#gigatic16

gigaTIC

X Congrés Iberoamericà de la Governança i la Gestió Avançada de les TIC

28 abril - Barcelona

Torre Telefónica - Diagonal 00

organitzen:

itSMF ESPAÑA Catalunya

ISACA Trust in, and value from, information systems Barcelona Chapter

Universitat de Barcelona

¿Estamos preparados para la nueva era cuántica?

José Ignacio LATORRE

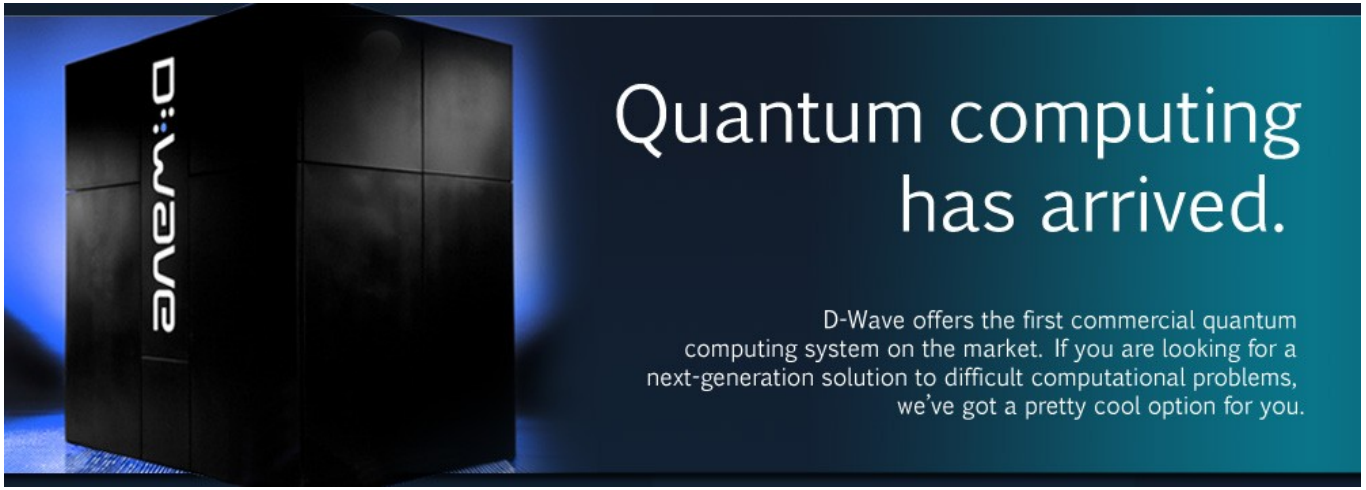
#gigaTIC16

¿Por qué?

Google

- Google compra un ordenador cuántico

  DWAVE2 10^8 speed up

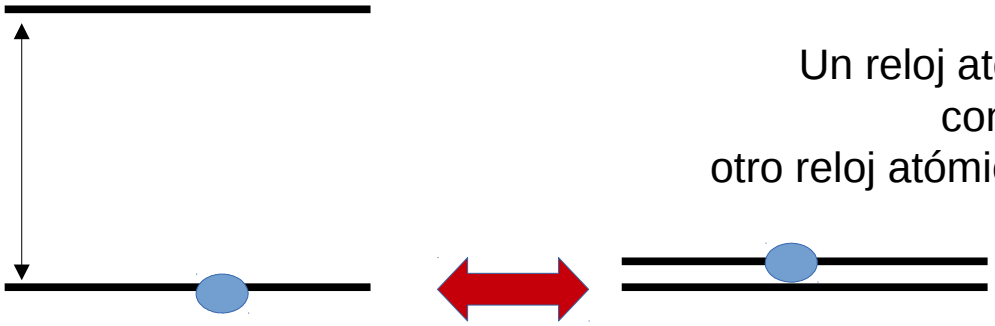


EU

- Flagship 1 GEuros

  Quantum Manifesto: Amsterdam 17/05/2016

REALIDAD



Un reloj atómico **preciso**
controla a
otro reloj atómico **ultra preciso !!!**

Aluminio

Berilio

Entrelazamiento CNOT Cirac-Zoller

Precisión de 1 parte en 10^{18}

Nueva generación de GPS con precisión de 1mm !!!!

¿Estamos preparados?

- ¿Va en serio?
- ¿Hay una revolución disruptiva en ciernes?
- ¿Qué principios se barajan?
- ¿Qué cambiará?
- ¿Qué negocios quedarán afectados?
- ¿De qué plazos se habla?
- ¿Seremos competitivos?

¿Estamos preparados?

- ¿Va en serio?

SÍ

- ¿Hay una revolución disruptiva en ciernes?

SÍ

- ¿Qué principios se barajan?

Principios genuinamente cuánticos

- ¿Qué cambiará?

Sensores, criptografía, computación, relojes, simulación

- ¿Qué negocios quedarán afectados?

Cyberseguridad, computación, nuevos materiales, diseño de fármacos,...

- ¿De qué plazos se habla?

Depende de la aplicación: de 0 a 20 años

- ¿Seremos competitivos?

Ojalá no perdamos este tren

Computación cuántica

Principios cuánticos

- Principio de superposición

Un qubit puede describir 0 y 1 a la vez

- Evolución

Las qubits se procesan en paralelo

- Medida

El resultado de la medida es probabilístico

Superposición

La función de onda describe la Información del sistema

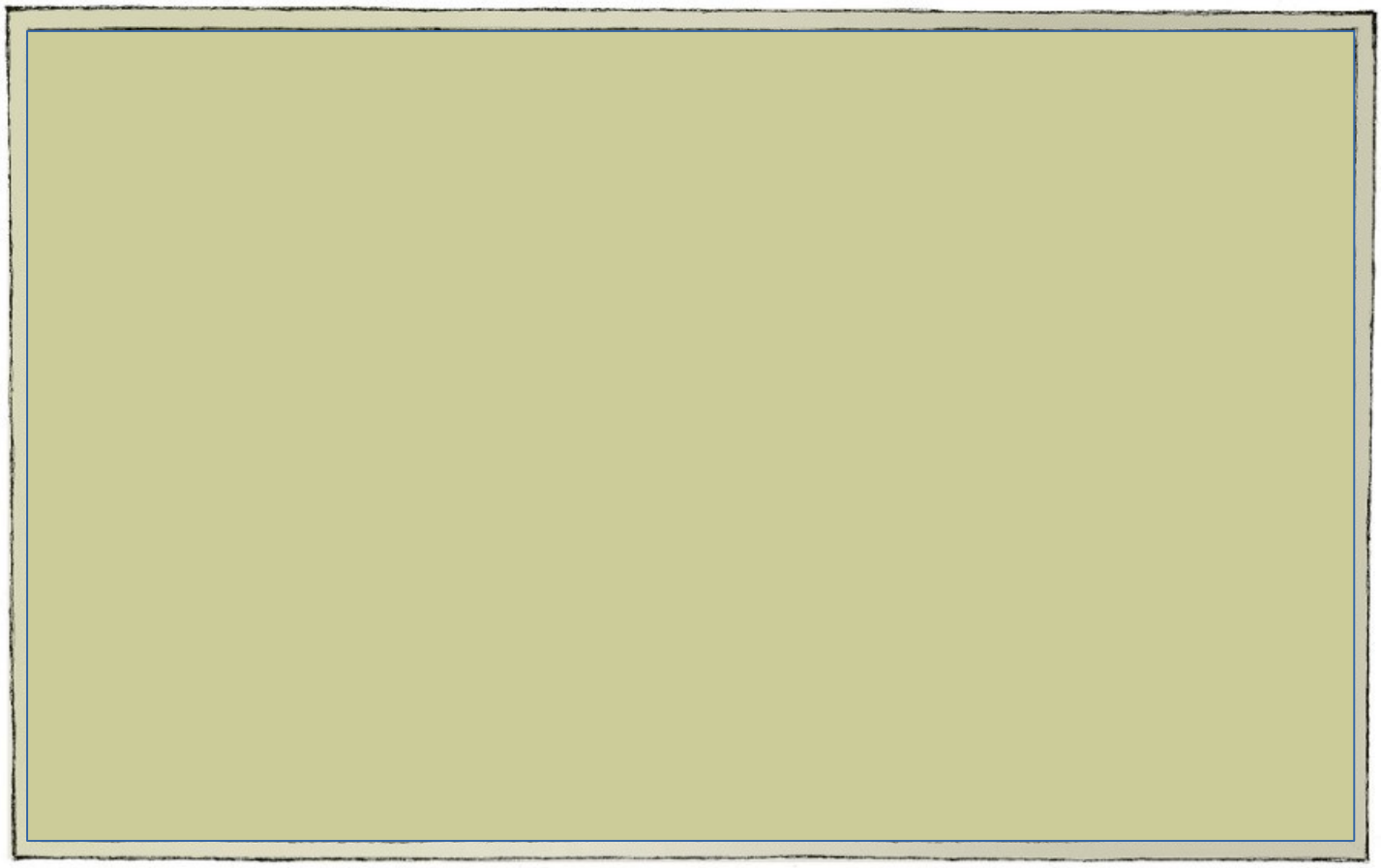
$$\psi$$

Si dos historias son compatibles, se suman

$$\psi_0 + \psi_1$$

Gato de Schrödinger

Schrödinger cat



Schrödinger cat

$$\Psi = \Psi_{vivo} + \Psi_{muerto}$$

QUBITS

Podemos crear qubits

Cualquier sistema de dos niveles proporciona un qubit

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

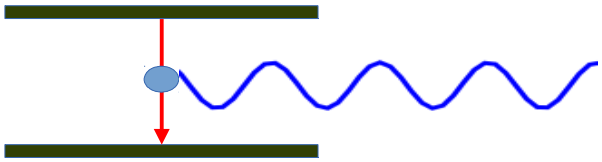
Átomos, fotones, corrientes superconductoras

¡Ya hemos usado 1 qubit!

GPS

Caesium ^{133}Cs

1 sec = 9 192 631 770 Hz



Reloj ultrapreciso, 1 parte en 10^{13}

Superposición exponencial

Ej: 3 qubits, 8 superposiciones

$$|\psi\rangle = |000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle$$

n qubits, 2^n superposiciones: ganancia exponencial

Procesamiento

$$|\psi\rangle = \underbrace{|000\rangle}_{0} + \underbrace{|010\rangle}_{2} + \underbrace{|110\rangle}_{6}$$

$$U_{+1}|\psi\rangle = U_{+1}|000\rangle + U_{+1}|010\rangle + U_{+1}|110\rangle$$

$$= \underbrace{|001\rangle}_{1} + \underbrace{|011\rangle}_{3} + \underbrace{|111\rangle}_{7}$$

¡¡ Computo en paralelo !!

Medida del resultado

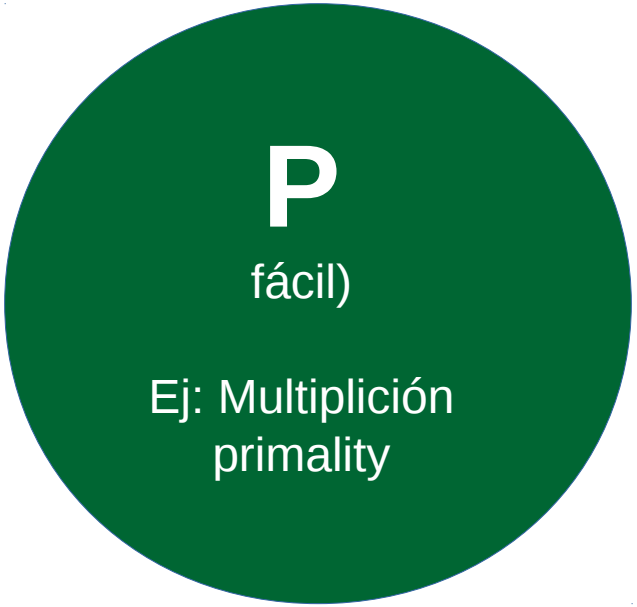
$$\psi = \alpha \left|001\right\rangle + \beta \left|011\right\rangle + \gamma \left|111\right\rangle$$

$$Prob\left(011\right) = \left|\beta^2\right|$$

Son necesarios algoritmos que lleven al estado
hacia una superposición fuertemente pesada en la solución

NO TRIVIAL

complejidad computacional
ordenadores clásicos



complejidad computacional
ordenadores cuánticos

Factorización

Ordenador clásico

$$e^{ct\, n^{1/3} (\log n)^{2/3}}$$

Ordenador cuántico

$$n^2 (\log n)(\log(\log n))$$

El algoritmo de Shor is exponencialmente más rápido

¿Qué ha cambiado ahora?

- Sistemas cuánticos bajo control
  - niveles atómicos en trampas de iones
  - polarizaciones de fotones
  - gases ultrafríos
  - corrientes superconductoras (DWAVE2)
- Manipulación
  - láseres
  - cavidades electromagnéticas
  - bajas temperaturas
- Decoherencia
  - control del entorno + algoritmos de corrección

ORDENADOR CUÁNTICO

=

CATÁSTROFE PARA LA CRIPTOGRAFÍA RSA

Status

- D-Wave2 (Google) es *a quantum annealing machine*
  No es un ordenador cuántico completo
  Resuelve problemas de **optimizatción** **10^8 más rápido** que un ordenador clásico

- Innsbruck ha producido una transformada de Fourier Cuántica de 5 qubits

- *Quantum error correction* evoluciona rápidamente

Please, no overselling

- Principios cuánticos controlados
- *Proofs of concept* ya realizadas
- Inversión internacional importante
- Competición geo-política(!!!!!)

- No es obvio cómo *escalar* los sistemas controlados
- No está claro qué tecnología será la mejor
- Los problemas con ganancia exponencial son limitados

- **Las apuestas políticas son muy alta**

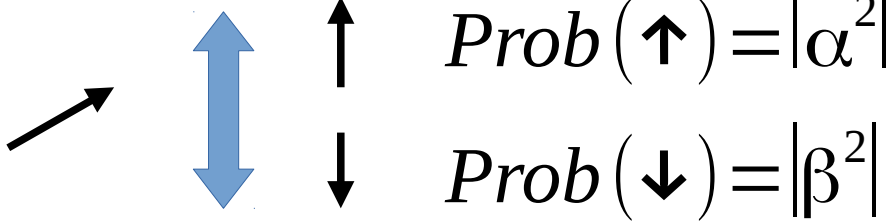
Criptografía cuántica

Principio cuántico

- Al medir, modificamos el objeto medido

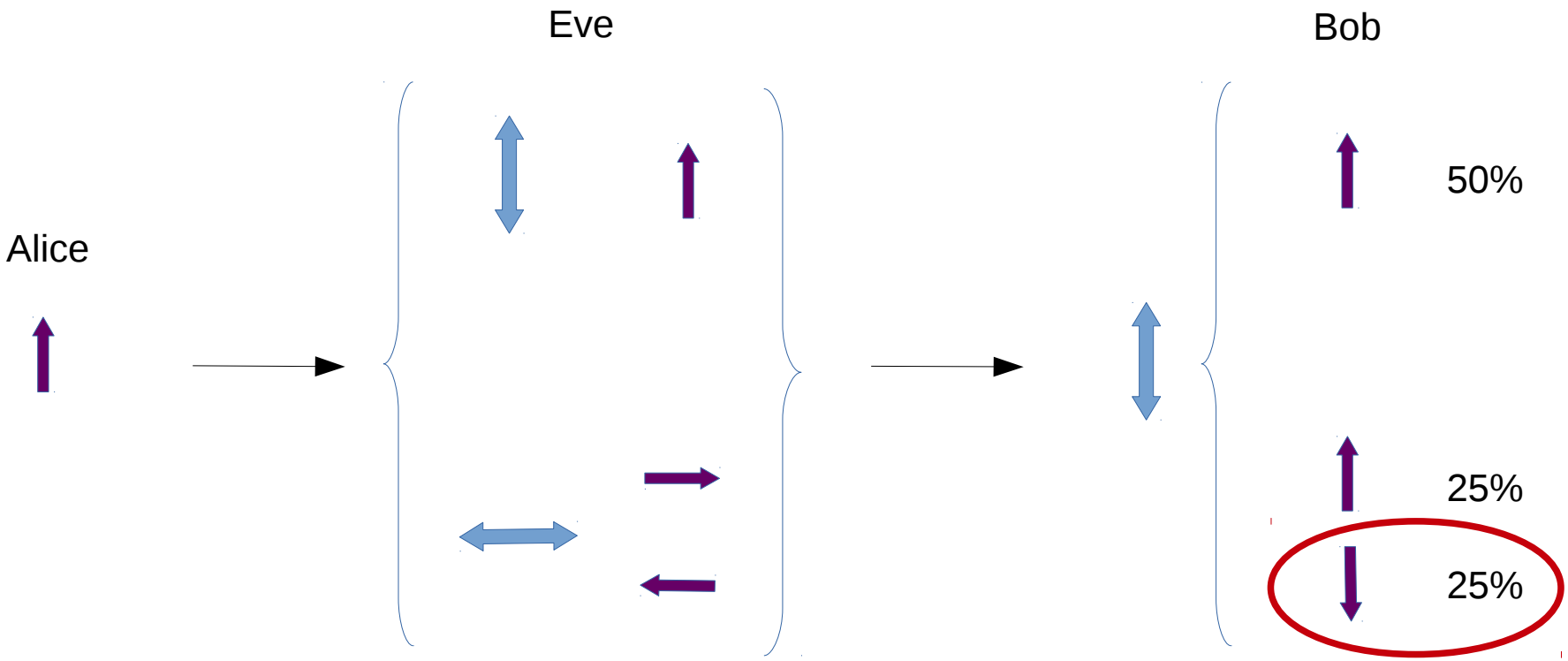
  (Principio de incertidumbre de Heisenberg)

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$



Si codificamos un mensaje en estados cuánticos,
podremos detectar si alguien lo ha leído!!!!!

Detectando a Eve



Seguridad certificada

- Eva siempre es dectectable
- Protocolos *device-independent (!!!)*

  Certificación de cajas negras
- El mensaje es seguro frente a ataques meta-cuánticos

- Nueva idea: criptografia post-quantum

Números aleatorios certificados

- El azar clásico no es certificable
- El azar cuántico de un qubit no es certificable
- El azar generado por sistemas de 2 qubits es certificable!!!!

- Existen implementaciones reales

Conclusión

Criptografía práctica viable

Sensores ultraprecisos en marcha

Simulación cuántica: medio-largo plazo

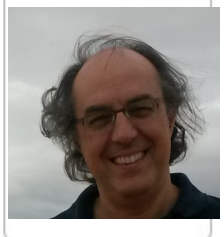
Computación cuántica: largo plazo

La verdadera pregunta no es **cuándo** llegará la nueva era cuántica

La pregunta es **quién** llegará primero

¿Estamos preparados para un futuro cuántico?

Detalls Contacte



Universitat de Barcelona

Nom del ponent

José Ignacio LATORRE

Adreça Correu

j.i.latorre@gmail.com

Telèfon Contacte

600530315

Twitter

@j_i_latorre