ue STEAM essentials

COMPUTACIÓN CUÁNTICA: ¿DE DÓNDE VENIMOS Y HACIA DÓNDE NOS DIRIGIMOS?

VICTOR ILISIE CHIBICI
Escuela de Ciencias, Ingeniería y Diseño
UNIVERSIDAD EUROPEA DE VALENCIA

Este artículo tiene como objetivo presentar de forma sencilla las bases sobre las cuales se sustenta el concepto de ordenador cuántico, así como el presente y el futuro de la computación cuántica. Por tanto, en la primera parte se describen algunos de los conceptos básicos detrás de la mecánica cuántica, tales como la función de onda, medición, colapso de un sistema o estados entrelazados. Junto a esto, también se describen fenómenos recientes que arrojan todavía más misterio sobre la naturaleza de las partículas subatómicas y el rango de validez de la física cuántica. En la segunda parte se describe la posibilidad de desarrollar un ordenador cuántico con una capacidad de cómputo muy superior a cualquier ordenador clásico y sus posibles aplicaciones. También se comentan los retos experimentales con los que nos encontramos hoy en día para su implementación física.

PALABRAS CLAVE •
Computación, mecánica cuántica, criptografía.

CÓMO CITAR ESTE ARTÍCULO •
Ilisie Chibici, Victor. 2022, *"Computación Cuántica: ¿De dónde venimos y hacia dónde nos dirigimos?"* en: UEM STEAM Essentials

INTRODUCCIÓN

"Puedo afirmar sin miedo a equivocarme que nadie entiende la mecánica cuántica". Esta frase se le atribuye al muy conocido físico teórico, Richard Feynman, en el año 1965, el mismo en el que recibiría su premio Nobel por sus descubrimientos en la electrodinámica cuántica. Casi seis décadas más tarde, después de extraordinarios avances tanto teóricos como experimentales y tecnológicos basados en aplicaciones de la física cuántica, la afirmación de Feynman sigue siendo válida.

Pero ¿cómo es posible avanzar sin entender? La sutileza reside en el hecho de que la física cuántica se entiende a nivel *matemático* u *operacional*, pero no conceptualmente. Es más, en los últimos años se han descubierto, tanto a nivel teórico como experimental, resultados que nos hacen cuestionar todavía más, los pilares de lo que consideramos *realidad* [1,2,3], como veremos en la sección "Todavía más misterio".

En conclusión, lo único que podemos hacer por ahora es operar con las matemáticas y hacer predicciones, pero sin terminar de entender los principios fundamentales que hacen que la física cuántica funcione, ¡pero funciona!, y no hace falta saber interpretarla para usarla y crear aplicaciones que seguro van a moldear el futuro de la humanidad.

Gracias a los padres de esta bonita y a la vez misteriosa rama de la física, tales como Max Planck, Werner Heisenberg, Niels Bohr, Erwin Schrödinger y Albert Einstein, entre otros, estamos rodeados de dispositivos cuánticos en nuestro día a día, sin darnos cuenta. Desde los fotodetectores que impiden el cierre de las puertas del ascensor al detectar a una persona, a los transistores presentes en, literalmente, todos los aparatos electrónicos que nos rodean, o los lectores ópticos y la resonancia magnética nuclear con aplicaciones médicas, son ejemplos de las aplicaciones de la física cuántica que han hecho mejorar con-

siderablemente nuestro nivel de vida y nos han permitido avanzar como civilización.

Otra aplicación que está siendo el foco de mucha investigación es la computación cuántica. Aunque todavía nos quede un largo camino hasta que seamos capaces de construir un ordenador cuántico plenamente funcional y al alcance de todo el mundo, los resultados tanto teóricos como experimentales son muy prometedores. Pero, antes de entrar en más detalles, vamos a echar un breve vistazo a los fenómenos físicos que nos han permitido plantearnos, en primer lugar, la posibilidad de construir un ordenador cuántico.

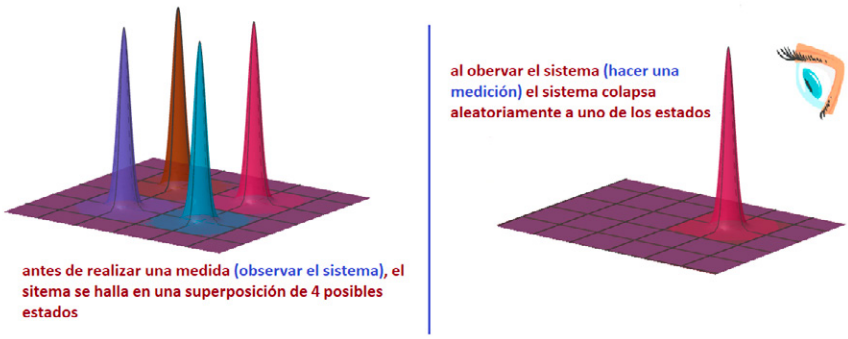


Figura 1 » Representación esquemática del colapso de un sistema cuántico al realizar una medición *(créditos: imagen de creación propia)*

BREVE ESBOZO DE LA FÍSICA CUÁNTICA

A continuación, tratemos de aclarar lo referente a los *misterios* que rodean la física cuántica. Para ello, vamos a exponer brevemente cuáles son las herramientas básicas que se emplean para describir los fenómenos a nivel subatómico. Uno de los axiomas fundamentales es que todo sistema viene descrito en términos de una *función de onda* asociada que contiene toda la información posible del sistema. Esta función se puede escribir como una suma (o superposición) de todos los posibles estados en los que podríamos encontrar dicho sistema al realizar una medición. Ahora bien, al realizar una medición, el sistema **colapsa** a uno de estos posibles estados **(elige uno de los estados)** según cierta distribución de probabilidad dada por la función de onda. A nivel cuántico, el concepto de *"estado"* engloba cualquier propiedad física de un sistema susceptible de ser medida. Los ejemplos más habituales de estados son: la velocidad, posición, energía o como veremos más adelante, el *espín*.

Lo anterior ya debería proporcionarnos los primeros indicios de lo que es la física cuántica. Lo primero que podemos observar es que la teoría es probabilística y no determinista, como lo es, por ejemplo, la física clásica. Para entenderlo mejor, una teoría es determinista cuando, dadas las condiciones iniciales de un sistema en un instante determinado, se puede deducir a través de las ecuaciones físicas correspondientes, su estado en cualquier instante posterior. Esto ocurre, por ejemplo, con las leyes de Newton en la descripción de cómo chocan dos bolas de billar. Sin embargo, esto no ocurre a nivel cuántico. Por tanto, lo único que podemos hacer es asignar una cierta probabilidad de que, después de efectuar una medición, obtengamos un resultado u otro; y hay más, una vez realizada la medida, el estado *colapsa* a uno de estos estados, y cualquier medición posterior dará como resultado ese mismo estado.

Veamos a qué se refiere el *colapso* con un ejemplo muy simplificado. Consideremos un sistema que puede encontrarse en uno de cuatro estados posibles después de realizar una medida, en este caso, de la posición. La mecánica cuántica nos dice que, antes de medir la posición, el sistema se halla en una superposición de los cuatro estados (o posiciones, ¡a la vez!). Esto está representado de forma simplificada en la Figura 1 (izquierda). Una vez realizada la medida, un observador detectará un único estado, de forma aleatoria, de los cuatro posibles (ver Figura 1, derecha), lo que, en términos cuánticos, se conoce como el *colapso* del sistema a uno de sus estados posibles. Si posteriormente el observador vuelve a medir la posición del sistema, lo encontrará en ese mismo estado (observará la misma posición).

¿Qué significa este colapso, qué es la función de onda o, por qué hemos de conformarnos con probabilidades y no con certezas? son algunas de las preguntas a las que todavía nos enfrentamos hoy en día en la comunidad científica. En principio, no sabemos lo que es realmente la función de onda, ya que en sí misma no tiene significado físico. Sin embargo, sabemos que su módulo al cuadrado es proporcional a la probabilidad de obtener un resultado. No sabemos por qué colapsa al hacer una medición y tampoco sabemos por qué la naturaleza, en su escala *más pequeña*, es probabilística. Pero sabemos que absolutamente todos los experimentos realizados hasta ahora respetan las leyes cuánticas.

TODAVÍA MÁS MISTERIO

En los últimos años, ha habido un avance tanto teórico como experimental sobre algunas ideas planteadas por primera vez en 1961 por el físico premio Nobel, Eugene Wigner. Su idea plantea la posibilidad de realizar mediciones cuánticas sobre sistemas mixtos microscópico-macroscópico [1,2,3]. Esto es, deducir si la descripción de un sistema mixto, formado por un subsistema cuántico (la parte microscópica) y un observador (la parte macroscópica) que realiza mediciones sobre dicho subsistema, se podría describir en términos cuánticos por un segundo observador (también

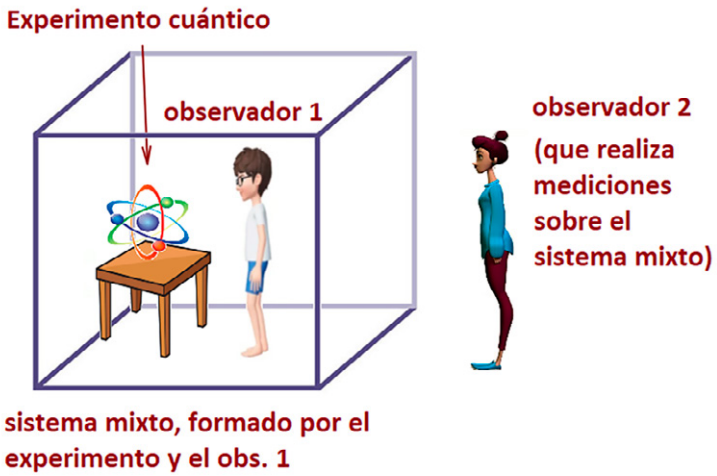


Figura 2 » Descripción gráfica de un sistema formado por un experimento cuántico y el observador 1, que a su vez será descrito por un observador externo, el observador 2 *(crédito:* https://www.bibliocad.com/es/biblioteca/personas-3d_52381/).

macroscópico) de todo el sistema anterior. Para un mejor entendimiento véase la Figura 2.

En uno de los artículos recientes que tratan este tema, publicado en la revista Nature Communications [1], los autores demuestran de forma teórica que las tres afirmaciones siguientes **no** pueden ser, a la vez, válidas:

1 » **universalidad:** la física cuántica se puede aplicar a escalas arbitrariamente grandes, tanto a escala microscópica como a escala macroscópica.

2 » **unicidad del resultado:** un observador, al realizar una medición sobre un sistema cuántico, obtiene un único resultado.

3 » **consistencia:** las mediciones de un observador no deben ser contradictorias con respecto a las de otro observador.

Grosso modo, haciendo las tres suposiciones anteriores y analizando los posibles resultados de las mediciones de los dos observadores, concluiríamos que los dos, en general, no se ponen de acuerdo sobre los resultados de sus mediciones. Con ello, llegaríamos a una contradicción lógica, ya que estaríamos incumpliendo la tercera suposición. La conclusión directa es que al menos alguna de las tres afirmaciones es falsa.

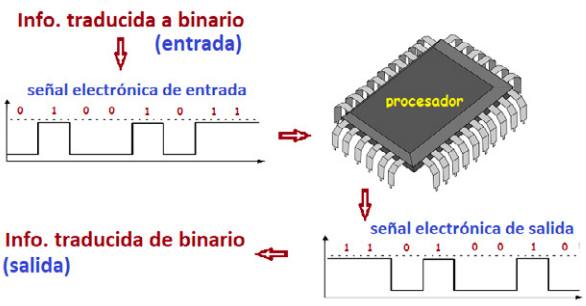
Lo que podría parecer simplemente una curiosidad a nivel teórico, tiene algunas implicaciones experimentales y algunas ya han sido corroboradas [4]. Por tanto, estamos ante un dilema todavía más grande con respecto a la naturaleza de la física cuántica y con respecto a la naturaleza misma. ¿A cuál de las tres suposiciones previas, todas ellas razonables, deberíamos renunciar? Cabría la posibilidad de que, al igual que ocurre con la Relatividad de Einstein, los resultados de las medidas cuánticas sean *relativas* al sistema de referencia o al observador. Sin embargo, no podemos sacar este tipo de conclusiones aún, sin indagar más en estos conceptos tanto a nivel teórico como experimental.

BASES DE LA COMPUTACIÓN CUÁNTICA

Tras la introducción de los conceptos previos, vamos a describir como se pueden usar estas ideas para el desarrollo de un ordenador cuántico. Pero antes, recordemos muy brevemente cómo funciona un ordenador clásico.

Un ordenador clásico, como todos bien sabemos, funciona a nivel fundamental con **bits** de información. Un bit es una unidad básica que puede tomar únicamente dos valores: 0 ó 1. A nivel electrónico, para que el procesador sepa interpretar los bits, se trabaja con señales correspondientes a dos voltajes: el bit 1 corresponde a la presencia de un pulso eléctrico dentro de un rango del voltaje, y el bit 0 corresponde a la ausencia de un pulso eléctrico (o equivalentemente, a un pulso por debajo de cierto umbral) (ver Figura 3). En este esquema hay una limitación importante, y es el hecho de que estamos obligados físicamente a codificar información cada vez más compleja solamente usando dos caracteres. Este aspecto se pudo subsanar gracias a los avances en el campo de la electrónica (procesadores cada vez más rápidos y pequeños) y la ingeniería de sistemas. Esta última ha permitido la distribución en paralelo del procesamiento de la información (procesadores u ordenadores enlazados) lo cual ha aumentado, al menos un orden de magnitud, las capacidades que alcanzarían un único ordenador [5]. Hoy en día, disponemos de aparatos electrónicos, mucho más rápidos que hace dos décadas. Gracias a eso, hemos podido avanzar hacia la 4ª Revolución Industrial, el IoT (Internet of Things) o el Machine Learning y la Inteligencia Artificial, que empiezan a jugar un papel importante en nuestras vidas diarias.

Figura 3 » Esquema del funcionamiento básico de la codificación de información mediante para un ordenador clásico, usando bits (0's y 1's) *(créditos: https://www.needpix.com/photo/23080/)*

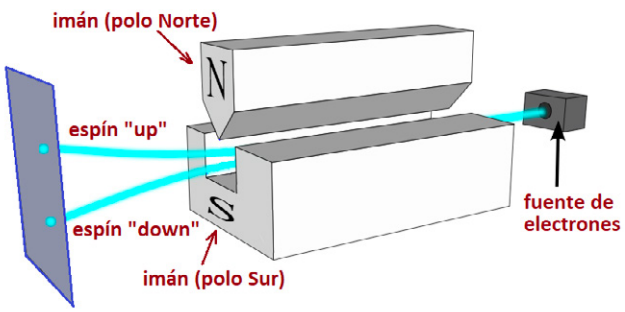


Por analogía, un sistema cuántico opera con **qubits** (quantum bits). La diferencia fundamental con respecto a un sistema clásico es que, mientras un bit clásico puede tomar solamente dos valores, un qubit es una superposición de dos posibles estados, antes de ser medido. Al realizar una medición, colapsará a uno de ellos con cierta probabilidad. De esto podemos concluir que la información que podemos almacenar con un solo qubit es muy pequeña, similar a la de un bit clásico. La diferencia fundamental, sin embargo, estriba en otra propiedad de los sistemas cuánticos, el ***entrelazamiento***. Como veremos a continuación, esta propiedad permitirá transmitir información equivalente a 2^N bits clásicos, únicamente usando N qubits entrelazados, donde N es cualquier número natural mayor que 2.

Un *estado entrelazado* es un estado formado por dos o más partículas, en el que la medición de una propiedad de una de ellas afecta a las propiedades de la otra. Consideremos como ejemplo el espín del electrón. El **espín** (o campo magnético intrínseco) es una propiedad característica de las partículas subatómicas y describe como interactúan estas partículas con un campo magnético externo y que además confieren las propiedades magnéticas de los materiales.

En la Figura 4, se presenta de forma esquemática uno de los experimentos en los que se detectó por primera vez el espín de las partículas subatómicas, el cual también es un ejemplo de "estado" cuántico. En el experimento original se lanzaron átomos de plata, pero el experimento se puede realizar con cualquier partícula. Si lo realizamos con electrones provenientes de una fuente, estos interactúan con el campo magnético inhomogéneo de los imanes, y en función de su espín, curvan su trayectoria y colisionan con la pantalla en la parte de arriba (spin "up") o en la parte de abajo (spin "down"). Este experimento demostró, además, que el spin de una partícula tiene valores discretos, lo cual implica que su naturaleza es cuántica. Esto es debido a que, clásicamente, uno esperaría que el spin tomara un valor continuo entre los dos valores medidos experimentalmente.

Figura 4 » Experimento de Stern-Gerlach, en el cual se lanza un chorro de electrones, desde una fuente situada en la parte derecha, a través del campo magnético producido por dos imanes. El resultado experimental se puede observar en la pantalla (parte izquierda) en la que impactan los electrones *(créditos:* https://en.wikipedia.org/wiki/Stern-Gerlach_experiment*)*



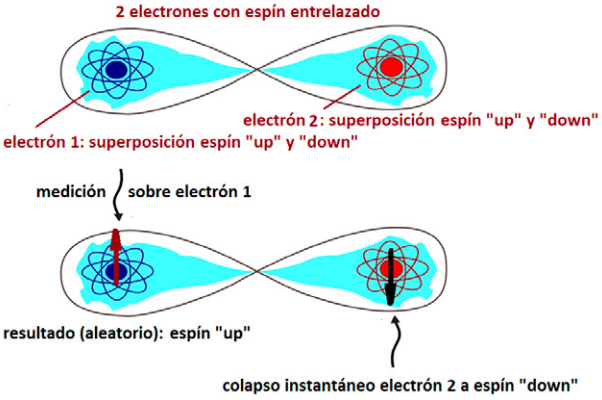
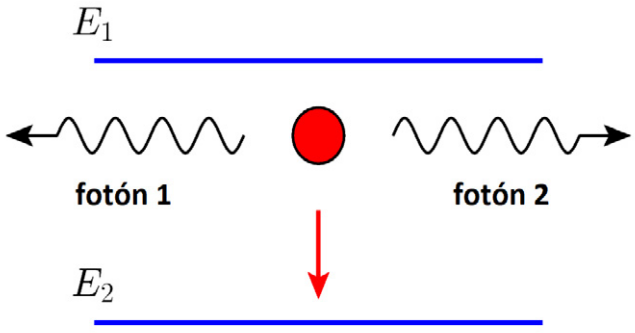


Figura 5 » Representación esquemática del estado entrelazado de dos electrones y su comportamiento al realizar una medida del espín sobre uno de ellos *(créditos:* https://www.researchgate.net/figure/Quantum-entanglement-8_fig1_349451988*)*.

Una vez visto lo que es el espín veamos a qué nos referimos cuando hablamos de *entrelazamiento*. Para entenderlo de forma intuitiva, consideremos una pareja de electrones con espín entrelazado, donde cada uno de ellos (antes de realizar ninguna medida) se halla en una superposición de espín "up" y espín "down". Cuando realizamos una medición del espín sobre uno de los electrones (electrón 1) y obtenemos un resultado aleatorio, por ejemplo "up", un observador puede estar al cien por cien seguro que el otro electrón (electrón 2) ha colapsado a un estado de espín "down" (ver Figura 5). A este colapso, Einstein lo llamo "misteriosa acción a distancia" y, aunque colaboró en su desarrollo, siempre creyó que debía haber una teoría "más completa" que la física cuántica.

El entrelazamiento cuántico, en general, se puede dar para dos o más partículas. Aquí, por simplicidad, se ha presentado el caso más sencillo. Para aclar de qué forma se puede preparar experimentalmente un estado entrelazado de dos partículas, veamos el siguiente ejemplo. Consideremos un supuesto átomo de espín cero que decae de un nivel de energía E_1 a otro inferior E_2, emitiendo dos fotones (ver Figura 6). Debido a que el espín es una propiedad que se conserva (similar a la conservación de energía) la suma de los espines individuales de los fotones debe ser cero. Por tanto, los fotones (que también poseen dos valores posi-

Figura 6 » Un átomo (rojo) que decae de un nivel de energía E1 a otro inferior E2 emitiendo dos fotones *(créditos: imagen de creación propia)*



bles para el espín, al igual que el electrón) estarán entrelazados, es decir, cuando se mida el espín de uno de ellos (por ejemplo, del fotón 1), se obtendrá un resultado aleatorio, y el espín del fotón 2 colapsará al espín contrario, conservando así el espín cero del átomo inicial.

A lo largo de las últimas décadas se han realizado numerosos experimentos y todos y cada uno de ellos han confirmado la existencia del entrelazamiento cuántico, con fotones o electrones, incluso a distancias de varios kilómetros [6, 7]. Experimentalmente se han hecho estudios sobre la velocidad de propagación de esta supuesta "interacción a distancia". Los resultados demuestran que supera la velocidad de la luz, en algunos casos, por cuatro órdenes de magnitud [8]. Estos resultados han generado bastante controversia, ya que, según la Relatividad de Einstein, nada puede viajar más rápido que la luz. Sin embargo, conceptualmente las dos teorías se pueden reconciliar, debido al hecho que, al hacer una medición sobre el sistema, el resultado es aleatorio y, por tanto, no se puede transmitir información a velocidades superlumínicas. Aun así, de nuevo, no se deberían sacar conclusiones precipitadas, y se debería esperar a que nuevos experimentos confirmen, o no, los resultados anteriores.

Después de décadas de investigación se concluyó que, debido a la propiedad del entrelazamiento, la cantidad de información que se puede almacenar y/o transmitir **con 2 o más qubits entrelazados** es mucho mayor que la que se podría almacenar y/o transmitir con dos o más bits clásicos. Esto, explicado de forma muy simplificada, se debe al hecho de que, mientras con dos bits se puede mandar una única combinación de los dos, a través de un canal de comunicación, **con dos qbits se pueden mandar al mismo tiempo todas las combinaciones posibles** (que en este caso serían 4). Para darnos una idea, la cantidad de información almacenada con 10 qbits es equivalente a la información que se almacenaría con 16000 bits clásicos. A medida que aumentamos la cantidad de qubits utilizada (N), aumenta de forma exponencial la cantidad equivalente necesaria de bits clásicos (2^N). La demostración de las afirmaciones anteriores requiere de conocimientos matemáticos y físicos muy avanzados y además tendríamos que introducir el fenómeno de interferencia cuántica. Por tanto, no vamos a entrar en más detalles [9].

CRIPTOGRAFÍA CUÁNTICA

No podemos hablar de computación cuántica sin mencionar otro campo íntimamente ligado, la criptografía cuántica. En general, la criptografía, se refiere a algoritmos implementados para cifrar mensajes, para asegurar que una tercera persona, al interceptarlos, no sea capaz de descifrarlos fácilmente. Se usa prácticamente en todas las aplicaciones informáticas, desde los servidores de correo electrónico hasta las compras efectuadas con las tarjetas de crédito. A nivel cuántico, debido a sus grandes diferencias con los sistemas clásicos, una encriptación cuántica tiene características muy distintivas, como el hecho de que un mensaje encriptado es imposible, por definición, de desencriptar, ya que al intentar interceptar el mensaje lo destruiríamos. Este hecho fue demostrado matemáticamente por lo que se conoce como el *Teorema de No-Clonación* [9]. Para terminar este artículo vamos a explicar, a grandes rasgos, de qué se trata.

Consideremos dos amigos, Alice y Bob, que tienen que compartir información confidencial a través de un canal cuántico. Para ello comparten, previamente, una clave que consiste básicamente en una secuencia de medidas que Bob debe realizar sobre el sistema de partículas (normalmente fotones) que recibe de parte de Alice (Figura 7). Sin esta clave, Bob no sabría cómo interpretar la información recibida. Imaginemos ahora una tercera persona, Eve, que intenta interceptar el mensaje. Al hacerlo, interactúa necesariamente con el sistema, y como se trata de un sistema cuántico, lo hace colapsar a un estado determinado. En otras palabras, Eve, al intentar leer el mensaje, lo destruye.

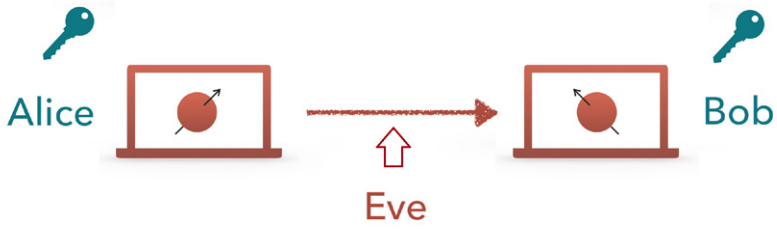


Figura 7 » Representación esquemática de la transmisión de información entre Alice y Bob a través de un canal cuántico. Una tercera persona, Eve, intenta interceptar dicho mensaje *(créditos:* www.weizmann.ac.il/complex/arnon/research-activities/quantum-cryptography*)*

Por otra parte, analizando los resultados que obtiene, Bob sería incluso capaz de darse cuenta de que hay alguien intentando interceptar el mensaje.

En la última década también ha habido un gran avance en el campo de la criptografía cuántica, y aunque "sobre papel" todo parece funcionar de maravilla, el gran reto sigue siendo el experimental.

Cuando esta tecnología esté a nuestro alcance, nos permitirá tener una total seguridad en las comunicaciones online o transacciones bancarias. La otra cara de la moneda la representa el peligro de que este tipo de tecnologías caigan en manos de organizaciones criminales, que sean capaces de comunicarse sin posibilidad de ser interceptadas por las

autoridades competentes. También cabe destacar, que la criptografía cuántica debe avanzar, por lo menos al mismo paso que la computación cuántica, ya que un ordenador cuántico, en principio, sería capaz de *romper* las encriptaciones clásicas en cuestión de unos pocos segundos. Las implicaciones de esto último serían, obviamente, desastrosas. En este sentido, actualmente, también se está investigando sobre la posibilidad de desarrollar encriptaciones clásicas capaces de sobrevivir a algoritmos cuánticos de desencriptación. Este campo recibe el nombre de criptografía post-cuántica [10,11,12] y su avance es crucial, ya que, la transición hacia lo cuántico se hará de forma gradual, y mientras, todos los equipos clásicos tendrán que estar igualmente protegidos.

PRESENTE Y FUTURO DE LA COMPUTACIÓN CUÁNTICA

Si bien a nivel teórico ha habido importantes avances en el campo, los grandes retos de hoy en día se encuentran a nivel experimental. El mayor problema consiste en mantener la coherencia cuántica de los qubits. El fenómeno de la decoherencia, grosso modo, es la pérdida de las propiedades cuánticas de un sistema debido a la continua interacción con el entorno. Como ejemplo, supone un gran reto mantener aislado un sistema de electrones durante intervalos amplios de tiempo. Para aislarlos se pueden usar trampas laser que operan a temperaturas muy bajas, a pocos grados por encima del cero absoluto (alrededor de unos -270 ˚C) y que normalmente pueden mantener aisladas las partículas durante unos pocos segundos.

Debido a lo anterior, hoy en día, las únicas operaciones computacionales que podemos realizar no pueden durar más que eso, unos segundos. Pero, dado que la potencia de cálculo de estos dispositivos es mucho mayor, puede bastar en muchos casos con unos segundos, para resolver problemas que a un ordenador clásico le costaría años de procesamiento. Además, los sistemas de refrigeración son económicamente muy costosos y requieren de mucho espacio físico. Estos son unos de los motivos por los cuales no podremos disponer de ordenadores cuánticos en nuestras casas a corto plazo. Por otra parte, hay campos muy activos de investigación, para la búsqueda de materiales más estables para la implementación física de los qubits.

A esta carrera por el desarrollo de un potente ordenador cuántico se han sumado compañías como Intel [13], Google [14], IBM [15] y Microsoft [16] entre otras. Por ahora, hay versiones de 5 qubits, relativamente estables, que mantienen la coherencia durante unos segundos. El último caso reportado corresponde a un equipo del MIT (Massachusetts Institute of Technology) [17], que logró un tiempo récord de 10 s, en febrero de este año. Existen también versiones menos estables que operan con un número entre 10 qubits (Delft University of Technology, Holanda) [18] y 20 qubits (IBM) [15]. Por otra parte, todas las estimaciones indican que, la supremacía cuántica, el punto a partir del cual ningún ordenador clásico podría alcanzar las capacidades de un ordenador cuántico, se alcanzará con 50 qubits. Si, bien, hay instituciones que afirman haber logrado implementar algunos algoritmos específicos con 50 o más qubits, para disponer de un ordenador programable y autónomo de estas características, quizás tengamos que esperar bastante.

En este sentido, no debemos confundir el número de qubits *físicos* y el de qubits *lógicos*, que puede, en general, no ser el mismo. En muchas aplicaciones, para paliar los efectos de la interacción con el entorno, se suele usar una gran cantidad de qubits *físicos* que dan lugar, *colectivamente*, a un número inferior de qubits *lógicos*, que son la unidad básica de información (a nivel cuántico) a la que nos referimos en este artículo.

Hoy en día, hay muchos equipos de investigación que trabajan de forma incesante para encontrar sistemas más estables, menos sensibles a las interacciones con el entorno y que, además, no necesiten operar a temperaturas tan bajas. Las principales líneas de investigación se desarrollan en el campo de los nanomateriales, tales como semiconductores y superconductores, grafeno, aleaciones de Silicio y Germanio, o aislantes topológicos [19], debido a sus interesantes propiedades físicas.

Encontrar materiales con estas características, supondrá un rápido avance hacia la creación de ordenador cuántico estable y al alcance de todos. Lo más probable es que todavía nos falte alrededor de una década para alcanzar ese objetivo. Pero una década pasa en un abrir y cerrar de ojos. Deberíamos pues, empezar a prepararnos ya para lo que nos espera en el futuro próximo gracias a esta nueva tecnología. Imaginemos por un momento lo que supondría un ordenador con capacidad de cómputo miles de veces superior al ordenador (clásico) más rápido de hoy en día. Unos pocos ejemplos son:

1 » Cerrar la brecha entre el crecimiento de la capacidad de almacenamiento, transmisión y la computación, para la continuidad del desarrollo de las tecnologías Big Data, lo cual supondría un salto cuantitativo y cualitativo en todas las aplicaciones relacionadas con el Internet of Things (IoT), o con la movilidad y el transporte entre otras. También supondría la capacidad de procesamiento, en tiempo real, de una cantidad enorme de datos, provenientes de diversas fuentes de todo el mundo (integración y análisis de distintas series de datos), junto a una capacidad también en tiempo real, de toma de decisiones, lo cual implicaría un gran avance en cuanto a crecimiento económico a escala local, a nivel de país o incluso mundial.

2 » La computación cuántica unida a la IA para la rápida resolución de problemas complejos de diversa índole. Esto podría tener importantes repercusiones en el avance de la ciencia básica y su impacto en la sociedad. Si hoy en día, la IA ha demostrado, en casos sencillos, su capacidad de encontrar patrones y redescubrir las leyes físicas (y de otros campos) simplemente procesado series de datos, imaginemos todo el potencial que encierra una IA con sus capacidades y velocidad multiplicadas por varios ordenes de magnitud. Puede que, por fin, nos ayudara a dar los pasos necesarios para encontrar fármacos contra el cáncer, o para la Gran Unificación de todas las leyes de la Física.

3 » Diseño rápido y optimización de dispositivos médicos: las simulaciones previas necesarias para el desarrollo y optimización de nuevo equipamiento médico, pasaría de tardar años a unos pocos días. Por tanto, los costes se reducirían de forma drástica, y la calidad de vida humana debido a estos avances, aumentaría también de forma proporcional. En este sentido, el diseño y la optimización de cualquier medio de transporte, desde coches hasta aviones, también se verían afectados positivamente.

Por otra parte, podríamos pensar que, debido al elevado coste de los primeros ordenadores cuánticos, su disponibilidad será exclusiva de las grandes corporaciones, generando así una brecha tecnológica entre los distintos miembros de la sociedad. Sin embargo, hoy en día, ya estamos viviendo esta situación, ya que las grandes corporaciones como IBM, Google o INTEL son las que tienen las primeras versiones de estos ordenadores (todavía en desarrollo), pero permiten/alquilan su uso, en la nube, a todo el público. Por tanto, todo indica que esa brecha será muy poco apreciable gracias a la computación en la nube.

Lo anterior ha sido simplemente un breve esbozo de los posibles beneficios que podría ofrecernos la computación cuántica, pero ¿quién sabe que otras posibles aplicaciones, por ahora impensables, podría proporcionarnos? Si pudiéramos echar una mirada fugaz al futuro, seguramente observaríamos algo digno de la mejor novela de ciencia ficción, o incluso ver superadas cualquiera de nuestras expectativas.

REFERENCIAS BIBLIOGRÁFICAS

1 » D. Frauchiger, R. Renner, ***Quantum theory cannot consistently describe the use of itself***, Nature Communications volume 9, 3711 (2018)

2 » C. Brukner, ***A No-Go Theorem for Observer Independent Facts***, Entropy 2018, 20(5), 350, MDPI

3 » P.A. Guerin, V. Baumann, F. del Santo, C. Brukner, ***A no-go theorem for the persistent reality of Wigner's friend perception***, Nature Communications volume 4, 93(2021)

4 » M. Proietti, A. Pickston, F. Graffitti, P. Barrow, D. Kundys, C. Branciard, M. Ringbauer, A. Fedrizzi, ***Experimental tests of local-observer independence***, Science Advances, Vol. 5, No 9

5 » T. Rauber, G. Rünger, ***Parallel Programming: for Multicore and Cluster Systems*** (2013), Springer Science & Business Media, ISBN 9783642378010

6 » Y. Yu et al., ***Entanglement of two quantum memories via fibers over dozens of kilometers***, Nature 578, 240–245 (2020)

7 » B. Hensen et al., ***Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres***, Nature 526, 682–686 (2015)

8 » J. Yin et al., ***Bounding the speed of 'spooky action at a distance***'. arXiv:1303.0614v1 [quant-ph]

9 » W.K. Wootters, and W.H., Zurek, ***A Single Quantum Cannot be Cloned***. Nature 299 (1982), pp. 802–803

10 » J. Preskill, ***Quantum computing 40 years later***, 2106.10522 [quant-ph] (2021)

11 » D.J. Bernstein, T. Lange, ***Post-quantum cryptography***, Naure 549, 188–194 (2017)

12 » F. Grasselli, ***Quantum Critography***, Springer International Publishing, 2021

13» https://www.intel.com/content/www/us/en/research/quantum-computing.html

14 » https://quantumai.google/

15 » https://quantum-computing.ibm.com/

16 » https://azure.microsoft.com/en-us/solutions/quantum-computing/

17 » https://learn-xpro.mit.edu/quantum-computing

18 » https://qutech.nl/research-engineering/

19 » A. Alfieri, S. B. Anantharaman, H. Zhang, D. Jariwala, ***Nanomaterials for Quantum Information Science and Engineering***, arXiv: 2202.03090, https://doi.org/10.1002/adma.202109621

20 » R. Orús, S. Mugel, E. Lizaso, ***Quantum computing for finance: Overview and prospects***, Reviews in Physics, Volume 4 (2019) 100028

21 » Y. Cao et al., ***Quantum Chemistry in the Age of Quantum Computing***, Chem. Rev. 2019, 119, 19, 10856–10915

22 » L. Spector, H. Barnum, H. J. Bernstein, N. S***wamy, Quantum Computing Applications of Genetic Programming, Advances in Genetic Programming, Volume 3***, pp. 135–160.

BIOGRAFÍA

Victor Ilisie es Graduado en Física por la Universidad de València y Doctor en Física Teórica por la misma universidad. Su actividad investigadora se ha centrado en la Fenomenología de la Física de Partículas a altas energías relacionada con el Bosón de Higgs y el origen de la masa en el Universo. Otro de sus campos de interés son la aplicación de la Física de Partículas a la Física Médica y ha colaborado en el desarrollo de varios detectores PET, SPECT y Cámaras Gamma con aplicaciones en el campo de la Oncología. Es autor un gran número de publicaciones en revistas indexadas de prestigio internacional, y de dos libros docentes. En la actualidad es docente/investigador en la Universidad Europea de Valencia e IP del grupo de Física Interdisciplinar y Matemática Aplicada (GFIMA) de la misma universidad.