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.

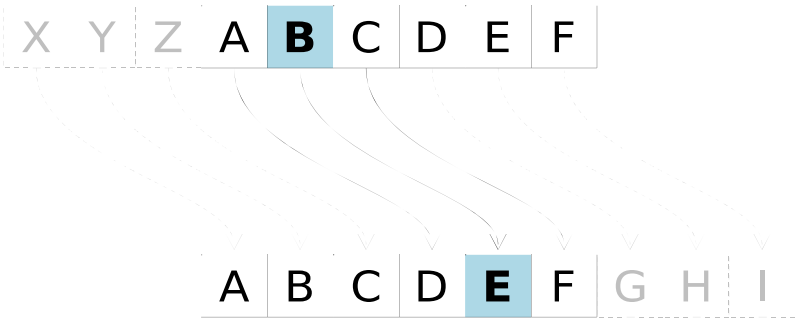
La 'chiave'...

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.



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

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

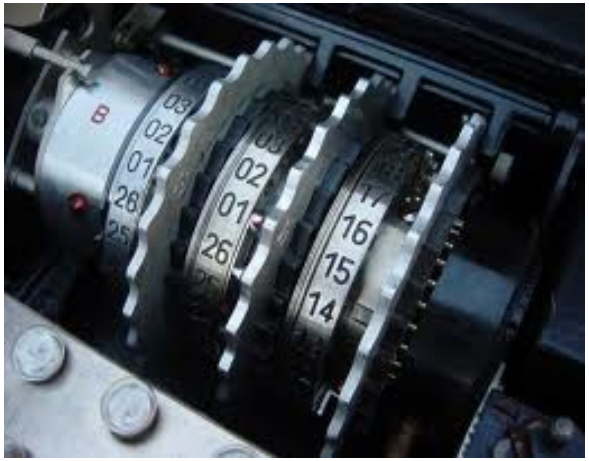
DZZDFFDUH LON NUUNGAFNENON LDOON DOOD RUD VHVZD

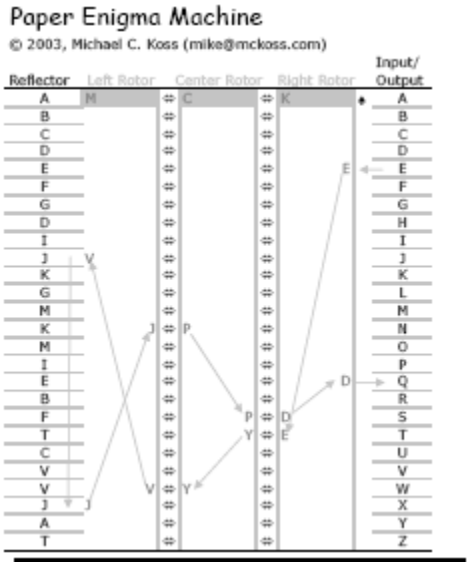
'attaccare gli irriducibili galli alla ora sesta'

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)

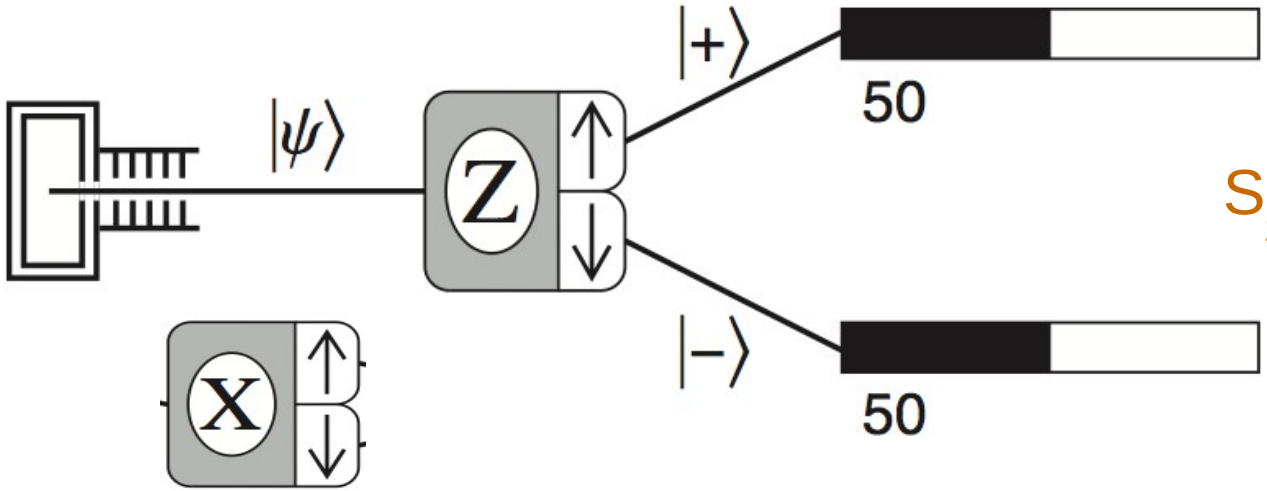
Crittografia 'quantistica'

- Idea di base: Sfruttare il fenomeno quantistico detto entanglement
- In linea di principio (esistono ancora difficoltà di realizzazione notevoli) è impossibile de-crittare il messaggio

Punto centrale: lo scambio della 'chiave'.

Un passo indietro...

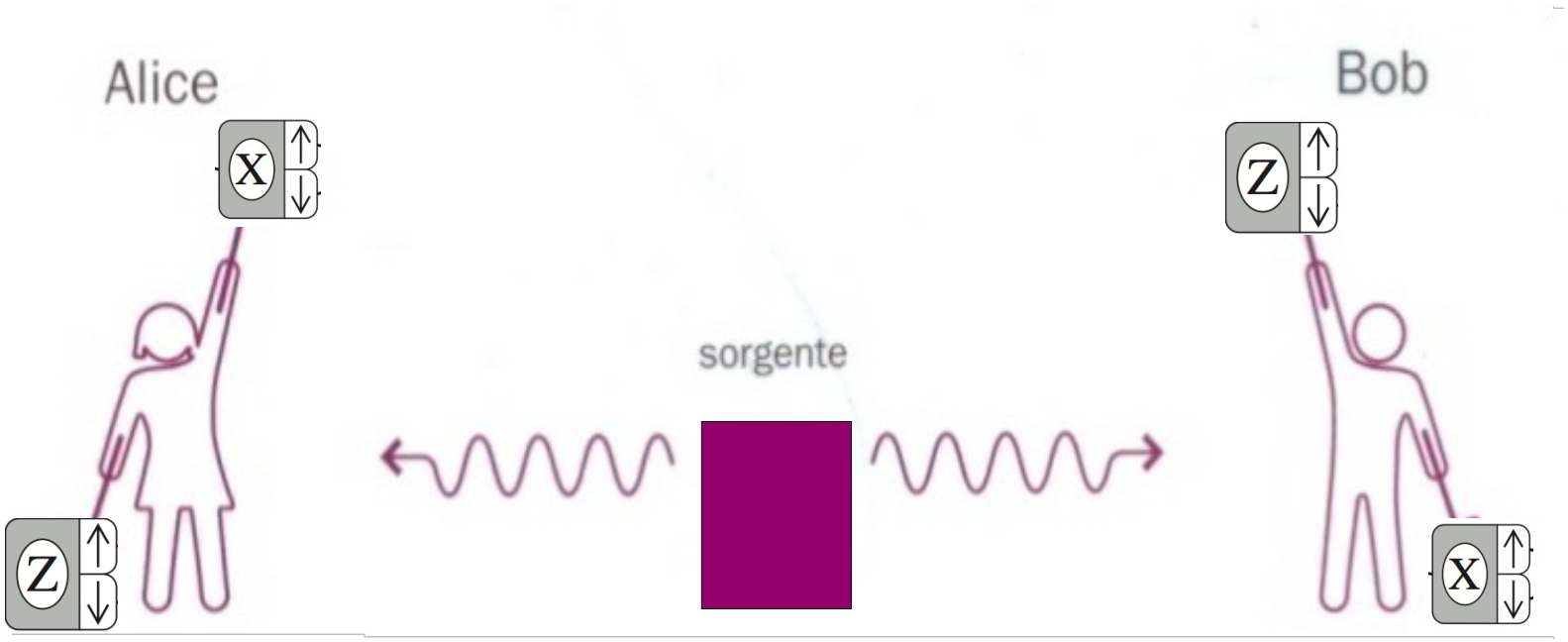
Atomi di argento attraverso apparato di Stern e Gerlach



$S_z = \pm \hbar/2$

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 »

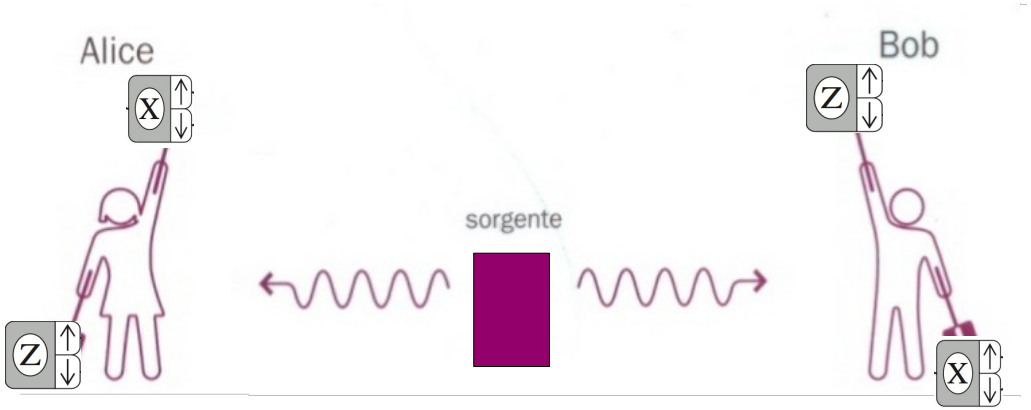
Se Alice e Bob misurano la stessa grandezza (ovvero entrambi S_z oppure S_x) → I risultati della misura – sebbene casuali – risultano identici (se Alice trova $+\hbar/2$ ($-\hbar/2$) allora lo stesso per Bob e viceversa).

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 completamente scorrelate

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'

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”?

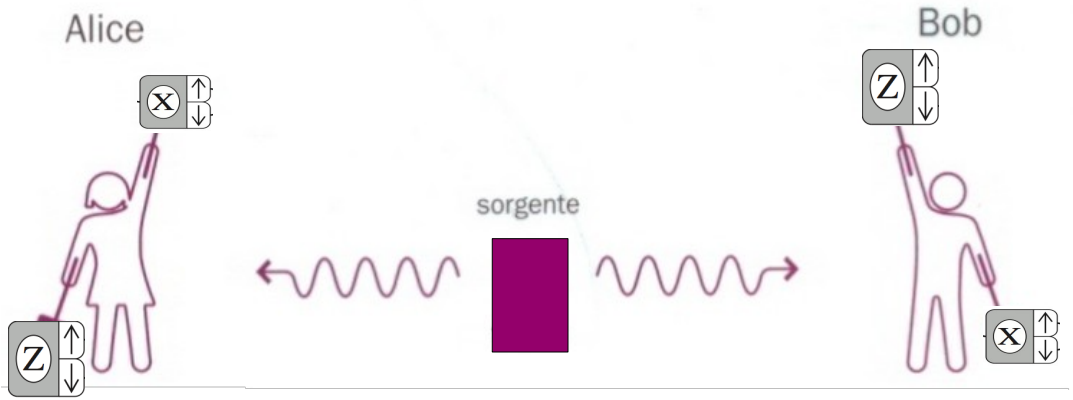
- Non si teletrasportano 'oggetti': particelle o addirittura persone

- 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 (incognito)

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

$|\psi\rangle_I$ 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 (incognito)

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

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

…….. +….+. :::

La misura di Alice distrugge questa sovrapposizione e collassare il sistema in uno di questi 4

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

Considerazione importante

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 : proibisce la creazione di copie identiche di uno stato sconosciuto

Fanta(?)Scienza?

1902 - *Le voyage dans la Lune*, film di Georges Melies

1969 – *Missione Apollo 11* e primo Uomo sulla Luna

1956 - *L'ultima domanda*, racconto di Isaac Asimov: prima intuizione (non scientifica) di 'computer quantistico'.

1981 - *Simulating Physics with Computers***, Richard P. Feynman: prima ipotesi scientifica sul computer quantistico

C(omputer) come U(niverso), U come C

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

Bit, cavi e porte logiche

'Dove' immaganizzare l'informazione: in qualunque sistema fisico che possieda due stati stabili e distinguibili.

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

Bit 'classico': assume 2 valori ('0' o '1')

Pensieri, condensatori...

I	=	1001001
n	=	0100000
p	=	1110000
r	=	1110010
i	=	1001001
n	=	....

'In principio era il verbo' (Vangelo di Giovanni)

Codice **A**merican **S**tandard **C**ode for **I**nformation **I**nterchange

...e logica

- 'Agire' sul valore dei bit
- Tutte le proposizioni logiche e i calcoli con 4 porte logiche (NOT, COPY, AND e OR)

George Boole, *'Indagine sulle leggi del pensiero'*

Computazione 'quantistica'

'Dove' immaganizzare l'informazione: atomo

Stato fondamentale → Valore |0>
Stato eccitato → Valore |1>

'Analogo' ma non 'identico' al condensatore

Discriminante classico-quantistico

|0, nessun fotone assorbito> + |1, fotone assorbito>

Sovrapposizione: non è in uno **o** nell'altro ma si trova 'contemporaneamente' in entrambi gli stati (in uno **e** nell'altro)

Cosa avviene 'nell'interazione'

'Parallelismo' quantistico

- Se i due stati si usano per immagazzinare informazione allora l'atomo ne registra 2 simultaneamente;
- Se ad ogni stato è associata un'operazione allora il computer svolge 2 operazioni in modo simultaneo.

'q-bit': unità di informazione che si può trovare anche in uno stato sovrapposto di |0> e |1>

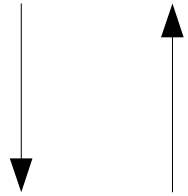
Un esempio...

|0> → 'calcola 2+2'

|1> → 'calcola 3+1'

|2> → 'calcola 4+0'

Quale operazione?



Quale fenditura?

CLASSICO: OPERAZIONI SEPARATE (1 O PIU' COMPUTER)
QUANTISTICO: OPERAZIONI SIMULTANEE SU 1 COMPUTER

Tutti i modi di scrivere il numero '4' come somma di interi non negativi

Potenti e...

1994, Peter Shor: dalla complessità esponenziale degli algoritmi di fattorizzazione classici, alla complessità polinomiale

Fattorizzazione di un numero di 400 cifre

→ Computer classico: 10^{10} anni

→ Computer quantistico < 3 anni

...minacciosi per gli attuali sistemi di sicurezza

Potenti e...

1996, Lov Grover: parallelismo quantistico e problema dell'ordinamento (algoritmi di ricerca)

Dato 1 milione di alternative. Qual'è il numero di ricerche che il computer effettua?

Computer classici: numero di ricerche è circa la metà del numero di alternative (½ milione).

Computer quantistici: numero di ricerche è la radice quadrata del numero di alternative (1.000).

...molto promettenti in tutti i contesti ad alto livello di informatizzazione

A che punto siamo (1)?

11 Maggio 2011: la D-Wave Systems annuncia il D-Wave One.

Computer quantistico basato su 128 q-bit (primo in commercio).

E' davvero un CQ a tutti gli effetti?

A che punto siamo (2)?

11 Aprile 2011: Seth Loyd, director of the Center for Extreme Quantum Information Theory at MIT

I: How many q-bits are there in today's quantum computers?

SL: *'We're up to around a dozen, so we can solve complicated equations really fast'.*

http://www.popsci.com/science/article/2011-10/seth-lloyd-particle-man

???

La comunità scientifica...

Rivista « PhysicsWorld »

21 Marzo 2013

'Quantum computing: Challenges, triumphs and applications'

http://physicsworld.com/cws/article/multimedia/2013/mar/21/quantum-computing-challenges-triumphs-and-applications

...dibattito e prove in corso sulle potenzialità del D-Wave One

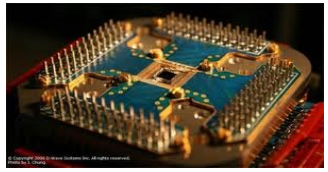
U(niverso) come C(omputer) e C come U

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).



Quanto lontani da Asimov?

21 Gennaio 2013 su giornali e radio

Articolo sul quotidiano “La Stampa” di Perio Bianucci “Prove tecniche di teletrasporto”.

Trasmissione 'Pagina 3' su RadioTre

La notizia del teletrasporto realizzato da Anton Zeilinger dell'Università di Vienna

21 Gennaio 2013 su giornali e radio

Articolo sul quotidiano “La Stampa” di Perio Bianucci “Prove tecniche di teletrasporto”.

Trasmissione 'Pagina 3' su RadioTre

La notizia del teletrasporto realizzato da Anton Zeilinger dell'Università di Vienna