MINISTERSTVO FINANCIÍ
SLOVENSKEJ REPUBLIKY

EFQM
Recognised for excellence
5 star - 2012

Postkvantová kryptografia

Pavol Zajac

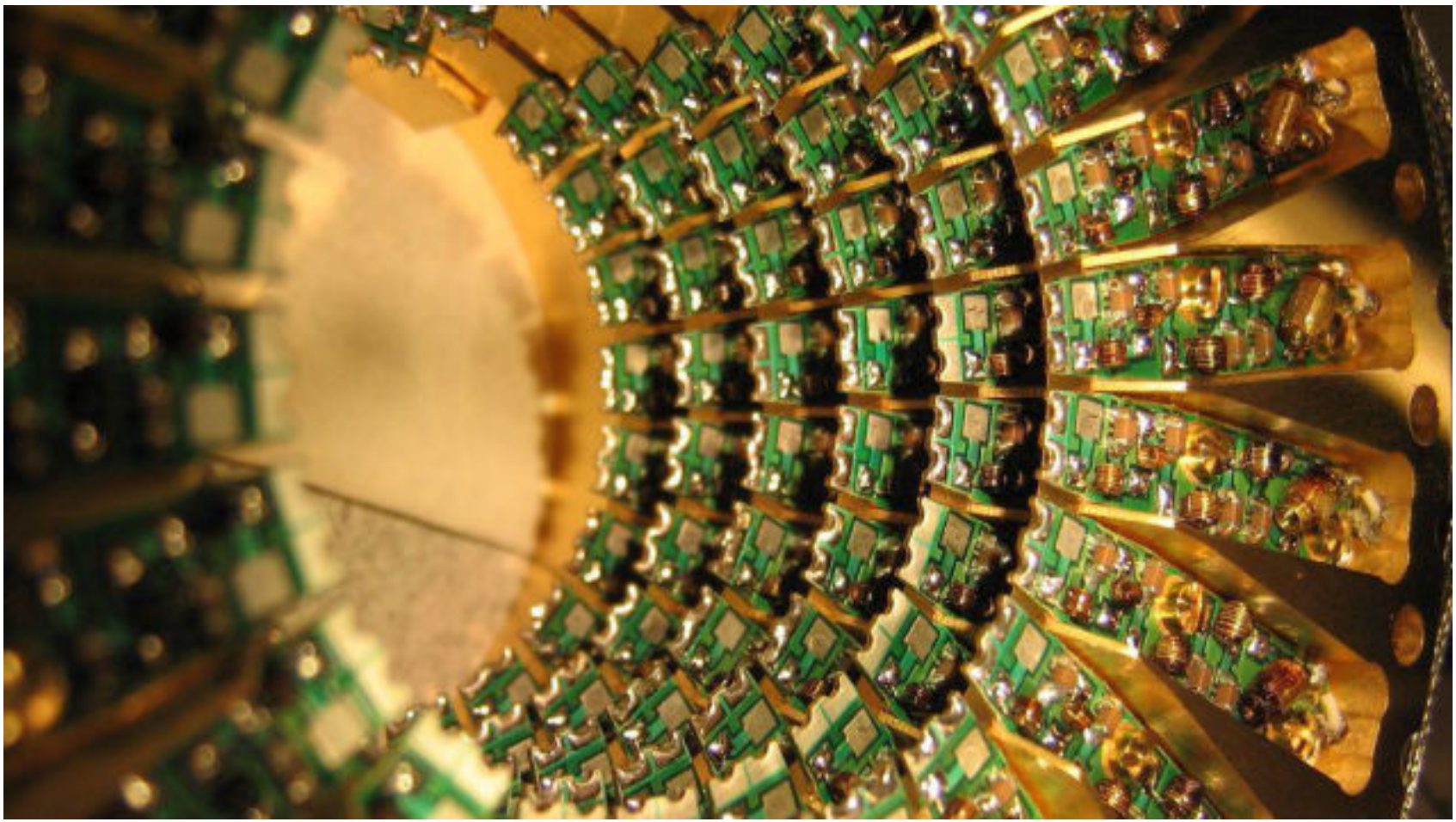
Ústav informatiky a matematiky, Fakulta elektrotechniky a informatiky
Slovenská technická univerzita v Bratislave

2014

KPMG
cutting through complexity™

Obsah prezentácie

Kvantový počítač



Kvantový počítač D-Wave

- Špecializované zariadenie na riešenie problému diskrétnej optimalizácie
- Analógia s analógovými počítačmi
- Kontroverzia, či to je vôbec „kvantový počítač”

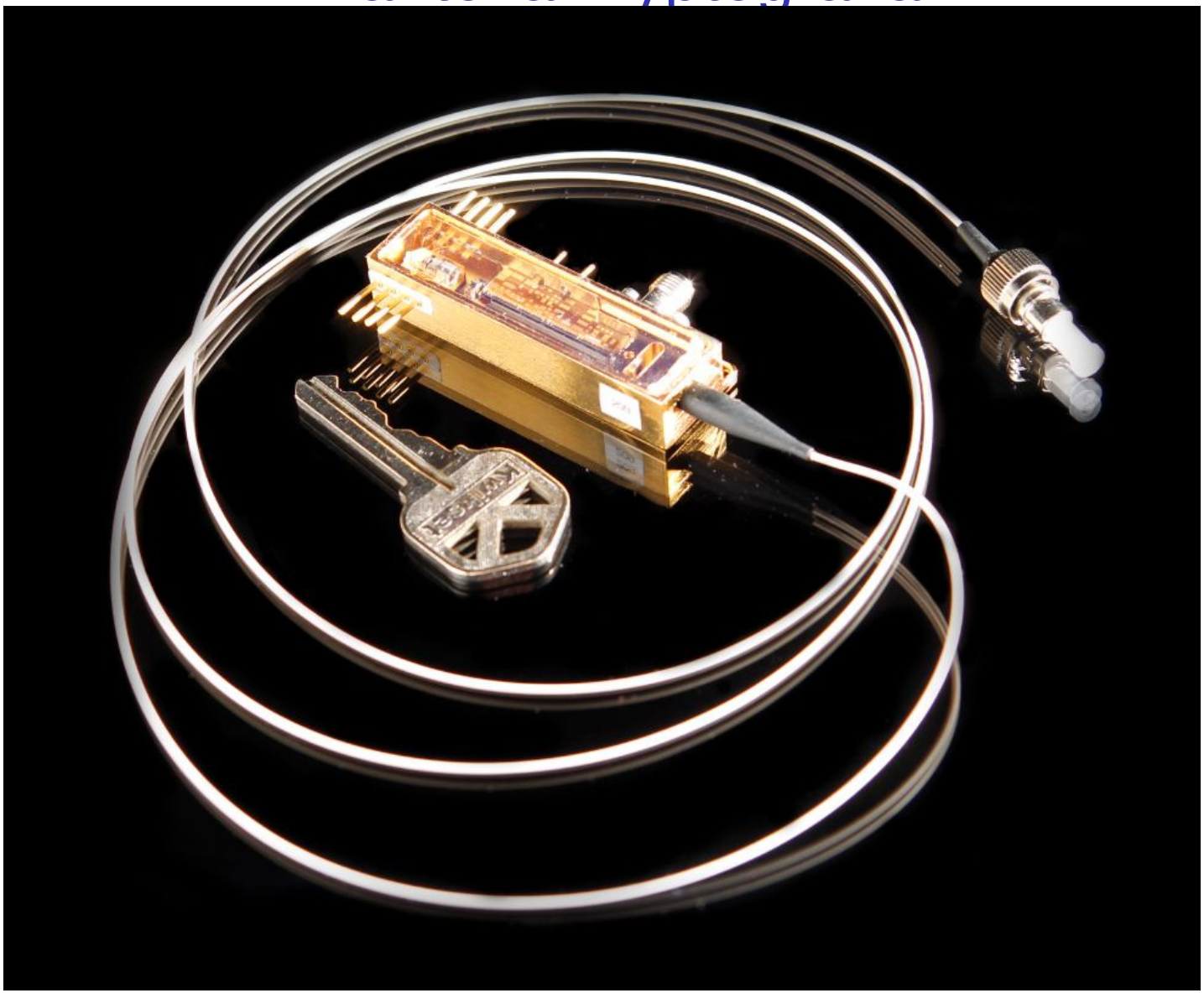
Univerzálny kvantový počítač

- Využíva kvantovo-mechanické princípy na univerzálne výpočty
- Kvantové bity (*qubit*) môžu reprezentovať veľa stavov naraz
- Rádovo rýchlejšie algoritmy na riešenie niektorých typov úloh
- Problém dekoherencie: je zložité vytvoriť kvantový počítač s veľkým počtom (previazaných) qubitov

Kvantový počítač a kryptografia

- Shor (1994):
  - faktorizácia n-bitového čísla pomocou n^2 kvantových hradiel
  - exponenciálne zrýchlenie voči klasickým algoritmom
  - existujú verzie na riešenie DLP a ECDLP: RSA, DSA, ECC nie sú bezpečné voči útočníkom s kvantovým počítačom
- Grover (1996):
  - prehľadá N hodnôt v čase $\sqrt{N}$
  - kvadratické zrýchlenie „brute-force” útokov
  - obrana: 2x dlhšie kľúče

Kvantová kryptografia



Kvantová kryptografia

- Kvantová kryptografia využíva kvantové javy na zabezpečenie kryptografických cieľov
- Kvantová výmena kľúča:
  - BB84 protokol: princíp kvantovej neurčitosti
  - E91 protokol: kvantové previazanie
- Nevýhoda: drahé riešenia, špecifická infraštruktúra

Postkvantová kryptografia

- Postkvantová kryptografia
  - skúma *klasické* kryptografické algoritmy odolné voči útokom na kvantovom počítači
  - nasaditeľná aj na súčasnej infraštruktúre
  - (zatiaľ) nie je tak efektívna ako bežné kryptografické algoritmy
- Symetrická kryptografia
  - štandardné algoritmy (AES, SHA-2,...) považované za bezpečné
  - potreba dlhších kľúčov (Grover), napr. AES-128 $\rightarrow$ AES-256
- Asymetrická kryptografia
  - štandardné algoritmy (RSA, DSA, ECC) nie sú bezpečné
  - potreba (staro-)nových postkvantových algoritmov

Postkvantová kryptografia

Hlavné smery výskumu:

- využitie jednosmerných (hašovacích) funkcií (*hash-based PQC*)
- dekódovací problém (*code-based PQC*)
- krátke vektory v grupe mrežových bodov (*lattice-based PQC*)
- sústavy nelineárnych rovníc (*MQ PQC*)
- iné...

Postkvantová kryptografia na báze hašovacích funkcií

Kryptografická hašovacia funkcia (SHA-2, SHA-3?,...):

- jednosmerná: nevieme invertovať $y = h(x)$
- bezkolízna: nevieme nájsť $h(x_1) = h(x_2)$
- ... nevieme zaútočiť ani na kvantovom počítači: zložitosť $O(2^{n/3}$ pre n-bitový odtlačok

Široké využitie v bežných systémoch:

- HMAC: odtlačok využívajúci tajný kľúč
- elektronický podpis: podpíše sa odtlačok dokumentu
- rôzne protokoly

El. podpis využitím iba hašovacích funkcií

Lamportova podpisová schéma:

- Tajný kľúč: $\big((r_{1,0}, r_{1,1}), (r_{2,0}, r_{2,1}) \ldots, (r_{n,0}, r_{n,1})\big)$
- Verejný kľúč: $\{p_{i,j} = h(r_{i,j}); i = 1, 2, \ldots, n; j = 0, 1\}$
- Podpis správy $m = (m_1, m_2, \ldots, m_n) \in \mathbb{Z}_2^n$ je n-tica $s = \big(r_{1,m_1}, r_{1,m_1}, \ldots, r_{1,m_n}\big)$
- Overenie podpisu: kontrola, či $p_{i,m_i} = h(r_{i,m_i})$

Analýza Lamportovej schémy

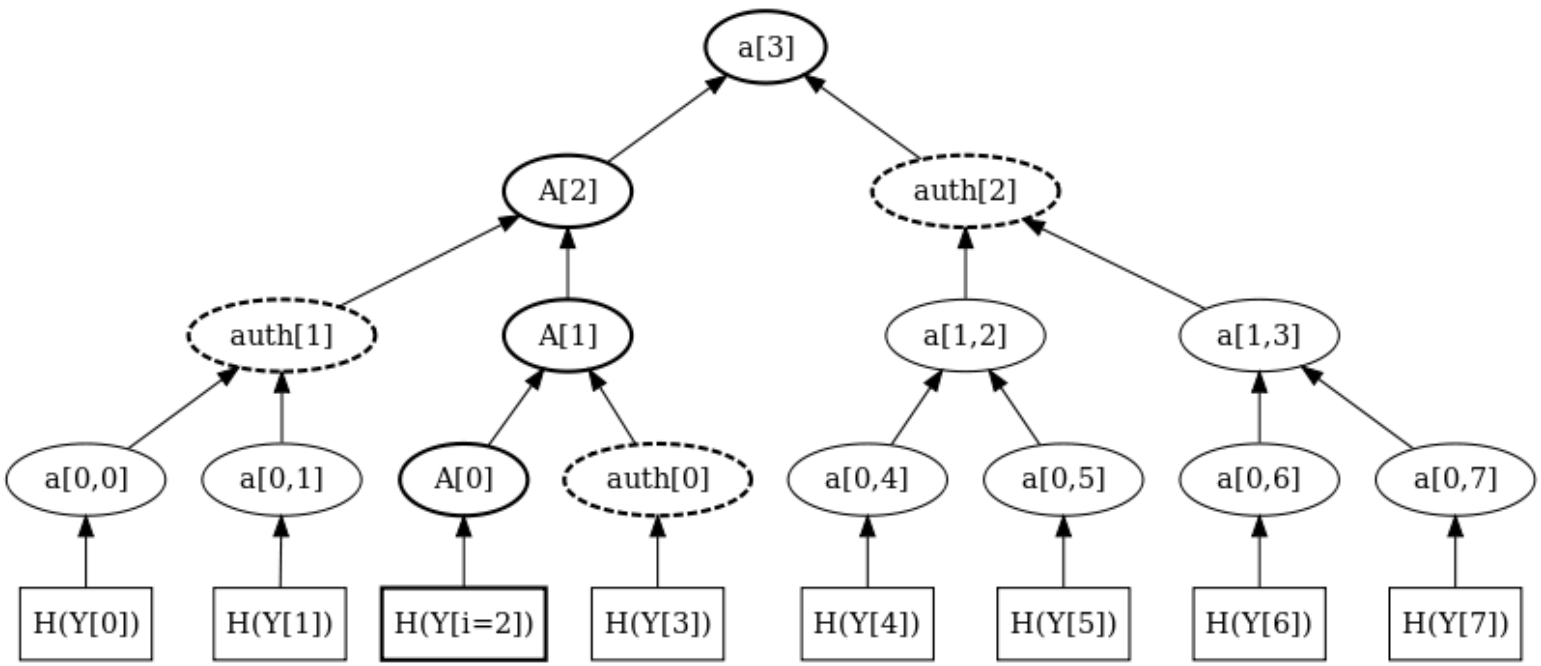
Pre 80-bitovú post-kvantovú bezpečnosť:

- 256-bitové odtlačky, podpisuje sa 256-bitový odtlačok dokumentu
- Verejný kľúč: $2 \times 256 \times 256$ bit = $16KB$
- Tajný kľúč: $16KB$, resp. PRNG so 128-bitovým kľúčom
- Overenie podpisu: SHA-2 odtlačky nad $8kB$: cca $70\mu s$ (RSA rádovo ms)
- Žiadne problémy s komplikovanou matematikou a programovaním (postačuje implementácia SHA-2/SHA-3)

Analýza Lamportovej schémy

Hlavná nevýhoda: Jednorázový podpis

- Reťazenie podpisov: nový verejný kľúč súčasť podpisu (hash-chains)
- Merkle trees:



Postkvantová kryptografia založená na dekódovacom probléme

McEliece-ov kryptosystém:

Tajný kľúč Goppov (n, k, t)-kód s generujúcou maticou G, matice S a P

Verejný kľúč $G' = S \cdot G \cdot P$

Šifrovanie $c = m \cdot G' + e$

Dešifrovanie

1. Dekóduj $c' = c \cdot P^{-1}$ na m'
2. Urči $m = S^{-1} \cdot m'$

Parametre McEliece

Rýchlejšie ako porovnateľné RSA, niektoré implementácie aj ako ECC.

Sec. Level	(n, k, t)	PK size [kB] Full PK	Systematic
50	(1024,524,50)	66	32
80	(2048,1751,27)	438	64
80	(1702,1219,45)	254	72
80	(2048,1696,32)	424	73
128	(3178,2384,68)	925	232
128	(4096,3604,41)	1802	217
256	(6944,5208,136)	4415	1104

Postkvantová kryptografia založená na dekódovacom probléme

Alternatívne varianty:

- Niederreiterov kryptosystém: Verejná kontrolná matica, efektívnejší prenosový pomer
- Iné typy kódov: snaha o zníženie veľkosti kľúčov
  - Goppa, 128bit sec.: od 200 kB
  - Wild MECS, 128bit sec.: od 90 kB
  - QC-MDPC, 128bit sec.: od 1 kB

Širšie využitie

- Elektronický podpis: Courtois, Finiasz, Sendrier 2001
- Zero-knowledge identifikácia: Stern 1994
- Hašovacie funkcie
- Protokoly: Zdieľanie tajomstva, oblivious-transfer, ...

CFS podpis

1. Nájdi platný dekódovateľný syndróm s_i, kde $s_i = h(h(m)|i)$
2. Dekóduj s_i (v tajnom kóde), t.j. nájdi z, pre ktoré $s_i = H \cdot z$
3. Podpis je $(z|i)$
4. Overenie podpisu: $H \cdot z = h(h(m)|i)$

Bezpečnosť a rýchlosť závisí na $t = w_H(z)$:

- Rýchlosť podpisu $O(t!)$, t nesmie byť priveľké (ale: algebraické útoky): rádovo desiatky sekúnd
- Dostatočná bezpečnosť iba pre veľké n, dĺžka kľúča je rádovo v MB

McEliece kryptosystém

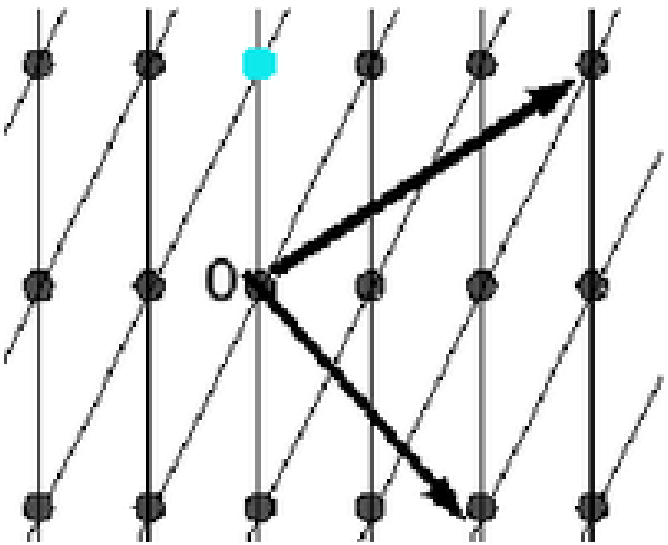
+ Rýchlejší ako porovnateľné RSA, niektoré implementácie aj ako ECC.
+ Ľahšie pochopiteľné algoritmy
+ Menšie možnosti útokov postrannými kanálmi.
- Rozsiahle kľúče.
- Neexistujúce štandardy.

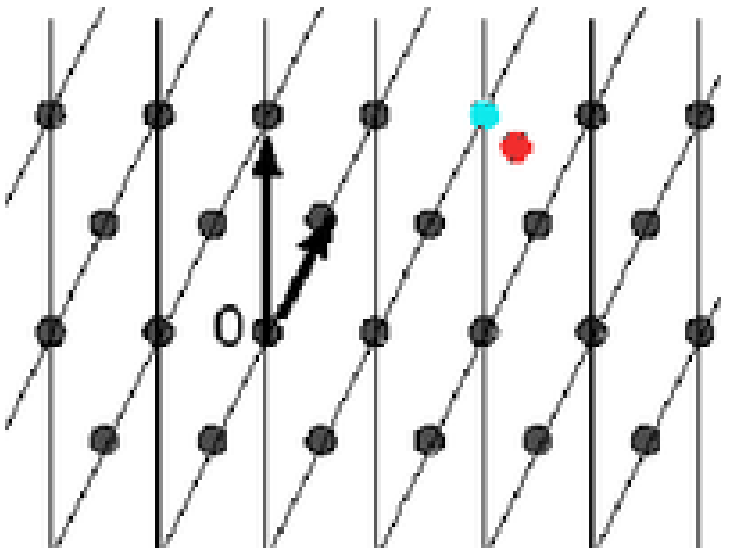
Postkvantová kryptografia využívajúca grupu mrežových bodov

Využíva náročnosť CVP/SVP v grupe mrežových bodov

- Ring-LWE (SVP)
- NTRU (CVP)

Postkvantová kryptografia využívajúca grupu mrežových bodov





Vlastnosti mriežkových systémov

- Podobné kryptografii založenej na kódoch
- Problém: Bezpečnosť vs. efektívnosť
  - Dôkazy bezpečnosti (teoretické) v najťažšej inštancii: neefektívne inštancie
  - Efektívne mriežkové systémy (GGH, verzie NTRU): existujú útoky/nie je jasná zložitosť
- Využívajú sa aj ako stavebný prvok Homomorfných systémov

Porovnanie s klasickými algoritmami (2013)

Schéma	Sec.	Podpis	PrivKey	PubKey	Sign	Verify
RSA-2048	112b	256B	2048B	256B	5 768 360	77 032
ECDSA	128b	64B	64B	32B	67 564	209 328
Ring-LWE	100b	1184B	256B	1536B	634 988	45 036

Postkvantová kryptografia na báze nelineárnych rovníc viac neznámych

- Systémy založené na algebraickej geometrii.
- Využíva náročnosť riešenia sústavy nelineárnych (kvadratických) rovníc viac neznámych nad konečným poľom.

MQ podpisy

Verejný kľúč:

$$P = (p_1(x_1, \ldots, x_n), ..., p_m(x_1, \ldots, x_n)),$$

kde

$$p_i(\mathbf{x}) = \sum_{k=1}^{n} P_{i,k} x_k + \sum_{k=1}^{n} Q_{i,k} x_k^2 + \sum_{k>j} R_{i,j,k} x_j x_k.$$

Podpis: $(\mathbf{x}, \mathbf{y})$, pričom $\mathbf{y} = f(mesg)$

Verifikácia: $y_i \stackrel{?}{=} p_i(\mathbf{x})$

MQ podpisy

Bezpečnosť:

1. Je ťažké riešiť sústavu $\{p_i(\mathbf{x}) = 0; i = 1, \ldots, m\}$

   Tajný kľúč: Afinné transformácie S, T, a tajná sústava P', ktorá sa dá riešiť ľahko.

2. Je ťažké odhaliť štruktúru tajnej sústavy zo znalosti P

Porovnanie MQ podpisov — 2008

Schéma	Podpis	PrivKey	PubKey	KeyGen	Sign	Verify
RSA-1024	1024b	128 B	320 B	2.7 sec	84 ms	2.0 ms
ECDSA-F_2^{163}	320b	48 B	24 B	1.6 ms	1.9 ms	5.1 ms
PMI+ $(136, 6, 18, 8)$	144b	5.5 kB	165 kB	1.1 sec	1.23 ms	0.18 ms
Rainbow $(2^8, 18, 12, 12)$	336b	24.8 kB	22.5 kB	0.3 sec	0.43 ms	0.40 ms
Rainbow $(2^4, 24, 20, 20)$	256b	91.5 kB	83 kB	1.6 sec	0.93 ms	0.74 ms
QUARTZ	128b	71.0 kB	3.9 kB	3.1 sec	11 sec	0.24 ms

Sumarizácia

- asymetrické algoritmy pre klasické počítače odolné voči útokom na kvantovom počítači;
- široké portfólio postkvantových algoritmov pre rôzne účely;
- aktívny výskum v oblasti bezpečnosti a efektívnosti;
- chýbajúca štandardizácia a nasadenie v rozšírených knižniciach.