
$\langle 10 \rangle = \{0, 10, 20, 30\}$
$\langle 20 \rangle = \{0, 20\}$

Cyclic groups

Theorem: if $(G,\circ)$ is a finite group, then for all $g \in G$:

$$g^{|G|} = e$$

Proof (finite cyclic groups):

$|G| = |\langle g \rangle| = n$

$$\overbrace{e \quad g^1 \quad g^2 \quad g^3 \quad \cdots \quad g^{n-1}}^{G} \quad g^n \quad g^{n+1} \quad g^{n+2} \quad \cdots$$

$g^n = g^3 \quad \Longrightarrow \quad g^{n-3} = e \quad \Longrightarrow \quad g^j = e \quad j < n$ contradiction!

Corollary I: $g^i = g^{i \bmod n} = g^{i \bmod |G|}$

Corollary II (Lagrange's theorem): if $H < G$ then the order of H divides the order of G (i.e $|H| \mid |G|$)

Groups of prime order

Corollary II (Lagrange's theorem): if $H < G$ then the order of H divides the order of G

Fact: any prime-order group is cyclic

Fact: any non-trivial element ($\neq e$) in a prime-order group is a generator

Warning: $\left(\boldsymbol{Z}_p^*, \cdot\right)$ is *not* a prime-order group! $\left|\boldsymbol{Z}_p^*\right| = p - 1$

Suppose $p = 2q + 1$, with q being prime; what are the possible sub-groups of $\left(\boldsymbol{Z}_p^*, \cdot\right)$?

$$\left|\boldsymbol{Z}_p^*\right| = p - 1 = 2q$$

$$\boldsymbol{Z}_p^* = \begin{cases} \{1\}, \\ \{1, -1\}, \\ H, \\ \boldsymbol{Z}_p^* \end{cases} \qquad |H| = q$$

Example: $\boldsymbol{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$

$11 = 2 \cdot 5 + 1$

$\{1\} < \boldsymbol{Z}_{11}^*$

$\{1, -1\} = \{1,10\} < \boldsymbol{Z}_{11}^*$

$H = \langle 3 \rangle = \langle 4 \rangle = \langle 5 \rangle = \langle 9 \rangle = \{1, 3, 4, 5, 9\} < \boldsymbol{Z}_{11}^*$

$\boldsymbol{Z}_{11}^* < \boldsymbol{Z}_{11}^*$

Before the break

- Groups
- Subgroups
- Cyclic groups
    - $(\boldsymbol{Z}_p^*, \cdot)$
- Prime order groups
    - Not $(\boldsymbol{Z}_p^*, \cdot)$! (order $p-1$)
    - $H < (\boldsymbol{Z}_p^*, \cdot)$ (prime-order subgroup)

Diffie-Hellman

$G = \langle g \rangle$ public

$$\xrightarrow{A = g^{a}}$$

$$\xleftarrow{B = g^{b}}$$

$a \overset{\$}{\leftarrow} \{1, \dots, |G|\}$

$b \overset{\$}{\leftarrow} \{1, \dots, |G|\}$

$Z \leftarrow B^{a} = (g^{b})^{a} = g^{ab}$

$Z' \leftarrow A^{b} = (g^{a})^{b} = g^{ab}$

Claim: $Z = Z'$

Diffie-Hellman – example

$$\boldsymbol{Z}^*_{1019} = \langle 2 \rangle$$

$$\xrightarrow{570}$$

$$\xleftarrow{72}$$

$493 \overset{\$}{\leftarrow} \{1, \dots, 1018\}$

$570 \leftarrow 2^{493} \bmod 1019$

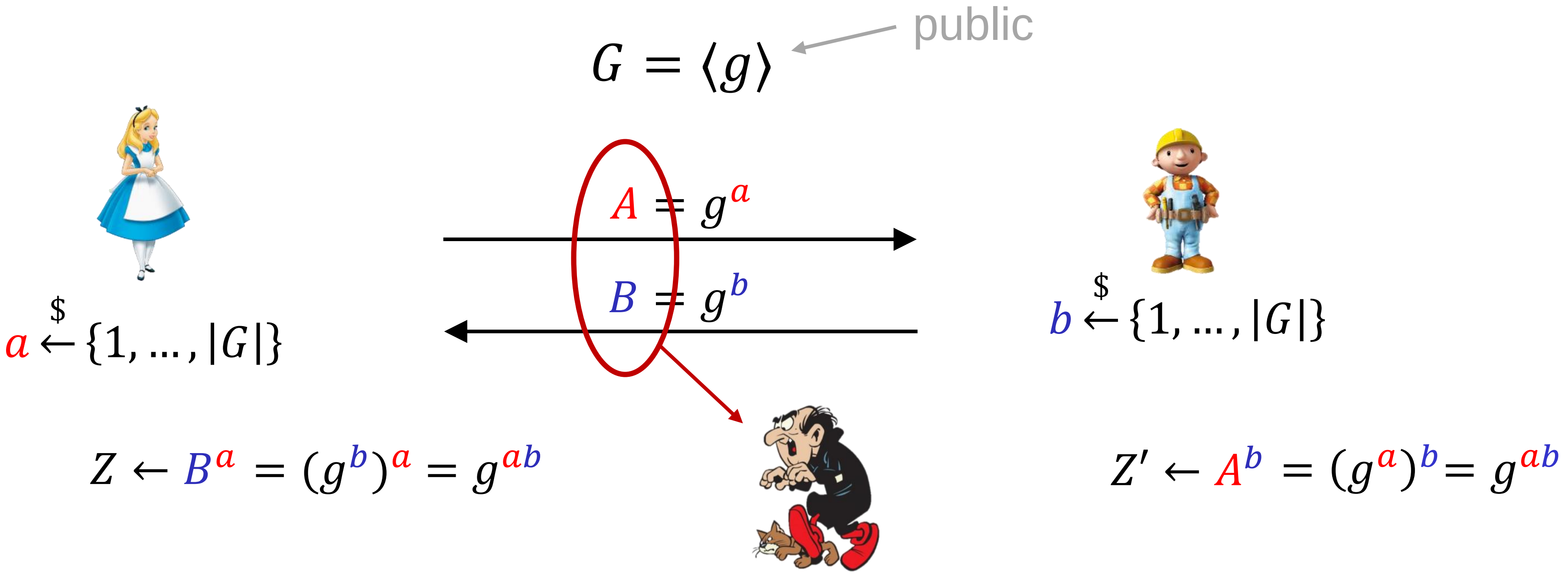
$Z \leftarrow 72^{493} \bmod 1019 \equiv \mathbf{531}$

$901 \overset{\$}{\leftarrow} \{1, \dots, 1018\}$

$72 \leftarrow 2^{901} \bmod 1019$

$Z' \leftarrow 570^{901} \bmod 1019 \equiv \mathbf{531}$

Diffie-Hellman



$G = \langle g \rangle$ public

$a \overset{\$}{\leftarrow} \{1, \dots, |G|\}$

$A = g^{a}$

$B = g^{b}$

$b \overset{\$}{\leftarrow} \{1, \dots, |G|\}$

$Z \leftarrow B^{a} = (g^{b})^{a} = g^{ab}$

$Z' \leftarrow A^{b} = (g^{a})^{b} = g^{ab}$

Security:

- Must be hard to compute $Z \leftarrow g^{ab}$ given g, A, B (DH assumption)
- Must be hard to find a (or b) given g, A, B (DLOG assumption)

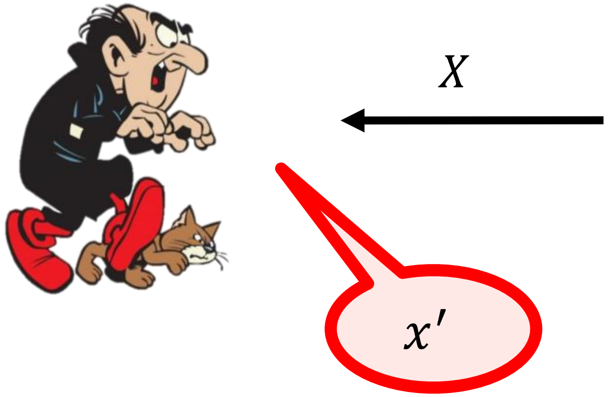
Doesn't work: $A \circ B = g^{a} \circ g^{b} = g^{a+b} \neq g^{ab}$

Discrete logarithm (DLOG) problem

```
$\mathbf{Exp}^{\mathrm{dl}}_{G,g}(A)$

$x \overset{\$}{\leftarrow} \{1,2,\dots,|G|\}$
$X \leftarrow g^x$
$x' \leftarrow A(X)$
**return** $x \overset{?}{=} x$
```

Public: $G = \langle g \rangle$



Challenger

$x \overset{\$}{\leftarrow} \{1,2,\dots,|G|\}$

$X \leftarrow g^x$

Adversary wins if $x' = x$

In other words: $x' = \mathrm{DLog}_g(X)$

Definition: The **DLOG-advantage** of an adversary A is

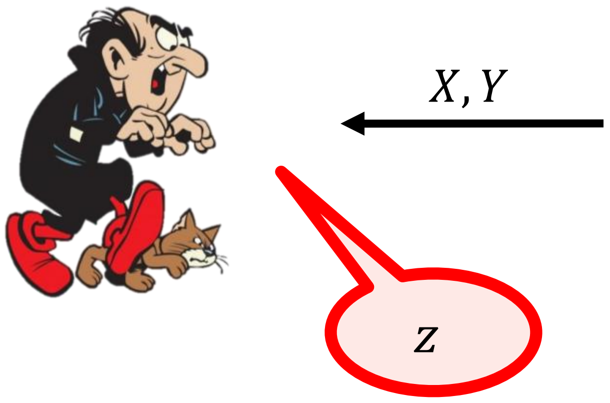
$$\mathbf{Adv}^{\mathrm{dlog}}_{G,g}(A) = \Pr\left[\mathbf{Exp}^{\mathrm{dlog}}_{G,g}(A) \Rightarrow \mathrm{true}\right]$$

Diffie-Hellman problem

$\mathbf{Exp}^{\mathrm{dh}}_{G,g}(A)$

```
$x, y \overset{\$}{\leftarrow} \{1,2,\dots,|G|\}$
$X \leftarrow g^x$
$Y \leftarrow g^y$
$z \leftarrow A(X, Y)$
return $g^z \overset{?}{=} g^{xy}$
```

Public: $G = \langle g \rangle$



X, Y

z

Challenger

$x, y \overset{\$}{\leftarrow} \{1,2,\dots,|G|\}$

$X \leftarrow g^x$

$Y \leftarrow g^y$

Adversary wins if $g^z = g^{xy}$

Definition: The **DH-advantage** of an adversary A is

$$\mathbf{Adv}^{\mathrm{dh}}_{G,g}(A) = \Pr\left[\mathbf{Exp}^{\mathrm{dh}}_{G,g}(A) \Rightarrow \mathrm{true}\right]$$

DLOG vs. DH

$\mathbf{Exp}^{\mathrm{dlog}}_{G,g}(A)$

```
$x \xleftarrow{\$} \{1,2,\ldots,|G|\}$
$X \leftarrow g^x$
$x' \leftarrow A(X)$
return $x \overset{?}{=} x$
```

$\mathbf{Exp}^{\mathrm{dh}}_{G,g}(A)$

```
$x, y \xleftarrow{\$} \{1,2,\ldots,|G|\}$
$X \leftarrow g^x$
$Y \leftarrow g^y$
$z \leftarrow A(X,Y)$
return $g^z \overset{?}{=} g^{xy}$
```

DLOG security $\Leftarrow$ DH security

DLOG security $\overset{?}{\Longrightarrow}$ DH security

Algorithms for solving DLOG

- Generic algorithms; works for *all* (cyclic) groups
  - Brute-force
    1. Given g and $X \in G$
    2. for $i = 1, 2, \ldots, |G|$ check if $g^i = X$

    running time: $\mathcal{O}(|G|) \approx \mathcal{O}(2^n)$, given $|G| \approx 2^n$

  - Are there better algorithms?

- Group-specific algorithms; exploits algebraic features of given group

Solving DLOG: the baby-step giant-step algorithm

Given: $X \leftarrow g^x$

Find: x

$Y \leftarrow g^n$ $\quad n \leftarrow \left\lceil \sqrt{|G|} \right\rceil$

$$\mathcal{O}\left(\sqrt{|G|} \cdot \log \sqrt{|G|}\right) \approx \mathcal{O}\left(\sqrt{|G|}\right)$$

$$\mathcal{O}\left(\sqrt{|G|}\right) \left\{ \begin{array}{l} X_0 \leftarrow Xg^{-0} \\ X_1 \leftarrow Xg^{-1} \\ X_2 \leftarrow Xg^{-2} \\ X_3 \leftarrow Xg^{-3} \\ \quad\vdots \\ X_i \leftarrow Xg^{-i} \\ \quad\vdots \\ X_n \leftarrow Xg^{-n} \end{array} \right.$$

Find “collision”: $X_i = Y^j$

$$Xg^{-i} \cdot g^i = g^{nj} \cdot g^i$$

$$X = g^{nj+i}$$

$$\mathrm{DLog}(X) = \mathrm{DLog}\left(g^{nj+i}\right)$$

$$x = nj + i$$

Time + memory: $\mathcal{O}\left(\sqrt{|G|}\right)$

$$\left. \begin{array}{l} Y^0 \\ Y^1 \\ Y^2 \\ Y^3 \\ \vdots \\ Y^j \\ \vdots \\ Y^n \end{array} \right\} \mathcal{O}\left(\sqrt{|G|}\right)$$

Generic algorithms for solving DLOG

- Baby-step, giant-step: time $\mathcal{O}\left(\sqrt{|G|}\right)$ memory $\mathcal{O}\left(\sqrt{|G|}\right)$
- Pollard's rho: time $\mathcal{O}\left(\sqrt{|G|}\right)$ memory $\mathcal{O}(1)$
- Pohlig-Hellman: time $\max_p \mathcal{O}(\sqrt{p})$ memory $\mathcal{O}(1)$ $\left(|G| = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}\right)$

- **Nechaev '94 & Shoup '97:** Solving DLog requires time $\Omega\left(\sqrt{|G|}\right)$ in *generic* groups

- Consequence: $\sqrt{|G|}$ must be large enough
  - $|G| \approx 2^{128}$ only gives $\sqrt{2^{128}} = 2^{64}$ security
  - $|G| \approx 2^{256}$ only gives $\sqrt{2^{256}} = 2^{128}$ security
  - $|G| \approx 2^{512}$ only gives $\sqrt{2^{512}} = 2^{256}$ security
  - etc...

Non-generic algorithms for DLOG

- Unfortunately, $(\boldsymbol{Z}_p^*, \cdot)$ is *not* a generic group!

- *Much* faster specific algorithms exist for solving DLOG in $\boldsymbol{Z}_p^*$
  - Index-calculus
  - Elliptic-curve method
  - Special number-field sieve (SNFS)
  - General number-field sieve (GNFS)

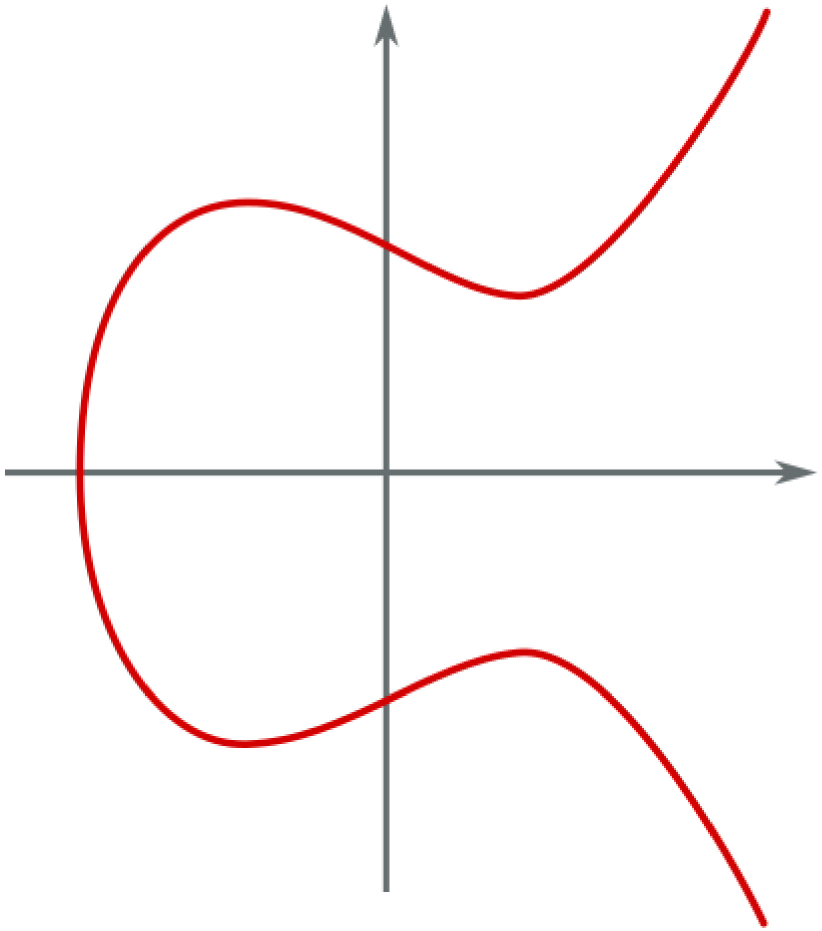
  } *exceptionally* complicated algorithms, requiring very advanced mathematics!

- Current DLOG-solving record: $|\boldsymbol{Z}_p^*| \approx 2^{795}$ using GNFS (Heninger et al. '19)
  - Previous records: https://en.wikipedia.org/wiki/Discrete_logarithm_records

- $|\boldsymbol{Z}_p^*| \geq 2^{2048}$ typically required as a minimum today

Better alternatives to $\boldsymbol{Z}_p^*$?

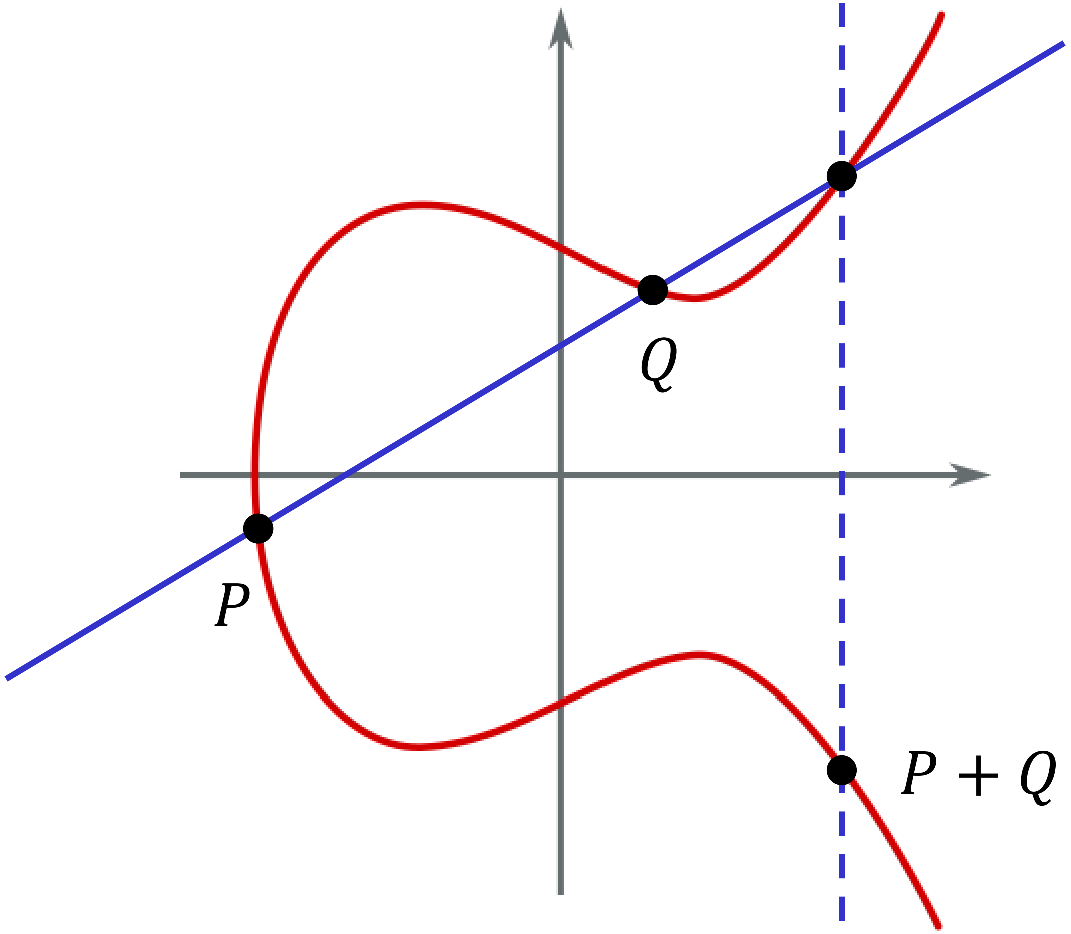
Elliptic curves



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

$$a, b, x, y \in \boldsymbol{R}$$

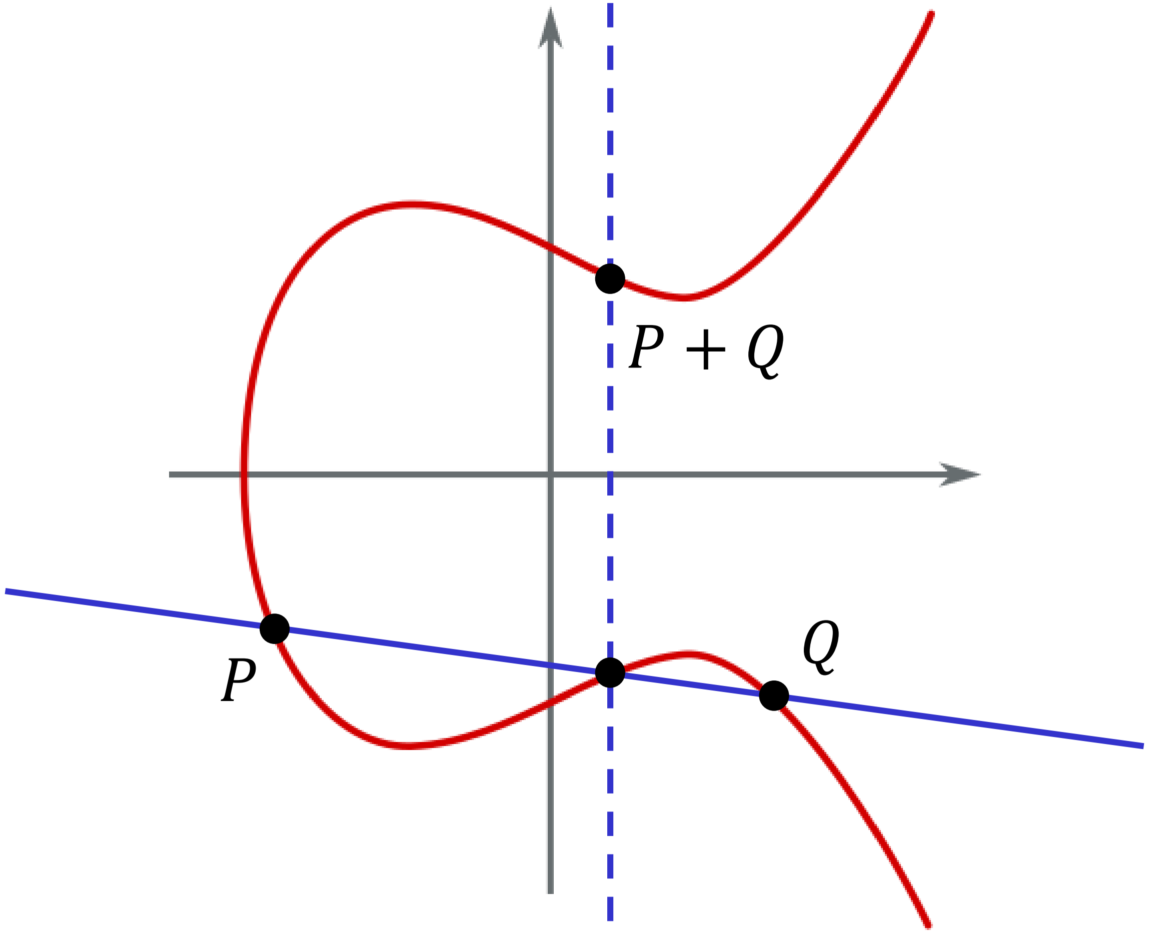
Elliptic curves



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

$$a, b, x, y \in \boldsymbol{R}$$

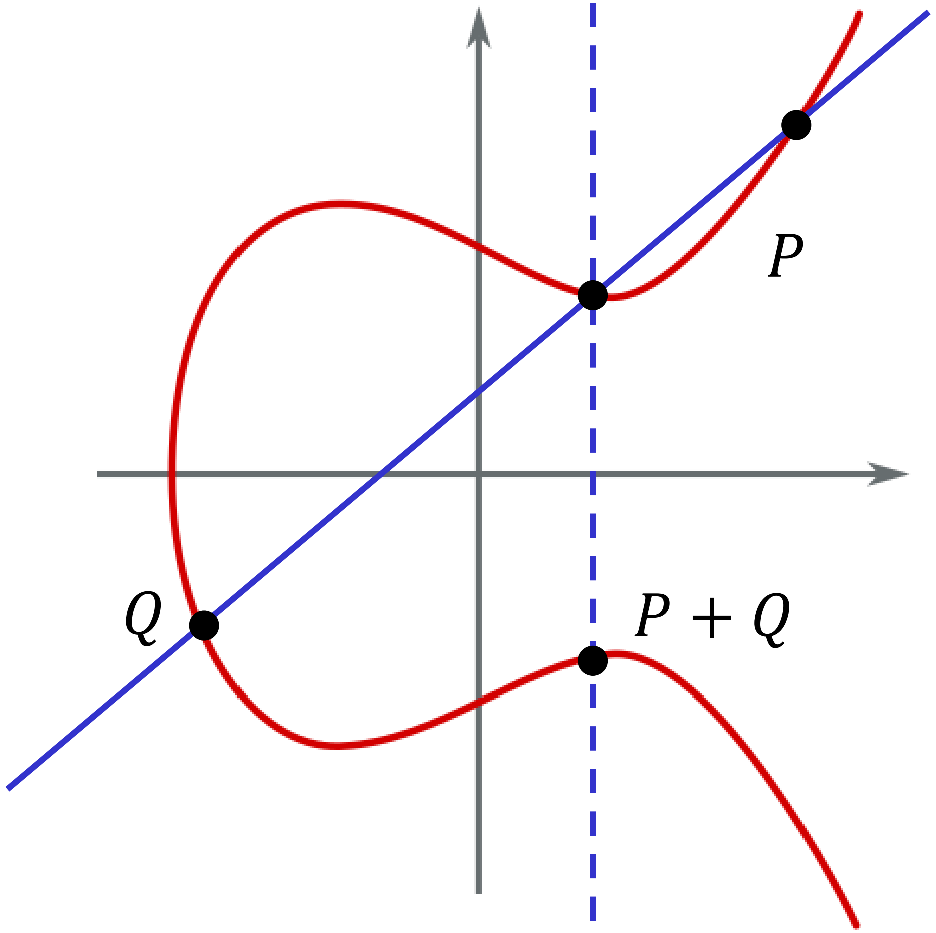
Elliptic curves



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

$$a, b, x, y \in \boldsymbol{R}$$

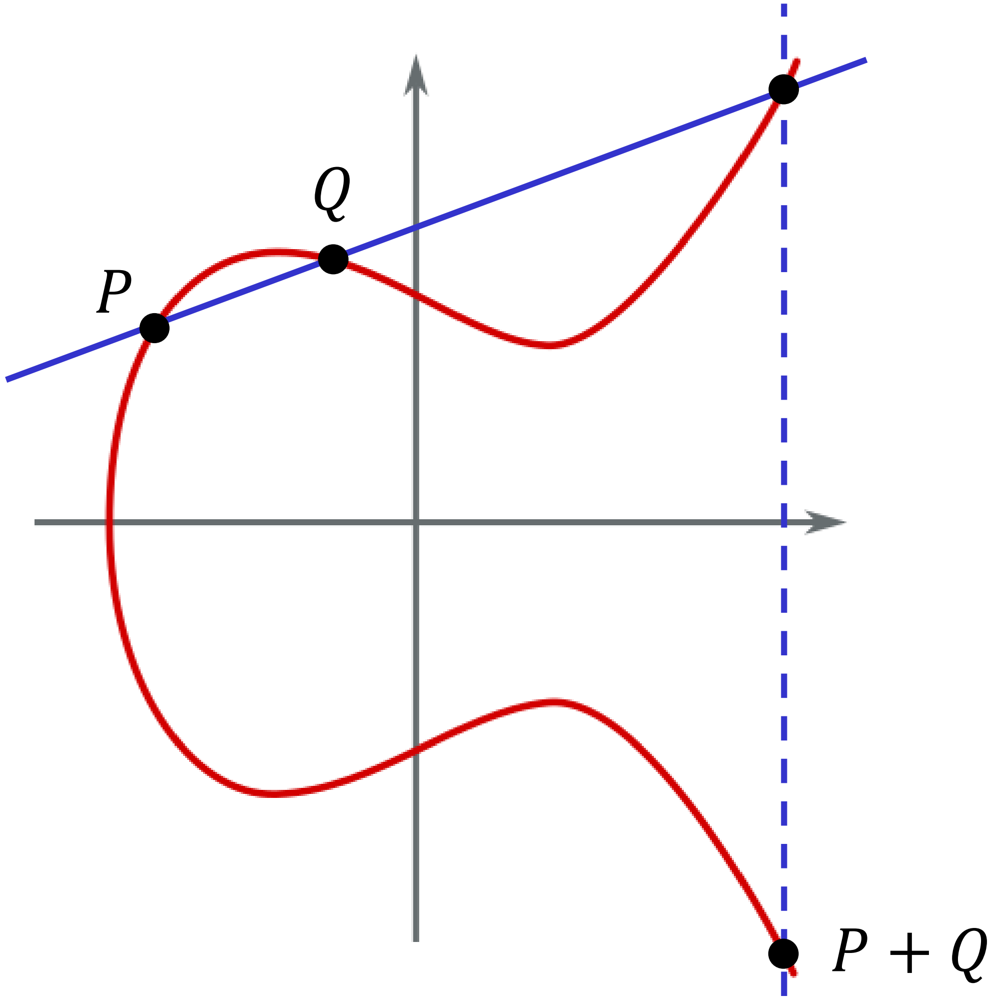
Elliptic curves



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

$$a, b, x, y \in \boldsymbol{R}$$

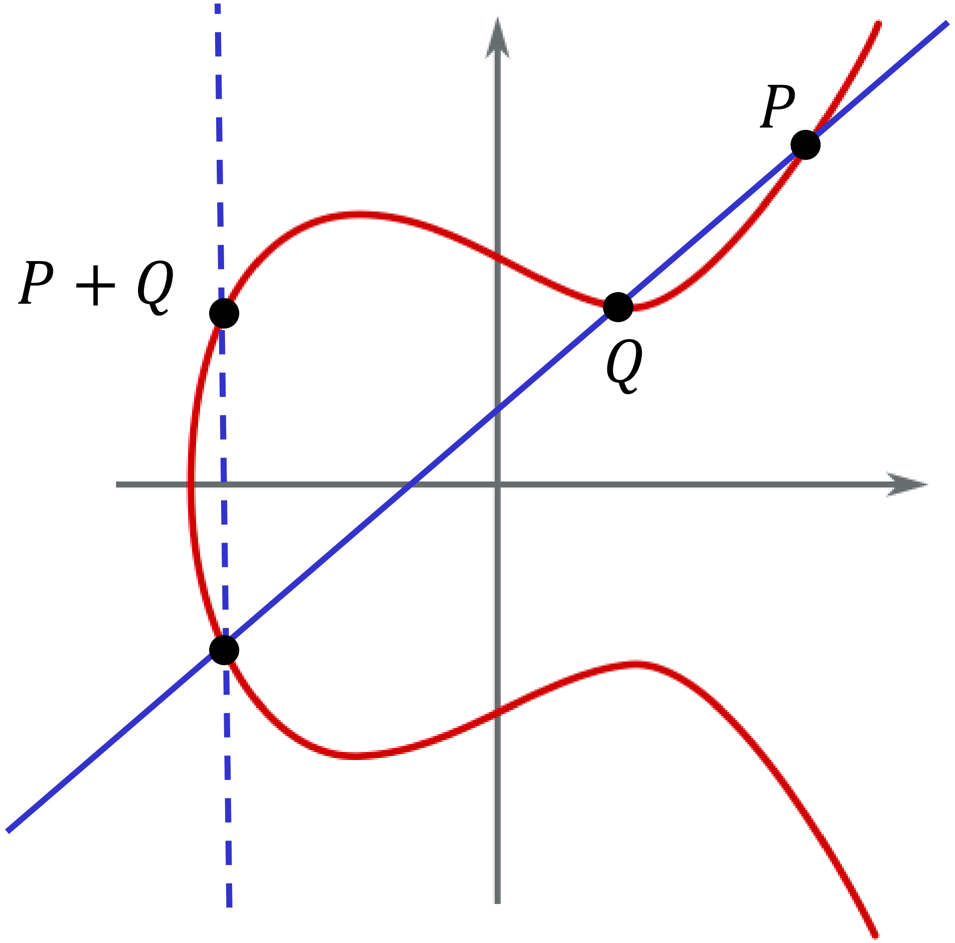
Elliptic curves



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

$$a, b, x, y \in \boldsymbol{R}$$

Elliptic curves



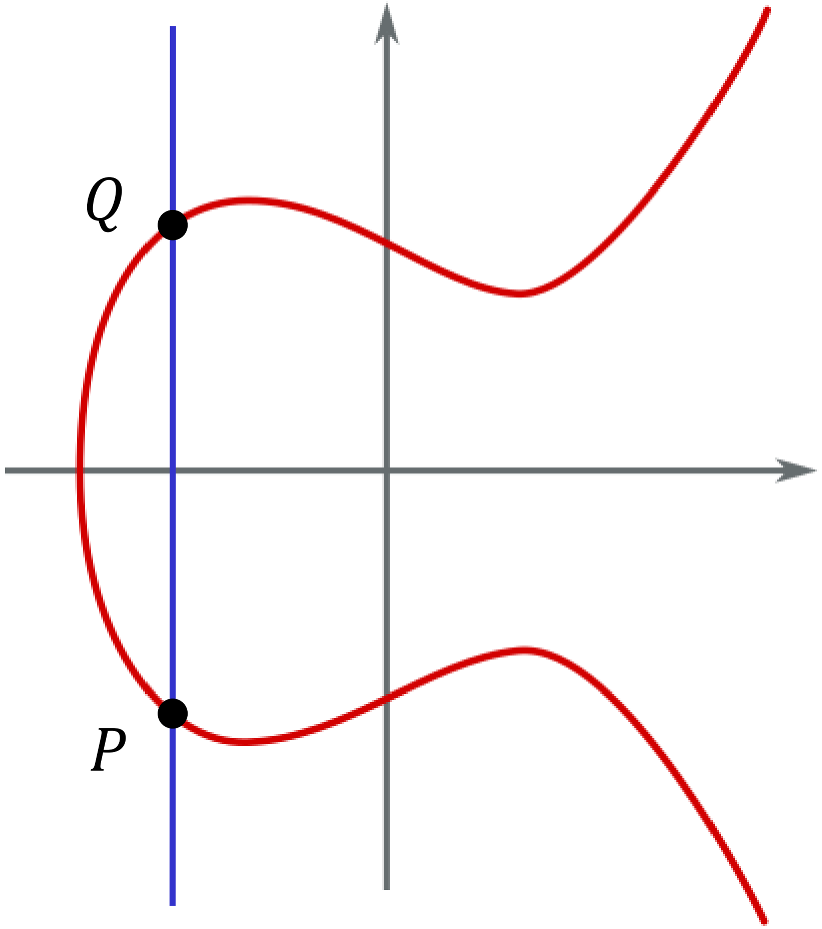
$$y^2 = x^3 + ax + b$$

$$a, b, x, y \in \boldsymbol{R}$$

Elliptic curves

$P + Q = \mathcal{O}$

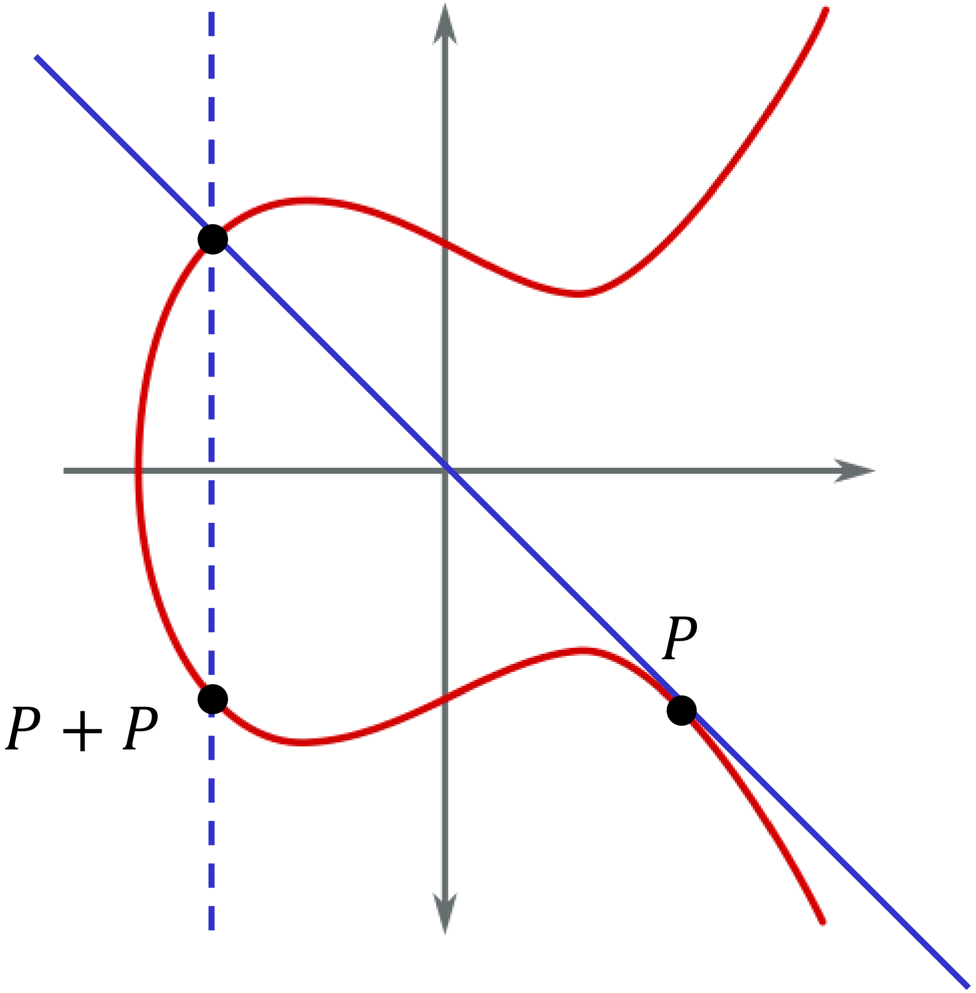
Identity element



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

$a, b, x, y \in \boldsymbol{R}$

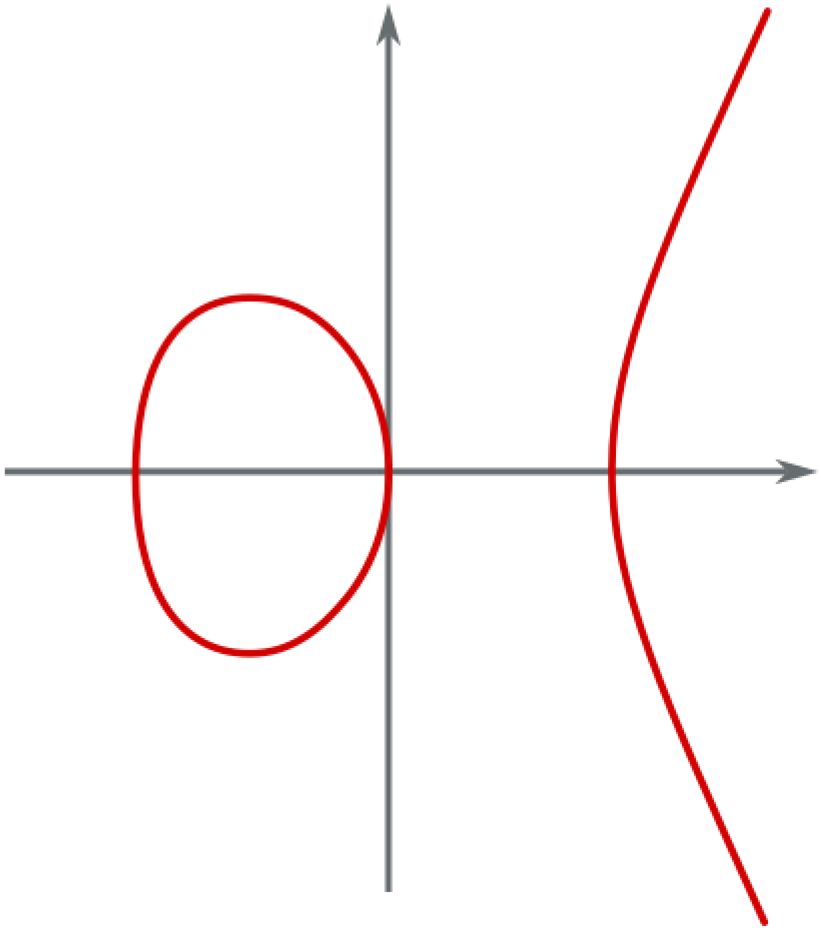
Elliptic curves



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

$$a, b, x, y \in \boldsymbol{R}$$

Elliptic curves

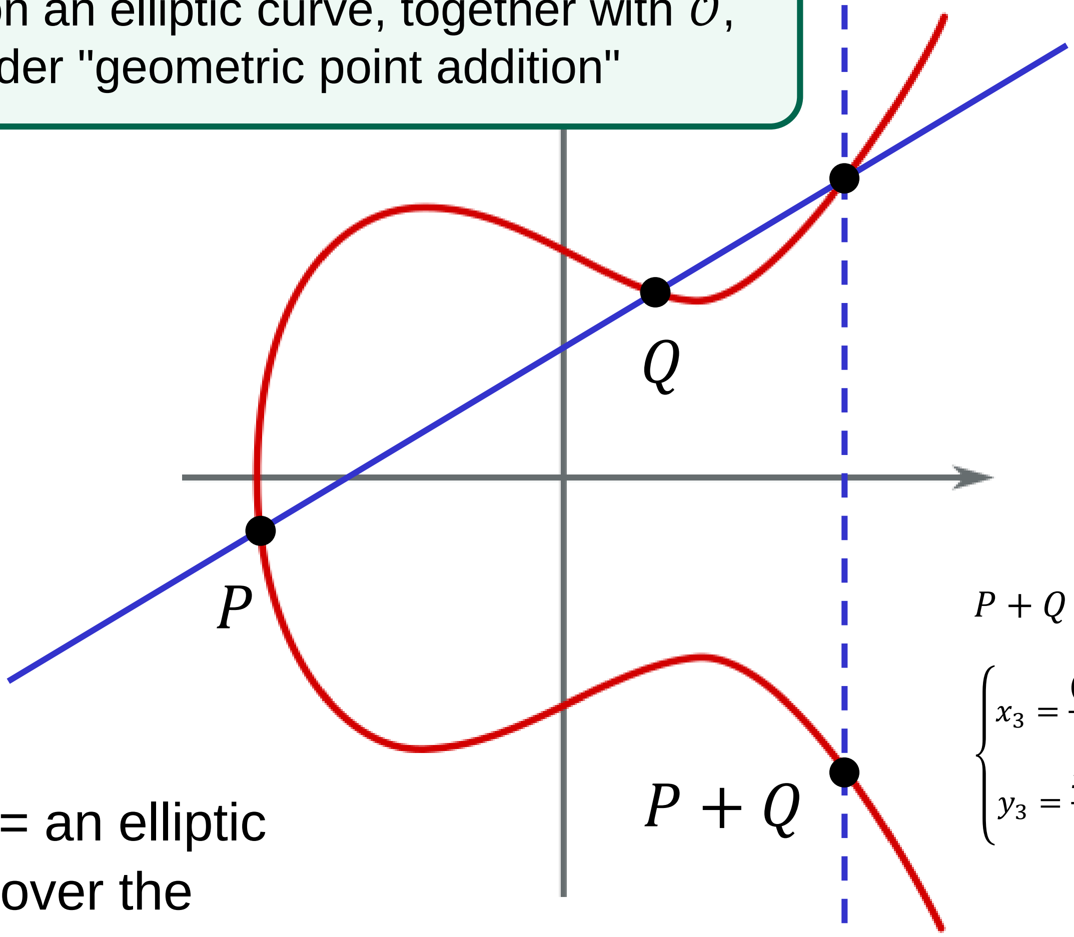


$$y^2 = x^3 + a'x + b'$$

$$a', b', x, y \in \boldsymbol{R}$$

Elliptic curves

Theorem: the points on an elliptic curve, together with $\mathcal{O}$, is an abelian group under "geometric point addition"



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

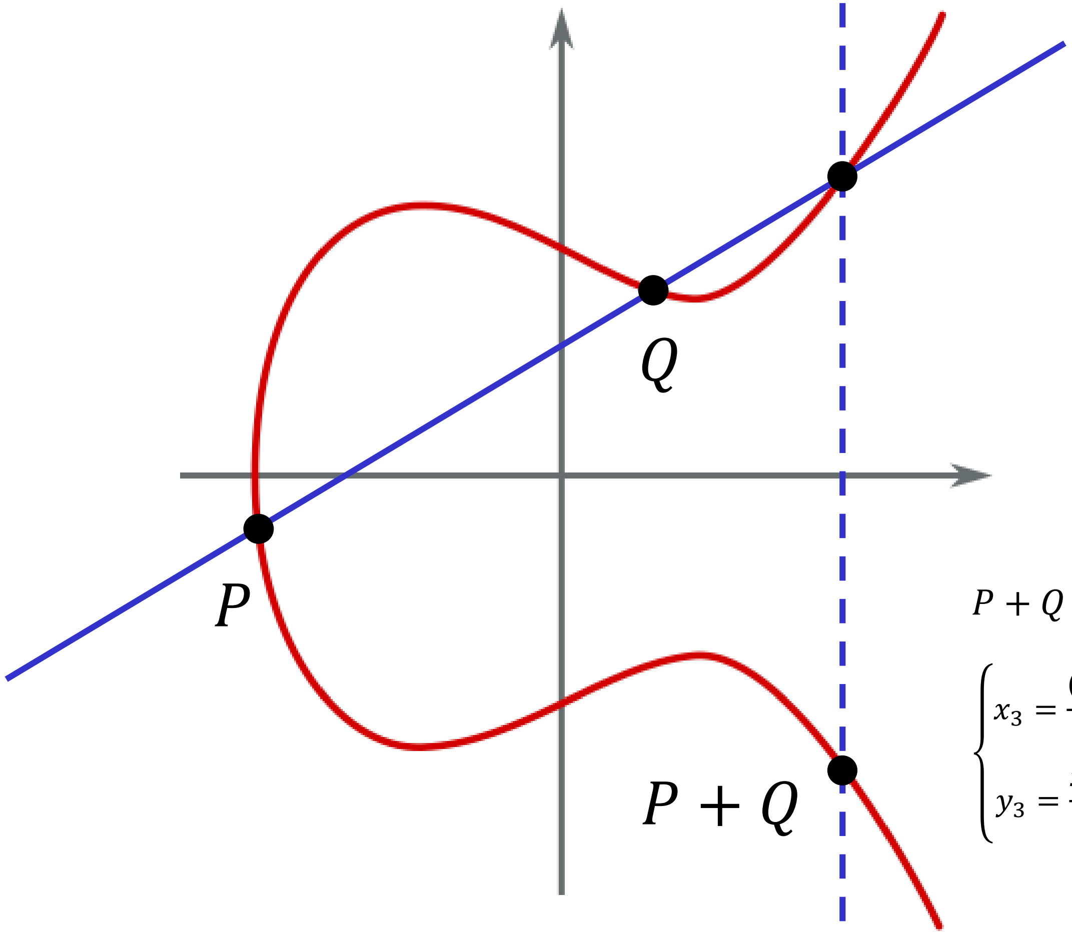
$$a, b, x, y \in \boldsymbol{R}$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$\begin{cases} x_3 = \dfrac{(x_1x_2 - 2a)x_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1x_2 + a)(x_1 + x_2) + 2y_1y_2 + 2b} \\ y_3 = \dfrac{x_1x_2(x_1 + x_2) - x_3\big((x_1 + x_2)^2 - x_1x_2 + a\big) - y_1y_2 - b}{y_1 + y_2} \end{cases}$$

Notation: $(E(\boldsymbol{R}), +)$ = an elliptic curve group defined over the reals

Elliptic curves



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

$$a, b, x, y \in \boldsymbol{Z}_p$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

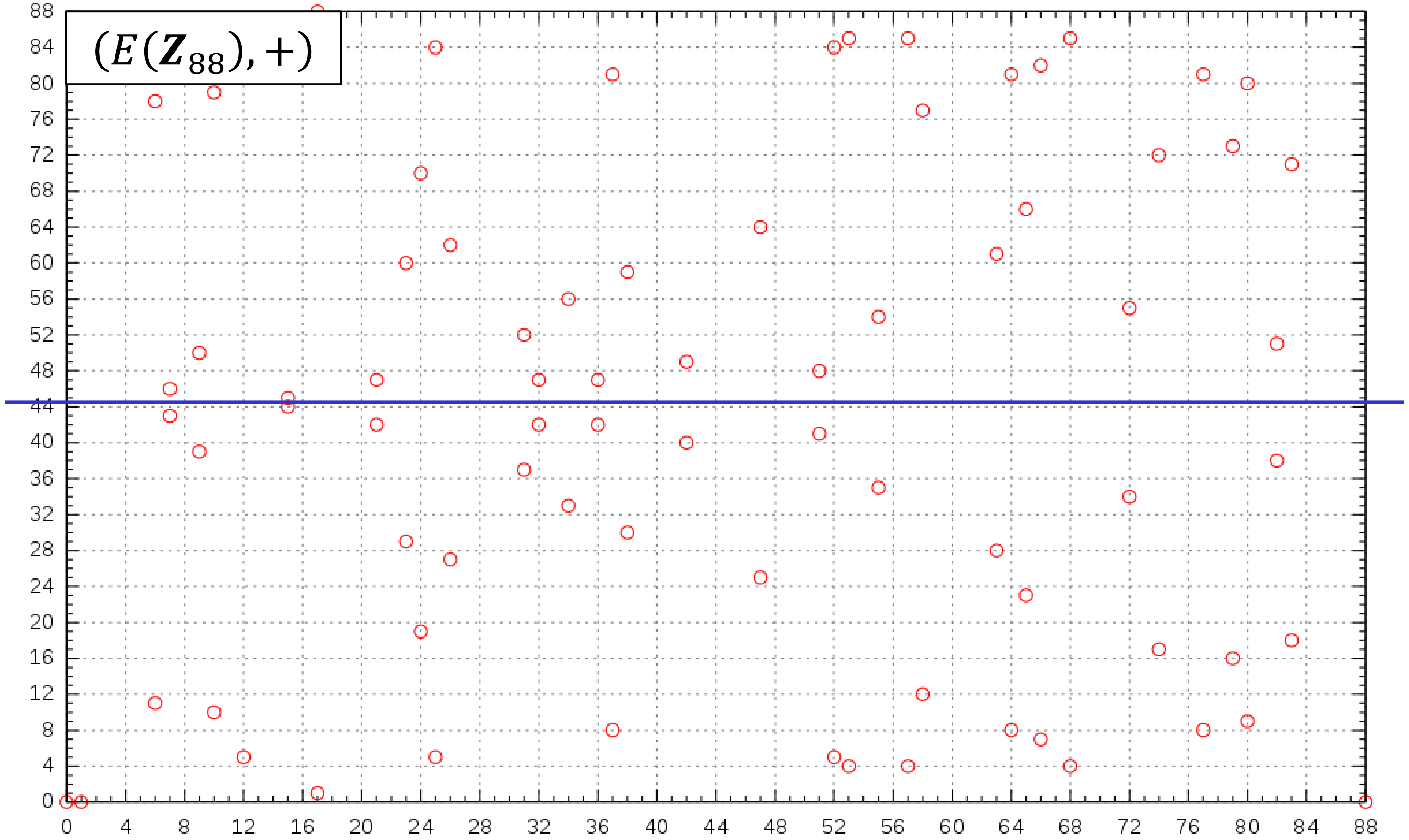
$$\begin{cases} x_3 = \dfrac{(x_1x_2 - 2a)x_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1x_2 + a)(x_1 + x_2) + 2y_1y_2 + 2b} \\ y_3 = \dfrac{x_1x_2(x_1 + x_2) - x_3\big((x_1 + x_2)^2 - x_1x_2 + a\big) - y_1y_2 - b}{y_1 + y_2} \end{cases}$$

Still valid!

Elliptic curves

Theorem: the points on an elliptic curve, together with $\mathcal{O}$, is an abelian group under "geometric point addition"

Notation: $(E(\boldsymbol{Z}_p),+)$ = an elliptic curve group defined over $\boldsymbol{Z}_p$



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

$$a, b, x, y \in \boldsymbol{Z}_{88}$$

$$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3, y_3)$$

$$\begin{cases} x_3 = \dfrac{(x_1x_2 - 2a)x_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1x_2 + a)(x_1 + x_2) + 2y_1y_2 + 2b} \\ y_3 = \dfrac{x_1x_2(x_1 + x_2) - x_3\big((x_1 + x_2)^2 - x_1x_2 + a\big) - y_1y_2 - b}{y_1 + y_2} \end{cases}$$

$\boldsymbol{E}(\boldsymbol{Z}_p)$ – properties

- Recall: $(\boldsymbol{Z}_p^*, \cdot)$ is *not* a generic group
    - Specialized attacks (GNFS) exploit algebraic structure $\Longrightarrow$ parameters must be bigger to compensate
    - $|\boldsymbol{Z}_p^*| \geq 2^{2048}$ required for security today
    - Bigger parameters $\Longrightarrow$ slower systems

- Currently no attacks that manage to exploit the algebraic structure of $(E(\boldsymbol{Z}_p^*), +)$
    - Best-know attacks are *generic attacks*:
        - Baby-step giant-step
        - Pollard-rho
        - etc…
    - **Nechaev '94 & Shoup '97:** *Generic* algorithms for solving DLog requires time $\Omega\left(\sqrt{|G|}\right)$
    - Consequently: elliptic curve crypto can use *much* smaller parameters
        - $|E(\boldsymbol{Z}_p)| = 2^{256}, 2^{384}, 2^{512}$ common in practice
        - Much faster than $\boldsymbol{Z}_p^*$-based crypto

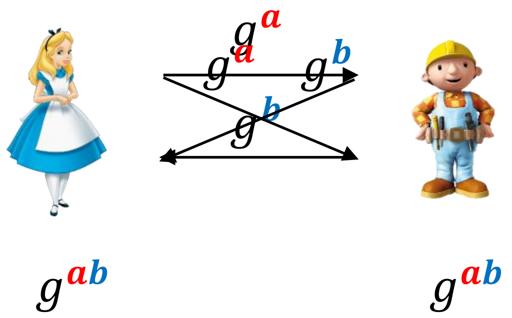
Cryptographic groups in practice

- $(\boldsymbol{Z}_p^*, \cdot)$ groups:
  - **TLS 1.3:** five specific groups allowed
    - size $\approx 2^{2048}, 2^{3072}, 2^{4096}, 2^{6144}, 2^{8192}$ (RFC 7919)
  - **IKEv2** (IPsec key exchange protocol): MODP groups
    - size $\approx 2^{768}, 2^{1024}, 2^{1536}, 2^{2048}, 2^{3072}, 2^{4096}, 2^{6144}, 2^{8192}$ (RFC 7296 and RFC 3526)
  - all p's are **safe primes** (i.e., of the form $p = 2q + 1$ where q is prime)

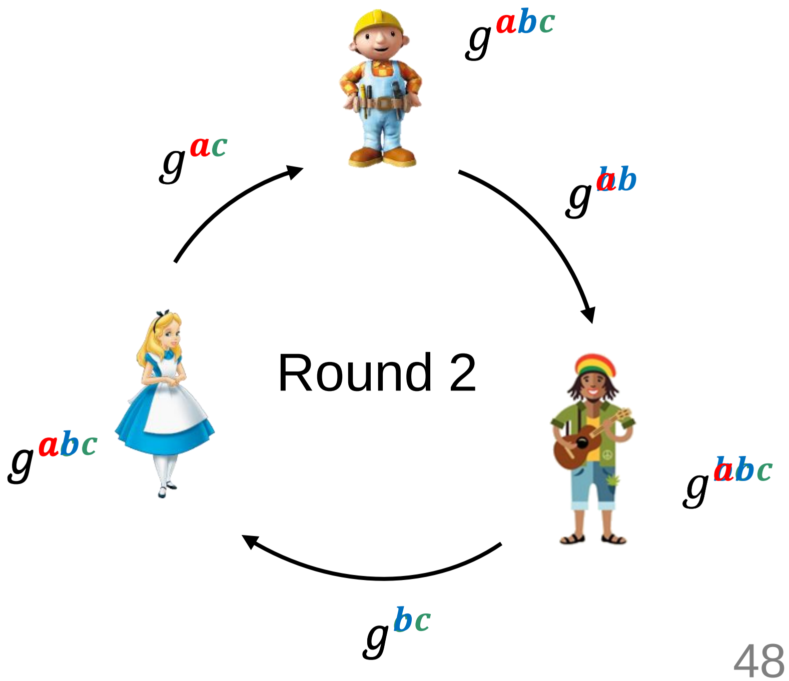
- $(E(\boldsymbol{Z}_p^*), +)$ groups
  - NIST groups: P-224, P-256, P-384, P-521
  - Curve25519 ($E : y^2 = x^3 + 486662x^2 + x$ and $p = 2^{255} - 19$) (Daniel J. Bernstein)
  - Curve448 ($E : y^2 + x^2 = 1 - 39081x^2y^2$ and $p = 2^{448} - 2^{224} - 1$) (Mike Hamburg)

N-party Diffie-Hellman

- N-party Diffie-Hellman possible in $N-1$ rounds



- 1-round N-party Diffie-Hellman:
  - $N=2$ – normal Diffie-Hellman
  - $N=3$ – Diffie-Hellman with *bilinear pairings* (**Joux ’00**)
  - $N \geq 4$ – open problem
    - Possible with *multilinear maps* (very advanced)
    - But we don’t know any secure multilinear maps



Summary

- Group theory
  - Group definition (associativity, identity, inverses)
  - Subgroups
  - Cyclic (subgroups)

- Diffie-Hellman key exchange protocol described in a generic group
  - Discrete logarithm (DLOG) problem and Diffie-Hellman (DH) problem must be hard in the concrete group used

- Two main groups used in cryptography (where DLOG and DH problems are believed to be hard):
  - $\left(\boldsymbol{Z}_p^*, \cdot\right)$ the group of non-zero integers modulo a prime p
    - Best algorithm to solve DLOG is the General Number Field Sieve (GNFS) which exploits the algrabraic structure of $\boldsymbol{Z}_p$
  - $\left(E\left(\boldsymbol{Z}_p\right), +\right)$ elliptic curve groups
    - Elements are points satisfying $y^2 = x^3 + ax + b$ where $a, b, x, y \in \boldsymbol{Z}_p$ (additionally, we need an identity element, which we artificially define to be the element $\mathcal{O}$. Note that $\mathcal{O}$ does *not* lay on the curve)
    - Group operation is "addition of points on curve" where the operation is motivated by the geometric idea
    - GNFS does not apply; best-known DLOG algorithms are *generic*: baby-step, giant-step, Pollard-rho, Pohlig-Hellman
    - Can use much smaller parameters $\Longrightarrow$ much faster than $\left(\boldsymbol{Z}_p^*, \cdot\right)$-based DH