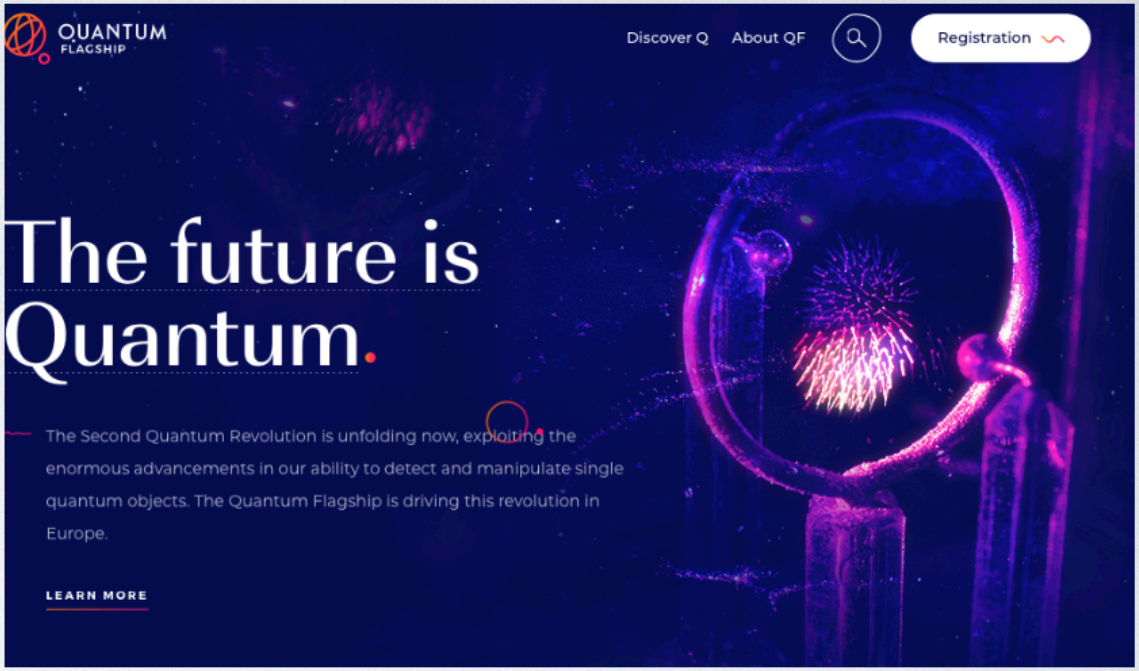
sviluppi delle scienze e tecnologie quantistiche

QUANTUM FLAGSHIP

https://qt.eu



Quantum Flagship in a nutshell.

01

1b €

Quantum Technology will be funded with at least one billion Euro by the European Commission.

02

10+ yrs

Flagship's timescale

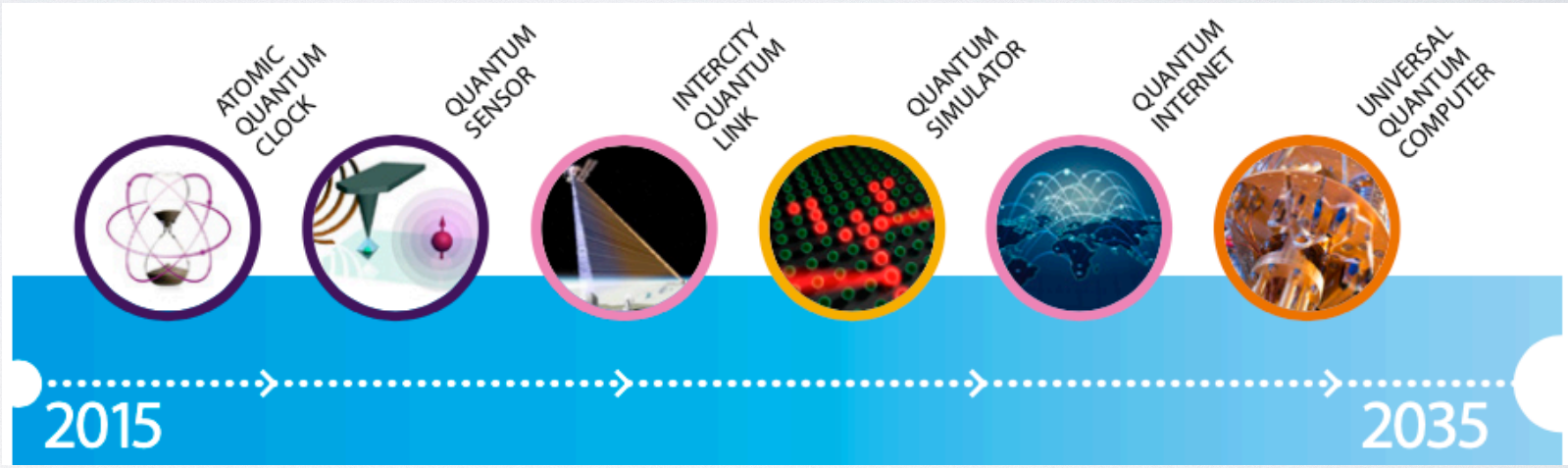
03

5000+

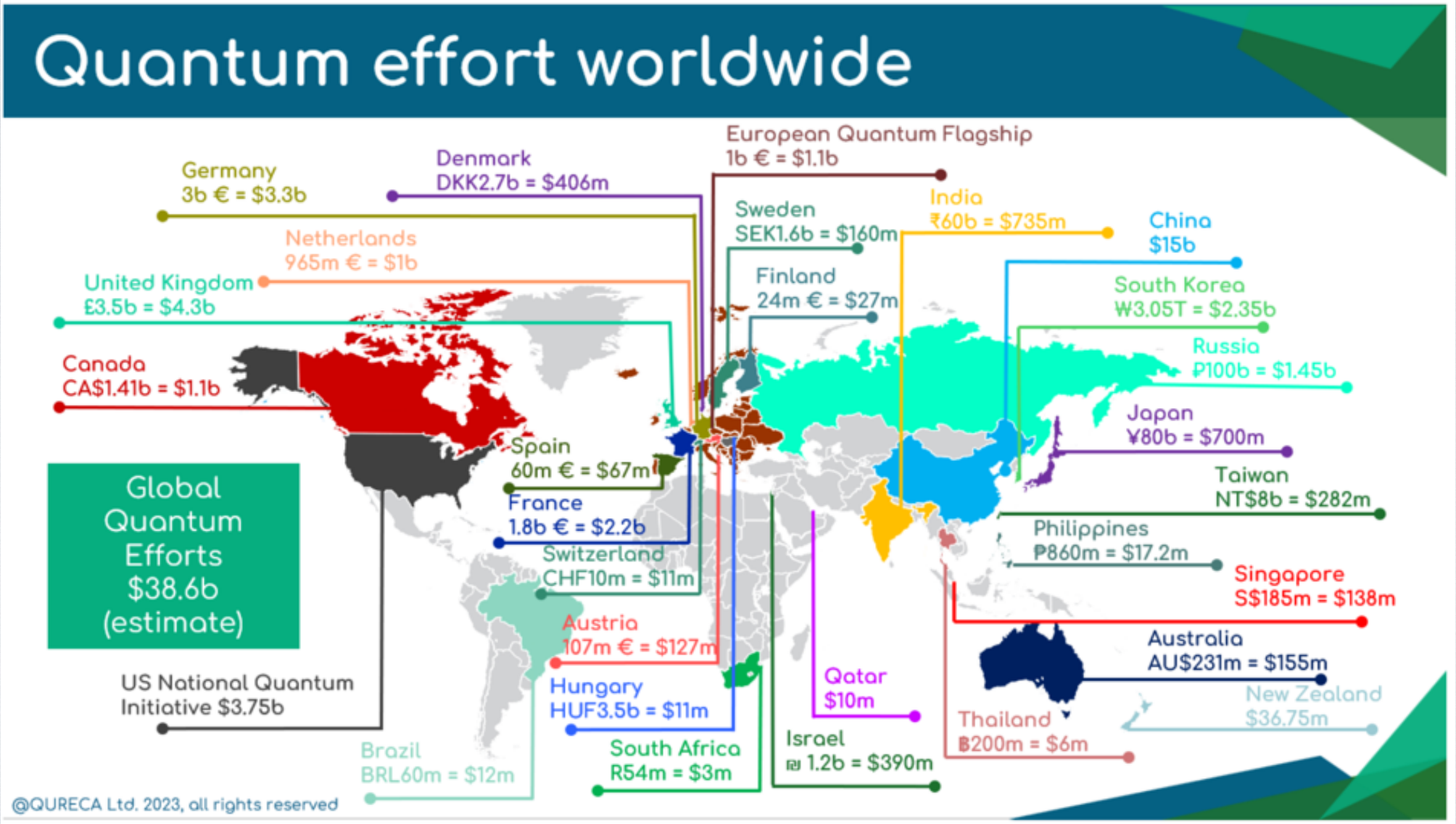
researchers residing in all EU and associated countries involved

"With quantum theory now fully established, we are required to look at the world in a fundamentally new way. ... The developments in the leading areas of quantum technologies can be expected to produce transformative applications with real practical impact on ordinary people." (Quantum Manifesto)

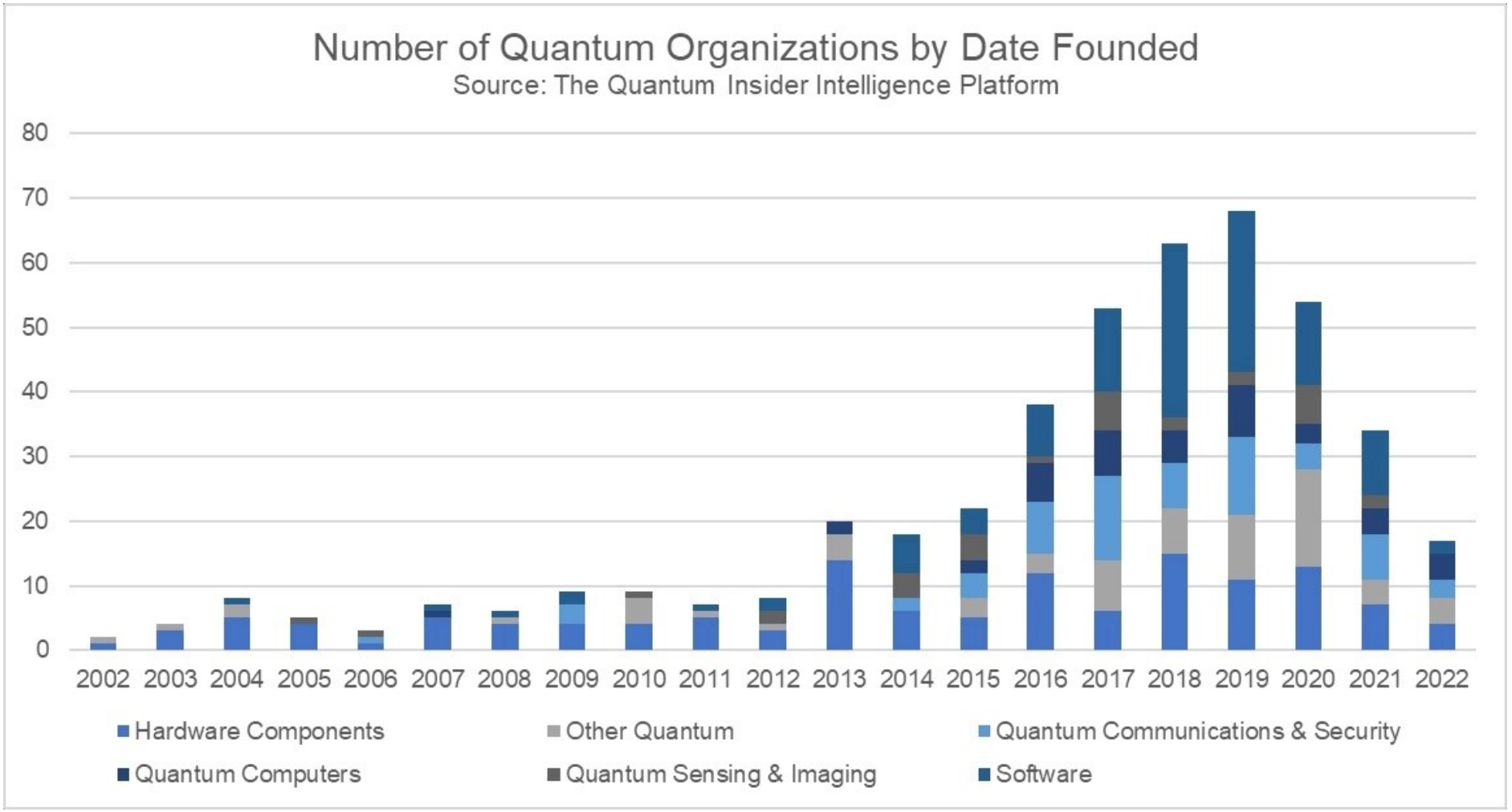
SECOND QUANTUM REVOLUTION



Quantum effort worldwide



https://thequantuminsider.com/2022/09/05/quantum-computing-companies-ultimate-list-for-2022/



TOP 10

10: Xanadu

Canadian quantum technology company Xanadu is a startup notable for exploring photonic quantum computing, which uses the quantum properties of light particles to run.

9: Toshiba

Toshiba's Quantum Key Distribution (QKD) program is working to secure network communications applying the fundamental laws of Quantum Physics.

8: Rigetti

Rigetti Computing builds and deploys integrated quantum computing systems leveraging superconducting qubit technology. These systems enable organisations to augment existing computational workflows with quantum processors.

7: Intel

Processor-maker Intel is leveraging its expertise in high-volume transistor manufacturing to develop 'hot' silicon spin-qubits, much smaller computing devices that operate at higher temperatures. Its Horse Ridge II cryogenic quantum control chip provides tighter integration, while the cryoprober enables high-volume testing that is helping to accelerate commercialisation.

6: Amazon

Amazon is building the framework for a quantum computer, advancing attempts to harness technology that can crunch huge amounts of data in seconds.

5: QCI

With a goal of delivering ready-to-run quantum systems that accelerate and simplify the adoption of quantum computing. Quantum Computing Inc (QCI) is on a mission to accelerate the value of quantum computing for real-world business solutions.

4: D-Wave

D-Wave systems use a process called quantum annealing to search for solutions to a problem.

3: Google

Google Quantum AI is advancing the state of the art of quantum computing and developing the tools for researchers to operate beyond classical capabilities.

2: Microsoft

For decades, Microsoft has been doing basic quantum physics research to solve some of society's largest, most complex challenges.

Microsoft has all the building blocks of a topological qubit—a new and unique qubit that will be faster, smaller, and more reliable than other qubits. In time, topological qubits will power Microsoft's fully scalable, highly secure, next-generation quantum computer.

1: IBM

Since becoming the first to offer cloud-based quantum computing access, IBM is continuing to release new versions of its quantum computing technologies.

It plans to release a 433-qubit processor called Osprey this year, with a 1,121-qubit processor called Condor to succeed it in 2023.

START UPs

in Europe

https://tech.eu/2023/05/19/10-european-quantum-computing-startups-that-approaching-superposition/

+ many other that are spin-off of academic projects

QUANTUM FLAGSHIP

https://qt.eu/

Explore the Quantum Principles

Basic Science

Basic Science

The area of Basic Science covers the research and development of basic theories and future ...

LEARN MORE

Communication

Communication security by quantum-safe cryptography is of strategic importance to consumers, ...

LEARN MORE

Computing

Quantum computation is among the most far-reaching and challenging goals of quantum technologies.

LEARN MORE

Sensing & Metrology

Quantum imaging devices can greatly improve imaging technologies.

LEARN MORE

Simulation

Quantum simulators based on the laws of quantum physics will allow us to overcome the shortcomings ...

LEARN MORE

Quantum Computing Infrastructure

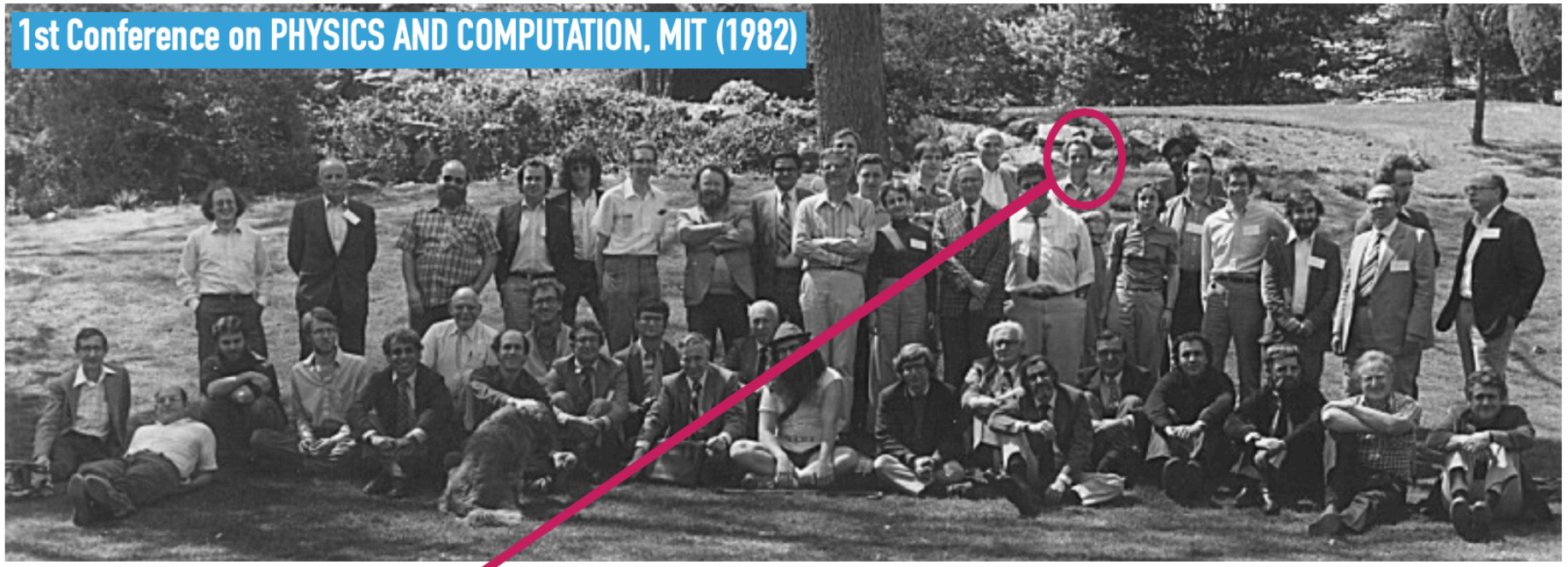
LEONARDO
CINECA

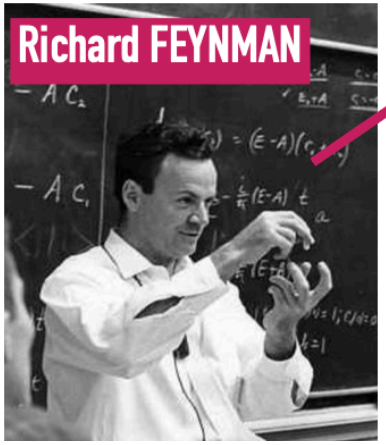
- **EuroQCS-Italy**: Hosted at CINECA in Italy, EuroQCS-Italy will **be integrated into the EuroHPC pre-exascale supercomputer** Leonardo. The consortium aims to develop a quantum computer **based on neutral atom qubits**, contributing to the advancement of quantum technologies in Europe.

https://leonardo-supercomputer.cineca.eu/eurohpc-quantum-computers/

i paradigmi della computazione quantistica

QUANTUM COMPUTER





"Nature isn't classical, dammit, and if you want to make a simulation of nature, you'd better make it quantum mechanical, and by golly it's a wonderful problem, because it doesn't look so easy."
(Richard Feynman, 1982)

MANY PLATFORMS

- Superconducting Qubits
- Neutral atoms
- Ions
- Photons
- NV Centers
- NMR
- ...

MANY TOOLS

- Quantum Programming:

QuTiP, Quipper, ...

- Quantum Emulators:

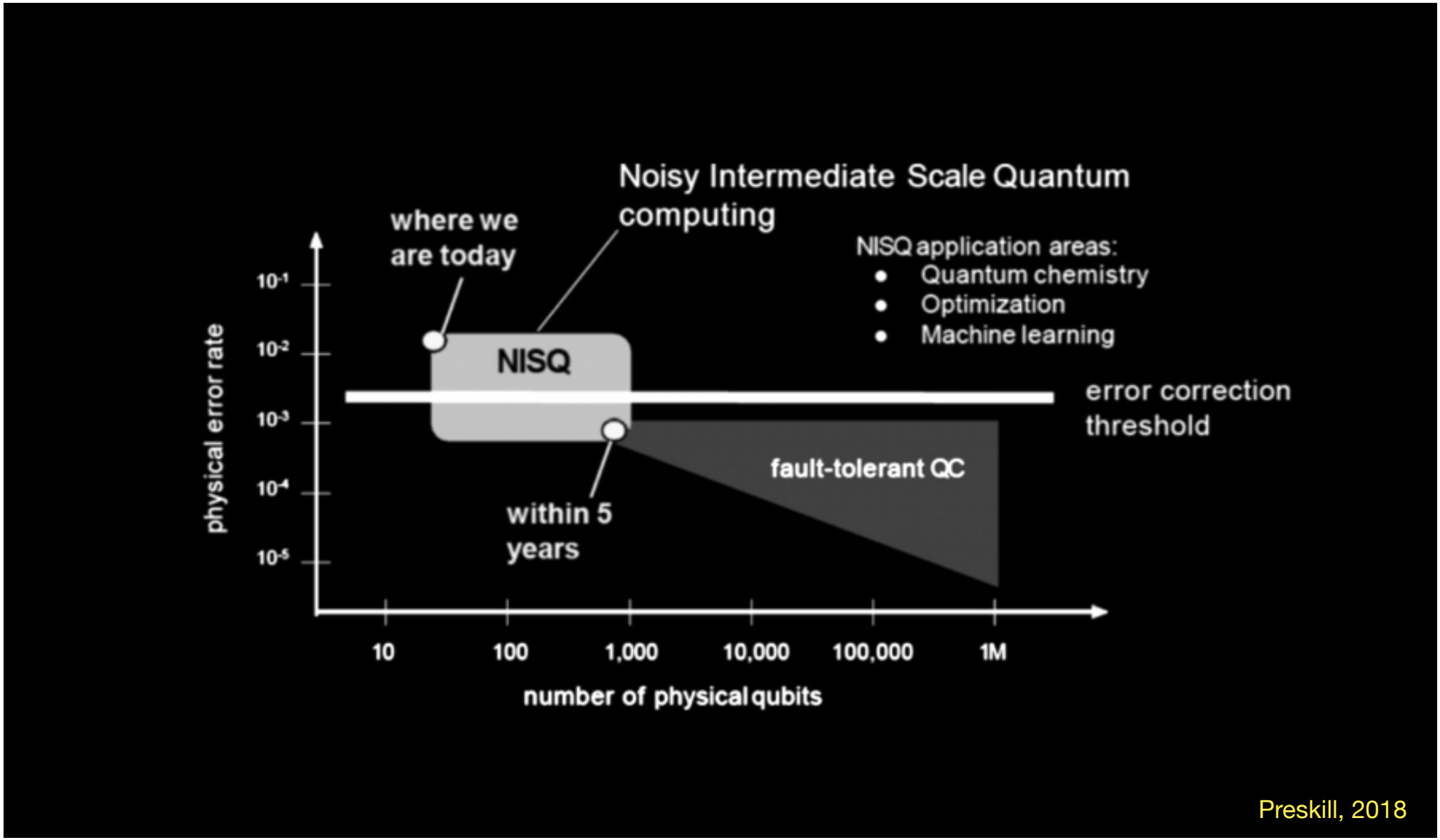
IBM Qiskit, Google Cirq, Pascal Pulser, D-wave Ocean, ...

- Quantum hardware in cloud:

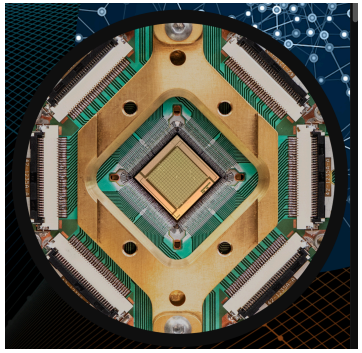
IBM, D-wave, (Pasqal/QuEra) ...

- Quantum SDK

software development kit


Noisy Intermediate Scale Quantum computing
where we are today
NISQ application areas:
Quantum chemistry
Optimization
Machine learning
NISQ
error correction threshold
fault-tolerant QC
within 5 years
physical error rate
10^{-1}
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10
100
1,000
10,000
100,000
1M
number of physical qubits
Preskill, 2018

D-WAVE



Superconducting
Qubits

5000+ qubits
1 Mlilion variables
100s applications

Quantum Development
Tools: Ocean in cloud

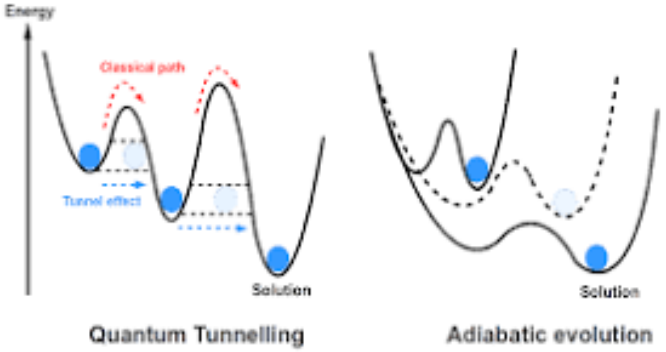
QUANTUM ANNEALING

can solve only
search/optimization problems

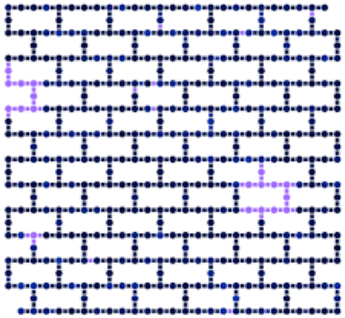
encode the solution as the minimum
of a quantum hamiltonian

the Hilbert space is search using
an adiabatic algorithm

quantum advantage: q-tunneling



IBM-Q



Superconducting
Qubits

Eagle: 127 (free)
Ospray: 433
Condor: 1121
(announced)

Development Tools:
IBM Quantum Lab

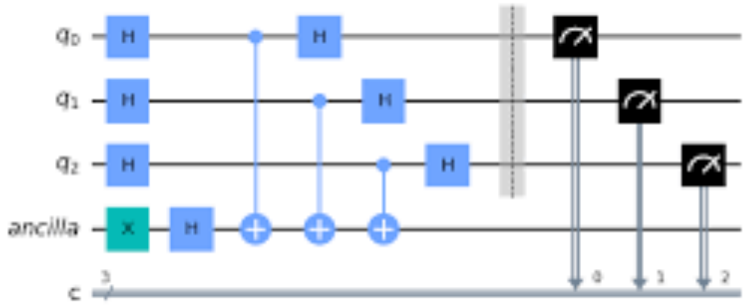
DIGITAL QC

algorithm as sequence of logic gates

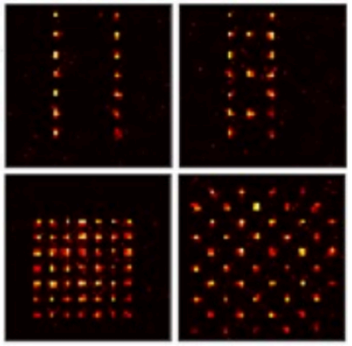
universality:
single qubits gates + CNOT

error mitigation
error correction

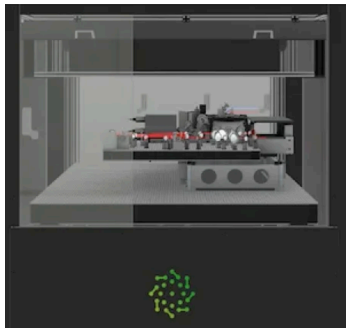
quantum advantage:
on 127 with error mitigation



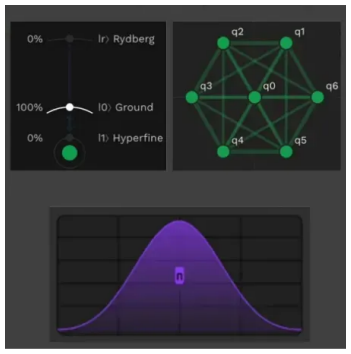
PASQAL



Rydberg atoms
variable geometry



variable (lab)
Fresnel: 100
(commercial)
2023: 324



Development Tools:
Pulser Studio (free)
100+ Emulator

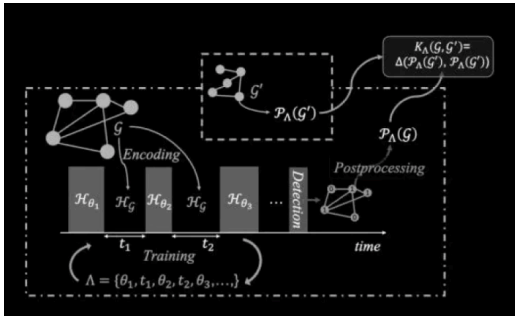
ANALOG QC

algorithm as sequence of
global transformations

non-universal
very efficient in complex systems

local pulses
error correction

quantum advantage: ??
topological flexibility



Open access to platform:
simulations and/or real hardware
tutorials
…

IBM: QISKIT https://www.ibm.com/quantum/qiskit

DWAVE: OCEAN https://www.dwavesys.com/solutions-and-products/ocean/

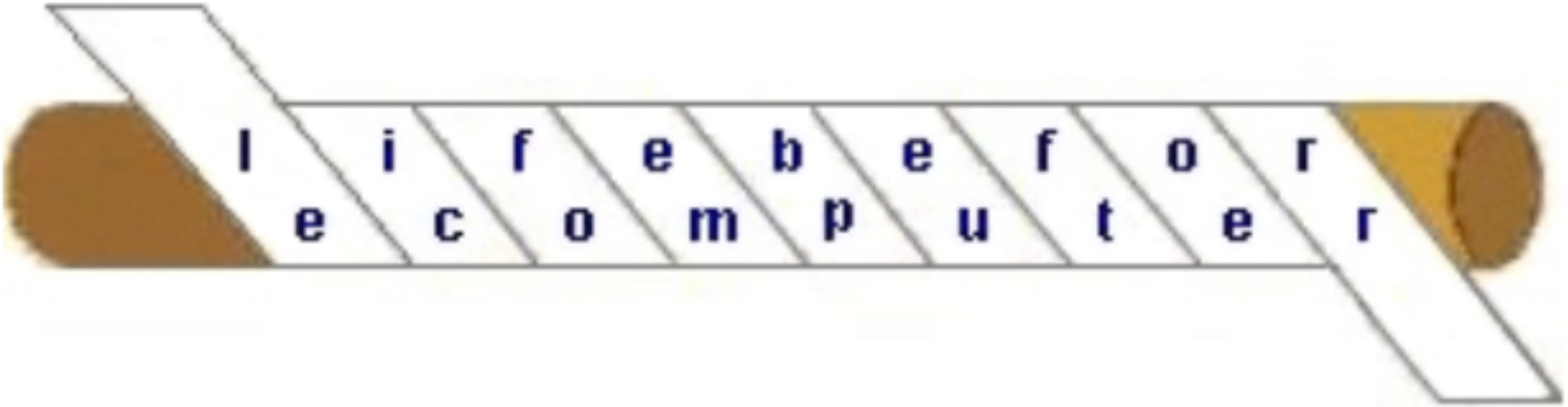
PASQAL: PULSER https://www.pasqal.com/solutions/pulser-studio

crittografia

CRITTOGRAFIA - il codice segreto

alcuni esempi storici

Scitala lacedemone (900 ac)



Il codice di Giulio Cesare:

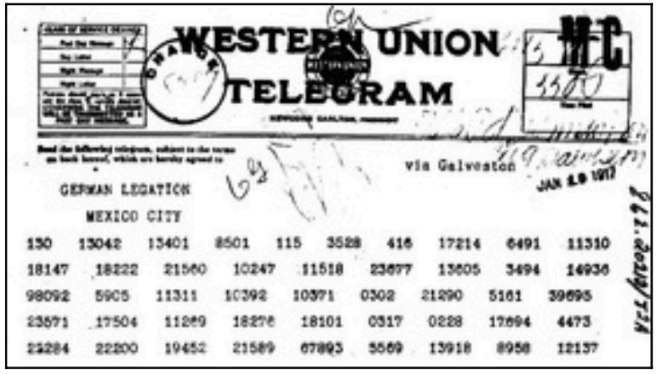
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P

Esercizio: YBELUGKQDJKC

Caratteristiche:

- sia chi spedisce che chi riceve deve conoscere la “chiave”

- se qualcuno intercetta la “chiave”, è in grado di decifrare i messaggi



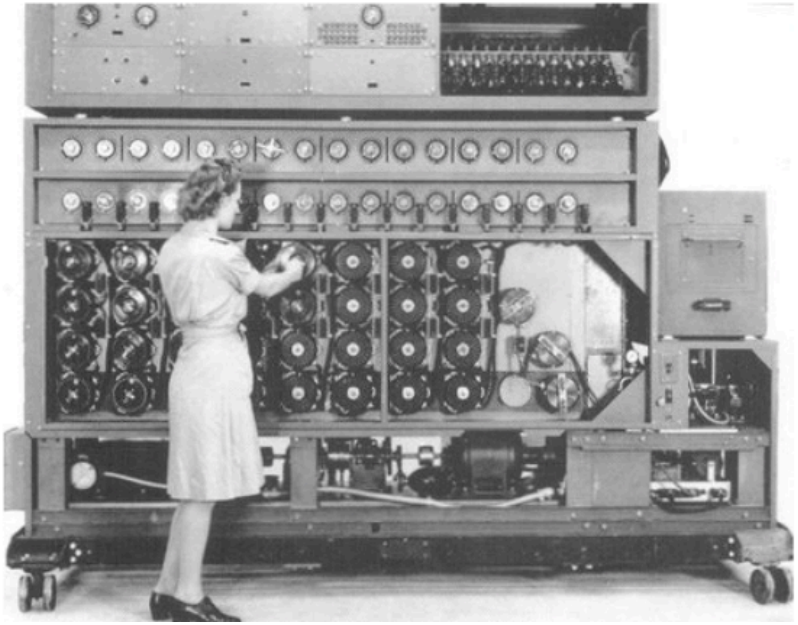
ENIGMA (II guerra mondiale)

macchina di codifica dell'esercito tedesco:

modello M3 ha 159×10^{18} combinazioni

https://www.101computing.net/enigma-machine-emulator/

https://www.101computing.net/turing-welchman-bombe-simulator/



TURING-WELCHMAN BOMBE

Stazione X (Bletchley Park, UK)

1945, più di 10000 persone il cui lavoro era interamente dedicato alla decodifica dei messaggi tedeschi; team dei matematici era diretto da Alan Turing

```
eb 04 af c2 bf a3 81 ec  00 01 00 00 31 c9 88 0c
0c fe c1 75 f9 31 c0 ba  ef be ad de 02 04 0c 00
d0 c1 ca 08 8a 1c 0c 8a  3c 04 88 1c 04 88 3c 0c
fe c1 75 e8 e9 5c 00 00  00 89 e3 81 c3 04 00 00
00 5c 58 3d 41 41 41 41  75 43 58 3d 42 42 42 42
75 3b 5a 89 d1 89 e6 89  df 29 cf f3 a4 89 de 89
d1 89 df 29 cf 31 c0 31  db 31 d2 fe c0 02 1c 06
8a 14 06 8a 34 1e 88 34  06 88 14 1e 00 f2 30 f6
8a 1c 16 8a 17 30 da 88  17 47 49 75 de 31 db 89
d8 fe c0 cd 80 90 90 e8  9d ff ff ff 41 41 41 41
```

Questo è il test online da risolvere per essere assunti come analisti al G.C.H.Q. (Quartier Generale Comunicazioni) inglese. Volete provare?

Nel caso riusciste a risolverlo apparirà questa schermata: è un lavoro duro per gente motivata, ma gli stipendi sono altissimi!

La crittografia a CHIAVE PUBBLICA:

- sistema asimmetrico che consta di due chiavi diverse, una pubblica per cifrare e una segreta per decifrare
- la chiave pubblica è un intero del tipo n=p*q, dove p e q sono due numeri primi
- la chiave segreta è legata al valore di uno dei due fattori

Sicurezza del protocollo si basa sul fatto che per trovare la chiave segreta è necessario conoscere i due fattori p e q: questo richiede un tempo lunghissimo per un computer

RSA-768 =
123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3

computer tipico: 10^{115} istruzioni elementari, CPU a 10 miliardi operazioni al secondo -> 10^{97} anni

rete di computer dedicata: fattorizzato nel 2009 dopo due anni di calcolo

un quantum computer? qualche giorno/ora!

se avessimo un quantum computer

I NOSTRI DATI SAREBBERO IN PERICOLO?

Febbraio 2016, National Security Agency USA ha lanciato un allarme,

invitando a usare chiavi più robuste

SI

ma . . .

la fisica quantistica fornisce anche un nuovo protocollo per

rendere sicure le nostre trasmissioni

CRITTOGRAFIA QUANTISTICA

Protocollo BB84

CRYPTO 1984: Advances in Cryptology pp 475-480 | Cite as

An Update on Quantum Cryptography

Authors | Authors and affiliations

Charles H. Bennett, Gilles Brassard

Protocollo BBM92

Milestone

Quantum cryptography without Bell's theorem

Charles H. Bennett, Gilles Brassard, and N. David Mermin
Phys. Rev. Lett. **68**, 557 – Published 3 February 1992

https://www.st-andrews.ac.uk/physics/quvis/

Quantum Cryptography (BB84 photons, BB84 spin)
Quantum Cryptography (B92)
☑ Quantum Cryptography (BBM92)