Applicazioni della Fisica Quantistica

EUGENIO BERTOZZI, DIPARTIMENTO DI FISICA E ASTRONOMIA, UNIVERSITA' DI BOLOGNA

'Genuinamente' quantistiche

- Crittografia
- Teletrasporto
- Quantum Computing

Crittografia

'Studio della trasformazione dell'informazione alla scopo di renderla sicura da destinatari e/o usi non voluti'.

- Diffusa: posta elettronica e protezione privacy bancaria
- Antica: esempi dal 1900 a.C.

Scitala lacedemone, 900 a.C.

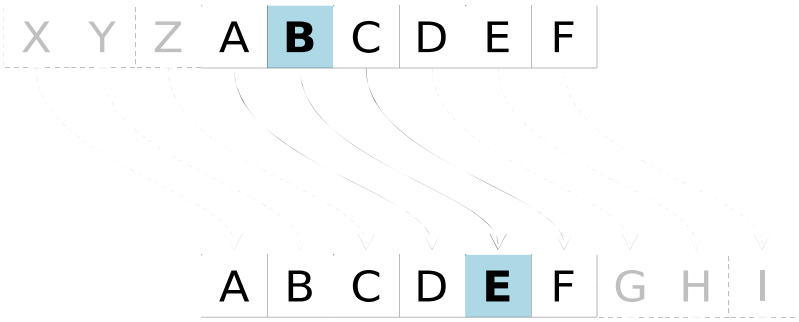
La 'chiave'...

Cifrario di Giulio Cesare, 100 a.C.

'Se aveva qualcosa di confidenziale da dire, lo scriveva in modo cifrato, ovvero scambiando l'ordine delle lettere di modo che nemmeno una parola potesse essere riconosciuta. Se qualcuno avesse voluto decifrare il messaggio avrebbe dovuto scambiare la quarta lettera dell'alfabeto con la prima'

Svetonio, Vita di Giulio Cesare

Cifrario di Giulio Cesare, 100 a.C.



$E_n(x) = (x + n) \bmod 26$

$D_n(x) = (x - n) \bmod 26$

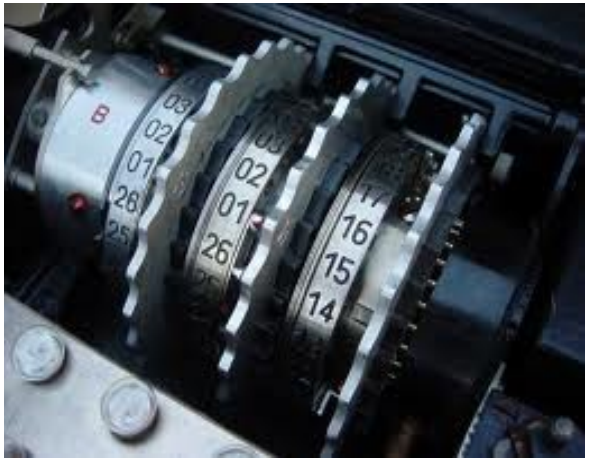
DZZDFFDUH LON NUUNGAFNENON LDOON DOOD RUD VHVZD

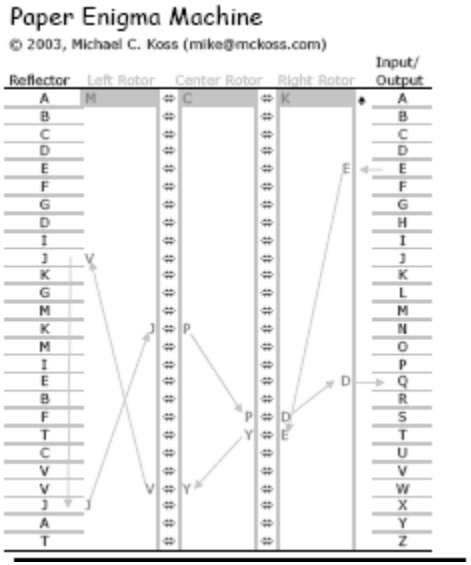
'attaccare gli irriducibili galli alla ora sesta'

NB: Il parametro 'n' può assumere solo 25 valori diversi

...l'algoritmo e la 'debolezza'.

Enigma, seconda guerra mondiale





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

La 'meccanica'...

Enigma, seconda guerra mondiale

David Kahn, The codebreakers: the story of secret writing

'Il continuo e sofferto girare della mente attorno al rompicapo che la occupava, la precoccupazione durante i pasti, l'insonnia, i risvegli improvvisi nel cuore della notte, la pressione per riuscire e la coscienza che un fallimento poteva avere conseguenze gravi per tutta la nazione, la disperazione delle interminabili settimane in cui il problema sembrava inattaccabile, le continue frustrazioni che seguivano a rari momenti di speranza, gli shocks mentali, la tensione, il logorio, l'urgenza e la necessità di segretezza, tutto si abbatteva furiosamente sul capo di Friedman'.

...e la 'complessità computazionale'.

Oggi: 'complessità' e 'sicurezza'

Un tipico acquisto in rete:

- Invio della “chiave pubblica” (256 cifre, prodotto di 2 numeri primi)
- Codifica dell'informazione (ad es del numero della carta di credito) e spedizione del 'pacchetto'
- De-codifica del messaggio (NB: è necessaria la conoscenza dei due numeri primi che fattorizzano la chiave pubblica)

Un eventuale intercettatore avrà in mano la chiave pubblica e i codici criptati. Quanto impiega a fattorizzare?

La 'chiave' pubblica.

La 'moltitudine' dei numeri primi

1 055 664 361 = 24151 × 43711 “facile”

RSA-640 (193 cifre decimali) =
3107418240490043721350750035888567930037346022842727545720161948823206440518
0815045563468296717232867824379162728380334154710731085019195485290073377248
22783525742386454014691736602477652346609 =

1634733645809253848443133883865090859841783670033092312181110852389333100104
50815121211816751157 9 ×

1900871281664822113126851573935413975471896789968515493666638539088027103802
10449895719126146557 1 **5 mesi su un cluster di 80 processori a 2.2 GHz.**

RSA-2048 (617 cifre decimali) **???** **> 10^{10} anni (età dell'Universo circa)**

R(ivest)**S**(hamir)**A**(dleman)

Crittografia 'classica'

- Idea di base: Spingere le difficoltà computazionali al limite della tecnologia al fine di scoraggiare possibili infrazioni

- In linea di principio è sempre possibile de-crittare il messaggio

'E' veramente da mettere in dubbio che l'intelligenza umana possa creare un cifrario che poi l'ingegno umano non riesca a decifrare con l'applicazione necessaria'

(EDGAR ALLAN POE)

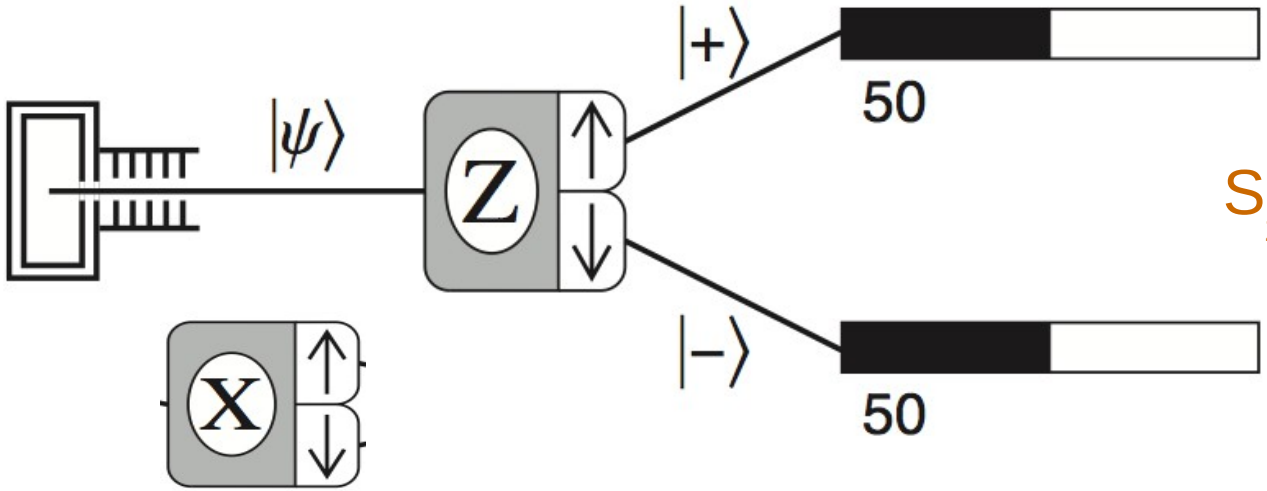
Crittografia 'quantistica'

- Idea di base: Sfruttare il fenomeno quantistico detto entanglement
- In linea di principio è impossibile de-crittare il messaggio

Punto centrale: lo scambio della 'chiave'.

Un passo indietro...

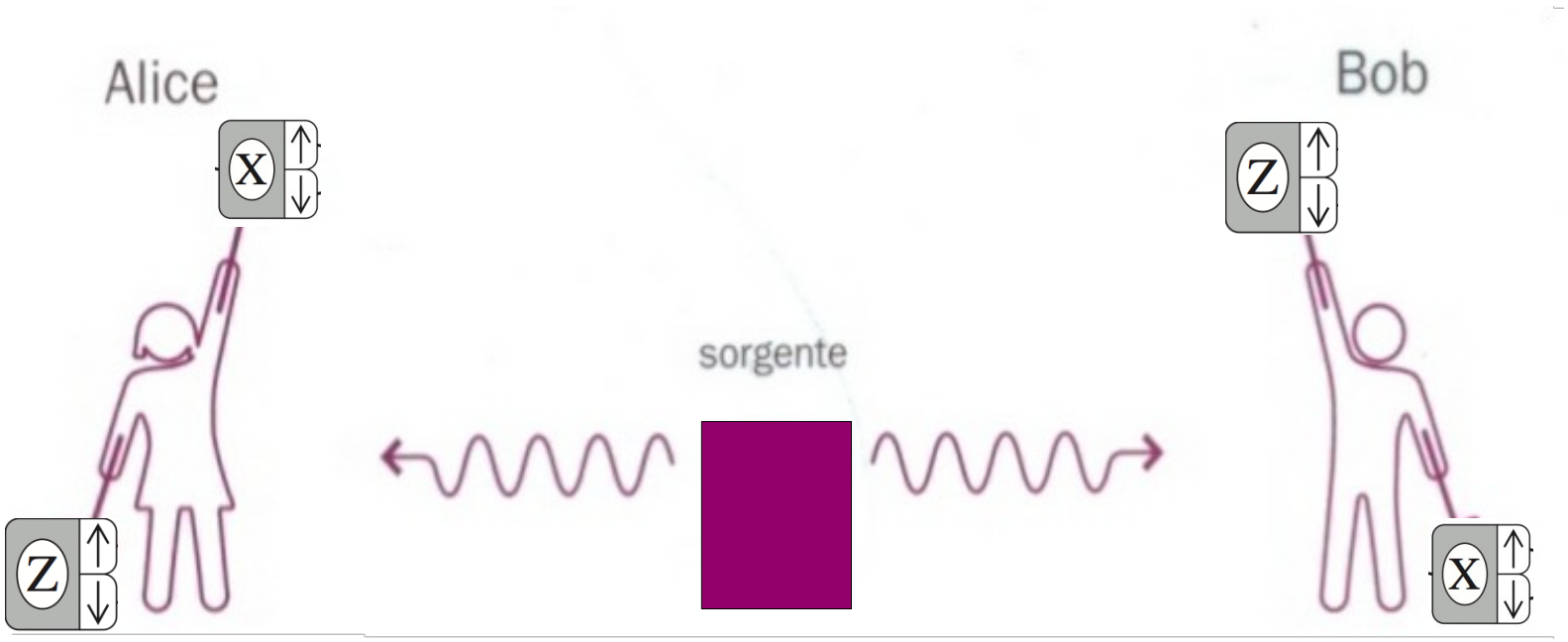
Atomi di argento attraverso apparato di Stern e Gerlach



$S_z = \pm \hbar/2$

Due possibili risultati per le misure di S_z e S_x

La situazione...



Scelgono liberamente, e indipendemente,
quale misura fare fra le due

Fenomenologia dell'entanglement...

LA MISURA: MISURE DI SPIN DI ATOMI DI ARGENTO FATTE LUNGO ASSE « X » E « Z »

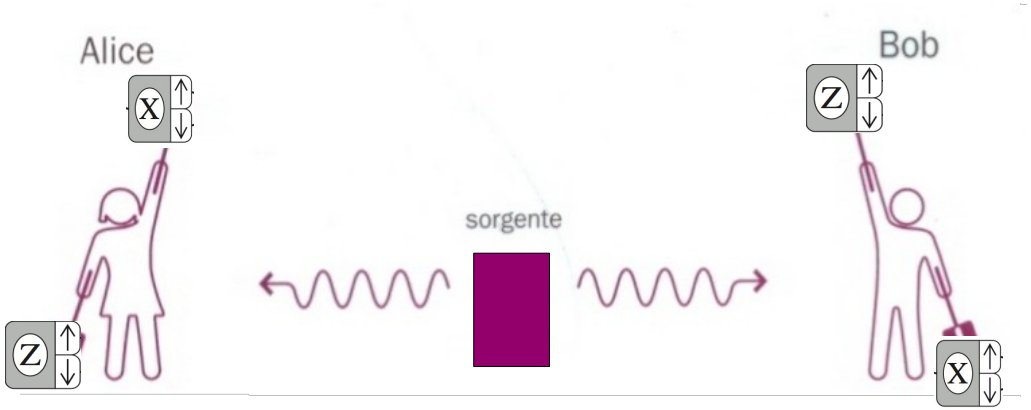
Se Alice e Bob misurano la stessa grandezza (ovvero entrambi S_z oppure S_x) → I risultati della misura – sebbene casuali – risultano identici (se Alice trova $+\hbar/2$ ($-\hbar/2$) allora lo stesso per Bob e viceversa).

Se eseguono misure miste (ad es Alice S_z e Bob S_x o viceversa) → Ognuno dei due misurerà per lo spin lungo l'asse da lui scelto il valore $\pm \hbar/2$ con probabilità ½

NB : Misure indipendenti

I quattro passi di un protocollo

- Passo 1. Emissione degli atomi dalla sorgente.
- Passo 2. Misure di spin (lungo « z » o « x »): libera scelta (+ħ/2 è “1” - ħ/2 è “0”)
- Passo 3. Comunicazione sequenza delle misure: canale tradizionale (telefono)
- Passo 4. Eliminazione dei casi in cui hanno eseguito misure diverse: cosa rimane?



Alice		Bob		Chiave
S_z	1	S_x	0	
S_z	1	S_z	1	1
S_x	1	S_x	1	0
S_z	1	S_x	1	
S_z	0	S_x	1	
S_z	0	S_z	0	0

sequenza 'pulita' di numeri: la chiave quantistica

La chiave quantistica è...

- Nota ad entrambi (in virtù dell'entanglement)
- Casuale (misura quantistica)
- Ignota a chi intercetta la telefonata ('cosa' hanno misurato *vs* 'risultato' delle misure)

La spia: Eva

Ciò che succede ad uno...

- Come si 'traduce' in formule? Qual è l'aspetto dell'entanglement a livello formale?
- Quali e quanti 'principi' della MQ si vanno a scomodare?

...si ripercuote istanteneamente sull'altro, a prescindere dalla distanza che li separa

Privacy e sicurezza nazionale

L'episodio della 'Pretty Good Privacy'

Privacy e sicurezza nazionale

L'episodio della 'Pretty Good Privacy'

Marzo 2014

a) 12 Marzo 2014 : quantum criptography and smartphone

Evitare di 'affidarsi' al sistema della banca

b) 27 Marzo 2014: Crittografia e paranoia : 'The ultimate physical limits of privacy' (Ekert, Renner; Nature, 507, 443)

http://www.quantumlah.org/

a) http://www.quantumlah.org/highlight/140312_oblivious_transfer.php
- Nature Commun.DOI:10.1038/ncomms4418 (2014), arXiv: 1308.5098

b) http://www.quantumlah.org/highlight/140327_nature_privacy.php

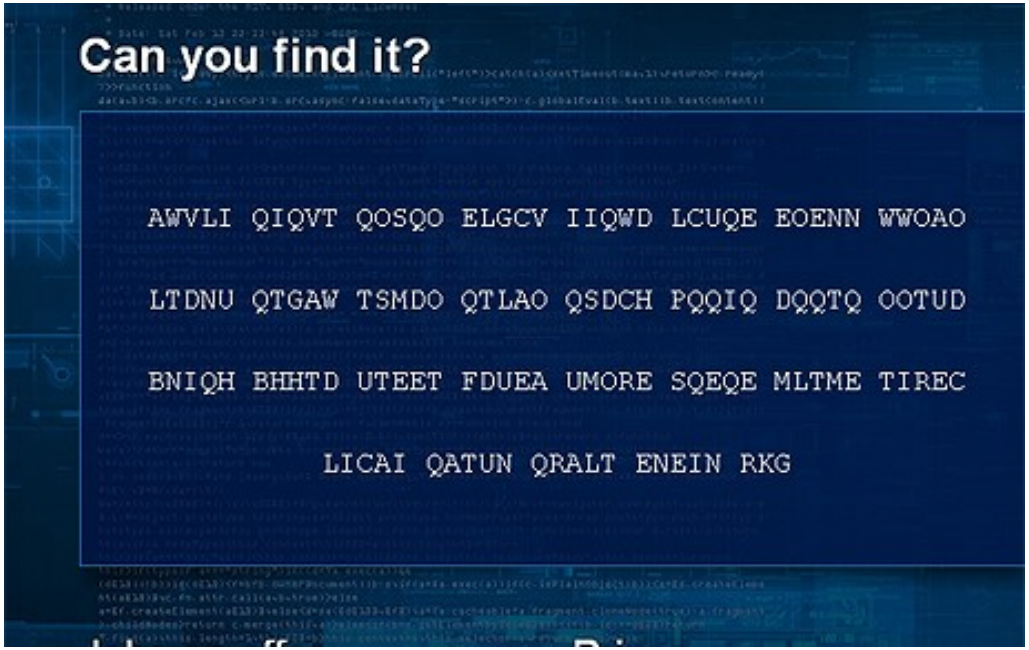
Center for Quantum Technologies (Singapore)

'Keeping secrets in a world of spy and mistrust'

Discussing 'paranoia' in operational terms

Artur Ekert, co-inventor of quantum cryptography, explains what it takes to keep our secrets secret.
Credit: Karol Jalochowski / CQT, National University of Singapore

Government Communications HeadQuarters (GCHQ)



'The unusual recruitment process launched by Britain's listening post will challenge applicants to crack a series of cryptic codes.

Entitled 'Can You Find It?', the brain teaser consists of 29 blocks of five letters which candidates have to decipher into five answers.

The answers then lead the applicant to an online 'treasure hunt' which hopefuls have six weeks to complete'.

Alice Philipson, The Telegraph, 11 Set. 2013

http://www.thecodex.com/en/gchq-can-you-find-it-solution

Teletrasporto

- …confine dell'Impero Romano (fino IV d.C.)
- ...fonte d'ispirazione per Johann Strauss jr. ('800) : Capodanno!
- ...laboratorio per il teletrasporto quantistico "Quantum Teletrasportation across the Danube", Nature 430 (2004) p. 849

...il fiume Danubio

Teletrasportare “cosa”?

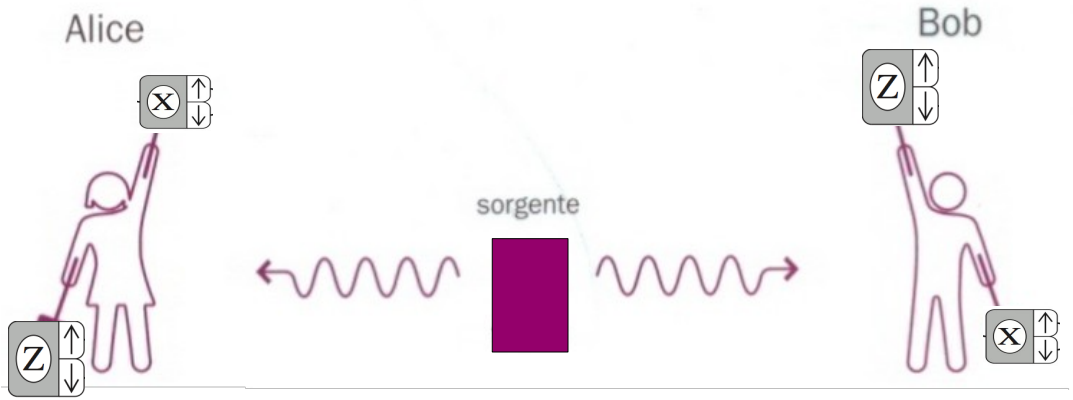
- Non si teletrasportano 'oggetti': particelle o addirittura persone

- Nella FQ all'oggetto (particella...) è associato uno 'stato' che contiene tutte le informazione fisiche sull'oggetto : questo è ciò che si teletrasporta.

...teletrasportare lo 'stato' di un oggetto microscopico (fotone, elettrone, atomo di argento …) : **??????**

Situazione iniziale

$$|\psi\rangle = [1/\sqrt{2}\ |\underline{1},+\rangle_Z\ |\underline{2},+\rangle_Z\ +\ 1/\sqrt{2}\ |\underline{1},-\rangle_Z\ |\underline{2},-\rangle_Z]$$



- Alice e Bob condividono una coppia di atomo entangled (**1** e **2**)
- Alice ha, nel suo laboratorio una particella (**3**) in uno stato di sovrapposizione

$$|\psi\rangle_I = \alpha\ |\underline{3},+\rangle_Z + \beta\ |\underline{3},-\rangle_Z$$

$|\psi\rangle_I$ è lo stato in cui si trova la particella **3**. Questo stato deve essere teletrasportato sulla particella **2**.

Situazione finale

$|\psi\rangle = [1/\sqrt{2}\ \ |\underline{1},+\rangle_Z\ |\underline{3},+\rangle_Z\ + 1/\sqrt{2}\ |\underline{1},-\rangle_Z\ |\underline{3},-\rangle_Z]$

$|\psi\rangle_I = \alpha\ |\underline{2},+\rangle_Z + \beta\ |\underline{2},-\rangle_Z$

- Alice ha nel suo laboratorio le particelle **1** e **3** che si trovano nello stato entangled
- Bob ha nel suo laboratorio la particella **2** che ha assunto lo stato che doveva essere teletrasportato

Ora è la particella **2** a trovarsi in $|\psi\rangle_I$. Particelle **1** e **3** in entangled. Entangled iniziale fra **1** e **2** distrutto.

Punto fondamentale...

Lo stato complessivo delle 3 particelle può essere espresso come sovrapposizione di 4 stati

$$|\psi\rangle_{TOT} = |\psi\rangle_I\,|\psi\rangle = \ldots. = [1/\sqrt{2}\,(\,|1,+\rangle_z\,|3,+\rangle_z + |1,-\rangle_z\,|3,-\rangle_z\,)]\,(\alpha|2,+\rangle_z + \beta|2,-\rangle_z) + \ldots.. + \ldots... +.$$

Alice fa una misura congiunta sulle particelle 1 e 2 (che ha a disposizione), distrugge questa sovrapposizione fa collassare il sistema nel nuovo stato [però, la misura avviene in un momento particolare]

… Separare ciò che può misurare Alice da Bob : entanglement si « sposta »

Considerazione

Non esiste un solo istante in cui lo stato

$|\psi\rangle_I = \alpha\, |\underline{\ldots},+\rangle_Z + \beta\, |\underline{\ldots},-\rangle_Z$

sia « in mano » ad Alice e Bob contemporaneamente (lo stato viene prima « distrutto » e poi « ricreato»).

No-cloning Theorem

Fisica e/o Metafisica?

La prospettiva di Michio Kaku sul Teletrasporto

Fisica e/o Metafisica?

La prospettiva di Michio Kaku sul Teletrasporto

Computer Quantistico

- 'Pensare' il computer quantistico (CQ) : l'idea
- 'Far funzionare' il CQ : gli algoritmi
- 'Costruire' il CQ : i 'quantum bit' (Q-bit)

...

'Pensare' il Computer Quantistico

L'idea e la sua fattibilità
'in teoria'

Simulating Physics with Computers

Simulating Physics with Computers

Richard P. Feynman

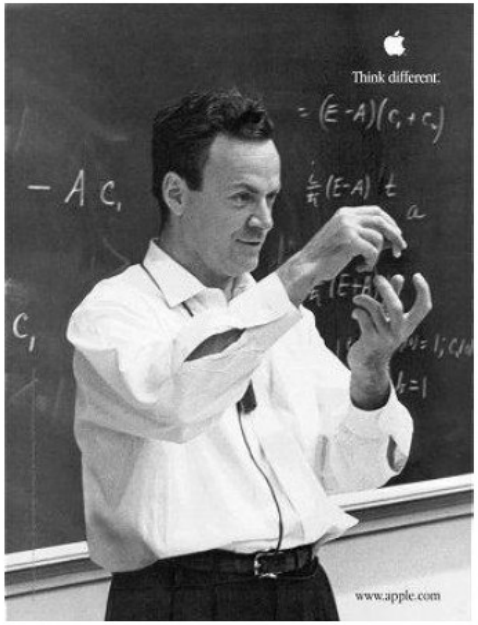
Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981

1. INTRODUCTION

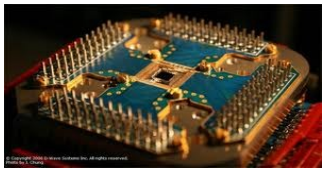
On the program it says this is a keynote speech—and I don't know what a keynote speech is. I do not intend in any way to suggest what should be in this meeting as a keynote of the subjects or anything like that. I have my own things to say and to talk about and there's no implication that anybody needs 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-*



'Not an *approximate* simulation of what physics ought to do... […] the possibility of an *exact* simulation of nature'

Simulating physics in a 'specific' way



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

Quantum Computer – Quantum Simulator

- Una macchina che funziona secondo le leggi della Fisica Quantistica (permettere di risolvere problemi ecc.)
- Una macchina che imita la realtà quantistica

'it's going to be necessary that everything that happens in a finite volume of space and time would have to be exactly analyzable with a finite number of logical operations'

Simulating time, space, probabilities, ...

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

The Universal Quantum Computer

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)

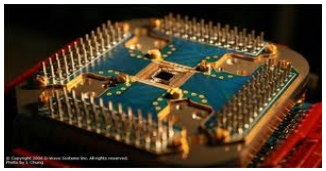
(*Communicated by R. Penrose, F.R.S. — Received 13 July 1984*)

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.

'Computing machines resembling the universal quantum computer could, in principle, be built and would have many remarkable properties'

Il limite della 'computabilità': 'Riscrivere' la macchina di Turing secondo le leggi della FQ



DAVID DEUTSCH Proceedings of the Royal Society of London A 400, pp. 97-117 (1985)

Due 'enunciati'

Every function which would naturally be regarded as computable can be computed by the universal Turing machine (Turing)

Ogni oggetto fisico su cui è possibile fare esperimenti

'Naturalmente' non
Ben collocabile nella struttura della fisica

Every finitely realizable physical system can be perfectly simulated by a universal model computing machine operating by finite means' (Deutsch)

Misura, preparazione, sistema fisico

Modello astratto ma teoricamente 'permesso'

DAVID DEUTSCH Proceedings of the Royal Society of London A 400, pp. 97-117 (1985)

'Far funzionare'...

Inventare algoritmi

Il Santo Graal della matematica

1992, Peter Shor – M.I.T: conferenza su quantum computing e 2 anni di lavoro in solitario

Fattorizzazione di un numero di 400 cifre

→ Computer classico: 10^{10} anni

→ Computer quantistico < 3 anni

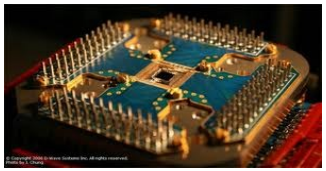
1994, algoritmo: dalla complessità esponenziale (classici) alla complessità polinomiale (quantistici)

The Fabric of Reality

To those who still cling to a single-universe world-view, I issue this challenge : explain how Shor's algorithm works. I do not merely mean predict that it will work, which is merely a matter of solving a few uncontroversial equations. I mean provide an explanation. When Shor's algorithm has factorized a number, using 10^{500} or so times the computational ressources that can be seen to be present, where was the number factorized? There are only about 10^{80} atoms in the entire visible universe, an utterly minuscole number compared with 10^{500}. So if the visible universe were the extent of physical reality, physical reality would not even remotely cointain the ressources required to factorize such a large number. Who did factorize it, then? How, and where, was the computation performed?

David Deutsch, 1997

Interpretazione della FQ: Universi Paralleli
(Everett, 1957, MWI)



Immagazzinare l'informazione...

Classicamente, in qualunque sistema fisico che possieda due stati stabili e distinguibili.

Condensatore scarico → Valore '0'
Condensatore carico → Valore '1'

… in un bit 'classico': assume 2 valori ('0' o '1')

Immagazzinare l'informazione

Quantisticamente, nell'atomo...

Stato fondamentale	→	Valore |0>
Stato eccitato	→	Valore |1>
Stato di sovrapposizione	→	*a* |0, nessun fotone assorbito> + *b* |1, fotone assorbito>

...o 'q-bit': unità di informazione che si può trovare anche in uno stato sovrapposto di |0> e |1> (spettro infinito di possibilità)

Su un Blog di fisici...

Physics Stack Exchange is a question and answer site for active researchers, academics and students of physics. It's 100% free, no registration required. Take the 2-minute tour ×

Is Shor's algorithm a demonstration of the many worlds interpretation?

David Deutsch is very fond of pointing out Shor's integer factorization algorithm is a demonstration of the many worlds interpretation. As he often asked, where else did all the exponentially many combinations happen?

Are there any other alternative interpretations of quantum mechanics which can explain Shor's algorithm, and the Deutsch-Jozsa and Simon's algorithm?

quantum-mechanics quantum-information quantum-interpretations

edited May 19 '11 at 19:08
David Z ♦
33.8k 11 57 132

asked May 19 '11 at 6:56
Piet
66 3

6 Answers

'Interpretations of quantum mechanics, unlike Gods, are not jealous, and thus it is safe to believe in more than one at the same time. So if the many-worlds interpretation makes it easier to think about the research you're doing in April, and the Copenhagen [SEGUE]

[segue] interpretation makes it easier to think about the research you're doing in June, the Copenhagen interpretation is not going to smite you for praying to the many-worlds interpretation. At least I hope it won't, because otherwise I'm in big trouble'.

Prospettiva di Peter Shor

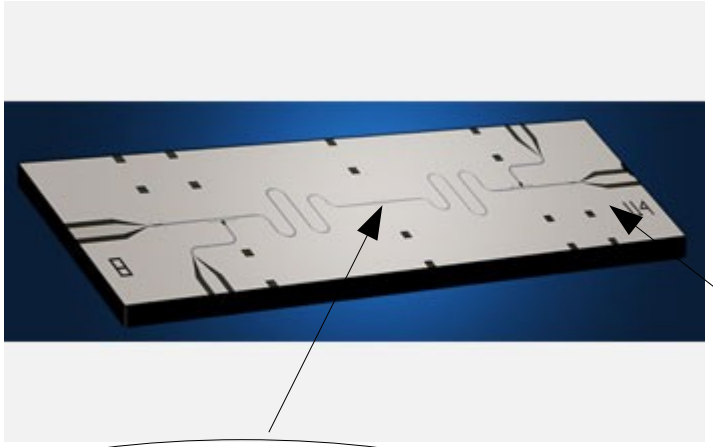
http://physics.stackexchange.com/

'Costruire' il Computer Quantistico...

'I'm sure they'll be useful in all sort of ways. I'm really a spectator, though, in experimental physics'
(Deutsch sullo 'Schoelkopf Lab')

Costruire il Q-Bit

Schoelkopf Lab's q-bit, Università di Yale



Nuclear magnetic resonance, cold ion trap, optical systems

Oggi, simulazione dei 'qbit' con SUPERCONDUTTORI (nanotecnologie)

Linea di trasmissione : coupling dei due qbit, mixing degli stati di ognuno (sovrapposizione ed entanglement)

Singolo qbit connesso all'altro mediante un linea trasmissione

SOLID-STATE QBITS

Yale

Simulazioni 'superconduttrici'

- Carica elettrica </> spin : i q-bit immagazzinano informazioni tramite le carica, non lo spin ma la logica binaria è la stessa. Oscillazioni di carica indotte da microonde.

- Atomo </> oggetto macroscopico : eccitazione di ognuno mediante scambio di coppie di Cooper con la 'repository', entanglement dei due attraverso supporto fisico. Simulazione dell'atomo.

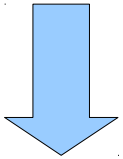
$S_z = \pm \hbar/2$, Q = ± 1, ….

A (|1>), S (|0>), SS (a|0> + b|1>)

Yale

Esempi di 'parallelismo-quantistico'

Più operazioni in parallelo...FIND THE QUEEN



4 alternative : computer classico 2,25 passi.
Quantistico : 1 solo!

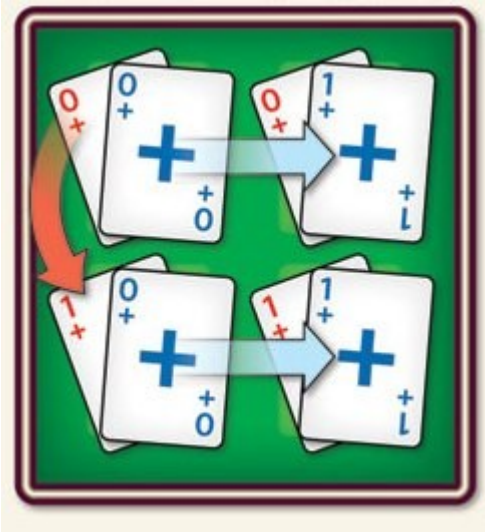
Rappresentazione dei 'Q-bit'

Colore delle carte (rosse e blu)	⟷	Posizione dei Q-bit [sx(red), dx(blu)]
Numeri sulle carte (0 e 1)	⟷	Stato dei Q-bit : A– S (fondamentale-eccitato, spin up-down,..)
Segno delle carte (+ e -)	⟷	Modalità di sovrapposizione dei Q-bit

FIND THE QUEEN

Stato di sovrapposizione

$\Psi \approx |0,0\rangle + |0,1\rangle + |1,0\rangle + |1,1\rangle$



...rappresentato in termini di carte

Operazioni 'lecite' sulle carte

'giro di colore': per ogni carta sul tavolo del colore scelto, viene aggiunta, a fianco, un'altra carta dello stesso colore e dello stesso segno ma con diverso contenuto

Giro colore su rosso e blu

IL GIOCATORE PUÒ CHIEDERE AL DEALER un...

Operazioni 'lecite' sulle carte

'cambio-carta': una carta a scelta di una coppia (a scelta) può essere sostituita con una carta del segno opposto

COPPIE IDENTICHE (O OPPOSTE) SO RIMUOVONO

Cambio carta da +1 a -1

IL GIOCATORE PUÒ CHIEDERE AL DEALER un...

Indovinare la coppia 'modificata'

Mr. Grover (terzo personaggio con gli occhi chiusi) chiede di 'cambiare-carta' promettendo che riuscirà ad indovinare quale coppia è stata modificata

[ad esempio] (+0,+1) ⟶ (+0,-1)

Allora Grover, a partire dalla nuova situazione, e tenendo gli occhi chiusi:
a) chiede carta su entrambi i colori;
b) cambia carta su (0,0);
c) chiede carta su entrambi i colori

A semplificazioni fatte rimane (1,0) la coppia che è la coppia modificata in partenza

...IL COMPUTER INDOVINA 'IN UN COLPO SOLO' LA COPPIA MODIFICATA FRA 4 ALTERNATIVE

Rivediamo le regole

1. *Cambiare carta [da |0,1> a |0,-1>]

$\Psi \approx$ |0,0> + |0,1> + |1,0> + |1,1>

generica sovrapposizione

$\Psi \approx$ |0,0> - |0,1> + |1,0> + |1,1>

entanglement

NASCONDO INFORMAZIONE

CREARE ENTANGLEMENT

2. *Fare un 'giro/i di colore'

$\Psi \approx$ |0,0> - |0,1> + |1,0> + |1,1>

entanglement

$\Psi =$ |1,0>

risultato

ESTRAGGO INFORMAZIONE

MANIPOLARE (PROPAGARE E POI DISTRUGGERE) ENTANGLEMENT

Una tappa 'intermedia'

$\Psi \approx$ |0,0> - |0,1> + |1,0> + |1,1>

$\Psi \approx$ |0,0> + |1,1>

$\Psi =$ |0,1>

L'ENTANGLEMENT VIENE 'PROPAGATO' FINO AD ESSERE LA SOMMA DI TERMINI (BASE DI BELL)

DISTRUTTO (MISURA)

PROPAGARE FINO A MASSIMIZZARE LO STATO ENTANGLED : LA FORMA DI BELL

Carte, conti...

Rotazioni di singolo Q-bit

$$|1\rangle \xrightarrow{H} |1\rangle + |0\rangle$$

Operazione sui 2 Q-bit

$$\begin{cases} |0\rangle \xrightarrow{C_{not}} |0\rangle \\ |1\rangle \xrightarrow{C_{not}} |0\rangle \end{cases}$$

MA... 'IN PRATICA'?

Il Computer...

Manipola lo stato entangled (nel quale è nascosta l'informazione) fino a massimizzarlo

CRITTOGRAFIA
(scambio della chiave)

BELL $\Psi \approx$ |0,0> + |1,1>

TELETRASPORTO
(misura congiunta)

Effettua la misura (distruzione dello stato entangled) ed estrae l'informazione ('un colpo solo')

RITORNO ALLA BASE...DI BELL!

A che punto siamo?

11 Maggio 2011: la D-Wave Systems annuncia il D-Wave One (128 Q-bit).

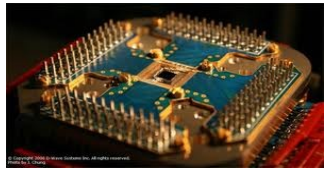
2013 : D-Wave Two (512 Q-bit). NASA e Google.

U(niverso) come C(omputer) e C come U

Se ogni atomo o molecola registra bit di informazione e le interazioni cambiano i rispettivi bit

→ Allora l'Universo 'calcola' e la sua storia è il risultato di un gigantesco calcolo quantistico. La fisica delle particelle e la MQ sono in realtà 'programmi' per l'Universo, disseminatori di complessità (Murray Gell Mann, Premio Nobel nel 1982).

Se con un computer quantistico di 300 qbit si possono eseguire più operazioni di quante siano tutte le particelle dell'Universo

→ Allora deve essere possibile 'simulare' l'Universo con un computer quantistico (Seth Loyd).

Ad un passo dalla FantaScienza?