

La (muy reciente) historia de la computación cuántica

A través de sus protagonistas

Una breve introducción a la computación cuántica

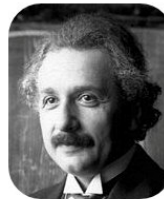


[Quantum computation with PhD comics](#)

Los inicios

Los orígenes

- 1935. Einstein, Podolsky y Rosen observan que la mecánica cuántica predice la existencia de aleatoriedad intrínseca. (Dios no juega a los dados!)



A. Einstein



B. Podolsky

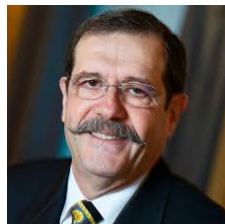


N. Rosen

- 1960 J. Bell propone un primer experimento (ideal) para observar ese efecto. Desigualdad de Bell.



- 1982. Alain Aspect (y otros) hacen el primer experimento en esta línea.



Los orígenes

Simulating Physics with Computers

Richard P. Feynman

Department of Physics, California Institute of Technology, Pasadena, California 91107

Received May 7, 1981



4. QUANTUM COMPUTERS—UNIVERSAL QUANTUM SIMULATORS

The first branch, one you might call a side-remark, is, Can you do it with a new kind of computer—a quantum computer? (I'll come back to the other branch in a moment.) Now it turns out, as far as I can tell, that you can simulate this with a quantum system, with quantum computer elements. It's not a Turing machine, but a machine of a different kind. If we disregard the continuity of space and make it discrete, and so on, as an approximation (the same way as we allowed ourselves in the classical case), it does seem to

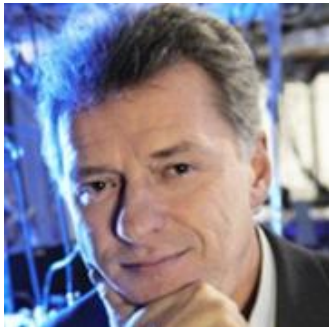
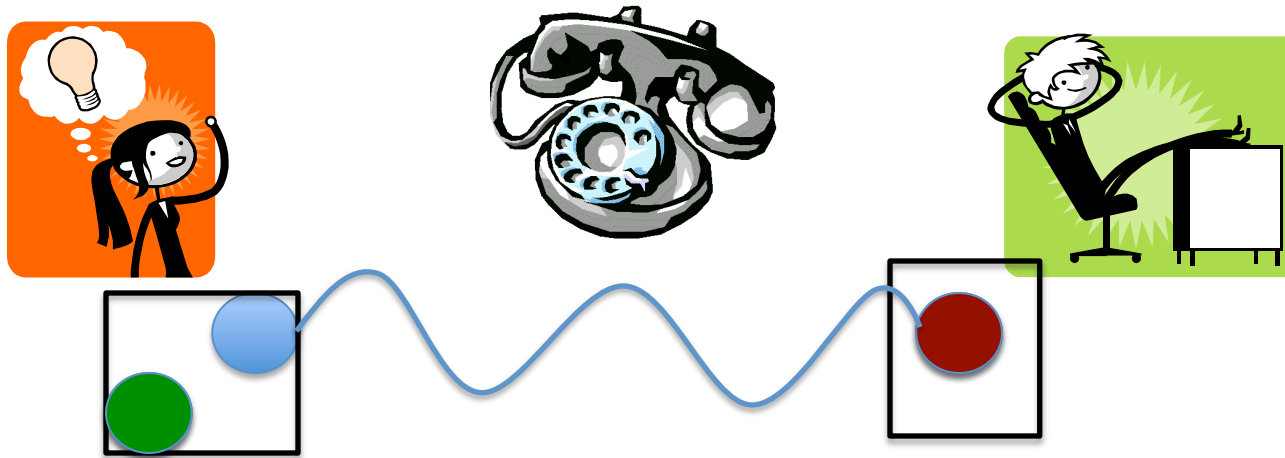
Los pioneros: Bennet y Brassard



1983. Protocolo de teleportación (y experimento asociado)

1984. Primera propuesta de criptografía cuántica (BB84)

La teleportación



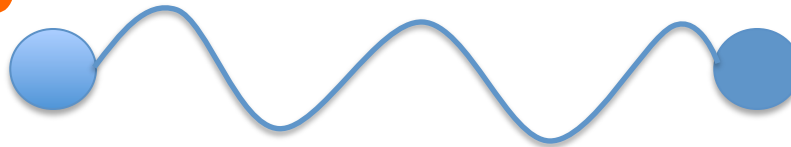
Eugene Polzik



Anton Zeilinger



Intercambio seguro de clave



010001110010010010



010001110010010010

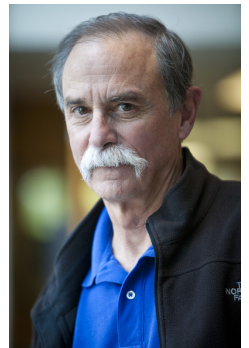
El boom. Los primeros 90.

1993. Formalización del ordenador cuántico: Máquina cuántica de Turing.



1994. Algoritmo de Shor. Un ordenador cuántico rompería la criptografía de clave pública (Premio Nevanlinna 1998).

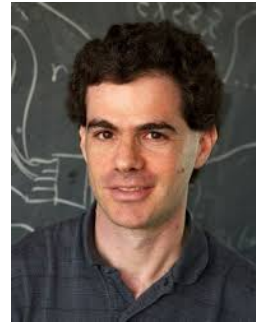
1995. Primera propuesta experimental de un ordenador cuántico utilizando iones atrapados. (Premio Nobel 2012. Premio Wolf 2013)



El desarrollo 1996-2013

El problema de los errores

1996. Computación cuántica tolerante a fallos. ¡Es posible!



Pero requiere hacer cada puerta cuántica con error menor que 10^{-5}

1999. Computación cuántica topológica



(Fundamental Physics Prize 2012)

[Quantum computation with PhD comics](#)



Esto ha permitido subir el error a 10^{-3}

Criptografía cuántica con seguridad demostrable

Demostración de seguridad de BB84

1999. Primera demostración. Lo-Chau-Mayers-Shor-Preskill.



2005. Demostración completa (sin hipótesis extra). Renato Renner.



Criptografía device-independent

1991. Artur Ekert sugiere utilizar desigualdades de Bell en criptografía.



2005. Barrett, Hardy y Kent sugieren la posibilidad de conseguir criptografía **device independent** con seguridad demostrable utilizando desigualdades de Bell.



Criptografía device-independent

2012. Vidick y Vazirani dan la primera demostración de seguridad.



2015. Primer experimento con la precisión necesaria para garantizar la seguridad. Grupo de Ronald Hanson (Delft).



Simulación cuántica

[TED Talk](#)

Simulación cuántica

1996. Seth Lloyd. Un ordenador cuántico puede simular la evolución de cualquier sistema cuántico.



1998. Propuesta de las redes ópticas de átomos ultrafríos para simular sistemas físicos complejos.



Simulación cuántica

2005. Algoritmo de simulación cuántica de química molecular. Grupo de Alán Aspuru-Guzik.



2011. Algoritmo de simulación cuántica de física de altas energías. Jordan-Lee-Preskill



Simulación cuántica

2015. Primer experimento en que la simulación cuántica mejora a la clásica: Many-body localization. Grupo de Immanuel Bloch.



La carrera hacia las tecnologías cuánticas 2013-2017

Tecnologías cuánticas hasta 2013

Pequeñas empresas o pequeños grupos en grandes empresas.



Tecnologías cuánticas hasta 2013

Y primera aplicación comercial: generador de números aleatorios.



USB



Y una aplicación ciertamente útil

The New York Times
Expect the World®

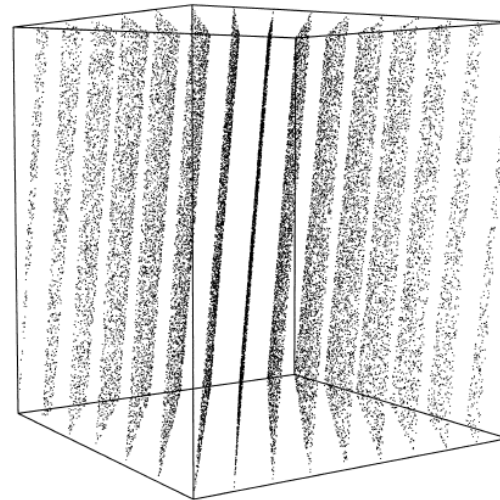
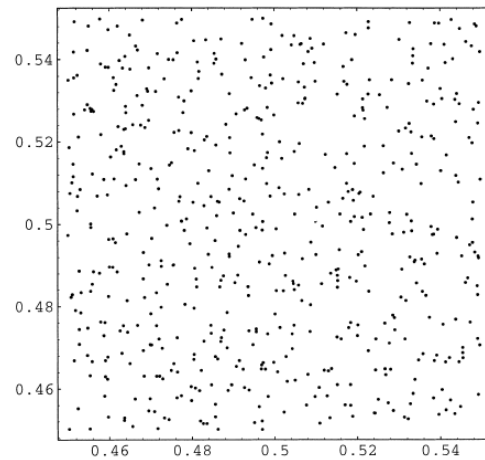
(September 2013) But internal memos leaked by a former N.S.A. contractor, Edward Snowden, suggest that the N.S.A. generated one of the random number generators used in a 2006 N.I.S.T. Standard - called the Dual_EC-DRBG standard – which contains a back door for the N.S.A.

Fuente de buena
parte de los fallos de
seguridad





Ejemplo: RANDU



PROBLEMA: La física clásica NO es aleatoria

2013

2013. Google entra en escena



Su objetivo. Usar el ordenador cuántico para AI.

2013. El gobierno de EEUU le sigue



200 millones de dólares a las principales universidades y centros de investigación.

2015. Intel también



50 millones de financiación iniciales para construir un ordenador cuántico en Delft

2016. Microsoft se une a la carrera



Contrata a Charles Marcus y a Leo Kouwenhoven

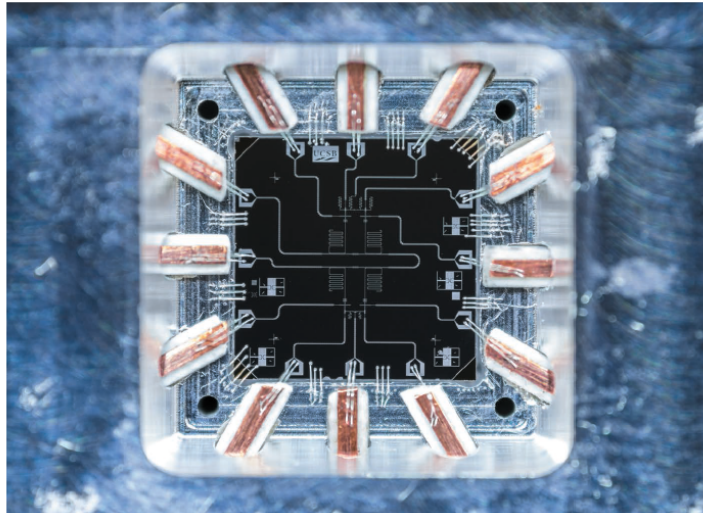
2017. IBM también



Nota de prensa. 6 de marzo de 2017. IBM prepara la construcción del primer ordenador cuántico universal para negocio y ciencia

[Anuncio](#)

2018. Europa invertirá 1 billón de euro en quantum technologies



A €1-billion (US\$1.1-billion) European flagship project could advance the state of quantum computing.

FUNDING

Billion-euro boost for quantum tech

¿Será este esfuerzo colectivo
suficiente para construir un
ordenador cuántico?

¡Esperemos que sí!