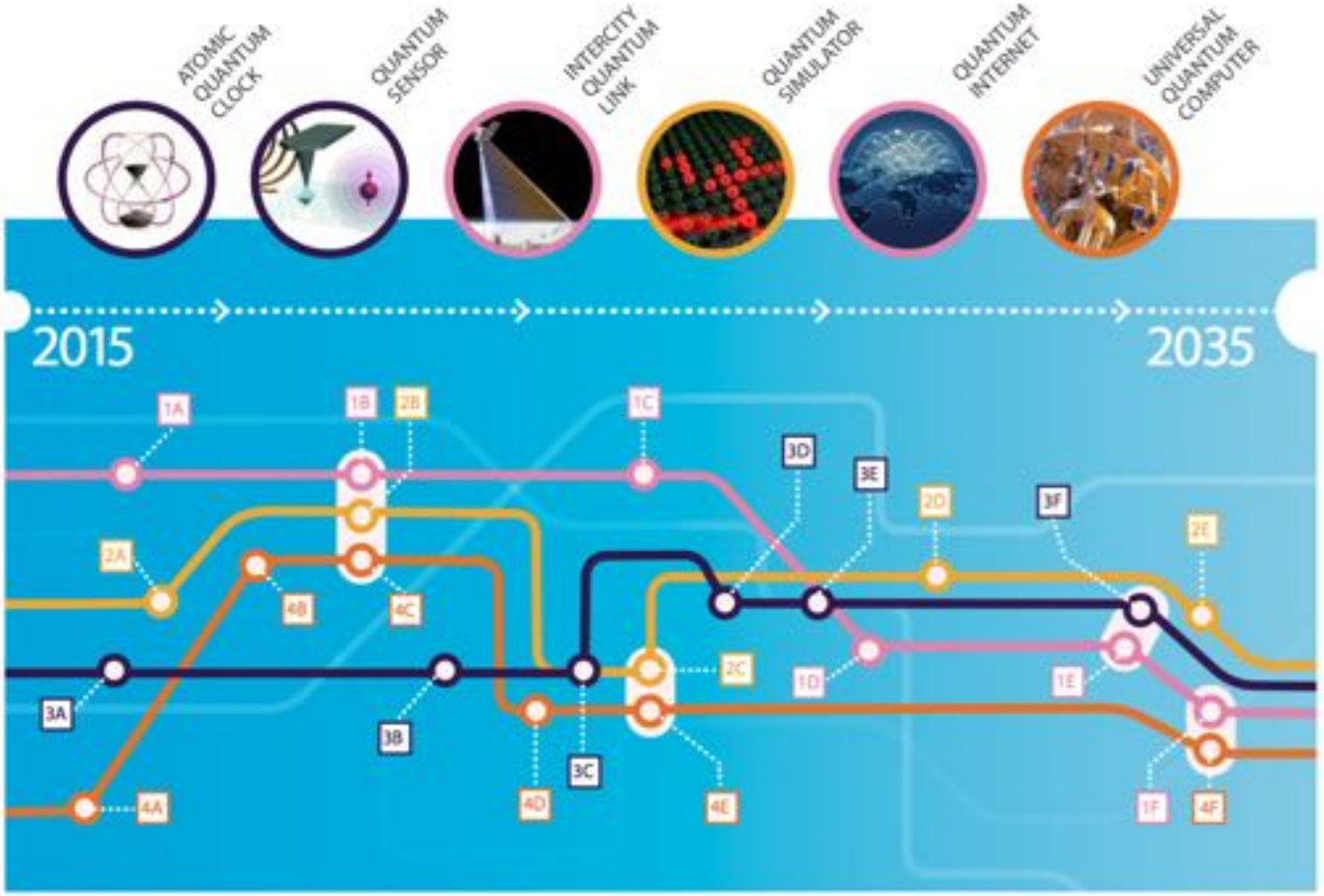
The second quantum revolution: quantum computation and information

Elisa Ercolessi
DIFA
U. Bologna



BOLOGNA - JUNE 29, 2016

ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA
IL PRESENTE MATERIALE È RISERVATO AL PERSONALE DELL'UNIVERSITÀ DI BOLOGNA E NON PUÒ ESSERE UTILIZZATO AI TERMINI DI LEGGE DA ALTRE PERSONE O PER FINI NON ISTITUZIONALI

European Commission will launch €1 billion quantum technologies flagship

Published on 17/05/2016

Günther H. Oettinger, Commissioner for the Digital Economy and Society outlined the Commission's plan to launch a €1 billion flagship initiative on quantum technology.

Share

Speaking at the Quantum Europe Conference organised by The Dutch presidency of the EU, the European Commission and the QuTech center in Delft, the Commissioner outlined his objective to reinforce European scientific leadership and excellence in quantum research and in quantum technologies.

Representatives of academia and industry presented the Quantum Manifesto to Commissioner Oettinger and to the Dutch Minister of Economic Affairs Henk Kamp. One point they made clear was that quantum secure communication and computing will be a key part of future computing infrastructure. The quantum flagship will be a key part of the data and computing Infrastructure which underpins the European Cloud Initiative, as part of the Commission's strategy to digitise European industry.

The Q-bit

- In Quantum Mechanics, the STATE of a system is described by a complex vector

$$|\psi\rangle = \begin{pmatrix} \psi_1 \\ \psi_2 \\ \vdots \\ \psi_n \\ \vdots \end{pmatrix} \quad , \quad \psi_j \in \mathbb{C}$$

- We can linearly combine vectors: **SUPERPOSITION PRINCIPLE**

- Familiar when dealing with forces, fields, waves …

- Not familiar when dealing with systems of particles in classical mechanics

- This means that also

$$|\psi\rangle = \alpha|\psi_1\rangle + \beta|\psi_2\rangle \quad , \quad \forall \alpha, \beta \in \mathbb{C}$$

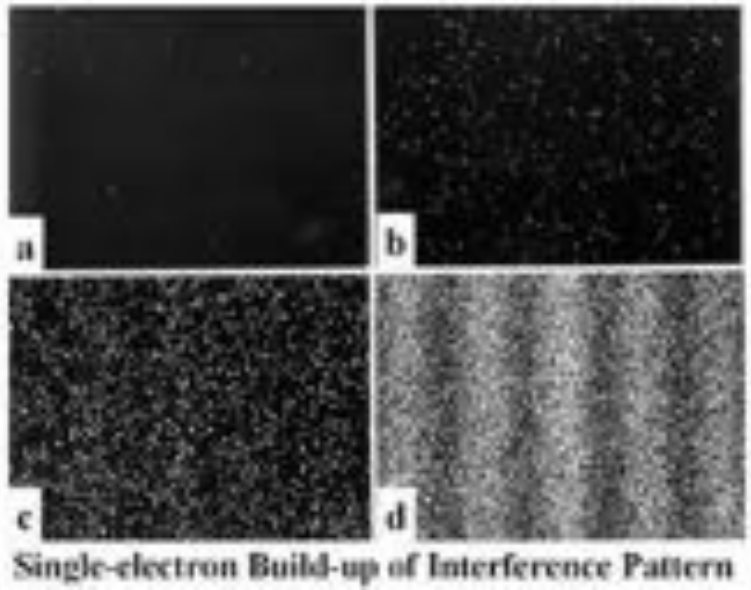
  is a possible state

- **PROBABILISTIC INTERPRETATION**

$$p_1 = |\alpha|^2$$
$$p_2 = |\beta|^2$$

is the probability to find the system in the first/second state

- Example:
  double slit
  experiment
  with single electrons



Single-electron Build-up of Interference Pattern

(“ … the heart of quantum mechanics …”, R. Feynman)

- **Q-BIT** = Two-Level System

  - two independent states (basis) $\quad |0\rangle \ , \ |1\rangle$

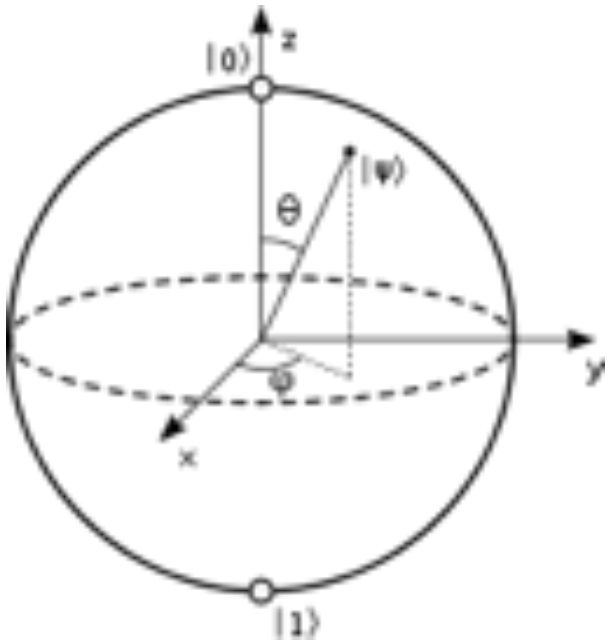
  - general state $\quad |\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$

  - a measurement gives

$|0\rangle$ *with probability* $p_1 = |\alpha|^2$, $|1\rangle$ *with probability* $p_2 = |\beta|^2$

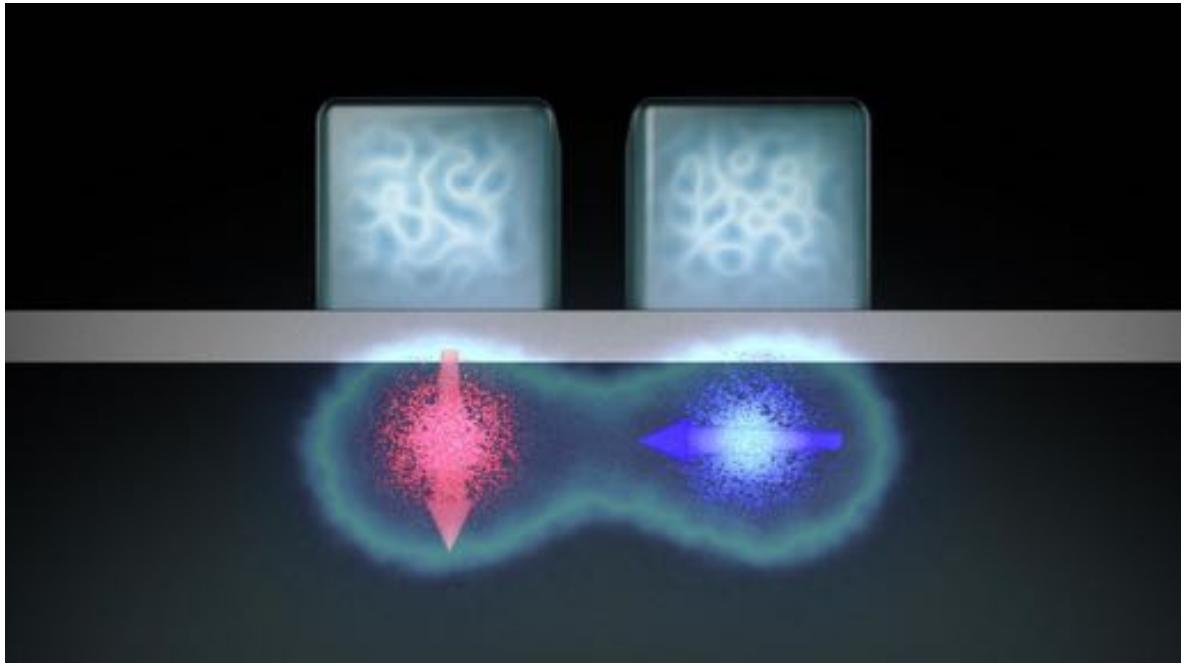
  - Bloch sphere: states are parametrized by two real numbers

$$\alpha = \cos\theta \ , \ \beta = e^{\imath\phi}\sin\theta$$



- *Much more information than a bit!*

- **TWO Q-BITS**



Computational basis

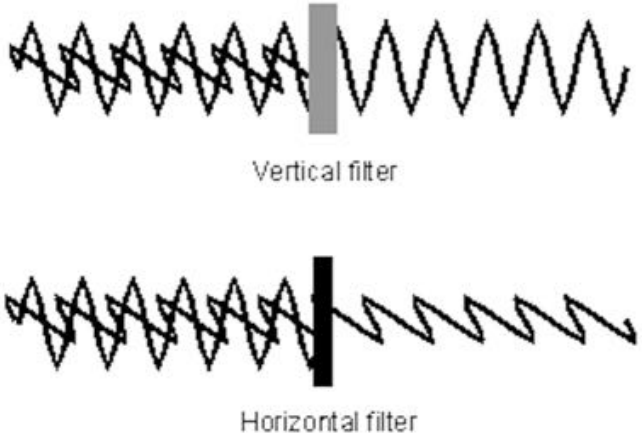
$$|Q_A Q_B\rangle = |00\rangle\ ,\ |10\rangle\ ,\ |01\rangle\ ,\ |11\rangle$$

General state

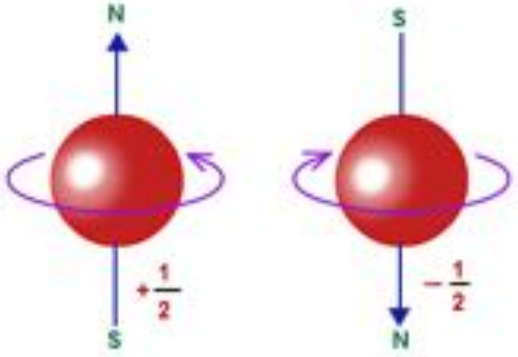
$$|Q_A Q_B\rangle = \alpha_{00}|00\rangle + \alpha_{10}|10\rangle + \alpha_{01}|01\rangle + \alpha_{11}|11\rangle$$

$$|\alpha_{00}|^2 + |\alpha_{10}|^2 + |\alpha_{01}|^2 + |\alpha_{11}|^2 = 1$$

- *Experimental realisations*

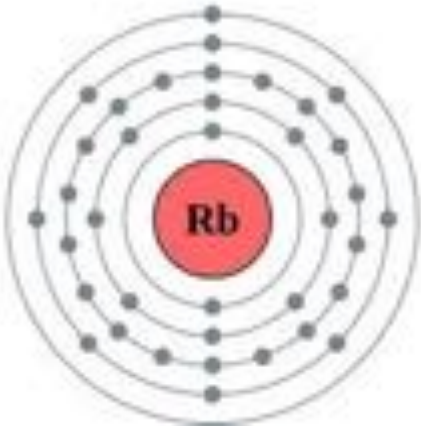


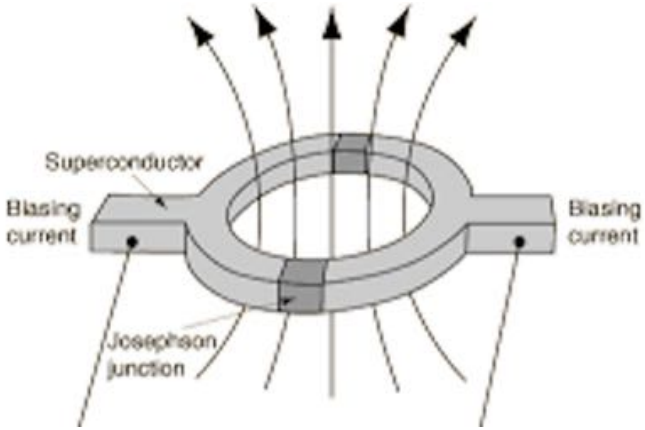
Photons: polarisation



Electrons: spin

Atoms: isotopes of Na, Rb, …





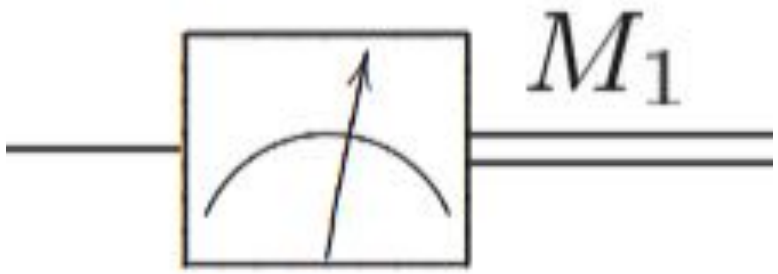
Superconducting Junctions

Gates

- We shall distinguish between:

- **MEASUREMENT**: "disruptive" transformation -> collapse of the vector

$$|\psi_{in}\rangle = \alpha|0\rangle + \beta|1\rangle \quad \Rightarrow \quad |\psi_{out}\rangle = \begin{cases} |0\rangle & , \ p_0 = |\alpha|^2 \\ |1\rangle & , \ p_1 = |\beta|^2 \end{cases}$$

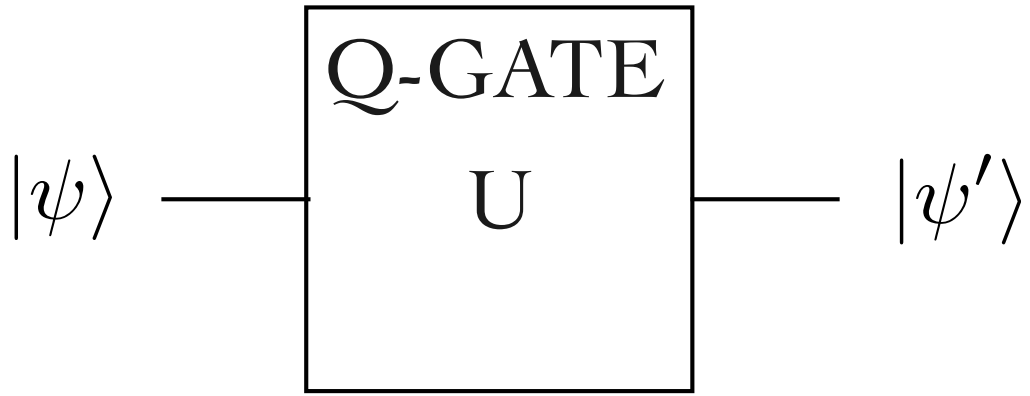


- **EVOLUTION**: transformation according to Schroedinger equation -> (unitary) evolution operator

$$U(t) \quad , \quad U^\dagger U = U^\dagger U = \mathbb{I}$$

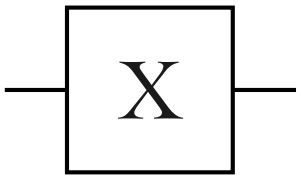
$$|\psi(t)\rangle = U(t)|\psi_0\rangle = \alpha(t)|0\rangle + \beta(t)|1\rangle$$

$$= \begin{pmatrix} u_{11} & u_{12} \\ u_{21} & u_{22} \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix}$$



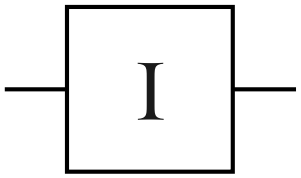
N.B. quantum gates are unitary, hence reversible

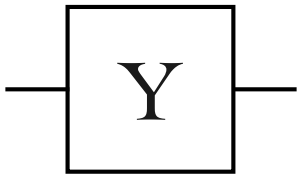
- *Examples of single q-bit gates*

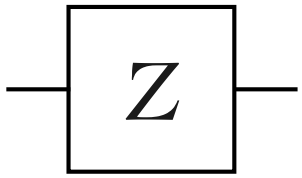


$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad NOT \ : \begin{cases} |0\rangle & \rightarrow & |1\rangle \\ |1\rangle & \rightarrow & |0\rangle \end{cases}$$

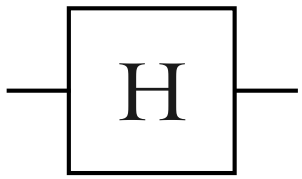
$$\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad Y = \begin{pmatrix} 0 & -\imath \\ \imath & 0 \end{pmatrix} \qquad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$







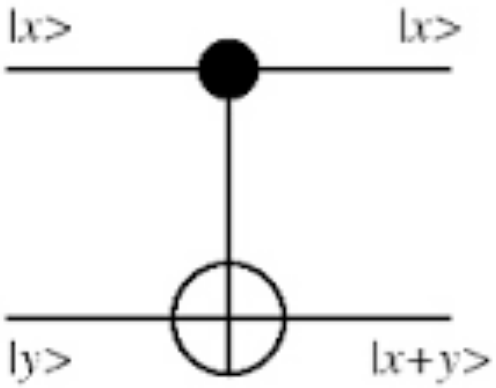
$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



$$HADAMARD \ : \begin{cases} |0\rangle & \rightarrow & \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle \\ |1\rangle & \rightarrow & \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle \end{cases}$$

- *Examples of two-q-bit gates*

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \qquad CNOT \;:\; \begin{cases} |00\rangle & \rightarrow & |00\rangle \\ |10\rangle & \rightarrow & |10\rangle \\ |01\rangle & \rightarrow & |10\rangle \\ |11\rangle & \rightarrow & |01\rangle \end{cases}$$



- Universal Quantum Gates:

CNOT + single q-bit gates

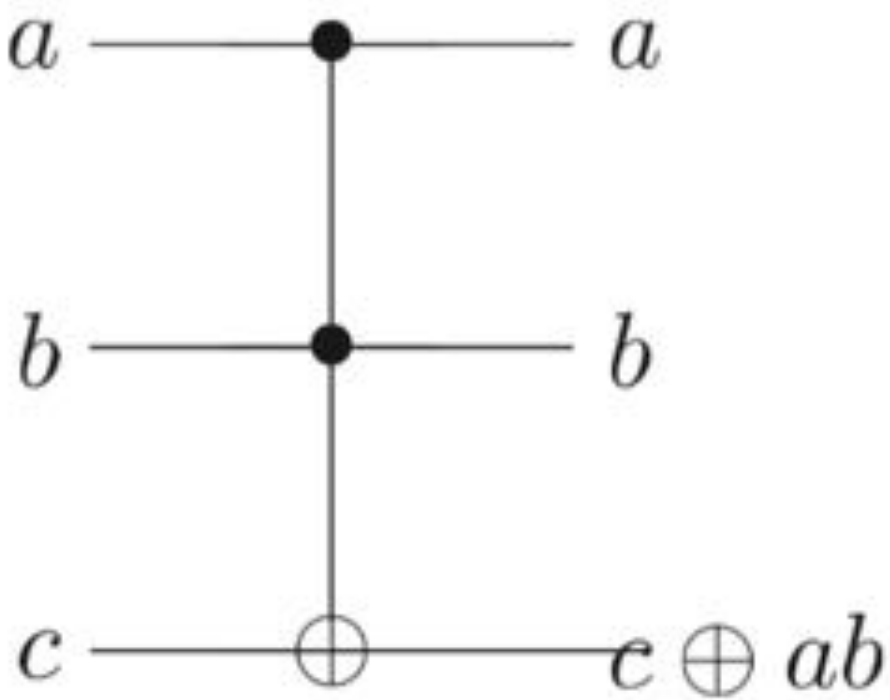
- TOFFOLI GATE

for classical computation,

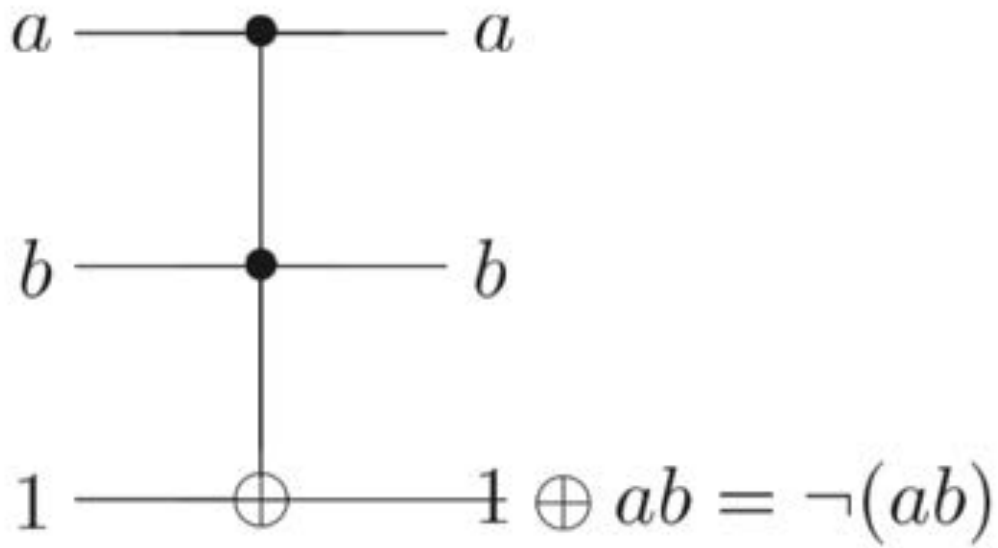
which requires

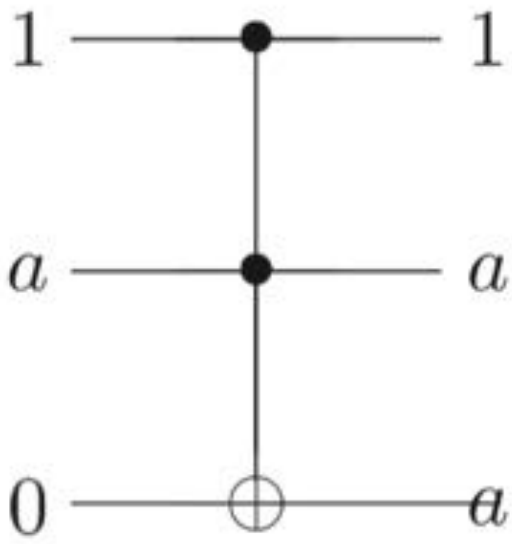
NAND and FAN-OUT

not trivial because of



No-cloning Theorem: it is not possible to perform a unitary transformation which replicates an arbitrary initial state



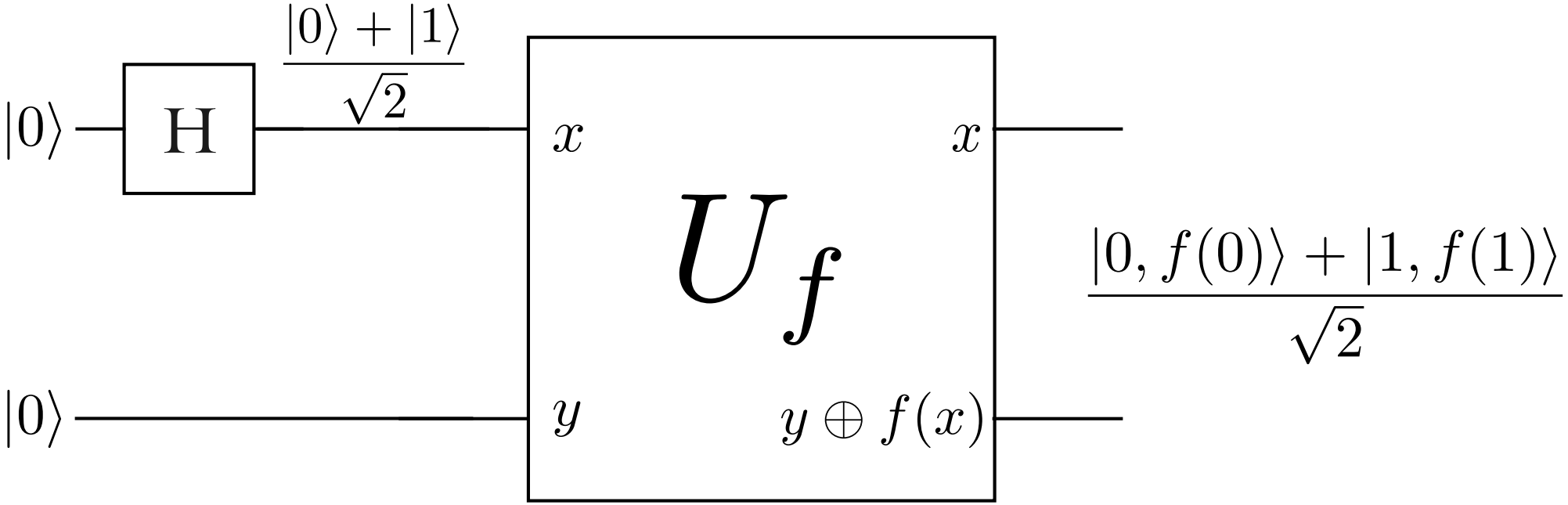


Algorithms

- **QUANTUM PARALLELISM**

quantum parallelism allows quantum computers to evaluate a function f(x) for many different values of x simultaneously

$$f : \{0, 1\} \rightarrow \{0, 1\}$$



- At the basis of many algorithms

  - extension to n q-bits: $\sum_x |x, f(x)\rangle$

  - Deutsch: calculates $f(0) \oplus f(1)$ in only one iteration

  - Deutsch-Jozsa: evaluate whether a function is constant or balanced in just one iteration

  - Quantum Fourier transform: exponential speed-up

  - Search problems (Grover): quadratic speed-up

  - Factorisation (Shor): exponential speed-up

- *Computational Complexity: from NP to P problems*

Entanglement

- BELL STATES:
  different basis
  from computational

$$|\chi_{\pm}\rangle = \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}$$

$$|\psi_{\pm}\rangle = \frac{|01\rangle \pm |10\rangle}{\sqrt{2}}$$

- Consider the following situation: with $|\psi_{+}\rangle$

- The first q-bit is sent to Alice, the second to Bob.

- If Alice makes a measurements she finds her q-bit in the |0>,|1> state with 50% probability: the state of Alice's q-bit is not defined a-priori.
The same holds for Bob's q-bit.

- Suppose Alice measures 0: this means that the global vector has collapsed to $|\psi_{fin}\rangle = |01\rangle$

- If Bob makes a measurements now, he finds that his q-bit is 100% in the |1> state!

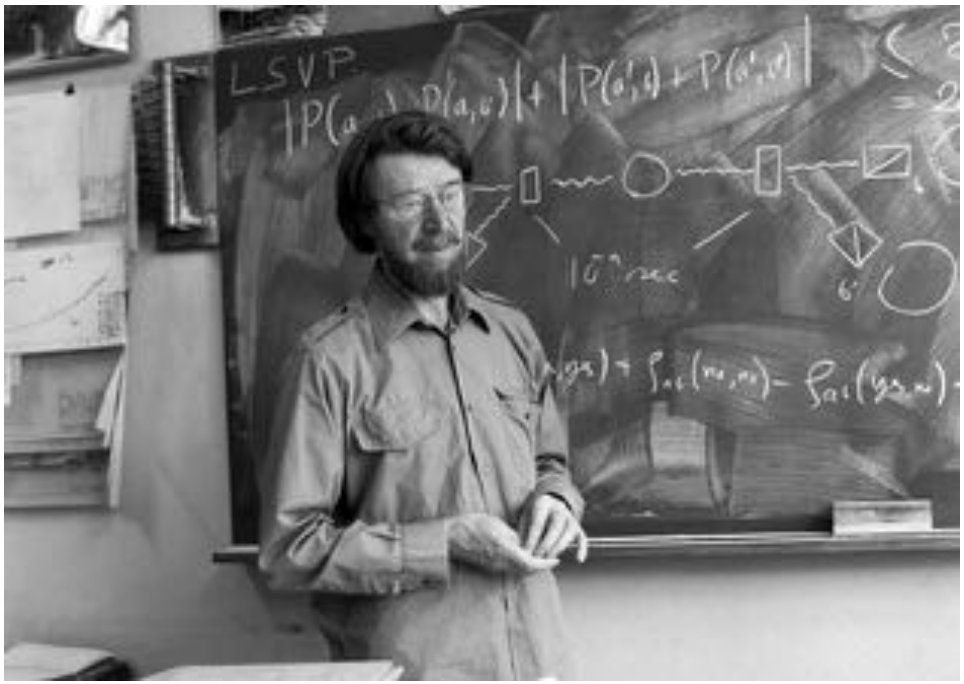
“ … that spooky action at a distance …”
(A. Einstein)

- Quantum Correlations (**ENTANGLEMENT**) exist between the two q-bits

- *Source of a long-standing debate*

  - Einstein vs. Bohr

  - Einstein-Podolsky-Rosen paradox



- Hidden variables

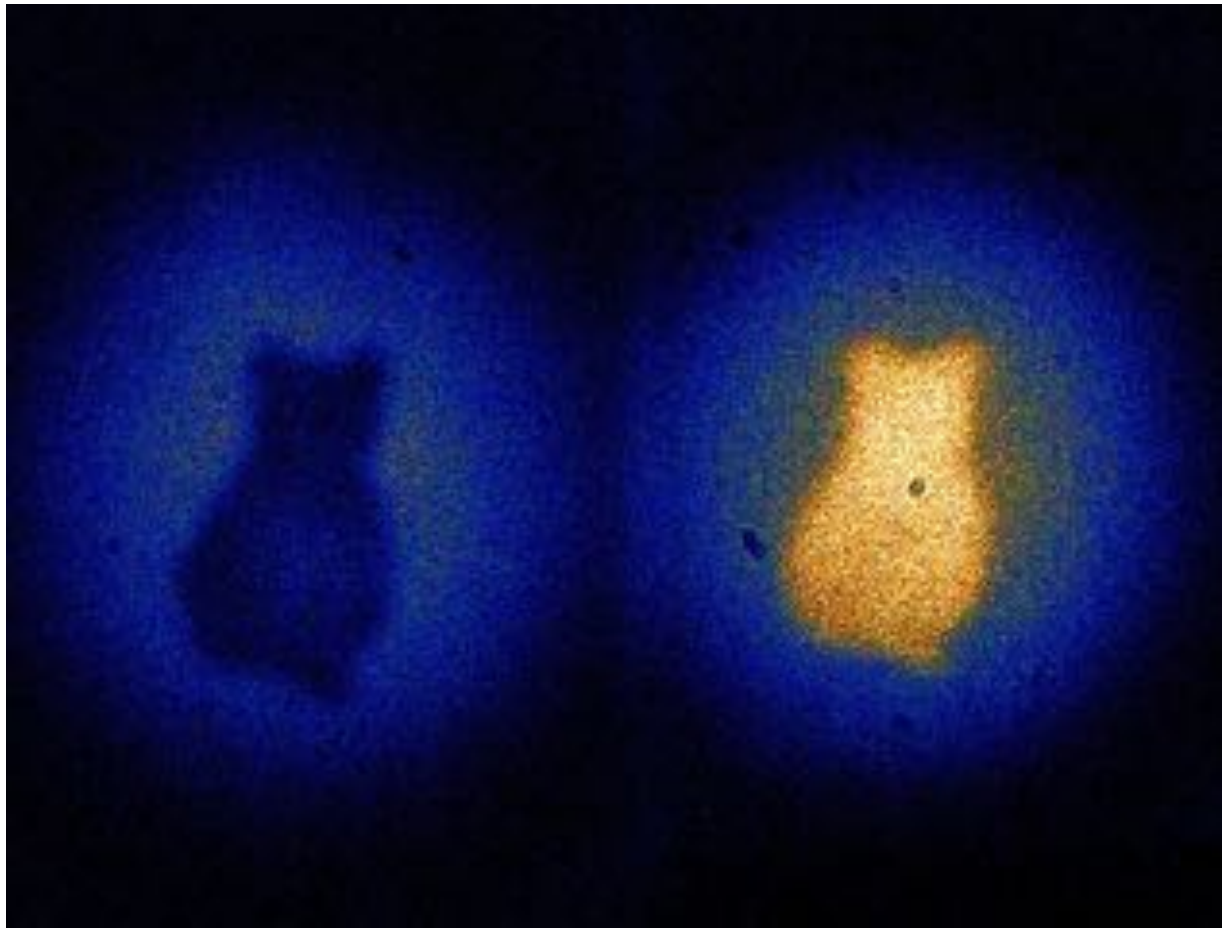
- Bell's theorem

- Aspect's experiments

Entanglement as a resource

"Quantum imaging with undetected photons"

Gabriela Barreto Lemos, Victoria Borish, Garrett D. Cole, Sven Ramelow, Radek Lapkiewicz & Anton Zeilinger
***Nature* 512, 409–412 (28 August 2014)**



- **CRYPTOGRAPHY** :

  - Public key distributions:

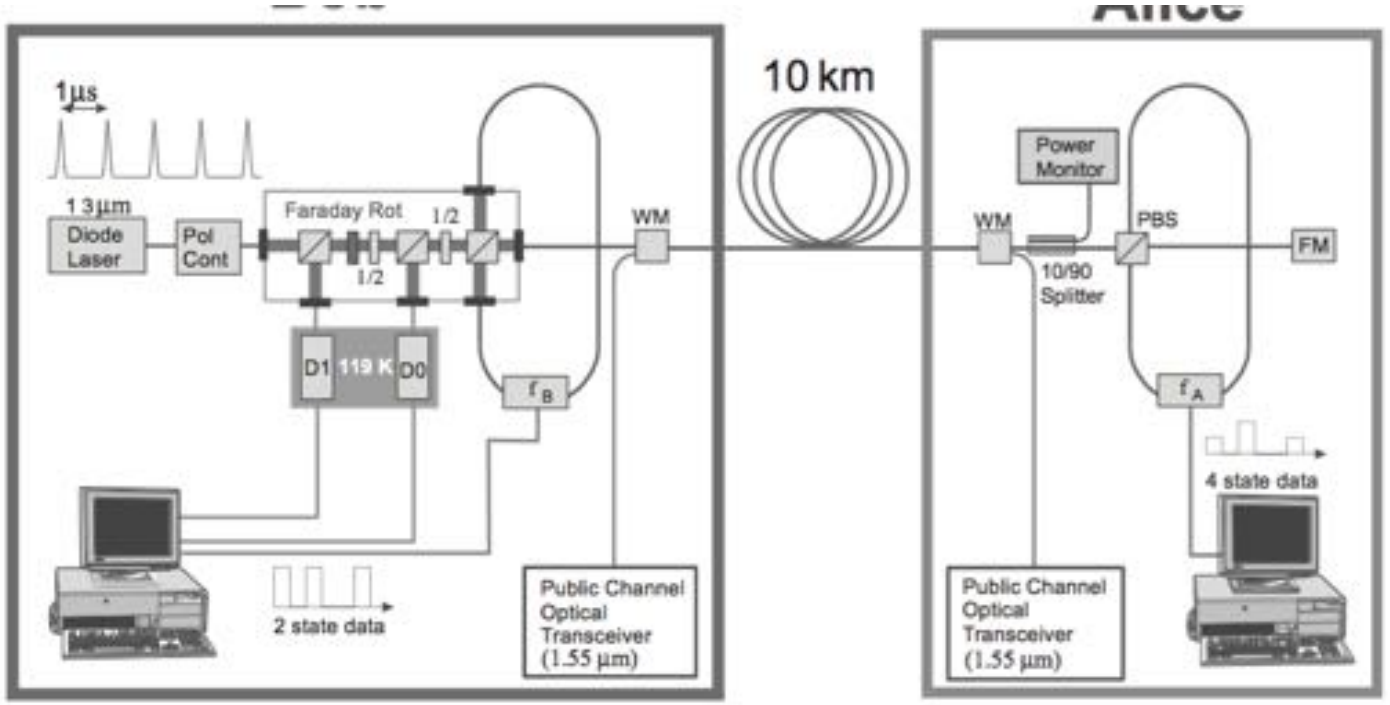
efficiency based on the fact that to use the key one has to know how to factorise a huge number

for classical computers this is a NP problem, but for quantum computers this is a P problem

  - Private key distributions: *Quantum Key Distribution*

Alice & Bob must share the key and this can be eavesdropped and stolen

Quantum protocols to share a private key between A and B



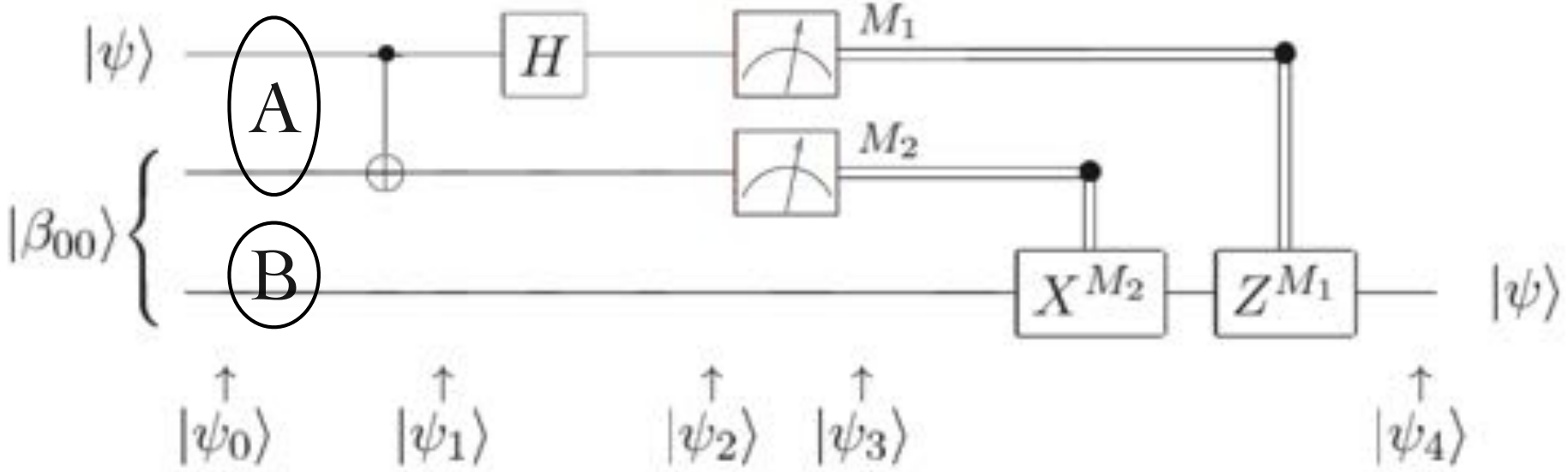
Security can be proven mathematically under the assumption that communication over public channels happens with an error rate lower than a given threshold

Basic idea: if Eve succeeds in eavesdropping the key, the system is so much disturbed that Alice and Bob know it has been stolen

- **TELEPORTATION**:
  exact reconstruction of the unknow state of a q-bit at a ∂istance (from Alice to Bob)

- it can be done thanks to assistance of a couple of entangled q-bits

- at the end of the protocol, when Bob has reconstructed the state, Alice's q-bit state is lost



Where are we?

- **CRYPTOGRAPHY** : Quantum Key Distribution over optical fibres

- First experiments: 40 km
- In 2004: first bank account transfer
- As of 2015: 350 km

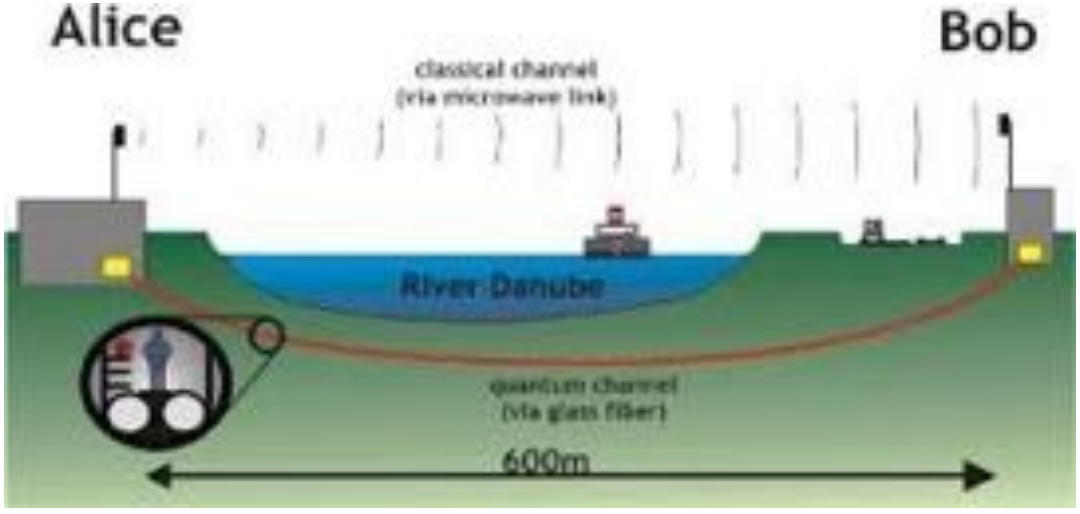
- Commercial: ID Quantique (Geneva), MagiQ Technologies (New York), QuintessenceLabs (Australia) and SeQureNet (Paris).

- Active research programmes: Toshiba, HP, IBM, Mitsubishi, NEC and NTT.

- **TELEPORTATION**: mainly with photons

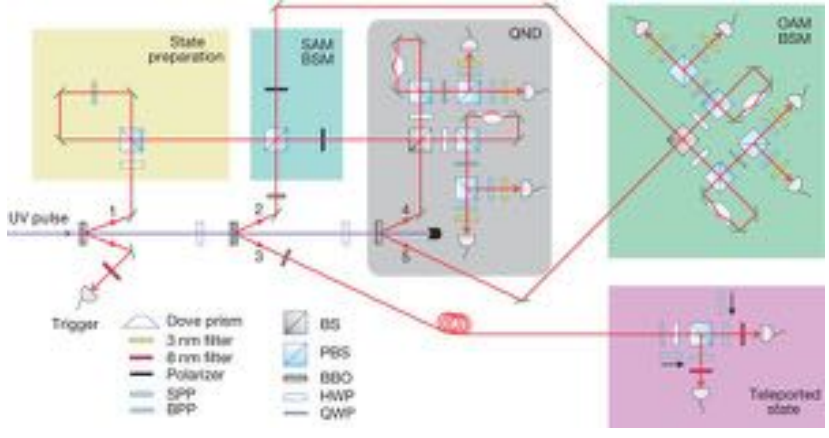
- First experiments: few meters (LENS in Florence)

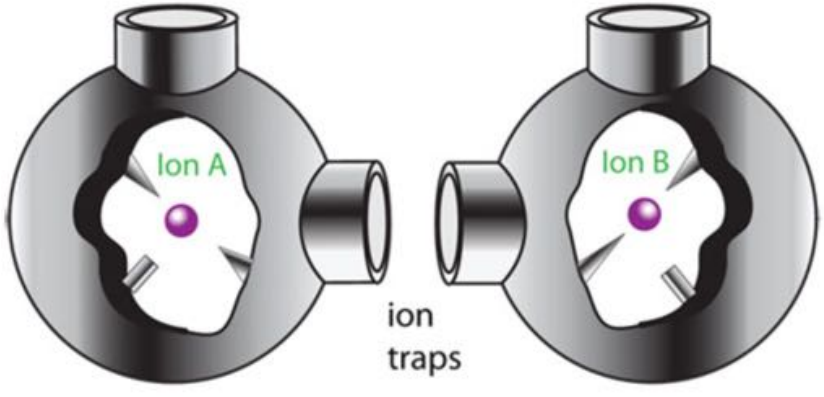
- In 2003: first teleportation across the Danube (Institute of Quantum Optics, Vienna)



- As of 2015: 100 km (NIST)

- Developments: … Multiple degrees of freedom
… Larger systems (atoms, cold gases,…)

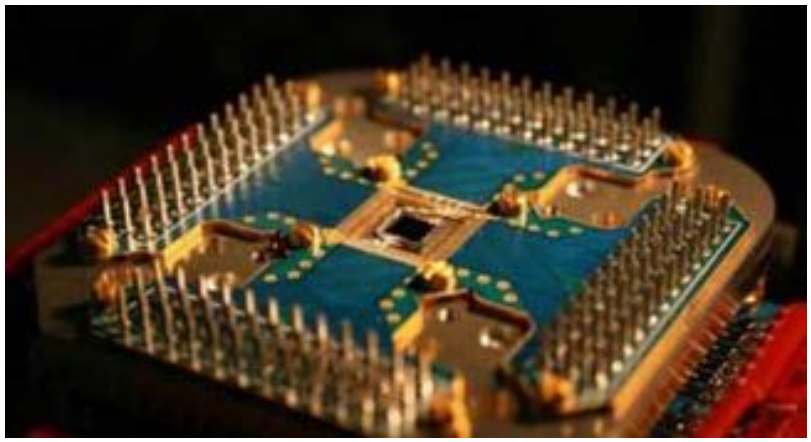




- **QUANTUM COMPUTERS:**

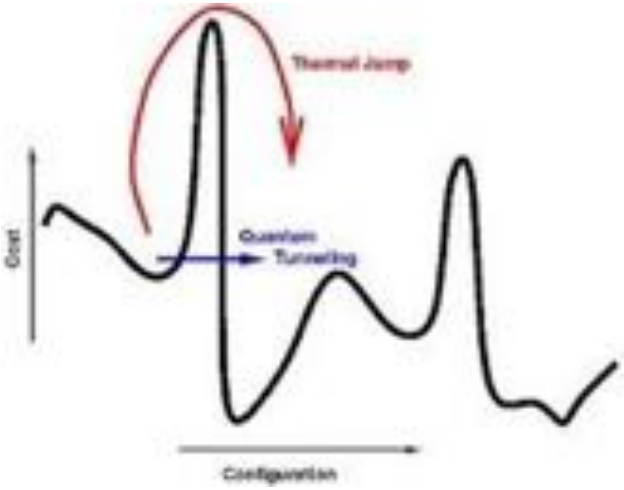
initialisation decoherence

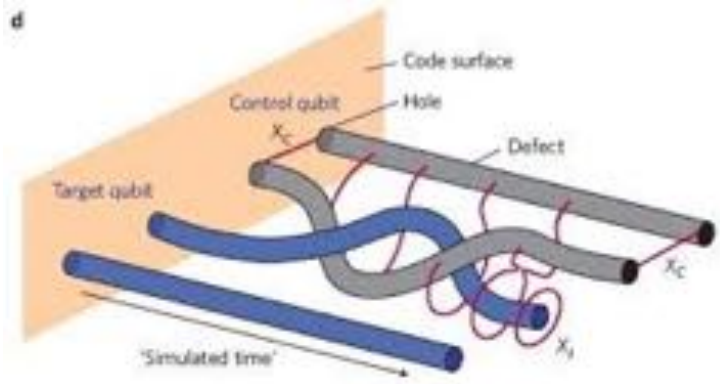
universality readability scalability



✦ Quantum gate arrays

✦ Adiabatic quantum computers





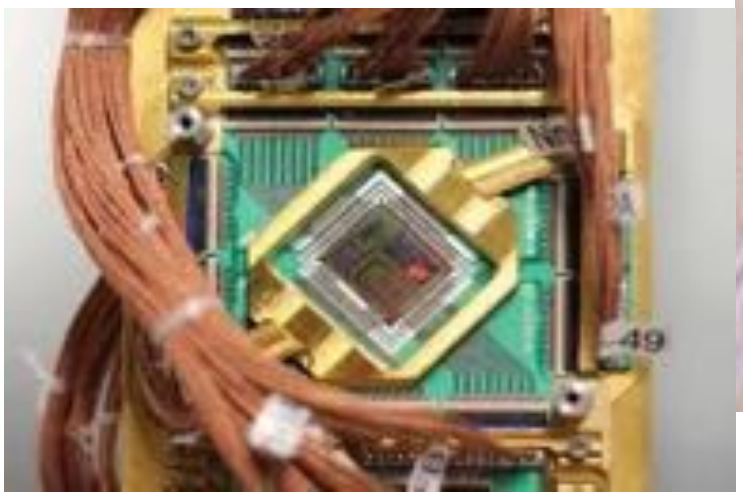
✦ Topological quantum computers

- Possible implementations:
  - photons
  - trapped atoms/ions
  - quantum dots
  - bose-einstein condensates
  - superconducting junctions
  - NMR
  - cavity QED
  - ....

- Several small implementation for specific problems: such as Shor's algorithm to factorise 15 on a 4 q-bit NMR computer in 2001, in 2012 factorisation of 21

- Other interesting news:

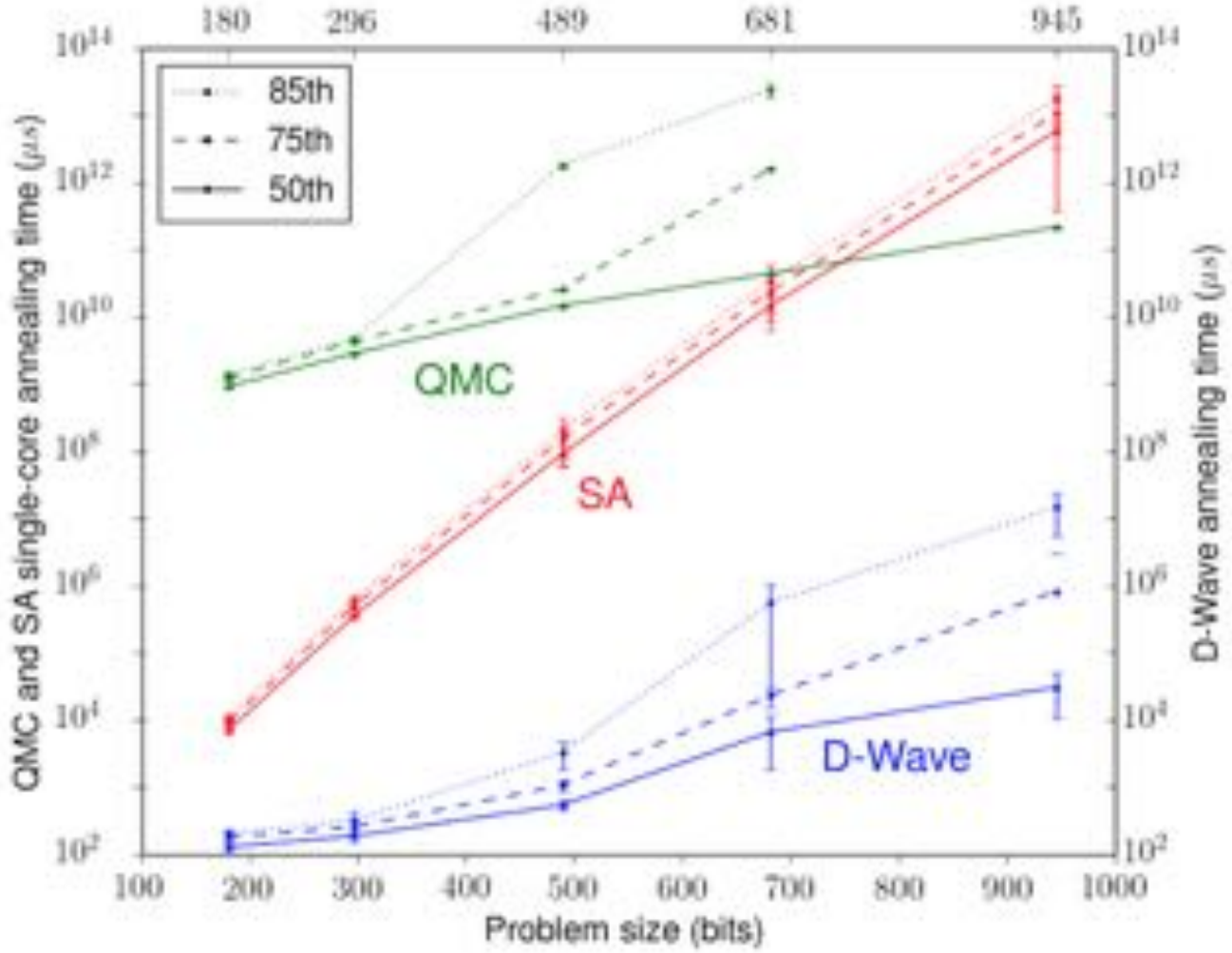
- *D-Wave Systems* (USA): in sold 2010 the first 128 q-bit processor, in 2012 the 512 q-bit processor, in 2015 the 1000+ 2X system



- Large debate between D-Wave & IBM over efficiency and actual use of quantum algorithms

- Cost: $ 15 million, bought by NASA & Google in 2015

- Speed-up: december 2015 from Google Lab



- *QC lab in the world*:

NASA	Bell Labs
Google	Microsoft
Apple	D-Wave

- *IBM cloud quantum computer*: 5 q-bits chip

What else?

- **QUANTUM SIMULATORS**:

  Simulating quantum mechanics is known to be a difficult computational problem, especially when dealing with large systems (R. Feynman).

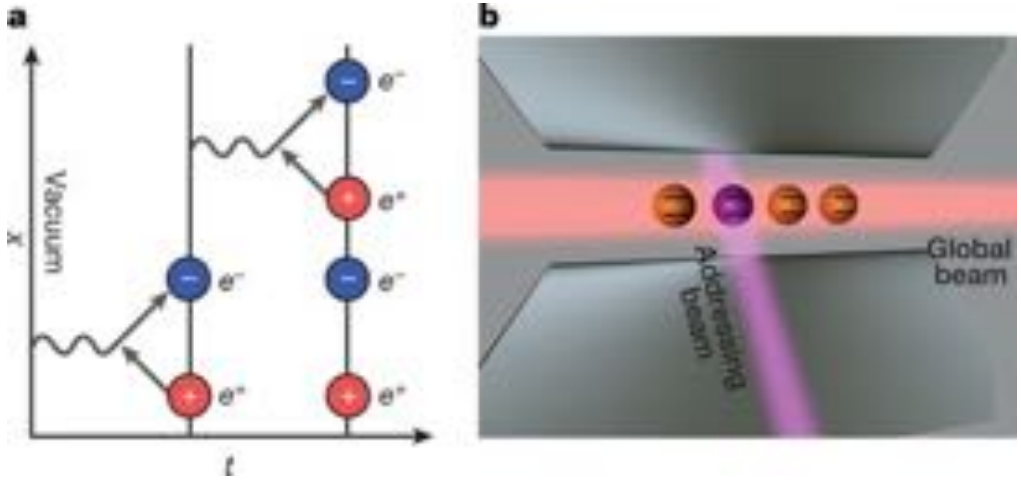
  This difficulty may be overcome by using some controllable quantum system to study another less controllable or accessible quantum system.

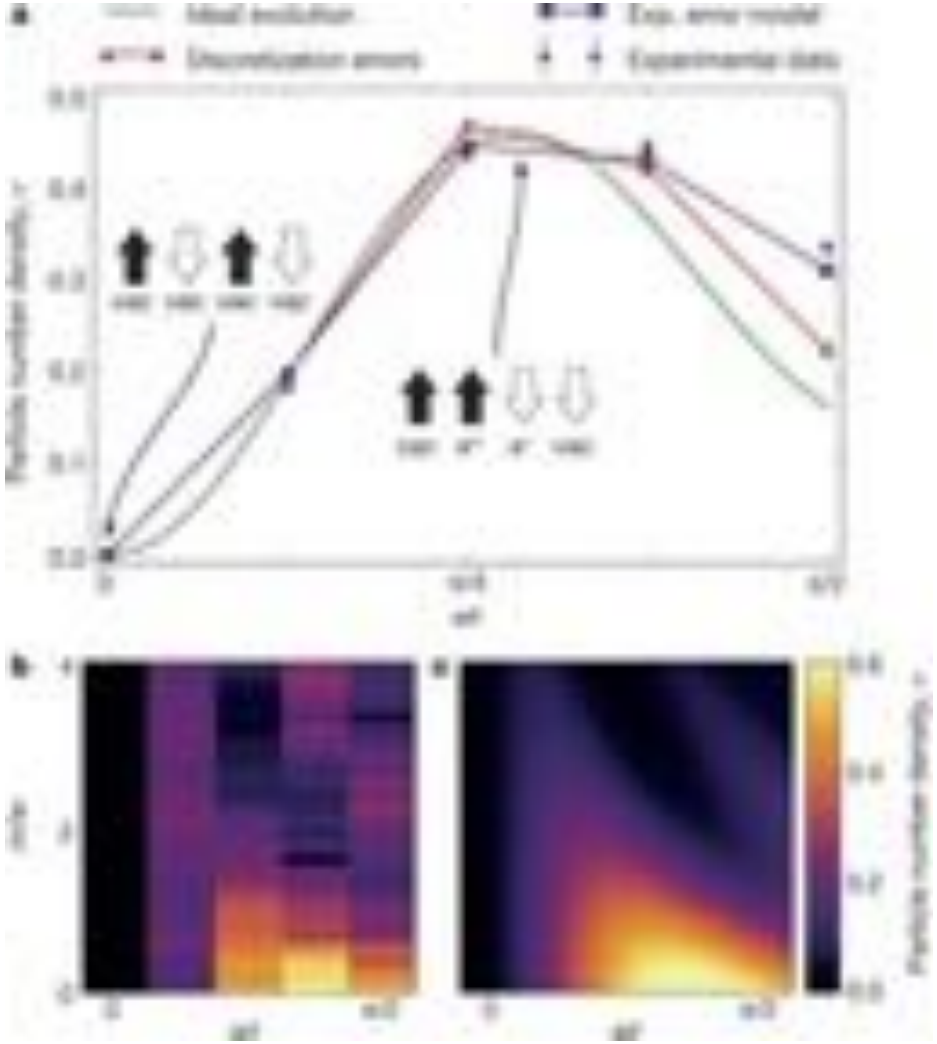
  Applications to the study of many problems in, e.g., condensed-matter physics, high-energy physics, atomic physics, quantum chemistry, and cosmology.

Real-time dynamics of lattice gauge theories with a few-qubit quantum computer

Esteban A. Martinez, Christine A. Muschik, Philipp Schindler, Daniel Nigg, Alexander Erhard, Markus Heyl, Philipp Hauke, Marcello Dalmonte, Thomas Monz, Peter Zoller & Rainer Blatt

Nature **534**, 516–519 (23 June 2016)





Textbooks:

J. Preskill - Quantum Computation -
http://www.theory.caltech.edu/people/preskill/ph229/

M.A. Nielsen, I.L. Chuang, Quantum Computation and Quantum Information, Cambridge, 2011