Zakřivená bezpečnost aneb eliptické křivky v praxi

Dominik Pantůček
dominik.pantucek@trustica.cz

Trustica s.r.o.

31.3.2016

Co je ECC?

- Elliptic curve cryptography.
- Kryptografie na eliptických křivkách.
- 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.

Co využívá:

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

Problém faktorizace velkých čísel

- p, q – prvočísla
- $n = p \cdot q$
- $\varphi(n) = (p-1)(q-1)$
- $e < \varphi(n) \wedge \neg e \mid \varphi(n)$
- $d; d \cdot e \equiv 1 \pmod{\varphi(n)}$
  - $\pmod{p}$ – notace "modulo" (zbytek po dělení),
- (n, e) - veřejný klíč,
- (n, d) - privátní klíč.
- Kryptografický systém: RSA – Ron-Shamir-Adleman
  - šifrování, podpis.

- p – prvočíslo,
- $0 \ldots p-1$ – konečné těleso,
  - $\pmod p$ – notace “modulo” (zbytek po dělení),
- g – generátor skupiny na konečném tělese
  - obvykle 2, 3 či 5
- n – pořadové číslo prvku skupiny,
- $a \equiv g^n \pmod p$ – prvek skupiny.
- Problém: Pokud známe a, g a p, nelze snadno určit n.

- Prvočíslo $p = 23$,
- Konečné těleso $\pmod{23} \equiv \{0 \dots 22\}$,
- Generátor $g = 2$,
- Číslo $n = 8$,
- $a \equiv g^n \pmod{p} \equiv 2^8 \pmod{23} \equiv 256 \pmod{23} \equiv 3$,
- Problém: $2^? \pmod{23} \equiv 3$

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

- 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.

- 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 . . .

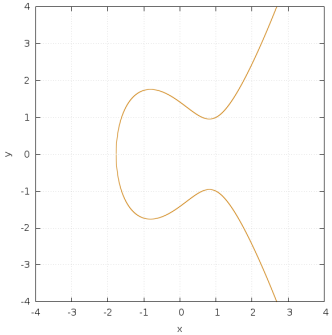
Síla kryptografických systémů

systém	velikost [bitů]	síla [bitů]
RSA	1024	80
	2048	112
	3072	128
	7680	192
DSA	1024 / 160	80
	2048 / 224	112
	3072 / 256	128
	7680 / 384	192
DH	1024 / 160	80
	2048 / 224	112
	3072 / 256	128
	7680 / 384	192

Síla kryptografických systémů

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

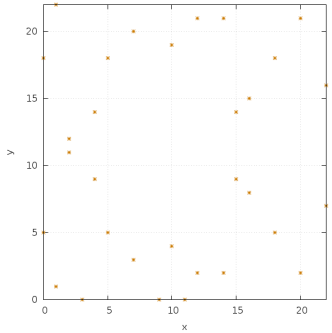
$$y^2 = x^3 + ax + b$$
$$y^2 = x^3 - 2x + 2$$



Pro eliptickou křivku e definujeme:

- Negace bodu: $B = -A$
  - $(B_x, B_y) = (A_y, -A_y)$
- Sčítání bodů: $C = A + B$
  - $-C = \overrightarrow{AB} \cap e$
- Zdvojnásobení bodu: $B = 2 \cdot A$
  - Obdobně jako sčítání, použitá přímka je tečnou v bodě A.
- Násobení bodu skalárem $B = n \cdot A$
  - Rozklad, například:
  - $B = 5 \cdot A = A + 4 \cdot A = A + 2 \cdot (2 \cdot A)$
- Problém: Známe A, známe B, $n = ?$

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



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

- 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 RSA: Baltimore CyberTrust Root

```
Data:    Version: 3 (0x2)    Serial Number: 33554617 (0x20000b9)
Signature Algorithm: sha1WithRSAEncryption
    Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
    Validity
        Not Before: May 12 18:46:00 2000 GMT
        Not After : May 12 23:59:00 2025 GMT
    Subject: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
            Modulus:
                00:a3:04:bb:22:ab:98:3d:57:e8:26:72:9a:b5:79:
                ... 15x ...
                78:8d:76:bf:fc:9e:8e:5d:2a:86:a7:4d:90:dc:27:
                1a:39
            Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            E5:9D:59:30:82:47:58:CC:AC:FA:08:54:36:86:7B:3A:B5:04:4D:F0
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:3
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
Signature Algorithm: sha1WithRSAEncryption
     85:0c:5d:8e:e4:6f:51:68:42:05:a0:dd:bb:4f:27:25:84:03:
     ... 12x ...
     fe:81:dc:32:6a:1e:b5:ee:3c:d5:fc:e7:81:1d:19:c3:24:42:
     ea:63:39:a9
```

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

Certifikát	Algoritmus	Bitů	Síla	Velikost
Baltimore CyberTrust Root	RSA	2048	112	891
Microsoft IT SSL SHA2	RSA	4096	$\approx$ 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 ECC: Baltimore CyberTrust Root

```
Data:    Version: 1 (0x0)    Serial Number: 33554617 (0x20000b9)
Signature Algorithm: ecdsa-with-SHA256
    Issuer: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
    Validity
        Not Before: May 12 18:46:00 2000 GMT
        Not After : May 12 23:59:00 2025 GMT
    Subject: C=IE, O=Baltimore, OU=CyberTrust, CN=Baltimore CyberTrust Root
    Subject Public Key Info:
        Public Key Algorithm: id-ecPublicKey
            Public-Key: (224 bit)            pub:
                04:af:fb:7a:ec:8d:d1:25:62:68:bb:d7:cd:ab:c9:
                df:97:cc:41:ba:b0:c2:ed:e2:46:ca:d0:dc:4d:35:
                fc:78:f3:a8:7b:e2:84:a9:f2:5a:15:84:4a:1e:d8:
                fa:e7:ed:fa:fe:84:f9:4c:ef:81:6a:2a
            ASN1 OID: secp224r1
            NIST CURVE: P-224
    X509v3 extensions:
        X509v3 Subject Key Identifier:
            1D:B7:9F:F2:EA:A2:CA:70:B6:2E:99:E5:22:E6:B5:32:04:81:F8:49
        X509v3 Basic Constraints: critical
            CA:TRUE, pathlen:3
        X509v3 Key Usage: critical
            Certificate Sign, CRL Sign
Signature Algorithm: ecdsa-with-SHA256
     30:3e:02:1d:00:8b:bf:d7:45:4a:d3:73:18:cb:7e:a3:c9:c8:
     72:b7:f7:f2:c0:6f:bc:15:ce:ba:2f:c4:75:87:68:02:1d:00:
     c2:a3:f1:45:06:13:1b:fb:e2:c9:ee:b3:09:93:3f:3f:e1:33:
     11:6b:2e:c3:89:c0:61:6e:11:df
```

- 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

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

- 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

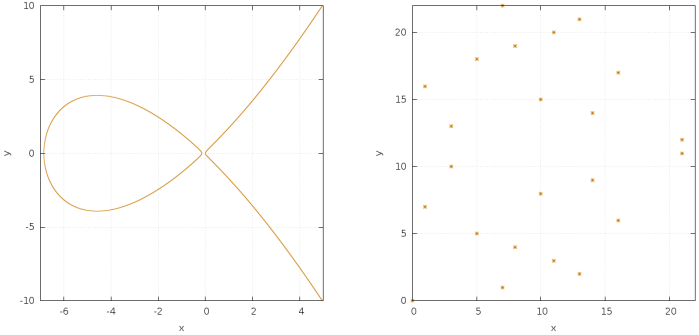
- National Institute of Standards and Technology.
- Vládní instituce USA.
- Dual_EC_DRBG
  (Dual Elliptic Curve Deterministic Random Bit Generator)
  - Známé slabiny.
  - Nedůvěryhodně zvolené základní body na křivce.
  - Dva náhodné body P, Q: ne-úplně-špatný generátor,
  - $Q = n \cdot P$, pokud známe 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 0 či inf,
  - musíme zvolit jiné parametry,
  - implementace zde často mají chybu,
  - typický postranní kanál nebo oslabení systému.
- Problém: práce s body, které nejsou na křivce.

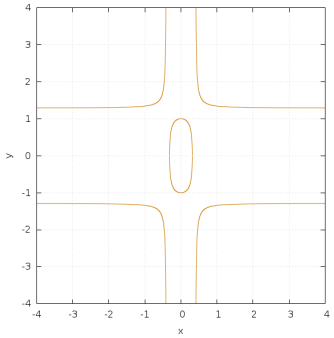
- Daniel J. Bernstein et al.: křivky "s méně problémy"

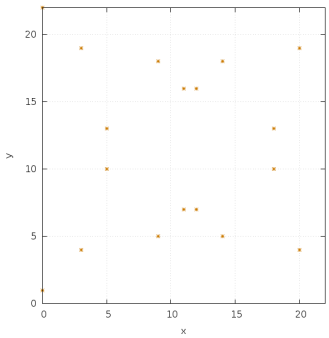
$$3y^2 = x^3 + 7x^2 + x$$



Alternativní křivky

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





- 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

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

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

- 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
- GNUTLS
- Network Security Services
- Microsoft CryptoAPI: Next Generation

- Podporuje ECC od verze 0.9.8 (5. července 2005)
- ECDSA – `ECDSA_*` `*-ECDSA-*`
- ECDH – `ECDH_*` `ECDH-*`
- Příklad (konfigurační řetězec): `ECDH-ECDSA-AES256-CBC-SHA384`

- GNU implementace
- Od verze 3.0.0. (29. červenec 2011)
- Konfigurační řetězce – zde se jim říká “priority”.
- Příklad: `ECDH-ECDSA-AES256-CBC-SHA384`

- Prohlížeče Chromium a Firefox používají knihovny NSPR a NSS.
- ECC je plně podporováno nejméně od roku 2009.
- Všechna vydání za posledních šest let ...
- Na straně klienta není potřeba žádná konfigurace.

- Windows Vista a novější, Windows Server 2008 a novější
- ECDSA – `BCRYPT_ECDSA_P256_ALGORITHM`
- ECDH – `BCRYPT_ECDH_P256_ALGORITHM`
- Example: `TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384`

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

... a odpovědi.

Děkuji za pozornost.