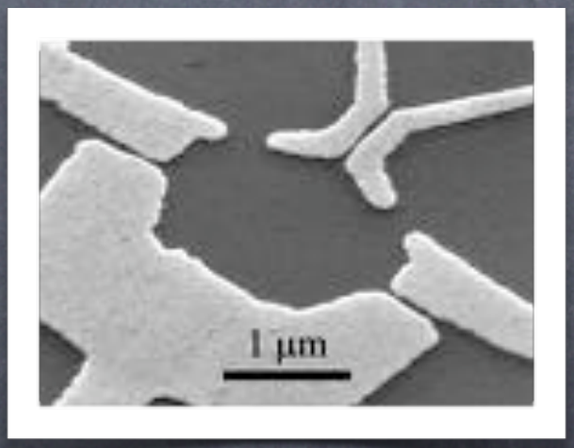
Computer quantistici, algoritmi ed implementazioni

Rosario Fazio
Scuola Normale Superiore
&
NEST-INFM-CNR

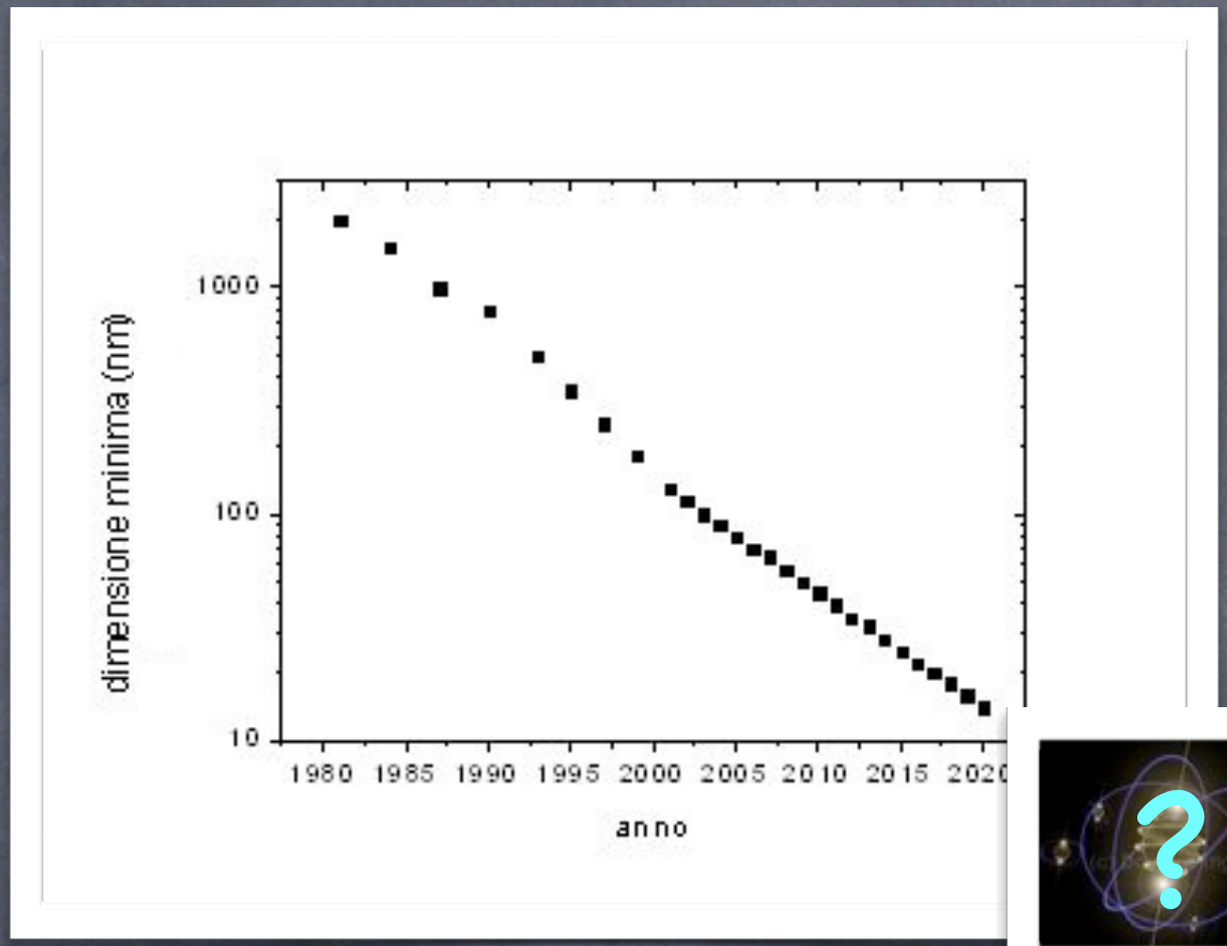
MATEMATICA, CULTURA E SOCIETA'
CRM Ennio De Giorgi, 21 maggio 2009

Qual e' la differenza?

Miniaturizzazione



Legge di Moore



13 April 2005, Gordon Moore:
"It can't continue forever. The nature of exponentials is that you push them out and eventually disaster happens."

Cosa succede se bisogna manipolare atomi?

There is plenty of room
at the bottom

R.P. Feynmann

Dilemma

Forzare un "computer atomico" a comportarsi come ENIAC?

Inventare nuove regole piu' adatte ai sistemi atomici?

Informazione Quantistica

Manipolazione di sistemi quantistici per la computazione

Bit

0 , 1

qubit

— stato

— s fondamentale

Una qualsiasi sovrapposizione dei due stati

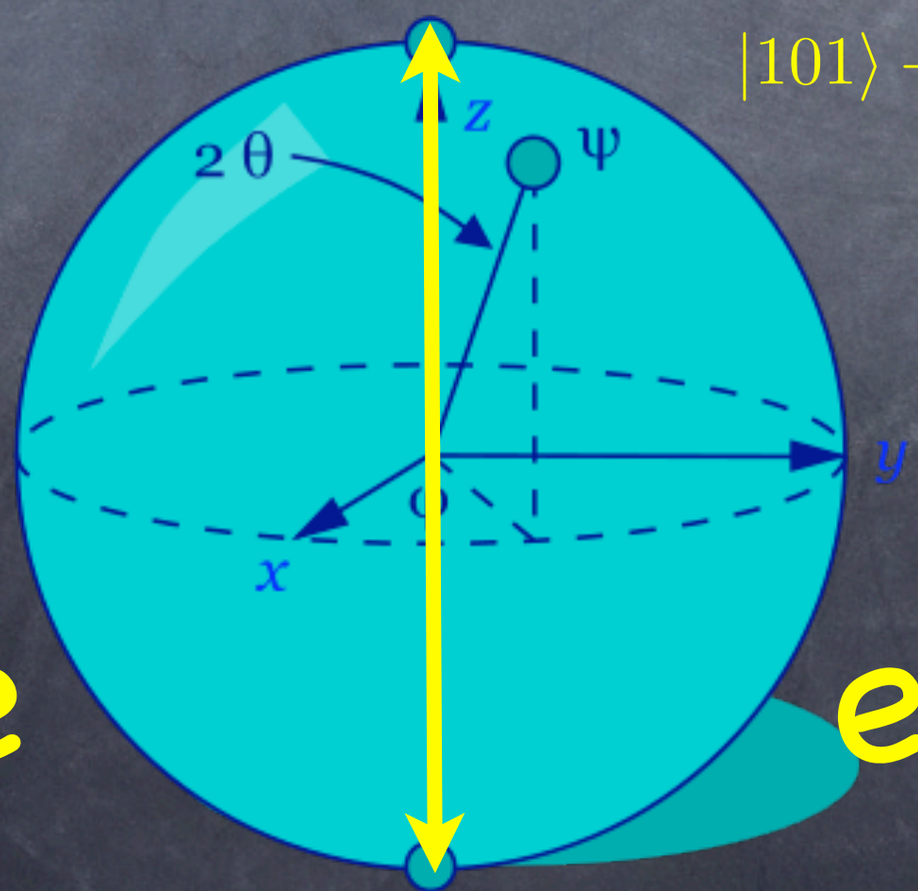
Parallelismo quantistico

Registro classico

101

Registro quantistico

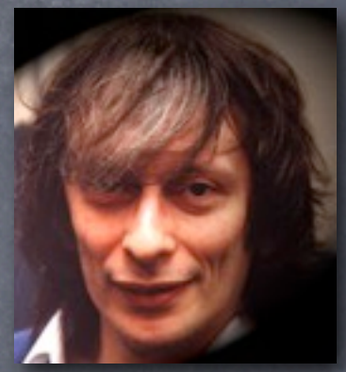
$$|000\rangle + |001\rangle + |010\rangle + |100\rangle +$$
$$|101\rangle + |101\rangle + |110\rangle + |111\rangle$$



Maggiore efficienza?

Algoritmo di Deutsch

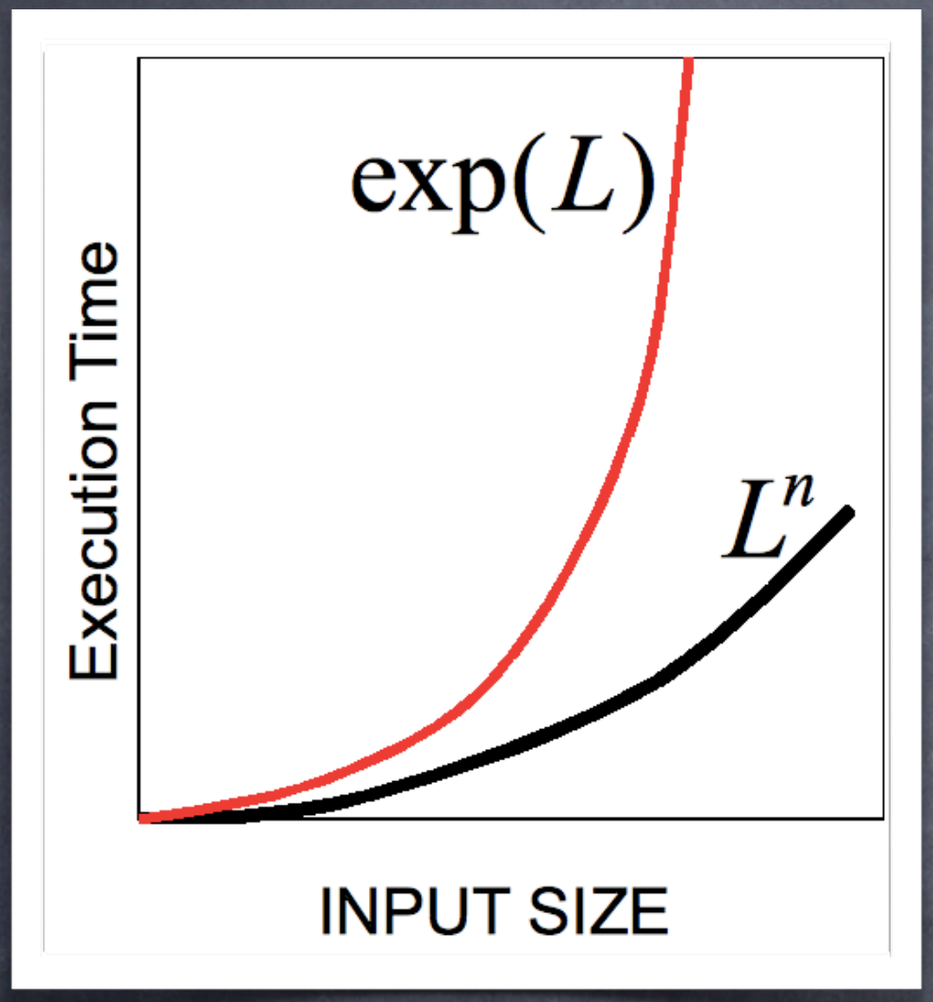
1985



Per scoprire "classicamente" se una moneta e' truccata bisogna guardare entrambi i lati

Con un computer quantistico e' possibile "guardarla" una sola volta

Problemi difficili?



Fattorizzazione

3267000013 x 5915587277 =
1.93262237108616 4e+19

$N \sim 10^L$ $\sqrt{N} \sim 10^{L/2}$

per L=100 ed un computer che esegue 10^6 divisioni al secondo

$T \sim 10^{44}\text{sec}$

185323955009471744507093833849366798683834244443114056794632807824057962331639 77

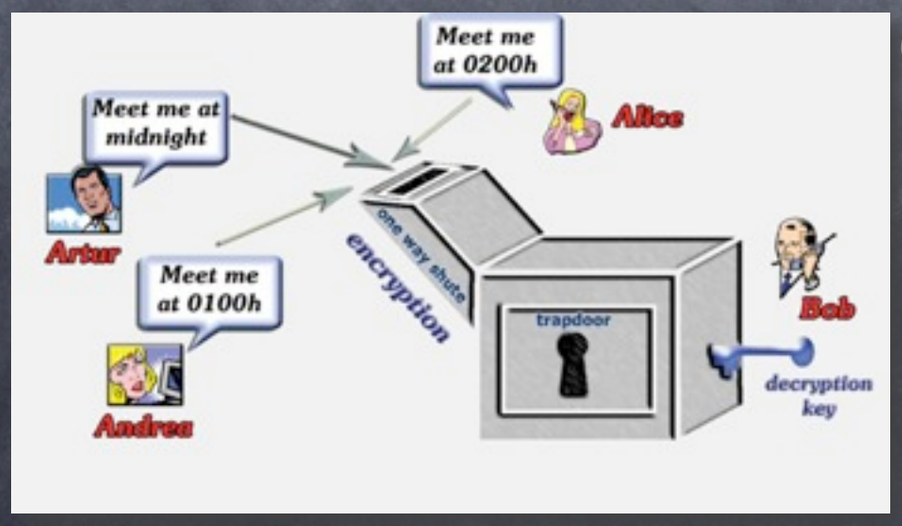
396886448368328825261738315775361178158184544378104372102216445533819958130149 59

-Fattorizzazione-
Algoritmo di Shor

Permette di trovare i fattori in un tempo polinomiale

1994

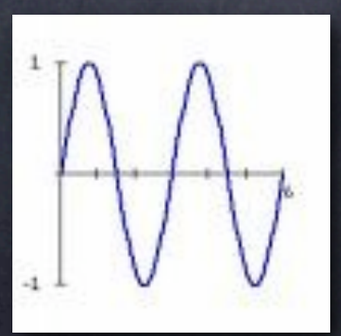
Importanza fondamentale nella crittografia a chiave pubblica

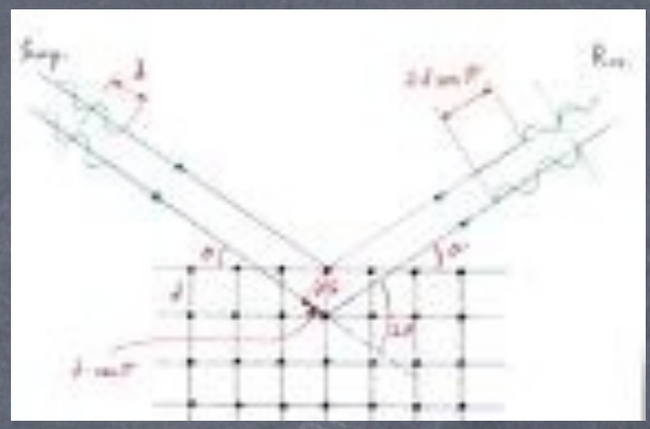


Basata sulla difficolta' a trovare i fattori primi di un numero N grande

-Algoritmo di Shor-
Come funziona?

La ricerca dei fattori primi puo' essere legata alla ricerca del periodo di una funzione





Crittografia Quantistica

Bennett Brassard 1984

Ingredienti fondamentali

- Principio di indeterminazione di Heisenberg
- Il processo di misura altera lo stato

Ekert 1991

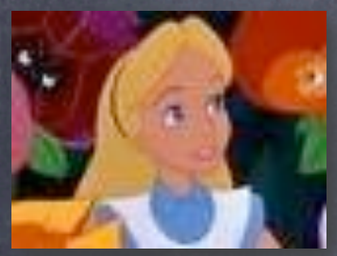
Protocolli basati sia su stati non ortogonali o sull'esistenza di stati entangled

Crittografia Quantistica

Protocollo di Bennett Brassard 1984

	0	1
Base Z	↕	↔
Base x	↘↙	↗↖

chiave 0100110



Alice

Bob

X X Z X Z Z X X X Z Z X

0 1 1 1 0 1 0 0 1 1 0 0

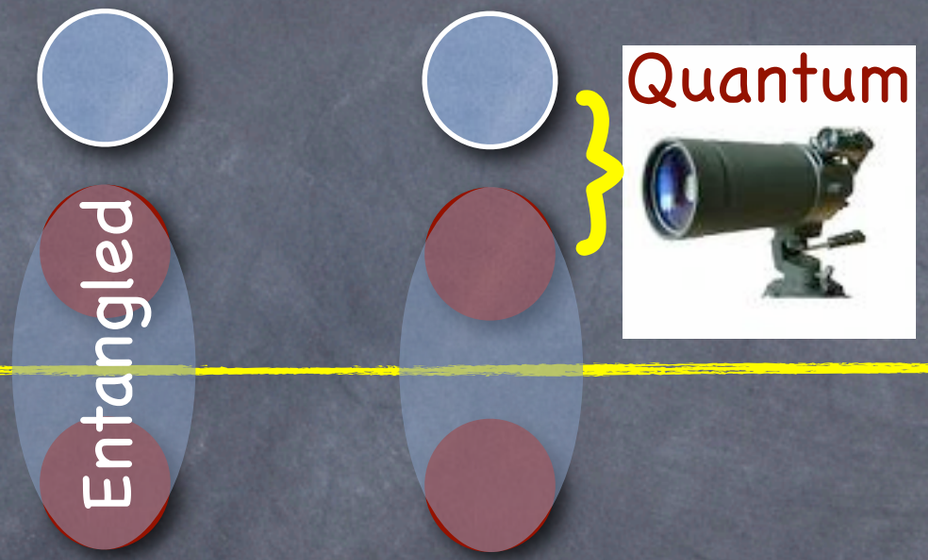
X Z X X Z X Z X X Z X X

. . .

0 1 1 1 0 0 1 0 1 1 1 0

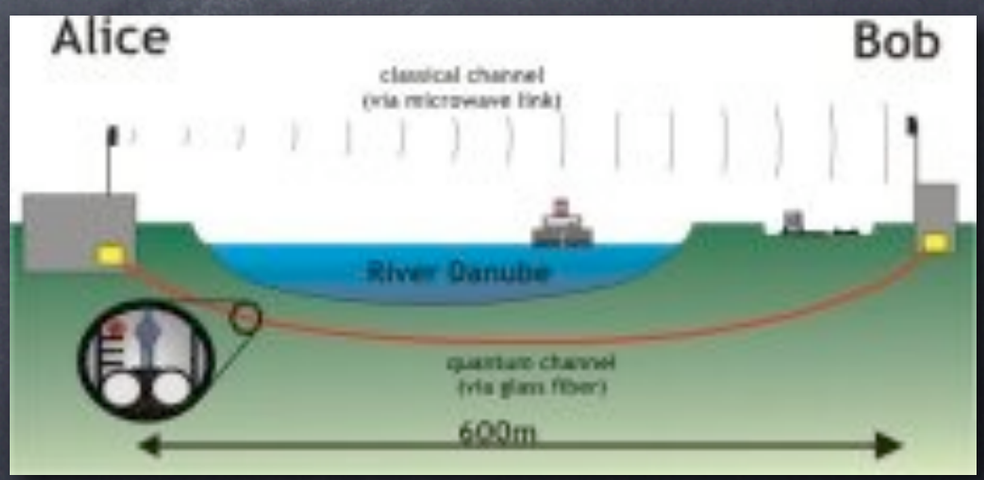
Teletrasporto Quantistico

Bennett et al 1993



Conferma sperimentale

D. Bouwmeester et al 1997
D. Boschi et al 1998

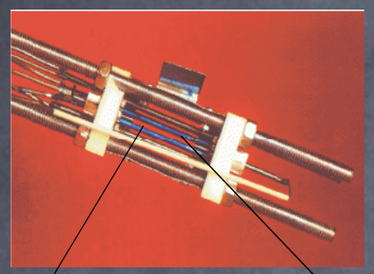


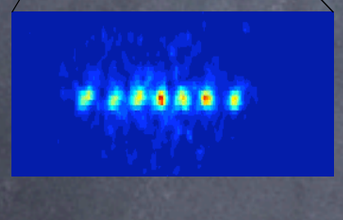
Come costruire un computer quantistico

- ✓ Avere a disposizione un insieme di qubit
- ✓ Sapere eseguire tutte le porte logiche necessarie
- ✓ Il computer quantistico deve essere protetto da varie sorgenti di rumore
- ✓ Essere in grado di misurare lo stato finale del computer

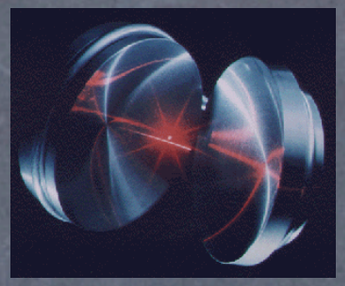
Computer quantistici

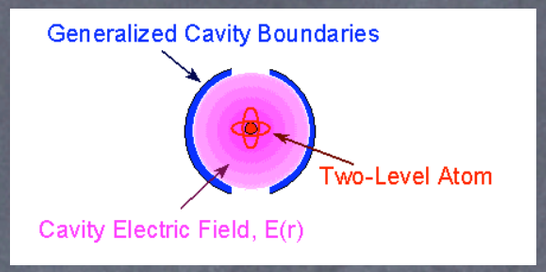
Ion traps





Cavity QED

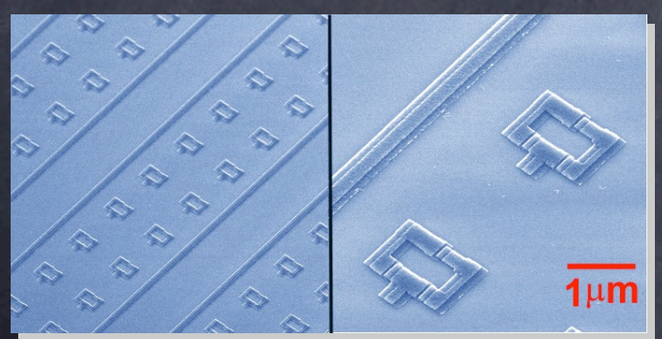




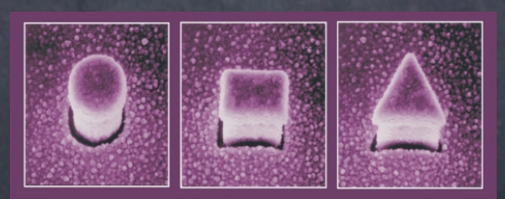
NMR

• • •

Superconducting circuits

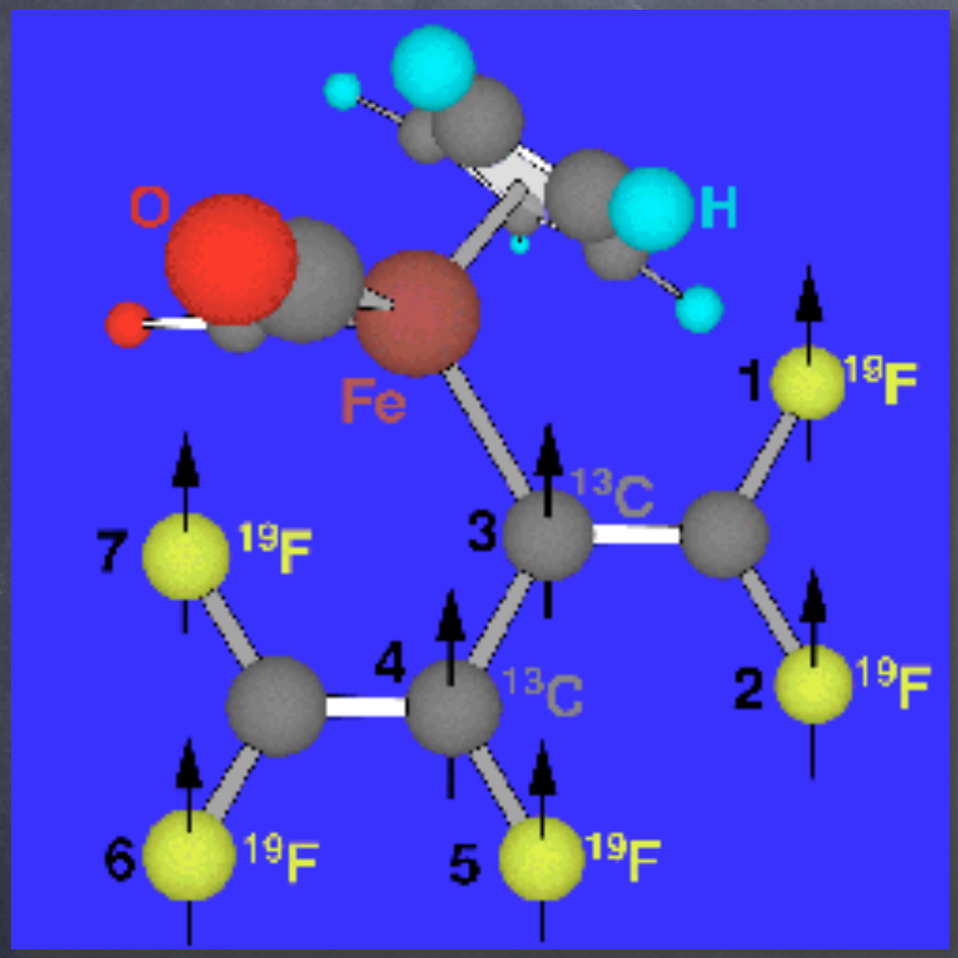


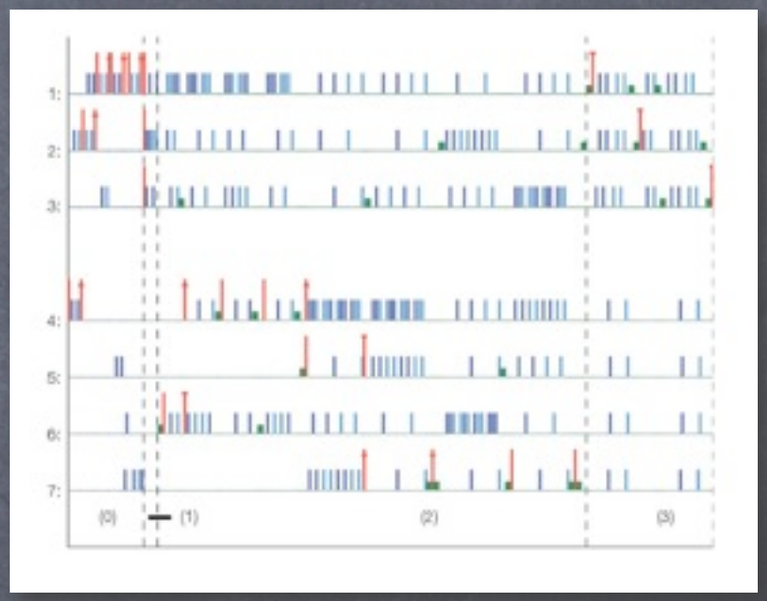
Quantum dots

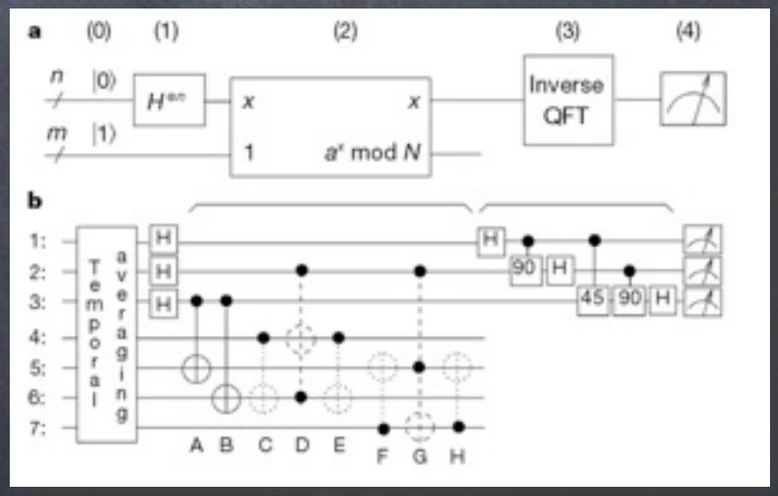


Fattorizzare N=15!

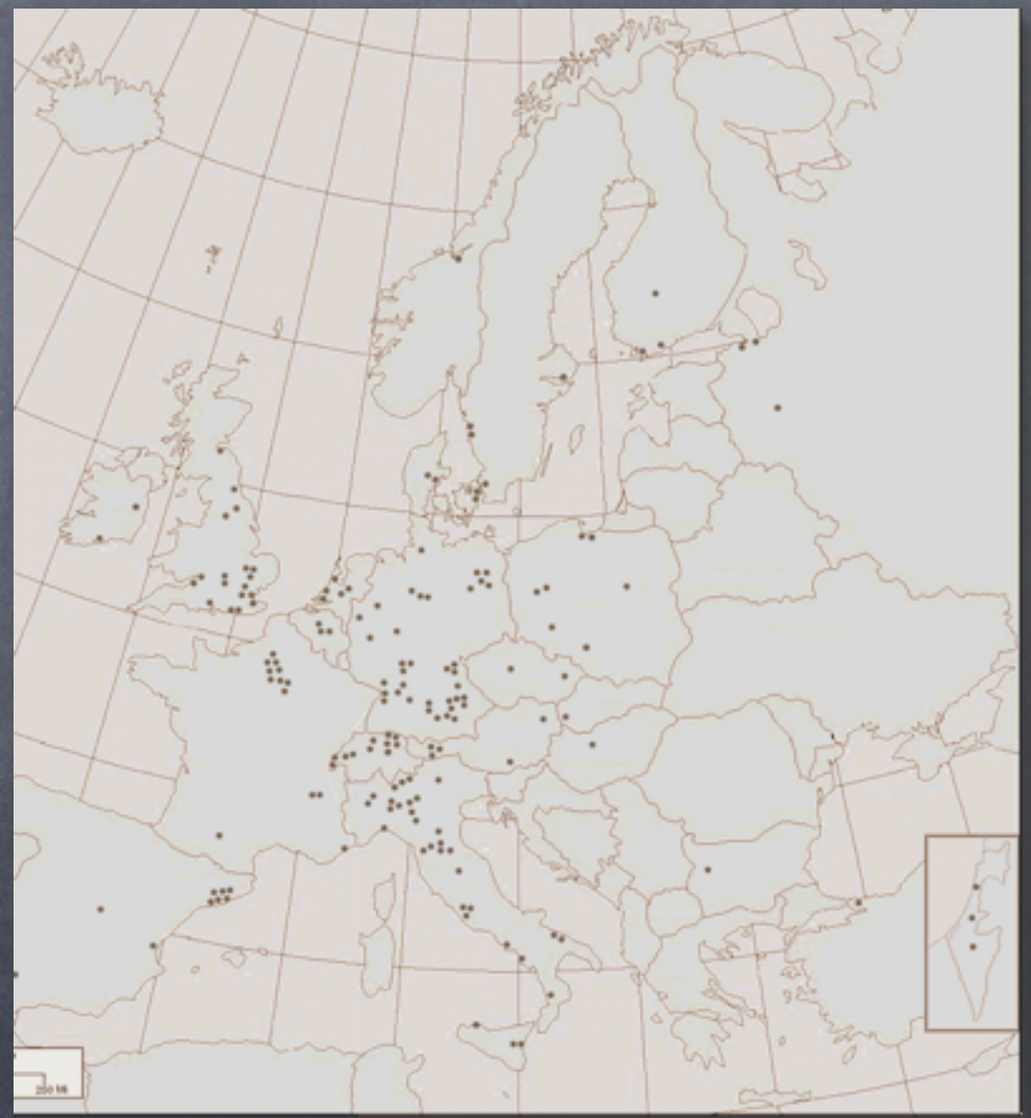
L. Vandersypen et al. 2001







Prospettive



Grazie dell'attenzione