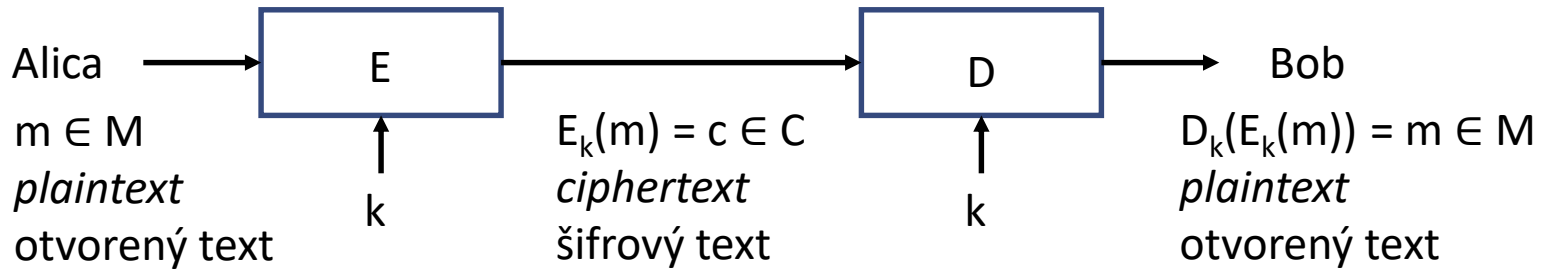
Kryptografické systémy
Asymetrická kryptografia 2

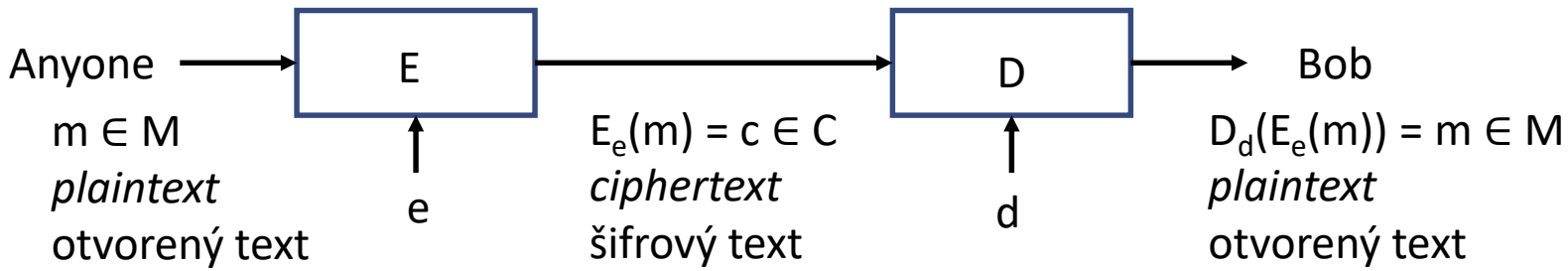
doc. RNDr. Jozef Jirásek, PhD.

ZS 2023

Kryptografické systémy s verejným kľúčom



k – tajný kľúč (secret key) Boba a Alice
problémy s bezpečným prenosom kľúča k adresátovi správy



e – verejný kľúč (public key) Boba
d – súkromný kľúč (private key) Boba

Princíp asymetrickej kryptografie

- pre šifrovaciu funkciu $E(e, m) = c$ je výpočet inverznej funkcie $E^{-1}(e, c) = m$
  výpočtovo (algoritmicky dokázateľne) zložitý – jednocestná resp. jednosmerná funkcia (one-way)
- na dešifrovanie existuje funkcia
  $$D(d, c) = E^{-1}(e, c) = m$$
  „zadné vrátka“ (trapdoor) – len ak poznáme d
- z e nie je možné jednoducho vypočítať d !

- $x \rightarrow x^e \bmod pq$ (RSA)
- $x \rightarrow x^2 \bmod pq$ (Rabin)

Princíp asymetrickej kryptografie

- pre šifrovaciu funkciu $E(e, m) = c$ je výpočet inverznej funkcie $E^{-1}(e, c) = m$
  výpočtovo (algoritmicky dokázateľne) zložitý – jednocestná resp. jednosmerná funkcia (one-way)
- na dešifrovanie existuje funkcia
  $$D(d, c) = E^{-1}(e, c) = m$$
  „zadné vrátka“ (trapdoor) – len ak poznáme d
- z e nie je možné jednoducho vypočítať d !

- $x \rightarrow x^e \bmod pq$ (RSA)
- $x \rightarrow x^2 \bmod pq$ (Rabin)
- $x \rightarrow g^x \bmod p$ $g^x \bmod p \rightarrow x$?

Hľadanie diskrétneho logaritmu

- $x \rightarrow g^x \bmod p \quad g^x \bmod p \rightarrow x$?

  problém diskrétneho logaritmu (DLP)

- ak g je generátor multiplikatívnej cyklickej grupy $\mathbb{Z}_p^*$
  t.j. $\forall\, i \in \{1, \ldots, p-1\} \;\; \exists\, j : \; g^j \bmod p = i$
  (umocňovaním $g^i \bmod p$ dostaneme všetky prvky z $\{1,\ldots,p-1\}$)
  je DLP ťažký problém (nepoznáme polynomiálne riešenie)

- $g^{p-1} \equiv 1 \pmod p \;\Rightarrow\; g^{(p-1)/2} \equiv -1 \pmod p$

  $(g^x)^{(p-1)/2} \equiv (g^{(p-1)/2})^x \equiv (-1)^x \pmod p$ - vieme zistiť paritu x

  (Pohling-Hellmanov algoritmus) – pre malé faktory (p-1)

- podobné postupy ako pri faktorizácii – porovnateľné bezpečné dĺžky kľúčov

Cyklická grupa $\mathbb{Z}_{13}^*$

a^0	a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	
1	2	4	8	3	6	12	11	9	5	10	7	1	* 2
1	3	9	1	3	9	1	3	9	1	3	9	1	
1	4	3	12	9	10	1	4	3	12	9	10	1	
1	5	12	8	1	5	12	8	1	5	12	8	1	
1	6	10	8	9	2	12	7	3	5	4	11	1	* 6
1	7	10	5	9	11	12	6	3	8	4	2	1	* 7
1	8	12	5	1	8	12	5	1	8	12	5	1	
1	9	3	1	9	3	1	9	3	1	9	3	1	
1	10	9	12	3	4	1	10	9	12	3	4	1	
1	11	4	5	3	7	12	2	9	8	10	6	1	* 11
1	12	1	12	1	12	1	12	1	12	1	12	1	

Testovanie generátora

- testovať stačí len pozície, kde $a^k \equiv 1 \pmod p$
- to môže byť len vtedy, keď $k \mid (p-1)$
- stačí testovať len najvyšší násobok - teda ak

  $(p-1) = q_1^{r1} q_2^{r2} \dots q_s^{rs}$ je prvočíselný rozklad

  a je generátor $\mathbb{Z}_p^*$ $\iff \forall\, i \in \{1,\dots,s\}$ $a^{(p-1)/qi} \not\equiv 1 \pmod p$
- pre $p = 2q + 1$ (bezpečné prvočíslo – (p-1) má faktory 2 a q)

  $\mathbb{Z}_p^*$ má $\phi(p-1) = \phi(2)\phi(q) = q - 1$ generátorov (~ 50 %)

  stačí testovať $a^q \not\equiv 1 \pmod p$
- možno použiť len podgrupu – pre $q \mid (p-1)$ vziať generátor $g = h^{(p-1)/q} \bmod p$ bude $\mathrm{ord}(g) = q$ ($g^q \equiv 1 \pmod p$ FLT)

Kryptografický systém ElGamal

Elgamal (1985)

- veľké náhodné p a generátor g grupy $\mathbb{Z}_p^*$
- náhodné d ∈ {2, ..., p-2} , $e = g^d \bmod p$
- verejný kľúč p, g, e súkromný kľúč d
- pre m ∈ $\mathbb{Z}_p^*$ a náhodné k ∈ $\mathbb{Z}_{p-1}$:

$$E_{p,g,e}(m) = (g^k \bmod p, (e^k \cdot m) \bmod p) = (r, s) = c$$

$$D_{p,g,d}(c) = s \cdot r^{-d} \bmod p = e^k \cdot m \cdot (g^k)^{-d} \bmod p =$$
$$= (g^d)^k \cdot (g^k)^{-d} \cdot m \bmod p = m$$

- randomizované šifrovanie (k musí byť stále iné)
- poznanie k dovolí dešifrovať $s \cdot e^{-k} \bmod p = m$
- výpočet d z e ⇒ DLP, výpočet k z r ⇒ DLP

ElGamal - zraniteľnosti

- homomorfná vlastnosť

$$E_{p,g,e}(m_1) = (g^{k1} \bmod p,\ e^{k1} \cdot m_1 \bmod p)$$

$$E_{p,g,e}(m_2) = (g^{k2} \bmod p,\ e^{k2} \cdot m_2 \bmod p)$$

$$(g^{k1}\, g^{k2} \bmod p,\ e^{k1}\, e^{k2} \cdot m_1\, m_2 \bmod p) = E_{p,g,e}(m_1 \cdot m_2)$$

- modifikovateľnosť správy

$$c = (r, s) \rightarrow (r, s \cdot m') = c'$$

$$D_{p,g,d}(c') = s \cdot m' \cdot r^{-d} \bmod p = e^k \cdot m \cdot m' \cdot (g^k)^{-d} \bmod p =$$
$$= (g^d)^k \cdot (g^k)^{-d}\, m \cdot m' \bmod p = m \cdot m'$$

- náhodnosť a nepredikovateľnosť k

Reálne eliptické krivky

riešenia integrálnych rovníc pre výpočet osí elíps
všeobecne v tvare $y^2 + axy + by = x^3 + cx^2 + dx + e$

pre potreby kryptografie $y^2 = x^3 + ax + b$ $(4a^3 + 27b^2 \neq 0)$

body $E = \{[x,y] \mid y^2 = x^3 + ax + b\} \cup \{O\}$

E je symetrická podľa x, O v nekonečne

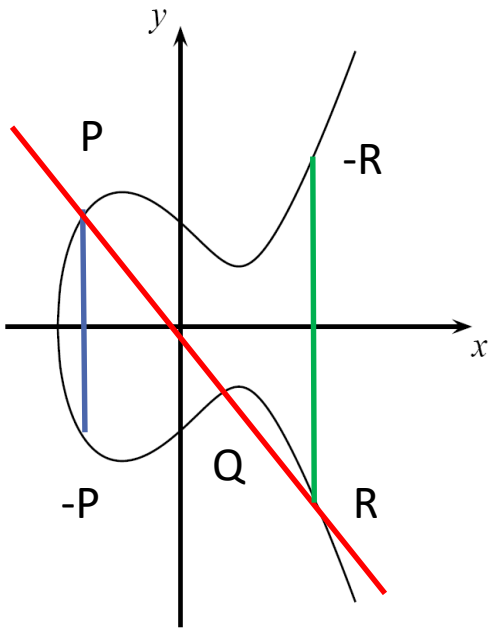
grupová operácia $\mathring{+}$ $P \mathring{+} O = O$

$P = [x, y]$, $-P = [x, -y]$, $P \mathring{+} (-P) = O$

priamka, určená dvomi bodmi z E
pretne E aj v treťom bode

$P \mathring{+} Q \mathring{+} R = O$ $P \mathring{+} Q = -R$

$P \mathring{+} P = -$ (priesečník dotyčnice v P s E)



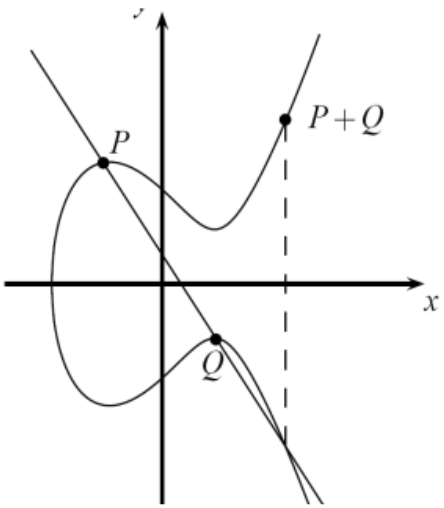
Reálne eliptické krivky

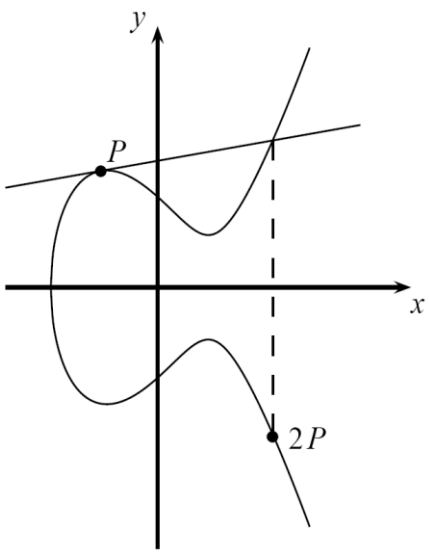
$[x_1, y_1] \mathring{+} [x_2, y_2] = [x_3, y_3] = [\lambda^2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1]$

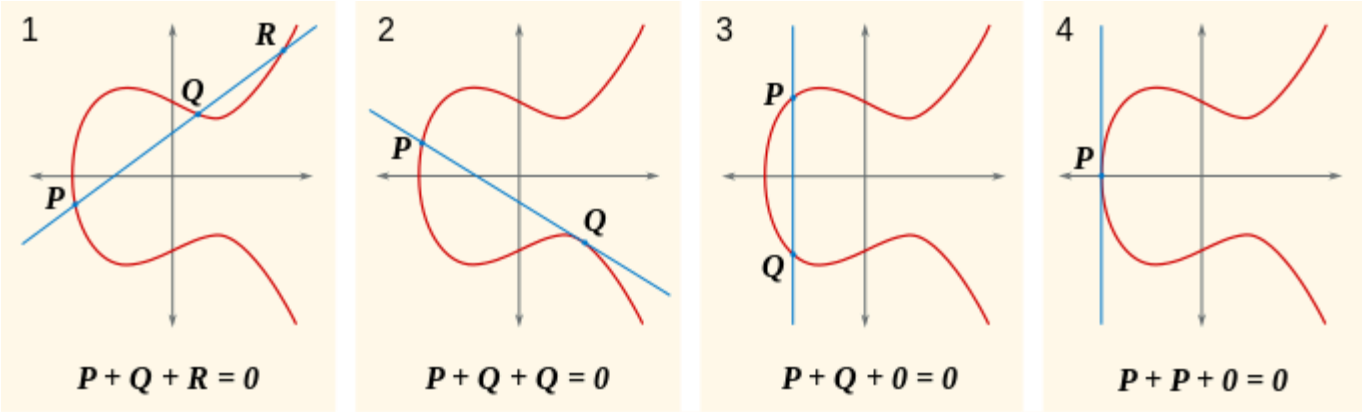
kde pre $[x_1, y_1] = [x_2, y_2]$ bude $\lambda = (3x_1^2 + a)/2y_1$

a pre $[x_1, y_1] \neq [x_2, y_2]$ $\lambda = (y_2 - y_1)/(x_2 - x_1)$

$\mathring{+}$ je komutatívna operácia

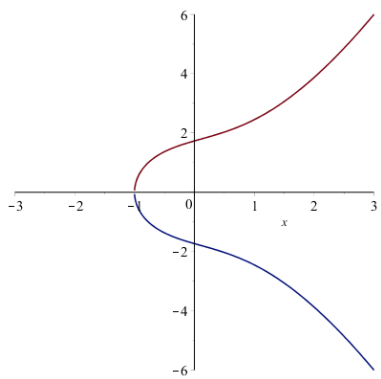




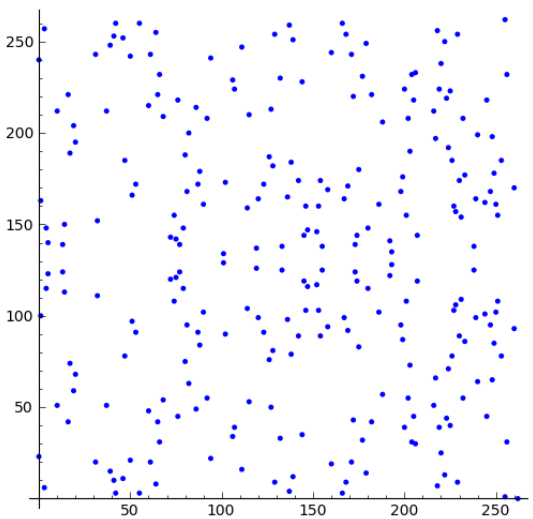

1
R
Q
P
P + Q + R = 0
2
P
Q
P + Q + Q = 0
3
P
Q
P + Q + 0 = 0
4
P
P + P + 0 = 0

Eliptické krivky nad konečným poľom

- GF(p) = $(\mathbb{Z}_p, +, \cdot)$ p – prvočíslo, všetky výpočty mod p
- $E_p(a,b) = \{[x, y] \in \mathbb{Z}_p \times \mathbb{Z}_p \mid y^2 \equiv x^3 + ax + b \pmod p\} \cup \{O\}$
  $a, b \in \mathbb{Z}_p$: $4a^3 + 27b^2 \not\equiv 0 \pmod p$ s operáciou $\mathring{+}$ mod p
- pre $P \in E$ $kP = P \mathring{+} P \mathring{+} \ldots \mathring{+} P$ $kP \rightarrow k$ ECDLP problém
- $p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$



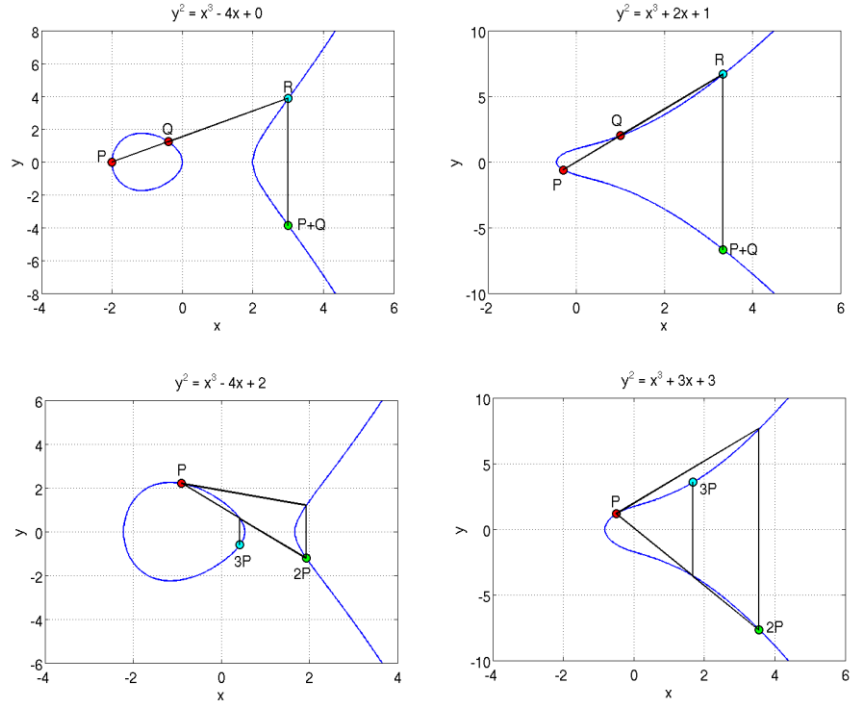
$y^2 = x^3 + 2x + 3$



$y^2 \equiv x^3 + 2x + 3 \bmod 263$

Vhodné krivky pre ECC

- iné krivky



EC pre Microsoft Media DRM (160 b = 20 B blok)

$y^2 = x^3 + 317689081251325503476317476413827693272746955927\,x$
$+\ 79052896607878758718120572025718535432100651934$
$(\mathrm{mod}\ 785963102379428822376694789446897396207498568951)$

Curve25519 (OpenSSH, ...) $y^2 \equiv x^3 + 486662\,x^2 + x \pmod{2^{255} - 19}$

NIST doporučenia pre ECC parametre

- NIST P-256 $p = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1$

$$y^2 = x^3 - 3x + 41058363725152142129326129780047268409114441015993725554835256314039467401291$$

$$|E| = 115792089210356248762697446949407573529996955224135760342422259061068512044369$$

- NIST P-384 (top secret) $p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$

$$y^2 = x^3 - 3x + 27580193559959705877849011840389048093056905856361568521428707301988689241309860865136260764883745107765439761230575$$

$$|E| = 39402006196394479212279040100143613805079739270465446667946905279627659399113263569398956308152294913554433653942643$$

ECC – Elliptic-curve cryptography

- Miller 1986, Koblitz 1987
- $(E, \mathring{+})$ grupa bodov diskrétnej eliptickej krivky
- generátor $G \in E$ podgrupy $ord(G) = q$ prvočíslo
- súkromný kľúč $d \in \mathbb{Z}_q$, verejný kľúč $Y = dG$
- pre $M \in E$ a náhodné $k \in \mathbb{Z}_q$: (ElGamalova schéma)
  $E_{p,a,b,Y}(M) = (kG, kY \mathring{+} M) = (R, S)$
  $D_{p,a,b,d}((R,S)) = S - dR = (kY \mathring{+} M) - dR = (kd)G \mathring{+} M - (kd)G = M$

- bod $P = [x, y] \in E$ možno reprezentovať dvojicou $(x, sign(y))$
- $m \rightarrow m^3 + am + b \equiv y^2 \bmod p$ s pravdepodobnosťou ~ 0,5 môžeme skúšať hodnoty $Tm+j$ $(j<T)$ a každú správu upraviť

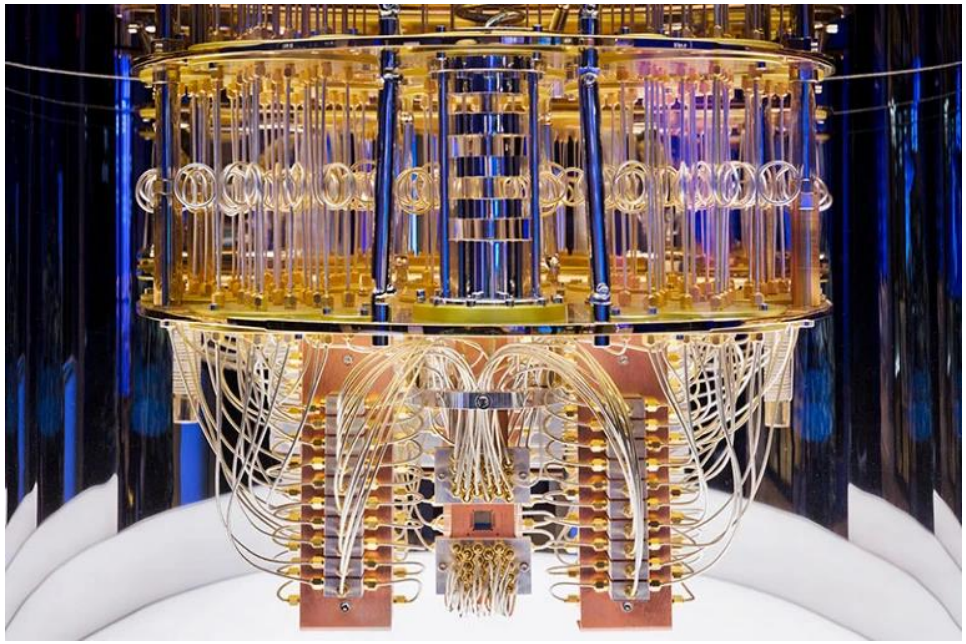
Ekvivalentné dĺžky kľúčov (NIST SP 800-57)

AES	RSA	DLP	ECC
48	480	480	96
56	640	640	112
64	816	816	128
80	1024	1024	160
112	2048	2048	224
128	3072	3072	256
160	5312	5312	320
192	7680	7680	384
256	15360	15360	512

Kvantové počítače

127 qubitový kvantový počítač
(IBM november 2021)

- na riešenie ECDLP
  s 256 b modulom
  treba 2330 qb
- na faktorizáciu
  2048 b RSA
  treba 4096 qb
  (Shorov alg.)



Postkvantová kryptografia

- faktorizáciu, DLP, ECDLP je možné riešiť polynomiálne pomocou kvantových počítačov (Shorov algoritmus)
- postkvantová kryptografia - založená na problémoch s ťažkým riešením aj s použitím kvantových počítačov
- problémy v mrežových bodoch n-rozmerných priestorov
  - lattice-based cryptography, LWE – learning with errors
  - ring learning with errors (Ring-LWE)
  - NTRU encryption (N-th degree truncated polynomial ring)
- multivariačná kryptografia
- kryptografia na báze autokorekčných kódov (McEliece)
- supersingulárne eliptické krivky

NIST PQC standard - 2022

- Public-Key Encryption/KEM

  CRYSTALS-Kyber (Ring-LWE + NTT)

- Digital Signature

  CRYSTALS-Dilithium, Falcon, SPHINCS

Ďakujem za pozornosť.

jozef.jirasek@upjs.sk