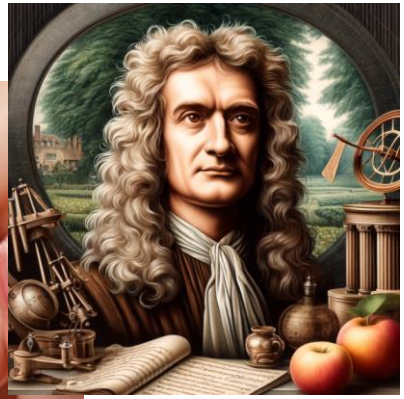
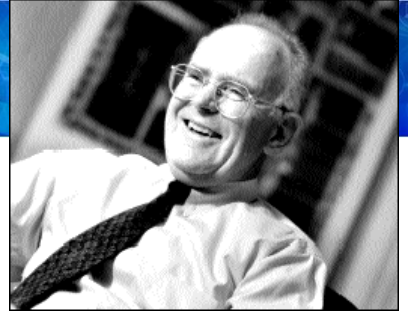
Kvantuminformatika és -kommunikáció – kicsi a bors, de erős

Imre Sándor, BME

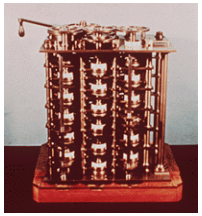
A TARTOMÁNY, AHOVÁ BEMERÉSZKEDÜNK

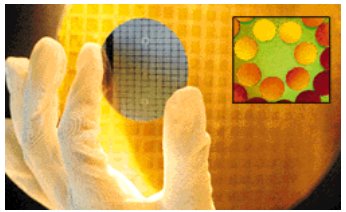
- 1 nanométer: ennyit nő a köröm 1 másodperc alatt!
- 29x félbevágunk egy almát
- A mm egymilliomod része.

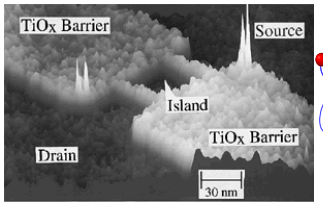


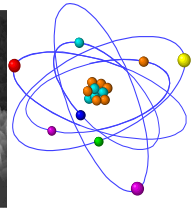


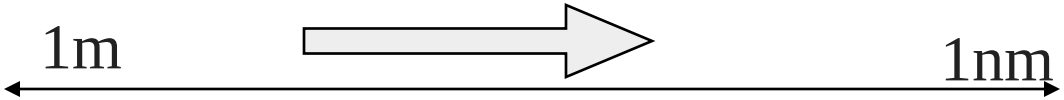
MOORE'S LAW







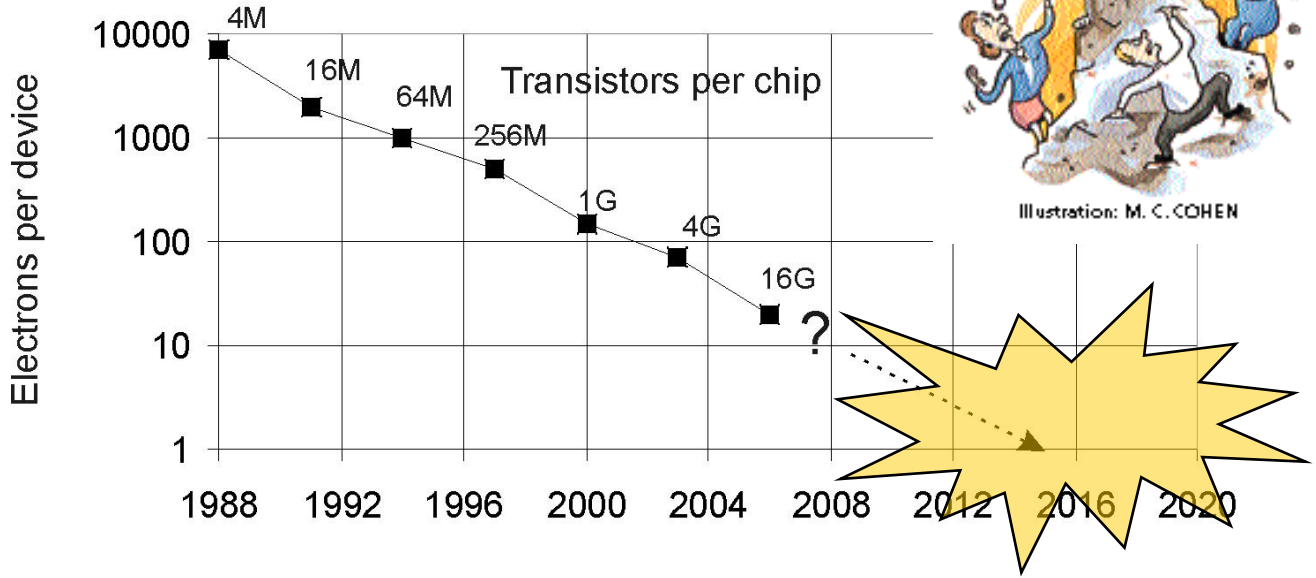




Minden 18 hónapban megduplázódik a mikroprocesszorok sebessége

KISEBB ☞ GYORSABB

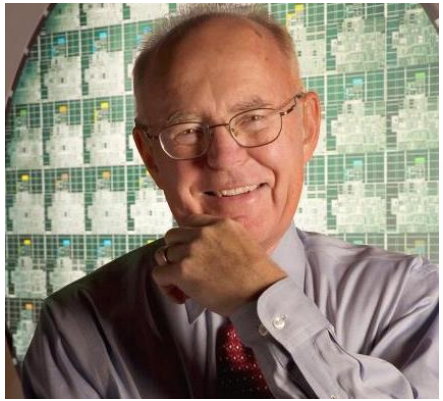
MOORE'S LAW



De meddig?

ULTRA-EXPONENTIAL SPEEDUP

MOORE'S LAW IS STILL ALIVE!



2023:
Condor – 1000+ qubits

2022:
Osprey – 433 qubits

2021:
Eagle - 127 qubits

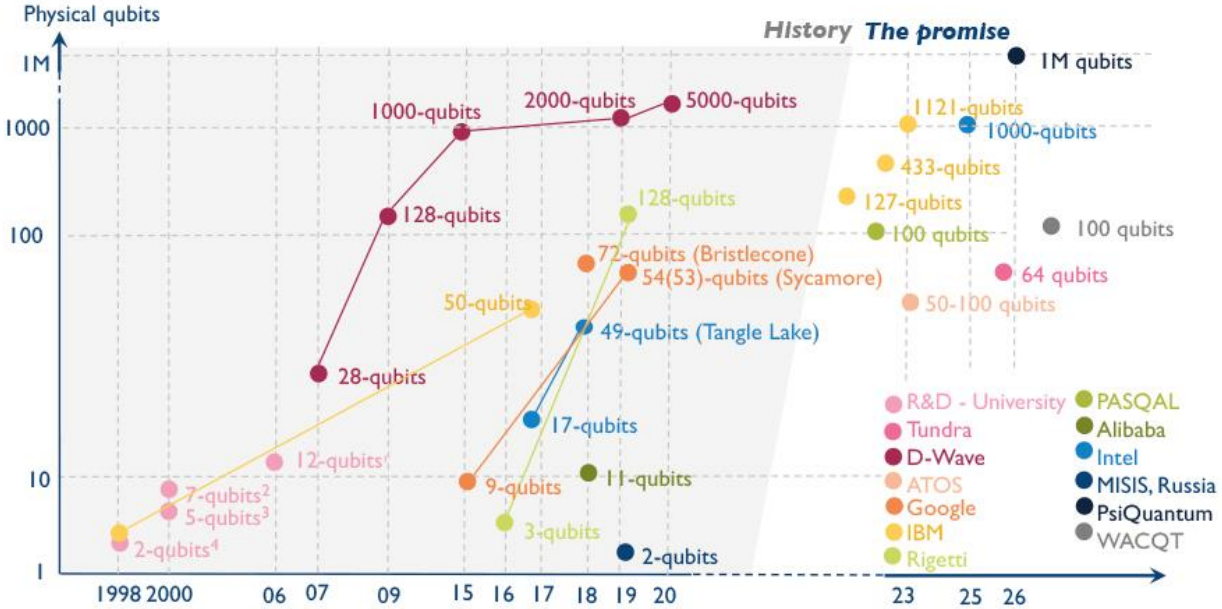
2020:
Hummingbird 65 qubits

2017:
Canary - 16 qubits

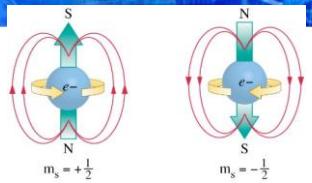
2016:
Canary - 5 qubits

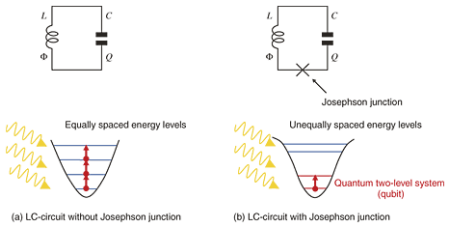
1998-2026 Physical qubit roadmap for quantum computer

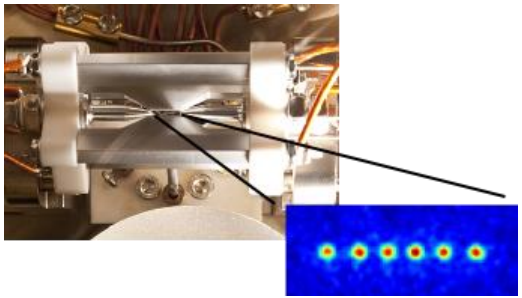
(Source: Quantum Technologies 2021, Yole Développement, June 2021)

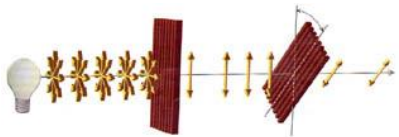


[1] (Institute for Quantum Computing, Perimeter Institute for Theoretical Physics, MIT)
[2] (Los Alamos National lab)
[3] (TU Munich)
[4] (Oxford University, IBM, UC Berkeley, Stanford, MIT)



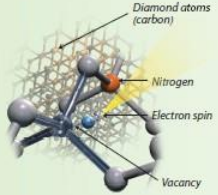




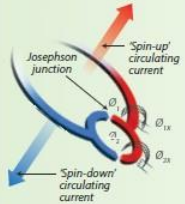


Four routes to quantum computing

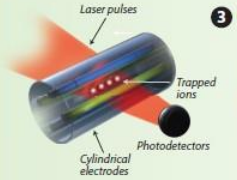
Physicists are developing different flavors of quantum computer, based on different types of quantum bits (qubits).



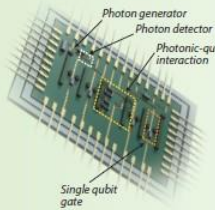
1 Spin qubits
Made from spins of electrons or nuclei trapped in a solid substrate, such as nitrogen vacancy centers in diamond. Can remain in superposition states for up to several seconds and can be compatible with current chip-manufacturing technology. Noise from solid-state environment could hamper scaling up.



2 Superconducting circuits
Superpositions of currents flowing in opposite directions around a superconductor at the same time. Being solid state, they are potentially easy to manufacture, but have relatively short coherence times and require low temperatures to operate.



3 Ion traps
Qubits reside in arrays of ions trapped in electric fields, with their quantum states manipulated by lasers. Very clean systems that don't suffer from defects, allowing for logic gates with low error rates—but scaling up will require new fabrication infrastructure.

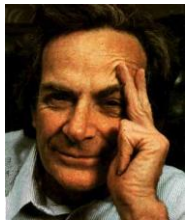


4 Photonic circuits
Qubits are encoded in the quantum states of photons travelling around circuits in silicon chips, which include etched waveguides and tiny linear optical components. Need for qubit redundancy could be minimized by photons' resistance to interference, but building photonic logic gates is difficult, and single-photon sources pose a technical challenge.

Illustration by Phil Saunders

5th Solvay conf. 1927

R. P. Feynmann 1985



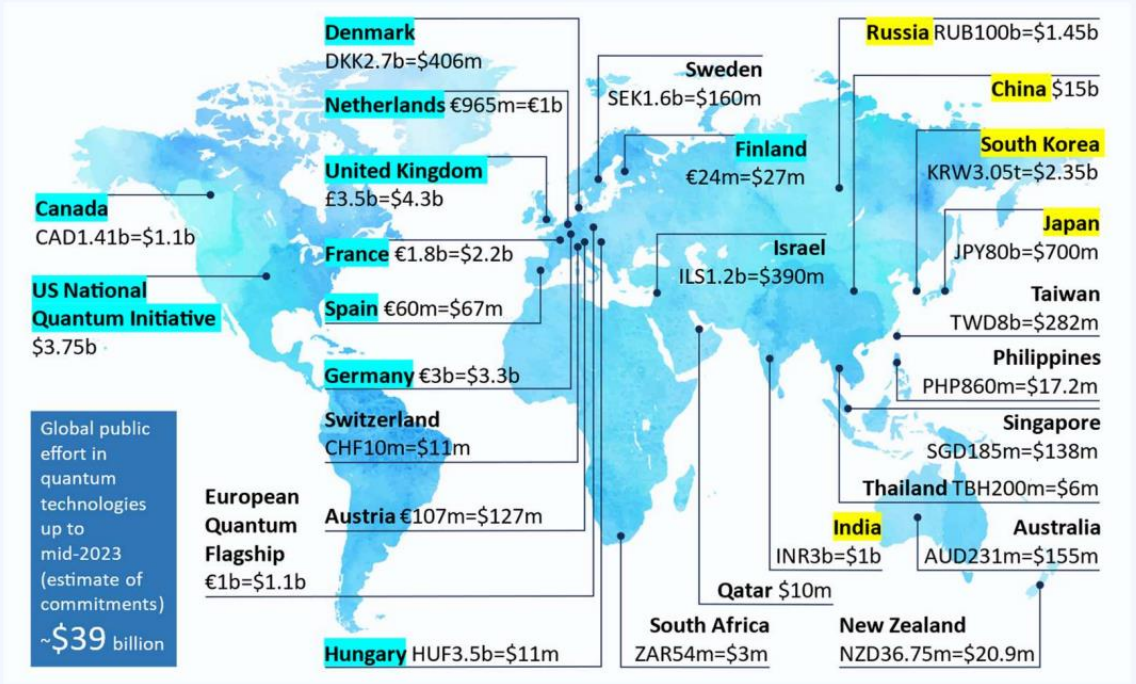
2018

2030

SHORT QUANTUM HISTORY

Global Investments

Investments in quantum technologies, both private and public, have grown greatly in the past years



Partial map of global committed public investments in quantum technologies by mid-2023. Source: QURECA / World Economic Forum

The “Mosca inequality”

Because of the “store now, decrypt later attack”, data may already be not secure if

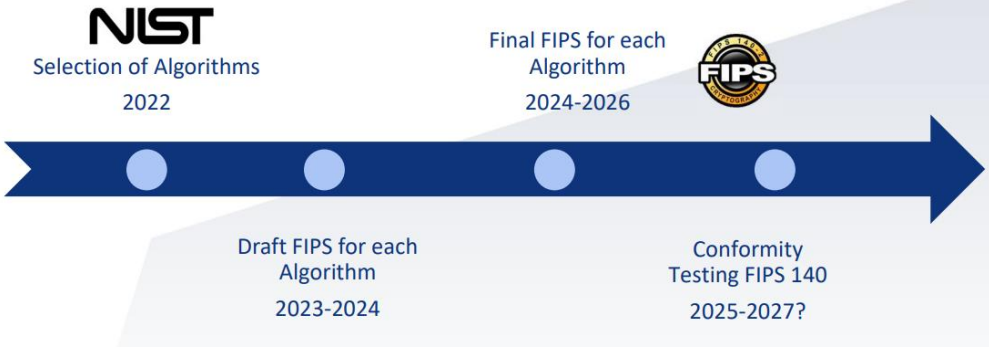
Quantum Threat Time
< Migration Time + Shelf-life Time

Time to quantum computer threat

Time needed to migrate to quantum-safe solutions

Time data needs to be secure for

POST-QUANTUM CRYPTOGRAPHY



FIPS = Federal Information Processing Standards


SECURITYWEEK
Malware & Threats | Security Operations | Security Architecture | Risk Management | CISO Strategy | ICS/OT | Funding/M&A

MANAGEMENT & STRATEGY

Tech Giants Form Post-Quantum Cryptography Alliance

The Linux Foundation, AWS, Cisco, IBM, and other tech companies establish the Post-Quantum Cryptography Alliance.

By Ionut Arghire
February 6, 2024

OQS

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STORE

COULDA BEEN A CONTENDER —

Post-quantum encryption contender is taken out by single-core PC and 1 hour

Leave it to mathematicians to muck up what looked like an impressive new algorithm.

DAN GOODIN - 8/2/2022, 8:31 AM

COMPANY INDUSTRIES SOLUTIONS SERVICES RESOURCES PARTNERS CONTACT

NIST PQC Finalists Update: It's Over For The Rainbow

by Edlyn Teske on 26. March 2022

CSG Quantum Cryptography Crypto-Agility Quantum Computing NIST

Last month, one of the three NIST finalists for post-quantum signature schemes received its final nail in the coffin: Ward Beullens, a PostDoc at IBM Research, published a practical key recovery attack against the Rainbow signature scheme.

IACR News item: 10 April 2024

Quantum Algorithms for Lattice Problems

Yilei Chen

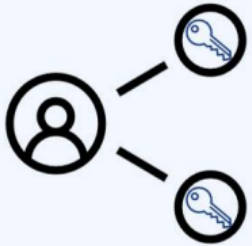
Note: Update on April 18: Step 9 of the algorithm contains a bug, which I don't know how to fix.

We show a polynomial time quantum algorithm for solving the learning with errors problem (LWE) with certain polynomial

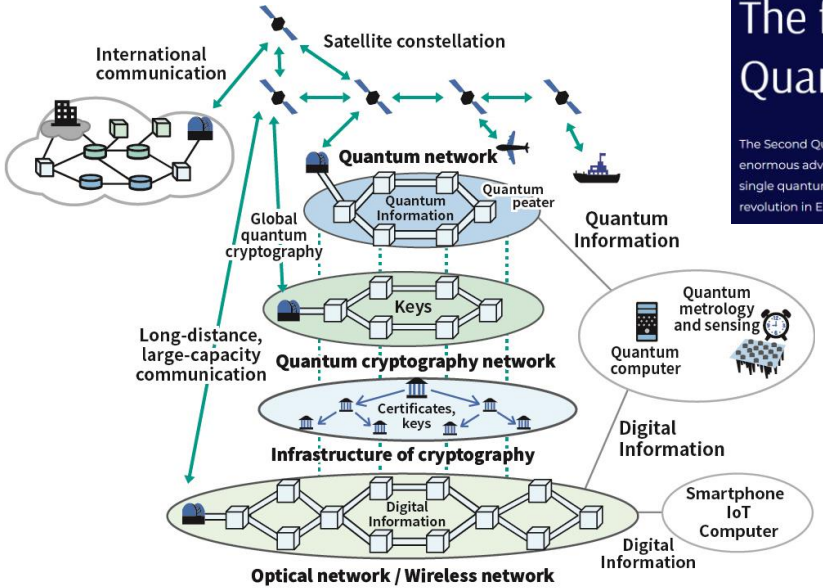
Post Quantum Cryptography

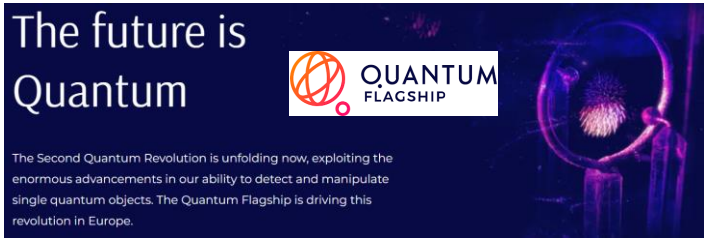
Quantum Key Distribution

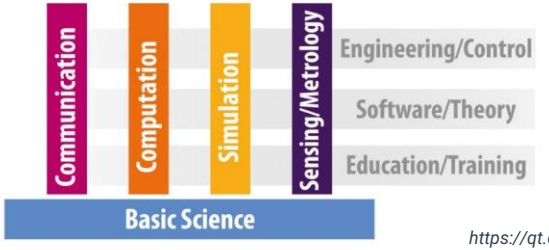
Pre-Shared Keys



Symmetric key cryptography





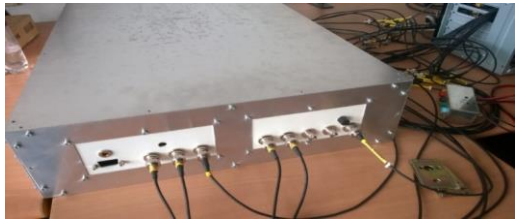


https://qt.eu/

Quantum Safe legislations and guidance

- **USA:** Quantum Computing Cybersecurity Preparedness Act (late 2023)
- **UK:** Guidance from NCSC on NIST standardizing Post Quantum Cryptography, legislation likely at the end of NIST process
- **EU:** whitepapers, but no EU-wide legislations

by Melchior Aelmans (Juniper Networks)



HUNQUTECH
2017-2021

ERICSSON

E·L·T·E

wigner

MŰEGYETEM 1782

BHE

NOKIA

FEMTONICS
ADVANCED MICROSCOPY

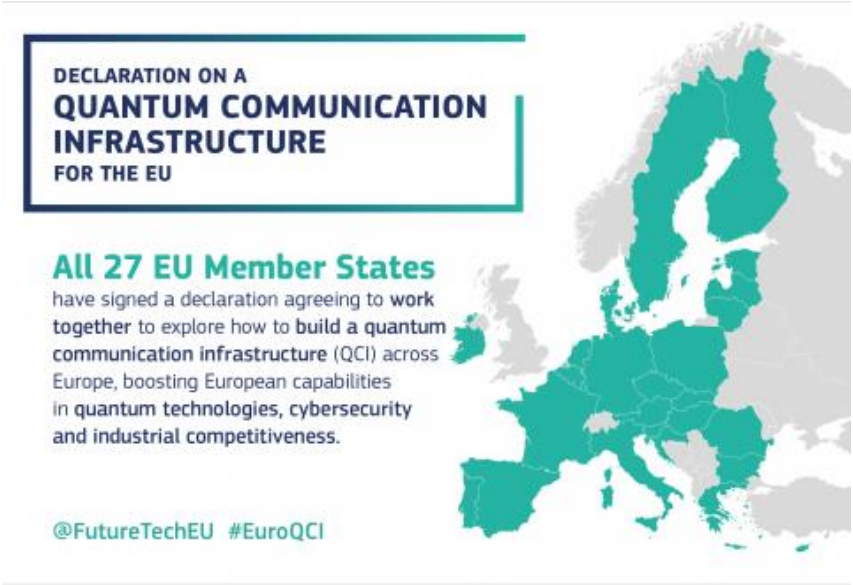
https://wigner.mta.hu/quantumtechnology/en/node/1

KVANTUMINFORMATIKA NEMZETI LABORATÓRIUM 2020-2024

https://qi.nemzetilabor.hu/hu

WE ARE PART OF EUROQCI

EuroQCI

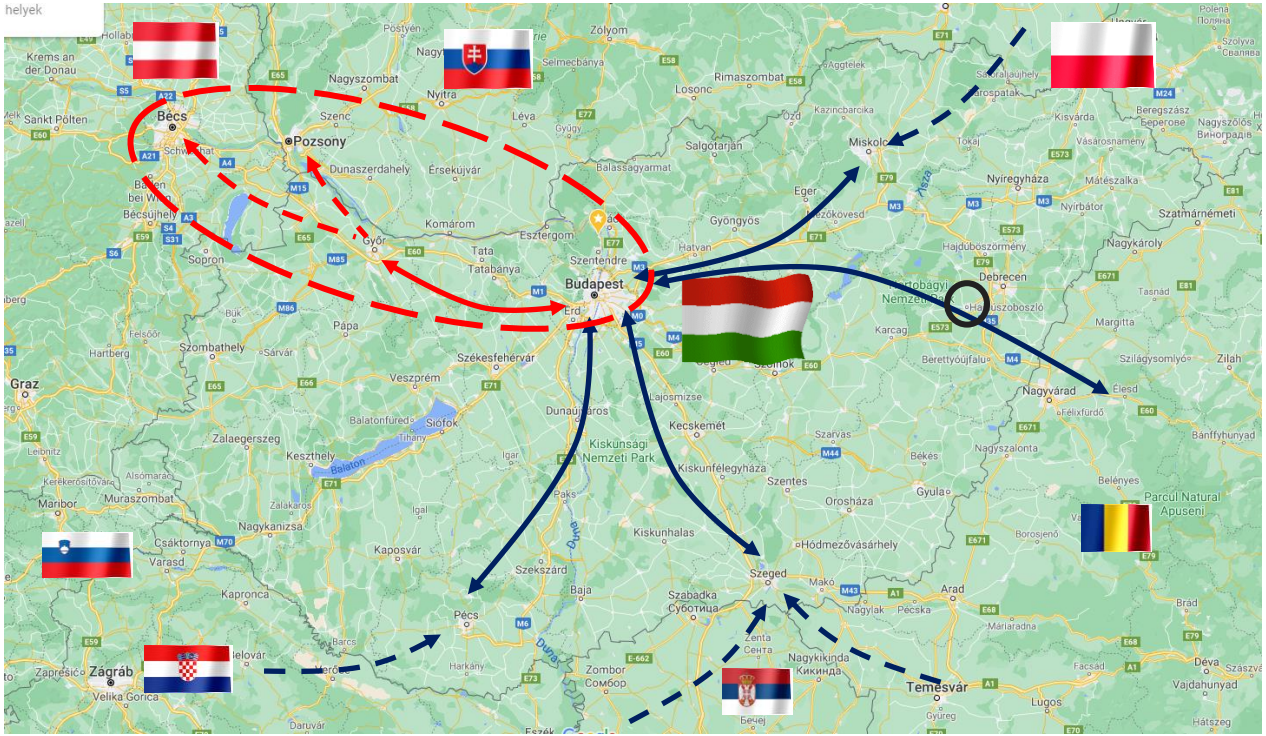


Hungarian activities

- Develop a QKD system using entangled photon pairs sent over a free-space optical telescope link.
- Install an optical ground station for satellite-based QKD systems.
- Realize a QKD system based on entangled photon pairs sent over an optical fiber link.
- Complete the development of a continuous variable QKD system.

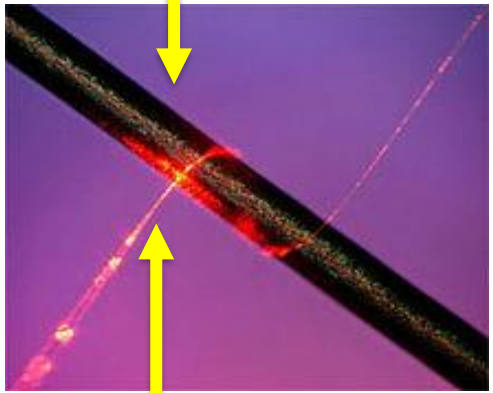
QCIHungary

EUROQCI - HUNGARIAN BACKBONE NETWORK 2024-2025

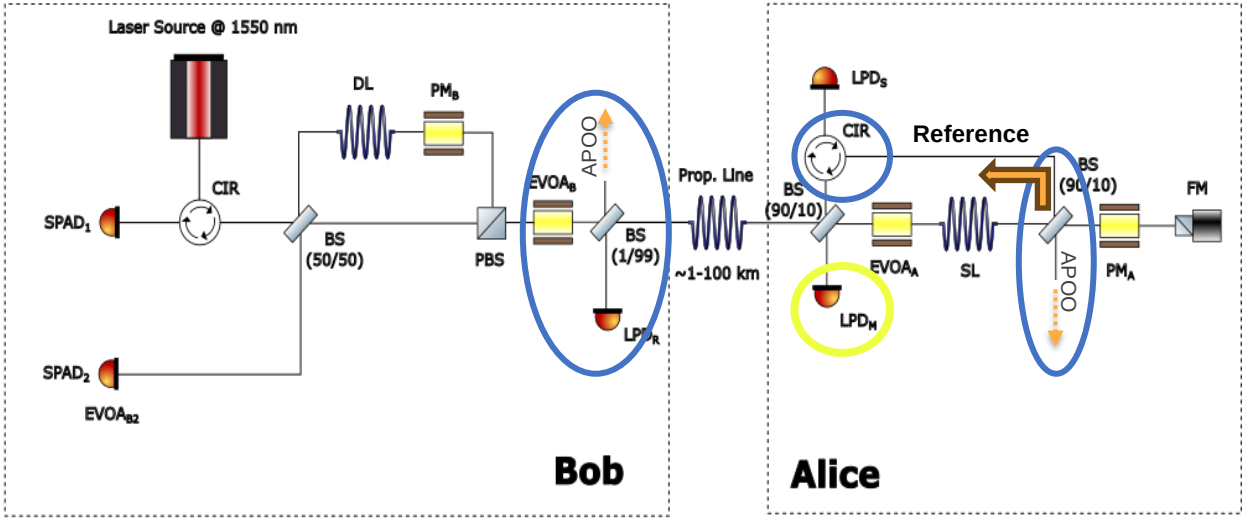


FIBER BASED QKD

This is your hair

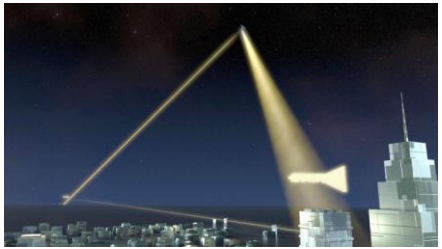


This is the core



AHOGY MI KULCSSZÉTOSZTUNK – 2024

Space segment: ESA-SAGA

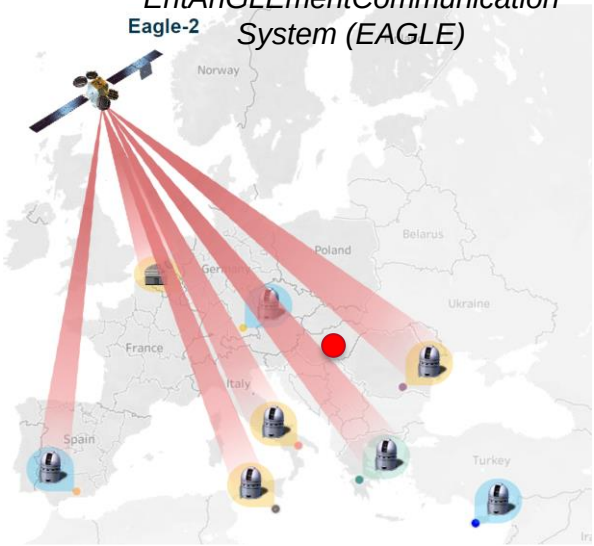


LEO/MEO: prepare and measure

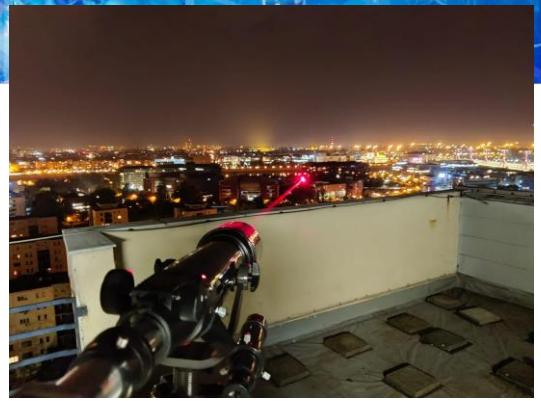
Quantum Cryptography TeleComSystem (QUARTZ)

GEO: entanglement based

EntAnGLEmentCommunication System (EAGLE)

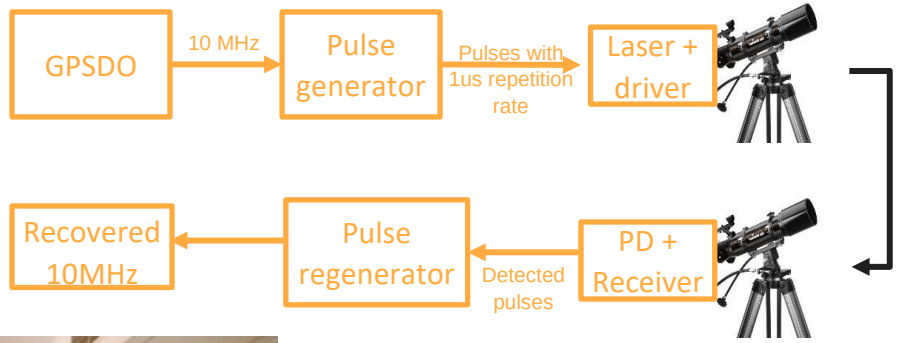


FREE SPACE QKD

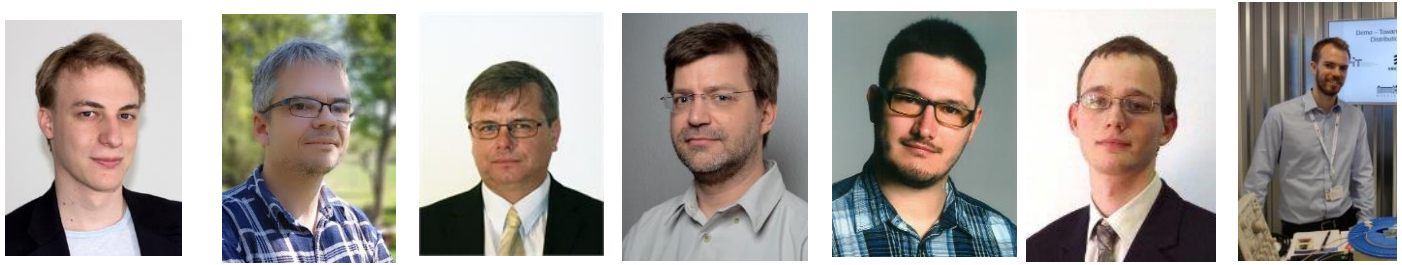


CLASSICAL SYNCRONIZATION

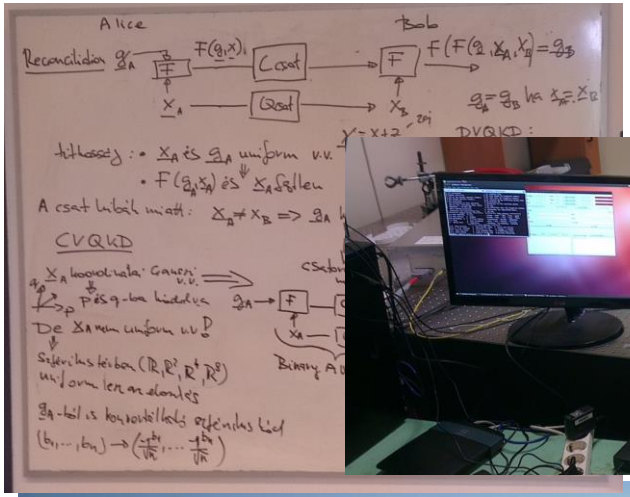
CERTAIN:
Complex electronic hardware for free-space entanglement-based quantum key distribution system

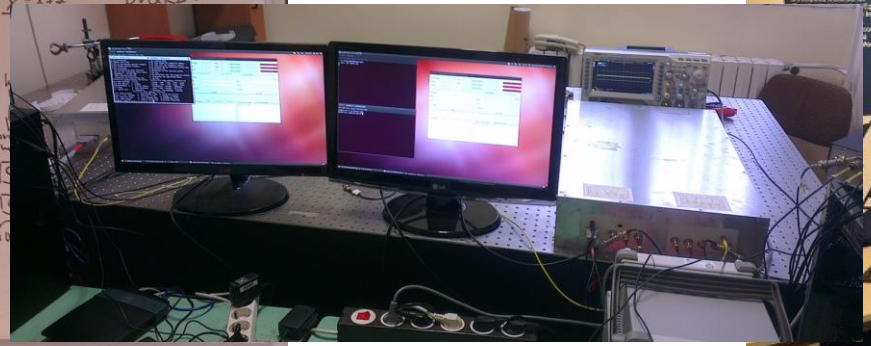


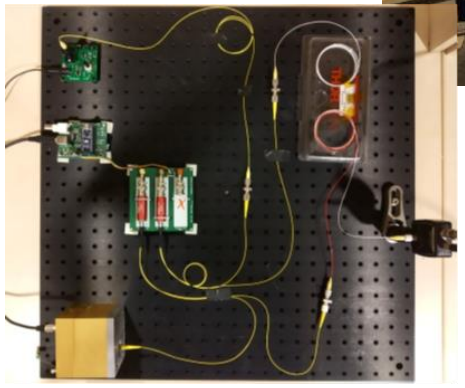
1550 / 650 nm experimental laser sync Alice / Bob

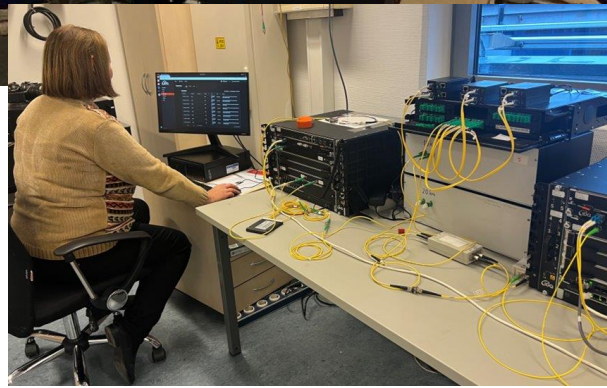


OUR QUANTUM COMMUNICATIONS RESEARCH GROUP


Alice
Bob
Reconciliation
Csat
Qsat
CVQKD







Competences and actual projects – fiber based

- Own developed Optical Quantum Random Number Generator
- BB84 QKD demonstration with own developed system *(in cooperation with Ericsson Hungary)*
- CV QKD long distance demonstration with own developed system as part of the national QKD network *(in cooperation with Hungarian Telekom and HUN-REN Wigner Research Centre for Physics)*
- Developing an entanglement-based QKD system (fiber-based, using SNSPD detectors)
- OpenQKD OpenCall: QuantumGigalink - Extension of high-speed leased line service with QKD encryption function *(in cooperation with Magyar Telekom)*
- Participation in the national project of the European Quantum Communication Infrastructure (EuroQCI)
- Modeling, analysis, planning, implementation and operational support of QKD networks *(in cooperation with NETvisor Zrt.)*

EuroQCI QCIHungary QNL Quantum Information National Laboratory HUNGARY ERICSSON ADVANET Magyarország Rendszerintegrációs Kft. Magyar Telekom Netvisor

Competences and actual projects – free-space and space

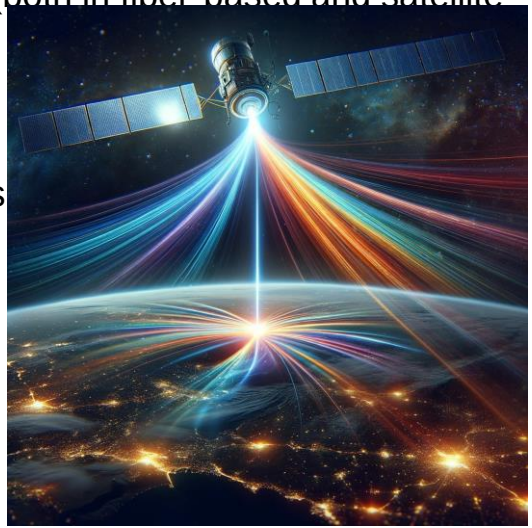
- Development of an entanglement-based free-space QKD over River Danube *(in cooperation with Vodafone Hungary)*
    - in-house entangled photon source at 810nm, in-house optical clock synchronization
- Participating in different ESA projects
    - QuStation - Quantum Communications Capable Optical Ground Stations in Hungary *(in cooperation with ATL Zrt.)*
    - Certain - Complex electronic hardware for free-space entanglement-based quantum key distribution system *(in cooperation with Relcom Kft.)*
    - DeQOS - Development of Quantum and Optical Communication for Satellite Systems Course *(in cooperation with ATL Zrt., C3S Ltd., E-Group Zrt.)*
- Deploying quantum-capable optical ground station
- Investigating the possibilities for cubesat-based QKD
- Theoretical work on future's satellite based QKD systems

C3S Relcom

EuroQCI QCIHungary Quantum Information National Laboratory HUNGARY esa ATL ADVANCED TECHNOLOGY OF LASER E-GROUP SOFTWARE & BEYOND vodafone

Research directions – quantum internet

- Developing and analyzing entanglement-based quantum communication protocols over the quantum internet (quantum wifi, superactivation of quantum channels)
- Analyzing different aspects of satellite-based quantum networks (architecture, configurations, routing)
- Investigation of application possibilities of different quantum memories (both in fiber-based and satellite-based networks)



Research directions – quantum computers

- Analyzing different quantum algorithms on different quantum computers
- Developing new algorithms for quantum computers

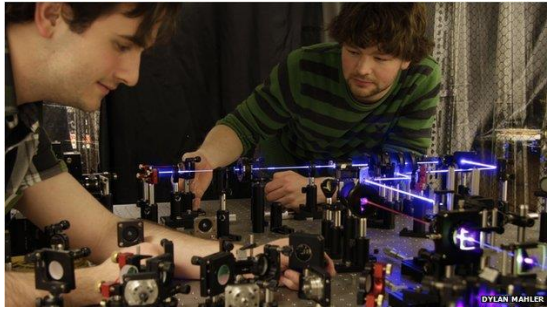
Educational activities (BSc, MSc, PhD)

- 20+ years experience

EuroQCI QCIHungary QNL Quantum Information National Laboratory HUNGARY

- Kvantumszámítógépek és alkalmazásaik
  - Alapok
  - Algoritmusok
  - Programozás
  - Benchmarking
  - AI, stb
- Kvantumhálózatok
  - Alapok
  - Kvantum-infoelmélet
  - Titkosító rendszerek
  - Kvantuminternet: vezetékes+műholdas
  - QRNG stb.
- Labor
  - Qszámítógép hardver
  - Qhálózat hardver
  - Programozás
  - QRNG stb.

MSC QUANTUM SPEC.



Jelenleg 10 kvantumos tárgy fut ~350 hallgatóval

Questions?