Criptografía en la era cuántica

GMV
INNOVATING SOLUTIONS

Criptografía en la era cuántica

La computación cuántica promete revolucionar la tecnología en los próximos años, cuando alcance potencia y fiabilidad suficientes. Su promesa se debe a que esta nueva tecnología ofrecerá una nueva manera de abordar ciertos problemas que actualmente son intratables por la computación clásica. Este gran avance, que supondrá un antes y un después en diversas disciplinas científicas, también pondrá en jaque la seguridad de nuestra información.

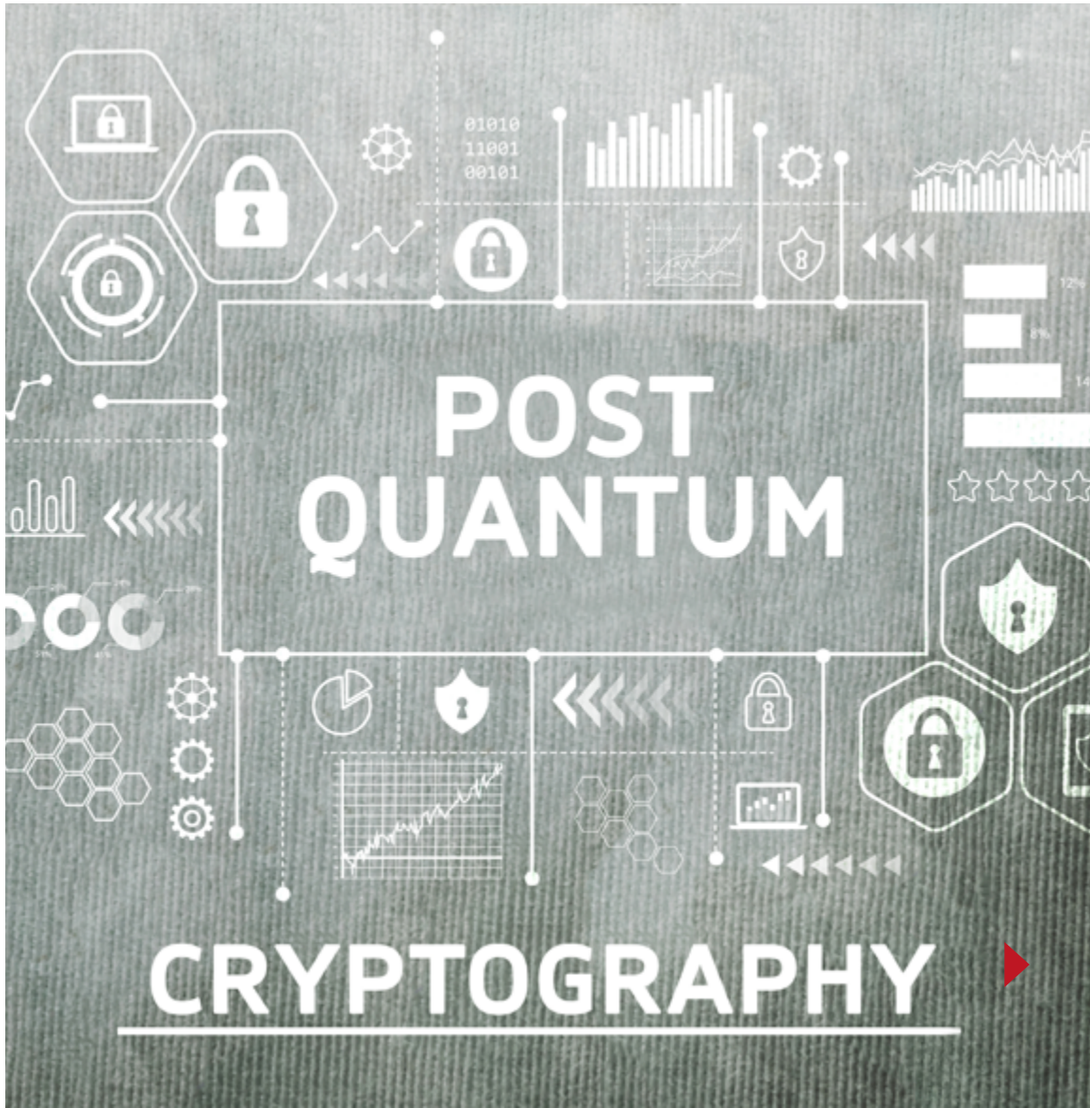
La criptografía actual se basa en algoritmos cuya fortaleza depende de la complejidad computacional de la operación inversa, que requeriría a un atacante con los ordenadores actuales y con los mejores ataques conocidos, millones de años en romper su seguridad. Los algoritmos más habituales se basan en la factorización de números primos o logaritmos discretos en grupos cíclicos, como es el caso de RSA y Diffie-Hellman, respectivamente. Sin embargo, se estima que el algoritmo cuántico de Shor y la búsqueda de Grover romperán estas claves criptográficas en cuestión de segundos, o las debilitarán sustancialmente.

Para proteger la información frente a estos futuros ataques surgen dos posibles soluciones:

La criptografía post-cuántica se basa en problemas matemáticos distintos y más complejos de los que plantea la criptografía actual implementables en hardware clásico, y que se piensa que son difíciles de resolver tanto para un ordenador convencional como uno cuántico.

La criptografía cuántica, y, en concreto, la distribución de claves cuánticas, consiste en distribuir la clave entre dos personas a través de un canal (fibra óptica, o aire), utilizando varios principios de la física cuántica para asegurar que la clave no es interceptada por un tercero, y que en caso de que se intente, el emisor/receptor puedan detectarlo.

Estas soluciones son muy distintas, pero no por ello excluyentes, por lo que en el futuro, se plantea emplear una combinación de ambas soluciones para conseguir la máxima seguridad posible.



EL CONCURSO DEL NIST PARA LOS ESTÁNDARES DE CRIPTOGRAFÍA POST-CUÁNTICA

IGNACIO LUENGO
Catedrático de Álgebra de la Universidad Complutense de Madrid e investigador del ICMAT, y uno de los pocos españoles en participar en el proceso de estandarización del NIST.

Ignacio Luengo, catedrático de Álgebra de la Universidad Complutense de Madrid e investigador del ICMAT

El Instituto Nacional de Estándares y Tecnología Americano (NIST) creó un grupo de trabajo sobre criptografía post-cuántica (PQC) en 2012, motivado por los avances de la computación cuántica y las amenazas que dicho avance suponen para las TIC. En 2016 el NIST, siguiendo indicaciones de la Agencia Nacional de Seguridad Americana (NSA) (2015), lanzó un concurso abierto para la selección de estándares de criptografía post-cuántica en dos categorías: firma digital (DS) y cifrado e intercambio de claves (PKE/KEM). Este concurso transparente y abierto buscaba la colaboración y el consenso de todos los sectores académicos e industriales involucrados. El NIST advirtió, que al contrario de otros concursos recientes (AES/SHA-3), en este caso se espera que sean elegidos varios estándares de varias tecnologías, en parte por las dificultades técnicas y también por la necesidad de prever futuros ataques cuánticos a las diferentes tecnologías.

El concurso se cerró en noviembre de 2017, y pasaron a la primera ronda 69 propuestas. Las tecnologías matemáticas o algoritmos usados en estas propuestas fueron: retículos (26), códigos correctores de errores (22), multivariable (19) y 10 de otras varias (hash, isogenias...). En julio de 2020 el NIST anunció los 7 candidatos que pasaban a la fase final (5 basados en retículos, 1 de códigos y 1 multivariable) más otros 8 candidatos de reserva. Se espera que los ganadores se anuncien entre 2023 y 2025.

El proceso incluye tres conferencias de estandarizacion. La primera tuvo lugar en Fort Lauderdale en abril de 2018 y en ella se presentaron las propuestas que pasaron la primera ronda, entre ellas la de Ignacio Luengo: El criptosistema post-cuántico DME (Double Matrix Exponentiation). La segunda conferencia fue en Santa Bárbara (California) y se centró en los candidatos que pasaron a la segunda ronda, las prestaciones de los candidatos y las perspectivas y necesidades de las TIC con participación de las principales empresas del sector: Amazon, IBM, Cisco, Microsoft...

En la evaluación de la seguridad y las prestaciones de los candidatos participan cientos de investigadores de universidades y empresas a

“El período de transición a la criptografía post-cuántica no está definido todavía, a la espera de la elección de los estándares por el NIST y otros organismos, pero no hay duda de que los algoritmos elegidos proporcionarán un nivel de seguridad y confianza muy bueno”

IGNACIO LUENGO, CATEDRÁTICO DE ÁLGEBRA DE LA UNIVERSIDAD COMPLUTENSE DE MADRID E INVESTIGADOR DEL ICMAT

través del foro del NIST, que cuenta con unos 1.300 miembros. En este foro se recogen las aportaciones, sugerencias e ideas sobre el proceso y las necesidades de las empresas según los diferentes usos. Por ejemplo, hay un consenso en que no hay necesidad de terminar el proceso rápidamente y sobre cómo debe de ser el proceso de transición de los esquemas actuales a los post-cuánticos. En general el NIST acepta las sugerencias sobre las que hay consenso. También se discuten cuáles pueden ser los puntos fuertes y débiles de cada propuesta. Por ejemplo, se prevé que para el despliegue de estos sistemas va a ser más crítico el uso del ancho de banda que la potencia de cálculo. Una de las dificultades del proceso de selección es que no existe una “bala de plata” o ganador claro. Cada tecnología o algoritmo tiene sus ventajas e inconvenientes (el que es más seguro tiene el inconveniente de un gran tamaño de clave, o el que es más rápido es menos seguro). Hay que decir que todos los algoritmos son seguros, y al decir más seguros significa que lleva más tiempo publicado y hay más confianza en su seguridad. Por ejemplo, los esquemas basados en códigos llevan 40 años siendo estudiados y resisten a los ataques, pero tienen un tamaño de clave casi prohibitivo.

En este proceso de búsqueda de estándares seguros contra ordenadores cuánticos participan otros organismos y comités de estándares, la mayoría de los cuales hacen su trabajo en coordinación con el concurso del NIST. Entre los organismos sectoriales destacamos el ISO a través del grupo ISO7IEC JTC 1/SC 27 “Information security, Cybersecurity and privacy protection”, el grupo ITU-T SC 17, el grupo IETF (Internet protocols, TLS, TCP...) o el grupo X9 (Financial Industry Standards). A nivel europeo el ETSI, que es uno de los institutos de estandarización reconocidos por la Union Europea, fundó en 2015 un grupo de especificaciones industriales conocido como TC Cyber Working Group for Quantum-Safe Cryptography. También ENISA, la agencia de ciberseguridad de la UE, está involucrada en el proceso de transición hacia la criptografía post-cuántica. China por su parte ha lanzado su propio concurso abierto para la elección de los estándares post-cuánticos, a través de la Chinese Association for Cryptographic Research (CACR) a la que se han presentado 38 candidatos. Respecto a la transición hacia estándares seguros aparte de los EEUU hay muchos países que tienen grupos trabajando a nivel nacional para desarrollar e implementar las estrategias de transición (Canadá, Francia, Alemania, Reino Unido y Suiza, entre otros). En España no hemos empezado todavía a ocuparnos a nivel nacional de la seguridad post-cuántica, por lo que iniciativas de divulgación como esta, promovida por GMV, son muy loables y necesarias.

El período de transición a la criptografía post-cuántica no está definido todavía, a la espera de la elección de los estándares por el NIST y otros organismos, pero no hay duda de que los algoritmos elegidos proporcionarán un nivel de seguridad y confianza muy bueno, debido a la experiencia y a la cantidad de trabajo empleada por los agentes involucrados.

CLAVES DEL ÉXITO DE UNA MIGRACIÓN CRIPTOGRÁFICA

ENRIQUE CRESPO
Responsable de Ciberseguridad del SKMF (Satelite Key Management Facility) de Galileo en GMV, grupo empresarial español con presencia internacional. Es experto en ciberseguridad y telecomunicaciones y trabaja como integrador de soluciones post-cuánticas en entornos críticos.

Enrique Crespo, responsable de ciberseguridad del SKMF de Galileo en GMV

Las actualizaciones de sistemas complejos con varios niveles de relación siempre son complejas. Si estas actualizaciones se centran en elementos criptográficos, se añaden unos elementos adicionales, algunos de los cuales no son obvios ni evidentes.

Aunque no es el único factor a tener en cuenta, la complejidad de los procesos de migración criptográfica está directamente relacionada con el propio diseño de la **Arquitectura Criptográfica**. Si las aplicaciones y sistemas llevan embebidos la lógica criptográfica, cualquier migración tendrá un coste alto porque habrá que llevarla a cabo aplicación por aplicación y sin una visión unificada de arquitectura criptográfica. Si la función criptográfica está correctamente aislada, siempre será más fácil llevar a cabo actuaciones mejor localizadas y que faciliten escenarios de transición. Por ello, entender que los activos criptográficos necesitan de gestión, tienen un ciclo de vida y una gestión específica relacionada con los activos que protegen, y están al servicio de la misión de negocio de la organización, es esencial para ejecutar con criterio cualquier actuación de migración criptográfica.

La usabilidad y propósito de los nuevos protocolos, principalmente en PQC, son distintos en varios aspectos de los que estábamos acostumbrados. Asimismo, es interesante reseñar que las implementaciones de los nuevos protocolos y primitivas criptográficas también tendrán su proceso de maduración como es normal en toda implementación tecnológica, y estos procesos no son inmediatos. De cara a una migración efectiva, entender estos condicionantes temporales es fundamental.

Para poder afrontar una migración criptográfica con garantías de éxito, es preciso **anticipar, analizar y entender** el impacto en nuestras aplicaciones y sistemas de una serie de factores, a parte del propio Diseño de la Arquitectura, como son tamaño de claves, tamaño de la información cifrada y firmada, rendimiento de las propias primitivas criptográficas, tamaño de mensajería generada (y en consecuencia ocupación de ancho de banda), normalización y estandarización de los tipos de datos de los nuevos protocolos, y API de consumo para aplicaciones y sistemas.

Además se debe **diseñar y desarrollar una estrategia de transición y convivencia**, ya que estos procesos no son inmediatos y requieren de pasos consolidados que permitan ir desarrollando la estrategia de migración.

“Entender que los activos criptográficos necesitan de gestión, tienen un ciclo de vida y una gestión específica relacionada con los activos que protegen, y están al servicio de la misión de negocio de la organización, es esencial para ejecutar con criterio cualquier actuación de migración criptográfica”

ENRIQUE CRESPO, RESPONSABLE DE CIBERSEGURIDAD DEL SKMF DE GALILEO EN GMV

Aunque se suele hablar poco de los datos que han sido objeto de primitivas criptográficas previas, su gestión es crítica, ya que siguen teniendo necesidades operativas. También es importante que puedan seguir siendo explotables por las aplicaciones en la infraestructura migrada.

En este contexto, todo lo específico al desarrollo técnico de las matemáticas de la PQC no deja de afrontar desafíos adicionales por el necesario proceso de maduración que requerirá. No podemos pensar que 40 años de trabajo de la comunidad científica internacional y la industria pueden equiparse de manera inmediata, si bien es verdad que llevamos muchas lecciones aprendidas que nos permiten avanzar con otra velocidad y mejores pautas.

No hay nada más práctico que una buena teoría, y en tiempos recientes hemos visto que la Ciencia es el medio para solventar situaciones complejas que, desgraciadamente, nos afectan a todos. La criptografía post-cuántica es una alternativa científica asumida como tal en el mundo de la industria y de la academia. Se está aplicando en escenarios y desarrollos concretos que ya son realidad. Estos desarrollos se anticipan a un escenario a corto-medio plazo de actualización criptográfica sin precedentes. Como señalábamos, durante 40 años hemos trabajo sobre unas bases criptográficas que van a transformarse, y, por consiguiente, transformará su ecosistema completo de relación.

EMBARCARSE EN EL VIAJE HACIA LA CRIPTO-AGILIDAD ES DIFÍCIL DE VENDER HASTA QUE ES DEMASIADO TARDE

DIETER BONG
Product manager en Utimaco, fabricante de hardware criptográfico.

Dieter Bong, product manager en Utimaco

No hay certeza sobre cuándo llegará el primer ordenador cuántico suficientemente potente, pero las señales apuntan a que tardará menos de diez años. Grandes jugadores como Google, IBM y Honeywell compiten en la carrera para desarrollar el ordenador cuántico de mayor rendimiento, y China ha anunciado que la computación cuántica va a ser una de sus principales prioridades en su plan a 5 años. Aquellos interesados en explotar esta tecnología de formas dañinas para obtener beneficios políticos o comerciales no tardarán mucho tiempo en aparecer. Si las organizaciones no implantan la **cripto-agilidad** lo antes posible, sus activos criptográficos pueden ser expuestos y convertirse en su talón de Aquiles, ya que los nuevos algoritmos no pueden implementarse simplemente presionando un botón.

La denominada **Evaluación de Riesgo Cuántico** proporciona una buena orientación en el viaje de cada empresa hacia la criptografía post-cuántica. Según Michele Mosca, cofundador del Instituto de Computación Cuántica de la Universidad Canadiense de Waterloo, esta evaluación se puede implementar en cinco pasos:

1. **Establecer un inventario** de activos de información importantes, poniendo foco en los datos sensibles y/o valiosos que requieren protección criptográfica.
2. **Investigar y vigilar** el desarrollo de los ordenadores cuánticos y de la criptografía post-cuántica: actualmente ataque de fuerza bruta.
3. **Identificar atacantes potenciales** y estimar cuándo podrán acceder a tecnologías cuánticas.
4. **Determinar el tiempo de vida** de los activos de información importantes: ¿cuánto tiempo es útil la información crítica? Este tiempo de vida debe contrastarse con el tiempo estimado que llevará actualizar sus sistemas a una infraestructura post-cuántica. También se debe **evaluar la eficacia y adaptabilidad** de los procedimientos criptográficos implementados actualmente, como por ejemplo algoritmos y longitudes de clave.

“Si las organizaciones no implantan la cripto-agilidad lo antes posible, sus activos criptográficos pueden ser expuestos y convertirse en su talón de Aquiles, ya que los nuevos algoritmos no pueden implementarse simplemente presionando un botón”

DIETER BONG, PRODUCT MANAGER EN UTIMACO

5. Planificar la actualización de la infraestructura post-cuántica, y prepararse para su puesta en marcha.

Mientras que el sector privado puede sentir una gran presión para evitar problemas de responsabilidad jurídica (por ejemplo, en el caso de automóviles conectados que se pueden ver comprometidos por su criptografía vulnerable y, por lo tanto, estarían expuestos a tener accidentes causados por hackers), el sector público tiene que lidiar con datos personales muy sensibles que deben mantenerse seguros y confidenciales durante décadas.

Hay varios pasos que se pueden tomar ahora para preparar su negocio para un futuro post-cuántico y evitar riesgos innecesarios. Algunos de los factores importantes de la cripto-agilidad y preguntas clave a plantear al preparar su negocio para un futuro post-cuántico son:

>> Considerar la velocidad de ejecución: cuánto tiempo llevará a su empresa migrar los protocolos de cifrado actuales a un nuevo cifrado post-cuántico. Asegurar de pensar en el futuro y no en el presente: ¿cómo puede proteger sus sistemas durante 20 años o más?

>> Observar el ciclo de vida de su producto: si el ciclo de vida de su producto es mayor a cinco años desde su diseño hasta su comercialización, tiene un problema. Industrias como la automoción, medidores inteligentes, el gobierno, las infraestructuras críticas y la IoT industrial tardan entre 2 y 4 años en diseñar productos que permanecerán en el mercado durante 7 años o más.

>> Planificación de costes: la implementación de firmware post-cuántico o el desarrollo y ejecución de algoritmos post-cuánticos es posible actualmente. Cada algoritmo post-cuántico se comporta de forma distinta y tiene fortalezas específicas, pero no existe un único algoritmo que se adapte a todos los propósitos. Comprender qué algoritmos se adaptan mejor a sus requisitos y qué impacto tendrán en su infraestructura de TI existente requiere tiempo y esfuerzo. Es importante planificar estos costes ahora para ahorrarle a su negocio futuros dolores de cabeza.

CRIPTOGRAFÍA POST-CUÁNTICA: LA SOLUCIÓN A LA AMENAZA CUÁNTICA

LUIS JIMÉNEZ
Subdirector General del Centro Criptológico Nacional (CCN-CNI), que se dedica a proteger la información clasificada y de elaborar y difundir normas y guías para garantizar la seguridad de sistemas TI y comunicaciones del estado. Ha sido uno de los primeros usuarios finales en buscar soluciones post-cuánticas.

Desde hace unos años no se deja de hablar de las tecnologías cuánticas. La publicación de noticias tanto en televisión como en prensa no especializada sobre la supremacía cuántica y el lanzamiento de satélites cuánticos ya no se confunden con escenas de una película de ciencia ficción, y es que, las tecnologías cuánticas han llegado para quedarse.

La carrera por el desarrollo de un ordenador cuántico computacionalmente relevante ha comenzado y grandes empresas como Google, IBM, Microsoft son algunos de los participantes. No debemos de olvidar que China también compite en esta carrera, y que recientemente (Diciembre 2020) ha proclamado su supremacía cuántica al resolver un problema con un ordenador cuántico en poco más de tres minutos, que con un superordenador clásico habría tardado en resolverse 600 millones de años.

La realidad es que la mayoría de nosotros no llegaremos a ver un ordenador cuántico, salvo en fotografías, ya que para que funcione correctamente se debe mantener aislado y a unas temperaturas muy bajas. Solo las empresas que desarrollan los ordenadores cuánticos y las naciones podrán tener acceso a un ordenador cuántico, sin embargo las empresas fabricantes pondrán los servicios cuánticos a disposición de otras empresas, universidades o particulares que quieran contratar las bondades de su computación, como de hecho ya está haciendo alguna de ellas.

Debemos tener en cuenta que no utilizaremos el ordenador cuántico en exclusiva, sino que lo haremos como algo complementario a los ordenadores de sobremesa o supercomputadoras. Cuando un ordenador de sobremesa no sea suficiente para realizar determinados cálculos, emplearemos un superordenador, y cuando con el superordenador no se obtengan resultados, será cuando se utilice el ordenador cuántico.

La llegada de un ordenador cuántico computacionalmente relevante está prevista para dentro de 10 años y tras realizar una inversión en investigación y desarrollo estimada de 1000 millones de euros. Este ordenador supondrá un nuevo reto para la criptografía y para la seguridad de la información, ya que supondrá el final de la criptografía de clave pública y el merme de la seguridad que proporciona el cifrado simétrico y la firma digital.

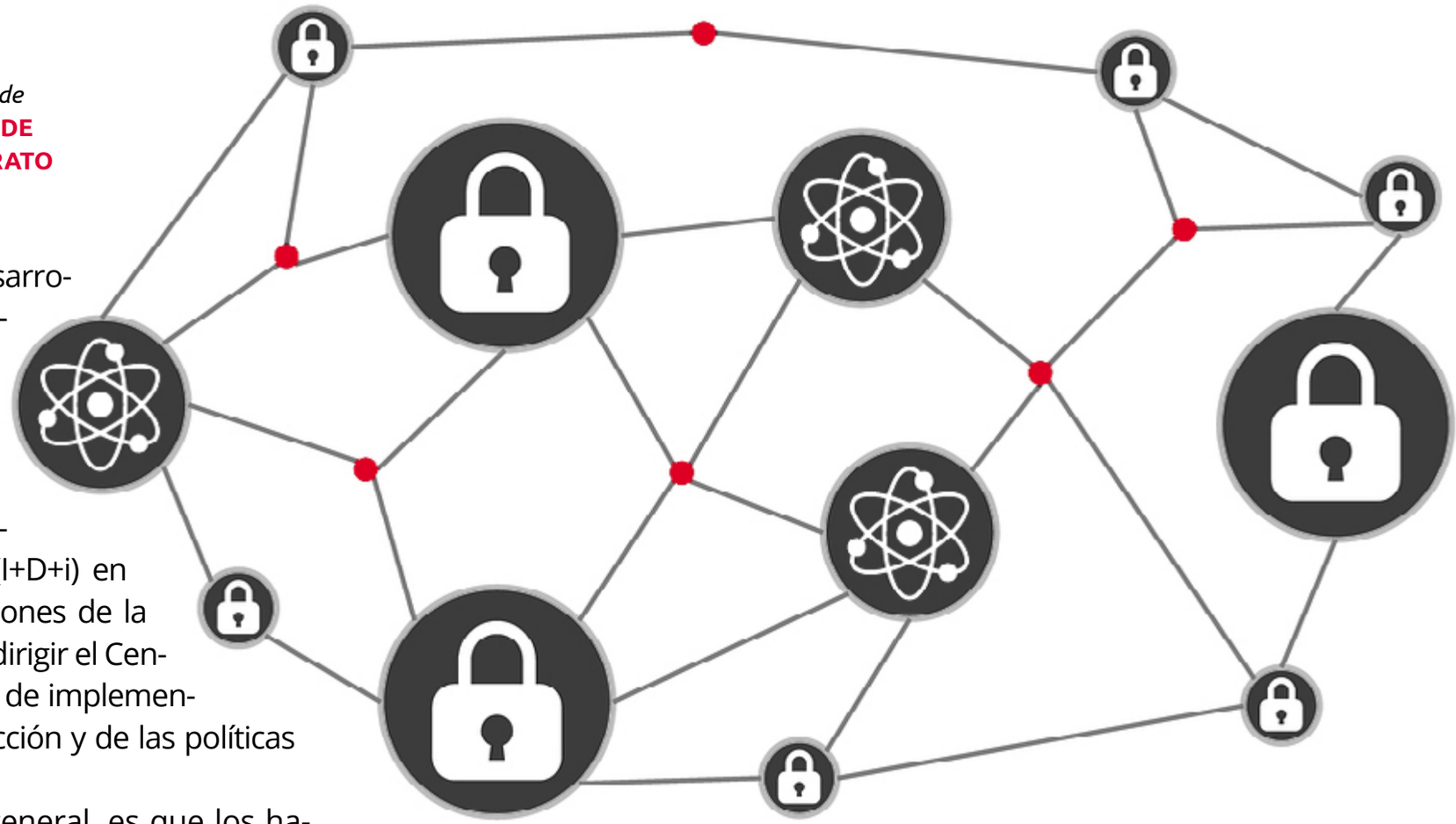
El futuro se aproxima y debemos de estar preparados. Para ello debemos analizar y conocer cuáles son los activos que queremos proteger y durante cuánto tiempo. Aquellos que queramos que sigan protegidos durante más de 10 años, debemos de comenzar a protegerlos empleando cifrados con mayor longitud de clave en el caso de los cifrados simétricos y comenzando a emplear criptografía post-cuántica o sistemas híbridos (criptografía actual + criptografía post-cuántica) en el caso de la firma digital o intercambio de claves, con el objetivo de que la migración sea lo más fluida posible.

Es de vital importancia tanto para la seguridad nacional como para las infraestructuras críticas que se comiencen a identificar los activos al igual que comenzar a tomar las medidas pertinentes para poder estar protegidos. La amenaza cuántica es una realidad y hay que estar preparados.

Aunque el concurso del NIST para escoger los estándares de la criptografía postcuántica (intercambio de claves y firma digital) aún no ha finalizado (está en la tercera ronda), sabemos que hay industria nacional de ciberseguridad que ya ha comenzado a desarrollar implementaciones de los algoritmos que han pasado a la tercera ronda, así como sistemas híbridos. Es fundamental que las empresas de seguridad de la TIC estén preparadas para cuando concluya el concurso del NIST, previsto para 2022-2024, y se decidan los algoritmos post-cuánticos. Hasta que no haya algoritmos ganadores y se publiquen los estándares, habrá que proteger los sistemas/comunicaciones empleando sistemas híbridos.

EL DESARROLLO DE LA CRIPTOGRAFÍA CUÁNTICA, Y EL INTERÉS EN EL ANILLO CUÁNTICO

Secretaría de Estado de Seguridad (Ministerio del Interior)
ENRIQUE BELDA ESPLUGUES, *Subdirector General de Sistemas de Información y comunicaciones para la Seguridad;* **JOSÉ CEBRIÁN DE BARRIO,** *Jefe de la O.P. SIRDEE y Área de I+D+i, y* **SANDRA CERRATO MORENO,** *Jefa de Proyectos de Innovación y Comunicaciones.*



Según el Real Decreto 734/2020 por el que se desarrolla la estructura orgánica del ministerio del Interior, le corresponde a la Subdirección General de Sistemas de Información y Comunicaciones para la Seguridad, entre otras funciones, "Acordar, coordinar, ejecutar y llevar a cabo cualquier otra acción necesaria relativa a la participación en proyectos europeos de investigación, desarrollo e innovación (I+D+i) en materia de seguridad de acuerdo con las instrucciones de la persona titular de la Secretaría de Estado, así como dirigir el Centro Tecnológico de Seguridad (CETSE) como órgano de implementación de las funciones específicas de esta Subdirección y de las políticas de I+D+i del órgano directivo"'.

Uno de los grandes problemas de la física en general, es que los hallazgos teóricos pueden tardar muchísimos años en tener aplicación práctica y muchos más en poder ser integrados en 'aparatos de consumo'. Por ejemplo, la superconductividad es la capacidad de conducir la corriente eléctrica sin resistencia y consecuentemente, sin pérdida de energía. Fue descubierta por K.Onnes en 1911 en el mercurio a unos 4ºK (-269ºC). En 1986 Bednorz y Müller descubrieron los superconductores cerámicos de 'alta temperatura', que funcionan a unos 90ºK (-183ºC). Actualmente se utilizan en los trenes 'maglev', máquinas de resonancia magnética y filtros de radiofrecuencias, pero están muy lejos de poder ser utilizados en 'aparatos de consumo' y han pasado más de 110 años desde su descubrimiento.

El nacimiento de la física cuántica es indeterminado, pero se pueden definir algunos puntos de inflexión: 1900, Max Planck, cualquier radiación de energía pue-

El Anillo cuántico de la Comunidad de Madrid permite demostrar el uso de técnicas QKD en un entorno de producción real, combinando la transmisión de datos y de claves cuánticas sobre la misma fibra, a la vez que demuestra cómo puede llevarse a cabo la gestión de estos servicios, y su uso por diferentes aplicaciones

de ser dividida en elementos de energía discretos; 1926, Schrödinger, ecuación de onda, distribución de la carga de un electrón en el espacio; 1932, Heisenberg, interacción de intercambio; y 20 de marzo de 2021, cuando se publicó que PsiQuantum lanzará el ordenador cuántico comercial antes de 2025.

La mecánica cuántica se utiliza en las placas solares (efecto fotoeléctrico), para realizar imágenes del cuerpo humano (resonancia magnética), en el microscopio de efecto túnel y para los superconductores.

Llevamos tiempo oyendo hablar de los ordenadores cuánticos y de las comunicaciones cuánticas. Ambos tienen dos problemas: la cantidad de datos que queremos 'transmitir' y la posibilidad de que los mismos sean interceptados (ver la comunicación entre Alice y Bob).

Una de las propiedades fundamentales de la física cuántica para realizar comunicaciones es el 'entrelazamiento' o 'fantasmagórico efecto a distancia', lo que permite comunicaciones libres de interferencias, independiente de la distancia y sin medio de transmisión conocido. Al cambiar el estado de una partícula entrelazada, cambia el estado de su partícula pareja de manera automática. En 1926 Einstein dijo refiriéndose a la física cuántica 'Dios no juega a los dados', pues parece que los dados son demasiado sencillos para él.

Por otro lado, tenemos los qbits, basados en la superposición cuántica, esto es 0, 1 o ambos al mismo tiempo, pero si alguien trata de observarlo, tomará uno de los dos valores. Con los bits tenemos una relación 'n' a 'n' resultados, mientras que con los qbits la relación es 'n' a '2n', pudiendo realizar de manera simultánea varias operaciones. En este sentido hay dos naciones (EEUU y China) que están invirtiendo muchísimo esfuerzo y dinero el alcanzar lo que se llama 'la supremacía cuántica'. El procesador 'Sycamore' de Google con 54 qbits ha resuelto operaciones en 200 segundos que el mejor ordenador clásico habría tardado 10.000 años.

A partir de este punto se han estudiado diferentes formas de transmisión, además de la capacidad de un canal cuántico para transmitir estados cuánticos (qbits), la capacidad de un canal cuántico asistido por medios clásicos para transmitir estados cuánticos y la capacidad de transmisión de un canal clásico asistido por el entrelazamiento.

ANILLO CUÁNTICO DE LA COMUNIDAD DE MADRID

El anillo cuántico de la Comunidad de Madrid fue un proyecto que se realizó en 2018 para el que se empleó una infraestructura de fibra proporcionada por Telefónica de España, conectando tres centros diferentes en el área metropolitana de Madrid, junto con equipos de distribución cuántica de claves CV-QKD (desarrollados por los Laboratorios de Investigación de Huawei en Múnich en los que también han colaborado la UPM), instalados en estos centros, además de módulos de gestión (basados en SDN, o Software Defined Networking, y desarrollados por el equipo de Innovación en Tecnologías de Red del GCTIO de Telefónica), y los mecanismos de integración (con tecnologías SDN y NFV desarrollados por la UPM).

La integración de todos estos elementos permite demostrar el uso de técnicas QKD en un entorno de producción real, combinando la trans-

misión de datos y de claves cuánticas sobre la misma fibra, a la vez que demuestra cómo puede llevarse a cabo la gestión de estos servicios, y su uso por diferentes aplicaciones.

La experiencia llevada a cabo se desarrolló sobre una infraestructura en producción y usando los sistemas de comunicaciones desplegados en redes ópticas estándar (destacando a su vez la madurez de esta tecnología), que admite conmutación con enlaces de hasta 60 Km cada uno.

Esta tecnología es capaz asimismo de tener más de 20 canales compartiendo la misma fibra y en la misma banda óptica que usa el canal cuántico, lo que le permite transmitir más de 2 Tbps de datos usando tecnología de comunicaciones estándar de 100 Gbps en redes de área metropolitana.

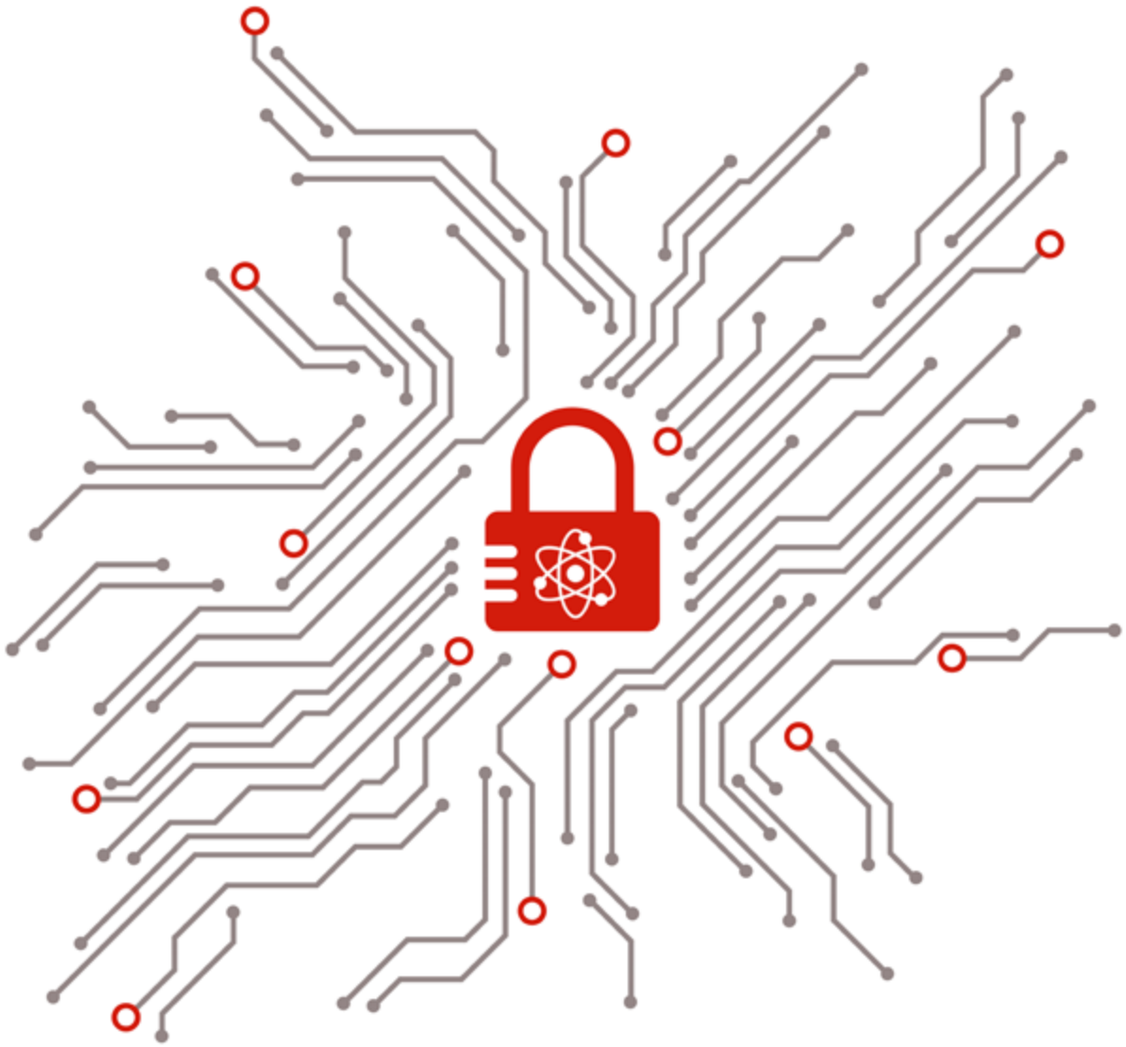
Actualmente este anillo cuántico, gracias al impulso que se pretende dar desde el Gobierno de España a las comunicaciones cuánticas con los planes de recuperación y resiliencia, se va a expandir, tratando de ser el CETSE uno de estos nuevos nodos del anillo.

¿POR QUÉ ES DE INTERÉS PARA EL CETSE PASAR A FORMAR PARTE DE ESTE ANILLO CUÁNTICO?

Uno de los motivos es que la solución cuántica puede ser en un futuro una solución de seguridad avanzada. Todas las comunicaciones seguras se basan en el uso de la criptografía, de manera que la información se cifra utilizando una clave que permite que sólo los participantes que la conocen sean capaces de descifrar los mensajes intercambiados entre ellos. Las técnicas actuales de criptografía están basadas en problemas matemáticos que son complejos de resolver. A medida que la capacidad de computación crece, el tiempo de resolución de estos problemas, y por tanto la seguridad de las claves, disminuye.

El tamaño de las claves y la complejidad de los algoritmos de encriptación han tenido que aumentar a medida que la capacidad de cálculo ha ido creciendo. Estas técnicas pueden quedar completamente obsoletas con la aparición de los ordenadores cuánticos, capaces de aplicar los principios de la Mecánica Cuántica para la resolución de problemas actualmente insolubles, incluyendo el romper las claves generadas por los métodos actuales de criptografía, haciendo inútiles la mayoría de las infraestructuras de seguridad en las comunicaciones.

Las tecnologías cuánticas ofrecen, sin embargo, una solución a la vulnerabilidad de los métodos actuales. Con estas tecnologías es posible aplicar principios cuánticos para intercambiar una clave entre los extremos de un canal de comunicaciones, de manera que esa clave sea segura frente a cualquier ataque, incluyendo los de un ordenador cuántico. La tecnología cuántica hace posible incluso que cualquier intento de ataque sea inmediatamente detectado.



CONCLUSIONES

La futura llegada de la computación cuántica pone en jaque la seguridad de la información con efecto retroactivo. Como solución a esto, surge la criptografía post-cuántica, que se basa en problemas matemáticos difíciles de resolver para ordenadores clásicos y cuánticos. Esta nueva solución requiere de tiempo para implementarla, y del liderazgo de empresas instituciones como el NIST, ETSI, IETF, etc. Además de la participación de integradores, usuarios finales, la comunidad matemática y fabricantes de equipos criptográficos. También surge la criptografía cuántica, que resuelve esta vulnerabilidad aplicando principios físicos cuánticos.

Es muy importante que las empresas sean conscientes del riesgo que conlleva un cambio tecnológico de esta magnitud, y que se empiecen a preparar para la migración a esta nueva criptografía, ya que este proceso es largo y ciertos datos requieren de mayor tiempo de confidencialidad. En el caso de la Administración Pública, no va a haber presión ciudadana por el cambio, debido a la falta de percepción del riesgo al estar este todavía alejado en el tiempo. Por tanto, la Administración Pública debe adoptar un rol de liderazgo e impulsar iniciativas que preparen a las instituciones de gobierno y a la industria del país.

En GMV, tal y como nos recuerdan, "siempre hemos apostado por la ciberseguridad, apostamos por la criptografía resistente a ordenadores cuánticos, y animamos a las empresas con necesidades relacionadas a contactar con nosotros para trabajar en asegurar la seguridad de su información a largo plazo". ■

MÁS INFORMACIÓN

- NIST Post-Quantum Cryptography Standardization process
- Securing Communications in the Quantum Computing Age
- Informe España Cuántica (AMETIC)
- Debemos abordar hoy la realidad post-cuántica

AGRADECIMIENTOS:

GMV quiere agradecer su colaboración en este Especial a los miembros de las siguientes organizaciones que han hecho esto posible: APTIE (Asociación para la Promoción de las Tecnologías e Industrias Estratégicas), Universidad Complutense de Madrid, Utimaco, CCN-CNI y Ministerio del Interior.