La nueva criptografía

Antonio Acín
ICREA Professor at ICFO-Institut de Ciencies Fotoniques, Barcelona
AXA Chair in Quantum Information Science

Col·legi Oficial d'Enginyers Industrials de Catalunya, Barcelona, 14 May 2019

ICFO

ICFO at a glance

- Born in 2002
- 400 People
- 26 Research Groups
- 14000 m^2
- 60 Research labs
- Mediterranean Technology Park, Castelldefels, Spain
- Programs: Info, Health, Energy
- Facilities: NanoFab, AdvEng, AdvImaging, BioLab, …
- ICFO+, ICFOnians, ICFO Young Minds, …
- Mission: Research, Grad Education & KTT
- 50+Nature family pubs; 30 ERCs; 6 spin-off companies

QUANTUM AT ICFO

ICFO researchers are at the forefront of a growing scientific community that is working to understand and harness the power of quantum phenomena in order to usher in revolutionary new quantum technologies and applications.

- ✓ 14 groups (11 experimental/ 3 theory)
- ✓ 150 researchers
- ✓ 14 ERC grants
- ✓ Quantum Info Axa Chair
- ✓ Participation in 7 projects of the QT Flagship (2 as coordinators)
- ✓ > 50 Nature-group papers
- ✓ A broad range of prototypes
- ✓ Multiple industrial collaborations
- ✓ Participation in Quantum ESA projects
- ✓ QuSide
- ✓ Learn more at http://quantumtech.icfo.eu

QUANTUM AT ICFO

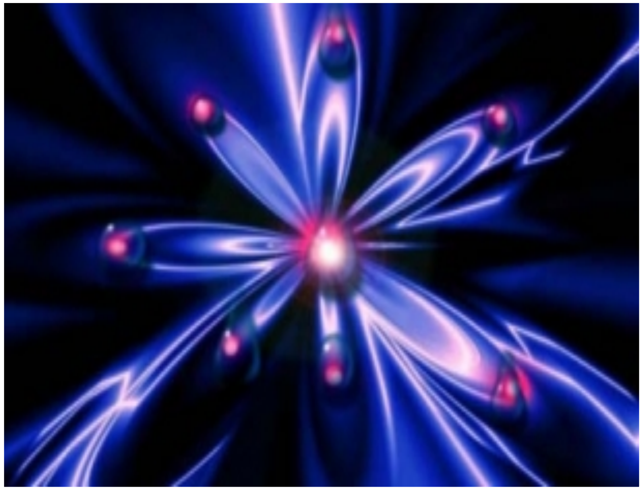
Quantum discoveries at ICFO are at the very forefront of today's research on quantum technologies.

- Quantum Communications
- Quantum Machine Learning & Quantum Algorithms
- Quantum Encryption
- Quantum Sensors
- Quantum Simulators
- High performance/Cloud Computing & experiments

Basics of quantum physics

Quantum physics

What happens when we move to the microscopic world?

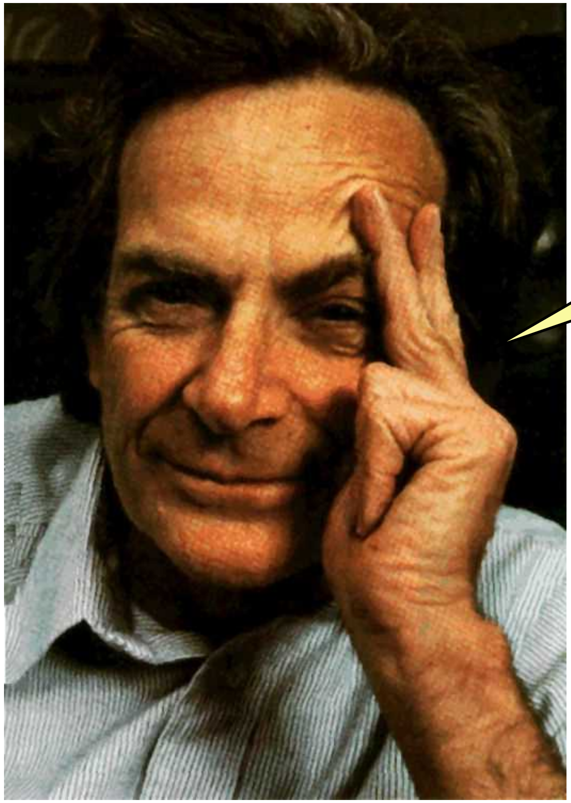


Newtonian Physics

Quantum Physics

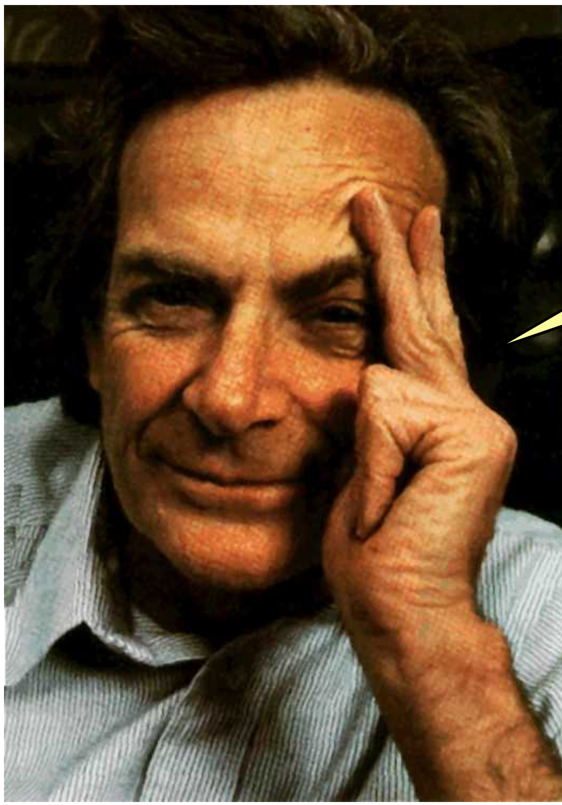
Quantum physics was created at the beginning of the XX century to explain several experiments at the microscopic scale. It radically changed our understanding of nature.

Warning!



I can safely say that nobody understand quantum physics.

Warning!



I can safely say that nobody understand quantum physics.

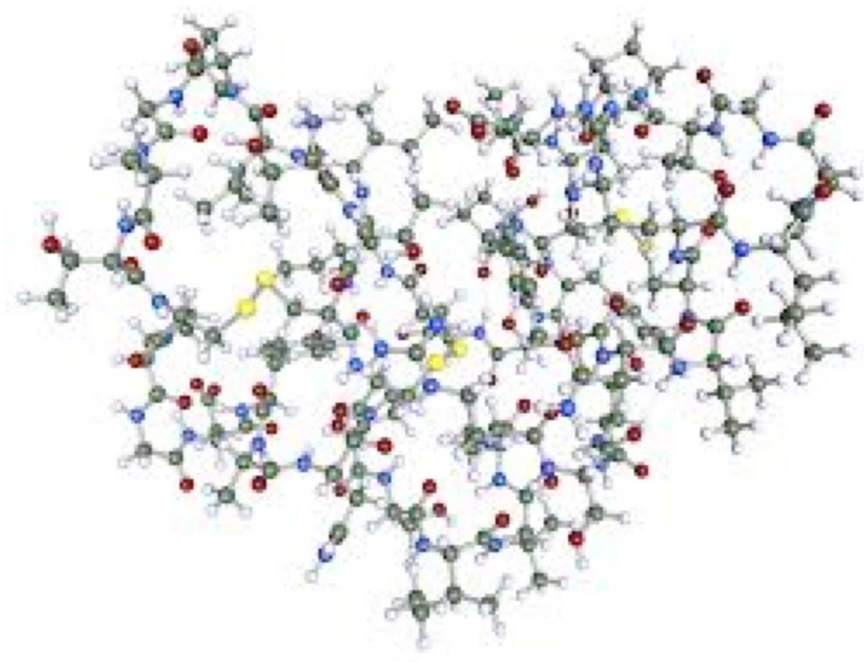
Richard Feynman
Nobel Prize in Physics (1965)

Basics of quantum physics

First postulate: to each physical system it is associated a complex Hilbert (vector) space. The state of the system is completely described by a normalized vector $|\psi\rangle$ in this space. And every vector in the space is a possible valid state of the system.

Basics of quantum physics

First postulate: to each physical system it is associated a complex Hilbert (vector) space. The state of the system is completely described by a normalized vector $|\psi\rangle$ in this space. And every vector in the space is a possible valid state of the system.

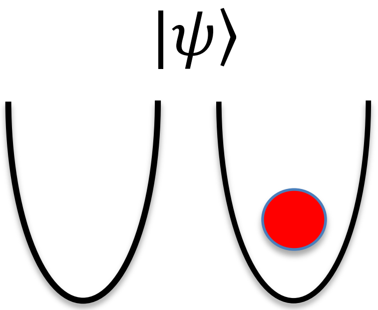


$$|\psi\rangle = \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix} \in C^d$$

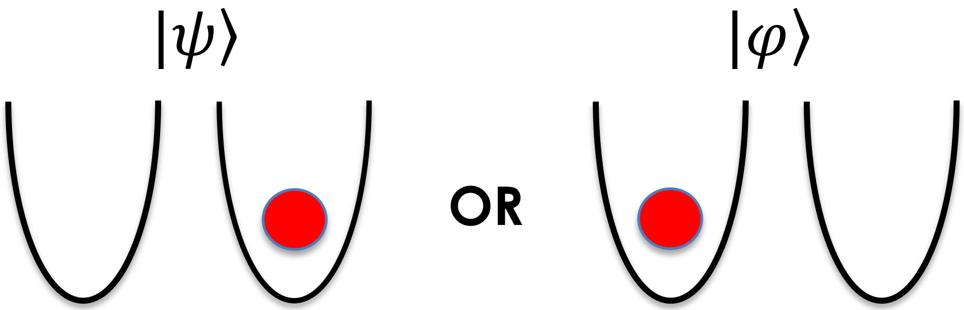
$$\lambda_j = a_j + ib_j$$

$$|\lambda_1| + \cdots |\lambda_d| = 1$$

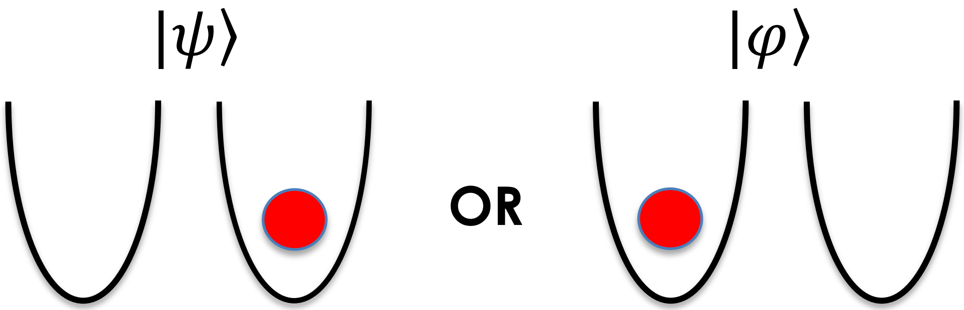
Quantum superpositions



Quantum superpositions



Quantum superpositions

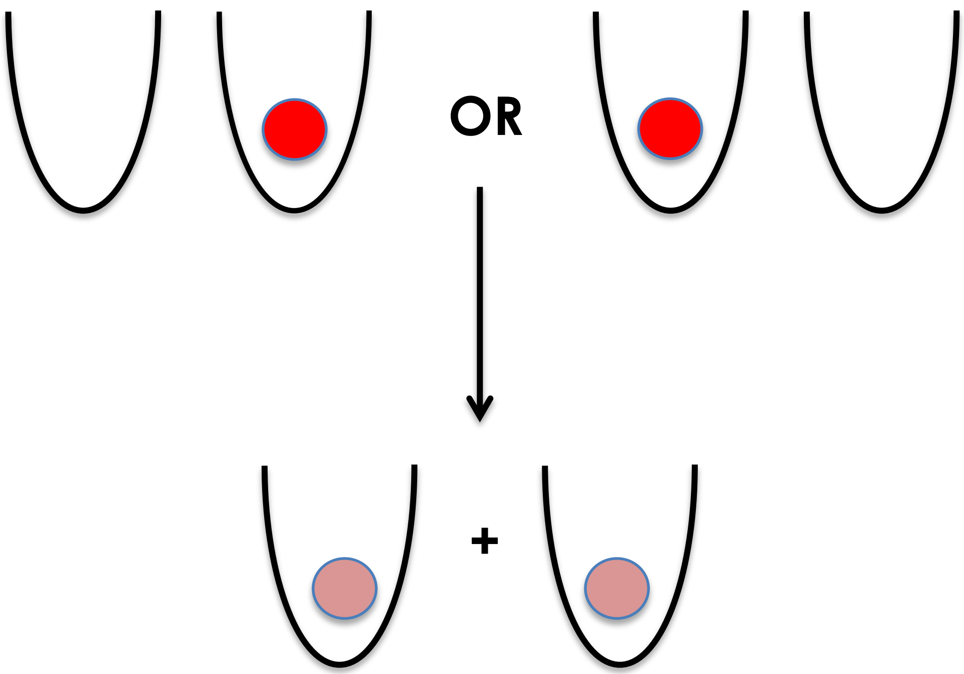


Vector spaces: the linear combination of two vectors is a new vector → a valid state of my physical system!

Quantum superpositions

A quantum system can be in a superposition of two states.

$|\psi\rangle$ $|\varphi\rangle$

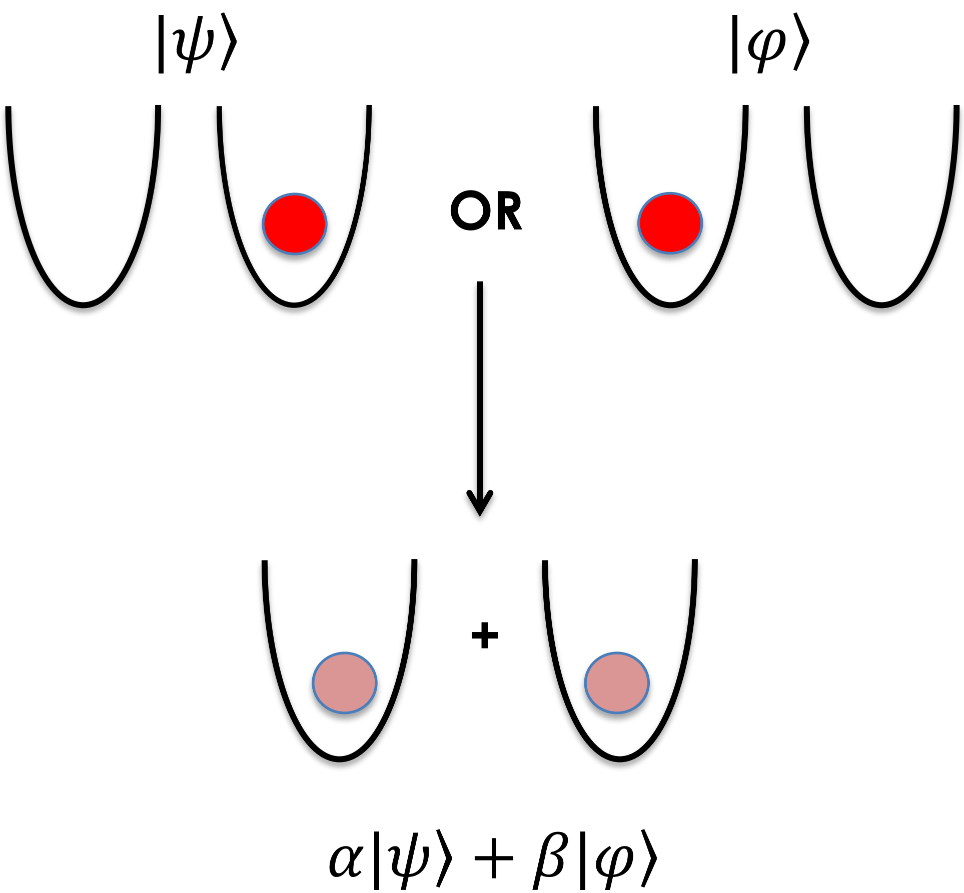


$$\alpha|\psi\rangle + \beta|\varphi\rangle$$

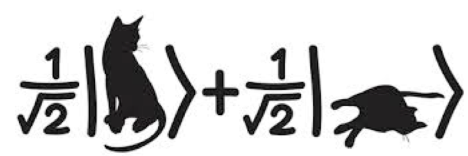
Vector spaces: the linear combination of two vectors is a new vector → a valid state of my physical system!

Quantum superpositions

A quantum system can be in a superposition of two states.

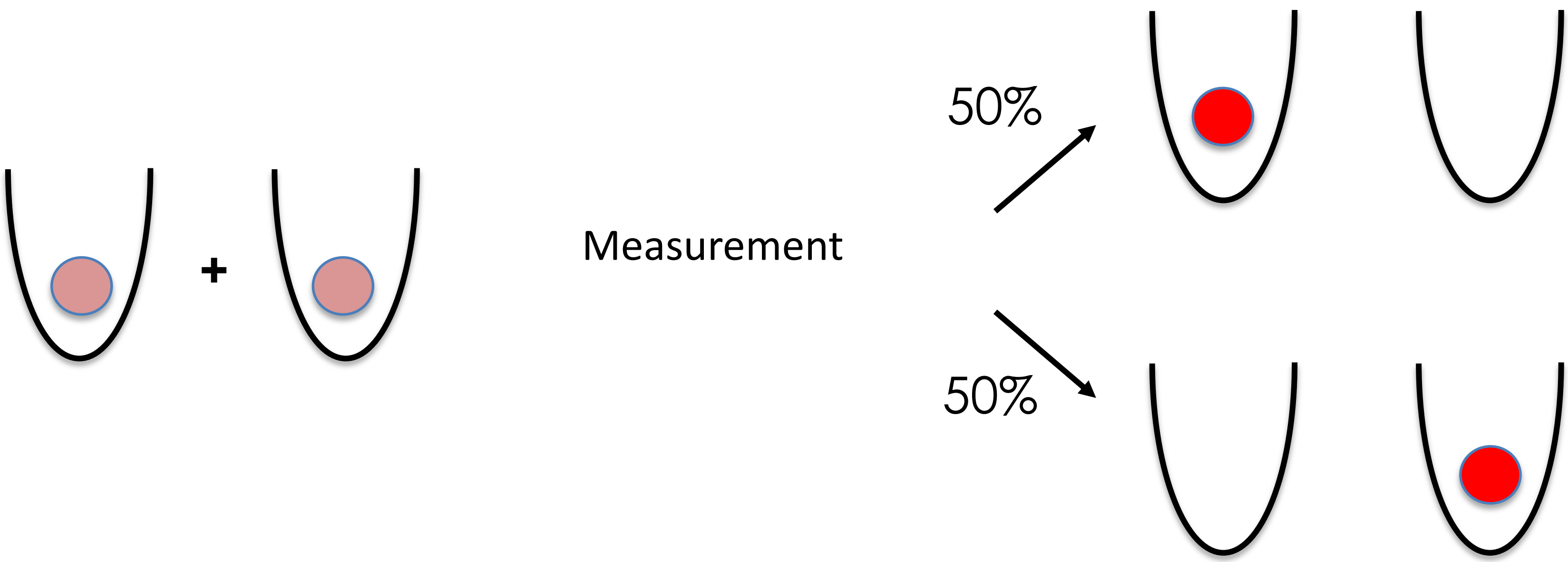


Schrodinger's cat

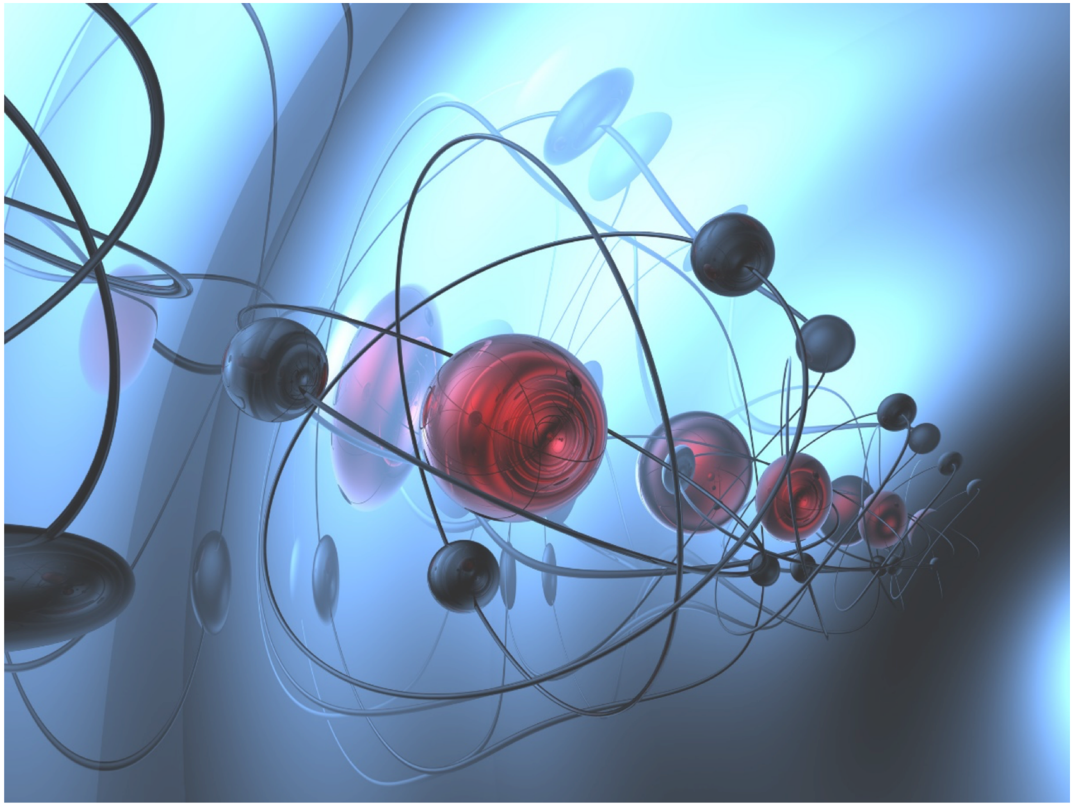


Uncertainty principle

When a system is measured, its state is perturbed.

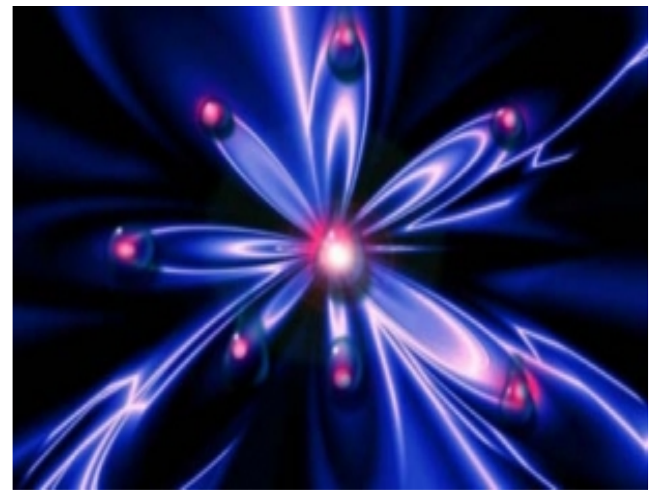


You may like it or not but… Quantum physics is everyday tested in many different labs worldwide. It is the theory that correctly describes the microscopic world, made of atoms, photons,…



Quantum physics

What happens when we move to the microscopic world?



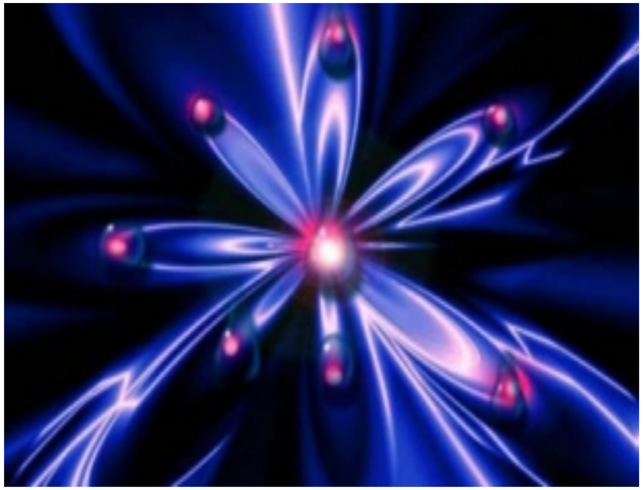
Newtonian Physics

Quantum Physics

Quantum physics was created at the beginning of the XX century to explain several experiments at the microscopic scale. It radically changed our understanding of nature.

Quantum information theory

What happens when we move information to the quantum world?



Classical information theory

Quantum information theory

The second quantum revolution: we are experiencing a similar process now in the context of information technologies.

Quantum information theory

Quantum physics: formalism that describes nature at the microscopic scale.

(Einstein, Planck, Bohr, Schrödinger, Heisenberg,…, first half of XX century).

↔

Information theory: set of laws describing how to transmit and process information.

(Shannon, 1950).

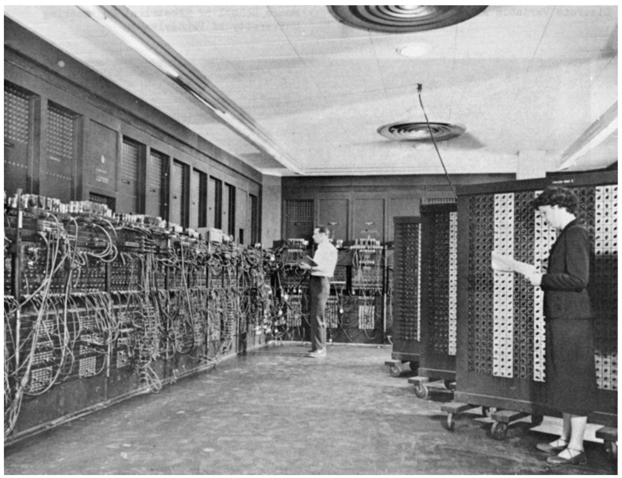
Why now?

Why now?

We have at our disposal techniques to control the quantum world.

Particle control in a quantum world
Serge Haroche and David J. Wineland have independently invented and developed methods for measuring and manipulating individual particles while preserving their quantum-mechanical nature, in ways that were previously thought unattainable.

Information technologies

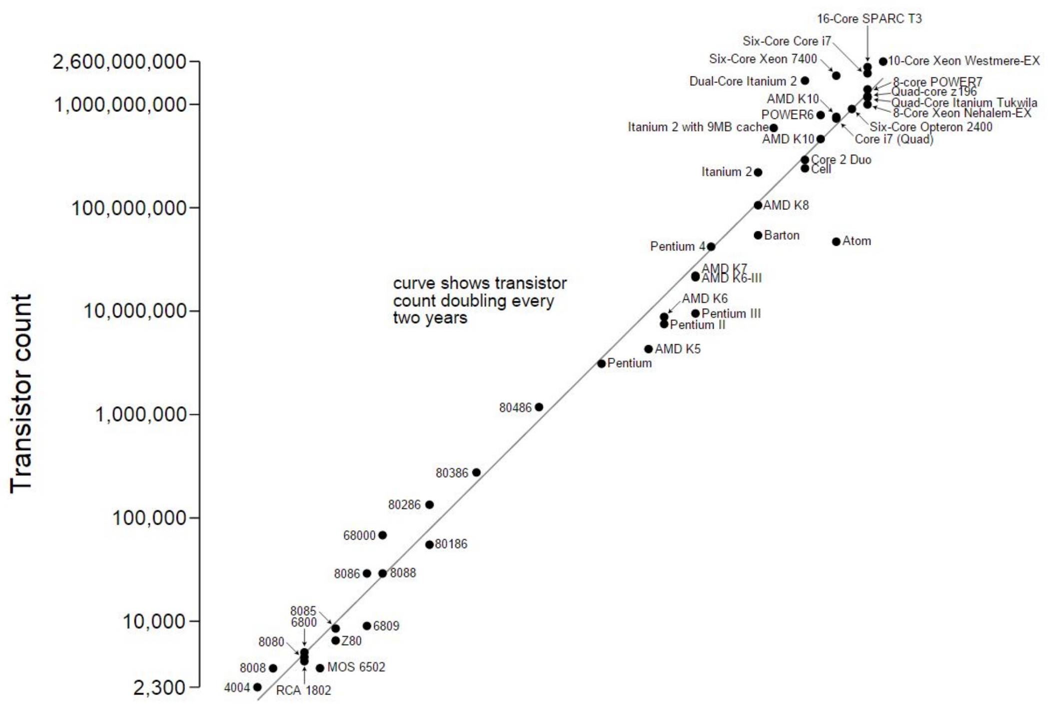


The unstoppable progress in miniaturization has brought us to the scenario in which information is stored on quantum particles (atoms or photons, for example).

Moore’s law

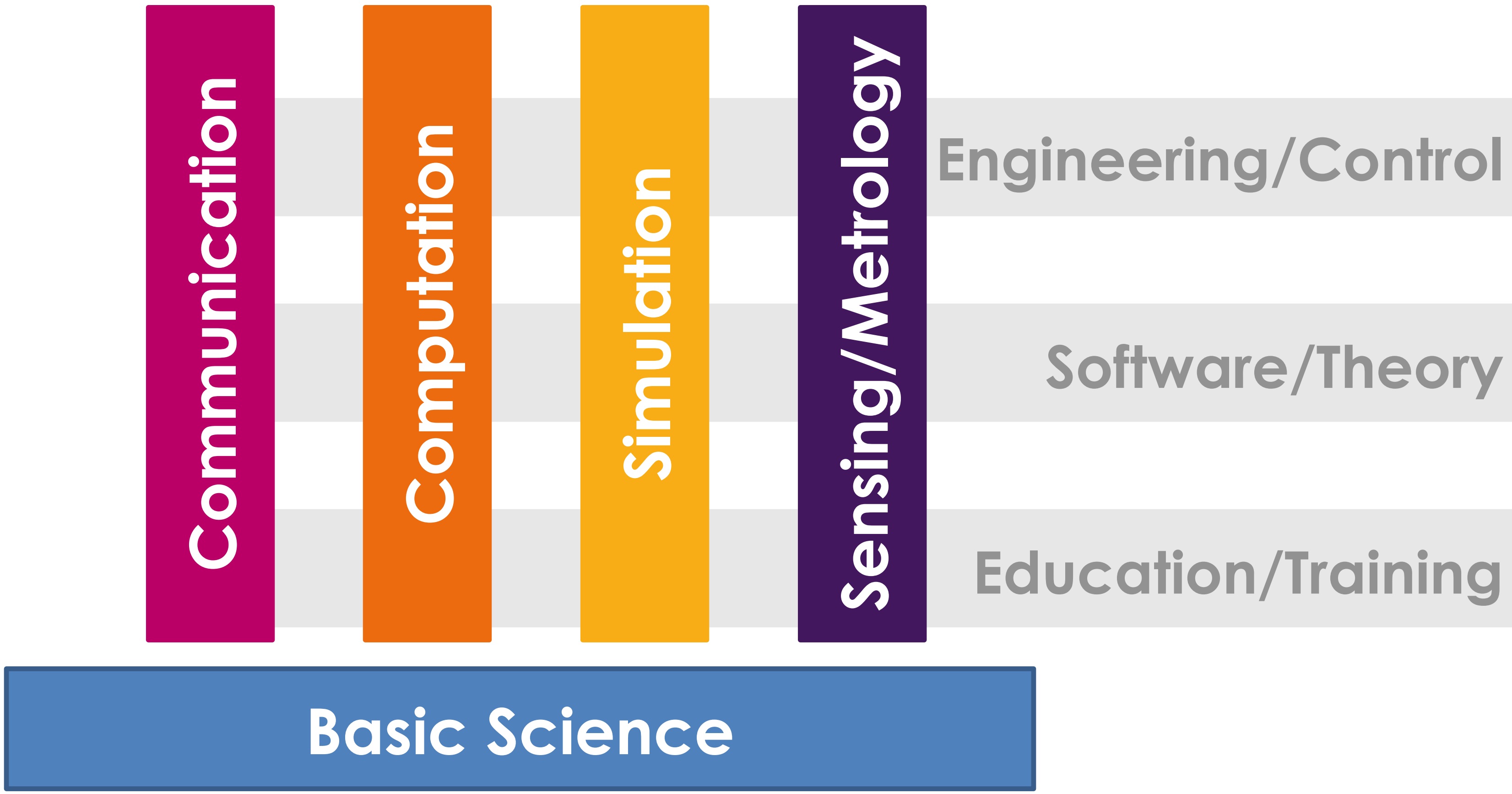
Moore's law is not a law but an observation: the number of transistors in an integrated circuit doubles about every two years. The observation is named after Gordon Moore, former CEO of Intel, whose 1965 paper described a doubling every year in the number of components per integrated circuit. Source: Wikipedia.

Microprocessor Transistor Counts 1971-2011 & Moore's Law



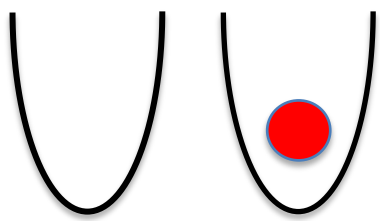
EU Flagship on Q Technologies

1 billion in 10 years



The quantum bit (qubit)

$$|0\rangle$$

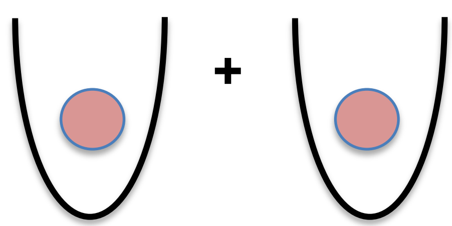


The quantum bit (qubit)

$|0\rangle$ $|1\rangle$

The quantum bit (qubit)

$|0\rangle$ $|1\rangle$

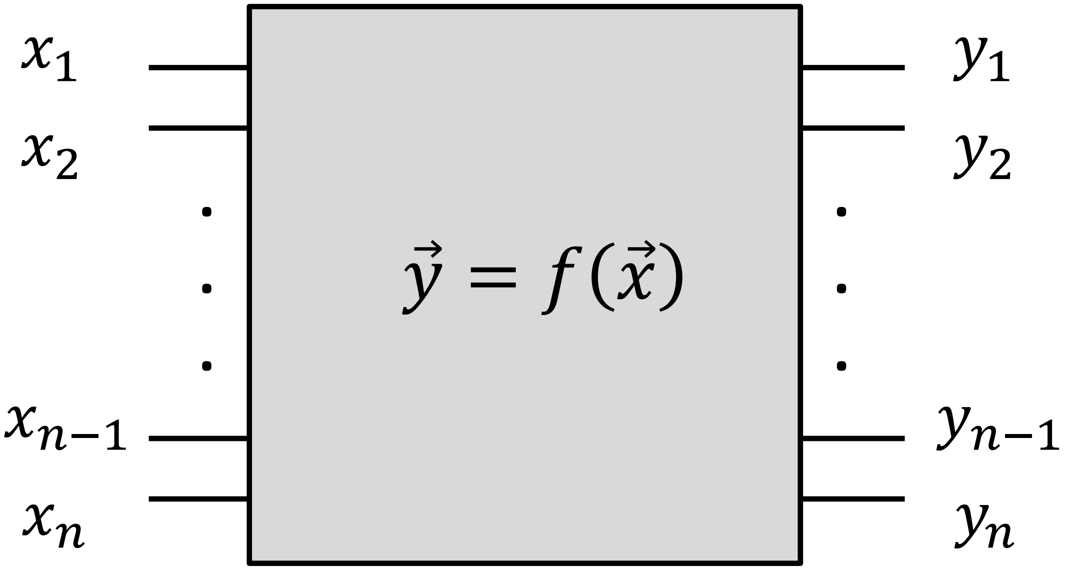


Qubits can be in superposition states.

$$\alpha|0\rangle + \beta|1\rangle$$

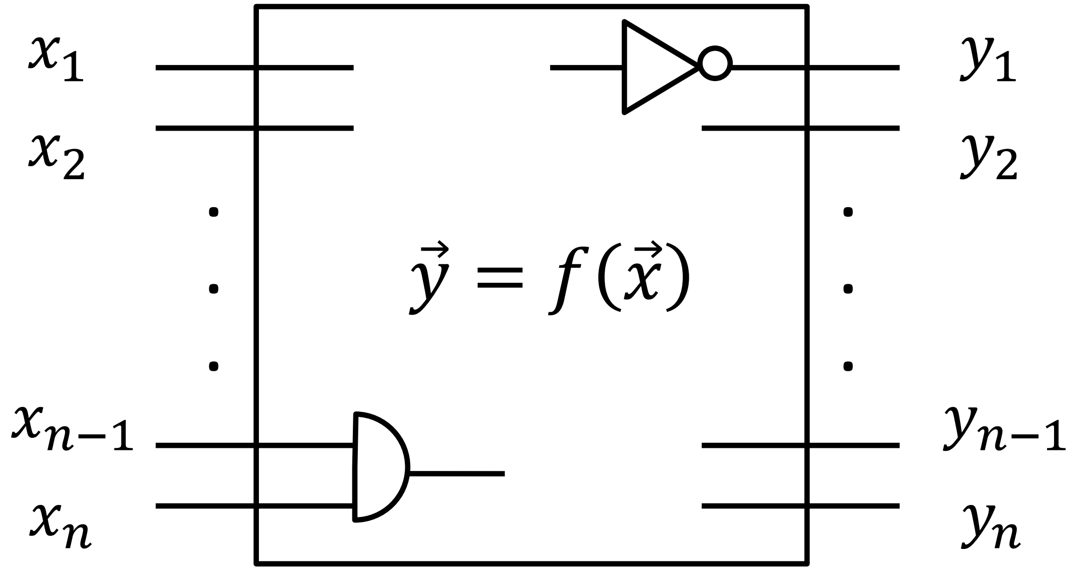
Quantum computation

Classical computer



Quantum computation

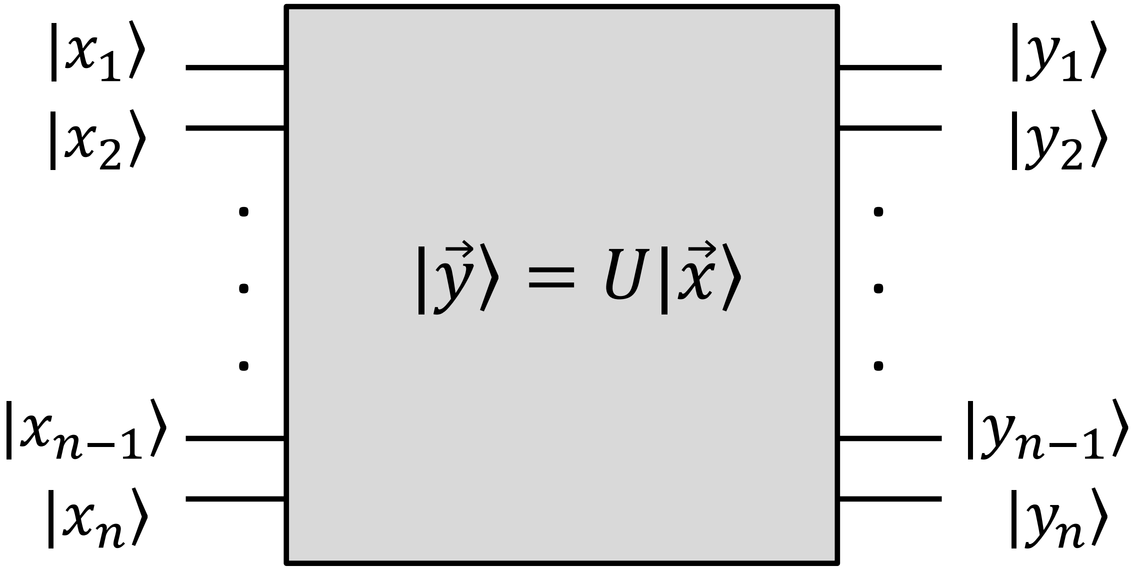
Classical computer



The computation can be decomposed into elementary functions: AND, OR, NOT,…

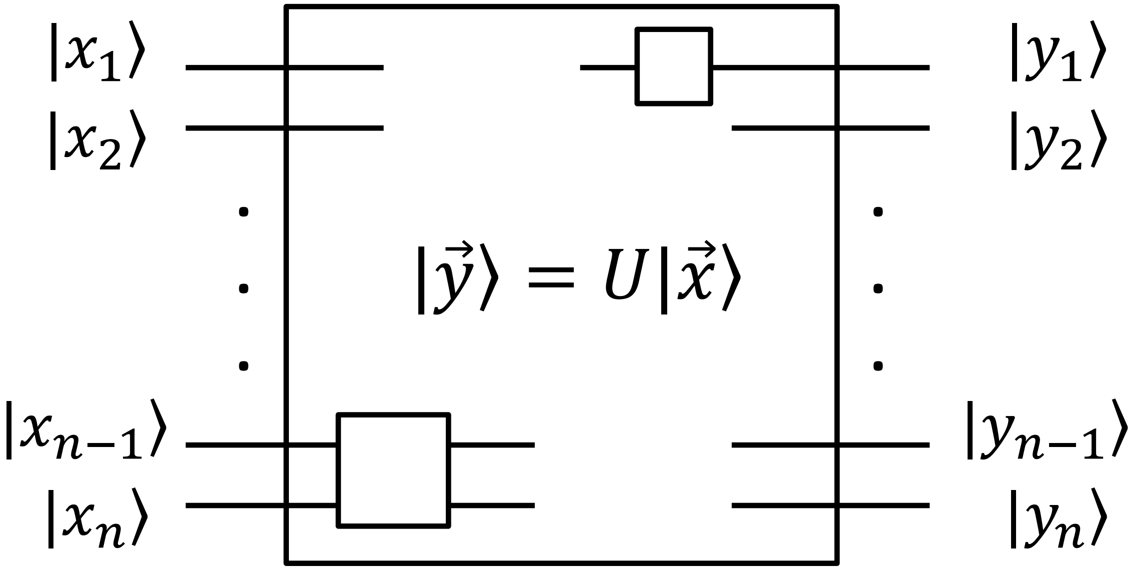
Quantum computation

Quantum computer



Quantum computation

Quantum computer



The computation can be decomposed into elementary unitary operations.

Shor’s algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

Shor's algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

6 = ?

Shor's algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

$$6 = 2 \times 3$$

Shor's algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

6 = 2 x 3

221 =

ICFO

Shor's algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

6 = 2 x 3

221 = 13 x 17

Shor’s algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

6 = 2 x 3
221 = 13 x 17

2.160.062.083 =

Shor's algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

6 = 2 x 3
221 = 13 x 17

2.160.062.083 = 38699 x 55817

Shor’s algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

6 = 2 x 3
221 = 13 x 17
2.160.062.083 = 38699 x 55817

22601385262034057849416540486101975135080389157197767183211977
68109445641817966676608593121306582577250631562886676970448070
00181114971186300211248792819948748206607013106658664608332798
28035603792053919801399464969552 61 =

Shor’s algorithm

An efficient quantum algorithm for factoring, a problem for which no efficient classical algorithm is known.

Peter Shor

6 = 2 x 3
221 = 13 x 17
2.160.062.083 = 38699 x 55817

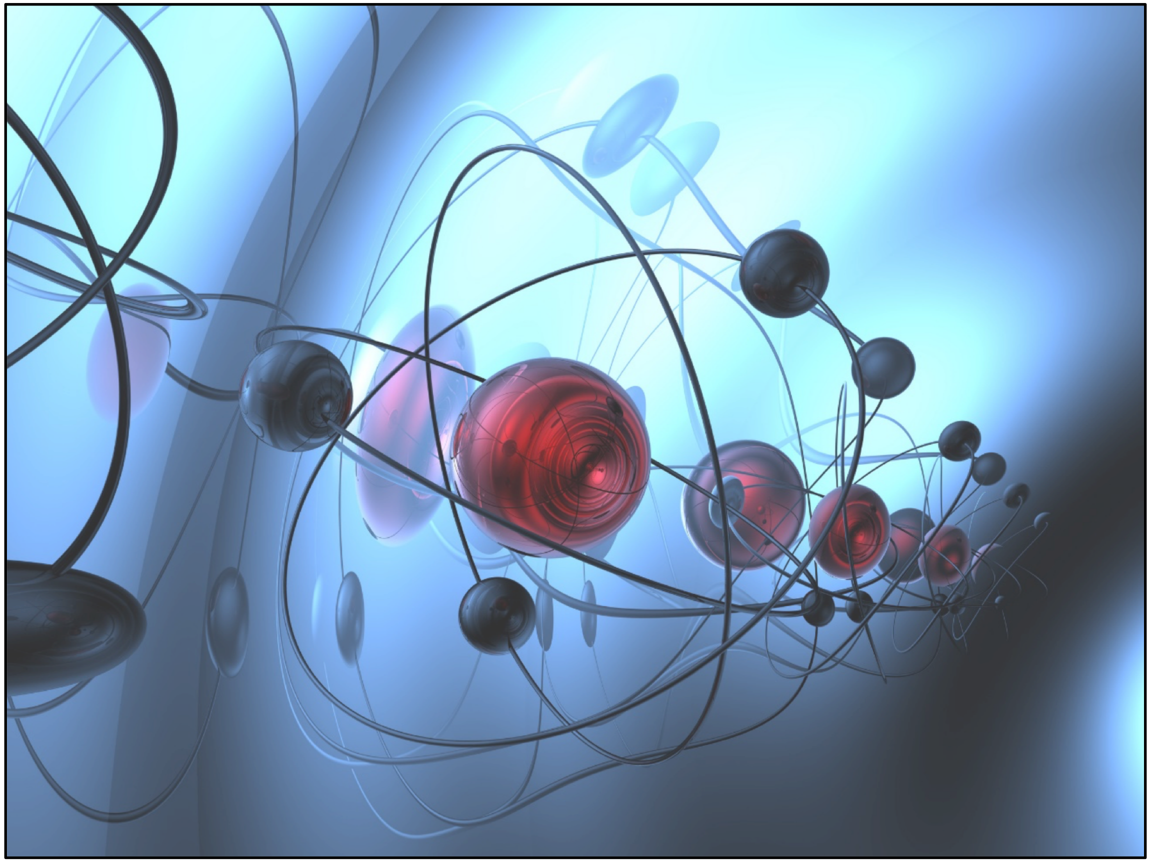
2260138526203405784941654048610197513508038915719776718321197768109445641817966676608593121306582577250631562886676970448070001811149711863002112487928199487482066070131066586646083327982803560379205391980139946496955261 =

No efficient classical algorithm is known.

ICFO

Factoring

Factoring is an easy problem for quantum computers.



ICFO

Factoring

2260138526203405784941654048610197513508038915719776718321197768109445641817966676608593121306582577250631562886676970448070001811149711863002112487928199487482066070131066586646083327982803560379205391980139946496955261 =

68636564122675662743823714992884378001308422399791648446212449933215410614414642667938213644208420192054999687

x

3292907439486349812049301549212935291916455196536233952462686051169290349309465246337824866390738191765712603

Cryptography

Alice

Multiply

Easy

Bob

Multiply

Easy

Eve

Factorize

Hard

Quantum secure?

Alice

Multiply

Easy

Bob

Multiply

Easy

Q-Eve

Factorize

Easy!!

Quantum secure?

Alice

Multiply

Easy

Bob

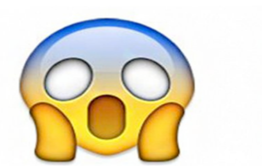
Multiply

Easy

Q-Eve

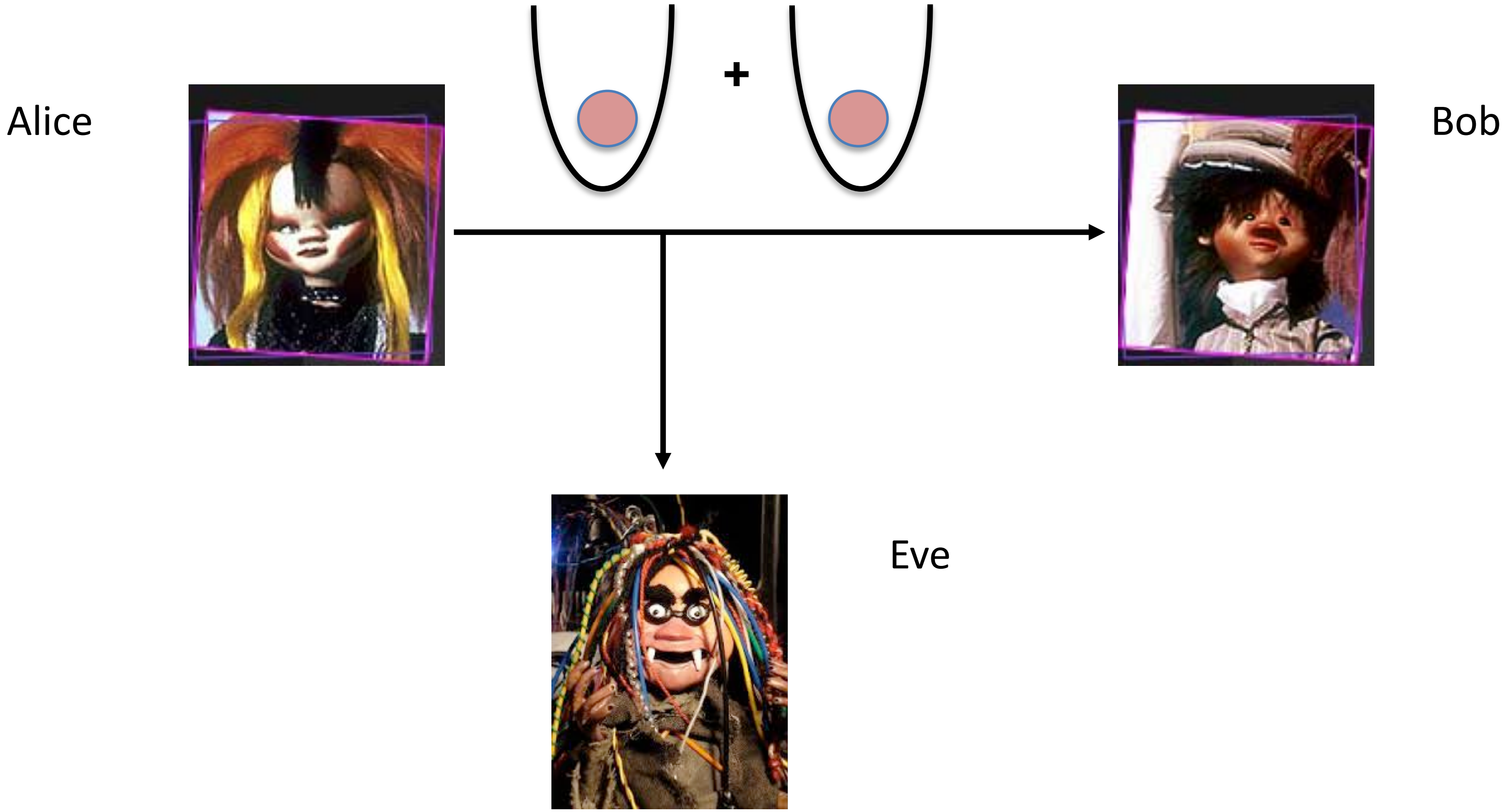
Factorize

Easy!!

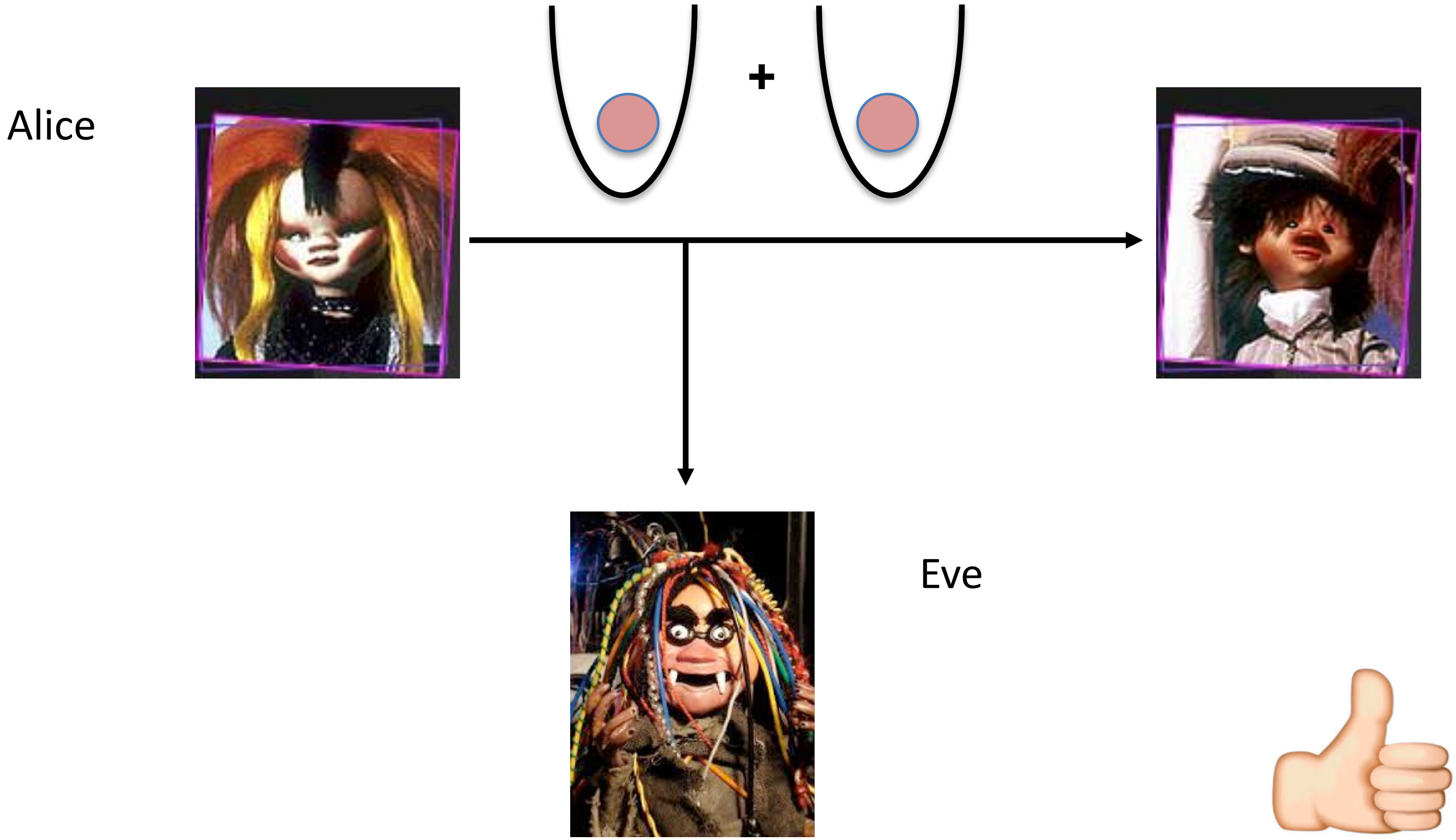


A quantum computer could break the most used scheme today for secure encryption!

Quantum cryptography



Quantum cryptography



The eavesdropper, when measuring the quantum particles, modifies their state and is detected → **Quantum Secure!!**

Quantum cryptography

- Standard cryptography is today based on **computational security**.
- Assumption: eavesdropper computational power is limited.

Quantum cryptography

- Standard cryptography is today based on **computational security**.
- Assumption: eavesdropper computational power is limited.
- Even with this assumption, security is unproven. Why do we believe that factoring is hard? We have tried to solve it for decades with no success.
- Is there a proof that factoring is hard? NO! Can we exclude that tomorrow a very smart mathematician will find an algorithm for efficient factorization? NO!

Quantum cryptography

- Standard cryptography is today based on **computational security**.
- Assumption: eavesdropper computational power is limited.
- Even with this assumption, security is unproven. Why do we believe that factoring is hard? We have tried to solve it for decades with no success.
- Is there a proof that factoring is hard? NO! Can we exclude that tomorrow a very smart mathematician will find an algorithm for efficient factorization? NO!
- Quantum computers sheds doubts on the long-term applicability of some of these schemes: factoring is easy on quantum computers.

ICFO

Quantum cryptography

- Standard cryptography is today based on **computational security**.
- Assumption: eavesdropper computational power is limited.
- Even with this assumption, security is unproven. Why do we believe that factoring is hard? We have tried to solve it for decades with no success.
- Is there a proof that factoring is hard? NO! Can we exclude that tomorrow a very smart mathematician will find an algorithm for efficient factorization? NO!
- Quantum computers sheds doubts on the long-term applicability of some of these schemes: factoring is easy on quantum computers.
- Computational security is cheap (software).

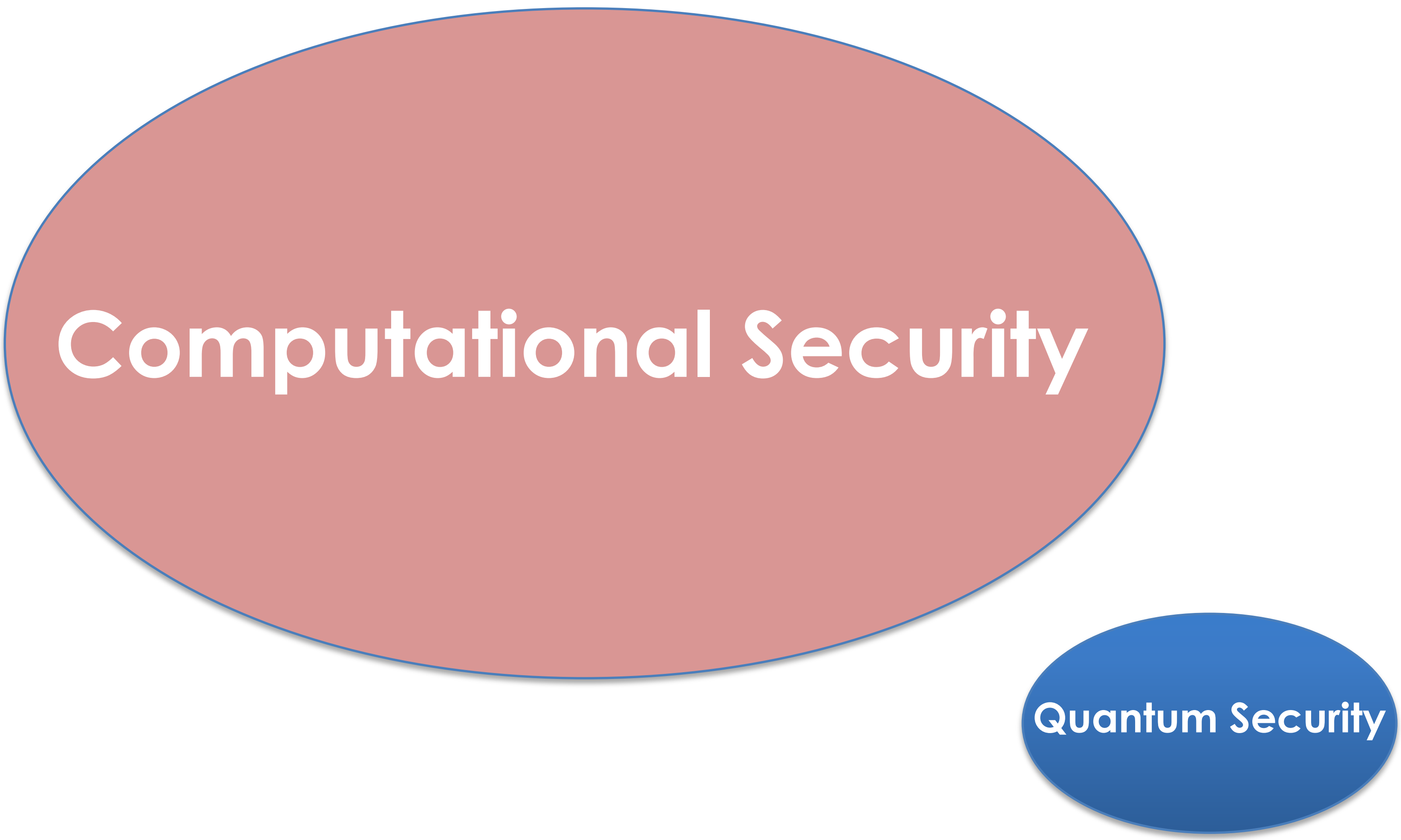
Quantum cryptography

- Standard cryptography is today based on **computational security**.
- Assumption: eavesdropper computational power is limited.
- Even with this assumption, security is unproven. Why do we believe that factoring is hard? We have tried to solve it for decades with no success.
- Is there a proof that factoring is hard? NO! Can we exclude that tomorrow a very smart mathematician will find an algorithm for efficient factorization? NO!
- Quantum computers sheds doubts on the long-term applicability of some of these schemes: factoring is easy on quantum computers.
- Computational security is cheap (software).
- Post-quantum cryptography: design protocols with security based on hard problems for a quantum computer.

Quantum cryptography

- Quantum cryptographic is based on **physical (quantum) security**.
- The implementation of these schemes is more demanding (hardware).
- Assumption: quantum physics offers a correct description of nature at the microscopic scale.
- To break the protocol, the eavesdropper should hack the physical implementation.

Crypto today



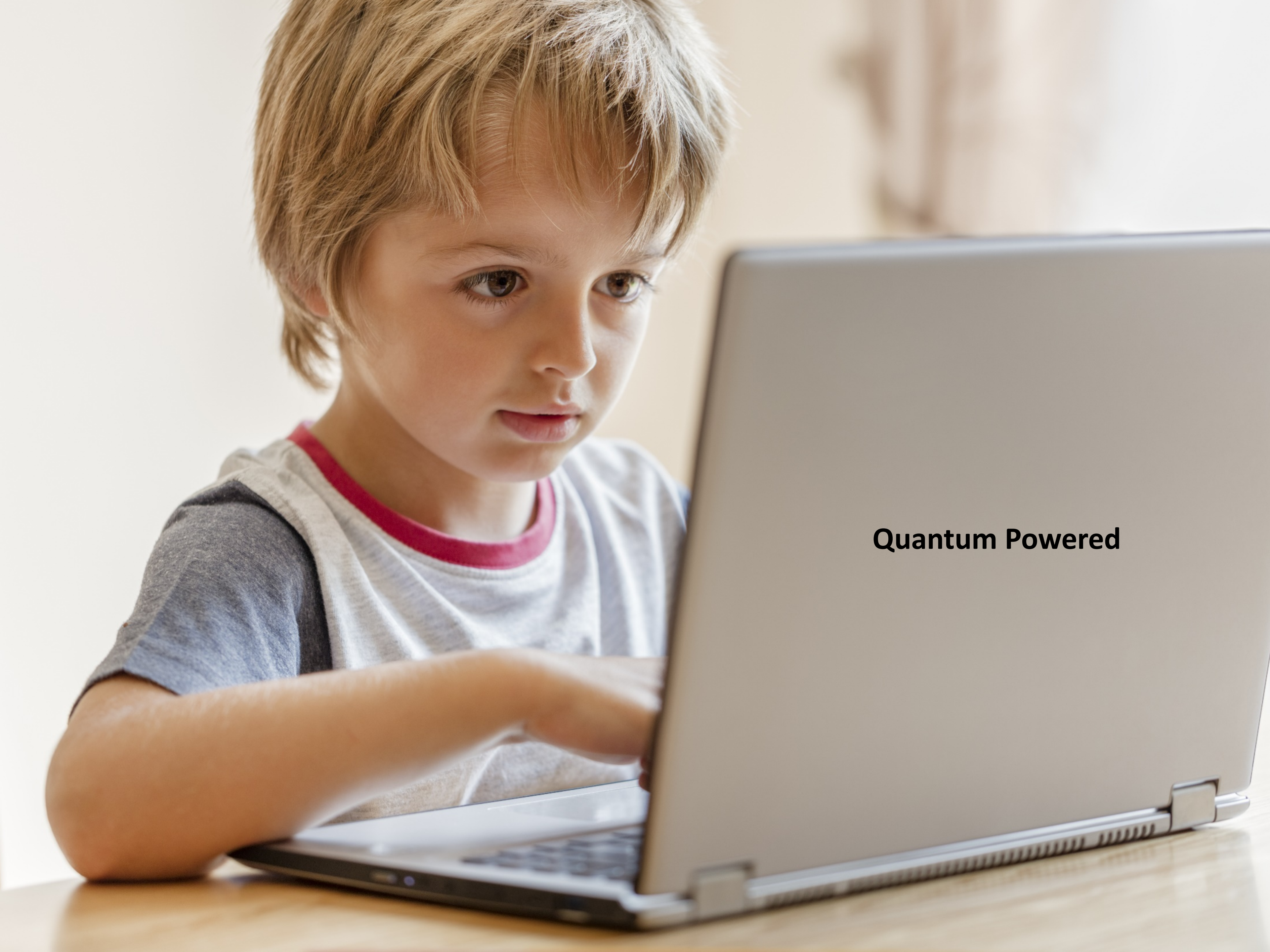
Crypto today

Computational Security

Crypto after the Flagship

Computational Security

Quantum Security


Quantum Powered