

# cybersecurity in the quantum era

radu ionicioiu



## plan

i. the quantum threat

ii. two solutions

iii. state-of-the-art



## digitalisation: the next frontier

- ◆ digital Europe



- ◆ government cloud



## digitalisation: the next frontier

- ◆ digital Europe
- ◆ government cloud

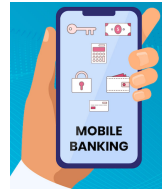


*cybersecurity is paramount*

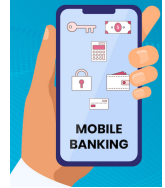




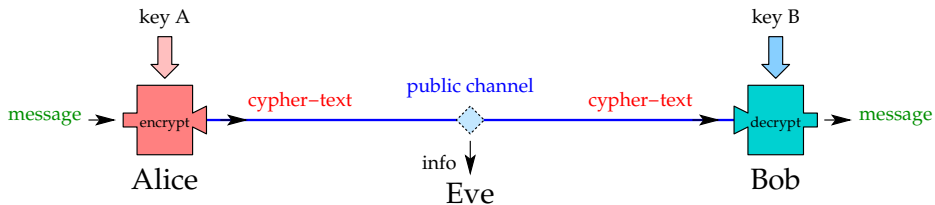
*crypto: we use it every day*



*crypto: we use it every day*



## classical crypto



♦ **symmetric:**  $key A = key B$

one-time pad (OTP), AES-256/512

♦ **asymmetric:**  $key A \neq key B$

public-key, RSA, DH

♦ authentication, digital signatures, privacy, security



the problem

*quantum computers will break internet security*

- ♦ secure communications
- ♦ authentication
- ♦ digital signatures
- ♦ critical infrastructure
- ♦ mobile networks/5G
- ♦ secure voting
- ♦ financial transactions  
mobile banking, POS, e-commerce
- ♦ software updating  
cars, computers

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



*how serious is the threat?*

# quantum computing

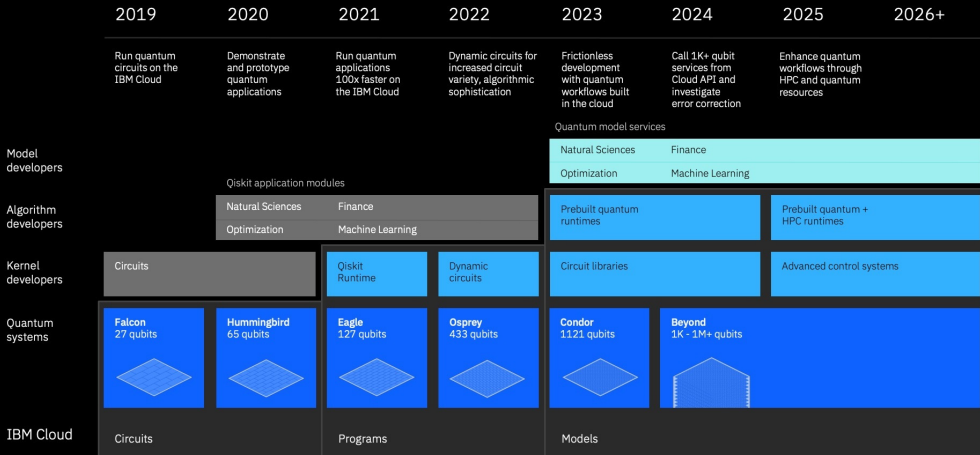
a **\$65 billion** industry by 2030



# IBM roadmap

## Development Roadmap

IBM Quantum



# 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, Canada<sup>13</sup>





*... 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)*



# PKC: status

## NOT QUANTUM SAFE



### RSA encryption

**The hard problem:**

Factoring large integers into prime numbers



### Diffie-Hellman key exchange

Solving  $g^a \bmod p = c$  for  $a$ , given  $g$ ,  $p$  and  $c$



### Elliptic curve cryptography

Finding the relation between two points on an elliptic curve

## QUANTUM SAFE



### Lattice-based crypto

Finding the nearest point in a high-dimensional lattice



### Code-based crypto

Decoding a certain kind of error-correcting code



### Hash-based crypto

Inverting a function that maps an input of arbitrary length to a fixed-length sequence

## QUANTUM SAFE?



### Multivariate crypto

*One scheme broken*

*February 2022*

Solving systems of nonlinear equations in many variables

### Isogeny-based cryptography

*One scheme broken*

*July 2022*

Finding a map that relates two elliptic curves



# NIST PQC

the finalists

- ◆ NIST: PQC selection 2017-2022

type	PKE/KEM	signature
lattice	CRYSTALS-Kyber	CRYSTALS-Dilithium FALCON
hash-based		SPHINCS+

- ◆ round 4 launched

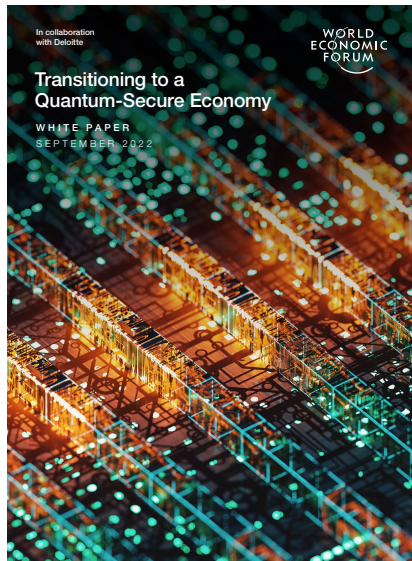


# World Economic Forum

## White Paper, September 2022

*"20 billion digital devices will need to be upgraded or replaced with post-quantum crypto in the next 20 years"*

*organizations should start planning for the transition now*



# PQC

deployed now

- ♦ **signal** protocol: enhanced by **PQC**
- ♦ protects from future threats of **quantum computers**
- ♦ **chrome**: Kyber KEM

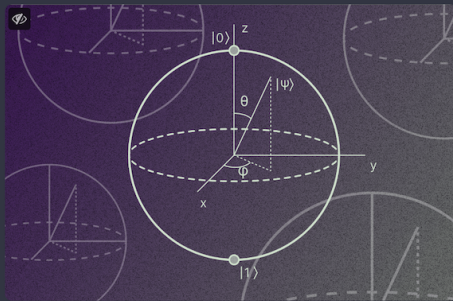


Signal

@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/](https://signal.org/blog/pqxdh/)



Sep 19, 2023 at 19:10 · 545 · 614



## 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 a quantum state  $\Rightarrow$  higher **QBER**, detectable

*Eve will be detected !*

classically impossible

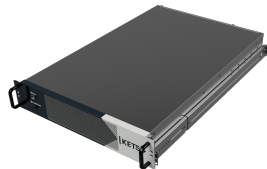




# QKD

## commercial

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



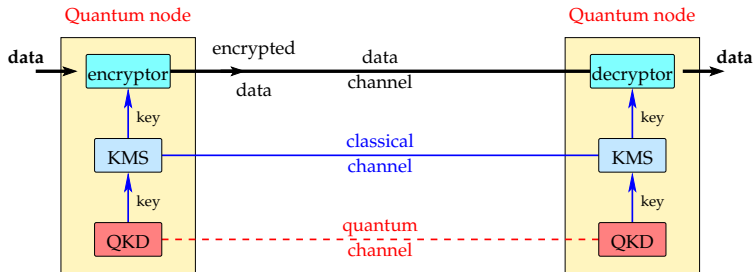
## quantum networks

QKD systems: point-to-point  $\Rightarrow$  need quantum communication networks

- ◆ 1st generation: trusted nodes
  - ▶ available now
  - ▶ low functionality: key distribution
- ◆ 2nd generation: quantum repeaters
  - ▶ challenging
  - ▶ advanced functionality: entanglement distribution, quantum internet, blind QC



## trusted quantum node



- ◆ **QKD**: establishes **secure keys** between neighbouring nodes
- ◆ **KMS**: shares keys between distant nodes
- ◆ **encryptor**: symmetric encryption (AES-256/512, OTP)



*what's going on worldwide?*

## DECLARATION ON A QUANTUM COMMUNICATION INFRASTRUCTURE FOR THE EU

### All 27 EU Member States

have signed a declaration agreeing to **work together** to explore how to **build a quantum communication infrastructure (QCI)** across Europe, boosting European capabilities in **quantum technologies, cybersecurity and industrial competitiveness.**

@FutureTechEU #EuroQCI



# QUANTUM COMMUNICATION INFRASTRUCTURE



Integrate quantum cryptography  
into critical communication systems



Combine terrestrial and satellite  
components for wide coverage



Protection of data networks, clock  
synchronization,  
e-voting,...



Backbone infrastructure  
for the quantum internet



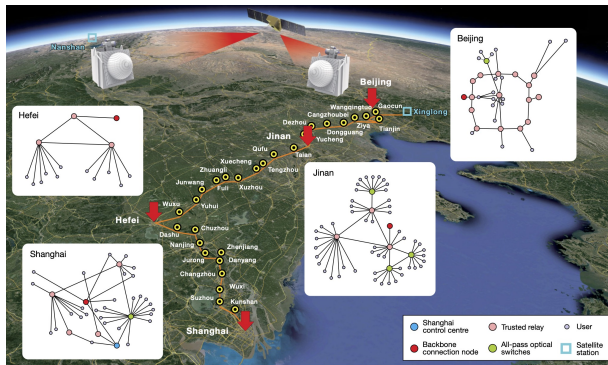


SAGA, Eagle1, Eagle2



# China

## Beijing-Shanghai quantum backbone, 2000 km ( $\simeq$ Bucharest-Brussels)

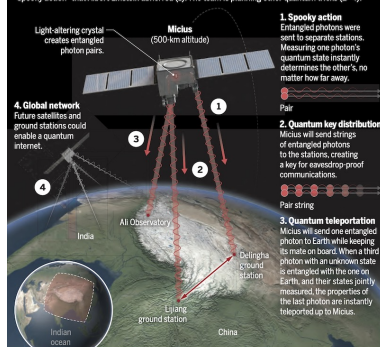


Nature **589**, 214 (2021)

Hefei: **46 nodes** intra-city quantum network

### Quantum leaps

China's Micius satellite, launched in August 2016, has now validated across a record 1200 kilometers the "spooky action" that Albert Einstein abhorred (1). The team is planning other quantum tricks (2-4).

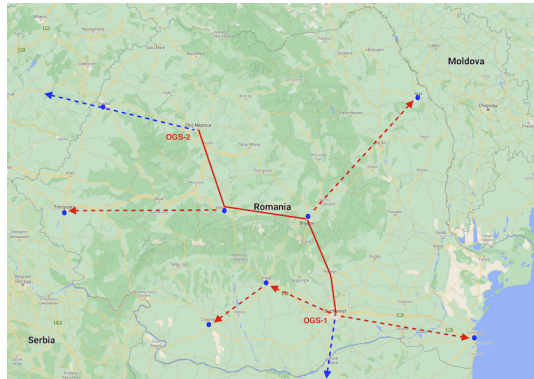


Science **356**, 1110 (2017)



*goal: develop the Romanian Quantum Communication Infrastructure*

- ◆ **Phase 1:** two intra-city q. networks: Bucharest, Cluj
- ◆ **Phase 2:** National Quantum Backbone (RoQBone): Bucharest–Cluj
- ◆ **Phase 3:** optical ground stations (OGS)
- ◆ **Phase 4:** cross-border links: HU, BG



**Phase 1,2:** Digital Europe Programme (RoNaQCI)



## RO national strategy in quantum communications

## ◆ Q1. research

quantum research hubs

## ◆ Q2. education and training

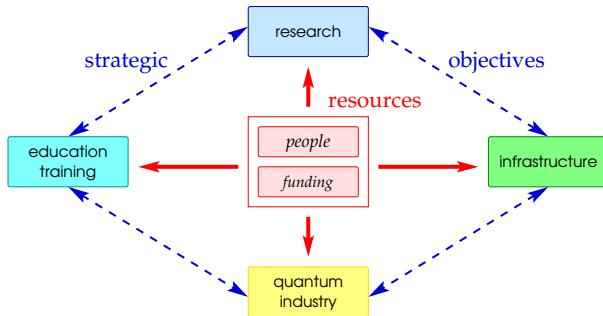
quantum specialists

## ◆ Q3. infrastructure

intra-city q. networks, national  
quantum backbone, cross-border links

## ◆ Q4. quantum industry

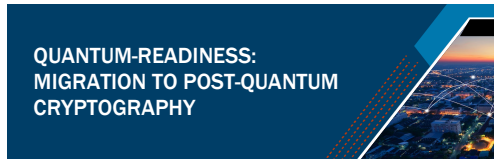
components, applications, services



what to do next?

*transition to **quantum-resistant** crypto*

- ◆ create a **quantum-readiness** roadmap
- ◆ inventory of **quantum-vulnerable** systems
- ◆ start **quantum risk assessment** processes
- ◆ replace HW, SW that use public-key algorithms with **quantum-resistant** ones



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

[www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms](http://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms)



## take home message

Q-Day is coming

*not **if**, but **when***

◆ short term: PQC

deployed now: signal, chrome, ...

◆ medium term: QKD

safer, but expensive

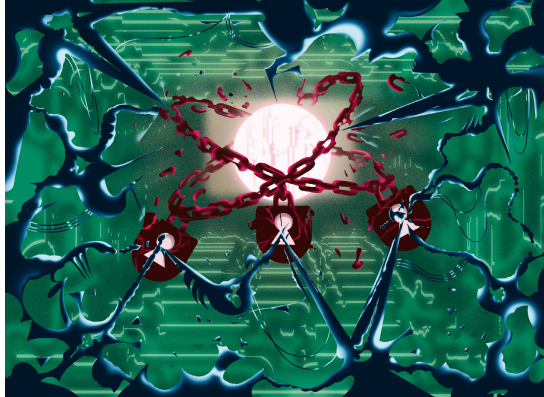
◆ long term: quantum internet

full quantum power & functionality

*prepare now, be safe later*



*are you ready?*



# PREPARING FOR Q-DAY

*thank you!*

