Center for Computational Simulation

Tecnologías Cuánticas para la Información y las Comunicaciones.

8ª Jornada CenitS

Computaex

Escuela Politécnica de Cáceres,

15 Dic. 2016

Vicente Martín
vicente@fi.upm.es

POLITÉCNICA "Engineering the future" | INTERNATIONAL CAMPUS OF EXCELLENCE

Universidad Rey Juan Carlos

UNIVERSIDAD COMPLUTENSE MADRID

UAM UNIVERSIDAD AUTONOMA DE MADRID

Center for
Computational Simulation

Índice.

- ¿Qué es la información cuántica? ¿Cuales son sus ingredientes?
- ¿Qué nos permite hacer?
- ¿Cuál es el estado de la técnica?
- Industria y Futuro

Información Cuántica.

“Information is physical”

Rolf Landauer, 1991

¿Qué es para nosotros la computación convencional?

- La capacidad de realizar un **conjunto de operaciones matemáticas sobre una entidad abstracta, el bit**, que puede estar **en uno de dos estados,** simbolizados por 0 o 1.
  - Ej: Una máquina de Turing sobre símbolos “0”, “1”.
  - Los bits los hemos representado en una máquina física de manera muy variada: voltajes, flip-flops... pero siempre asumiamos “0”, o “1”

Center for Computational Simulation

Información Cuántica.

- Y ahora nos dedicamos a aplicar una serie de puertas lógicas sobre unos cuantos bits de entrada hasta que al final obtenemos unos resultados...
  - Este es el **modelo de circuitos**, tal vez extendido con la capacidad de repetir la aplicación del mismo bloque de puertas sobre la salida...
  - Un programa es la especificación de qué puertas, en qué secuencia, sobre qué bits y qué condición de parada...
- Finalmente es un **modelo matemático** idealizado que se implementa sobre un **sistema físico**.

Información Cuántica.

… a veces hemos ido más allá del bit simple y asumido bits probabilistas...

- En vez de 0 o 1, podían estar en 0 con probabilidad *p* y en 1 con *1-p*
  - Esto está bien, algunos algoritmos probabilistas son más eficientes que ninguno de los deterministas conocidos...
  - … y no se sabe si se puede convertir un algoritmo probabilista en uno determinista de manera eficiente...

Pero, **seamos más extremos...**

¿qué pasaría si la Naturaleza nos diese más posibilidades?

Información Cuántica.

Imaginemos que **usamos las teoría física más exitosa que tenemos a mano para construir el bit más versátil que la naturaleza nos permita.**

Mecánica Cuántica y bits

(¿una extraña pareja?)

Center for Computational Simulation

Información Cuántica.

El **Qubit.**

(Lista de ingredientes y modo de empleo)

- En mecánica cuántica los sistemas (aislados) **están descritos por estados** (caracterizados por un conjunto de números cuánticos).
    - Un átomo en su estado de energía más bajo.
    - Un fotón en un estado de polarización horizontal.
    - Un conjunto de iones vibrando al unísono en una trampa electromagnética.
- La naturaleza es discreta... no existe un continuo de elementos, y esto está descrito por la mecánica cuántica.

Center for Computational Simulation

Información Cuántica.

El **Qubit.**

(Lista de ingredientes y modo de empleo)

- Definamos **dos estados cuánticos** como **0 y 1: |0> y |1>**
  - |> es un "ket" en la notación de Dirac y sirve para denotar un estado cuántico: **|0> significa "el estado cuántico que representa al valor 0 del qubit"**...
    - Sea cual sea su implementación física: la polarización de un fotón, estados de espín, el nivel más bajo de energía de un ión...
  - Un estado genérico de un **qubit** se escribe como **$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$**

Información Cuántica.

Bit vs
Pbit vs
Qubit

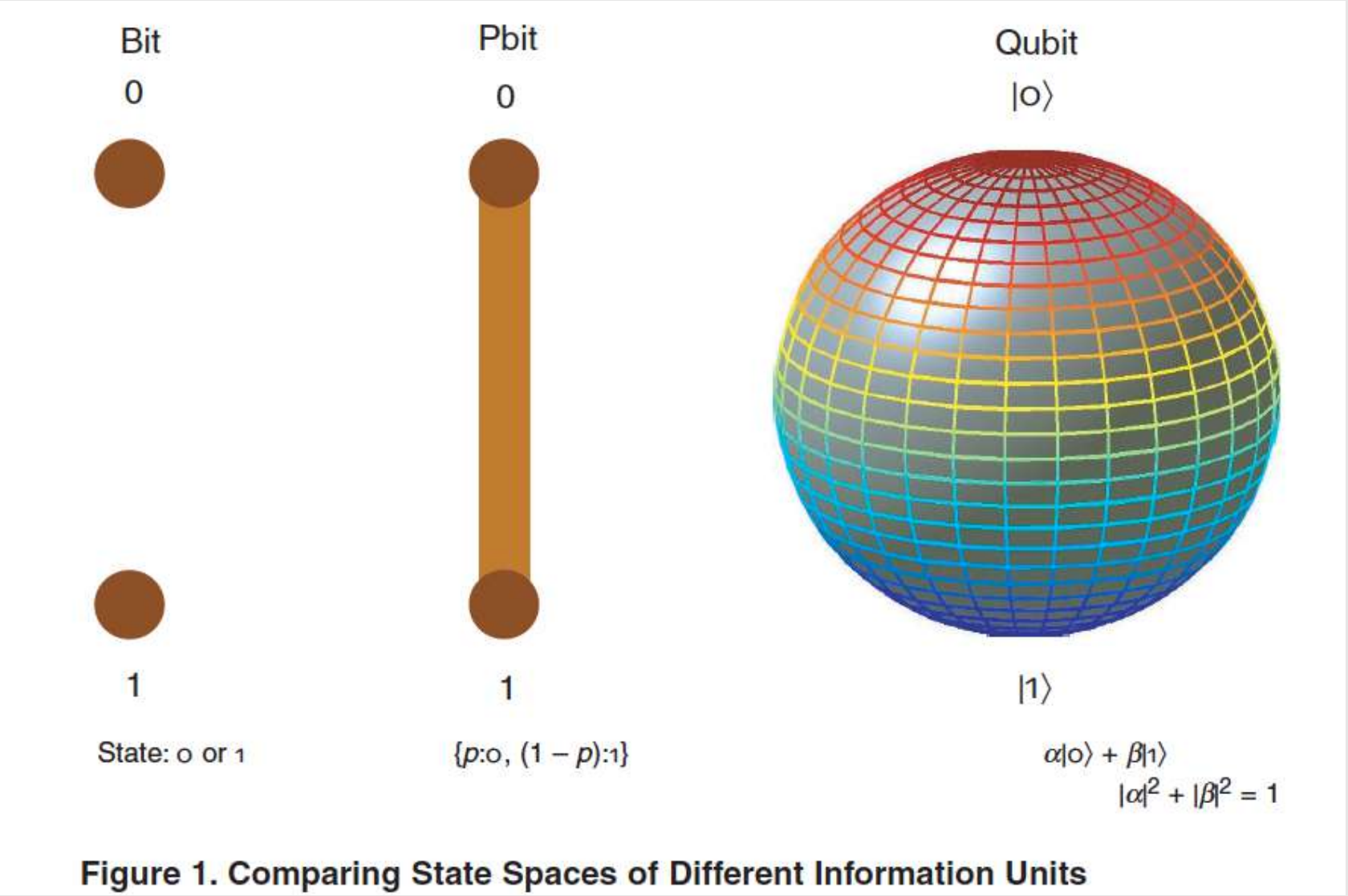


Figure 1. Comparing State Spaces of Different Information Units

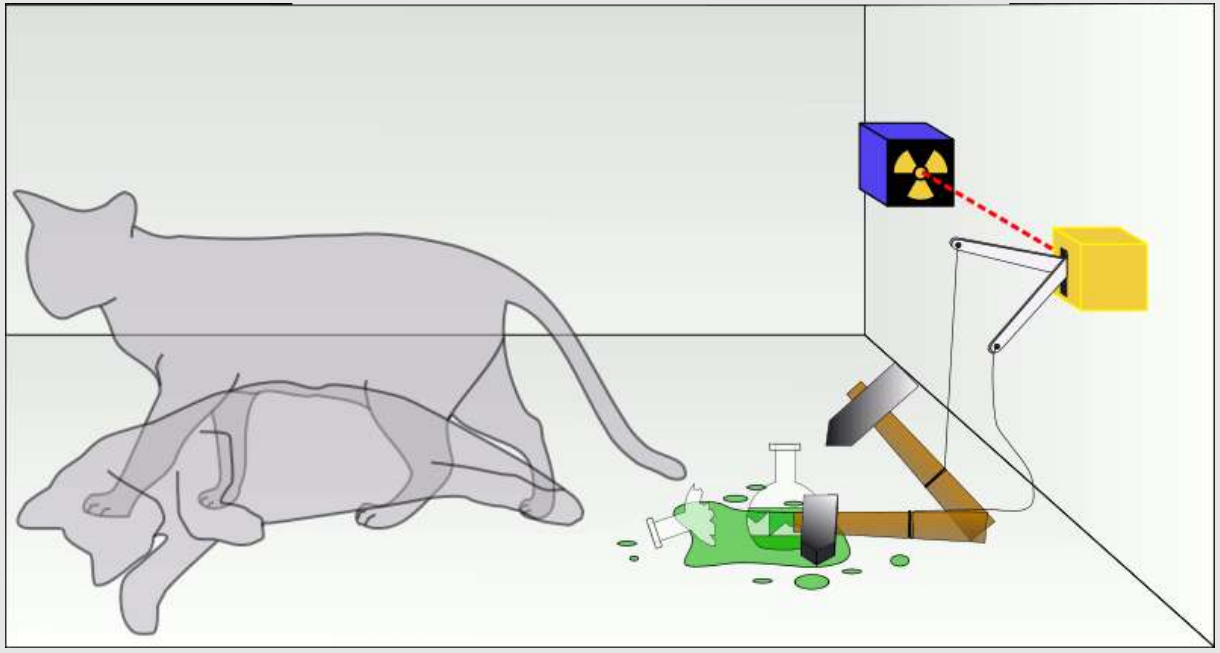
Información Cuántica.

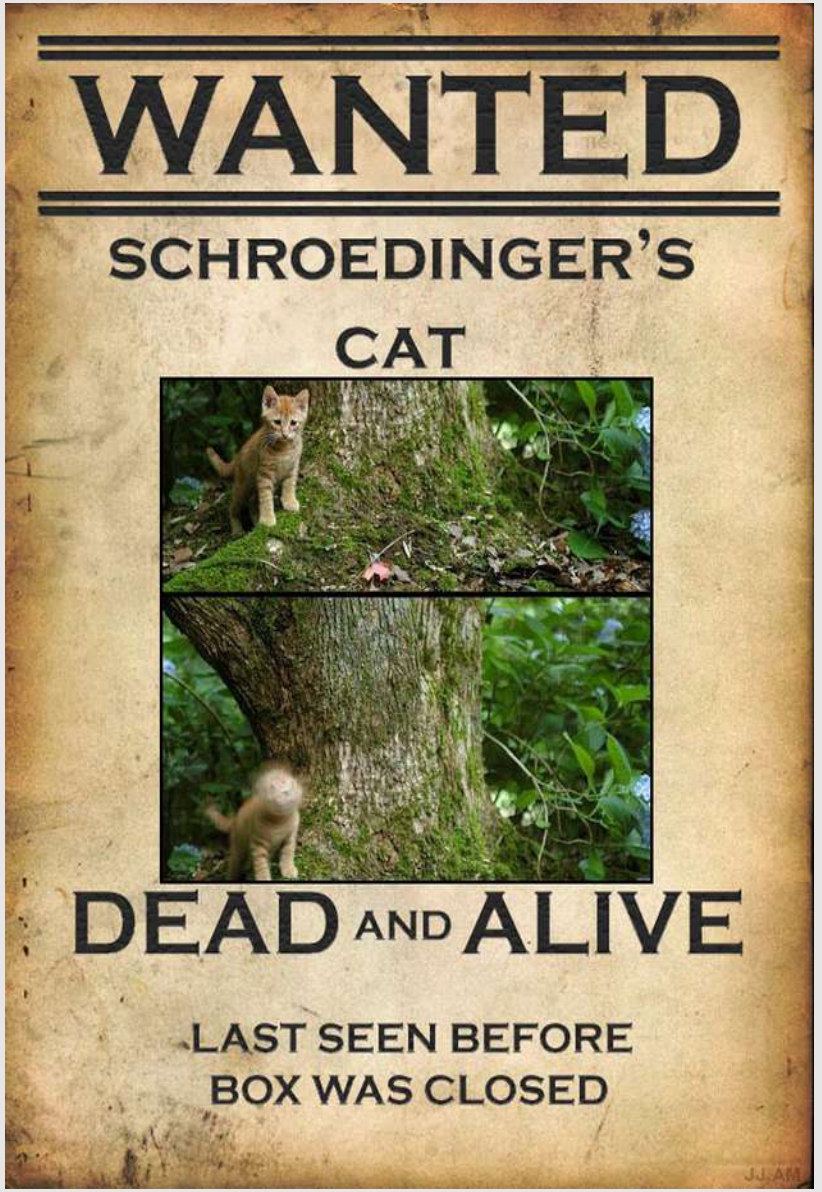
- **Lectura** (medida): Si leemos un qubit **$\alpha|0\rangle + \beta|1\rangle$,** obtenemos **0 (y el qubit se queda en el estado $|0\rangle$) con probabilidad α^2** y 1 (el qubit se queda en $|1\rangle$) con probabilidad β^2 (nótese que $\alpha^2+\beta^2 = 1$)
  - Nótese que **la lectura modifica el estado del qubit.**
  - Teorema de la No-clonación: **No se puede copiar un estado cuántico desconocido.**

Información Cuántica.

¿Y?

- ¿Recordais el gato de Schroëdinger?





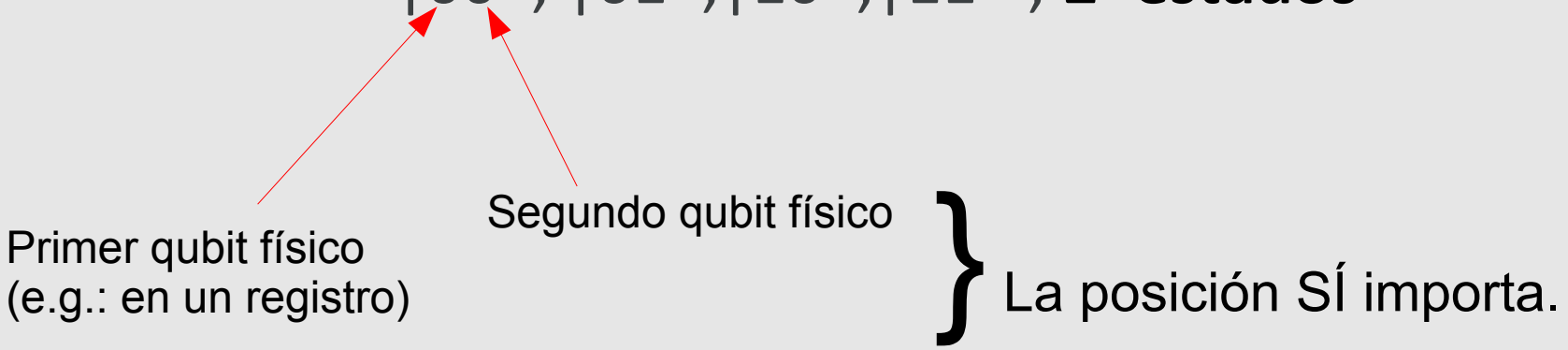
No solemos ver gatos en una combinación lineal de gato vivo/gato muerto... ¿por qué?: Decoherencia,
Uno de los motivos por los que es difícil hacer ordenadores cuánticos...

Información Cuántica.

¿Y si tenemos dos qubits?

- Puede estar en una combinación lineal de todos los estados de la base:

$|00\rangle, |01\rangle, |10\rangle, |11\rangle$; **2^2 estados**



Información Cuántica.

¿Tres qubits?

|000>, |001>,|010>,|011>,|100>,|101>,|110>,|111>; **2^3 estados**

El número de estados base crece exponencialmente con el número de qubits

- Técnicamente estamos en un espacio de Hilbert de dimensión 2^q (q=número de qubits)... **el espacio de Hilbert es un sitio muy grande**. Pero además...
- Observación: Un estado de 3 qubits puede contener una combinación lineal de “todos los números del 0 al 7”

Información Cuántica.

Con dos qubits ya aparecen cosas “curiosas”...

- Por ejemplo el estado:

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

Es lo que se llama un **estado entrelazado** (no separable) : no se puede poner como producto de el primer qubit por el segundo.

Información Cuántica.

¿Lo que significa...?

- … que lo que le pasa al primer (segundo) qubit esta correlacionado con lo que le pasa al segundo (primer) qubit: si medimos el primer qubit y nos da un 0, sabemos que el segundo es también un 0. Si es un 1, el otro también lo es... independientemente de si están cerca o lejos cuando se miden.

Esto es la **no-localidad de la mecánica cuántica.**

Información Cuántica.

- Que, además de servir para que Einstein y Bohr estuviesen en desacuerdo sobre lo que se denomina paradoja EPR (descrita en 1935), con profundas implicaciones para la física... *"la descripción de la realidad dada por las funciones de onda [la mecánica cuántica] no es completa"*
  - Discusión zanjada el año pasado a favor de Bohr, con tres experimentos clave sobre la violación de las desigualdades de Bell... justo en el centenario de la relatividad general.
- Sirven para hacer teleportación cuántica.
- Sirven para hacer criptografía cuántica.
- Sirven para mejorar la precisión de medidas.
- ...

Center for Computational Simulation

Información Cuántica.

Estos son los ingredientes esenciales...

¿Por qué tanto lio?

- Inicialmente (circa 1980) la idea era simular sistemas cuánticos.
  - Hemos visto que representar un sistema cuántico con uno clásico requiere recursos exponenciales (en espacio).
    - Se pensaba que no sería posible simular sistemas cuánticos relevantes con ordenadores clásicos.
    - La simulación de sistemas cuánticos es muy importante en tecnologías: semiconductores, nano-cosas, farmacología, quantum control (ley de Moore?)

Información Cuántica.

- En 1995 **Shor** desarrolló un algoritmo que **resolvía en tiempo polinomial en un ordenador cuántico el problema de la factorización en primos**, cuando el mejor clásico conocido es exponencial.
  - Esto rompe RSA, Diffie-Hellman y los criptosistemas basados en curvas elípticas.. la práctica totalidad de los sistemas de criptografía de clave pública... **Después de un ordenador cuántico, la criptografía no será lo mismo**...

Información Cuántica.

- En **1973 Wiesner** se dio cuenta que la mecánica cuántica se podía usar para hacer moneda infalsificable. La idea sirvió para que, en **1983, Bennet y Brassard** inventasen la **Criptografía Cuántica** con el primer protocolo de distribución de claves (**Q**uantum **K**ey **D**istribution), el **BB84**.
  - Los protocolos de **QKD son demostrablemente seguros** (information theoretical security – ITS) solo comparable a la seguridad del cuaderno de un solo uso (One Time Pad)
- En 1993 se construyo ya un aparato de laboratorio. **En 2001, el primer sistema QKD comercial.**

Center for Computational Simulation

Información Cuántica.

- En 1996, **Grover** inventó un algoritmo de búsqueda que permitía hacer **búsquedas no dirigidas en una base de datos de tamaño *N* en tiempo O(√*N*)** (comparado con O(*N*) de una clásica)
- En la **actualidad** se espera que un ordenador cuántico **revolucione** los campos que tengan **problemas de optimización** global. Se están buscando **aplicaciones en inteligencia artificial**, **teoría de control**, **medición de precisión**, etc.

Implementaciones y Situación Tecnológica.

Y, en la práctica, ¿qué se ha hecho?

Implementaciones y Situación Tecnológica.

Todo tipo de demostraciones de concepto con muchas variantes tecnológicas.

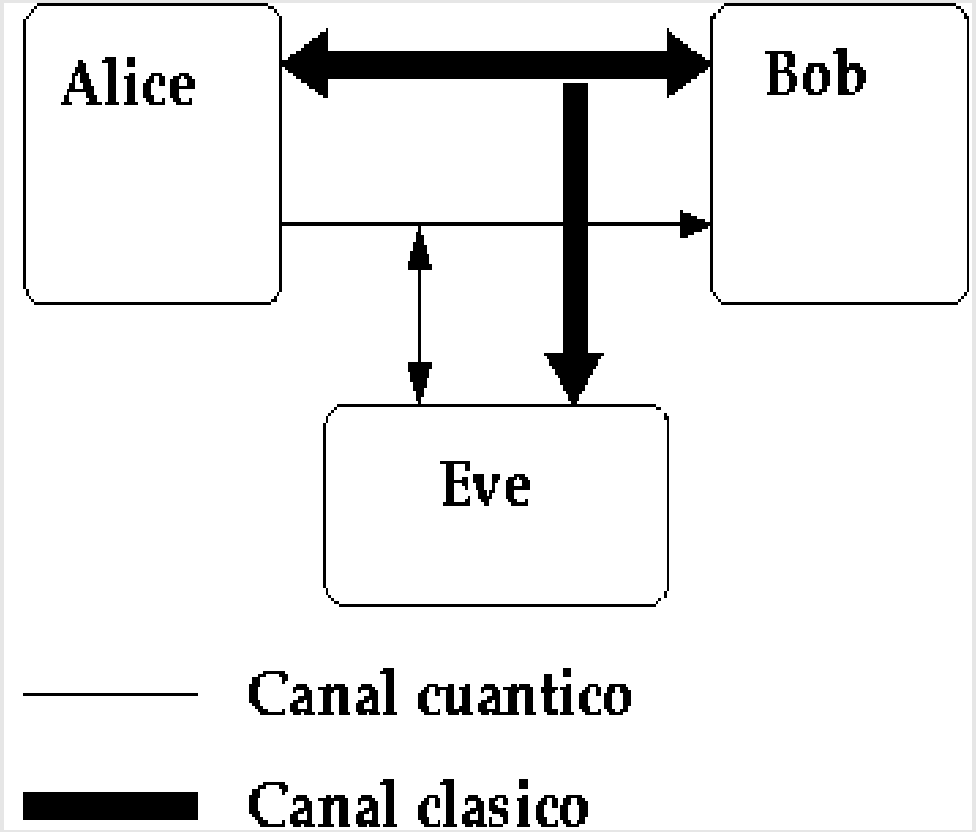
- Generación de sistemas entrelazados: ya habitual
- Teleportación de estados cuánticos. Desde unos pocos centímetros a 144 Km. Con partículas masivas y fotones.
- Algoritmos de Grover y Shor en unos pocos qubits y con tecnologías de iones, de resonancia magnética nuclear, etc. Corrección de errores.
- QKD: comercial. Redes de más de 2000 Km. Links con satélites.
- Computación cuántica adiabática y simuladores.
- Etc, etc, etc...

Implementaciones y Situación Tecnológica.

Un vistazo más detallado: Criptografía cuántica*.

Ingredientes:

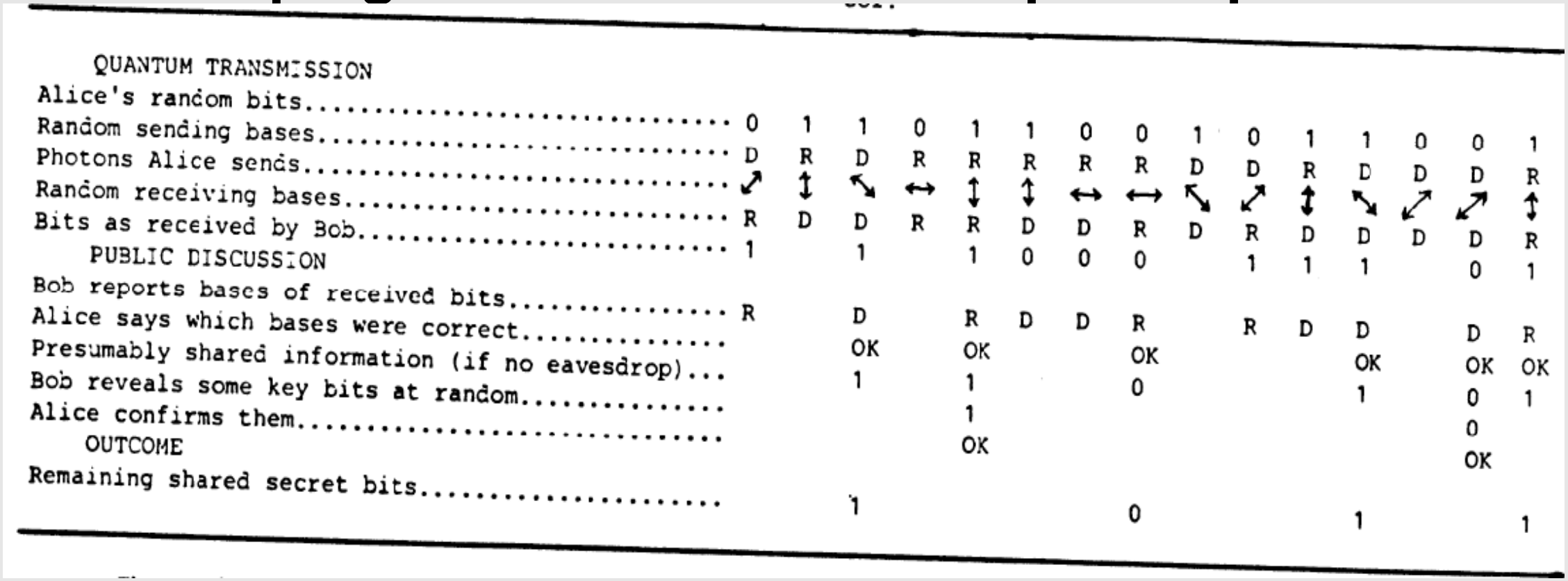
- Un **emisor de qubits** (típicamente fotones) individuales (Alice)
- **Receptores** de qubits individuales (Bob)
- Un **canal cuántico** (capaz de transmitir los qubits de Alice a Bob)
- Un **canal clásico** (público pero **autenticado**)
- … y un espía (Eve)



* Criptografía cuántica se suele usar como sinónimo de distribución cuántica de claves. Es un abuso de notación.

Implementaciones y Situación Tecnológica.

Criptografía cuántica: BB84 el primer protocolo



QUANTUM TRANSMISSION														
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Bennet, Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing“ International Conference on Computers, Systems and Signal Processing. Bangalore, 1984

Implementaciones y Situación Tecnológica.

Criptografía cuántica: BB84 el primer protocolo

ALICE
Emisor

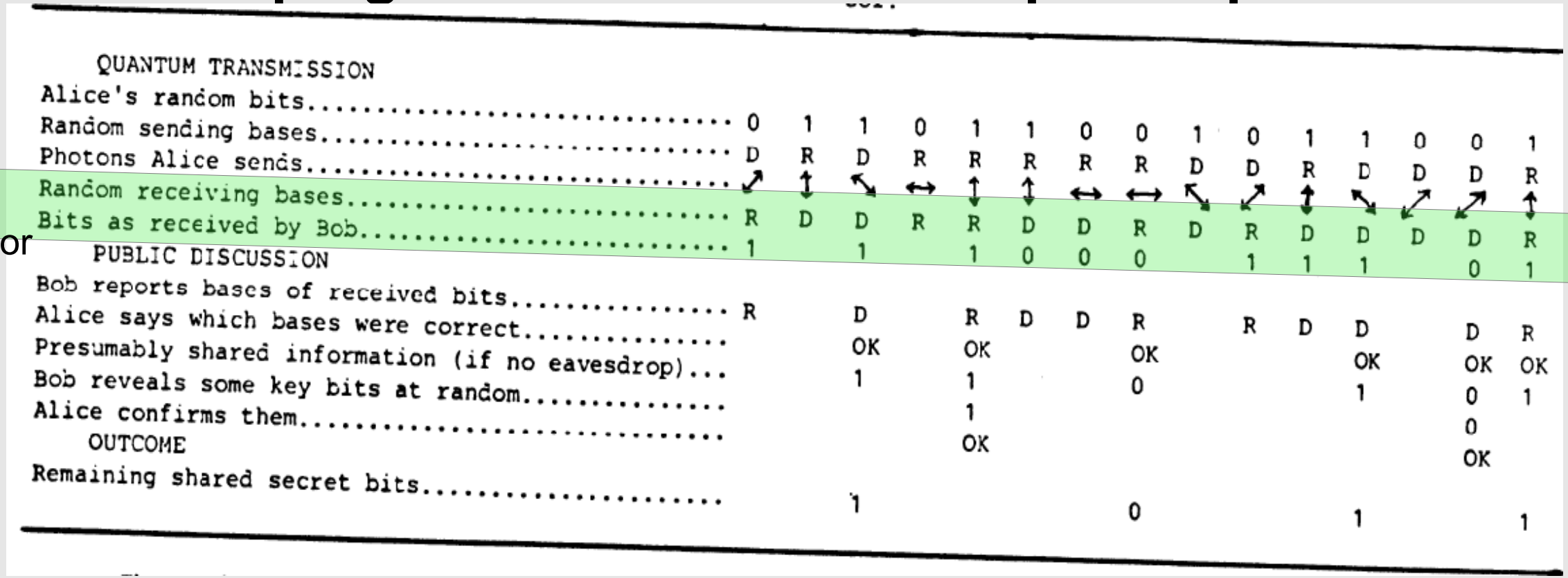
QUANTUM TRANSMISSION														
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Bennet, Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing“ International Conference on Computers, Systems and Signal Processing. Bangalore, 1984

Implementaciones y Situación Tecnológica.

Criptografía cuántica: BB84 el primer protocolo

BOB receptor



QUANTUM TRANSMISSION															
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

Bennet, Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing“ International Conference on Computers, Systems and Signal Processing. Bangalore, 1984

Implementaciones y Situación Tecnológica.

Criptografía cuántica: BB84 el primer protocolo

QUANTUM TRANSMISSION														
Alice's random bits	0	1	1	0	1	1	0	0	1	0	1	1	0	0	1
Random sending bases	D	R	D	R	R	R	R	R	D	D	R	D	D	D	R
Photons Alice sends	↗	↕	↘	↔	↕	↕	↔	↔	↘	↗	↕	↘	↗	↗	↕
Random receiving bases	R	D	D	R	R	D	D	R	D	R	D	D	D	D	R
Bits as received by Bob	1		1		1	0	0	0		1	1	1		0	1
PUBLIC DISCUSSION															
Bob reports bases of received bits	R		D		R	D	D	R		R	D	D		D	R
Alice says which bases were correct			OK		OK			OK				OK		OK	OK
Presumably shared information (if no eavesdrop)			1		1			0				1		0	1
Bob reveals some key bits at random					1									0	
Alice confirms them					OK									OK	
OUTCOME															
Remaining shared secret bits			1					0				1			1

(CLÁSICA)

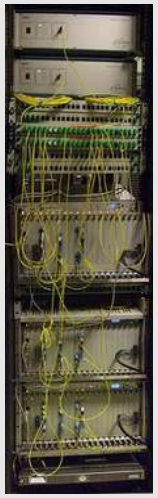
Detección de Intrusos y Corrección de errores (ruido)

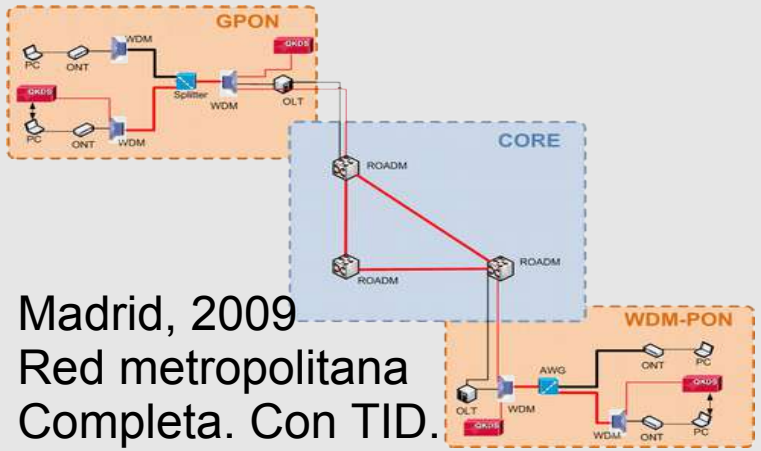
Bennet, Brassard. „Quantum Cryptography: Public Key Distribution and Coin Tossing“ International Conference on Computers, Systems and Signal Processing. Bangalore, 1984

Implementaciones y Situación Tecnológica.

Criptografía cuántica en la práctica.

- Sistemas y empresas **comerciales**: Id Quantique, Huawei, Toshiba, NEC, Quintessence, etc. y **muchos laboratorios.**
- **Despliegue en redes**, metropolitanas (conmutadas) y de largo alcance (nodos confiables).





Madrid, 2009
Red metropolitana
Completa. Con TID.

Beijing-Shangai
2016. 2000 Km.
Nodos confiables.

Nota: QKD es un sistema de **clave simétrica** que está intrínsecamente **limitado por la distancia**. En la actualidad, unos pocos centenares de Km.

Implementaciones y Situación Tecnológica.

Un vistazo más detallado: Computación cuántica. Caveats.

Es inevitable que las manipulaciones que realicemos en un sistema cuántico para hacer el cálculo no sean perfectas.

- ¿Podemos **corregir un sistema** que modificamos cuando medimos?
- ¿Es posible realizar una **computación cuántica** de manera **indefinida**?
  - Sí a ambas: códigos correctores de errores y teorema del umbral.

Center for Computational Simulation

Implementaciones y Situación Tecnológica.

Computación cuántica: modelos.

- Basada en puertas (modelo de circuitos)
- Computación cuántica adiabática
- Simuladores cuánticos

Implementaciones y Situación Tecnológica.

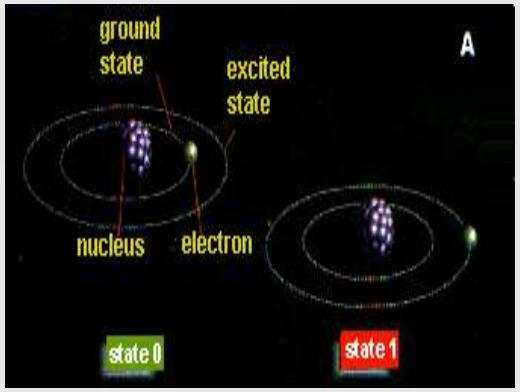
Computación cuántica con puertas.

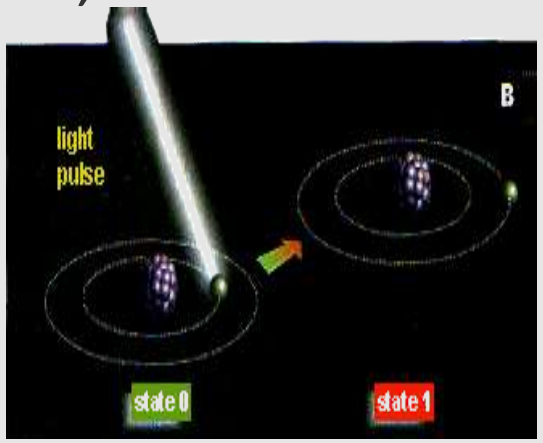
- Este es el modelo “canónico”: una serie de puertas cuánticas formando un circuito se aplican a una serie de qubits.
- **¿Cómo es una puerta cuántica?**
  - Depende mucho de qué tecnología se esté usando para el qubit... y hay muchas (i.e.: no tenemos un ganador claro)
    - En el estado fundamental de un átomo.
    - En el flujo o la carga en un anillo superconductor.
    - En la polarización de un fotón.
    - En un qubit topológico...

Implementaciones y Situación Tecnológica.

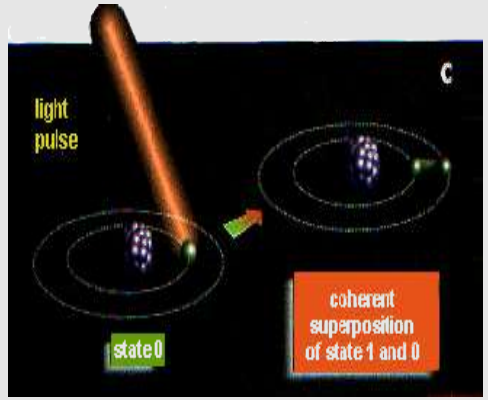
Un ejemplo de puerta cuántica: la raíz cuadrada de NOT.

- Qubit codificado en los dos estados de más baja energía de un átomos. Se dirige un haz de láser de la frecuencia dada por la diferencia de energía entre niveles. Esto cambia el estado, llevándolo a cero si era uno y a uno si era cero: NOT





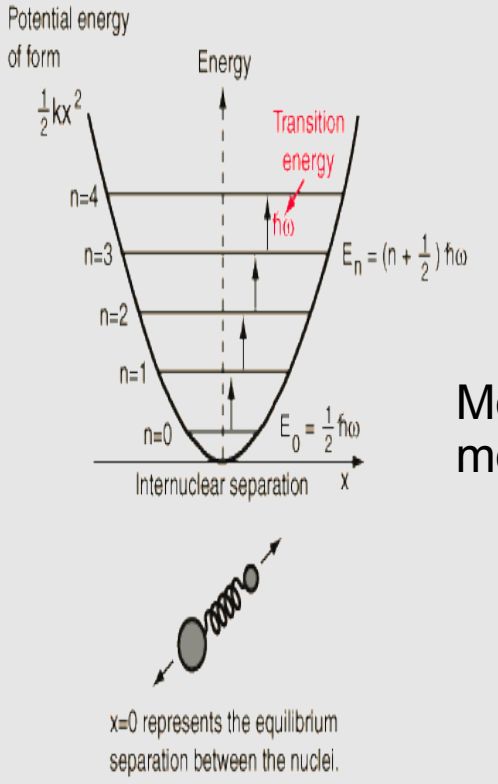
- Un pulso con la mitad de energía pone el qubit en una superposición de |0> y |1>. La raíz de NOT

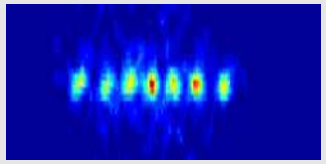


Implementaciones y Situación Tecnológica.

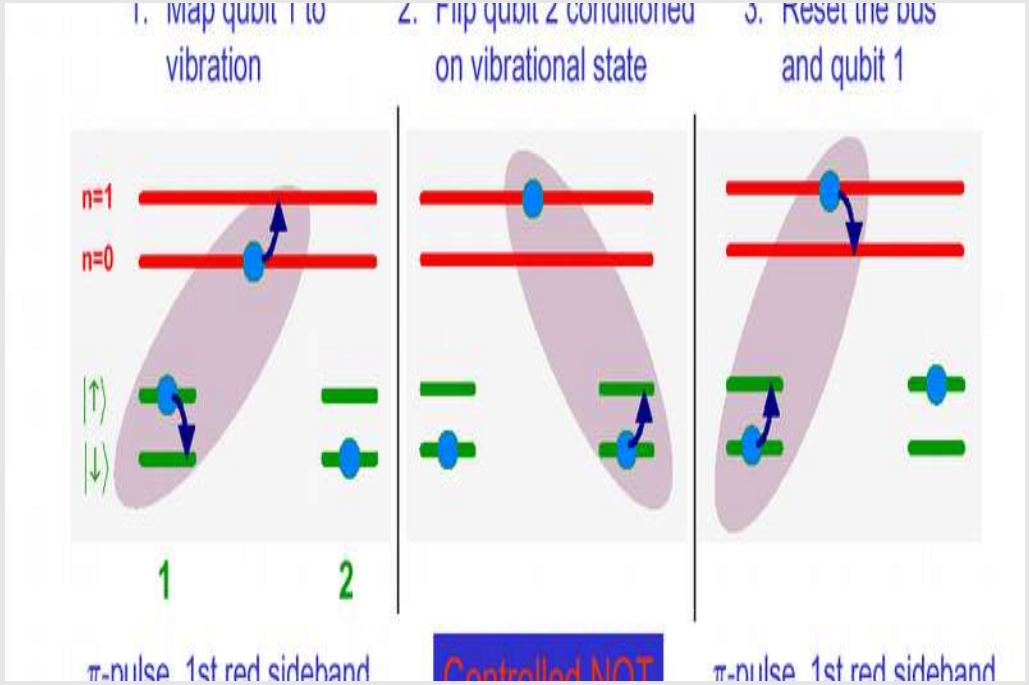
Computación cuántica: Trampas de Iones.

- Qubits en los estados más bajos de un dispositivos que confina los iones en un campo electromagnético: trampa de iones





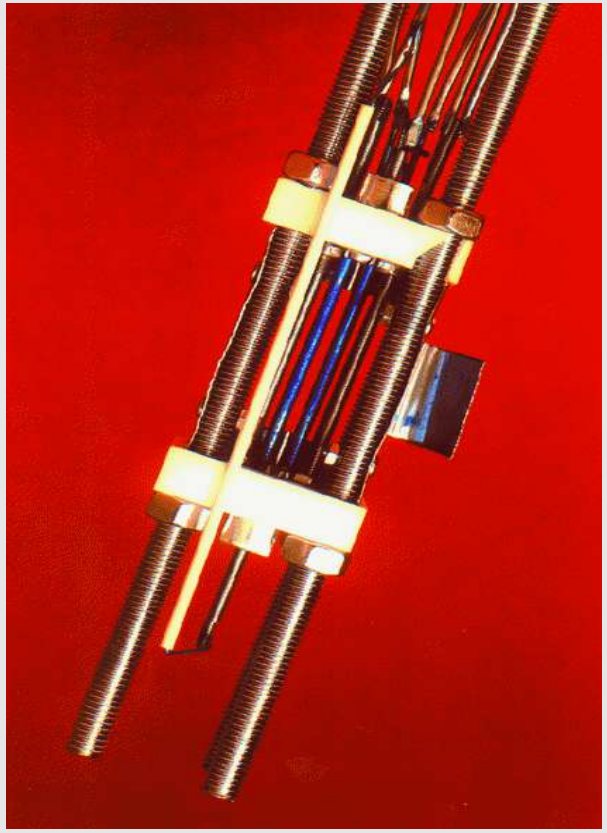
Modo 'stretch', el primer modo colectivo excitado



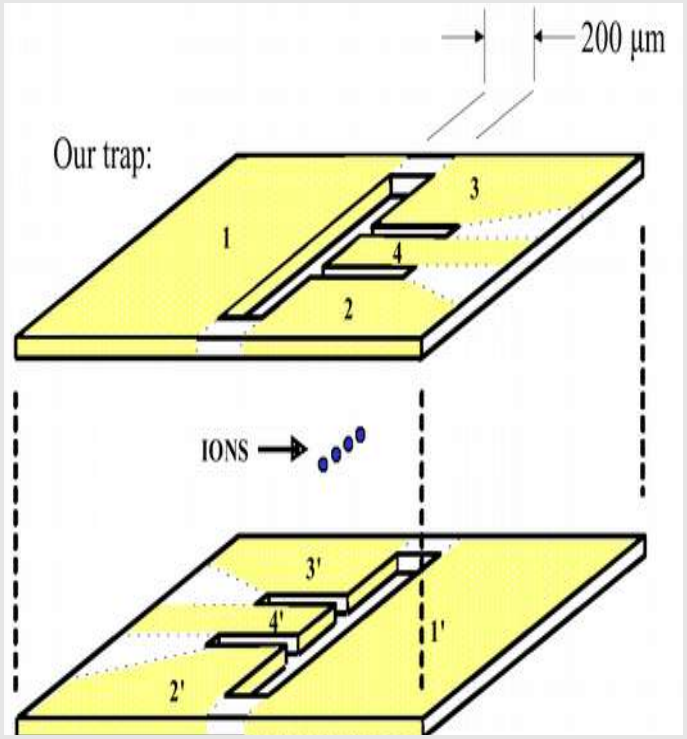
Puerta de dos qubits usando un modo colectivo: bus de fonón.

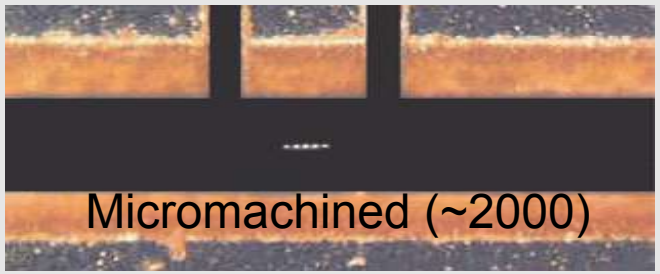
Implementaciones y Situación Tecnológica.

Trampas de iones: tecnología

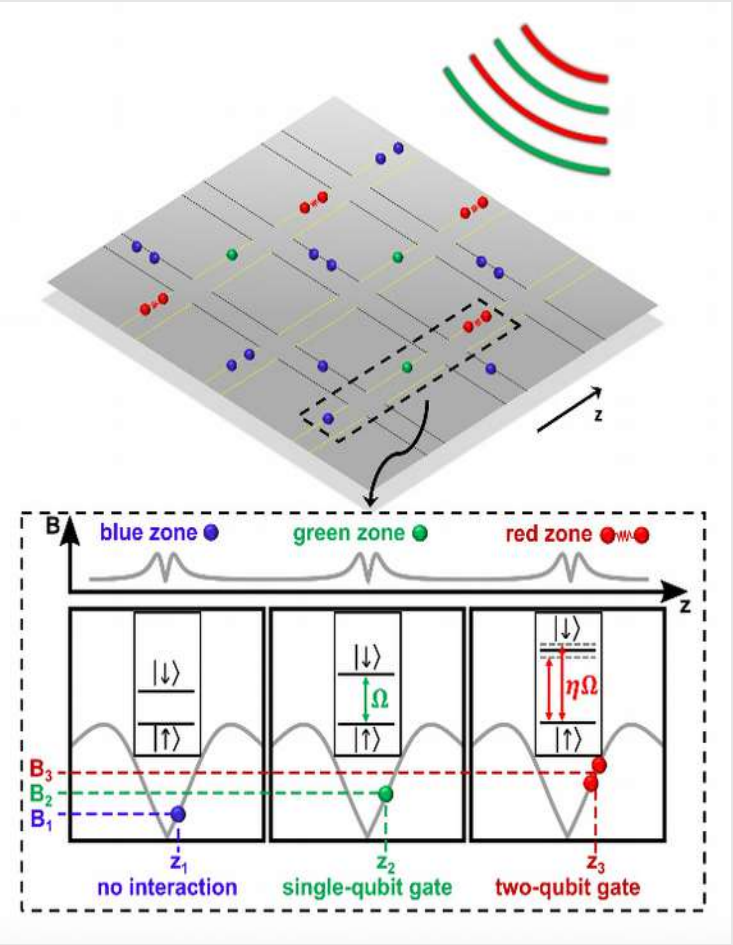


Iniciales (~1990)





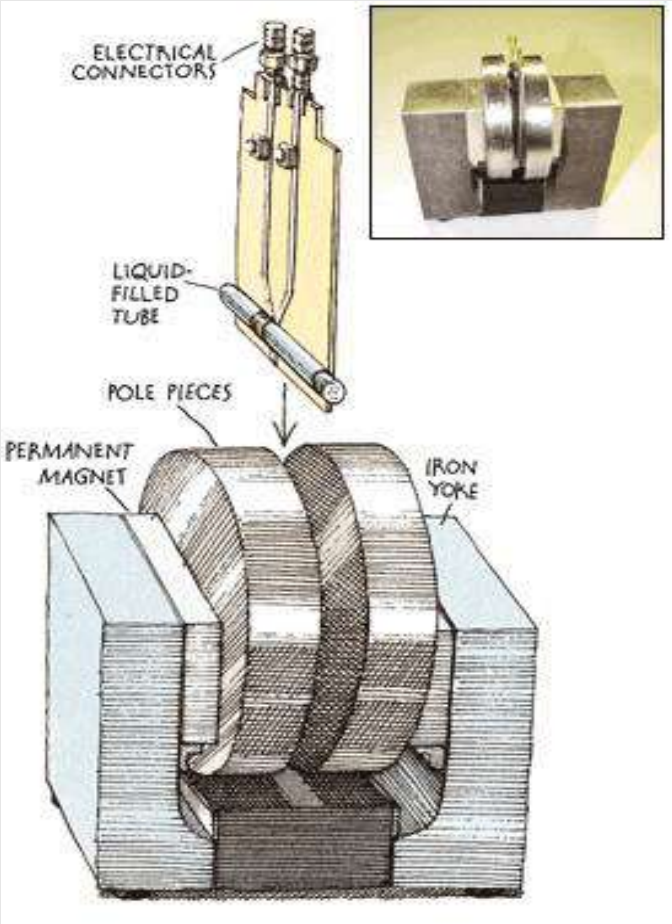
Micromachined (~2000)



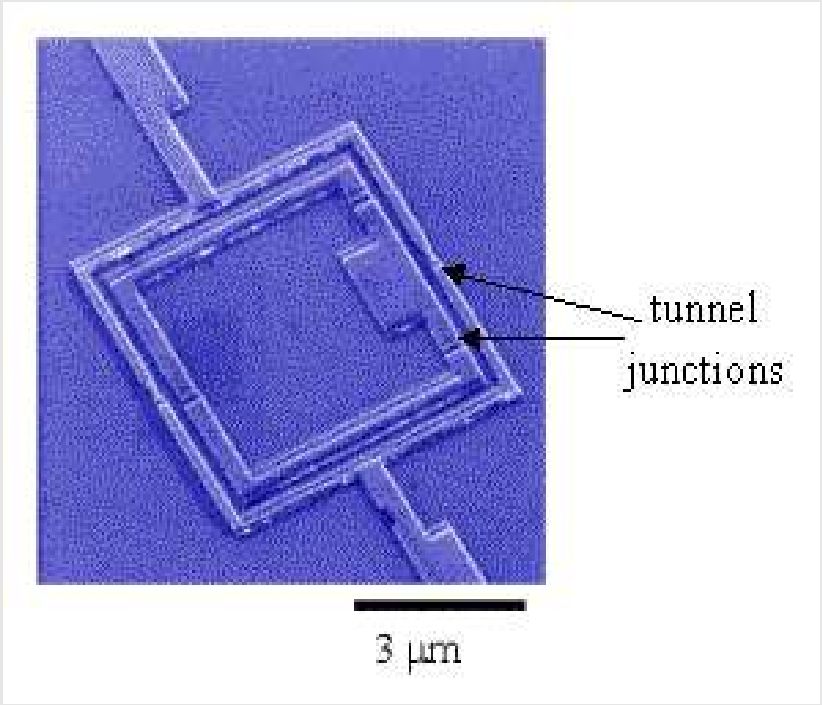
Con campo de radiación global (2016)
Escalable.

Implementaciones y Situación Tecnológica.

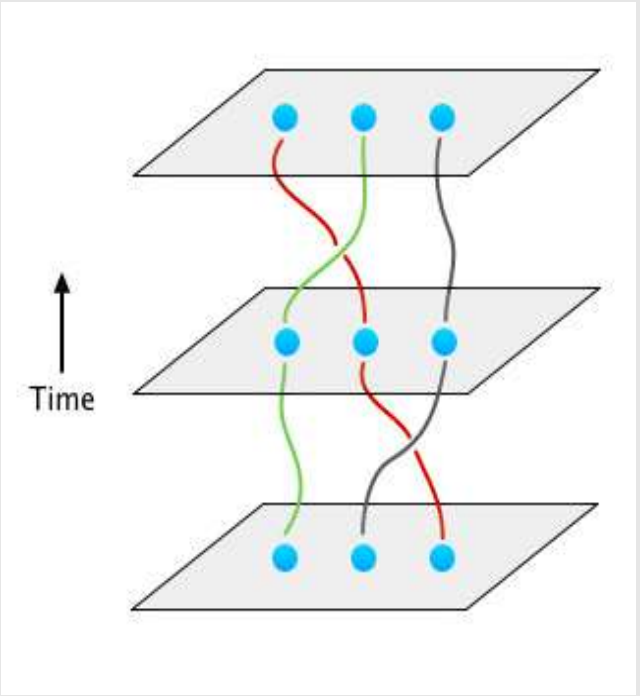
Modelo de puertas: galería.



NMR: cada molécula en el líquido
Es un ordenador cuántico de unos pocos qubits direccionados por pulsos en la bobina.



Qubit de flujo con superconductores.



Qubits topológicos, autoprotegidos frente a errores, se trenzan para realizar puertas. Este es el camino Tomado por MicroSoft y también por uno de los equipos de Google.

Implementaciones y Situación Tecnológica.

Computación cuántica adiabática.

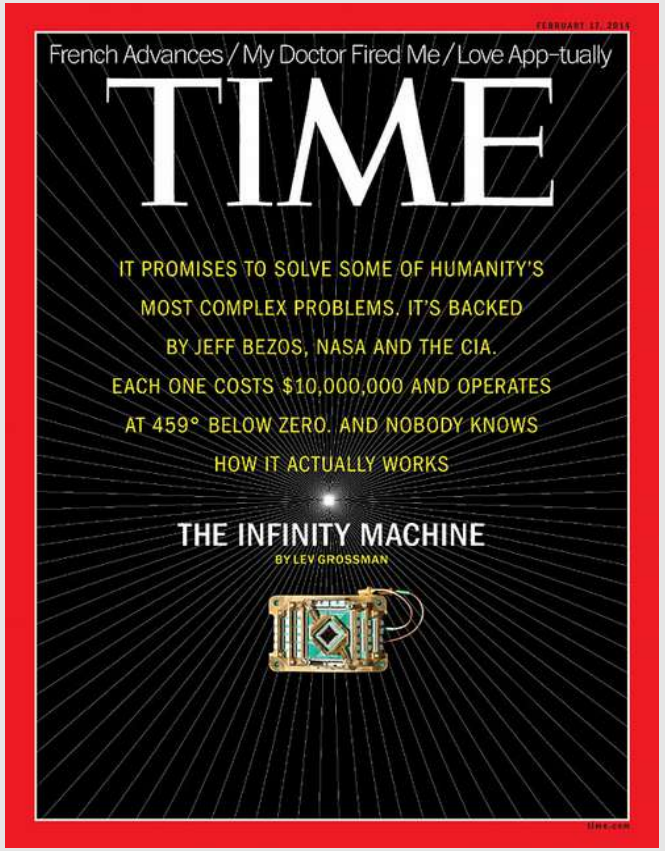
- Formalmente **equivalente** al modelo de puertas.
- El Hamiltoniano que describe el sistema físico se hace evolucionar (de manera suficientemente lenta) desde su estado fundamental (conocido a *t=0*) hasta otro del que sabemos que codifica en su estado fundamental la solución al problema.
  - Usamos dos funciones, *A(t)* que disminuye de 1 a 0 y *B(t)* que aumenta de 0 a 1 cuando *t* va de 0 a 1 (en unidades de tiempo adecuadas).

$$H(t) = A(t)\,H(0) + B(t)\,H(1)$$

Implementaciones y Situación Tecnológica.

Computación cuántica adiabática.

- Este es el modelo elegido por Dwave, que ha sido tan publicitado.

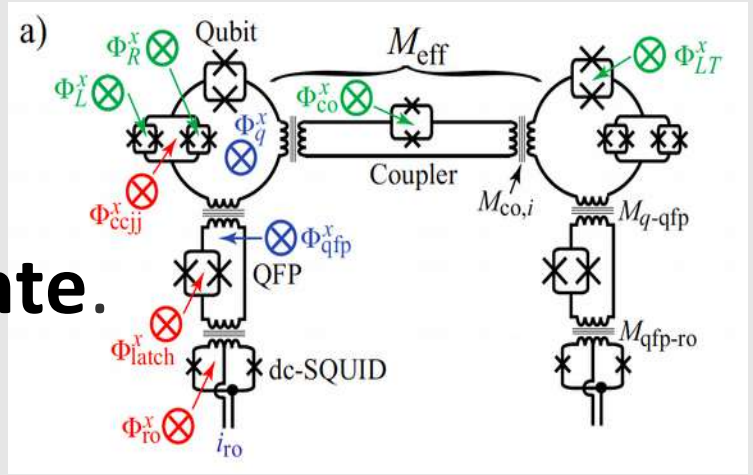


Wired 20-5-2014

Implementaciones y Situación Tecnológica.

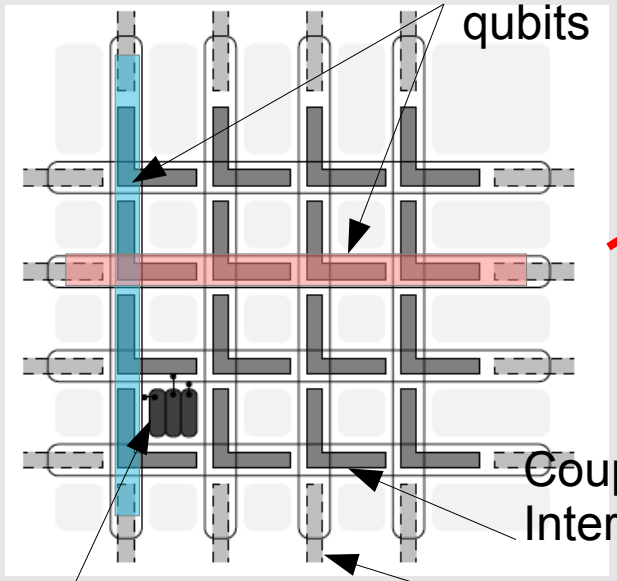
Computación cuántica adiabática.

- La **implementación de DWave es limitada** (no todos los qubits interactúan con todos).
  - Realiza un proceso conocido como “quantum annealing”
- Hay **dudas razonables** sobre si es realmente cuántico.
- Se ha hecho benchmarking, pero los resultados hay que juzgarlos con cuidado.
- … pero su **ingeniería de qubits es impresionante**.
- Y han abierto nuevas vías.



Implementaciones y Situación Tecnológica.

Computación cuántica adiabática: DWave



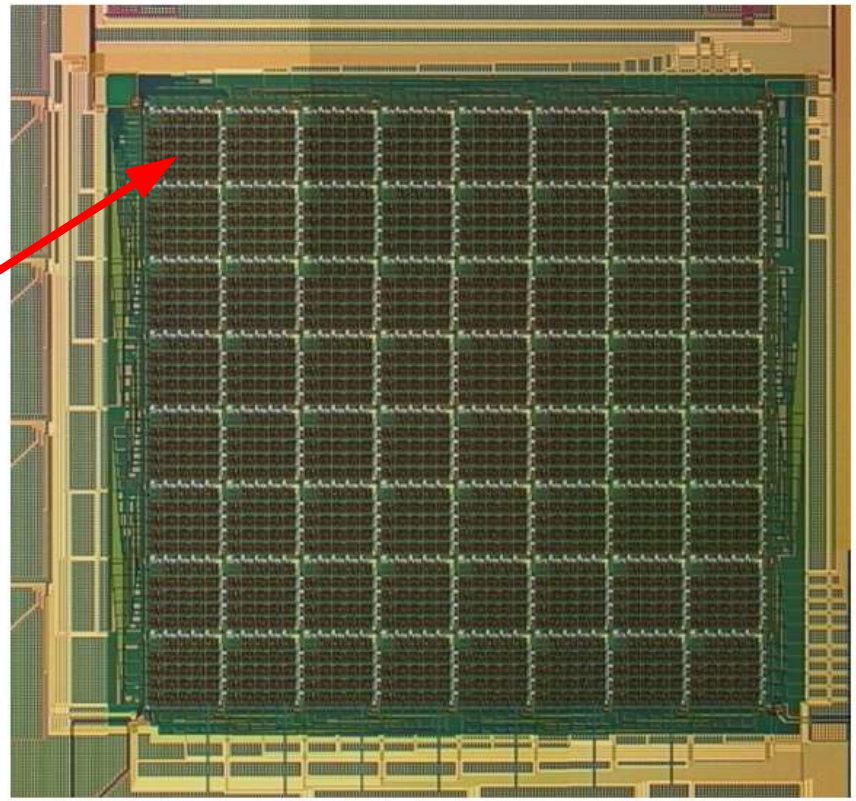
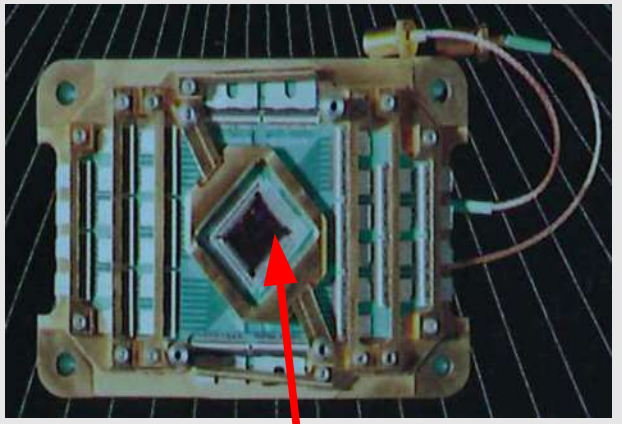
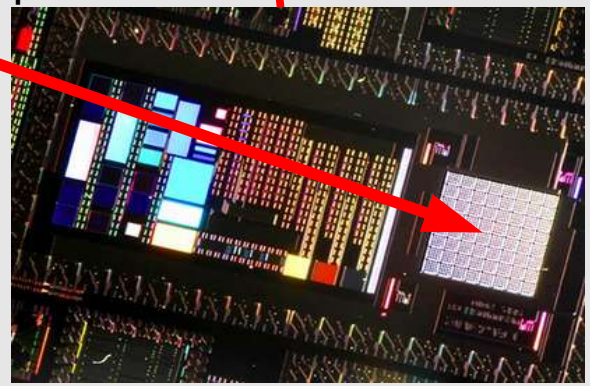


Fig. 9. Microphotograph of an active portion ($\sim 3.5 \times 3.5\,\mathrm{mm}^2$) of D-Wave Two processor chip, 8×8 array of 8-qubit unit tiles, one unit tile is $335\,\mu\mathrm{m}$ on the side. This picture was taken before deposition of the last metal layer (serving as skyplane), making internal structure visible.



Above: Dwave full 512 qubits processor:

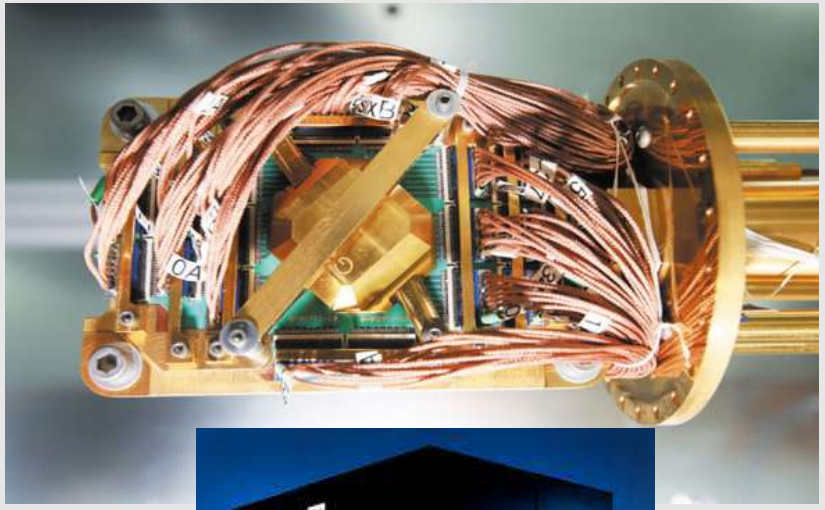


64 qubits

Bunyk et al. ArXiv:1401.5504

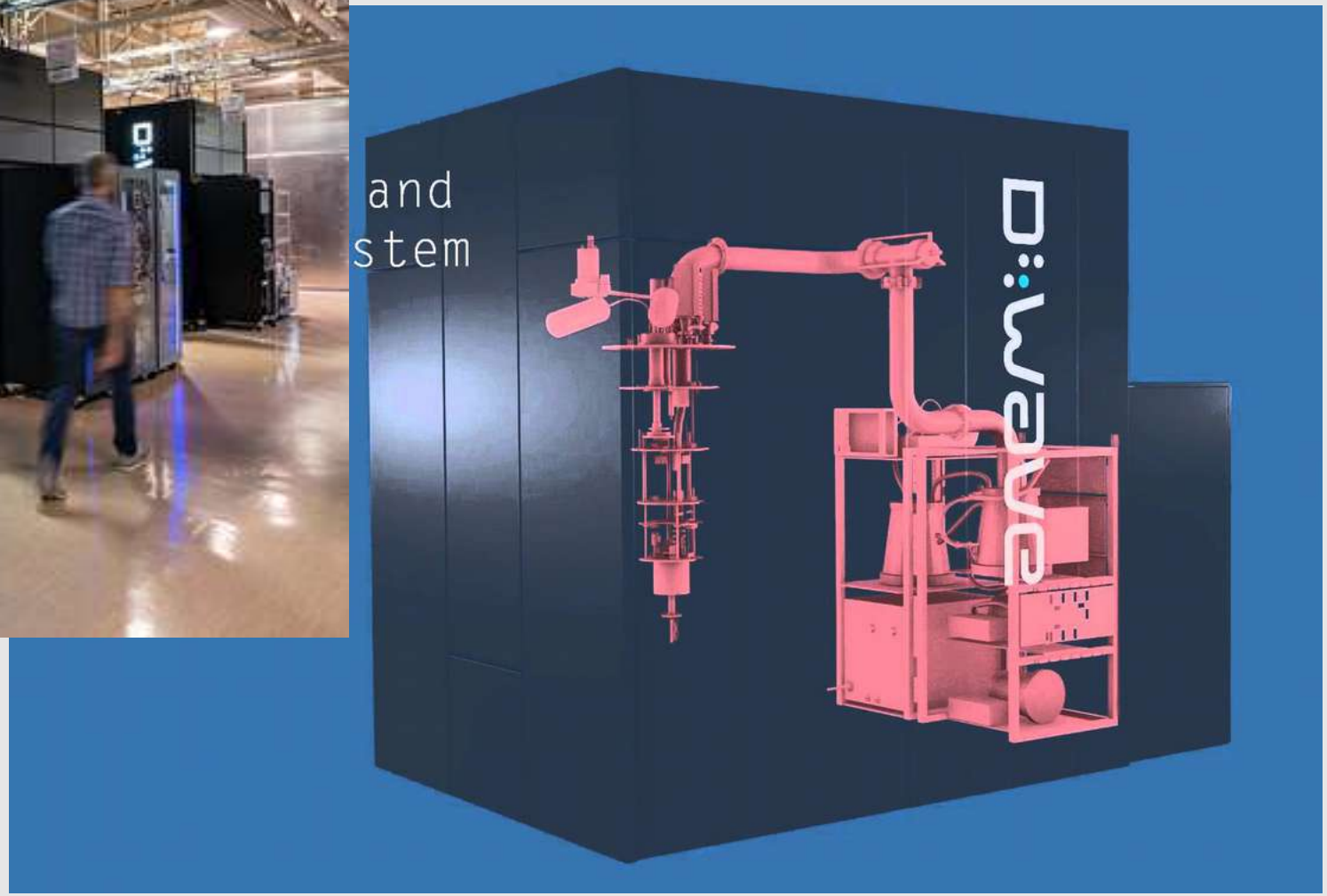
Implementaciones y Situación Tecnológica.

Computación cuántica adiabática: DWave



Implementaciones y Situación Tecnológica.

Computación cuántica adiabática: DWave



Implementaciones y Situación Tecnológica.

Simuladores cuánticos.

- **Se simula un sistema** (físico o "algorítmico") **usando otro.**
- Modificando los parámetros que regulan el hamiltoniano del simulador se puede emular un rango de sistemas.
- **Se cree más fácil**, con la tecnología existente, llegar a resolver problemas de tamaño moderado en el corto plazo usando un simulador que llegar a construir un ordenador cuántico completo, con la necesaria corrección de errores.

Implementaciones y Situación Tecnológica.

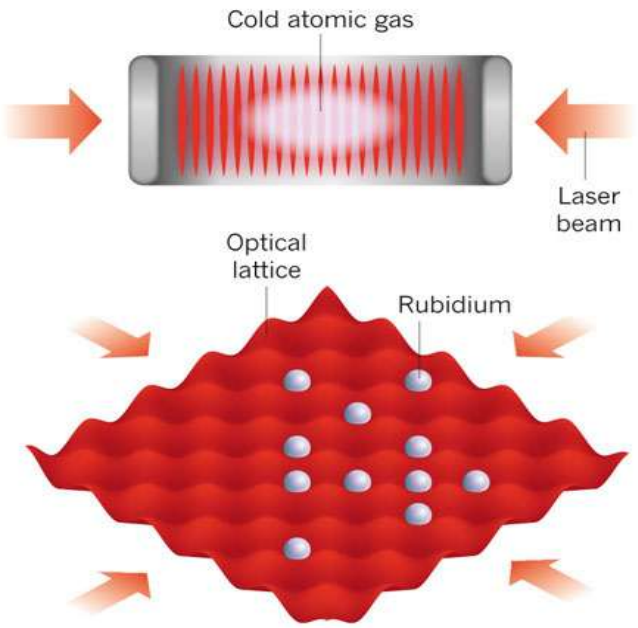
Simuladores cuánticos: ejemplos

QUANTUM BOARD GAMES

The set-ups of quantum simulators are different, but the concept is the same: first take atoms, ions or electrons, cool them to cryogenic temperatures and arrange them in an orderly grid. Then tune the interactions on the grid to mimic a more complex material.

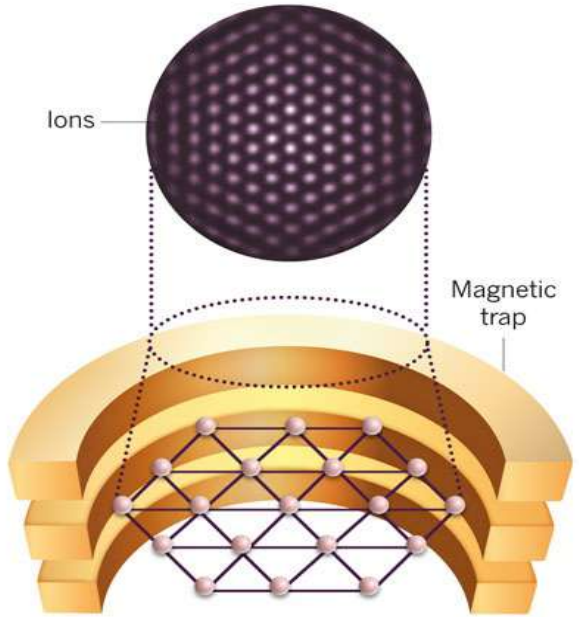
COLD ATOMS

Rubidium atoms are held in place by criss-crossed laser beams, which can also be used to tweak individual particles. A single pair of lasers holds the atoms in a one-dimensional column (top), whereas two pairs hold them in a grid (bottom). Some excitations in the grid system behave like the Higgs particle.



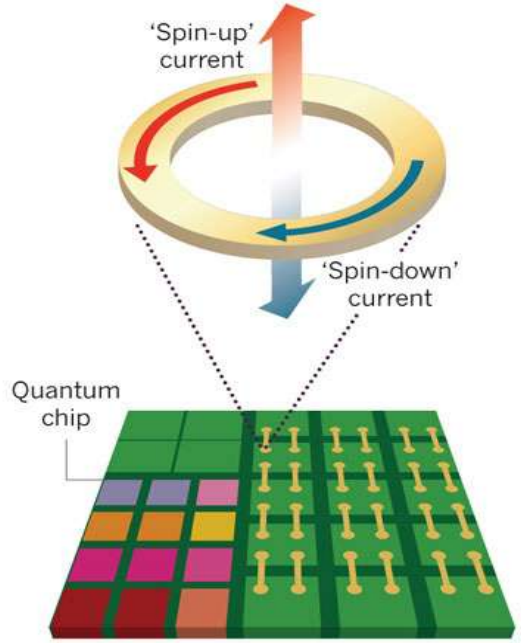
TRAPPED IONS

A combination of electric and magnetic fields trap charged, ionized atoms in an orderly grid. The ions wiggle and rotate in a way that mimics the interactions of quantum magnetism — a phenomenon that can't be simulated in classical systems.



SUPERCONDUCTING LOOPS

A quantized loop of current can flow clockwise, anticlockwise or in a superposition of both in a superconducting circuit (top). An array of such loops (bottom) can be manipulated to simulate various quantum systems — and perhaps even biological processes such as photosynthesis.



Implementaciones y Situación Tecnológica.

Simuladores cuánticos.

- Se abren nuevas vías algorítmicas:
  - E.g.: Un **simulador para factorizar en primos.**
  - Una nueva aproximación, evitando tener que construir un ordenador capaz de ejecutar el algoritmo de Shor.
  - Con implicaciones más allá del dispositivo:
    - Distribución de primos (hipótesis de Riemann)
    - ¿Nuevos algoritmos de factorización? (sin cribas)

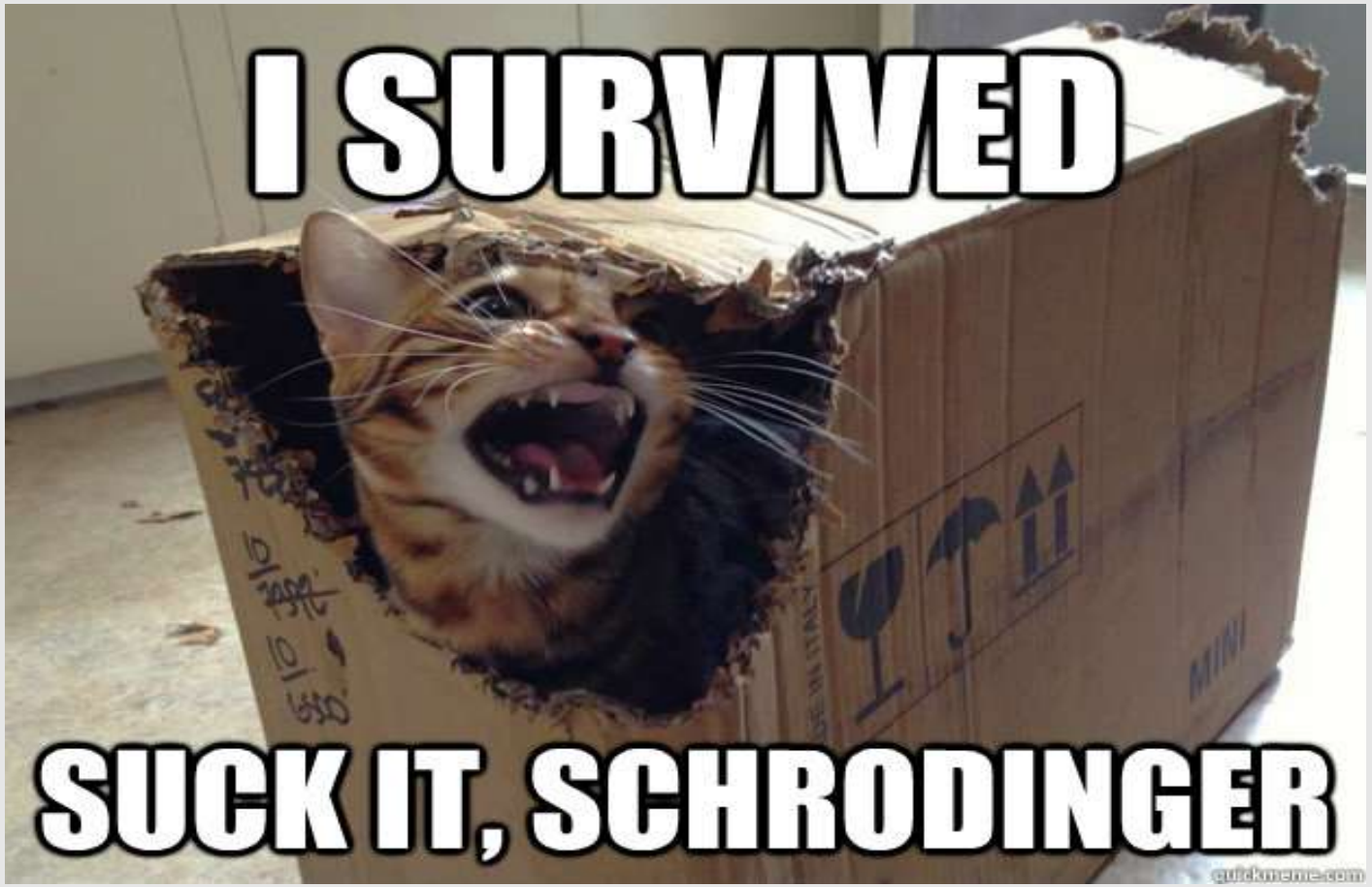
J.L Rosales, V. Martin, “Quantum Simulation of the factorization problem”
http://dx.doi.org/10.1103/PhysRevLett.117.200502

Interés en Investigación e Industria

- Las tecnologías cuánticas están despertando cada vez un mayor interés, tanto desde el punto de vista científico, tecnológico e industrial.
- Con grandes polos de atracción de talento e inversión (e.g.: Canadá IQC & Perimeter, Holanda Qutech)
- En Europa se ha aprobado una iniciativa Flagship (1000 M€) cuya estructura se está discutiendo. Empezará a fines de 2017.
  - Con un High Level Industry Steering Committee formado por 10 empresas.
- Con grandes empresas que están apostando: Microsoft, Google, Intel...
  - Y también alguna empresa y think tank española: VLC photonics, Elite, Entanglement Partners, Barcelona Qubit...

CCS
Center for
Computational Simulation

¡Gracias por su atención!

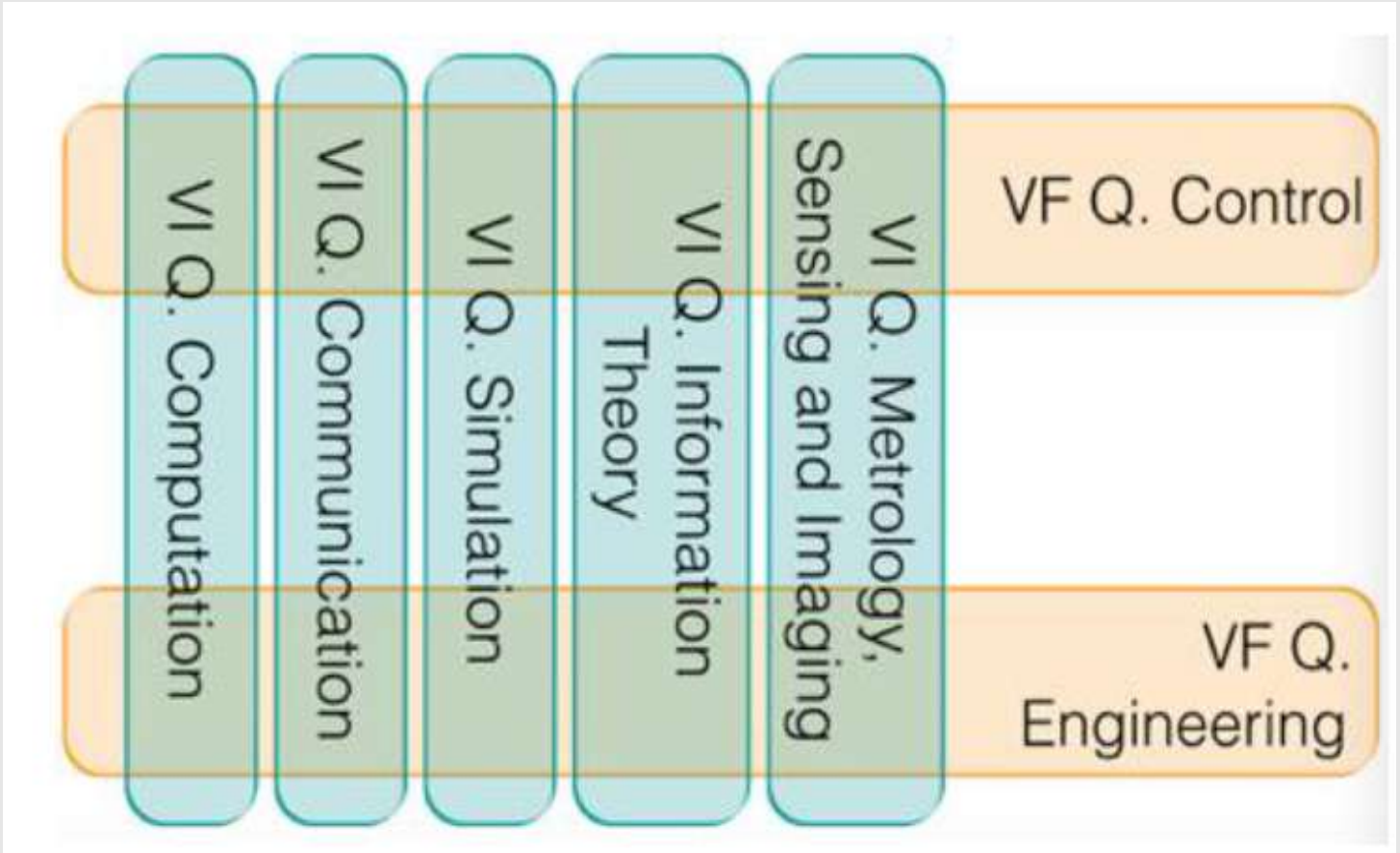


$|;-)\rangle$

Si han llegado hasta aquí... y tienen alguna pregunta...

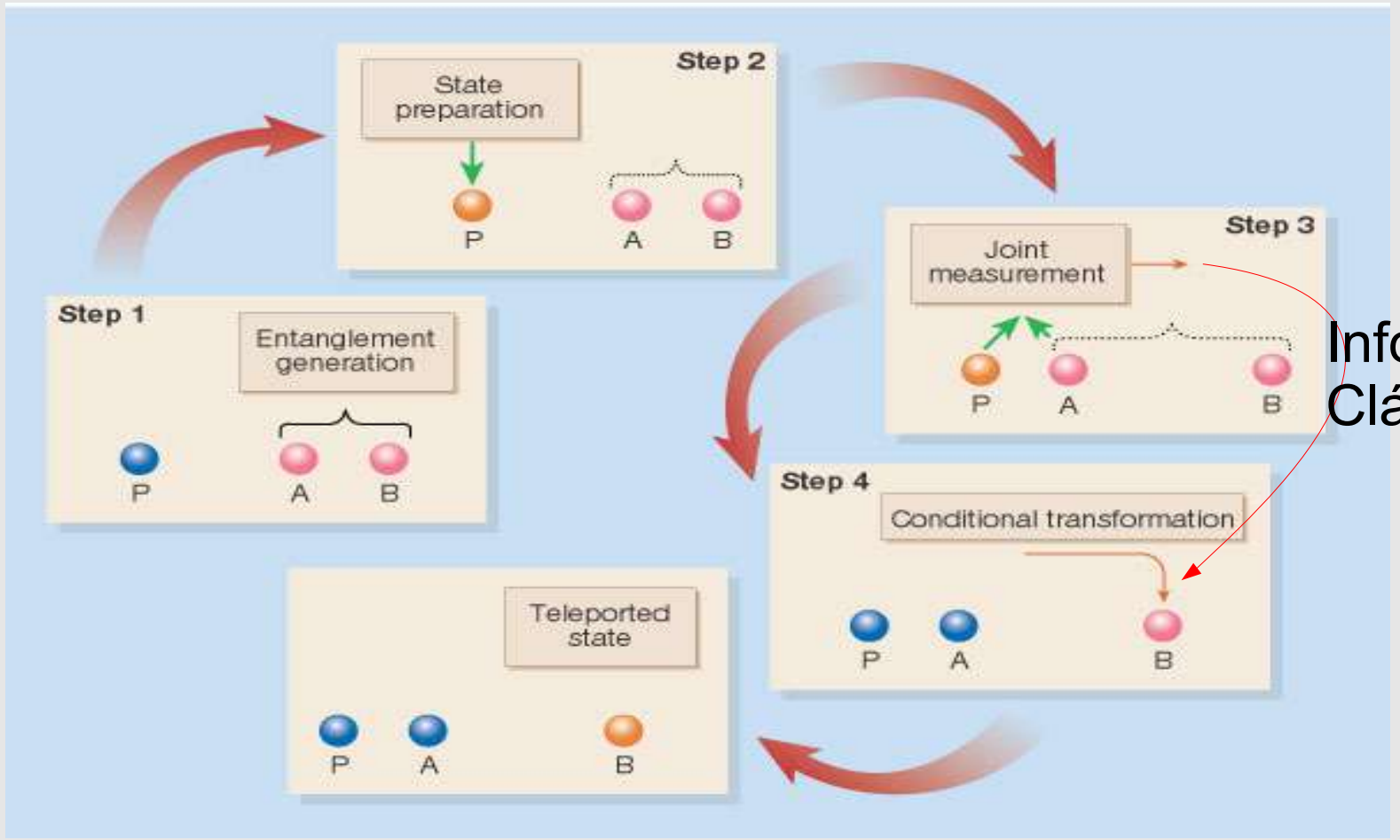
Quantum flagship structure

- VI = Virtual Institute
- VF = Virtual Facility



Teleportación cuántica

Teleportación cuántica: qubit(desconocido)+EPR+2bits transmitidos = qubit(desconocido) en otro lugar.



Información Clásica: 2 bits

I.

I.