Procesamiento Cuántico de Datos

Miguel Arizmendi, Gustavo Zabaleta

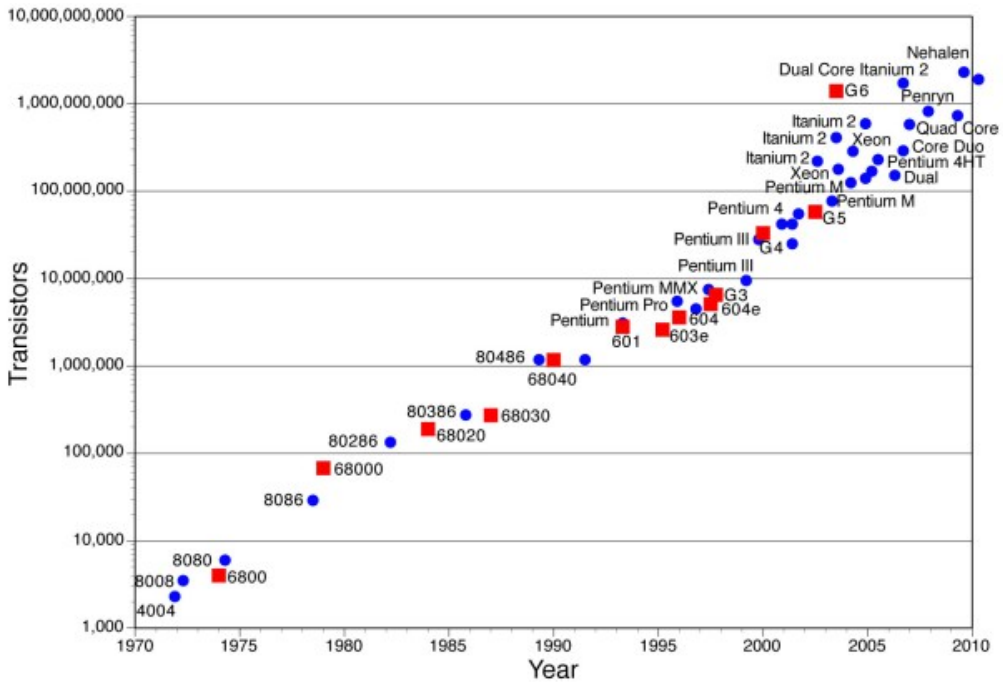
Doctorado en Ingeniería
O. Modelado y Simulación Computacional

3 de noviembre de 2016

Ley de Moore (1965-?)

Cada 18-24 meses la velocidad de los microprocesadores se duplica
Y se disminuye su tamaño

2016.. La ley de Moore se tambalea..



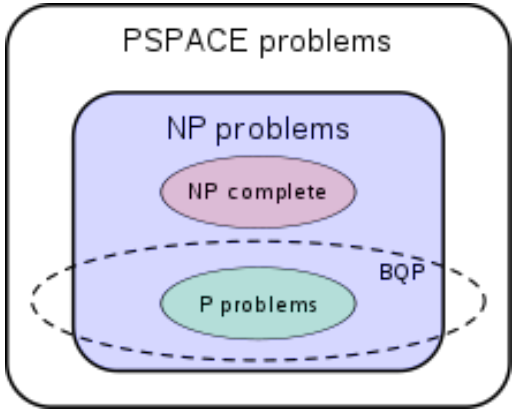

El Intel® 4004, el primer microprocesador de Intel, tenía 2300 transistores.
X 1.000 MILLONES
Los actuales procesadores superan los 1000 millones de transistores.
Comparado con el Intel® 4004, los actuales procesadores de 14nm ofrecen un rendimiento 3.500 veces superior, una eficiencia 90.000 veces mejor y una reducción del coste de 1/60.000.
Si la eficiencia de combustible de automóviles hubiera mejorado al mismo ritmo que la Ley de Moore, una persona podría fácilmente conducir un coche durante toda su vida llenando una sola vez el depósito de gasolina.
intel
LA LEY DE MOORE CUMPLE 50 AÑOS
desde 1965 a 2015
Si el precio de un rascacielos cayera al ritmo de la Ley de Moore, podrías comprarte uno por menos de lo que cuesta un PC a día de hoy.
Si un teléfono Android con procesador Intel hubiese sido fabricado con la tecnología de 1971, sólo el microprocesador tendía el tamaño de una plaza de aparcamiento.
1 MINUTO
El viaje a la Luna en 1969 duró tres días. Si la Ley de Moore se aplicara a los viajes espaciales, esa misma expedición sólo conllevaría un minuto.

Visiones de la Mecánica Cuántica

Visión Física Tradicional	**Visión Computacional**
Teoría Física a escala atómica	Modelo de Computación con amplitudes en lugar de probabilidades
Pesimista (Incertidumbre de Heisenberg)	Optimista (Algoritmos más rápidos)

Complejidad Algorítmica

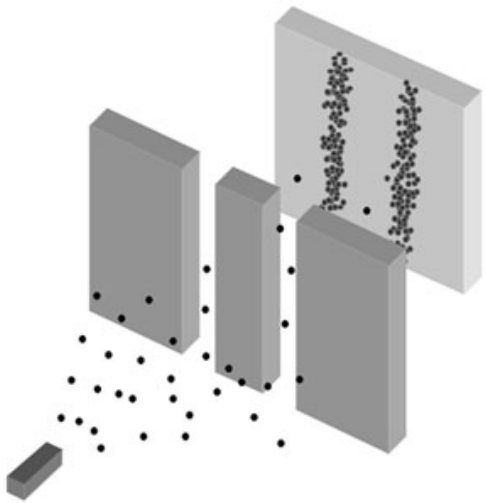
Tiempo y Espacio necesarios para resolver un problema



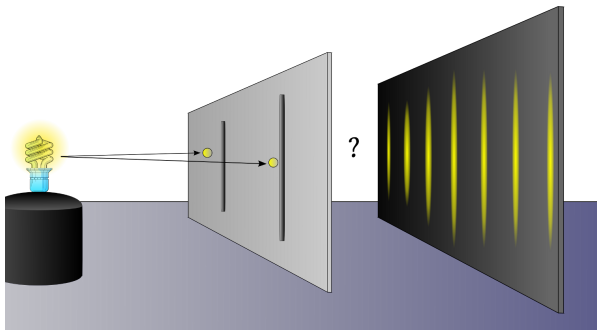
PSPACE: Espacio polinomial n^k.
Problemas **NP**: Problemas de resolución fácil en una dirección y muy duros en la inversa.
Por ejemplo Factorización de enteros, Problema del viajante de comercio o búsqueda de combinaciones para nuevas drogas.

Interferencia de Young

- Partículas Clásicas



- Partículas Cuánticas



Cambia la lógica

Clásico

Proposición **A**: Componente **z** de spin es +1
Proposición **B**: Componente **x** de spin es +1
A *or* **B** es equivalente a **B** *or* **A**

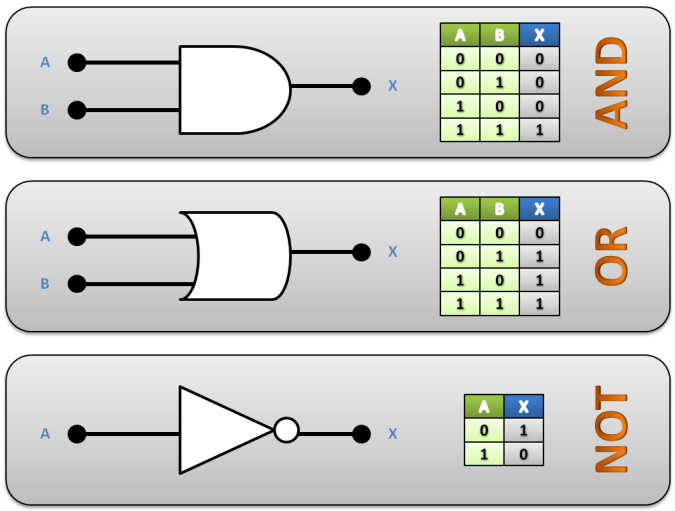
Cuántico

Proposición **A**: Componente **z** de spin es +1
Proposición **B**: Componente **x** de spin es +1
A *or* **B** **no** es equivalente a **B** *or* **A**
Inicialmente **A** es verdadero $\rightarrow$ **A** *or* **B** se verifica si se mide primero el spin según **z**.
Si se mide primero según **x** se cumplirá que es +1 o -1. Pero si después se mide el spin según **z** será +1 o -1.

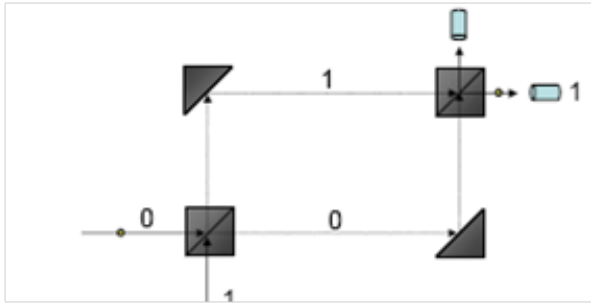
Hay probabilidad $\frac{1}{4}$ de que **A** *or* **B** sea falso.

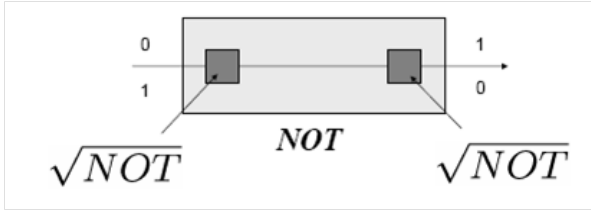
Compuertas Clásicas y Cuánticas

Compuertas Clásicas



Compuertas Cuánticas





Tesis de Church-Turing(Versión Fuerte)

Cualquier algoritmo puede ser simulado **eficientemente** con una máquina de Turing

A Universal Turing Machine,

A laptop computer, with extra disks

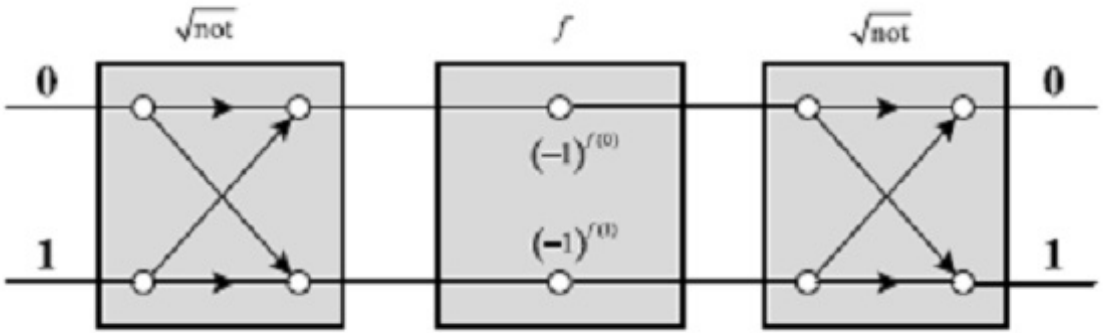
(but not a pocket calculator or a digital wrist watch)

Primer Desafío a la Tesis de Church-Turing(Versión Fuerte)

Test de Solovay-Stressen para determinar si un entero es primo con una cierta probabilidad. **Imposible** para una máquina de Turing determinista! $\rightarrow$ Nueva Tesis de Church-Turing: Cualquier algoritmo puede ser simulado **eficientemente** con una máquina de Turing *probabilista*.

Siguientes Desafíos a la Tesis de Church-Turing(Versión Fuerte)

- Problema de Deutsch (1985): Evaluar $f(x) \forall x$ en un solo paso



Período de una función

Búsqueda de período

Función $f : \{1, .., 2n\} \rightarrow \{1, .., 2n\}$
$\exists$ entero $r / f(x) = f(x + r) \; \forall x$
Problema : Encontrar r
Clásico : $2^{n/3}$ pruebas
Cuántico : polinomio de n pruebas

Aplicaciones

Búsqueda de datos a gran escala (Searching Big Data)

Una máquina que puede buscar en una cantidad de datos siempre creciente y localizar las conexiones dentro de ellos, podría tener un impacto tremendo en muchas industrias.

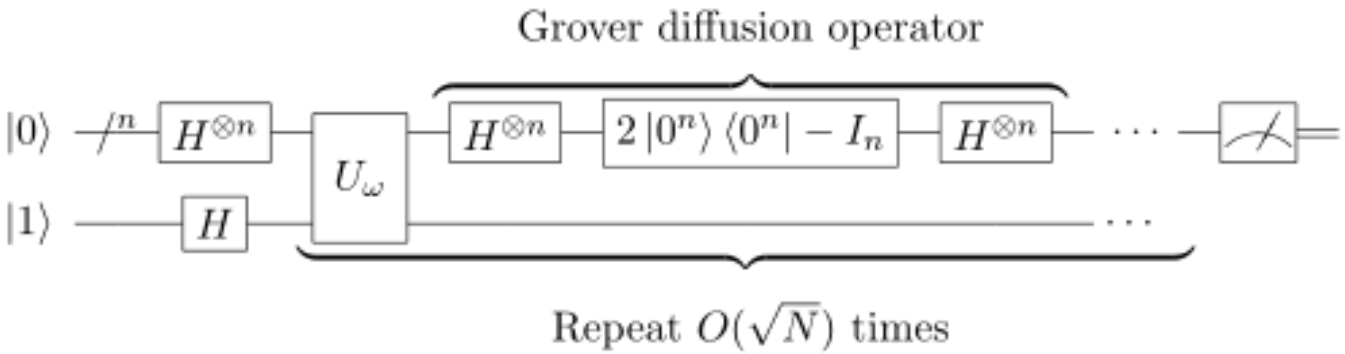
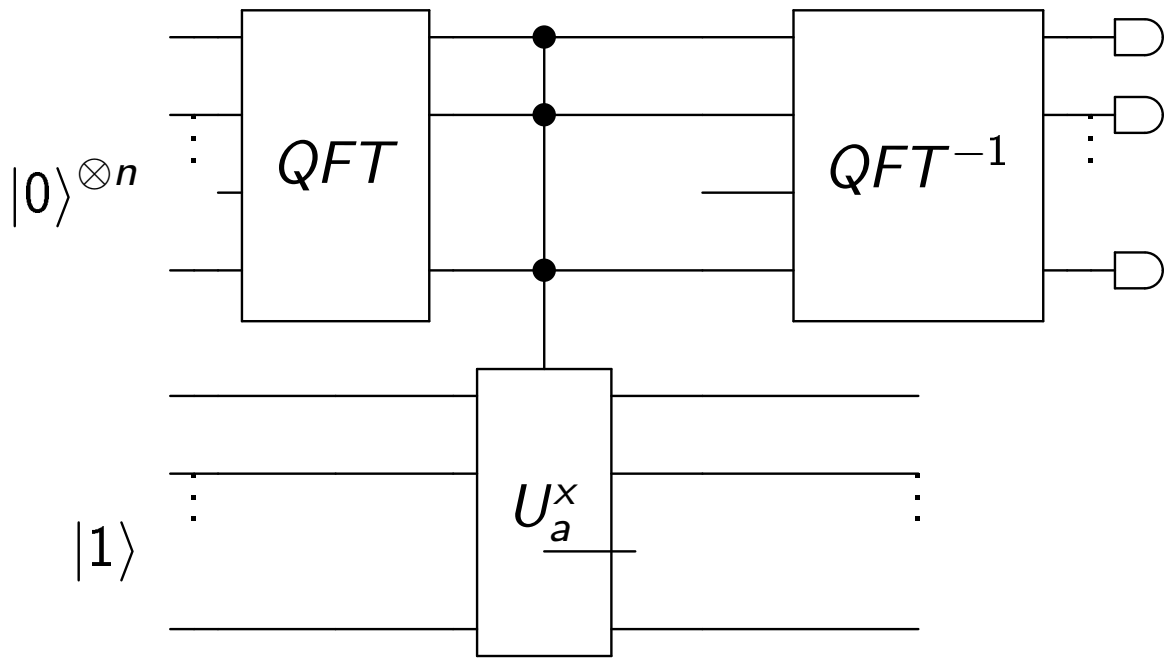


Figura: Algoritmo de Búsqueda de Lov Grover

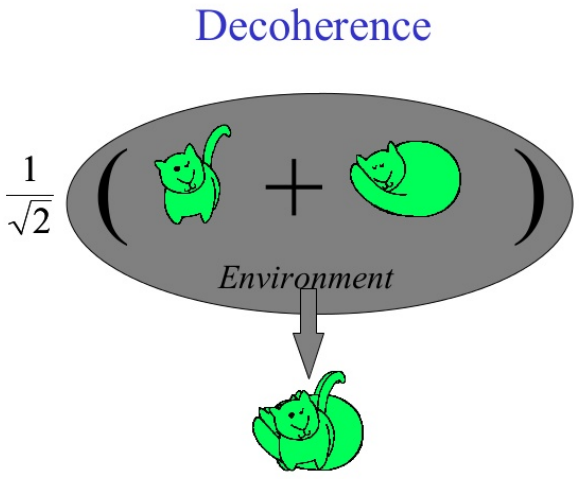
Factorización de Enteros (Shor 1994)

Tiempo $O(log(N)^3)$
Espacio $O(log(N))$

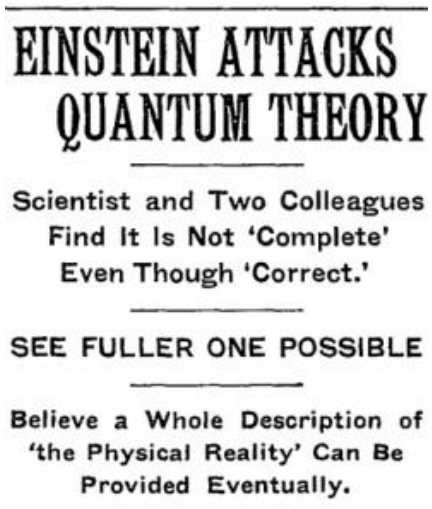


Características de la Computación Cuántica

- Paralelismo Cuántico
- Superposición Cuántica
- Decoherencia



- Entanglement



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

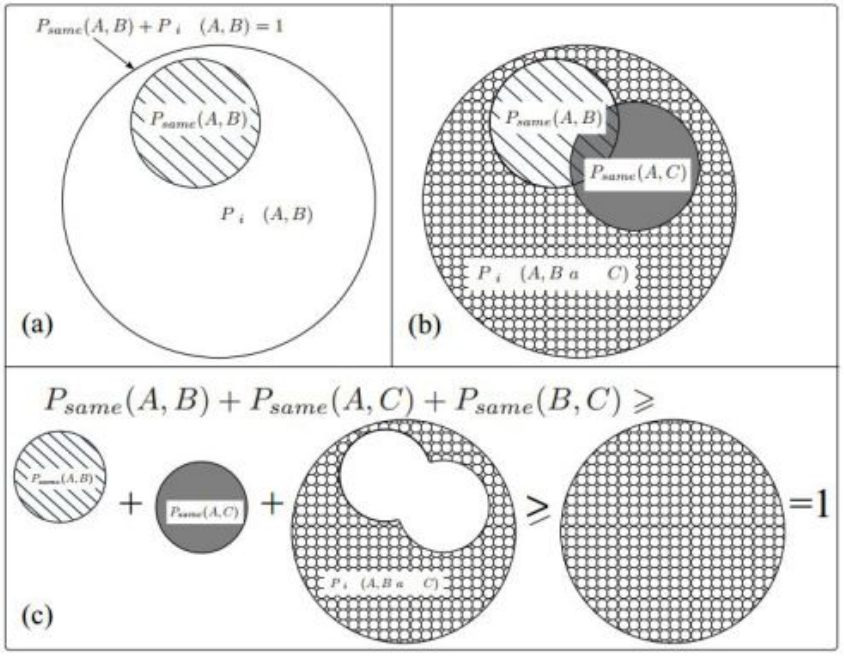
SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

Entanglement y Desigualdad de Bell

Caso Clásico: Dos monedas iguales

A chicas o grandes (0 o 1)
B doradas o plateadas (0 o 1)
C 50*cent* o 1*peso* (0 o 1)
Propiedades *contrafactuales (realismo)* y *locales*



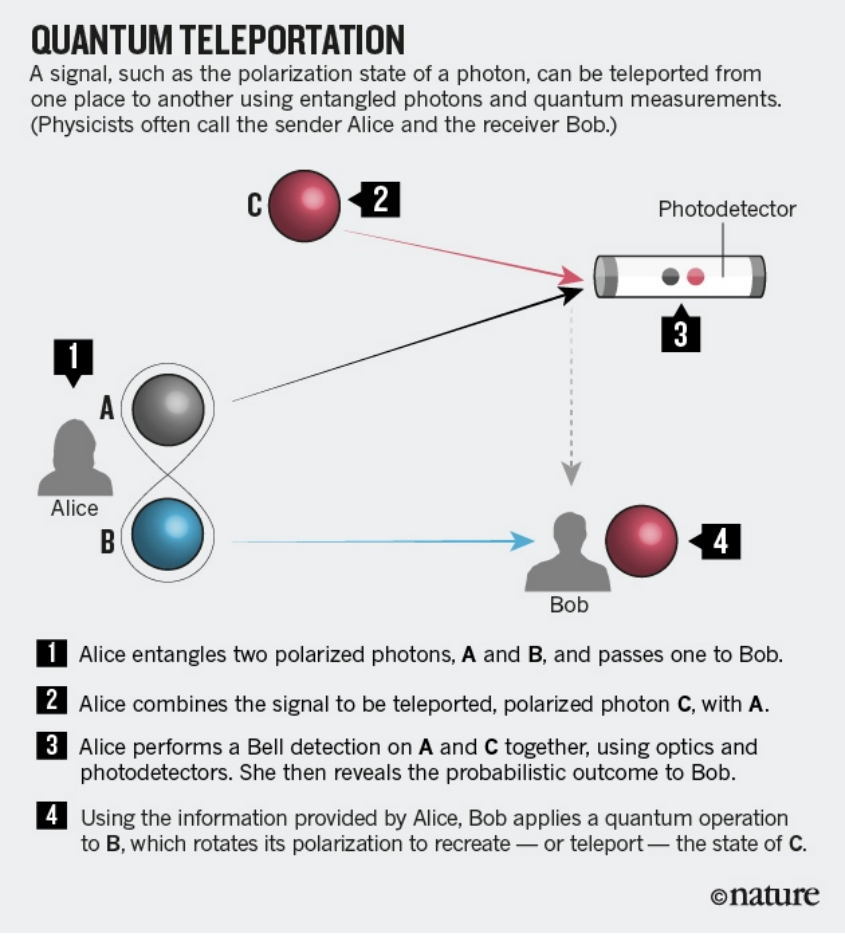
Entanglement y Desigualdad de Bell

Caso Cuántico con entanglement

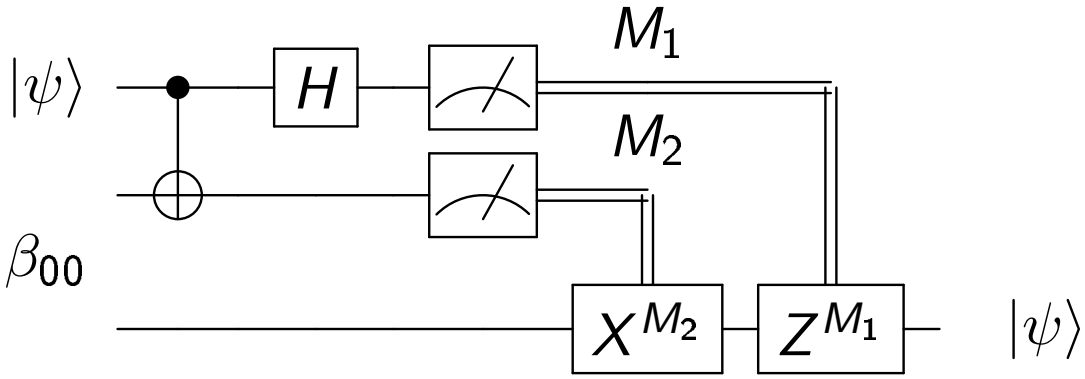
$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$P_{same}(A, B) + P_{same}(A, C) + P_{same}(B, C) = \frac{3}{4} < 1$$

Teleportación

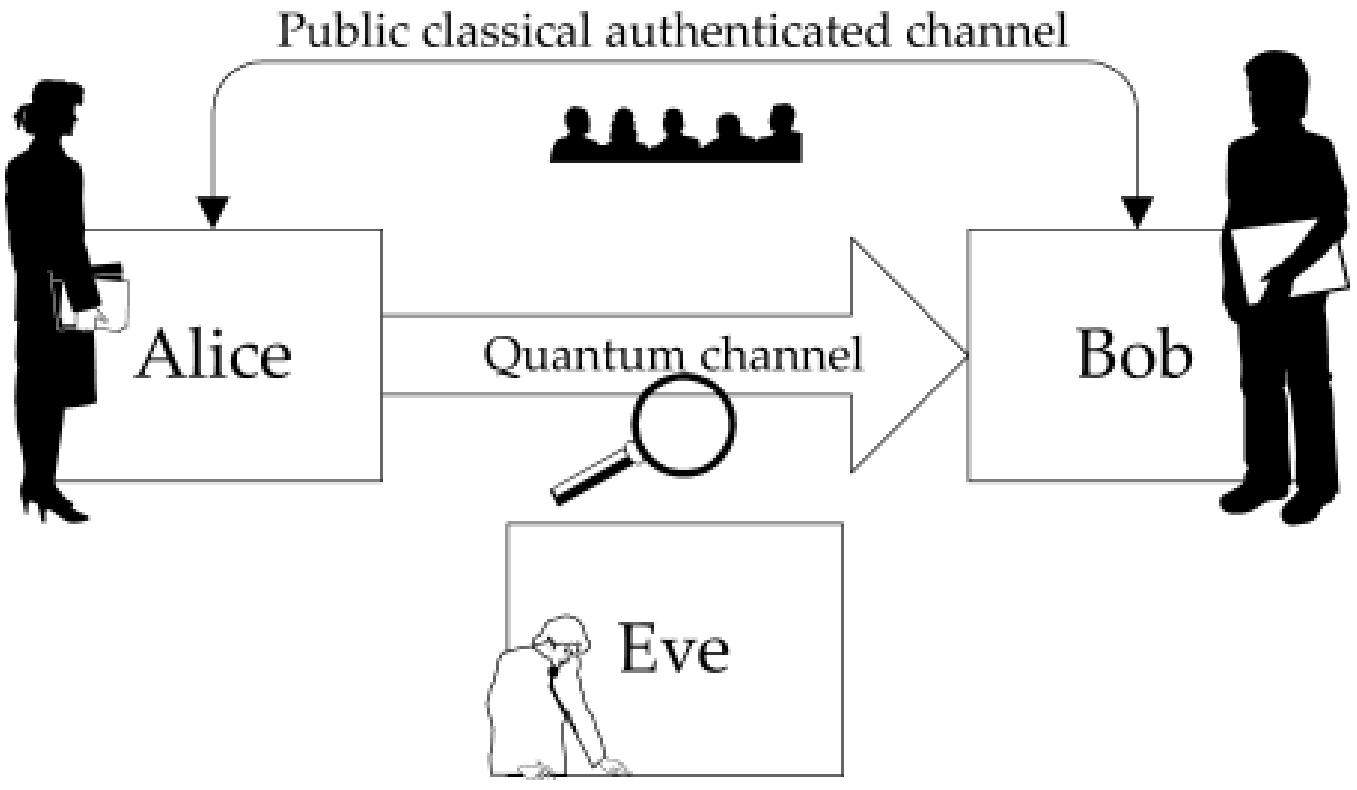


Teleportación

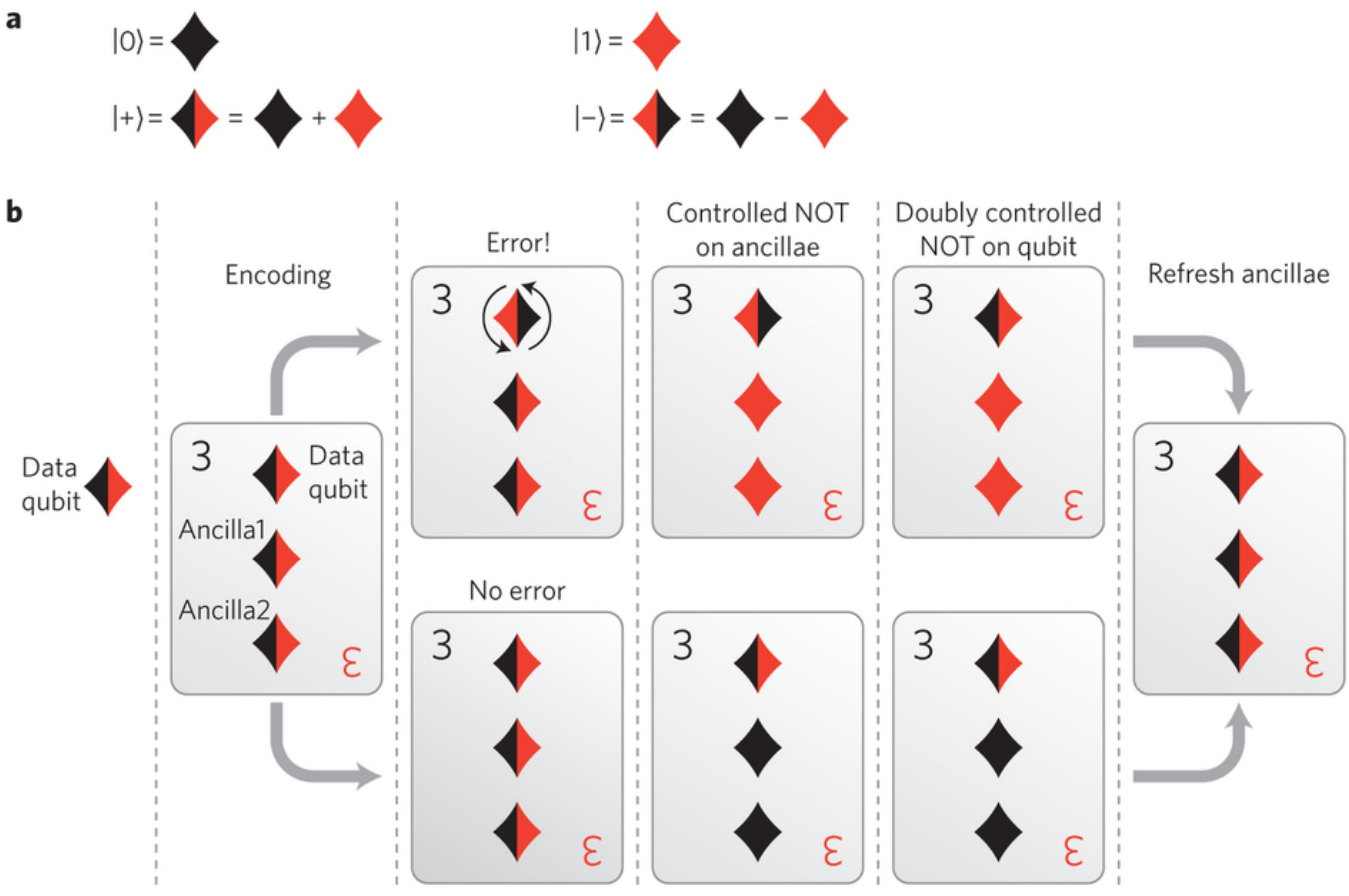


Imposibilidad de Clonado de Qubits

Criptografía

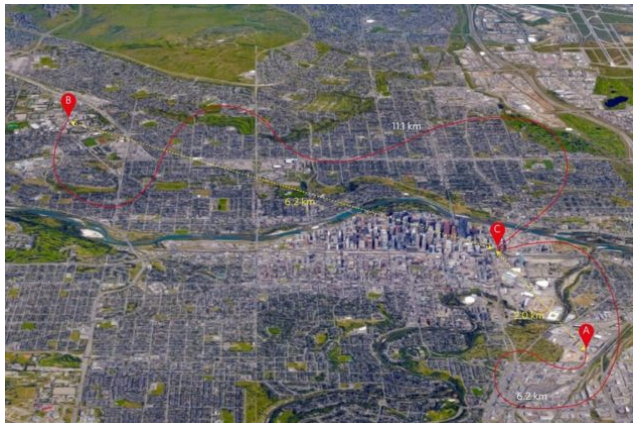


Detección y Corrección de errores



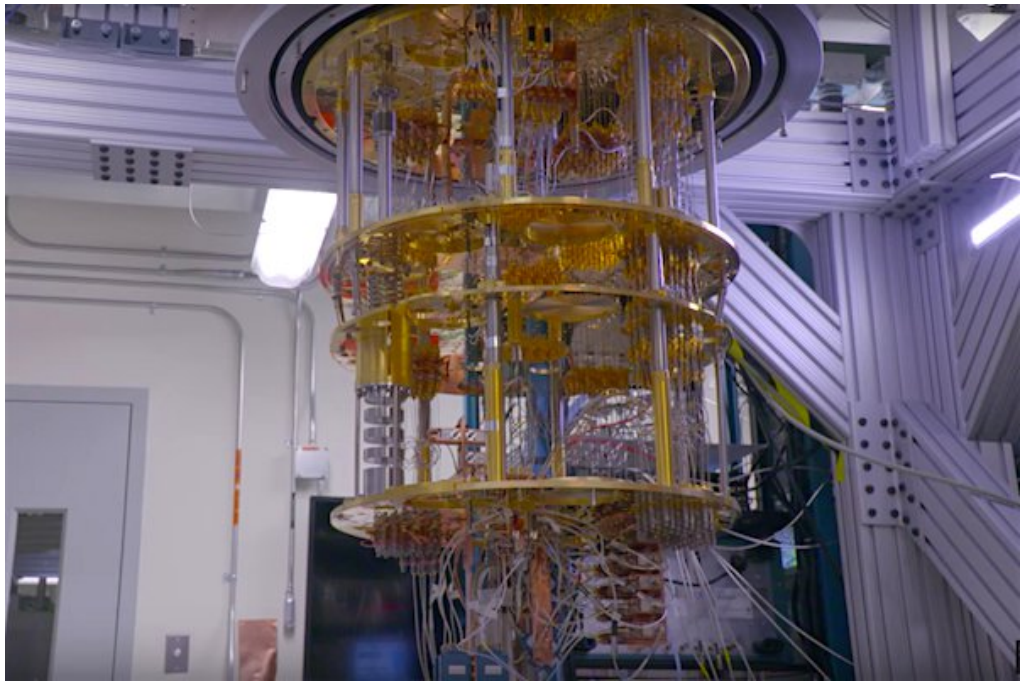
Transmisión de la información

- Procesamiento de Información Cuántica
- Redes Cuánticas (Internet cuántico?)



- Protocolos
- Control de acceso al medio asistido por Computación Cuántica
- Asignación del Espectro

Computadora Cuántica en los Laboratorios de IBM



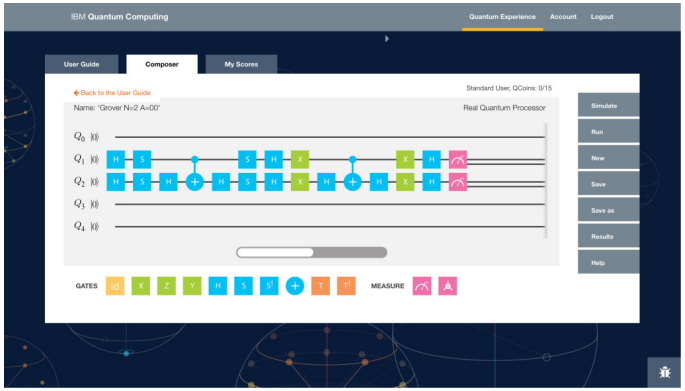


Figura: IBM permite jugar con su computadora