



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore



# CRITTOGRAFIA QUANTISTICA

Stefania Pagliara

Dipartimento di Matematica e Fisica

[stefania.pagliara@unicatt.it](mailto:stefania.pagliara@unicatt.it)



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## COS'È LA CRITTOGRAFIA QUANTISTICA?

La crittografia quantistica è una forma avanzata di crittografia che si serve dei principi della meccanica quantistica per garantire la sicurezza delle comunicazioni.

Essa sfrutta la trasmissione di bit tramite emissione e rilevamento di singoli fotoni con diversa polarizzazione.





UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## QUALI SONO I VANTAGGI?

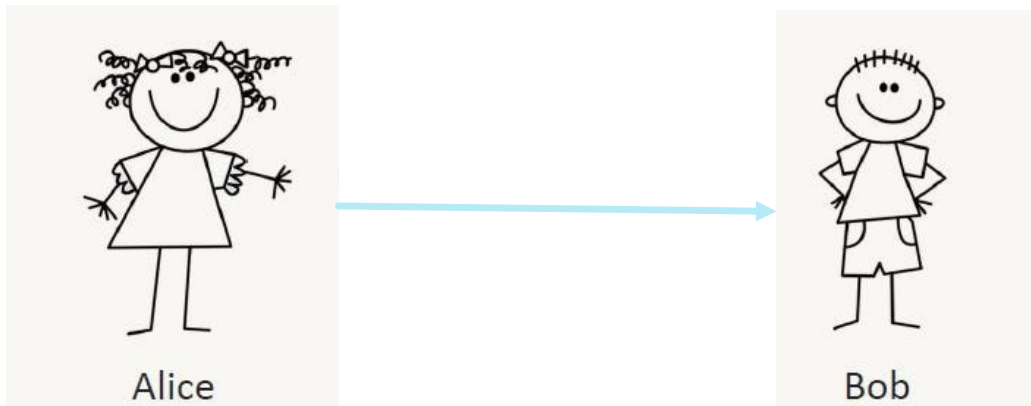


Con l'avvento dei computer quantistici è emersa la necessità di ideare un nuovo metodo crittografico, perché pratiche come la **fattorizzazione in numeri primi** potrebbero essere violate da algoritmi quantistici. Il vantaggio di questo nuovo metodo è che consente di rilevare qualsiasi tentativo di intercettazione delle informazioni trasmesse.



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## COME FUNZIONA?



**Alice** trasforma il testo in chiaro in un testo cifrato mediante un algoritmo di codifica

**Bob** estrae il testo in chiaro mediante un algoritmo di decodifica

Gli algoritmi di codifica e decodifica usano un'informazione segreta nota come chiave



# CRITTOGRAFIAMO UNA PAROLA

## Regole:

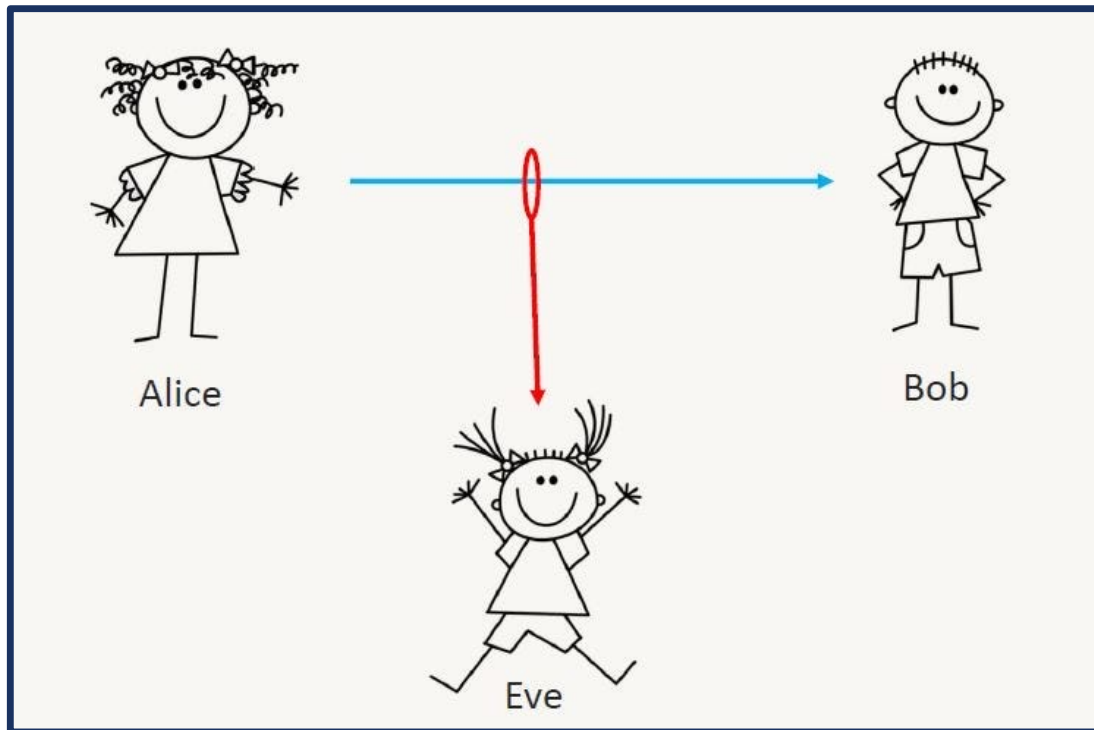
- $0 + 0 = 0$
- $1 + 0 = 1$
- $0 + 1 = 1$
- $1 + 1 = 0$

Alice	Word	T				E				S				T							
	Binary word	1	0	0	1	1	0	0	1	0	0	1	0	1	0	0	1	1			
		+																			
	Key (random)	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	0	1	
	Encrypted message	0	1	0	0	1	1	0	1	0	1	0	0	1	1	0	0	1	1	1	0
Bob		+																			
	Key (as above)	1	1	0	1	0	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
	Binary word	1	0	0	1	1	0	0	1	0	0	1	0	0	1	0	1	0	0	1	1
		+																			
	Word	T				E				S				T							



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# QUANTUM KEY DISTRIBUTION



## Protocollo BB84

(Charles H. Bennett e Gilles Brassard - 1984)

## PRINCIPIO DI KERCKHOFF

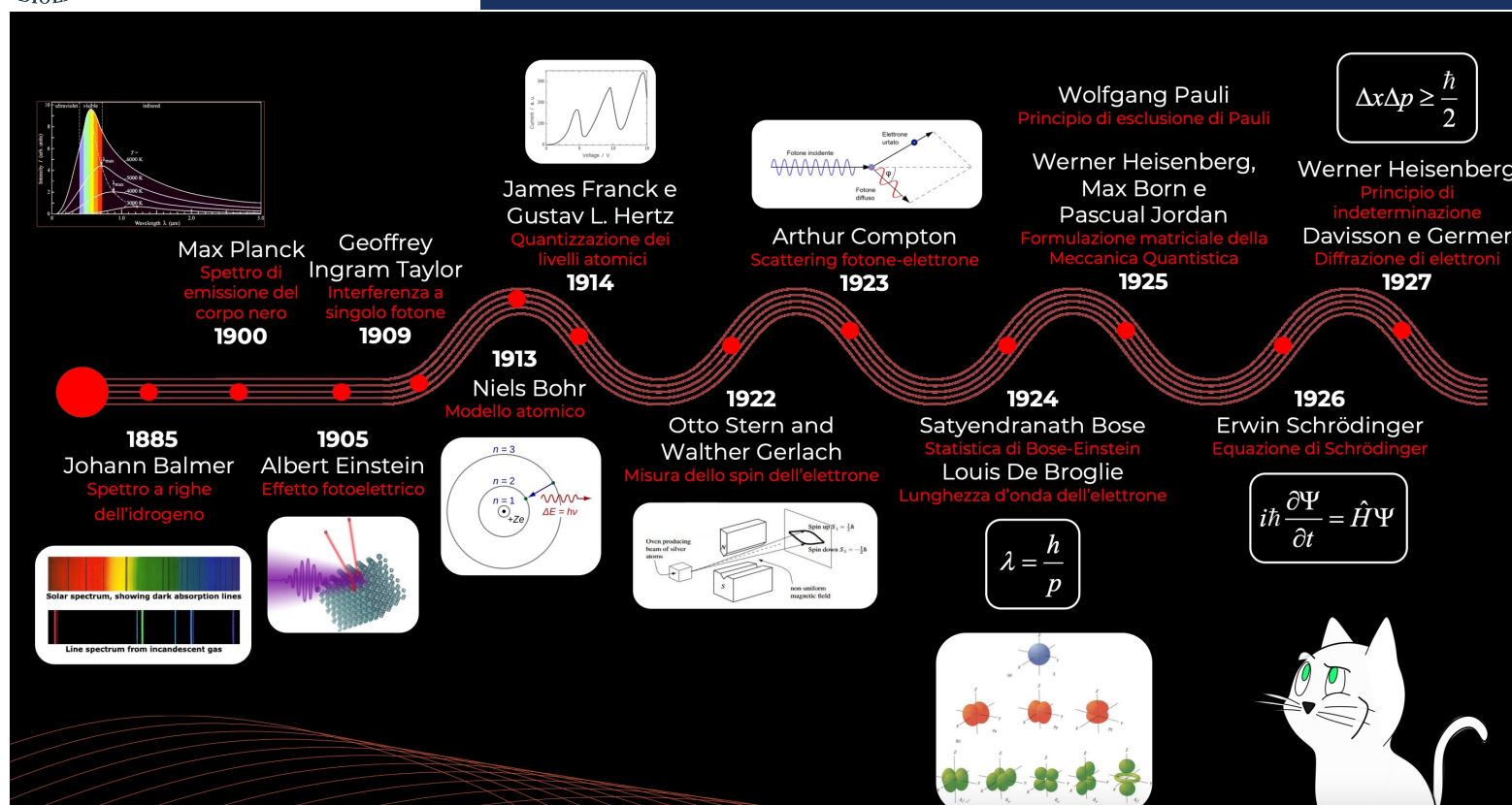
*la sicurezza di un sistema crittografico  
non dipende dalla segretezza dell'algoritmo,  
ma solo da quella della sua chiave.*

Come può la meccanica quantistica  
garantire la sicurezza della chiave?



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# VIAGGIO NELLA MECCANICA QUANTISTICA

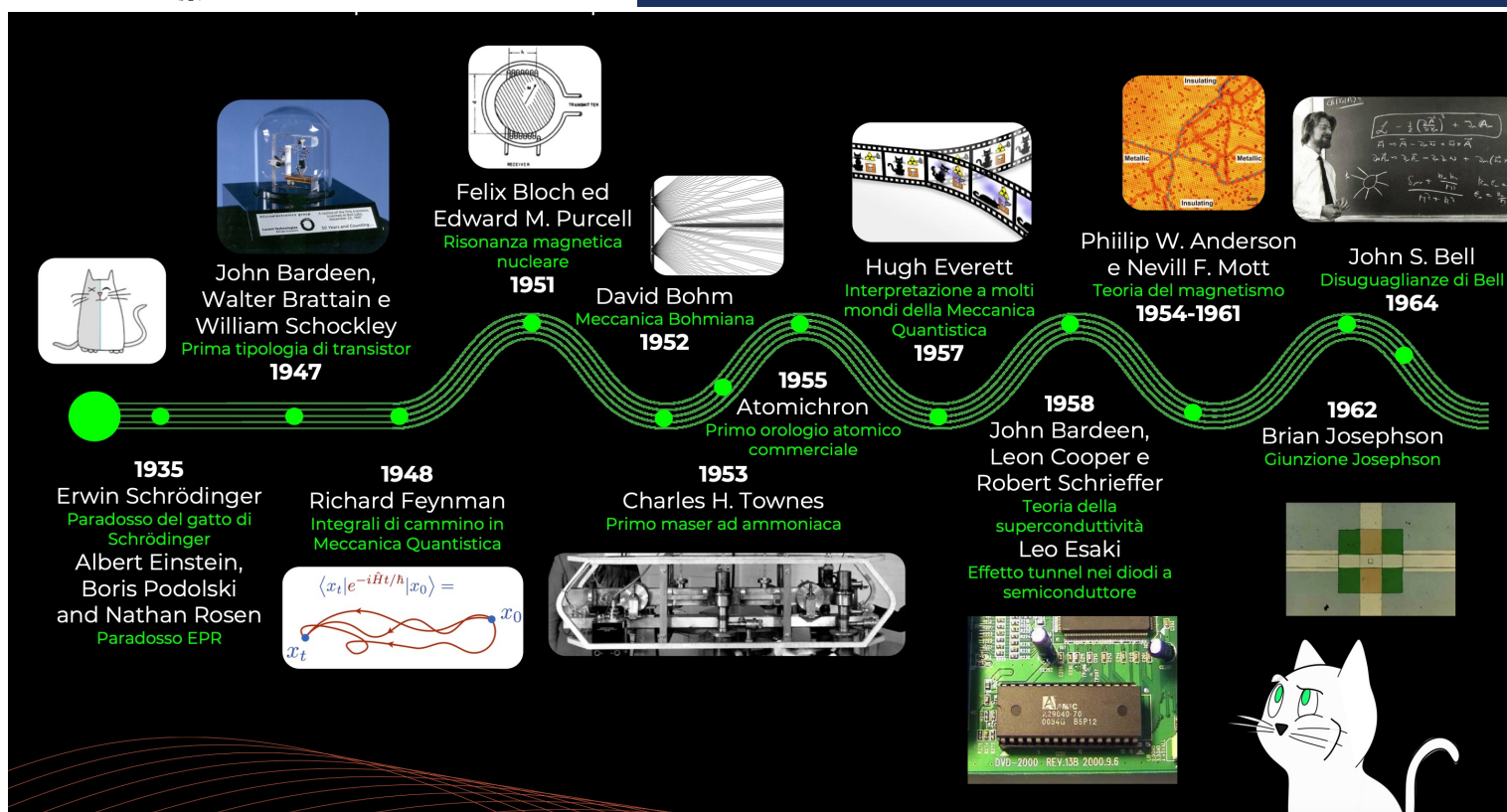


ITALIAN QUANTUM WEEKS



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# VIAGGIO NELLA MECCANICA QUANTISTICA



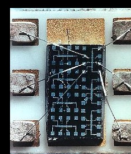
## LA PRIMA RIVOLUZIONE QUANTISTICA

ITALIAN QUANTUM WEEKS



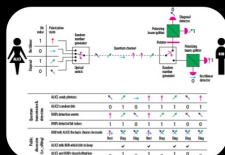
UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# VIAGGIO NELLA MECCANICA QUANTISTICA



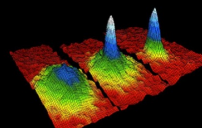
Klaus von Klitzing  
Effetto Hall Quantistico  
1980

Richard Feynman  
Simulazioni quantistiche  
1981

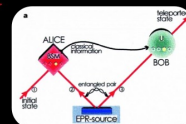


Charles Bennett e Gilles Brassard  
Protocollo crittografico BB84  
1984

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



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



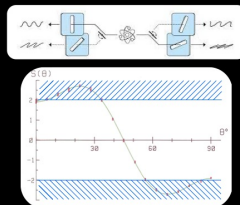
Anton Zeilinger e Sandu Popescu  
Prima realizzazione sperimentale del teletrasporto quantistico  
1997

Quantum Manifesto  
IBM-Quantum experience  
2016

D-Wave  
2011

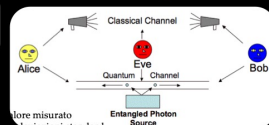
1982

Alain Aspect  
Violazione sperimentale delle disuguaglianze di Bell



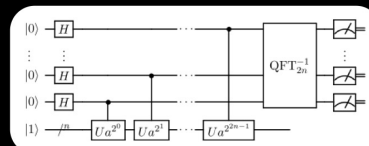
1991

Artur Ekert  
Protocollo crittografico E91



1994

Peter Shor  
Algoritmo di fattorizzazione



1996

Lov Grover  
Algoritmo quantistico di ricerca

2022

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

## LA SECONDA RIVOLUZIONE QUANTISTICA

ITALIAN QUANTUM WEEKS





UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# VIAGGIO NELLA MECCANICA QUANTISTICA

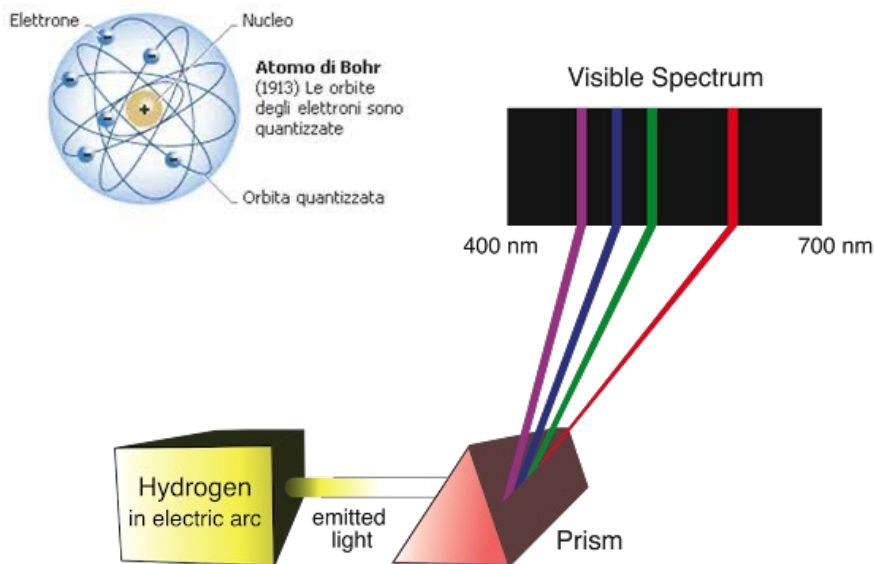
Dai primi esperimenti si capisce subito che:

I **corpi microscopici**, gli atomi, le molecole, gli elettroni, si comportano in modo completamente diverso da quanto previsto da tutte le leggi fisiche sino ad allora conosciute e da qualunque altra cosa si avesse esperienza.

**Leggi nuove ma anche di tipo nuovo, non deterministiche nel senso classico.**

«Chi non resta sbalordito dalla meccanica quantistica evidentemente non la capisce»

Niels Bohr, 1927



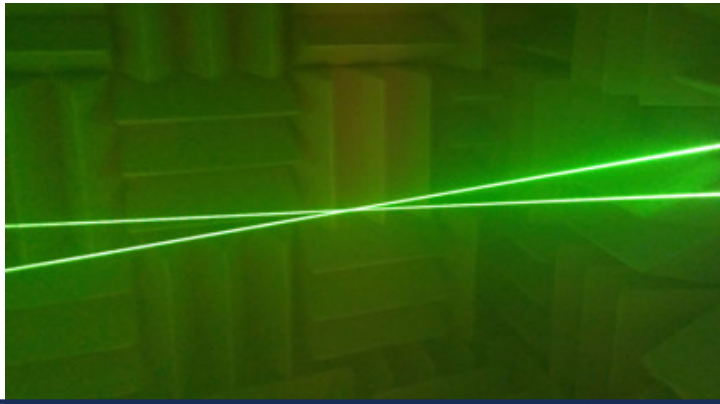
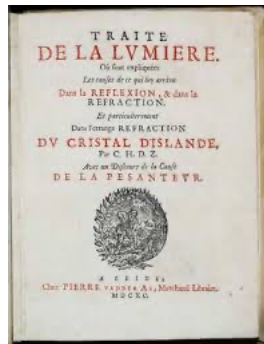


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# ANTEFATTO

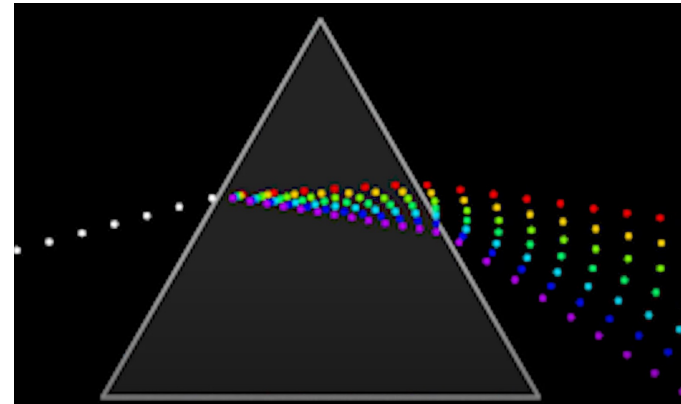
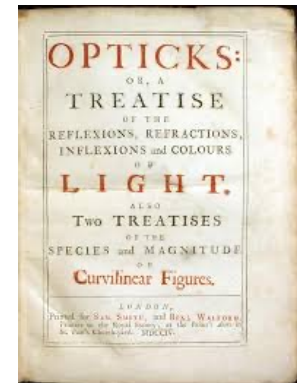
## Onda

Christiaan  
Huygens  
1690



## Particella

Isaac  
Newton  
1704

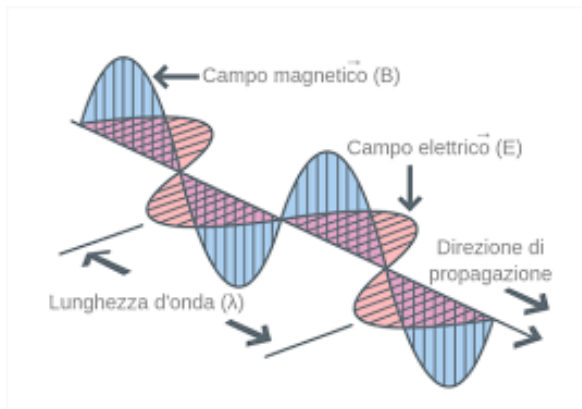


# LA NATURA ONDULATORIA DELLA LUCE

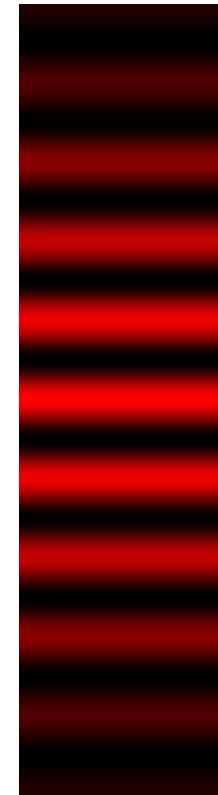
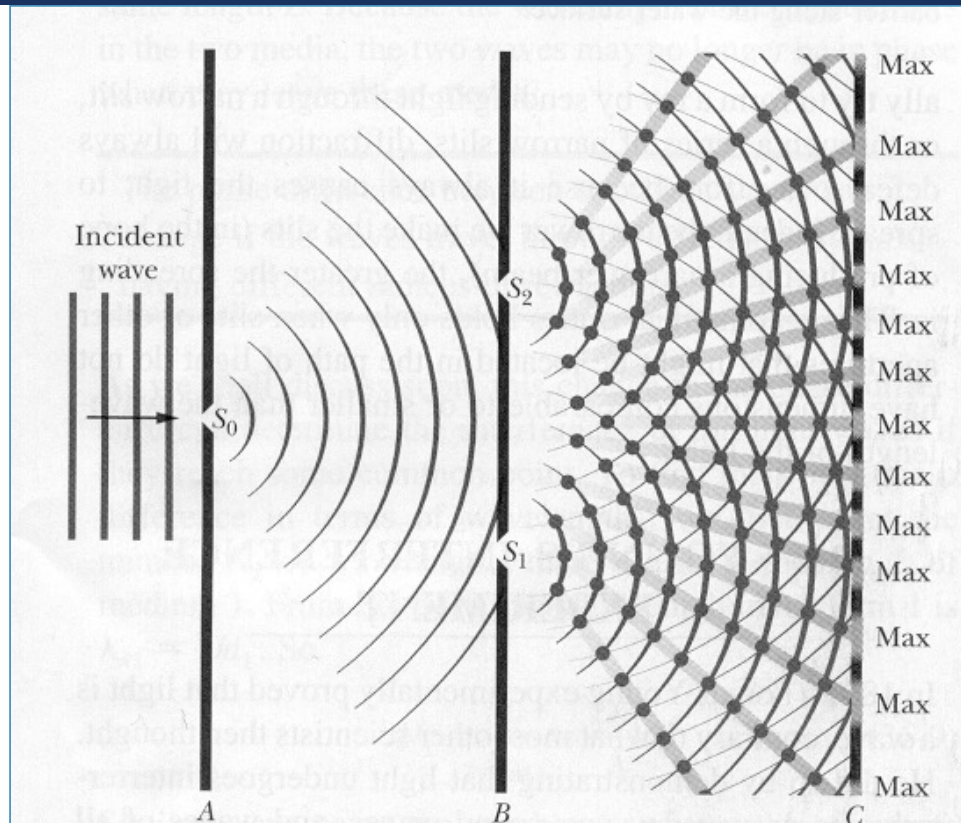
## Onda

### INTERFERENZA

Thomas Young  
1804



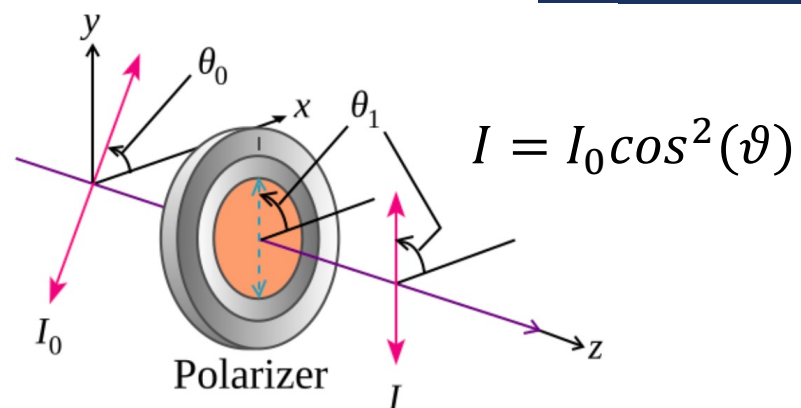
Equazioni di Maxwell, 1865



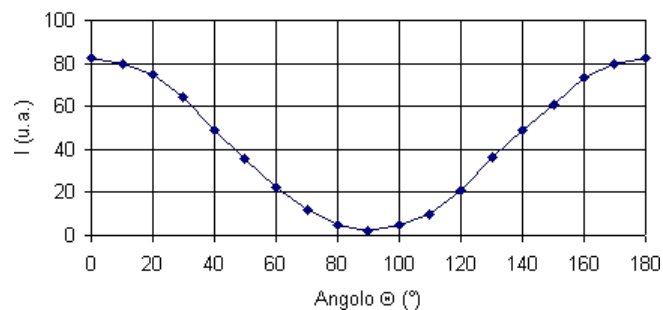


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# POLARIZZAZIONE DELLA LUCE

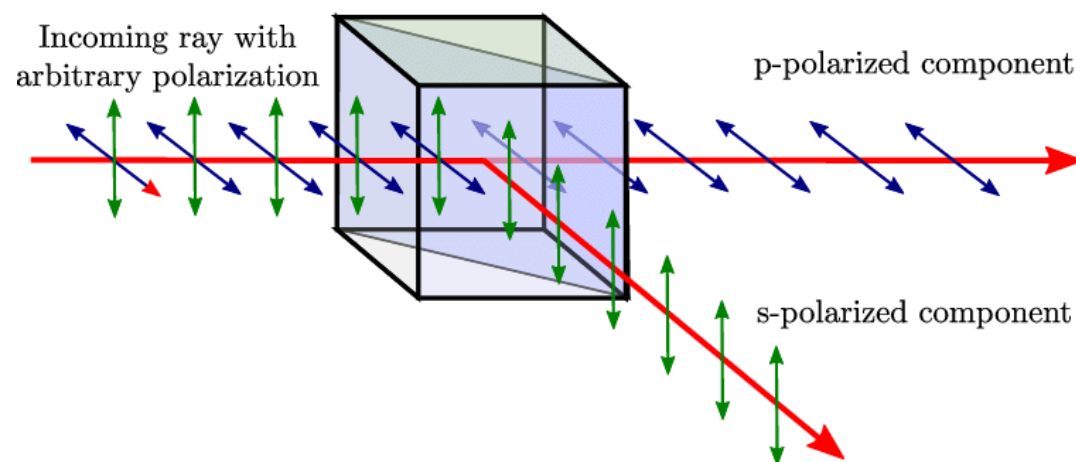


Intensità luminosa in funzione di  $\Theta$  (u.a.)



Fisica Classica:

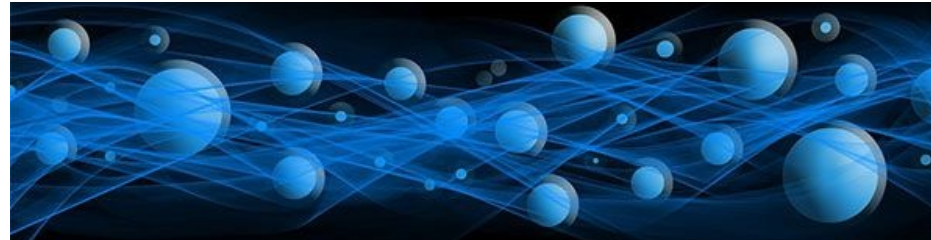
La legge di Malus (1809)





UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## Natura corpuscolare della luce



### Fotoni

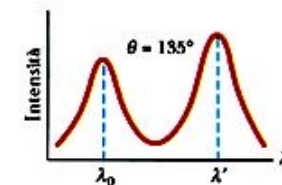
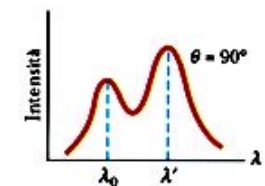
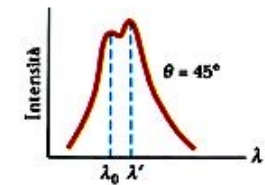
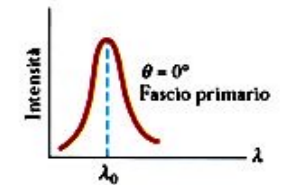
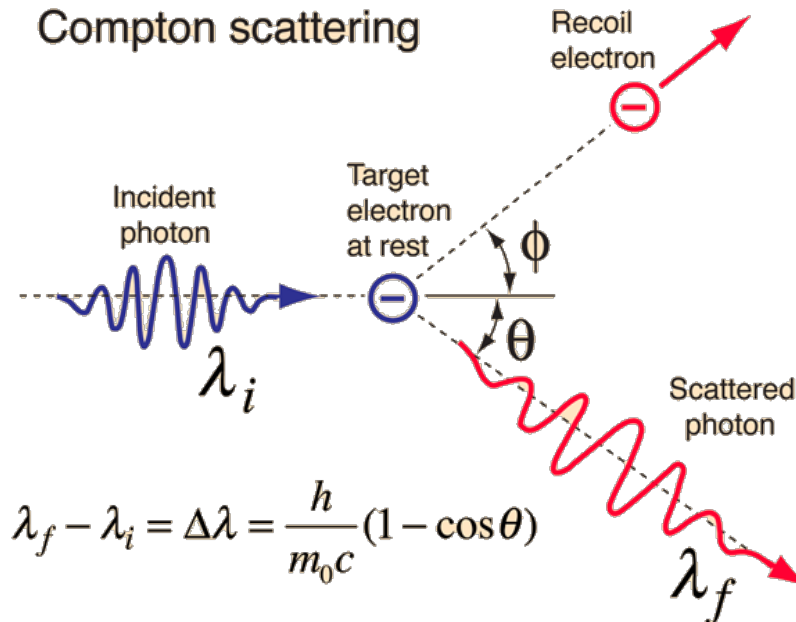
$$E = h\nu$$

$$p = \frac{h\nu}{c}$$

Costante di Planck

$$h = 6.63 \times 10^{-34} \text{ Js}$$

### Compton scattering







UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# NATURA QUANTISTICA DELLA LUCE

## Onda e corpuscolo



**Fotone**

Effetto fotoelettrico,  
Diffusione Compton

Natura corpuscolare della luce



$$E = h\nu$$

$$p = \frac{h\nu}{c}$$



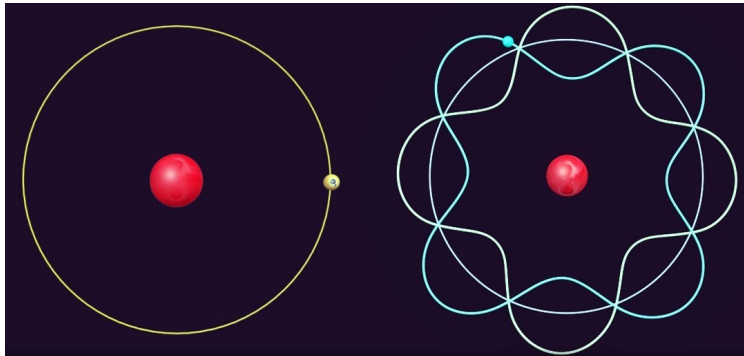
Esperimento di Young  
Interferometro

Natura ondulatoria della luce



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## Elettroni come onde



Nel 1923 Louis de Broglie postulò che la materia ordinaria può avere proprietà ondulatorie, con lunghezza d'onda  $\lambda$  legata alla quantità di moto  $p$  come nel caso della luce:

Relazione di  
de Broglie, 1923

lunghezza d'onda di de Broglie

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

Costante di Planck

$$h = 6.63 \times 10^{-34} \text{ Js}$$



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

**Domanda:**

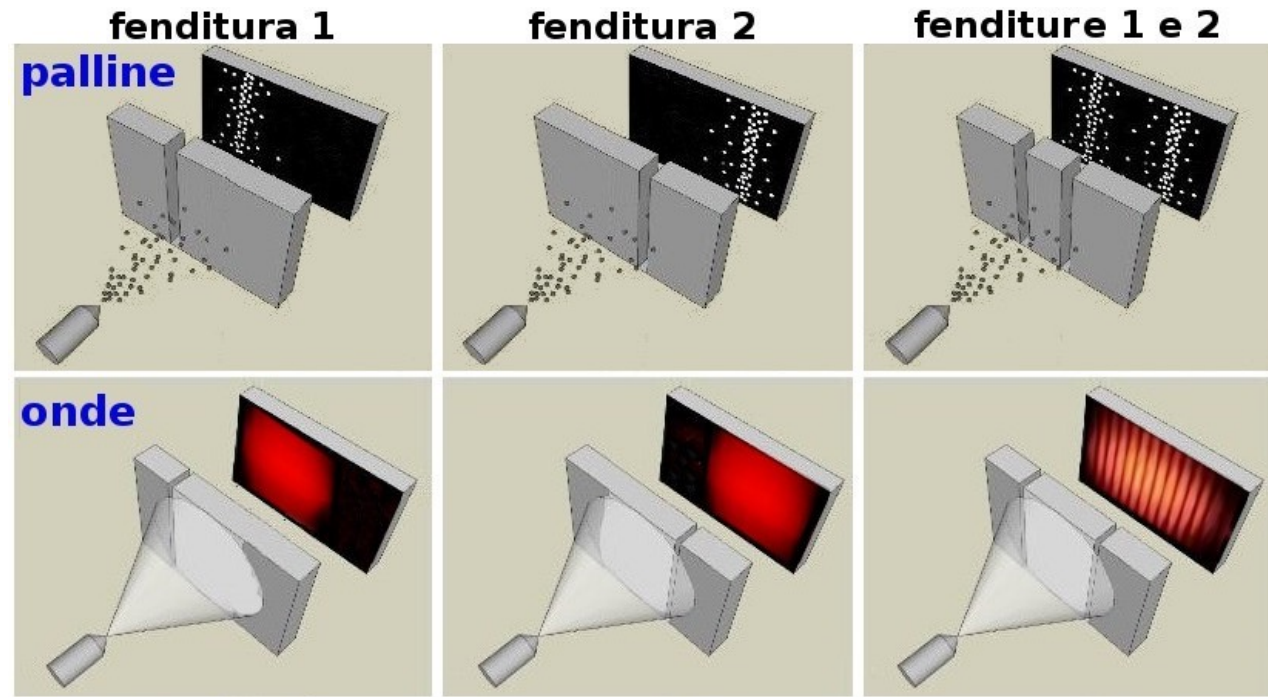
Posso utilizzare lo stesso esperimento per studiare il comportamento onda-corpuscolo?

$$P_{12} = P_1 + P_2$$

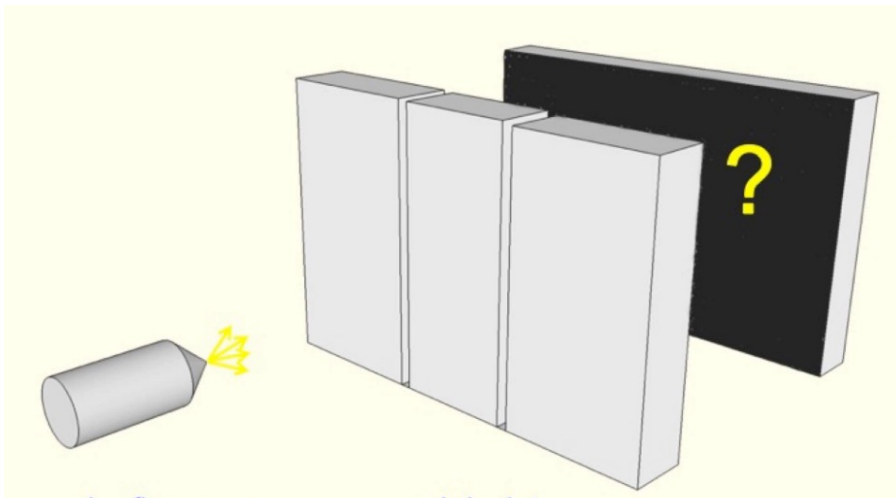
No Interferenza

$$P_{12} \neq P_1 + P_2$$

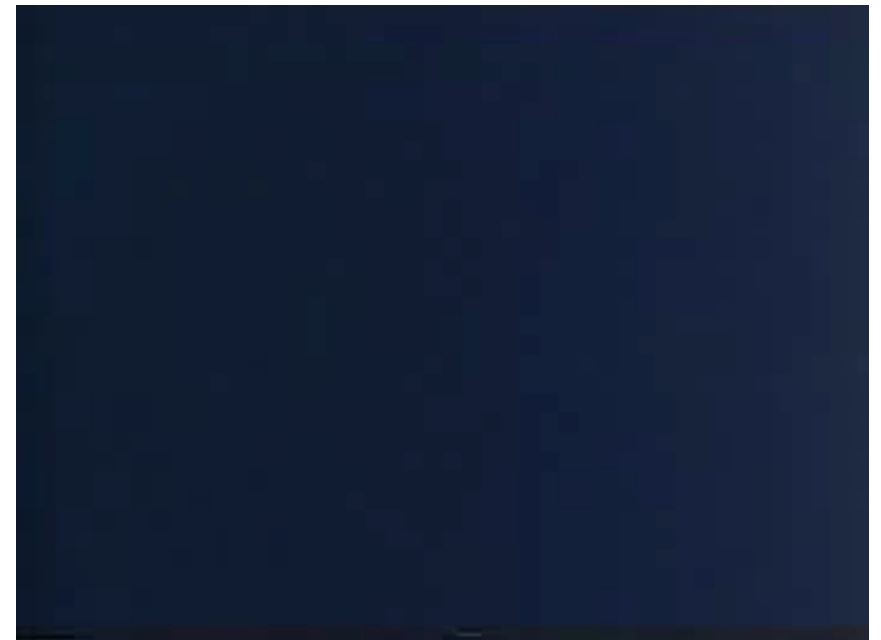
Interferenza



# Interferenza quantistica



Singolo elettrone-fotone

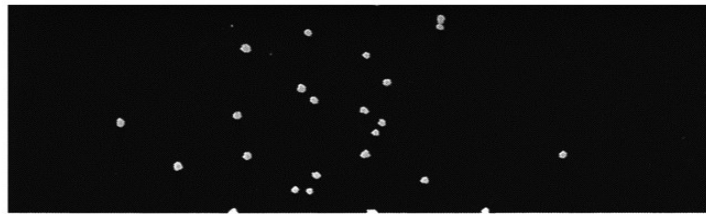


-Pier Giorgio Merli, Gian Franco Missiroli  
e Giulio Pozzi (1976)  
- Tonomura (1989)

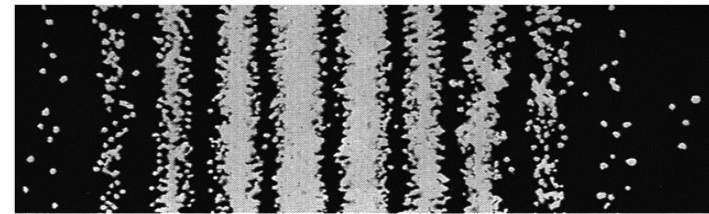


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

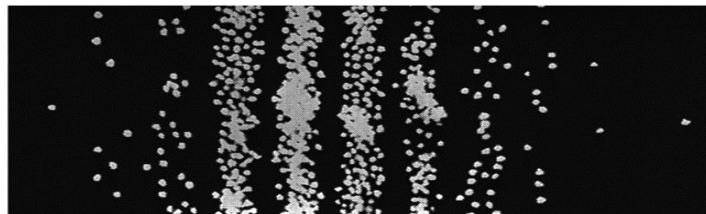
Figure di diffrazione/interferenza formate da una serie di elettroni che attraversano due fenditure



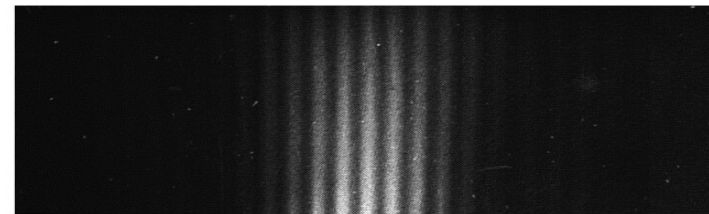
(a)



(c)



(b)



(d)

- Ciascun punto indica un elettrone che colpisce lo schermo collocato dietro le fenditure.
- Sequenza di elettroni che arriva “costruisce” la figura di interferenza.

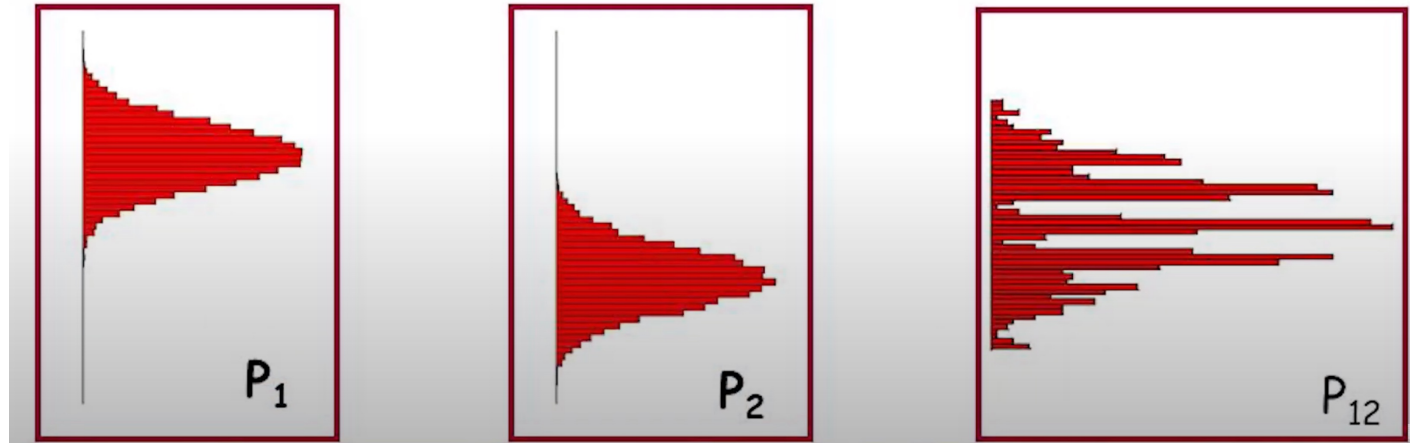




UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

$$P_{12} \neq P_1 + P_2$$

Interferenza



Alcune osservazioni:

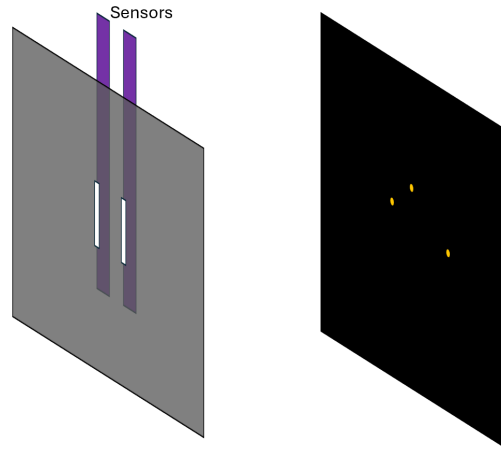
- Cosa accade nella posizione dei minimi o del massimo centrale?
- Non esiste alcuna traiettoria complicata quanto si vuole che può spiegare il percorso di questi elettroni/fotoni

Tutto quello che possiamo dire è che l'elettrone, una volta emesso, colpirà lo schermo con una certa probabilità. **Non possiamo più prevedere con certezza dove esso andrà, cade il determinismo classico.**

La vera domanda è:  
che giro fanno questi  
elettroni/fotoni?



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore



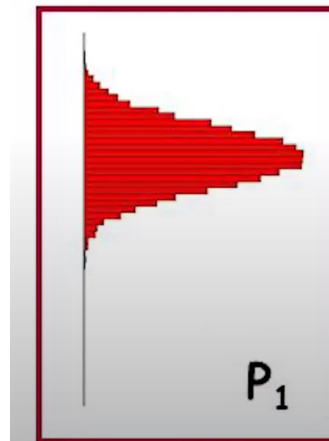
Vedo gli elettroni che passano o dalla fenditura 1 o dalla fenditura 2

$$P_{12} = P_1 + P_2$$

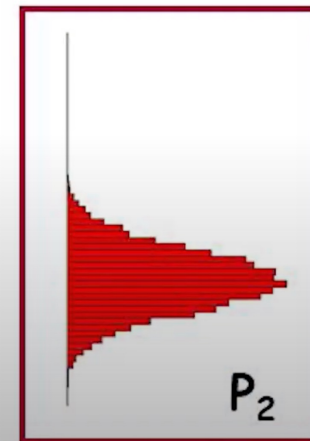
No Interferenza

Andando ad osservare gli elettroni abbiamo modificato il risultato dell'esperimento

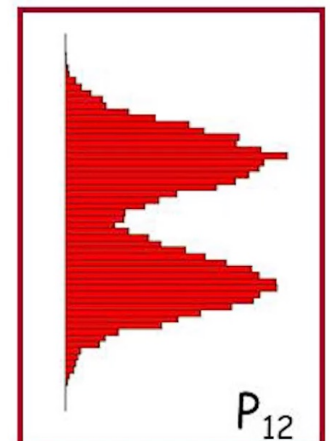
**Due concetti parziali e complementari, che non possono manifestarsi contemporaneamente**



$P_1$



$P_2$



$P_{12}$



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# PRINCIPIO DI INDETERMINAZIONE

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

Werner Karl  
Heisenberg  
1927



Nell'esperimento di interferenza non si può misurare con precisione la posizione dell'elettrone senza alterarne lo stato.

Attenzione: il principio non esprime un limite legato alla misura, ma ad una proprietà intrinseca dei sistemi fisici!



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

I risultati dell'esperimento delle due fenditure sono sorprendenti  
ma la matematica per fortuna è la stessa delle onde classiche!

### Onde classiche

$$I = |h|^2$$

h: Ampiezza dell'onda

I: Intensità

$$I_{12} = |h_1 + h_2|^2$$

### Elettroni

$$P = |\varphi|^2$$

$\varphi$ : Ampiezza di probabilità

P: Probabilità

$$P_{12} = |\varphi_1 + \varphi_2|^2$$



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

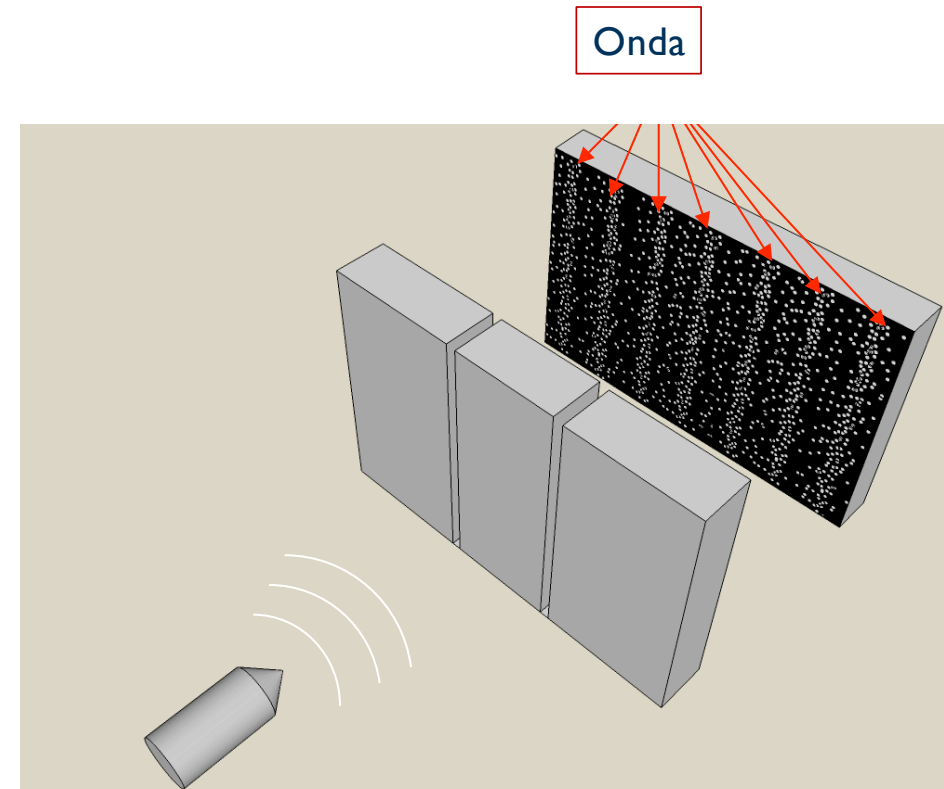
$$\varphi = \varphi_1 + \varphi_2$$

L'ampiezza di probabilità è la somma delle due ampiezze.

L'elettrone passa simultaneamente attraverso le due fenditure.

Senza spezzarsi mai, l'elettrone arriva sullo schermo come particella.

**Questa è l'idea della sovrapposizione quantistica!**





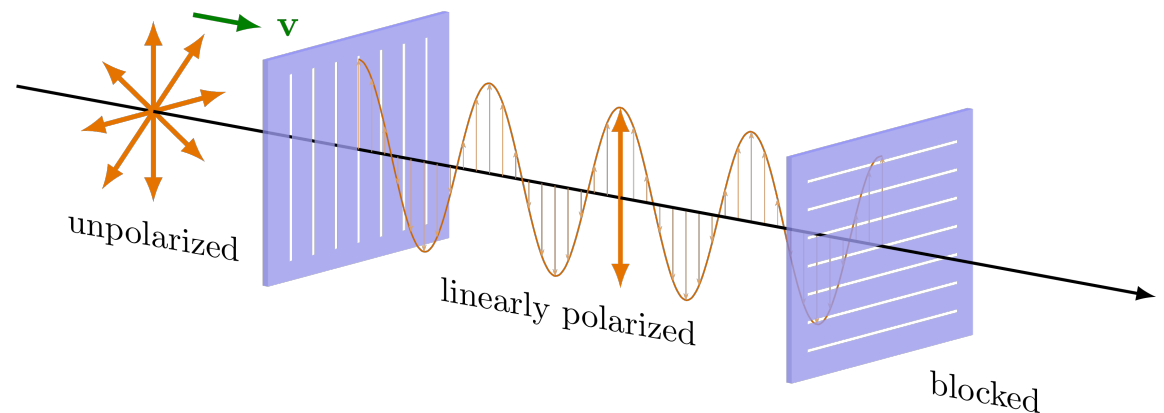


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

La sovrapposizione quantistica vale per qualunque proprietà fisica di qualunque sistema quantistico

## POLARIZZAZIONE DELLA LUCE

Se considero un **SINGOLO FOTONE** polarizzato orizzontalmente nel suo percorso incontra un polarizzatore verticale ha il 100% di probabilità di essere fermato. Se il polarizzatore è inclinato orizzontalmente invece esso sarà trasmesso al 100%.



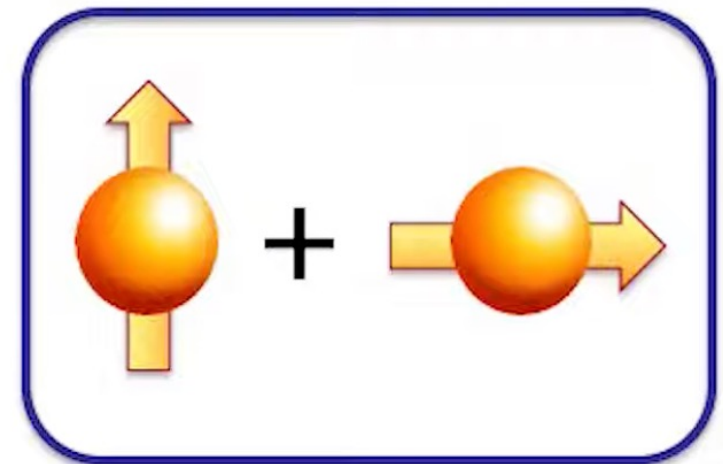


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## SINGOLO FOTONE

Se l'angolo tra la polarizzazione del fotone e quella del polarizzatore è di  $45^\circ$  ci sarà **una probabilità del 50%** che esso venga trasmesso. Il risultato della misura è deterministico solo se l'angolo tra le polarizzazioni è di  $0^\circ$  o  $90^\circ$ .

**LO STATO DI POLARIZZAZIONE DI UN FOTONE VIENE DEFINITO IN TERMINI DI AMPIEZZA DI PROBABILITÀ.**



$$\varphi = \varphi_1 + \varphi_2$$



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore



**TiqTaqToe**

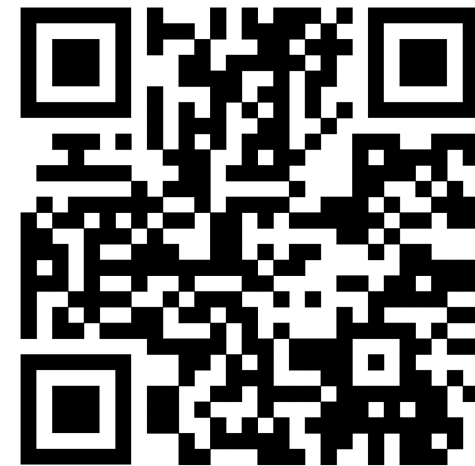
Looking for more quantum game content?

Visit [QuantumPlayed.com!](https://quantumplayed.com/)

Quick Match

Ongoing Matches

Local Tournaments



<https://tiqtaqtoe.com/>

Goff, Allan (2006). "Quantum tic-tac-toe: A teaching metaphor for superposition in quantum mechanics". *American Journal of Physics*. 74 (11): 962–973.



Einstein dice a Niels Bohr:

“Davvero crede che la luna non sia là quando non c’è nessuno ad osservarla?”

I fotoni sono stati gli oggetti quantistici più utilizzati negli esperimenti dagli anni 2000 ad oggi. In modo perfetto, come mai era successo ad altre teorie nella storia della fisica, la meccanica quantistica si accorda con i dati sperimentali: in un certo senso è più vera della nostra intuizione (A. Zeilinger).



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## LA CRITTOGRAFIA QUANTISTICA?

La crittografia quantistica è una forma avanzata di crittografia che si serve dei principi della meccanica quantistica per garantire la sicurezza delle comunicazioni.

Essa sfrutta la trasmissione di bit tramite emissione e rilevamento di singoli fotoni con diversa polarizzazione.



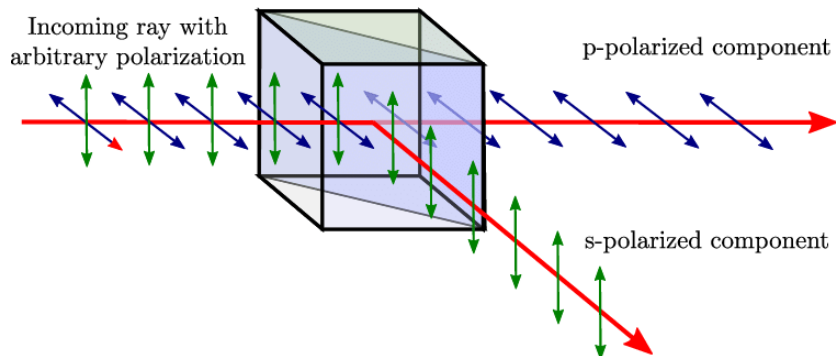


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## SINGOLO FOTONE

**LO STATO DI POLARIZZAZIONE DI UN FOTONE VIENE DEFINITO IN TERMINI DI AMPIEZZA DI PROBABILITÀ.**

$$\varphi = \varphi_1 + \varphi_2$$



$$|45^\circ\rangle = (|H\rangle + |V\rangle)/\sqrt{2}; \quad |-45^\circ\rangle = (|H\rangle - |V\rangle)/\sqrt{2}$$

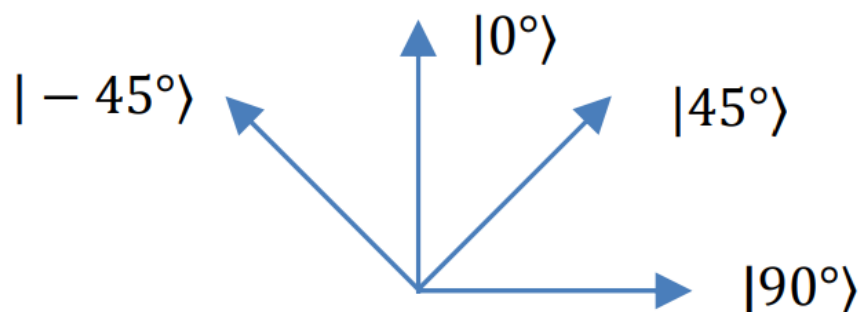
$$|H\rangle = (|45^\circ\rangle + |-45^\circ\rangle)/\sqrt{2}; \quad |V\rangle = (|45^\circ\rangle - |-45^\circ\rangle)/\sqrt{2}$$





UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## COME FUNZIONA: INTRODUZIONE



	0	1
+		
x		

Mittente (Alice) e destinatario del messaggio (Bob) scelgono una base randomica ( $0^\circ, 90^\circ$ ;  $-45^\circ, 45^\circ$ ) per ogni bit che il primo intende trasmettere. Se si vuole generare una chiave crittografica anche i bit scelti dal mittente saranno casuali.

I bit sono determinati dal vettore della base della polarizzazione del fotone che si seleziona: 0 se si sceglie  $0^\circ$  o  $-45^\circ$  e 1 se si sceglie  $90^\circ$  o  $45^\circ$ .

Per i principi della meccanica quantistica il risultato di una misura del bit fatta dal ricevitore è deterministico solo se la base scelta è uguale a quella del mittente. Se Alice e Bob scelgono la stessa base allora il bit mandato sarà uguale a quello ricevuto al 100% (si fa notare che le basi sono note in quanto pubbliche).

La chiave crittografica sarà composta da questi bit.



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## SIMULAZIONE CON APPARATO THORLABS

L'esperimento è una semplice simulazione del processo effettivo, perché utilizza luce classica invece dei singoli fotoni. Il setup è composto da 3 unità principali: Alice, Bob e Eve. Alice invia il messaggio, Bob lo riceve e Eve lo intercetta.

Le principali componenti dell'apparato sono  $\lambda/2$ -plate, polarizing beamsplitter, laser e sensori.

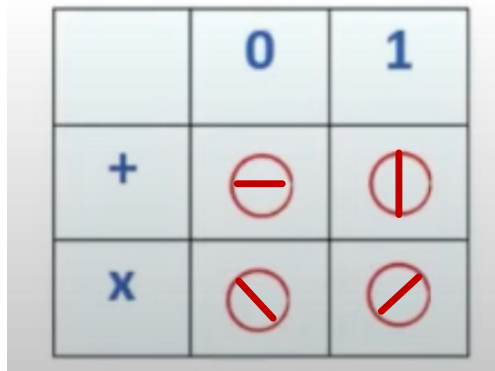




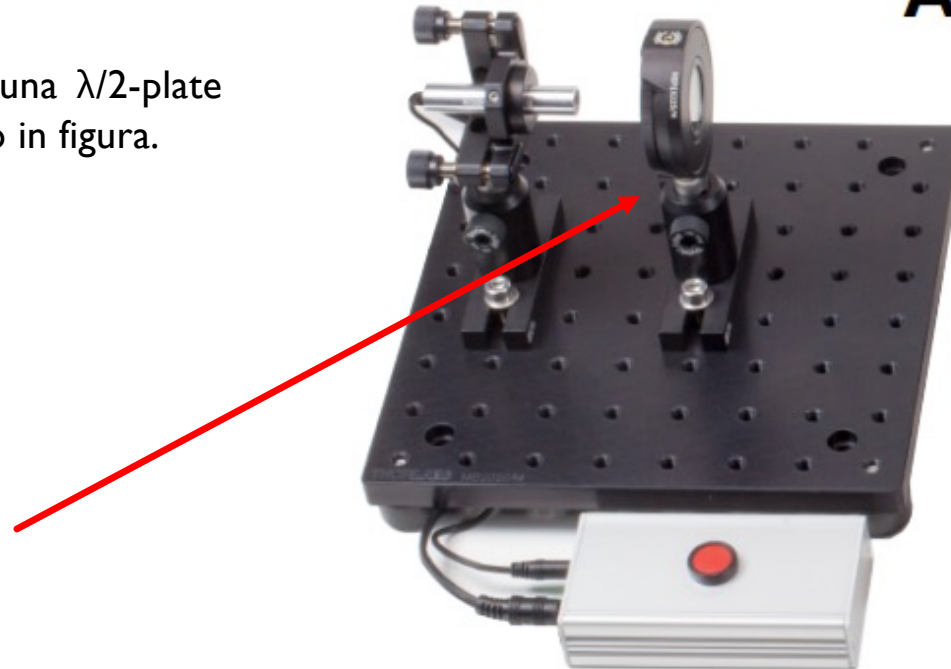
UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## ALLESTIMENTO: ALICE

L'unità Alice è composta da un laser ed una  $\lambda/2$ -plate graduata da  $-45^\circ$  a  $90^\circ$ , come rappresentato in figura.



**Alice**



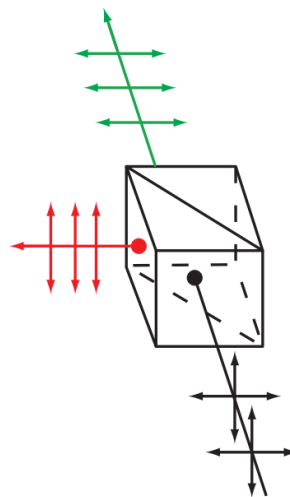


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## ALLESTIMENTO: BOB

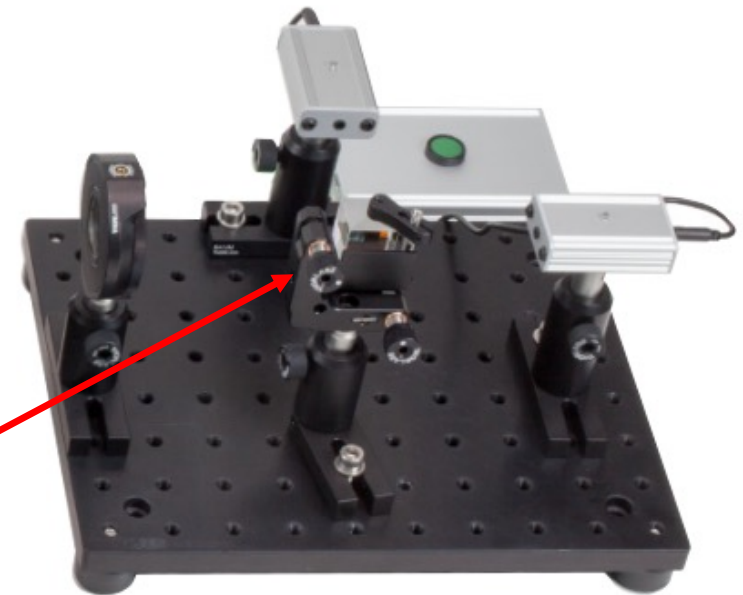
L'unità Bob è composta da una  $\lambda/2$ -plate graduata da  $0^\circ$  a  $45^\circ$ , un polarizing beamsplitter e due sensori, come rappresentato in figura.

Il polarizing beamsplitter riflette di  $90^\circ$  la luce incidente polarizzata verticalmente, e lascia passare quella polarizzata orizzontalmente.



Polarizing  
Beamsplitter Cube

**Bob**









UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## Protocollo BB84

Bit inviato da Alice												
Base di Alice												
Alice invia												
Base di Bob												
Fotone ricevuto da Bob			.									
Bit ricevuto da Bob												
Stessa base?												
Alice conserva bit												
Bob conserva bit												
Bit di verifica (scelti arbitrariamente)												
CHIAVE												

	0	1
+		
x		

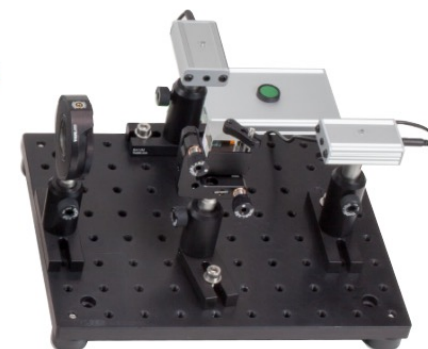


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

Bit inviato da Alice	1	0	1	1	0	1	1	0	0	1	0	1
Base di Alice	+	+	x	x	+	+	+	x	+	x	x	+
Alice invia	⊕	⊖	⊗	⊗	⊖	⊕	⊕	⊗	⊖	⊗	⊗	⊕

	0	1
+	⊖	⊗
x	⊗	⊗

Bob







UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## COME FUNZIONA: BIT E BASI, CASI POSSIBILI

Alice		Bob		
State	Basis, Bit	Chosen Basis	State	Measured Bit
$ 0^\circ\rangle$	+, 0	+	$\hat{M}_+  0^\circ\rangle =  0^\circ\rangle$	0
		×	$\hat{M}_\times  0^\circ\rangle = \frac{1}{\sqrt{2}}  45^\circ\rangle - \frac{1}{\sqrt{2}}  -45^\circ\rangle$	0 or 1
$ 90^\circ\rangle$	+, 1	+	$\hat{M}_+  90^\circ\rangle = - 90^\circ\rangle$	1
		×	$\hat{M}_\times  90^\circ\rangle = \frac{1}{\sqrt{2}}  45^\circ\rangle + \frac{1}{\sqrt{2}}  -45^\circ\rangle$	0 or 1
$ 45^\circ\rangle$	×, 1	+	$\hat{M}_+  45^\circ\rangle = \frac{1}{\sqrt{2}}  0^\circ\rangle - \frac{1}{\sqrt{2}}  90^\circ\rangle$	0 or 1
		×	$\hat{M}_\times  45^\circ\rangle =  45^\circ\rangle$	1
$ -45^\circ\rangle$	×, 0	+	$\hat{M}_+  -45^\circ\rangle = \frac{1}{\sqrt{2}}  0^\circ\rangle + \frac{1}{\sqrt{2}}  90^\circ\rangle$	0 or 1
		×	$\hat{M}_\times  -45^\circ\rangle = - -45^\circ\rangle$	0

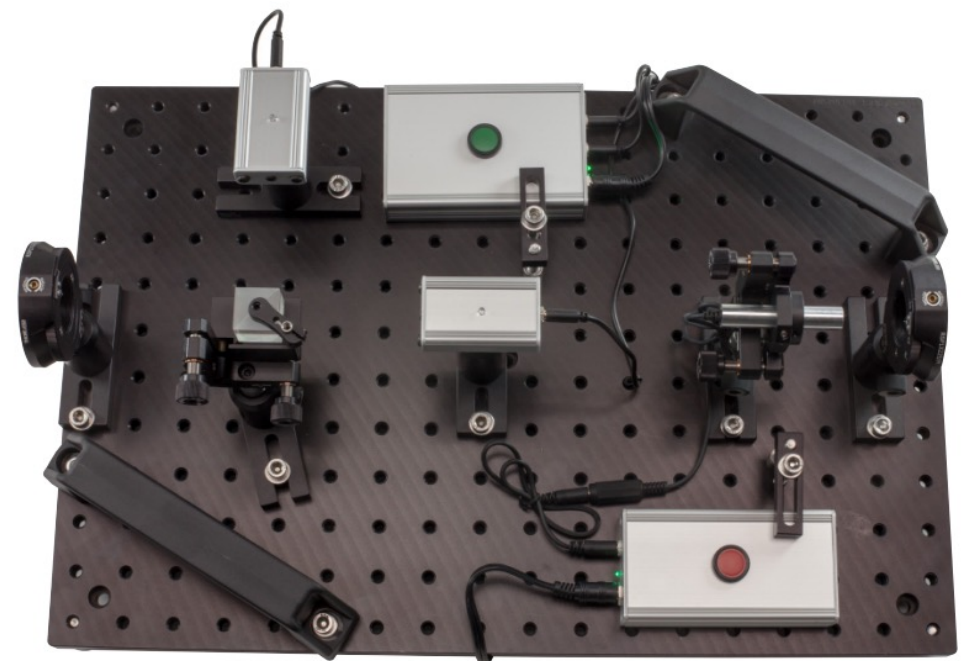
- Bases of Alice & Bob Identical → Bit can be Used as Key Bit
- Bases of Alice & Bob Not Identical → Measurement is Discarded



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## ALLESTIMENTO: EVE

Eve è composta di due parti: la prima allestita come Bob e la seconda come Alice; come rappresentato in figura.



 **Eve**



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## INTERCETTAZIONE DEL MESSAGGIO

A questo punto se un terzo (Eve) intercettasse il messaggio per la creazione della chiave, una volta ricevuto il bit, non saprebbe la base scelta dal mittente. Dovrebbe quindi selezionare casualmente una base e spedire nuovamente il bit ricevuto.

Esiste quindi una probabilità del 25% che Eve venga scoperta.

Alice		Eve			Bob		
Basis, Bit	State	Basis	State	State Sent	Basis	State	Measured Bit
+, 0	$ 0^\circ\rangle$	+	$\hat{M}_+  0^\circ\rangle =  0^\circ\rangle$	$ 0^\circ\rangle$	+	$\hat{M}_+  0^\circ\rangle =  0^\circ\rangle$	0
		×			×	$\hat{M}_\times  0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
		×	$\hat{M}_\times  0^\circ\rangle = \frac{ 45^\circ\rangle}{\sqrt{2}} - \frac{ -45^\circ\rangle}{\sqrt{2}}$	$ 45^\circ\rangle$ or $ -45^\circ\rangle$	+	$\hat{M}_+  45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$ or $\hat{M}_+  -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1 0 or 1
		×			×	$\hat{M}_\times  45^\circ\rangle =  45^\circ\rangle$ or $\hat{M}_\times  -45^\circ\rangle = - -45^\circ\rangle$	1 0
+, 1	$ 90^\circ\rangle$	+	$\hat{M}_+  90^\circ\rangle = - 90^\circ\rangle$	$ 90^\circ\rangle$	+	$\hat{M}_+  90^\circ\rangle = - 90^\circ\rangle$	1
		×			×	$\hat{M}_\times  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	0 or 1
		×	$\hat{M}_\times  90^\circ\rangle = \frac{ 45^\circ\rangle}{\sqrt{2}} + \frac{ -45^\circ\rangle}{\sqrt{2}}$	$ 45^\circ\rangle$ or $ -45^\circ\rangle$	+	$\hat{M}_+  45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$ or $\hat{M}_+  -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1 0 or 1
		×			×	$\hat{M}_\times  45^\circ\rangle =  45^\circ\rangle$ or $\hat{M}_\times  -45^\circ\rangle = - -45^\circ\rangle$	1 0



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# INTERCETTAZIONE DEL MESSAGGIO

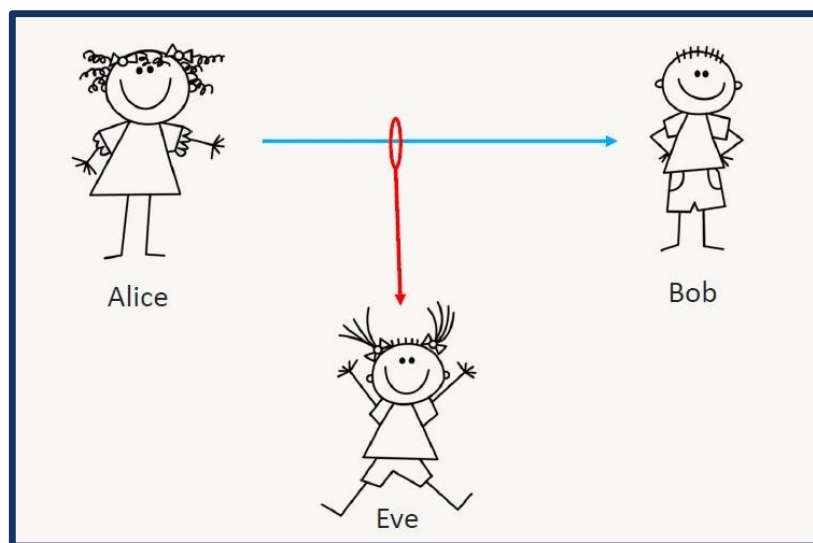
- Bases of Alice & Bob & Eve Identical → Eve is Not Noticed
- Bases of Alice & Bob Not Identical → Measurement is Discarded Anyway
- Bases of Alice & Bob Identical; Bits are Incidentally Identical, Eve is Not Noticed
- Bases of Alice & Bob Identical; Bits Incidentally Differ → *Eve is Uncovered*

x, 1	45°⟩	+	$\hat{M}_+  45^\circ\rangle = \frac{ 0^\circ\rangle}{\sqrt{2}} - \frac{ 90^\circ\rangle}{\sqrt{2}}$	0°⟩ or  90°⟩	+	$\hat{M}_+  0^\circ\rangle =  0^\circ\rangle$ or $\hat{M}_+  90^\circ\rangle = - 90^\circ\rangle$	0 1
					×	$\hat{M}_\times  0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$ or $\hat{M}_\times  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	<span style="color: red;">0</span> or <span style="color: cyan;">1</span> <span style="color: red;">0</span> or <span style="color: cyan;">1</span>
		×	$\hat{M}_\times  45^\circ\rangle =  45^\circ\rangle$	45°⟩	+	$\hat{M}_+  45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle - \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
					×	$\hat{M}_\times  45^\circ\rangle =  45^\circ\rangle$	1
x, 0	-45°⟩	+	$\hat{M}_+  -45^\circ\rangle = \frac{ 0^\circ\rangle}{\sqrt{2}} + \frac{ 90^\circ\rangle}{\sqrt{2}}$	0°⟩ or  90°⟩	+	$\hat{M}_+  0^\circ\rangle =  0^\circ\rangle$ or $\hat{M}_+  90^\circ\rangle = - 90^\circ\rangle$	0 1
					×	$\hat{M}_\times  0^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle - \frac{1}{\sqrt{2}} -45^\circ\rangle$ or $\hat{M}_\times  90^\circ\rangle = \frac{1}{\sqrt{2}} 45^\circ\rangle + \frac{1}{\sqrt{2}} -45^\circ\rangle$	<span style="color: cyan;">0</span> or <span style="color: red;">1</span> <span style="color: cyan;">0</span> or <span style="color: red;">1</span>
		×	$\hat{M}_\times  -45^\circ\rangle = - -45^\circ\rangle$	-45°⟩	+	$\hat{M}_+  -45^\circ\rangle = \frac{1}{\sqrt{2}} 0^\circ\rangle + \frac{1}{\sqrt{2}} 90^\circ\rangle$	0 or 1
					×	$\hat{M}_\times  -45^\circ\rangle = - -45^\circ\rangle$	0



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

# QUANTUM KEY DISTRIBUTION



PROBABILITÀ CHE BOB RICEVA IL BIT CORRETTO:

$$P = \frac{1}{2} \cdot 1 + \frac{1}{2} \cdot \frac{1}{2} = \frac{3}{4}$$

Probabilità che  
EVE indovini la  
base

Probabilità che  
EVE non  
indovini la base

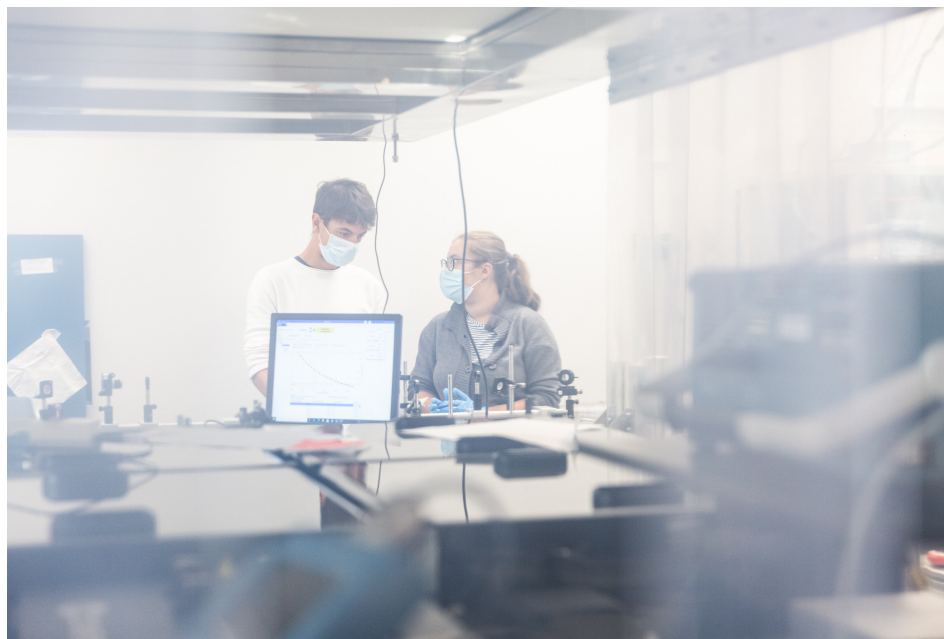
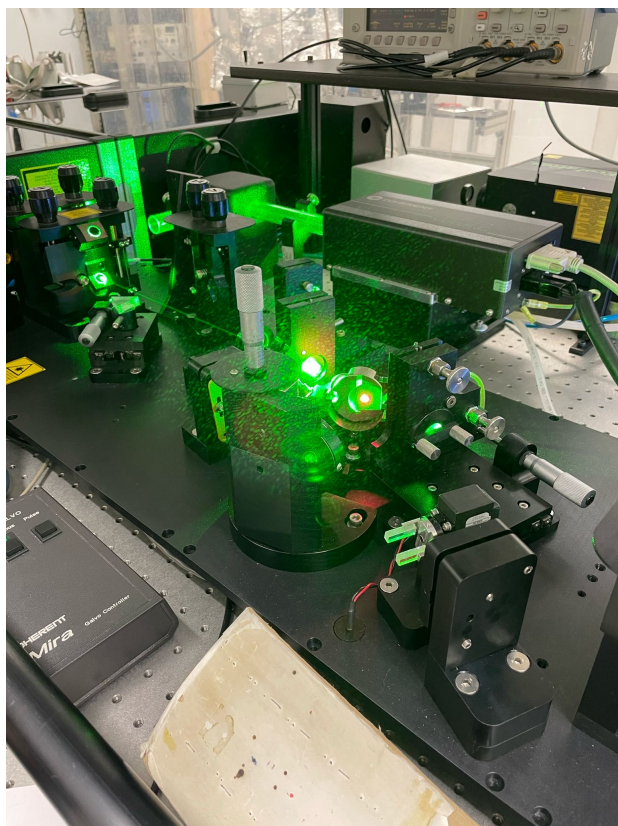
*C'è una probabilità del 75% che Alice e Bob non si accorgano della presenza di Eve e quindi una probabilità di registrare un errore del 25%.*



UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## LA NOSTRA RICERCA

LASER AL FEMTOSECONDO PER SPETTROSCOPIE ULTRAVELOCI





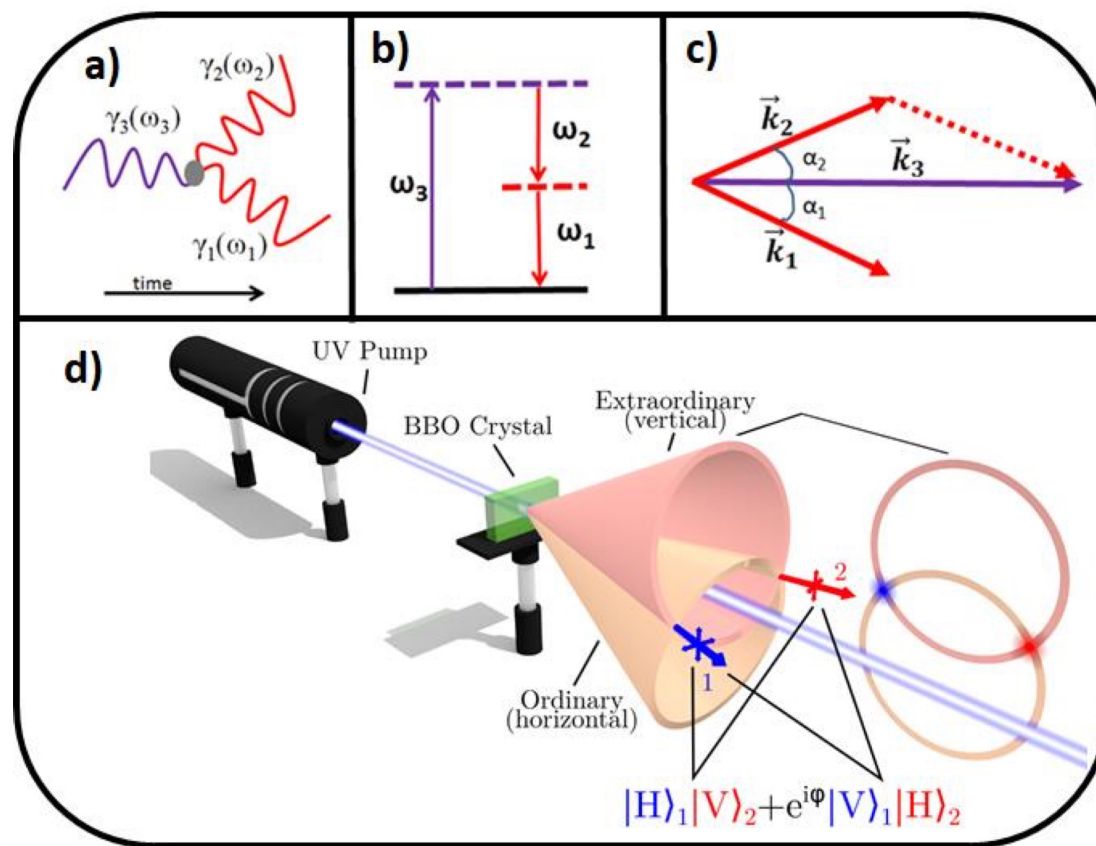


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

## LA NOSTRA RICERCA

Come si generano sorgenti a singolo fotone?

Spontaneous Parametric Down  
Conversion



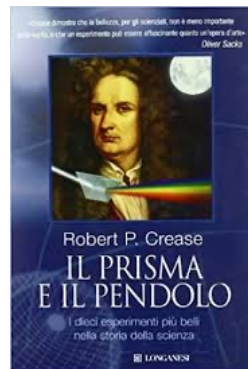


UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore



Nel maggio 2002 lo storico e filosofo della scienza **Robert Crease** ha lanciato una singolare indagine.

Dalle pagine della rivista specializzata Physics World chiedeva ai suoi lettori, ricercatori di fisica di tutto il mondo, di segnalare candidati per ...l'esperimento più bello della fisica... e di spiegare in che cosa consistesse la bellezza di questi esperimenti.



- È un esperimento fondamentale
- È un esperimento concettualmente semplice
- È un esperimento convincente

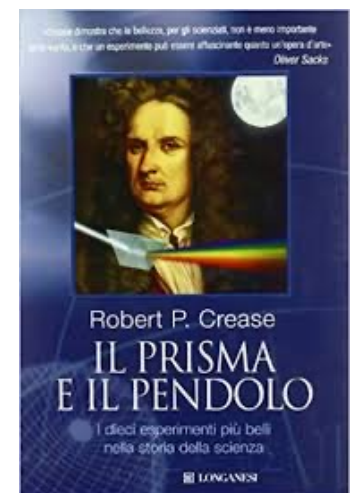
- Eratostene: la misurazione della circonferenza terrestre
- Galileo: la leggenda della caduta dei gravi dalla Torre di Pisa
- Galileo: l'esperimento del piano inclinato
- Newton: la scomposizione della luce con prismi
- Cavendish: la determinazione del peso della Terra
- Young: la scoperta del carattere ondulatorio della luce
- Foucault: la dimostrazione della rotazione terrestre col pendolo
- Millikan: l'esperimento della goccia d'olio
- Rutherford: la scoperta del nucleo atomico
- L'esperimento dell'interferenza quantistica di elettroni singoli

## La classifica:

### 01 L'esperimento della doppia fenditura applicato all'interferenza da elettrone singolo

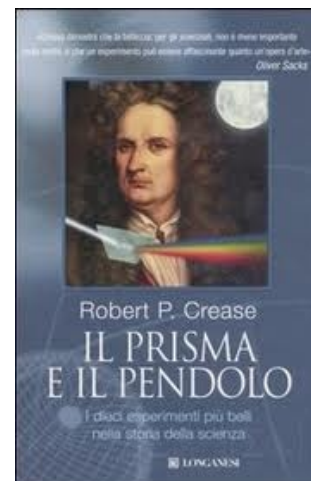
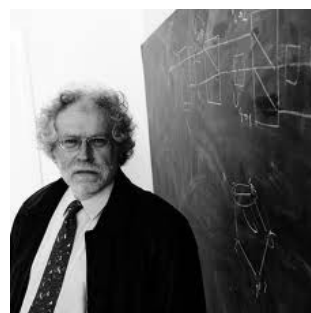
Robert Crease scrive...

esso contiene l'essenza della meccanica quantistica. Ha tutte le caratteristiche che permettono di definire un esperimento bello. È di importanza strategica nel senso che è capace di convincere anche il più scettico sui fondamenti della teoria dei quanti. È semplice, facile da capire nonostante i risultati siano rivoluzionari. (...) Il mondo della meccanica quantistica è e rimarrà assolutamente lontano dal senso comune indipendentemente da quanto si conosca la teoria. L'esperimento di interferenza di elettroni con elettroni singoli pone la realtà dinanzi ai nostri occhi in modo semplice, chiaro e coinvolgente. È quindi presumibile che rimarrà nel pantheon degli esperimenti meravigliosi per molti anni a venire....

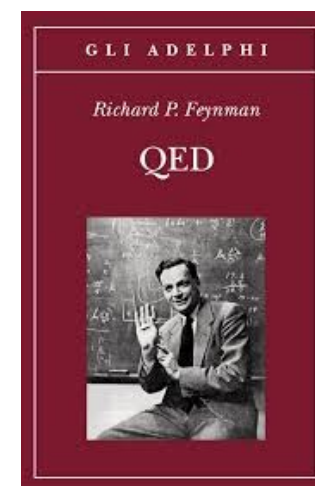




UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore



- Eratostene: la misurazione della circonferenza terrestre
- Galileo: la leggenda della caduta dei gravi dalla Torre di Pisa
- Galileo: l'esperimento del piano inclinato
- Newton: la scomposizione della luce con prismi
- Cavendish: la determinazione del peso della Terra
- Young: la scoperta del carattere ondulatorio della luce
- Foucault: la dimostrazione della rotazione terrestre col pendolo
- Millikan: l'esperimento della goccia d'olio
- Rutherford: la scoperta del nucleo atomico
- L'esperimento dell'interferenza quantistica di elettroni singoli

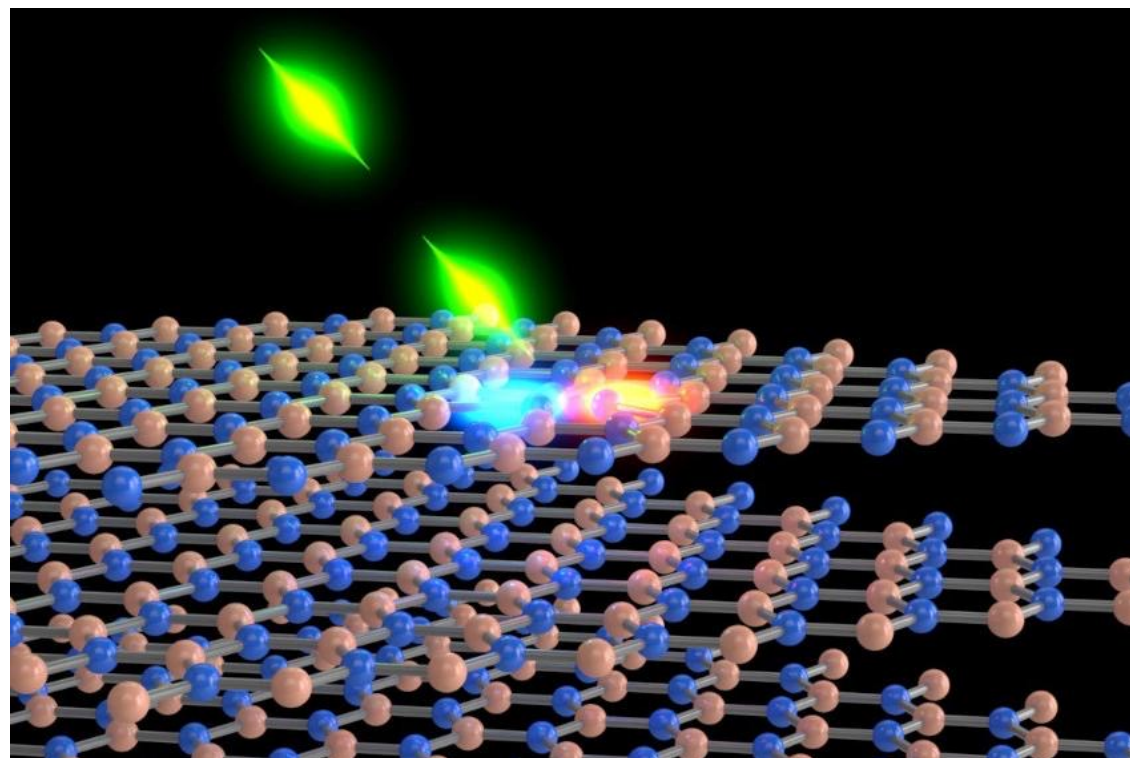






UNIVERSITÀ  
CATTOLICA  
del Sacro Cuore

GRAZIE A  
TUTTI PER  
L'ATTENZIONE





GRAZIE