Computación Cuántica

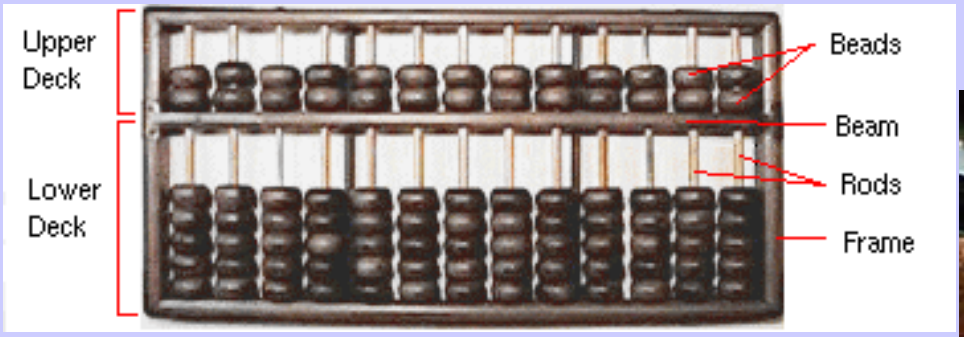
Marcos Saraceno
Departamento de Fisica - CNEA

Desde 1997, colaboración UBA-CNEA-CITEFA
Juan Pablo Paz, Alejandro Hnilo, Augusto Roncaglia
Leonardo Ermann, Cecilia Cormick, M.S.

Raymond Laflamme (UW)
Many Knill (LANL)
Wojciech Zurek (LANL)
David Cory (MIT)

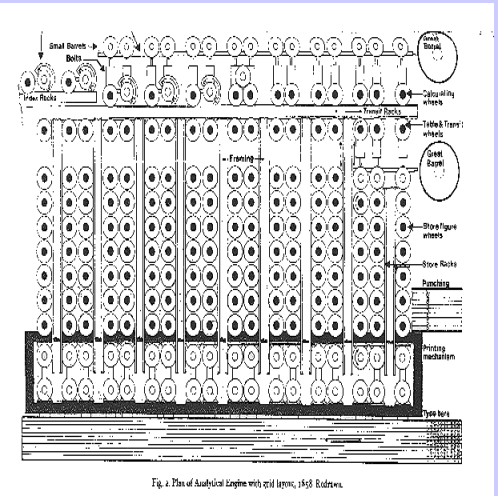
Las etapas de la computacion

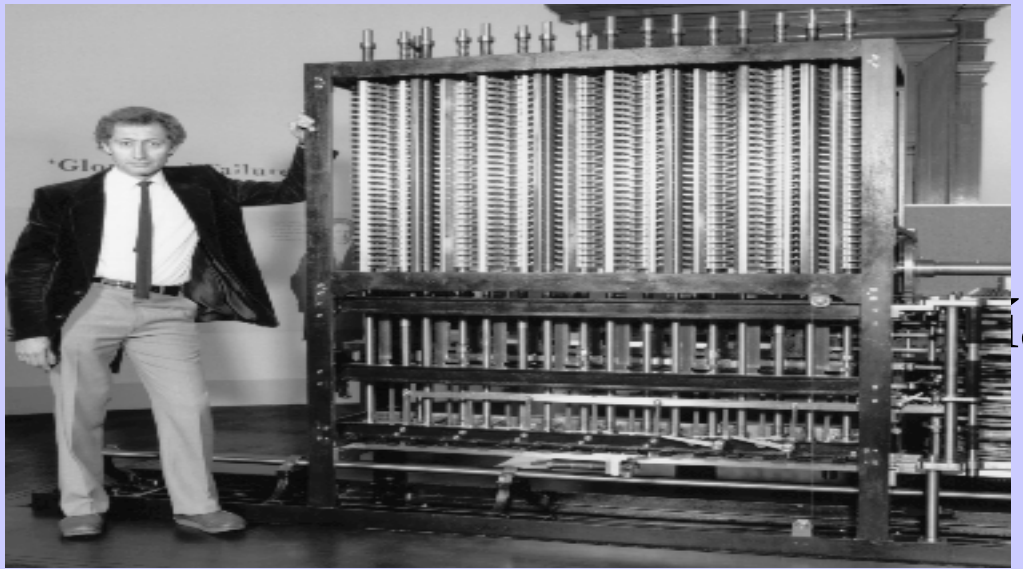
La etapa mecanica : Palancas , engranajes,..(Escala: metro)



Ábaco (chino, siglo XIII).

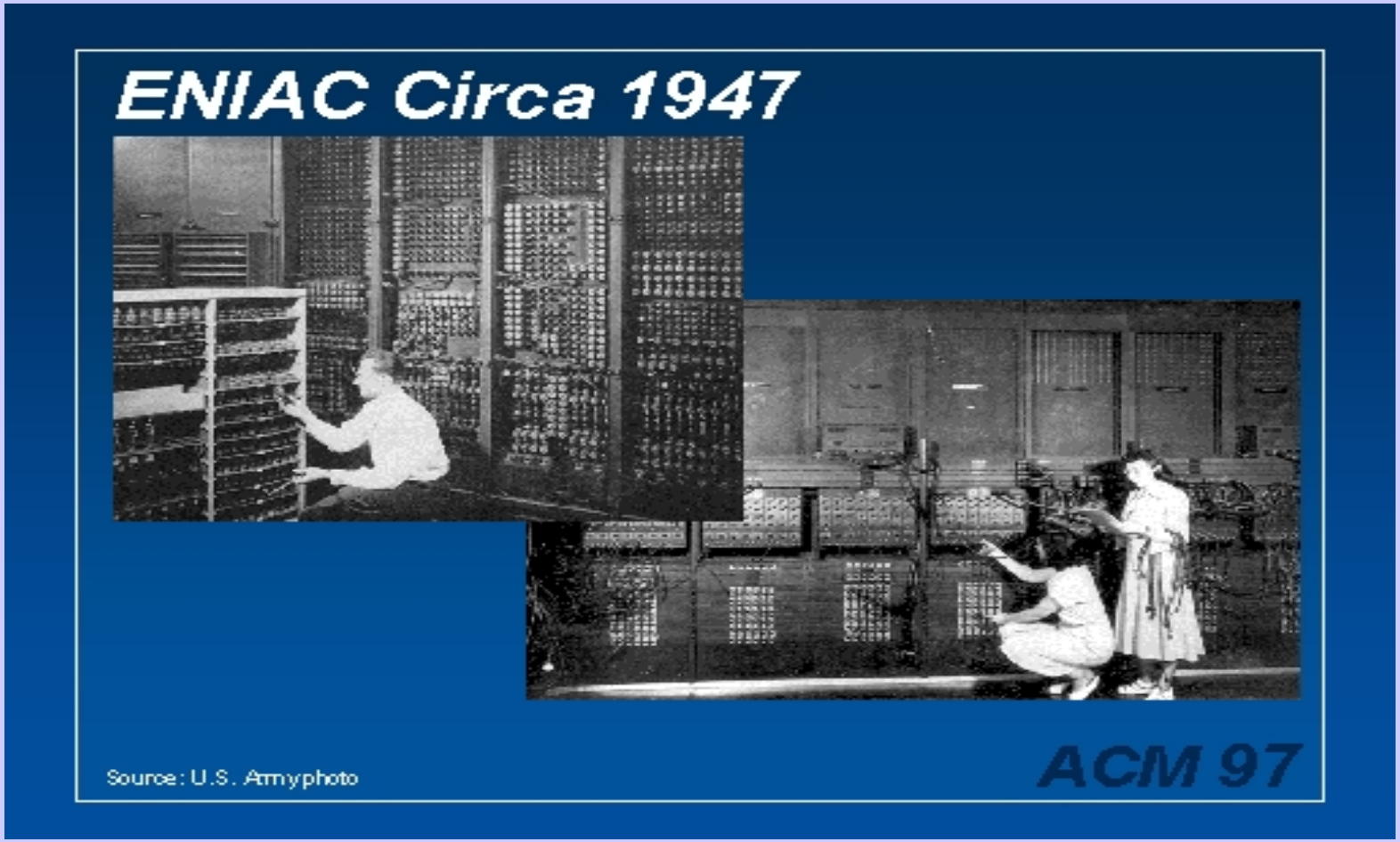
La maquina diferencial de Babbage (1830)





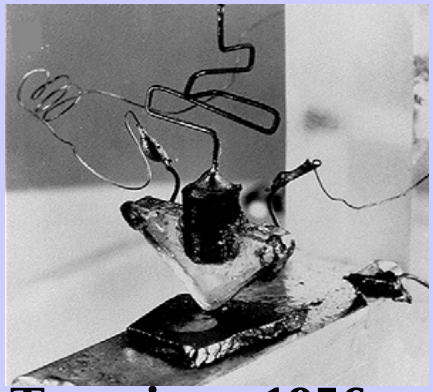
ía

La etapa electronica: valvulas termoionicas, interruptores Mecanicos, cintas de papel, tarjetas. (Escala: cm)

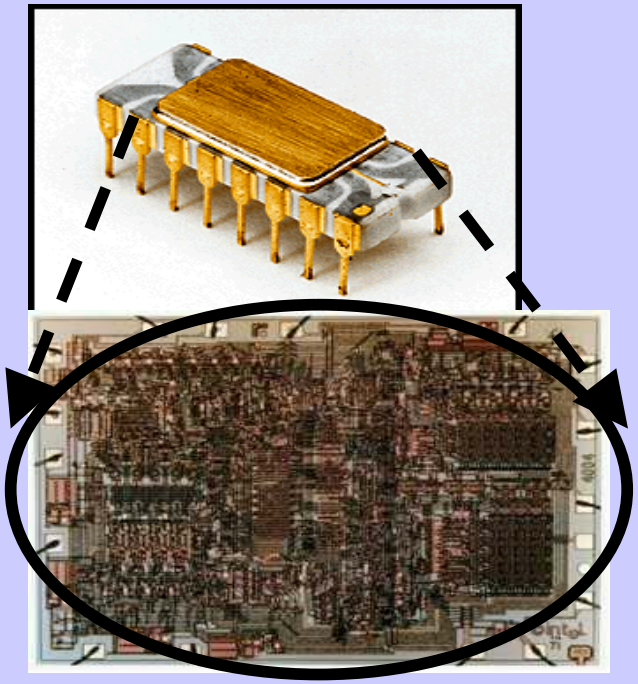


La etapa microelectronica: transistores, circuitos integrados, estados de carga de capacitores, dominios magneticos. (Escala=micron)

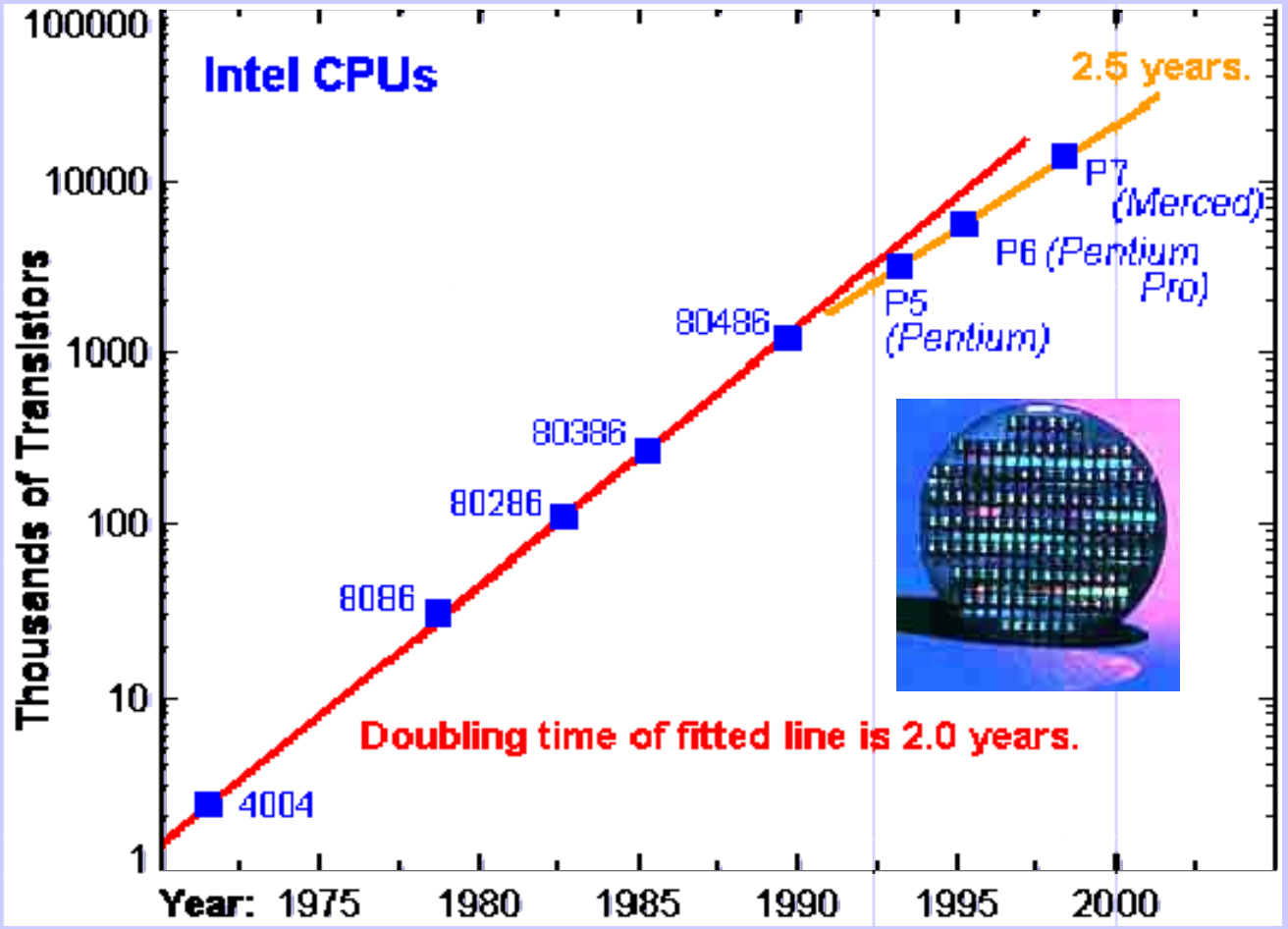
(Ley de Moore: El número de transistores por chip se duplica cada 18 meses.)



Transistor 1956



Intel 4004: 2500 transistores



Qué es una computadora?

Sistema que almacena, procesa y transmite información. Esta implementado sobre un sustrato material y por lo tanto su comportamiento - y sus limitaciones - esta regido por leyes fisicas.

La relatividad limita la velocidad con la que se puede transmitir la informacion.

La termodinamica rige la disipacion de energia cuando se borra informacion .

La mecanica cuantica ???

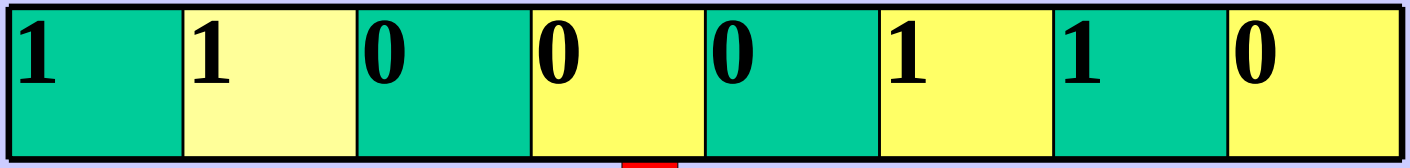
Información es física! No hay información sin una representación material concreta!

Computadoras Clásicas

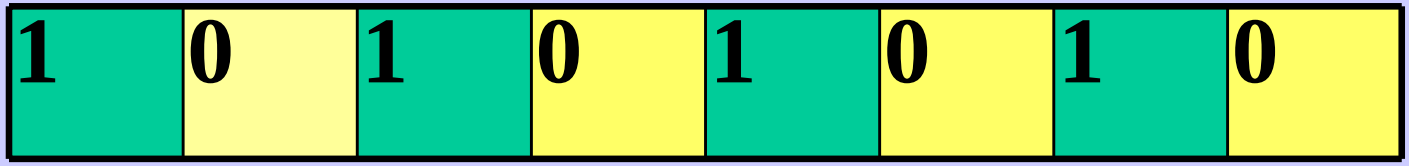
- Los estados computacionales están codificados en tiras de N bits con valores 0 o 1
- Los estados computacionales son realizados por medio de objetos clásicos macroscópicos (agujeros en una cinta de papel, cargas en un capacitor, dominios magnéticos en un disco duro, etc...)
- La computadora ejecuta secuencialmente un cálculo por vez y recorre una "trayectoria" en el espacio de estados. En cada instante la computadora está en un estado computacional bien definido.

Evolución de una computadora clásica

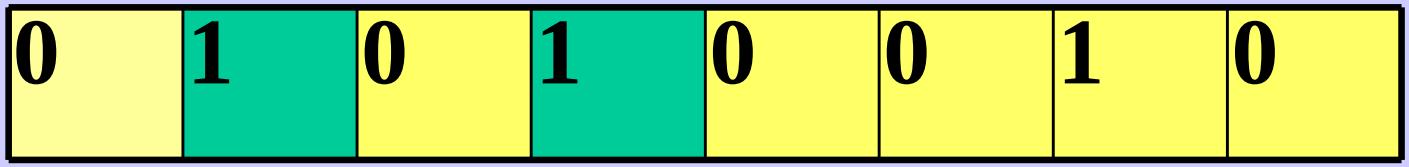
Estado inicial



Primer paso:



Segundo paso:

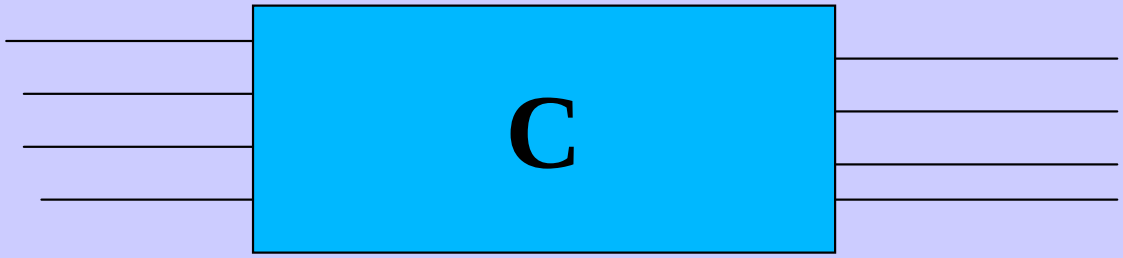


Etc...

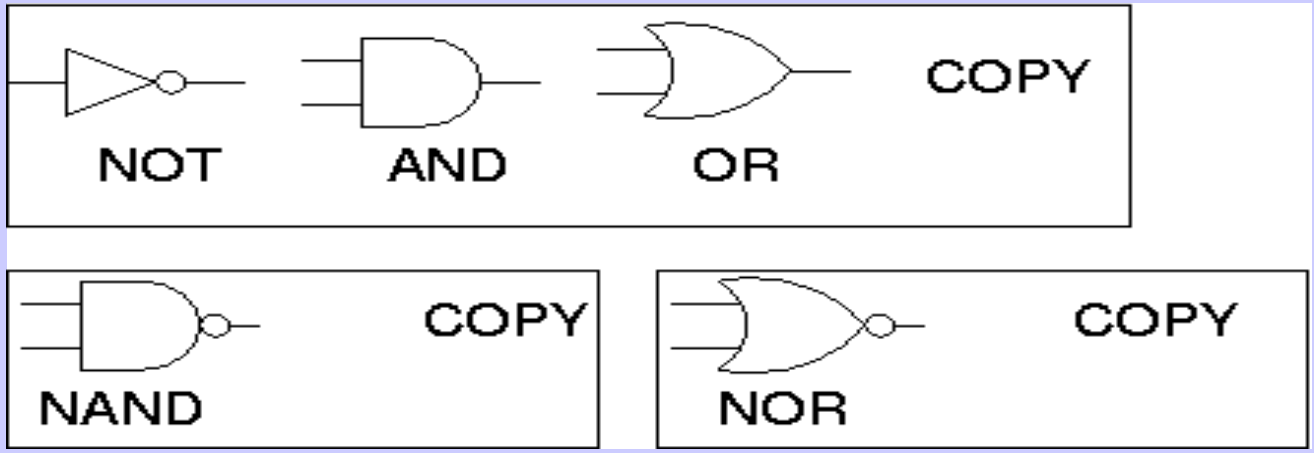
.

La computadora recorre una secuencia de estados: Sigue una trayectoria!

El modelo de computación clásica



La construcción practica de una computadora se basa en el siguiente teorema: Toda función C es realizable por medio de un numero limitado de compuertas standard llamados conjuntos universales.



Problemas fáciles y difíciles (para una computadora clásica)

- El tamaño del espacio computacional Ω crece exponencialmente con el numero N de bits.

- Problemas fáciles: Son los que requieren un numero de operaciones polinomial en N

  * Suma y producto de dos numeros
  * Búsqueda de un dato en una base ordenada

- Problemas difíciles: Son los que requieren un numero de operaciones del orden de Ω. Requieren explorar todo el espacio computacional.

  * Encontrar los factores primos de un número.
  * Búsqueda en una base desordenada.
  * Viajante de comercio.

Teoria de la complejidad...

Mecánica Cuántica (I)

• Linealidad: Un sistema cuántico que puede existir en los estados $|0>$ o $|1>$ tambien puede ser preparado en las combinaciones lineales

$$|\Psi>=\alpha|0>+\beta|1>$$

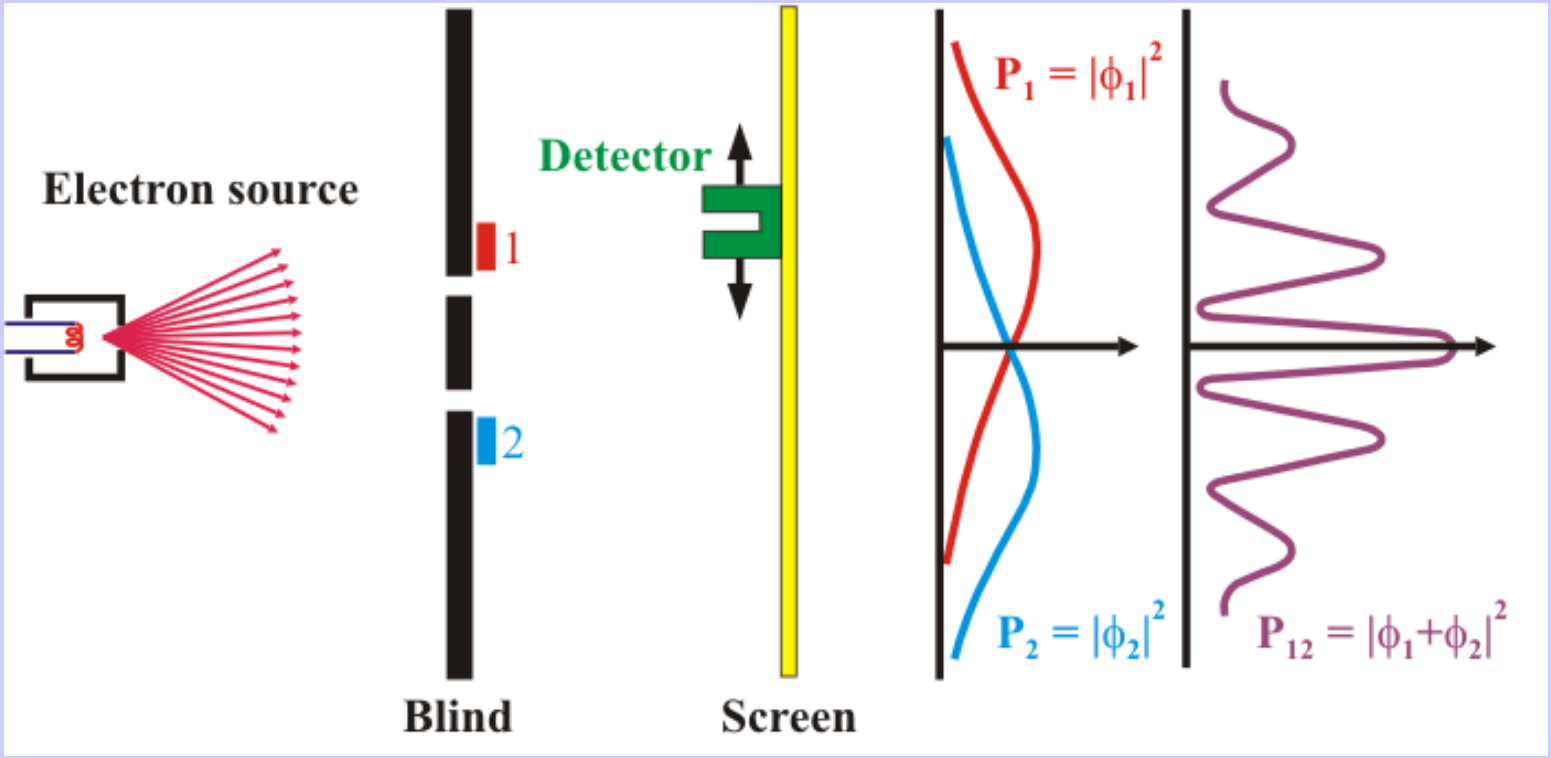
En este estado el sistema se encuentra a la vez en $|0>$ y en $|1>$. Este estado es muy distinto a una mezcla estadística de $|0>$ y $|1>$.

• Interferencia: Los sistemas cuánticos se propagan como ondas y se detectan como partículas. La probabilidad de detección proviene de la interferencia de todos los caminos que la partícula puede tomar.

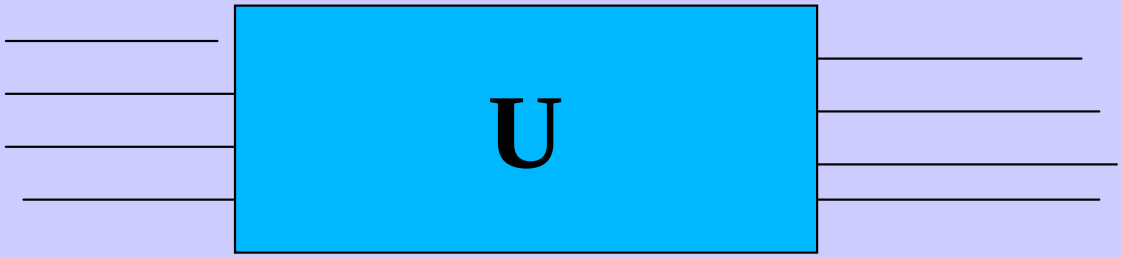
Mecánica Cuántica (II)

• Entrelazamiento: Es uno de los efectos mas misteriosos y anti-intuitivos de la mecánica cuántica. Implica correlaciones "extrañas" entre partículas que han interactuado en el pasado y que persisten a pesar que éstas se separen y dejen de interactuar.

• Decoherencia: Es la gran enemiga de la computación cuántica. Es producida por las interacciones del sistema con su entorno, ya que ningun sistema está completamente aislado. La decoherencia hace que las combinaciones lineales de objetos macroscópicos decaigan muy rapidamente y el sistema se vuelva clásico.


Electron source
1
2
Detector
Blind
Screen
$P_1 = |\phi_1|^2$
$P_2 = |\phi_2|^2$
$P_{12} = |\phi_1+\phi_2|^2$

El modelo de computación cuántica

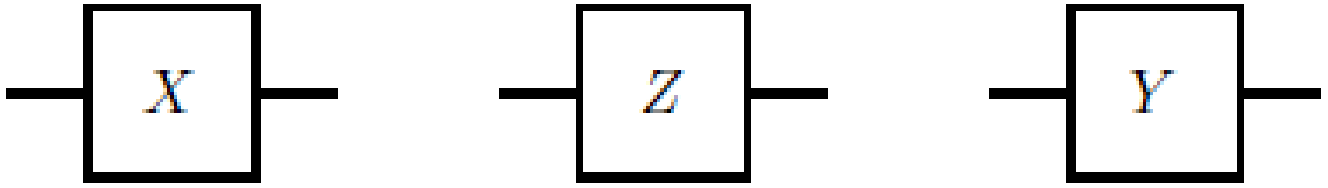


Los estados computacionales son conjuntos de sistemas cuánticos de dos niveles (**qubits)** y la transformación entre la entrada y la salida es una evolución unitaria. La computadora puede operar tanto sobre los estados computacionales como sobre sus combinaciones lineales (paralelismo cuántico)

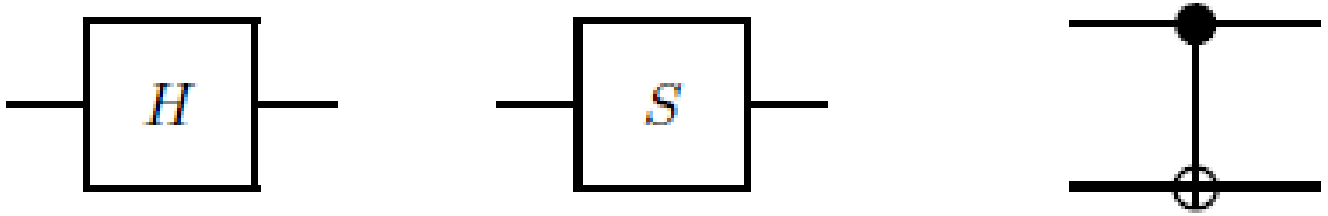
Teorema: toda transformación **U** se puede implementar por medio de compuertas cuánticas universales operando en subconjuntos de uno y dos qubits

Las operaciones básicas sobre un qubit

$$\hat{X} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad \hat{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \hat{Y} = i\hat{X}\hat{Z} = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$$



$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \hat{S} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \quad CNOT_{ij}$$



La computadora cuántica ideal

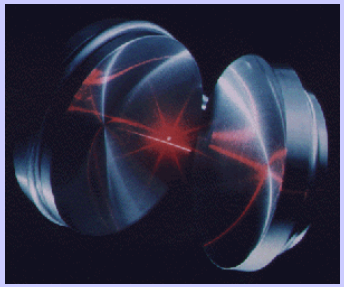
- Producir y almacenar en forma estable estados cuánticos. La interacción con el medio debe ser débil, caracterizada por un tiempo de decoherencia (τ_Q) largo.
- Interactuar con esos estados por medio de operaciones elementales (compuertas cuánticas). Requiere interacciones fuertes para poder efectuar las operaciones rapidamente. (τ_{op})
- Medir confiablemente el resultado. Requiere buen cociente señal/ruido.

Sistema	τ_Q	τ_{op}	N_{op}
Spin Nuclear	$10^{-2} - 10^{8}$	$10^{-3} - 10^{-6}$	$10^{5} - 10^{14}$
Spin Electron	10^{-3}	10^{-7}	10^{4}
Trampa de iones	10^{-1}	10^{-14}	10^{13}
Carga electron(GaAs)	10^{-10}	10^{-13}	10^{3}
Punto Cuantico	10^{-6}	10^{-9}	10^{3}
Cavidad Optica	10^{-5}	10^{-14}	10^{9}
Cavidad de Microondas	10	10^{-4}	10^{4}

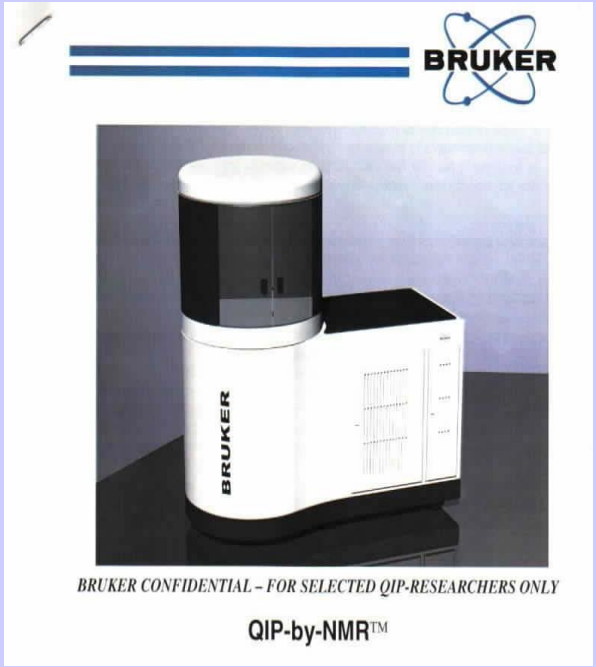
Algunas implementaciones experimentales donde se procesan sistemas cuanticos sencillos

Trampa de atomos frios

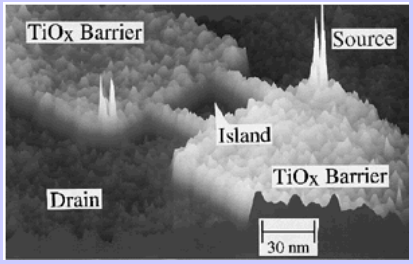
Cavidades opticas



Resonancia mag. nuclear

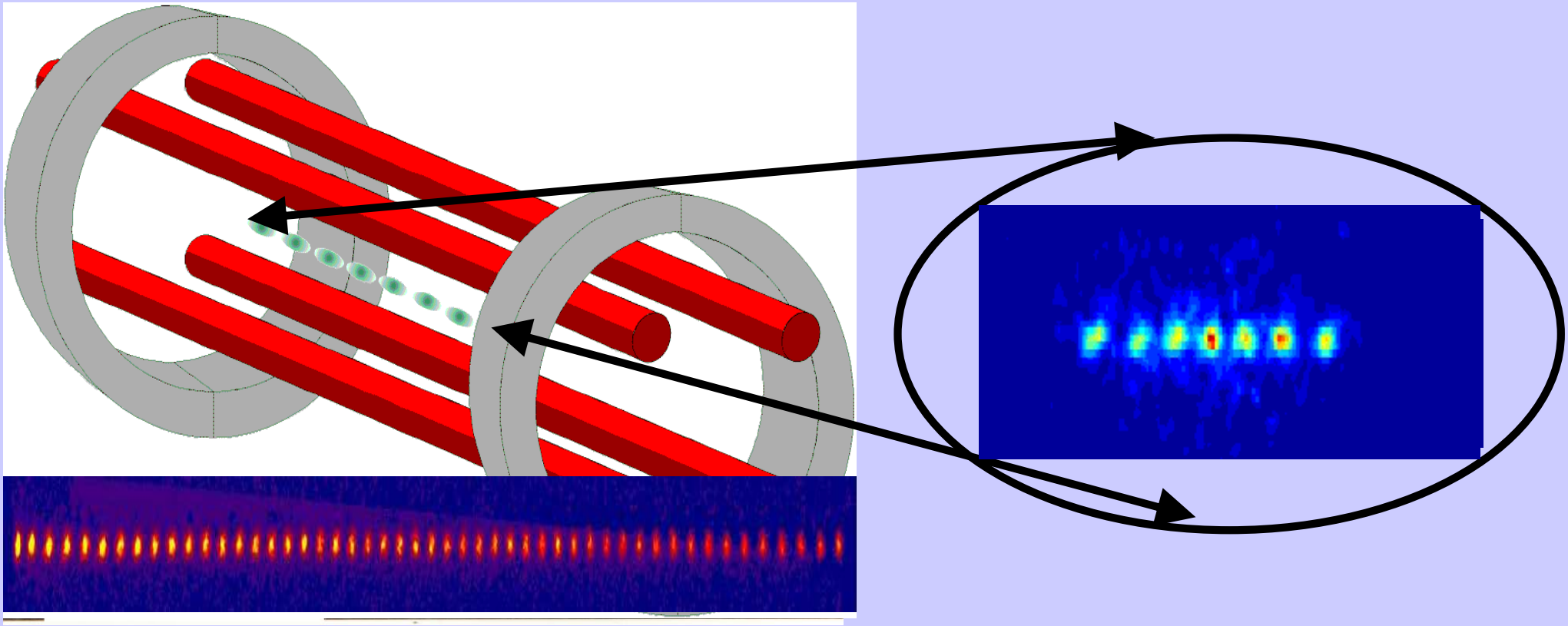


Single electron transistor



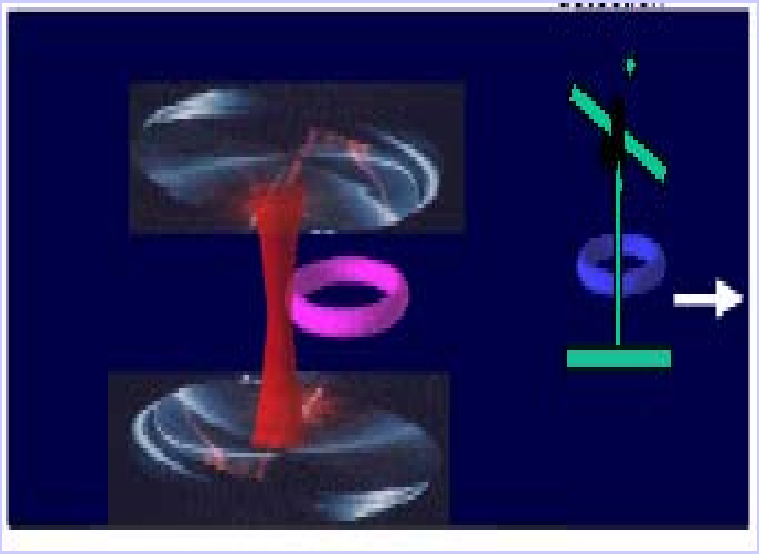
La trampa de atomos frios

Iones de rubidio enfriados y confinados por campos electromagneticos son excitados selectivamente por pulsos laser. Se utiliza el estado fundamental y otro metaestable como qubit.

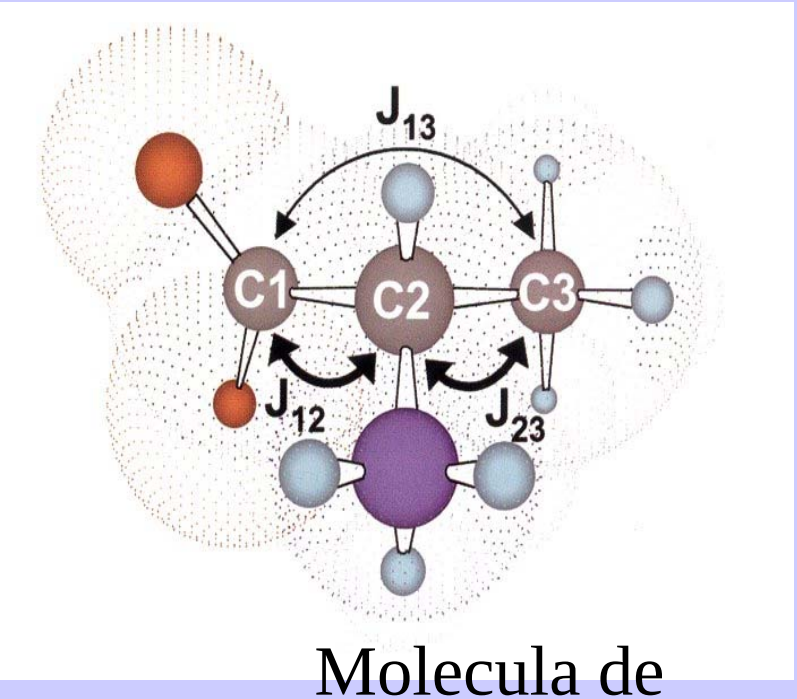


Atomos en cavidades de alto Q

Se crea un modo del campo e.m. en una microcavidad.
Se inyectan atomos “planetarios” que interactuando con el campo se entrelazan con el. Al pasar por una segunda cavidad se crean interacciones entre las dos cavidades



Computacion Cuantica con resonancia magnetica nuclear (NMR)



Molecula de Alanina

Se utilizan como qubits los spines nucleares de moleculas organicas "grandes" (3 a 10 nucleos). El programa se ejecuta por medio de pulsos de radiofrecuencia y se utilizan las interacciones spin-spin entre los nucleos para efectuar las compuertas que involucran dos qubits.

Ventajas: tiempos de decoherencia muy largos. Muestras liquidas a temperatura ambiente. Para extraer informacion es necesario hacer promedios que reducen el cociente senal/ruido exponencialmente con el numero de qubits. Experimentos con tres qubits son standard y se podria llegar hasta 10 qubits.

Algunos algoritmos donde la eventual construcción de una computadora cuántica permite hacer cosas “imposibles”.

a) La transformada de Fourier
b) La búsqueda en una base de datos desordenada
c) La factorización de números grandes
d) La teleportación de estados cuánticos
e) Distribución segura de claves criptográficas

La transformada de Fourier Cuántica

El algoritmo de transformada de Fourier rápida es muy conocido en el procesamiento de señales y en el tratamiento numérico de ecuaciones diferenciales. Obtiene su máxima ventaja cuando la dimensión de los datos N es potencia de dos y permite reducir los recursos necesarios de NxN a $Nxlog(N)$.

Existe un algoritmo cuántico que permite realizar la transformada con recursos proporcionales simplemente a $log(N)$

La búsqueda en una base de datos desordenada

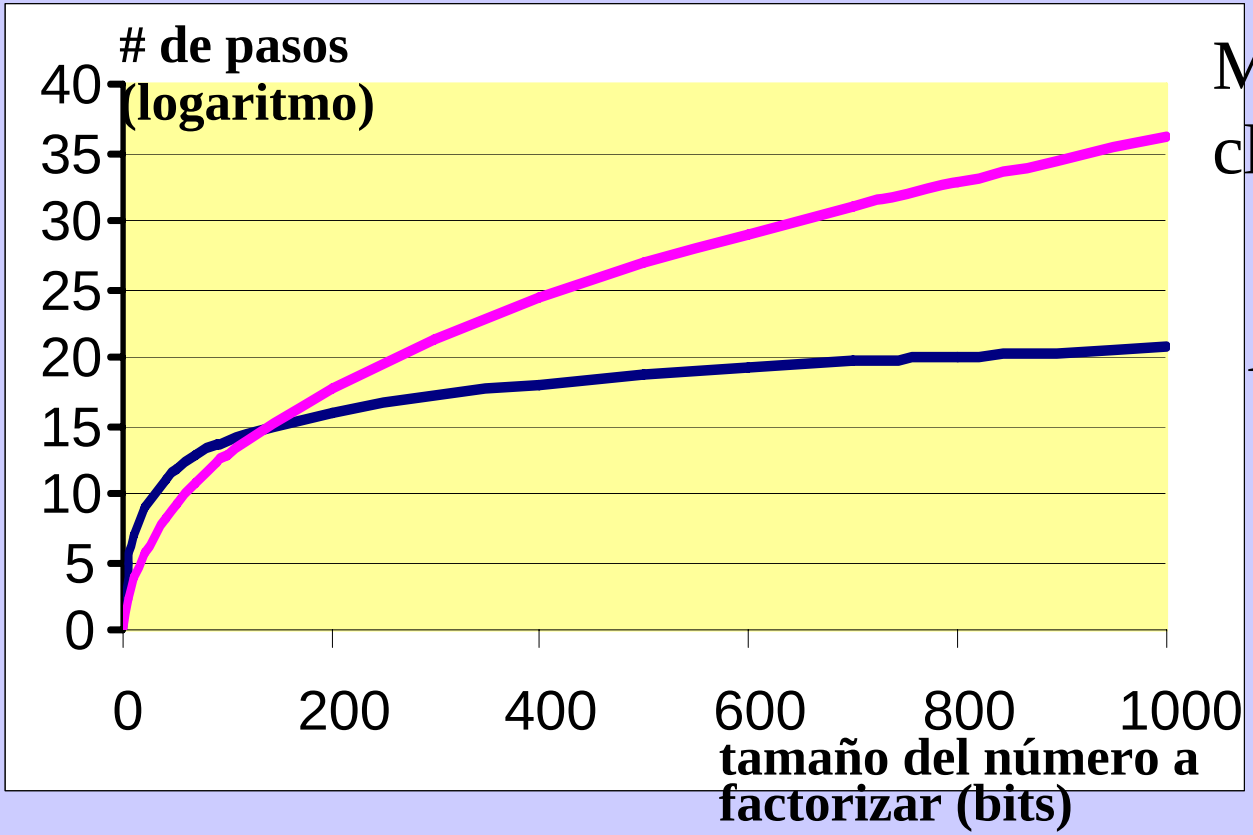
La búsqueda de un dato en una base ordenada (buscar un apellido en la guía telefónica) es un procedimiento eficiente que requiere una cantidad de consultas a la guia que es proporcional a *log(N).* En cambio en una base desordenada (buscar el apellido que corresponde a un dado numero) el numero de consultas es proporcional a N y es muy ineficiente.

El algoritmo cuántico de Grover permite encontrar el apellido buscado con un numero de consultas (cuánticas!) proporcional a *sqrt(N).*

El algoritmo de Shor para la factorizacion

RSA-576 (172 dígitos), encontrar P y Q tales que P x Q =188198812920607963838697239461650439807163563379417382700763356422988859715234665485319060606504743045317388011303396716199692321205734031879550656996221305168759307650257059 (ver detalles en www.rsa.com)

EL algoritmo de Shor permite factorizar un numero en un tiempo polinomial en el numero de bits .



Mejor algoritmo clásico

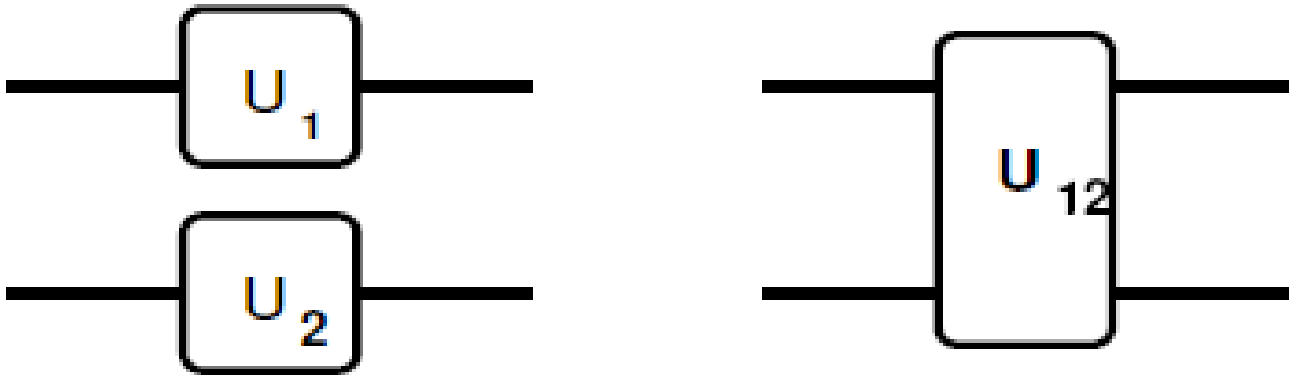
Algoritmo cuántico

El entrelazamiento como recurso

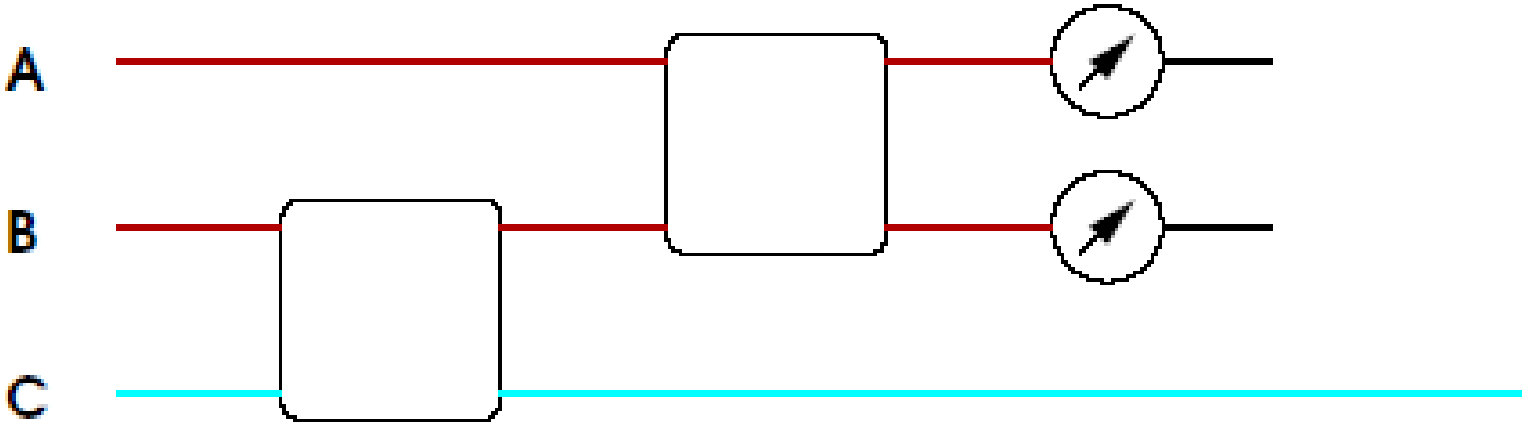
La descripción cuántica de sistemas compuestos permite dos clases de estados:

- Estados separables $|\Psi\rangle_A|\Phi\rangle_B$
- Estados entrelazados $\alpha|\Psi\rangle_A|\Phi\rangle_B + \beta|\Psi'\rangle_A|\Phi'\rangle_B$

En general los estados separables se pueden preparar actuando *localmente* sobre cada uno de los sistemas mientras que los estados entrelazados surgen a causa de una interacción y pueden mantenerse entrelazados aunque se encuentren espacialmente separados.



El algoritmo de teleportación (2)



1)Crear un estado entrelazado (BC) y enviar lejos a C

2) Esperar un rato

3)Crear en A el estado $|\Psi\rangle$ a teleportar

4) Entrelazar $|\Psi\rangle$ con B

5) medir A y B y enviar (clásicamente) el resultado a C (2 bits)

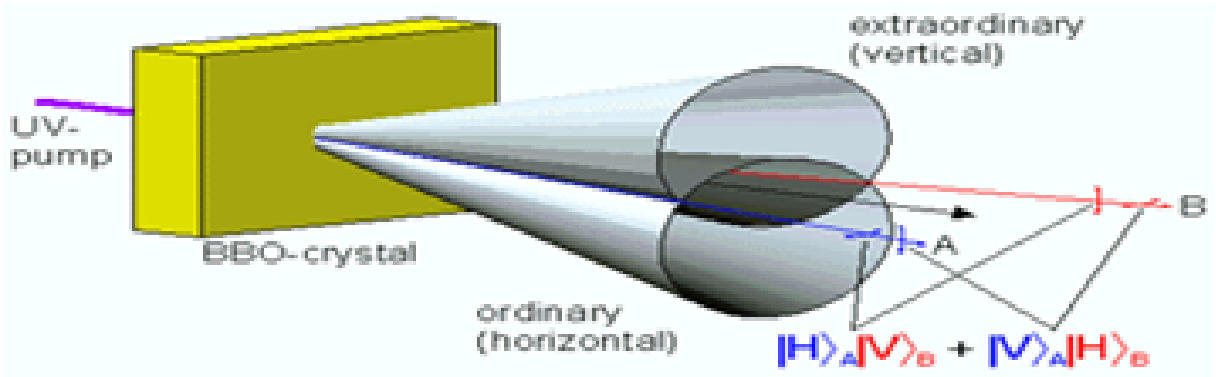
6) Con esta información operar localmente sobre C para reobtener $|\Psi\rangle$

Recursos necesarios

- Efectuar operaciones sobre cada qubit
- Crear estados entrelazados (requiere operaciones sobre dos qubits)
- Estados individuales y entrelazados estables
- Medición del estado de cada qubit

Para transmitir el estado cuántico de un qubit hace falta disponer de un par de qubits entrelazados y transmitir dos bits de información clásica.

Fuente de fotones con polarizaciones entrelazadas



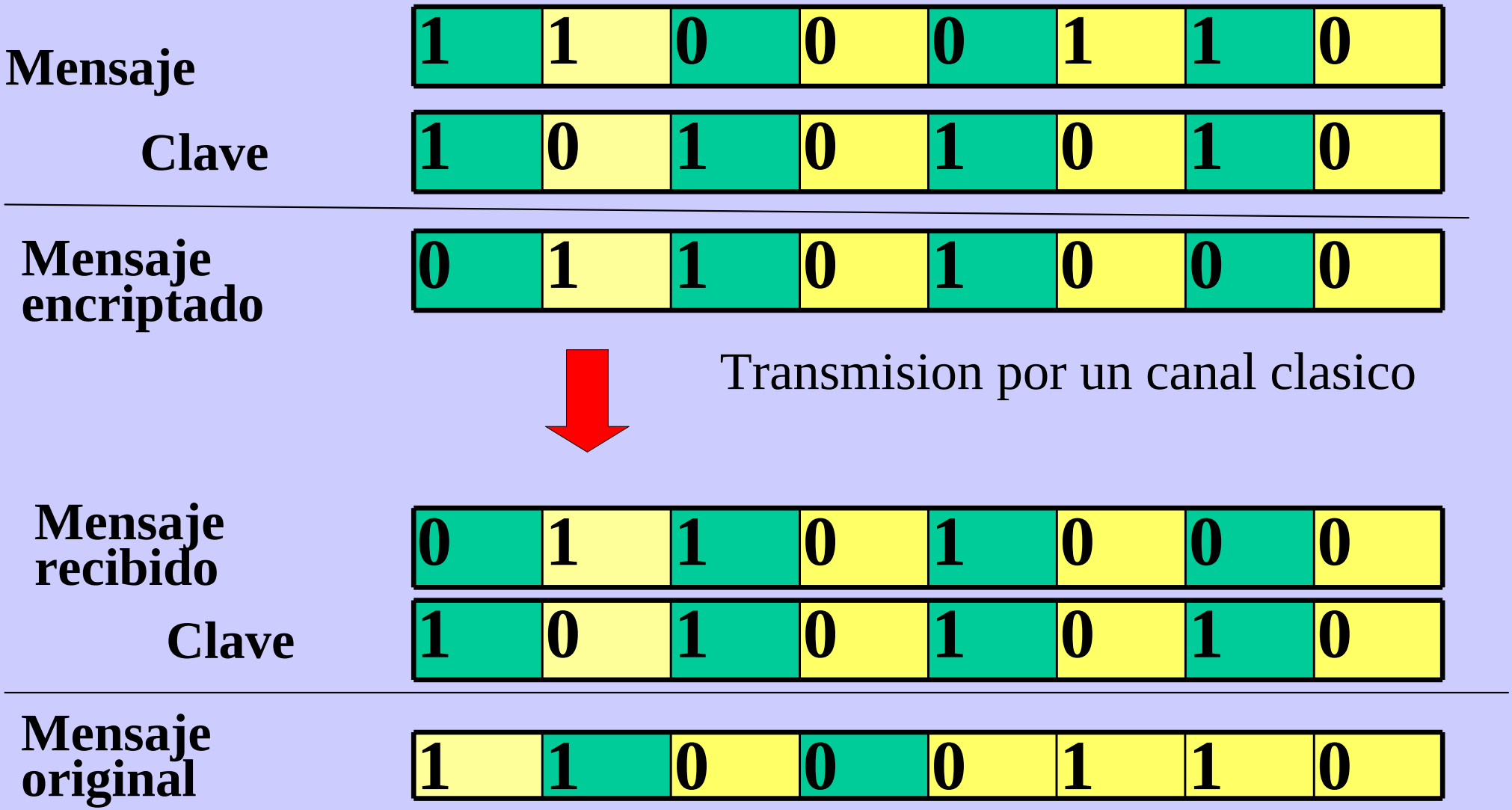
from Zeilinger et. Al.

En un cristal no-lineal un haz ultravioleta genera dos haces infrarrojos (A y B), con polarizaciones distintas (H y V). En la interseccion de los dos haces las polarizaciones estan entrelazadas.

Los hitos de la teleportación

- 1997 Zeilinger group (Vienna), Nature**390**,575(1997)
  Fotones entrelazados, estado de polarización a distancias de 1 metro.
- 1998 Kimble group (Caltech), Science **282**,706(1998)
  Estados coherentes ópticos. Variables continuas, distancias de metros.
- 1998 Laflamme (Los Alamos), Nature 396,92, (1998)
  . Spin nuclear , distancias moleculares.
- 2004 Blatt group (Innsbruck) Nature,**429**,734 ,2004
  2004 Wineland group (NIST) Nature,**429**,737 ,2004
  . Átomos en una trampa de iones, distancias de micrones
- 2004 Zeilinger group (Vienna) Nature**430**,849,2004
  Fotones bajo el Danubio (600m).

Criptografia Clásica



El sistema es seguro siempre que la clave se utilice solamente una vez, de manera que el problema práctico es como generar y distribuir las claves en forma segura.

Existe un protocolo (BB84) que utiliza la mecánica cuántica y permite intercambiar claves por medio de secuencias de fotones polarizados a traves de fibras opticas o aun por aire. El sistema utiliza un canal cuántico para intercambiar la clave y luego un canal clásico para la transmision encriptada. Lo que lo hace incondicionalmente seguro es que cualquier intento de espiar la transmision por una tercer parte es detectado y puede ser corregido.

Avances en criptografia cuantica

Bennett, Brassard (1984) Protocolo de distribucion de claves
Bennett (1991) demostracion de principio (metros)
Rarity et.al. (1991)factibilidad de transmision por aire
Townsend et. Al. (1995) factibilidad de transmision por fibra

Sistemas “comerciales”
Id Quantique (Suiza) (2002) 60km por fibra
Toshiba Research Europe (UK)(2003) 100km por fibra
BBN Technologies(USA) Red de 6 servidores
(2004) primera transaccion bancaria utilizando encriptacion cuantica

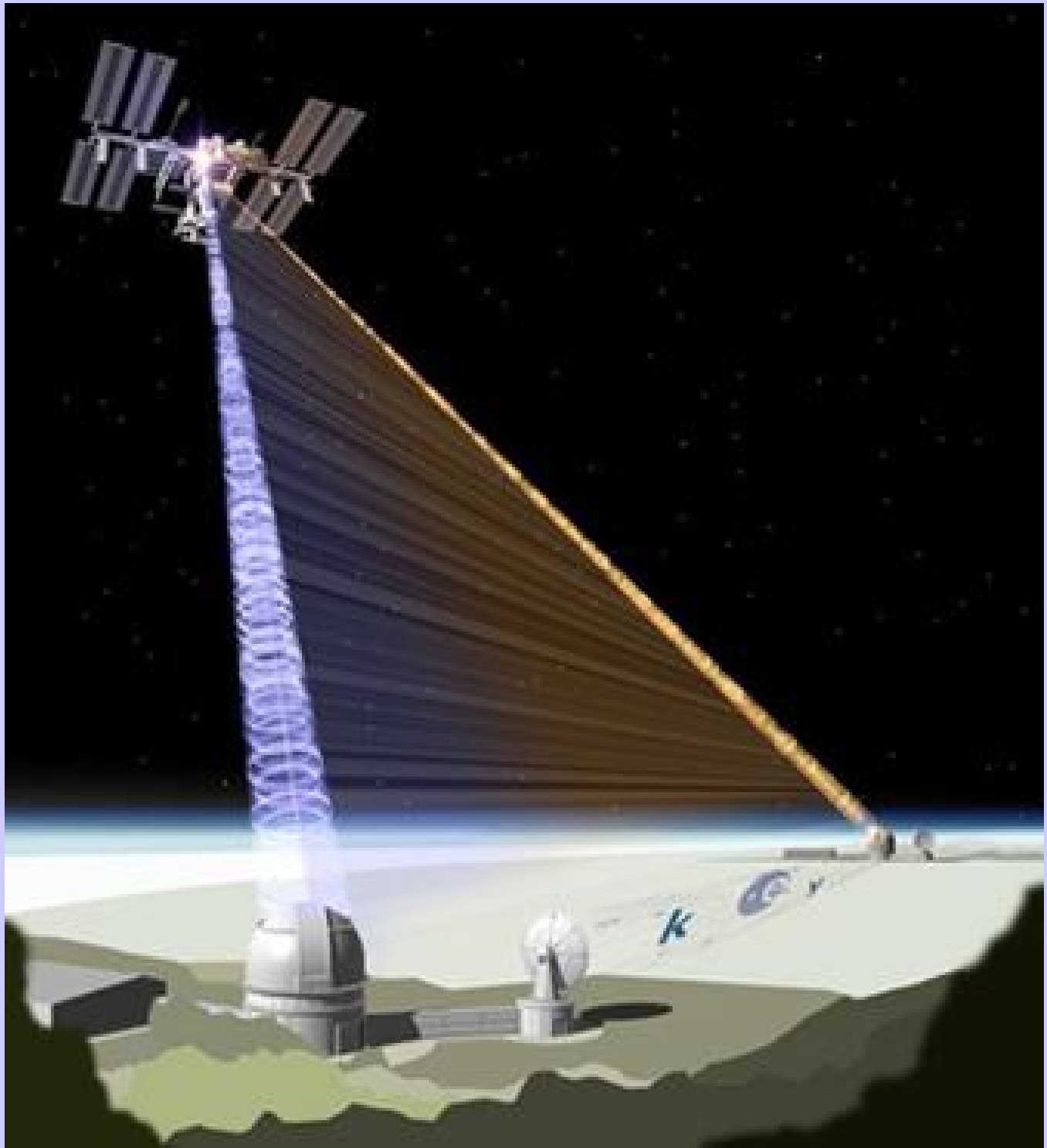
El “mapa de ruta” (Los Alamos(2003) http://qist.lanl.gov

“ ..*desarrollar para 2014 un conjunto de tecnologias practicas de criptografia cuantica lo suficientemente maduras, robustas y accesibles, para poder, ya sea por si solas, o integradas con sistemas convencionales de seguridad informatica, como para proveer nuevos y mas seguros sistemas de comunicacion…*”

http//:homepage.univie.ac.at/Rupert.Ursin/php/?Research:Free_Space

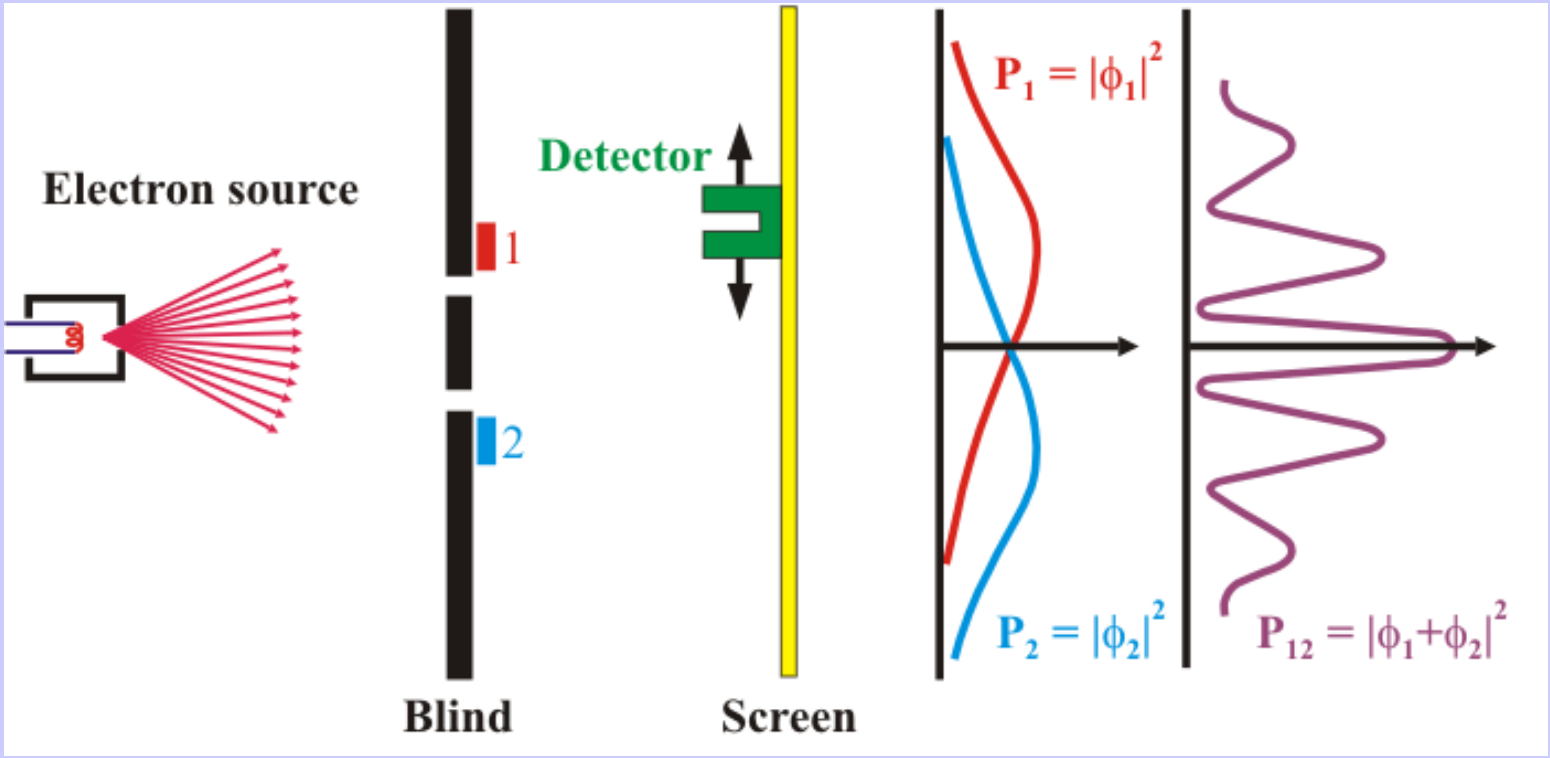
Space-QUEST

Proyecto ESA para
Distribuir claves
criptograficas entre
Estaciones terrestres
alejadas
(2014)



Conclusiones

En estos años se celebra el centenario del descubrimiento de las propiedades cuánticas de la materia. En estos primeros cien años se han estudiado estos efectos en todos los sistemas naturales, desde las partículas subnucleares hasta las estrellas de neutrones. Los próximos cien años prometen ser los de la **ingeniería cuántica,** donde el objetivo es construir y manipular objetos cuánticos artificiales con propiedades diseñadas con propósitos específicos



Este experimento ha sido repetido con neutrones, átomos, y hasta con moléculas de carbono 60. No parece haber dificultades de principio en seguir aumentando la masa y el tamaño de los proyectiles…..

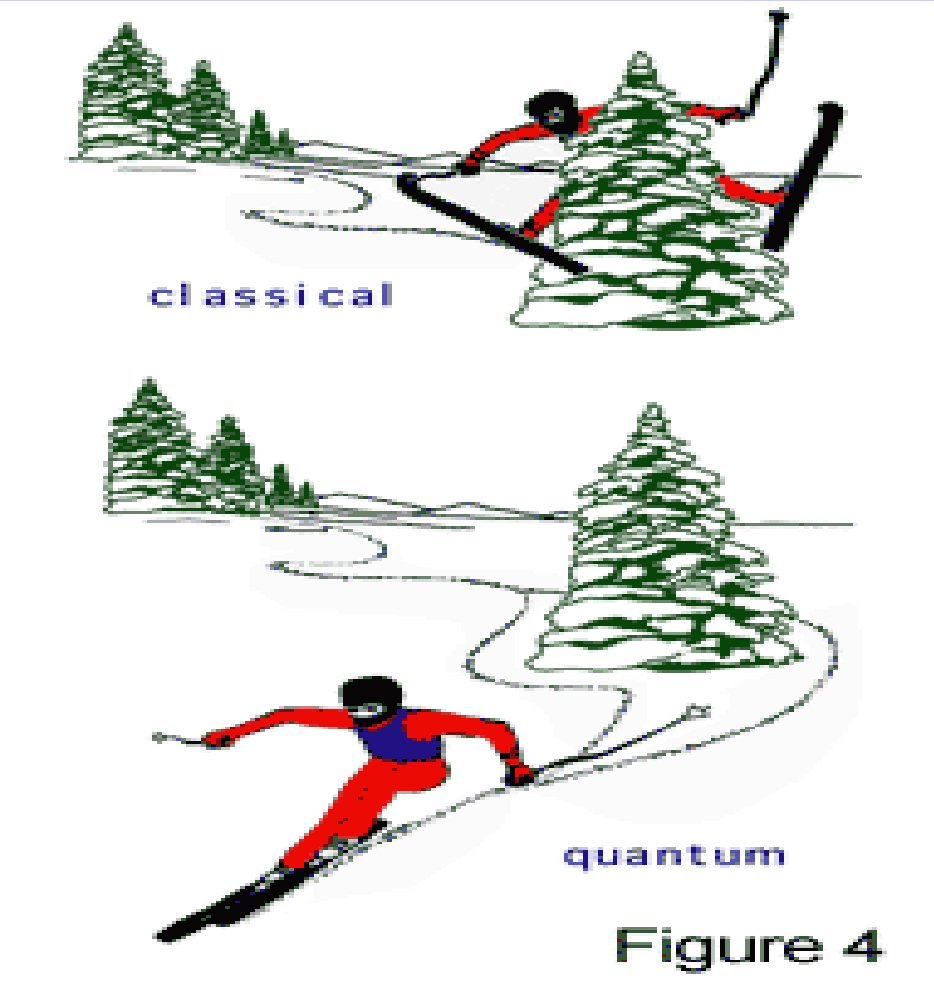


Figure 4

Muchas gracias !

Fin