Los desafíos de la información cuántica

Jorge Franganillo
Facultad de Información y Medios Audiovisuales
Universidad de Barcelona
franganillo@ub.edu
https://franganillo.es

Resumen: La física cuántica, la ciencia de lo infinitamente pequeño, es tan chocante y misteriosa que suena a ciencia ficción por cuanto desafía al sentido común y obliga a un cambio radical en la manera de percibir la realidad. Los resultados de sus experimentos son irrebatibles y revolucionan incluso el mundo de la información. Los científicos estudian cómo usar las leyes fundamentales de la física cuántica para mejorar la transmisión y el procesamiento de información. Este propósito promete nuevas y fascinantes tecnologías para el futuro, pero no está libre de dificultades y limitaciones, ni permite pensar que el ordenador cuántico sustituirá al ordenador eléctrico convencional.

Palabras clave: teoría de la información cuántica, informática cuántica, criptografía

Title: *The grand challenges of quantum information*

Abstract: Quantum physics, the science of the infinitely small, is so surprising and mysterious that sounds like science fiction since it certainly defies common sense and forces us to radically change the way we perceive reality. The results of its experiments are irrefutable; they are revolutionizing even the information world. Now scientists are studying how to use fundamental laws of quantum physics to improve information transmission and processing, which promises exciting new technologies in the future. Yet, it is not without its difficulties and limitations, nor it suggests that quantum computers might replace conventional electric computers.

Keywords: quantum information theory, quantum computing, cryptography

1. Introducción

Hace poco más de un siglo, el descubrimiento de la mecánica cuántica supuso una transformación sin precedentes en nuestra manera de entender el mundo físico, que procede de la mecánica clásica de Isaac Newton. La física newtoniana se basa en observaciones de objetos cotidianos que dieron lugar a leyes que a su vez fueron probadas y difundidas desde entonces. Pero a finales del siglo XIX, los físicos comenzaron a diseñar instrumentos que les permitían investigar la materia diminuta, y descubrieron que la física de Newton no se podía

aplicar en el nuevo mundo de lo infinitamente pequeño. Lo que estaba establecido como procesos claros, determinados e inmutables resultó tener, en sus raíces subatómicas, un comportamiento turbio y caprichoso, y de esta manera la ciencia necesitó construir un modelo nuevo para explicar el mundo de lo diminuto: la física cuántica.

La física cuántica no reemplaza a la física newtoniana, que explica los objetos macroscópicos, sino que la complementa por cuanto llega adonde la física clásica no llega: el mundo subatómico. Esto resulta tan revolucionario que los grandes descubrimientos de la relatividad especial y general pueden parecer a su lado como unas simples variaciones sobre cuestiones clásicas. Albert Einstein, el padre de la teoría de la relatividad, detestaba los aspectos aleatorios y «fantasmagóricos» de la mecánica cuántica, y los rechazó durante toda su vida, pero aceptaba que falla la física newtoniana cuando un fenómeno se aleja de la experiencia cotidiana, un extremo que unos años antes ya había descubierto Max Planck, el padre de la física cuántica.

La teoría cuántica es sin duda uno de los logros intelectuales más destacados del siglo XX porque revoluciona por completo nuestra comprensión de los procesos físicos, y hoy está demostrando sus frutos tras décadas de lentos pero firmes pasos. Actualmente se aplica con éxito en la cosmología: los quarks y los gluones son firmes candidatos a constituir las partículas elementales. La comunidad física domina las fórmulas, pero no se puede decir que comprenda del todo la teoría. En efecto, hay importantes cuestiones interpretativas que siguen sin resolverse, tal vez porque resolverlas exige no sólo una visión física, sino también decisiones metafísicas (Polkinghorne, 2002).

La física cuántica revela hechos insólitos que provocan perplejidad, suenan a ciencia ficción. En efecto, los objetos microscópicos tienen propiedades físicas que contravienen nuestra experiencia cotidiana. Son ejemplos de ello la superposición cuántica: una partícula puede estar en muchos lugares a la vez. Y el entrelazamiento cuántico: el estado cuántico de dos átomos hace que estén mutuamente correlacionados, de tal modo que lo que le ocurre a uno le afecta al otro, aun cuando los átomos estén separados, incluso en diferentes hemisferios de la Tierra. Queda visto que al micromundo no lo gobiernan las leyes newtonianas, con las que estamos familiarizados, sino un conjunto de leyes diferente: las leyes cuánticas (Dirac, 1981).

Pero disfrutar de las ideas cuánticas no debería ser un patrimonio exclusivo de los físicos teóricos. Aunque la plena articulación de la teoría requiere recurrir a un sofisticado andamiaje matemático, muchos de sus conceptos básicos son accesibles para quienquiera que esté interesado en la historia de estos notables descubrimientos. Puede ser que a los profesionales de la información nos parezca una ciencia remota, ajena a nuestro común interés, pero es evidente que nos afecta, y cada vez más de cerca, porque los científicos están estudiando cómo usar las leyes fundamentales de la física cuántica para mejorar la transmisión y el procesamiento de información, un propósito que promete nuevas y apasionantes tecnologías en el futuro, aunque no está libre de dificultades y limitaciones.

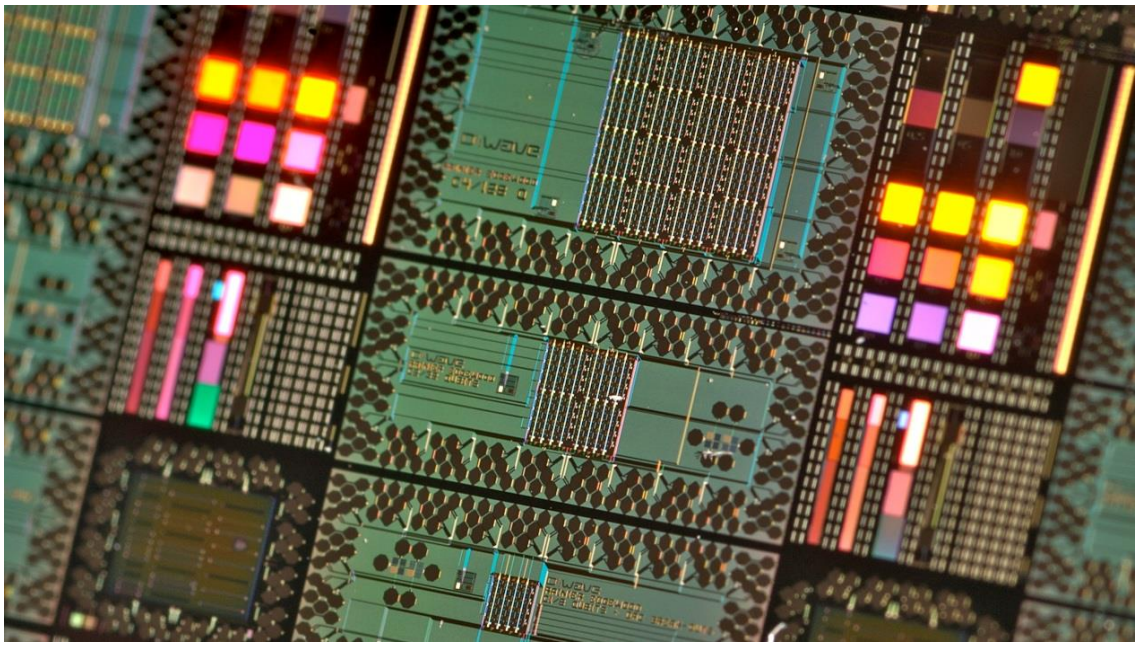

Figura 1. Lámina y procesadores para el temple cuántico — © D-Wave Systems

2. Limitaciones físicas de la información clásica

La ciencia de la información cuántica nace, durante las dos últimas décadas del siglo XX, de la intersección de la física, las matemáticas y la informática. Actualmente, el procesamiento de la información cuántica es una aplicación de la física cuántica que representa un enfoque revolucionario para el tratamiento de la información.

Ya sea clásica o cuántica, la información es física. Por lo tanto, nos conviene entender los procesos físicos que afectan el estado de los sistemas que transportan información. Los procesos físicos para el

almacenamiento, la transformación y la transmisión de información clásica se rigen por las leyes de la física clásica, pero estas leyes limitan la capacidad de aumentar la velocidad y la densidad de los circuitos clásicos. El principal problema es que los dispositivos generan calor en una magnitud mayor que la capacidad física de disiparlo (Marinescu y Marinescu, 2012). Esta limitación ha sido la motivación principal para buscar una manera alternativa de construir mecanismos informáticos que superen las dificultades. Y aquí la mecánica cuántica puede ser la solución: la informática cuántica es hoy un camino prometedor.

3. Características de la información cuántica

La información cuántica es información almacenada como propiedad de un sistema cuántico (por ejemplo, la polarización de un fotón o el espín de un electrón) y se puede almacenar, transmitir y procesar según las leyes de la mecánica cuántica.

La comunicación cuántica implica:

— Una fuente suministradora de sistemas cuánticos en un estado determinado; podría ser un láser de fotones monocromáticos o una trampa de iones.
— Un canal (ruidoso) que «transporta» el sistema cuántico; podría ser una fibra óptica o un conjunto de iones atrapados.
— El destinatario que recibe y decodifica la información cuántica; el receptor podría ser una célula fotoeléctrica o un fotodetector de fluorescencia inducida por láser (Lloyd, 1997).

A su vez, la información cuántica tiene cuatro propiedades especiales:

— El estado de un sistema cuántico no puede medirse o copiarse sin perturbarlo.
— Pueden entrelazarse los estados cuánticos de dos sistemas.
— En el conjunto de dos sistemas con un estado definido, ninguno de los sistemas individuales tiene un estado propio.
— Ciertos estados de un sistema cuántico (los denominados «no ortogonales») son imposibles de distinguir.

En referencia a la primera propiedad, Bennet (2004) apunta una metáfora: «La información cuántica es como la información en un sueño: al intentar describirle un sueño a otra persona, el interlocutor cambia el recuerdo de lo soñado, y entonces comienza a olvidar el sueño, y acaba recordando sólo lo que ha dicho sobre él».

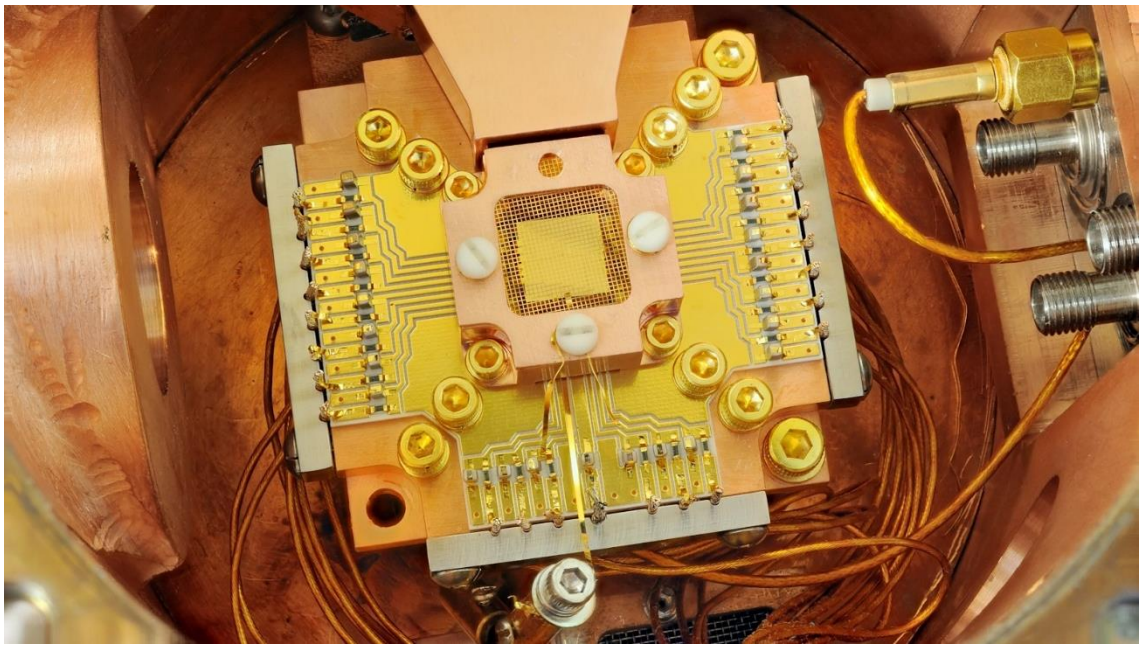

Figura 2. Trampa de iones, en un ordenador cuántico — © National Standards Institute

4. Algunos problemas

En física cuántica, muchas propiedades observables no tienen valores definidos, con lo que la mejor descripción del estado de un sistema no es un valor concreto, sino un catálogo de las probabilidades de obtener determinados valores inciertos (Cabello, 2007). Esto se debe a que en física cuántica el observador no está aislado del universo mecánico, sino que influye en el objeto observado. Dado que cualquier observación es una interacción entre un sistema clásico y uno cuántico, las propiedades cuánticas de las partículas son extremadamente frágiles. Por lo tanto, es imposible predecir con certeza el comportamiento de un sistema cuántico ante una operación determinada.

El fenómeno del entrelazamiento de partículas es una de las claves para desarrollar ordenadores cuánticos que sean más veloces que los actuales. Actualmente se están invirtiendo importantes sumas de dinero en investigar la viabilidad de la informática cuántica. De hecho, ya se han construido algunos ordenadores cuánticos, pero aún no son lo bastante sofisticados y, por lo tanto, funcionan como meros conceptos teóricos (Piper y Murphy, 2002).

Si la informática cuántica se hace realidad más allá de lo experimental, la situación cambiará radicalmente. Entrelazando cúbits (bits cuánticos) individuales, un ordenador cuántico podría resolver problemas con más rapidez que uno de memoria digital magnética.

Pero el entrelazamiento se complica cuando se manejan más de dos partículas, y así, la misma propiedad que inspira el desarrollo de la informática cuántica, al mismo tiempo la limita.

La interacción con el entorno causa además un problema importante en el procesamiento de información cuántica: la decoherencia. Esta propiedad provoca en las partículas un comportamiento que muestra coherencia matemática, pero incoherencia lógica. Y muchos principios de la física cuántica son implícitamente decoherentes. Por ser ilógicos, ni siquiera los científicos más eminentes han podido comprender el comportamiento de los principios decoherentes, que tienen serios problemas de formulación e interpretación en el plano filosófico, cuya base es la lógica. Pero igualmente han sido aceptados, incluso sin ser entendidos, porque sirven de base para explicar ciertos fenómenos cuánticos.

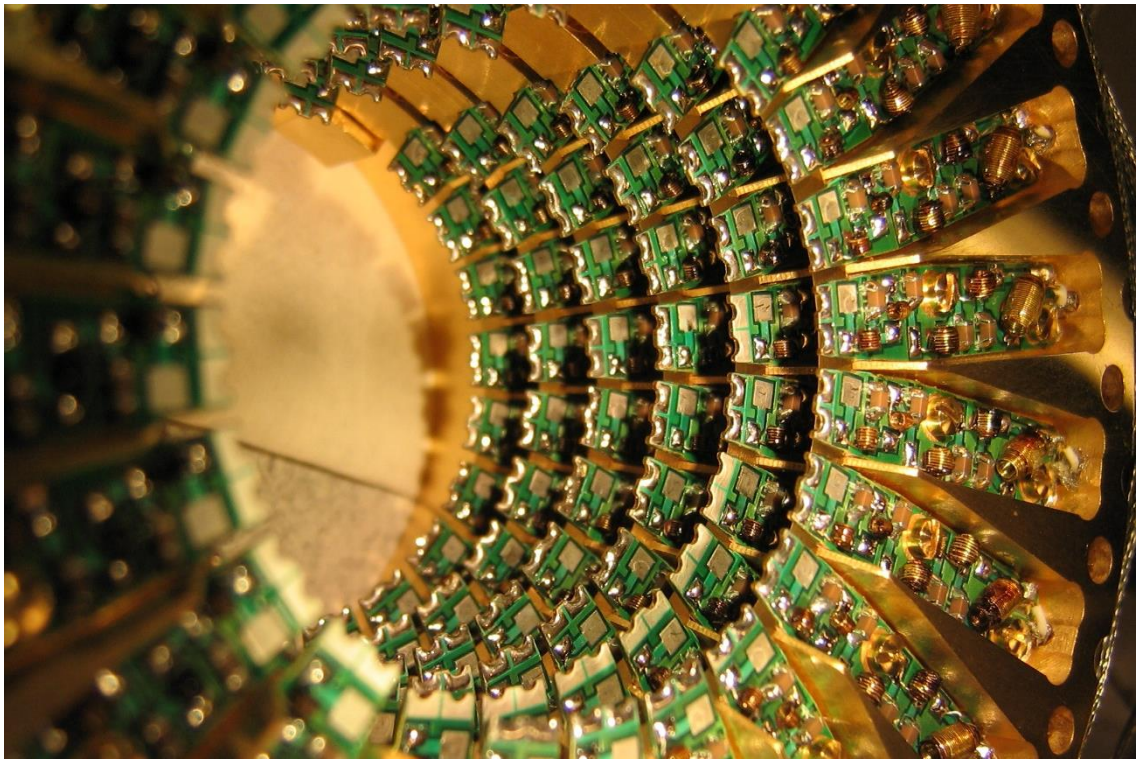

Figura 3. Filtro de elementos concentrados, en un ordenador cuántico — © D-Wave Systems

5. Informática y criptografía

Para la criptografía, la información cuántica tiene ciertas propiedades destacables: los cúbits permiten ejecutar cálculos exponenciales con una rapidez muy superior a la de los ordenadores eléctricos convencionales. Así, en principio, un ordenador cuántico podría resolver rompecabezas

que la informática actual no puede resolver con eficacia. La teoría cuántica de la información también permite diseñar algoritmos para la distribución de claves cuánticas y para la teleportación cuántica. Y es fácil detectar la escucha ilegítima de un canal de comunicación cuántico.

Considerando que el canal cuántico es ruidoso, la comunicación sólo puede ser fiable mediante un sistema de corrección de errores. El inconveniente es que la complejidad de los circuitos implicados en la corrección de errores va mucho más allá de las posibilidades tecnológicas de hoy en día. Para que la informática cuántica sea tolerante con los errores aún faltan años de investigación, pero esto es posible, y de hecho ya existen buenos códigos de corrección de errores cuánticos (Marinescu y Marinescu, 2012). Estos desarrollos teóricos van acompañados de adelantos en la comunicación cuántica. Prueba de ello es que de la criptografía cuántica se ha comercializado ya una aplicación: la distribución cuántica de claves (Ouellette, 2004).

La criptografía cuántica consiste en usar fenómenos cuánticos para cifrar información o para romper sistemas criptográficos. Así, permite intercambiar una clave de manera segura y, al menos hipotéticamente, podría vulnerar esquemas de cifrado de clave pública como RSA o *ElGamal*. La ventaja principal de la criptografía cuántica es que permite ejecutar ciertas tareas que se consideran irrealizables mediante la comunicación clásica. Un ejemplo de ello es que cualquier intento de espiar la distribución de una clave cuántica perturba el contenido del mensaje, y el receptor podrá saber que alguien ha tratado de leerlo.

6. Entusiasmo y prudencia

El avance de la tecnología del siglo XX obliga a considerar la creación y la gestión de información como una disciplina científica. En este contexto, la miniaturización de la electrónica permitió fabricar ordenadores cada vez más pequeños y eficientes, pero esto tiene límites, y pronto dejará de obedecer a la ley de Moore, según ha insistido el propio Moore (Gardiner, 2007). Aun así, muchos investigadores son sensibles a la posibilidad de construir un ordenador tan pequeño que controle las propiedades cuánticas de los sistemas físicos como la luz, los átomos y las moléculas (Rosas-Ortiz, 2008). Al fin y al cabo, en el

desarrollo de la informática y la telemática modernas, la mecánica cuántica ha estado siempre presente.

Salvando la extraordinaria complejidad de manipular más de dos partículas entrelazadas, Thomas Monz y un grupo de investigación dirigido por Rainer Blatt experimentan desde 2005 con varias partículas entrelazadas. Y ya han superado su propio récord de entrelazamiento de cúbits: en abril de 2011 superaron el límite de 8 cúbits y lograron producir un registro cuántico de 14 cúbits al confinar 14 átomos de calcio dirigiéndolos con haces de láser en una trampa de iones (Monz et al., 2011). De esta manera constituyen una base posible para un ordenador cuántico de uso comercial.

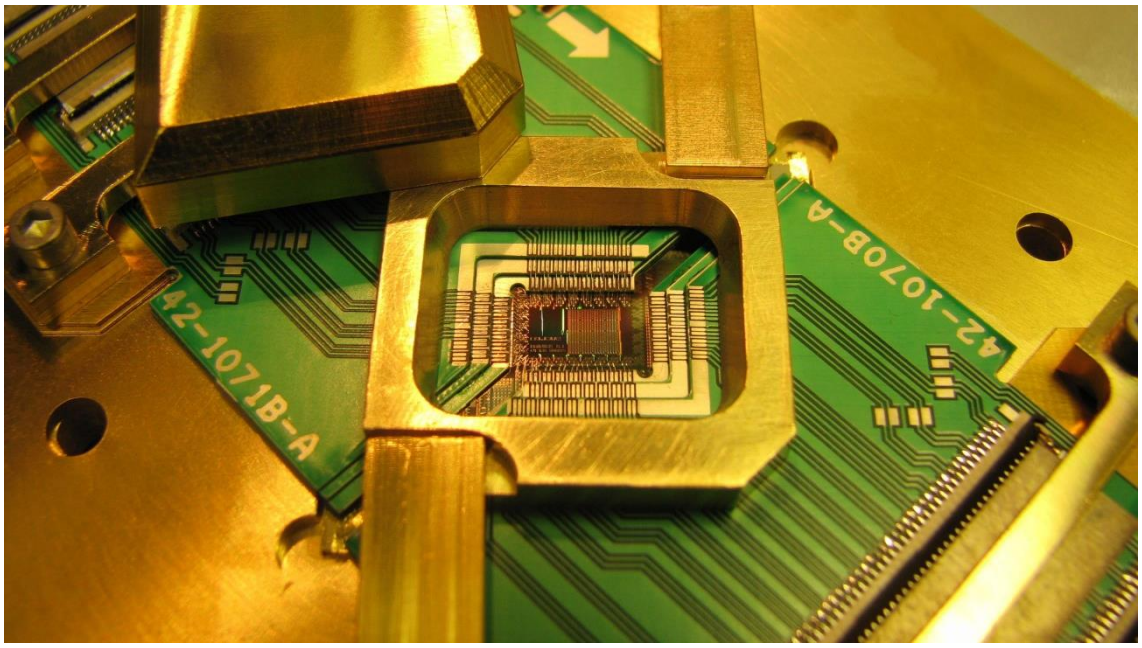

Figura 4. Procesador Rainier de 128 cúbits — © D-Wave Systems

El ordenador cuántico abrirá unas posibilidades de procesamiento que hoy son imposibles de llevar a cabo en un ordenador convencional. Pero esta afirmación, según matiza Aronson (2008), se refiere sólo al tiempo de cálculo de ciertos algoritmos. En otros aspectos, los ordenadores cuánticos apenas proporcionarían una cierta mejora, poco perceptible, frente a los ordenadores actuales. Existen pruebas de que los futuros ordenadores se enfrentarán a muchas de las limitaciones de sus homólogos convencionales.

En esto que parecía la historia de una máquina milagrosa, capaz de hacer malabarismos con valores infinitos, parece como si los científicos hubieran olvidado explicarnos que el ordenador cuántico

no va a sustituir el ordenador personal que está sobre nuestra mesa de trabajo. A los cúbits no los veremos a cargo de la informática doméstica. Y no es que los físicos, expertos en superar obstáculos tecnológicos, no hayan sabido domesticarlos: es simplemente que el ordenador cuántico, aun cuando se haya sofisticado lo bastante, permanecerá limitado a unas pocas aplicaciones especializadas.

En efecto, el extraño comportamiento de los cúbits requiere programas informáticos dedicados y una arquitectura particular para resolver, en definitiva, sólo un tipo de cálculo: los problemas combinatorios. Si el ordenador cuántico estuviese generalizado en la actualidad, sería incapaz de realizar dos tareas distintas como, por ejemplo, buscar información en una base de datos y descomponer un número en factores primos (Fontez, 2012). Y aunque un ordenador cuántico puede manejar otros algoritmos, no son la clase de algoritmos que resultarían útiles para nuestra vida diaria. A falta de algoritmos dedicados, la singularidad de los cúbits condena al ordenador cuántico a convertirse en una máquina tan «lenta» como un ordenador convencional, o quizá más.

Bibliografía

Aronson, Scott (2008). «The limits of quantum computers». *Scientific american*, febrero, v. 293, n. 3, p. 50. https://scientificamerican.com/article/the-limits-of-quantum-computers

Bennet, Charles (2004). «Quantum information processing». *Computer Science: Reflections on the Field, Reflections from the Field*. Washington, DC: National Academies Press, pp. 51–56.

Cabello, Adán (2007). «Introducción [a un número especial sobre información cuántica]». *Revista española de física*, abril-junio, v. 21, n. 2.

Dirac, Paul (1981). *The principles of quantum mechanics*. Oxford, EE.UU.: Oxford University Press.

Fontez, Mathilde (2012). «L'ordinateur quantique n'est pas pour nous». *Science & Vie*, junio, n. 1137, pp. 50.

Gardiner, Bryan (2007). «Gordon Moore predicts end of Moore's Law (again)». *Wired*, 18 septiembre. https://wired.com/business/2007/09/idf-gordon-mo-1

Klimov, Andrei B. (2008). «Información cuántica: ideas y perspectivas». *Cinvestav*, enero-marzo, v. 27, n. 1, pp. 12–17. https://www.fis.cinvestav.mx/~orosas/REVCINV/p12.pdf

Lloyd, S. (1997) «Capacity of a noisy communication channel». *Phys. Rev. A*, n. 55, pp. 1613–1622.

Marinescu, Dan C.; Marinescu, Gabriela M. (2012). *Classical and quantum information*. Amsterdam; Boston: Elsevier.

Monz, Thomas *et al.* (2011). «14-qubit entanglement: creation and coherence». *Physical Review Letters*, abril, v. 106, n. 13, pp. 1–4. https://doi.org/10.1103/PhysRevLett.106.130506

Ouellette, Jenniffer (2004). «Quantum key distribution». *The Industrial Physicist*, diciembre, pp. 22–25.

Piper, Fred C.; Murphy, Sean (2002). *Cryptography: a very short introduction*. Oxford, EE.UU: Oxford University Press.

Polkinghorne, John (2002). *Quantum theory: a very short introduction*. Oxford, EE.UU: Oxford University Press.

Rosas-Ortiz, Óscar (2008). «Presentación [de un número monográfico sobre información cuántica]». *Cinvestav*, enero-marzo, v. 27, n. 1, pp. 2–3. https://www.fis.cinvestav.mx/~orosas/REVCINV/pres.pdf

Cómo citar este artículo

Franganillo, Jorge (2012). «Los desafíos de la información cuántica». *ThinkEPI*, vol. 7. <https://franganillo.es/cuantica.pdf>