QCIHungary projekt feladatai és az európai EuroQCI együttműködés

János Mohácsi, Nemzetközi K+F vezető, GÉANT igazgató

QCIHungary koordinátor

KIFÜ

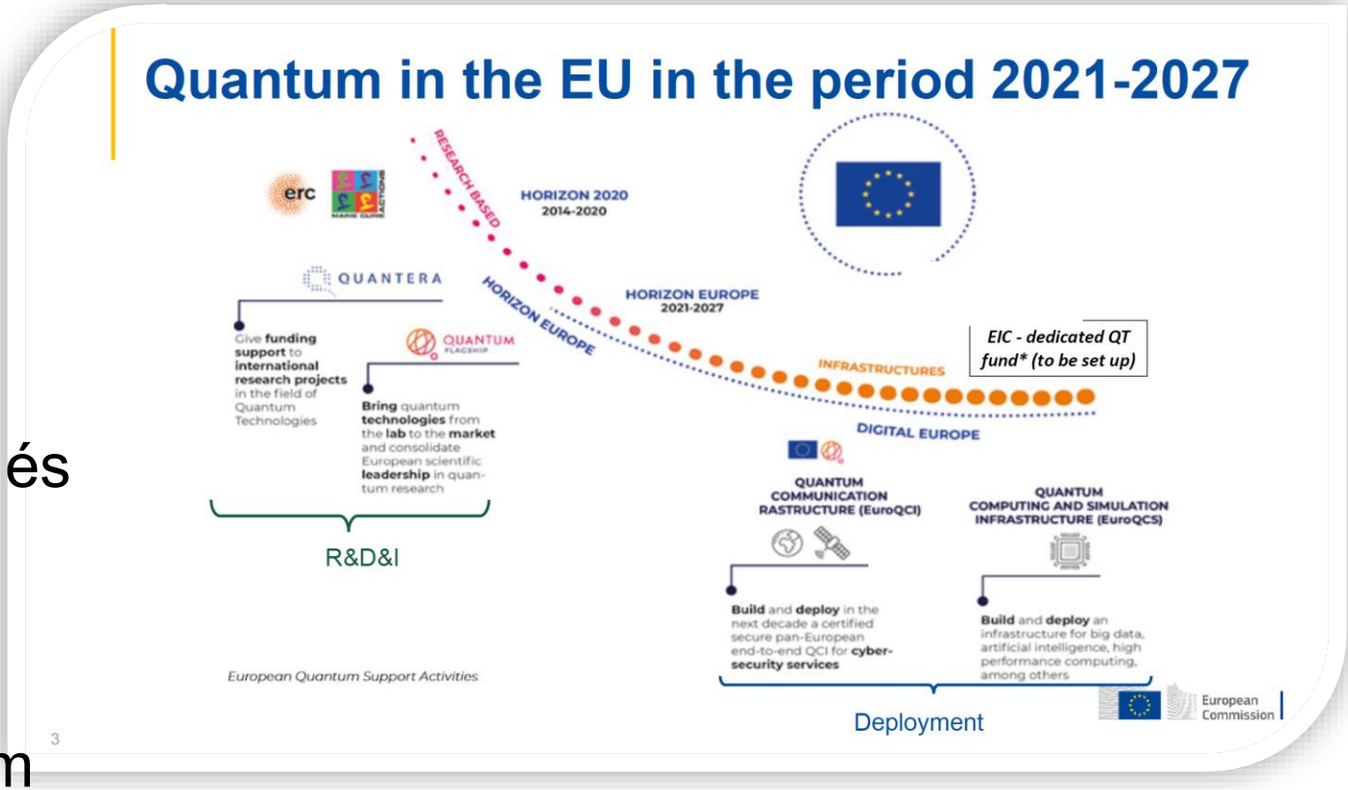
HUNOG 2024

Áttekintés

- Kvantum technológia és európai kezdeményezések
- QCIHungary – a magyar hozzájárulás az európai kvantum kommunikációs kezdeményezésekhez
- QKD és PQC
- Összefoglaló

Kvantum az EU-ban: ökösziszténák létrehozása

- Kvantuninformatika - kvantummechanika által leírt hatások manipulálása és kihasználása.
- 2. kvantumforradalom
- Quantum Manifesto EU 2016-ban - kvantuminformatika fontossága Európa számára, és ütemtervet készít a kutatási és valós alkalmazásokhoz.
- A jövőbeni programok
- Számos program és kezdeményezés az EU részéről: Quantum Flagship, Quantum Internet Alliance, egyes ESA tevékenységek, Európai Kvantumkommunikációs Infrastruktúra (EuroQCI) és (EuroQCSI) kezdeményezés

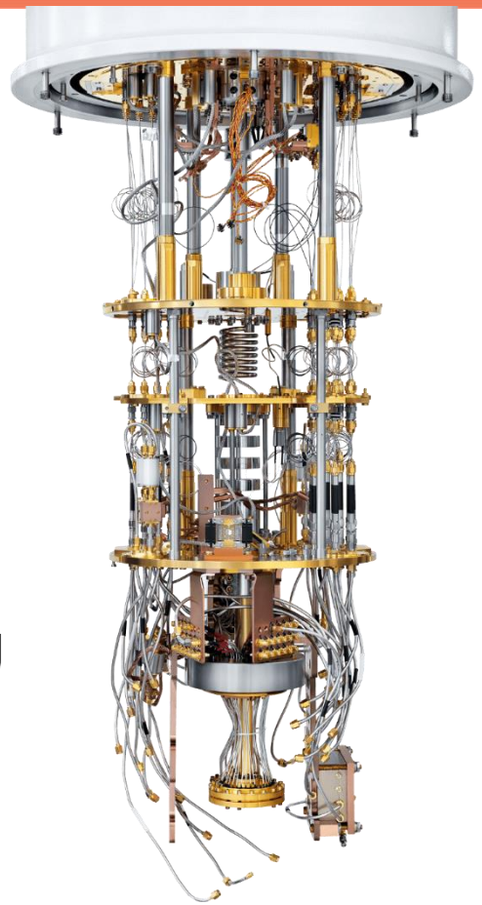


Quantum Computers

Két* algoritmus veszélyezteti a hagyományos kriptográfiát

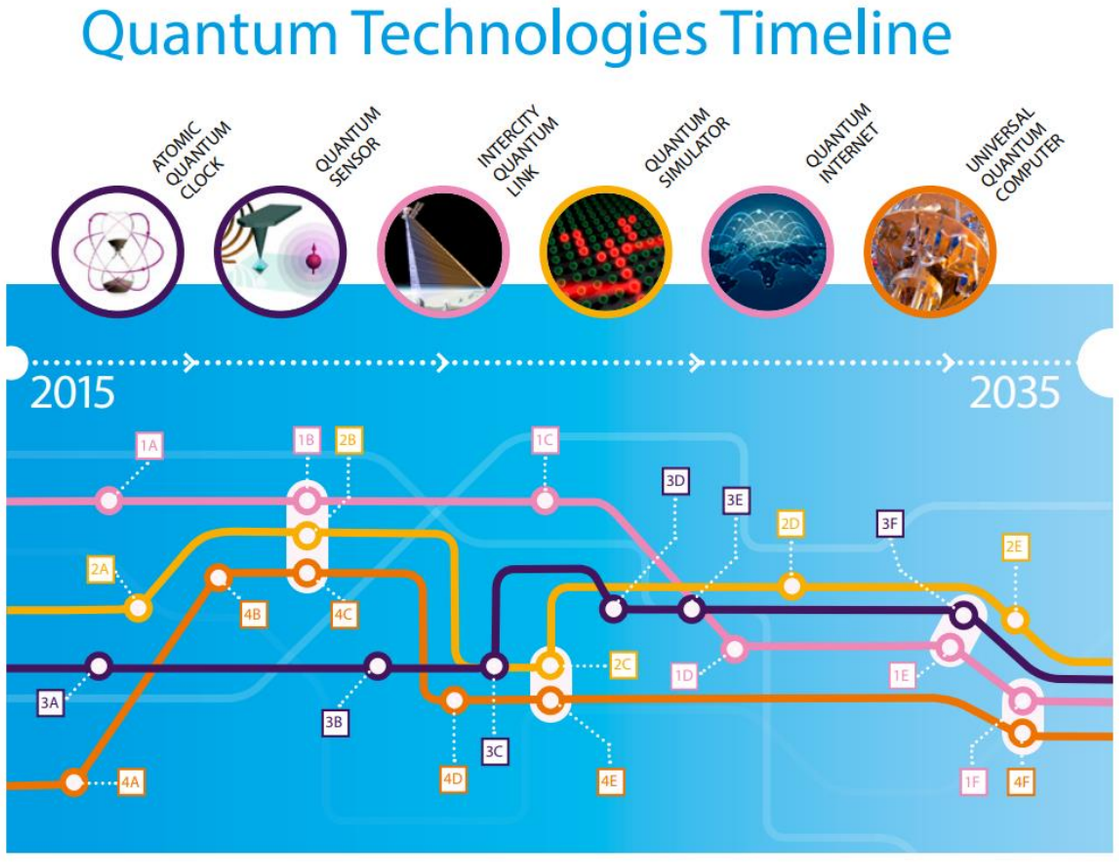
- Shor algoritmus (1994) az sorozatok keresése
  - Primfelbontás ⇒ RSA törés
  - diszkrét logaritmusok keresése ⇒ ECC és DH törés
- Grover keresési algoritmusa
  - N méretű területen keresés $\sqrt{N}$ lekérdezéssel ⇒ 2^n kulcs kipróbálása csak 2^(n/2) kvantumlekérdezéssel ⇒ dupla kulcshossz elegendő a szimmetrikus titkosításhoz
  - nehéz párhuzamosítani
  - kevésbé gyorsul a gyakorlatban a szuperszámítógépekhez képest
- Mindkettőhöz nagyméretű, hibatűrő kvantumszámítógépekre van szükség
- ezek nem léteznek (még)
- Megoldások:

1. Kvantum kriptográfia alkalmazása
   - Használjunk kvantum effektust a kriptográfiához - BB84 – one time pad
2. Posztkvantum kriptográfia
   - A klasszikus algoritmusok amelyekről úgy gondolják, hogy ellenállnak a kvantumtámadásoknak



*) Több algoritmus létezik, de hatásuk a széles körben elterjedt kriptográfiára nagyjából megegyezik Grover algoritmusával.

Quantum Technologies - background



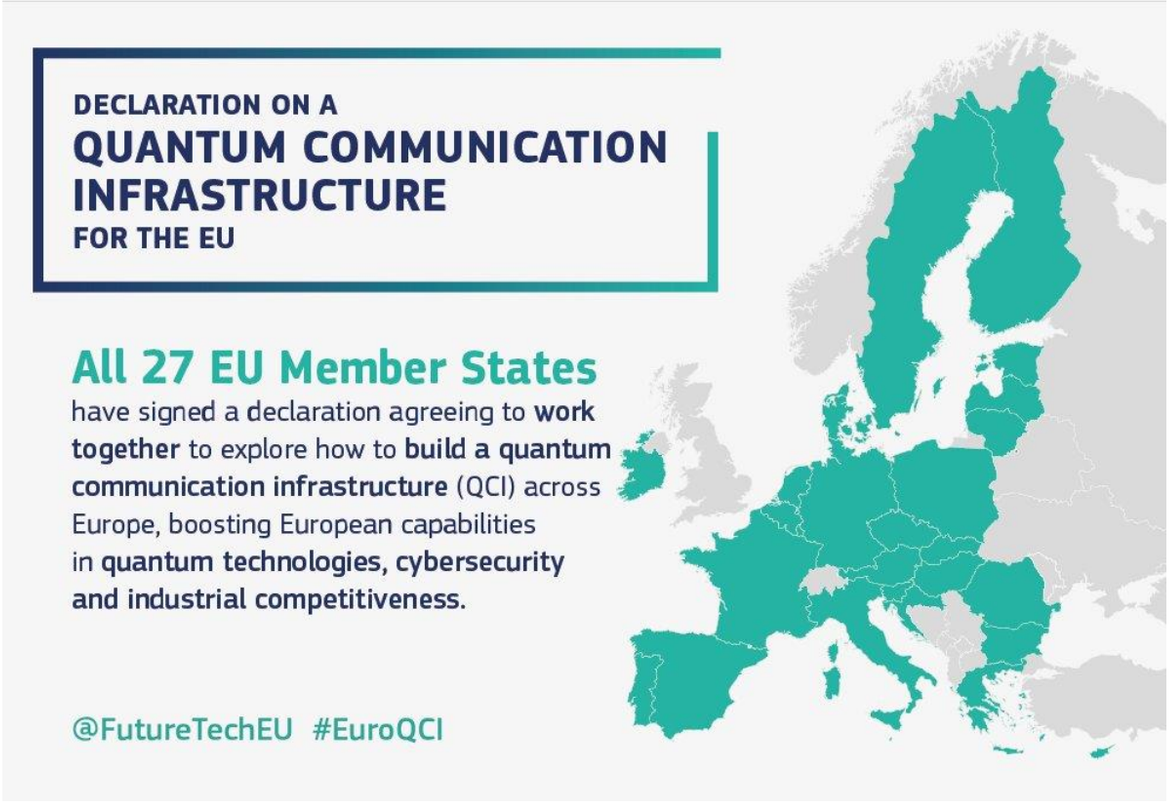
https://qt.eu/app/uploads/2018/04/93058_Quantum-Manifesto_WEB.pdf

	1. Communication	2. Simulators	3. Sensors	4. Computers
0 – 5 years	A Core technology of quantum repeaters B Secure point-to-point quantum links	A Simulator of motion of electrons in materials B New algorithms for quantum simulators and networks	A Quantum sensors for niche applications (incl. gravity and magnetic sensors for health care, geosurvey and security) B More precise atomic clocks for synchronisation of future smart networks, incl. energy grids	A Operation of a logical qubit protected by error correction or topologically B New algorithms for quantum computers C Small quantum processor executing technologically relevant algorithms
5 – 10 years	C Quantum networks between distant cities D Quantum credit cards	C Development and design of new complex materials D Versatile simulator of quantum magnetism and electricity	C Quantum sensors for larger volume applications including automotive, construction D Handheld quantum navigation devices	D Solving chemistry and materials science problems with special purpose quantum computer > 100 physical qubit
> 10 years	E Quantum repeaters with cryptography and eavesdropping detection F Secure Europe-wide internet merging quantum and classical communication	E Simulators of quantum dynamics and chemical reaction mechanisms to support drug design	E Gravity imaging devices based on gravity sensors F Integrate quantum sensors with consumer applications including mobile devices	E Integration of quantum circuit and cryogenic classical control hardware F General purpose quantum computers exceed computational power of classical computers

- A kvantumtechnológiák különböző területei
- Minden terület össze van kötve
- Előre kell lépni egy területen, hogy továbbléphessen a következőre

European Quantum Communication Infrastructure - EuroQCI

EuroQCI



Since **June 2019**, all 27 EU Member States have signed the **EuroQCI Declaration**, signaling their commitment to establish the EuroQCI

The participating countries are working with the **European Commission** and the **European Space Agency** to design and deploy the EuroQCI

The aim of the EuroQCI is to safeguard **sensitive data** and **critical infrastructures**, providing an additional security layer based on **quantum physics**

Building the EuroQCI will boost Europe's capabilities in **quantum technologies**, **cybersecurity** and **industrial competitiveness**.

EuroQCI földi rendszer - menetrend

22 23 24 25 26 27 28 29 30

Studies
Design & architecture

Support and coordination - PETRUS

First deployment phase (DEP)
First national networks to experiment with QKD technology

Support and coordination

Expand 1st Generation National QCI
(maintain & expand, use cases, gov. services operations, EU tech...)

2nd Gen. (accredited EUCI / NatCI)

First deployment phase (CEF)
Optical ground stations and cross-border links

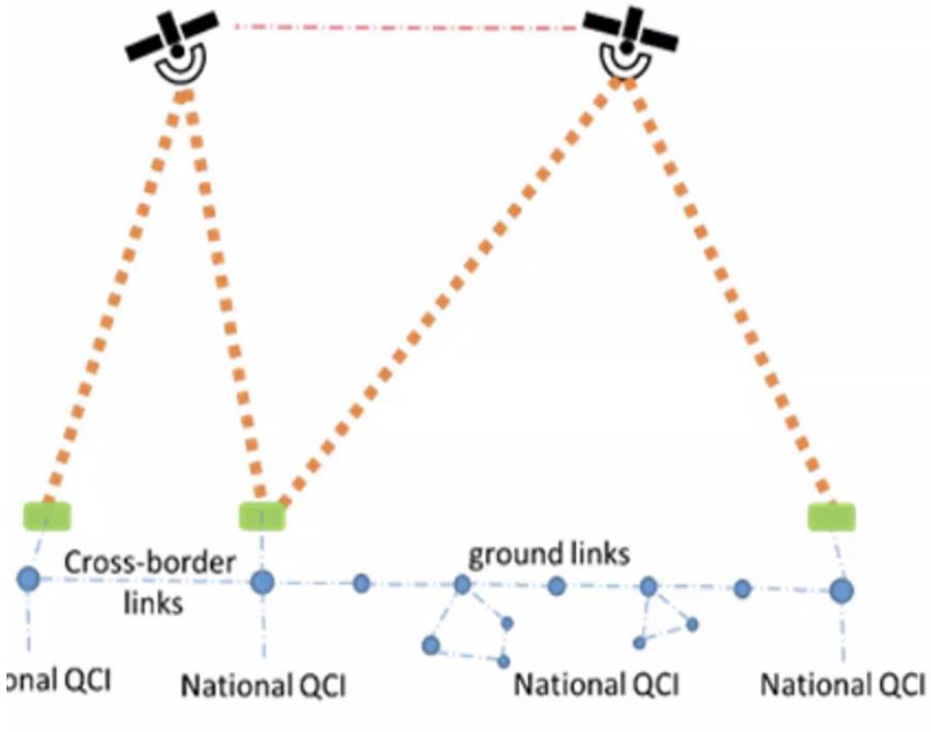
EU QKD technologies
Maturing EU Qcomm technologies

Prepare QKD tech for 2nd Generation
(Market ready & ready for EUCI certif.)

Deployment of a EuroQCI testing & evaluation infra. (NOSTRADAMUS) & transfer to hosting entity

- **Hosting entity operational**
- **QKD Certification Lab**
- **AQUA approval**

EuroQCI műholdas rendszer - menetrend



Eagle 1 – LEO satellite for in-orbit demonstration and early tests

- Eagle 1 under development, led by ESA
- Funded by Horizon Europe / ESA / Industry
- Operations:
  - QKD proof of concept & testing interfaces with OGS
- Launch Nov 2025-Feb 2026

1st Generation - deployment of LEO satellite(s) with EU technology

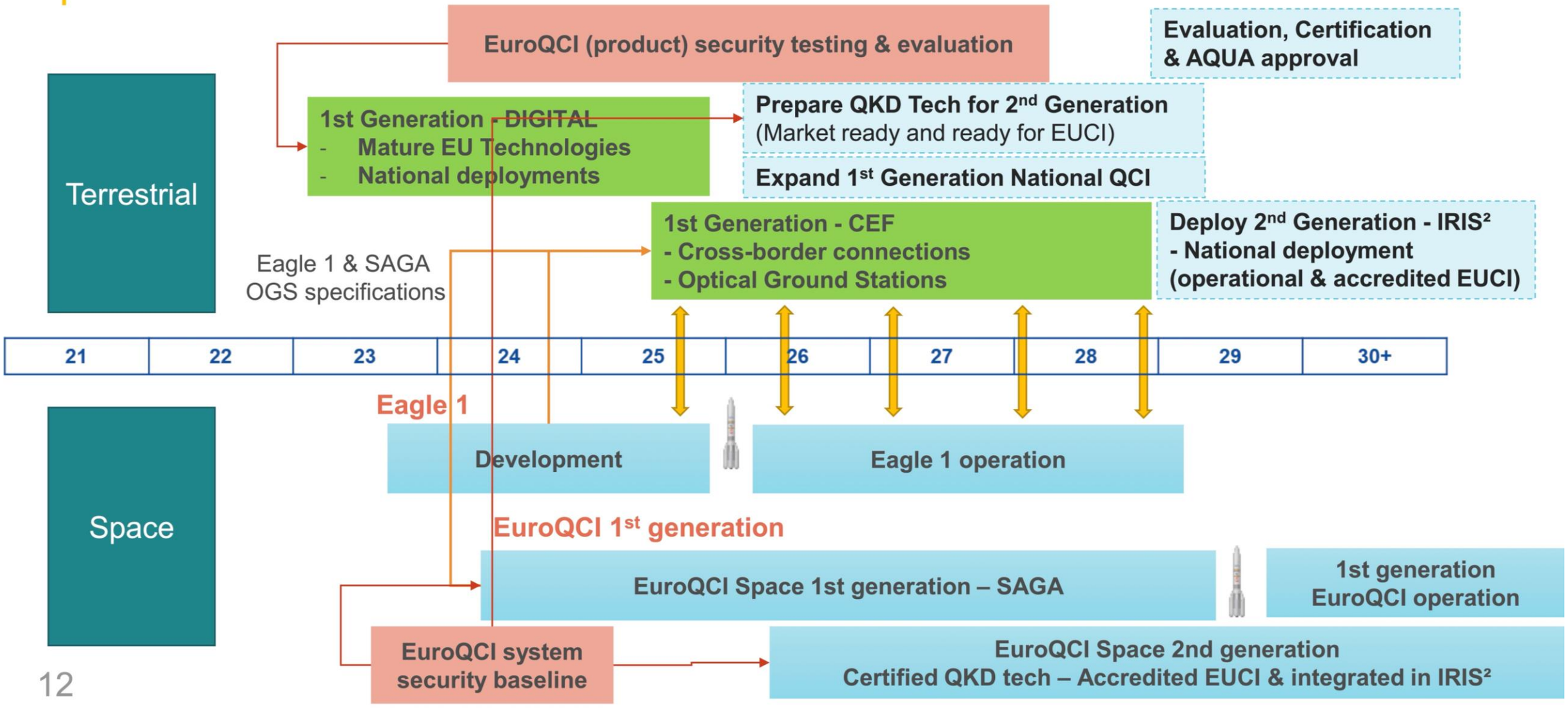
- First prototype satellite by EU/ESA
- Possibly additional satellites by Member States
- Operations:
  - Exchange quantum keys between different sites on EU territory
  - First validation of end-to-end system: interconnected LEO satellites + ground stations + terrestrial systems
  - Initial coverage of user and security requirements – incremental approach

2nd Generation - deployment of a fully operational system integrated with IRIS² for secure connectivity

- Full coverage of user and security requirements

European Commission

EuroQCI - tervezett menetrend

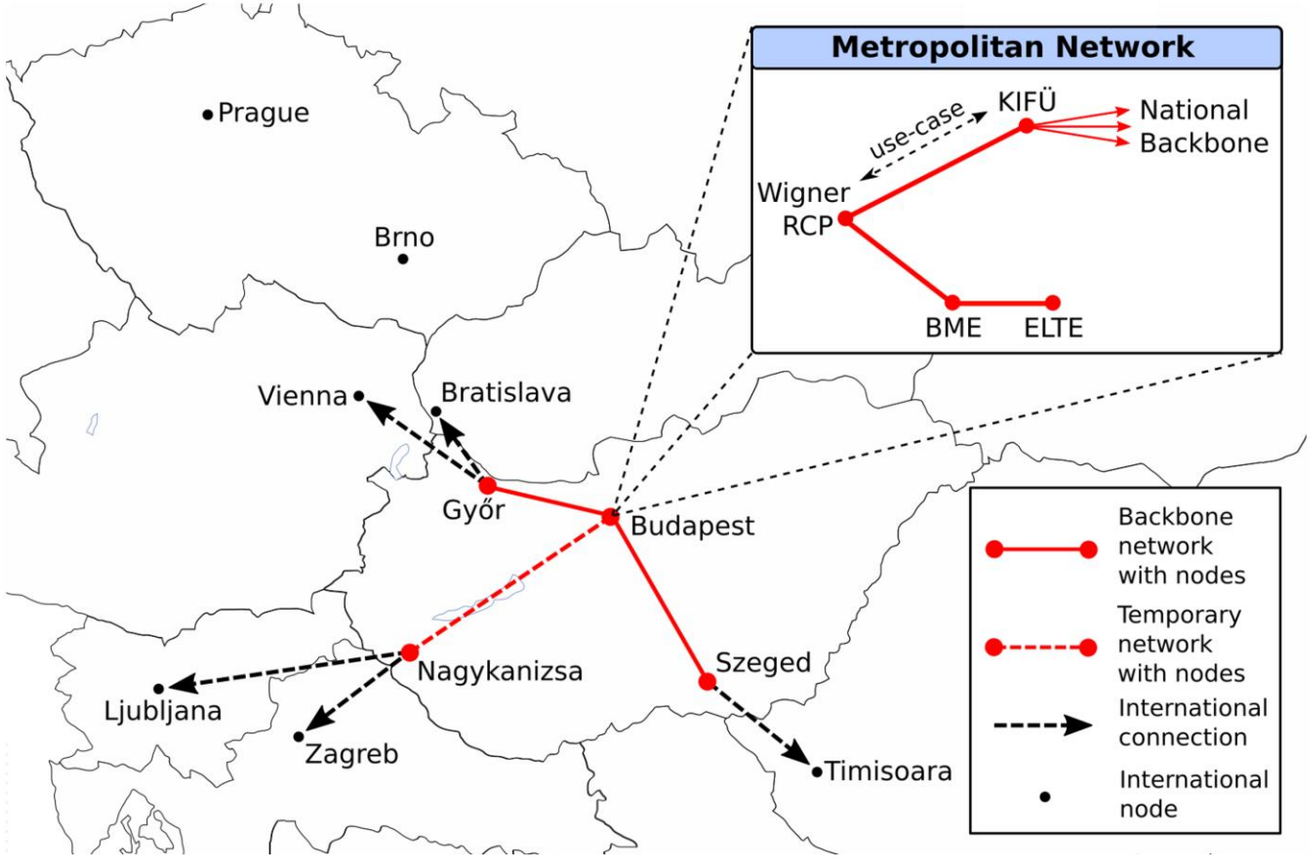


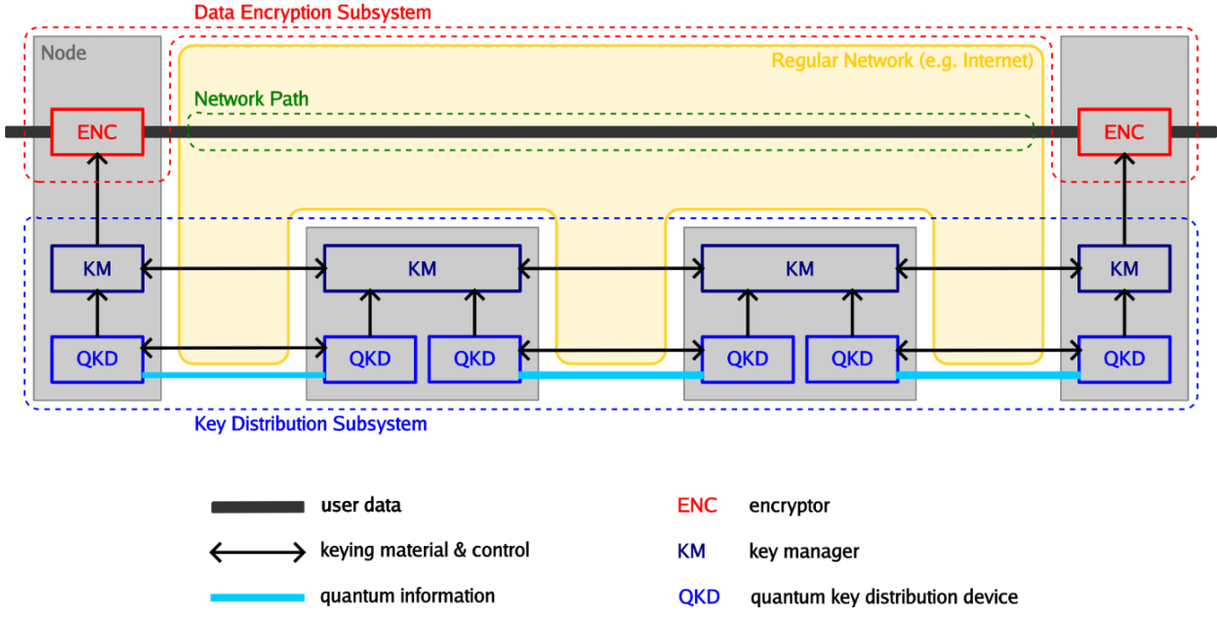
QCIHungary projekt célok – EuroQCI DEP

1. A QCI Hungary projekt fő célja egy **leendő magyar QKD teszt és kutatási kommunikációs hálózat** alapelemeinek **kiépítése**.
2. A részcélok közé tartozik a **hálózat tesztelése** valós **közhasználati** eseteken keresztül.
3. **Magyar QKD rendszerek működésének továbbfejlesztése.**
4. Szakértők és jövő nemzedékek **képzése és oktatása**
5. **Nemzetközi együttműködés** az EU kvantumkommunikációs ökoszisztémájában való sikeres részvétel érdekében.
6. A pályázat részét képezik a későbbi, **műhold** által közvetített **kvantumkommunikáció** felé megtett lépések
7. QKD-vel kapcsolatos szoftverek fejlesztése.

Partnerek :
KIFÜ, BME, ELTE, Winger RCP
Társult partner:
Magyar Telekom, Vodafone Magyarország

QCIHungary topológia és architektúra





célok

Bővebb információ:

- NWS 2023 konferencián
- https://qcihungary.hu

QKD problémák és PQC mint alternatíva ?

Diigital Sicher BSI (2021) „Quantum cryptography is a complement to post-quantum cryptography that should be researched and tested further, but it is not yet ready for widespread use.”

NSA (2022) álláspont

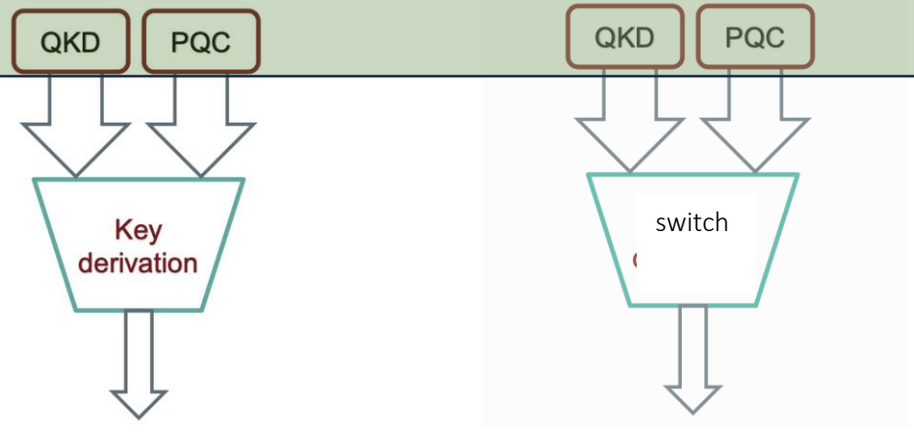
BSI position paperon QKD_2024.01.26

QKD megoldandó feladatok

- 100-120 km-nél nagyobb távolság a QKD dobozok között?
- Kulcsok elosztása olyan helyeken, ahol nincsenek QKD dobozok a „kvantumbiztonság” megtartásával? - Biztonságos kulcscsere a QKD dobozok és a felhasználók között?
- VPN szerű működés ? – Távol/mobil felhasználók
- Többpontos QKD?
- Szabványosság -minden szinten?

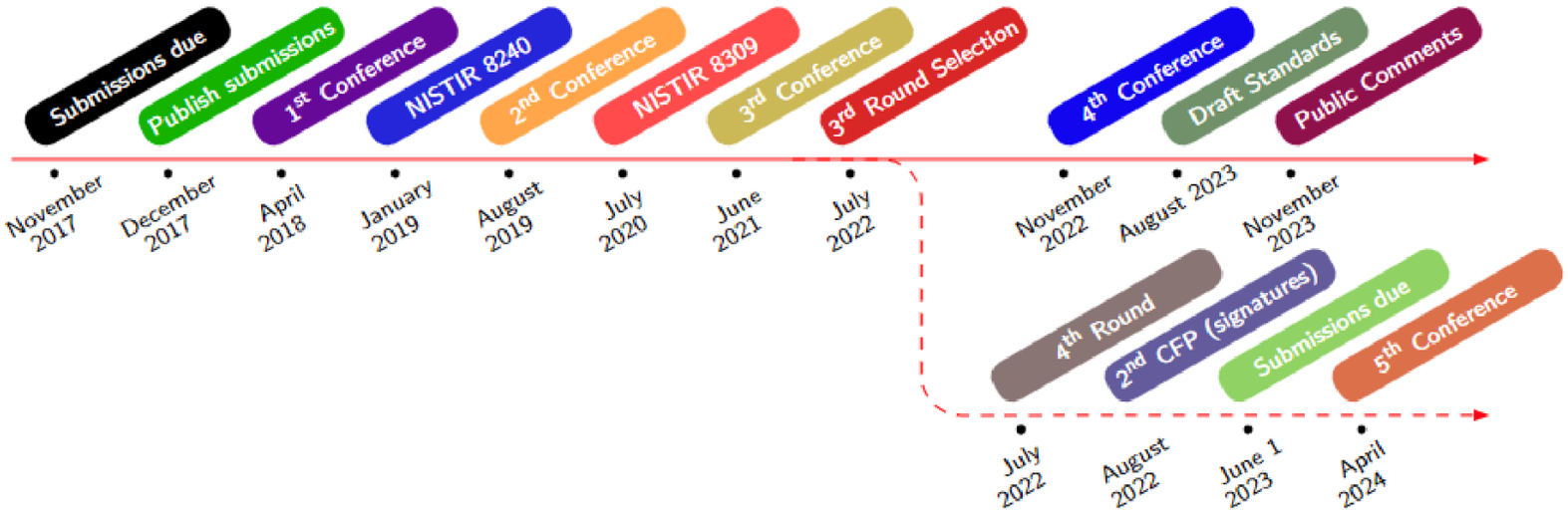
PQC?

PQC és QKD egymást kiegészítő megoldások



Post-quantum cryptography (PQC)

- Nyilvános kulcsú kriptográfia, amely a faktoráláson és a diszkrét logaritmuson kívül más problémákon alapul – amelyek jelenlegi tudásunk szerint kvantum számítógépen is nehéz megoldani
- Nyilvános kulcsú titkosítási és Digitális aláírási algoritmusok
- **Jelöltek:**
  - Lattice-based cryptography
  - Code-based cryptography
  - Multivariate cryptography
  - Hash-based cryptography
  - Isogeny-based cryptography
- 2017-ben kezdődött
  - 1. forduló: 69 pályamű
  - 2. forduló: 26 jelöltet választottak ki
  - 3. forduló: 15 jelöltet választottak ki
    - Kiválasztottak
      - KEM: CRYSTALS-Kyber
      - Signature: CRYSTALS-Dilithium, Falcon, SPHINCS+
  - 4. forduló: 4 jelöltet választottak ki (2022)
    - Kiválasztottak (2022.11)
      - KEM: Classic McEliece, BIKE, HQC
      - Signature: új javaslatokat vártak 2023 június 1-ig



A nyertes(ek) szabványosítottak:

- FIPS 203: ML-KEM (KYBER)
- FIPS 204: ML-DSA (DILITHIUM)
- FIPS 205: SLH-DSA (SPHINCS+)

Összefoglaló -Kérdések?

- Kvantum számítógépek hamarosan jól használhatók lesznek

1. QKD tesztelését és használhatóságának fejlesztését folytatni kell – QCIHungary egy lehetőség Magyarország számára
2. PQC mint alternatíva
   - PQC algorimusok/alkalmazások tesztelését el kell kezdeni
   - A PQC bevezetésének megtervézését el kell kezdeni

Mohácsi János
mohacsi.janos@kifu.gov.hu