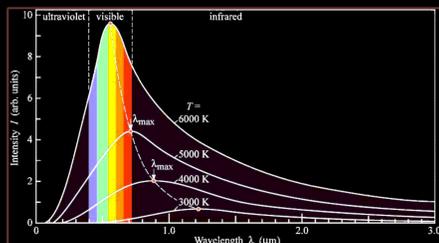


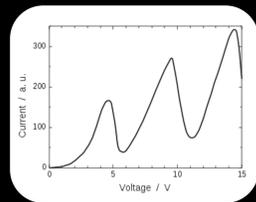
VIAGGIO NELLA MECCANICA QUANTISTICA

dai primi esperimenti alla teoria

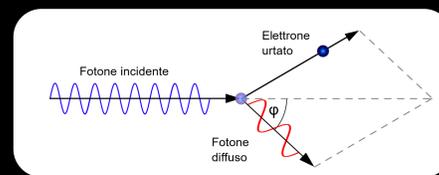


Max Planck
Spettro di emissione del corpo nero
1900

Geoffrey Ingram Taylor
Interferenza a singolo fotone
1909



James Franck e Gustav L. Hertz
Quantizzazione dei livelli atomici
1914



Arthur Compton
Scattering fotone-elettrone
1923

Wolfgang Pauli
Principio di esclusione di Pauli

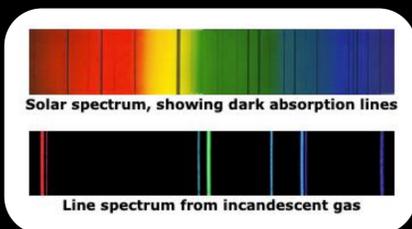
$$\Delta x \Delta p \geq \frac{\hbar}{2}$$

Werner Heisenberg, Max Born e Pascual Jordan
Formulazione matriciale della Meccanica Quantistica
1925

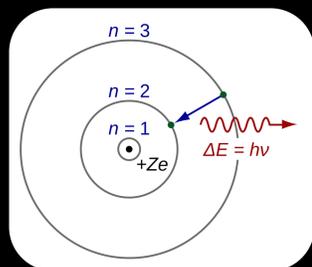
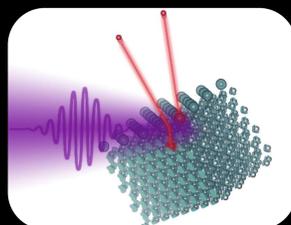
Werner Heisenberg
Principio di indeterminazione
Davisson e Germer
Diffrazione di elettroni
1927



1885
Johann Balmer
Spettro a righe dell'idrogeno

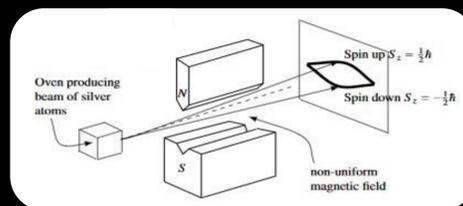


1905
Albert Einstein
Effetto fotoelettrico



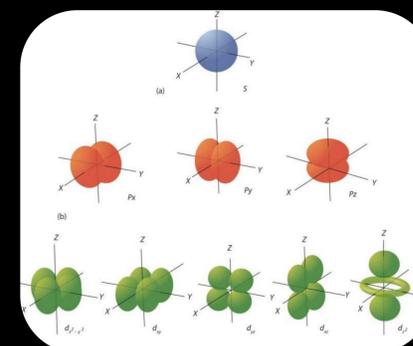
1913
Niels Bohr
Modello atomico

1922
Otto Stern and Walther Gerlach
Misura dello spin dell'elettrone



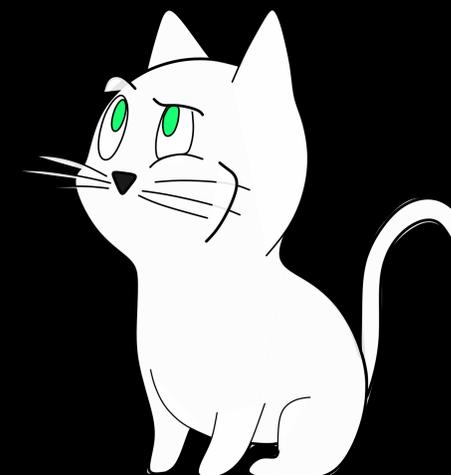
1924
Satyendranath Bose
Statistica di Bose-Einstein
Louis De Broglie
Lunghezza d'onda dell'elettrone

$$\lambda = \frac{h}{p}$$



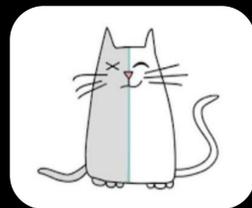
1926
Erwin Schrödinger
Equazione di Schrödinger

$$i\hbar \frac{\partial \Psi}{\partial t} = \hat{H} \Psi$$

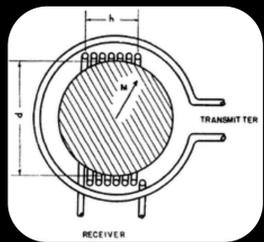


VIAGGIO NELLA MECCANICA QUANTISTICA

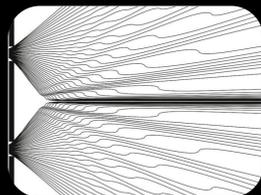
la prima rivoluzione quantistica



John Bardeen, Walter Brattain e William Shockley
Prima tipologia di transistor
1947



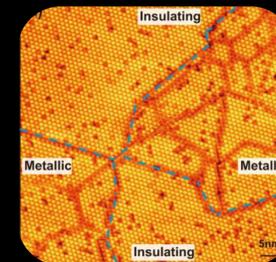
Felix Bloch ed Edward M. Purcell
Risonanza magnetica nucleare
1951



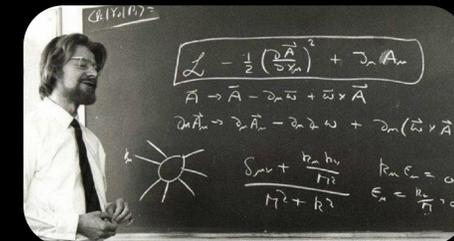
David Bohm
Meccanica Bohmiana
1952



Hugh Everett
Interpretazione a molti mondi della Meccanica Quantistica
1957



Philip W. Anderson e Nevill F. Mott
Teoria del magnetismo
1954-1961



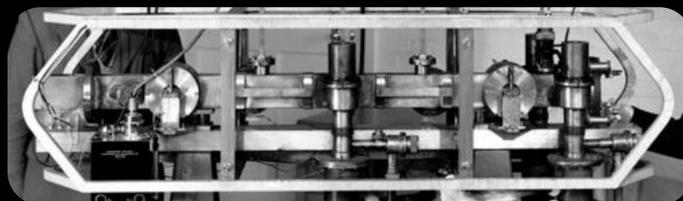
John S. Bell
Disuguaglianze di Bell
1964



1935
Erwin Schrödinger
Paradosso del gatto di Schrödinger
Albert Einstein, Boris Podolski and Nathan Rosen
Paradosso EPR

$$\langle x_t | e^{-i\hat{H}t/\hbar} | x_0 \rangle =$$

1948
Richard Feynman
Integrali di cammino in Meccanica Quantistica



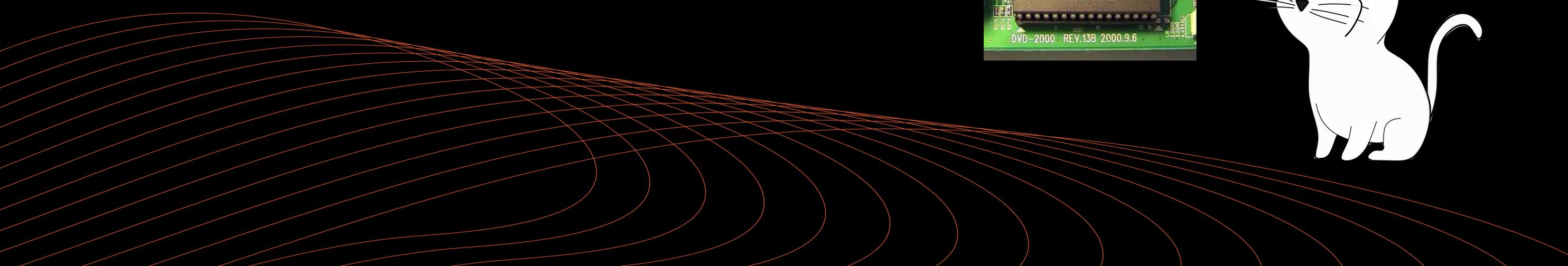
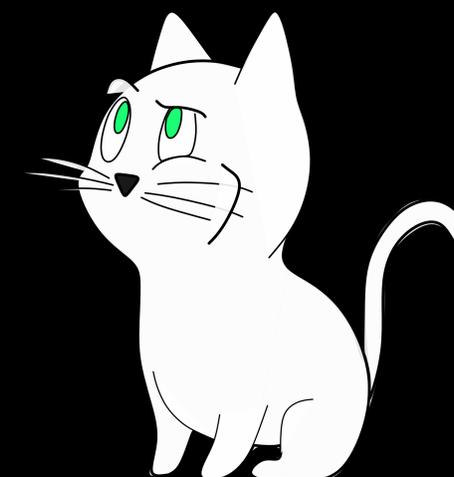
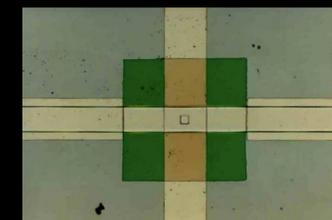
1953
Charles H. Townes
Primo maser ad ammoniac

1955
Atomichron
Primo orologio atomico commerciale

1958
John Bardeen, Leon Cooper e Robert Schrieffer
Teoria della superconduttività
Leo Esaki
Effetto tunnel nei diodi a semiconduttore

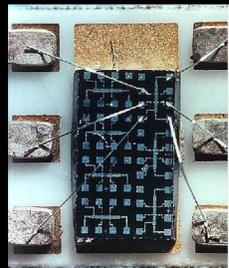


1962
Brian Josephson
Giunzione Josephson



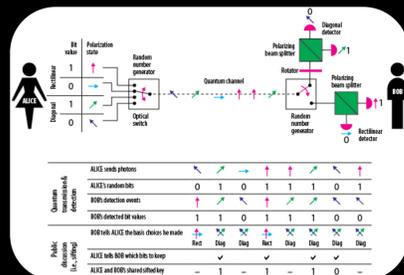
VIAGGIO NELLA MECCANICA QUANTISTICA

la seconda rivoluzione quantistica



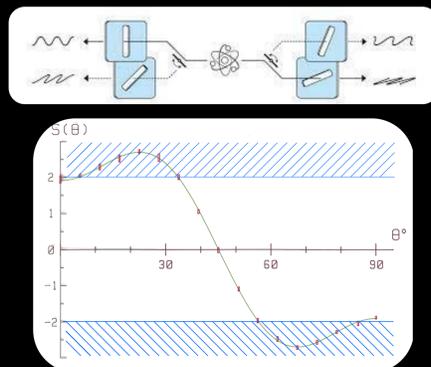
Klaus von Klitzing
Effetto Hall Quantistico
1980

Richard Feynman
Simulazioni quantistiche
1981



Charles Bennett e Gilles Brassard
Protocollo crittografico BB84
1984

Alain Aspect
Violazione sperimentale delle disuguaglianze di Bell

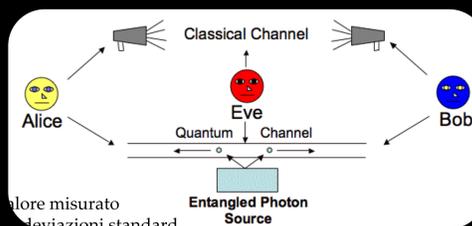


1980-93
Moungi G. Bawendi, Louis E. Brus e Alexei I. Ekimov
Quantum dots (punti quantici)

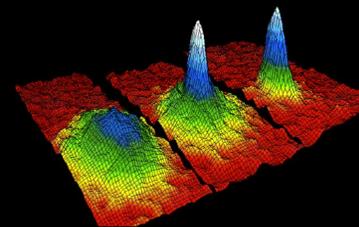


Charles Bennett, Gilles Brassard, Claude Crepeau, Richard Jozsa, Asher Peres, William Wootters
Prima proposta teorica di teletrasporto quantistico
1993

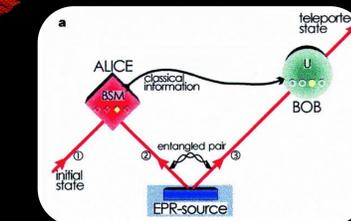
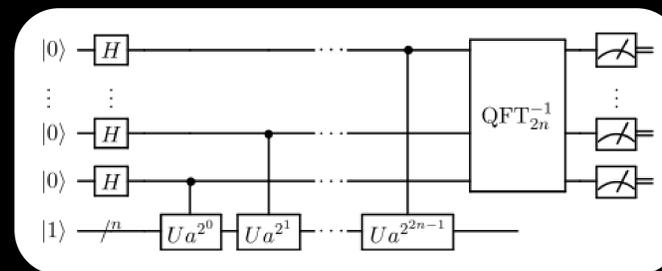
Artur Ekert
Protocollo crittografico E91



Eric Cornell, Wolfgang Ketterle, Carl Wieman
Condensati di Bose
1995



1994
Peter Shor
Algoritmo di fattorizzazione



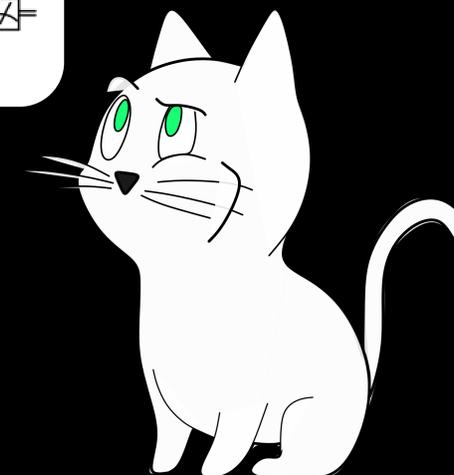
Anton Zeilinger e Sandu Popescu
Prima realizzazione sperimentale del teletrasporto quantistico
1997

1996
Lov Grover
Algoritmo quantistico di ricerca

Quantum Manifesto
IBM-Quantum experience
2016

D-Wave
2011

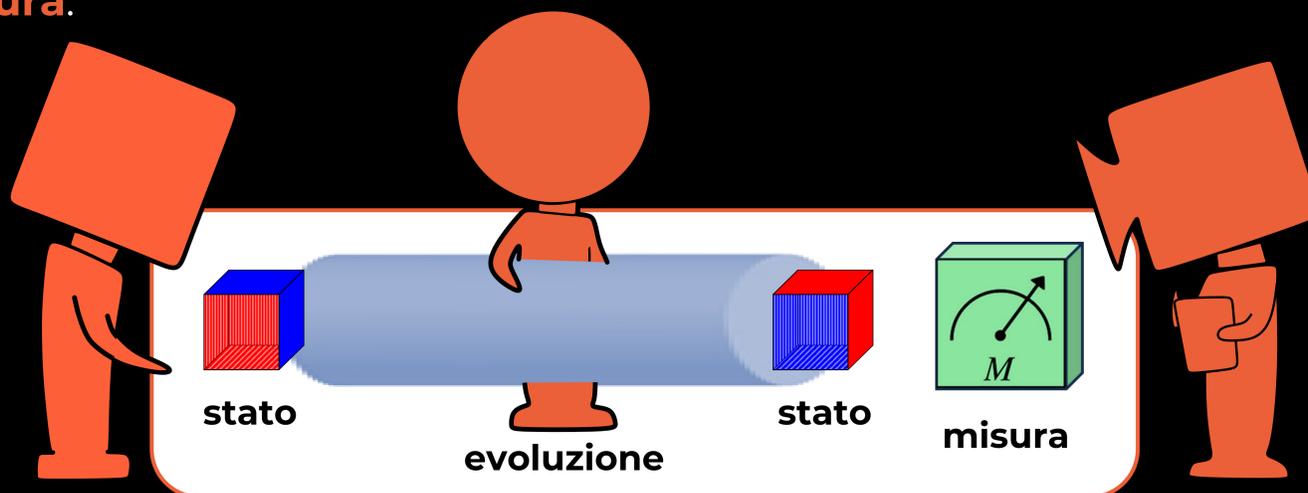
2022
John Clauser, Alain Aspect e Anton Zeilinger
Premio Nobel per i lavori pionieristici sulle tecnologie quantistiche



LE REGOLE DEL GIOCO

assiomi della meccanica quantistica

La teoria quantistica descrive le **proprietà** di un sistema fisico (**stato**), la loro **evoluzione** e la loro **misura**.

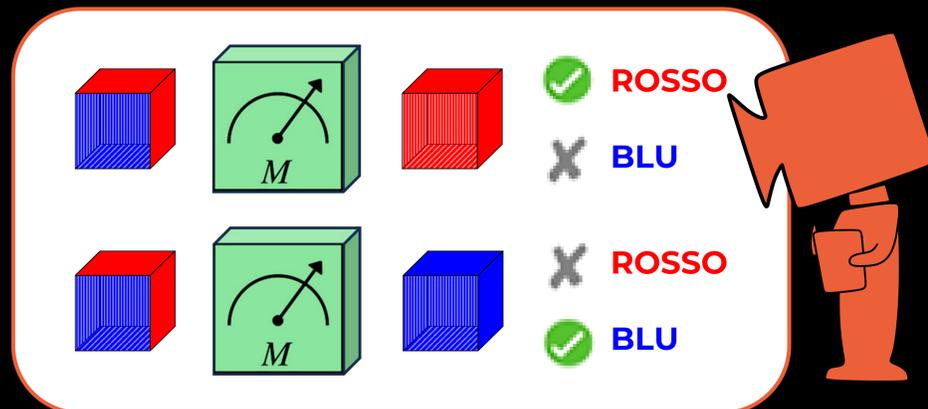


STATO DI UN SISTEMA

In un mondo con soli due colori, $|R\rangle$ e $|B\rangle$, lo stato di colore $|C\rangle$ di un oggetto è dato da una combinazione (**sovrapposizione**)
 $|C\rangle = c_R |R\rangle + c_B |B\rangle$ con $|c_R|^2 + |c_B|^2 = 1$

$|C\rangle = \sqrt{\frac{1}{3}} |R\rangle + \sqrt{\frac{2}{3}} |B\rangle$

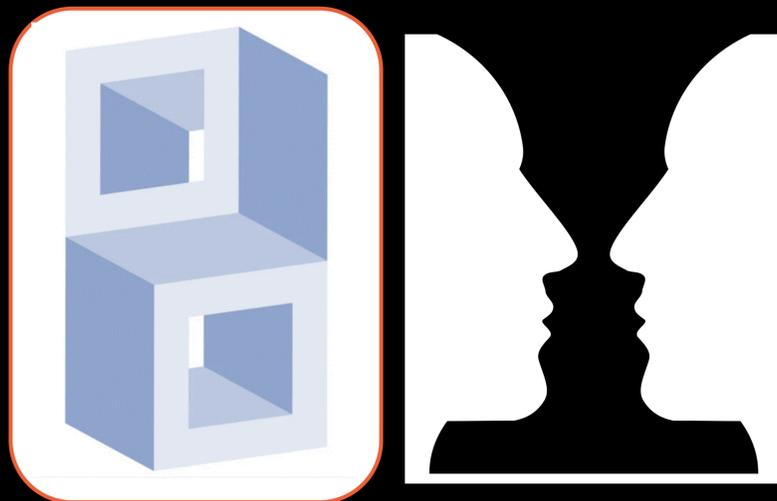
MISURA



- La misura di colore ha come risultato solo rosso o solo blu.
- Il risultato della singola misura è **imprevedibile**.
- La probabilità di misurare rosso è $p_R = |c_R|^2$ e quella di misurare blu è $p_B = |c_B|^2$.
- Dopo la misura lo stato è rosso o blu (regola di Born)

Quando si osserva un'immagine bistabile si percepisce solo una delle due immagini che coesistono in una specie di **stato di sovrapposizione**.

L'**osservazione** ha un ruolo cruciale: lo stato di sovrapposizione collassa in uno dei due stati quando viene osservato.



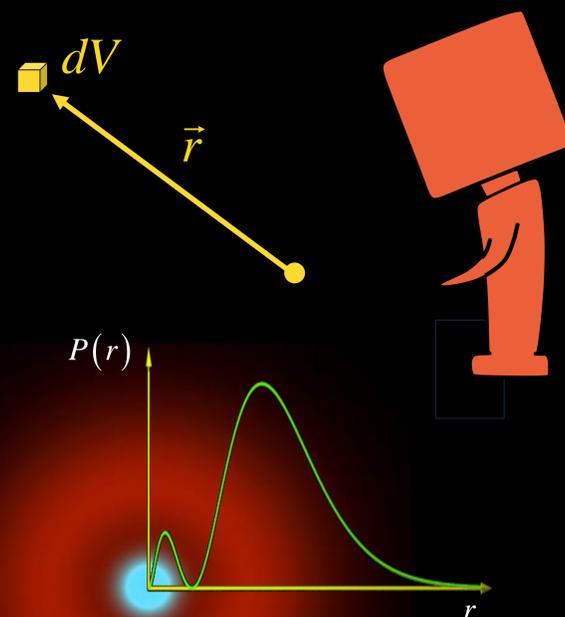
Lo stato di un elettrone in un sistema fisico è descritto dalla sua funzione d'onda, che associa ad ogni punto dello spazio un valore numerico (complesso). Il modulo al quadrato di questo valore fornisce la **probabilità di misurare l'elettrone** in quel punto.

$$P(\vec{r}, t) dV = |\Psi(\vec{r}, t)|^2 dV$$

ATOMO DI IDROGENO

In un atomo di idrogeno l'elettrone è legato al protone del nucleo dall'interazione di Coulomb. Si trova quindi in una regione di spazio attorno al nucleo stesso.

La funzione d'onda che descrive il suo stato è chiamata **orbitale**. A ciascun orbitale è associata un'energia ben definita e un valore più probabile della distanza dal nucleo.



Orbitale 2s

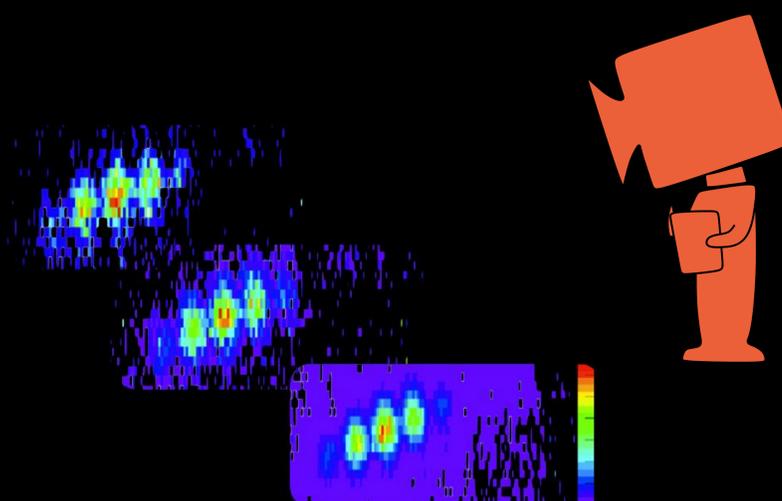
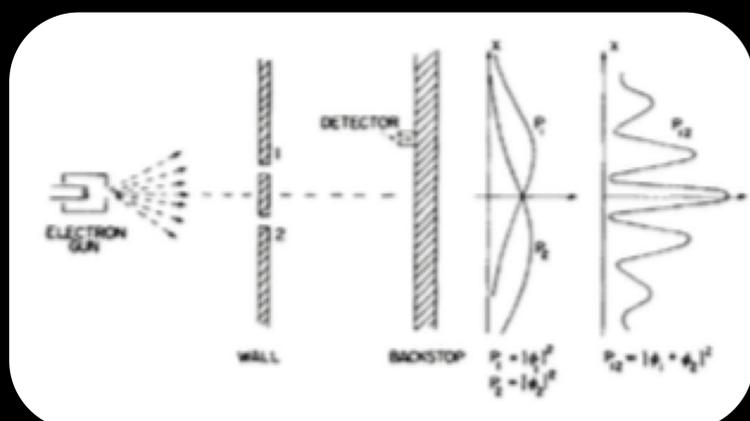
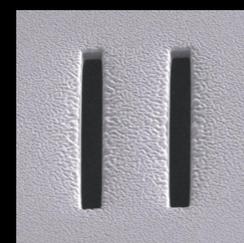
ESPERIMENTO DI FEYNMAN

Un fascio di elettroni viene mandato su una doppia fenditura.

Lo stato di ogni elettrone dopo le fenditure è descritto da una **sovrapposizione di due stati**:

$$\psi_{12}(r) = \psi_1(r) + \psi_2(r)$$

Dove $\psi_1(r)$ descrive il passaggio solo dalla prima fenditura e $\psi_2(r)$ quello solo dalla seconda.



La probabilità di misurare l'elettrone in ogni punto di uno schermo $p(r) = |\psi_{12}(r)|^2$ mostra i massimi e i minimi tipici di una figura di **interferenza**.

PROPRIETÀ INCOMPATIBILI

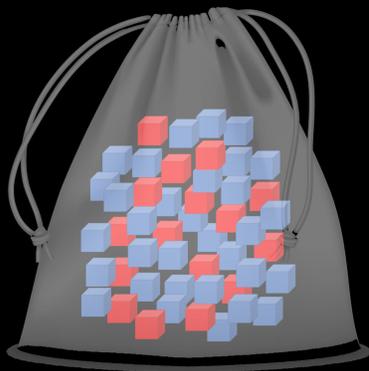
indeterminazione quantistica

”La sovrapposizione che si verifica nella meccanica quantistica è di natura essenzialmente diversa da quella che si verifica nella teoria classica”.

P.A.M. Dirac

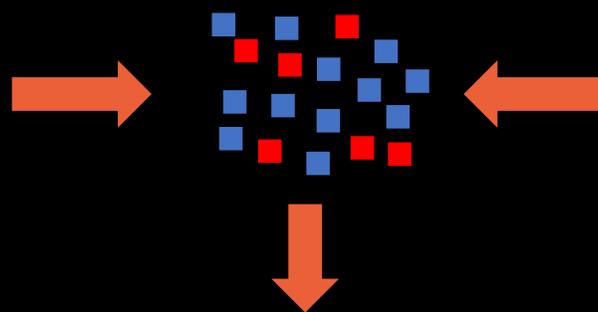
STATO MISTO

Il sacchetto contiene cubetti completamente rossi **e** blu.



CLASSICO

Misuriamo il **colore** osservando la faccia superiore del cubetto **senza poter osservare le altre.**



STATO DI SOVRAPPOSIZIONE

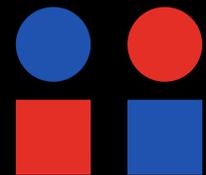
Il sacchetto contiene cubetti con facce rosse **e** blu.



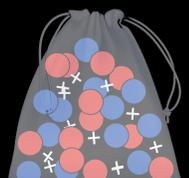
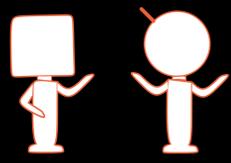
QUANTISTICO

La misura non distingue gli stati misti dagli stati di sovrapposizione: occorre misurare due **proprietà** diverse **incompatibili** fra loro.

Prendiamo un sacchetto pieno di gettoni che possono avere solo due colori (**rosso** o **blu**) e due forme (tonda o quadrata).



0. Alice e Bob preparano un sacchetto con i vari gettoni di colore e forma diversi

	ESPERIMENTO "CLASSICO"	ESPERIMENTO "QUANTISTICO"	
1. Alice seleziona solo i gettoni rossi 			...la misura quantistica modifica lo stato dei gettoni, che saranno rossi ma in uno stato di sovrapposizione di forme diverse .
2. Bob seleziona solo i gettoni tondi 			...avendo misurato una proprietà incompatibile, ora i gettoni saranno in un nuovo stato: tondi ma in sovrapposizione di colori diversi .
3. Alice misura di nuovo il colore dei gettoni 	I gettoni saranno comunque tutti rossi .	Alice troverà metà delle volte gettoni di colore blu e metà delle volte di colore rosso . 	

Alice può distinguere uno stato classico misto da uno di sovrapposizione quantistica!

MISURE INCOMPATIBILI

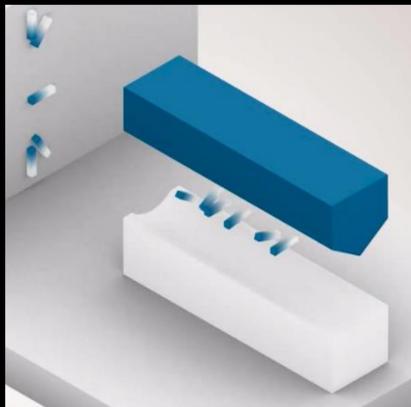
lo spin e l'esperimento di Stern-Gerlach

FASCIO DI CALAMITE

1. Generiamo un **campo magnetico non uniforme**



2. Mandiamo un fascio di **calamite** attraverso il campo magnetico



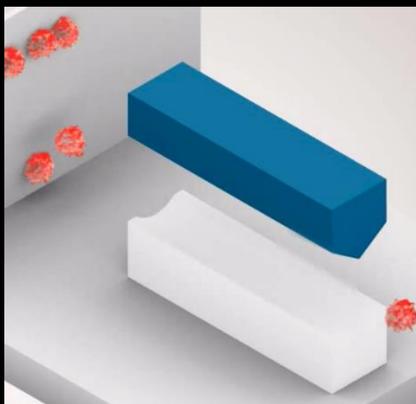
3. Osserviamo che il fascio si sparpaglia



ogni calamita è deviata a seconda della sua orientazione iniziale

Una calamita è descritta dal vettore momento magnetico $\vec{\mu}$, diretto dal polo SUD al polo NORD. La posizione sullo schermo dipende dalla componente lungo z di questo vettore μ_z .

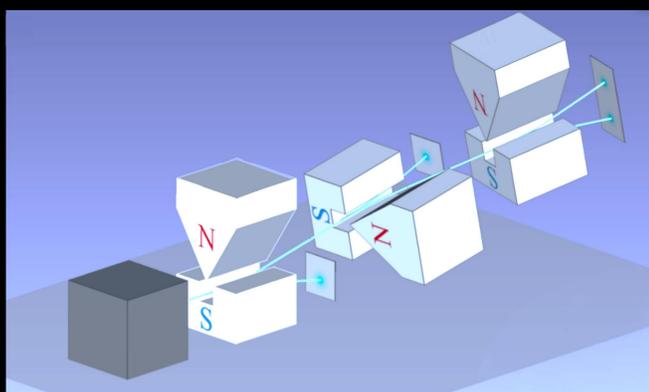
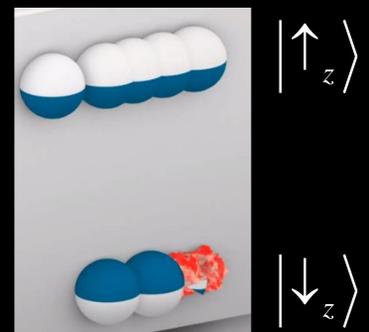
FASCIO DI ELETTRONI



Il fascio non si sparpaglia ma si divide in due!

Il risultato si spiega con lo **spin** \vec{s} , una **proprietà puramente quantistica** dell'elettrone.

Il momento magnetico dell'elettrone è $\vec{\mu} = \frac{e}{mc} \vec{s}$
La componente dello spin in un campo magnetico può avere solo i due valori $\pm \hbar/2$



Consideriamo una serie di **tre magneti Stern-Gerlach**:

- il primo è orientato **lungo z** e divide il fascio in due
- selezioniamo gli elettroni nello stato $|\uparrow_z\rangle$ e li mandiamo nel secondo magnete orientato **lungo x**
- il fascio si divide nuovamente in due
- selezioniamo lo stato $|\uparrow_x\rangle$ e lo inviamo nel terzo magnete orientato **lungo z**
- all'uscita del terzo magnete troviamo ancora due fasci mentre ci aspetteremmo solo $|\uparrow_z\rangle$!

Le misure dello spin lungo x e lungo z sono **incompatibili!**

Il risultato dipende dall'ordine delle misure che non **non commutano!**

➔ Gli stati lungo x sono **sovrapposizione** degli stati lungo z:

$$|\uparrow_x\rangle = \frac{|\uparrow_z\rangle + |\downarrow_z\rangle}{\sqrt{2}}$$

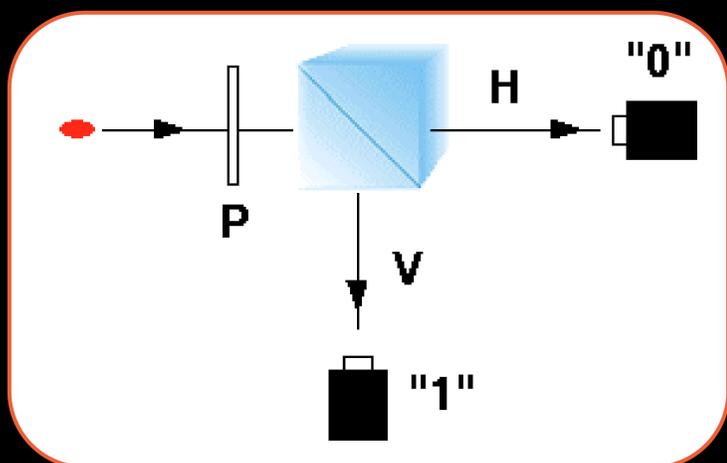
NUMERI CASUALI

Non esiste condizione sufficiente per stabilire la casualità di una sequenza di numeri ma esistono proprietà statistiche specifiche che forniscono criteri necessari.

- Si possono generare sequenze **pseudo-casuali** usando algoritmi matematici complessi a partire da un seed.
- Si possono generare sequenze **genuinamente casuali** usando processi fisici come il lancio di una moneta o di un dado, l'estrazione di un numero del lotto...
- Tuttavia la fisica classica non consente una perfetta casualità perché l'esito di un processo fisico classico è noto se sono note le condizioni iniziali.



CASUALITÀ QUANTISTICA



- Per gli assiomi della meccanica quantistica, una misura su uno stato di sovrapposizione fornisce esiti **intrinsecamente casuali**.
- Un generatore quantistico di numeri random deve mantenere la coerenza della sovrapposizione quantistica degli stati.
- Esempi di sistemi quantistici
 - Decadimenti nucleari
 - Misura di un singolo fotone dopo un beam splitter
 - Misura di un singolo fotone polarizzato a 45° dopo un beam splitter polarizzatore
 - tempi di arrivo dei fotoni emessi da singoli atomi o singole molecole.

Molte applicazioni hanno bisogno di bit casuali per il loro funzionamento

- **Macchine per giochi d'azzardo equi**: slot machines, poker online, bingo, roulette
 - **Calcolo**: realizzazione del calcolatore universale, ottimizzazione di algoritmi
 - **Crittografia classica**: chiavi una tantum, crittografia a chiave pubblica
 - **Simulazioni**: Metodo Monte Carlo, Algoritmo di Metropolis, Random walk



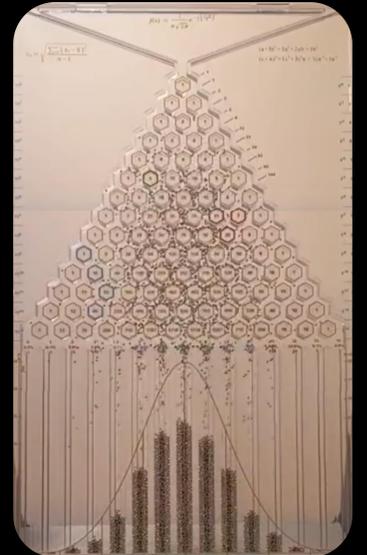
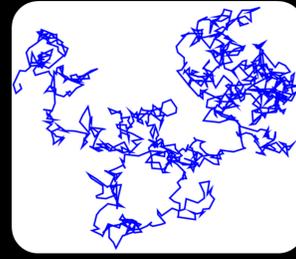
RANDOM WALK

passeggiata quantistica

EVOLUZIONE CASUALE

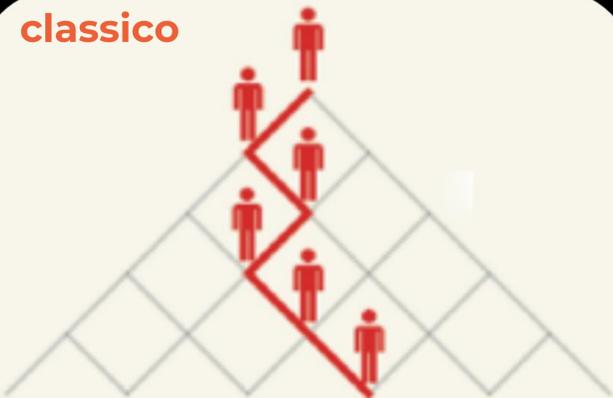
Quando una particella diffonde in un fluido si muove a zig-zag cambiando direzione ad ogni passo. Il modello è quello del **random walk**, o **cammini casuali**:

- Per una **particella classica** la direzione è decisa a caso, dal lancio di una moneta.
- Muovendosi a caso, la particella rimane a lungo vicino al punto di partenza: la diffusione è un processo lento.



Random walk sulla retta

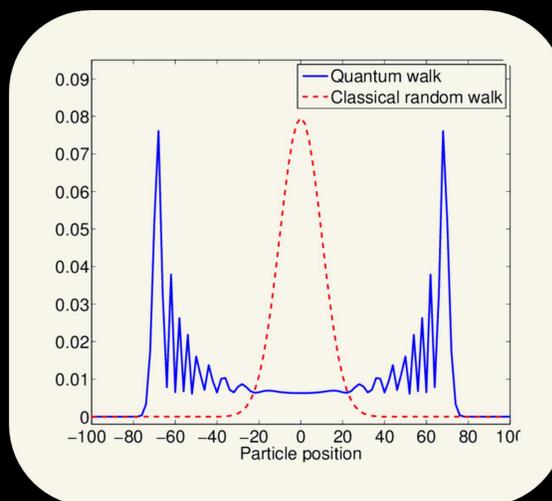
classico



quantistico



- Per una **particella quantistica**, si usa una **moneta quantistica**, in uno stato di **sovrapposizione**.
- Lo stato della particella è una sovrapposizione di tutte le posizioni possibili e questo genera **interferenza quantistica**.
- La particella quantistica si allontana più velocemente di quella classica.



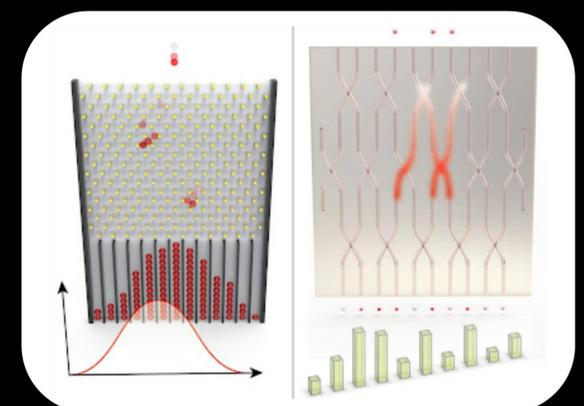
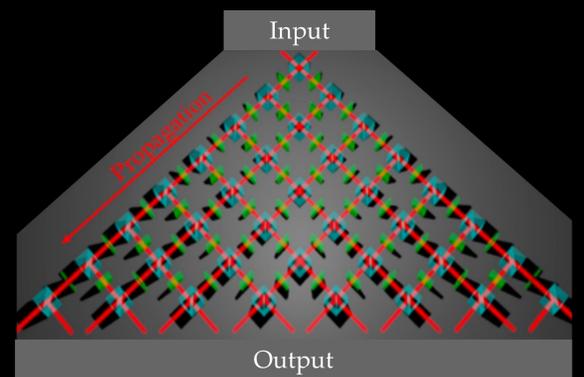
Esperimenti in sistemi di ioni, singoli atomi e **fotoni** in fibra e in guida d'onda.

Il random walk quantistico ha applicazioni nell'ottimizzazione di algoritmi e simulazioni.

Un apparato di **boson sampling** fotonico ha dimostrato la risoluzione del problema in modo più efficiente di un computer classico:

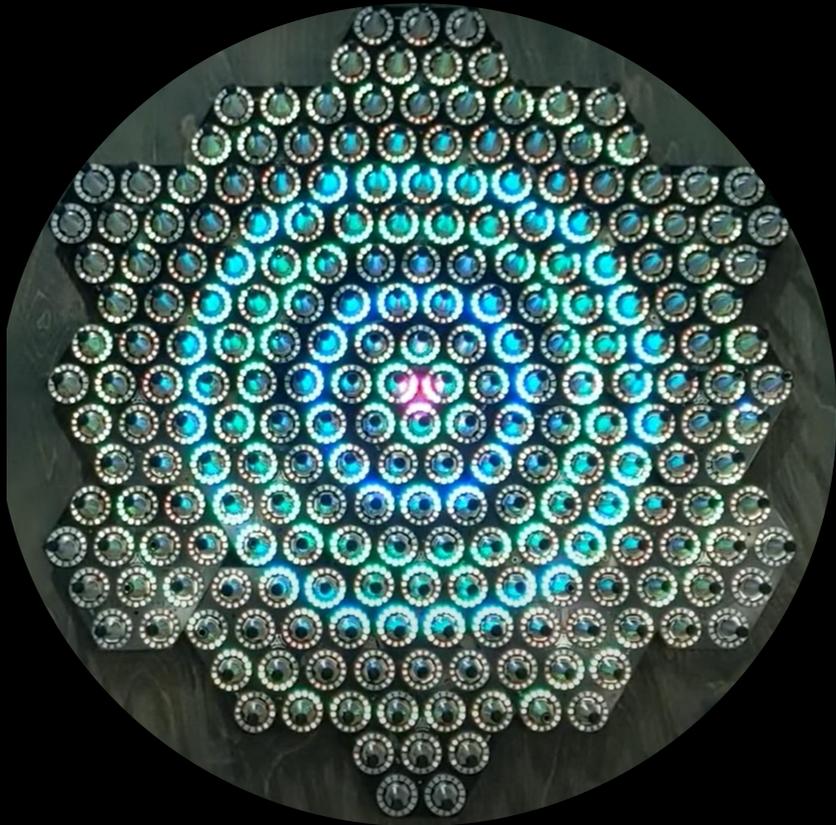


vantaggio quantistico!



QUANTUM GARDEN

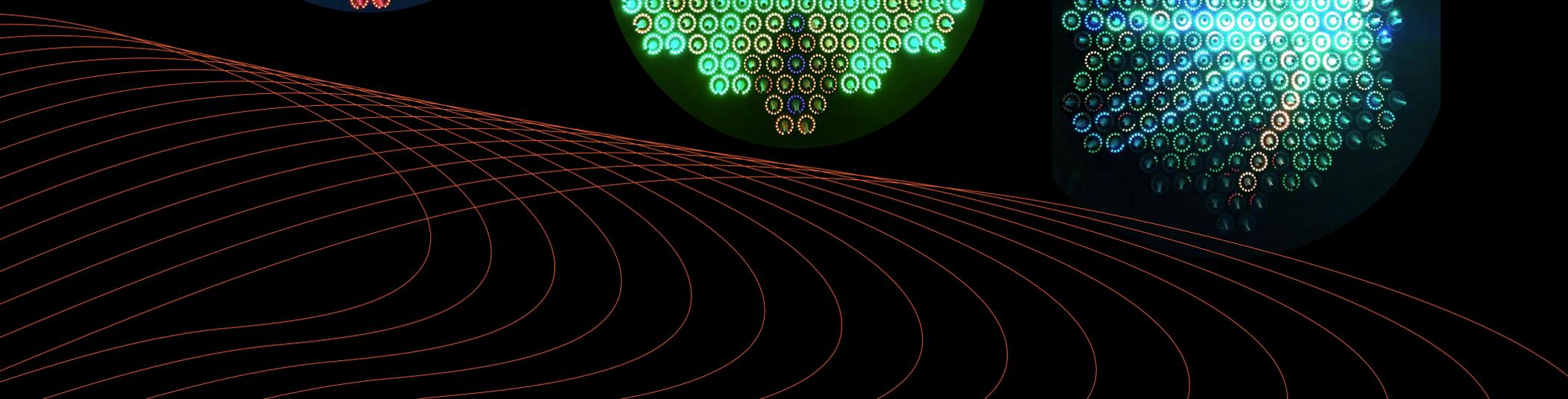
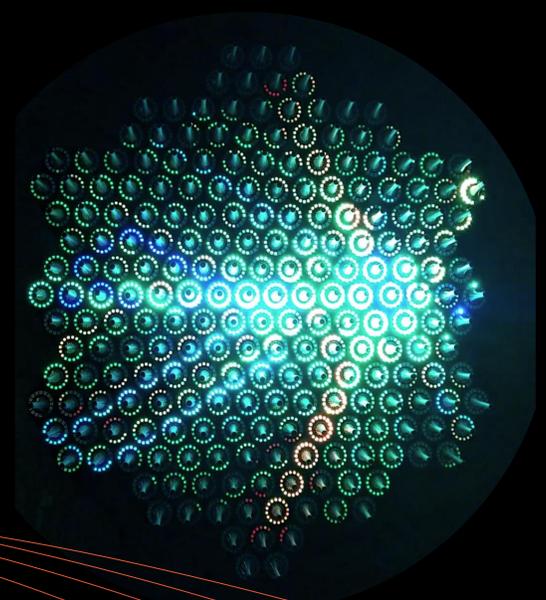
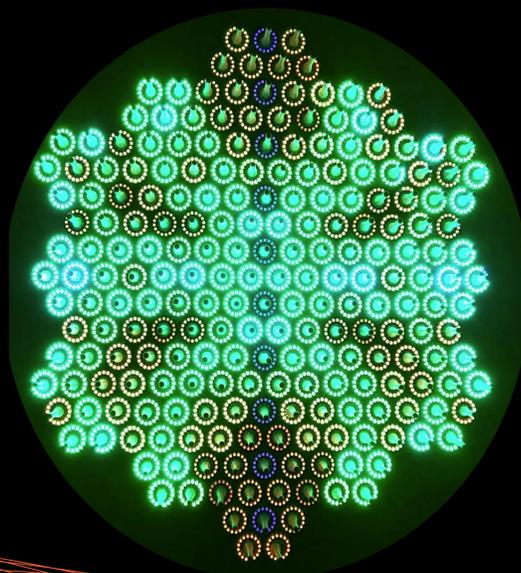
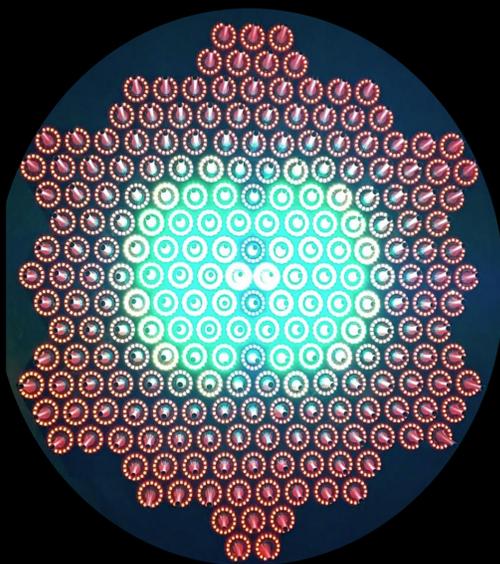
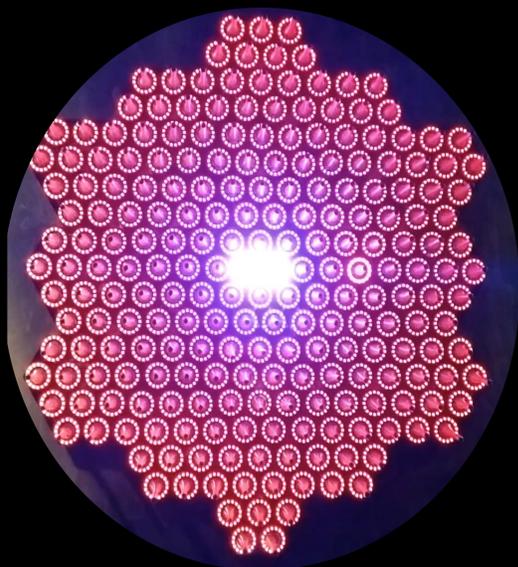
Robin Baumgarten



Quantum Garden è realizzato dal game artist **Robin Baumgarten** in collaborazione con un gruppo di fisici quantistici guidati dalla professoressa Sabrina Maniscalco (Università di Aalto e Università di Turku).

Quantum garden è un'installazione artistica interattiva che dimostra i concetti chiave della fisica quantistica, come la sovrapposizione quantistica, l'interferenza e l'equazione di Schrödinger.

- Toccando le molle si genera numericamente una particella in **sovrapposizione quantistica** di posizioni.
- La luminosità rappresenta la **probabilità di osservare** la particella in quel punto.
- La sovrapposizione quantistica iniziale evolve secondo l'equazione di Schrödinger che simula un **random walk** a tempo continuo su una rete quantistica.
- Toccando un punto del Garden si effettua una **osservazione della posizione** della particella che fa collassare la funzione d'onda in un punto qualunque, a seconda del valore della probabilità.



LE REGOLE DEL GIOCO

assiomi della meccanica quantistica

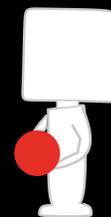
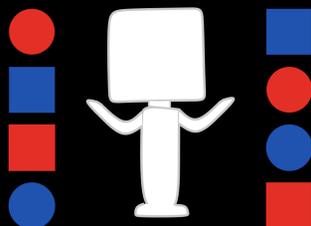
"Non chiamerei [l'entanglement] **uno** ma piuttosto **il** tratto caratteristico della meccanica quantistica, quello che rafforza tutto il suo allontanamento dalle linee di pensiero classiche."

E. Schrödinger

SISTEMI COMPOSTI

Classicamente, lo stato di un sistema composto da due sottosistemi si può scrivere come **prodotto** degli stati dei singoli stati $\psi_{1,2} = \psi_1\psi_2$ (**stato fattorizzabile**).

→ I due sottosistemi possono essere correlati classicamente e **soddisfano** le **disuguaglianze di Bell**.



$$S = \langle a_C b_C \rangle + \langle a_C b_F \rangle + \langle a_F b_C \rangle - \langle a_F b_F \rangle$$

$$-2 \leq S \leq 2$$

Quantisticamente, esistono anche stati **non fattorizzabili (entangled)** $\psi_{1,2} \neq \psi_1\psi_2$ che mostrano **correlazioni quantistiche**.

$$|\psi_{1,2}\rangle = \frac{1}{\sqrt{2}} (|0\rangle_1 |0\rangle_2 + |1\rangle_1 |1\rangle_2)$$

I due elettroni dell'atomo di Elio occupano l'orbitale più interno, con orientazione opposta dei loro spin (**Principio di esclusione di Pauli**)



1s



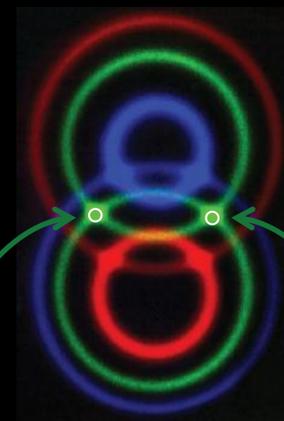
$$|\uparrow_z\rangle_1 |\downarrow_z\rangle_2$$

$$|\downarrow_z\rangle_1 |\uparrow_z\rangle_2$$

Siccome gli elettroni sono indistinguibili fra loro, lo **stato di spin** è la **sovrapposizione dei due possibili stati**.

$$|\psi_{1,2}\rangle = \frac{1}{\sqrt{2}} (|\uparrow_z\rangle_1 |\downarrow_z\rangle_2 - |\downarrow_z\rangle_1 |\uparrow_z\rangle_2)$$

Il processo non lineare di "down conversion di tipo II" produce **coppie di fotoni entangled** in polarizzazione all'intersezione fra l'anello superiore (polarizzato verticalmente) e l'anello inferiore (polarizzato orizzontalmente).



$$|\psi_{1,2}\rangle = \frac{1}{\sqrt{2}} (|H\rangle_1 |V\rangle_2 + |V\rangle_1 |H\rangle_2)$$

ENTANGLEMENT

correlazioni paradossali

IL GATTO DI SCHRÖDINGER

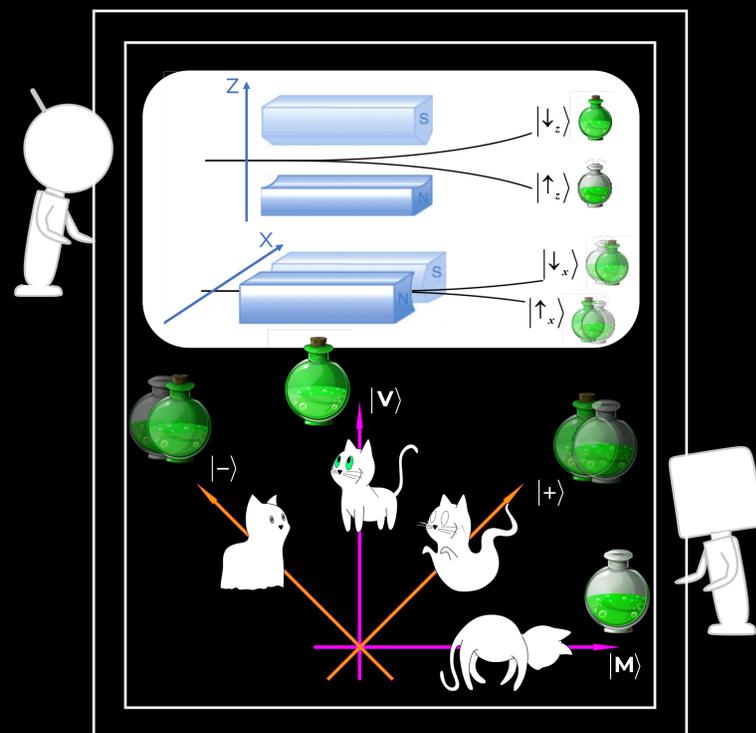
Nel 1935, Erwin Schrödinger descrisse un esperimento dalle conseguenze paradossali. Si considera uno **stato entangled** fra un sistema **macroscopico**, un gatto, e uno **microscopico** quantistico, ad esempio lo spin di un elettrone in uscita da un apparato di Stern-Gerlach.

- Lo stato dello spin può essere in uno stato di sovrapposizione

$$|\uparrow_x\rangle = \frac{|\uparrow_z\rangle + |\downarrow_z\rangle}{\sqrt{2}} \quad |\downarrow_x\rangle = \frac{|\uparrow_z\rangle - |\downarrow_z\rangle}{\sqrt{2}}$$

- quindi anche il gatto può essere in uno stato di sovrapposizione

$$|+\rangle = \frac{|\mathbf{V}\rangle + |\mathbf{M}\rangle}{\sqrt{2}} \quad |-\rangle = \frac{|\mathbf{V}\rangle - |\mathbf{M}\rangle}{\sqrt{2}}$$



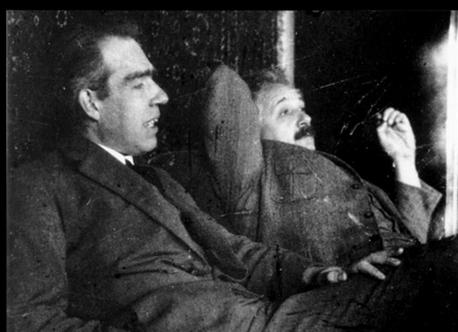
$$|\Psi_{e,G}\rangle = \frac{|\uparrow_z\rangle|\mathbf{V}\rangle + |\downarrow_z\rangle|\mathbf{M}\rangle}{\sqrt{2}} = \frac{|\uparrow_x\rangle|+\rangle + |\downarrow_x\rangle|-\rangle}{\sqrt{2}}$$

Poiché gli stati di sovrapposizione vivo/morto non sono osservabili (se apriamo la scatola troviamo sempre il gatto vivo o morto) l'entanglement di un sistema microscopico/macroscopico sembra paradossale!

I sistemi macroscopici, come i gatti, non permangono in stati di sovrapposizione a causa della **decoerenza** che li rende sistemi classici.

PARADOSSO EPR

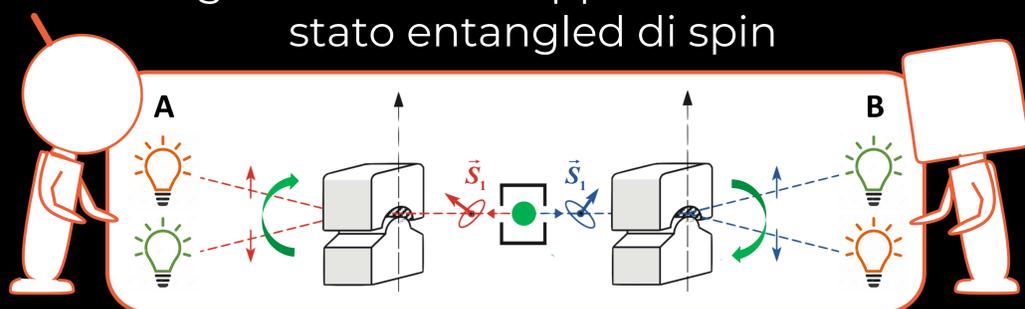
MAY 15, 1935 PHYSICAL REVIEW VOLUME 47
Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?
 A. EINSTEIN, B. PODOLSKY AND N. ROSEN, *Institute for Advanced Study, Princeton, New Jersey*
 (Received March 25, 1935)



Nel 1935 Einstein, Podolsky e Rosen (EPR) propongono un **esperimento mentale** (Gedankenexperiment) in cui mostrano che la meccanica quantistica è **incompleta** perché è in contraddizione con alcune ipotesi ragionevoli sulla realtà fisica: **realismo** e **località**.

SCHEMA ESPERIMENTO EPR

Una sorgente emette coppie di elettroni in uno stato entangled di spin

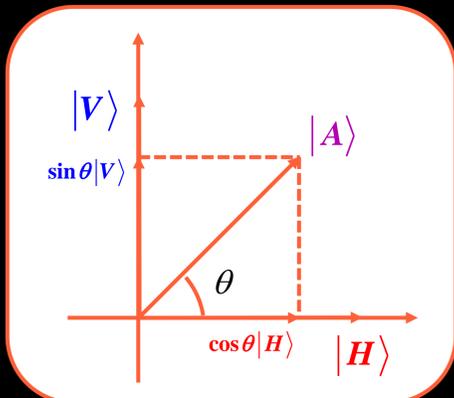
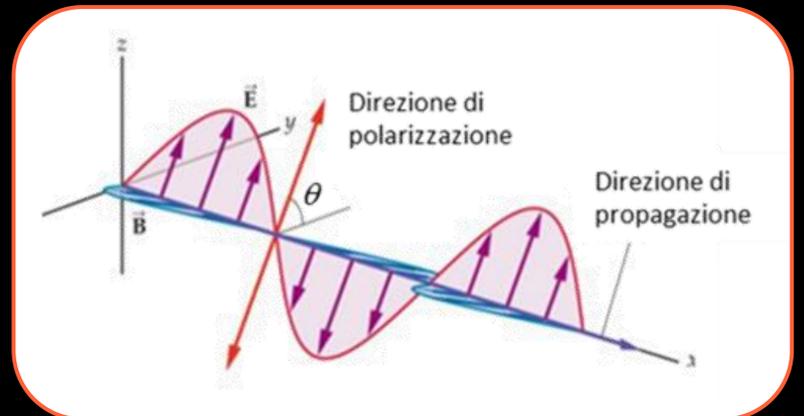


$$|\psi_{1,2}\rangle = \frac{1}{\sqrt{2}} (|\uparrow\rangle_1 |\downarrow\rangle_2 - |\downarrow\rangle_1 |\uparrow\rangle_2)$$

- Alice e Bob misurano lo spin in direzioni diverse che corrispondono a **proprietà incompatibili** per la meccanica quantistica
- Calcolando le correlazioni dei risultati delle misure si dimostra la **violazione** delle **disuguaglianze di Bell**.

ONDE ELETTROMAGNETICHE

La polarizzazione indica la direzione di oscillazione del campo elettrico di un'onda elettromagnetica. Se la polarizzazione è lineare, la direzione di oscillazione rimane fissata durante la propagazione dell'onda.



Un generico stato di polarizzazione lineare è descritto da un vettore $|A\rangle$ nel piano perpendicolare alla direzione di propagazione della luce:

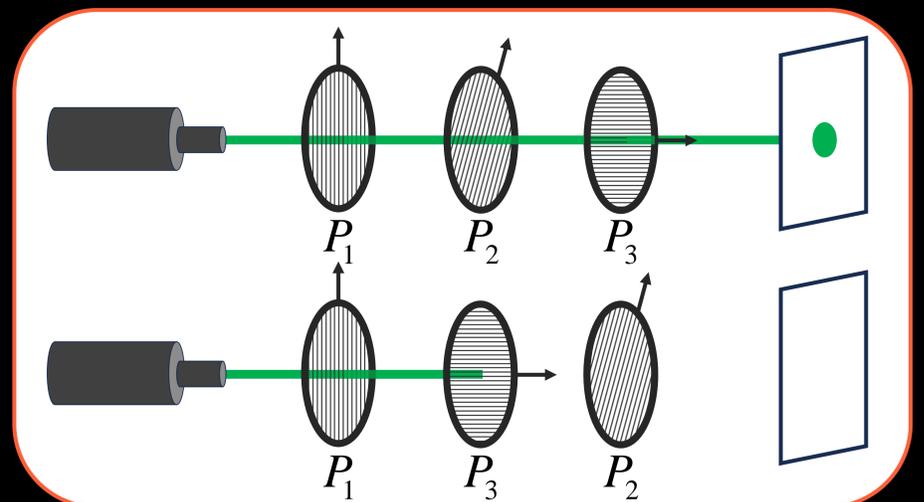
$$|A\rangle = \cos \theta |H\rangle + \sin \theta |V\rangle$$

POLARIZZATORI

Un **polarizzatore** è un elemento ottico che trasmette la componente dell'onda polarizzata in direzione del suo asse ottico e assorbe quella polarizzata ortogonalmente.

Il polarizzatore realizza una misura quantistica lungo una certa direzione.

Una sequenza di polarizzatori ad angoli diversi non commuta: scambiando l'ordine l'intensità cambia.



Se lo stato della luce è uno stato di Fock di **singolo fotone**, invece di parlare di intensità si parla di probabilità di misurare il singolo fotone.

Un fotone polarizzato ad un angolo θ rispetto all'asse del polarizzatore viene trasmesso con probabilità $\cos^2 \theta$.

Considerando N singoli fotoni incidenti, avremo $N_T = N \cos^2 \theta$ fotoni trasmessi, come prevede la **Legge di Malus**.

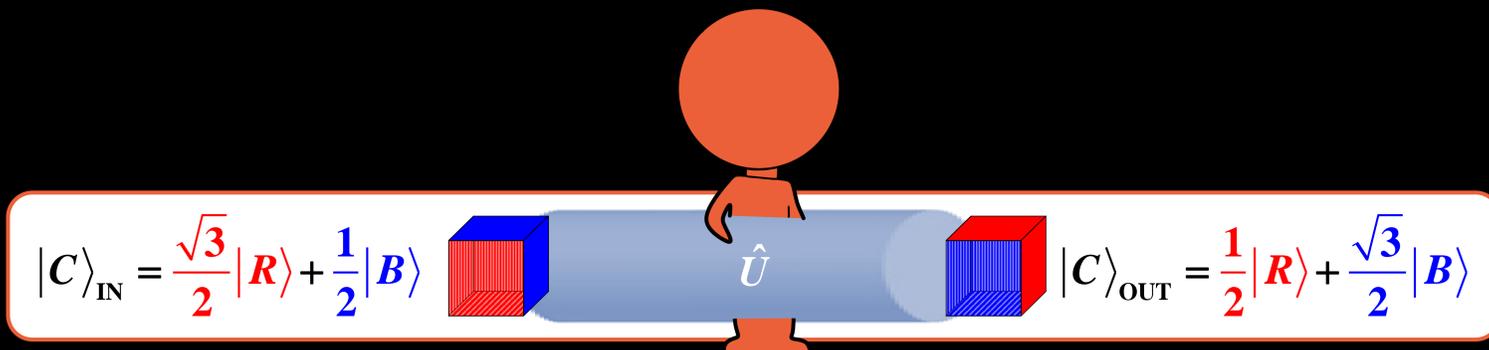


LE REGOLE DEL GIOCO

assiomi della meccanica quantistica

EVOLUZIONE

L'evoluzione temporale trasforma lo stato iniziale del sistema in un altro stato possibile.



Lo stato del sistema isolato evolve nel tempo in accordo con l'**equazione di Schrödinger**

$$i\hbar \frac{d}{dt} \psi = \hat{H} \psi$$

\hat{H} operatore Hamiltoniano legato all'energia del sistema
 \hbar costante di Planck ridotta

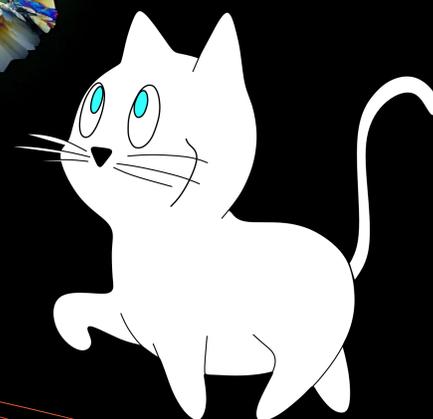
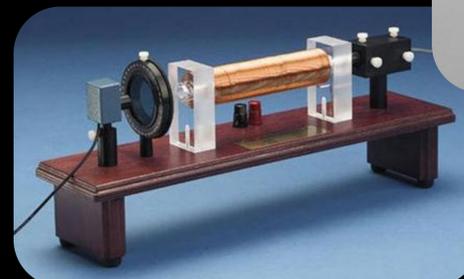
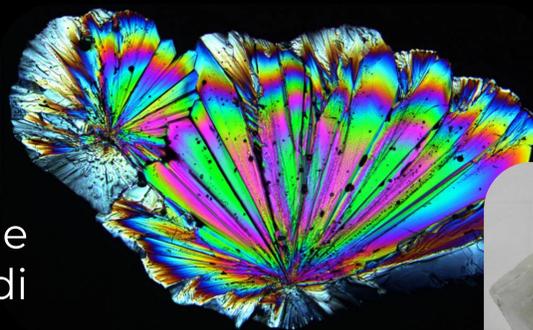
Simbolicamente possiamo anche scrivere

$$|C\rangle_{\text{OUT}} = \hat{U} |C\rangle_{\text{IN}}$$

\hat{U} è legato ad \hat{H}

EVOLUZIONE DELLA POLARIZZAZIONE

- **Attività ottica** dei materiali come le molecole chirali (glucosio) che possono ruotare il piano di polarizzazione della luce linearmente polarizzata.
- **Modulatori elettro-ottici** che sfruttano l'effetto Pockels o l'effetto Kerr, modificando lo stato di polarizzazione della luce in risposta a un campo elettrico applicato.
- **Effetto Faraday**, che si verifica quando la luce attraversa un materiale sotto l'influenza di un campo magnetico esterno.
- **Materiali birifrangenti**, che modificano la polarizzazione della luce in base alla sua direzione di propagazione all'interno del materiale: lamine a mezz'onda e a quarto d'onda, materiali fotoelastici.



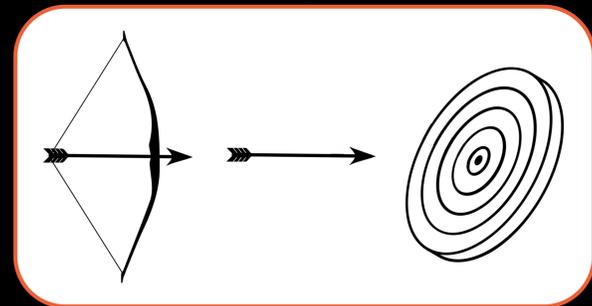
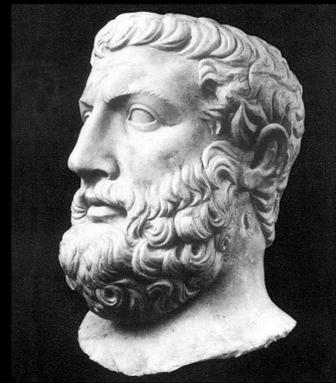
EFFETTO ZENONE

congelare l'evoluzione

IL PARADOSSO DELLA FRECCIA

Zenone di Elea, filosofo del V sec. a.C. è celebre per i suoi paradossi, tra cui il **paradosso della freccia**.

- Una freccia in volo osservata in un istante molto breve appare immobile, dato che in quell'istante può solo occupare una certa posizione nello spazio.
- Poiché il tempo è fatto di singoli istanti e la freccia è immobile in ognuno di essi, essa risulta immobile sempre, ovvero **il moto è impossibile**.

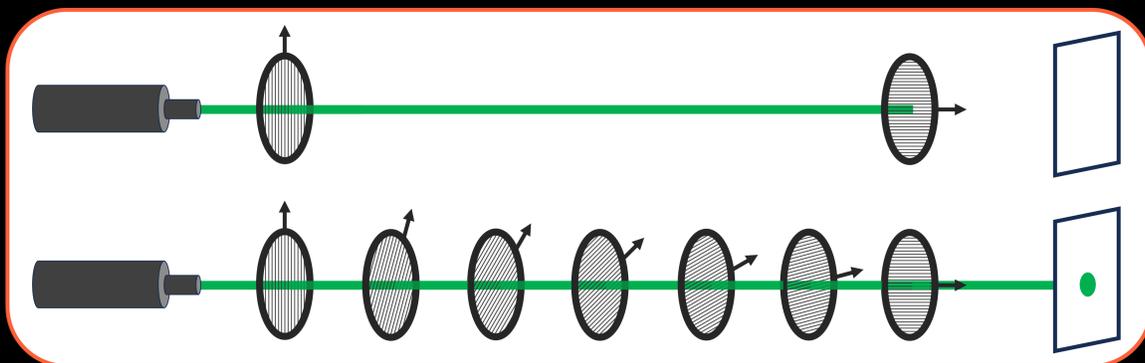


EFFETTO ZENONE QUANTISTICO

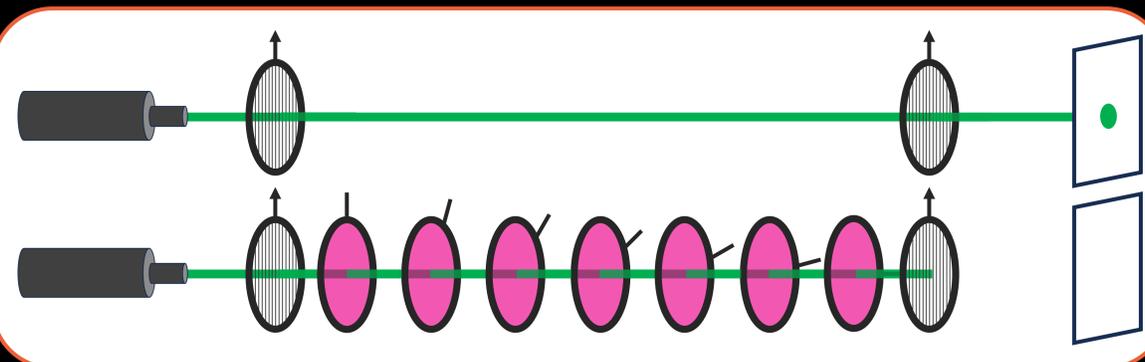
L'evoluzione di un sistema quantistico è inibita o addirittura soppressa se il sistema è sottoposto a una **serie infinita di misure ravvicinate**.

Una **sequenza di polarizzatori** sfasati di angoli uguali modifica lo stato mantenendo l'intensità.

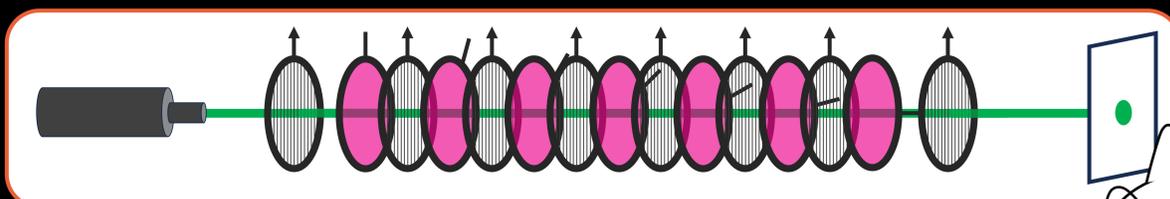
$$I_N = I_0 \left[\cos^2 \left(\frac{\pi}{2N} \right) \right]^N \xrightarrow{N \rightarrow \infty} I_0$$



Consideriamo l'**evoluzione** di uno stato di polarizzazione che passa da verticale a orizzontale.



Inseriamo molti polarizzatori allineati con la direzione iniziale della polarizzazione.



Misure intermedie ripetute congelano l'evoluzione dello stato!



SIMULAZIONI

soluzioni di problemi complessi

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

R.P. Feynman

SIMULATORI QUANTISTICI

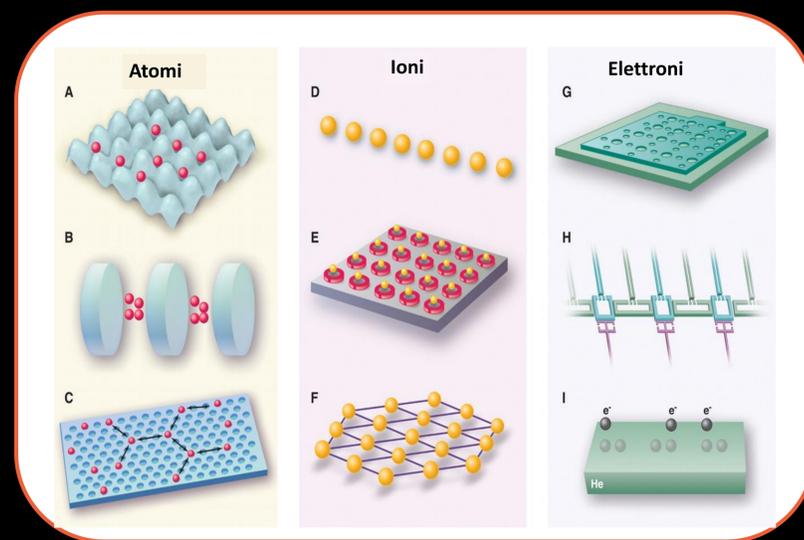
Le **simulazioni numeriche** sono l'approccio standard allo studio della dinamica dei sistemi quantistici. Spesso le simulazioni sono complesse e richiedono molto tempo.

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:

atomi o **ioni** intrappolati in reticoli ottici o cavità, **elettroni** in atomi e molecole artificiali, **circuiti superconduttori**, e sfruttano **sovrapposizione** ed **entanglement**.

I **quantum annealers** sono computer quantistici utilizzati per risolvere problemi di ottimizzazione, trovando la **soluzione senza calcolarla!** Il più celebre è D-Wave.



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



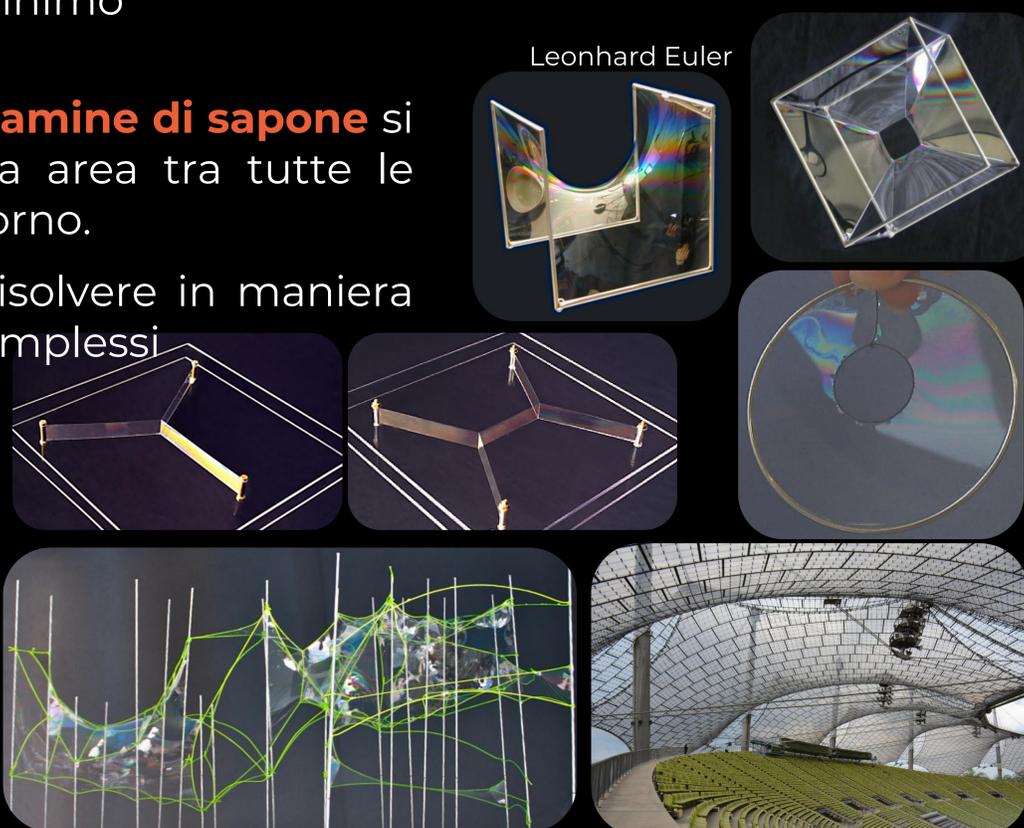
BOLLE DI SAPONE

"Nulla accade nell'universo che non faccia capo a qualche criterio di massimo o di minimo"

A causa della tensione superficiale, le **lamine di sapone** si dispongono a **minimizzare** la propria area tra tutte le possibili superfici aventi lo stesso contorno.

Usando i film di sapone si possono risolvere in maniera **analogica**, ovvero senza fare calcoli, complessi **problemi di minimo** come:

- la ricerca di reti minime
- la costruzione di tensostrutture
- il problema di Didone (ottimizzazione dell'area dato il perimetro).



Otto Frei – Stadio Olimpico Monaco di Baviera 1972

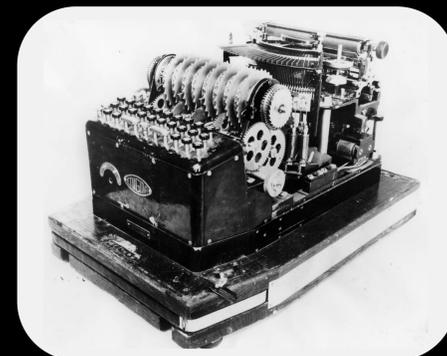
SICUREZZA NELLA COMPLESSITÀ

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

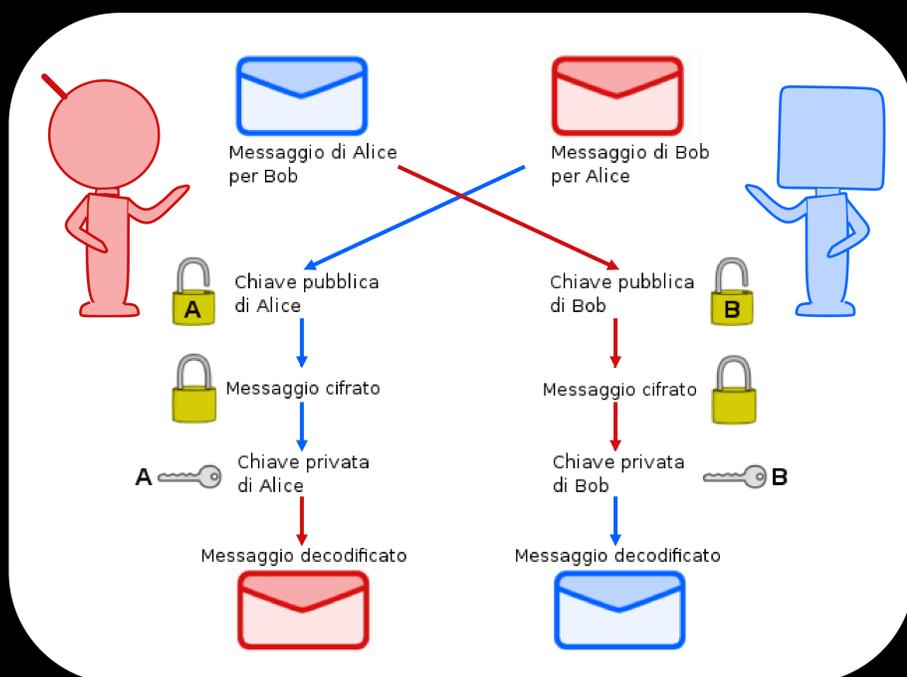
Tecnica per garantire l'**autenticazione** e il **contenuto** di informazioni trasmesse tramite vari canali di comunicazione.

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).



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.

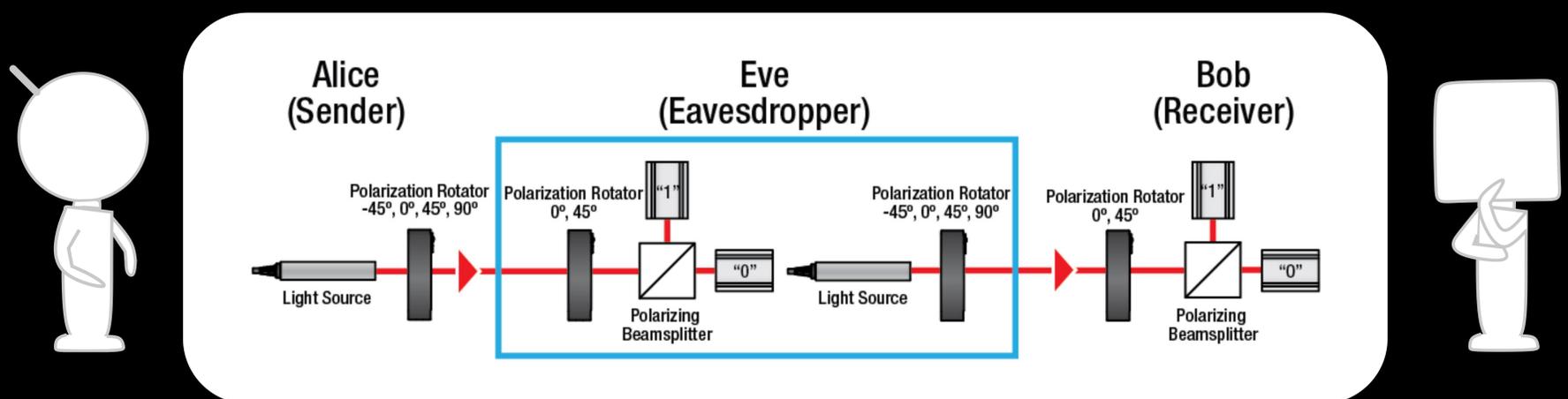
Le chiavi di accesso sono basate su **algoritmi complessi** (fattorizzazione di numeri interi grandi, logaritmo discreto) perché sia computazionalmente (quasi) impossibile calcolarle con tecniche classiche.

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**.

CHIAVI CRITTOGRAFICHE SICURE

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 1984 Bennet & Brassard proposero un protocollo di **crittografia quantistica** noto come protocollo BB84.



- Per costruire la **chiave crittografica** sicura (sequenza casuale di 0 e 1) Alice invia a Bob una sequenza di qbit codificati nello stato di polarizzazione di un fotone.
- Alice sceglie a caso fra due due "alfabeti", ovvero due diverse basi di polarizzazione (H/V e $+45^\circ/-45^\circ$).
- Bob misura scegliendo a caso una delle due basi.
- Per ottenere la chiave crittografica, Alice e Bob comunicano pubblicamente la sequenza delle basi e selezionano solo i risultati ottenuti per basi uguali.

Lo schema si basa sulle proprietà degli stati di **sovrapposizione** e delle **misure incompatibili**.

La presenza di un intercettatore (Eve) introduce errori nella trasmissione che permettono ad Alice e Bob di individuarne la presenza.

Il protocollo funziona anche con luce classica ma è perfettamente sicuro solo se utilizza singoli fotoni!

QUBIT

logica quantistica

Nei **computer quantistici** l'unità dell'informazione classica, ovvero il **bit**, viene sostituita dal **qubit** e la logica classica si trasforma in **logica quantistica**.

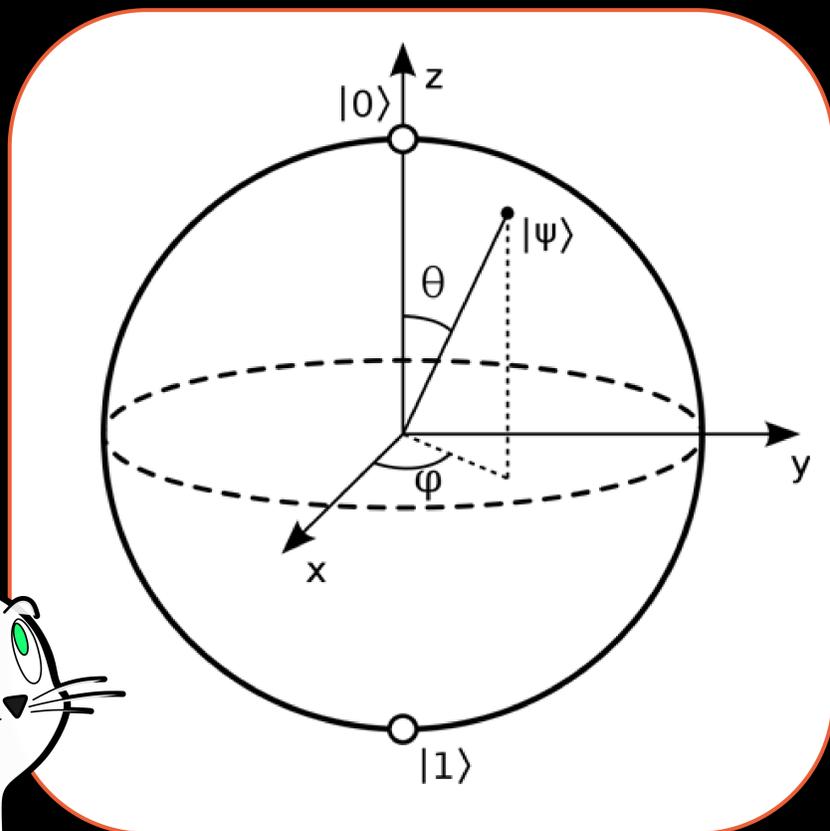
Il **bit** è come la faccia di una moneta classica che può essere solo testa = **0** o croce = **1**

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



SFERA DI BLOCH

Lo stato di un qubit si può rappresentare come un punto sulla superficie di una sfera chiamata **Sfera di Bloch**.



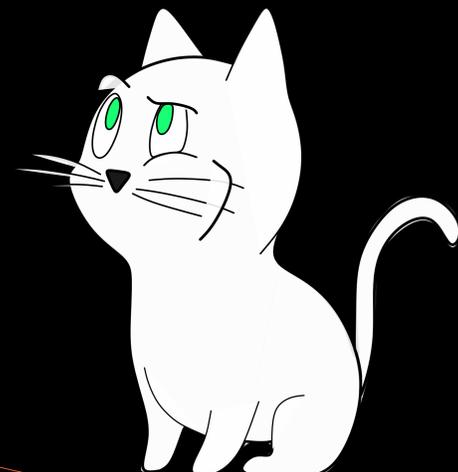
$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

$$0 \leq \theta \leq \pi$$

$$0 \leq \varphi < 2\pi$$



Ogni trasformazione dello stato del qubit corrisponde a una **rotazione** sulla sfera di Bloch.



QUBIT

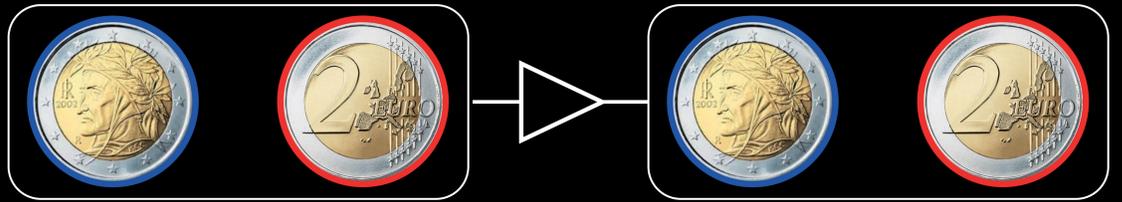
logica quantistica

Le porte logiche quantistiche o **gate quantistici**, rappresentano le operazioni che si possono effettuare sui qbit.

- Le porte quantistiche possono essere estensioni delle porte logiche classiche

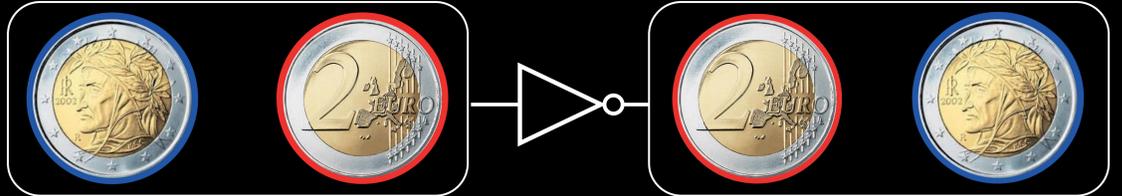
IDENTITÀ

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



NOT

$$\text{NOT}(c_0|0\rangle + c_1|1\rangle) = c_0|1\rangle + c_1|0\rangle$$



- oppure possono essere nuove operazioni genuinamente quantistiche

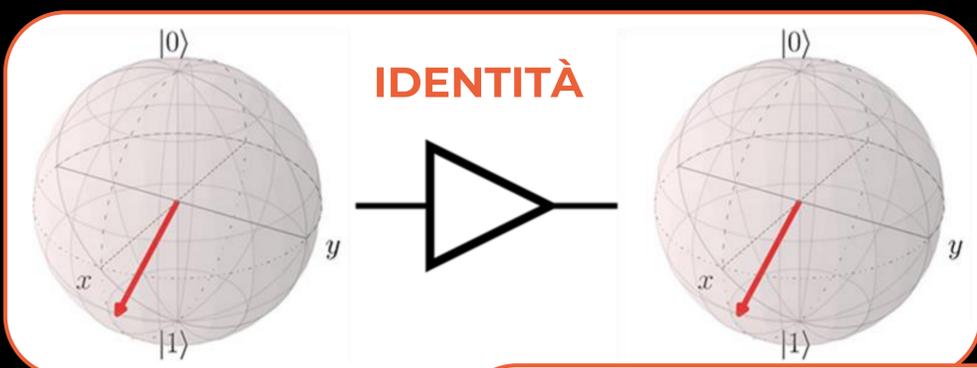
HADAMARD



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



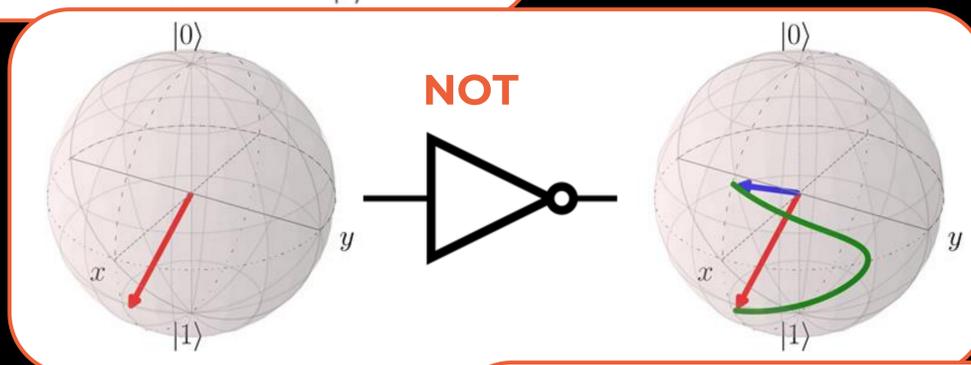
$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$



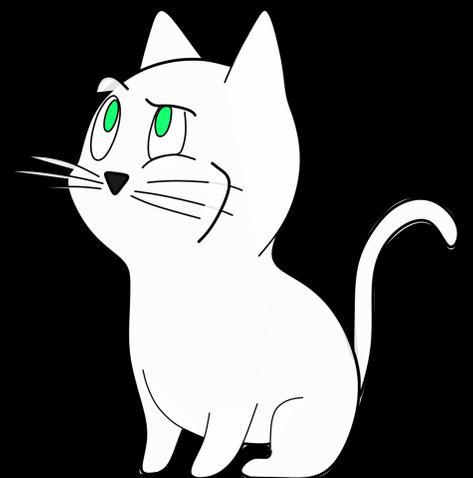
IDENTITÀ

L'identità non modifica lo stato

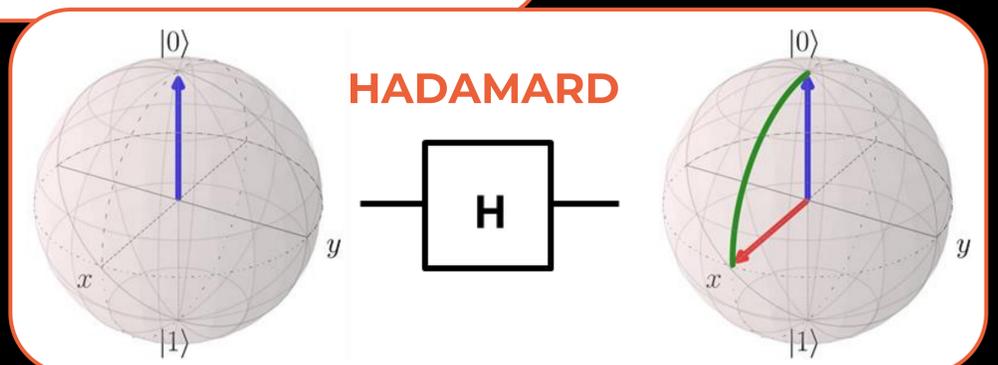
La porta NOT compie una rotazione di 180° attorno all'asse \hat{x}



NOT



La porta HADAMARD compie una rotazione di 180° attorno all'asse $(\hat{x} + \hat{z})/\sqrt{2}$



HADAMARD

H

ALGORITMI QUANTISTICI

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

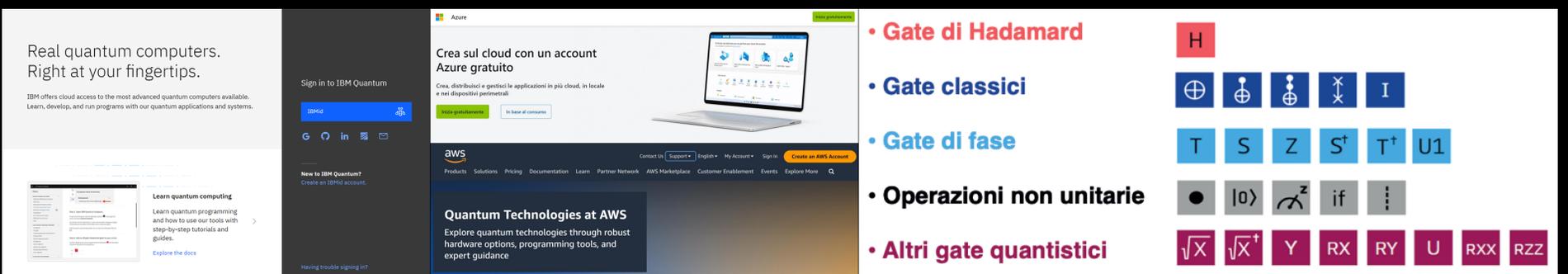


Gli **algoritmi quantistici** possono essere eseguiti solo da computer che usano risorse quantistiche, ovvero in grado di generare **stati di sovrapposizione** o **stati entangled** e di manipolarli mantenendone le caratteristiche quantistiche, ovvero la **coerenza**.

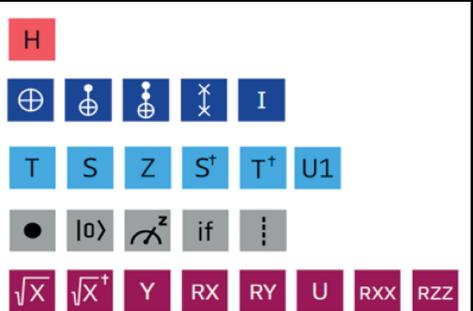
Celebri algoritmi quantistici sono: Shor, Grover, Deutsch, Fast Fourier Transform...

COMPUTER QUANTISTICI REALI

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**.



- Gate di Hadamard
- Gate classici
- Gate di fase
- Operazioni non unitarie
- Altri gate quantistici



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**.

