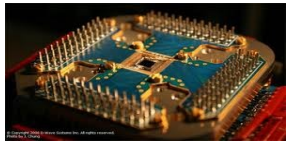
Applicazioni della Meccanica Quantistica

EUGENIO BERTOZZI, DIPARTIMENTO DI FISICA,
UNIVERSITA' DI BOLOGNA

'Genuinamente' quantistiche

- Crittografia 
- 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.

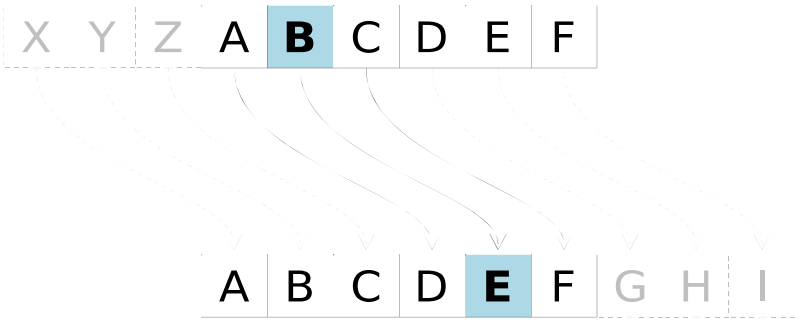
La 'chiave'...

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.



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

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

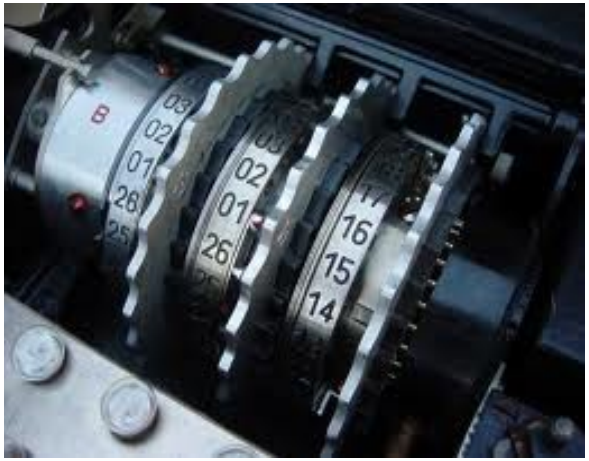
DZZDFFDUH LON NUUNGAFNENON LDOON DOOD RUD VHVZD

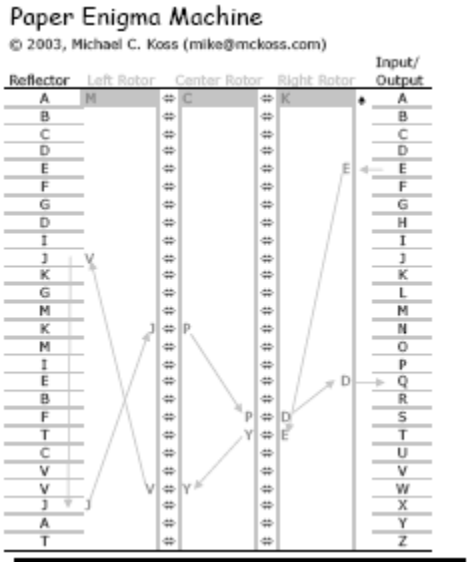
'attaccare gli irriducibili galli alla ora sesta'

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 la natura quantistica dei fotoni e l'entanglement

- In linea di principio (esistono ancora difficoltà di realizzazione notevoli) è impossibile de-crittare il messaggio

Punto centrale: lo scambio della 'chiave'.

Protocollo di Eckert, 1991

LA MISURA: POLARIZZAZIONE DEI FOTONI IN DIREZIONE VERTICALE E A 45°

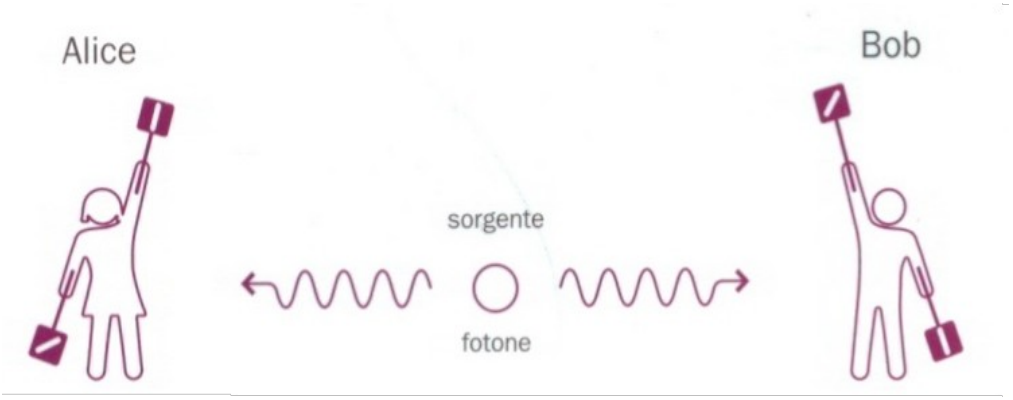
Se si eseguono misure uguali (ad es. sinistra-verticale, destra-verticale) → I risultati della misura – sebbene casuali – risultano identici

Se si eseguono misure miste (ad es. sinistra-verticale, destra-45°) → Non è possibile dire nulla: ogni fotone “sopravviverà” o verrà assorbito dalla lastra con probabilità ½

'Il' fenomeno: l'entanglement

I quattro passi

- Passo 1. Emissione dei fotoni dalla sorgente.
- Passo 2. Misure di polarizzazione (verticale o a 45°): libera scelta ('1' passa, '0' no)
- Passo 3. Comunicazione sequenza delle misure: canale tradizionale (telefono)
- Passo 4. Eliminazione dei casi in cui hanno eseguito misure diverse: cosa rimane?



Alice		Bob		
filtro utilizzato	esito della misura	filtro utilizzato	esito della misura	chiave
▯	1	⁄	0	
⁄	0	▯	1	
▯	1	▯	1	1
▯	0	⁄	1	
⁄	0	⁄	0	0
⁄	1	⁄	1	1
⁄	0	▯	1	
▯	1	⁄	0	
▯	0	▯	0	0
▯	1	⁄	1	
⁄	0	⁄	0	0

sequenza 'pulita' di numeri: la chiave quantistica

La chiave quantistica è...

- Identica per entrambi (fotoni entangled)
- 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'

Fanta(?)Scienza?

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

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

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

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>

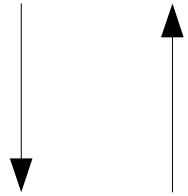
Un esempio...

|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).

Molti dubbi su 'cosa sia' realmente

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

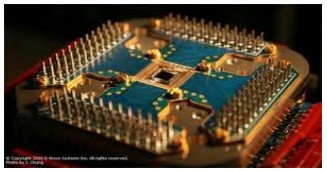
???

La comunità scientifica...

'At the moment it is impossible to say if D-Wave's quantum computer is intrinsically equivalent to a classical computer or not. So until more is known about their error rates, caveat emptor is the least one can say'.

Wim van Dam, 'Quantum computing: In the 'death zone'?', *Nature Physics 3, 220 - 221 (2007)* doi:10.1038/nphys585 (Departments of Computer Science and Physics, University of California, Santa Barbara)

Necessità di 'trasparenza': Caveat emptor



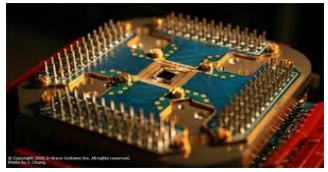
U(niverso) come C(omputer) e C come U

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 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?

Per la discussione...

- La MQ sembra fornire: la possibilità di ottenere un livello di sicurezza inviolabile (entanglement) e, contemporaneamente,un strumento per rendere attaccabili tutti i sistemi di crittografia attualmente utilizzati (computer quantistico). La fisica avanzata e le sue implicazioni...

- La prima idea (scientifica) di computer quantistico risale agli anni 80. Nel 2011 questi computer risolvono solo equazioni differenziali. La fisica avanzata e i suoi tempi...

...