DIRE L'INDICIBILE
l'entanglement quantistico

ITALIAN QUANTUM WEEKS

FARE DI QONTO
Il qubit e la logica quantistica

Il **bit** si comporta come la faccia di una moneta classica che può essere solo testa = **0** o croce = **1**

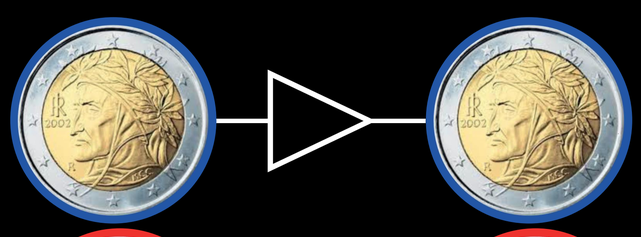
Il **qubit** si comporta come la faccia di una moneta quantistica che può essere anche una **sovrapposizione** di testa = **0** e croce = **1**

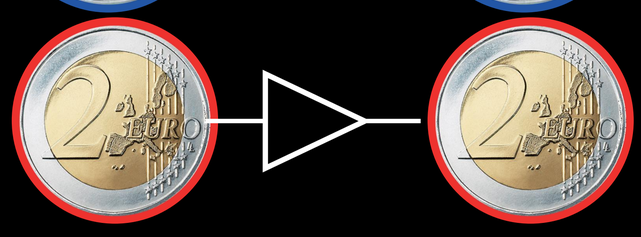
$|0\rangle$   $|1\rangle$

$$\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

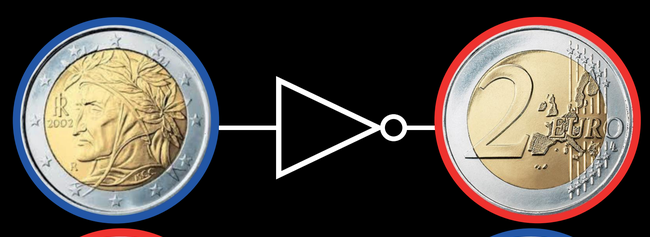
Le porte logiche classiche sono operazioni che agiscono sui bit.
Le porte logiche più semplici sono a singola variabile, ne esistono di due tipi...

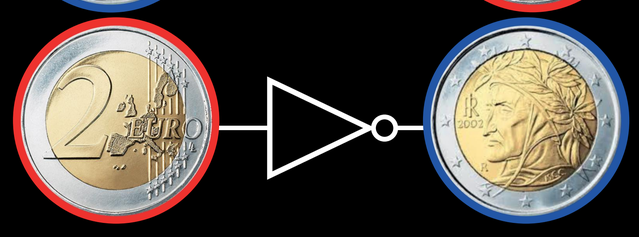
IDENTITÀ

$I|0\rangle=|0\rangle$ 

$I|1\rangle=|1\rangle$ 

NOT

$\mathrm{NOT}|0\rangle=|1\rangle$ 

$\mathrm{NOT}|1\rangle=|0\rangle$ 

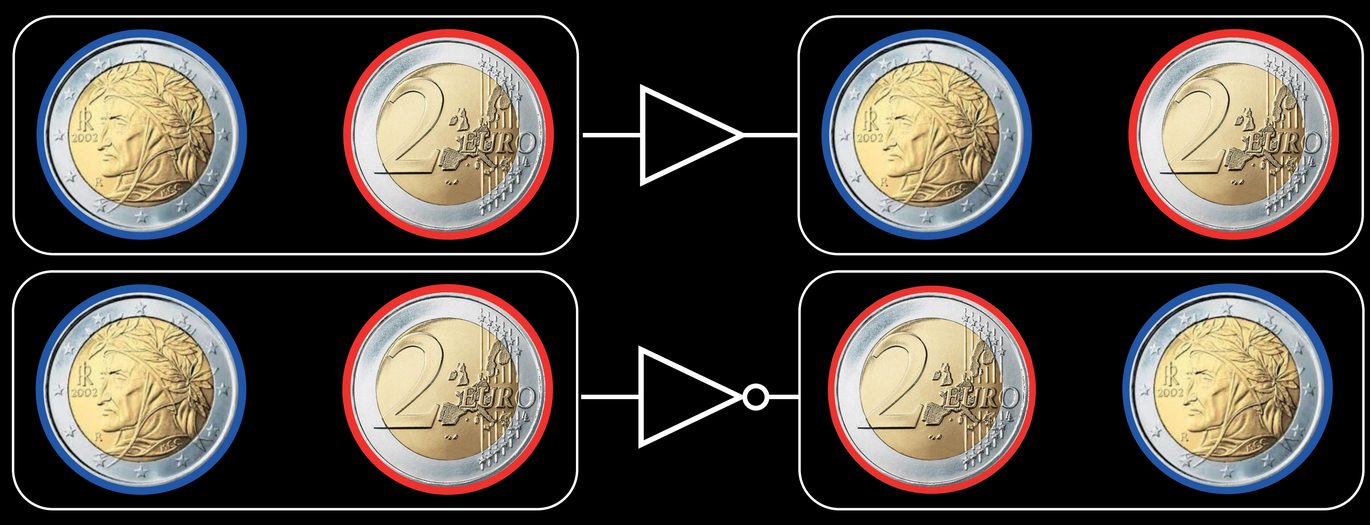
...che si possono estendere ai qubit

IDENTITÀ

$$I\left(c_0|0\rangle+c_1|1\rangle\right)=c_0|0\rangle+c_1|1\rangle$$

NOT

$$\mathrm{NOT}\left(c_0|0\rangle+c_1|1\rangle\right)=c_0|1\rangle+c_1|0\rangle$$



HADAMARD

La logica quantistica permette di realizzare nuove porte logiche che non hanno un corrispondente classico

$$H|0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}}$$

$$H|1\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}}$$

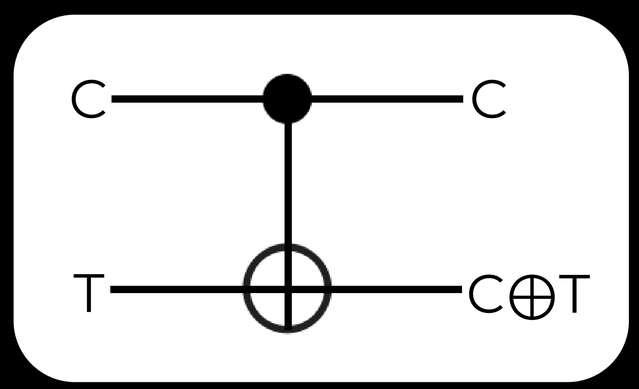
DIRE L'INDICIBILE
l'entanglement quantistico

ITALIAN QUANTUM WEEKS

BIT E QUBIT
Entanglement = Sovrapposizione + Correlazione

La **Porta Not Controllata** (CNOT) è una porta logica quantistica a due qubit essenziale per la costruzione dei computer quantistici

INPUT		OUTPUT	
Controllo	Target	Controllo	Target
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

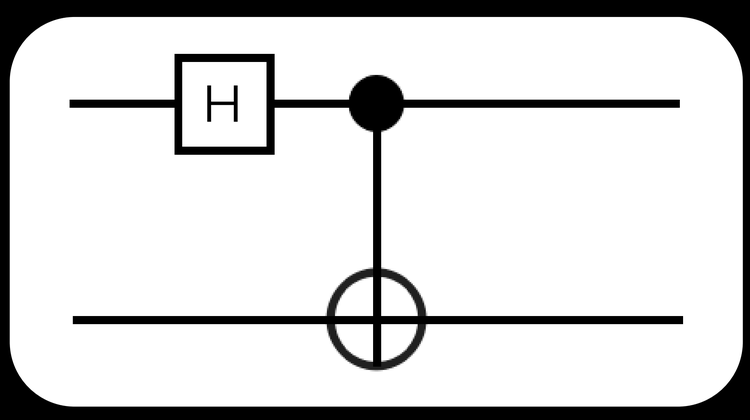


La Porta **CNOT** agisce su due qubit: inverte lo stato del secondo qubit (target, T) se e solo se il primo qubit (controllo, C) è $|1\rangle$.

La Porta CNOT forma, insieme alle operazioni a singolo qubit di rotazione e shift di fase, un insieme universale di **porte logiche quantistiche**: qualsiasi operazione unitaria può essere scomposta in una combinazione di porte CNOT e delle suddette porte a singolo qubit.

Costruzione di stati di Bell

Le porte CNOT e Hadamard possono essere usate per costruire gli **stati di Bell**, i più semplici esempi di stati entangled a due qubit.



Ad esempio lo stato di Bell $\left|\Phi^{+}\right\rangle = \frac{|0\rangle_C|0\rangle_T + |1\rangle_C|1\rangle_T}{\sqrt{2}}$

si ottiene facendo agire il circuito in figura sullo stato iniziale $|0\rangle_C|0\rangle_T$

$$\mathbf{CNOT}\left(H_C \otimes I_T\right)|0\rangle_C|0\rangle_T = \mathbf{CNOT}\left(\frac{|0\rangle_C + |1\rangle_C}{\sqrt{2}}\right)|0\rangle_T = \frac{|0\rangle_C|0\rangle_T + |1\rangle_C|1\rangle_T}{\sqrt{2}} = \left|\Phi^{+}\right\rangle$$

sovrapposizione

correlazione

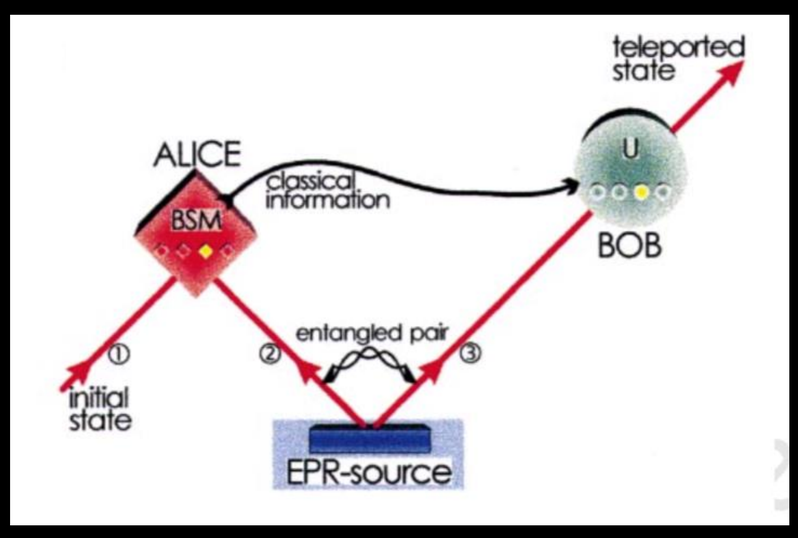
È possibile lavorare con porte logiche quantistiche da casa accedendo, per esempio, alla piattaforma **IBMQ**.

DIRE L'INDICIBILE
l'entanglement quantistico

ITALIAN QUANTUM WEEKS

L'ENTANGLEMENT ALL'OPERA
Le applicazioni dell'entanglement

Come dimostrato anche da Zeilinger in alcuni lavori pionieristici di fine anni '90, l'**entanglement è una risorsa** utile per la realizzazione di diversi **protocolli di informazione quantistica** che sono usati nelle diverse **tecnologie quantistiche**, in particolare nel calcolo quantistico.



Crediti a Nature 390, 575-579 (1997)

TELETRASPORTO QUANTISTICO

Trasmissione e ricostruzione su distanze arbitrarie dello stato di un sistema quantistico sconosciuto.

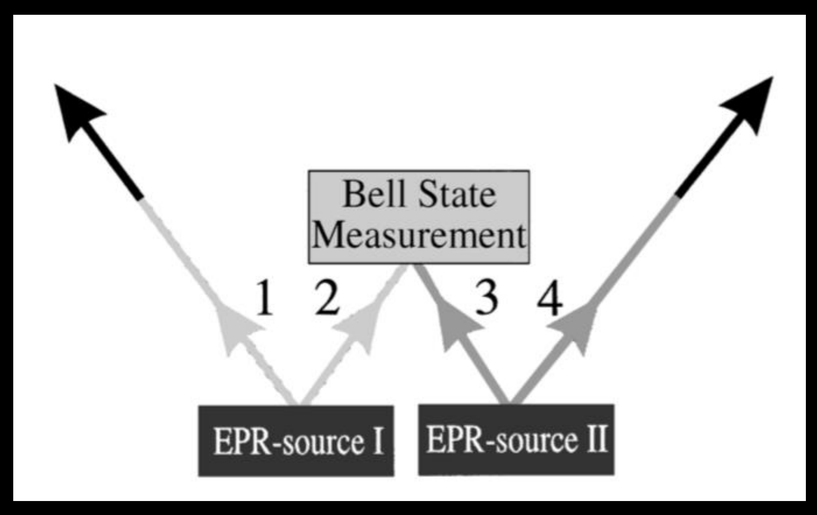
Lo schema originale riguarda il teletrasporto dello stato di polarizzazione di un fotone da Alice a Bob.

- Alice e Bob condividono una coppia di fotoni entangled in polarizzazione
- Alice sovrappone ad un beam splitter il fotone da trasportare al suo fotone entangled e misura la polarizzazione su almeno due basi distinte (misure di Bell)
- Alice comunica a Bob il risultato delle misure
- Sulla base delle informazioni di Alice, Bob applica delle rotazioni di polarizzazione al suo fotone entangled ottenendo lo stato di polarizzazione del fotone iniziale.

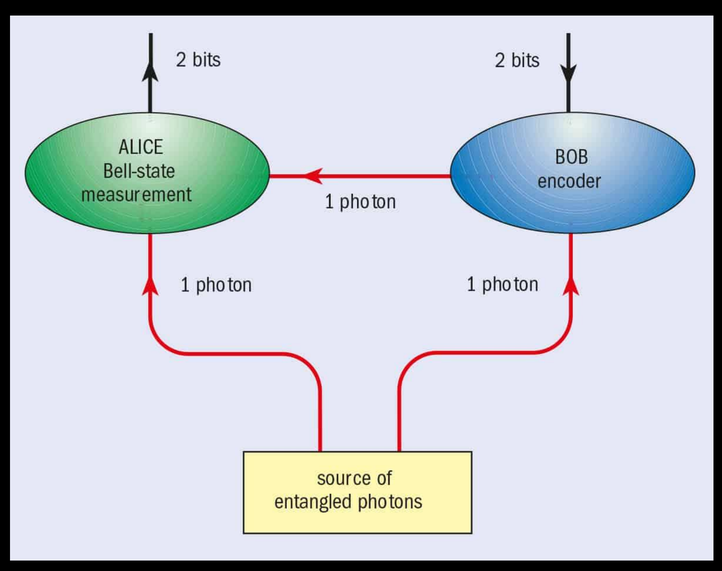
ENTANGLEMENT SWAPPING

Questo protocollo consente di rendere entangled due fotoni che hanno un'origine differente e che non hanno mai interagito tra di loro.

Lo schema di realizzazione prevede la generazione di due coppie di fotoni entangled in polarizzazione. Un fotone di una coppia viene sovrapposto ad un beam splitter con un fotone dell'altra coppia. Eseguendo di nuovo misure di Bell, cioè su basi di polarizzazione differente, all'uscita del beam splitter, si rendono entangled tra loro i due fotoni rimanenti che non hanno interagito.



Crediti a Phys. Rev. Lett. 80, 3891-3894 (1998)



SUPERDENSE CODING

E' un protocollo che permette di comunicare un numero di bit classici di informazione trasmettendo un numero minore di qubit.

La condizione necessaria è che mittente e destinatario condividano una risorsa entangled.

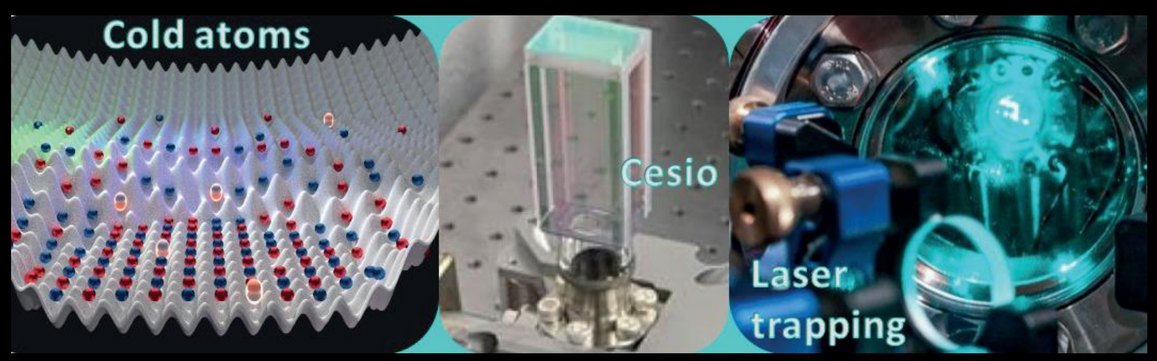
Protocollo di Charles H. Bennett e Stephen Wiesner (1970, pubblicato nel 1992) realizzato nel 1996 dal gruppo di Zeilinger.

DIRE L'INDICIBILE
l'entanglement quantistico

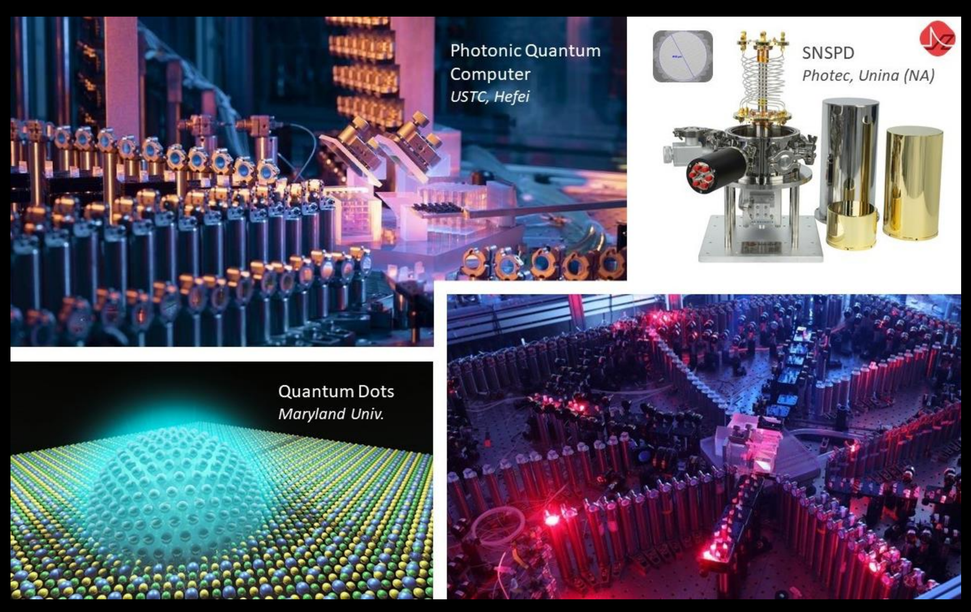
ITALIAN QUANTUM WEEKS

CHE FACCIA HA UN COMPUTER QUANTISTICO?
Un problema, soluzioni diverse

In un quantum computer ad **atomi freddi**, gli atomi sono bloccati in un reticolo artificiale con dei laser in una camera a vuoto spinto. In questo modo gli atomi sono quasi fermi, la temperatura del sistema è perciò prossima allo zero assoluto.

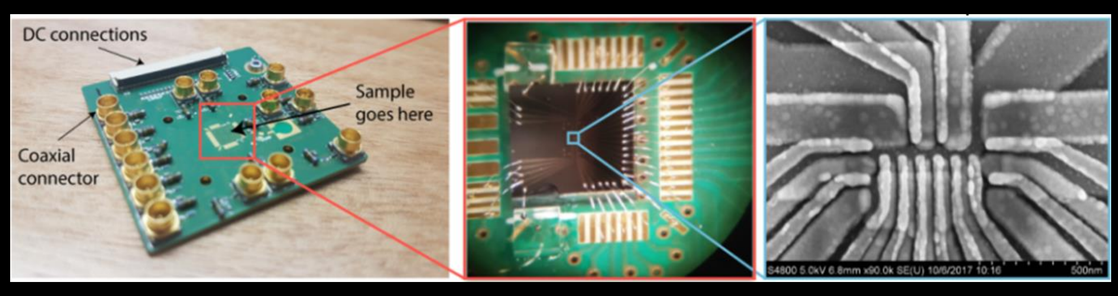


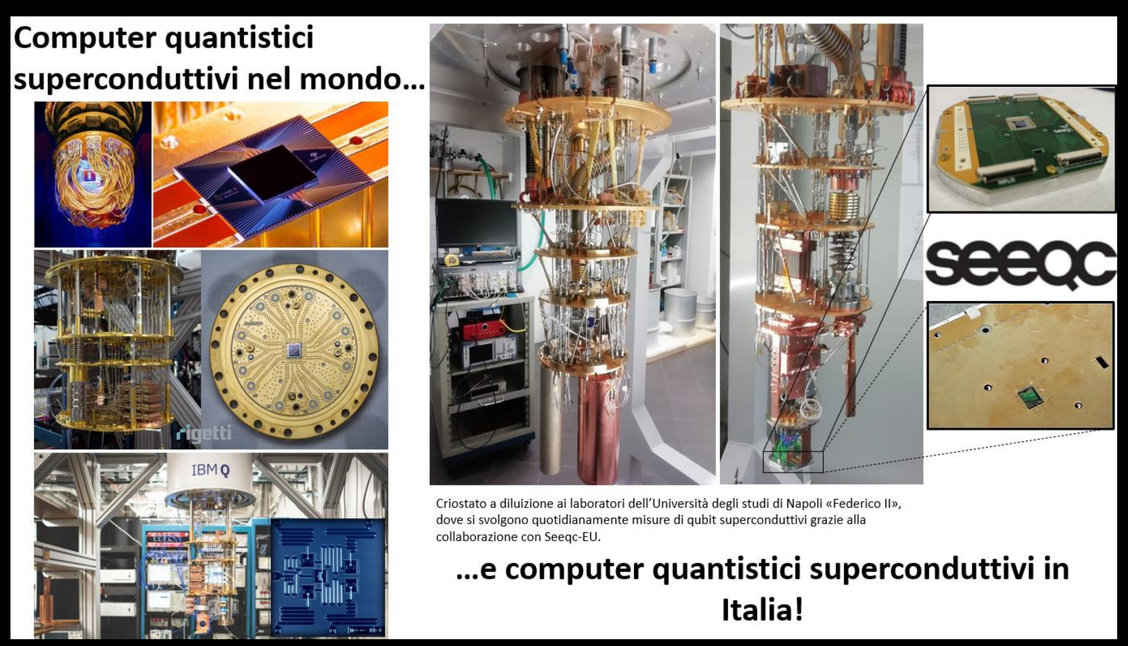
Con un laser si può modificare lo stato del qubit facendolo passare da un livello energetico ad un altro, oppure modificare il reticolo, simulando sistemi come atomi o molecole.



Per ottenere un **computer quantistico fotonico**, bisogna disporre di una sorgente di singoli fotoni, di un sistema di ottiche (lenti, specchi, filtri, beam splitter), che fungono da porte logiche, e di rivelatori molto sensibili che siano in grado di misurare il singolo fotone e quindi fornire l'informazione sullo stato del qubit.

La Intel Corporation negli ultimi anni ha spinto la propria ricerca verso la realizzazione di chip composti da **spin qubit** per la realizzazione di computer quantistici: chip in silicio di circa 50 nanometri, visibili solo al microscopio elettronico, con fili stampati che collegano i qubit al mondo esterno.





I **qubit superconduttivi** necessitano di un ambiente criogenico perché:
1) l'alluminio, di cui sono fatti quasi tutti, è superconduttivo solo al di sotto di -272.15°C;
2) la separazione tra i livelli del qubit è tanto più definita quanto più bassa è la temperatura di lavoro.

Serve anche un'elettronica a microonde, perché i segnali di controllo/lettura di un qubit superconduttivo devono lavorare a frequenze corrispondenti alle sue eccitazioni energetiche (qualche gigahertz).

Un esempio di quello che possono fare attualmente i qubit superconduttivi?

SCAN ME

Usa il QRcode per ascoltare la prima compilation musicale composta dal computer quantistico a 16 qubit superconduttivi IBM Guadalupe!

DIRE L'INDICIBILE
l'entanglement quantistico

ITALIAN QUANTUM WEEKS

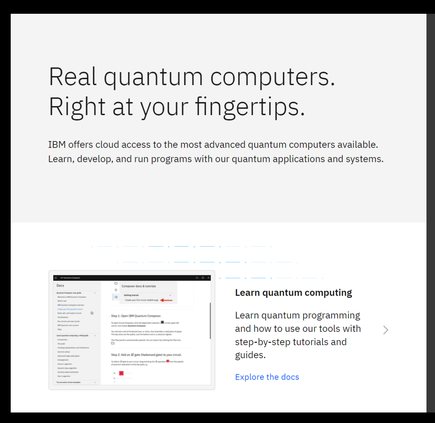
ALGORITMI QUANTISTICI PER TUTTI
Programmare un computer quantistico

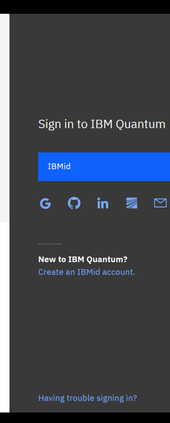
Un **algoritmo** è una sequenza di operazioni (porte logiche/gate) che possono essere realizzate su un calcolatore. Un algoritmo è rappresentabile in forma circuitale.

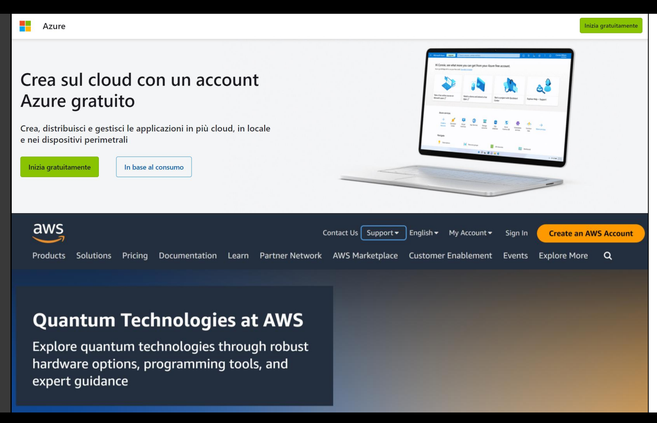
Gli **algoritmi quantistici** possono essere eseguiti solo da computer che usano risorse quantistiche, ovvero in grado di generare **stati di sovrapposizione** o **stati entangled** e di manipolarli mantenendone le caratteristiche quantistiche, ovvero la **coerenza**.

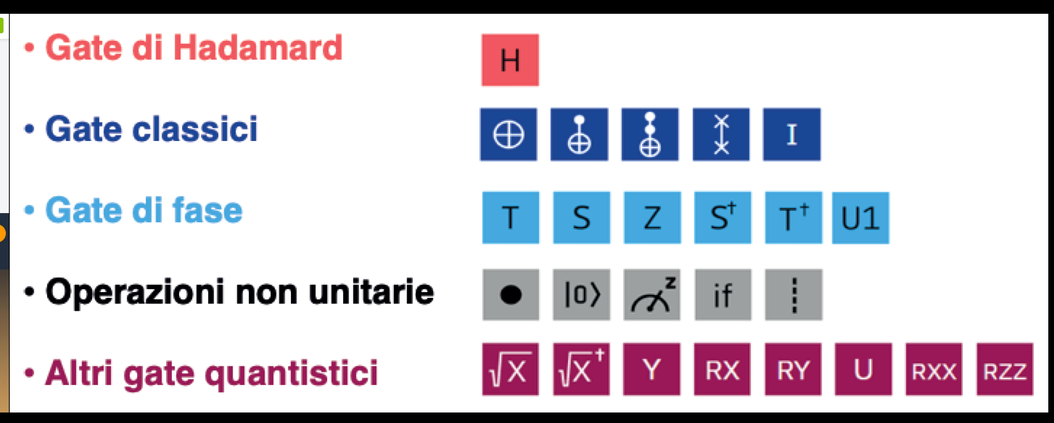
Celebri algoritmi quantistici sono: Shor, Grover, Deutsch...

E' possibile accedere a **computer quantistici reali** tramite alcune **piattaforme online** come IBM Quantum Experience, Amazon Braket e Microsoft Azure Quantum che permettono di eseguire algoritmi quantistici sia su dei **simulatori classici** che su **macchine reali** utilizzando un certo numero di **porte logiche**.

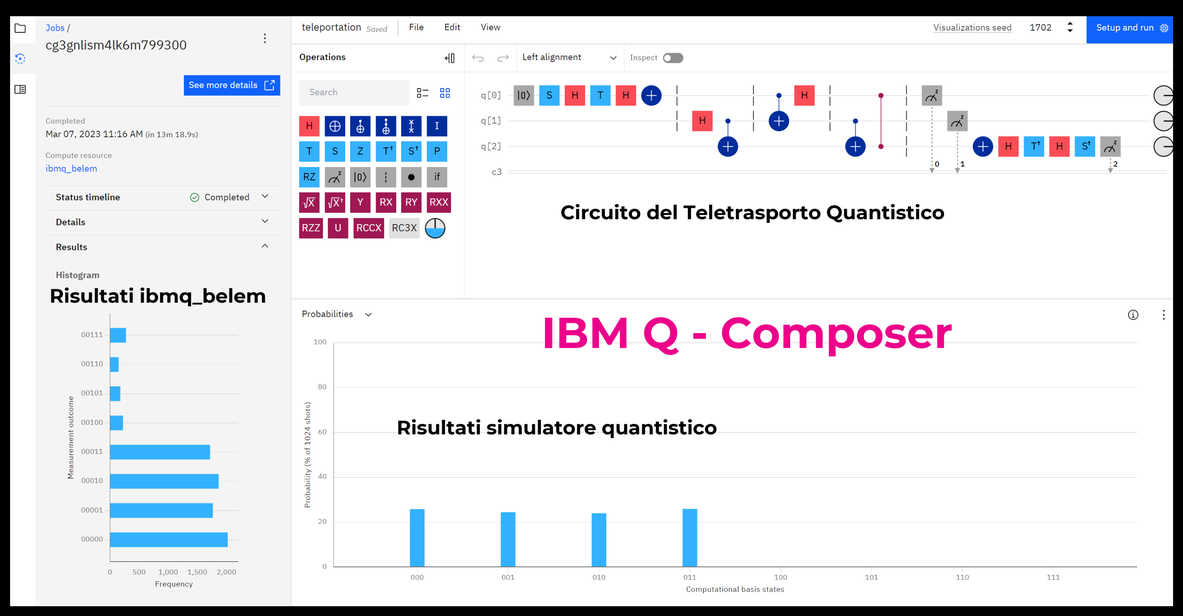








Algoritmo del Teletrasporto Quantistico su IBM Q



IBM Q - Composer

Algoritmo del teletrasporto quantistico sul simulatore di **IBM Q** e sul computer reale a 5 qubit **ibmq_belem**.
Il computer reale ha risultati peggiori a causa degli **errori sperimentali** dovuti alla **decoerenza**.

DIRE L'INDICIBILE
l'entanglement quantistico

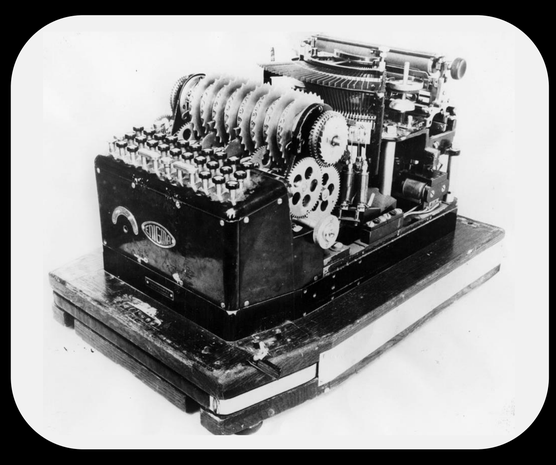
ITALIAN QUANTUM WEEKS

MANTENIAMO IL SEGRETO!
Crittografia classica

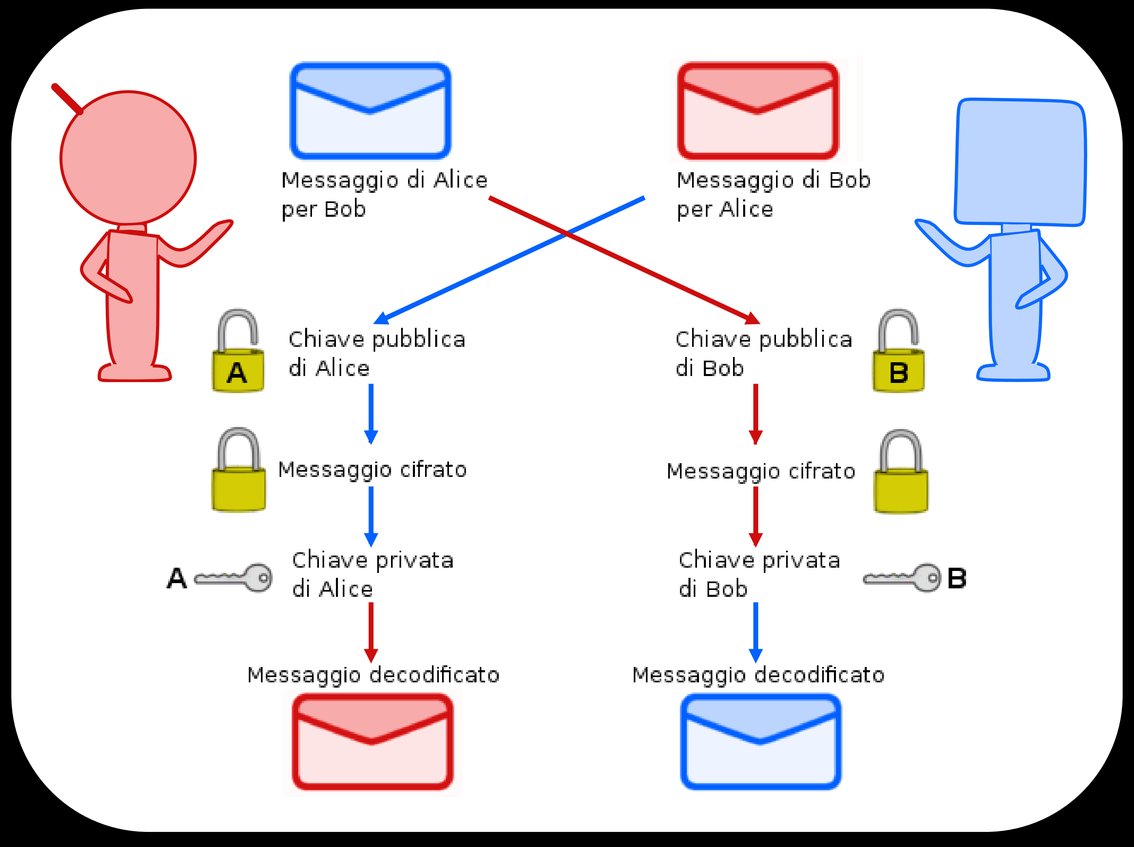
Criptazione o **crittografia** - dal greco κρυπτός = **nascosto**

Tecnica per garantire l'**autenticazione** e il **contenuto** di informazioni trasmesse tramite vari canali di comunicazione.

Non si nasconde il messaggio in sé, ma il suo **significato**, rendendone il testo incomprensibile attraverso un algoritmo, noto solo al mittente e al destinatario, che effettua sostituzioni e trasformazioni sul testo in chiaro.
Il destinatario può invertire il procedimento e ricavare il testo originale.



La crittografia moderna utilizza il **sistema RSA** (Rivest, Shamir e Adleman) che si basa su



Chiave pubblica,
nota a tutti,
necessaria per **cifrare**
il messaggio.

Chiave privata,
nota solo al destinatario,
che permette a lui soltanto di
decifrare il messaggio.

La sicurezza si basa sulla complessità

Le chiavi di accesso sono basate su **algoritmi complessi** (fattorizzazione di numeri interi grandi, logaritmo discreto) perché sia computazionalmente (quasi) impossibile calcolarle con tecniche classiche.

Il protocollo è **vulnerabile** ai miglioramenti della potenza computazionale o alla scoperta di algoritmi efficienti per risolvere i problemi sottostanti, come ad esempio l'**algoritmo di Shor**.

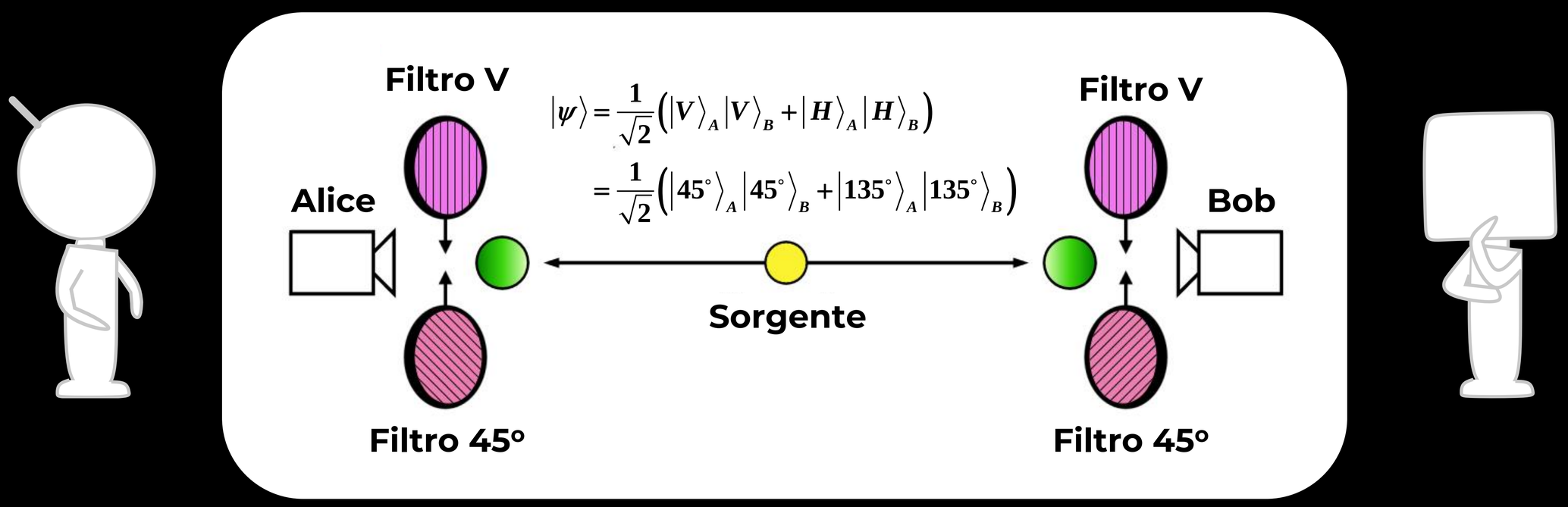
DIRE L'INDICIBILE
l'entanglement quantistico

ITALIAN QUANTUM WEEKS

QUALCUNO CI ASCOLTA...
Crittografia quantistica

Gli stessi principi che potenziano i computer quantistici offrono anche una soluzione sicura al problema della distribuzione delle chiavi necessarie per **cifrare** e **decifrare** i messaggi.

Nel 1991, Artur K. Ekert propose un protocollo di **crittografia quantistica** ora noto come protocollo E91.



Il protocollo E91 utilizza coppie di **fotoni entangled**, distribuiti in modo che le due parti coinvolte nella comunicazione, Alice e Bob, ricevano un fotone da ciascuna coppia.

Lo schema si basa su **due proprietà dell'entanglement**:

Gli stati entangled sono **perfettamente correlati**:
quando Alice e Bob misurano con i polarizzatori orientati nello stesso modo, ottengono sempre la stessa risposta con il 100% di probabilità.

I **risultati** delle **misure** sono **casuali**:
è impossibile per Alice prevedere se lei (e quindi Bob) otterrà la polarizzazione verticale o la polarizzazione orizzontale

Ogni tentativo di intercettazione da parte di un intruso distruggerà le correlazioni tra gli stati entangled, producendo risultati errati per le misure compiute da Alice e da Bob.

Alice e Bob si possono accorgere dell'intercettazione.

DIRE L'INDICIBILE
l'entanglement quantistico

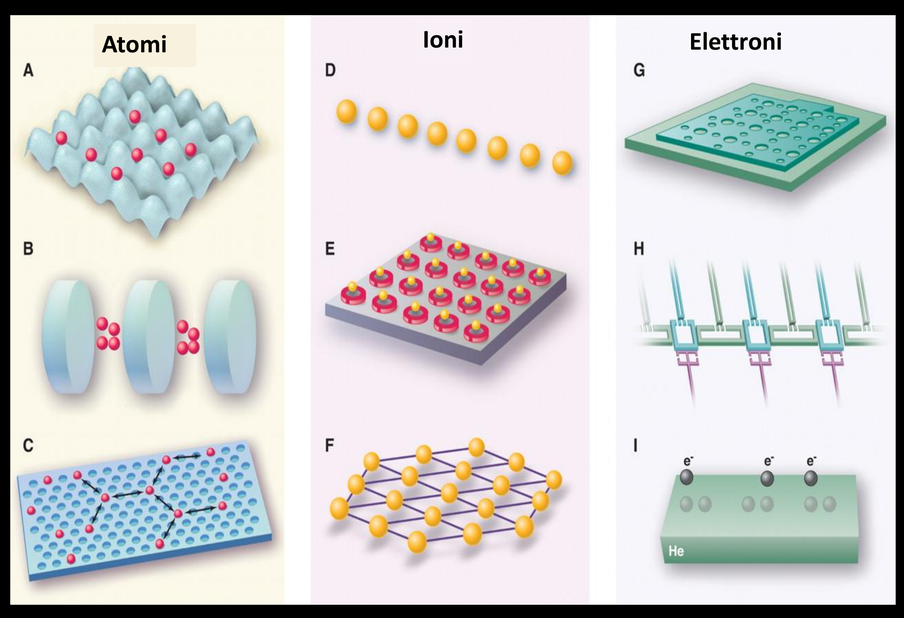
ITALIAN QUANTUM WEEKS

FACCIAMO COME SE...
I simulatori quantistici

"...la natura non è classica, e se vuoi fare una simulazione della natura, faresti meglio a farla quantistica...".

R.P. Feynman

L'approccio standard allo studio della dinamica dei sistemi quantistici per i quali sia difficile realizzare un esperimento reale è utilizzare le simulazioni numeriche. Tuttavia ci sono casi di problemi non calcolabili.



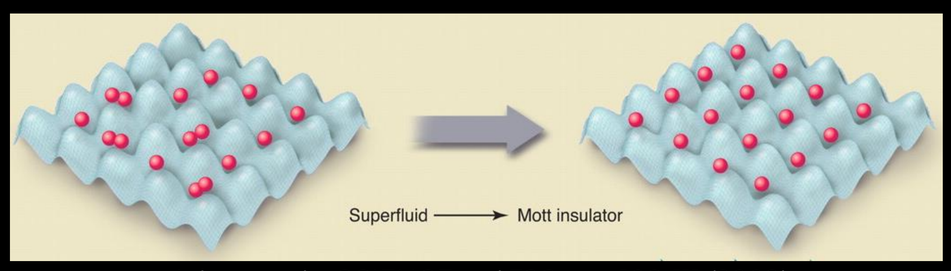
Adattato da *SCIENCE, vol 326, pp. 108-111 (2009)*

I **simulatori quantistici** sono strutture quantistiche artificiali, controllabili e manipolabili in laboratorio, costruite per simulare con precisione i comportamenti quantistici della materia.

Possono essere di varia natura e sfruttano **sovrapposizione** ed **entanglement**.

Atomi intrappolati

Atomi intrappolati in **reticoli ottici** di cui si controllano le profondità delle buche consentono di simulare la fisica dei modelli di spin e le transizioni di fase quantistica da un superfluido ad un isolante di Mott.

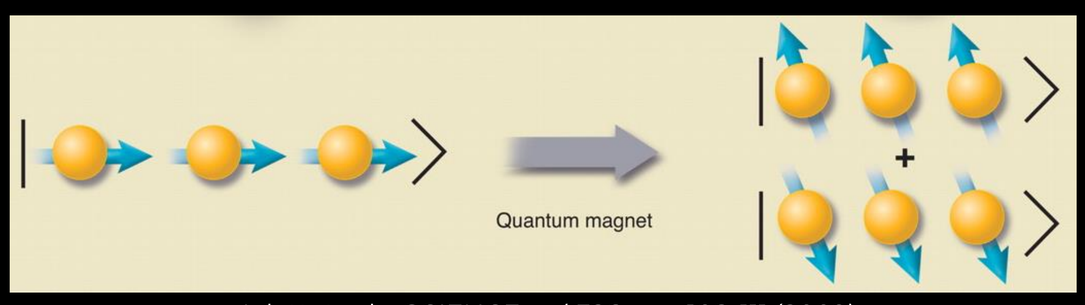


Adattato da *SCIENCE, vol 326,, pp. 108-111 (2009)*

Atomi intrappolati **in cavità** e manipolati da un laser esterno formano polaritoni, che consentono di simulare il modello di Bose-Hubbard e transizioni di fase quantistiche.

Ioni intrappolati

Gli ioni, essendo carichi, sono più facili da misurare e manipolare singolarmente.
Si usano per studiare la transizione dall'ordine paramagnetico a quello ferromagnetico.



Adattato da *SCIENCE, vol 326,, pp. 108-111 (2009)*

Elettroni

Si possono costruire **atomi** e **molecole artificiali** per verificare la meccanica quantistica a scale macroscopiche e per simulare reazioni chimiche.
Si usano **quantum dots semiconduttori,** che hanno il vantaggio di poter raggiungere temperature di Fermi molto basse e di poter avere interazioni coulombiane a lungo raggio, o **circuiti superconduttori**, confinando gli elettroni su piccole isole superconduttive e manipolandoli anche con correnti e tensioni.

Quantum annealers

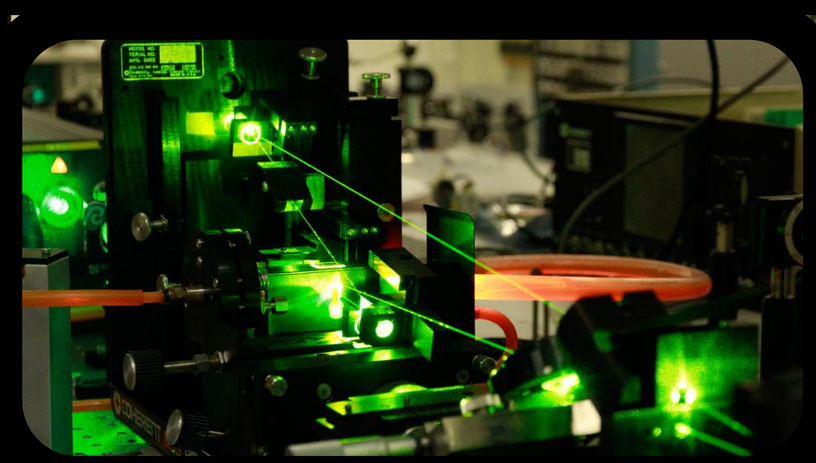
Sono computer quantistici che simulano il processo di annealing, in cui un materiale viene riscaldato e poi gradualmente raffreddato per raggiungere uno stato di bassa energia.
Sono utilizzati per risolvere problemi di ottimizzazione, trovando la soluzione senza calcolarla!
Il più celebre quantum annealer è D-Wave.

DIRE L'INDICIBILE
l'entanglement quantistico

ITALIAN QUANTUM WEEKS

MISURA PER MISURA
La metrologia quantistica

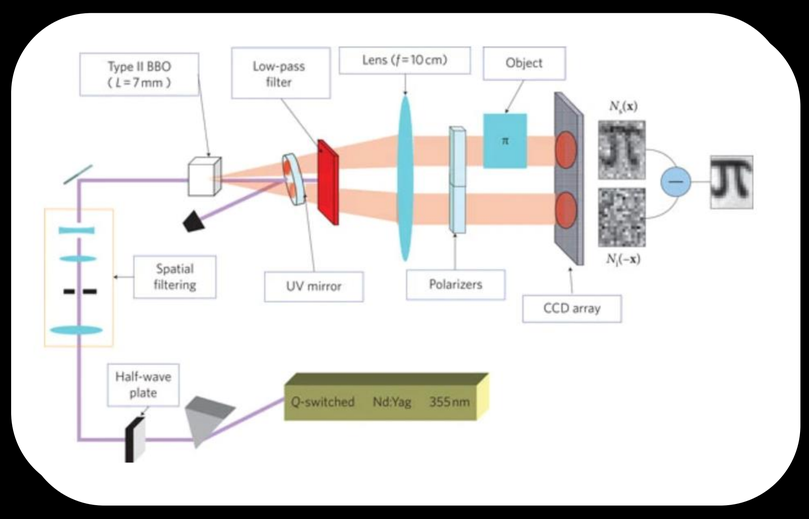
La **metrologia quantistica** sfrutta i comportamenti quantistici di luce e materia per migliorare gli apparati e le strategie di misura, rendendoli più precisi ed accurati rispetto a quelli basati sulle proprietà classiche. Tra le proprietà quantistiche, viene sfruttato anche l'entanglement.



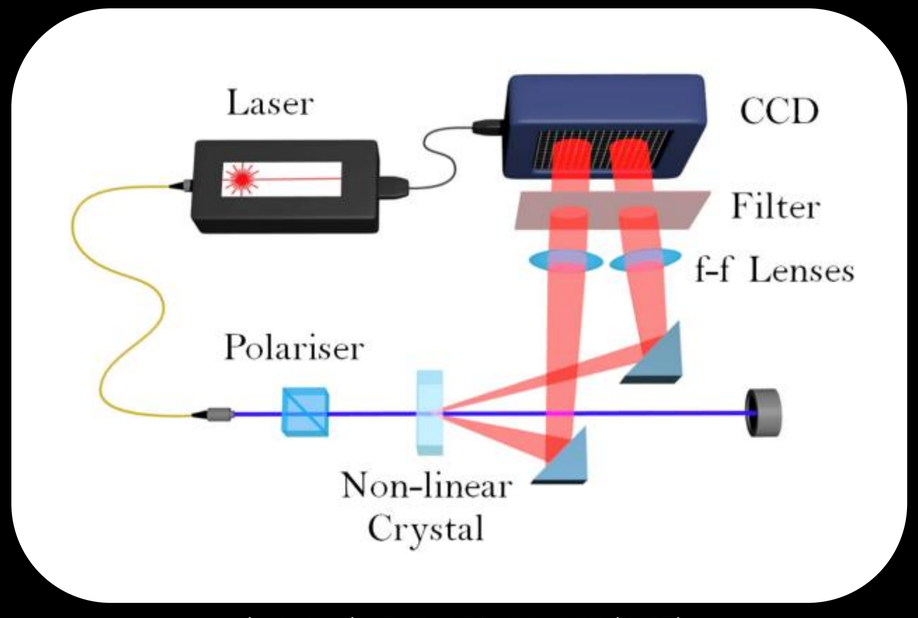
Crediti a University of Copenhagen

Imaging quantistico

L'entanglement è particolarmente utile per il miglioramento delle tecniche di **imaging**, tra cui la ricostruzione ottimale di immagini di campioni, ad esempio biologici o chimici, fotolabili e degradabili. L'uso di luce entangled permette di ottenere immagini con un contrasto maggiore rispetto a quelle ottenute con luce classica.



Adattato da *Nature Photon.* **4,** 227-230 (2010)



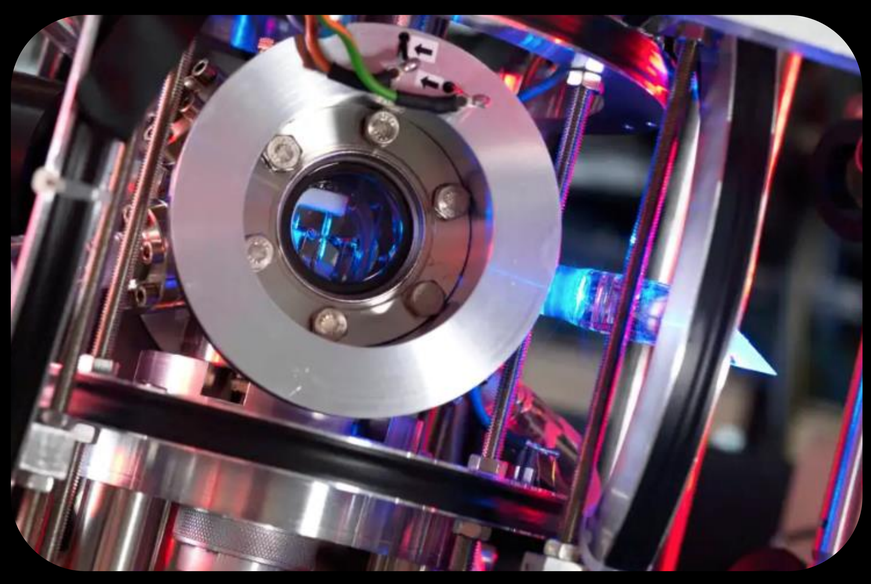
Adattato da *J. Opt.* **19,** 094002 (2017)

Calibrazione assoluta dei rivelatori

Le correlazioni esibite da stati entangled della luce possono essere sfruttate anche nella cosiddetta **radiometria quantistica**, che consiste nella possibilità di calibrare in maniera assoluta rivelatori in grado di contare i fotoni in diversi regimi di intensità con un singolo apparato sperimentale.

Sincronizzazione degli orologi atomici

L'entanglement è stato anche sfruttato di recente per la sincronizzazione di due orologi atomici, che attualmente rappresentano i campioni per la misura del tempo e la definizione del secondo. Questo permetterà di eseguire misure più accurate nell'ambito della ricerca cosmologica, per esempio sarà utile per lo studio della materia oscura e della gravità.



Crediti a New Scientist.com

DIRE L'INDICIBILE
l'entanglement quantistico

ITALIAN QUANTUM WEEKS

QUANTUM TIQ-TAQ-TOE
By Evert van Nieuwenburg

GET IT ON Google Play

Download on the App Store

Gioca **online**

https://quantumtictactoe.com/play

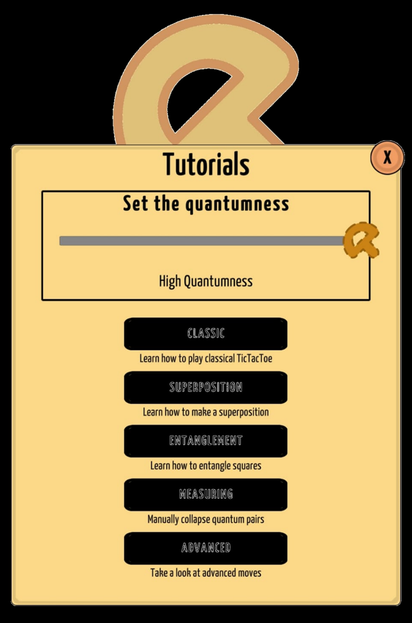
Oppure **scarica l'app** inquadrando il QR code!

Cosa è il Tiq Taq Toe quantistico?

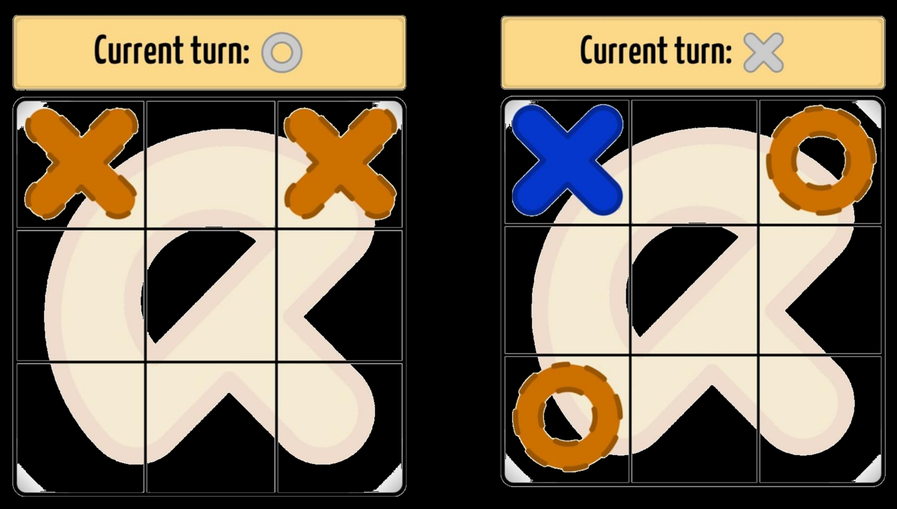
Il TiqTaqToe quantistico è molto simile **al gioco del Tris classico**. Ogni partita dura meno di un minuto!
Due giocatori si alternano e scelgono le caselle su cui mettere il proprio simbolo. Tre simboli X in fila (o in colonna o in diagonale) fanno vincere quel giocatore.

Per cominciare, provate il gioco classico tenendo il cursore della "Quantumness" tutto a sinistra (No Quantum)

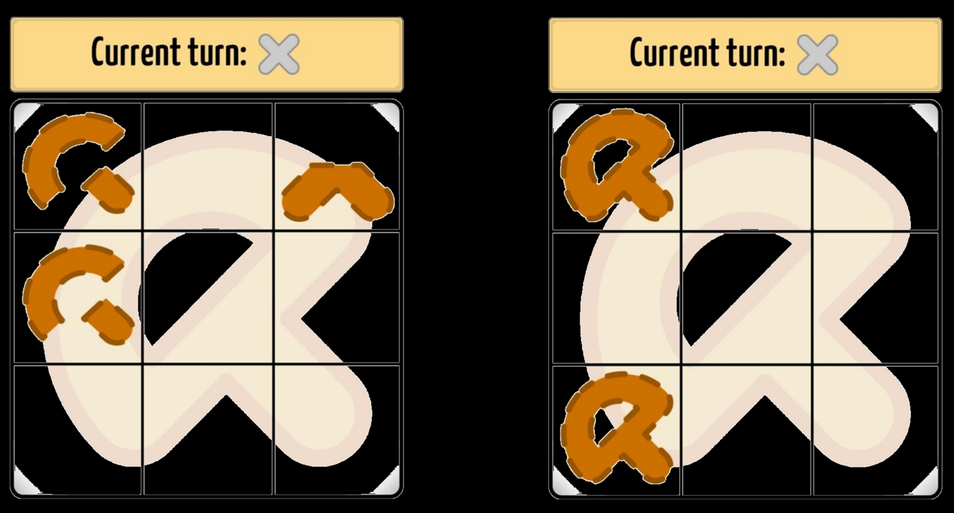
Come si gioca?



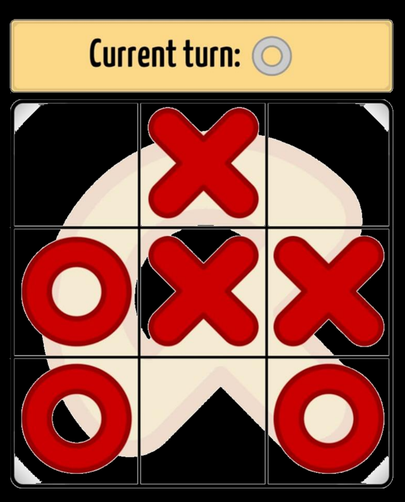
Imposta il cursore della "**Quantumness" tutto a destra nelle impostazioni**: questo sbloccherà tutte le possibili mosse quantistiche!



Per giocare la tua prima mossa quantistica, trascina il tuo dito da una casella vuota a un'altra. Ora la griglia è in uno stato di **sovrapposizione quantistica.** Anche il tuo avversario può creare una sovrapposizione quantistica trascinando il proprio dito fra due caselle vuote



Per creare **Entanglement** fra te e il tuo avversario, trascina il dito fra una casella vuota e una occupata dal simbolo del tuo avversario, oppure fra una casella vuota e una in cui il tuo avversario ha creato una sovrapposizione



Quando la griglia è piena, verrà automaticamente fatta una **misura quantistica**, che renderà ogni casella classicamente vuota o occupata.
Il gioco può continuare, fino a che la griglia non si riempie di simboli classici...
...e viene eletto **il vincitore!**