



the future is quantum
technologies for the 21st century

radu ionicioiu



what are quantum technologies

and why

you will need them



*what will be a key technology
in the 21st century?*

revolutions

a historical perspective

1.0: industrial

work as a resource



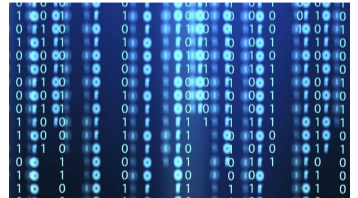
2.0: electronics

electricity as a resource



3.0: digital

information as a resource



two key points

KP 1: science drives technology

new science \Rightarrow *new technologies*

KP 2: it's all about resources

harnessing resources is key

generate, transport, control, transform, use



revolution 4.0: quantum
the second quantum revolution

quantum

the driving technology of the 21st century



the art of controlling

individual quantum systems

to perform useful tasks



quantum resources

superposition, entanglement, nonlocality, duality

quantum features:

- ◆ no **classical** analogue
- ◆ **essential** for quantum technologies
- ◆ **goal**: harness quantum systems for useful tasks

generate, transport, control, transform, use



QUANTUM TECHNOLOGY APPLICATIONS



Ultra-precise clocks

Navigation systems
Smart energy grids
Timestamp financial transactions

Medical Imaging Techniques



Nuclear magnetic imaging
Detailed visualization
Advancing Imaging Techniques



Simulators

Quicker drug development
New materials

Quantum Key Distribution



Most Secure Communications
Eavesdropping detection



Sensors

Oil and gas exploration
High-precision geodesy and navigation

Quantum Computing

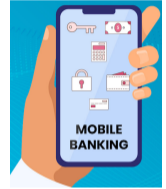


Machine Learning
Artificial Intelligence
Big data



quantum communications

crypto: we use it every day



the problem

quantum computers will break internet security

- ◆ secure communications
- ◆ digital signatures
- ◆ mobile networks
5G, 6G, ...
- ◆ financial transactions
mobile banking, POS, e-commerce
- ◆ authentication
- ◆ critical infrastructure
- ◆ blockchain
bitcoin, ethereum, ...
- ◆ software updating
cars, computers

⇒ need to avoid the *quantum apocalypse* (Q-Day)



how serious is the threat?

Mosca equation

"store now, decrypt later" (SNDL) attack

Migration time

The number of years needed to properly and safely migrate the system to a quantum-safe solution

Shelf-life time

The number of years the information must be protected by the cyber-system



Threat timeline

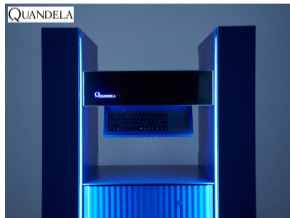
The number of years before the relevant threat actors will be able to break the quantum-vulnerable systems

Danger zone

Source: Michele Mosca, University of Waterloo, Canada¹³

quantum computing

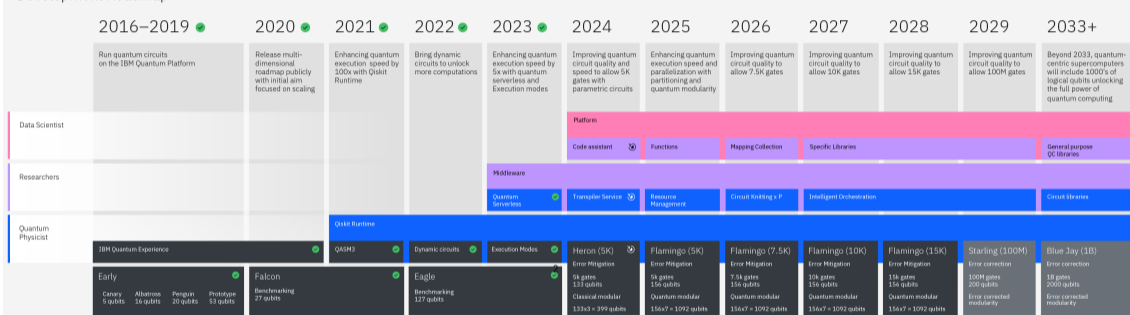
a **\$65 billion** industry by 2030



IBM roadmap

Development Roadmap

IBM Quantum



... any solutions?

Q-Day

two ways out

1. **the classical way**: post-quantum crypto (PQC)

find quantum-resistant, public-key classical algorithms \Rightarrow **NIST PQC**

2. **the quantum way**: quantum key distribution (QKD)

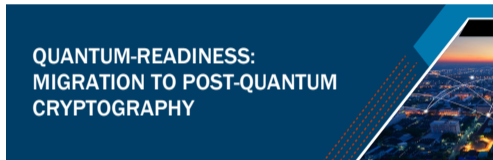
use the power of quantum + symmetric crypto (AES, OTP)



what to do?

transition to *quantum-resistant* crypto

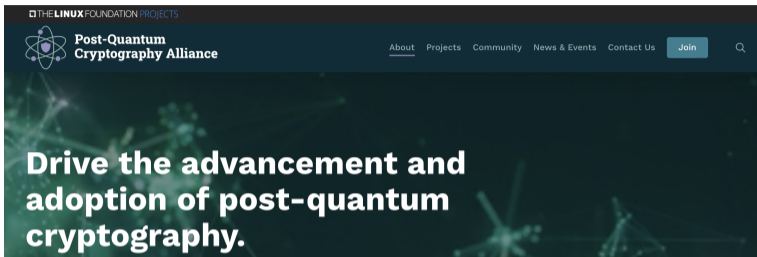
- ◆ create a **quantum-readiness** roadmap
- ◆ start **quantum risk assessment**
- ◆ replace public-key algorithms with **quantum-resistant** ones



NIST NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

20 billion devices to be upgraded/replaced with PQC in the next 20 years

post-quantum crypto alliance



General

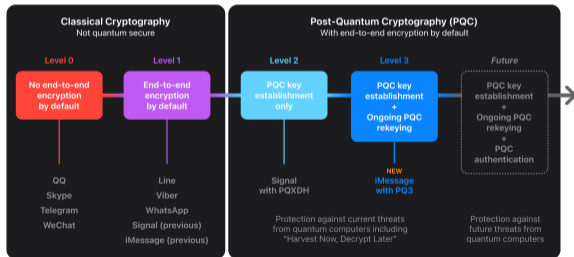


PQC: deployed

◆ signal protocol: enhanced by PQC

◆ 🍏 : iMessages with PQ3

Quantum-Secure Cryptography in Messaging Apps



Signal
@signalapp@mastodon.world

Announcing PQXDH! The first step in post-quantum resistance for the Signal Protocol, PQXDH protects your Signal calls & chats from potential future threats of breakthroughs in quantum computing. And it's already rolling out to Signal clients everywhere.

signal.org/blog/pqxdh/

The bottom part of the screenshot shows a blurred image of a Bloch sphere, a mathematical representation of a qubit's state in quantum mechanics. It features a 3D coordinate system with x, y, and z axes. The north pole is labeled $|0\rangle$ and the south pole is labeled $|1\rangle$. A vector representing a quantum state $|\psi\rangle$ is shown originating from the center, with its orientation defined by angles θ and ϕ .

the quantum way: QKD

1. use **quantum resources** to securely distribute keys
2. use keys in **symmetric crypto** (OTP, AES etc)

quantum solves 2 problems:

- ◆ true (**quantum**) randomness
- ◆ secure key distribution
eavesdropper detected



the quantum way: QKD

why does it work?

- ◆ no-cloning theorem \Rightarrow Eve **cannot clone** an **unknown quantum state**
- ◆ measurement changes the state \Rightarrow you **listen**, you **leave a trace**

Eve will be detected !

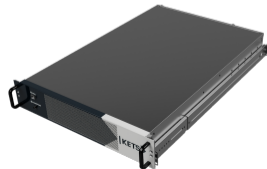
classically impossible



QKD

commercial

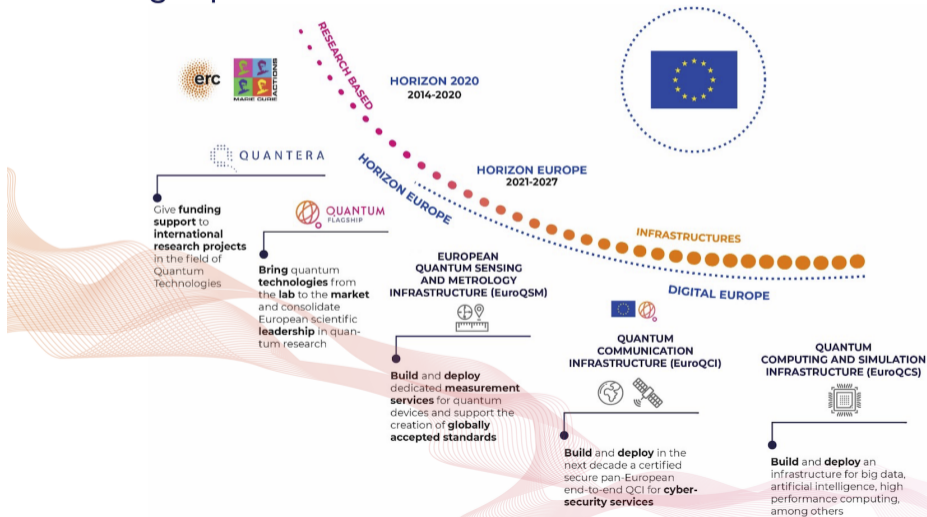
- ◆ providers: IDQ, ThinkQuantum, Toshiba, QTI, KeeQuant, Kets Quantum, QO Jena, LuxQuanta ...
- ◆ € 150-300 k/pair



quantum: worldwide



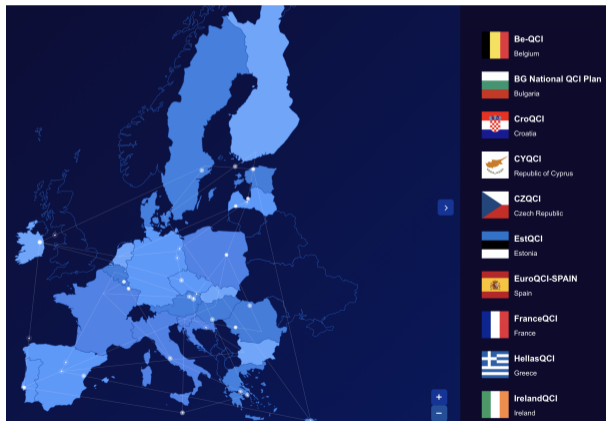
From Flagship to Fleet



Petrus: building EuroQCI




- ◆ network of 27 national QCI
- ◆ fiber + free-space links
- ◆ cross-border links










EuroQCS

- ◆ 6 sites across EU
- ◆ applications
 - ▶ molecular simulations: **new medicines**
 - ▶ new materials: **batteries**
 - ▶ traffic optimisation: **maps**
 - ▶ logistics: **EMAG**
 - ▶ scheduling: **Bolt Glovo**
- ◆ R&D, industry need **quantum computers**



The EuroHPC JU has selected six sites across the European Union to host and operate the first EuroHPC quantum computers in:

-  Czechia
-  France
-  Germany
-  Italy
-  Poland
-  Spain



BOSCH



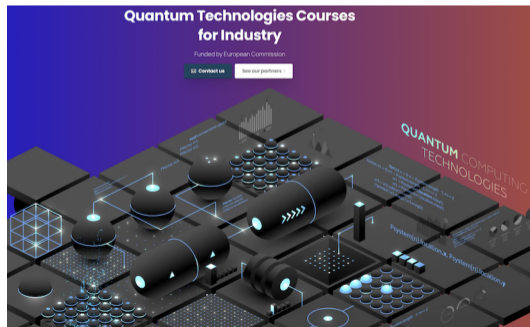
MERCK



SIEMENS

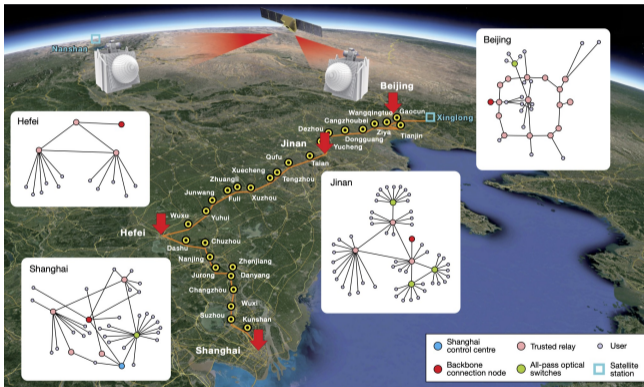
VOLKSWAGEN
AKTIENGESELLSCHAFT

EU quantum ecosystem



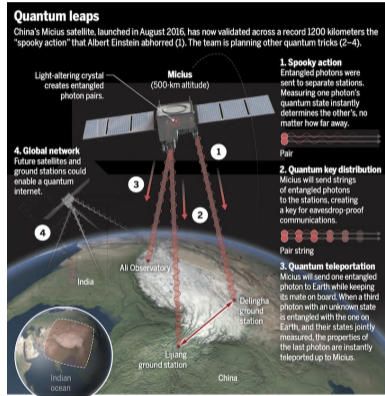
China

Beijing-Shanghai quantum backbone, 2000 km (\approx Bucharest-Brussels)



Nature 589, 214 (2021)

Hefei: 46 nodes intra-city quantum network



Science 356, 1110 (2017)

quantum @RO

Vision

quantum: the driving technology in 21st century

Mission

develop quantum technologies in Romania

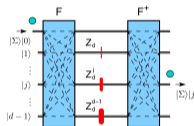
Strategic objectives

- ◆ *research*
- ◆ *education*
- ◆ *dissemination*

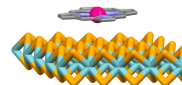
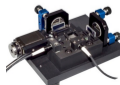


- ◆ €1.14 Mil
- ◆ 5 partners, 5 projects
- ◆ grant: UEFISCDI (PCCDI)
- ◆ <https://roqnet.ro/qutech-ro/>

P1: Q-INFO	P2: Q-CHIP	P3: Q-VORTEX
IFIN-HH	INFLPR	IMT
quantum information quantum simulation quantum protocols	integrated quantum photonics 3D laser <i>fabrication</i>	optical vortices lithography

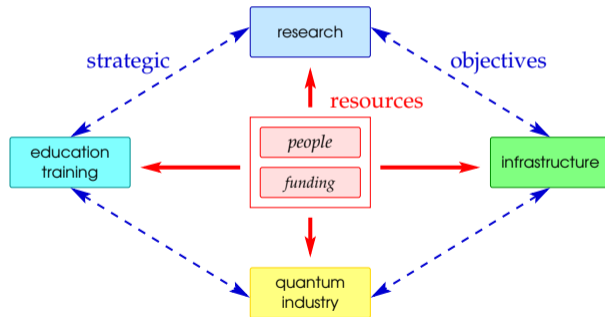


P4: Q-LAB	P5: Q-FERMI
UPB	ITIM-Cluj
Applied quantum optics Lab IBM-Q Lab quantum source	quantum computation with Majorana Fermions



RO national strategy in quantum communications

- ◆ **Q1. research**
quantum research hubs
- ◆ **Q2. education and training**
quantum specialists
- ◆ **Q3. infrastructure**
intra-city q. networks, national quantum backbone, cross-border links
- ◆ **Q4. quantum industry**
components, applications, services



take home message

1. whatever you do, there's a *quantum app* for that
(to help you do it better/faster/safer)

2. quantum is coming: not *if*, but *when*

are you ready for quantum?



Thank you!

