

Dos fotones entrelazados transportan la misma información. Si uno se modifica, el otro también lo hace... aun a distancia.

INTERNET CUÁNTICO

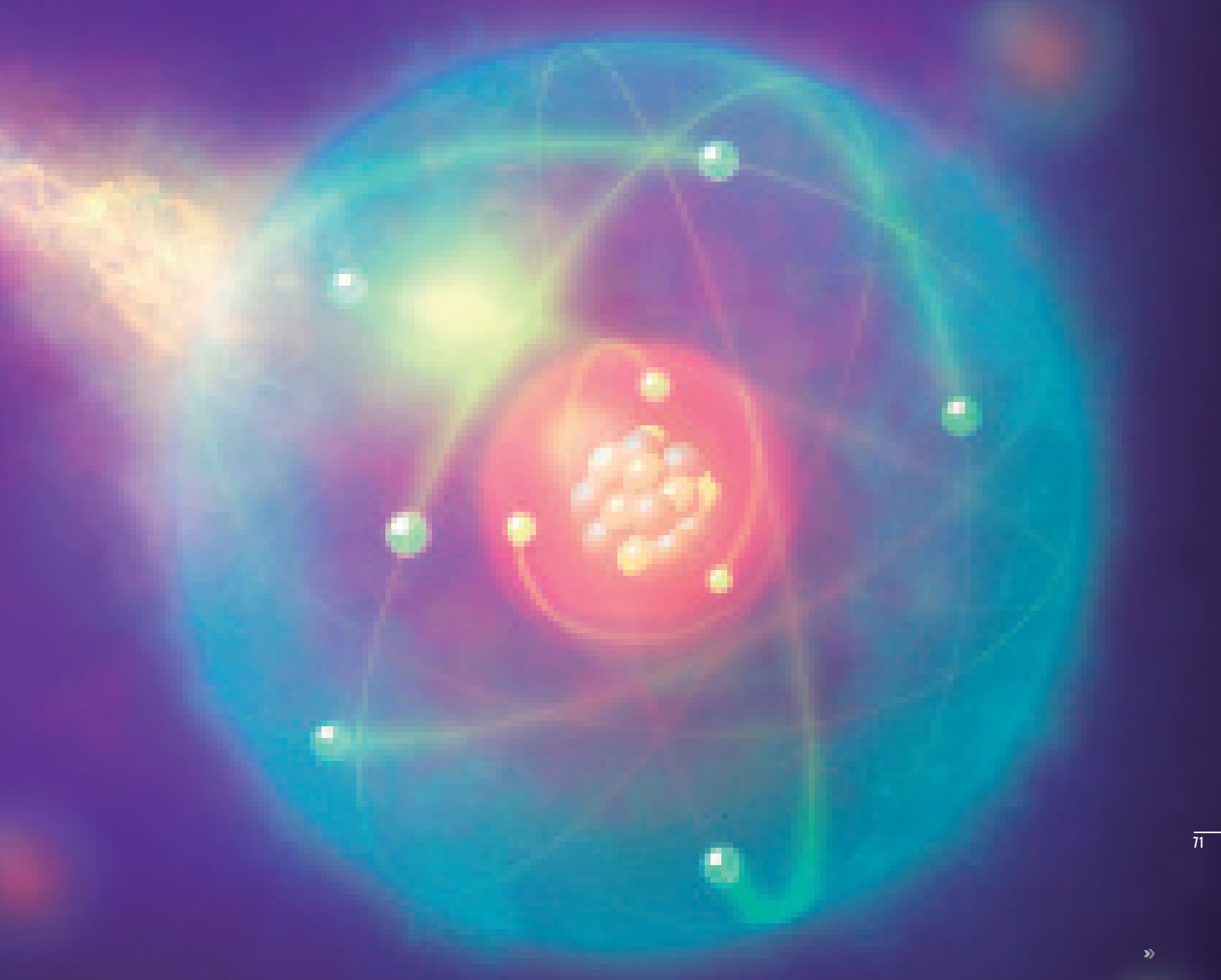
Enlazar la luz con la materia, y enviar el resultado a larga distancia es el gran reto de la física cuántica. China, Europa y Estados Unidos lo ven factible: todos compiten en la carrera para convertir la teoría en una realidad. Pero no va a suceder mañana, ni va a sustituir a las redes de comunicación que usamos hoy. Funcionará en paralelo al internet clásico, para proteger las infraestructuras críticas y la información sensible.

9

de febrero de 2021. Oldsmar, Florida (EE. UU.). A las 8 am, los sistemas automatizados de una planta potabilizadora que abastece a 15 000 hogares multiplicaron por 100 los niveles de sosa cáustica que se usa para tratar el agua. En pequeñas cantidades, esta sustancia corrosiva sirve para eliminar metales y reducir la acidez. Pero, en dosis mayores, es venenosa. Un hacker había accedido de forma remota al sistema informático que controla los procesos químicos de la estación depuradora. Al parecer, un operario se dio cuenta esa misma tarde, justo a tiempo para impedir el desastre. Hoy, el caso sigue siendo investigado por el FBI, que aún no ha logrado esclarecer la identidad del atacante, ni si actuó desde suelo estadounidense o desde el extranjero.

Por suerte, no pasó de un buen susto. Pero sirvió para dejar cla-

ro que existe el riesgo de que se repita algo parecido en el futuro. “Los ataques –terroristas, entre naciones...– serán cada vez más tecnológicos, por eso, hay muchos países y compañías interesados en apoyar la protección de infraestructuras críticas, como la red de agua potable o el suministro eléctrico, la comunicación entre administraciones, o los registros médicos de los sistemas de salud”, apunta a MUY el físico Hugues de Riedmatten, director del Grupo de Fotónica Cuántica con Sólidos y Átomos del Instituto de Ciencias Fotónicas (ICFO), en Barcelona. Es lo que nos responde cuando le preguntamos por qué la Unión Europea, China y Estados Unidos están tan interesados en subvencionar la investigación en internet cuántica.



tico. Porque resulta que la seguridad será, precisamente, una de sus aplicaciones estrella. “En el internet convencional, tenemos métodos de encriptación muy buenos que usamos a diario, por ejemplo, en las transacciones bancarias. Sin embargo, sabemos que, si tuviéramos suficiente poder computacional, un hacker podría acceder al sistema. Algo que no puede pasar con el internet cuántico”, añade Tracy Northup, científica del Instituto de Física Experimental de la Universidad de Innsbruck (Austria).

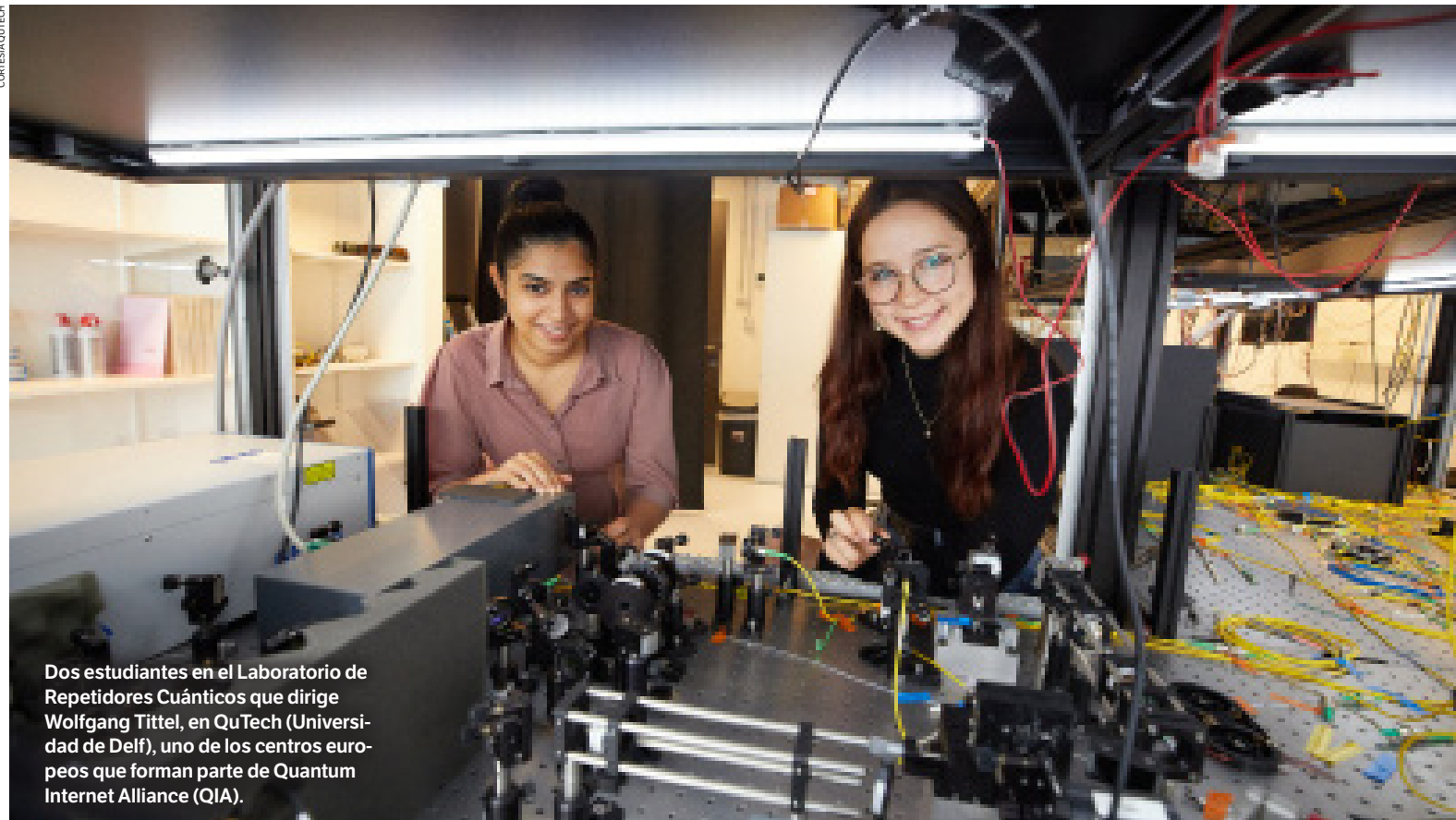
FRUTO DE ESTE INTERÉS SE CREÓ, EN 2018, LA QUANTUM INTERNET ALLIANCE (QIA), DE LA QUE FORMAN PARTE MÁS DE VEINTE CENTROS DE INVESTIGACIÓN de toda Europa. Entre ellos, están el equipo de Northup y el de Riedmatten. Stephanie Wehner, una genio de la física y la informática que trabaja en la Universidad Tecnológica de Delft (QuTech), en Países Bajos, es la coordinadora de QIA. Su ambicioso objetivo es desarrollar una red europea en que la información se transmita en estado cuántico de extremo a extremo. En un artículo publicado en *Science* en 2018, Wehner establecía las fases para conseguirlo: aún se encuentran en la primera, conectar Delft con otras tres ciudades holandesas. “Creemos que es factible, ¡pero no lo sabremos seguro si no lo intentamos! Los científicos europeos están a la cabeza de los logros más significativos en este campo en las últimas décadas, y es hora de sacarle partido a esa experiencia. Ahora nos toca desarrollar el hardware por el que circulará la información cuántica, más el software que controlará cómo se distribuye, y las aplicaciones que funcionarán en esa red”, dice Northup a MUY.

La base de esta idea está en la física cuántica que, según Riedmatten, “nos permite codificar la información de una forma diferente a como se ha hecho hasta ahora, aprovechando sus propiedades de superposición y entrelazamiento”. ¿Qué? ¿Cómo? Empecemos por el principio.

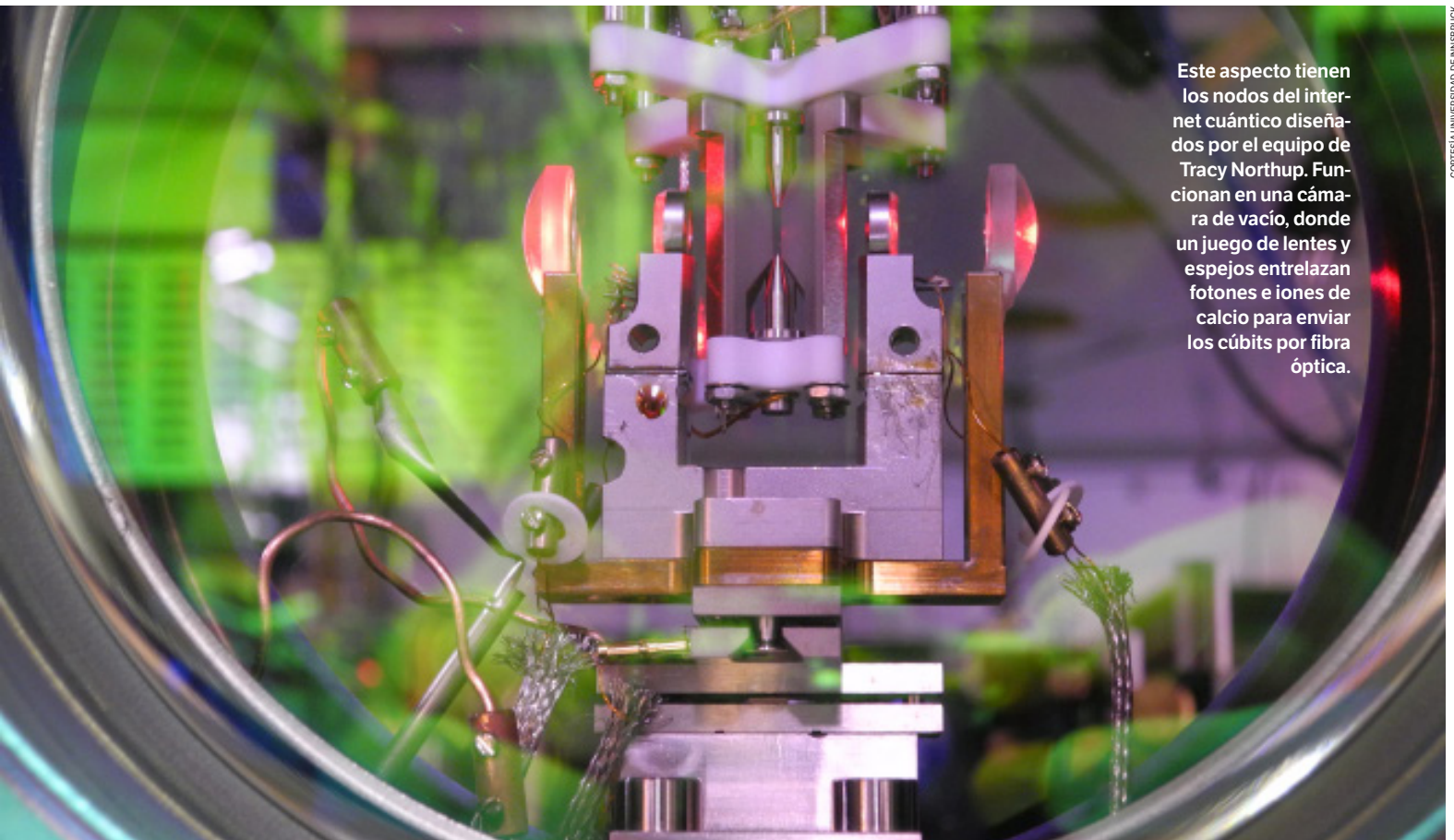
Si queremos llevar la información de un ordenador a otro de forma cuántica, la moneda de cambio es el fotón –partícula elemental que compone la luz–. “Como son partículas cuánticas,

puedes ponerlas en una superposición de propiedades. Y una de las propiedades más interesantes de manipular es la polarización –hacer circular el fotón a izquierdas o a derechas–. La información cuántica se da en la superposición de polarizaciones en un fotón. Es lo que se llama cúbit –*qbit* o *quantum bit*, en inglés–, formado por dos estados cuánticos”, indica a MUY Edén Figueroa, director del Grupo de Tecnología de Información Cuántica en el departamento de Física y Astronomía de la Universidad de Stony Brook (Nueva York). Mientras los bits tradicionales que navegan por el internet clásico son 0 o 1, los cúbits tienen la posibilidad de representar a la vez los valores 0 y 1. Por eso, tienen una capacidad de guardar información mucho mayor. Además, esta curiosa propiedad de la mecánica cuántica –llamada superposición– es lo que hace que la información sea tan escurridiza e imposible de manipular por terceros. Resulta que, cuando se observa o intercepta un cúbit, su delicado estado mixto se colapsa y se convierte en 0 o en 1. Con ello, se destruye la información cuántica que portaba, dejando la huella de la intrusión.

¿Y cómo metemos los cúbits de información que queremos enviar en los fotones? “Puedes codificar tu fotón, cargándole el estado de polarización que elijas. Para eso, creas el fotón y lo pasas por un dispositivo llamado modulador electroóptico, al que



Dos estudiantes en el Laboratorio de Repetidores Cuánticos que dirige Wolfgang Tittel, en QuTech (Universidad de Delft), uno de los centros europeos que forman parte de Quantum Internet Alliance (QIA).



Este aspecto tienen los nodos del internet cuántico diseñados por el equipo de Tracy Northup. Funcionan en una cámara de vacío, donde un juego de lentes y espejos entrelazan fotones e iones de calcio para enviar los cúbits por fibra óptica.

pones cierto voltaje para que cambie la fase del campo eléctrico. Ese cambio es lo que determina la superposición de polarizaciones para ese fotón. Así, consigues el cúbit que tú quieres”. Parece fácil, al menos, por la familiaridad con que lo explica Figueroa.

AHORA QUE YA TENEMOS LA MATERIA PRIMA, EL CÚBIT, EL REQUISITO NÚMERO UNO PARA HABLAR DE INTERNET CUÁNTICO ES EL ENTRELAZAMIENTO. “Si tienes una pareja de fotones entrelazados y envías cada uno en direcciones distintas, a dos puntos separados, por ejemplo, por cien kilómetros, cada vez que haces una medición en un fotón, el otro reacciona inmediatamente, altera la información en el otro extremo”, nos explica Figueroa. No es que una partícula esté en dos sitios a la vez, sino que hay dos partículas que tienen el mismo estado a la vez. Aunque estén en lugares diferentes, su estado es compartido y un cambio en uno implica un cambio en el otro.

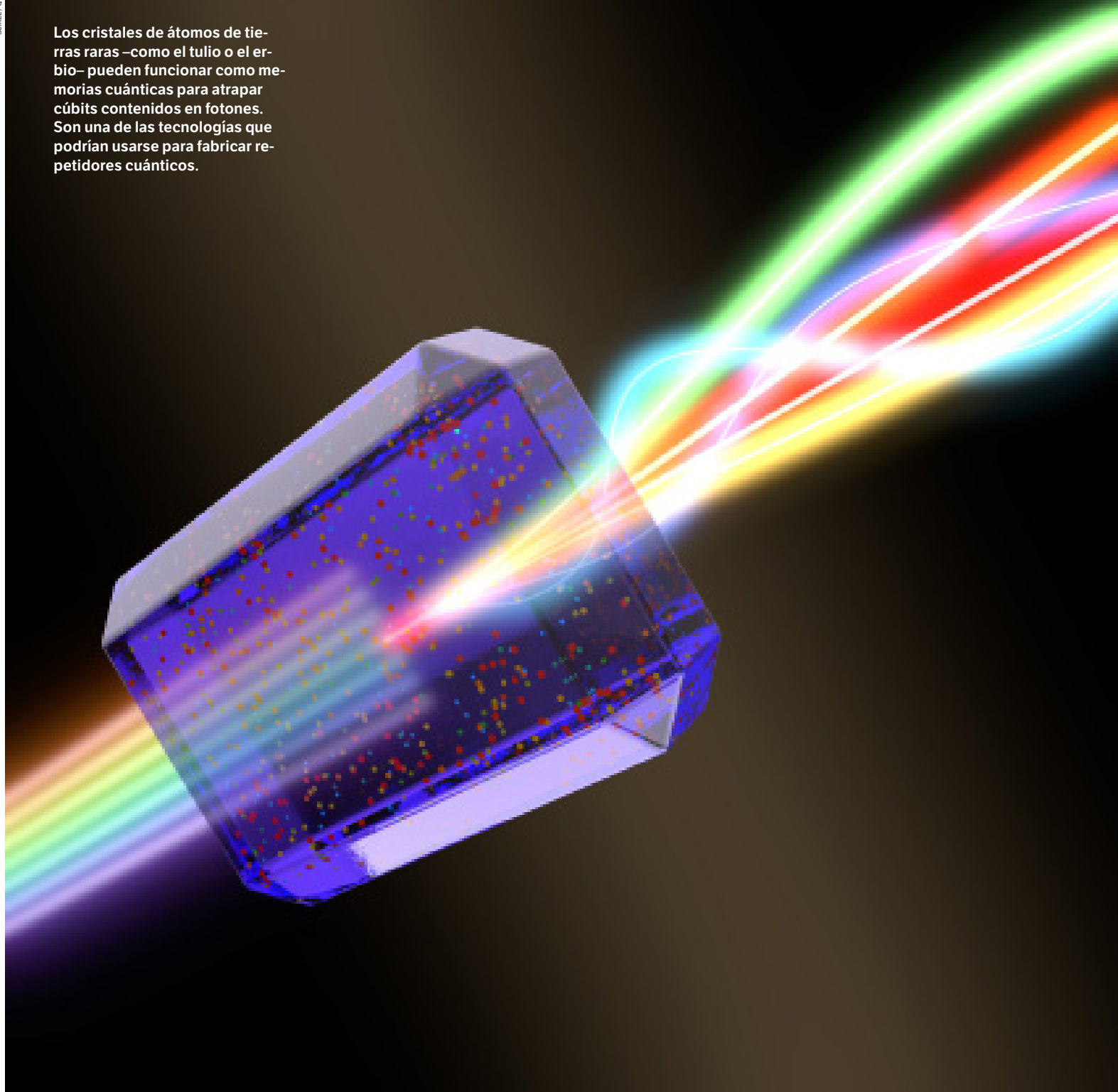
Al otro lado del charco, Eden Figueroa y sus seis estudiantes de postdoctorado acaban de demostrar en enero de este año que es posible conectar el campus de la Universidad Estatal de Nueva York y con el Laboratorio Nacional de Brookhaven, separados por 158 kilómetros, empleando memorias cuánticas a temperatura ambiente, de forma que la información codificada en el origen se mantenía al recibirla en el destino. “Estamos desarrollando diferentes tecnologías que se necesitan para construir el primer prototipo de internet cuántico”, nos cuenta en entrevista telefónica. “Lo primero es crear fuentes de fotones sencillos, es decir, que con cada pulso que aplicas a la fuente, sale un solo fotón. Lo siguiente es tener fuentes de fotones entrelazados: cada vez que aprietas el botón, la fuente emite dos fotones cuyo estado está correlacionado”. Pero su niño mimado son las memorias cuánticas, “una tecnología muy bonita que está basada en átomos”, nos dice con entusiasmo, en la que lle-

va diez años trabajando y que es el requisito número dos para empezar a construir redes cuánticas. “Imagina que tienes dos fotones entrelazados que están viajando en la fibra y quieres hacer la medición en uno. Para eso, necesitas un sistema que pueda almacenar la información de ese fotón, mientras esperas que el otro fotón llegue a la estación de medición en su punto de destino”, señala.

Otro especialista en memorias cuánticas es Riedmatten. En sus palabras, “sirven para hacer una sincronización entre los tramos de una red. Guardan el resultado de una operación, hasta que los demás tramos de la red consigan realizar también esta operación o tarea con éxito”. Un ejemplo de operación típica sería establecer entrelazamiento entre dos puntos. Es un proceso que no funciona siempre, ni se consigue a la primera: “Si tienes un tramo de 100 km en fibra óptica, solo llegan 1% de los fotones transmitidos, por eso la probabilidad de generar entrelazamiento es muy pequeña. Hacen falta múltiples intentos, hasta que la memoria cuántica emite una señal avisando de que se ha conseguido”, apunta. Cuando queremos establecer una red multinodo, en que dos puntos están conectados a través de, al menos, un tercero, una memoria cuántica permite almacenar el entrelazamiento entre los puntos 1 y 2, mien-

Cuando se intercepta un cúbit, su delicado estado cuántico se colapsa: se corrompe la información, adelantando la intrusión

Los cristales de átomos de tierras raras –como el tulio o el erbio– pueden funcionar como memorias cuánticas para atrapar cúbits contenidos en fotones. Son una de las tecnologías que podrían usarse para fabricar repetidores cuánticos.



tras se consigue enlazar con el 3. “Entonces, podemos juntar todos los tramos para que la distancia sea más larga”, señala el físico.

Es lo que llamamos repetidor cuántico. Según Riedmatten, “si todos los nodos tienen que funcionar al mismo tiempo, la probabilidad total disminuye de forma exponencial al número de nodos. Pero, si puedes guardarlo en la memoria cada vez que funcione, el tiempo total no va a depender del número de tramos”.

OTRA VENTAJA MÁS DE LOS REPETIDORES CUÁNTICOS ES QUE PERMITEN ENTRELAZAR FOTONES DE FORMA REMOTA, o sea, no hace falta que salgan entrelazados desde la misma fuente. Imagina que tienes un par de cúbits entrelazados en el tramo A y B, y otra pareja en el tramo C y D. “Al hacer una medida conjunta entre B y C, las memorias A y D quedarán correlacionadas, aunque nunca haya habido interacción

entre ellas. Al hacer la medición, los fotones en B y C desaparecen, pero el entrelazamiento se mantiene entre A y D. Es una clave para conseguir el internet a larga distancia”, recalca Riedmatten.

Aunque hay otros métodos, las memorias más utilizadas en los experimentos usan átomos fríos para almacenar los estados cuánticos. Esta tecnología reúne eficacia –la probabilidad de que un fotón entre en la memoria sin perder el entrelazamiento con su compañero es del 90 %– con un tiempo de coherencia aceptable –el tiempo que se puede guardar la información de forma que

Las memorias cuánticas son una pieza clave para poder enviar cúbits entrelazados entre varios tramos de una red

no se pierden las superposiciones cuánticas, que en la actualidad de unos cientos de milisegundos –.

Como era de esperar, el aspecto de estas memorias poco se parece a sus homólogas digitales. Las de átomos fríos son nubes de rubidio enfriado con láseres en una cámara de vacío. Los láseres apuntan en todas las direcciones para ralentizar los átomos hasta el punto en que apenas se mueven, con lo que baja su temperatura hasta decenas de microkelvin. Entonces, se mapea o imprime la luz en ellos: “El fotón entra en estos átomos fríos, y se para completamente. Es como si se pudiera parar la luz”, observa Riedmatten.

AUNQUE LOS ÁTOMOS NO OCUPAN NADA, LOS DISPOSITIVOS BASADOS EN ESTA TECNOLOGÍA SON GRANDES Y APARATOSOS. Ocupan una mesa de dos por dos metros, por el equipo de láseres que hay alrededor. Para superar este inconveniente, su grupo del ICFO está investigando con otro sistema más pequeño y manejable: “los dispositivos de estado sólido, donde un cristal captura directamente el fotón y le impide moverse. No necesitamos los láseres”, explica Riedmatten. En concreto, los cristales que utilizan en su laboratorio están formados por átomos de tierras raras, “porque tienen una configuración de electrones que los aísla de su entorno, los hace menos maleables y proporciona tiempos de coherencia muy largos”, añade. Una propuesta diferente es la de Figueroa, que emplea memorias cuánticas a temperatura ambiente compuestas por vapor de rubidio en un tubo de cristal de dos centímetros de largo, que cabrían en una caja de zapatos. Su intención es hacerlas más asequibles y manejables, con menos requisitos técnicos que las memorias de átomos fríos o de estado sólido.

Así las cosas, el objetivo último de las investigaciones en curso es “demostrar por primera vez un repetidor cuántico que funcione. No se ha logrado aún preservar el entrelazamiento para poder medirlo

con las memorias cuánticas”, afirma Figueroa. Todo un reto científico y de ingeniería. “En años recientes, hemos visto demostraciones muy interesantes de conexiones de punto a punto en distancias cortas usando distintos sistemas. El próximo paso implicará conexiones más complejas –multinodo–, en distancias largas y con más cúbits, para poder realizar tareas de comunicación cuántica más complejas”, según apunta Northup. Por el momento, su equipo ha logrado enviar un fotón entrelazado con un ión de calcio –uno de los sistemas de hardware que podrían armar el internet cuántico– a 50 kilómetros por fibra óptica, sin que se perdiera el entrelazamiento. Y el hito más reciente de Riedmatten ha sido demostrar un entrelazamiento entre memorias cuánticas de estado sólido usando luz a frecuencias de telecomunicaciones, el pasado mes de enero. La idea es poder ajustar su tecnología a las redes actuales de fibra óptica que ya tenemos.

Mientras, la meta en la carrera mundial hacia el internet cuántico apunta a dianas cada vez más alejadas. Según Figueroa, lo ideal para lograr un sistema que abarque todo el planeta es una combinación de fibra y espacio libre. “Si el entrelazamiento se quiere hacer entre 100 o 150 kilómetros, se puede lograr por fibra. Si quieres hacerlo entre continentes, debes usar satélites. Lo que no está claro

QKD, una realidad hoy

Yo tengo un ordenador normal conectado a internet por fibra óptica que se comunica con una estación y, entre ambos, intercambian claves cuánticas que se han generado usando la luz –cúbits codificados en fotones– y viajan en paralelo a la información enviada”, cuenta a MUY el profesor Juan José Ripoll, investigador del Instituto de Física Fundamental del CSIC, en Madrid. Esto es lo que se conoce como red de distribución de clave cuántica –QKD, por sus siglas en inglés– y supone una “capa de seguridad encima de la seguridad ordinaria de cifrado que ya tenemos”.

No se trata de internet cuántico en toda regla, aunque emplea algunos de sus principios. Las redes QKD son sistemas de criptografía que transmiten claves en forma de cúbits, protegidas por las leyes de la mecánica cuántica. Pero no existe entrelazamiento. “El mensaje se transmite cifrado de forma ordinaria, lo que se envía de forma cuántica entre las dos estaciones es la clave. Se necesitan para ello dos dispositivos de distribución de clave cuántica, en que ambos generen esas claves de forma sincronizada, uno en el lugar del emisor y otro en el del receptor”, explica Ripoll, que participa en proyecto European Quantum Communications Infrastructure de la CE.

Poco a poco, las redes QKD se están implementando en infraestructuras críticas y gubernamentales. Existen ya

en España, Austria, Holanda y Alemania. La más larga está en China y cubre una distancia de 2000 km entre Pekín y Shanghai, a través de fibra óptica. Ripoll prevé que, “en un plazo de tres o cuatro años, el envío de claves cuánticas por satélite será una realidad práctica, eficaz para poner en contacto dos puntos separados por miles de kilómetros de forma segura”.



A corto plazo, los sistemas de criptografía QKD se podrán combinar con repetidores cuánticos

El reto actual está en crear repetidores cuánticos que puedan preservar la información intacta en distancias cada vez mayores

es cómo puedes conseguir que la memoria reciba el fotón por el espacio libre, por satélite”, nos dice. Su equipo de la Universidad Stony Brook colabora con la Universidad de Padova y el Matera-Laser-Ranging-Observatory (ambos en Italia) para responder este interrogante.

En paralelo, el sueño de Riedmatten es reunir en un mismo sistema todas las cualidades que necesitamos para tener una buena memoria cuántica. “Todavía no lo hemos conseguido. Una tecnología es mejor para almacenar durante largo tiempo, otra es mejor para la eficacia, otra es mejor para guardar más de un cúbit...”, reconoce. Su segunda gran apuesta es crear entrelazamiento entre memorias cuánticas a larga distancia, “pero fuera del laboratorio”. Porque, por ahora, todas las demostraciones en que se ha conseguido han tenido lugar a través de kilómetros de cable fibra óptica, sí, pero enrollado en una habitación y protegido de interferencias exteriores.

POR AHORA, TIENE PINTA DE QUE "EL INTERNET CUÁNTICO NO ES PARA MAÑANA, SINO QUE SERÁ A MUY LARGO PLAZO. Vamos a hacer una pequeña red de momento y luego vamos a ir extendiéndola. Para ampliarlo a nivel continental, hacen falta decenas de años. Hacerlo a nivel local, en una ciudad o un país, quizá se pueda conseguir en los próximos cinco o siete años. De hecho, hay planes para intentarlo entre Bar-

celona y Madrid”, nos avanza Riedmatten.

Tampoco será un sustituto del internet clásico, sino que ambos coexistirán en el futuro, según los expertos. Enviar un email que no sea de alto secreto o ver una película en *streaming* son cosas que la WWW convencional hace muy bien, mientras su hermano cuántico se especializa en comunicaciones seguras.

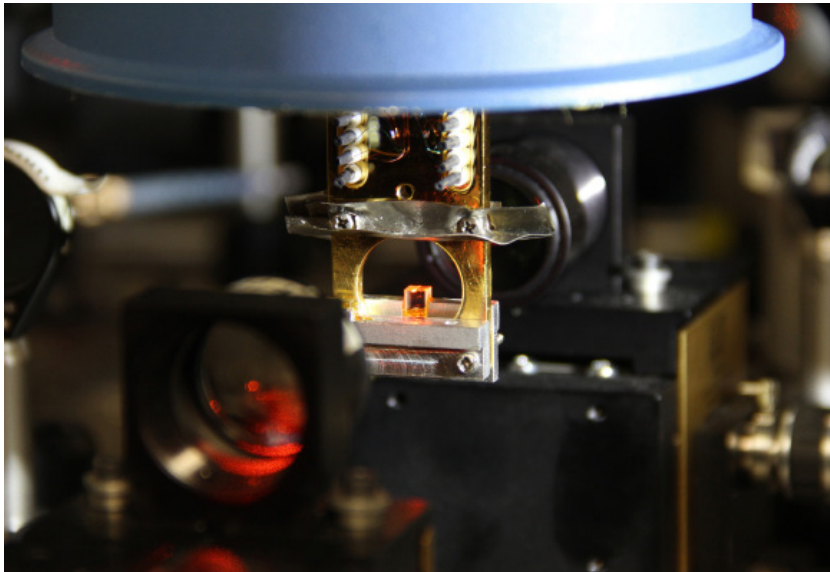
POR SU PARTE, FIGUEROA AUGURA QUE, PARA DENTRO DE 10 AÑOS, ESTARÁ OPERATIVA OTRA UTILIDAD de este tipo de redes: la astrometría cuántica. “Consiste en un sistema de sensores conectados a través de entrelazamiento que cubren una distancia bastante larga, de cientos de kilómetros, y eso te permite detectar con mucha precisión partículas astronómicas que vienen del espacio exterior –como materia oscura, neutrinos...–”. Y, para dentro de 20 años, “una vez que tengamos repetidores cuánticos en varios lugares, se podrá hacer computación cuántica distribuida. Es decir, unir distintos ordenadores cuánticos para hacer simulaciones mucho más grandes y poderosas de las que hace un solo procesador cuántico”, apostilla el científico.

Un poco antes, quizá, se haga realidad la

Dueto de luz y materia

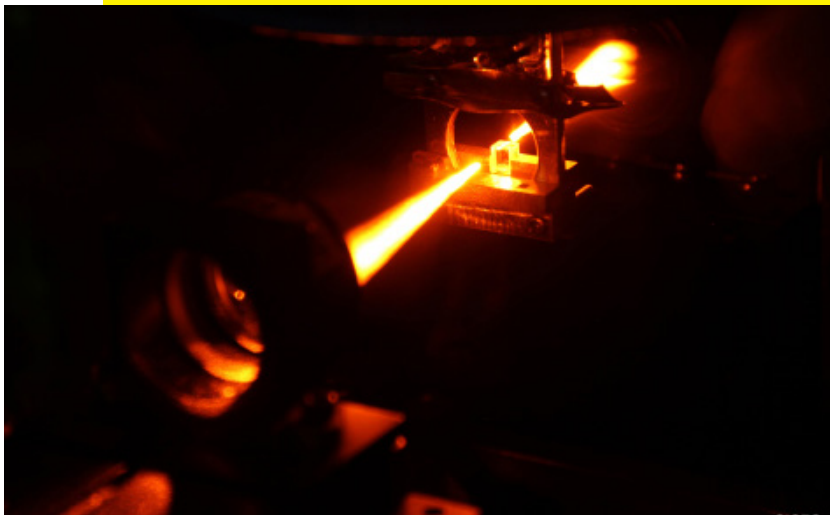
Quizá, puedas preguntarte cómo funcionan las imprescindibles memorias cuánticas, es decir, cómo pasa la información en cúbits desde el fotón original a los átomos de memoria. Y aquí nos sumergimos en otra piscina maravillosa de la física cuántica: la interacción entre la luz y la materia. Porque la memoria cuántica consiste en eso: tenemos el cúbit encuadrado en un estado de polarización del fotón (luz) y lo vamos a transferir a los átomos de una memoria cuántica (materia), para que los guarde. “El fotón deja de existir, pero se imprime su estado en los átomos de la memoria”, señala Riedmatten. Si todo funciona según lo esperado, se mantendrá el entrelazamiento entre la memoria y el segundo fotón que se envió, compañero del que ha quedado capturado por la memoria. “En un caso ideal, el estado del fotón antes y después de este proceso es exactamente el mismo –algo que se conoce como alta fidelidad–. Por otra parte, cuanto mayor es el tiempo de almacenamiento, menor será la fidelidad de la memoria”, añade este experto.

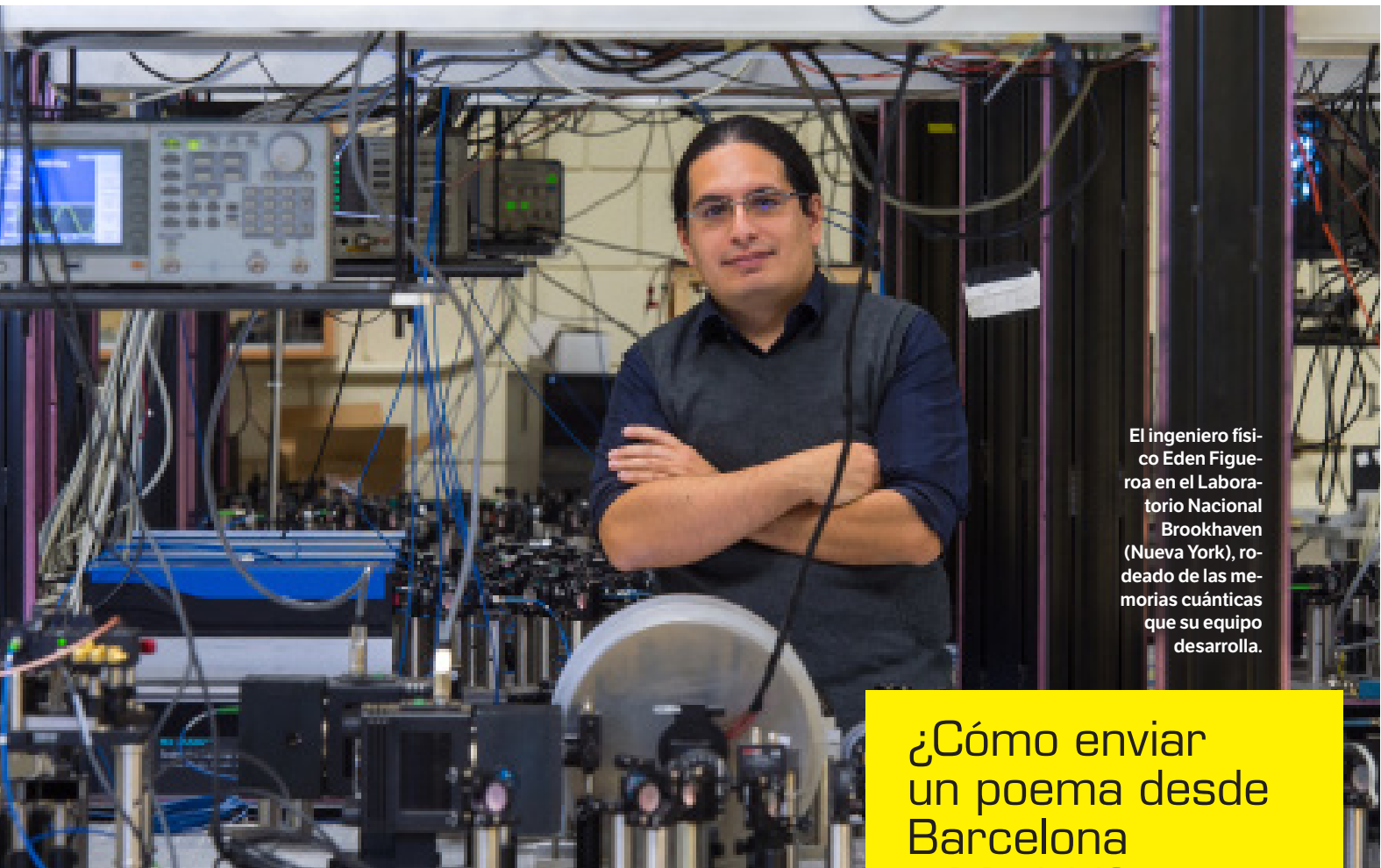
CORTESÍA ICFO



En el laboratorio de Hugues Riedmatten, en el ICFO de Barcelona, un láser dispara un haz de luz para imprimir las propiedades del fotón en los átomos de una memoria de estado sólido, formada por cristales de praseodimio.

CORTESÍA ICFO





CORTESÍA LABORATORIO NACIONAL BROOKHAVEN

El ingeniero físico Eden Figueroa en el Laboratorio Nacional Brookhaven (Nueva York), rodeado de las memorias cuánticas que su equipo desarrolla.

¿Cómo enviar un poema desde Barcelona a Madrid?

En un canal cuántico, la información se codifica en cúbits, que equivalen a estados de polarización en un fotón. ¿Pero cómo se traduce eso a la transmisión de algo más allá de un 1 o un 0, digamos, por ejemplo, un poema? “Es una cuestión teórica todavía. Esperemos que algún día sea posible, pero aún no se puede hacer”, nos responde Eden Figueroa. “Lo primero que se necesitaría es tener dos fotones entrelazados que estén comunicando dos lugares, por ejemplo, Barcelona y Madrid. Para eso, en un punto intermedio, por ejemplo, Zaragoza, tienes una fuente que lanza esas dos partículas entrelazadas: una se va a Madrid y otra, a Barcelona. En Barcelona, tienes los fotones donde has codificado el poema—cada fotón puede portar dos bits de información—. Entonces, haces una medición en Barcelona entre el fotón entrelazado que vino de Zaragoza y el fotón que tiene los bits del poema. Cuando haces la medición, por las propiedades de la mecánica cuántica—un fenómeno que se llama teleportación—, los cúbits que estaban en Barcelona, a través del entrelazamiento, se van a viajar a Madrid”. El proceso tendrá que repetirse múltiples veces, hasta que todas las palabras del poema quedan transmitidas por el canal cuántico.

Mientras, las memorias cuánticas servirán para avisar de cuándo cada uno de los fotones entrelazados llega a Barcelona o Madrid. “Solo cuando las dos han recibido sendos qbits, puedes hacer la medición en los fotones de Barcelona para mandar el poema vía teleportación a Madrid”, concluye.

computación cuántica ciega –o en la nube–. Como nos explica Northup, “en el futuro, habrá problemas científicos que solo los procesadores cuánticos puedan solucionar, pero no todos los investigadores tendrán acceso al suyo propio. Por eso, tendrán que enviar el trabajo para que lo resuelva un ordenador cuántico en otro lugar, de forma remota. Este podrá hacer las operaciones que se le piden, sin saber cuál era la pregunta. Así, nadie puede acceder al contenido del trabajo ni a sus datos, ni siquiera la compañía propietaria de la tecnología en cuestión. Todo lo contrario que sucede con los servicios en la nube que usamos hoy, como gmail, por ejemplo”, señala esta investigadora.

CUANDO QUEREMOS SABER, A LA HORA DE LA VERDAD, DE QUÉ LE SERVIRÁ AL CIUDADANO DE A PIE TODO ESTE TINGLADO CUÁNTICO, Northup confía en que “beneficiará a la gente porque ofrecerá comunicaciones seguras en la vida cotidiana, por ejemplo, protegiendo la privacidad de nuestros datos médicos o financieros”. Pero, como todo, también tiene sus riesgos: puede aumentar la seguridad de las comunicaciones, sí, aunque también podría hacer más frágiles las redes tradicionales. “Si la tecnología de computación cuántica cayera en malas manos, sería un problema, igual que pasa con las bombas nucleares. Quién va a hacer uso de ella primero y quién va a hacerlo después es algo que los gobiernos todavía están tratando de delimitar”, admite Figueroa. ¿Y no va a servir para acrecentar las diferencias de poder entre países?, le preguntamos. “Ese es un tema que me preocupa. ¡Imagínate, estás hablando con un mexicano que trabaja en Estados Unidos! Lo que hacemos en mi equipo es tecnología que utiliza sistemas sencillos, que no son demasiado complicados, pero funcionan. Uno de mis sueños es hacerlos lo más económicamente accesibles para que otras naciones puedan adquirirlos. Probablemente, empezarán a comercializarse en los próximos cinco años. Lo deseable es que, eventualmente, todos los países estén dotados de redes de internet cuántico, igual que ha pasado con el internet clásico”. □