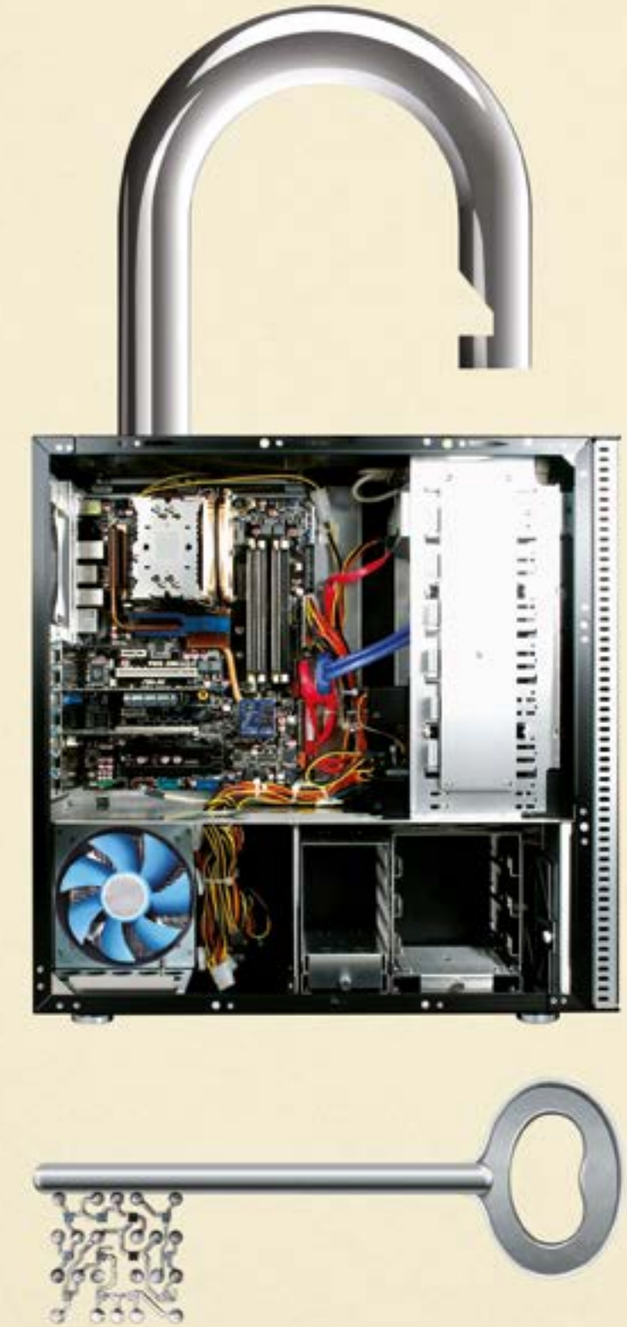
¡CONTRARRELOJ!

TEXTO:
PINO CABALLERO GIL, DANIEL ESCÁNEZ EXPÓSITO, JORGE GARCÍA DÍAZ
ILUSTRACIÓN:
SEAN MACKAOUI

Nuestros secretos podrían quedar expuestos en cuanto aparezcan los primeros ordenadores cuánticos de gran potencia. Esta es la carrera contrarreloj que hoy libran las personas expertas en criptografía por la ciberseguridad en la era cuántica.



Hace pasado 30 años desde que la coautora de este artículo publicó el primer libro en español dedicado íntegramente a la criptografía: *Introducción a la criptografía* (Editorial Ra-Ma, 1996). En aquel momento todo era nuevo, y la seguridad de la información, una disciplina exótica incluso en el entorno académico, invisible para el gran público. Por eso, un libro que llevaba en su título la palabra "criptografía" solo podía entenderse como un tratado sobre mensajes secretos del más allá. Aquella obra pionera, llena de algoritmos matemáticos, se mostraba en muchas librerías en las estanterías dedicadas a los fenómenos paranormales. Resulta paradójico que, tres décadas después, esa materia se haya convertido en el pilar que sostiene nuestra civilización digital.

Hoy, la seguridad *online* es tan importante como la seguridad a pie de calle. Los sistemas criptográficos consiguen sostener el sistema en una trepidante carrera contra quienes, a veces, consiguen hackearlos. Pero... ¿y en el futuro? La computación cuántica que se avecina, con un alcance casi ilimitado, ¿reforzará la seguridad o la pondrá en riesgo?

"Cambiar todas nuestras tecnologías hacia una criptografía resistente a la computación cuántica representa una de las mayores transformaciones de infraestructura en la historia de la ciberseguridad moderna"

Asistimos, de nuevo, a una revolución en materia de ciberseguridad. Nos enfrentamos al auge de aquello que, hasta hace apenas una década, se consideraba casi ciencia ficción: la computación cuántica.

EL OCASO DE LA CRIPTOGRAFÍA ACTUAL

Imaginemos que la seguridad de casi todas nuestras comunicaciones, ya sean bancarias, por Internet, correo electrónico, Internet de las cosas, tarjetas inteligentes, etc., dejara de ser segura de repente. El caos generado sería de dimensiones colosales. Eso podría fácilmente ocurrir dentro de unos pocos años si no se sustituyen urgentemente los dos algoritmos criptográficos más utilizados en todas las tecnologías actuales: el llamado RSA (siglas de Rivest, Shamir y Adleman, sus inventores) y los basados en curvas elípticas. En ambos casos, el funcionamiento se basa en dos claves: una pública y otra privada, conectadas mediante una función matemática unidireccional. Con la clave privada es muy fácil crear la clave pública, pero extremadamente difícil hacer lo contrario: conseguir la clave privada a partir de la pública. Esa dificultad se debe a que requiere resolver un problema matemático difícil, lo que hace que la contraseña sea segura.

Sin embargo, cuando haya un ordenador cuántico con capacidad suficiente para resolver esos problemas difíciles en poco tiempo, estaremos en peligro. Y ya existen los algoritmos cuánticos necesarios para comprometer la base de la criptografía de clave pública actual. Uno de ellos es el algoritmo de Shor.

Shor tiene la habilidad de encontrar patrones ocultos en los números. Esto le permite resolver los problemas de la factorización y del logaritmo discreto en los que se basa RSA, o los basados en curvas elípticas. Su viabilidad contra los algoritmos criptográficos de clave pública actuales está supeditada a desarrollos en la computación cuántica que aún no están del todo conseguidos. Es decir, ya existe el algoritmo, ahora falta la máquina. Hay dos obstáculos críticos: el número de cúbits y el control de la decoherencia cuántica. Esta última destruye la superposición antes de completar el cómputo, corrompiendo el resultado.

Uno de los chips cuánticos más potentes hoy en día tiene poco más de 1 100 cúbits físicos (con ruido y errores). Sin embargo, aunque teóricamente bastarían unos pocos miles de cúbits lógicos (sin ruido ni errores) para romper el cifrado RSA con 2 048 bits de clave, la fragilidad de los sistemas cuánticos actuales eleva la cifra necesaria hasta cientos de miles de cúbits físicos. Romper la criptografía elíptica con 256 bits de clave requiere un tercio de los recursos cuánticos necesarios para romper RSA-2048, pero tampoco es viable hoy en día.

Si el algoritmo de Shor compromete la criptografía de clave pública, otro algoritmo cuántico, el algoritmo de Grover (1996), puede utilizarse para poner a prueba la criptografía de clave secreta.

GROVER Y LA CLAVE SECRETA

En este tipo de criptografía, los participantes usan la misma clave secreta para cifrar y descifrar los mensajes. De hecho, el actual estándar de cifrado simétrico, presente en multitud de tecnologías, es el algoritmo AES (Advanced Encryption Standard).

El algoritmo de Grover es, en esencia, un algoritmo cuántico de fuerza bruta. Mientras que un ordenador clásico tendría que probar una a una cada posibilidad de clave secreta para intentar encontrar la correcta, el algoritmo de Grover se aprovecha de la superposición cuántica y el entrelazamiento entre cúbits para descubrir la clave de una manera mucho más rápida.

Sin embargo, la protección contra el algoritmo de Grover es muy sencilla: basta con duplicar el tamaño de la clave, sin necesidad de cambiar el algoritmo de cifrado. Por el contrario, el algoritmo de Shor nos obliga a buscar alternativas matemáticas completamente nuevas, que fundamentan la criptografía postcuántica.

Aunque todavía no existen ordenadores cuánticos suficientemente potentes como para ejecutar los algoritmos de Shor y Grover contra los tamaños de claves criptográficas actuales, ya podemos afirmar que no estamos a salvo, pues se están interceptando y almacenando datos cifrados con la intención de descifrarlos cuando exista un ordenador cuántico capaz de vulnerar esos sistemas criptográficos. Este tipo de estrategia se conoce como "*Harvest Now, Decrypt Later*".

EL ALGORITMO DE SHOR

tiene la habilidad de encontrar patrones ocultos en los números. Esto le permite resolver los problemas de la factorización y del logaritmo discreto en los que se basa RSA, o los basados en curvas elípticas.

EL ALGORITMO DE GROVER

se aprovecha de la superposición cuántica y el entrelazamiento entre cúbits para descubrir la clave de una manera mucho más rápida.

Ya existen los algoritmos cuánticos necesarios para comprometer la base de la criptografía de clave pública secreta actual.

Si seguimos utilizando criptografía que no está preparada para resistir ataques cuánticos, nuestros secretos actuales serán descubiertos en cuanto aparezcan los primeros ordenadores cuánticos de gran potencia.

TRANSICIÓN POSTCUÁNTICA

Cambiar todas nuestras tecnologías hacia una criptografía resistente a la computación cuántica representa una de las mayores transformaciones de infraestructura en la historia de la ciberseguridad moderna. Este movimiento global busca proteger nuestras comunicaciones digitales frente a la amenaza cuántica. Para lograrlo, pueden adoptarse tres enfoques: utilizar exclusivamente computación clásica, emplear tecnologías cuánticas o combinar ambas. En el primer caso hablamos de criptografía postcuántica; en el segundo, de criptografía cuántica; y en el tercero, de criptografía híbrida cuántica.

Para anticiparse al escenario de vulnerabilidad que plantea la computación cuántica, el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST, por sus siglas en inglés) inició en 2016 un proceso de estandarización sin precedentes para seleccionar los algoritmos de criptografía postcuántica que protegerán nuestras infraestructuras digitales en las próximas décadas.

Tras años de evaluación y escrutinio, y un concurso científico internacional, en agosto de ▶

QML es una disciplina que fusiona la computación cuántica con el aprendizaje automático clásico para procesar grandes cantidades de información.

2024 publicó los primeros estándares oficiales de criptografía postcuántica (National Institute of Standards and Technology, 2025).

La seguridad de los algoritmos estándares postcuánticos se fundamenta en que, aunque están diseñados para ejecutarse en ordenadores clásicos, se basan en problemas matemáticos que, según el conocimiento actual, resisten tanto ataques clásicos como cuánticos.

El núcleo de esta nueva generación de algoritmos se apoya principalmente en la criptografía basada en retículos. Los estándares ML-KEM (derivado de CRYSTALS-Kyber) para el cifrado y ML-DSA (derivado de CRYSTALS-Dilithium) para firmas digitales sustituyen los problemas numéricos tradicionales de la factorización y el logaritmo discreto por estructuras geométricas en espacios de cientos o miles de dimensiones. Mientras que los ordenadores cuánticos destacan en la búsqueda de periodicidades numéricas, no se conoce actualmente ningún algoritmo cuántico o clásico eficiente capaz de resolver estos problemas de retículos de alta dimensión.

Sin embargo, la adopción de estos estándares plantea retos técnicos significativos. Las claves y firmas postcuánticas suelen ser considerablemente más grandes que las clásicas, lo que obliga a actualizar protocolos de red y optimizar el almacenamiento. No obstante, la publicación de estos estándares en 2024 marcó el inicio de la era de la llamada criptoagilidad o capacidad de actualizar rápidamente los sistemas criptográficos ante nuevos avances científicos.

ESCUDO CUÁNTICO

Si la computación cuántica está llamada a ser el arma definitiva para vulnerar los sistemas de cifrado actuales, resulta natural y necesario buscar en las mismas leyes de la física una línea de defensa. La distribución cuántica de claves (QKD, por sus siglas en inglés) se alza como una de las aplicaciones más maduras y prometedoras de las tecnologías cuánticas aplicadas a la ciberseguridad. Es un método de comunicación cuántica que permite a dos partes generar de forma segura una clave secreta compartida y aleatoria. La QKD aprovecha las leyes de la mecánica cuántica para establecer las bases de una seguridad teórica perfecta garantizando que cualquier intento de interceptación sea físicamente detectable debido a la perturbación de un sistema al ser medido y al teorema de no clonación.

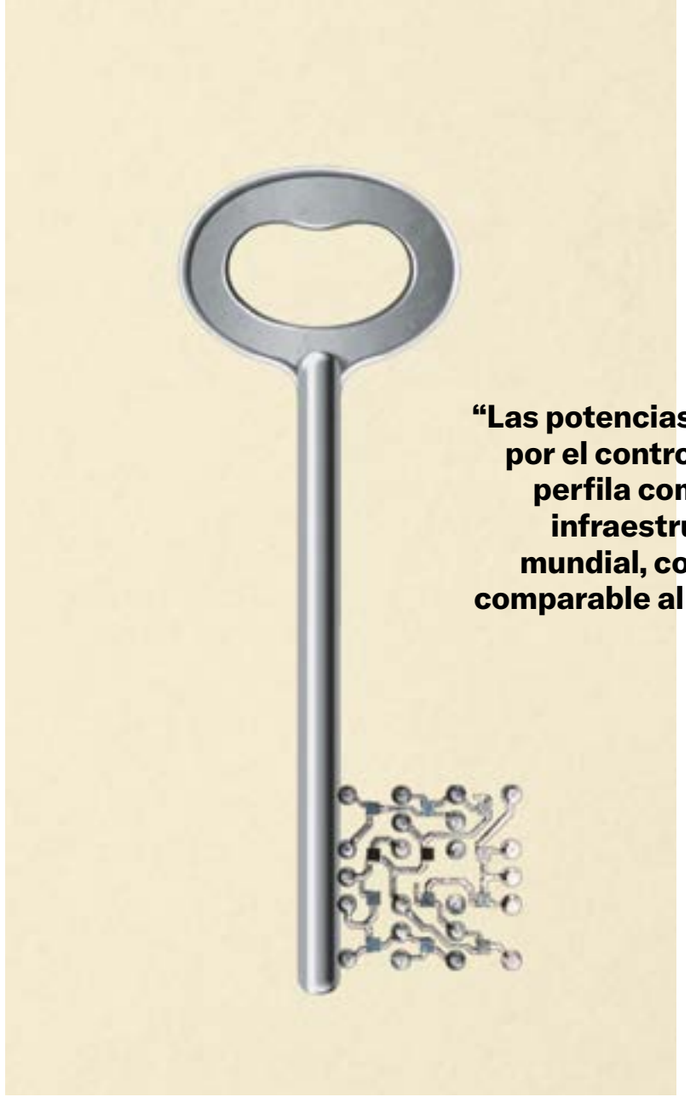
Sin embargo, el despliegue de la QKD a escala global se enfrenta a desafíos prácticos, como los elevados costes de implementación, las limitaciones de alcance físico de la fibra óptica y la compleja integración con las infraestructuras de red ya existentes.

Este escenario ha impulsado el desarrollo de arquitecturas híbridas bajo el paradigma de la criptoagilidad, que permite combinar criptografía tradicional (como el actual estándar AES), criptografía postcuántica (como los estándares postcuánticos del NIST) y criptografía cuántica basada en QKD allí donde sea viable. Esta simbiosis dota a las organizaciones de una resiliencia tecnológica que evita la dependencia exclusiva de una única solución emergente.

“La computación cuántica está llamada a ser el arma definitiva para vulnerar los sistemas de cifrado actuales. Resulta natural y necesario buscar en las mismas leyes de la física una línea de defensa”

En estos días, el catálogo de criptografías primitivas se extiende hacia protocolos que aseguran la identidad y consiguen niveles de eficiencia impensables con la criptografía tradicional.

Entre ellos destacan las firmas digitales cuánticas, que garantizan la autenticidad y no repudio de los mensajes mediante las leyes de la física. Las pruebas cuánticas de conocimiento nulo y la autenticación cuántica de identidad ofrecen soluciones robustas y seguras para autenticar la identidad sin revelar ningún tipo de información sobre la clave privada del usuario. Por último, una de las fronteras más prometedoras es el bloqueo de datos cuánticos, que permite proteger volúmenes masivos de información mediante claves extremadamente cortas. Estas son las soluciones en las que trabajamos. A día de hoy, completan un ecosistema donde la física blinda las comunicaciones futuras.



En paralelo, trabajamos en el aprendizaje automático cuántico (QML, *Quantum Machine Learning*). El QML es una disciplina que fusiona la computación cuántica con el aprendizaje automático clásico para procesar grandes cantidades de información. Aunque todavía se encuentra en una fase exploratoria, estos modelos podrían identificar patrones de amenaza que resultan invisibles para la inteligencia artificial clásica.

Finalmente, dado que el mantenimiento de *hardware* cuántico propio es extremadamente costoso y complejo, la computación cuántica en la nube se ha consolidado como la forma más práctica y eficiente de acceder a estos recursos. Este modelo democratiza el uso de procesadores cuánticos reales sin necesidad de grandes inversiones en infraestructura física. Esto favorece el prototipado rápido de nuevas soluciones de seguridad y fomenta una investigación colaborativa global, indispensable para anticiparse a los ataques.

“Las potencias ya compiten por el control de lo que se perfila como la próxima infraestructura crítica mundial, con un impacto comparable al del petróleo”

GEOPOLÍTICA DE LA CUÁNTICA

La investigación en cuántica ha dejado de ser un nicho académico para transformarse en un asunto estratégico que redefinirá el poder mundial en el siglo XXI. Las potencias ya compiten por el control de lo que se perfila como la próxima infraestructura crítica mundial, con un impacto comparable al del petróleo.

Estados Unidos y China lideran esta carrera cuántica. El ecosistema estadounidense se basa en una simbiosis descentralizada entre respaldo estatal y sector privado. Gigantes como IBM, Google y Microsoft lideran la inversión, dominando el panorama de las patentes en *software* y *hardware* cuántico.

China, por el contrario, se enfoca hacia una estrategia centralizada y sin inversión privada, aunque con niveles de inversión pública que superan a los de Estados Unidos. Apuesta por la computación cuántica y ha tomado la delantera en comunicaciones cuánticas seguras mediante satélites, una ventaja decisiva en ciberdefensa y espionaje.

Europa, pese a su excelencia académica y programas como la Estrategia de la Europa Cuántica (Comisión Europea, 2025), se enfrenta a la fragmentación de sus mercados y a un menor flujo de capital privado.

La hegemonía cuántica representa una carrera hacia una nueva forma de poder. La nación que domine su tecnología y aplicaciones tendrá una capacidad de influencia sin precedentes. La soberanía cuántica será un factor determinante en las alianzas y conflictos internacionales del futuro.