La era cuántica, de las comunicaciones a la computación

Las tecnologías cuánticas, con especial traslación en la computación cuántica, lleva con nosotros algún tiempo, aunque está siendo ahora cuando los requerimientos de refrigeración y la estabilidad de estos equipos comienza a dar lugar a máquinas capaces de ofrecer cálculos nunca antes viables. La supremacía cuántica, anunciada -y posteriormente rebatida- por varios fabricantes a lo largo de los últimos meses, nos posiciona en un momento trascendental para la adopción real de esta innovación, llevándola de las musas al teatro.

El 23% de las empresas de todo el mundo ya está trabajando en las tecnologías cuánticas o planea hacerlo con el objetivo de desarrollar al menos una aplicación comercial importante en los próximos tres a cinco años, según recoge el estudio *'Quantum technologies: How to prepare your organization for a quantum advantage now',* publicado recientemente por el Instituto de Investigación Capgemini.

Compañías como IBM están, por el lado de los fabricantes industriales, impulsando esta vertiginosa carrera cuántica. La multinacional anunció su primer ordenador cuántico en 2016, con apenas 5 cúbits. Un año después, hizo lo propio con uno de 16 cúbits, seguido seis meses después por otro de 20 cúbits de capacidad. En aquel 2018, su mejor computador cuántico universal (esto es, diseñado con un propósito general) tenía 50 cúbits. Posteriormente, IBM presentó su procesador 'Eagle' de 127 cúbits en noviembre de 2021, mientras que en 2022 la compañía presentó su nuevo equipo, 'Osprey' de 433 cúbits. En 2023 verá la luz 'Condor', el primer procesador cuántico del mundo con más de 1.000 cúbits, y para 2025 se espera el primer computador de 4.000 cúbits.

"La computación cuántica está avanzando mucho más rápido de lo que nos hubiésemos esperado hace unos años. En muy pocos años, hemos pasado de prototipos de uno o dos cúbits a ordenadores que ya pueden abordar problemas que los computadores clásicos no pueden", introduce **Gonzalo Vázquez**, **investigador del Signal Processing and Learning Group (GTSA) UC3M**. "Ahora se empiezan a buscar problemas útiles en los que sea práctico emplear estos ordenadores cuánticos, aunque todavía falta escalar tanto el tamaño de los equipos como la calidad de los cúbits para que sus resultados sean competitivos respecto a otras técnicas de optimización o de simulación que existen".

"El desarrollo de la teoría de la información y de la comunicación sentó las bases de la tecnología que usamos actualmente. Nuestra investigación, entre otras líneas, se centra en extender esta teoría al mundo cuántico para así diseñar nuevos sistemas de comunicaciones y de procesado de la información", añade el experto.

La segunda revolución cuántica

Aunque la computación cuántica represente la parte más destacada y notoria a nivel mediático, no podemos obviar que las tecnologías cuánticas comprenden un sinfín de tecnologías y aplicaciones

heterogéneas. Muchas de ellas, disponibles comercial y ampliamente usadas desde hace años, como los láseres o algunas técnicas de fabricación de semiconductores.

Así lo entiende **Alberto Ibort**, investigador del grupo de **Matemática Aplicada a Control, Sistemas y Señales** de la UC3M: “Las aplicaciones de la mecánica cuántica van mucho más allá de la computación cuántica. Hay toda una batería de tecnologías muy maduras que se vienen usando desde el siglo pasado y otras que se están desarrollando en estos momentos como sensores cuánticos, memorias, criptografía o generación de claves cuánticas. Por ejemplo, en los procesos electorales de Suiza ya se emplean claves cuánticas generadas por dispositivos de una empresa del país, y también empresas colaboradoras en proyectos de la Universidad Carlos III de Madrid vienen desarrollando y comercializándolas desde hace más de diez años. En el consorcio **QUITEMAD** (QUantum Information TEchnologies MADrid) estamos desarrollando prototipos para la generación de claves cuánticas en fibra óptica comercial”.

El equipo de Ibort lleva, de hecho, varios años especializándose en tomografía cuántica, una variante del TAC tradicional (tomografía axial computarizada) con mayor nivel de detalle, o el control cuántico “tanto a nivel conceptual como aplicado, sobre cómo manejamos esos estados cuánticos”.

Por todo ello, Alberto Ibort define el momento que vivimos como una “segunda revolución cuántica” que se distingue de la anterior -presente desde hace décadas- en tanto que “estamos explorando los aspectos más sutiles y delicados, conceptualmente más peliagudos, de la mecánica cuántica”.

Criptografía y ciberseguridad en clave cuántica

Uno de los campos más maduros en el desarrollo de tecnologías basadas en la mecánica cuántica es el de la ciberseguridad, con empresas que llevan más de una década trabajando en soluciones de esta índole. En concreto, el área ligada a la generación de claves criptográficas y de aleatoriedad ha encajado muy bien con el propósito de este análisis, si bien su supremacía (o no) respecto a las tecnologías y sistemas clásicos todavía es objeto de debate entre la comunidad científica.

“En el mundo de la criptografía hay mucha cautela a la hora de hablar de la de la verdadera supremacía que pueda tener esta tecnología sobre las clásicas. No es una alternativa como tal, sino que tiene algunos casos de uso muy específicos para cierto tipo de transmisiones en los que sí ha demostrado su utilidad. Pero quizás no sea una alternativa a la a la criptografía clásica, sino más cuenta con un nicho de aplicación muy específico en el que realmente sí que es exitoso”, detalla **Juan Tapiador**, **investigador del Grupo de Seguridad de las Tecnologías de la Información y las Comunicaciones (COSEC) UC3M**.

Eso en lo que atañe a la generación de clave criptográficas, porque otro es el tema que preocupa a la sociedad y a empresas de medio mundo: ¿Habrá equipos capaces de comprometer la ciberseguridad de los nuevos computadores cuánticos y romper los algoritmos criptográficos diseñados hasta el momento?

De nuevo, Tapiador se muestra reservado ante esta posibilidad. “Hay una cierta clase de funciones criptográficas que sí se ven amenazadas por los ordenadores cuánticos, pero la comunidad hace varios años que tomó cartas en el asunto y las principales organizaciones e instituciones internacionales han llevado a cabo ya distintas rondas de propuestas de algoritmos”, adelanta. Estas revisiones han provocado, de hecho, que se dejen de recomendar algunos de estos algoritmos y se apueste, en palabras del investigador, por una nueva generación -denominada ‘poscuántica´- que sea verdaderamente resistente a cualquier tecnología de naturaleza cuántica tal y como la conocemos hoy en día.

“Es un campo muy especulativo, nadie sabe qué puede pasar de las sinergias entre computación cuántica, inteligencia artificial o el ‘machine-learning’. Puede haber muchas cuestiones de privacidad, de predicción, de ataques de fuerza bruta contra sistemas biométricos o contra sistemas basados en contraseñas. Es un impacto en las aplicaciones de seguridad que hoy en día aún no podemos comprender”, añade.

Honorio Martín, **investigador del grupo de Diseño Microelectrónico y Aplicaciones (DMA),** profundiza en esa línea de pensamiento: “Todo es ahora mismo muy nuevo, muy confuso y hay muchísima gente trabajando en las implementaciones de los estándares postcuánticos, especialmente en implementaciones seguras y fiables en criptografía postcuántica, que es donde por ejemplo nosotros estamos trabajando”.

Martín, en concreto, ha desarrollado un generador de números aleatorios basado en fenómenos clásicos: “Lo que busco en este momento es, en los generadores cuánticos comerciales que existen, qué vulnerabilidades pueden tener, cómo podemos influenciar su funcionamiento para que la entropía que se extrae del proceso final sea más baja. Y, por supuesto, proponer una contramedida que mejore el sistema”.

Un camino en el que existe un enorme esfuerzo investigador en la capa de microelectrónica “para adaptarse a los nuevos protocolos y nuevos cifrados”, como detalla el experto.

Futuro ilusionante, pero con pragmatismo

Pese a los anuncios de las grandes tecnológicas y el interés suscitado entre empresas y organismos de innovación de todo el mundo, los expertos académicos de la Universidad Carlos III de Madrid defienden una visión más pragmática del devenir inmediato de esta tecnología, a la que ven un futuro ilusionante pero sólo tras superar muchos retos pendientes en el camino.

Erik Torrontegui, investigador Ramón y Cajal del Departamento de Física de la UC3M, lleva trabajando desde el 2008 en el campo de las tecnologías cuánticas, ve grandes ventajas en su uso, pero se muestra escéptico con respecto a los anuncios grandilocuentes de algunos gigantes tecnológicos “Cómo anunciar más y más qubits en un ordenador cuántico cuando apenas podemos controlar de manera eficiente sistemas de unos pocos qubits. Hoy por hoy, todas las tecnologías

cuánticas enfrentan un problema de coherencia, el tiempo de vida de los qubits, que viene a ser del orden de microsegundos. Eso ya da una muestra de la profundidad de los circuitos y de los sistemas. Primero debemos superar estos retos técnicos".

Lo que sí ve más maduro Torrontegui, al igual que sus compañeros, es el uso de otros fenómenos cuánticos "conocidos desde hace cien años" pero que no estaban disponibles desde el punto de vista de la ingeniería, como el entrelazamiento o la superposición que van más allí de su aplicación exclusiva a la computación cuántica. "Yo me dedico al control de los sistemas cuánticos, cómo manipularlos y sacar provecho de ellos. También he trabajado en el desarrollo de protocolos para la mejora de sensores cuánticos, diseño de puertas más robustas, etc." indica, antes de reforzar el potencial de innovaciones como los sensores cuánticos, capaces de trabajar a temperatura ambiente y con mayor sensibilidad.

En busca de los casos de uso

Casos de uso que van desde la mejora de la sostenibilidad en sus operaciones y el descubrimiento de nuevos materiales para la fabricación de baterías, hasta un aumento de la seguridad de la información mediante el cifrado cuántico, pasando por el desarrollo de sensores médicos y la reducción en la emisión de gases industriales nocivos.

Por su parte, las organizaciones de servicios financieros están experimentando para fijar con mayor precisión los precios de los activos de riesgo, optimizar su cartera de servicios para obtener mejores rendimientos y detectar fraudes. En el caso de las empresas sanitarias, uno de sus propósitos es acortar el ciclo de desarrollo de los medicamentos.

Solventar los últimos flecos en el desarrollo de la computación cuántica, establecer los modelos adecuados para su explotación y definir los nuevos ecosistemas que aprovechen esta tecnología son los retos para los próximos cursos, a medida que nos vamos introduciendo en esta era cuántica en la que el carácter bipolar de unos y ceros dará lugar a esa superposición de estados que amplíe nuestra forma de pensar y entender la informática.

ODS implicados: 5, 9, 16, 17

Más información de interés para innovar juntos:

Grupos de Investigación participantes en la validación de este reto:

- Grupo de Tratamiento de la Señal y Aprendizaje (GTSA)
- Arquitectura de Computadores, Comunicaciones y Sistemas (ARCOS)

- Matemática Aplicada a Control, Sistemas y Señales
- Computer Security Lab (COSEC)
- Diseño Microelectrónico y Aplicaciones (DMA)
- Departamento de Física

Startups y Spinoffs del programa de Incubación de la UC3M relacionadas:

- LeapWave technologies
- Cyclomed Technologies

Laboratorios del Parque Científico UC3M relacionados:

- Laboratorio de Antenas asociado al Grupo de Radiofrecuencia, Electromagnetismo, Microondas y Antenas (GREMA)