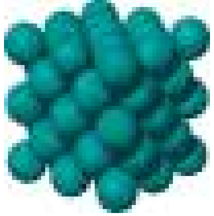


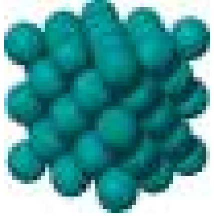
Esperimenti di Informazione Quantistica con i metodi dell’Ottica Quantistica

Gruppo di Ottica Quantistica

Dipartimento di Fisica

Università di Roma “La Sapienza”

Roma, 3 Febbraio 2009



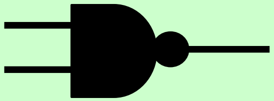
Informazione classica vs. Informazione quantistica

Classical Information: Boolean logic

Bit: variabile dicotomica (0 o 1)

Elaborazione dell'Informazione

Logic gate NAND: porta universale

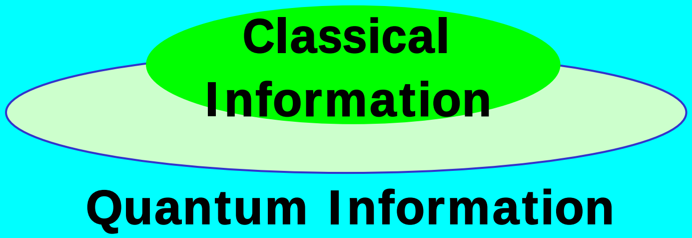


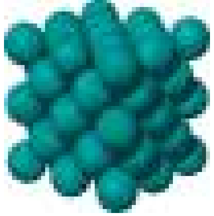
Teoria dell'Informazione Meccanica Quantistica → Informazione Quantistica

Spazio di Hilbert $\boldsymbol{H_2}$ di dimensione 2 with basis $\left\{ |\mathbf{0}\rangle, |\mathbf{1}\rangle \right\}$

Quantum bit (qubit): quantum state in $\boldsymbol{H_2}$

$$\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \quad \boldsymbol{con} \;\; \alpha, \beta \in C \quad \boldsymbol{e} \;\; |\alpha|^2 + |\beta|^2 = \mathbf{1}$$





Obiettivi

Dagli aspetti più fondamentali alle tecnologie quantistiche emergenti

Fisica fondamentale

L'entanglement essenziale per investigare le proprietà **non-locali** della meccanica quantistica:

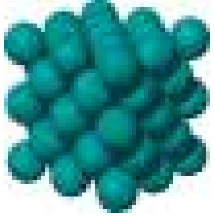
- Bell tests
- Quantum to classical transition
- *Condensed matter physics:*
- Studio diretto delle proprietà di many body quantum systems

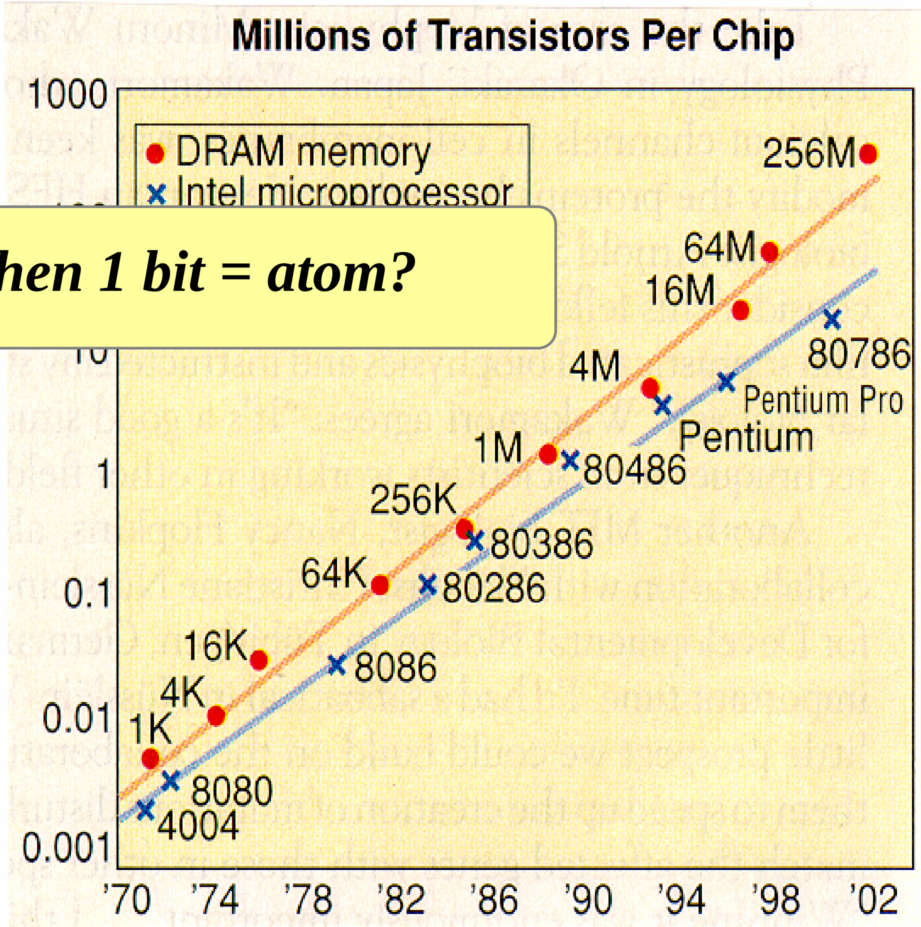
Fisica applicata

L'entanglement rappresenta una nuova risorsa per **quantum information processing**:

- Quantum cryptography
- Quantum metrology
- Quantum computation
- Quantum simulation

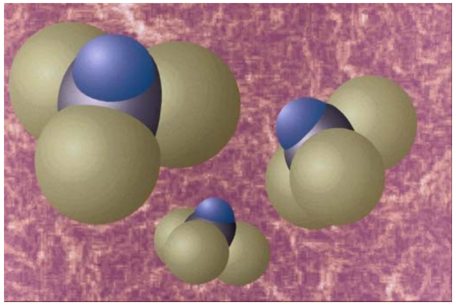
La legge di Moore





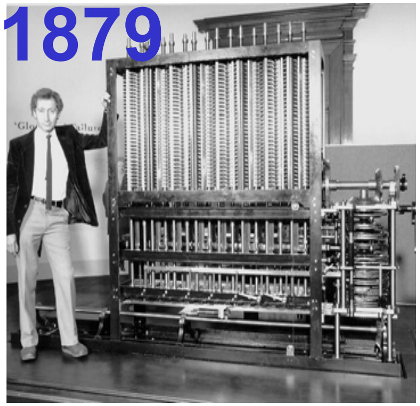
What happens when 1 bit = atom?

2020



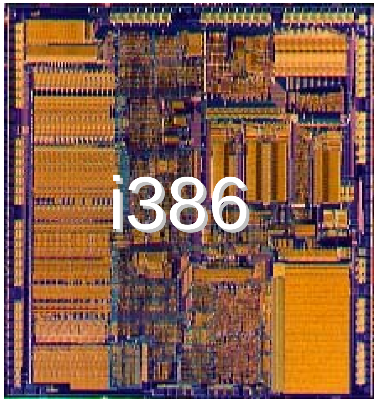
1 nanometer

1879



1 pollice

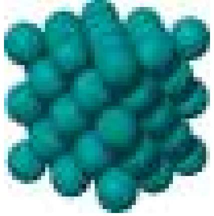
1986



1 micrometer

« Le prestazioni dei processori, e il numero di transistor ad esso relativo, raddoppiano ogni 18 mesi. »

Quantum computation: Idea originale



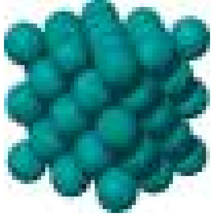
Richard Feynman

"*There's Plenty of Room at the Bottom*"
(1959 APS annual meeting)

"When we get to the very, very small world – say circuits of seven atoms - we have a lot of new things that would happen that represent completely new opportunities for design. **Atoms on a small scale behave like nothing on a large scale, for they satisfy the laws of quantum mechanics…**"

- **Computation with coherent atomic-scale dynamics.**
- **The behaviour of a quantum computer is governed by the laws o quantum mechanics.**

Information processing mediante porte logiche

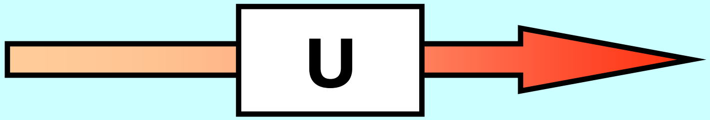


Informazione classica → **unità d'informazione: bit**

Informazione quantistica → **unità d'informazione: qubit**

Porta logica ad 1 qubit

$$|\psi_{in}\rangle = \alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle \qquad |\psi_{out}\rangle = U\left(\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle\right)$$



Pauli Operators

$$\sigma_Z\left(\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle\right) = \alpha|\mathbf{0}\rangle - \beta|\mathbf{1}\rangle$$

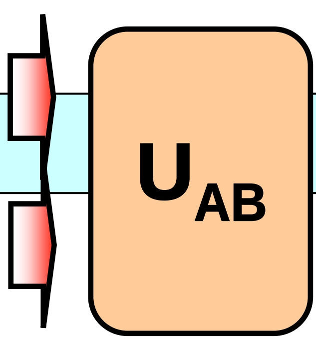
$$\sigma_X\left(\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle\right) = \beta|\mathbf{0}\rangle + \alpha|\mathbf{1}\rangle$$

$$i\sigma_Y\left(\alpha|\mathbf{0}\rangle + \beta|\mathbf{1}\rangle\right) = \alpha|\mathbf{1}\rangle - \beta|\mathbf{0}\rangle$$

Interazioni fra qubits: gate per 2 qubits

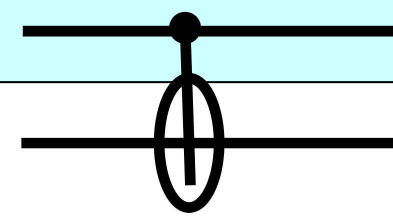
$|\psi\rangle_A$

$|\phi\rangle_B$



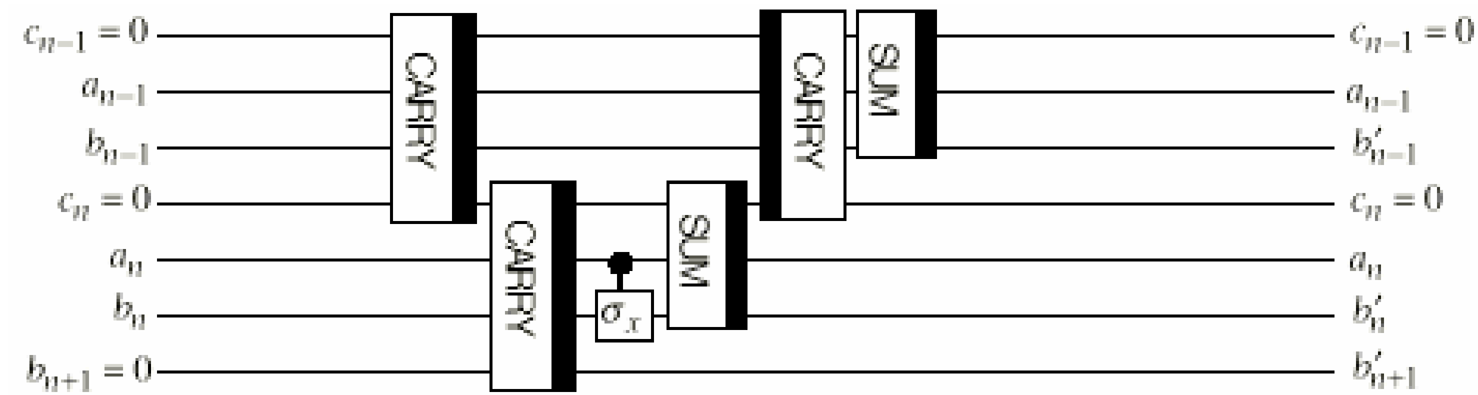
$$U_{AB}\left(|\psi\rangle_A |\phi\rangle_B\right)$$

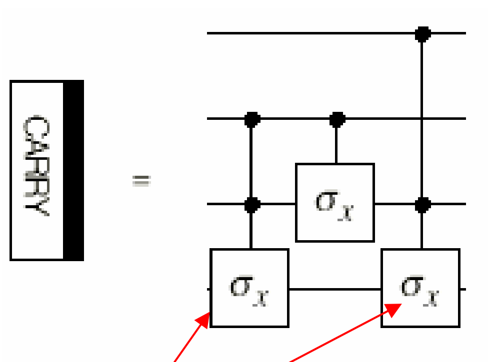
Control-NOT gate

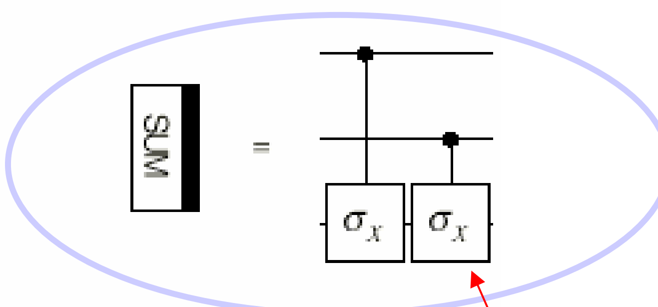


Circuito quantistico

Quantum adder

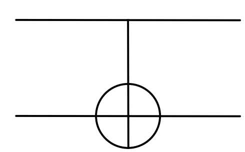






- Here we use Pauli rotations notation.
- Controlled σ_x is the same as controlled NOT

Controlled-controlled σ_x is the same as Toffoli



Controlled σ_x is the same as Feynman

Entanglement

Entanglement: correlazione unica dei sistemi quantistici

2 qubit nello stato $|\Phi\rangle_{AB} \in \boldsymbol{H}_A \otimes \boldsymbol{H}_B$

$|\Phi\rangle_{AB}$ Entangled state $\Leftrightarrow$ $\nexists \; |\varphi\rangle_A, |\phi\rangle_B$

$$|\Phi\rangle_{AB} = |\varphi\rangle_A \otimes |\phi\rangle_B$$

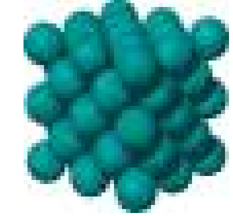
$$|\Psi^-\rangle_{AB} = 2^{-1/2}\left(|1\rangle_A |0\rangle_B - |0\rangle_A |1\rangle_B\right) \Rightarrow \rho_A = \rho_B = \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2}$$

$$|\Psi^-\rangle_{AB} = 2^{-1/2}\left(|\phi\rangle_A |\phi^\perp\rangle_B - |\phi^\perp\rangle_A |\phi\rangle_B\right) \Rightarrow$$

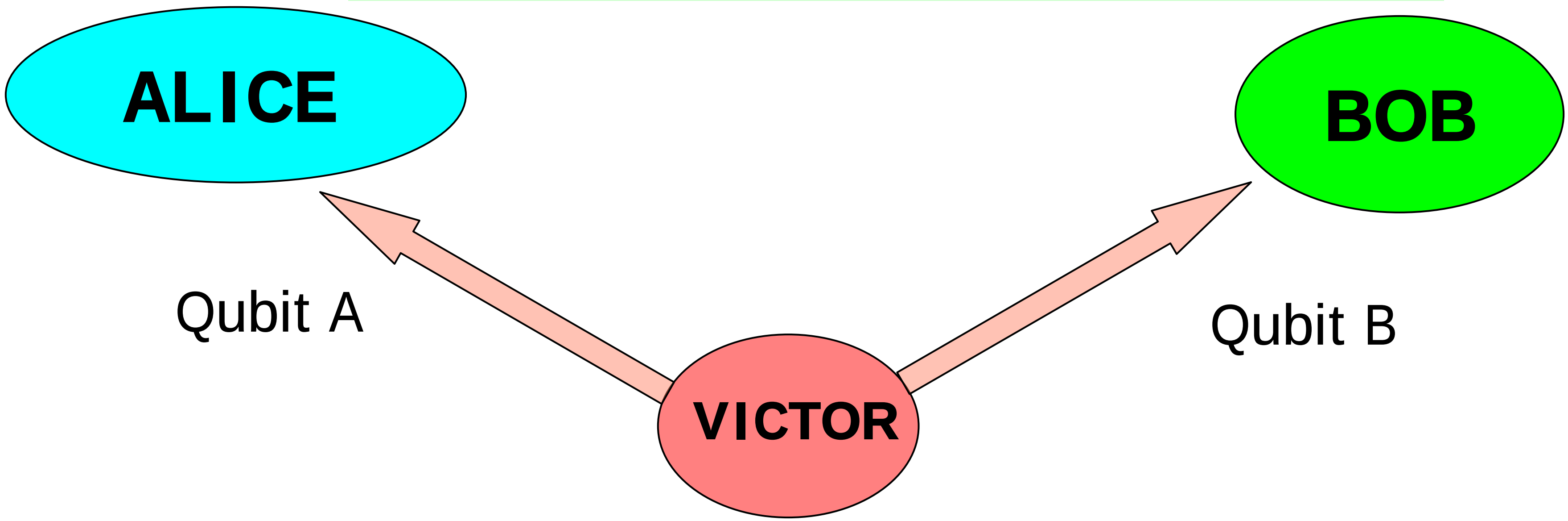
correlazioni in tutte le basi

“The best possible knowledge of the whole system does *not* include the best possible knowledge of its parts” (Schroedinger 1935)

Entanglement: non località



$$\left|\Psi^-\right\rangle_{AB} = 2^{-1/2}\left(\left|1\right\rangle_A\left|0\right\rangle_B - \left|0\right\rangle_A\left|1\right\rangle_B\right)$$



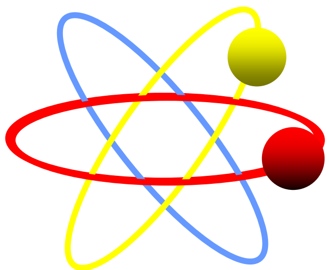
Misura sul qubit A → Informazione sullostato del qubit B

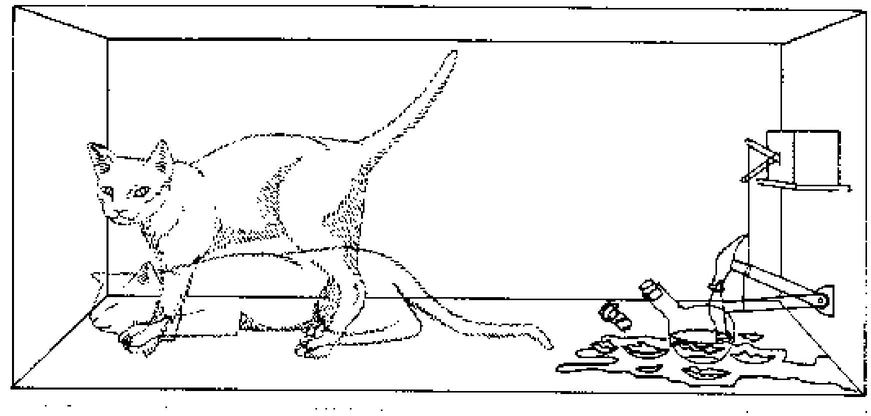
Einstein: “spooky action at distance”

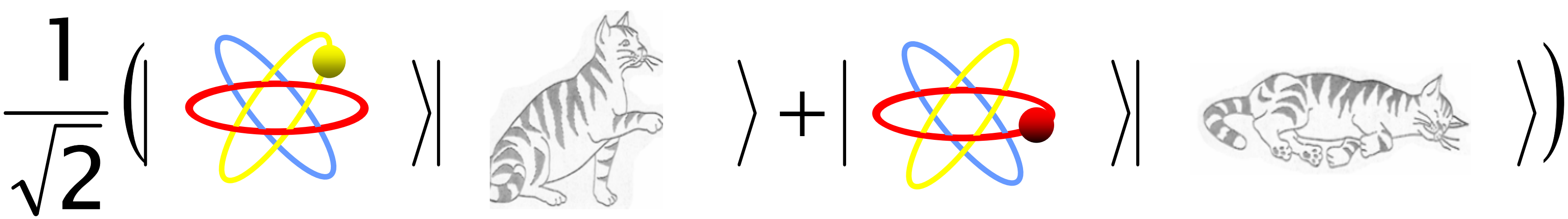
Entanglement: nuova risorsa per l’elaborazione dell’Informazione Quantistica

Transizione quantistico→classico
Il paradosso del gatto di Schroedinger

Atomo decade







Atomo non decaduto

Gatto vivo

Atomo decaduto

Gatto morto

Stato di sovrapposizione
(vivo <u>e</u> morto)

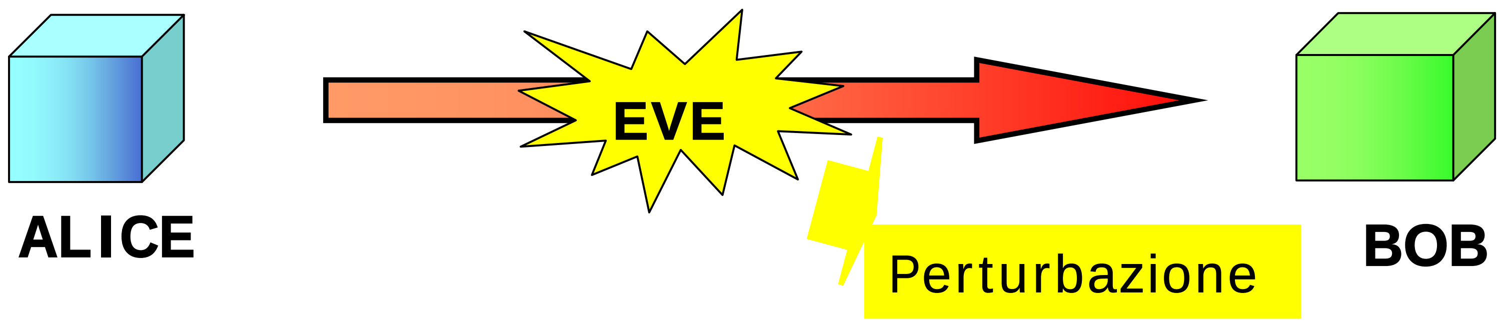
Perdita di coerenza

mistura statistica
(vivo <u>o</u> morto)

Crittografia quantistica: l’idea

Affidare la sicurezza della trasmissione alle leggi della fisica:

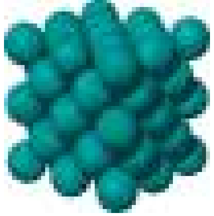
“Non è possibile effettuare una misura su un sistema quantistico senza perturbarlo”



Spionaggio ⇒ Misura ⇒ Perturbazione

Scopo della crittografia quantistica: distribuire una chiave segreta tra due utenti da usare come one-time pad

Nessuna perturbazione ⇒ Chiave sicura



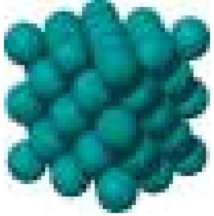
Necessario manipolare in modo controllato sistema quantistico

DIVERSI APPROCCI SPERIMENTALI:

- **<u>Singoli ioni</u>** intrappolati con campi magnetici e manipolati mediante laser
- Dispositivi superconduttori: **<u>SQUID</u>** (Superconducting Quantum Interference Device)
- **<u>Atomi neutri</u>** in reticoli ottici
- **<u>Singoli fotoni</u>** in stati entangled
- **<u>Spin in semiconduttori</u>** (electron or nuclear spins)

etc..

Quantum Optics for Quantum Information Processing



- Qubit state $\alpha|0\rangle + \beta|1\rangle \Longrightarrow \alpha|H\rangle + \beta|V\rangle$

  Polarizzazione di un singolo fotone

  $|0\rangle \Leftrightarrow |H\rangle$ ***polarizzazione orizzontale***

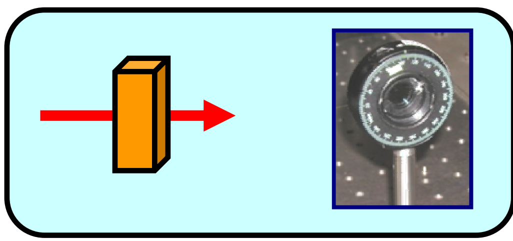
  $|1\rangle \Leftrightarrow |V\rangle$ ***polarizzazione verticale***

  Mode of the electromagnetic field (k,λ)

  $\lambda = \mathbf{800}nm$

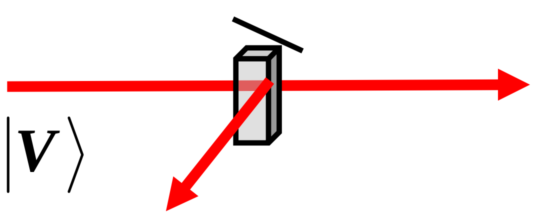
- Trasformazione del qubit

  Rotazione della polarizzazione: lamine



- Misura proiettiva

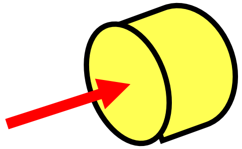
  polarizing beam splitter



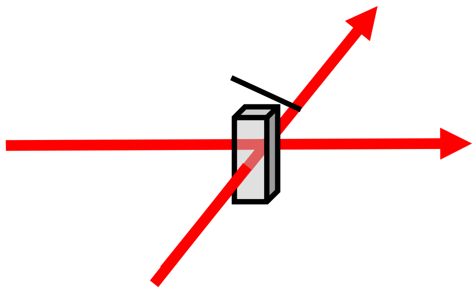
$|H\rangle$

$|V\rangle$

Rivelatore a singolo fotone



- Interazione
  - Lineare
    Polarizing beam-splitter
    Beam-splitter:
    - Bell measurement



  - Non-lineare
    - Mezzo amplificatore
    - Interazione con atomi

- Generazion di stati entangled
  - Interazione parametrica
- Hardware più adatto per comunicazione quantistica

Generazione di stati bifotoni: Fluorescenza parametrica

- Interazione fra un fascio laser molto intenso ed un cristallo

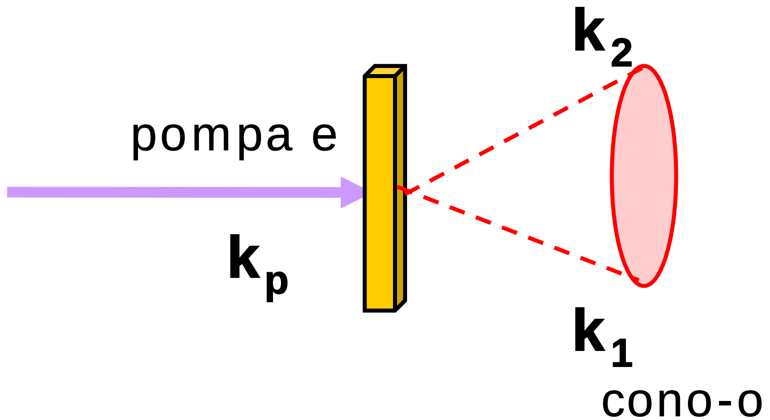
- Fenomeno non-lineare del 2° ordine (avviene in cristalli non-centrosimmetrici $\chi^{(2)} \neq 0$): accoppiamento fra onde di diverse frequence dovuto al contributo di polarizzazione non-lineare

- Conservazione dell'energia

$$\hbar\omega_P = \hbar\omega_1 + \hbar\omega_2$$

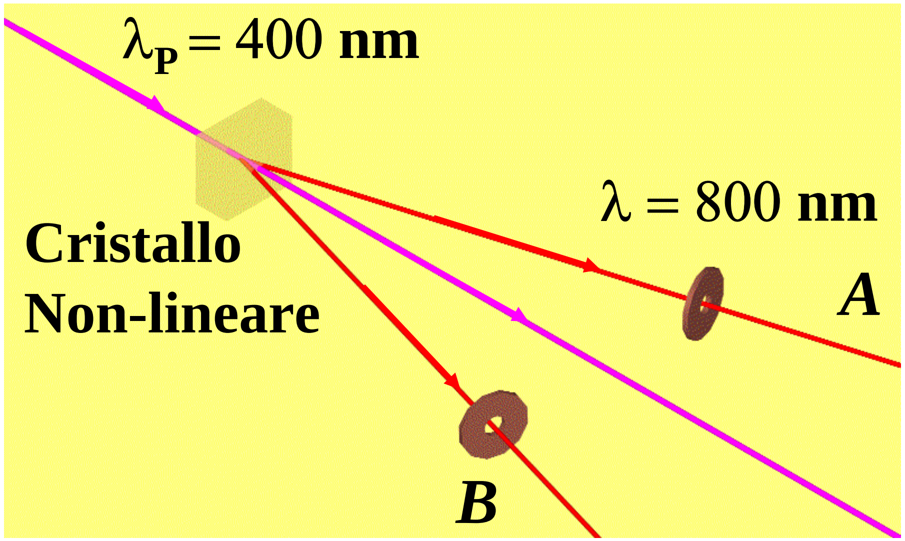
- Conservazione del momento (phase-matching)

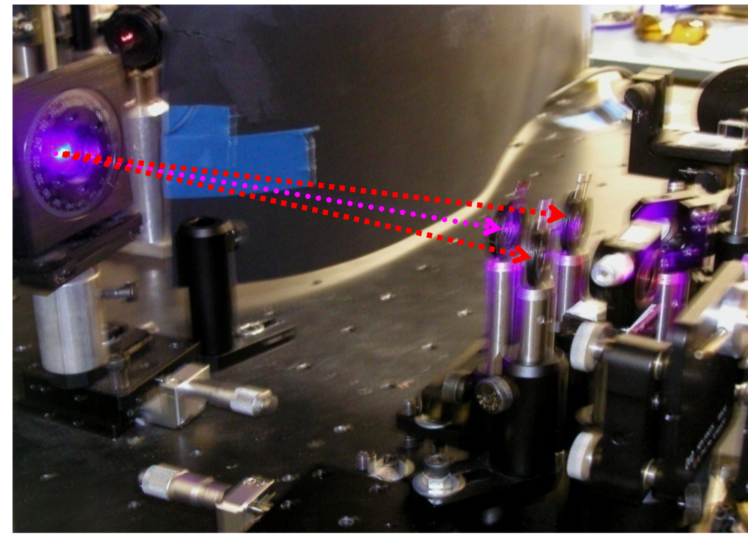
$$\vec{k}_P = \vec{k}_1 + \vec{k}_2$$



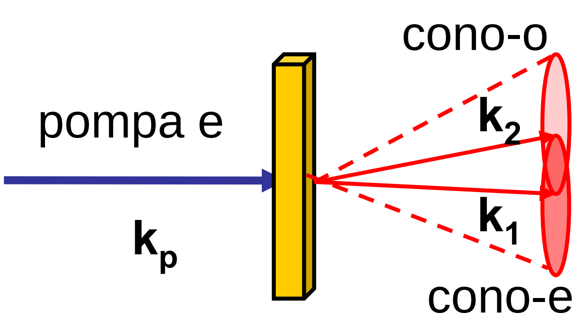
- Regime spontaneo: efficienza molto bassa probabilità che un fotone di pompa generari una coppia $\approx 10^{-9}$

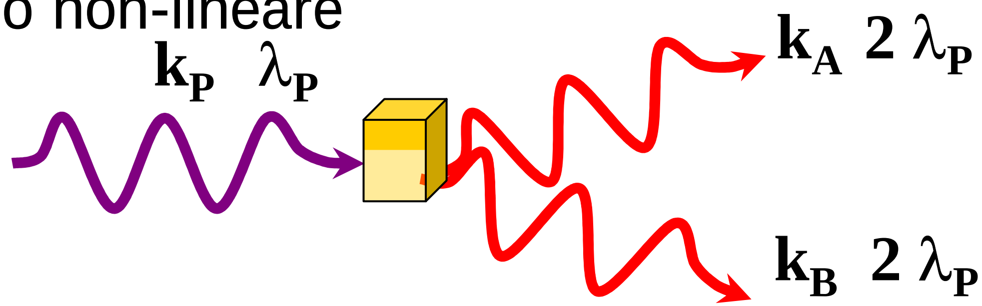
Generazione di stati entangled in polarizzazione





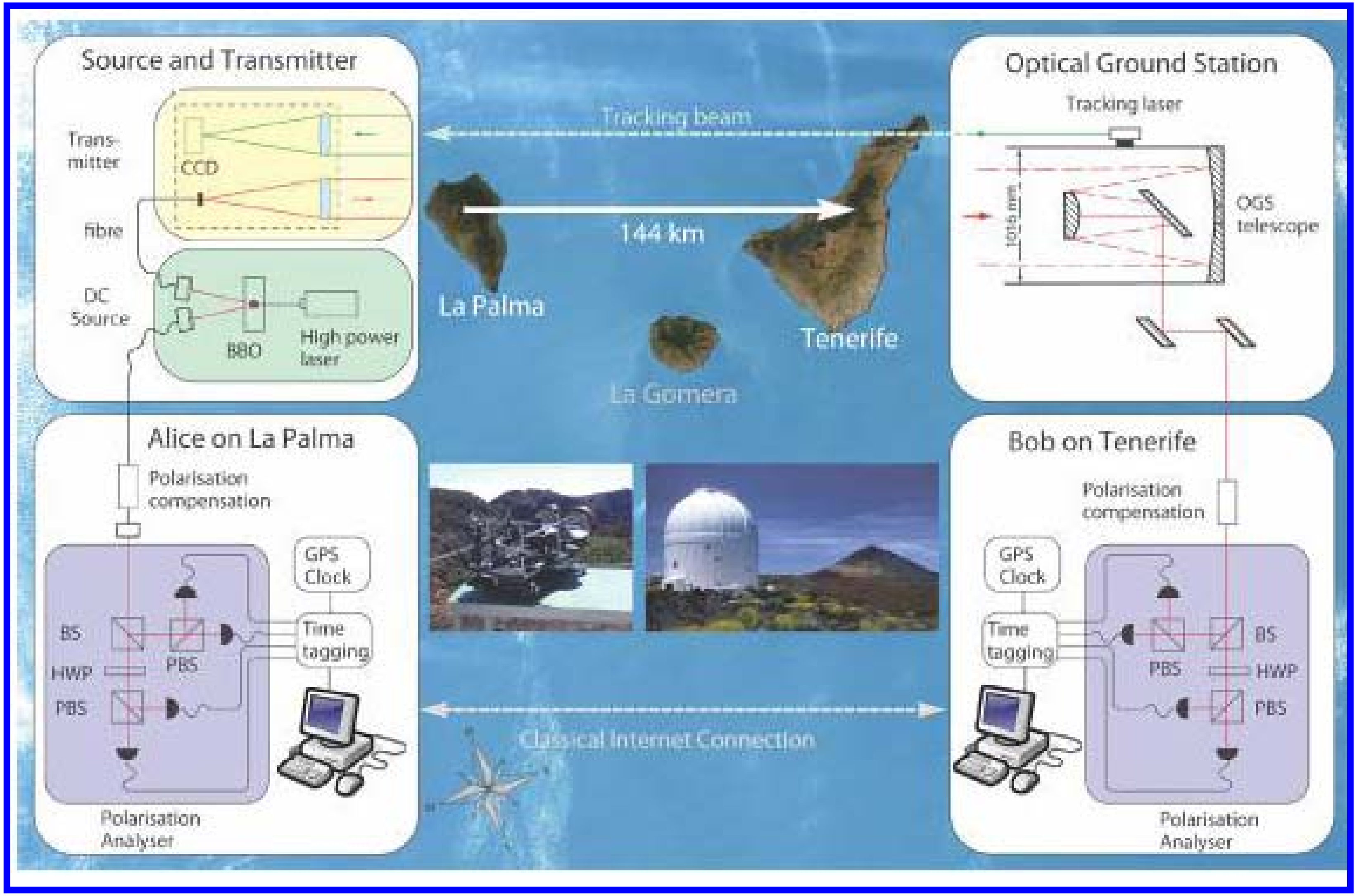
Interazione parametrica: cristallo non-lineare e LASER di frequenza ν_P





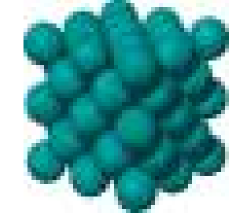
$$\left|\Psi^-\right\rangle_{AB} = \frac{\left|V\right\rangle_A \left|H\right\rangle_B - \left|H\right\rangle_A \left|V\right\rangle_B}{\sqrt{2}}$$

Crittografia quantistica su lunga distanza: 144 km

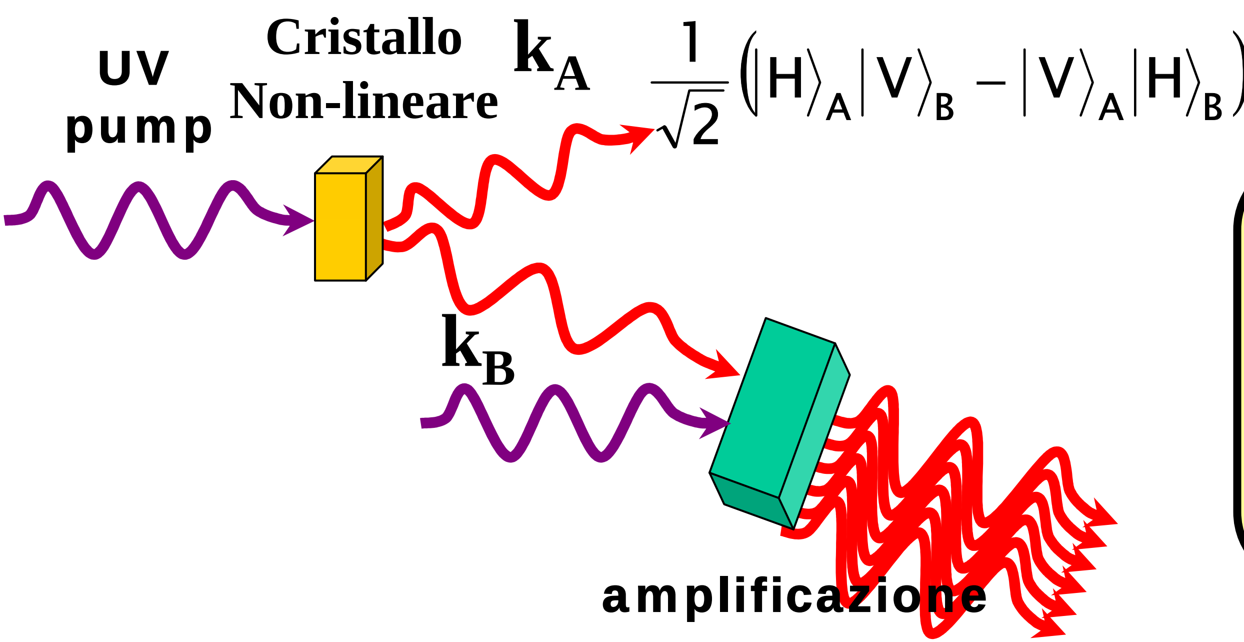


- Attività di ricerca:
  - Studio della transizione quantistico→classico
    - Generazione di stato di “Gatto di Schrodinger”
    - Test di non-località con violazione crescente
  - Generazione di stati entangled di molti qubits
    - Entanglement di due particelle in diversi gradi di libertà
    - Computazione quantistica con fotoni
    - Studio di circuiti quantistici integrati
    - Momento angolare orbitale di stati a singolo fotone
  - Sviluppo di protocolli di informazione quantistica
    - Trasmissione su canali di comunicazione rumorosi
    - Quantum private queries

Transizione mondo quantistico → classico



Amplificazione di una coppia di fotoni entangled



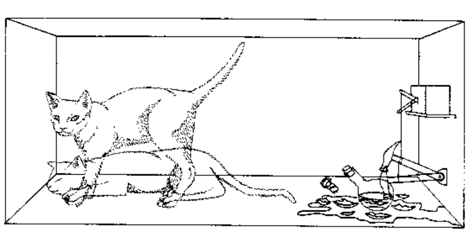
Amplificatore macroscopico

Iniezione

Stato quantistico

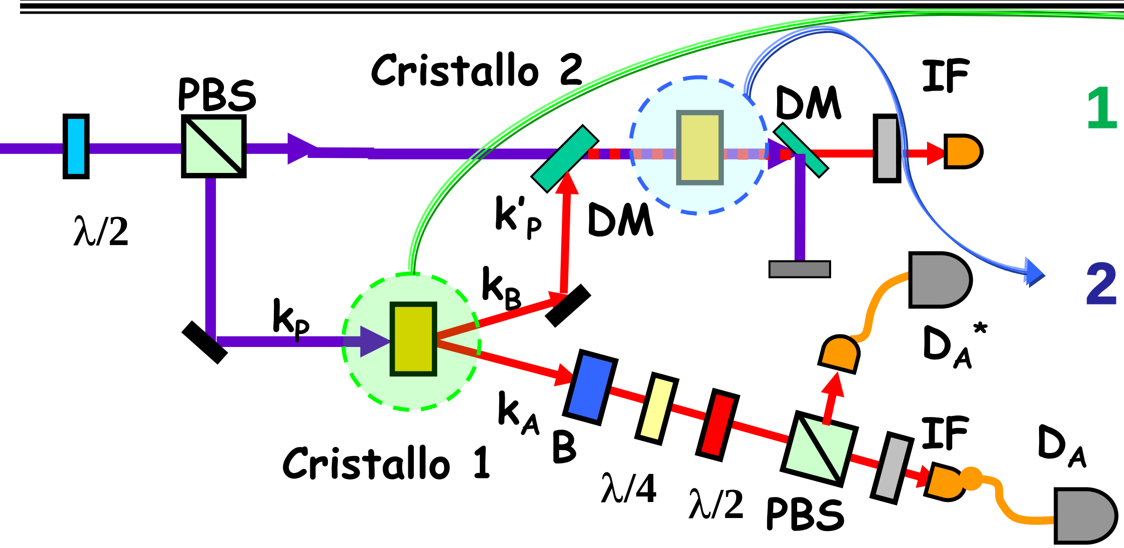
(stato a singolo fotone)

- **Multiphoton entanglement: nuove prospettive in quantum information**
- **"Schroedinger apologue": Entanglement fra un singolo fotone ed un "cat" state**



$$|\Sigma\rangle = \frac{1}{\sqrt{2}}\left(|H\rangle|\quad\rangle + |V\rangle|\quad\rangle\right)$$

Stati entangled a molte particelle

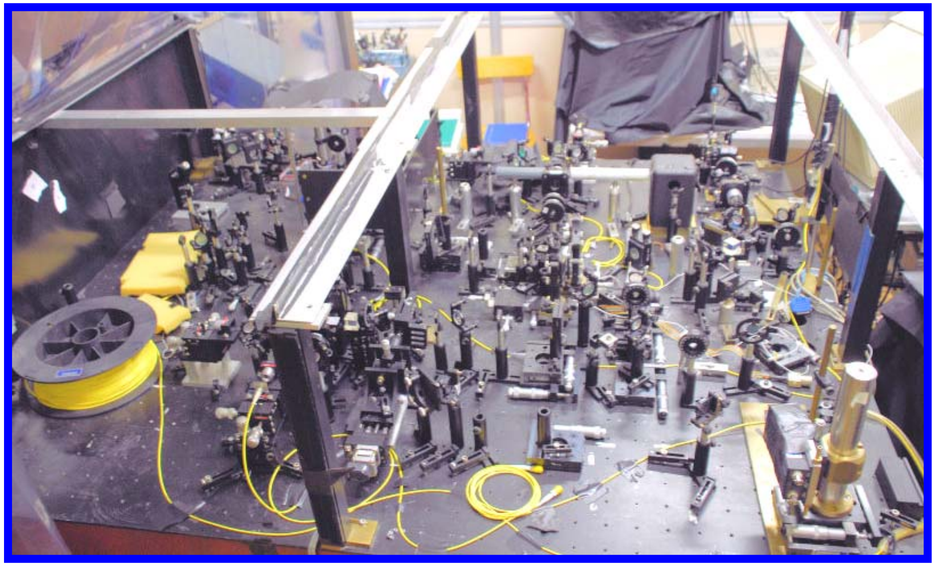


1. Generazione della coppia entangled
2. Amplificazione

$\langle n \rangle \sim 5 \times 10^4$ particelle

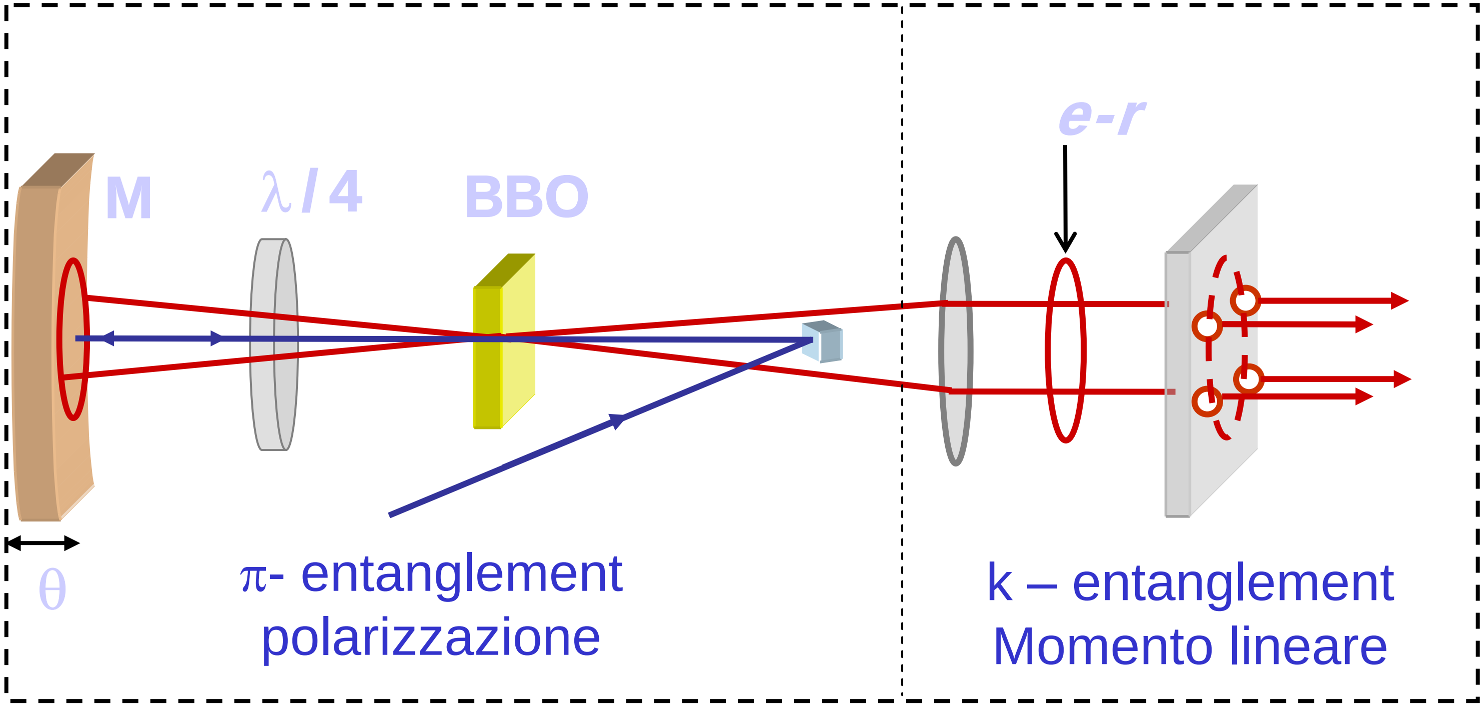
Prospettive:

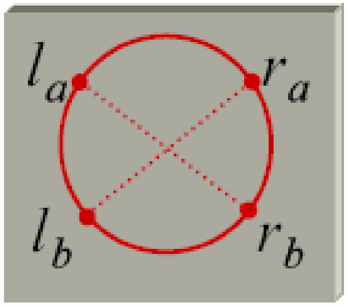
- Accoppiamento ed entanglement con un sistema atomico
- Entanglement tra due sistemi Macroscopici
- Decoerenza e transizione mondo quantistico-> mondo classico



Hyper-entangled states

Entanglement su diversi gradi di libertà

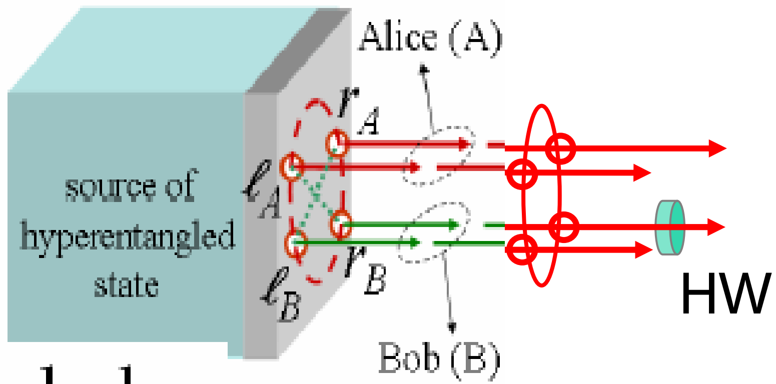


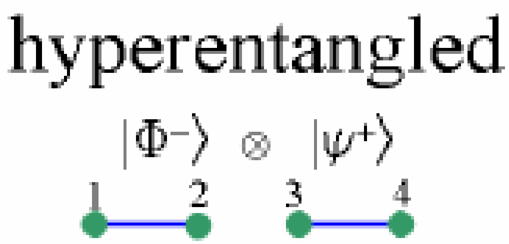


$$|\Pi\rangle = \frac{1}{\sqrt{2}}\left[|H_a H_b\rangle + e^{i\theta}|V_a V_b\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|l_a r_b\rangle + e^{i\phi}|r_a l_b\rangle\right]$$

2 photons → 4 qubits

Creazione di cluster states da hyper-entangled states



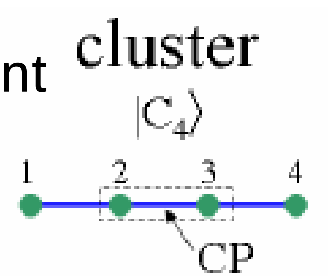


$$|\Pi\rangle = \frac{1}{\sqrt{2}}\left[|H_a H_b\rangle + e^{i\theta}|V_a V_b\rangle\right] \otimes \frac{1}{\sqrt{2}}\left[|l_a r_b\rangle + e^{i\phi}|r_a l_b\rangle\right]$$

qubit

entanglement

Porta logica C-NOT
fra momento e polarizzazione

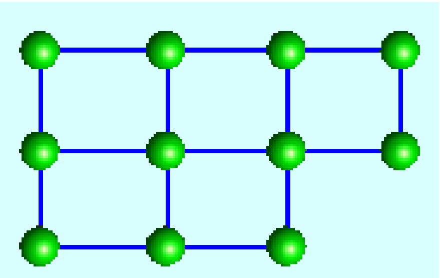


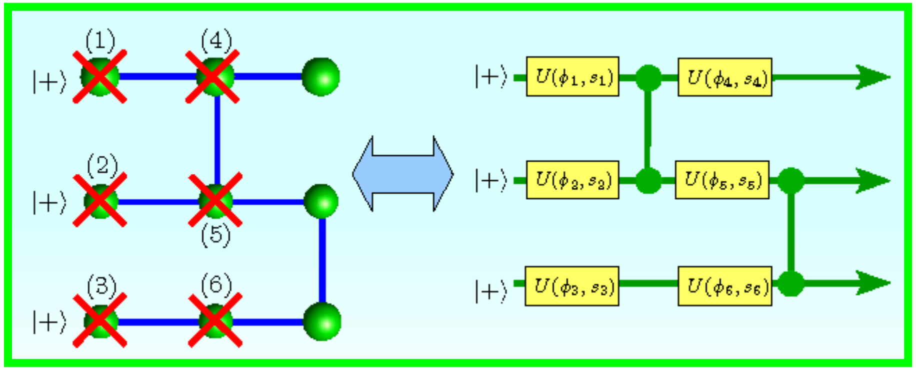
$$\frac{1}{4}\left[|H_a l_a\rangle|H_b r_b\rangle + |H_a r_a\rangle|H_b l_b\rangle + |V_a l_a\rangle|V_b r_b\rangle - |V_a r_a\rangle|V_b l_b\rangle\right]$$

Risorsa fondamentale per la one-way quantum computing

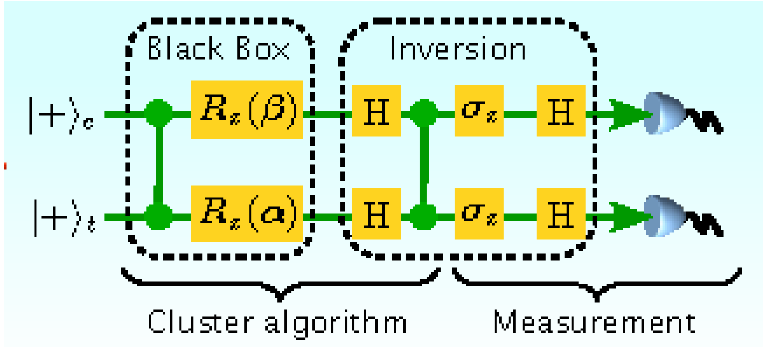
Computazione quantistica con fotoni

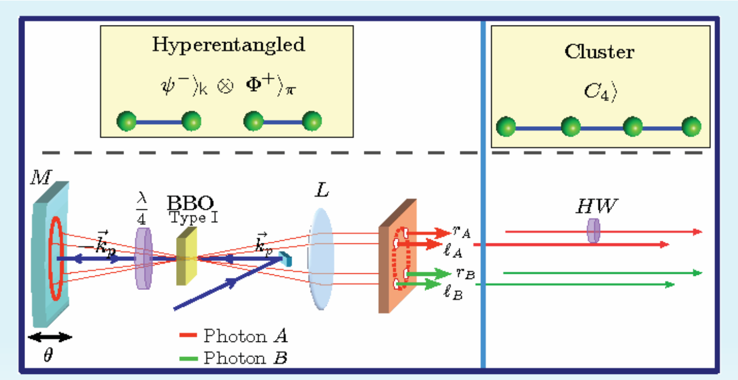
- One-way quantum computing
  - Cluster states: stato entangled di n qubits
  - Serie di misure e rotazioni su singolo qubits





- Computazione quantistica con i fotoni

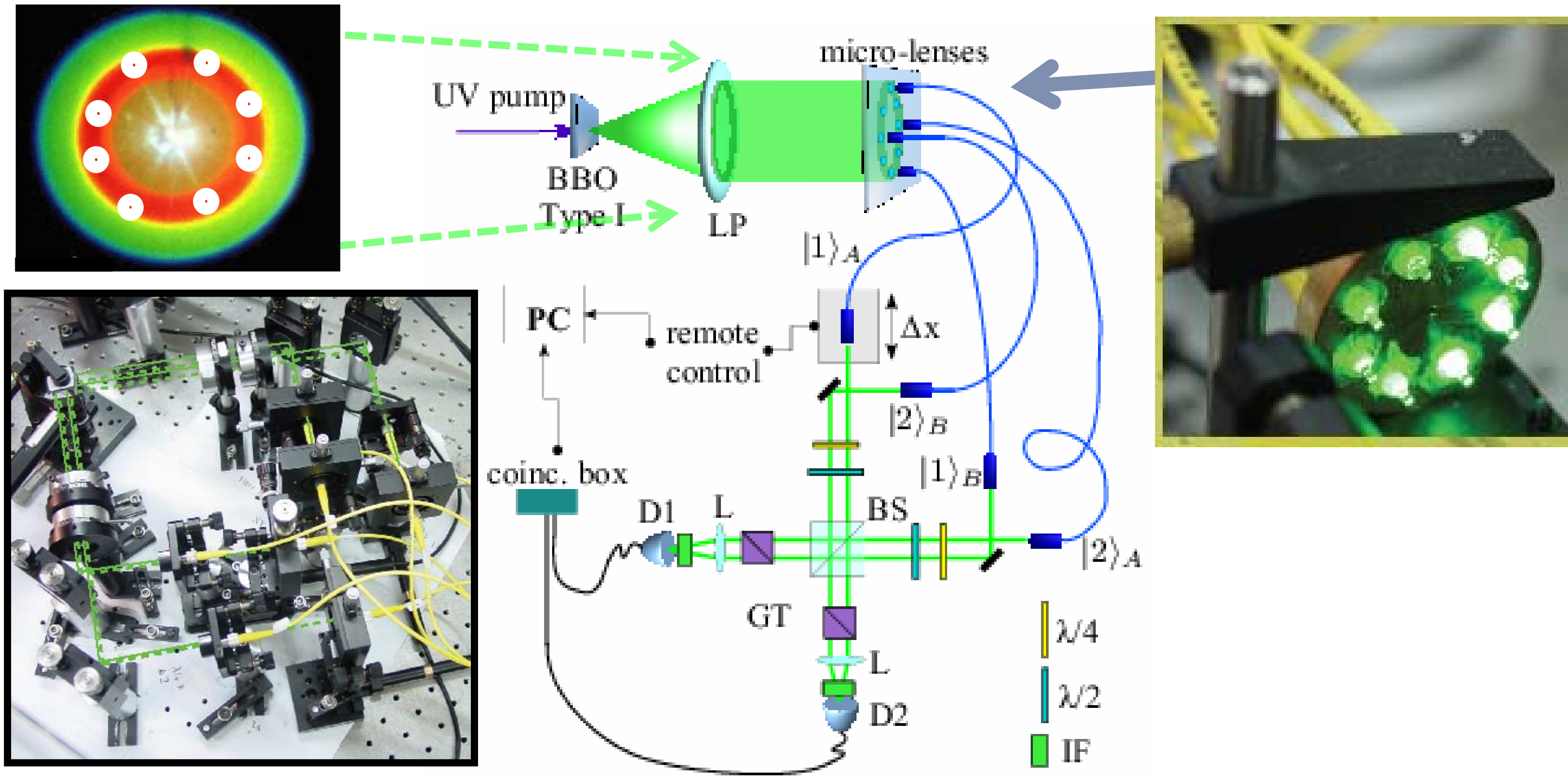




Generazione di stati entangled di molti qubits

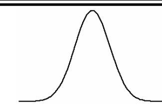
- Aumento numero di qubits n:

Generazione coerente di coppie di fotoni su un più modi

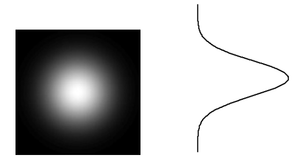


Momento angolare orbitale del singolo fotone

$\mathrm{HG}_{00} = \mathrm{LG}_{00}$

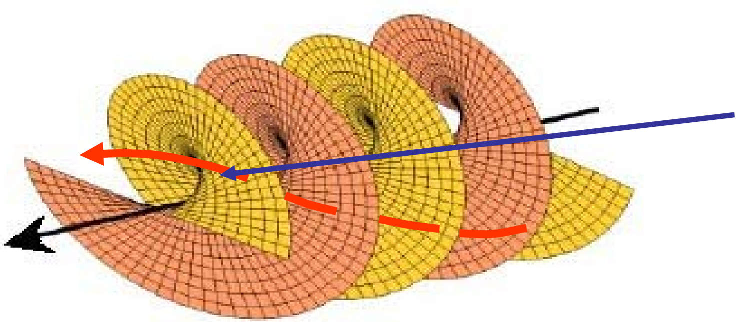


TEM_{00} mode :



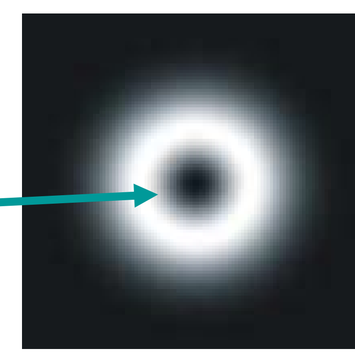
Laguerre-Gauss : $u_{p,l}(r,\varphi,z) \propto u(r,z)e^{il\varphi}$

Termine di fase elicoidale
$l = 0\ ,\pm 1\ ,\pm 2\ ,\ldots$



Punto di incontro delle fasi diverse al variare dell'angolo

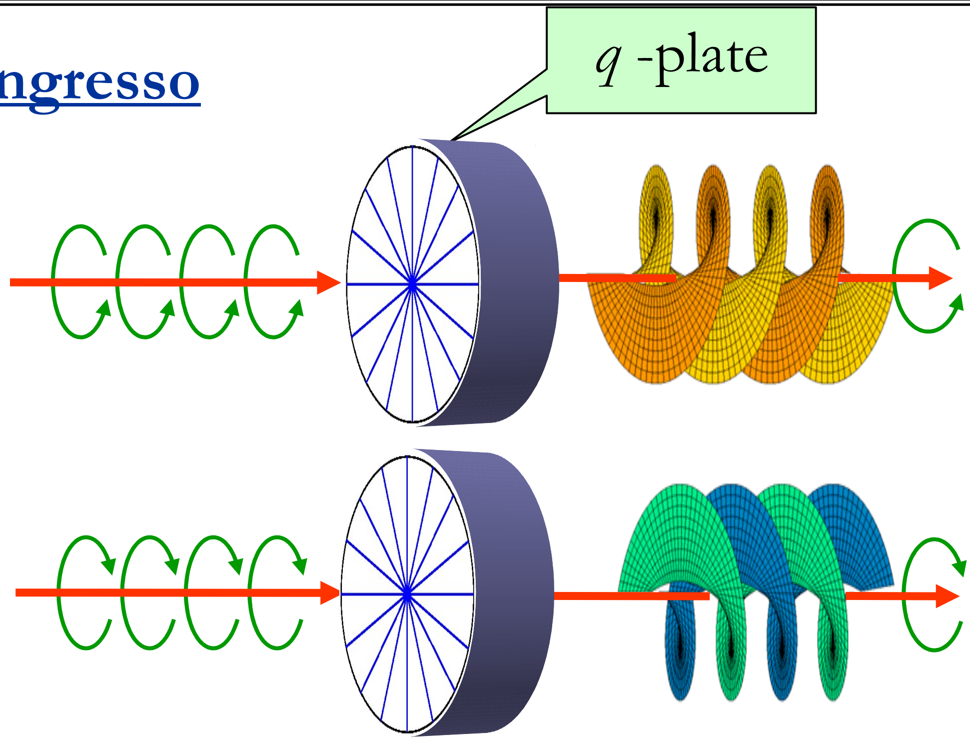
Doughnut Mode (vortice ottico)



L'OAM trasportato è pari a **$l\hbar$ per fotone**

Manipolazione del momento angolare orbitale: q-plate

Stato in ingresso — **Stato in uscita**



Spin: $S_z = -\hbar$
TEM$_{00}$: $L_z = 0$

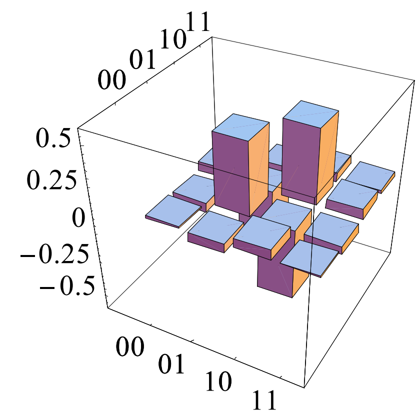
Spin: $S_z = +\hbar$
Orbitale: $L_z = -2\hbar$

Spin: $S_z = +\hbar$
TEM$_{00}$: $L_z = 0$

Spin: $S_z = -\hbar$
Orbitale: $L_z = +2\hbar$

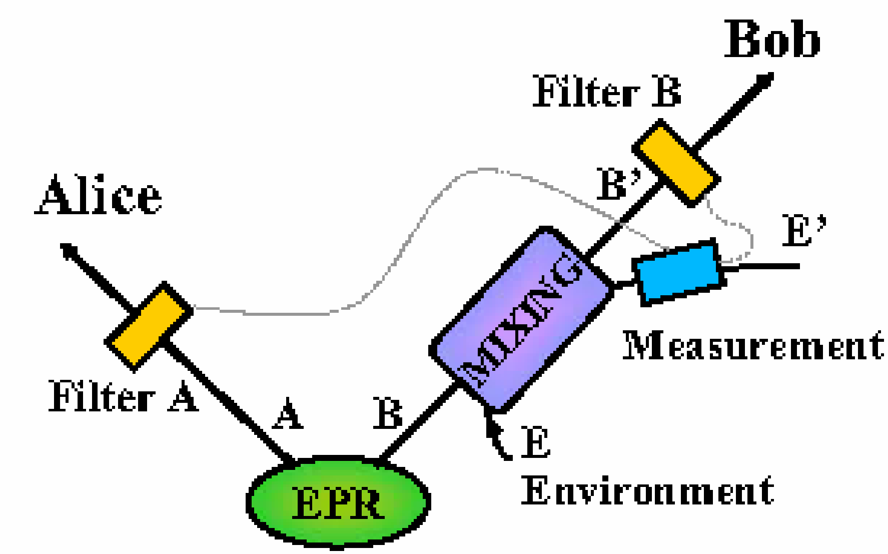
Entanglement fra diversi gradi di libertà

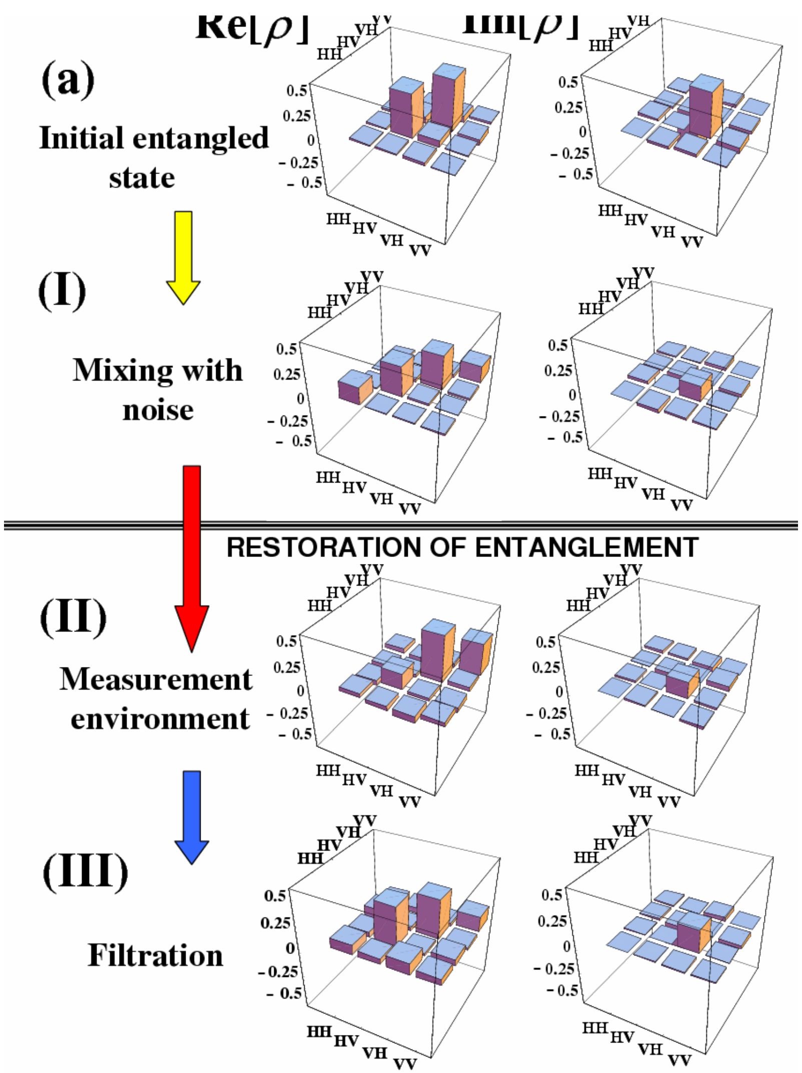
$$\left.\begin{array}{l}|H\rangle_\pi |0\rangle_l \\ |V\rangle_\pi |0\rangle_l\end{array}\right\} \xrightarrow{QP} \frac{1}{\sqrt{2}}\left(|L\rangle_\pi |-2\rangle_l \pm |R\rangle_\pi |+2\rangle_l\right)$$



Protocolli di informazione quantistica

- Sviluppo di protocolli per la trasmissione di fotoni entangled su canali di comunicazione rumorosi



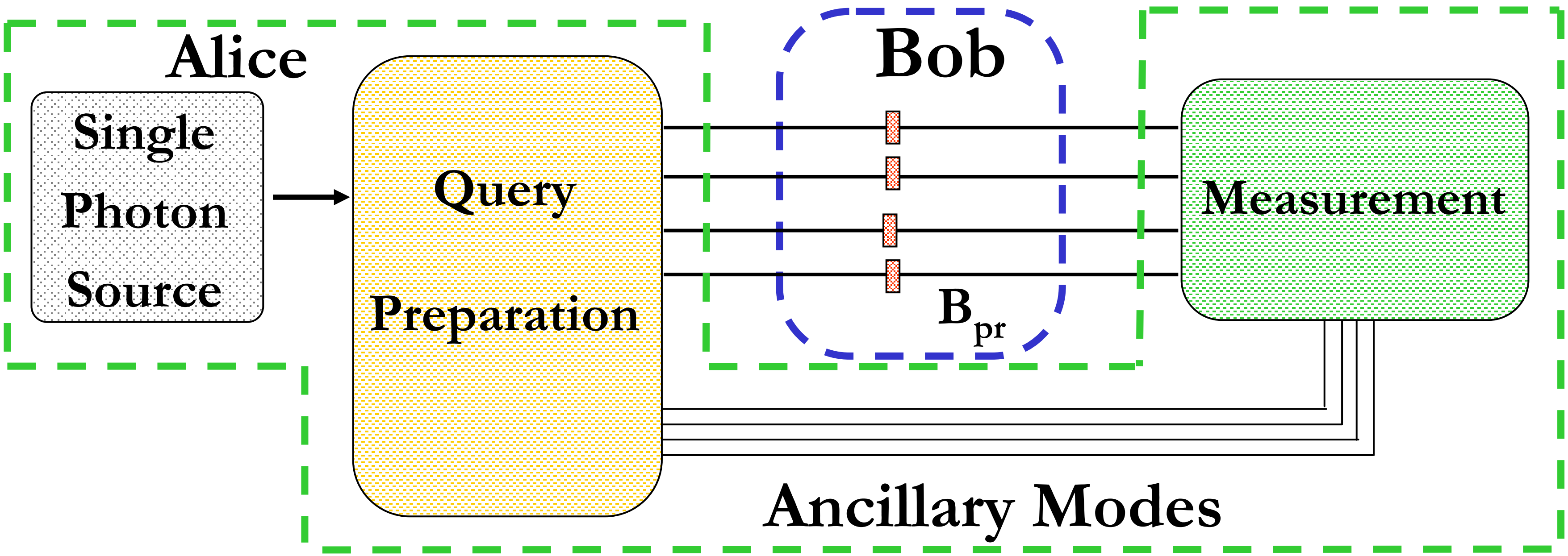


Protocolli di informazione quantistica
Quantum Private Queries

Alice → User Privacy

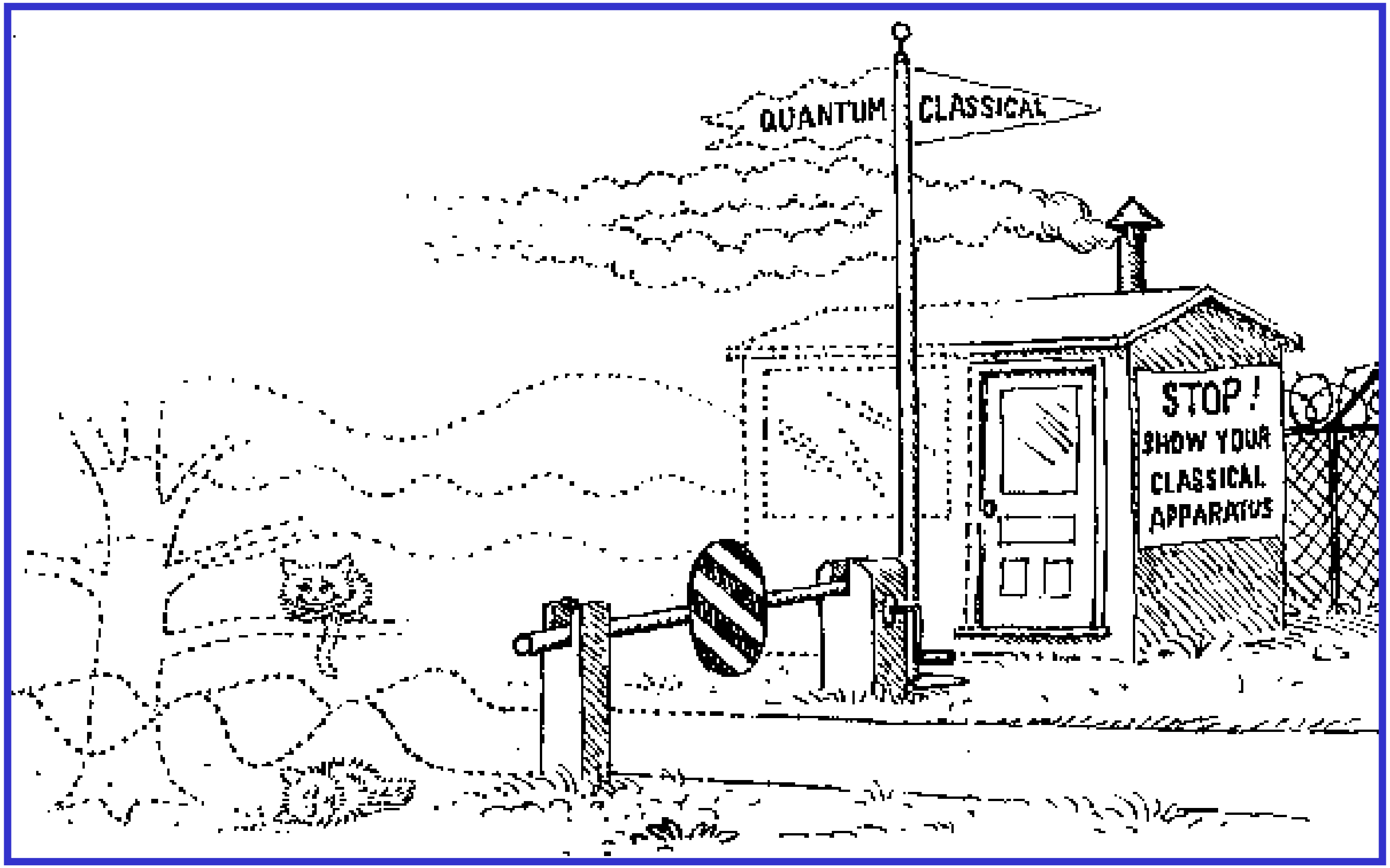
Bob → Database Privacy

→ **QPQ protocol:** interrogare il database con un multi-qubit per garantire la sicurezza di Alice e Bob



Implementazione Sperimentale:

Singolo Fotone
- Modo spaziale → **Qubit register**
- Polarizzazione → **Qubit bus**



http://quantumoptics.phys.uniroma1.it