Kvantová a post-kvantová kryptografie

Milan Radojčić

SSPŠaG – KBB

14. dubna 2026

Hlavní body

Hlavní body

- **Kvantový počítač**
  - Založený na principech kvantové mechaniky.
  - Informace je uložena v **qubitech** – můžou být zároveň 1 i 0, ale při přečtení je z něj 1 nebo 0 s určitou pravděpodobností.
  - Existují problémy, které se dají řešit mnohem rychleji na kvantových počítačích než na klasických.
- **Post-kvantová kryptografie** (PQC)
  - tvorba klasických šifer, které jsou odolné proti útokům pomocí kvantových počítačů
- **Kvantová kryptografie**
  - využívá principy kvantové mechaniky v kryptografii

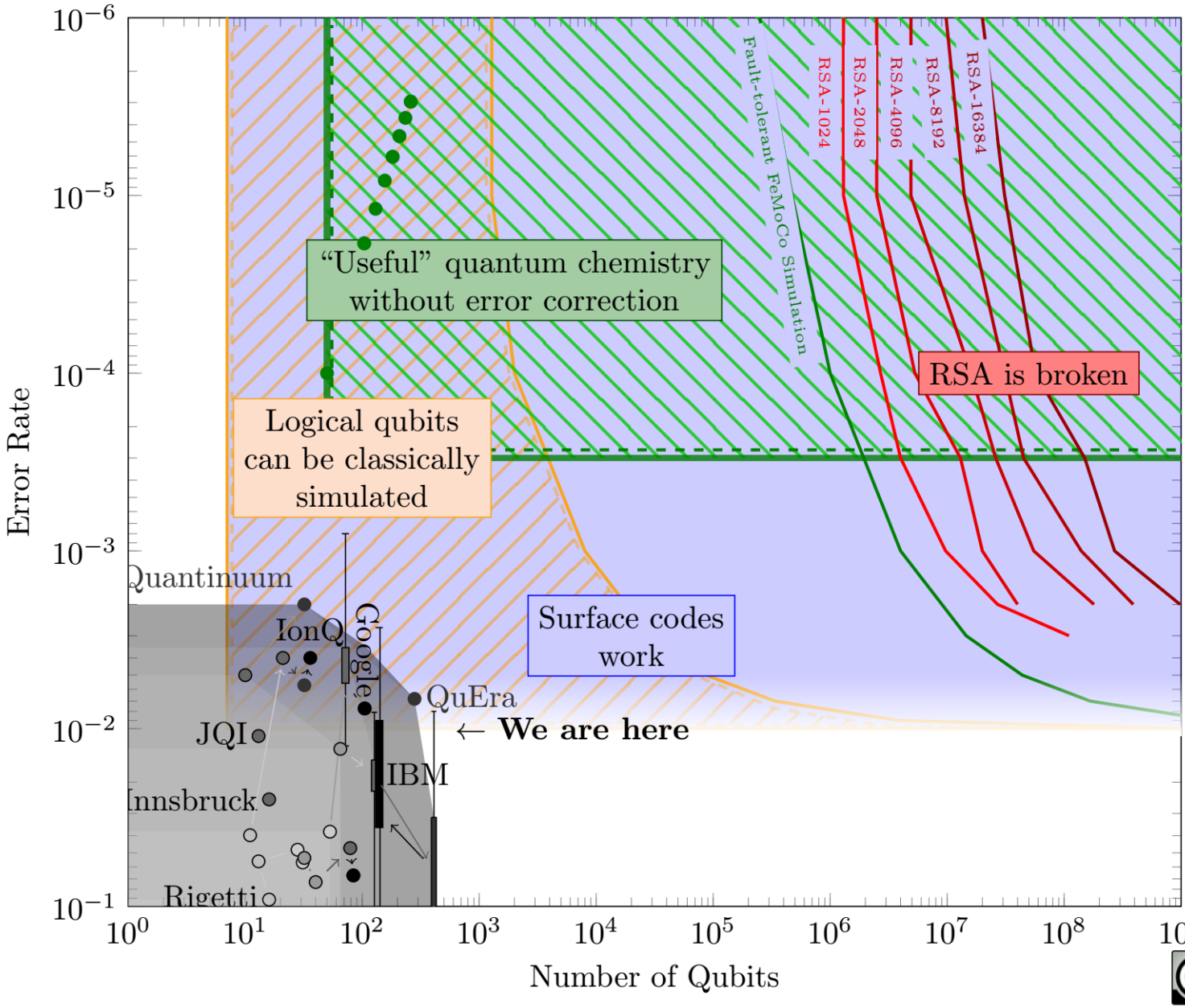
Shorův algoritmus (1994)

- Algoritmus pro rychlejší (v polynomiálním čase) počítání diskrétních logaritmů a faktorizování čísel.[1]
- Teoreticky dokáže rozbít RSA a DHE.
- Největší číslo, které bylo pomocí něj faktorizováno je 21...

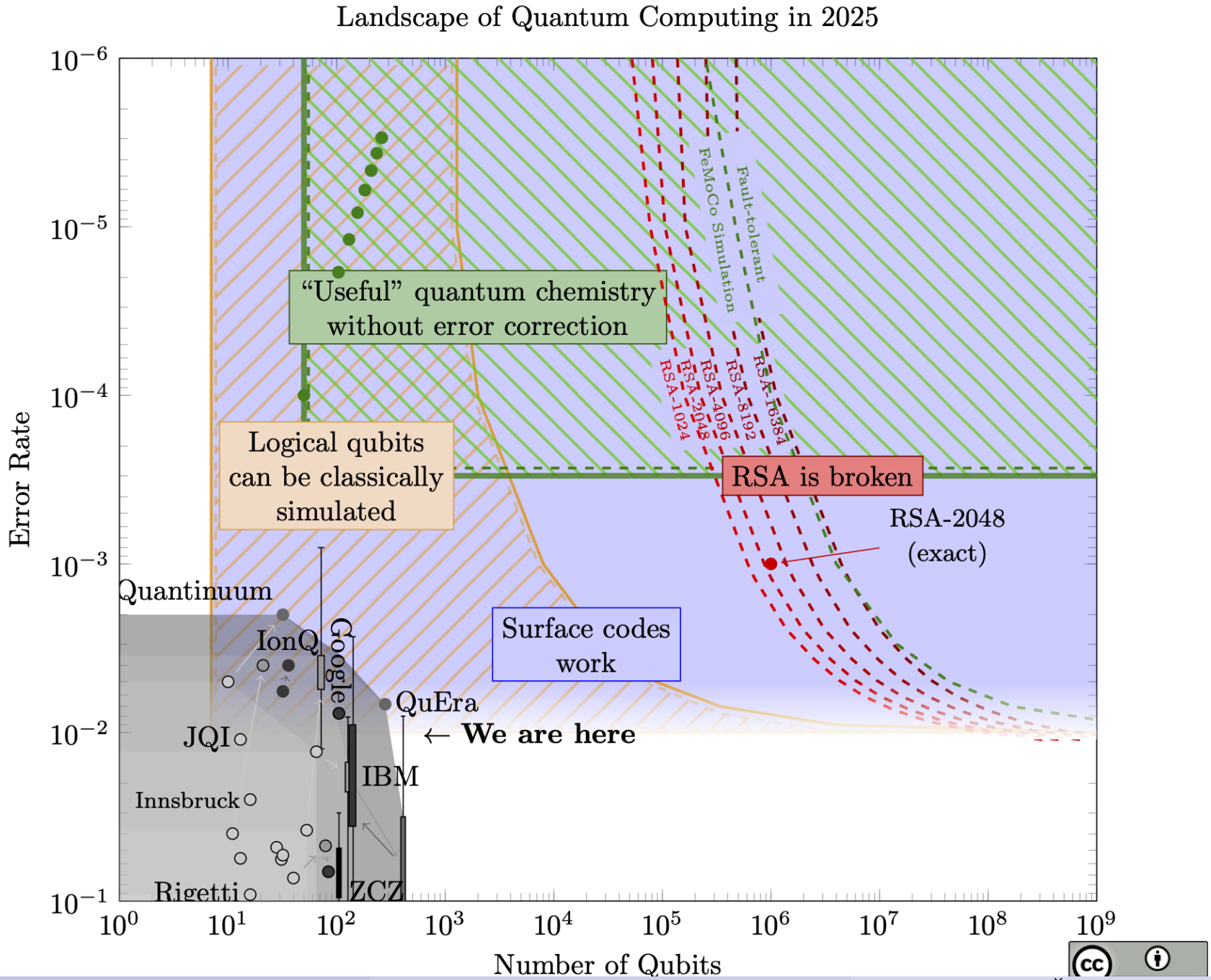
[1] Ve skutečnosti řeší obecnější problém.

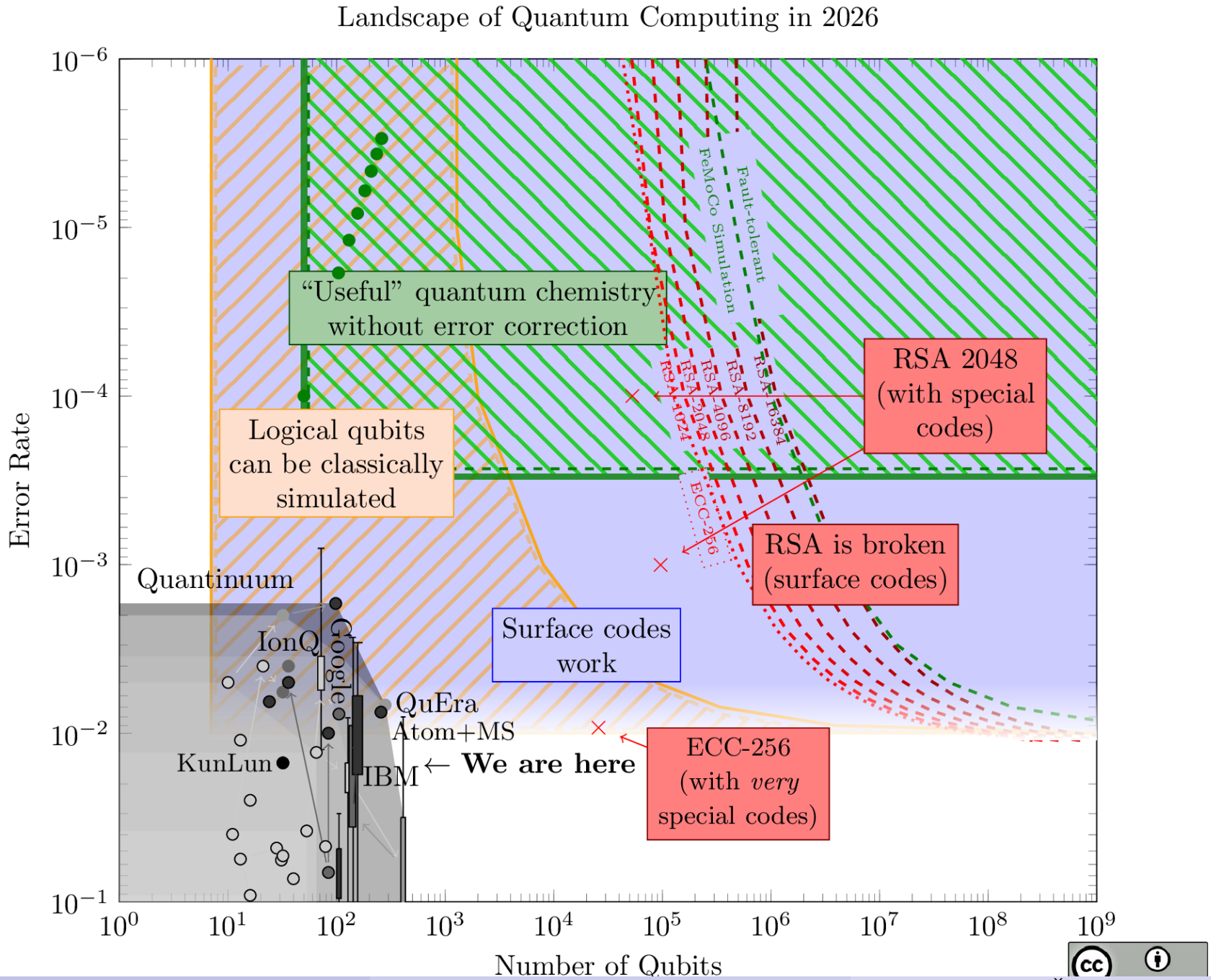
Groverův algoritmus (1996)

- Algoritmus, pomocí kterého jsme schopni zjistit pro zadané y a libovolnou funkci f x, takové, že $f(x) = y$.
- Pokud je n počet vstupů, tak Groverův algoritmus dokáže najít vstup jen po $\sqrt{n}$ krocích, místo klasických n.
- Například pro 128-bitový AES dokáže najít správný klíč jen pomocí 2^{64} iterací.
- V praxi není jednoduše použitelný...



Stav k roku 2024, Zdroj obrázku: Samuel Jacques - `https://sam-jaques.appspot.com/quantum_landscape_2024`


Landscape of Quantum Computing in 2025
Error Rate
Number of Qubits
10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
10^{0}
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
10^{6}
10^{7}
10^{8}
10^{9}
"Useful" quantum chemistry without error correction
Logical qubits can be classically simulated
Surface codes work
RSA is broken
RSA-2048 (exact)
Fault-tolerant
FeMoCo Simulation
RSA-1024
RSA-2048
RSA-4096
RSA-8192
RSA-16384
Quantinuum
IonQ
Google
QuEra
← We are here
JQI
IBM
Innsbruck
Rigetti
ZCZ


Landscape of Quantum Computing in 2026
Error Rate
Number of Qubits
10^{-6}
10^{-5}
10^{-4}
10^{-3}
10^{-2}
10^{-1}
10^{0}
10^{1}
10^{2}
10^{3}
10^{4}
10^{5}
10^{6}
10^{7}
10^{8}
10^{9}
"Useful" quantum chemistry without error correction
Logical qubits can be classically simulated
Surface codes work
RSA 2048 (with special codes)
RSA is broken (surface codes)
ECC-256 (with *very* special codes)
Fault-tolerant
FeMoCo Simulation
RSA-6384
RSA-8192
RSA-4096
RSA-2048
RSA-1024
ECC-256
Quantinuum
IonQ
Google
QuEra
Atom+MS
KunLun
IBM
← We are here

Hlavní body

Co teď?

- Symetrické šifry ohroženy nejsou.
- Potřeba **nahradit asymetrické** systémy.
  - podpisy (certifikáty)
  - zřízení společného klíče
- RSA a DHE jsou založeny na těžkých matematických problémech.
- Je potřeba **najít způsoby jak využít jiné problémy**.

Post-kvantové algoritmy

- Adopce post-kvantových šifer je pomalá.
  - časově i paměťově náročnější na výpočet
  - **míň prověřené matematické základy**
- V TLS1.3 se v současné době používá **hybridní přístup**.
  - Používají se klasické i PQC algoritmy.
  - K dešifrování komunikace je potřeba prolomit oba.
- Od roku 2016 běží soutěž od NISTu, ke standardizování nových post-kvantových algoritmů.
  - Celkem vybráno 5 algoritmů.
  - 3 už jsou standardizovány.

Post-kvantové algoritmy vybrané NISTem

- **Kyber** (ML-KEM)
  - Module-Lattice based Key Encapsulation Mechanism
- **Dilithium** (ML-DSA)
  - Module-Lattice based Digital Signature Algorithm
- **SPHINCS$^+$** (SLH-DSA)
  - Stateless Hash-Based Digital Signature Algorithm
- **Falcon** (FN-DSA)
  - Fast Fourier lattice-based compact signatures over NTRU
- **HQC**
  - Code-based public key encryption scheme

V závorkách jsou standardizovaná jména.

Porovnání ML-KEM vs. X25519

		Velikost klíče (v bytech)		Počet operací/s	
Algoritmus	**PQ?**	**Klient**	**Server**	**Klient**	**Server**
ML-KEM-512	Ano	800	768	45,000	70,000
ML-KEM-768	Ano	1,184	1,088	29,000	45,000
ML-KEM-1024	Ano	1,568	1,568	20,000	30,000
X25519	Ne	32	32	19,000	19,000

Zdroj dat: `https://blog.cloudflare.com/pq-2024/`

Porovnání velikostí post-kvantových podpisů

			Velikost (v bytech)		Čas na CPU	
		PQ?	**VK**	**Podpis**	**Podpis**	**Ověření**
Standard	**Ed25519**	Ne	32	64	1	1
	RSA-2048	Ne	256	256	70	0.3
Vybrány	**ML-DSA-44**	Ano	1,312	2,420	4.8	0.5
	FN-DSA-512	Ano	897	666	8	0.5
	SLH-DSA-128s	Ano	32	**7,856**	**8,000**	2.8
	SLH-DSA-128f	Ano	32	**17,088**	550	7
Stále v soutěži	**MAYO$_{\text{one}}$**	Ano	1,168	321	4.7	0.3
	MAYO$_{\text{two}}$	Ano	**5,488**	180	5	0.2
	SQISign I	Ano	64	177	**60,000**	**500**
	UOV Is-pkc	Ano	**66,576**	96	2.5	2
	HAWK512	Ano	1,024	555	2	1

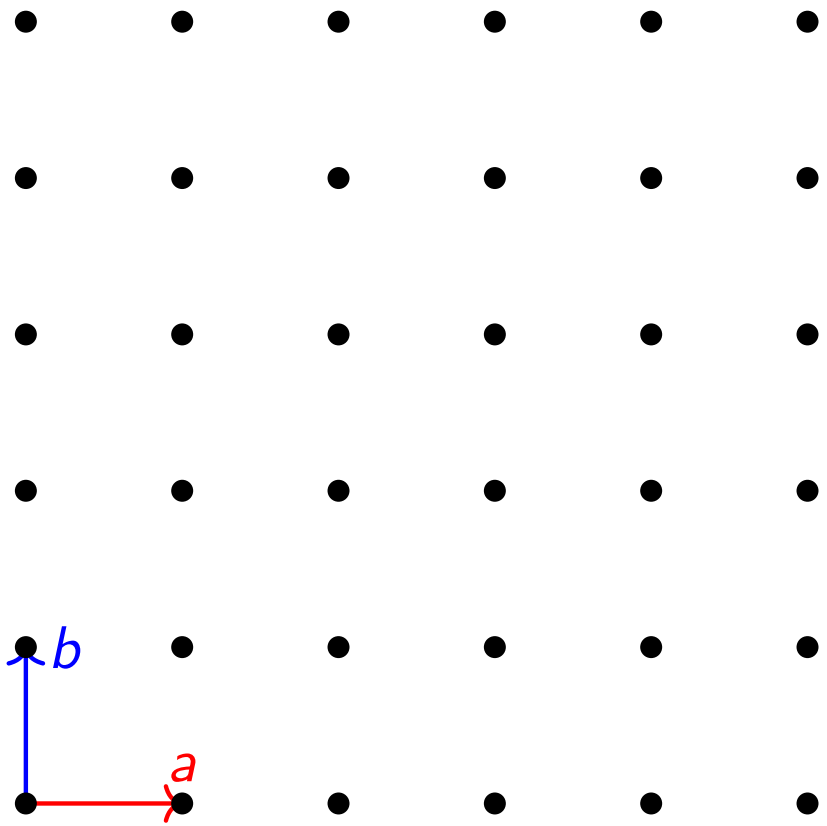
Zdroj dat: `https://blog.cloudflare.com/pq-2024/`

Aktuální stav v prohlížečích

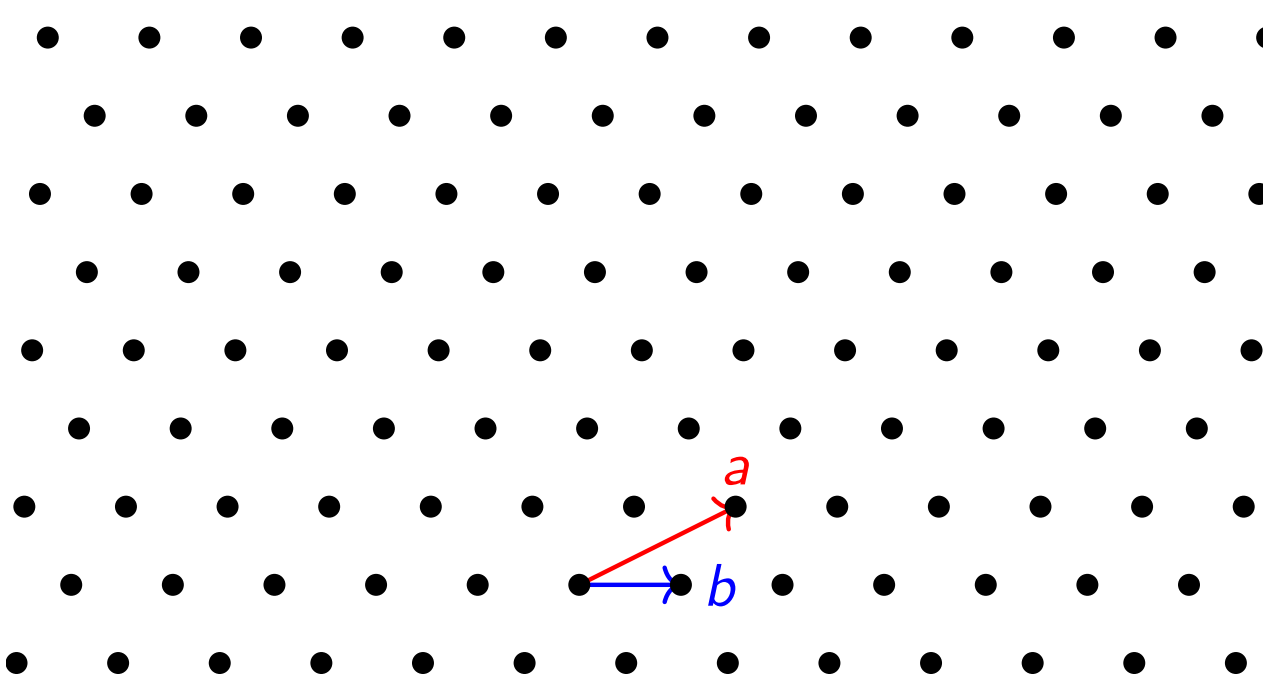
- Firefox a Chrome podporují **hybridní klíče**[2].
- Je potřeba je ale explicitně zapnout.
  - Viz například `https://www.netmeister.org/blog/pqc-2025-02.html`.
- Na stránce `https://pq.cloudflareresearch.com` se dá ověřit, zda vám hybridní klíče fungují.

[2] post-kvantový + klasický

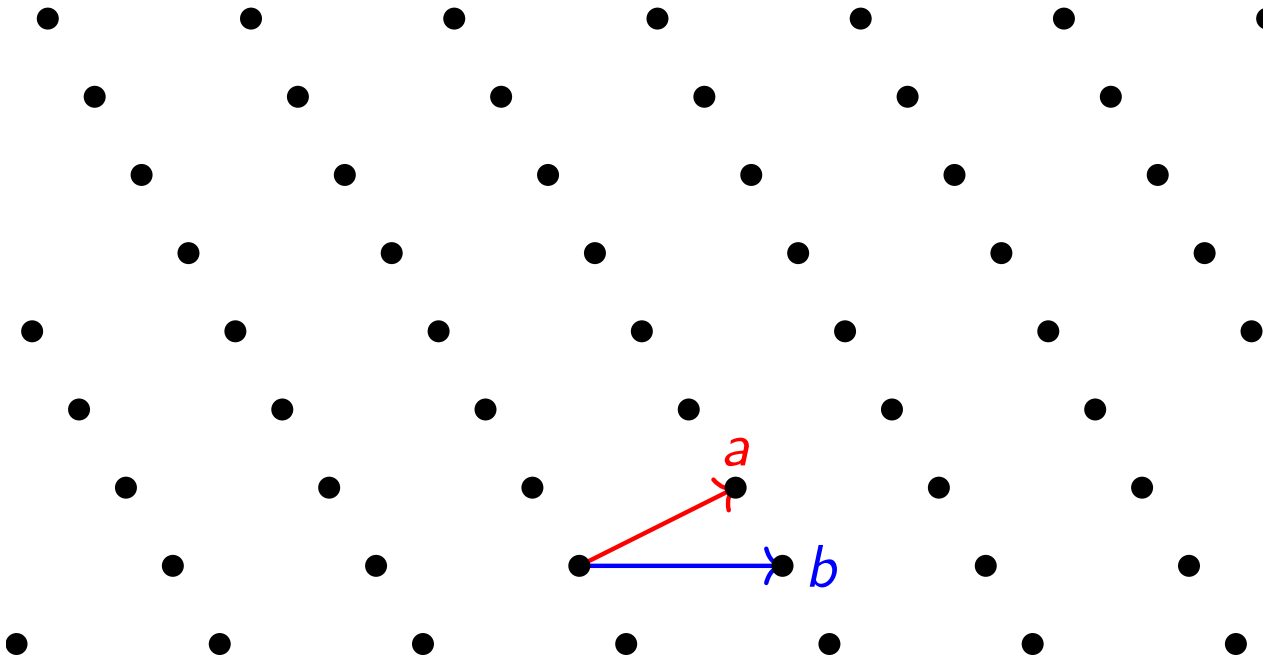
Kryptografie na mřížce



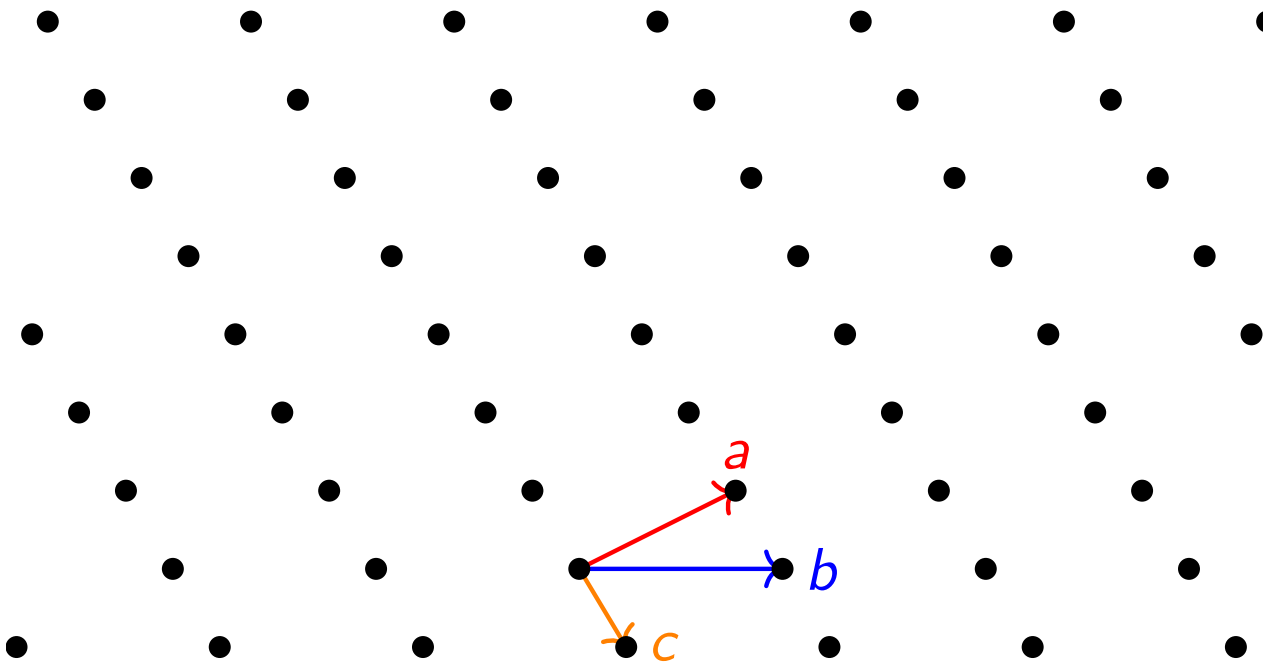
Kryptografie na mřížce



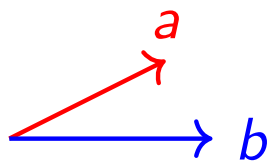
Shortest vector problem



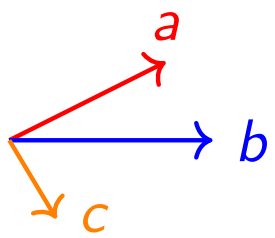
Shortest vector problem



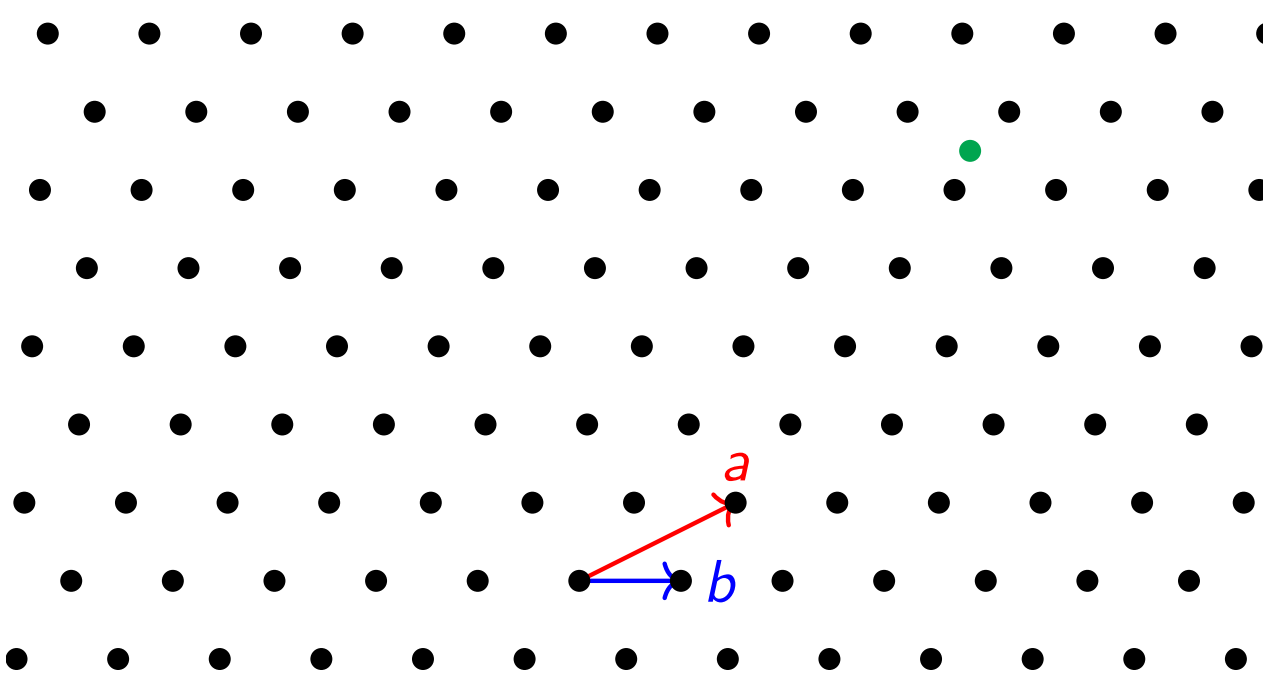
Shortest vector problem



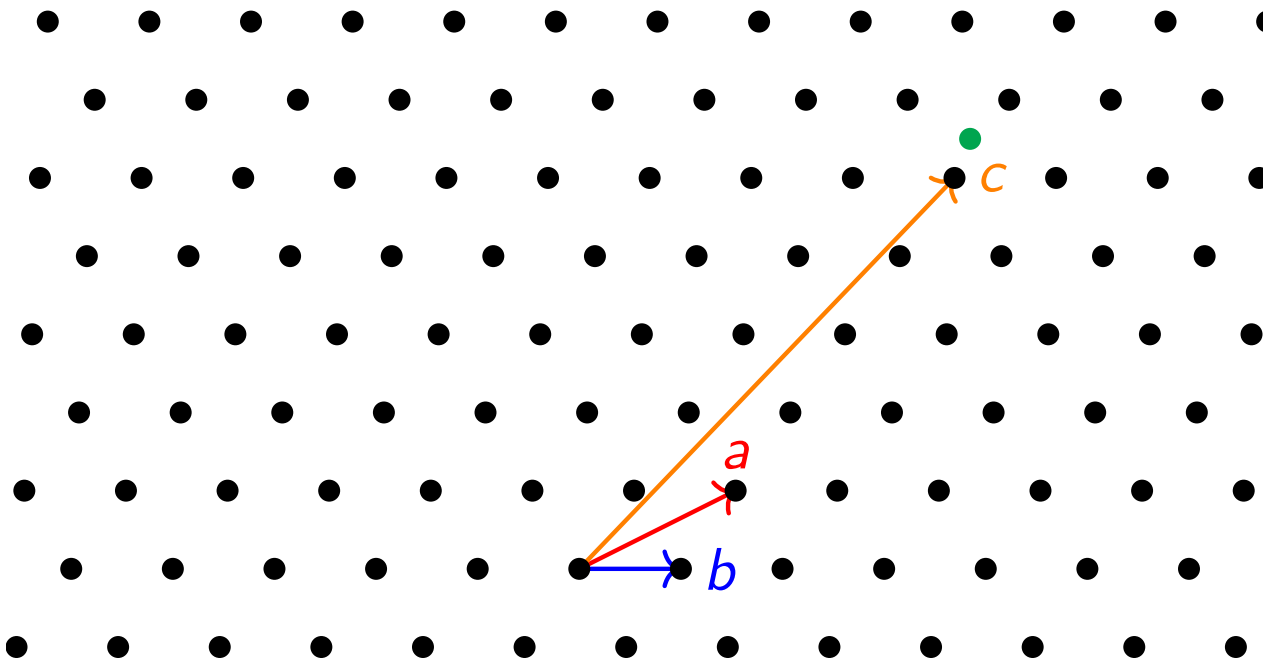
Shortest vector problem



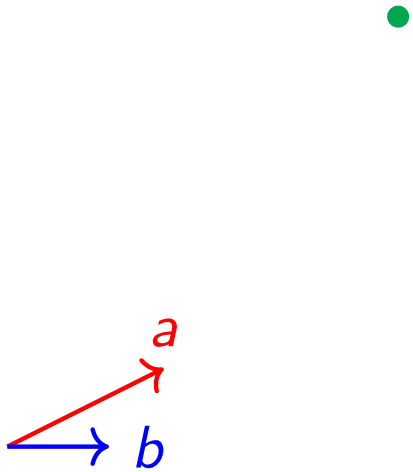
Closest vector problem



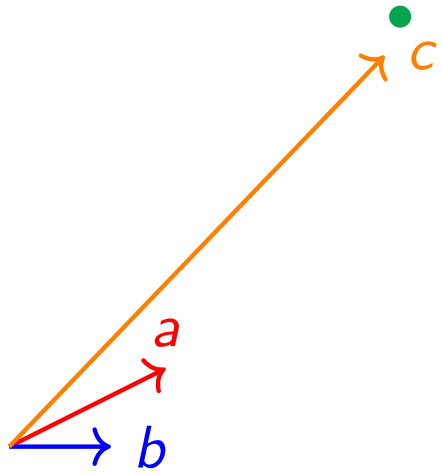
Closest vector problem



Closest vector problem



Closest vector problem



Hlavní body

Kvantová kryptografie

- Využívá principy kvantové mechaniky v kryptografii.
- **Kvantová distribuce klíče**
  - **protokol BB84**
  - Lze se dohodnout na sdíleném klíči s možností detekce odposlechu.
  - Vyžaduje speciální zařízení.
- OpenQKD – Testování kvantové distribuce klíče v Evropě.
  - Několik stanic rozmístěných po Evropě.
  - Jedna je v Ostravě