Eliptické křivky

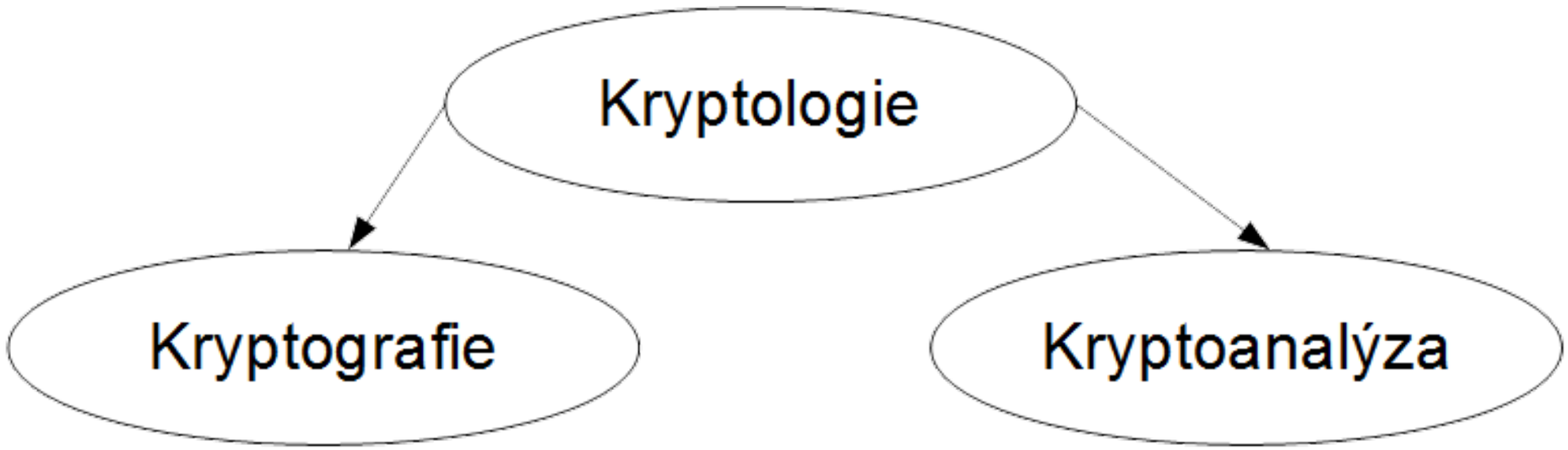
Petr Nižnanský

Agenda

- Symetrická a asymetrická kryptografie
- Eliptické křivky
  - Sčítání bodů
  - Problém diktrétní logaritmu
  - ECC v praxi

Kryptologie

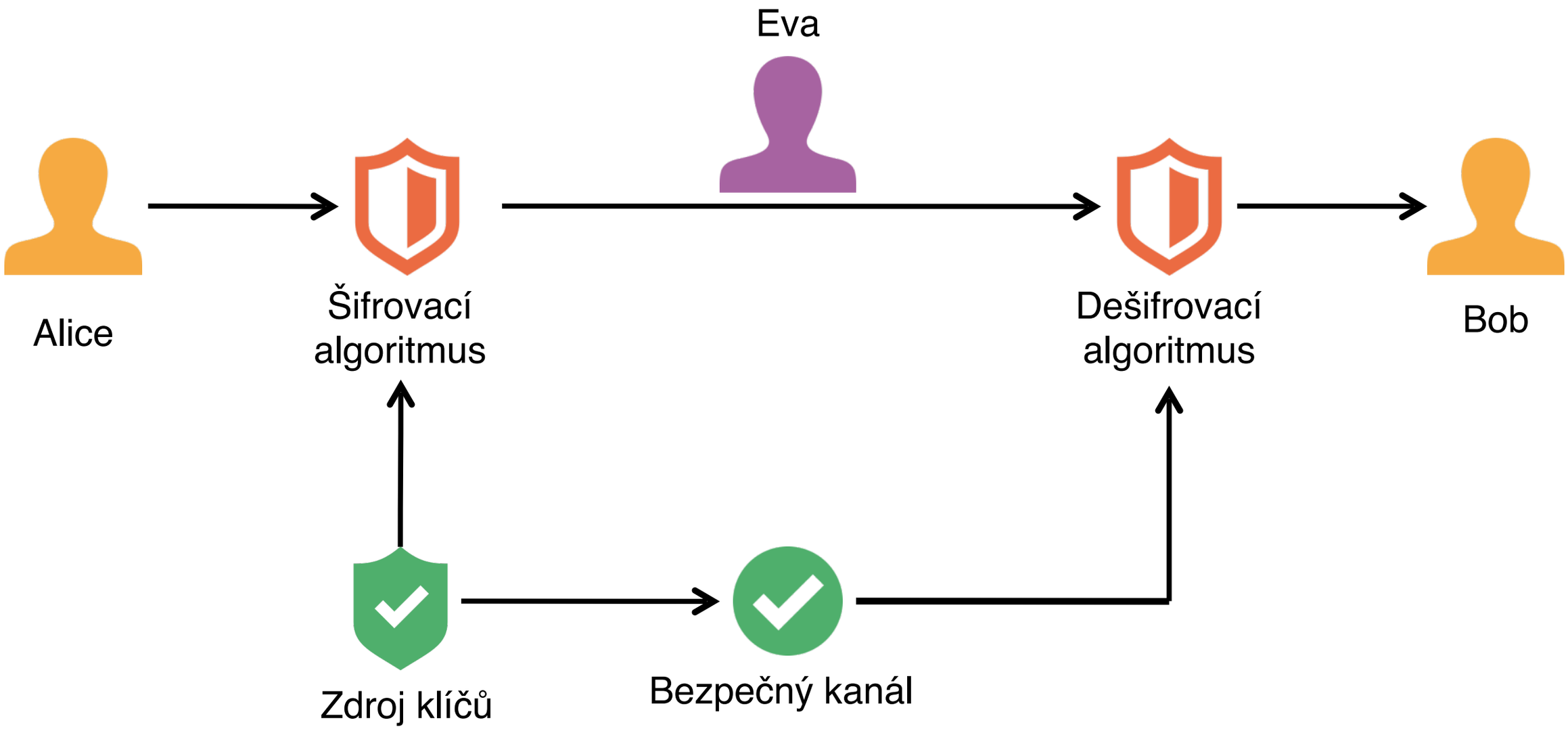
- z řečtiny kryptós tajný nebo skrytý, logos věda



návrh šifrovacích systémů

odhalování slabin v šifrovacích systémech

Symetrická kryptografie

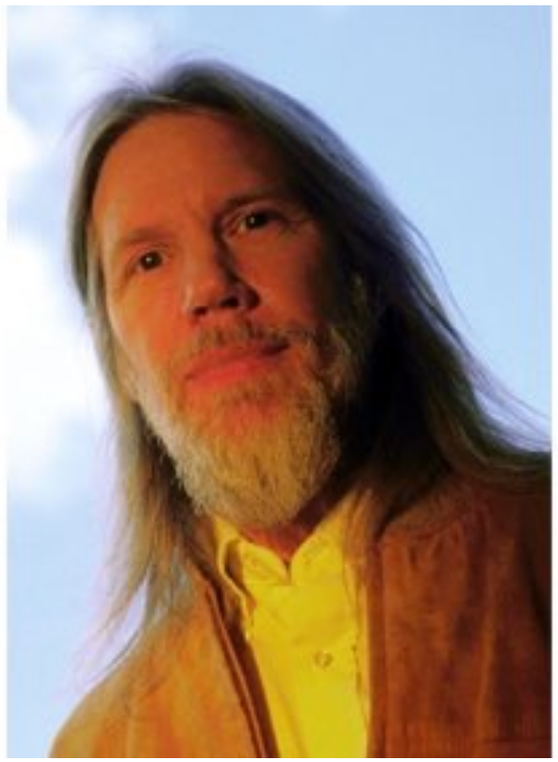


Distribuce klíčů

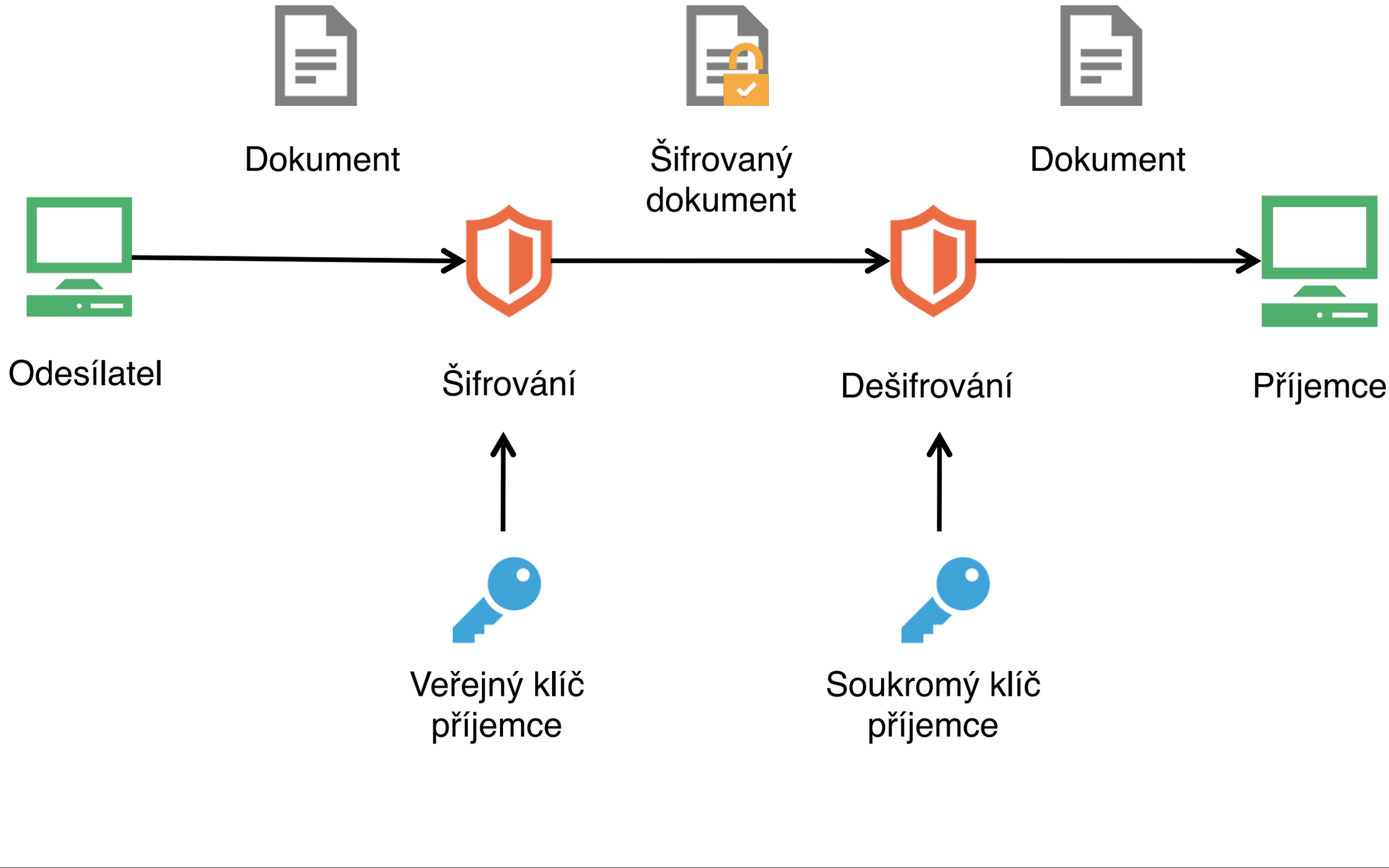
- V symetrické kryptografii musí každý účastník s každým sdílet tajný klíč.
- Každý z *n* účastníků musí mít *n-1* klíčů.
- Celkem je *n(n-1)/2* klíčů.
- Problém s jejich distribucí!

Asymetrická kryptografie

- 1976 - New Directions in Cryptography - Whitfield Diffie, Martin Hellman
- 1977 - RSA - Ron Rivest, Adi Shamir, Leonard Adleman
- Vše vymyšleno nezávisle 1970 a 1974 v GCHQ - odtajněno 1997



Asymetrická kryptografie

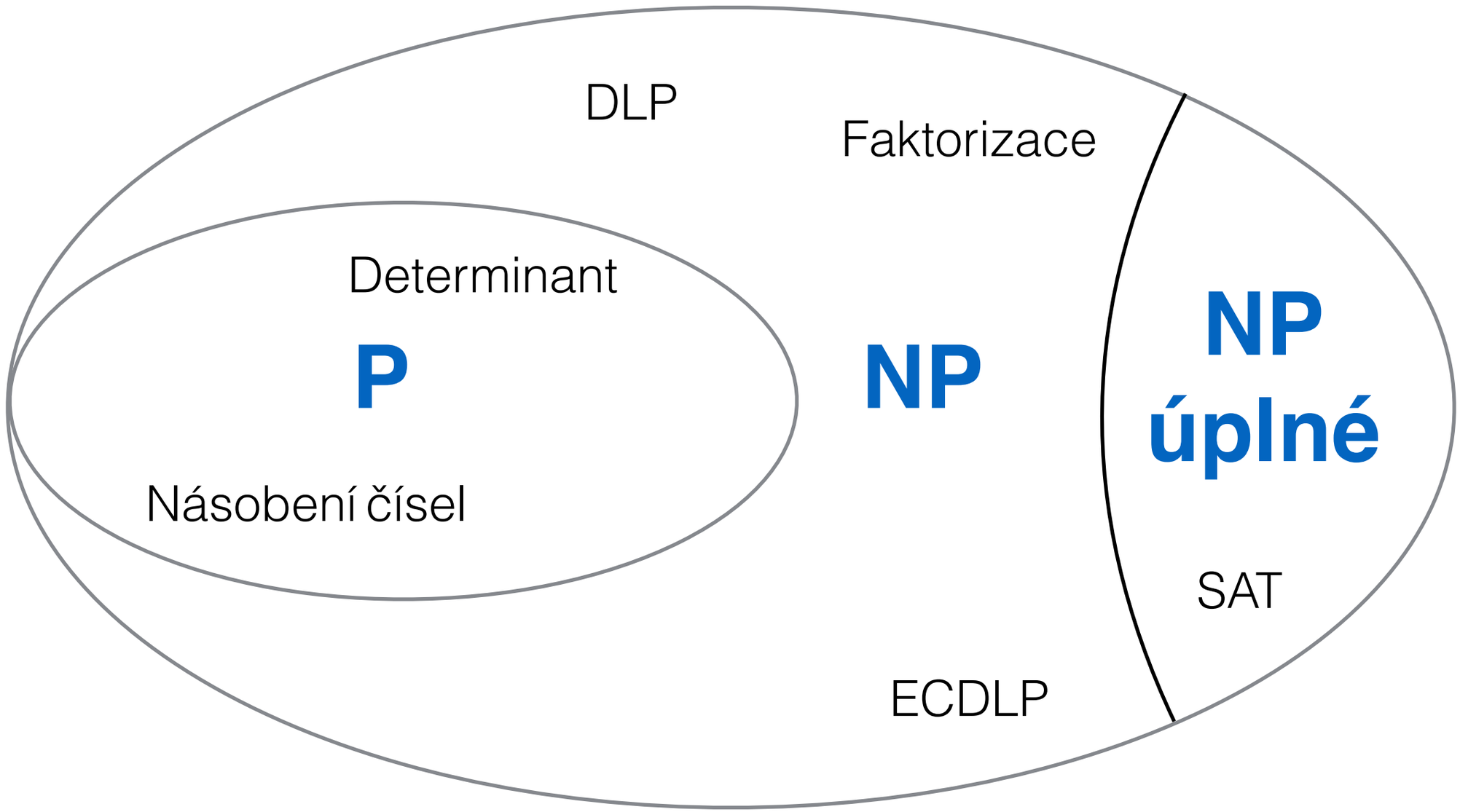


Asymetrická vs. symetrická

- Symetrická kryptografie
  - Jeden společný klíč
  - Musíme ho tajně předat
  - Problém: distribuce klíčů

- Asymetrická kryptografie
  - Dvojice klíčů VK (veřejný klíč) a PK (privátní klíč)
  - VK můžeme veřejně vystavit
  - PK musíme strážit
  - Problém: původ klíče

$P \stackrel{?}{=} NP$

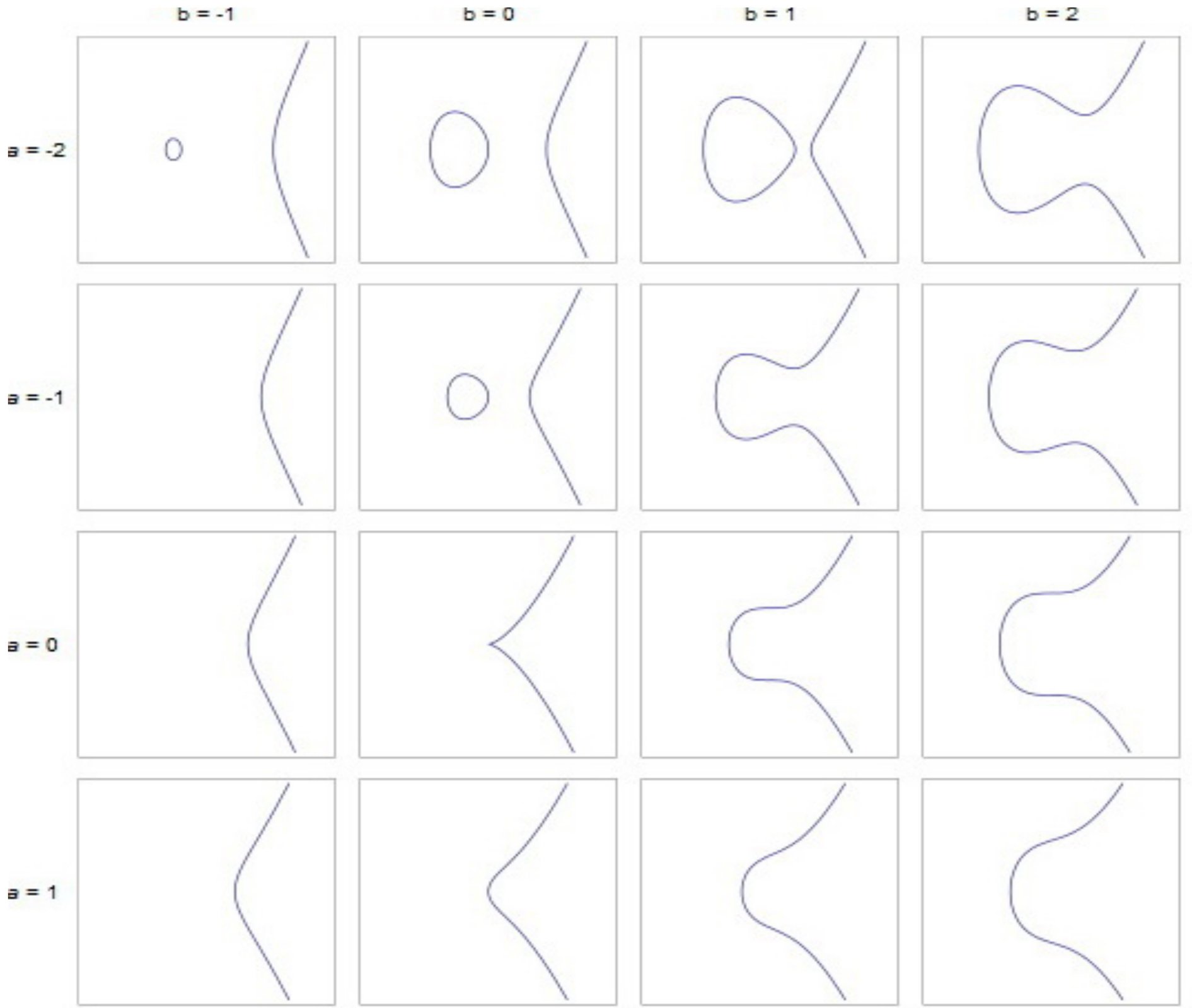


Eliptické křivky

Eliptické křivky

- Navrženo v roce 1985 nezávisle: Neal Koblitz a Victor S. Miller

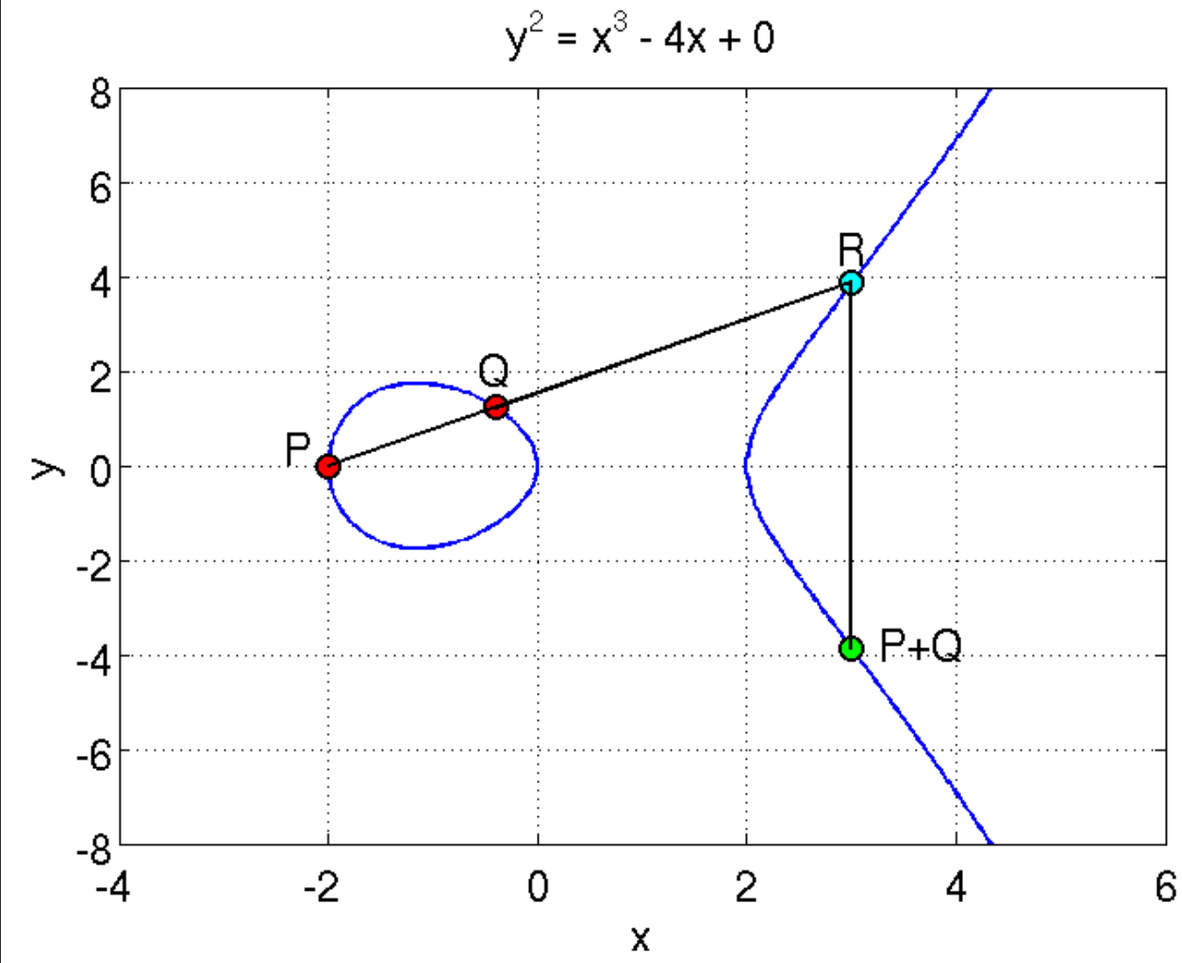
- Co je eliptická křivka?
  - Křivka s rovnicí: $y^2 = x^3 + ax + b$; a,b konstanty
  - Symetrická podle osy x
  - Navíc definovaná operace sčítání bodů na křivce
  - Další vlastnosti…

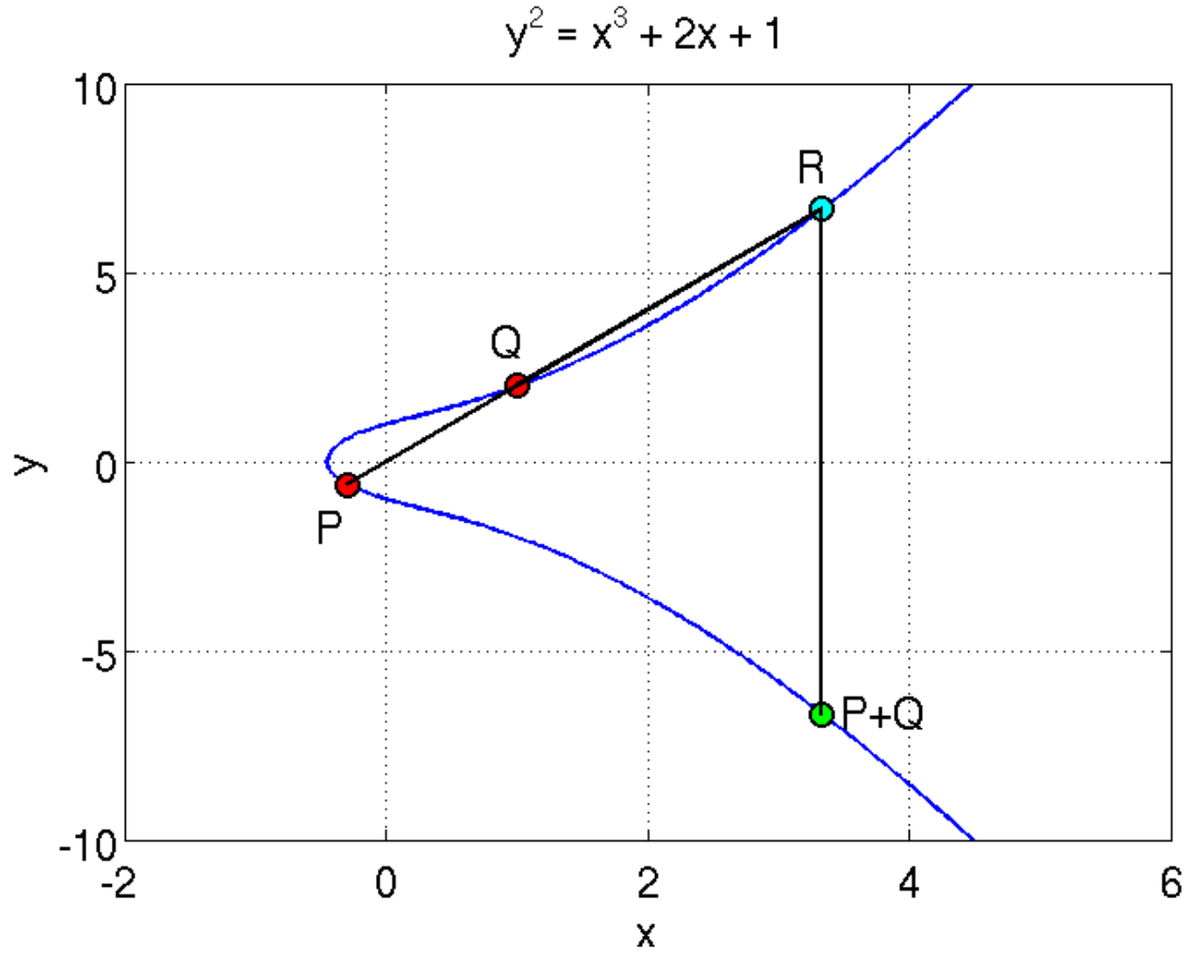


Příklady eliptických křivek

Co to sčítání bodů na křivce?

Sčítání bodu na křivce



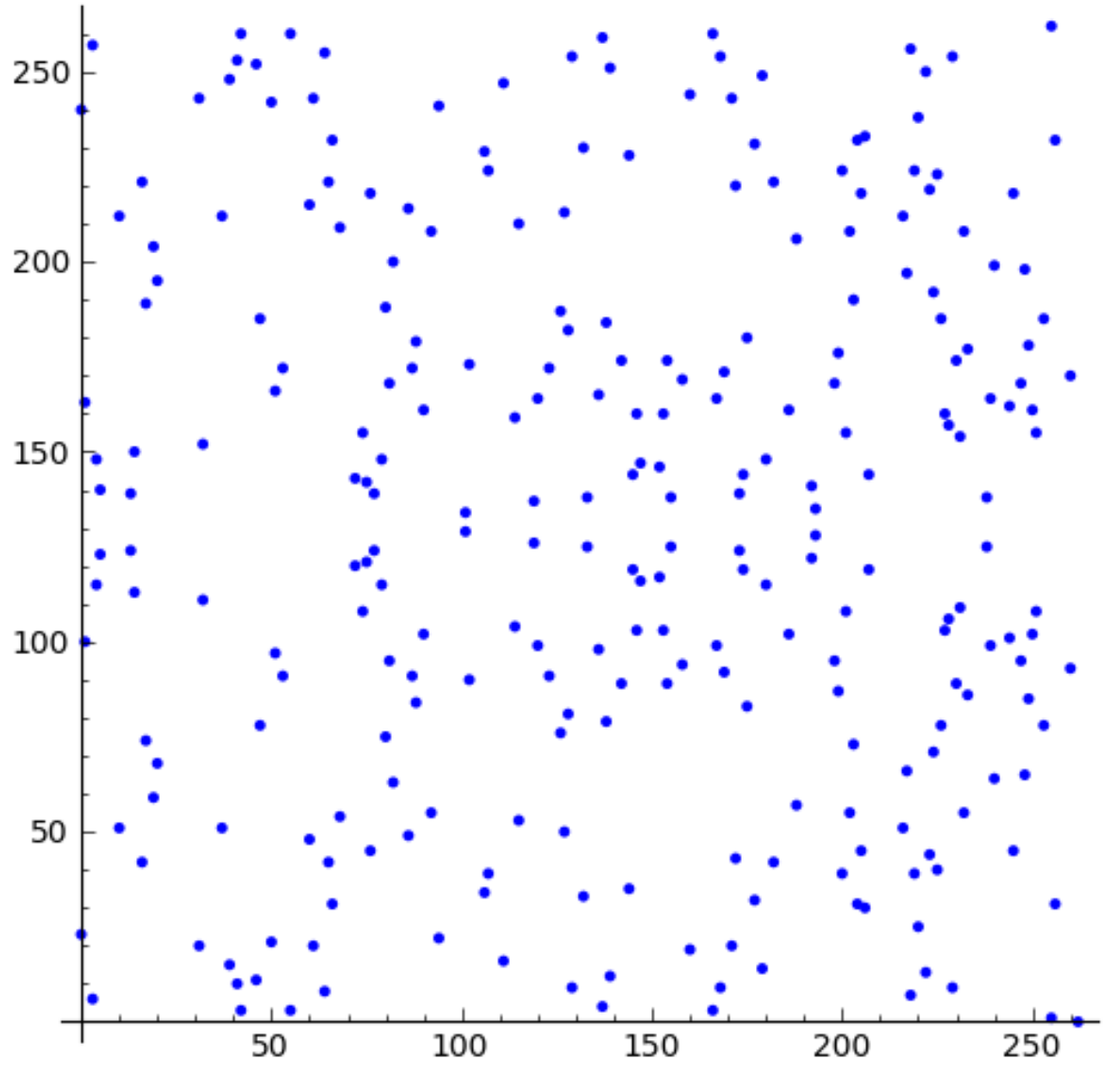


- Sčítání bodů P a Q
  - přímka vedocí body P a Q protne el. křivku v právě jednom bodě R - matematická vlastnost
  - výsledkem součtu je “zrcadlový obraz” bodu R

Konečná eliptická křivka

- Reálná čísla jsou jedním z číselných oborů (těles), kde mohu uvažovat eliptickou křivku.

- Přirozená čísla modulo *n* jsou dalším.



$y^2 = x^3 + 2x + 3$ modulo 263

Eliptická křivka jako grupa

- Množina bodů na křivce s operací sčítání tvoří grupu.
- $E(K) = \{(x, y) \in K \times K : y^2 = x^3 + ax + b\} \cup \{O\}$
- Co můžu dělat s (konečnou) grupou?
- Můžu se ptát na **diskrétní logaritmus**.
- Předtím ale…

Příklady dalších group

- Přirozená čísla se sčítáním modulo *n*
  $Z_n = (\{0, 1, 2, \ldots, n\text{-}1\}, +)$

- Přirozená čísla s násobením modulo prvočíslo *p*
  $Z_p^* = (\{1, 2, \ldots, p\text{-}1\}, *)$

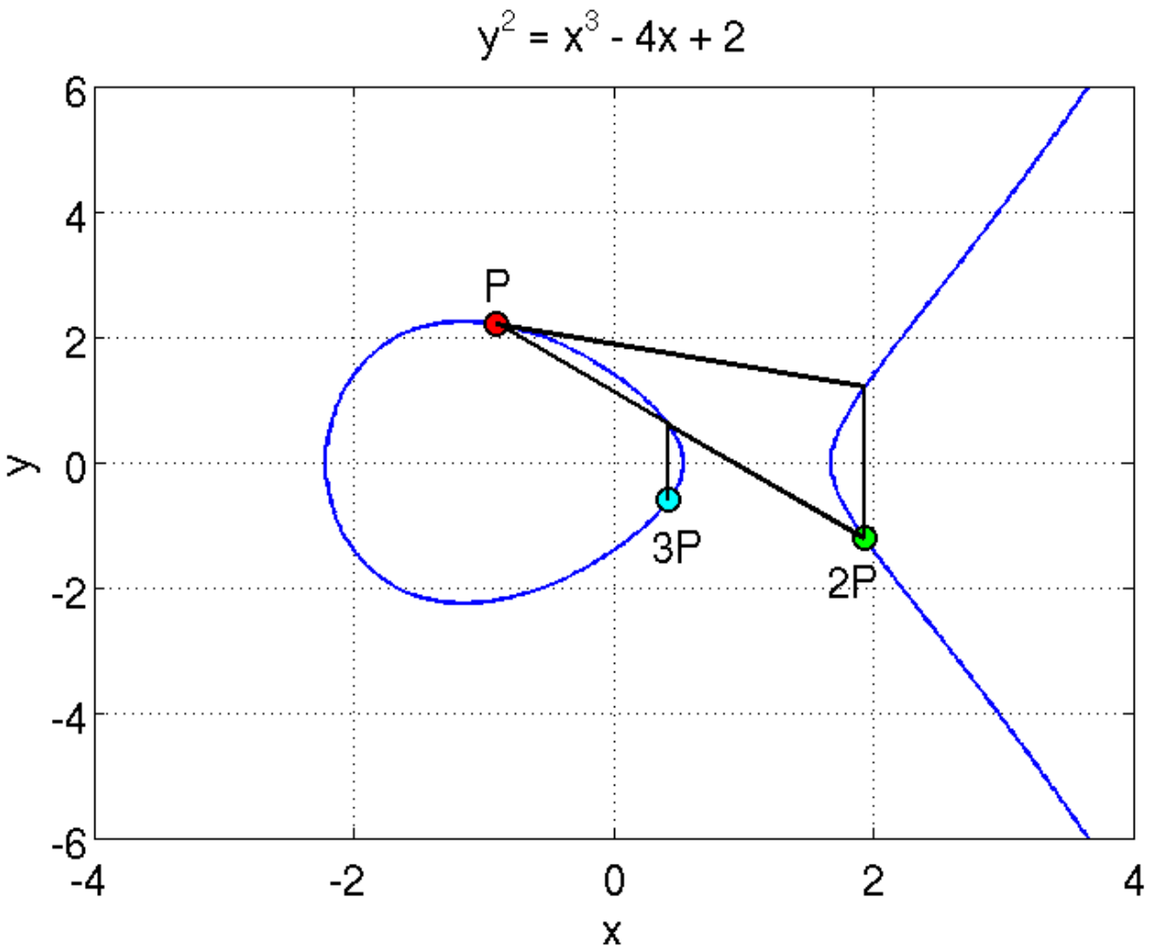
Diskrétní logaritmus

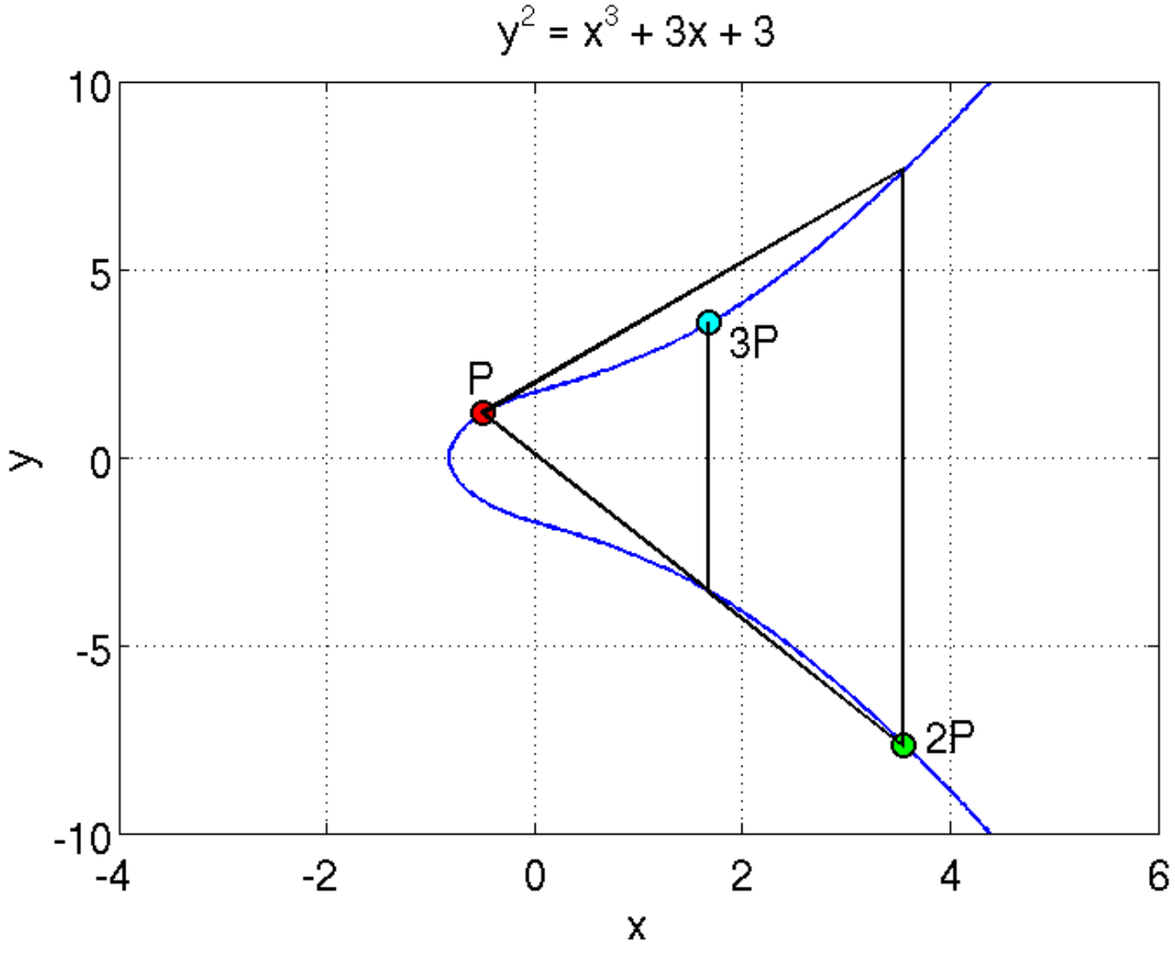
- Obecná grupa G = (*G*, #); *a*,*b* ∈ G
- Otázka: Existuje k, že *a* = k*b* (= b + b + b +…+ b)*?*

- Z_n = ({0, 1, 2, …, n-1}, +)
  - Pro *a*, *b* hledám k, že *a* = k*b* mod *n*
  - Eukalidův algoritmus - jednoduchý problém

- Z_p^* = ({1, 2, …, p-1}, *)
  - Pro *a*, *b* hledám k, že $a = b^k \bmod p$
  - Není znám žádný rychlý algoritmus

Násobení bodu na křivce





- Násobení bodů P
  - sečtu bod P se sebou samým = tečna procházející bodem P
  - obecně *k*P = P + P + P + … + P (*k* krát)

Elliptic Curve Discrete Log Problem

- Pro body A a B na křivce chceme najít k, že A = kB.
- Triviální algoritmus
  - zkoušet B, 2B, 3B, 4B, …
- Pollard's Rho
  - rychlejší ale pořád pomalé
- Zatím není znám rychlý algoritmus na řešení tohoto problému.

Srovnání rychlostí

Symmetric Key Size (bits)	RSA and Diffie-Hellman Key Size (bits)	Elliptic Curve Key Size (bits)
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

NIST Recommended Key Sizes

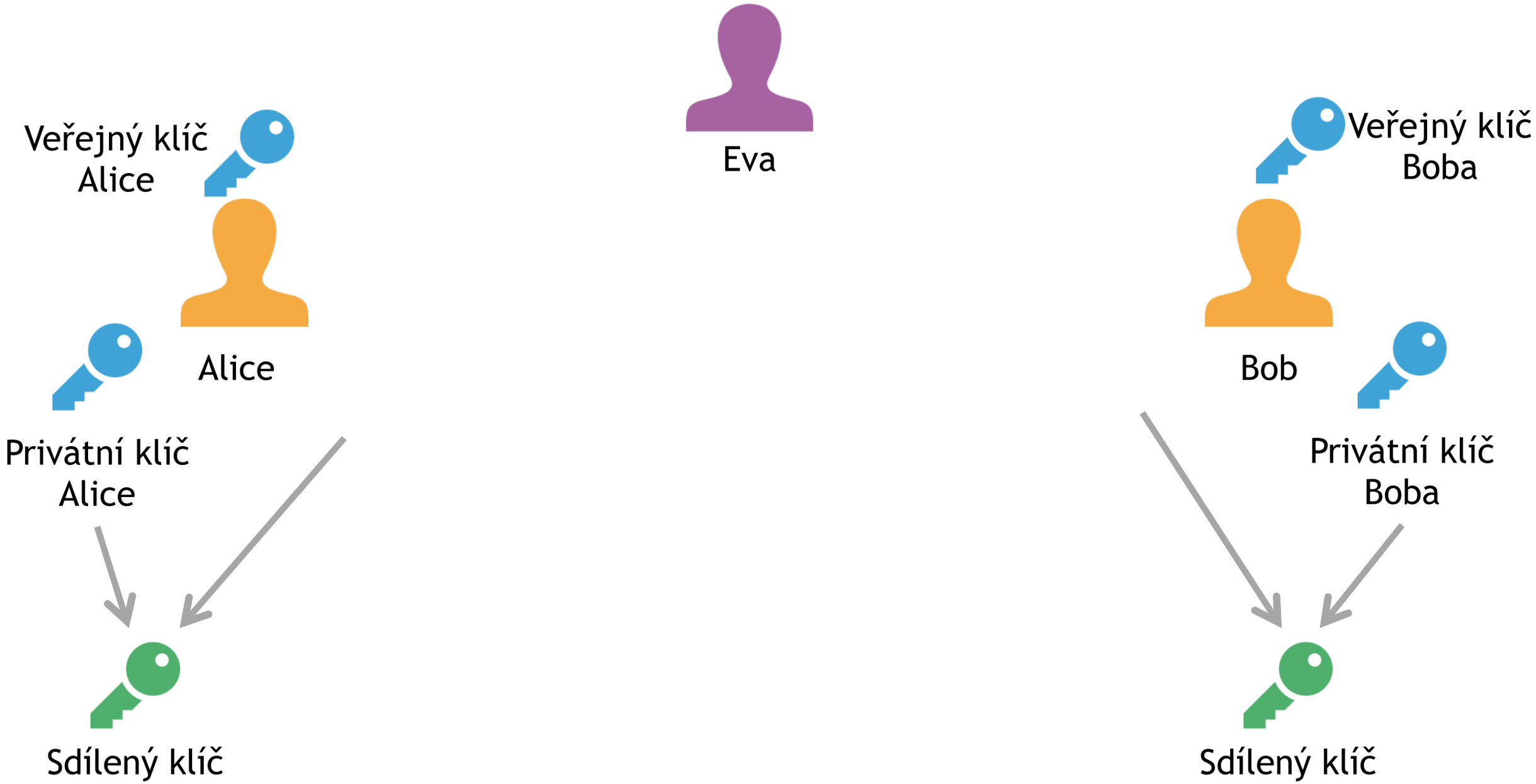
ECDH, ECDSA

- Účastníci se vždy na začátku musí dohodnout na konkrétní křivce $y^2 = x^3 + ax + b$ a bodu na ní G.
  - Sáhnu po standardu: NIST (FIPS 186-4), ECC Brainpool, SECG
  - Vygeneruji si sám - pro odvážné :-)

- Soukromý klíč je přirozené číslo d

- Veřejný klíč je bod na křivce Q = dG (spolu s křivkou)

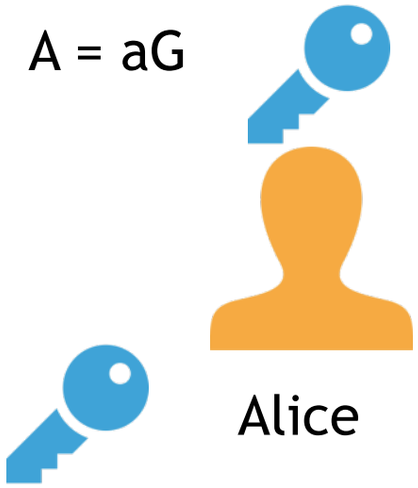
Diffie-Hellman



ECDH

Eva

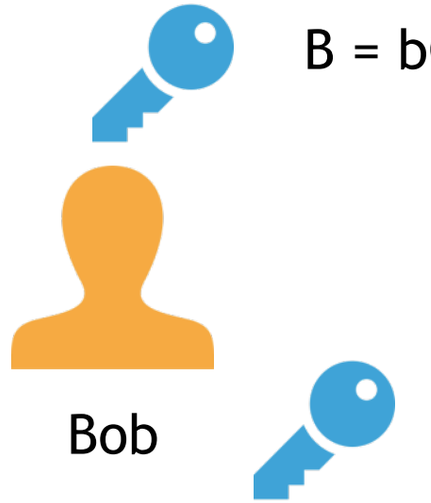
A = aG



Alice

a

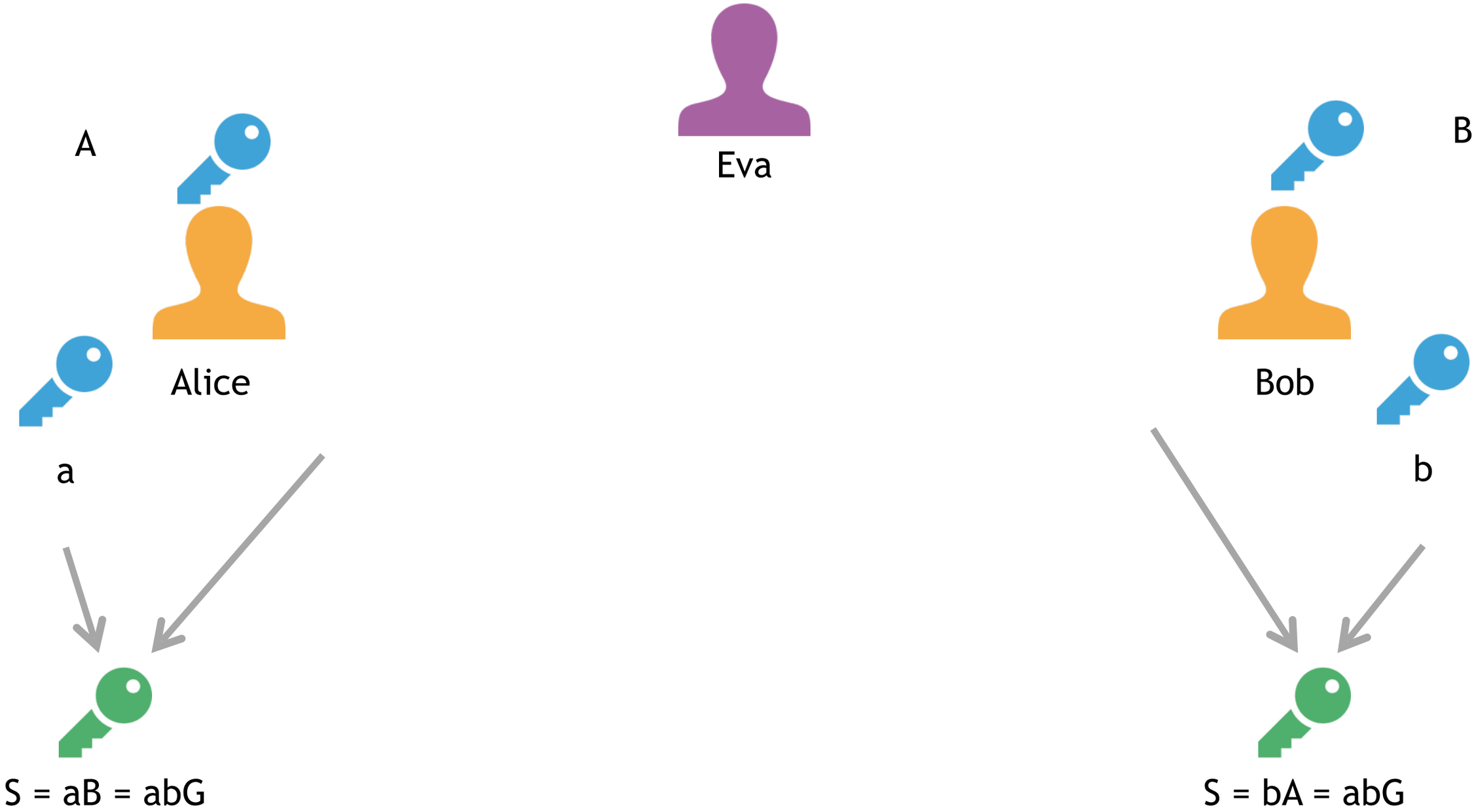
B = bG



Bob

b

ECDH



ECDSA

1. Zvol **náhodné** číslo k, $1 \leq k \leq n - 1$

2. $k\mathrm{G} = (x_1, y_1)$; $r = x_1 \bmod n$

3. $e = \mathrm{HASH}(m)$

4. $s = k^{-1}(e + rd) \bmod n$

Podpisem zprávy m je dvojice (r, s).

Sony Playstation 3

Pokud *k* je konstanta, je *r* stejné pro všechny podpisy.

$$s_1 = k^{-1}(e_1 + rd) \qquad s_2 = k^{-1}(e_2 + rd)$$

$$s_1 - s_2 = k^{-1}(e_1 - e_2)$$

$$k = (e_1 - e_2)/(s_1 - s_2)$$

$$d = (ks_i - e_i)/r$$

d je privátní klíč!!!

Tady udělali inženýři ze Sony chybu.

Eliptické křivky v praxi

Eliptické křivky v praxi

- SSH
  - testovací vzorek - 12 mil.
  - 10.3% podporovalo ECDSA pro autentizaci
  - 13,8% podporovalo ECDH pro výměnu klíčů
- TLS
  - testovací vzorek - 30,2 mil.
  - 7,2% podporovalo ECDH pro výměnu klíčů

https://eprint.iacr.org/2013/734.pdf

Eliptické křivky v praxi

- Austrian e-ID
  - Rakouská občanka - smart card
  - Čip obsahuje RSA nebo ECDSA klíč
  - Sesbíráno 828 911 certifikátů
  - 58% veřejných klíčů ECC

- Bitcoin
  - Potvrzování transakcí - ECDSA
  - K veřejný klíč
  - HASH160 = RIPEMD-160(SHA-256(K))

base58(0x00 || HASH160 || SHA-256(SHA-256(0x00 || HASH160))/2^{224})

https://eprint.iacr.org/2013/734.pdf

Kvalifikovaní poskytovatelé certifikačních služeb

- První certifikační autorita
- PostSignum
- EIdentity

Všechny autority podporují pouze RSA.

Výhody a nevýhody ECC

- Výhody
  - kratší klíče
  - rychlejší výpočty
- Nevýhody
  - přetrvávající obavy ohledně bezpečnosti/prozkoumanosti křivek
  - chybí masivnější nasazení
  - patenty

Děkuji za pozornost