Postkvantová kryptografie

Úvod a současný stav

prof. Ing. Jan Hajný, Ph.D.

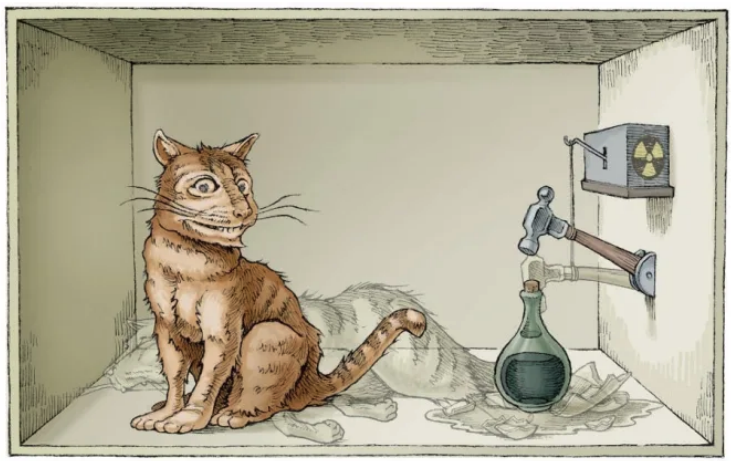
Vysoké učení technické v Brně
hajny@vut.cz
https://axe.vut.cz

Funded by the European Union

Kvantové počítání - základní principy

Kvantová mechanika:

- vlastnosti nelze měřit bez jejich ovlivnění,
- objekty (částice) mohou být v tzv. superpozici, tj. kombinaci více stavů najednou (Schrödinger),
- kvantová mechanika má nedeterministický charakter - důležitou roli hraje pravděpodobnost.



Obrázek: Schrödingerova kočka.

Kvantové počítání - základní principy

Počítání s qubity:

- superpozice se využívá pro počítání s qubity - základními jednotkami, které jsou 0 i 1 najednou,
- qubity umožňují masivní "paralelizaci" výpočtu a tedy zrychlení pro některé operace,
- v současnosti jsou nejčastěji využívány supravodivé qubity[1],
- existují i jiné přístupy: zachycené ionty, kvantové tečky, či fotony,
- existují i další principy, jako quantum annealing[2].

[1] https://medium.com/qiskit/how-the-first-superconducting-qubit-changed-quantum-computing-forever-

[2] https://www.dwavesys.com

Kvantové počítání - Aktuální stav

IBM[3]:

- 2023: IBM Eagle: 127 qubitů,
- 2024: IBM Heron: 133 (399) qubitů, oprava chyb,
- 2025: IBM Flamingo: 156 (1092) qubitů, oprava chyb.

Google:

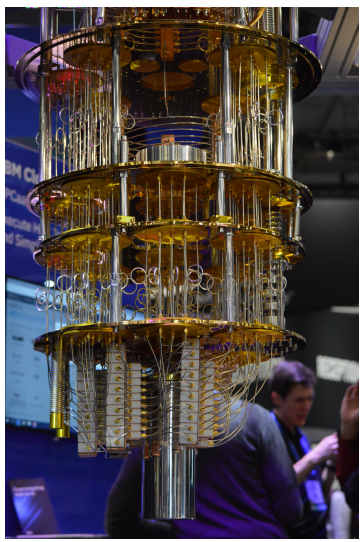
- 2019: Sycamore: 53 qubitů,
- 2024: $5 mil. výzva pro praktické využití.

Microsoft:

- 2025: Majorana: 8 "topologických"qubitů.

Anhui Research Center (China):

- 2024: Origin Wukong: 72 qubitů,
- byl k dispozici online.



Obrázek: Kvantový počítač IBM Q System One.

Kvantové počítání - Bezpečnostní hrozba

Shorův algoritmus

- kvantový algoritmus publikovaný v roce 1994,
- může být využit pro efektivní faktorizaci, tj. nalezení p, q pro $n = pq$, a pro výpočet diskrétních logaritmů $x = dlog_g c$,
- může běžet v polynomiálním čase, tj. $\log(n)$,
- pro svůj běh potřebuje "plný" kvantový počítač.

Kvantové počítání - Bezpečnostní hrozba

Groverův algoritmus

- kvantový algoritmus objevený v roce 1996,
- je určený pro rychlé nestrukturované hledání, tj. např. hledání vstupy nespecifikované funkce pro známý výstup,
- složitost výpočtu je $\sqrt{(n)}$, kde n je velikost definičního oboru.
- algoritmus tedy poskytuje kvadratické zrychlení.

Kvantové počítání - Bezpečnostní hrozba

Asymetrická kryptografie

- protokoly pro ustanovení klíčů: (EC)**DH** založeno na složitosti problému diskrétního logaritmu,
- digitální podpisy: RSA, (EC)**DSA** založeno na složitosti problému faktorizace a diskrétního logaritmu,
- šifrování: **ElGamal** založeno na složitosti problému diskrétního logaritmu.

Symetrická kryptografie

- blokové symetrické šifry založeny na složitosti hledání klíče.

Prokazatelná kryptografie

- Σ-protokoly pro důkazy s nulovou znalostí: založeno na složitosti problému diskrétního logaritmu,
- ...

Kvantové počítání - Bezpečnostní hrozba

Zhodnocení: Asymetrická kryptografie

- Zcela zranitelná zejména Shorovým algoritmem.
- Doporučení: přechod na postkvantovou kryptografii.

Symetrická kryptografie

- Částečně zranitelná zejména Groverovým algoritmem.
- Doporučení: použití minimálně 256b klíčů pro 128b úroveň bezpečnosti.

Prokazatelná kryptografie

- Zcela zranitelná zejména Shorovým algoritmem.
- Doporučení: Ve výzkumu.

Legislativa, doporučení autorit

"Důsledkem kvantové zranitelnosti schváleného algoritmu je nutné ho v nepříliš vzdáleném časovém horizontu nahradit vhodnou kvantově odolnou kryptografií." NÚKIB

National Authorities

- NUKIB (ČR): Minimum Requirements for Cr. Algorithms
- NSA (USA): Commercial National Security Algorithm Suite 2.0
- BSI (Německo): Quantum-safe cryptography – fundamentals, current developments and recommendations

Evropská komise

- EU: Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

Standardizace

- NIST: Post-Quantum Cryptography Standardization

Řešení

Řešení kvantových hrozeb

Řešení 1: Kvantová kryptografie

Kvantová kryptografie: Kvantová distribuce klíčů (Quantum Key Distribution)

- známá od 80. let, založená na kvantové fyzice,
- není založena na předpokladech složitosti matematických problémů, bezpodmínečně bezpečná (teoreticky),
- existující řešení: Toshiba, ID Quantique, . . . ,
- nasazováno v rámci různých projektů: EuroQCI, CZ-QCI, ...

Nedostatky: velmi drahé (zhruba 6 mil. Kč za spojení), neověřená bezpečnost implementace, použitelné pouze pro klíčovou expanzi, není doporučeno autoritami jako úplné řešení[4], složitá integrace s existujícími ICT prvky, nedostatečná standardizace, podpora, zkušenosti, . . .

[4] Position Paper on Quantum Key Distribution

Řešení 1: Kvantová kryptografie

Kvantová kryptografie: Kvantová distribuce klíčů (Quantum Key Distribution)

Základní princip:

- přenáší se qubity po optickém vlákně či ve volném prostoru,
- qubity nejčastěji ve formě fotonů či jejich shluků,
- měří se např. polarizace fotonů - protokol BB84,
- z kvantové mechaniky vyplývá neměřitelnost bez ovlivnění,
- ovlivnění lze detekovat, tedy jakákoliv interakce (měření) úročníkem lze detekovat,
- zároveň se využívá nedeteterministická povaha částic, např. pro náhodné generování čísel: Quantum Random Number Generators (QRNG).

Řešení 1: Kvantová kryptografie

Kvantová kryptografie: Kvantová distribuce klíčů

Obrázek: Zařízení pro kvantové ustanovení klíčů v laboratoři VUT v Brně.

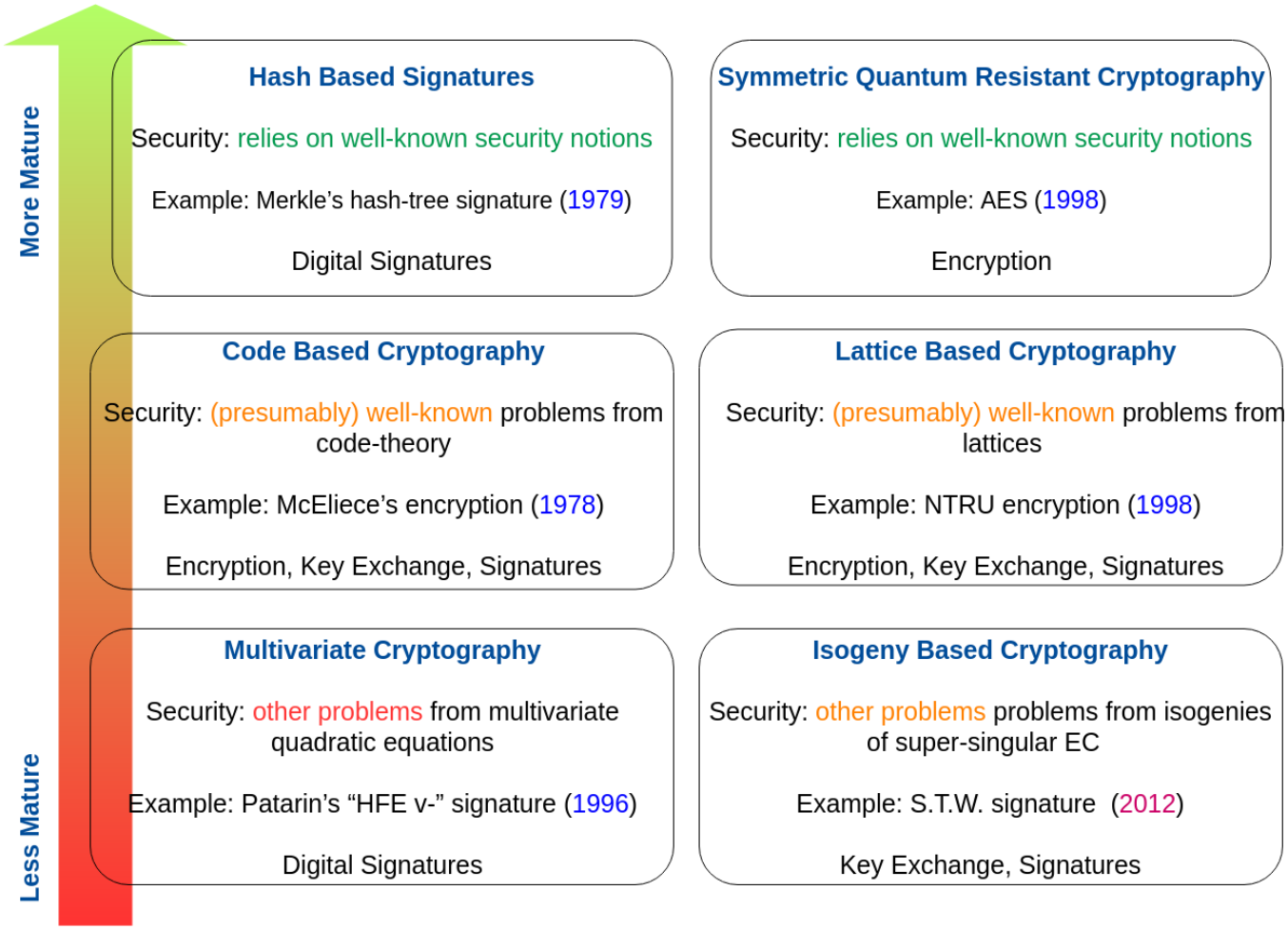
Řešení 2: Postkvantová kryptografie (PQC)

Postkvantová kryptografie

- *snadná* integrace s existující ICT infrastrukturou, není třeba speciální HW, levné,
- existující softwarové implementace: Open Quantum Safe, . . . ,
- podporováno národními autoritami: UK, US, Německo, Francie, Švédsko, Holandsko, . . . ,
- hotové standardy k dispozici: CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON (mřížky) and SPHINCS+ (hash)

Problémy: stále založeno na složitosti matematických problémů; náročnější, než klasická kryptografie.

Přehled vyspělosti rodin PQC



Obrázek: Rodiny PQC.

Řešení 3: Hybridní kryptografie

Hybridní kryptografie

- kombinuje odlišné přístupy: QKD, PQC a klasickou kryptografii,
- cílem je zasjistit bezpečnost i v případech, kdy některý přístup selže,
- doporučeno některými autoritami: BSI, ANSSI, . . . , ale původně nikoliv NSA,
- vhodné alespoň pro přechodné období,
- možnost kombinovat i různé PQC rodiny.

Kryptografická agilita

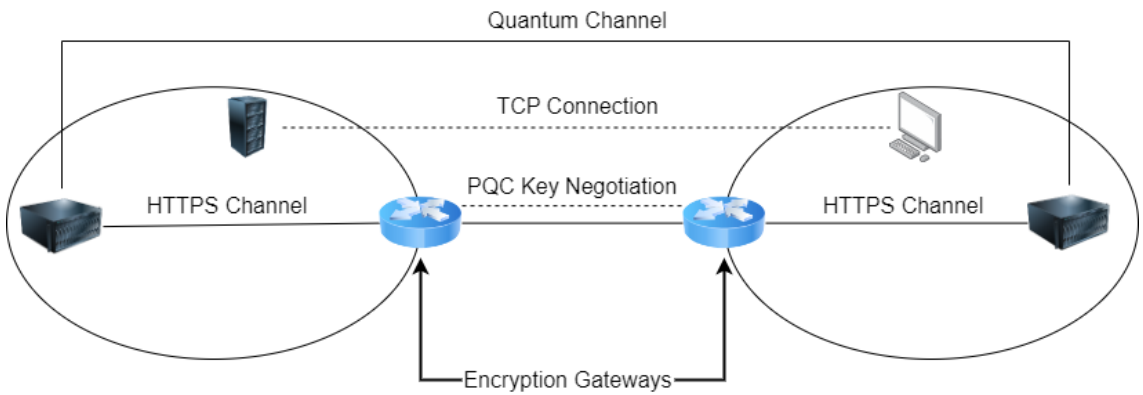
- přístup umožňující snadné změny parametrů a šifer.

Problémy: pomalejší, náročnější na paměť, více prostoru pro chyby.

Open-Source Šifrátor

Výstup projektu CHESS: Open-Source šifrátor

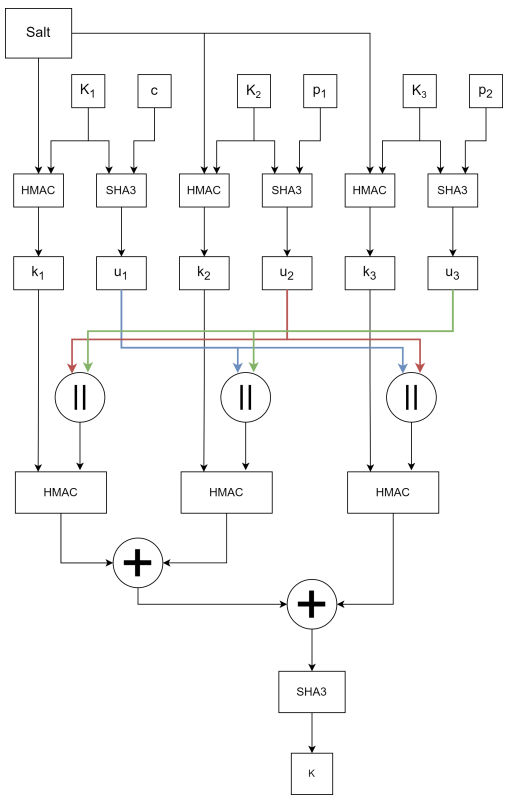
- jednoduchá open-source implementace pro bezpečnou VPN,
- založeno na Linux OS, kombinuje ECDH, PQC - CRYSTALS-Kyber,
- volitelně je možno využít QKD, např. IDQ Clavis,
- testováno mezi Brnem a Estonskem, vyvíjeno na VUT,
- otevřeno pro spolupráci: https://github.com/gabsssq/Linux-network-traffic-encryptor



Open-Source Šifrátor

Výstup projektu CHESS: Open-Source šifrátor

- Klasická kryptografie: ECDH-512,
- Kvantová kryptografie: IDQ Clavis 3,
- Postkvantová kryptografie:
  - CRYSTALS-Kyber 768,
- Šifrování: AES-256-GCM,
- Kombinace klíčů: vlastní[5].



[5]S. Ricci et Al, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography," in IEEE Access, vol. 12, 2024.

Mezinárodní projekty

Open-Quantum Safe

- knihovna v C: liboqs stěmito algoritmy:
  - BIKE, Classic McEliece, CROSS, Dilithium, Falcon, FrodoKEM, HQC, Kyber, LMS, MAYO, ML-DSA, ML-KEM, NTRU-Prime, SPHINCS+, XMSS,
- testovací implementace známých protokolů a integrace s OpenSSL:
  - TLS, SSH, X.509, S/MIME, ...
- dostupné zde: `https://openquantumsafe.org`

Závěr a otázky k zamyšlení

Jednoduché závěry:

- Přechod na kvantově odolnou kryptografii je nutnost z důvodu možnosti útoků *store and decrypt later*.
- PQC je mnohem blíže praktickému nasazení než QKD.
- Konkrétní algoritmy a doporučení autorit jsou již k dispozici.
- Integrace s existující infrastrukturou a službami je větší problém než samotná kryptografie.
- Kryptografická agilita je nutnost.

Provokativní otázky:

- Bude vůbec někdy použitelný kvantový počítač sestaven?
- Jsou současné kvantové počítače hrozbou pro IT?
- Jsou současné PQC algoritmy skutečně bezpečné[6]?

[6] Yilei Chen, *Quantum Algorithms for Lattice Problems*, https://eprint.iacr.org/2024/555

Děkuji za pozornost.

The workshop is supported by the NCC-CZ, project entitled „Development of Capacities and Support of Collaboration in Post-Quantum Cryptography (DeCaPoQ). Research work is funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.