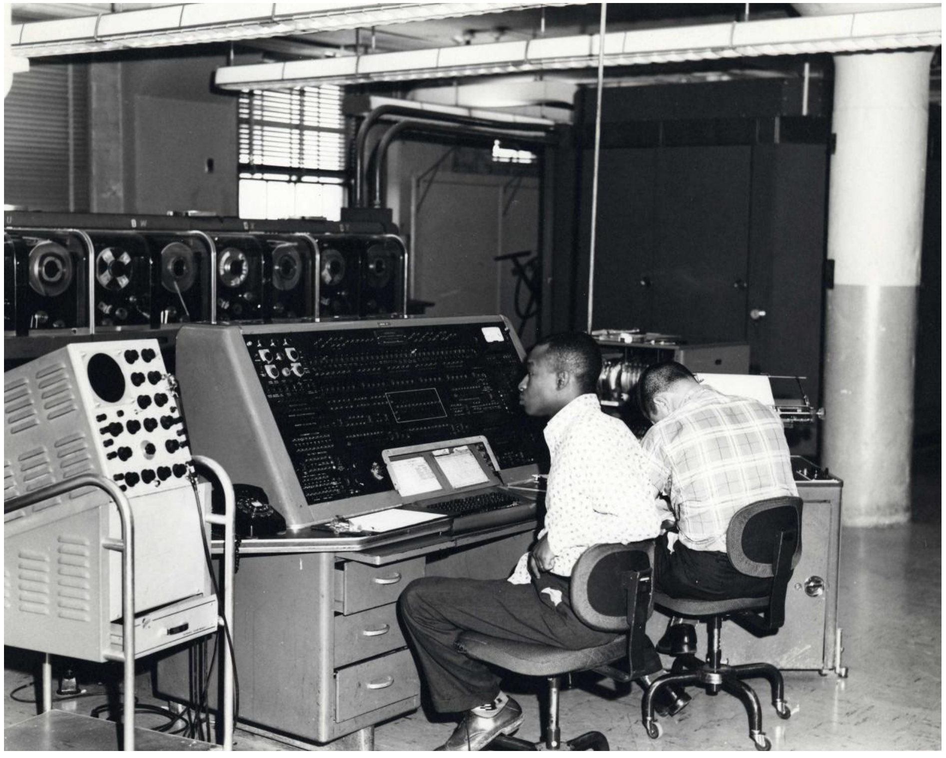
Il computer quantistico: concetti di base ed ultimi sviluppi

Oliver Morsch
INO-CNR, Pisa

- **Introduzione:** Il computer “classico” e la legge di Moore
- **La fisica del c.q.**: La sovrapposizione e gli stati entangled
- **Problemi della realizzazione:** decoerenza; criteri di Di Vincenzo
- **Stato dell'arte:** i sistemi fisici sotto indagine
- **Qualche approccio in più dettaglio**
- **Il simulatore quantistico:** computer quantistici “su misura”
- **Prospettive per il futuro:** quando si potrà comprare un c.q.?

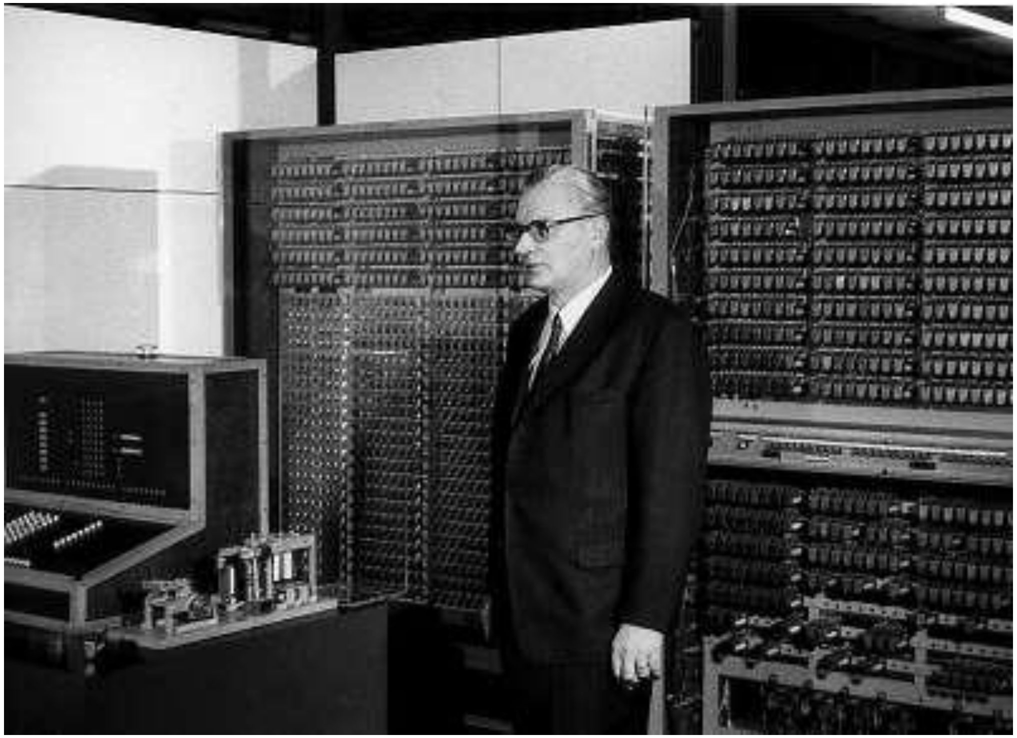
Il computer “classico”



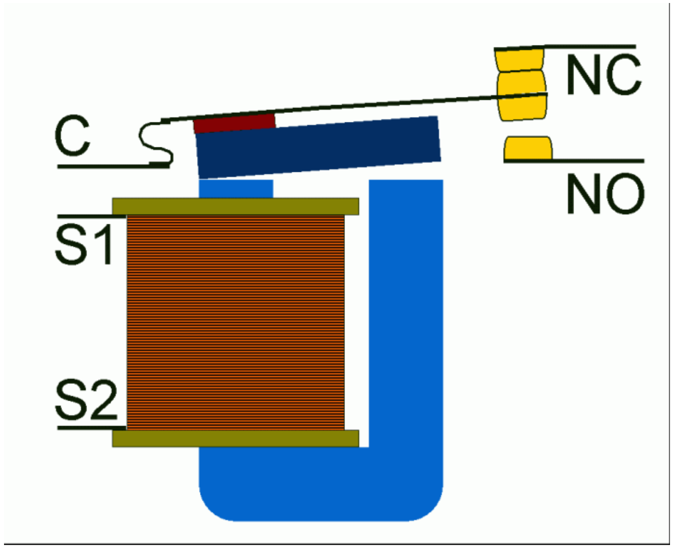
A UNIVAC computer at the Census Bureau, ca. 1960.

Netbook, 2010

Il computer a relais



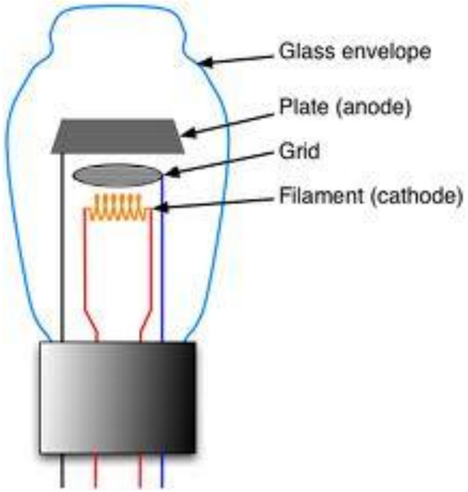
Konrad Zuse e lo “Zuse Z3”



il relais elettrico

Il computer con tubo a vuoto

Osaka University Vacuum Tube Computer



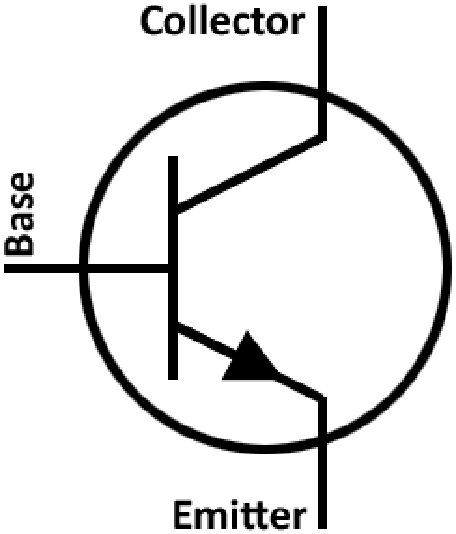
tubo a vuoto

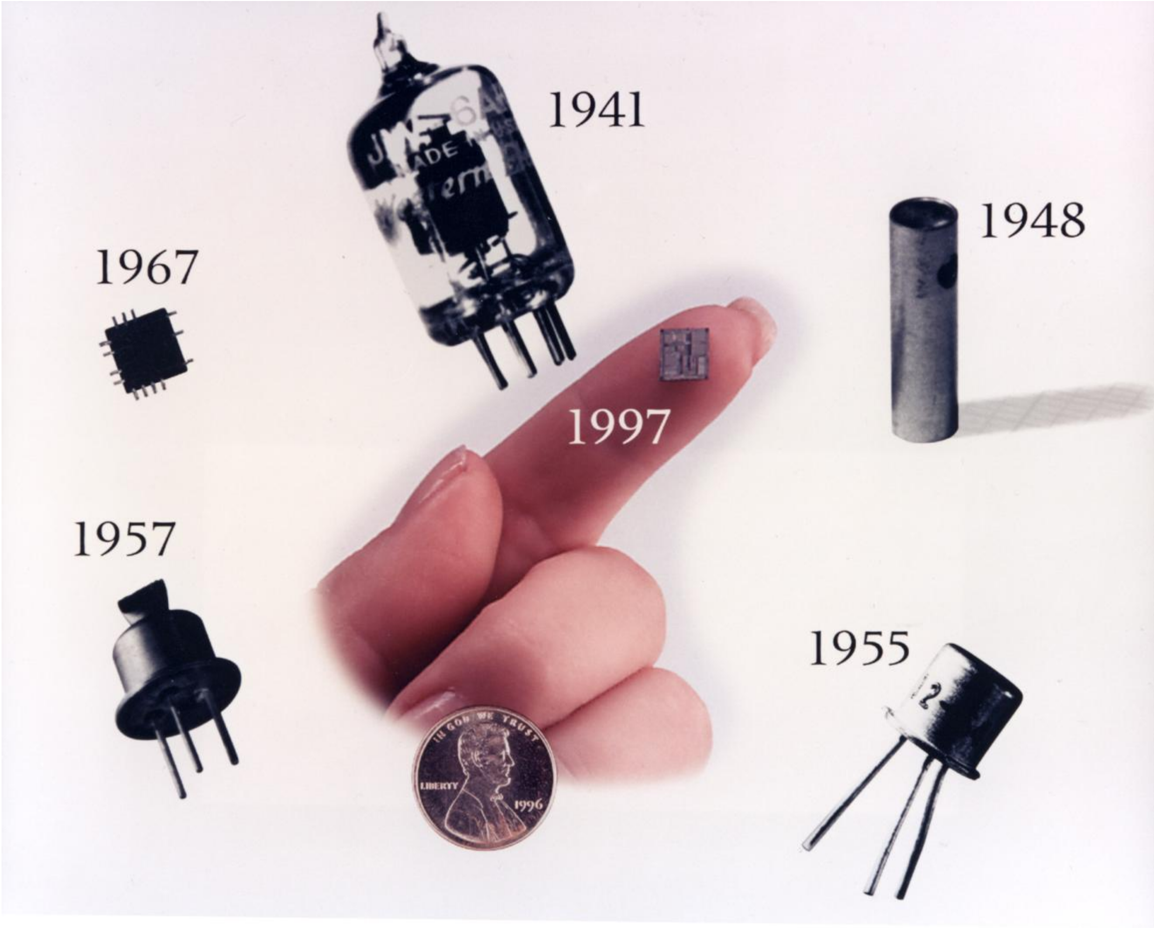
La scoperta cruciale: il transistor

Transistor (the "Crystal Triode")

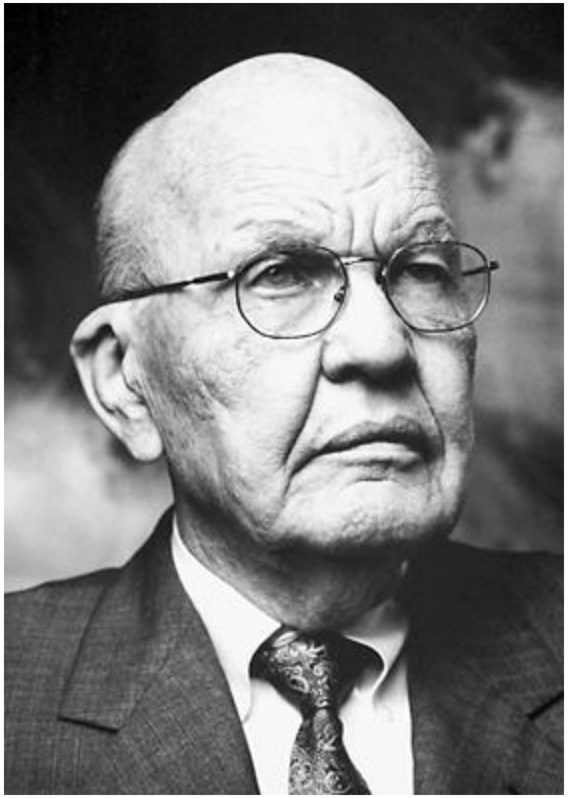
William Shockley, John Bardeen, Walter Brattain: Premio Nobel 1956

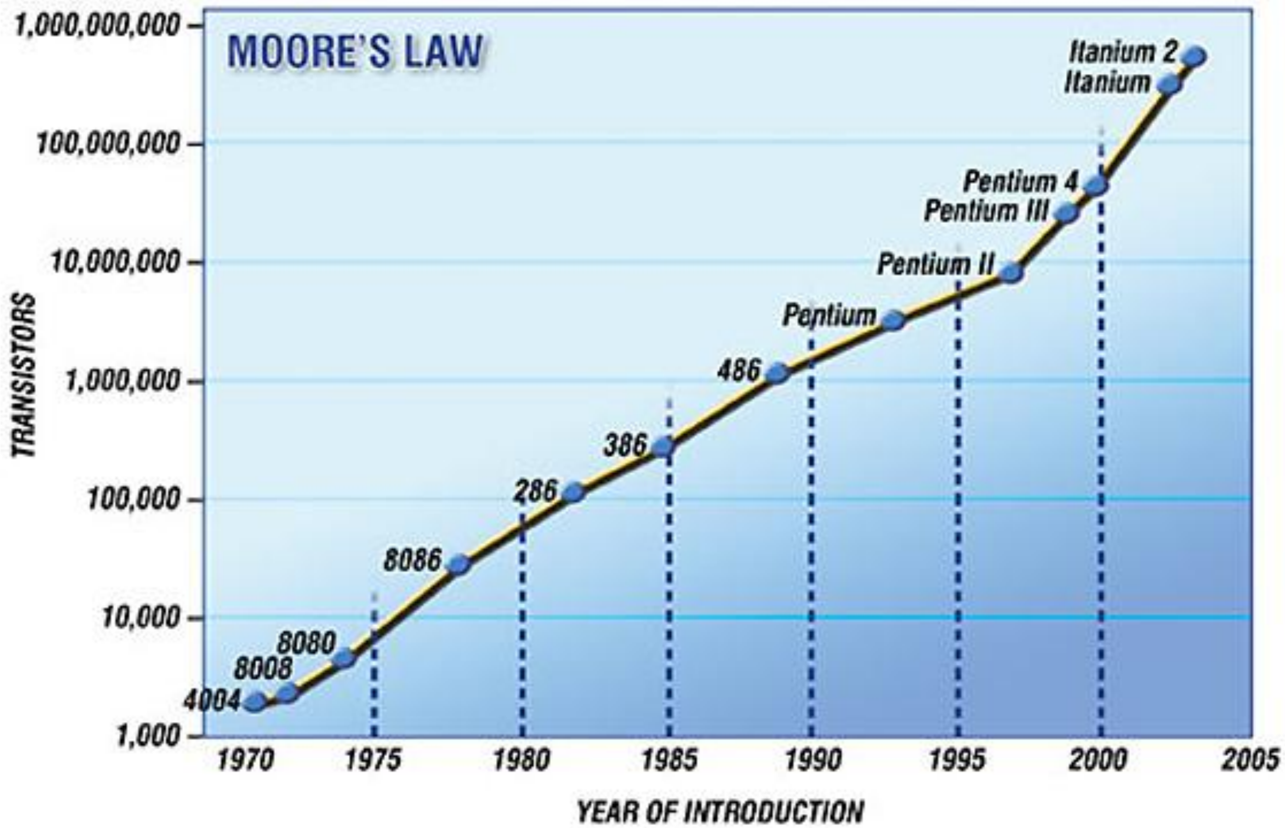
Dal transistor al circuito integrato





La legge di Moore





Jack Kilby
Premio Nobel 2000

L’inizio del computer quantistico: gli articoli di Feynman e Deutsch

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

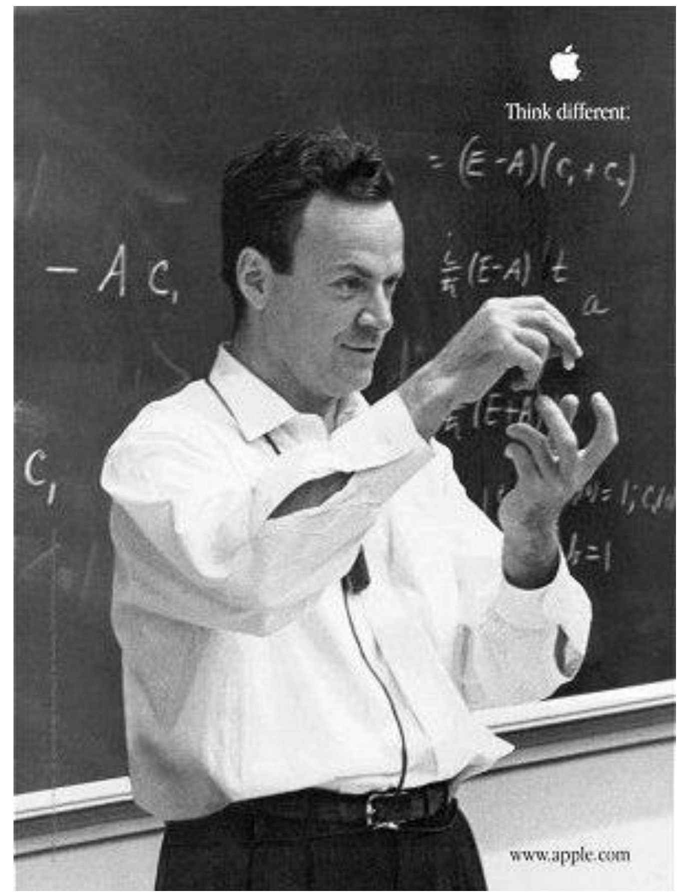
Received May 7, 1981

1. INTRODUCTION

On the program it says this is a keynote speech—and I don’t know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there’s no implication that anybody needs to talk about the same thing or anything like it. So what I want to talk about is what Mike Dertouzos suggested that nobody would talk about. I want to talk about the problem of simulating physics with computers and I mean that in a specific way which I am going to explain. The reason for doing this is something that I learned about from Ed Fredkin, and my entire interest in the subject has been inspired by him. It has to do with learning something about the possibilities of computers, and also something about possibilities in physics. If we suppose that we know all the physical laws perfectly, of course we don’t have to pay any attention to computers. It’s interesting anyway to entertain oneself with the idea that we’ve got something to learn about physical laws; and if I take a relaxed view here (after all I’m here and not at home) I’ll admit that we don’t understand everything.

The first question is, What kind of computer are we going to use to simulate physics? Computer theory has been developed to a point where it realizes that it doesn’t make any difference; when you get to a *universal computer*, it doesn’t matter how it’s manufactured, how it’s actually made. Therefore my question is, Can physics be simulated by a universal computer? I would like to have the elements of this computer *locally intercon-*

International Journal of Theoretical Physics, Vol. 21, Nos. 6/7, 1982



L'inizio del computer quantistico: gli articoli di Feynman e Deutsch

Quantum theory, the Church-Turing principle and the universal quantum computer

DAVID DEUTSCH*

Appeared in *Proceedings of the Royal Society of London A* **400**, pp. 97-117 (1985)[†]

(*Communicated by R. Penrose, F.R.S. — Received 13 July 1984*)

Abstract

It is argued that underlying the Church-Turing hypothesis there is an implicit physical assertion. Here, this assertion is presented explicitly as a physical principle: 'every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means'. Classical physics and the universal Turing machine, because the former is continuous and the latter discrete, do not obey the principle, at least in the strong form above. A class of model computing machines that is the quantum generalization of the class of Turing machines is described, and it is shown that quantum theory and the 'universal quantum computer' are compatible with the principle. Computing machines resembling the universal quantum computer could, in principle, be built and would have many remarkable properties not reproducible by any Turing machine. These do not include the computation of non-recursive functions, but they do include 'quantum parallelism', a method by which certain probabilistic tasks can be performed faster by a universal quantum computer than by any classical restriction of it. The intuitive explanation of these properties places an intolerable strain on all interpretations of quantum theory other than Everett's. Some of the numerous connections between the quantum theory of computation and the rest of physics are explored. Quantum complexity theory allows a physically more reasonable definition of the 'complexity' or 'knowledge' in a physical system than does classical complexity theory.

Introduzione:
Cos'è un computer quantistico?

computer classico:

INPUT → 01001011101011 → algoritmo → OUTPUT

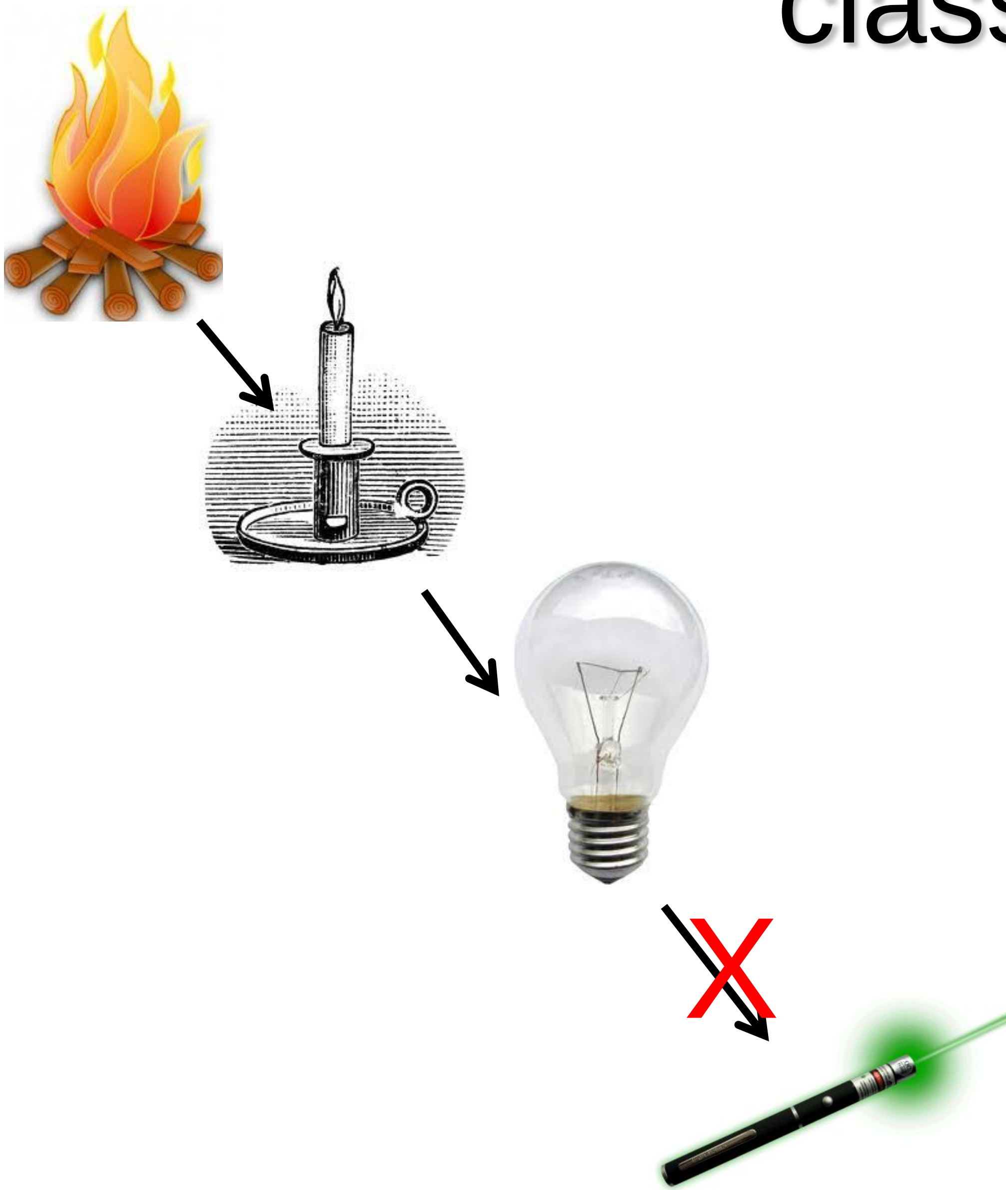
bit

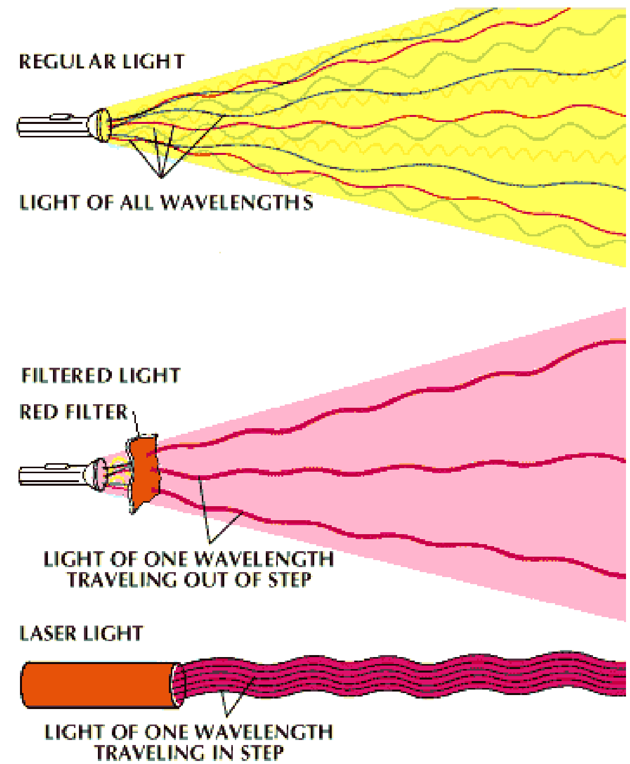
computer quantistico:

INPUT → 10011010011011
10101001011001
01010011001010 → algoritmo quantistico → OUTPUT

qubit

Il computer quantistico è fondamentalmente diverso da quello classico!

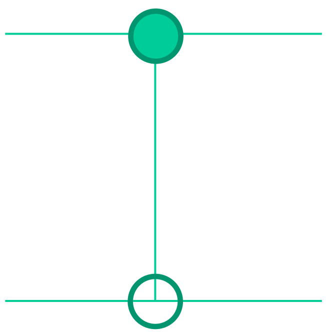




Concetto di base di un computer quantistico

Set di porte quantistiche universali: cNOT e porta a singolo qubit

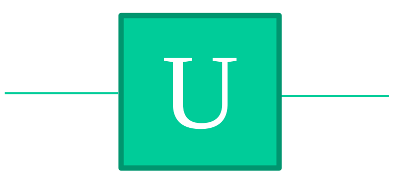
controllo



target

porta cNOT

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} I & 0 \\ 0 & \sigma_x \end{pmatrix}$$

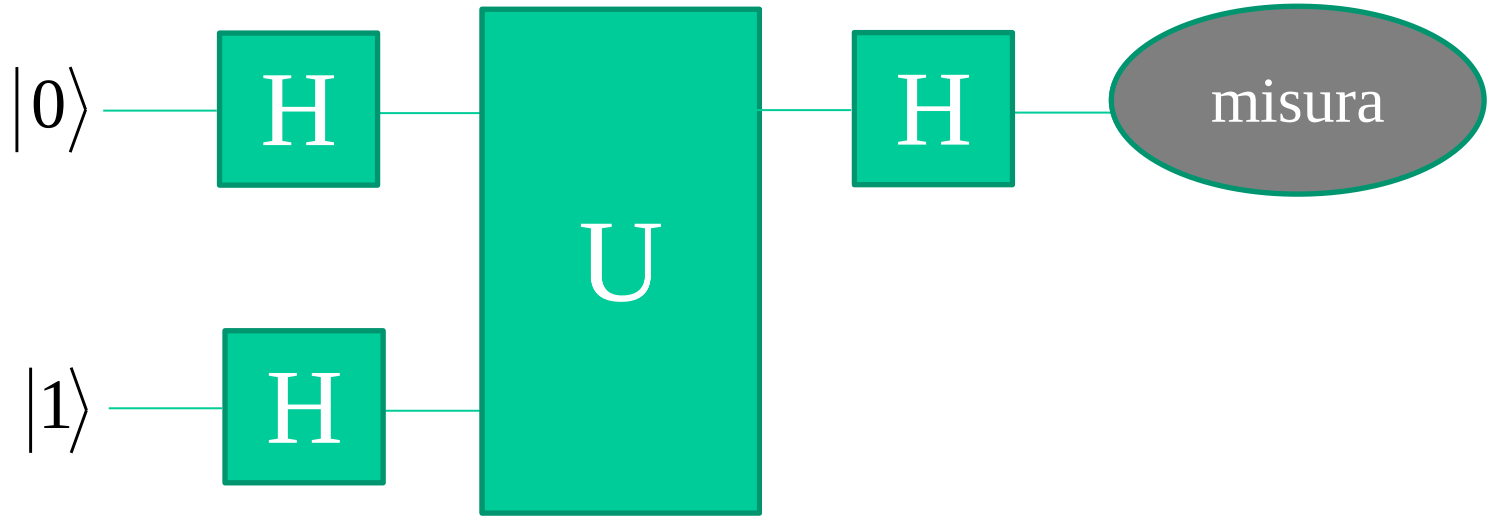


porta a singolo qubit, e.g.
porta di Hadamard H

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

trasforma |0> e |1> in
stati di sovrapposizione

Esempio di un algoritmo quantistico



algoritmo di Deutsch (controlla se una funzione e costante o bilanciata)

Introduzione:
a cosa serve un computer quantistico?

sfruttando il parallelismo quantistico diventano possibili algoritmi efficienti per problemi che con algoritmi classici non si possono risolvere in tempi utili

algoritmo di Shor:
fattorizzazione di numeri;
tempo di calcolo cresce come L^3 anziché $\exp(L^{1/3})$

algoritmo di Grover:
ricerca in un database;
tempo di ricerca cresce come sqrt(N) anziché N/2

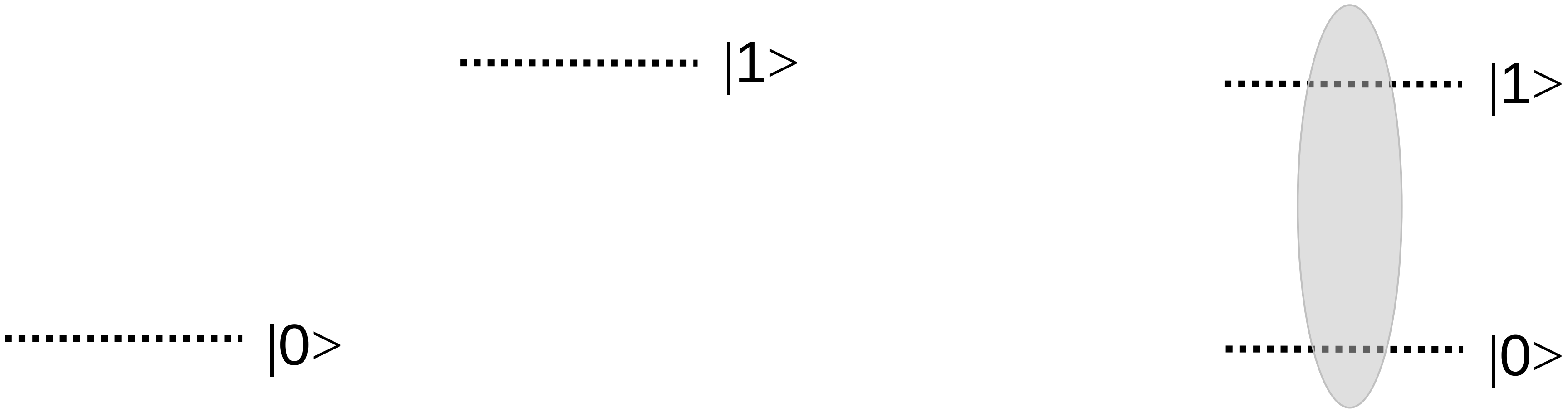
algoritmo di Deutsch-Josza:
decidere se una moneta è truccata;
basta 1 tentativo anziché 2

Principi della fisica quantistica

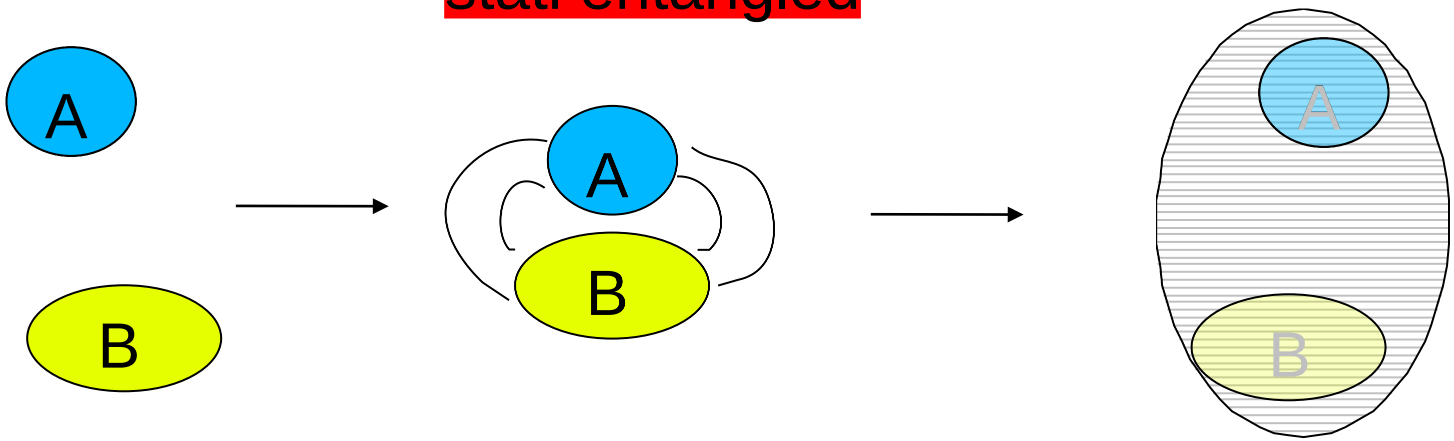
sovrapposizione

fisica classica

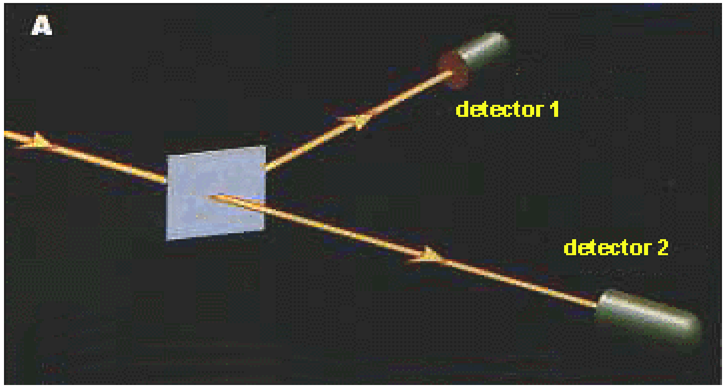
fisica quantistica

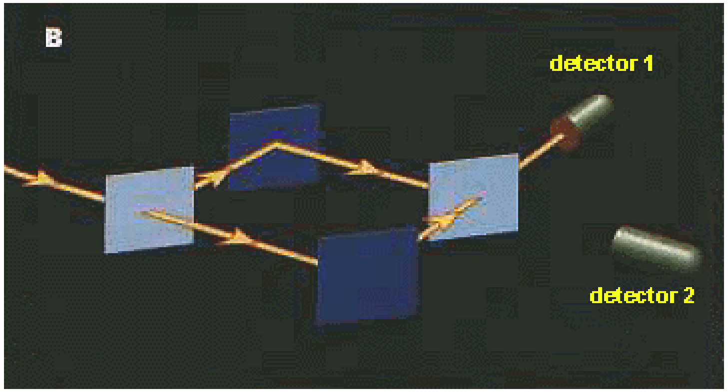


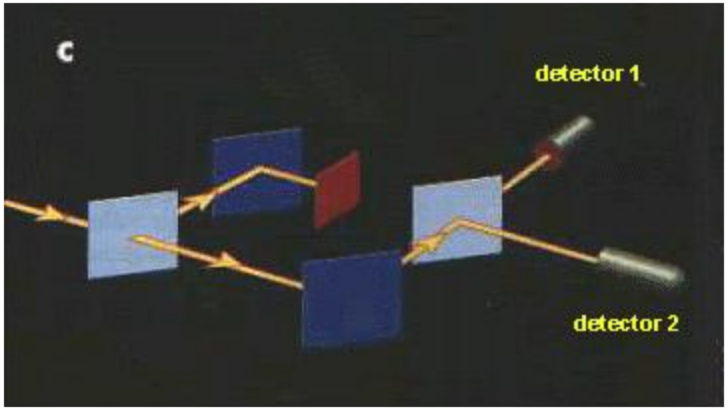
stati entangled



Fisica quantistica: *principio di sovrapposizione*







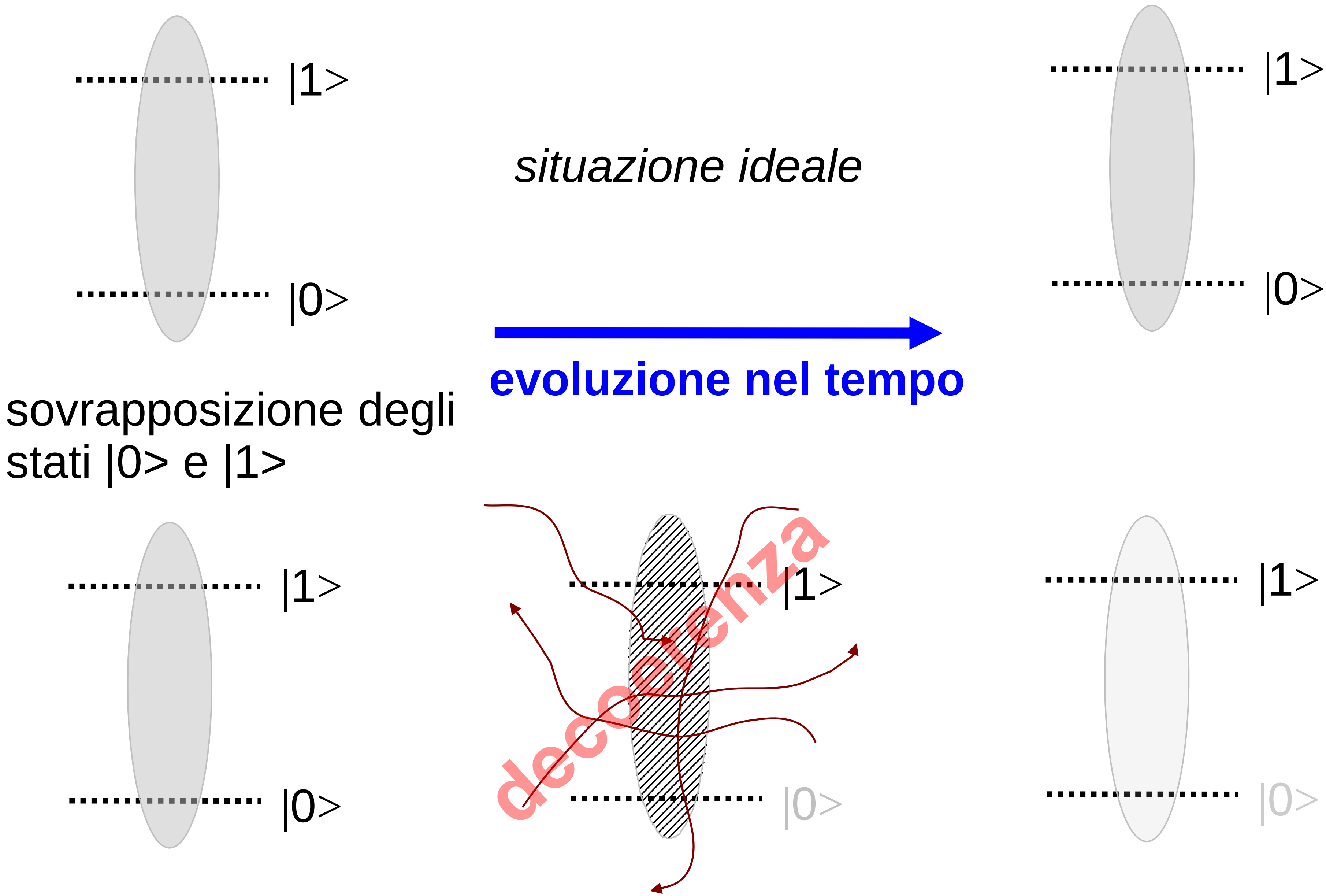
Cosa ci vuole:
I criteri di Di Vincenzo

- **Scalabilità e qubits ben definiti**
- **Possibilità di inizializzare lo stato dei qubit**
- Tempo di coerenza molto maggiore al tempo di un gate
- **Un set universale di gates quantistici**
- **Possibilità di leggere selettivamente i qubits**

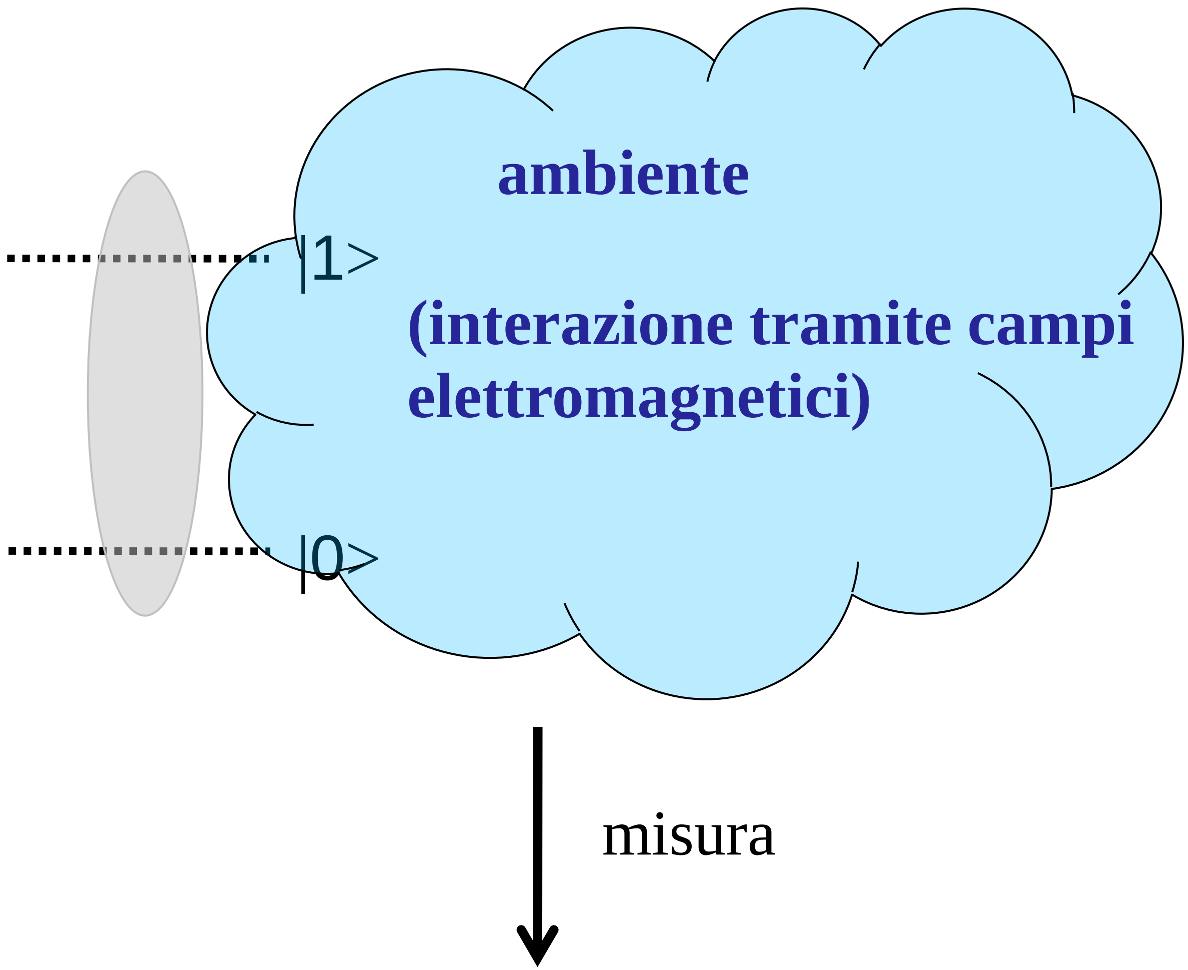
e in più, per creare reti di computer quantistici:

- **possibilità di convertire qubit stazionari in qubit volanti**
- **possibilità di trasmettere qubit volanti**

Problema principale della realizzazione: la *decoerenza*



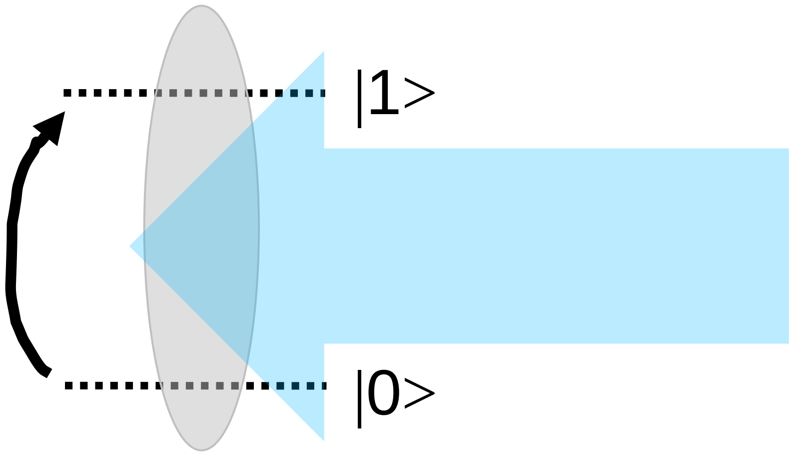
Che cosa provoca la decoerenza?



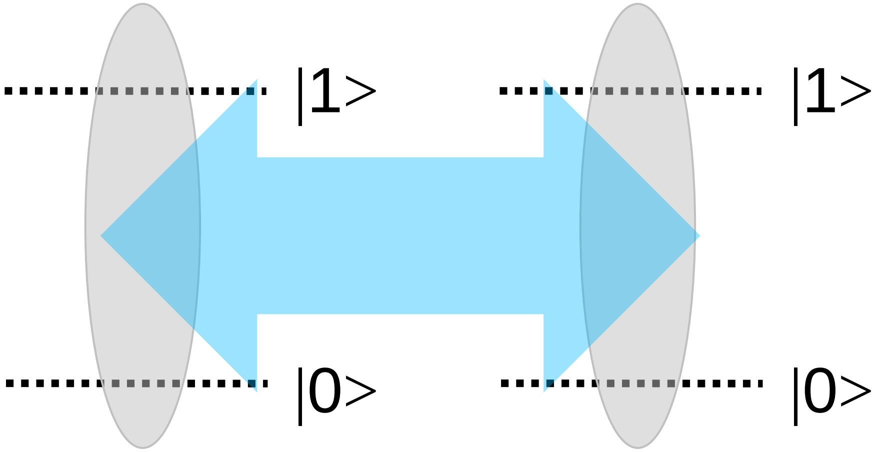
traccia sugli stati dell'ambietene -> coerenza sparisce, sembra stato misto

Basta eliminare qualsiasi interazione?

NO!

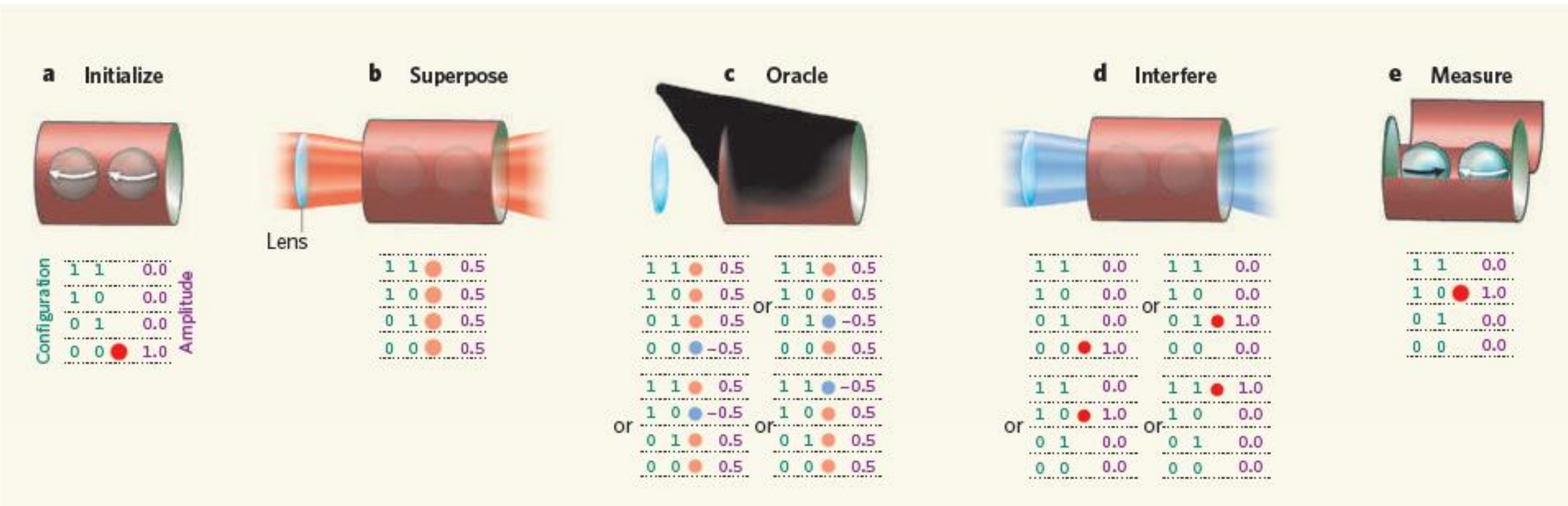


per controllare il qubit (cioè, effetuare porte a singolo qubit) bisogna far interagire il sistema con un campo esterno, per esempio un fascio laser oppure delle microonde

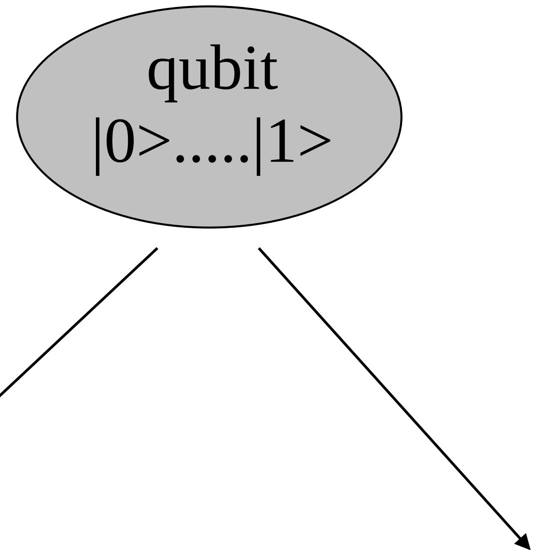


per le porte a 2 qubit (es.: CNOT), due qubit devono interagire (più forte l'interazione, più veloce la porta!)

Concetto di base di un computer quantistico



Qubits «naturali» ed «artificiali»



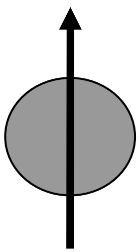
«naturali»:
- atomi
- molecole
- fotoni

«artificiali»:
- superconduttori
- quantum dots
- impurità

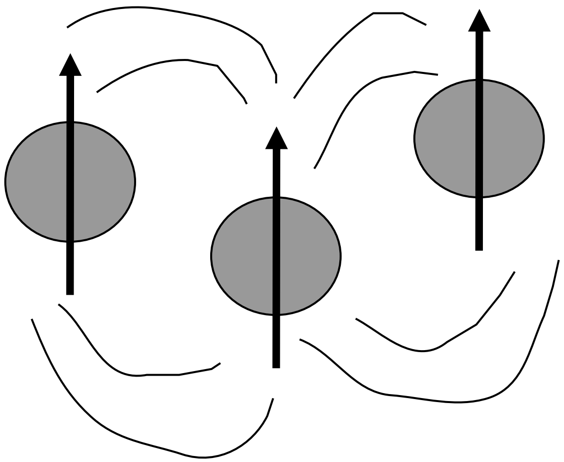
Stato dell'arte:
I sistemi fisici sotto indagine

- **NMR (risonanza magnetica):** spin nucleari in una molecola
- **Ioni intrappolati**: stato interno dell'ione
- **Reticoli ottici:** stato interno di atomi dentro un potenziale periodico
- **fotoni**
- **Stato solido**
- **Superconduttori**

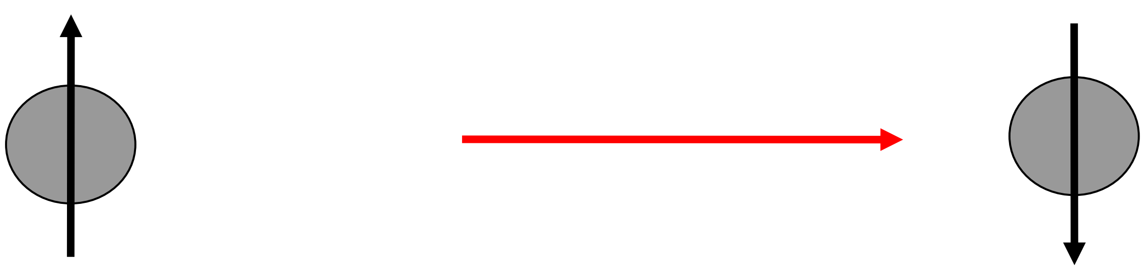
NMR (risonanza magnetica)



nucleo con spin /
momento magnetico



campo elettromagnetico

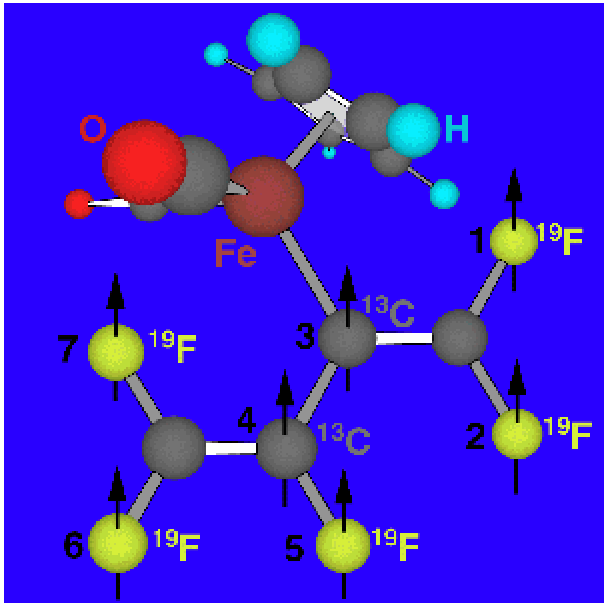


questa frequenza dipende da interazioni con altri spin

lo spin cambia direzione per una frequenza ben definita del campo elettromagnetico

Computer quantistico NMR

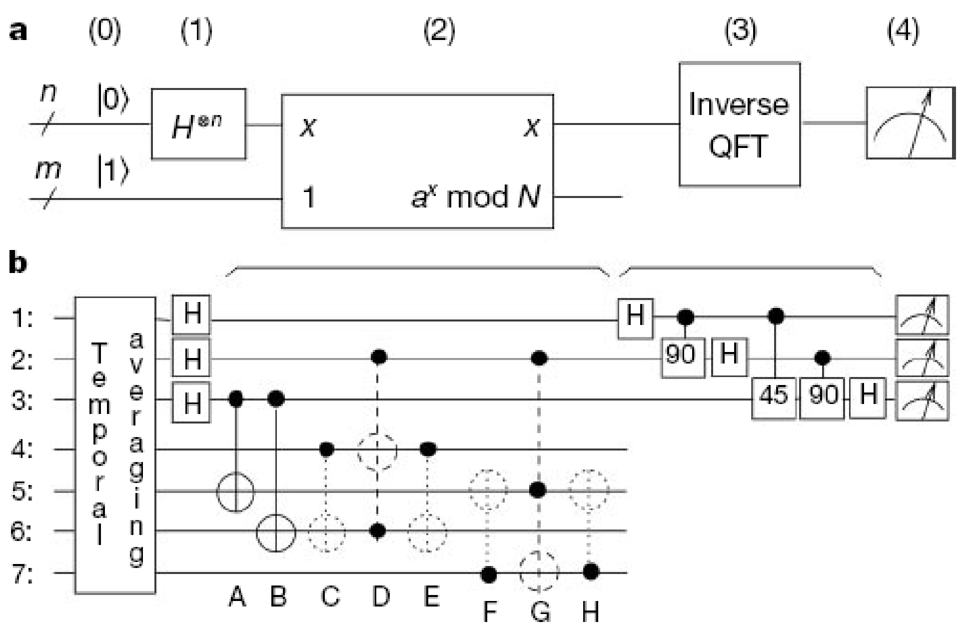
con NMR, si può estrarre l'architettura di una molecola

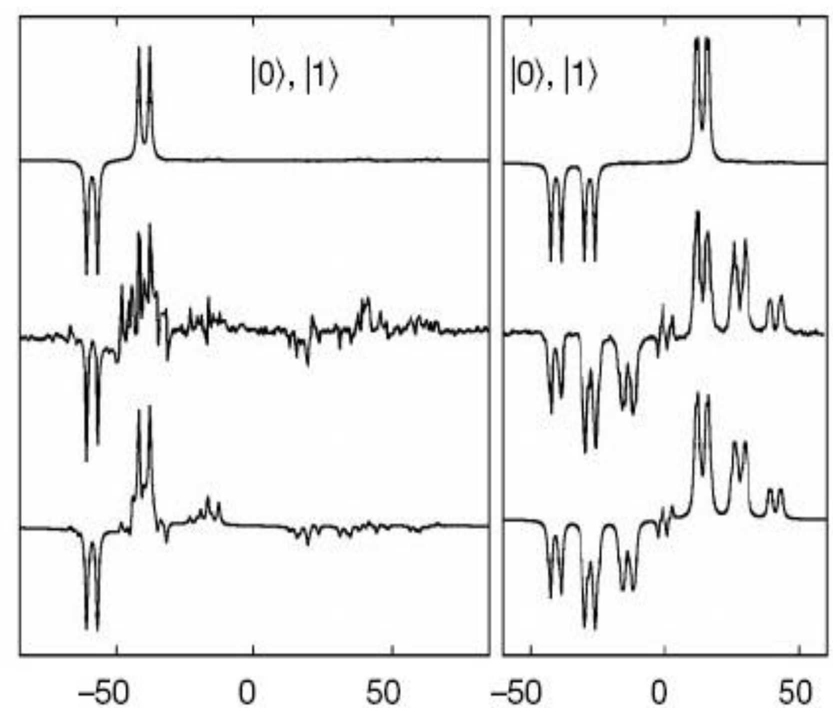


conoscendo l'architettura della molecola, con NMR si può agire in maniera controllata sui suoi spin

agendo sugli spin e sfruttando le loro interazioni, si può inizializzare un registro e si possono applicare dei gates

Computer quantistico NMR





Computazione quantistica con ioni: *la proposta di Cirac e Zoller (1995)*

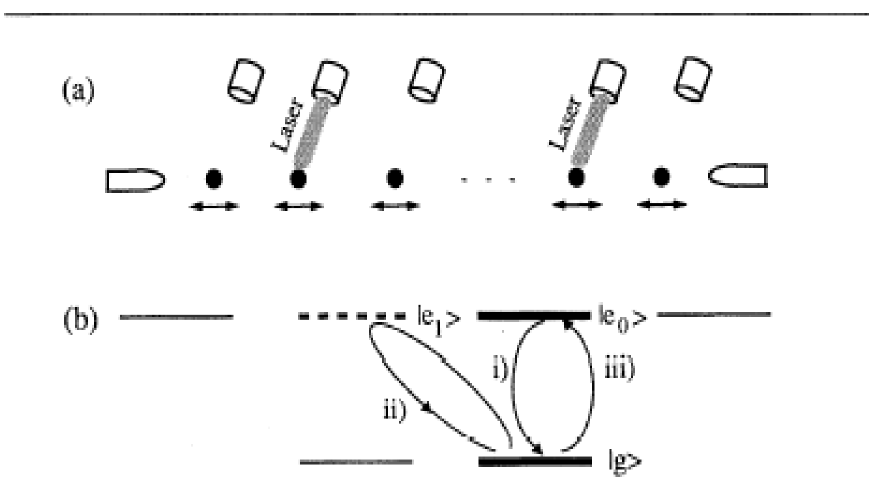
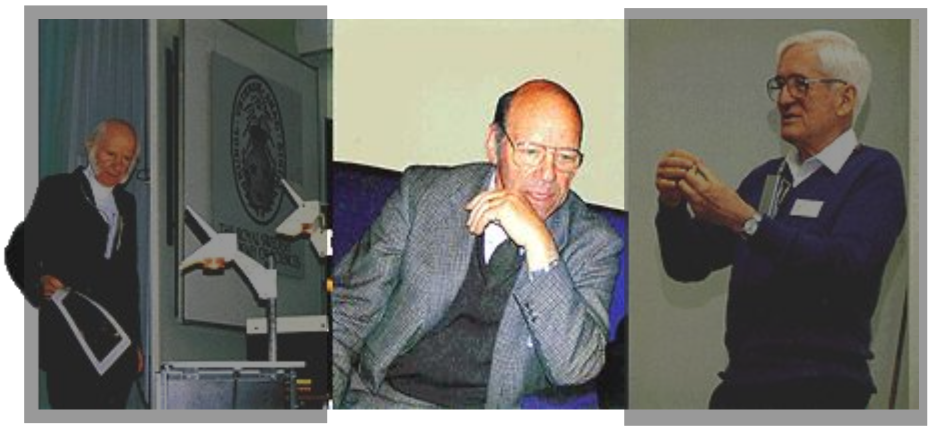


FIG. 1. (a) N ions in a linear trap interacting with N different laser beams; (b) atomic level scheme.

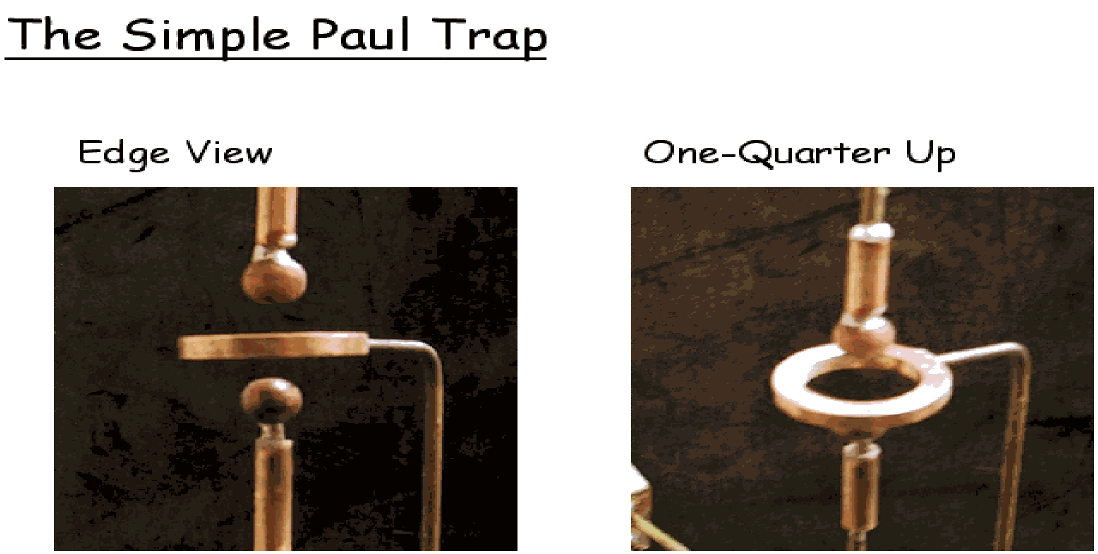
In this Letter we show that a set of N cold ions interacting with laser light and moving in a linear trap [7] provides a realistic physical system to implement a quantum computer. The distinctive features of this system are (i) it allows the implementation of n-bit quantum gates between any set of (not necessarily neighboring) ions, (ii) decoherence can be made negligible during the whole computation, and (iii) the final readout can be performed with unit efficiency.

Phys. Rev. Lett. 74, 4091 (1995)

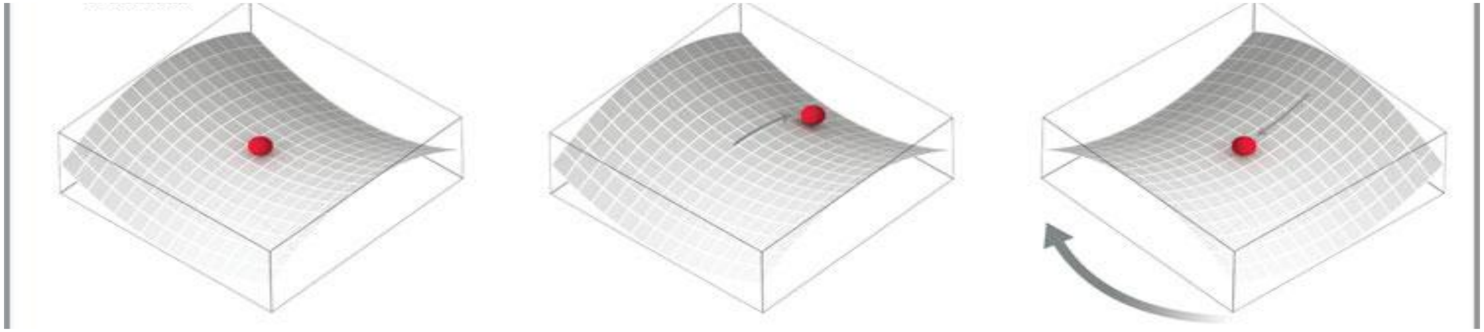
Cenni storici: la trappola di Paul



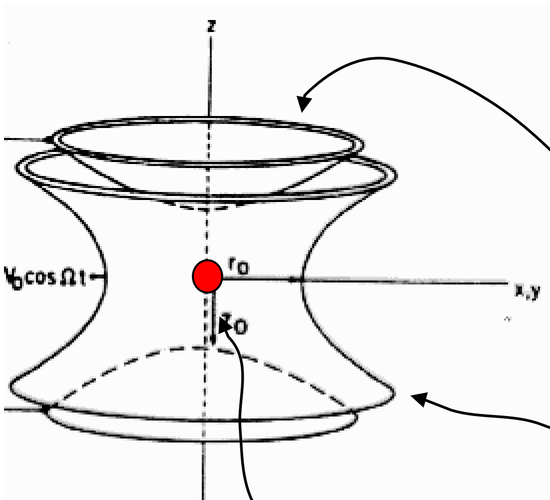
W. Paul 1958: trappola dinamica per ioni; usata per riferimenti stabili di frequenza (premio Nobel 1989)



La «sella ruotante»



Ioni intrappolati: *tecniche*

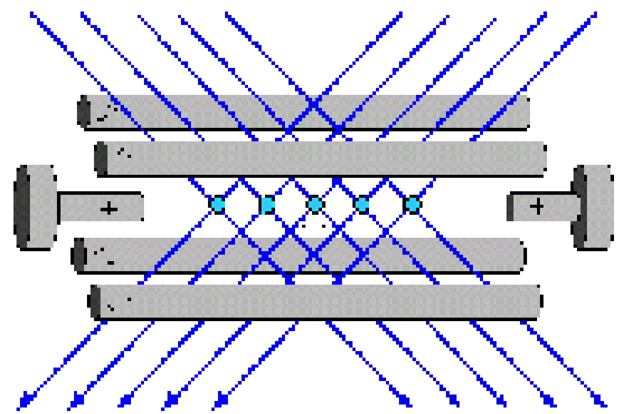


tecnica di base: la trappola di Paul

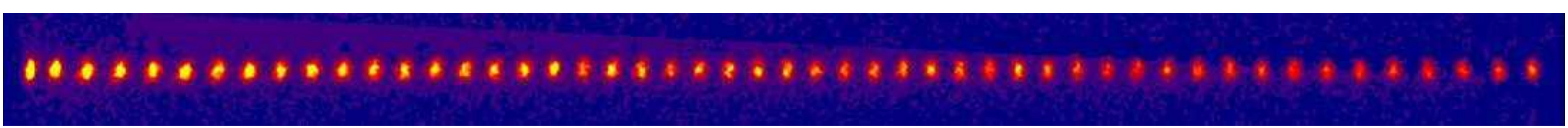
campi elettrici oscillanti che creano una trappola stabile (“sella ruotante”)

ione intrappolato

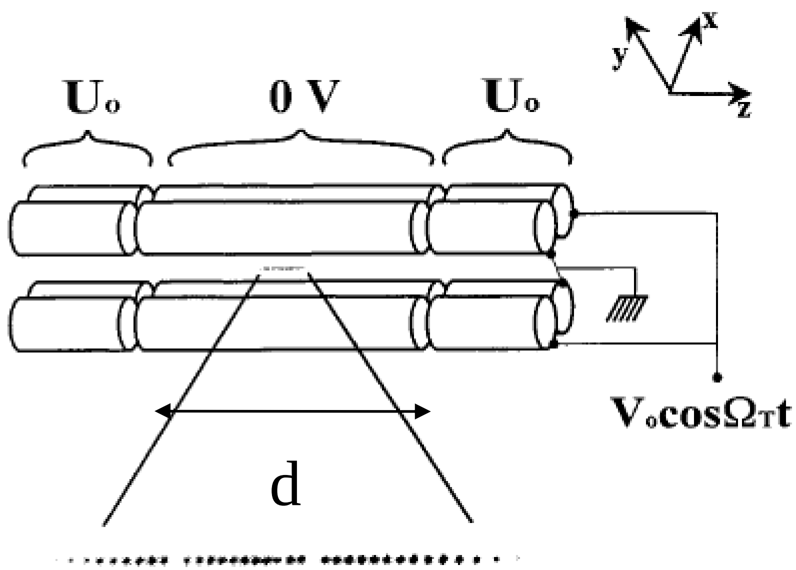
trappola di Paul **lineare**

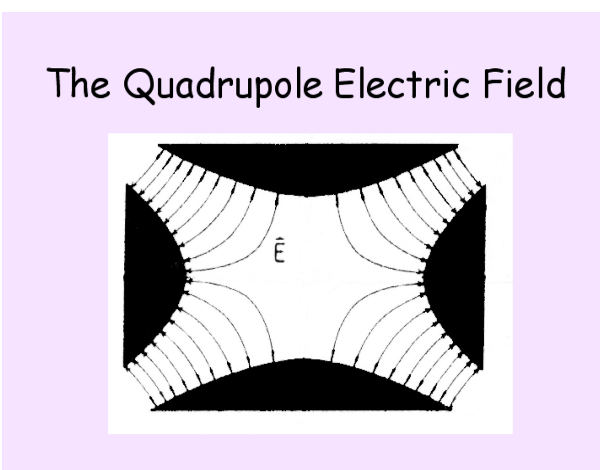


catena di ioni interagenti tramite repulsione di Coulomb

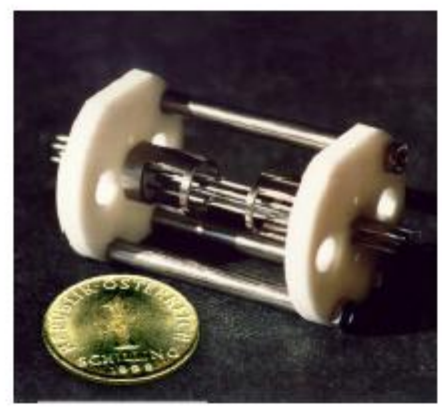


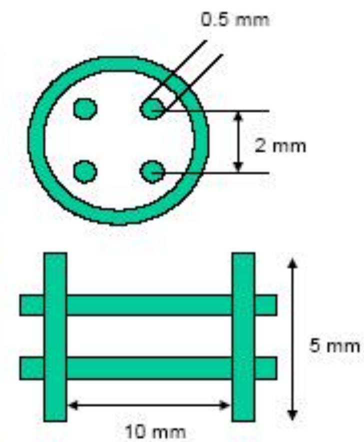
Trappola di Paul: *parametri tipici*





separazione degli elettrodi: 100 micrometri fino a alcuni mm;
campo r.f.: 10-300 Mhz;
$\mathbf{V_0}$~ 100 V

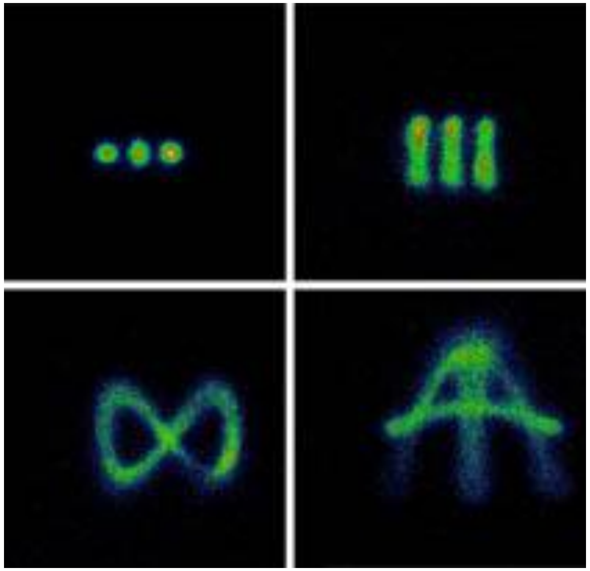




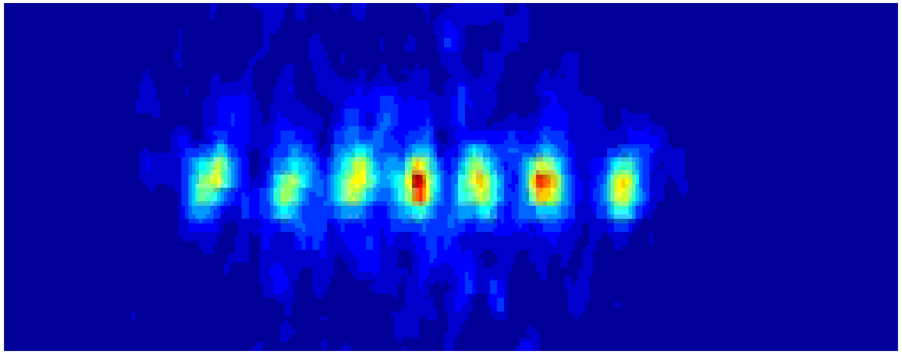
$\kappa \approx 0.05$ $\omega_z \approx 700$ kHz $\omega_{x,y} \approx 1.2 - 2$ MHz

=> **frequenza radiale di trappola:** da 100 kHz a 10 Mhz;
separazione tra due ioni: 1 micrometro fino a 15 micrometri

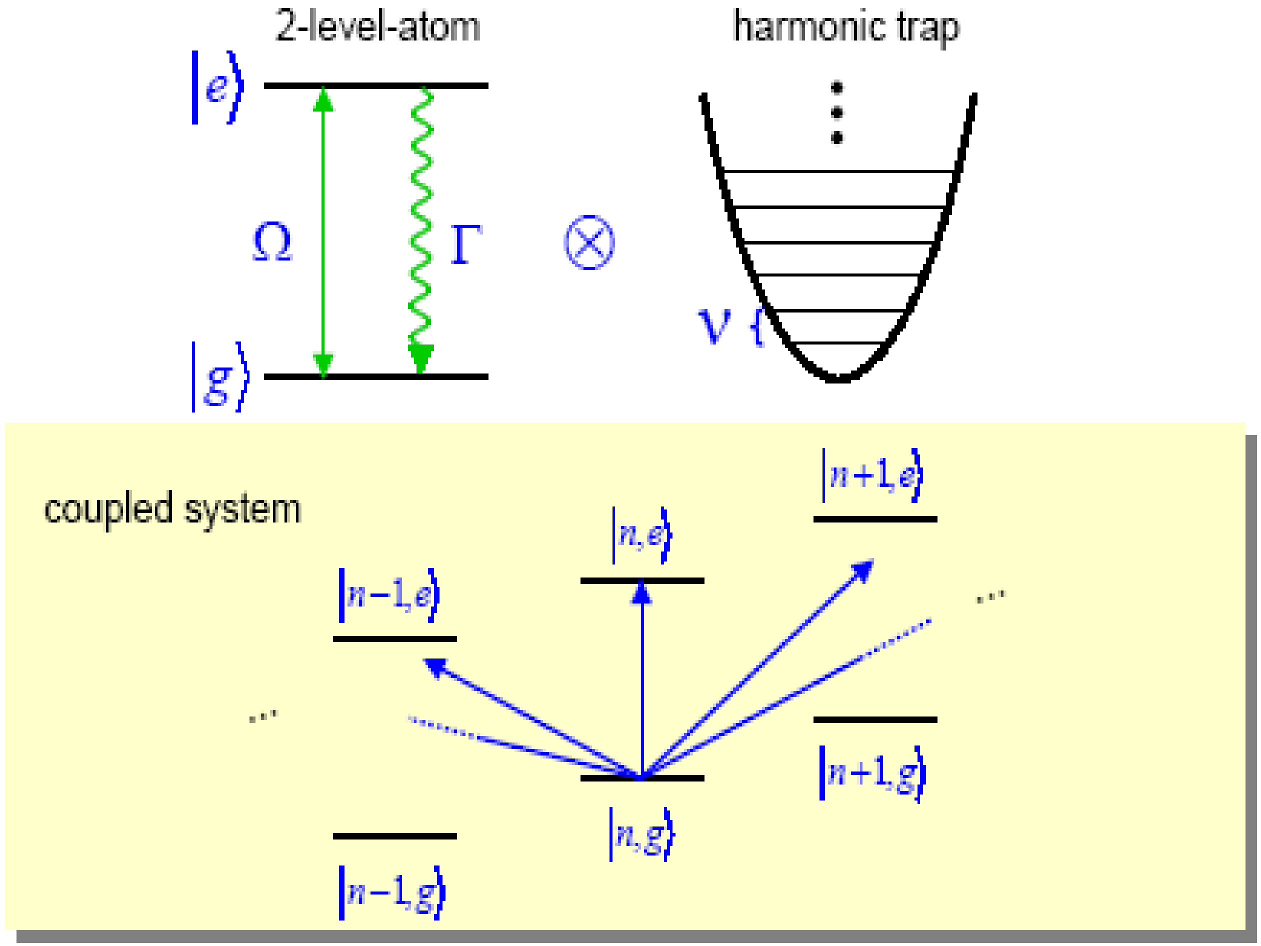
Ioni intrappolati: *tecniche*



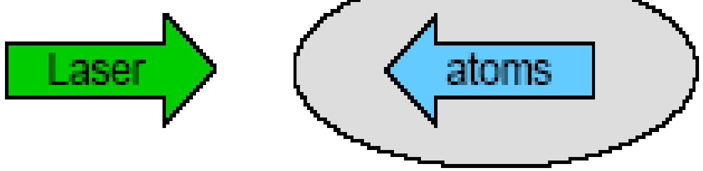
creazione di stati di moto degli ioni -> stati entangled

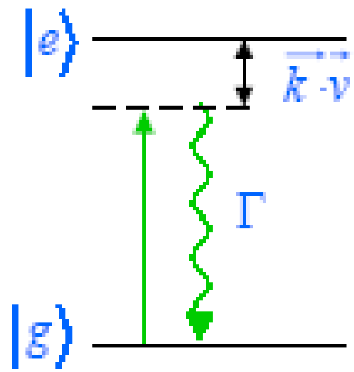


Moto quantistico degli ioni

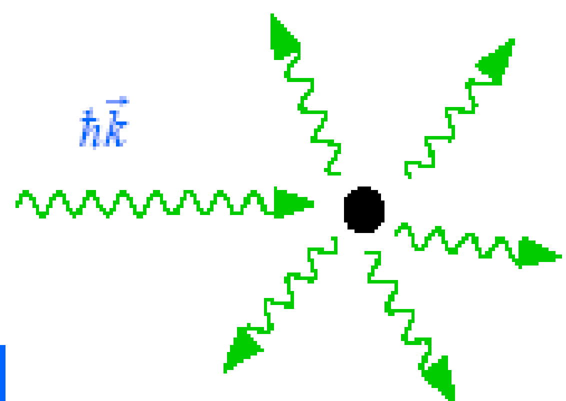


Raffreddamento laser





momentum transfer $\hbar\vec{k}_{abs},\ -\hbar\vec{k}_{em}$



$$\frac{|\hbar\vec{k}|}{m} = \Delta v \approx 1\,cm/s$$

$$\Delta\vec{p} = n\hbar\vec{k}_{abs} + \underbrace{\sum \hbar\vec{k}_{em}}_{=0}$$

$$\Delta\vec{p} = \langle n\rangle\hbar\vec{k}_{abs}$$

Doppler cooling limit:

$$E_D = \hbar\frac{\Gamma}{2}$$

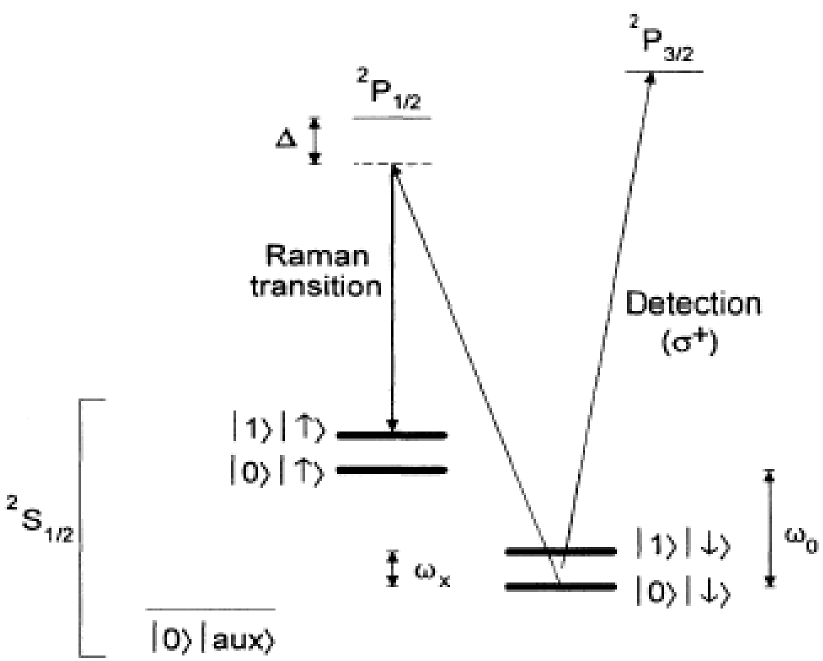
Realizzazione del CNOT

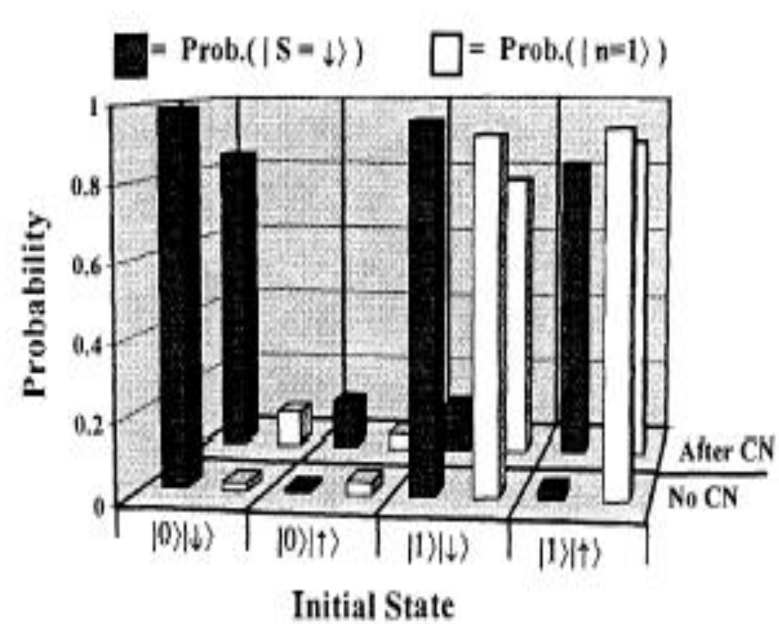
VOLUME 75, NUMBER 25 PHYSICAL REVIEW LETTERS 18 DECEMBER 1995

Demonstration of a Fundamental Quantum Logic Gate

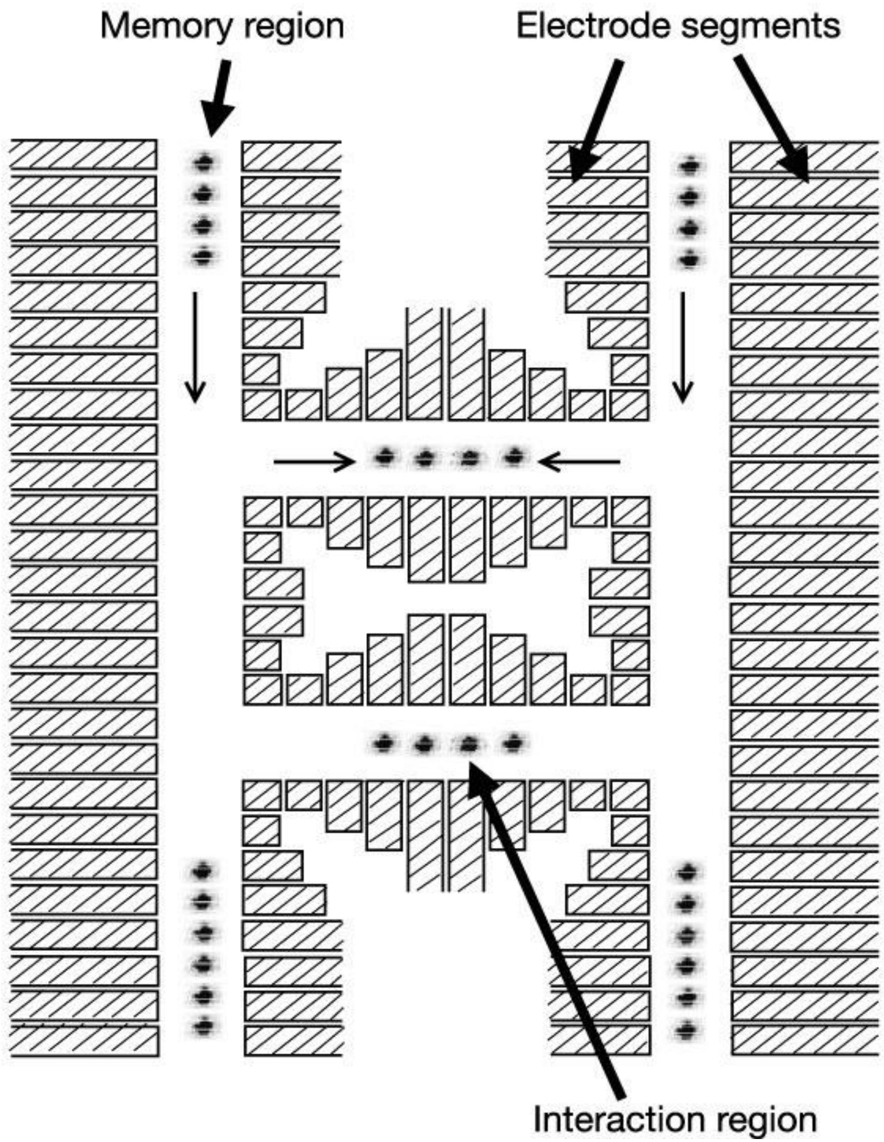
C. Monroe, D. M. Meekhof, B. E. King, W. M. Itano, and D. J. Wineland
National Institute of Standards and Technology, Boulder, Colorado 80303
(Received 14 July 1995)

We demonstrate the operation of a two-bit "controlled-NOT" quantum logic gate, which, in conjunction with simple single-bit operations, forms a universal quantum logic gate for quantum computation. The two quantum bits are stored in the internal and external degrees of freedom of a single trapped atom, which is first laser cooled to the zero-point energy. Decoherence effects are identified for the operation, and the possibility of extending the system to more qubits appears promising.



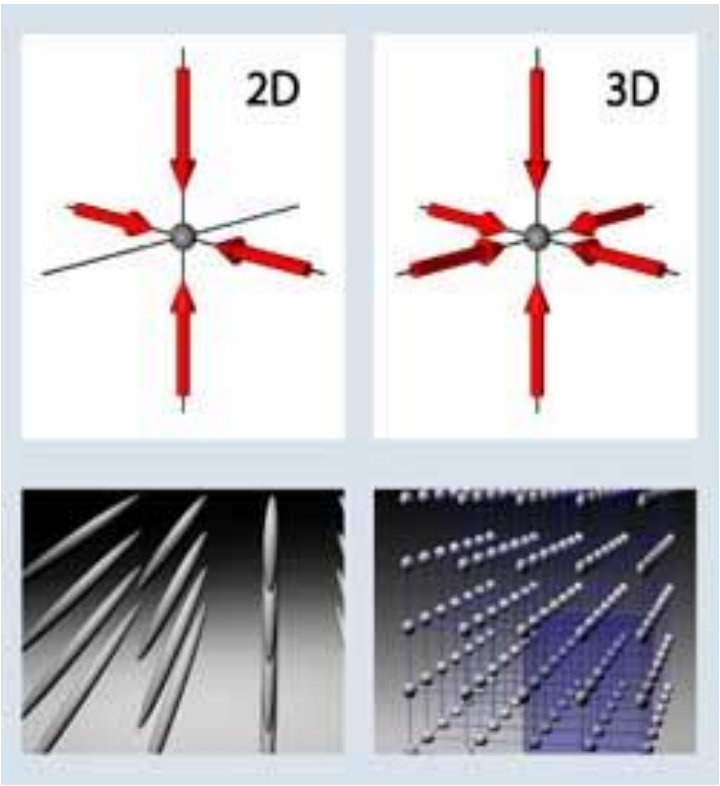


Ioni intrappolati: *tecniche*



Nature **417**, 709

Atomi neutri in reticoli ottici



vantaggi:

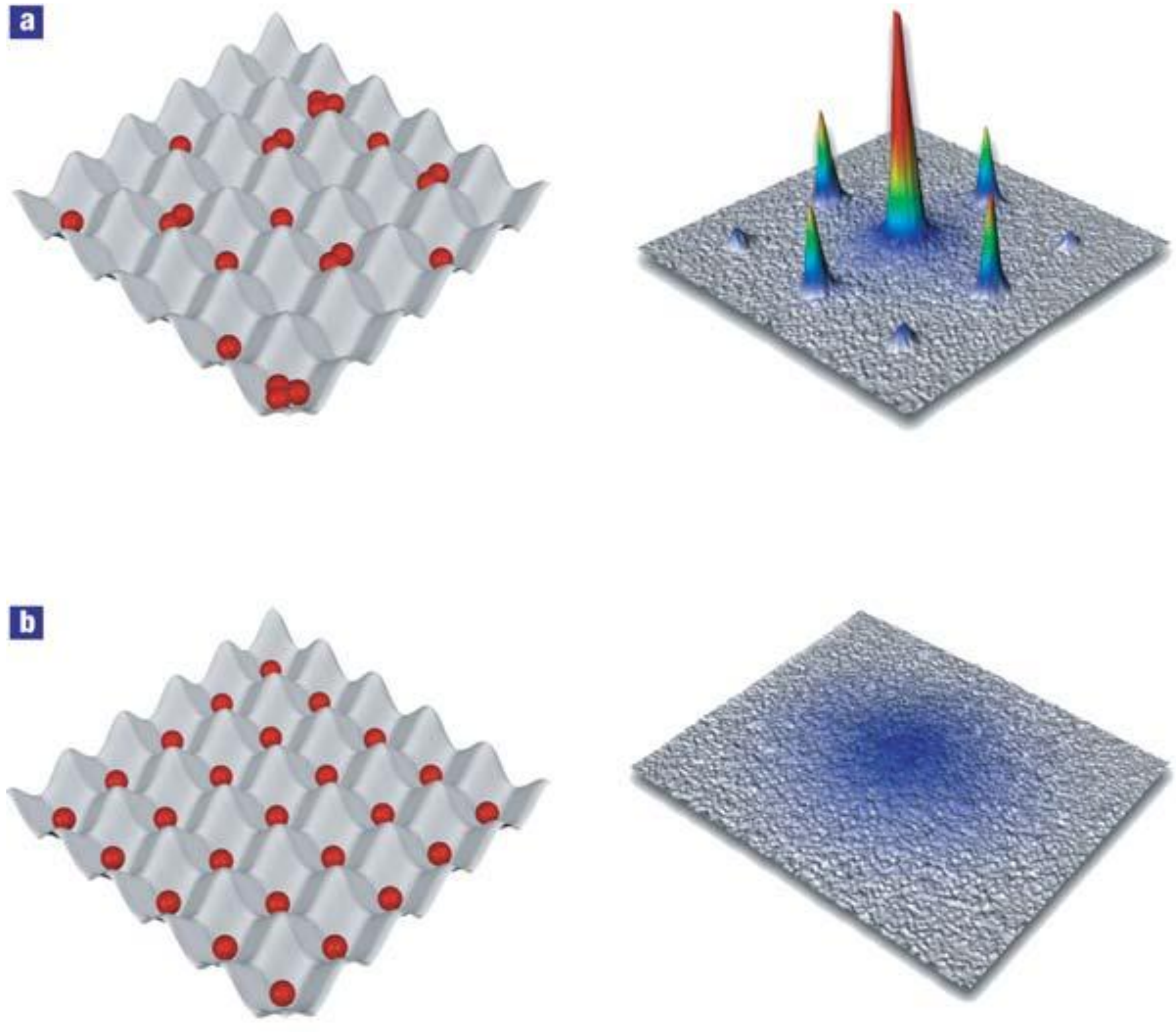
- controllo eccellente sulla geometria del reticolo
- atomi neutri interagiscono meno con l'ambiente
- sfrutta tecnologie ben studiate

svantaggi:

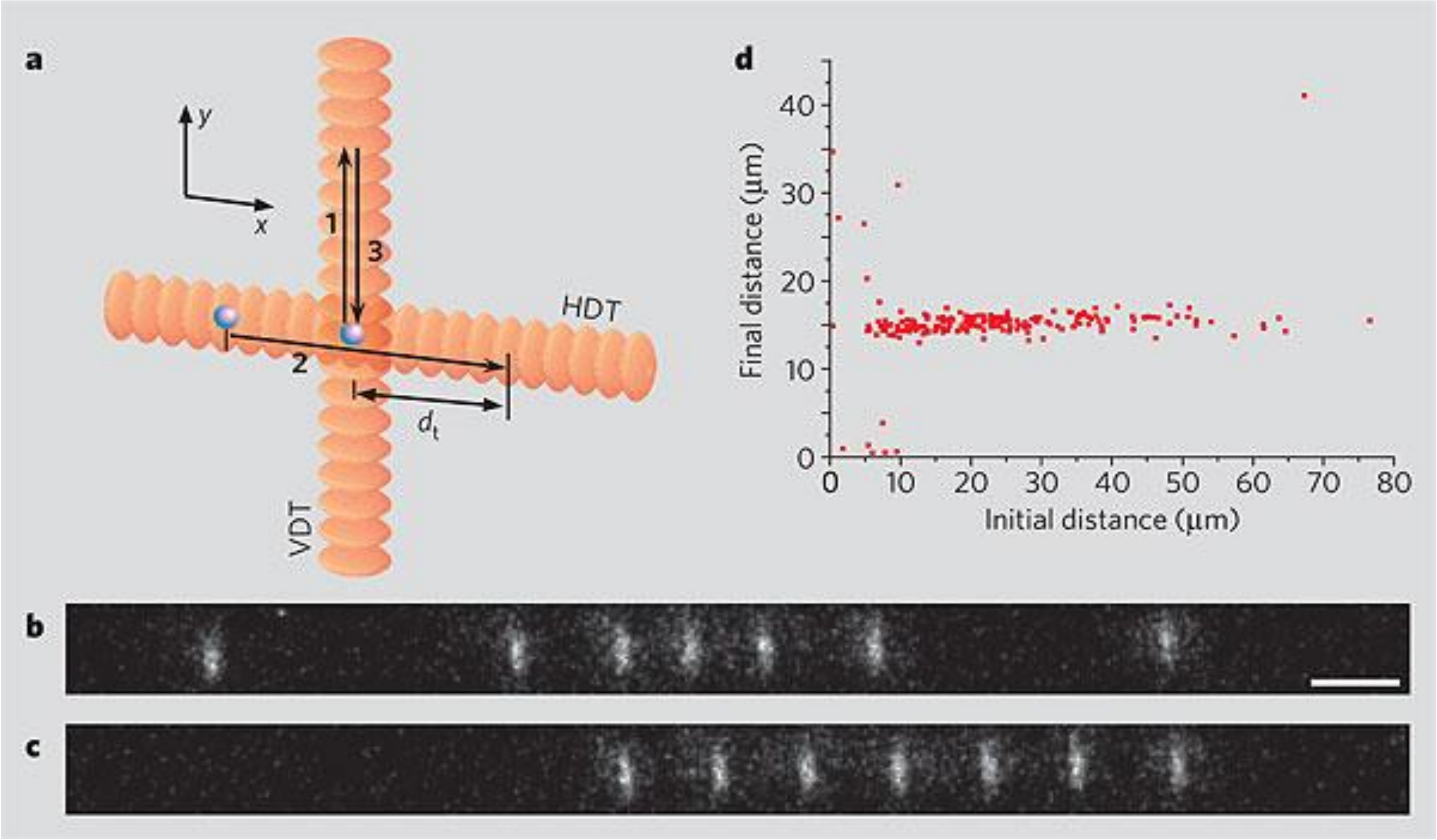
- difficile accedere a un singolo atomo
- mancanza di un'interazione forte tra gli atomi

fasci laser incrociati creano un “cristallo artificiale” in cui gli atomi vengono intrappolati in delle mini-gabbie

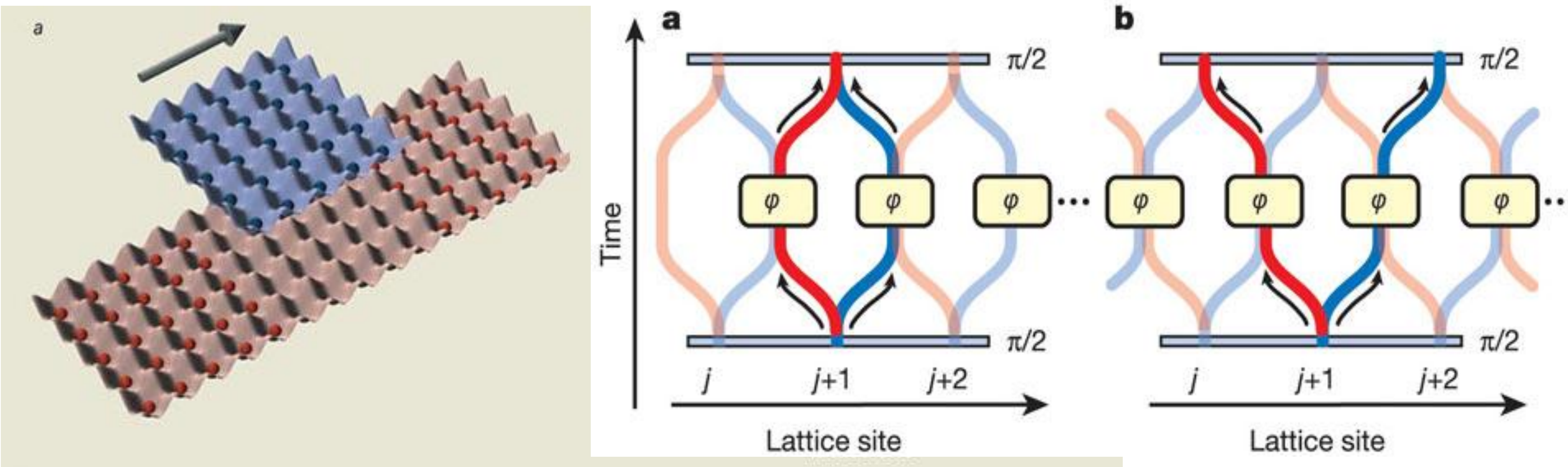
L'isolante di Mott



Approcci alternativi

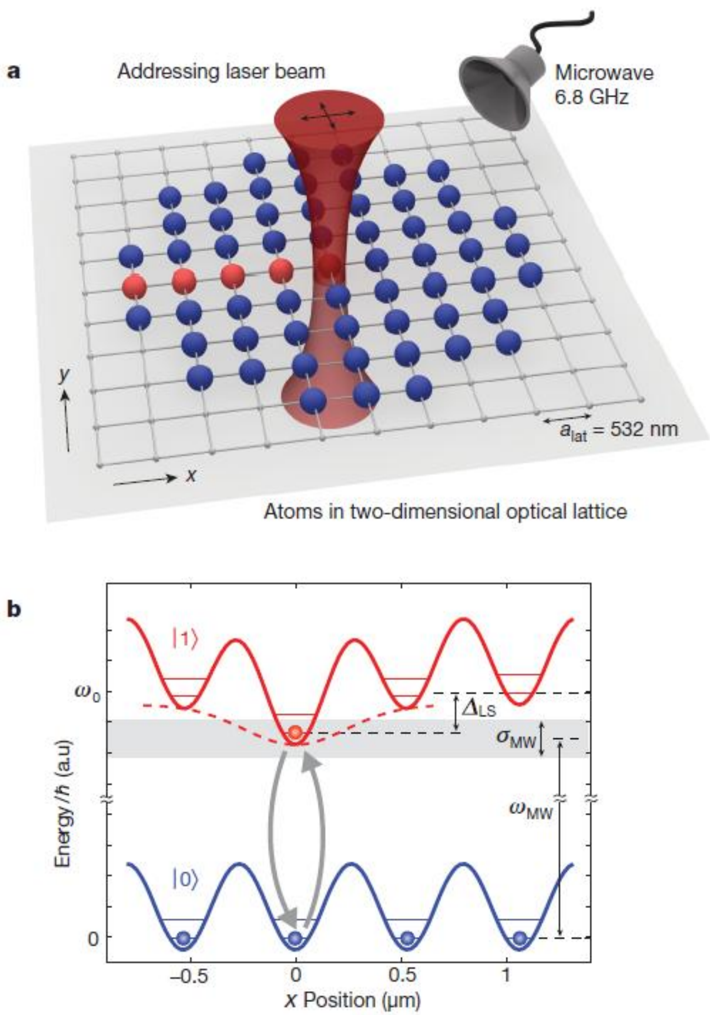


Atomi neutri in reticoli ottici: *creazione di stati entangled*



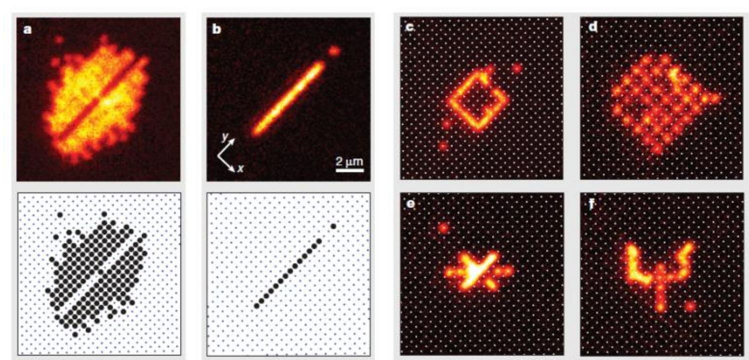
Nature **425**, 937

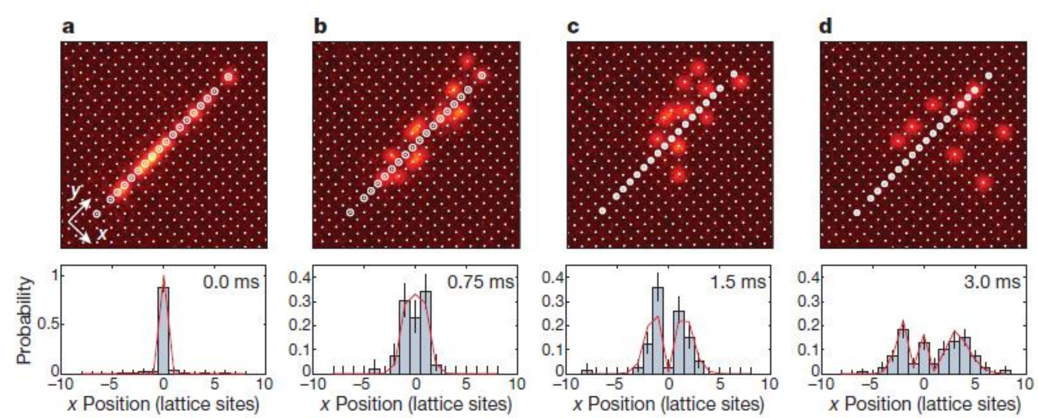
Atomi neutri in reticoli ottici



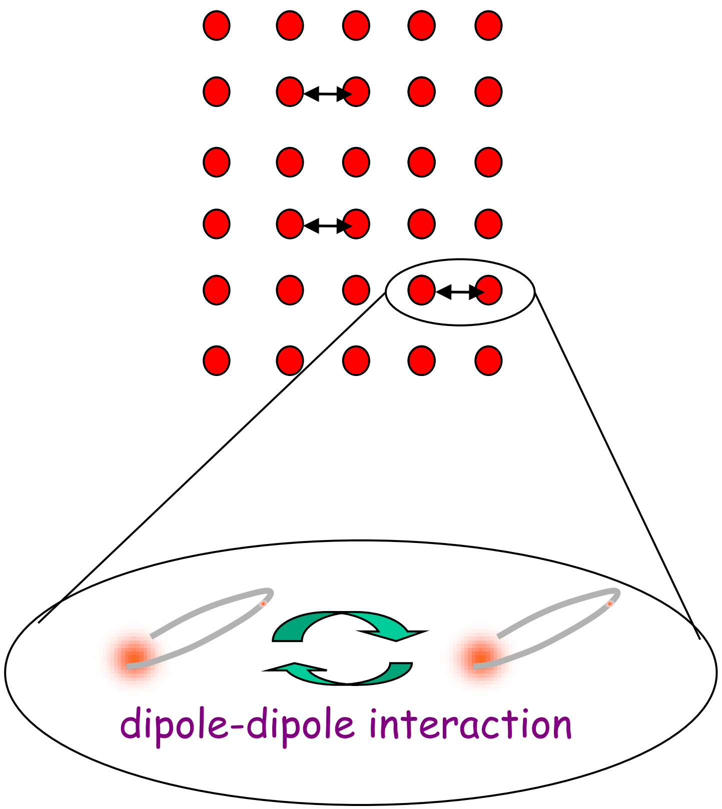
Single-spin addressing in an atomic Mott insulator

Christof Weitenberg[1], Manuel Endres[1], Jacob F. Sherson[1]†, Marc Cheneau[1], Peter Schauß[1], Takeshi Fukuhara[1], Immanuel Bloch[1,2] & Stefan Kuhr[1]





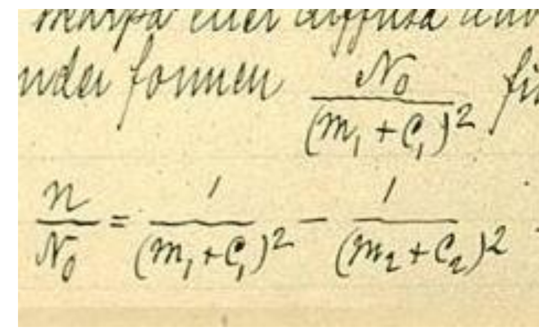
Porte quantistiche con stati di Rydberg



Properties of Rydberg atoms:

High principal quantum number "n"

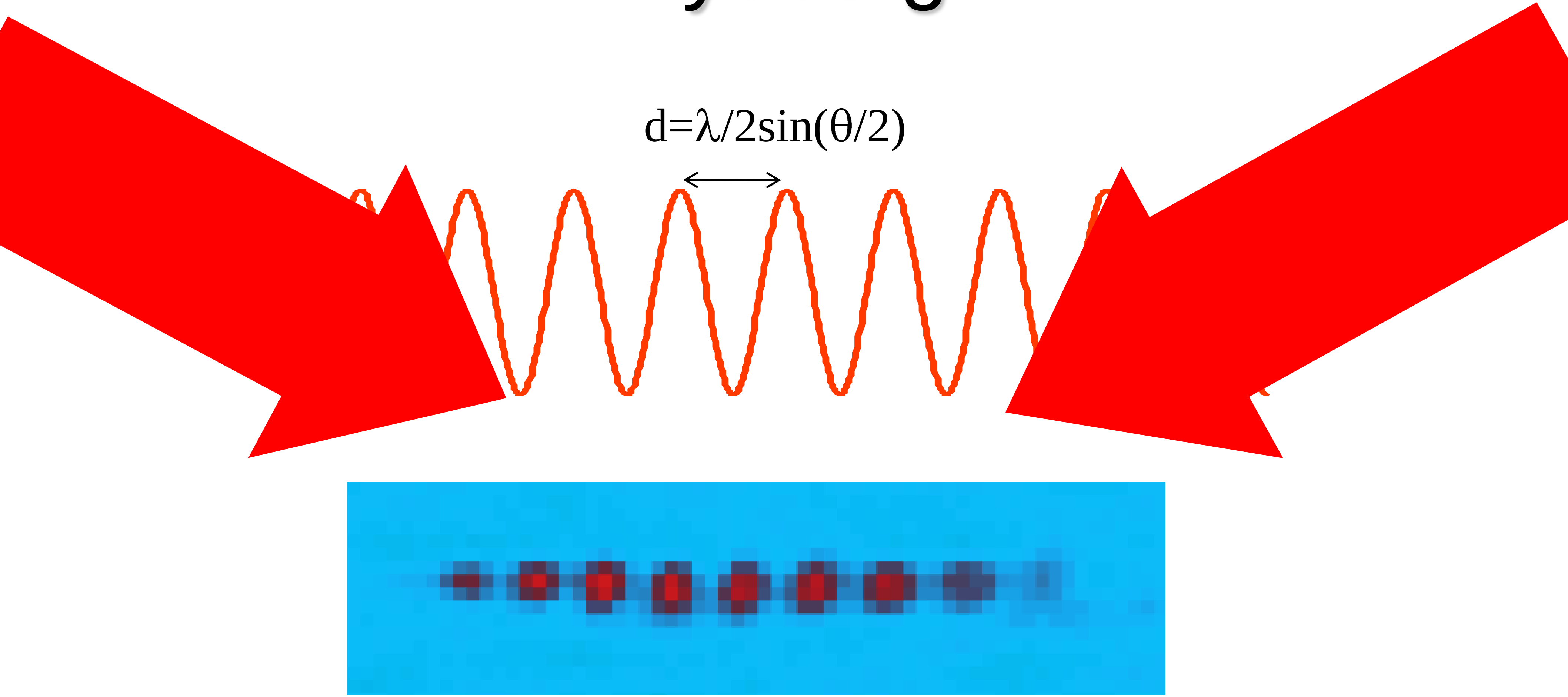
- Classical radius : ~ $2\ n^2\ a_0$
  n=1 0.5A n=100 1 μm n=200 4μm



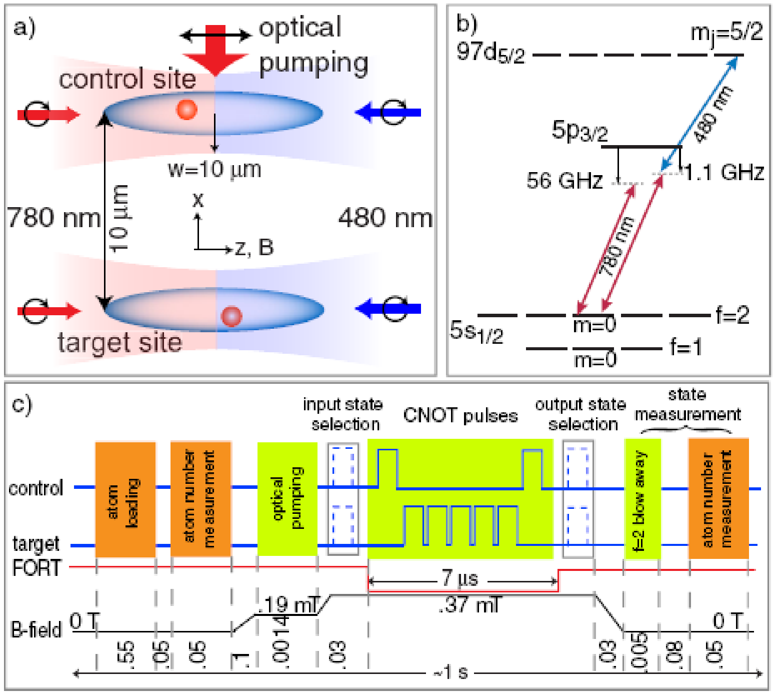
- Lifetime: ~ n^3
  n=100 1 ms
- Ionization field E_{ion} ~ n^{-4}
  n=100 10 V/cm
- Polarizability ~ n^7
  Dipole moment : ~ $n^2\ ea_0$
  n=100 10,000 D (H_2O ~2 D)

→ Long range dipole-dipole interaction

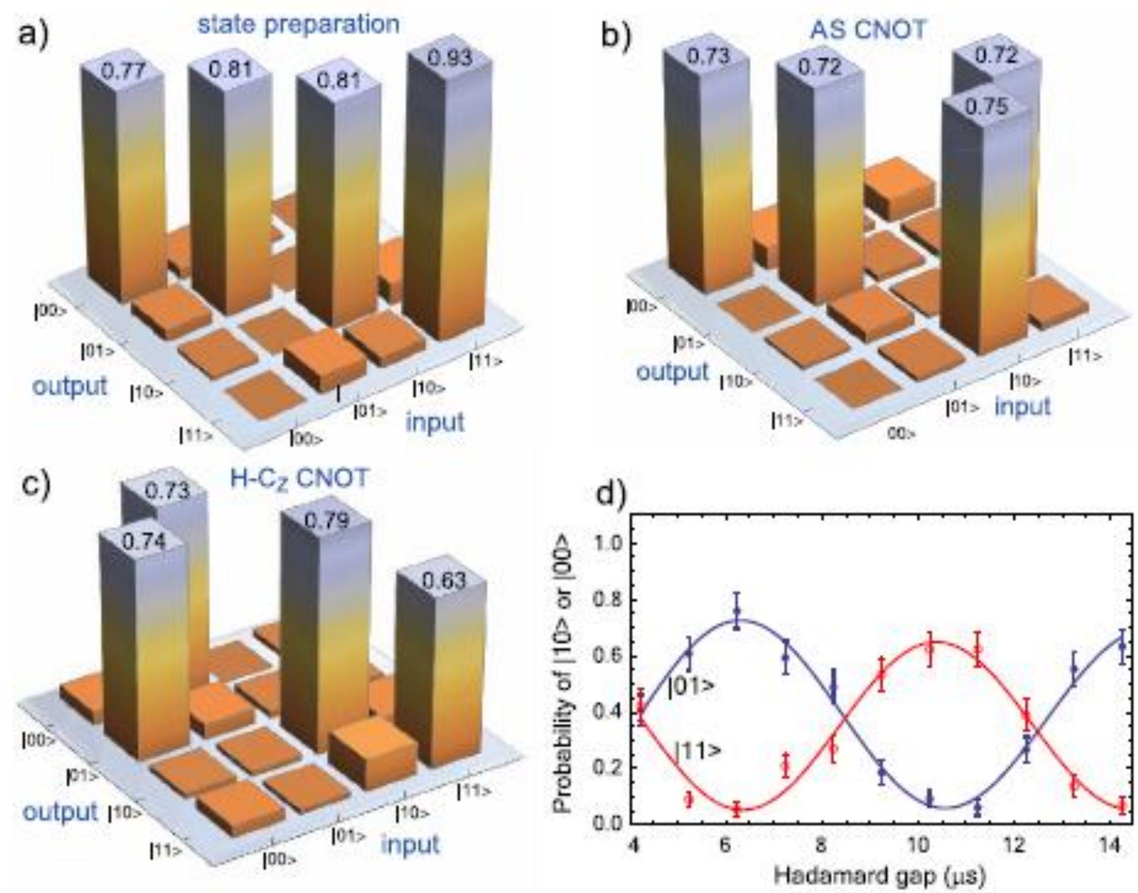
Porte quantistiche con stati di Rydberg



Porte quantistiche con stati di Rydberg



Rydberg cNOT gate



NMR, ioni, reticoli:
cosa riescono a fare?

NMR: algoritmo di Deutsch-Josza; algoritmo di Shor (fattorizza 15)

Nature **393**, 143; **414**, 883

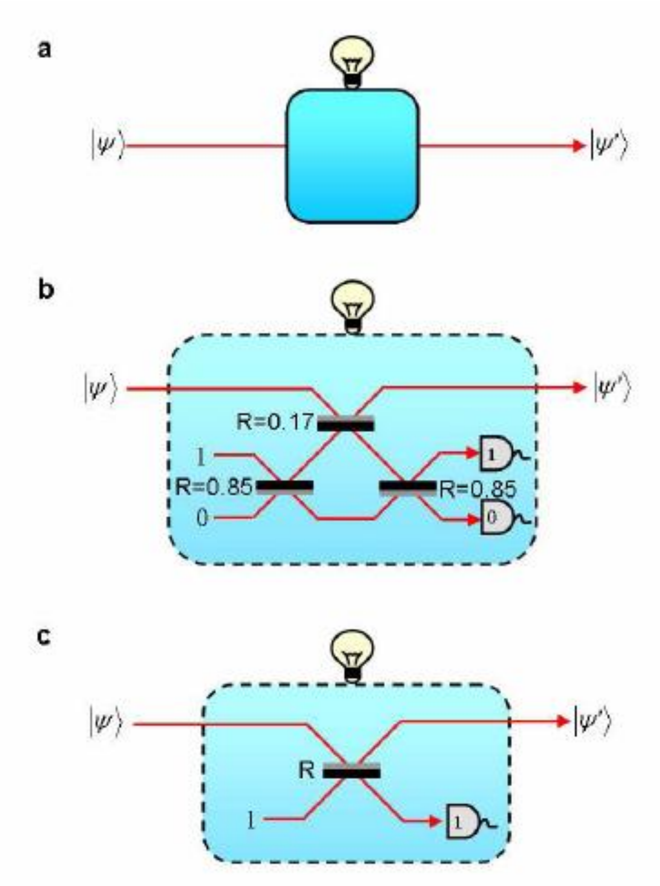
ioni: algoritmo di Deutsch-Josza; CNOT gate

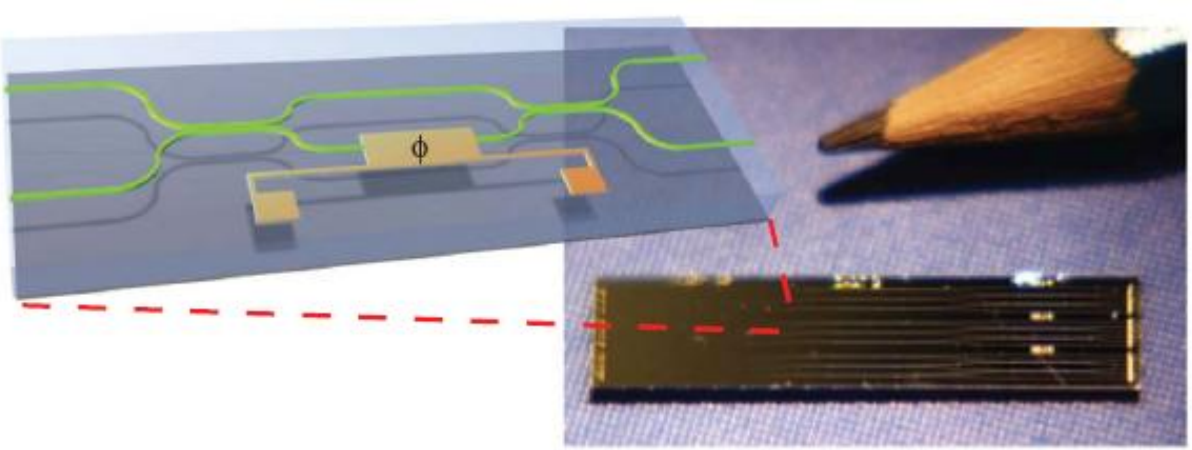
Nature **421**, 48; Phys. Rev. Lett. **89**, 267901

reticoli: creazione di stati entangled

Nature **425**, 937

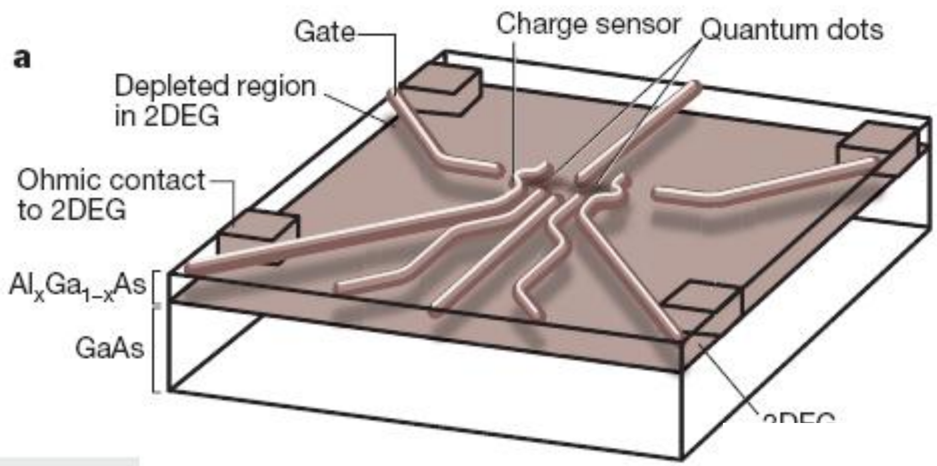
Computer quantistico con fotoni

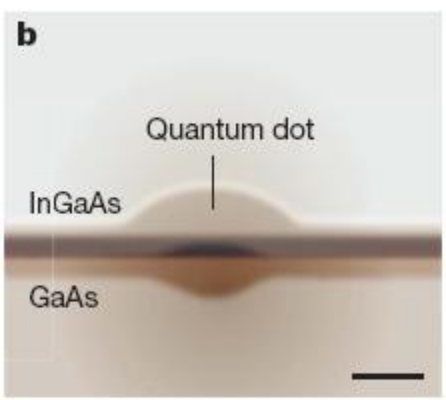


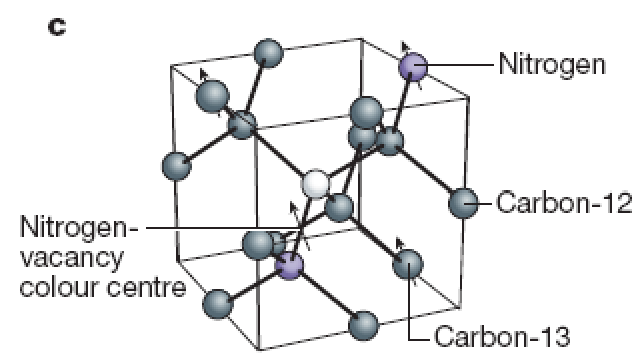


Jeremy O'Brien, Bristol

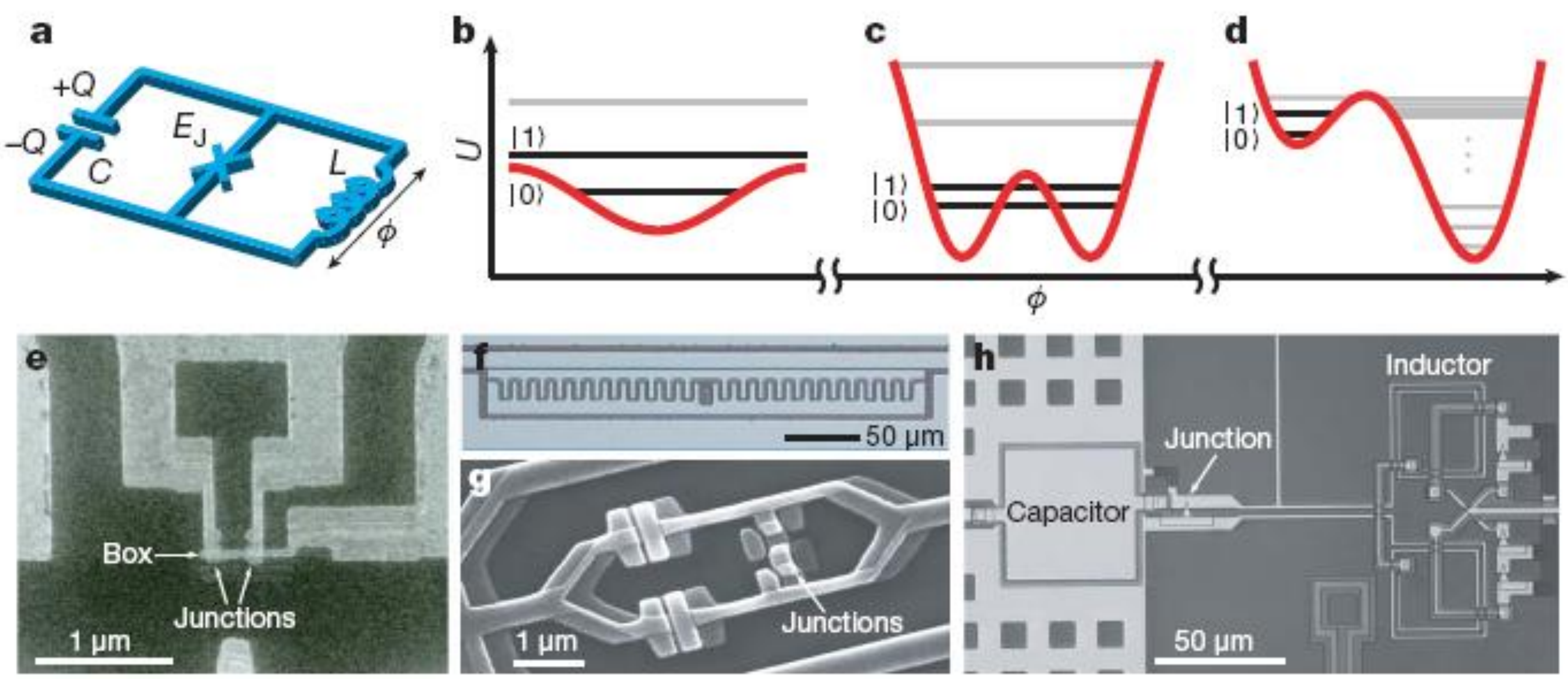
Computer quantistico nello stato solido



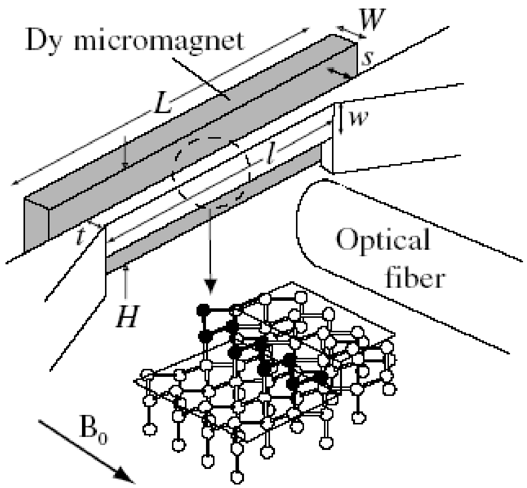




Computer quantistico con superconduttori



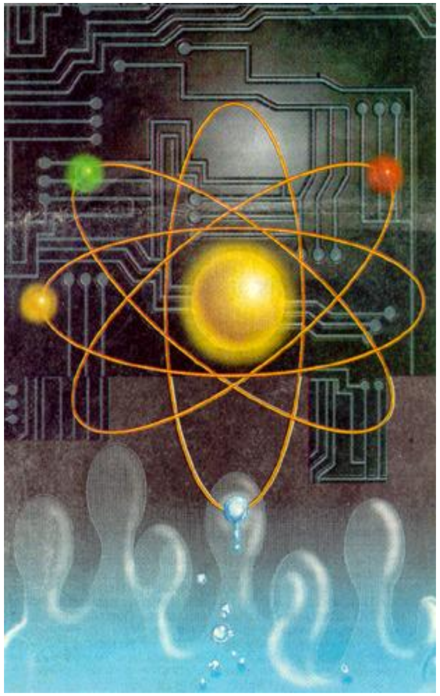
Prospettive per il futuro:
alcuni sviluppi recenti



proposte per c.q. in cristalli di Si usando NMR; tecnologie già molto sviluppate, sembra fattibile

realizzazione di uno stato entangled tra un atomo e un fotone: possibilità di trasmissione di informazione quantistica

Il 'road map' dell' ARDA:
obiettivi per il futuro



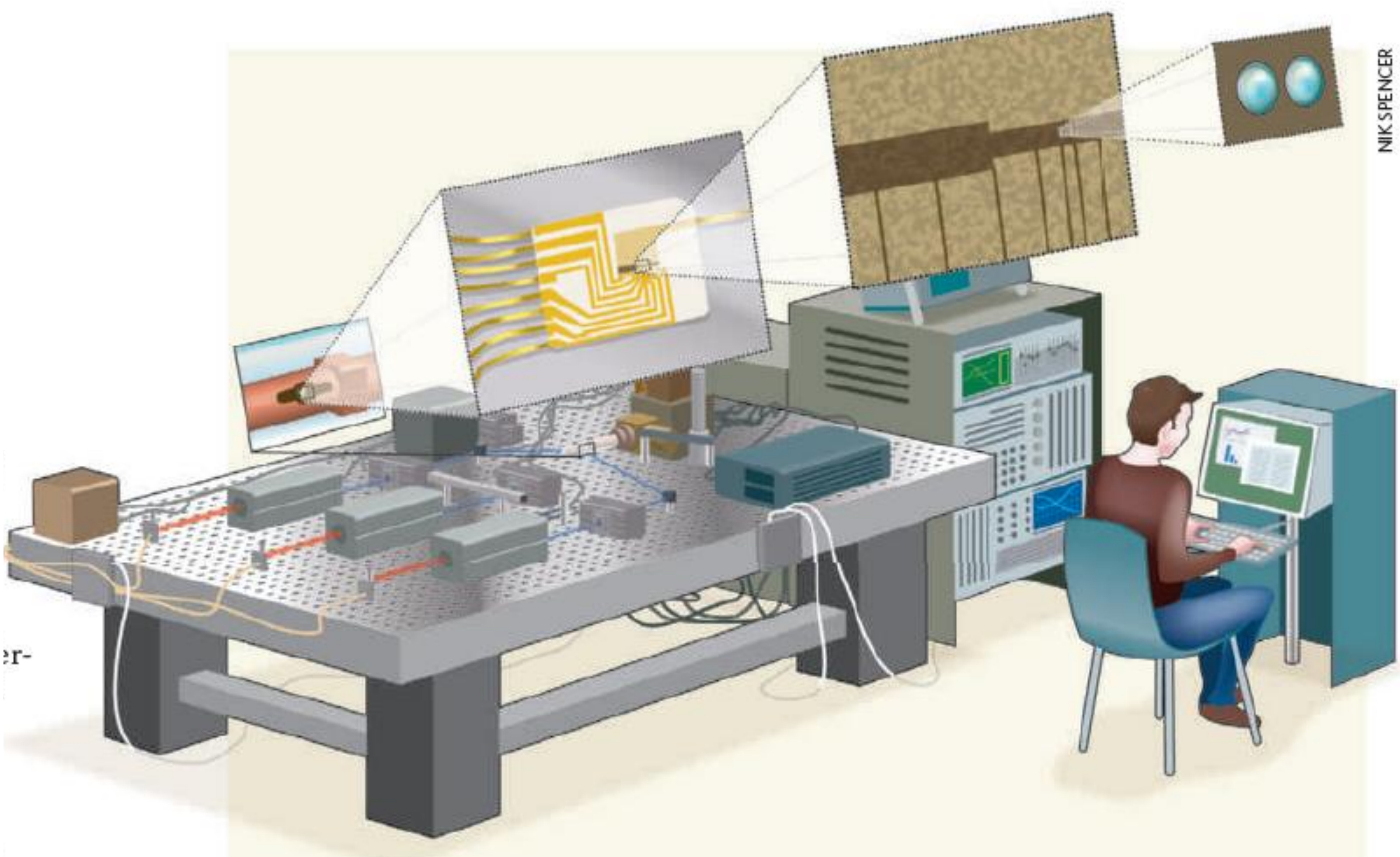
entro il 2007:

- stati entangled 'on-demand'
- correzione di errori ripetitiva
- trasferimento coerente di informazione quantistica
- sistema con 10 qubit

entro il 2012:

- implementazione di un algoritmo con resistenza agli errori
- 'benchmark': c.q. più complesso di una simulazione classica
- sistema con 50 qubit

Prospettive per il futuro:
quando si potrà comprare un c.q.?



Vol 463|28 January 2010 E. Knill

Prospettive per il futuro: *quando si potrà comprare un c.q.?*

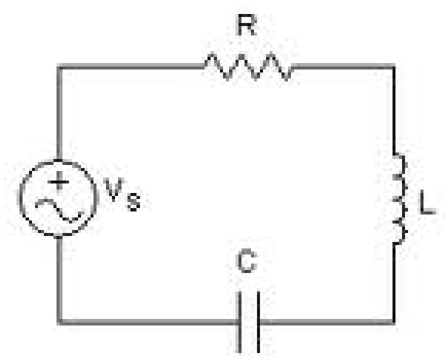
risposta facile: nessuno lo sa!

però......

- computer quantistici sono utili per scopi ben definiti, perciò basterebbe avere un 'plug-in', per esempio, per la fattorizzatione
- strada facendo, si imparano molte cose sulla fisica quantistica
- al momento, varie tecnologie vengono esplorate, è presto per dire quale sarà quella vincente
- nel caso peggiore: se non si può realizzare, almeno si impara perchè non si può

Il simulatore quantistico

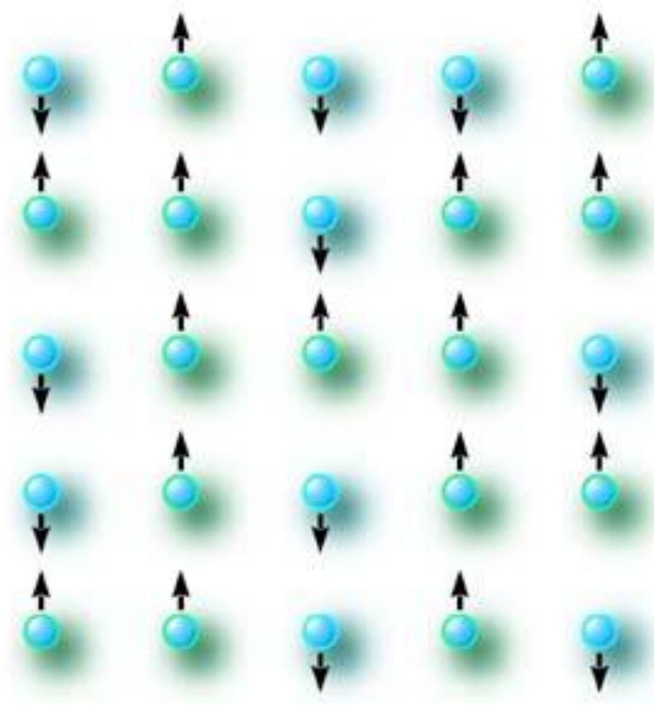
$$L\frac{d^2q}{dt^2}+R\frac{dq}{dt}+\frac{q}{C}=V$$



- multi-purpose
- quantum gates
- algorithms

- single-purpose
- implements a Hamiltonian
- computer calculation intractable
- analogue or digital

Il simulatore quantistico: modello di Ising

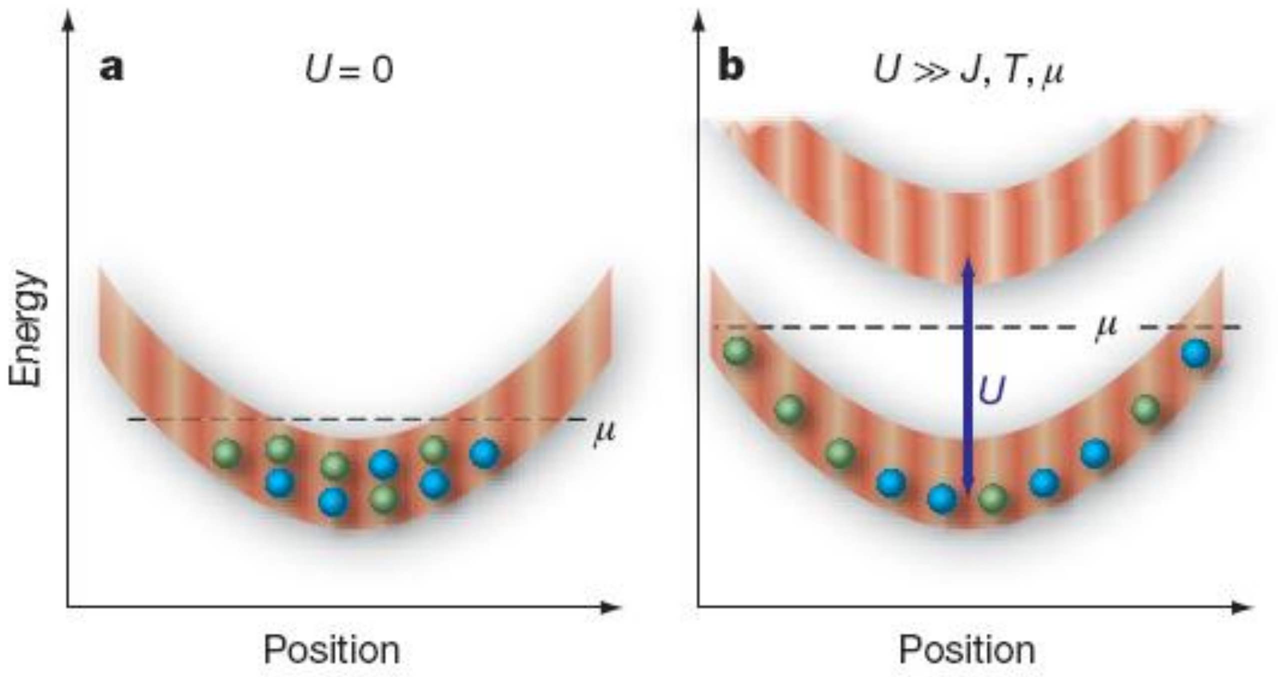


$$\mathcal{H}_{\mathrm{P}} = \sum_{i=1}^{N} h_i \sigma_i^z + \sum_{i,j=1}^{N} J_{ij} \sigma_i^z \sigma_j^z$$

Il simulatore quantistico

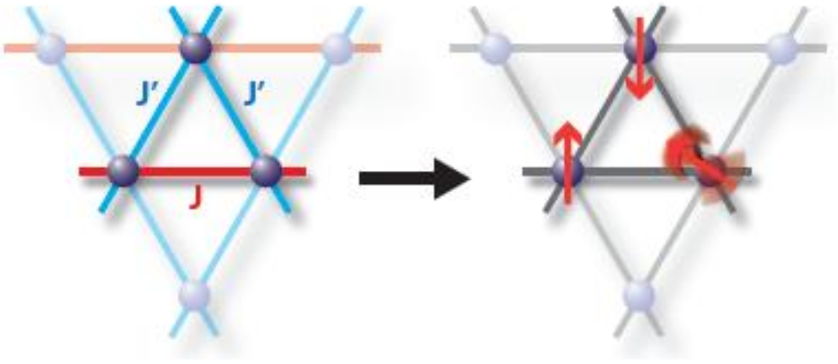
Il modello Fermi Hubbard

$$\hat{H} = -J \sum_{\langle ij \rangle, \sigma} \left(\hat{c}^{\dagger}_{j\sigma} \hat{c}_{i\sigma} + \mathrm{h.c.} \right) + U \sum_{i} \hat{n}_{i\uparrow} \hat{n}_{i\downarrow} + \sum_{i} \varepsilon_i \hat{n}_i.$$



Rilevante per la superconduttività ad alta temperatura critica

Il simulatore quantistico

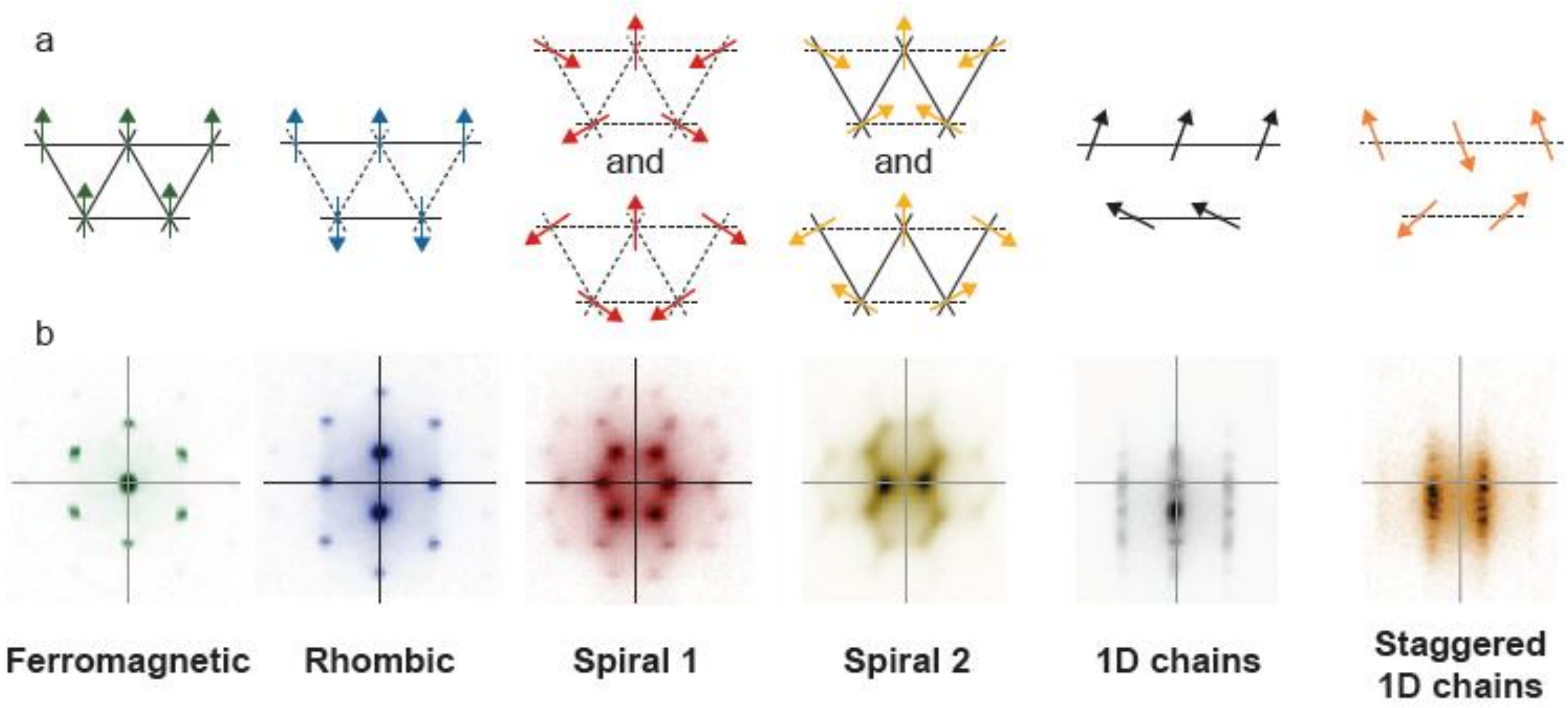


Si può controllare il termine di tunneling J agitando il reticolo. Così si simula un sistema di spin frustrati controllando il segno di J.

$$\hat{H}_0 = -J \sum_{\langle i,j \rangle} (\hat{c}_i^\dagger \hat{c}_j + \hat{c}_j^\dagger \hat{c}_i) + \frac{U}{2} \sum_j \hat{n}_j(\hat{n}_j - 1) + K \cos(\omega t) \sum_j j \hat{n}_j,$$

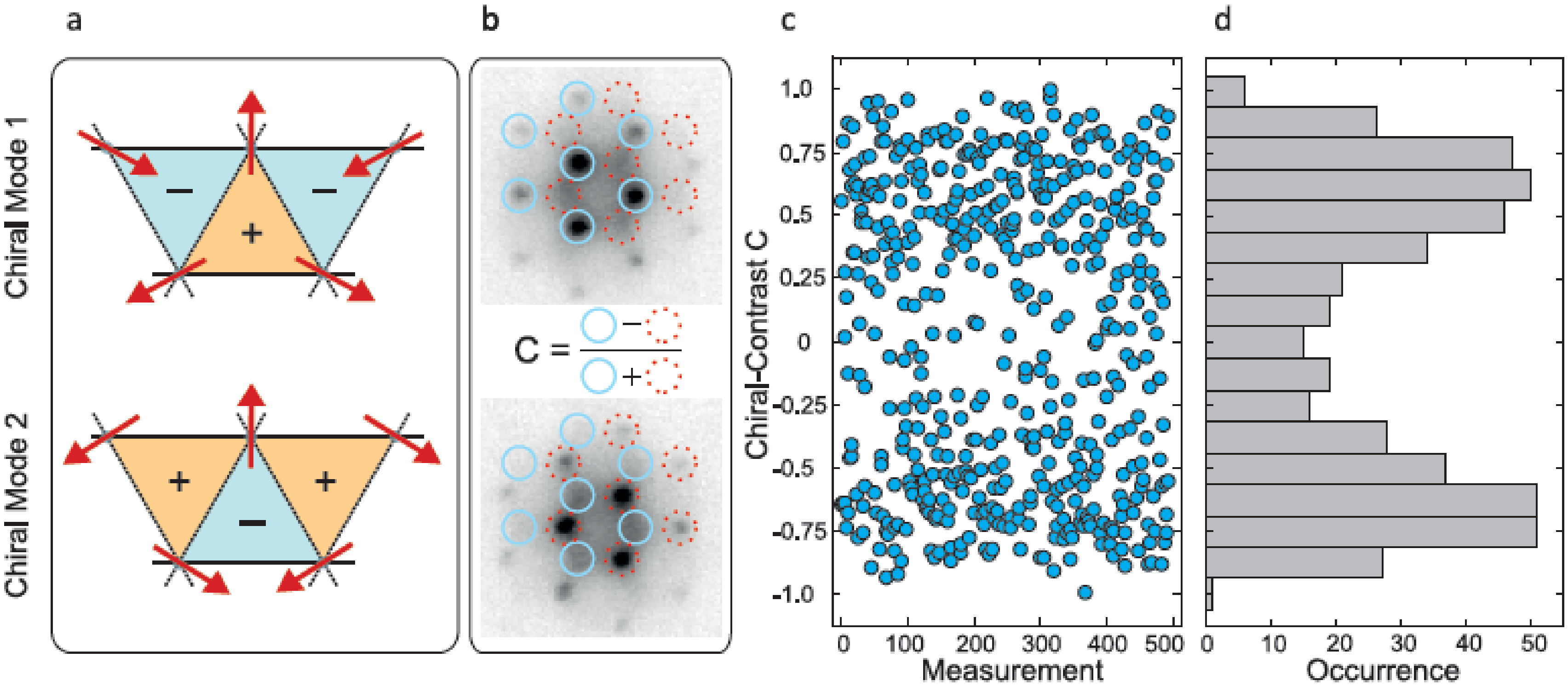
$$J_{\mathrm{eff}} = J \mathcal{J}_0(K/(\hbar\omega)),$$

Il simulatore quantistico



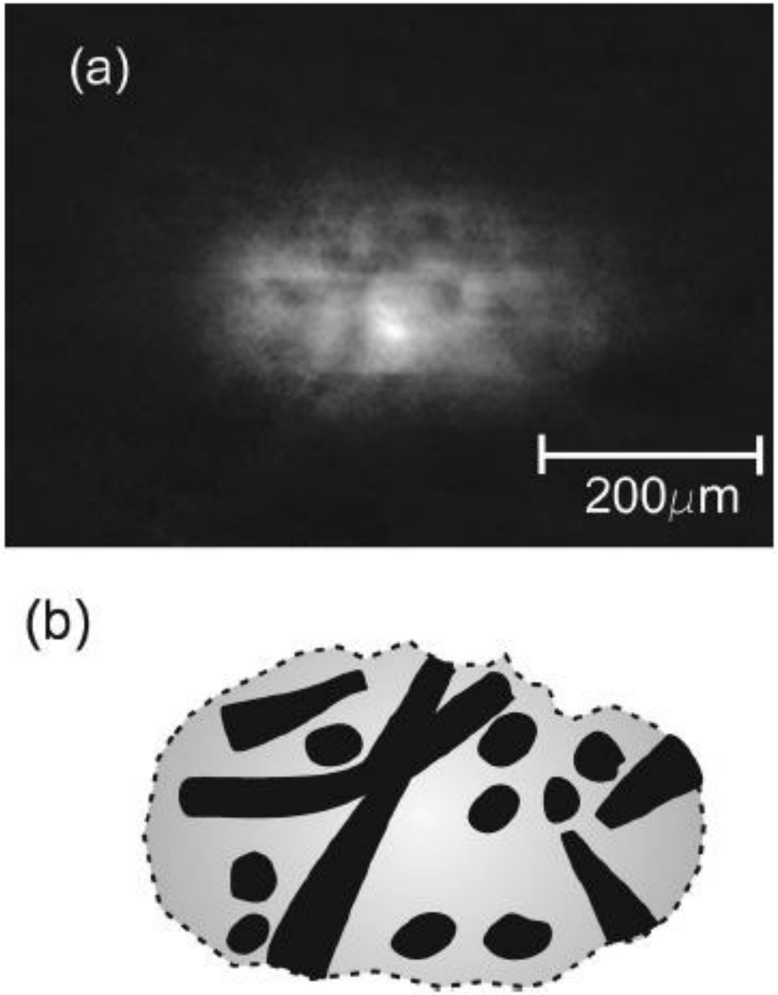
Il simulatore quantistico

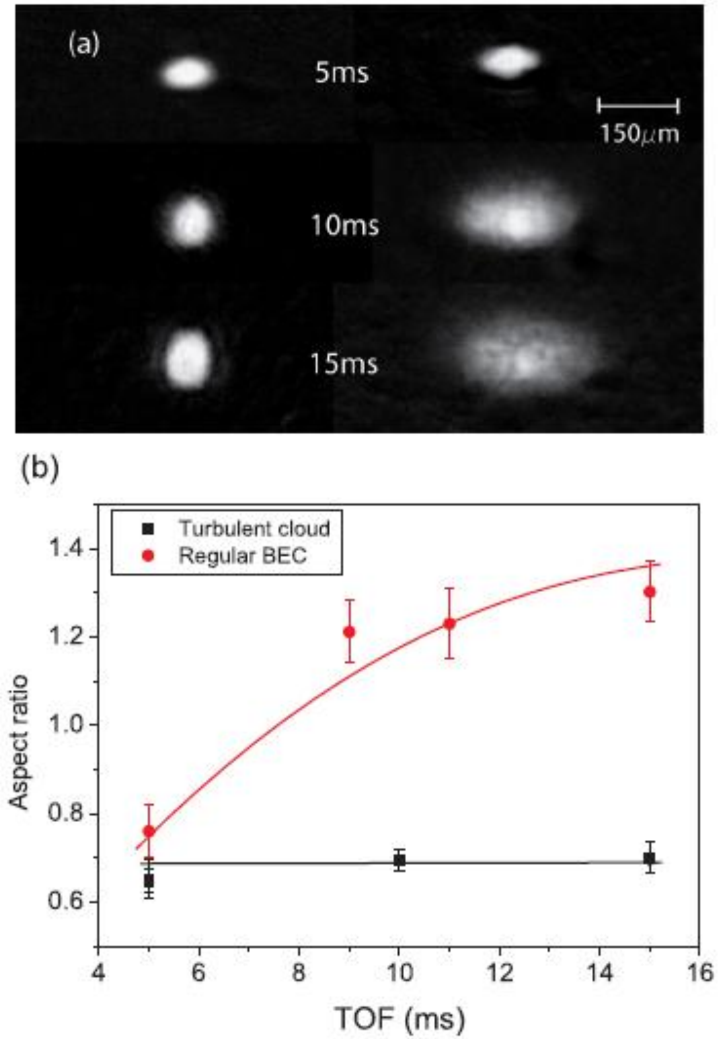
Rottura di simmetria spontanea tra due modi chirali



Il simulatore quantistico

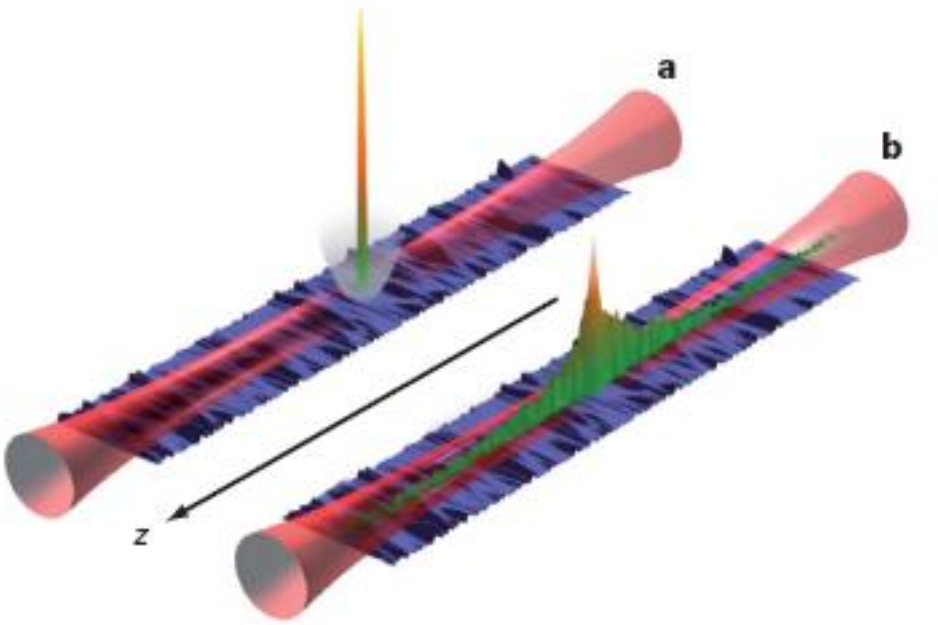
Quantum turbulence



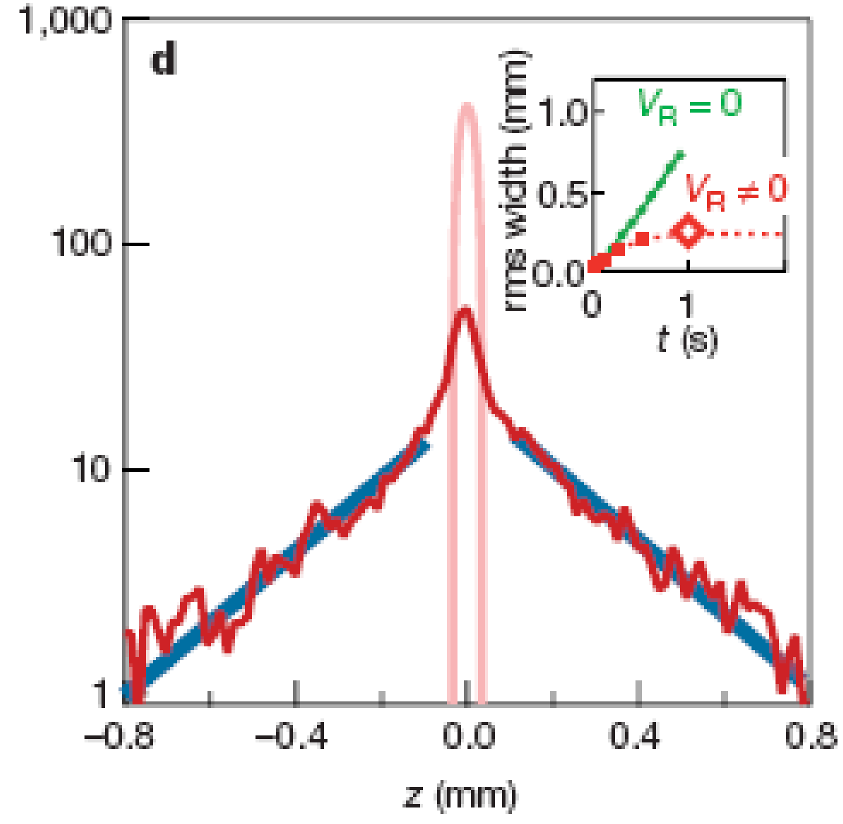


Il simulatore quantistico

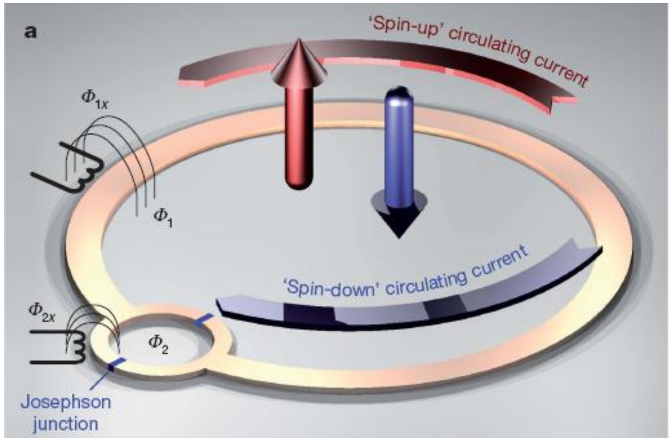
Localizzazione di Anderson in potenziali disordinati

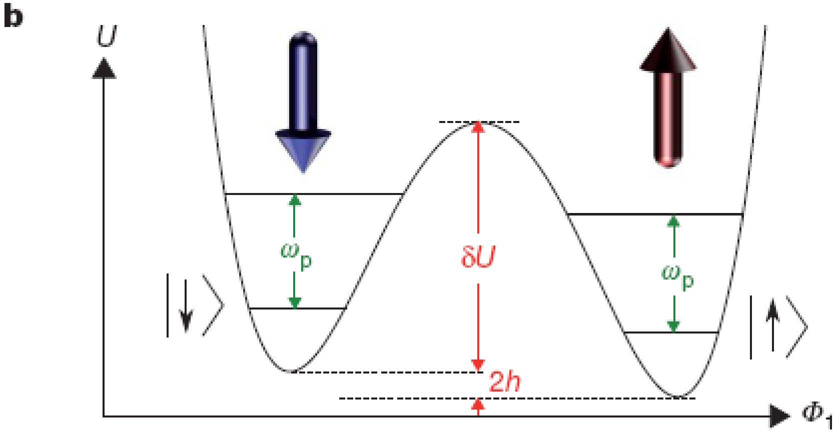


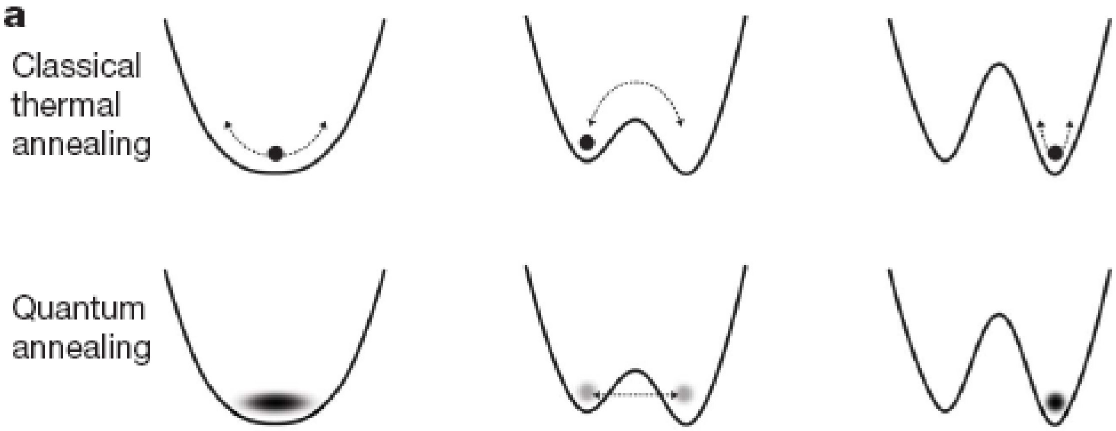
Vol 453 | 12 June 2008 | doi:10.1038/nature07000



Il simulatore quantistico: “annealing”







D-Wave: il primo computer quantistico commerciale?

D-Wave One is a high performance computing system designed for industrial problems encountered by fortune 500 companies, government and academia. Our current superconducting 128-qubit processor chip is housed inside a cryogenics system within a 10 square meter shielded room.

If you are interested in finding out if our products meet your needs please contact us for more information: sales@dwavesys.com

http://www.dwavesys.com