CRIPTOGRAFÍA

Algoritmos post-cuánticos y seguridad digital: ciencia para un futuro resiliente

El IMSE trabaja en un proyecto pionero que combina fotónica, algoritmos e identidades digitales robustas para construir sistemas de comunicación cuántica seguros y escalables

Por **Érika López Palma**

Cada día, millones de dispositivos se conectan, intercambian datos, y se exponen a riesgos. Desde el robo de credenciales bancarias hasta la suplantación de identidad, los ataques digitales son una realidad constante. Pero lejos de alimentar el miedo, la comunidad científica trabaja para anticiparse, proteger y construir un ecosistema digital más seguro.

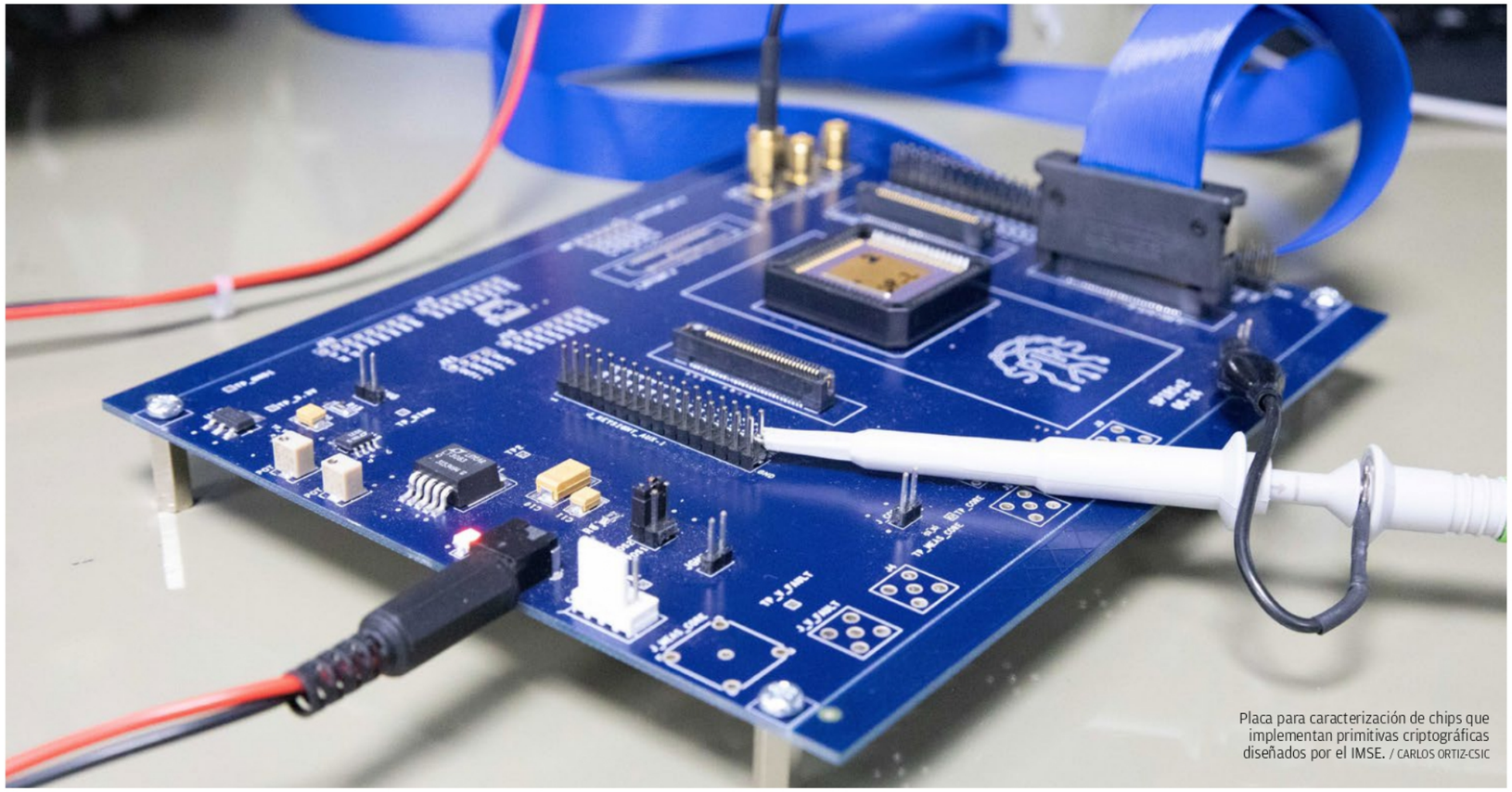
"A cualquiera que le han robado cualquier información que considere sensible, un hackeo, dinero en el banco... Creo que se da cuenta en ese instante del problema de la seguridad", reflexiona **Piedad Brox**, investigadora del Instituto de Microelectrónica de Sevilla (IMSE-CSIC). "No hay que cerrarse en banda a no entrar en el mundo digital. Hay que seguir las recomendaciones de los organismos expertos en ciberseguridad para protegerse".

La seguridad digital no es solo una cuestión técnica: es un reto social, económico y ético. Y en este contexto, la llegada de la computación cuántica plantea un desafío sin precedentes.

La computación cuántica promete revolucionar la forma en que procesamos información. Su capacidad para realizar cálculos masivos en paralelo podría permitir romper los algoritmos criptográficos que hoy protegen nuestras comunicaciones, transacciones y datos personales.

Algoritmos como RSA, ECC o DH, basados en problemas matemáticos difíciles para los ordenadores clásicos (como la factorización de números primos o el logaritmo discreto), podrían ser vulnerables ante un ordenador cuántico suficientemente potente. Esto pondría en riesgo desde correos electrónicos hasta infraestructuras críticas.

La criptografía post-cuántica (PQC) surge como respuesta: un conjunto de algoritmos diseñados para resistir ataques cuánticos. Se basan en problemas matemáticos que, incluso para un ordenador cuántico, siguen siendo difíciles, como los sistemas de retículos, códigos de corrección de errores, funciones hash o isogenias de curvas elípticas.



Placa para caracterización de chips que implementan primitivas criptográficas diseñados por el IMSE. / CARLOS ORTIZ-CSIC

La PQC no depende de principios cuánticos, sino de estructuras matemáticas resistentes a la computación cuántica. Entre los algoritmos más prometedores se encuentran Kyber: basado en retículos, para cifrado de clave pública; Dilithium: también basado en retículos, para firmas digitales; Classic McEliece: basado en códigos de corrección de errores y SPHINCS+, basado en funciones hash, para firmas digitales. Y estos algoritmos están siendo evaluados por organismos internacionales como el NIST (National Institute of Standards and Technology), de EEUU, que lidera un proceso de estandarización para definir los futuros estándares criptográficos post-cuánticos.

¿Qué es QKD y por qué necesita identidades robustas?

La distribución cuántica de claves (QKD, por sus siglas en inglés) permite compartir claves criptográficas entre dos partes de forma segura, utilizando propiedades de la mecánica cuántica. Si un tercero intenta interceptar la clave, el sistema lo detecta automáticamente, gracias al principio de no clonación y al colapso de la función de onda.

Sin embargo, QKD no es invulnerable. Aunque la clave se transmite de forma segura, los dispositivos emisores y receptores pueden ser atacados. Aquí entra en juego la necesidad de identidades digitales robustas: sistemas que permitan verificar que los transmisores y receptores son quienes dicen ser, y que no han sido suplantados.

"Estamos trabajando en la generación de identidades digitales robustas para aumentar la seguridad de los transmisores y receptores QKD en el ámbito de las comunicaciones cuánticas y para el desarrollo de sistemas de procesado basados en criptografía post-cuántica (PQC) para que las comunicaciones cuánticas sean resilientes frente a futuros ataques realizados desde ordenadores cuánticos", explica **Macarena Martínez**.

El proyecto del IMSE-CSIC: ciencia aplicada a la seguridad cuántica

Desde el Instituto de Microelectrónica de Sevilla, Macarena Martínez y Piedad Brox lideran la participación de este instituto en un proyecto pionero que combina QKD, PQC y fotónica integrada para construir sistemas de comunicación cuántica seguros y escalables. El proyecto se articula en torno a dos líneas principales: generación de identidades digitales robustas: mediante sistemas ópticos avanzados, se crean huellas digitales únicas que permiten autenticar dispositivos QKD, y procesado seguro con algoritmos PQC: se desarrollan sistemas electrónicos que integran algoritmos resistentes a ataques cuánticos, garantizando la confidencialidad y autenticidad de la información.

Ambas líneas convergen en un objetivo común: construir infraestructuras de comunicación cuántica seguras, escalables y adaptables.

La investigadora Macarena Martínez, del Instituto de Microelectrónica de Sevilla. / CARLOS ORTIZ-CSIC

Una de las innovaciones más prometedoras del proyecto es la incorporación de fotónica integrada para generar identidades digitales robustas, dado que esta tecnología permite implementar sistemas ópticos avanzados directamente en chips, reduciendo costes y aumentando la eficiencia.

El proyecto CryptoPIC (Seguridad avanzada en chips de fotónica integrada) explora esta vía. Está financiado por un Proyecto de Generación de Conocimiento coordinado entre los Institutos de Microelectrónica de Barcelona y Sevilla, y busca integrar soluciones de seguridad en el propio hardware, desde el diseño.

"Los matemáticos piensan y crean un algoritmo; hay gente que piensa cómo atacarlos y los diseñadores microelectrónicos tenemos que ir pensando en desarrollar sistemas digitales que integren todos estos avances. La dificultad radica en que el diseño debe ser modular para adoptar criptoagilidad, es decir, estos sistemas deben adaptarse para que podamos incorporar cambios que los hagan más robustos", señala Piedad Brox.

De esta forma, comprendemos un término clave: la criptoagilidad, que es la capacidad de un sistema para adaptarse rápidamente a nuevos algoritmos criptográficos. En un entorno cambiante, donde las amenazas evolucionan, esta flexibilidad es esencial.

Divulgación para concienciar

"Uno tendría que traducir al mundo digital lo que hace uno con su propia casa, no dejar las puertas abiertas... Hay que ser responsable con la información que uno maneja", advierte Macarena Martínez. "No hay que transmitir miedo, sino que hay que seguir las precauciones para no ir revelando información que no nos interesa".

La divulgación científica tiene aquí un papel clave: explicar los riesgos sin generar pánico, y mostrar cómo la investigación trabaja para protegernos.

La seguridad cuántica no es solo una cuestión técnica. Tiene implicaciones profundas en la privacidad, la soberanía tecnológica y la confianza digital. ¿Quién controla las infraestructuras cuánticas? ¿Cómo se garantiza que los sistemas sean auditables y transparentes? ¿Qué papel juegan los organismos públicos en la protección de los ciudadanos? El trabajo del CSIC, y en particular del IMSE, se inscribe en una visión de ciencia pública, colaborativa y orientada al bien común. La participación en proyectos europeos y nacionales garantiza que el conocimiento generado se traduzca en soluciones accesibles, auditables y éticas.

El trabajo de Macarena Martínez y Piedad Brox en el IMSE-CSIC es un ejemplo de cómo la ciencia española se anticipa a los retos del futuro. En un mundo donde la seguridad digital será cada vez más crítica, sus investigaciones son una apuesta por la resiliencia, la innovación y la confianza. "Esperamos que algunas de las cosas que estamos haciendo hoy sean una realidad dentro de diez años, que los productos futuros de comunicaciones cuánticas serán más rápidos y más seguros", concluye Macarena.

Ciencia Digital: una apuesta estratégica del CSIC

La investigación en criptografía post-cuántica y comunicaciones seguras no ocurre en el vacío. Forma parte de una apuesta más amplia del CSIC por la transformación digital de la ciencia, articulada a través de iniciativas como la Plataforma Temática Interdisciplinar (PTI) Ciencia Digital.

Esta plataforma, impulsada por el CSIC, busca acelerar la adopción de tecnologías digitales en todos los ámbitos de la investigación científica. Desde la inteligencia artificial hasta la computación de alto rendimiento, pasando por la gestión de datos FAIR y la ciberseguridad, la PTI Ciencia Digital promueve una ciencia más conectada, reproducible y abierta.

En este marco, el desarrollo de sistemas criptográficos seguros y resilientes es una prioridad. La protección de datos científicos, la autenticación de dispositivos en redes de sensores, y la integridad de las comunicaciones entre centros de investigación son elementos clave para garantizar la confianza en la infraestructura digital de la ciencia.

Los proyectos liderados por Macarena Martínez y Piedad Brox en el IMSE-CSIC se alinean con estos objetivos. No solo contribuyen al avance de la criptografía post-cuántica, sino que proponen soluciones concretas para proteger las futuras redes de comunicación científica, especialmente aquellas basadas en tecnologías cuánticas.

Además, la colaboración entre institutos del CSIC, como Sevilla y Barcelona en el proyecto CryptoPIC, refleja el espíritu interdisciplinar y cooperativo que impulsa la PTI Ciencia Digital. La integración de fotónica, electrónica, matemáticas y teoría de la información en un mismo proyecto es ejemplo de cómo la ciencia digital requiere nuevas formas de trabajo colaborativo.

Infraestructuras seguras para una ciencia conectada

En un contexto donde los datos científicos se generan, comparten y analizan a escala global, la seguridad digital se convierte en una infraestructura crítica. La posibilidad de que un ataque comprometa resultados, manipule datos o interrumpa comunicaciones entre laboratorios es una amenaza real.

Por eso, el CSIC apuesta por una ciencia conectada pero segura, donde las tecnologías digitales se desarrollan con criterios de robustez, auditabilidad y resiliencia. La criptografía post-cuántica y la QKD no son solo herramientas para proteger bancos o gobiernos: son también tecnologías clave para proteger la ciencia misma.

El trabajo del IMSE-CSIC contribuye a esta visión, desarrollando soluciones que podrían aplicarse en redes científicas, sistemas de control industrial, dispositivos médicos y comunicaciones críticas. La incorporación de identidades digitales robustas y procesado seguro en chips fotónicos abre la puerta a una nueva generación de dispositivos científicos seguros desde el diseño.

La investigadora Piedad Brox, del Instituto de Microelectrónica de Sevilla. / CARLOS ORTIZ-CSIC

El CSIC y el Hub Nacional de Excelencia en Comunicaciones Cuánticas

En abril de 2025, el Ministerio para la Transformación Digital y de la Función Pública aprobó el Real Decreto 317/2025, que regula la concesión directa de subvenciones a entidades de referencia en el ámbito de las comunicaciones cuánticas. El objetivo: fomentar la colaboración científica en el marco de la Estrategia Nacional de Inteligencia Artificial, dentro del Plan de Recuperación, Transformación y Resiliencia, financiado por la Unión Europea-Next Generation EU.
El CSIC participa activamente en el Hub Nacional de Excelencia de Comunicaciones Cuánticas, y el Instituto de Microelectrónica de Sevilla es uno de sus nodos clave. La colaboración entre centros, universidades y empresas busca acelerar el desarrollo de tecnologías cuánticas seguras, con impacto en sectores como defensa, banca, salud y telecomunicaciones.