

Tecnologie quantistiche

dal computer quantistico alle telecomunicazioni

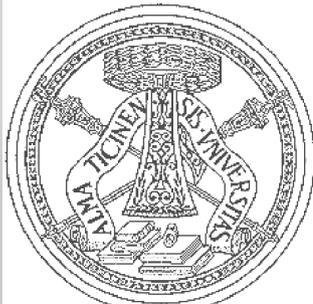


Lorenzo
Maccone

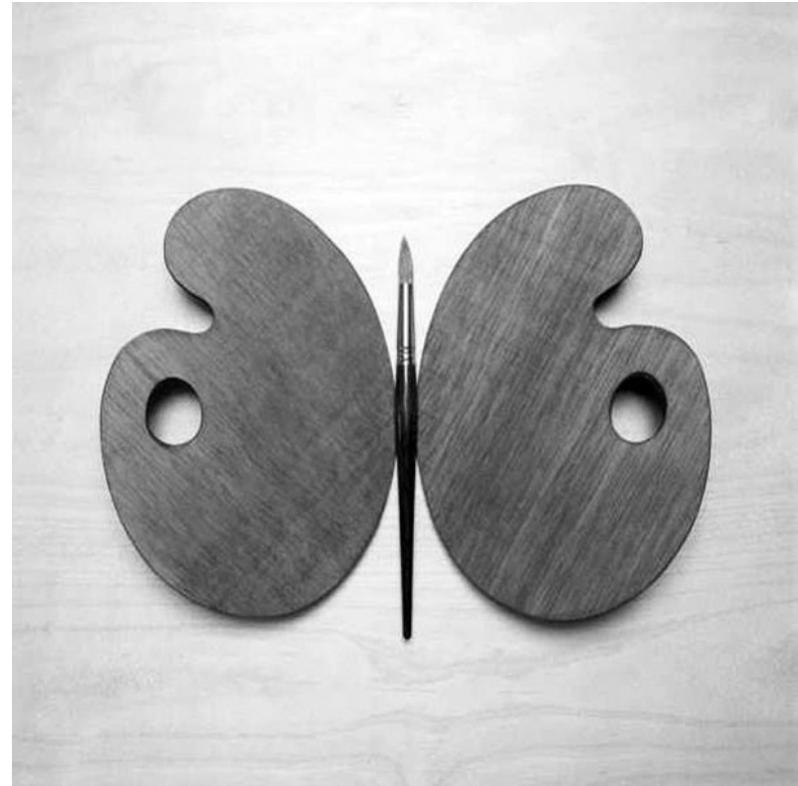
Dipartimento di Fisica,
INFN Sez. Pavia,
Universita' di Pavia

maccone@unipv.it

QUit
quantum information
theory group
www.qubit.it

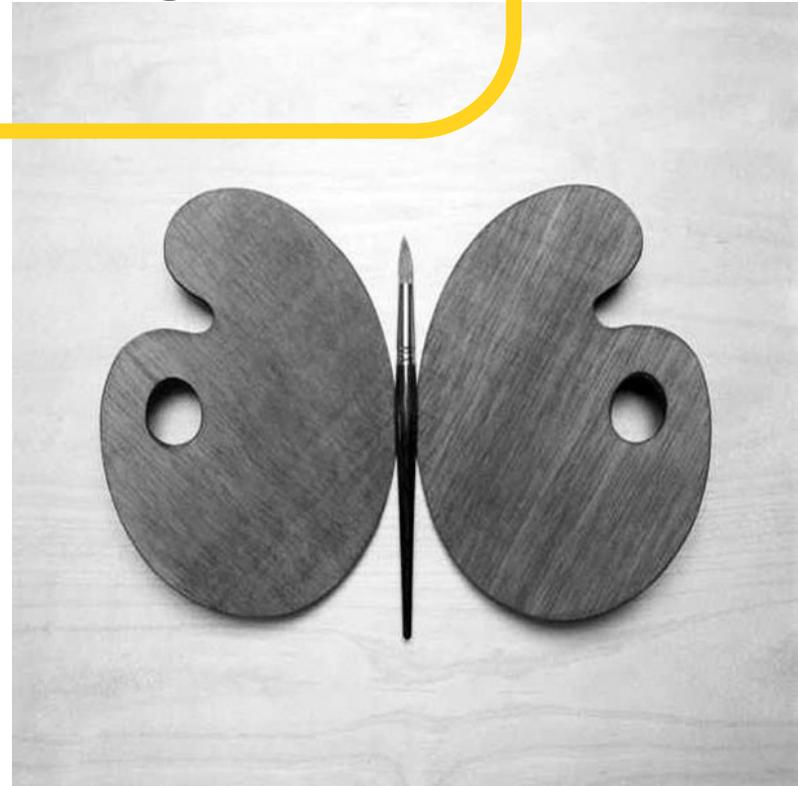


Tecnologia quantistica?



Tecnologia quantistica?

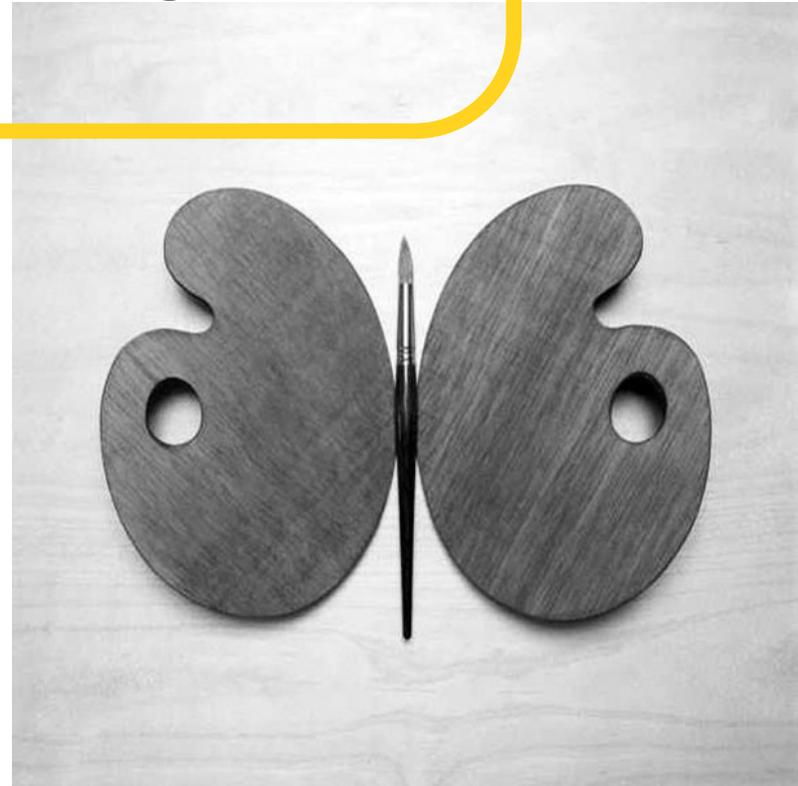
Applicazione della
meccanica quantistica a
problemi tecnologici



Tecnologia quantistica?

Applicazione della
meccanica quantistica a
problemi tecnologici

Oggi e' ambito di
ricerca avanzata

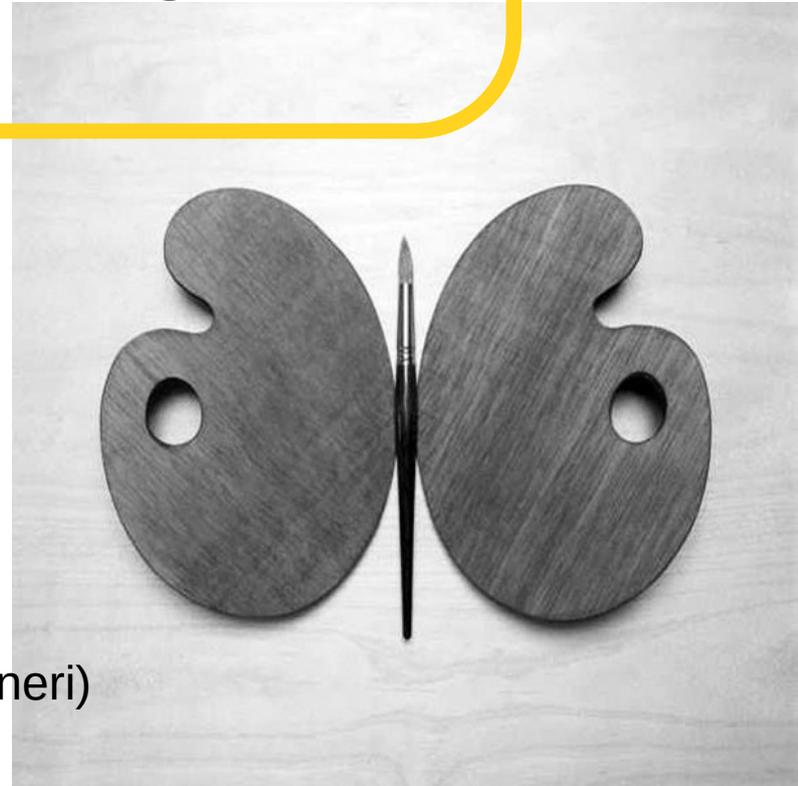


Tecnologia quantistica?

Applicazione della
meccanica quantistica a
problemi tecnologici

Oggi e' ambito di
ricerca avanzata

(ci lavorano ancora i fisici, piu' che gli ingegneri)



Cos'e' la meccanica quantistica?



Cos'e' la meccanica quantistica?

La teoria fisica che
descrive il nostro mondo



Cos'è la meccanica quantistica?

La teoria fisica che
descrive il nostro mondo

Non ne vediamo gli effetti
nella vita di tutti i giorni: I
nostri sensi sono limitati



Cos'è la meccanica quantistica?

La teoria fisica che
descrive il nostro mondo

Non ne vediamo gli effetti
nella vita di tutti i giorni: I
nostri sensi sono limitati

Vediamo solo gli effetti della
fisica classica

(quella che si studia alle superiori)



Perche' usare la meccanica
quantistica?

Perche' usare la meccanica quantistica?

Viviamo in un mondo quantistico, ma nella vita di tutti i giorni ne vediamo una minima parte (il sottoinsieme descritto dalla fisica classica).

Perche' usare la meccanica quantistica?

Viviamo in un mondo quantistico, ma nella vita di tutti i giorni ne vediamo una minima parte (il sottoinsieme descritto dalla fisica classica).

Favola del girino che vive nella pozzanghera e una notte vede le stelle per la prima volta!



Perche' usare la meccanica quantistica?

Viviamo in un mondo quantistico, ma nella vita di tutti i giorni ne vediamo una minima parte (il sottoinsieme descritto dalla fisica classica).

Favola del girino che vive nella pozzanghera e una notte vede le stelle per la prima volta!

La scoperta della MQ e' come scoprire le stelle



Perche' usare la meccanica quantistica?

Viviamo in un mondo quantistico, ma nella vita di tutti i giorni ne vediamo una minima parte (il sottoinsieme descritto dalla fisica classica).

Favola del girino che vive nella pozzanghera e una notte vede le stelle per la prima volta!

La scoperta della MQ e' come scoprire le stelle
improvvisamente il nostro mondo si espande!



Visto che il nostro mondo e'
quantistico, perche' limitare la nostra
tecnologia al sottoinsieme classico?!



Visto che il nostro mondo e' quantistico, perche' limitare la nostra tecnologia al sottoinsieme classico?!

Tecnologie quantistiche

- Trasmissione di info
- Misurazioni ultraprecise
- Crittografia
- Computazione avanzata
- Aumento nell'efficienza di motori, celle fotovoltaiche, etc.
- Aumento della velocita' dei computer
- etc....



Cosa si guadagna a usare MQ?



Cosa si guadagna a usare MQ?

Per alcuni problemi: niente

viviamo nel mondo classico, alcuni problemi sono già risolti efficientemente con MC



Cosa si guadagna a usare MQ?

Per alcuni problemi: niente

viviamo nel mondo classico, alcuni problemi sono già risolti efficientemente con MC

Altri problemi: MOLTO!



Cosa si guadagna a usare MQ?

Per alcuni problemi: niente

viviamo nel mondo classico, alcuni problemi sono già risolti efficientemente con MC

Altri problemi: MOLTO!

Uno degli scopi principali oggi delle quantum technologies:



Cosa si guadagna a usare MQ?

Per alcuni problemi: niente

viviamo nel mondo classico, alcuni problemi sono già risolti efficientemente con MC

Altri problemi: MOLTO!

Uno degli scopi principali oggi delle quantum technologies:

scoprire nuovi ambiti dove MQ aiuta!



Parole chiave:



Parole chiave:

standard quantum limit (SQL)



Parole chiave:

standard quantum limit (SQL)

limite (precisione, efficienza, velocità, etc.)

raggiungibile con fenomeni classici



Parole chiave:

standard quantum limit (SQL)

limite (precisione, efficienza, velocità, etc.)

raggiungibile con fenomeni classici

Heisenberg bound



Parole chiave:

standard quantum limit (SQL)

limite (precisione, efficienza, velocità, etc.)

raggiungibile con fenomeni classici

Heisenberg bound

limite ultimo (imposto dalla fisica)



Parole chiave:

standard quantum limit (SQL)

limite (precisione, efficienza, velocità, etc.)

raggiungibile con fenomeni classici

Heisenberg bound

limite ultimo (imposto dalla fisica)

**tecnologie quantistiche: se
 $SQL < \text{Heisenberg}$**



la ricerca oggi in Europa



la ricerca oggi in Europa

Quantum technologies flagship:

L'Europa oggi ha deciso di investire (10^9 euro) sulle tecnologie quantistiche, realizzando che la tecnologia del futuro sarà basata sulla MQ.



Di cosa stiamo parlando?!?

Esempi di tecnologie quantistiche

- Quantum computer
computazioni rapidissime
- Metrologia quantistica
misure alla precisione ultima
- telecomunicazioni
trasmissione di informazione



Cos'e' un computer quantistico?



Cos'è un computer quantistico?

un computer che utilizza fenomeni quantistici per svolgere computazioni



Cos'è un computer quantistico?

un computer che utilizza fenomeni quantistici per svolgere computazioni

- Complementarietà (principio di sovrapposizione)
- Entanglement



Cosa ci si guadagna ad usare un quantum computer?

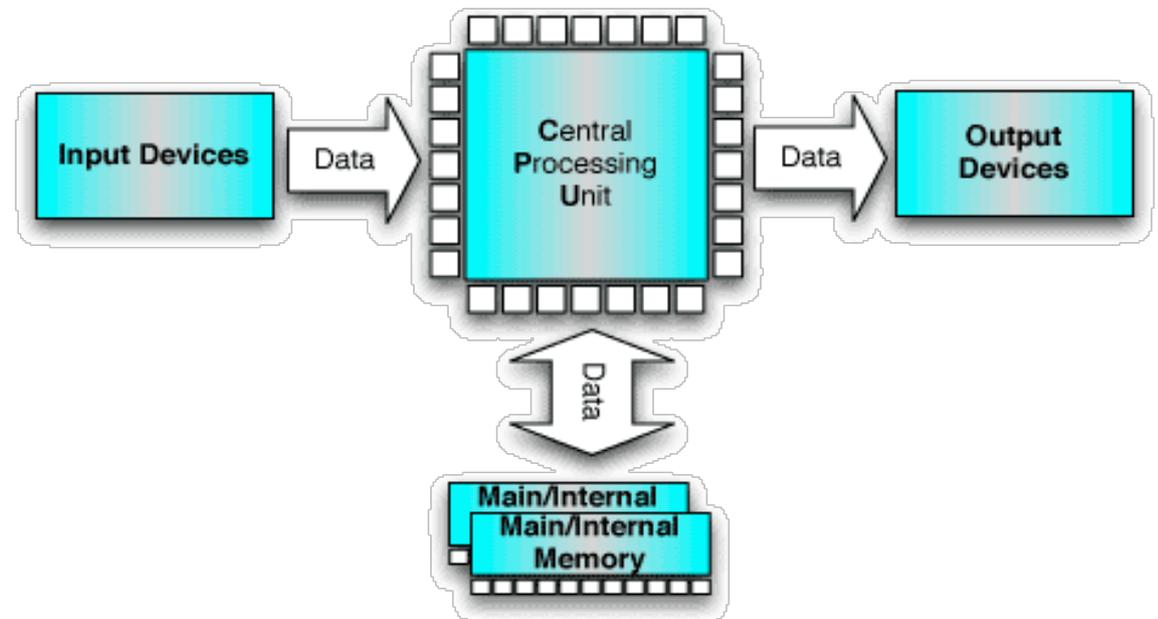


Cosa ci si guadagna ad usare un quantum computer?

Puo' svolgere tutte le computazioni di un computer classico, ma e' molto piu' veloce per alcuni calcoli (non per tutti)



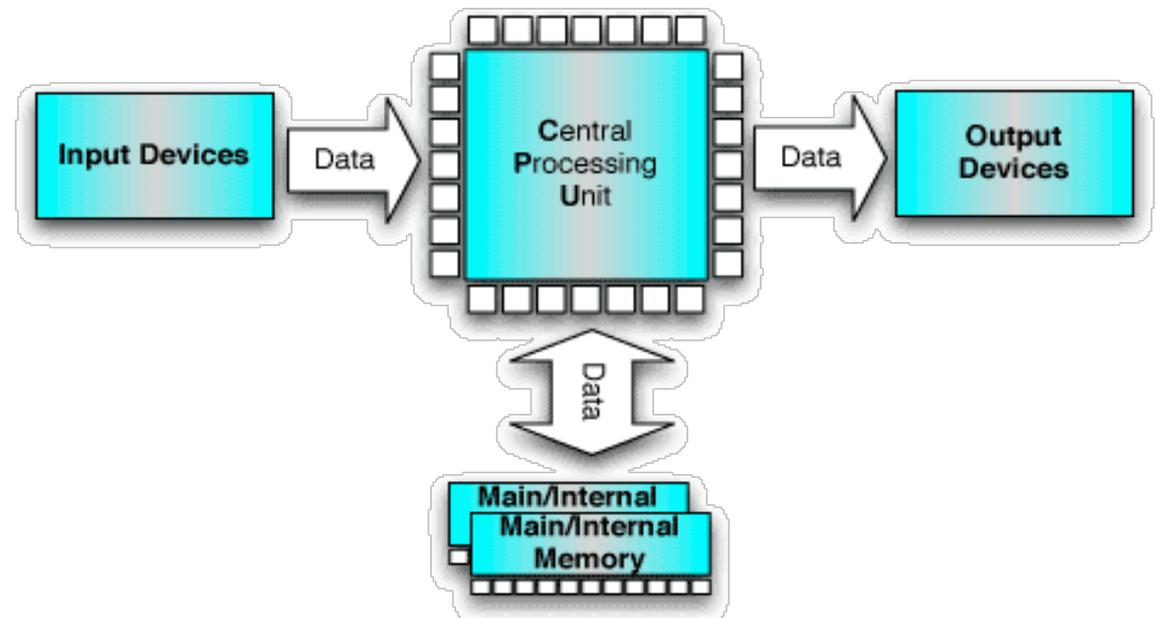
Come funziona?



Come funziona?

Computer classico:

input: informazione (codificata in bits)

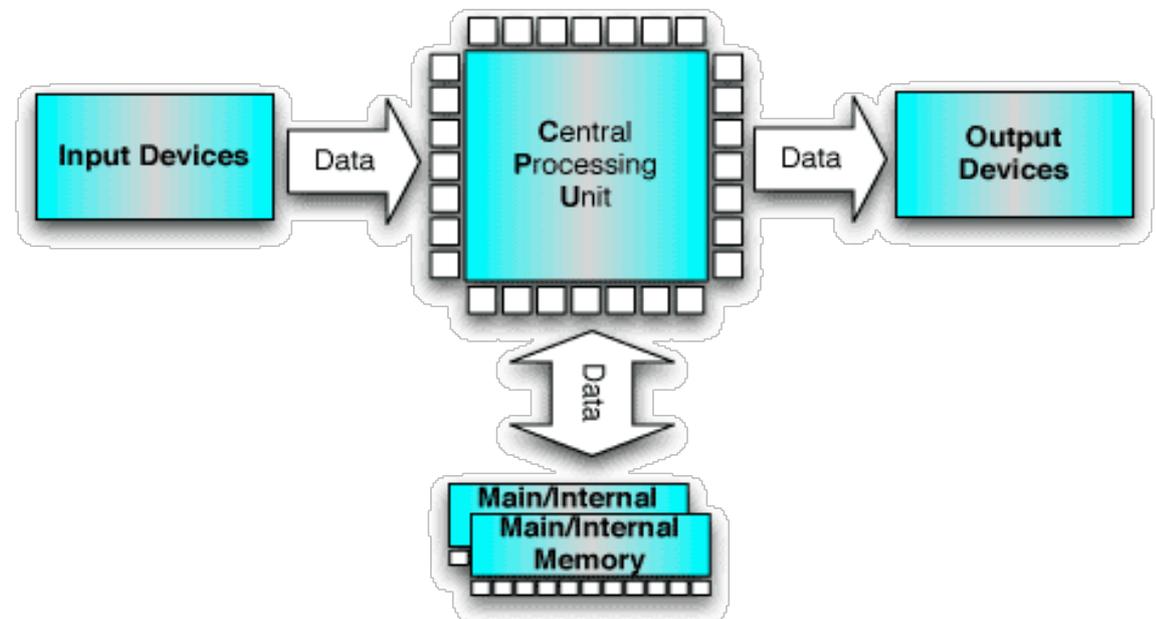


Come funziona?

Computer classico:

input: informazione (codificata in bits)

elaborazione: circuiti elettronici (svolgono operazioni matematiche sui bits)



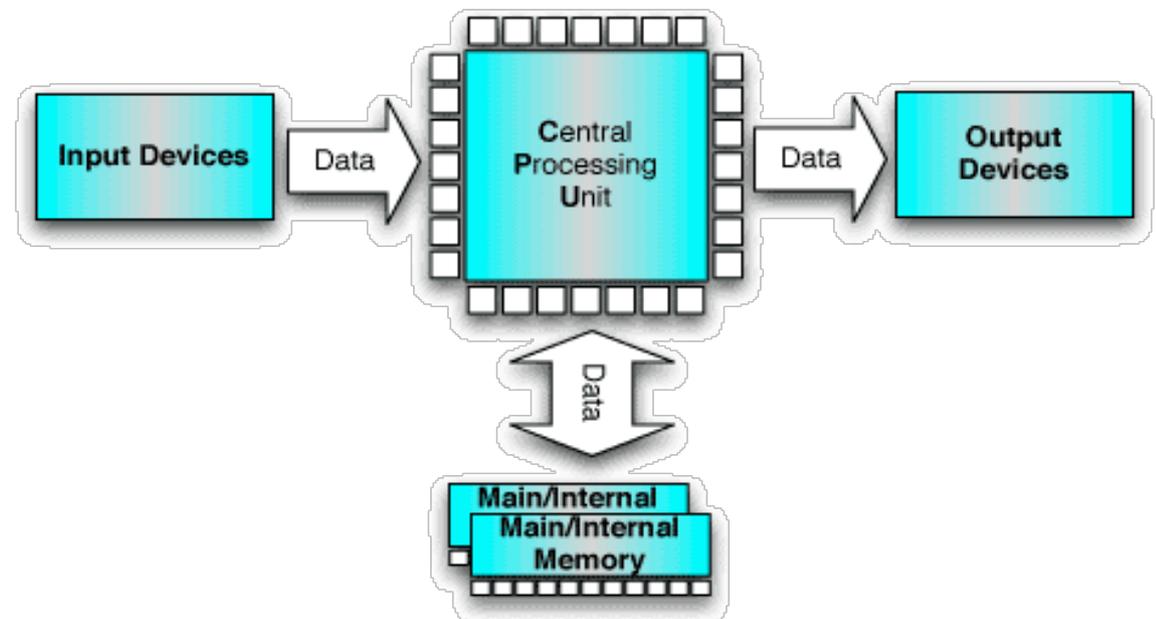
Come funziona?

Computer classico:

input: informazione (codificata in bits)

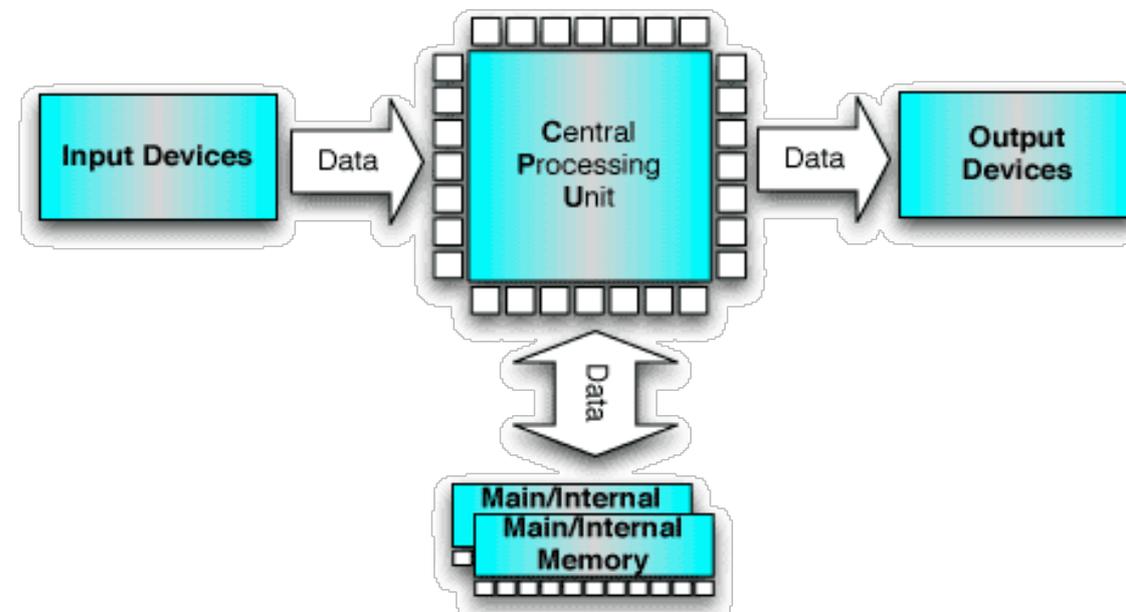
elaborazione: circuiti elettronici (svolgono operazioni matematiche sui bits)

output: risultato



Come funziona?

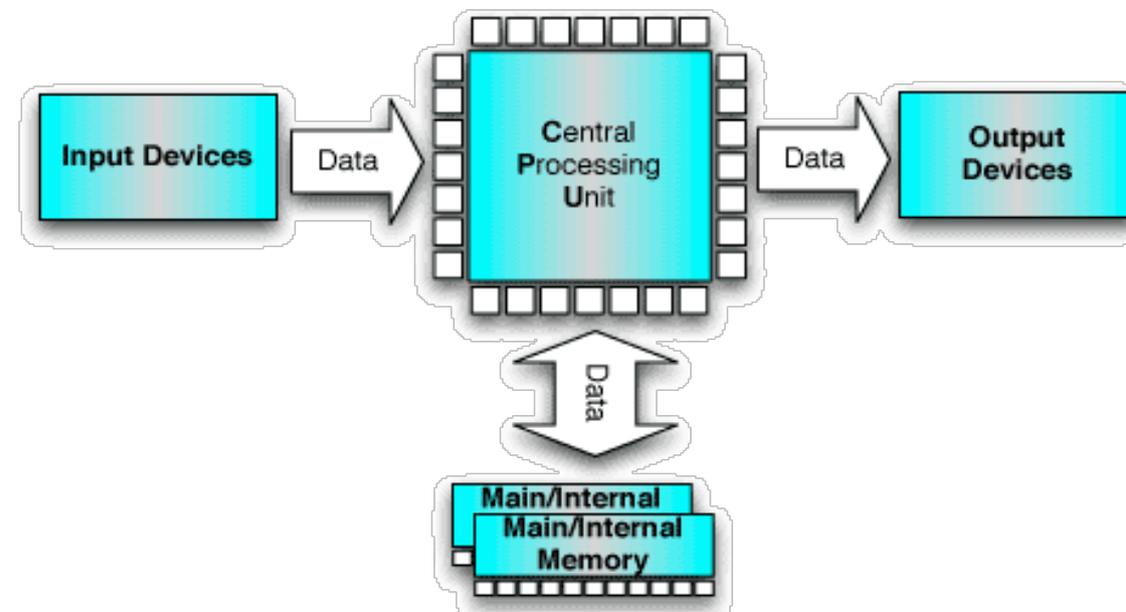
Computer quantistico:



Come funziona?

Computer quantistico:

input: informazione (codificata in *quantum* bits: qubits)

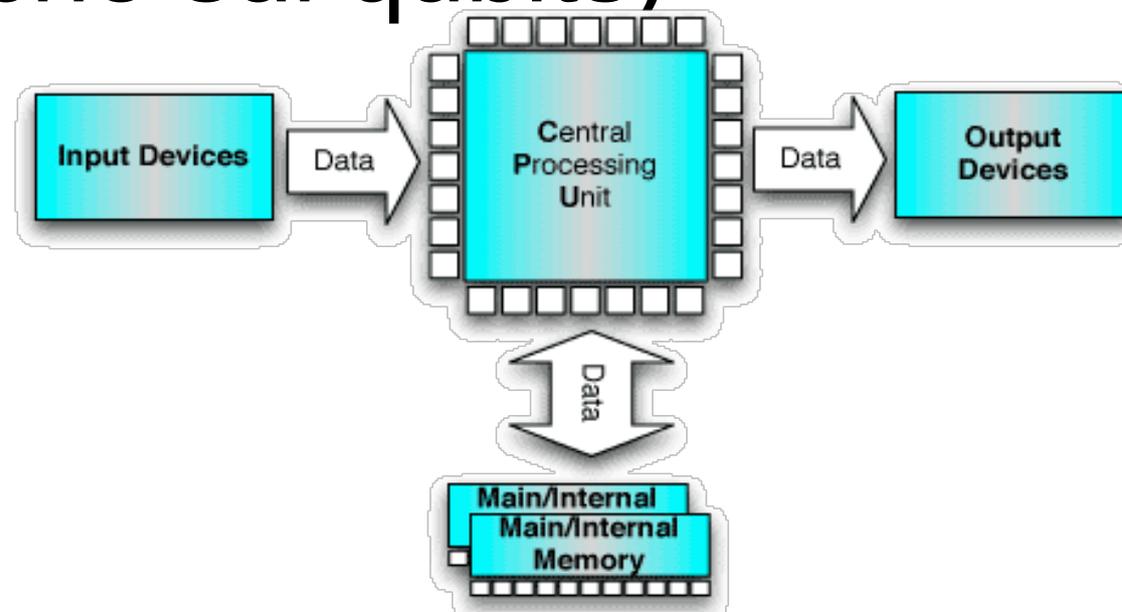


Come funziona?

Computer quantistico:

input: informazione (codificata in *quantum* bits: qubits)

elaborazione: circuiti quantistici (svolgono operazioni matematiche sui qubits)



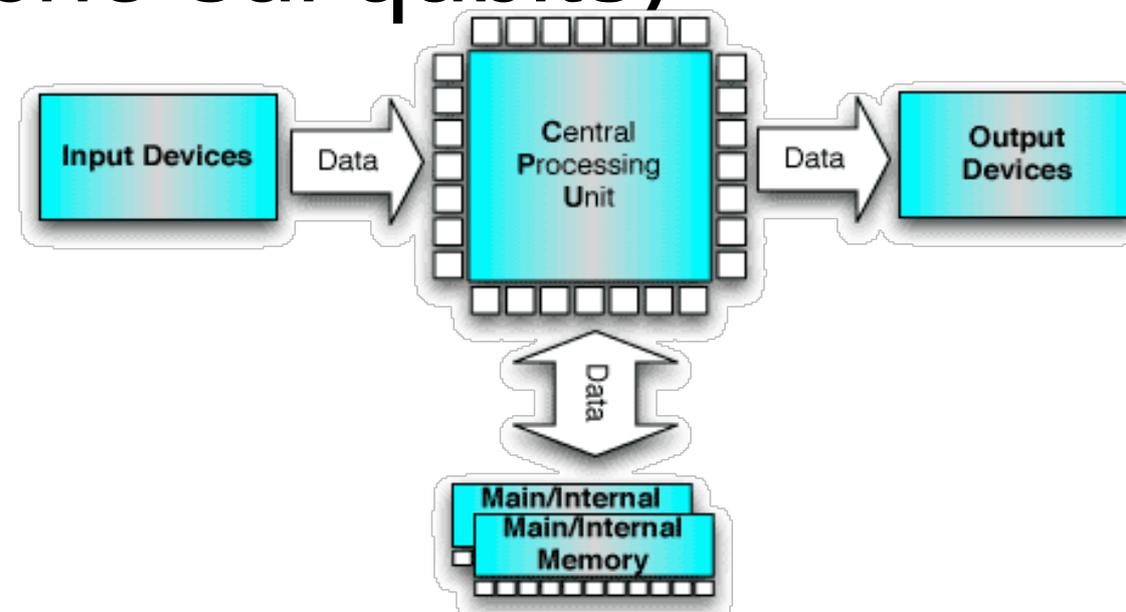
Come funziona?

Computer quantistico:

input: informazione (codificata in *quantum* bits: qubits)

elaborazione: circuiti quantistici (svolgono operazioni matematiche sui qubits)

output: risultato



Cos'e' un qubit?



Cos'e' un qubit?

Un sistema quantistico a due livelli.

Per esempio lo spin di un elettrone: $+1/2$ e $-1/2$.



Cos'e' un qubit?

Un sistema quantistico a due livelli.

Per esempio lo spin di un elettrone: $+1/2$ e $-1/2$.

Posso chiamare "0" e "1" i due livelli.



Cos'e' un qubit?



Un sistema quantistico a due livelli.

Per esempio lo spin di un elettrone: $+1/2$ e $-1/2$.

Posso chiamare "0" e "1" i due livelli.

e' un sistema quantistico: puo' accedere a fenomeni quantistici come la sovrapposizione (complementarieta'), entanglement, etc.

Complementarieta'?!



Complementarieta'?!

Ogni sistema ha **proprietà' complementari**,
che **non** possono essere contemporanea-
mente conosciute con precisione



Complementarieta'?!

Ogni sistema ha **proprietà' complementari**,
che **non** possono essere contemporanea-
mente conosciute con precisione

proprietà: qualcosa che si può misurare, per esempio la
posizione, la velocità, il peso



Complementarieta'?!

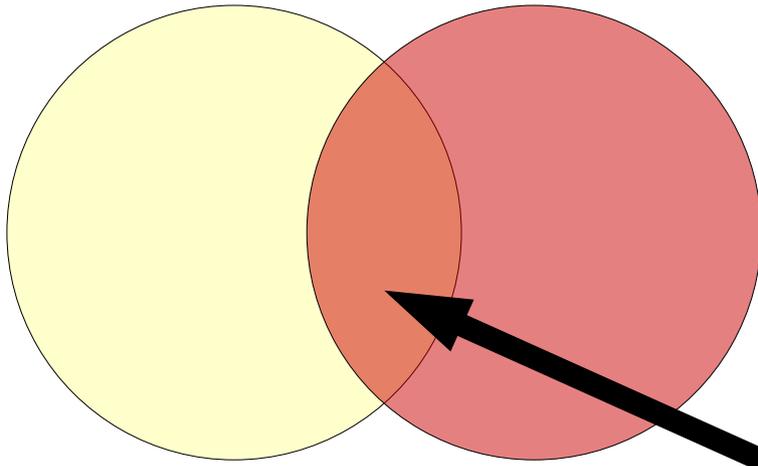
Ogni sistema ha **proprietà' complementari**,
che **non** possono essere contemporanea-
mente conosciute con precisione

proprietà: qualcosa che si può misurare, per esempio la
posizione, la velocità, il peso



Proprietà' complementari si
ottengono “sovrapponendo”:
principio di sovrapposizione q.

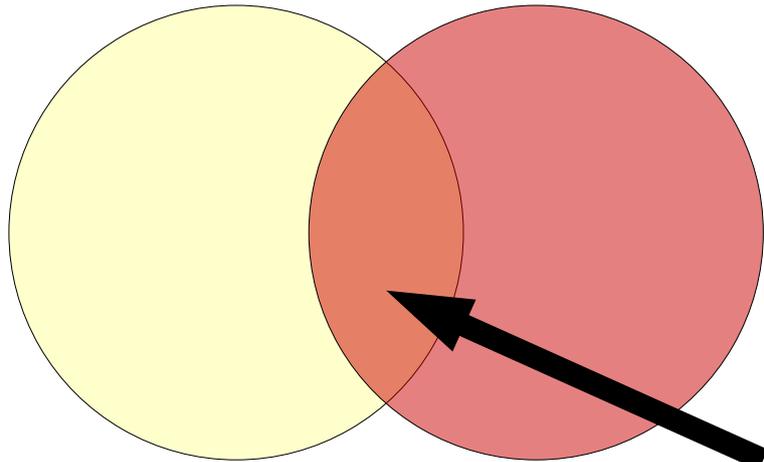
Metafora per la complementarità:



arancione è giallo+rosso

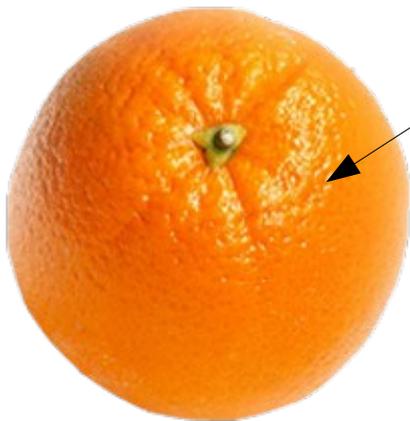
“arancionità” è complementare a giallo/rosso

Metafora per la complementarietà:



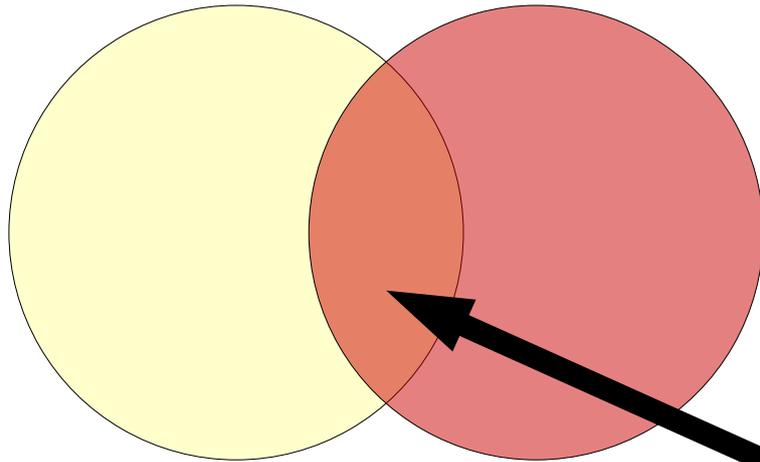
arancione è giallo+rosso

“arancionità” è complementare a giallo/rosso



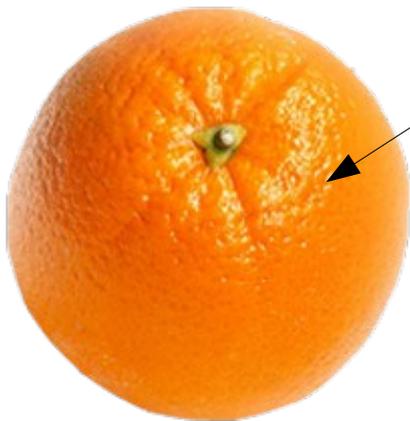
arancia non è nè gialla nè rossa, è contemporaneamente gialla e rossa.

Metafora per la complementarità:



arancione è giallo+rosso

“arancionità” è complementare a giallo/rosso

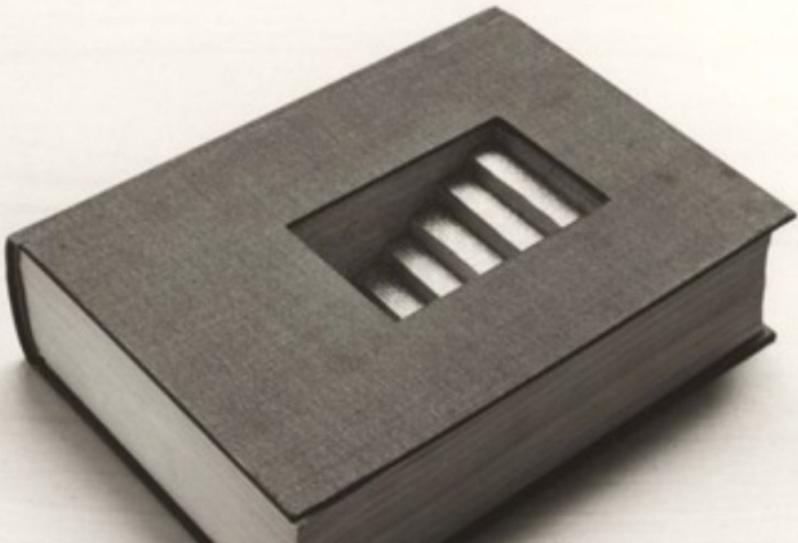


metafora incompleta:
riguarda un'unica proprietà (colore),
mentre la complementarità
quantistica riguarda proprietà diverse
(posizione, velocità, etc.)

Relazioni di indeterminazione di Heisenberg

conseguenza dell'esistenza di proprietà complementari

piu' conosco bene una proprietà
meno conosco bene le sue
proprietà complementari



Relazioni di indeterminazione di Heisenberg

conseguenza dell'esistenza di proprietà complementari

piu' conosco bene una proprietà
meno conosco bene le sue
proprietà complementari

esempio: posizione e momento



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

Per la nostra mente non abituata a concetti quantistici, questo è difficile (impossibile?) da “capire”:

cosa vuol dire che la posizione della mia auto non è definita?! Dov'è la mia auto!?



Non vediamo la complementarità (e l'indeterminazione) nella vita di tutti i giorni.

Conosciamo sia la posizione che la velocità della nostra auto (SPERIAMO!)



Non vediamo la complementarità (e l'indeterminazione) nella vita di tutti i giorni.

Conosciamo sia la posizione che la velocità della nostra auto (SPERIAMO!)



perchè non conosciamo nessuna delle due molto precisamente: se sapessimo che l'auto ha una velocità di 50.123153428941234132142412... Km/h (32 cifre), perderemmo informazione sulla sua posizione per qualche cm.

Non vediamo la complementarità (e l'indeterminazione) nella vita di tutti i giorni.

Conosciamo sia la posizione che la velocità della nostra auto (SPERIAMO!)



perchè non conosciamo nessuna delle due molto precisamente: se sapessimo che l'auto ha una velocità di 50.123153428941234132142412... Km/h (32 cifre), perderemmo informazione sulla sua posizione per qualche cm.

Il record di misura più precisa al mondo è 18 cifre!!!

Perche' la complementarieta' e' utile in un computer quantistico?

Sembra piu' che altro una limitazione!



Perche' la complementarieta' e' utile in un computer quantistico?

Sembra piu' che altro una limitazione!

Ma un quantum bit puo' usare le proprieta' complementari di un bit!!!



Perche' la complementarieta' e' utile in un computer quantistico?

Sembra piu' che altro una limitazione!

Ma un quantum bit puo' usare le proprieta' complementari di un bit!!!

proprieta' di un bit: $\{0, 1\}$

proprieta' di un qubit: $\{0,1\}$; $\{+,-\}$; $\{+i,-i\}$...



Perche' la complementarieta' e' utile in un computer quantistico?

Sembra piu' che altro una limitazione!

Ma un quantum bit puo' usare le proprieta' complementari di un bit!!!

proprietà di un bit: $\{0, 1\}$

proprietà di un qubit: $\{0,1\}$; $\{+,-\}$; $\{+i,-i\}$...

sono tutte proprietà complementari: una sola e' conoscibile ad un certo istante, ma se sono abbastanza furbo, posso usarle tutte nella mia computazione



Esempio: algoritmo di Deutsch-Jozsa

ho una scatola che calcola una funzione di un bit: $f(0)=a$; $f(1)=b$.
Voglio scoprire se $a=b$, *usando la scatola **una volta sola**!!*



Esempio: algoritmo di Deutsch-Jozsa

ho una scatola che calcola una funzione di un bit: $f(0)=a$; $f(1)=b$.
Voglio scoprire se $a=b$, *usando la scatola una volta sola!!*

uso $\{+,-\}$ invece di $\{0,1\}$: e' complementare, quindi un qubit "+" non e' ne' 0, ne' 1.

In un certo senso e' **contemporaneamente 0 e 1**



Esempio: algoritmo di Deutsch-Jozsa

ho una scatola che calcola una funzione di un bit: $f(0)=a$; $f(1)=b$.
Voglio scoprire se $a=b$, *usando la scatola una volta sola!!*

uso $\{+,-\}$ invece di $\{0,1\}$: e' complementare, quindi un qubit "+" non e' ne' 0, ne' 1.

In un certo senso e' **contemporaneamente 0 e 1**

uso un solo qubit "+" scopro se $a=b$!



L'algoritmo di Deutsch-Jozsa (per una scatola con n bits di input) puo' scoprire se una funzione e' bilanciata o costante con un aumento esponenziale in n di velocita' rispetto ad algoritmi classici deterministici. Se uno considera algoritmi classici probabilistici, allora c'e' un incremento di solo un fattore due...

la sovrapposizione c'e' anche in sistemi continui classici (onde in uno stagno)



la sovrapposizione c'e' anche in sistemi continui classici (onde in uno stagno)

il quantum computer e' solo un computer analogico?!?



la sovrapposizione c'e' anche in sistemi continui classici (onde in uno stagno)

il quantum computer e' solo un computer analogico?!?



NO!

I computer analogici sono limitati dal fatto che basta un minimo errore per rovinare tutto.

E' per questo che usiamo computer digitali!

la sovrapposizione c'e' anche in sistemi continui classici (onde in uno stagno)

il quantum computer e' solo un computer analogico?!?



NO!

I computer analogici sono limitati dal fatto che basta un minimo errore per rovinare tutto.

E' per questo che usiamo computer digitali!

Quantum error correction (Peter Shor): si possono correggere gli errori.

la sovrapposizione c'e' anche in sistemi continui classici (onde in uno stagno)

il quantum computer e' solo un computer analogico?!?



NO!

I computer analogici sono limitati dal fatto che basta un minimo errore per rovinare tutto.

E' per questo che usiamo computer digitali!

Quantum error correction (Peter Shor): si possono correggere gli errori.

il QC ha i vantaggi di computer analogici e digitali

cos'e' l'entanglement?



cos'e' l'entanglement?

correlazione tra variabili complementari.



cos'e' l'entanglement?

correlazione tra variabili complementari.

Anche se non sono definite contemporaneamente, possono essere **correlate**



cos'e' l'entanglement?

correlazione tra variabili complementari.

Anche se non sono definite contemporaneamente, possono essere **correlate**

$\{0,1\}$; $\{+,-\}$ sono complementari: un qubit non puo' avere proprieta' 0 e -. Solo una delle due e' definita,

ma due qubit possono avere *stesse* proprieta' anche complementari: se misuro $\{0,1\}$ su entrambi ottengo lo stesso risultato e se misuro $\{+,-\}$ su entrambi, ottengo di nuovo lo stesso risultato!



cos'e' l'entanglement?



correlazione tra variabili complementari.

Anche se non sono definite contemporaneamente, possono essere **correlate**

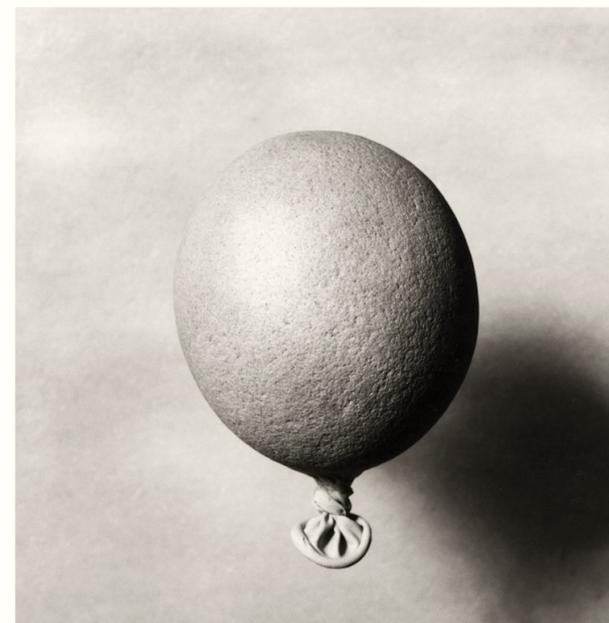
$\{0,1\}$; $\{+,-\}$ sono complementari: un qubit non puo' avere proprieta' 0 e -. Solo una delle due e' definita,

ma due qubit possono avere *stesse* proprieta' anche complementari: se misuro $\{0,1\}$ su entrambi ottengo lo stesso risultato e se misuro $\{+,-\}$ su entrambi, ottengo di nuovo lo stesso risultato!

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|++\rangle + |--\rangle}{\sqrt{2}}$$

(scoperto da Einstein e battezzato da Schroedinger)

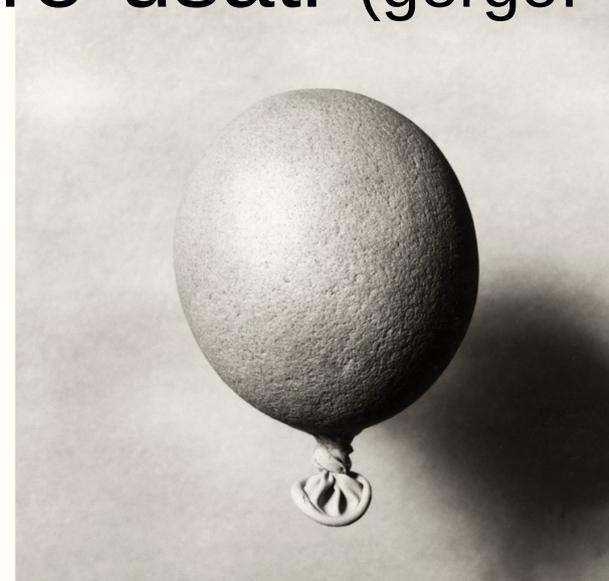
tutti gli algoritmi quantistici
usano entanglement?



tutti gli algoritmi quantistici usano entanglement?

Fino a qualche anno fa si pensava di sì: algoritmi senza entanglement avrebbero potuto essere simulati efficientemente su un computer classico

invece esistono altri fenomeni quantistici (discord) che possono anche essere usati (gergo: DQC1)



quali calcoli sono piu' veloci
su un quantum computer?



quali calcoli sono piu' veloci
su un quantum computer?

E' molto difficile scrivere software specifico per un quantum computer: bisogna saper sfruttare sapientemente la complementarita'!



quali calcoli sono piu' veloci su un quantum computer?

E' molto difficile scrivere software specifico per un quantum computer: bisogna saper sfruttare sapientemente la complementarita'!

ad oggi esistono molti algoritmi. I piu' famosi:

Fattorizzazione

Grover search

Simulazione di sistemi quantistici



fattorizzazione: dato un numero a devo cercare
i numeri b e c tali che $a = b \times c$

fattorizzazione: dato un numero a devo cercare i numeri b e c tali che $a = b \times c$

quasi tutti i sistemi crittografici in uso oggi sono basati sull'assunzione che fattorizzare numeri grandi e' molto difficile (anche se e' semplice verificare la soluzione: basta moltiplicare i due numeri)

fattorizzazione: dato un numero a devo cercare i numeri b e c tali che $a = b \times c$

quasi tutti i sistemi crittografici in uso oggi sono basati sull'assunzione che fattorizzare numeri grandi e' molto difficile (anche se e' semplice verificare la soluzione: basta moltiplicare i due numeri)

NON e' difficile per un quantum computer!

Questa fu la scoperta (Peter Shor) che fece decollare la computazione quantistica

fattorizzazione: dato un numero a devo cercare i numeri b e c tali che $a = b \times c$

quasi tutti i sistemi crittografici in uso oggi sono basati sull'assunzione che fattorizzare numeri grandi e' molto difficile (anche se e' semplice verificare la soluzione: basta moltiplicare i due numeri)

NON e' difficile per un quantum computer!

Questa fu la scoperta (Peter Shor) che fece decollare la computazione quantistica

Oggi abbiamo vari protocolli crittografici post-quantum: sicuri anche contro un quantum computer

Grover search: ricerca in un database non strutturato



Grover search: ricerca in un database non strutturato

dal numero di telefono devo cercare in un elenco telefonico il nome associato



Grover search: ricerca in un database non strutturato

dal numero di telefono devo cercare in un elenco telefonico il nome associato

e' utile anche per velocizzare la soluzione di problemi dove e' difficile calcolare una soluzione, ma e' facile verificare se ho trovato una soluzione (problemi NP):



Grover search: ricerca in un database non strutturato

dal numero di telefono devo cercare in un elenco telefonico il nome associato

e' utile anche per velocizzare la soluzione di problemi dove e' difficile calcolare una soluzione, ma e' facile verificare se ho trovato una soluzione (problemi NP):

Provo tutte le possibili soluzioni sequenzialmente!



simulazione di sistemi quantistici



simulazione di sistemi quantistici

La dimensione dello spazio degli stati di un sistema quantistico aumenta esponenzialmente con il numero di gradi di liberta'.



simulazione di sistemi quantistici

La dimensione dello spazio degli stati di un sistema quantistico aumenta esponenzialmente con il numero di gradi di liberta'.

Impossibile simulare sistemi quantistici mediamente complicati su computer classici:

lo stato di 300 qubits e' descritto da 2^{300} numeri!



esistono quantum computer?



esistono quantum computer?

Non ancora!



esistono quantum computer?

Non ancora!

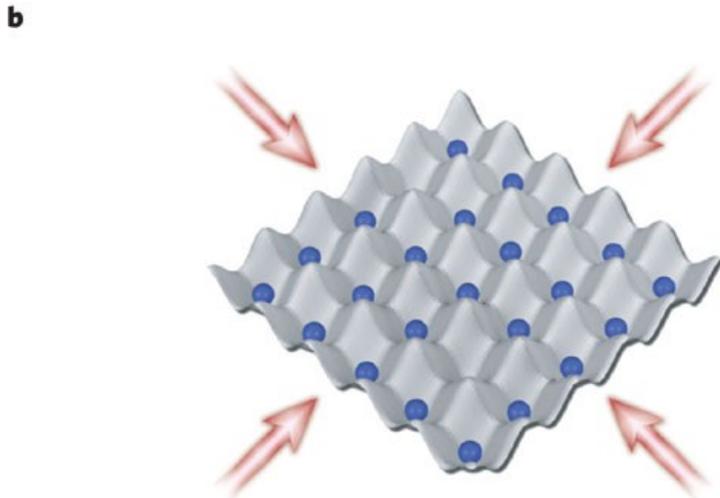
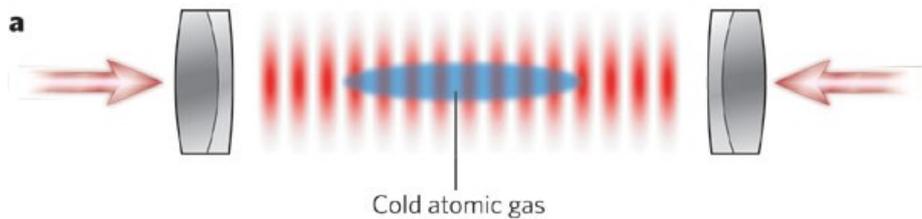
Molti gruppi stanno cercando di creare un quantum computer: non e' ancora chiaro quale sia la tecnologia piu' promettente



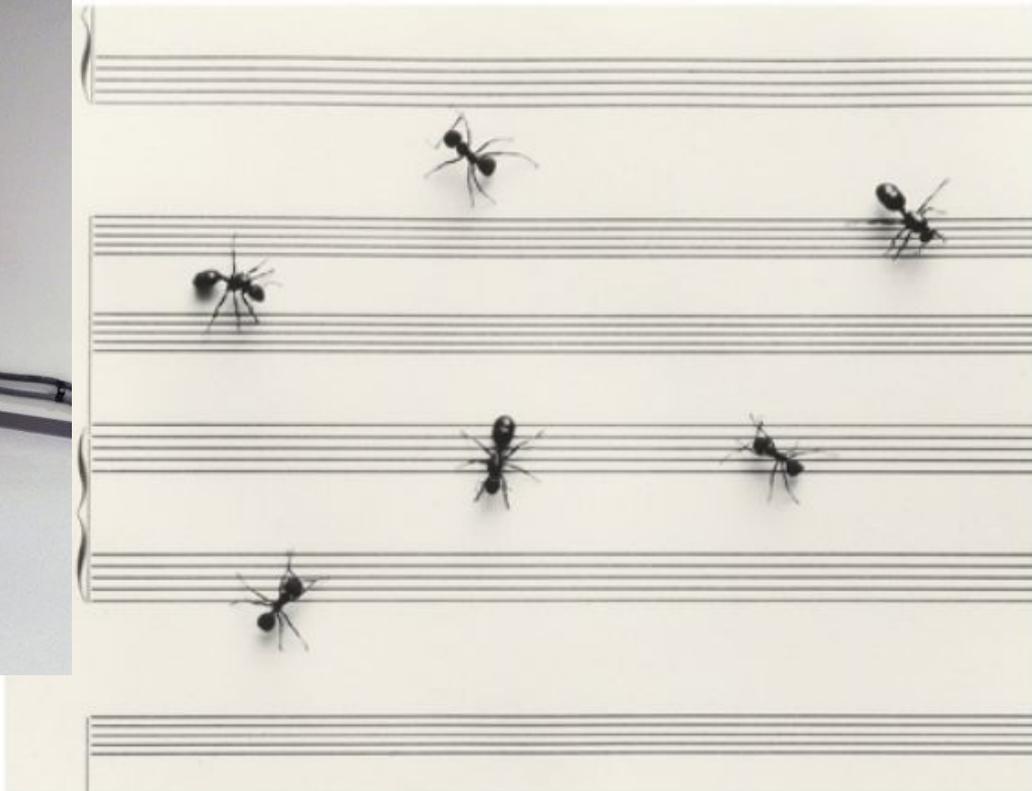
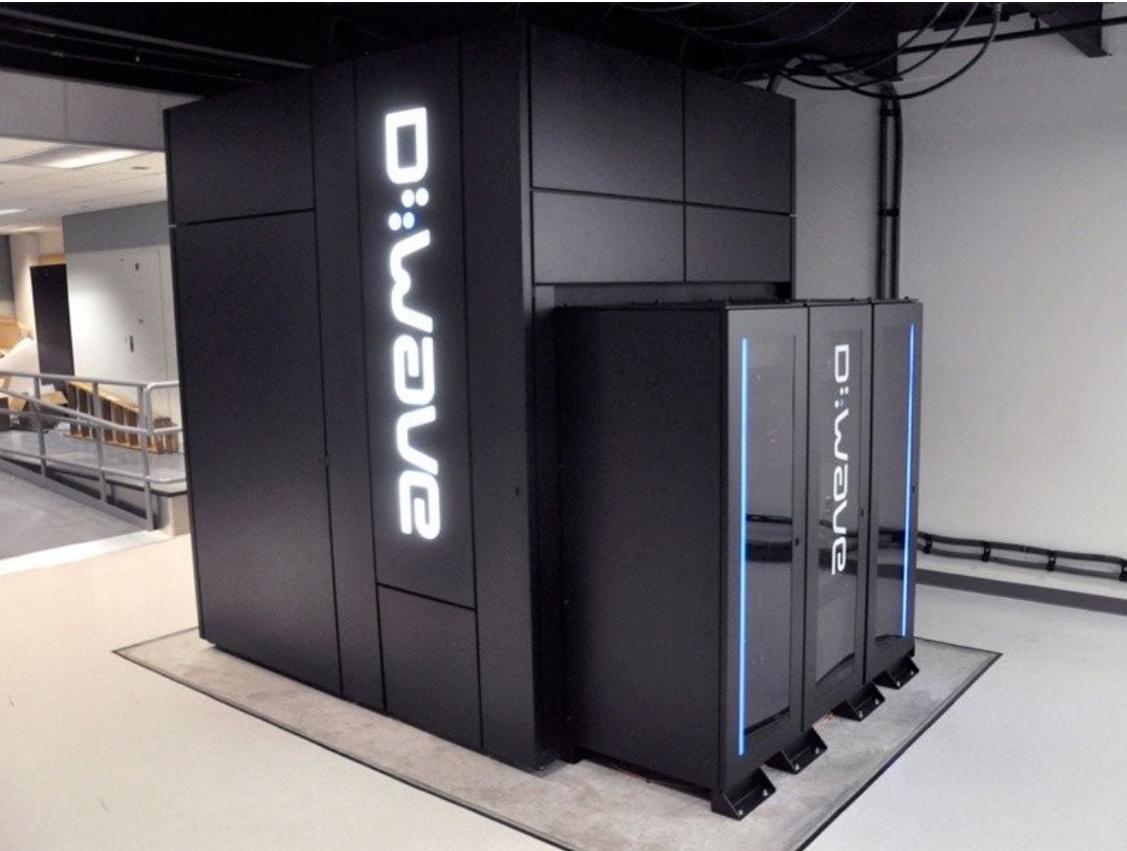
esistono quantum computer?

Non ancora!

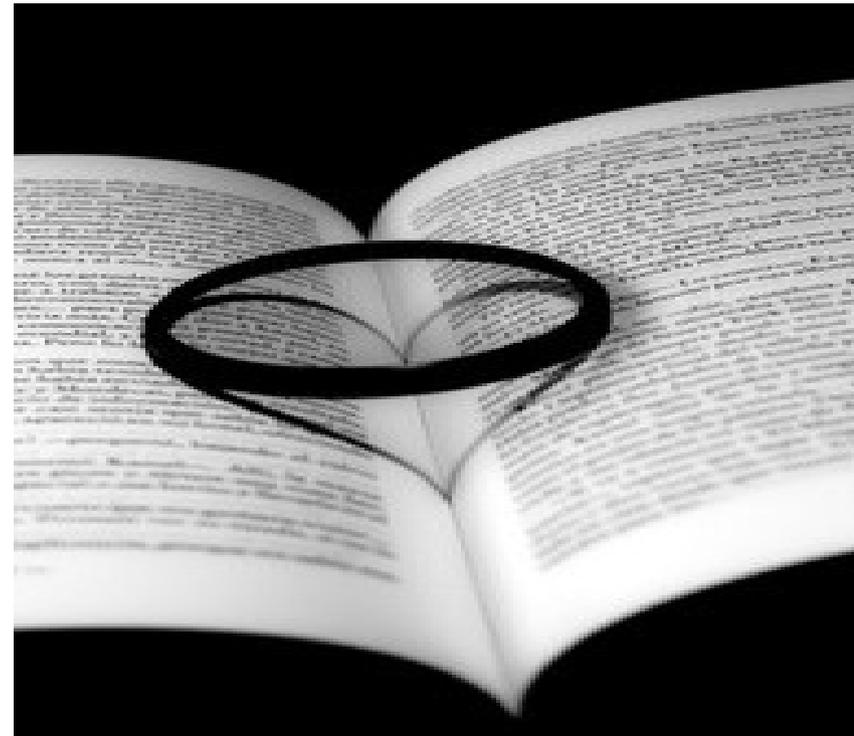
Molti gruppi stanno cercando di creare un quantum computer: non e' ancora chiaro quale sia la tecnologia piu' promettente forse optical lattice?



Oggi esistono molti prototipi: Dwave, rigetti, google, ibm, amazon braket.



quando avremo un vero quantum computer?



quando avremo un vero quantum computer?

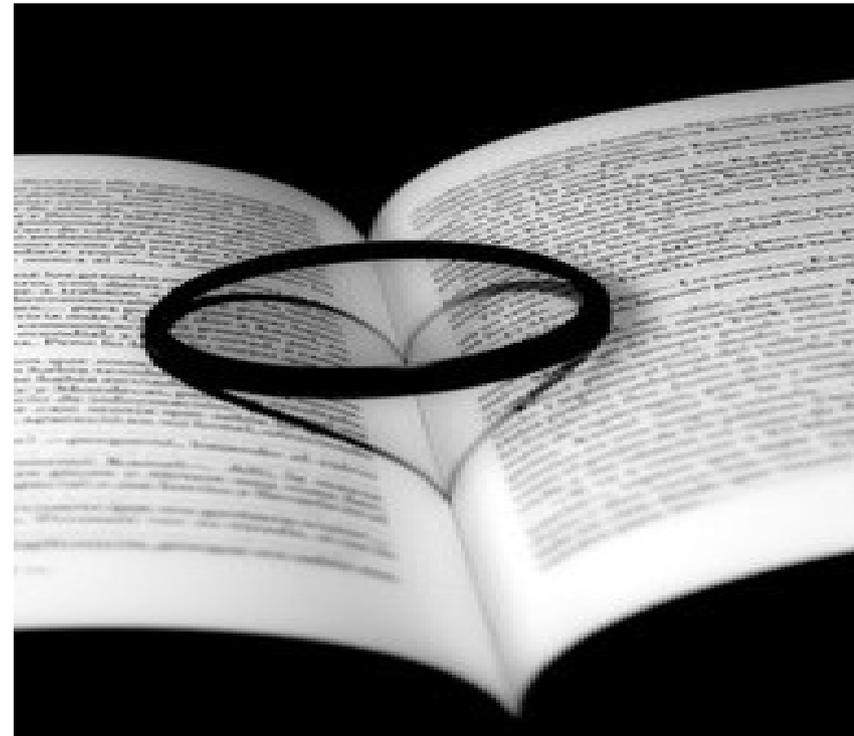
Non lo so



quando avremo un vero quantum computer?

Non lo so

Difficile fare previsioni sulla tecnologia senza rendersi ridicoli!



quando avremo un vero quantum computer?

Non lo so

Difficile fare previsioni sulla tecnologia senza rendersi ridicoli!

"I think there is a world market for maybe five computers."

Thomas Watson,
president of IBM



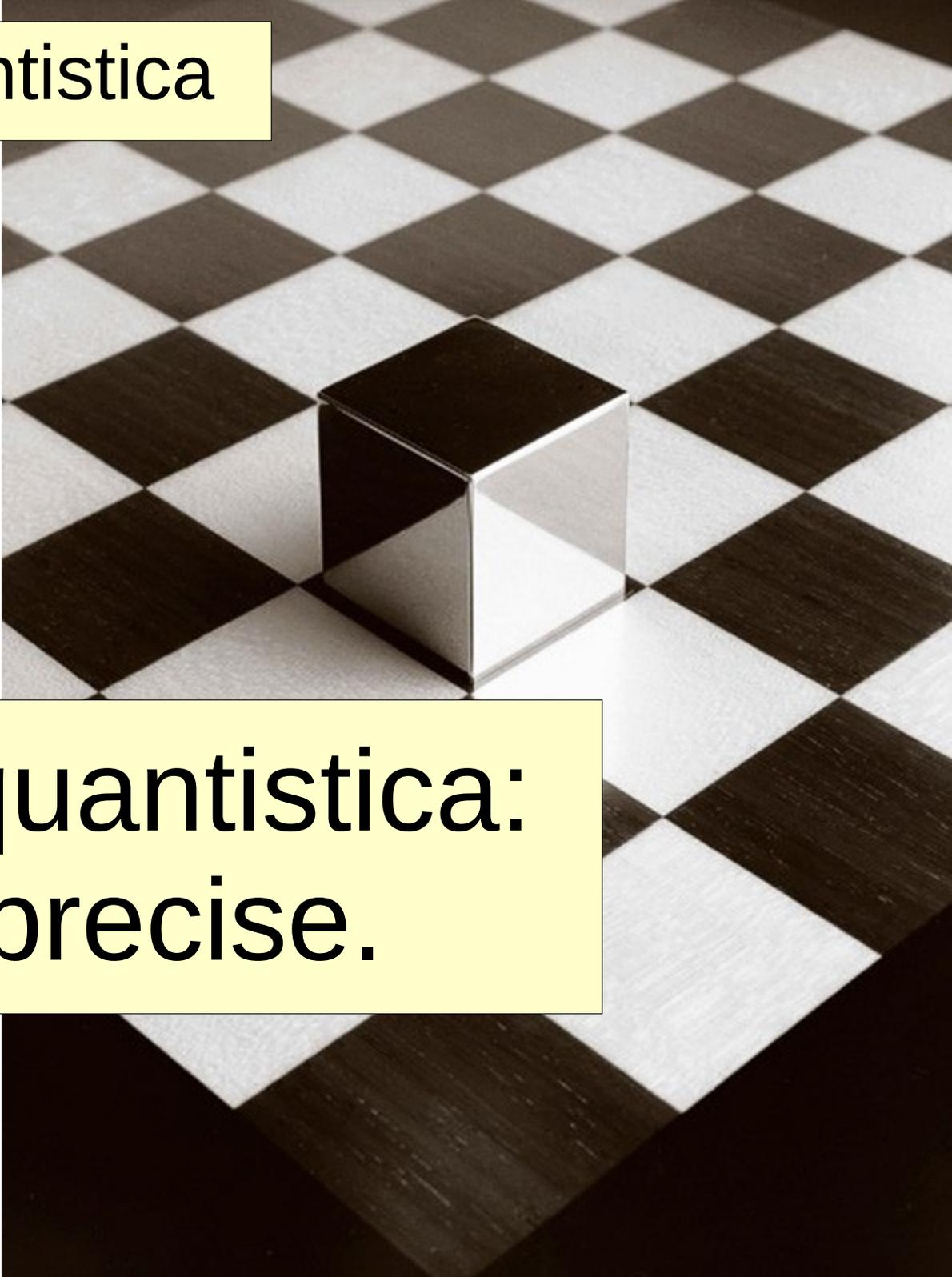
i miei risultati in quantum computation

Quantum RAM: memoria quantistica ad accesso casuale (brevettata).

Quantum Private Queries: algoritmo per fare una ricerca su Google senza che Google possa sapere cosa hai cercato.

Blind quantum computation: Alice fa eseguire una computazione al computer di Bob ma lui (in controllo del computer) non puo' sapere cosa lei ha calcolato.

Altra tecnologia quantistica

A 3D rendering of a metallic cube with a brushed metal texture, positioned on a black and white checkered floor. The perspective is from a slightly elevated angle, looking down at the cube. The floor tiles are diamond-shaped and recede into the distance, creating a strong sense of depth and perspective. The lighting is soft, casting a subtle shadow from the cube onto the floor.

Metrologia quantistica:
misure ultraprecise.

Cos'è una misurazione? 3 stadi

Cos'e' una misurazione? 3 stadi

1. Preparazione dell'apparato di misura



Cos'e' una misurazione? 3 stadi

1. Preparazione dell'apparato di misura



2. Interazione con l'oggetto da misurare



Cos'e' una misurazione? 3 stadi

1. Preparazione dell'apparato di misura



2. Interazione con l'oggetto da misurare



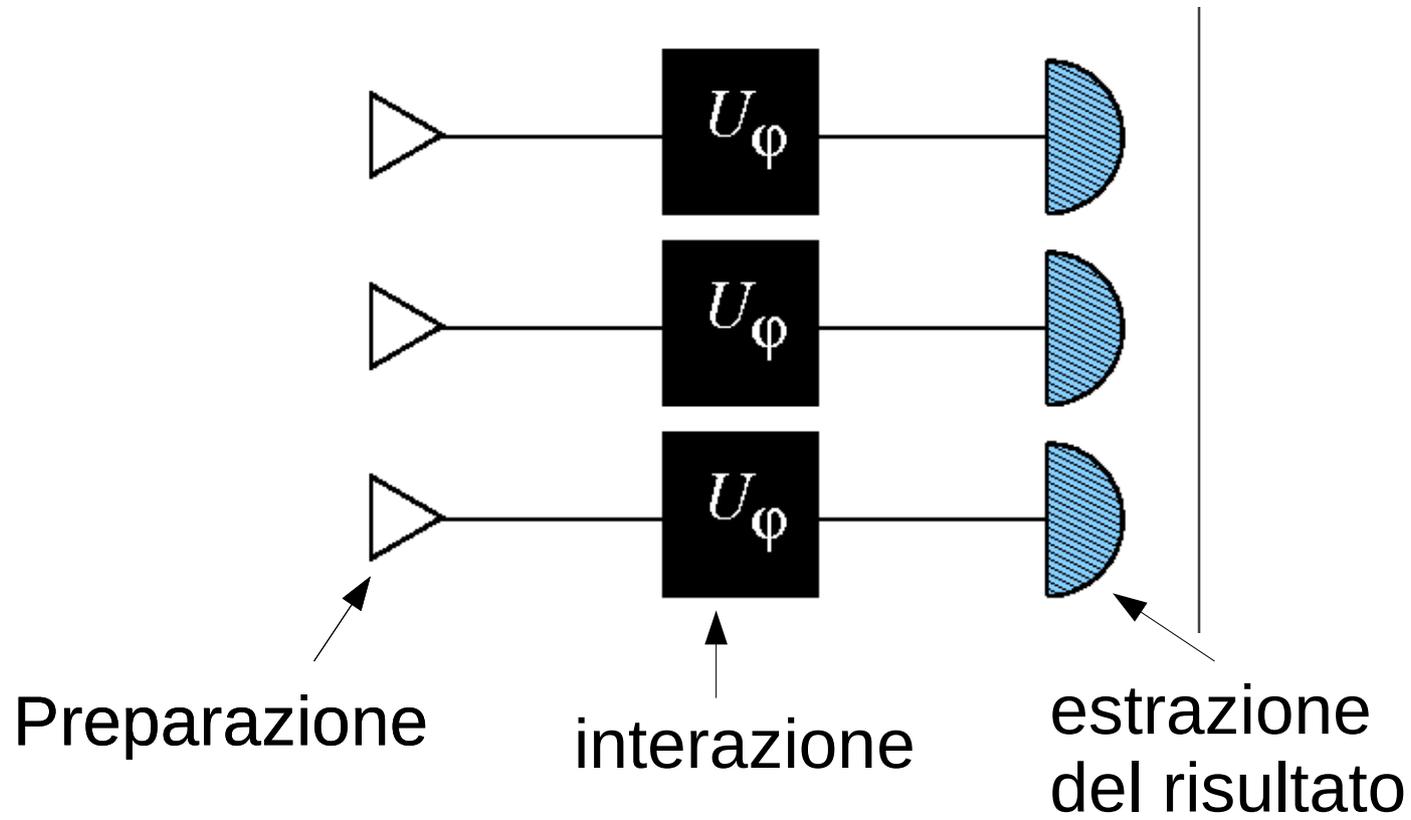
3. Estrazione del risultato



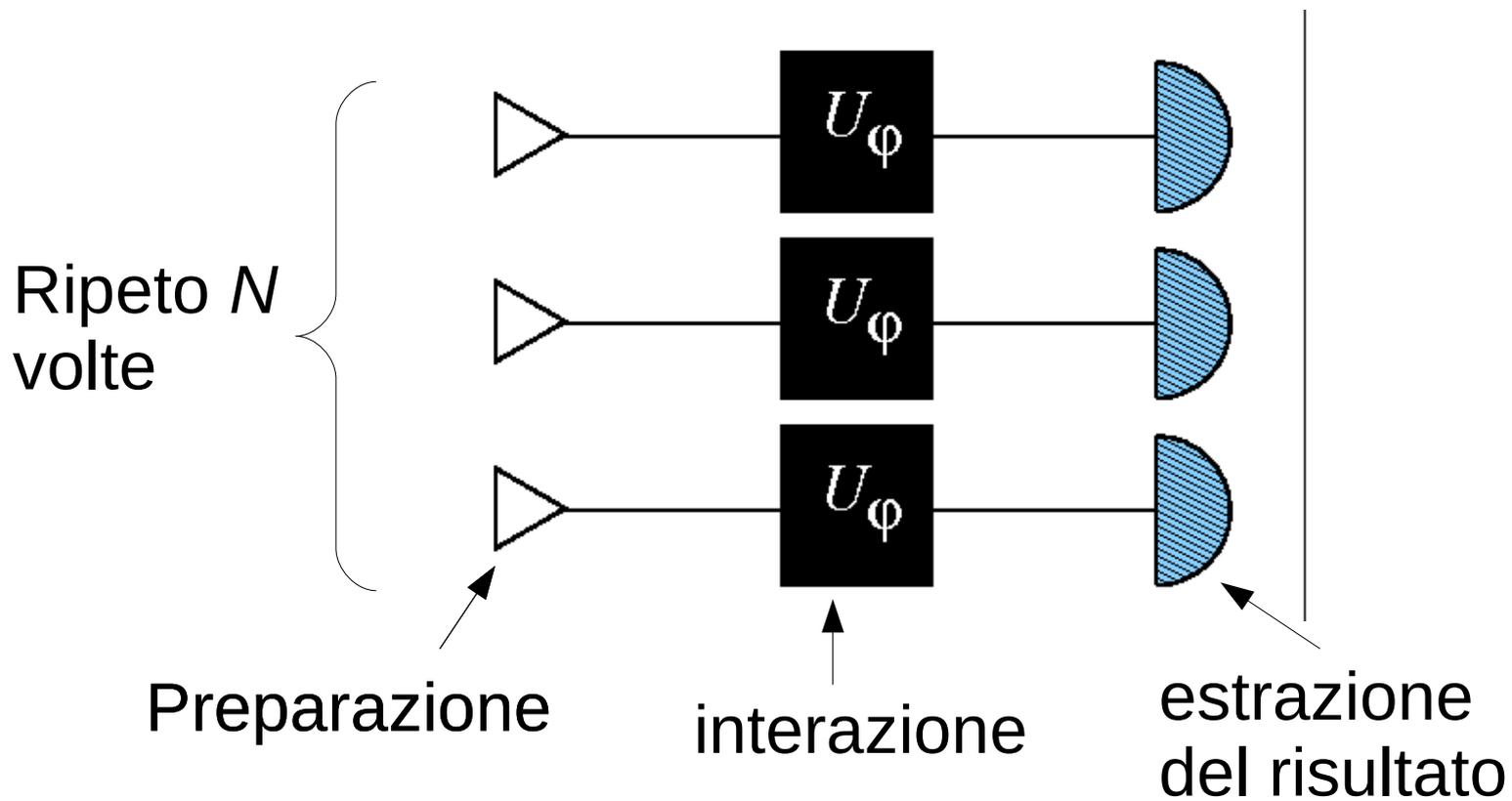
(4. Ripetere piu' volte per ridurre gli errori statistici)



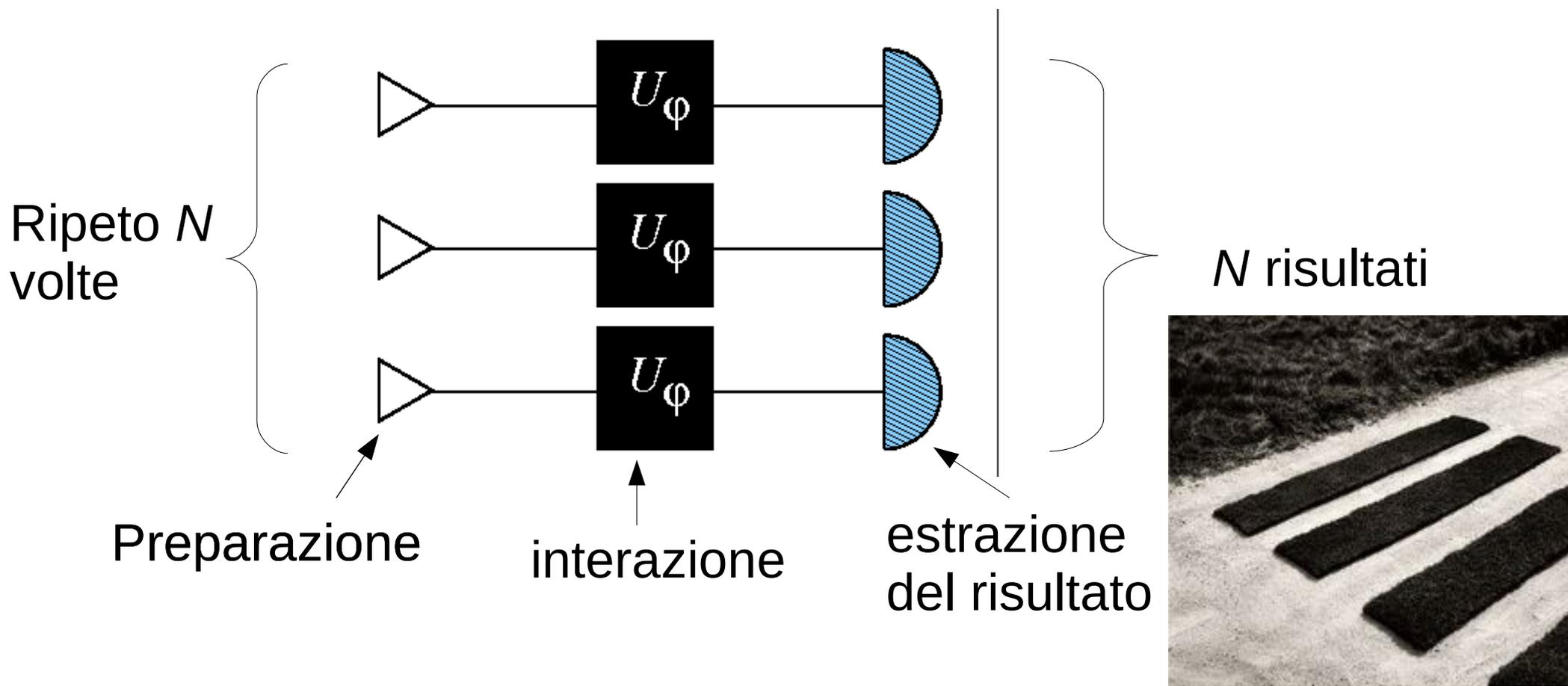
(4. Ripetere piu' volte per ridurre gli errori statistici)



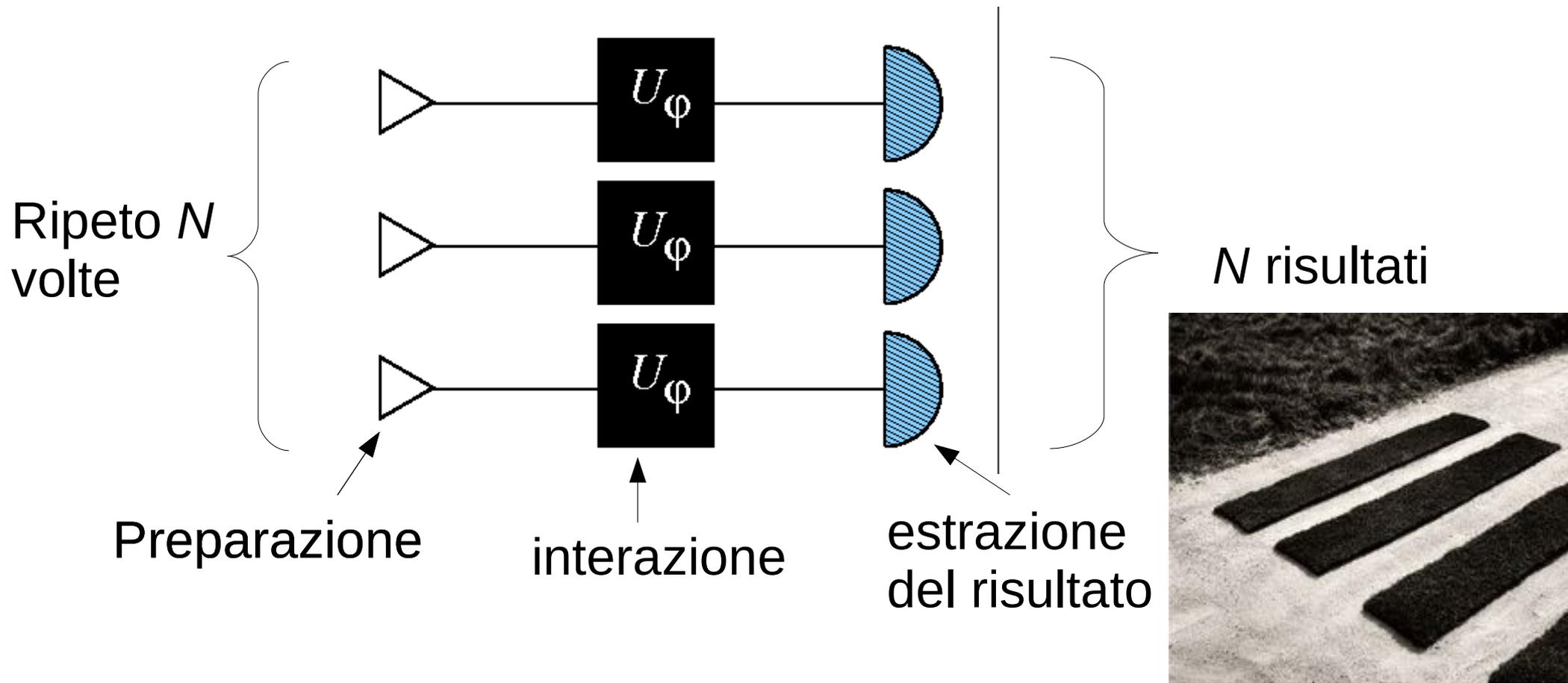
(4. Ripetere piu' volte per ridurre gli errori statistici)



(4. Ripetere piu' volte per ridurre gli errori statistici)

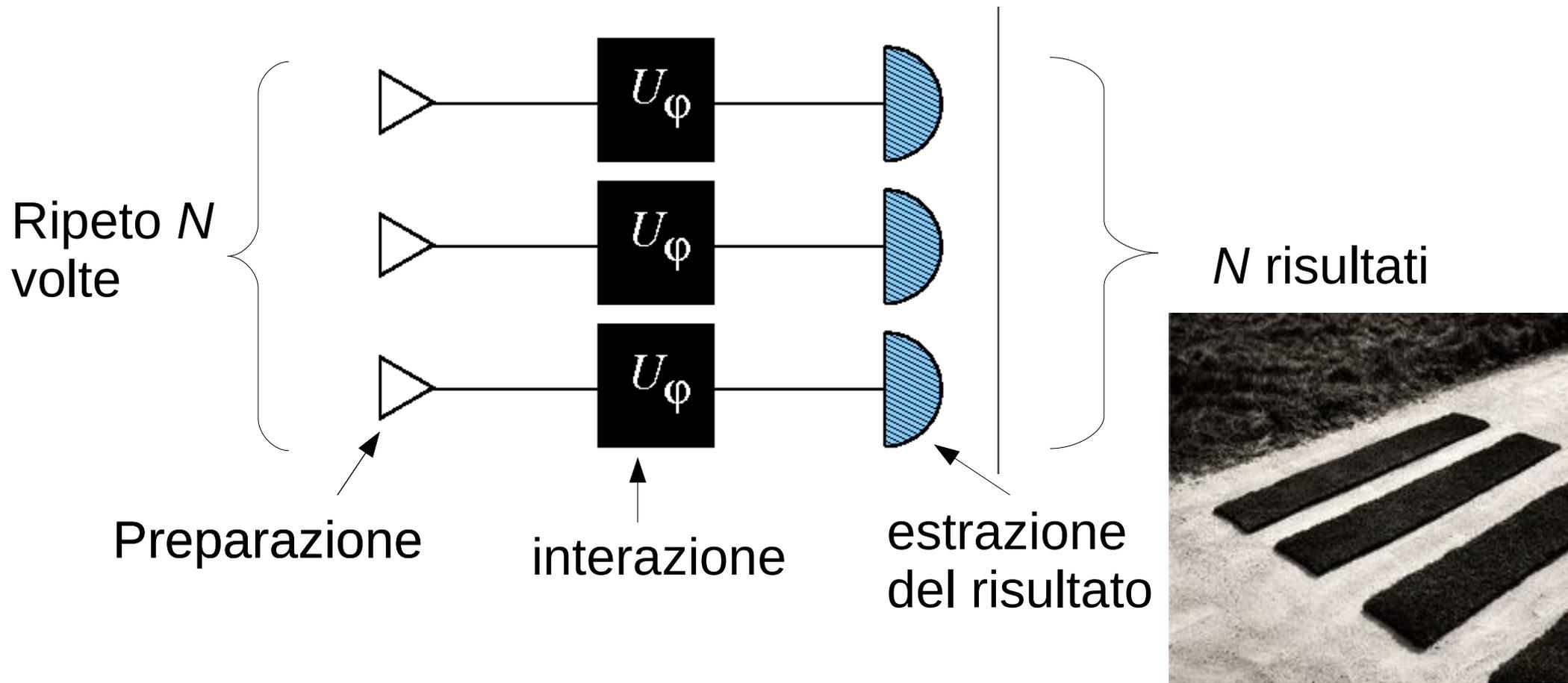


(4. Ripetere piu' volte per ridurre gli errori statistici)



Risultato finale: media dei risultati.

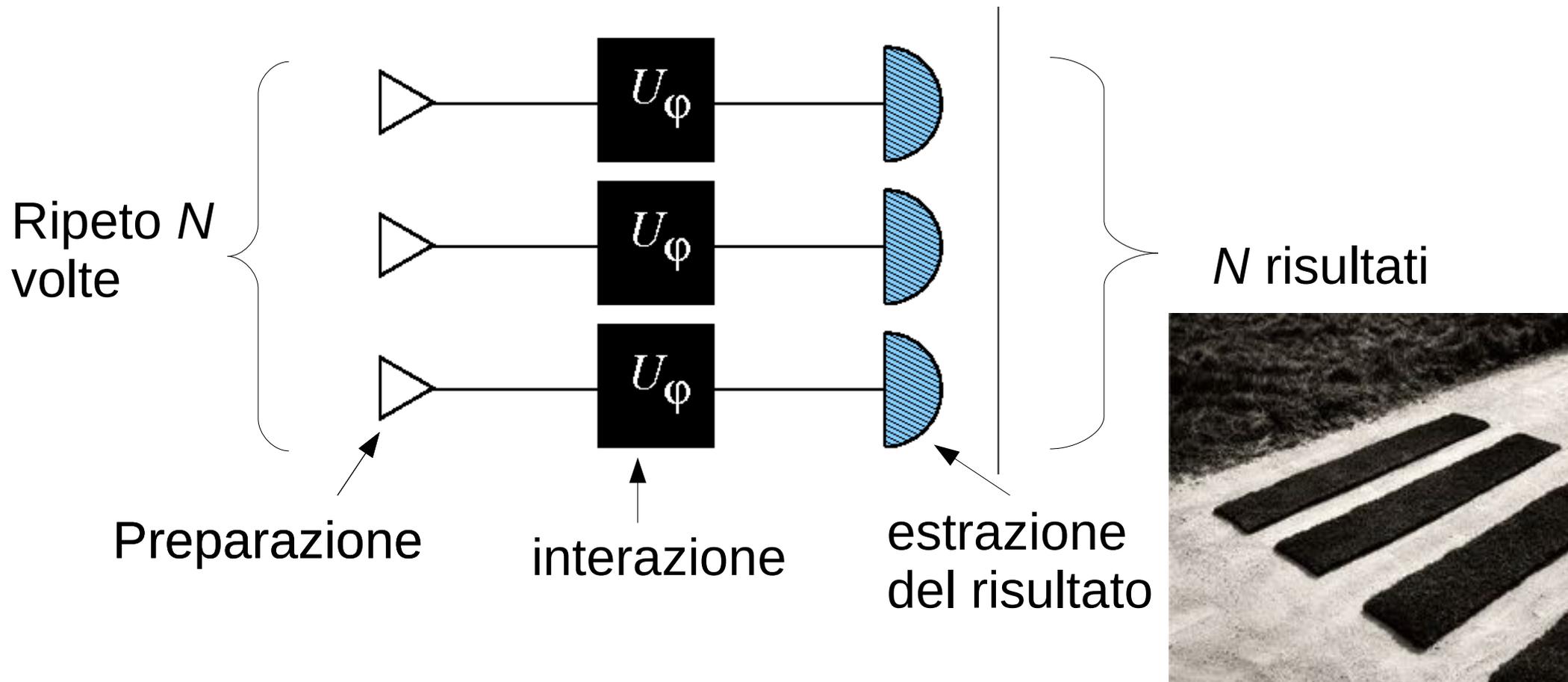
(4. Ripetere piu' volte per ridurre gli errori statistici)



Risultato finale: media dei risultati.

Errore?

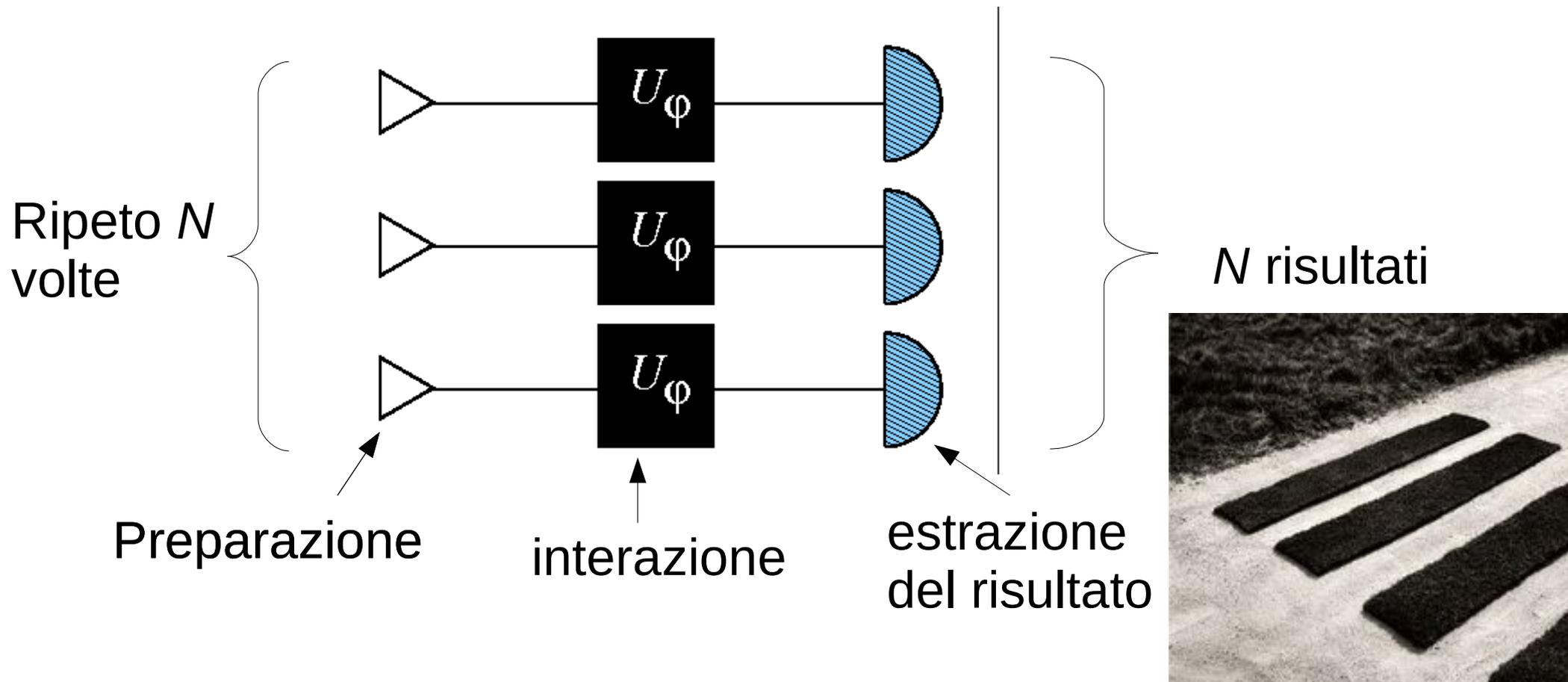
(4. Ripetere piu' volte per ridurre gli errori statistici)



Risultato finale: media dei risultati.

Errore? $\Delta\varphi \propto \frac{1}{\sqrt{N}}$

(4. Ripetere piu' volte per ridurre gli errori statistici)



Risultato finale: media dei risultati.

Errore? $\Delta\varphi \propto \frac{1}{\sqrt{N}}$ (teorema del limite centrale)

Errore $\rightarrow \Delta\varphi \propto \frac{1}{\sqrt{N}}$ (standard quantum limit)

posso fare meglio?



Errore $\rightarrow \Delta\varphi \propto \frac{1}{\sqrt{N}}$ (standard quantum limit)

posso fare meglio?

SI'!!

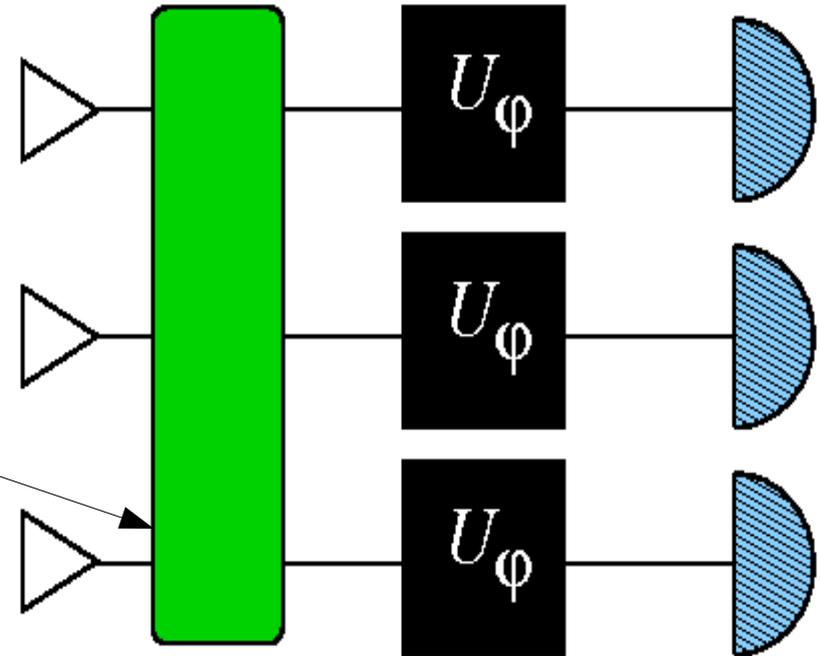


Errore $\rightarrow \Delta\varphi \propto \frac{1}{\sqrt{N}}$ (standard quantum limit)

posso fare meglio?

SI'!!

se uso **entanglement**
tra gli apparati di
misura

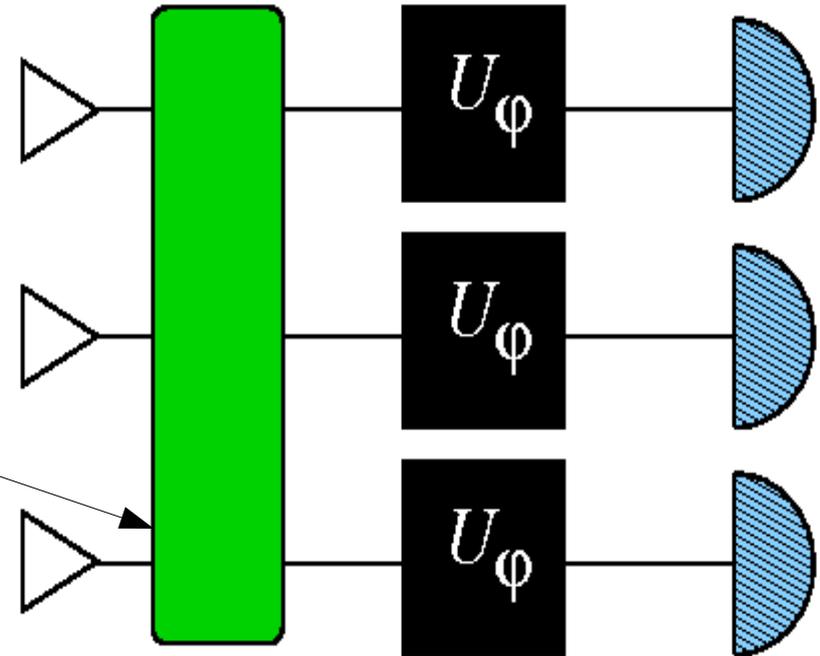


Errore $\rightarrow \Delta\varphi \propto \frac{1}{\sqrt{N}}$ (standard quantum limit)

posso fare meglio?

SI'!!

se uso **entanglement**
tra gli apparati di
misura



posso ridurre l'errore

a $\Delta\varphi \propto \frac{1}{N}$

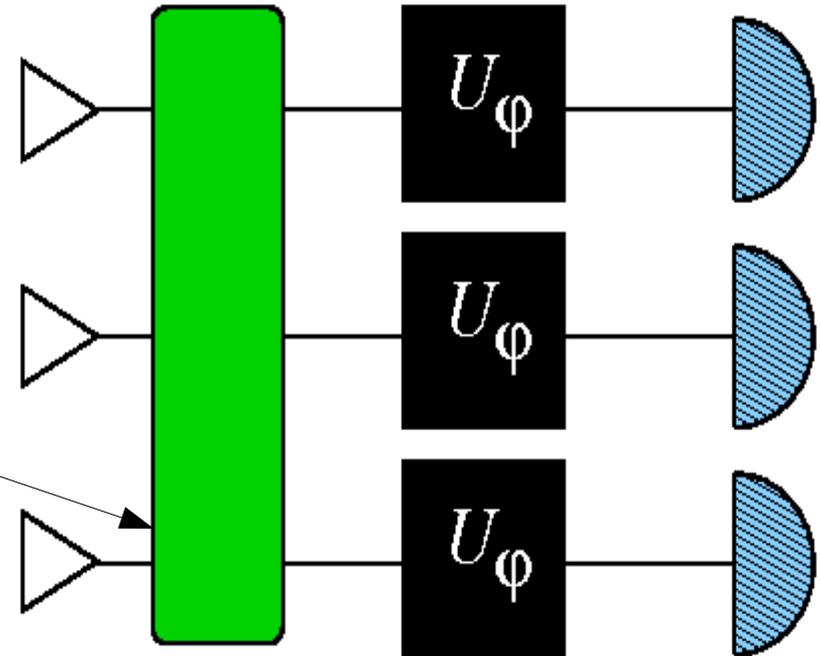


Errore $\rightarrow \Delta\varphi \propto \frac{1}{\sqrt{N}}$ (standard quantum limit)

posso fare meglio?

SI'!!

se uso **entanglement**
tra gli apparati di
misura



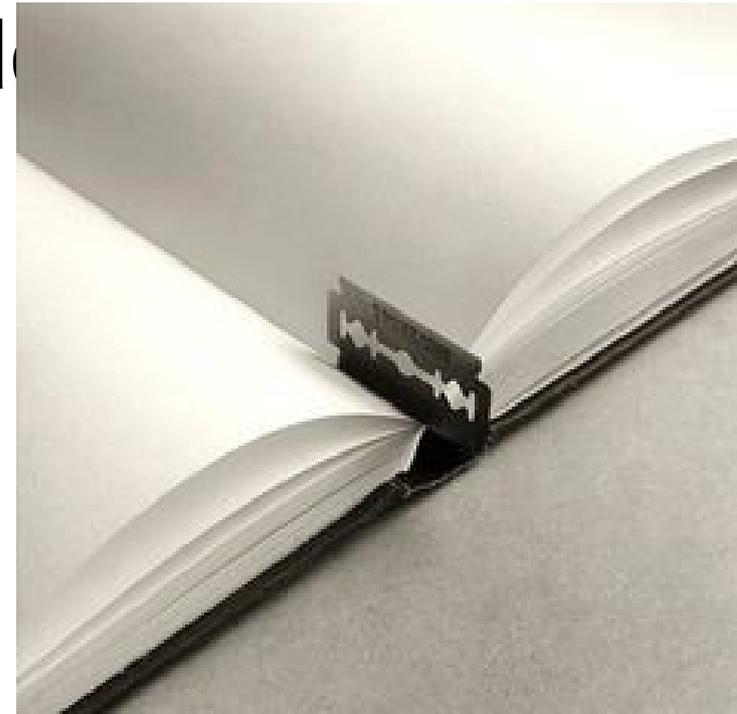
posso **ridurre** l'errore

a $\Delta\varphi \propto \frac{1}{N}$ (Heisenberg bound)



Tecniche applicabili a qualunque tipo di misura!!

- Misura di posizione e tempo (quantum gps)
- Misure interferometriche (onde)
- Orologi atomici
- etc.



Altra tecnologia quantistica

Telecomunicazioni
quantistiche



Quanta informazione posso trasmettere?



Quanta informazione posso trasmettere?

Perche' costano cosi' tanto i gigabyte del mio telefono?

Perche' non posso scaricare da internet un film in 1 secondo?



Quanta informazione posso trasmettere?

Perche' costano cosi' tanto i gigabyte del mio telefono?

Perche' non posso scaricare da internet un film in 1 secondo?

Capacita' di canale



Quanta informazione posso trasmettere?

Perche' costano cosi' tanto i gigabyte del mio telefono?

Perche' non posso scaricare da internet un film in 1 secondo?

Capacita' di canale

misura la capacita' di un canale di comunicazione (onde radio per il cellulare, cavo telefonico per l'adsl) di trasmettere informazione



segnali elettrici nel cavo telefonico=elettroni
onde radio=fotoni



segnali elettrici nel cavo telefonico=elettroni
onde radio=fotoni



l'informazione e' codificata in sistemi fisici

segnali elettrici nel cavo telefonico=elettroni
onde radio=fotoni



l'informazione e' codificata in sistemi fisici

quindi e' la fisica a dire quanta
informazione posso trasmettere!!

segnali elettrici nel cavo telefonico=elettroni
onde radio=fotoni

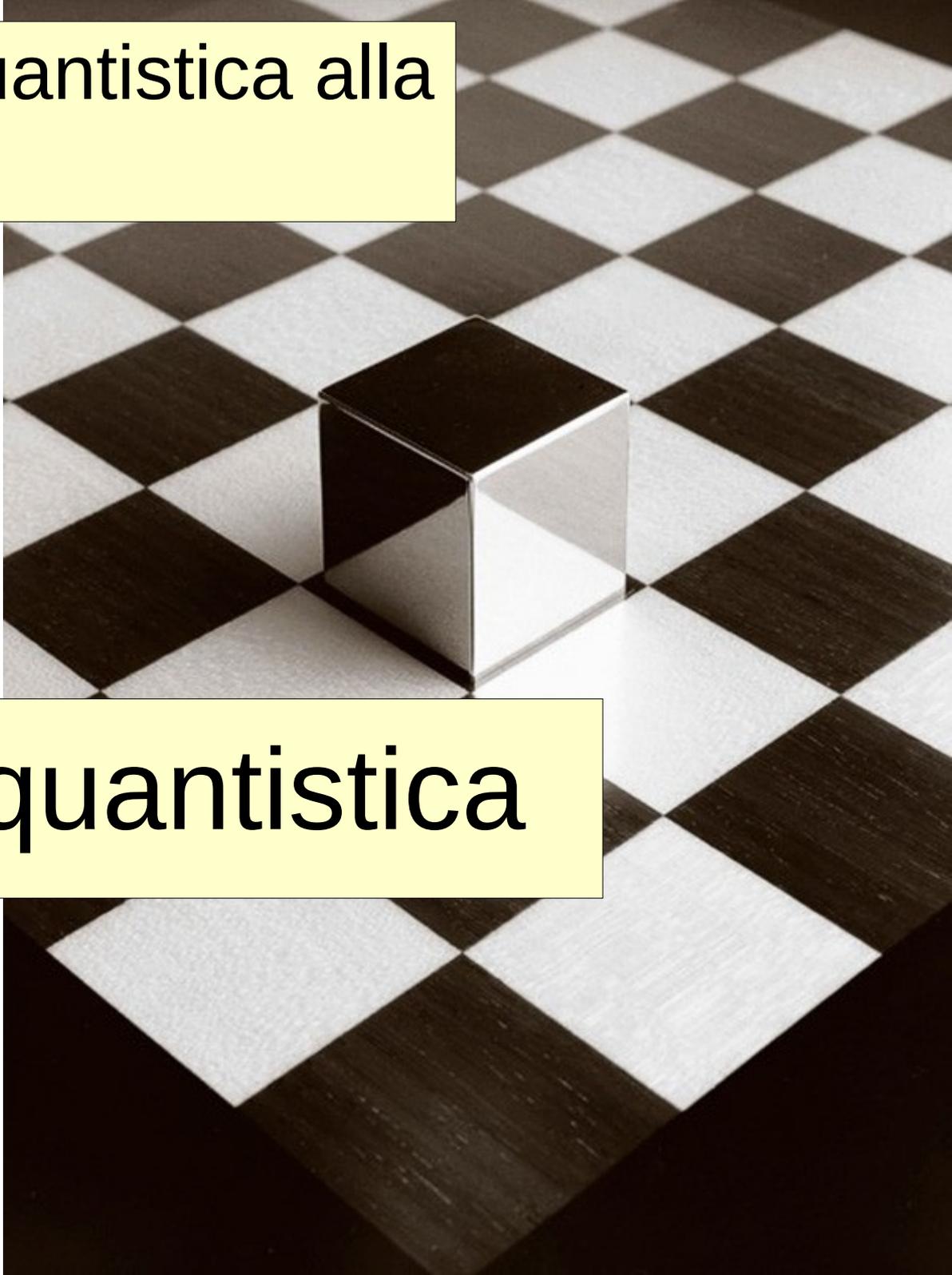


l'informazione e' codificata in sistemi fisici

**quindi e' la fisica a dire quanta
informazione posso trasmettere!!**

in telecomunicazioni siamo molto vicini ai limiti quantistici!
Ad esempio: in comunicazioni via satellite.

Altra applicazione quantistica alla
telecomunicazione

A 3D rendering of a metallic cube with a brushed metal texture, positioned on a black and white checkered floor. The cube is centered in the lower half of the image, casting a soft shadow on the floor. The checkered pattern recedes into the distance, creating a sense of depth.

Crittografia quantistica

tutti i sistemi crittografici in uso oggi (whatsapp)
si basano su assunzioni: **assumiamo che
l'avversario non sia abbastanza potente.**



tutti i sistemi crittografici in uso oggi (whatsapp)
si basano su assunzioni: **assumiamo che
l'avversario non sia abbastanza potente.**

(abbiamo già visto che se il nostro avversario
ha un computer quantistico siamo fritti!)



tutti i sistemi crittografici in uso oggi (whatsapp) si basano su assunzioni: **assumiamo che l'avversario non sia abbastanza potente.**

(abbiamo già visto che se il nostro avversario ha un computer quantistico siamo fritti!)

crittografia quantistica=sicurezza incondizionata



tutti i sistemi crittografici in uso oggi (whatsapp) si basano su assunzioni: **assumiamo che l'avversario non sia abbastanza potente.**

(abbiamo già visto che se il nostro avversario ha un computer quantistico siamo fritti!)

crittografia quantistica=sicurezza incondizionata

per scoprire i nostri segreti, l'avversario dovrebbe violare le leggi fisiche



tutti i sistemi crittografici in uso oggi (whatsapp) si basano su assunzioni: **assumiamo che l'avversario non sia abbastanza potente.**

(abbiamo già visto che se il nostro avversario ha un computer quantistico siamo fritti!)

crittografia quantistica=sicurezza incondizionata

per scoprire i nostri segreti, l'avversario dovrebbe violare le leggi fisiche

→ **impossibile!**



crittografia quantistica:
applicazione della
complementarieta'



**crittografia quantistica:
applicazione della
complementarieta'**



codificate l'informazione su un sistema che puo' avere due possibili valori complementari e fate in modo che solo il destinatario possa sapere quali sono

**crittografia quantistica:
applicazione della
complementarieta'**



codificate l'informazione su un sistema che puo' avere due possibili valori complementari e fate in modo che solo il destinatario possa sapere quali sono

L'avversario e' bloccato dal principio di indeterminazione!!!

Incondizionatamente
sicura?!



Incondizionatamente
sicura?!

Solo se l'implementazione e' corretta in tutto!



Incondizionatamente sicura?!

Solo se l'implementazione e' corretta in tutto!

La prima implementazione dimostrativa
era totalmente insicura:
l'apparato era rumorosissimo.

“click” se una proprieta'
“clock” se l'altra



Incondizionatamente sicura?!

Solo se l'implementazione e' corretta in tutto!

La prima implementazione dimostrativa
era totalmente insicura:
l'apparato era rumorosissimo.

“click” se una proprieta'
“clock” se l'altra

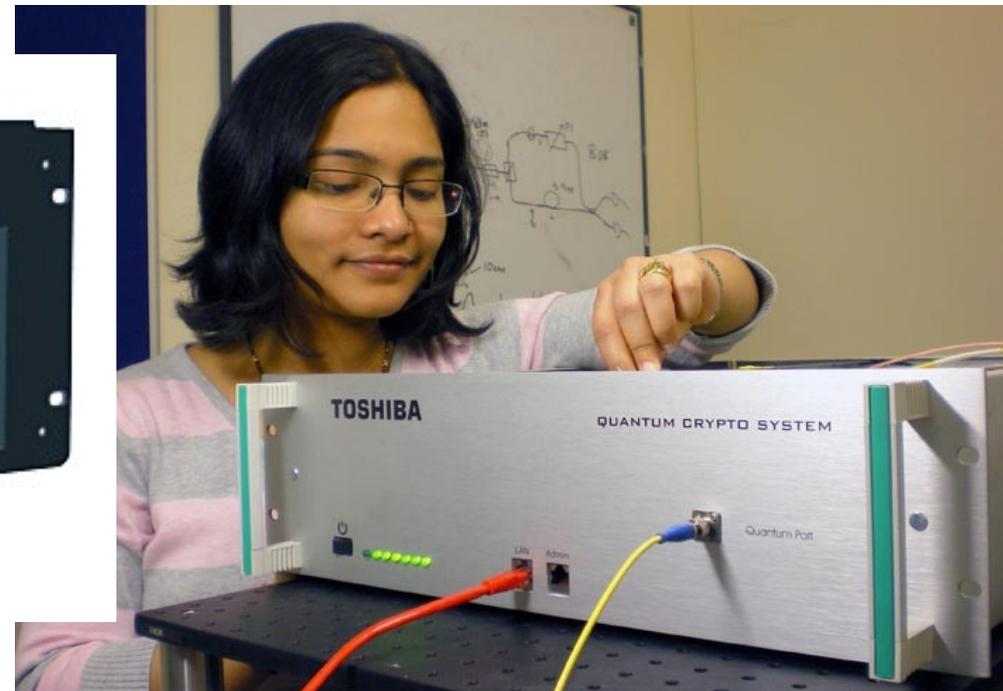


Bastava che l'avversario ascoltasse

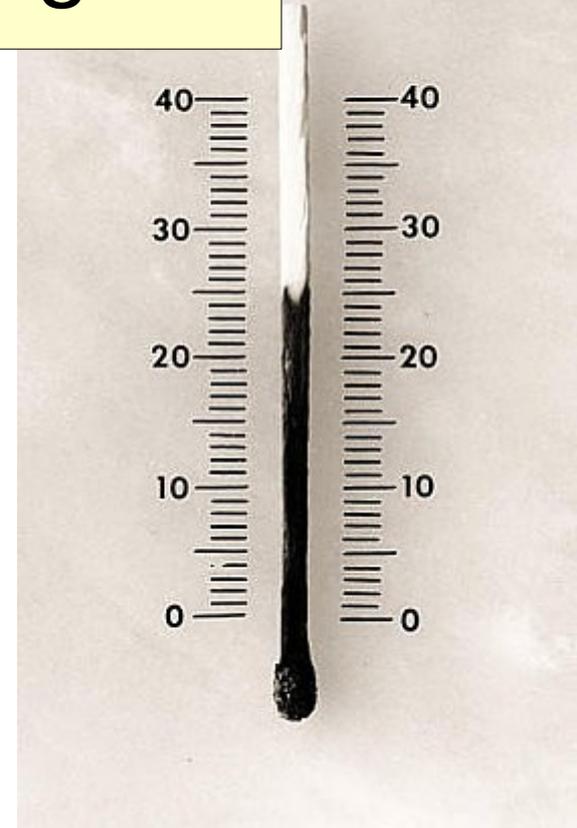
crittografia quantistica:
e' la tecnologia
quantistica piu' matura



esistono gia' implementazioni commerciali

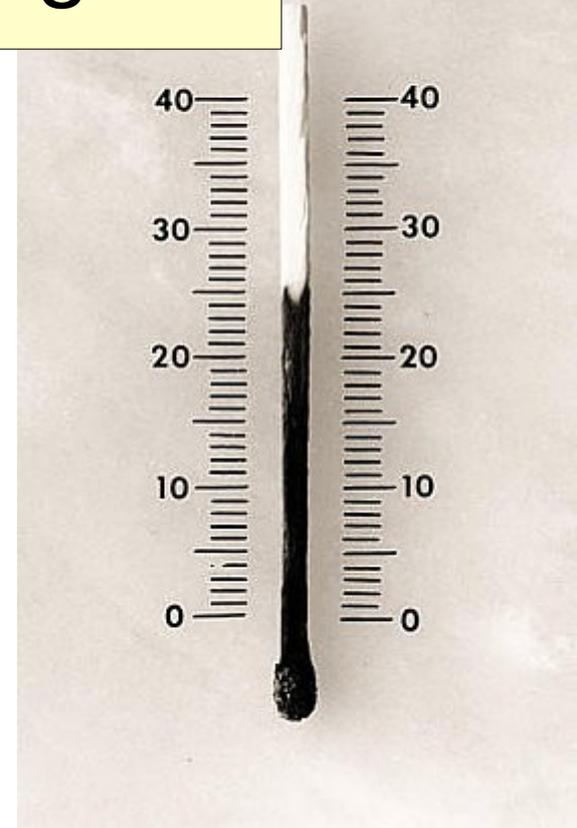


q. tech: solo una rivoluzione tecnologica?



q. tech: solo una rivoluzione tecnologica?

NO!

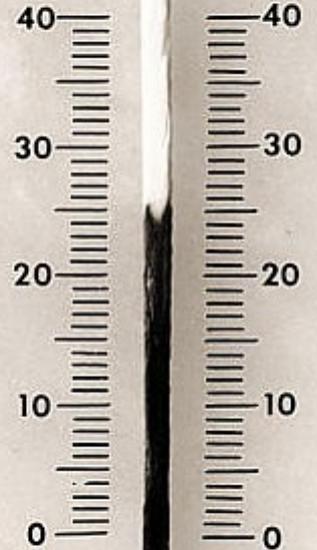


q. tech: solo una rivoluzione tecnologica?

NO!

analizzare la fisica dal punto di vista
dell'elaborazione di informazione:

rivoluzione anche a livello concettuale

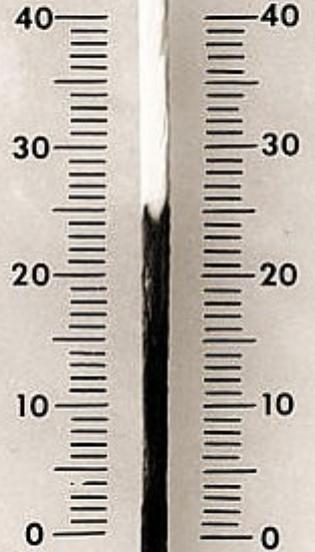


q. tech: solo una rivoluzione tecnologica?

NO!

analizzare la fisica dal punto di vista dell'elaborazione di informazione:

rivoluzione anche a livello concettuale

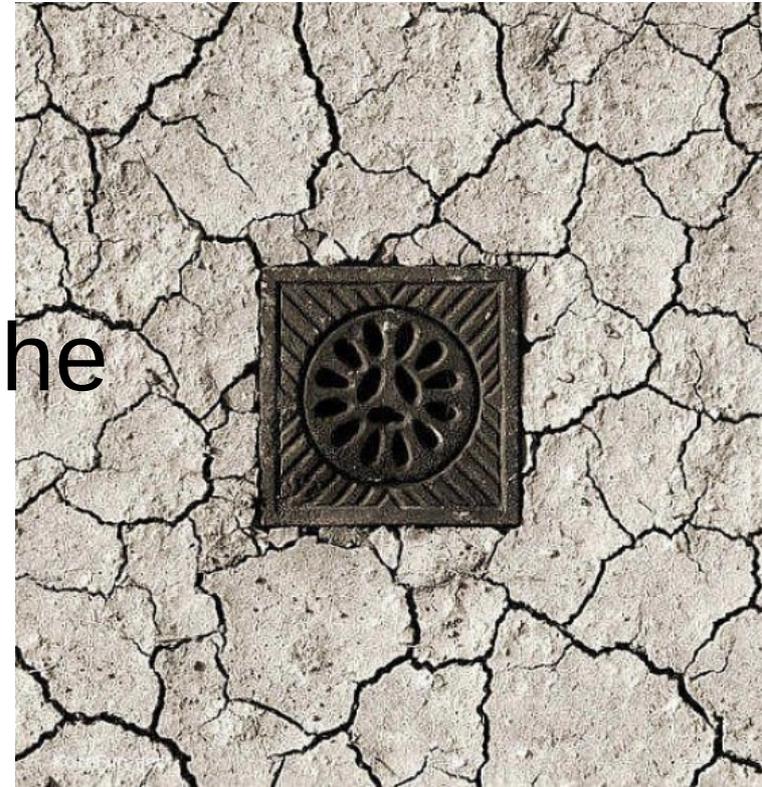


esempio: gravita' quantistica!

Le ultime idee sulla fisica quantistica dei buchi neri vengono dal pensare quali tipi di operazioni uno potrebbe fare con un buco nero.

Di cosa ho parlato?

- Le tecnologie quantistiche: perche' MQ e cosa sono
 - Il quantum computer:
usare qubits invece di bits
- Complementarieta' (o sovrapposizione) ed entanglement
 - Metrologia quantistica
 - telecomunicazioni quantistiche
- tq: rivoluzione tecnologica,
ma anche concettuale



Take home message

Lorenzo Maccone
maccone@unipv.it

[Figure: Chema Madoz]



**Quantum technology:
il futuro della tecnologia..
ma non solo!**



