A poszt-kvantum korszak kihívásai

Orosz Nándor
Projekt- és szolgáltatásigazgató

RelNet technológia

Alapfogalmak

KVANTUM-APOKALIPSZIS

Annak az időszaknak a kezdet.e, amikortól a hagyományos titkosítások kvantumszámítógépekkel reális időn belül törhetőkké válnak.

POSZT-KVANTUM KRIPTOGRÁFIA

Olyan titkosító algoritmusok használata, amelyek a matematikusok szerint védettek a kvantumszámítógéppel történő törés ellen.

KVANTUMBIT (QUBIT)

A kvantumszámítógép egy bitje, ami nem csak 0 vagy 1 állapotot vehet fel, hanem ezen belül eloszlást követ.

Alapfogalmak

KVANTUM-ÖSSZEFONÓDÁS

Két részecske (leggyakrabban foton) kvantum szintű tulajdonságai szinkronizálásra kerülnek, szuperszimmetrikus módon. Innen (az összefonódás megszűnéséig) a paramétereik valós időben együtt változnak.

"HAGYOMÁNYOS" DETEKTOR

Egyetlen foton detektálására alkalmas detektor, a félbeszakított fotonpár optikai szálon továbbított tagját fogadja. **Tipikus áthidalható távolság 70-85km**.

SZUPRAVEZETŐ FOTONDETEKTOR

Olyan fotondetektor, ami szupravezető hőmérséklet-tartományban dolgozik, emiatt zajvédettebb, így az **áthidalható távolság 300-400km-re növekszik**

Mi ez a hype? Valós fenyegetés?
És ha igen, mikor? 2024? 2025? 2030?

Mi ez a hype?

Az asszimmetrikus kulccserét **Shor algoritmusa** sebezhetővé teszi, ha kellően fejlett kvantumszámítógépünk van.

A publikus kulcsból prím faktorizálással (RSA) lehet a privát kulcsot visszafejteni (ez a mai számítógépekkel nehéz, hosszadalmas folyamat).

A kvantumszámítógépek gyorsan képesek prím faktorizációt végezni.

Mi ez a hype?

Egy 4000 qubittel rendelkező kvantumszámítógép elméletileg sikeresen törheti az RSA-2048 titkosítást – másodpercek alatt.

		Size (bytes)	
Algorithm	PQ	**Public key**	**Ciphertext**
Kyber512	✅	800	768
RSA-2048	❌	256	256

Mi ez a hype?

Az IBM roadmap nyilvános:

2024	2025	2026	2027	2029	2033+
Expand the utility of quantum computing.	**Demonstrate quantum-centric supercomputing.**	**Automate and increase the depth of quantum circuits.**	**Scale quantum computing.**	**Deliver a fully error-corrected system.**	**Deliver quantum-centric supercomputers with 1,000's of logical qubits.**
We will improve the quality and speed of quantum circuits to allow running 5,000 gates with parametric circuits.	In 2025, we will demonstrate the first quantum-centric supercomputer by integrating modular processors, middleware, and quantum communication. We will also enhance the quality, execution, speed, and parallelization of quantum circuits.	We will enable quantum circuits with 7,500 gates through circuit quality improvement.	We will scale qubits, electronics, infrastructure, and software to reduce footprint, cost, and energy usage. The quality of quantum circuits will improve to allow running 10,000 gates.	We will bring users a quantum system with 200 qubits capable of running 100 million gates.	Beyond 2033, quantum-centric supercomputers will include thousands of qubits capable of running 1 billion gates, unlocking the full power of quantum computing.

Quantum Annealing

Jelenleg a D-Wave Advantage2 már 7000+ (más típusú topológia, un. quantum annealing, kvantum völgybejárás) kvantumbittel rendelkezik. Sokkal zajtűrőbb, mint a hagyományos qubitek.

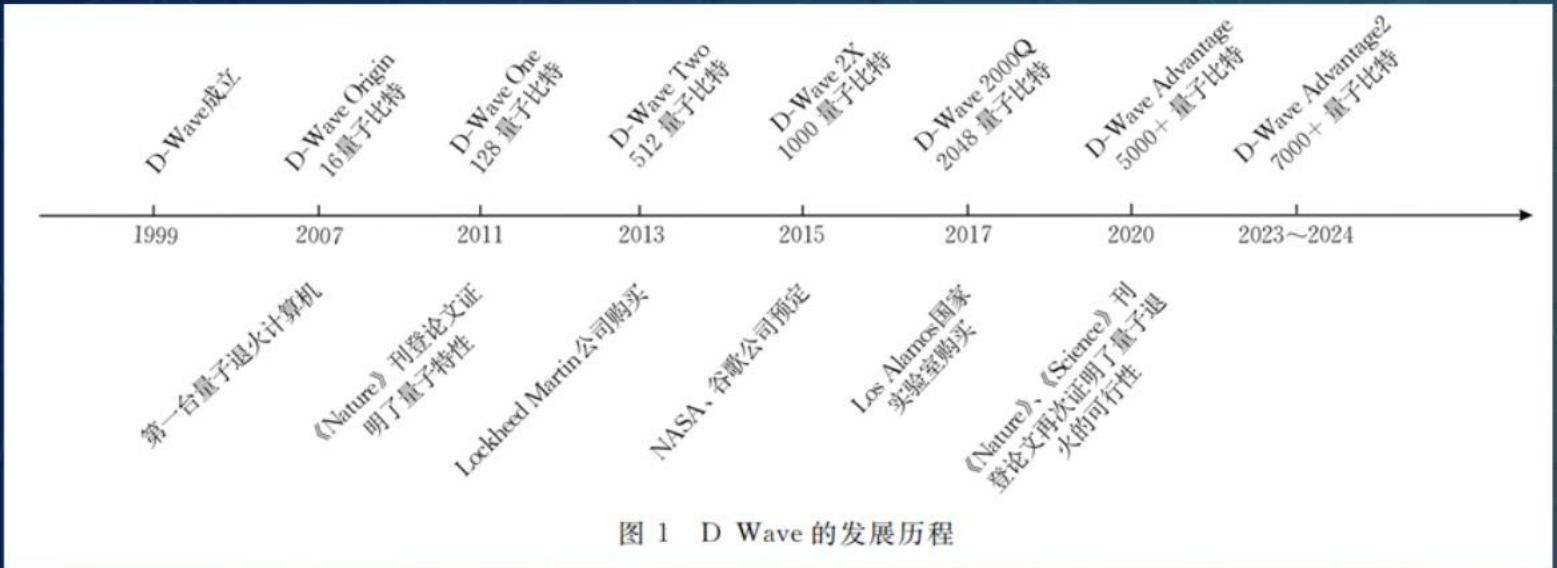


图 1　D Wave 的发展历程

Ezen típusú kvantumszámítógép esetén 10’000 stabil, hibajavított qubittel törhetővé válnak a 2048 bites RSA kulcsok. Ez azért fájó, mert ezen típusú kvantumszámítógépre korábban azt mondták egyes szakértők, hogy nem lehet rajta kódtörő algoritmust futtatni, mert más a topológiája.

Már megtörtént, valószínűsíthető kvantum-törések:

KÍNAI KUTATÓK

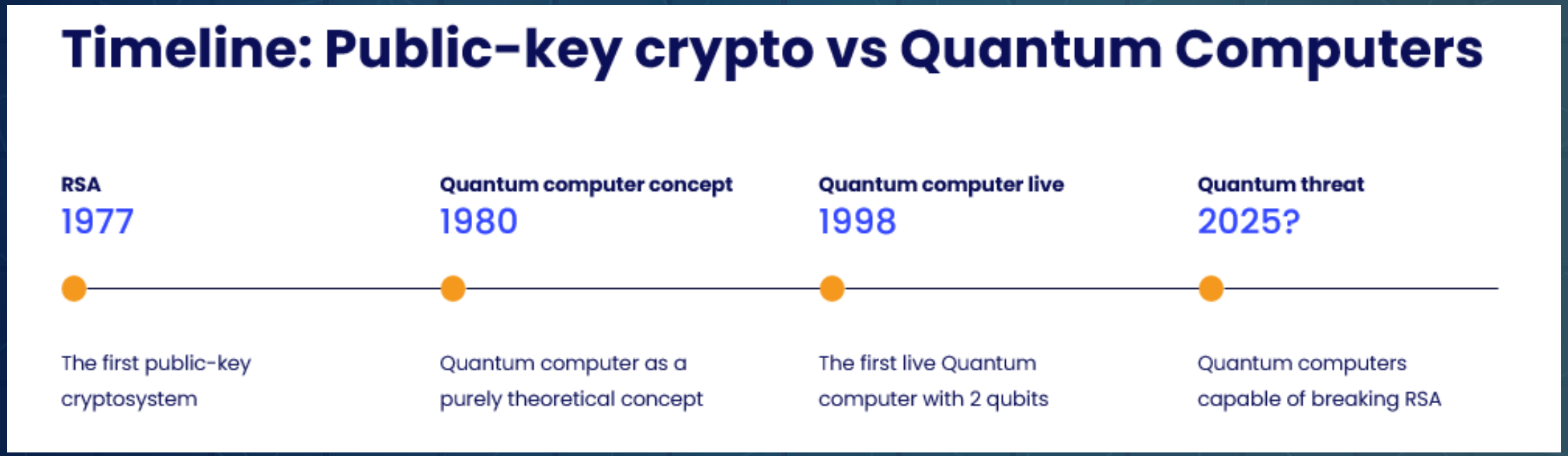
Laborban sikeres RSA törés 22bites titkosításon D-Wave Advantage2 géppel

OLASZORSZÁG

Egy benzinkút hálózat OT WAN kapcsolatait törték fel

Nem valós rendelésekkel több millió EUR kár

Már megtörtént, valószínűsíthető kvantum-törések:



Bizonyos tekintetben a poszt-kvantum korszak hajnala 2024 októberében elkezdődött.

Kik futják a kockázatot?

- titkos ügyirat kezelők, nemzetvédelem
- személyes adatokat kezelő szervezetek
- beszerzés, tenderezés
- OT – ipari rendszerek (rövid és gyakran fixre beégetett kulcsok)
- bitcoin és altcoinok
- pénzügyi szektor
- MSP-k, akik ügyfelek rendszereit menedzselik
- VPN-ek (IPSEC és SSL)

Kockázatok kezelése /1

HAGYOMÁNYOS TITKOSÍTÁSÚ RENDSZEREKBEN

1

Hosszabb (minimum 4096 bit) hosszú kulcsok használata

Elliptikus Görbék (ECC) esetén:

- ECC 256bit = RSA3072
- ECC 512bit = RSA15360

tisztán szakértői munkával is megvalósítható

2

Kulcs életciklus lerövidítése, gyakoribb kulcs-csere

3

Fel kell tárni az állandóra letett (pre-shared) kulcsok használatát (különösen OT rendszerekben) és becsatornázni valamilyen rendszeresen frissülő kulcsos (pl. PAM) megoldásba

Kockázatok kezelése /2

POSZT-KVANTUM KRIPTOGRÁFIA

1. Olyan titkosító algoritmusok használata, amelyek a matematikusok szerint védettek a kvantumszámítógéppel történő törés ellen

négy befutó: Kyber, Dilithium, FALCON, SPHINCS+

2. A NIST szabványügyi testület meghirdetett egy PQC „versenyt”

3. A jövőben fog kiderülni, tényleg törésállóak-e ezen algoritmusok

Kockázatok kezelése /2

POSZT-KVANTUM KRIPTOGRÁFIA

GYAKORLATI MEGVALÓSÍTÁS

SSH NQX

Definíció alapján kvantum-törésálló algoritmusok használata

- Nem szükséges hozzá kvantum-számítógép
- Két rétegű titkosítás, belül egy korszerű hagyományos, de 8192 bit hosszú kulcsos titkosítás, majd azon felüli rétegben a Kyber titkosítás
- **Előny:** olcsóbb, mint a QKD megoldás, DWDM nélkül is működik (ethernet, wifi, 5G)
- **van ilyen teszteszközünk a RelNetben, kérésre oda tudjuk adni tesztelésre**

Kockázatok kezelése /3

KVANTUM ALAPÚ KULCSELOSZTÁS

QKD

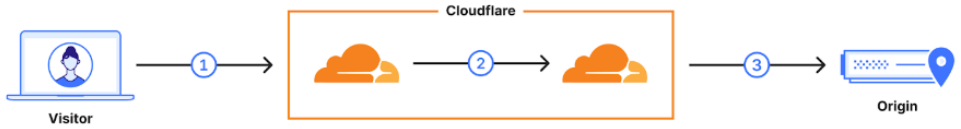
Definíció alapján nem lehallgatható

- Nem kvantum kulcsot oszt el, hanem hagyományosat
- Nem kell hozzá kvantumszámítógép
- Maga a csatorna kvantum szintű, MITM támadás ellen védett
- Meglévő DWDM optikai hálózaton képes működni

Három nagy QKD gyártóval van a RelNet partnerségben és egy DWDM gyártóval (PacketLight).

PQC teszt a saját böngészőben

Cloudflare Research: Post-Quantum Key Agreement



On essentially all domains served (1) through Cloudflare, including this one, we have enabled hybrid post-quantum key agreement. We are also rolling out support for post-quantum key agreement for connection from Cloudflare to origins (3). Check out our blog post the state of the post-quantum Internet for more context.

You are using *X25519Kyber768Draft00* which is **post-quantum secure**.

Deployed key agreements

Available with TLSv1.3 including HTTP/3 (QUIC)

Key agreement	TLS identifier
X25519MLKEM768	`0x11ec` (recommended)
X25519Kyber768Draft00	`0x6399` (obsolete), `0xfe31`
~~X25519Kyber512Draft00~~	`0xfe30`

You are using *X25519* which is **not post-quantum secure**.

Deployed key agreements

Available with TLSv1.3 including HTTP/3 (QUIC)

Key agreement	TLS identifier
X25519MLKEM768	`0x11ec` (recommended)
X25519Kyber768Draft00	`0x6399` (obsolete), `0xfe31`
~~X25519Kyber512Draft00~~	`0xfe30`

Szabályzói előírások, amikből a kvantum-titkosítás igény kiolvasható:

- 2020/18 EU JOUN rendelet (kiberbiztonsági stratégia)
- 2023/20 EU JOIN rendelet (kvantumtechnológiákra vonatkozó kockázatértékelés azonosított kockázatai)
- 2024/2393 EU ajánlás (posztkvantum kriptográfiára való átállás) – ld. linkgyűjtemény
- 2022/2555 EU irányelv (NIS 2) - + 2025 év eleji hazai Kibervédelmi törvény
- 2022/2554 EU rendelet (DORA)

Elvihető üzenetek

... de nem vagyunk védtelenek!

Kérdések?

Hivatkozások, források /1

Cloudflare PQC böngésző teszt: https://pq.cloudflareresearch.com

A kvantumszámítógépek működése, gyakorlati felhasználása és jövője (Asbóth János): https://www.youtube.com/watch?v=fLNtLPKf40s

ELTE Atomcsill – Youtube videokönyvtár: https://www.youtube.com/@elteatomcsill8013

Széchenyi Gábor: Kvantumszámítógép — a munkára fogott kvantummechanika (Atomcsill, 2019.04.25.): https://www.youtube.com/watch?v=Or9HFo-8qyI

EU ajánlás a PQC átállásról: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=OJ:L_202401101

Hivatkozások, források /2

NIST véglegesített szabványok:

https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

(Kyber át lett nevezve ML-KEM -re)

Kvantum számítógép státusz (2024 áprilisi állapot):

https://csrc.nist.gov/csrc/media/Projects/post-quantum-cryptography/documents/pqc-seminars/presentations/14-quantum-computers-06042024.pdf

Ugyanez a prezi videóban:

https://www.nist.gov/video/quantum-computers-state-development-cryptoanalysis

Köszönöm megtisztelő figyelmüket!

Ezen felül szeretnék köszönetet mondani

Az SSH és PacketLight gyártók szakértőinek a belső (gyakran még kutatási fázisban lévő) anyagaikba nyújtott betekintésért,

Kőrössi Ádám, Csongrádi Eszter és Poór Gergő kollégáimnak a szakmai véleményezésért,

Veréb Stellának a prezi képi világának kialakításáért.