Zakřivená bezpečnost aneb eliptické křivky v praxi

Dominik Pantůček
dominik.pantucek@trustica.cz

Trustica s.r.o.

9.11.2016

Co je ECC?

- Elliptic curve cryptography.
- Kryptografie na eliptických křivkách.
- Asymetrický kryptografický systém.

Asymetrický kryptografický systém

Umožňuje:

- předání zašifrované informace protistraně,
- podpis předáváné informace
  - a jeho ověření.
- Nevyžaduje znalost sdíleného klíče oběma stranami.
- Používá veřejné a soukromé klíče.

Asymetrický kryptografický systém

Co využívá:

- "jednocestné" vlastnosti některých matematických problémů,
- v současnosti především:
  - problém faktorizace velkých čísel,
  - problém diskrétního logaritmu.

Asymetrické kryptografické systémy

Problém faktorizace velkých čísel:

- Kryptografický systém: RSA
  - šifrování, podpis.

Problém diskrétního logaritmu:

- DSA – Digital Signature Standard / Digital Signature Algorithm
  - podpis a jeho ověření.
- DH – Diffie-Hellman
  - výměna klíčů – šifrování.

Kryptografické systémy: bezpečnost

- Snadnost odvození tajných (soukromých) informací
  - z čitelných (veřejných).
- Síla (parametr bezpečnosti/security parameter) – počet iterací výpočtu.
- Obvykle vyjádřena logaritmicky o základu 2.
- n-bitová bezpečnost: nutnost 2^n iterací pro prolomení.

Síla kryptografických systémů

- i7-5600U CPU 2.60GHz $\times$ 4 jádra,
- teoreticky 2600000000 $\times$ 4 $\approx$ 10000000000
  - $\approx 10 \cdot 10^9$ operací za sekundu,
- cluster 1000 serverů,
- stáří vesmíru $13,8 \cdot 10^9$ let.

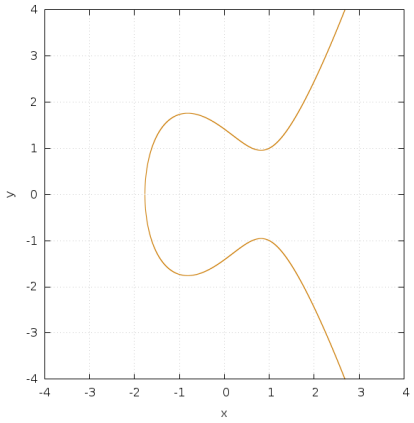
síla (bity)	čas
80	3 833 let
112	16 464 665 330 209 let = 1 193 vesmírů
128	78 190 457 vesmírů
140	320 268 112 014 vesmírů
192	144235934992782133596473811 9 ...

Síla kryptografických systémů

	velikost [bitů]		
síla [bitů]	RSA	DSA/DH	ECC
112	2048	2048/224	224
128	3072	3072/256	256
$\approx$ 140	4096	4096/280	(280)
192	7680	7680/384	384

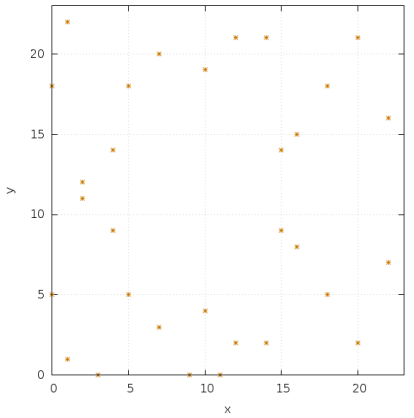
Eliptické křivky

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

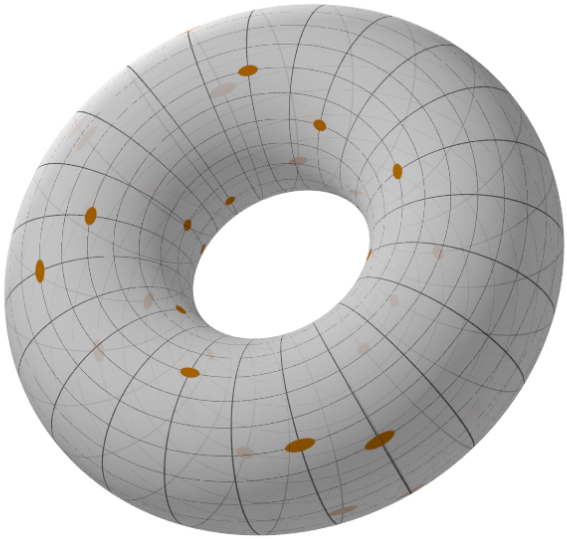


Eliptické křivky na konečném tělese

$$y^2 = x^3 + ax + b \pmod{p}$$
$$y^2 = x^3 - 2x + 2 \pmod{23}$$



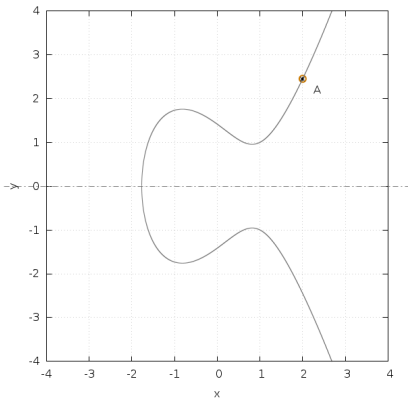
Eliptické křivky na konečném tělese

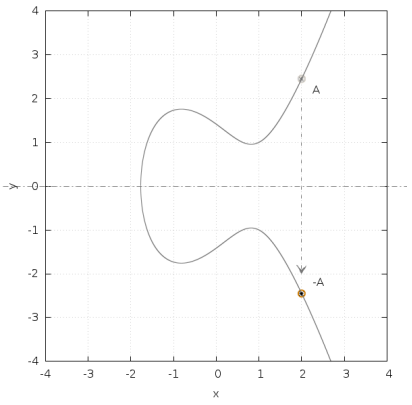


Eliptické křivky – aritmetika

Pro eliptickou křivku e definujeme:

- Negace bodu: $B = -A$
  - $(B_x, B_y) = (A_x, -A_y)$

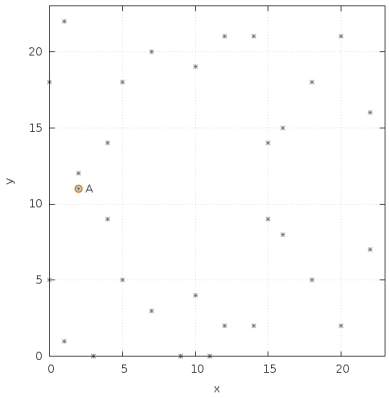




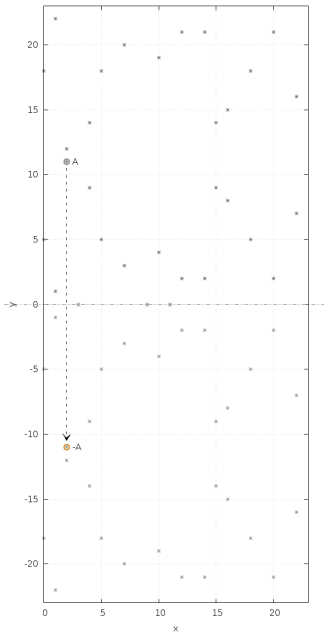
Eliptické křivky – aritmetika

Pro eliptickou křivku $e \pmod p$ definujeme:

- Negace bodu: $B = -A$
  - $(B_x, B_y) = (A_y, -A_y) \pmod p$



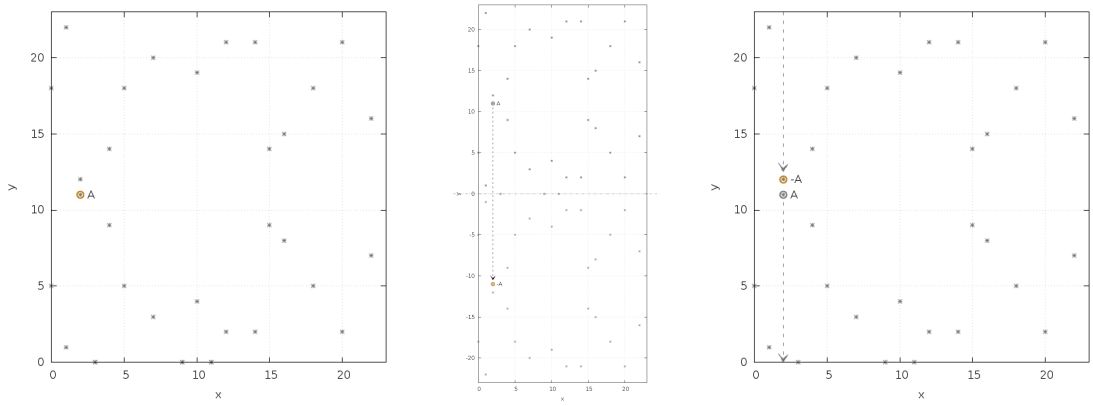
Eliptické křivky – aritmetika



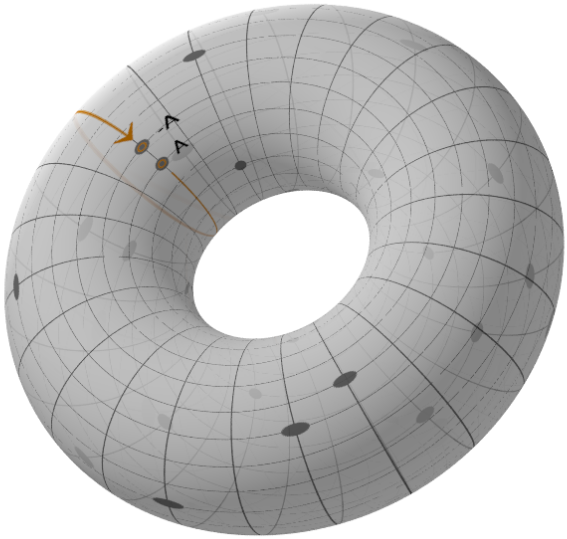
Eliptické křivky – aritmetika

Pro eliptickou křivku $e \pmod p$ definujeme:

- Negace bodu: $B = -A$
  - $(B_x, B_y) = (A_y, -A_y) \pmod p$



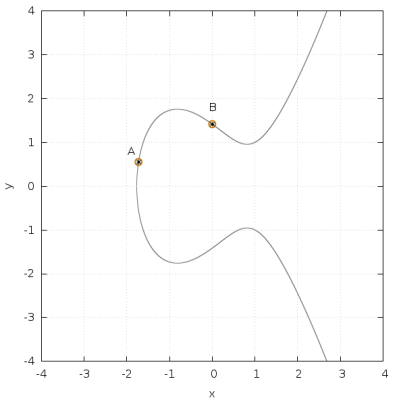
Eliptické křivky – aritmetika

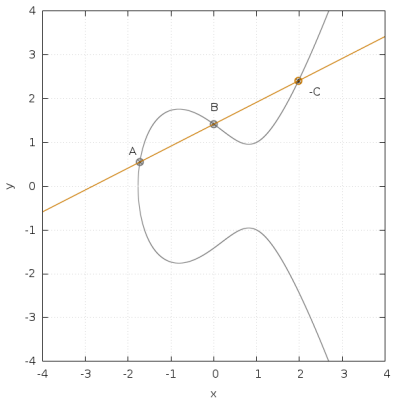


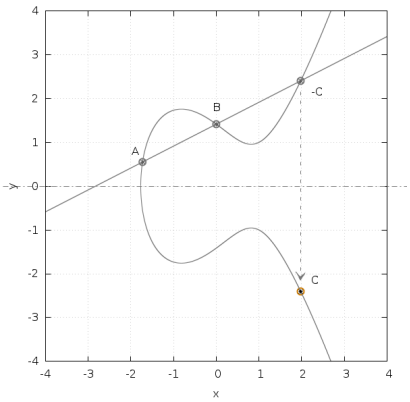
Eliptické křivky – aritmetika

Pro eliptickou křivku e definujeme:

- Sčítání bodů: $C = A + B$
  - $-C = \overrightarrow{AB} \cap e$



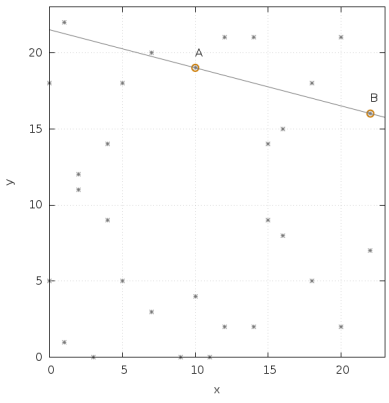




Eliptické křivky – aritmetika

Pro eliptickou křivku $e \pmod p$ definujeme:

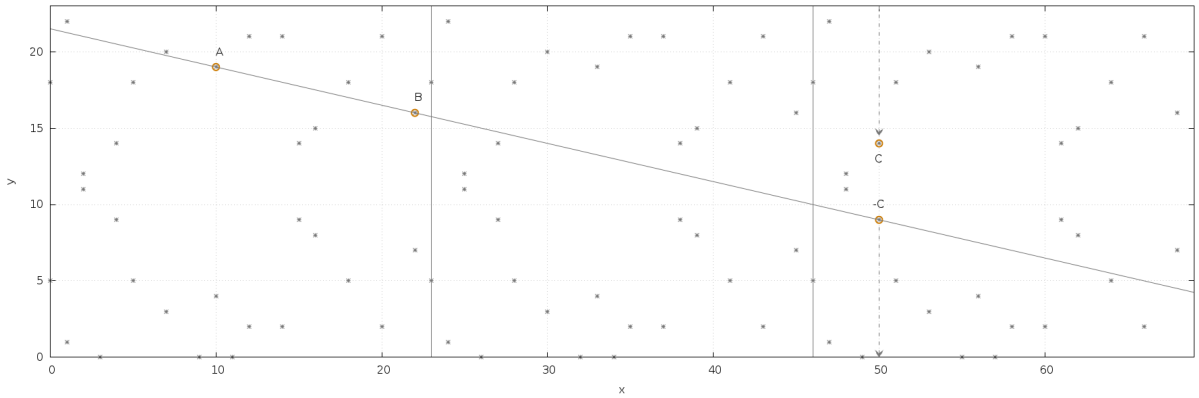
- Sčítání bodů: $C = A + B$
  - $-C = \overrightarrow{AB} \cap e$



Eliptické křivky – aritmetika

Pro eliptickou křivku $e \pmod p$ definujeme:

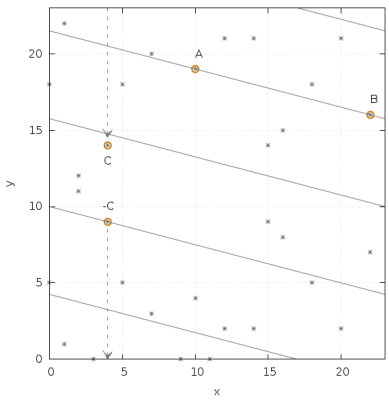
- Sčítání bodů: $C = A + B$
  - $-C = \overrightarrow{AB} \cap e$
  - lze zobrazit jako opakování konečného tělesa.



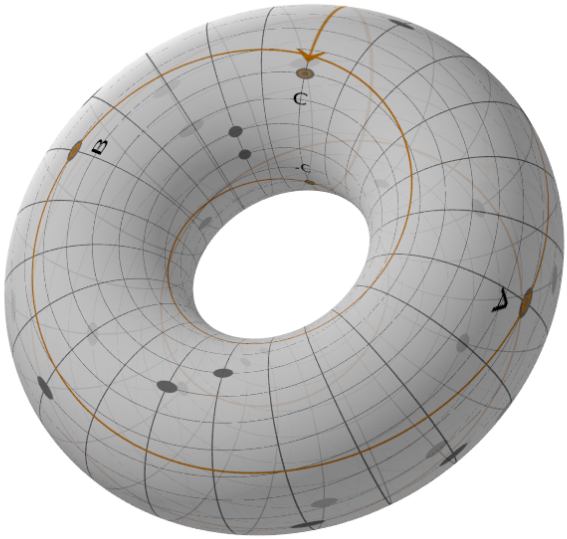
Eliptické křivky – aritmetika

Pro eliptickou křivku $e \pmod p$ definujeme:

- Sčítání bodů: $C = A + B$
  - $-C = \overrightarrow{AB} \cap e$
  - lze zobrazit jako pokračování přímky na konečném tělese.



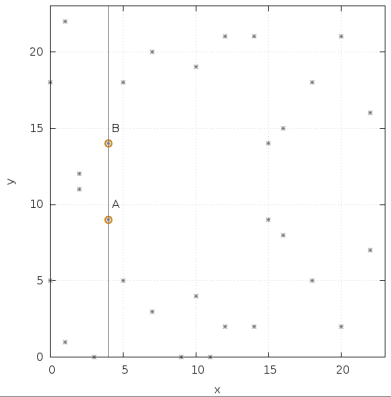
Eliptické křivky – aritmetika

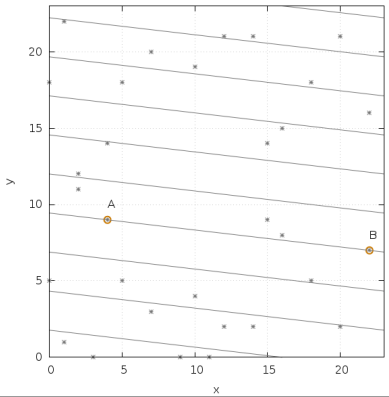


Eliptické křivky – aritmetika

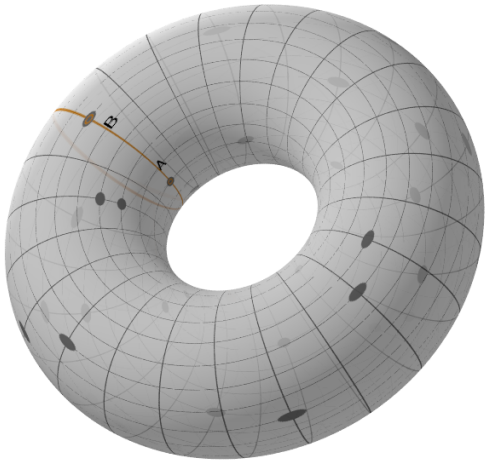
Pro eliptickou křivku $e \pmod p$ definujeme:

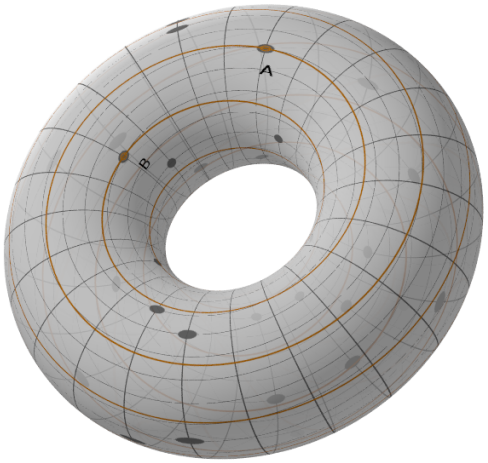
- Sčítání bodů: $C = A + B$
  - $-C = \overrightarrow{AB} \cap e$
  - pokud se jedná o opačné body na křivce, výsledkem je bod O,
  - pokud protíná křivku jen ve dvou bodech, které nejsou opačné, výsledkem je ∞.





Eliptické křivky – aritmetika

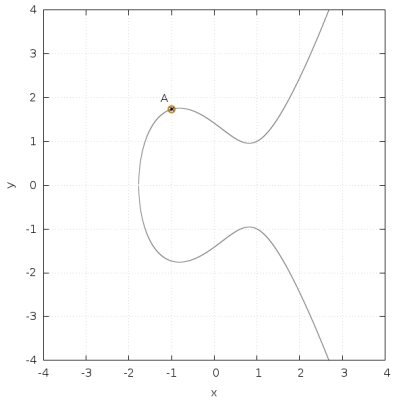


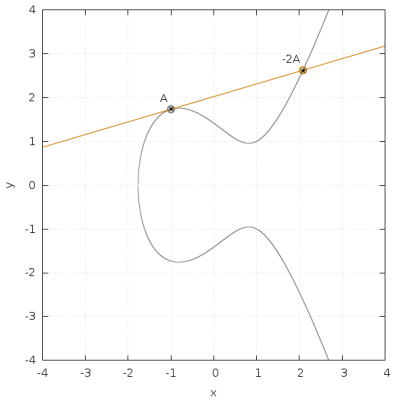


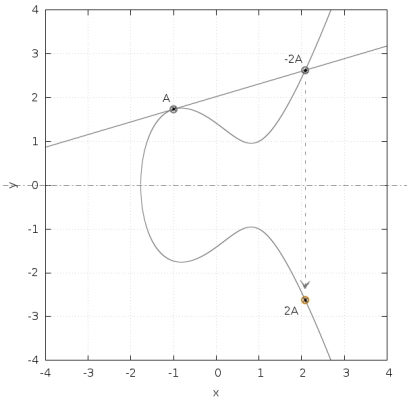
Eliptické křivky – aritmetika

Pro eliptickou křivku $e \pmod p$ definujeme:

- Zdvojnásobení bodu: $B = 2 \cdot A = A + A$
  - Obdobně jako sčítání, použitá přímka je tečnou v bodě A.

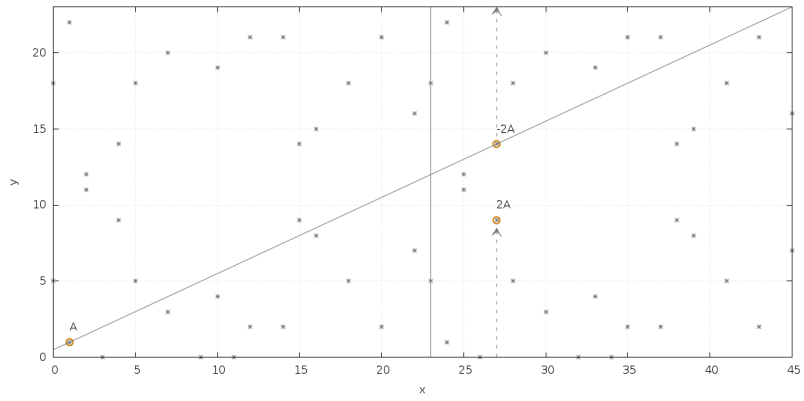


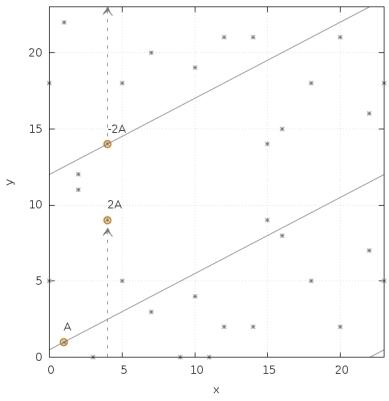




Eliptické křivky – aritmetika

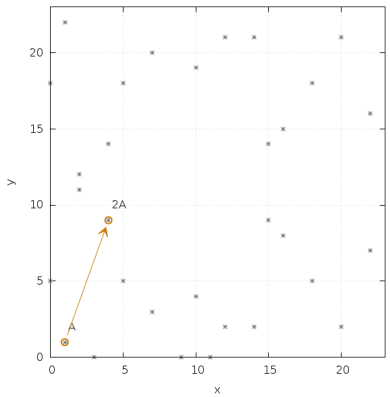
- Zdvojnásobení bodu: $B = 2 \cdot A \pmod{23}$
  - Obdobně jako sčítání, použitá přímka je “tečnou” v bodě A.

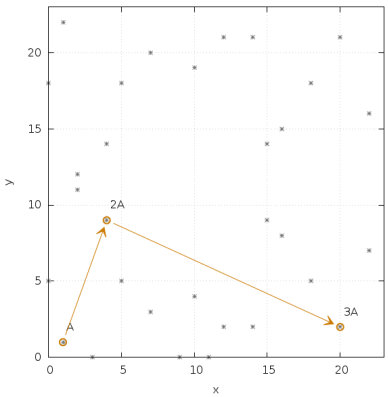


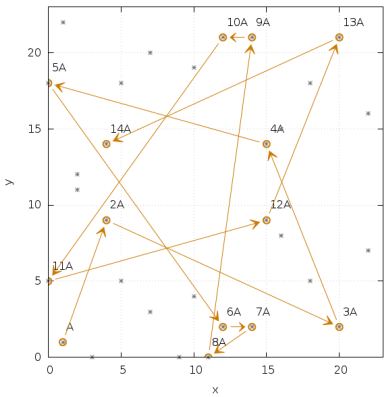


Eliptické křivky – aritmetika

- Násobení bodu skalárem $B = n \cdot A$
  - Rozklad:
  - $B = 5 \cdot A = A + 4 \cdot A = A + 2 \cdot (2 \cdot A)$







Problém diskrétního logaritmu na eliptické křivce

- $B = n \cdot A \pmod{p}$
- Problém: ze známých A a B vypočítat n.
- ECDSA
  - podpisy,
  - certifikáty.
- ECDH
  - šifrování,
  - výměna symetrických klíčů.

Praktické aplikace

- X.509 certifikáty,
- navázání TLS spojení,
- DNSSEC,
- šifrování a podepisování zpráv OpenPGP.

X.509 certifikáty: RSA

- https://www.microsoft.com/
- C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
  - C=US, ST=Washington, L=Redmond, O=Microsoft Corporation, OU=Microsoft IT, CN=Microsoft IT SSL SHA2
    - C=US, ST=WA, L=Redmond, O=Microsoft Corporation, CN=www.microsoft.com

X.509 certifikáty: RSA

- https://www.microsoft.com/ – stávající certifikáty:

Certifikát	Algoritmus	Bitů	Síla	Velikost
Baltimore CyberTrust Root	RSA	2048	112	891
Microsoft IT SSL SHA2	RSA	4096	≈ 140	1509
www.microsoft.com	RSA	2048	112	1707
Celkem	–	–	112	4107

- Velikosti v bytech, formát DER.
- Síla řetězu certifikátů je rovna síle nejslabšího článku.

X.509 certifikáty: ECC

- https://www.microsoft.com/ – ECC certifikáty:

Certifikát	Algoritmus	Bitů	Síla	Velikost
Baltimore CyberTrust Root	ECDSA	224	112	475
Microsoft IT SSL SHA2	ECDSA	384	192	882
www.microsoft.com	ECDSA	224	112	1088
Celkem	–	–	112	2445

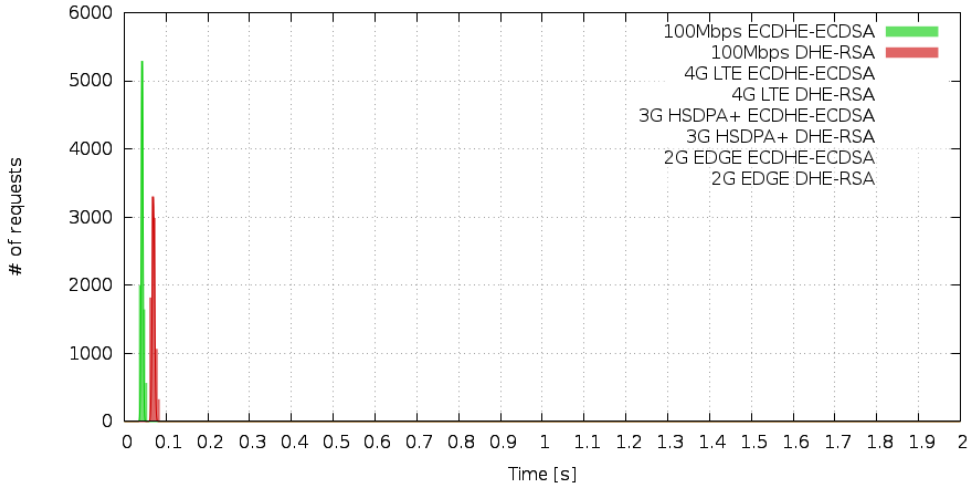
- Velikosti v bytech, formát DER.
- Síla řetězu certifikátů je rovna síle nejslabšího článku.
- 4096-bitová RSA byla aproximována nejbližší silnější ECDSA.

ECC TLS

TLS 1.2 umožňuje:

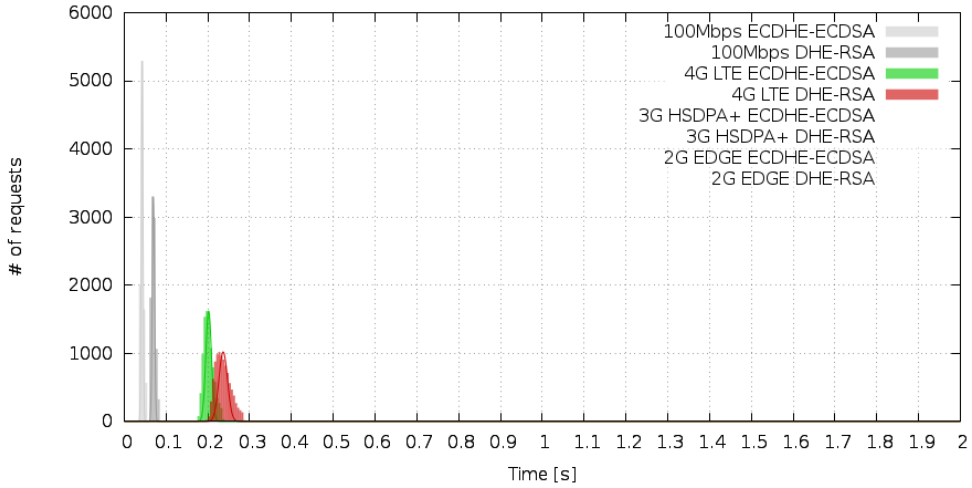
- ECDH – Elliptic Curve Diffie-Hellman
  - ECDH-ECDSA-AES128-CBC-SHA256
  - ECDH-RSA-AES128-CBC-SHA256
  - ECDH-DSA-AES128-CBC-SHA256
- ECDHE – ECDH Ephemeral:
  - pro každé spojení nové náhodné privátní klíče.
  - ECDHE-ECDSA-AES128-CBC-SHA256
  - ECDHE-RSA-AES128-CBC-SHA256
  - ECDHE-DSA-AES128-CBC-SHA256
- Pouze autentizace ECDSA:
  - DH-ECDSA-AES128-CBC-SHA256
  - DHE-ECDSA-AES128-CBC-SHA256

Statistika handshaků: 100Mbps



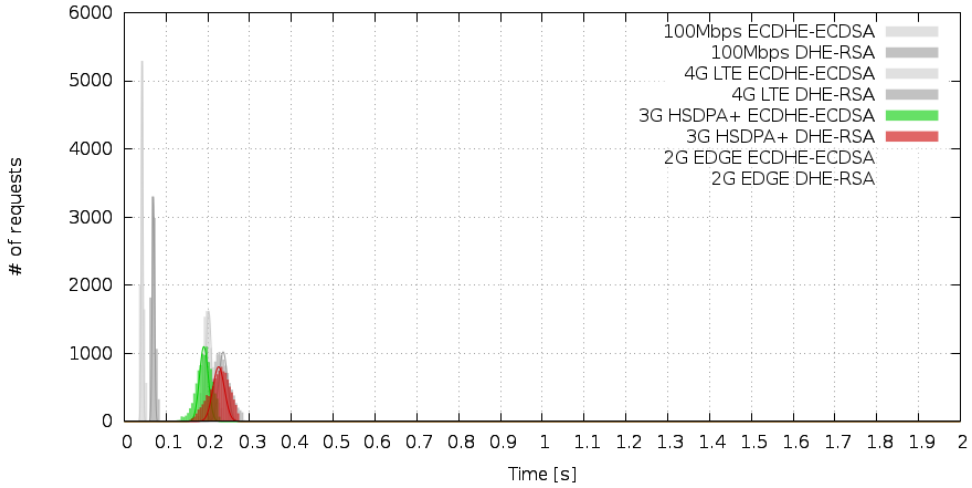
$$\bar{t}_{ECC} = 0.043 \pm 1.33 \cdot 10^{-5}$$
$$\bar{t}_{DLP} = 0.070 \pm 2.37 \cdot 10^{-5}$$

Statistika handshaků: 4G LTE



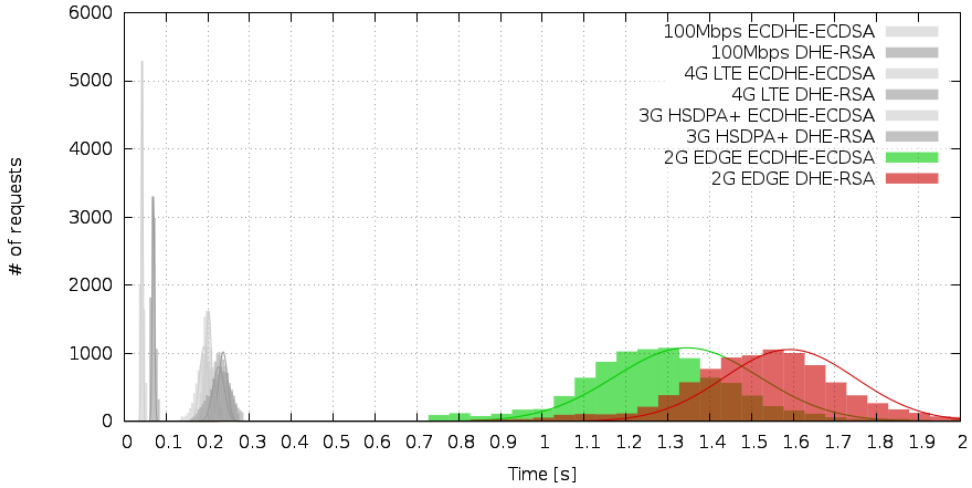
$$\bar{t}_{ECC} = 0.20 \pm 1.43 \cdot 10^{-4}$$
$$\bar{t}_{DLP} = 0.23 \pm 3.32 \cdot 10^{-4}$$

Statistika handshaků: 3G HSDPA+



$$\bar{t}_{ECC} = 0.19 \pm 3.44 \cdot 10^{-4}$$
$$\bar{t}_{DLP} = 0.23 \pm 6.03 \cdot 10^{-4}$$

Statistika handshaků: 2G EDGE



$$\bar{t}_{ECC} = 1.35 \pm 9.42 \cdot 10^{-2}$$
$$\bar{t}_{DLP} = 1.59 \pm 7.80 \cdot 10^{-2}$$

ECC DNSSEC

- Možnost podepisovat zóny standardizovanými ECC algoritmy:
- 13 – ECDSA-P256/SHA-256
- 14 – ECDSA-P256/SHA-384
- Možnost distribuovat odpovídající ECDSA klíče.

ECC OpenPGP

- GNUPG podporuje standardizované ECC:
- NIST křivky P-256, P-384 a P-521,
- Brainpool křivky P-256, P-384 a P-512,
- pro šifrování i podpis.

Proč (ne)používat ECC?

- Pro:
  - vyšší síla (bezpečnost) ECC algoritmů
  - při nižší bitové délce.
  - Nižší výpočetní náročnost.
- Proti:
  - obavy z neznámého,
  - obavy z chyb v implementacích,
  - problémy standardů.
- K zamyšlení:
  - (ne)odolnost proti útokům postranními kanály,
  - kompatibilita s používaným software,
  - objektivní zhodnocení.

NIST standardy

- National Institute of Standards and Technology.
- Vládní instituce USA.
- Dual_EC_DRBG
  (Dual Elliptic Curve Deterministic Random Bit Generator)
  - Známé slabiny.
  - Nedůvěryhodně zvolené základní body na křivce.
  - Dva náhodné body P, Q: ne-úplně-špatný generátor,
  - $Q = n \cdot P$, pokud známe n, lze určit výstup bez znalosti interního stavu.
- DSS, ECDSS (ECDSA)
- secpNNNrX – např. secp224r1
- sectNNNkX – např. sect283k1
- v základu bezpečné.

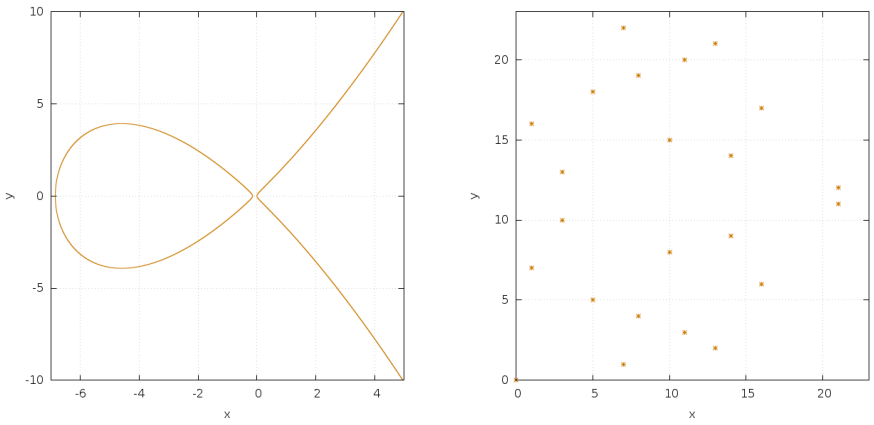
NIST standardy: problémy křivek

- Aritmetické operace na NIST křivkách je těžké implementovat správně,
- i korektní implementace těžko řeší útoky postranními kanály,
  - délka výpočtů je závislá na konkrétních číslech, nejen na bitové šířce.
- Problém: při výpočtech se objeví jako mezivýsledek bod O či ∞,
  - musíme zvolit jiné parametry,
  - implementace zde často mají chybu,
  - typický postranní kanál nebo oslabení systému.
- Problém: práce s body, které nejsou na křivce.

Alternativní křivky

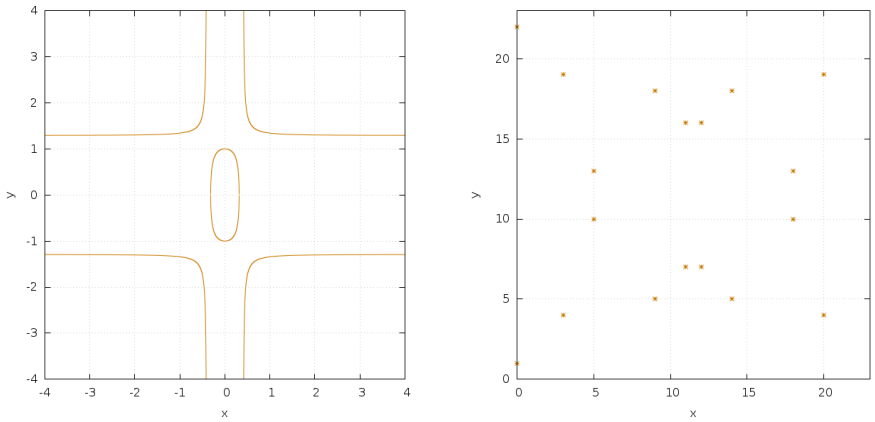
- Daniel J. Bernstein et al.: křivky "s méně problémy"

$$3y^2 = x^3 + 7x^2 + x$$



Alternativní křivky

$$10x^2 + y^2 = 1 + 6x^2y^2$$



Alternativy

- Curve25519 – Montgomery curve

$$y^2 = x^3 + 486662x^2 + x \pmod{2^{255} - 19}$$

- Ed25519 – Twisted Edwards curve

$$-x^2 + y^2 = 1 - \frac{121665}{121666}x^2y^2 \pmod{2^{255} - 19}$$

- X25519 (DH)
- EdDSA

Zavádění a standardizace alternativ

- IETF, formou RFC
  - Curve25519 – X25519
  - Ed25519 - EdDSA
- Silnější varianty, například Ed448

$$y^2 + x^2 = 1 - 39081x^2y^2 \pmod{2^{448} - 2^{224} - 1}$$

- DNSSEC
  - O. Sury, CZ.NIC, R. Edmonds, Farsight Security, Inc.: Ed25519 for DNSSEC
- OpenPGP
  - W. Koch: EdDSA for OpenPGP
  - Experimentální implementace Ed25519 v GNUPG – pouze pro podpisy.

Software

- OpenSSL
  - Podporuje ECC od verze 0.9.8 (5. července 2005)
- GNUTLS
  - Od verze 3.0.0. (29. červenec 2011)
- Network Security Services
  - Prohlížeče Chromium a Firefox používají knihovny NSPR a NSS.
  - ECC je plně podporováno nejméně od roku 2009.
- Microsoft CryptoAPI: Next Generation
  - Windows Vista a novější, Windows Server 2008 a novější.

Závěr

- ECC je zde.
- Software existuje.
- Je možné nasazovat.
- Je vhodné se u toho dobře zamyslet.
- Je nutné s ECC počítat.

Reference

- Elaine Barker: NIST Special Publication 800-57 Part 1 Revision 4 – Recommendation for Key Management, Part 1: General
- Elaine Barker, Lily Chen, Allen Roginsky and Miles Smid: NIST Special Publication 800-56A Revision 2 – Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, May 2013
- NIST: FIPS PUB 186-4 – Digital Signature Standard (DSS), July 2013
- IETF pracovní verze standardů:
  - A. Jivsov: Elliptic Curve Cryptography (ECC) in OpenPGP (draft-jivsov-openpgp-ecc), June 2012
  - W. Koch: EdDSA for OpenPGP (draft-koch-eddsa-for-openpgp-03), August 28, 2015
  - S. Josefsson and N. Moeller: EdDSA and Ed25519 (draft-josefsson-eddsa-ed25519-03), May 12, 2015
  - S. Josefsson and I. Liusvaara: Edwards-curve Digital Signature Algorithm (EdDSA) (draft-irtf-cfrg-eddsa-00), October 7, 2015
  - O. Sury, CZ.NIC, R. Edmonds, Farsight Security, Inc.: Ed25519 for DNSSEC (draft-ietf-curdle-dnskey-ed25519-01), February 16, 2016

Otázky

... a odpovědi.

Děkuji za pozornost.