FMI - La computación cuántica y el sistema financiero - acción espeluznante a distancia

Extracto

La era de la computación cuántica está a punto de comenzar, con profundas implicaciones para la economía global y el sistema financiero. El rápido desarrollo de la computación cuántica trae beneficios y riesgos. Las computadoras cuánticas pueden revolucionar industrias y campos que requieren una potencia informática significativa, incluido el modelado de mercados financieros, el diseño de nuevos medicamentos y vacunas efectivos y el empoderamiento de la inteligencia artificial, así como la creación de una forma nueva y segura de comunicación (Internet cuántico). Pero también descifrarían muchos de los algoritmos de cifrado actuales y amenazarían la estabilidad financiera al comprometer la seguridad de la banca móvil, el comercio electrónico, la tecnología financiera, las monedas digitales y el intercambio de información en Internet. Si bien el trabajo sobre el cifrado cuántico seguro aún está en progreso, las instituciones financieras deben tomar medidas ahora para prepararse para la transición criptográfica, evaluando los riesgos futuros y retroactivos de las computadoras cuánticas, haciendo un inventario de sus algoritmos criptográficos (especialmente las claves públicas) y construyendo agilidad criptográfica para mejorar la resiliencia general de la ciberseguridad.

Palabras clave: computación cuántica, cifrado cuántico-seguro, ciberseguridad, fintech.

“No puedo creer seriamente en ello (…)

La física debe representar una realidad en el tiempo y el espacio,

libre de acción espeluznante a distancia”.

Albert Einstein**2**

I. INTRODUCCIÓN

La revolución cuántica está en marcha, con el ritmo de las innovaciones acelerándose en los últimos años. El ejemplo más notable y muy discutido de la tecnología cuántica es la computación cuántica: el uso de la física cuántica para realizar cálculos que son intratables incluso para los superordenadores clásicos actuales y futuros más potentes.**3** Las principales empresas tecnológicas ya han desarrollado prototipos funcionales de computadoras cuánticas y han proporcionado acceso a ellos a los investigadores a través de sus servicios en la nube. En todo el mundo, docenas de proyectos conocidos están en marcha, desde grandes corporaciones hasta nuevas empresas y universidades, para construir sistemas cuánticos utilizando diferentes tecnologías centrales. Si uno de ellos supera los obstáculos tecnológicos actuales y crea una computadora cuántica completamente funcional o encuentra una manera de utilizar los modelos existentes para resolver tareas computacionales prácticas que están más allá de los límites de las computadoras convencionales, tendría profundas implicaciones.

La computación cuántica tiene el potencial de transformar la economía global y el sector financiero, al acelerar el descubrimiento científico y la innovación. Las computadoras cuánticas completamente funcionales, cuando aparezcan, deberían revolucionar las industrias y los campos que requieren una potencia de cálculo significativa para simulaciones y optimizaciones que son demasiado complejas para las computadoras convencionales. Para el sistema financiero, las máquinas cuánticas pueden reducir en gran medida el tiempo para analizar posiciones de riesgo complejas o ejecutar simulaciones de Monte Carlo, así como aumentar su precisión. La computación cuántica también puede acelerar el aprendizaje automático y la inteligencia artificial.

Más allá de la computación, las tecnologías cuánticas dan lugar a nuevas formas de transmisión de datos rápidas y seguras (es decir, Internet cuántico), que se ha probado con éxito y, al menos en teoría, será irrompible. Otra perspectiva a largo plazo es la criptografía cuántica, que podría mejorar la ciberseguridad.

Sin embargo, las computadoras cuánticas también descifrarían muchos algoritmos criptográficos que sustentan la ciberseguridad actual. Los algoritmos que permiten la seguridad del sistema financiero, incluidas las comunicaciones por Internet, las transacciones bancarias móviles y las monedas digitales y las tecnologías de contabilidad distribuida, podrían quedar obsoletos o requerirían una actualización significativa. Para algunas aplicaciones, puede que ya sea demasiado tarde debido a los riesgos retroactivos que presentan las computadoras cuánticas, ya que cualquier información que se asuma segura hoy en día puede ser capturada y almacenada, y luego descifrada una vez que se crean computadoras cuánticas eficientes.**4** De hecho, casi cualquier mensaje personal o financiero cifrado enviado y grabado hoy puede ser descifrado por una poderosa computadora cuántica en el futuro. La mayoría de las instituciones financieras y los reguladores aún no han internalizado estos nuevos riesgos.

Mientras esperan los estándares de cifrado cuántico seguro, los reguladores del sistema financiero pueden desempeñar un papel importante al crear conciencia sobre los riesgos potenciales. Las instituciones financieras deben tomar medidas ahora para prepararse para una transición criptográfica. Deben evaluar los riesgos futuros y retroactivos de las computadoras cuánticas, incluida la información que ya ha sido capturada o que puede ser capturada ahora, almacenada y explotada años después. Las instituciones financieras deben desarrollar planes para migrar la criptografía actual a algoritmos resistentes a la cuántica. Como primer paso, deben hacer un inventario de la criptografía de clave pública utilizada dentro de la institución, así como por socios y proveedores externos. Estos eventualmente tendrán que ser transferidos a la criptografía postquantum una vez que los estándares estén disponibles. Y, por último, deben desarrollar agilidad criptográfica para mejorar la resiliencia general de la ciberseguridad en el futuro. Las experiencias pasadas de reemplazos de algoritmos, aunque mucho más simples que la transición a estándares postquantum, muestran que pueden ser extremadamente disruptivos y, a menudo, tardan años o décadas en lograrse. Por lo tanto, el momento de actuar es ahora.

El resto del documento está organizado de la siguiente manera. En la sección II se describen los conceptos clave de la computación cuántica, en las secciones III y IV se examinan los posibles beneficios y riesgos de las computadoras cuánticas, y en la sección V se resumen los principales mensajes y se presenta el camino a seguir. Para completar el cuadro, los anexos del documento proporcionan un glosario de términos técnicos (Anexo I), una breve historia del cifrado, el criptoanálisis y las computadoras digitales (Anexo II), y una descripción de los principales algoritmos criptográficos actualmente en uso y sus vulnerabilidades (Anexos III y IV).

II. ¿QUÉ ES LA COMPUTACIÓN CUÁNTICA?

La computación cuántica es el uso de fenómenos cuánticos como la superposición y el entrelazamiento para realizar cálculos. La unidad básica de una computadora cuántica es qubit (abreviatura de bit cuántico), típicamente realizada por propiedades cuánticas de partículas subatómicas, como el espín de electrones o la polarización de un fotón. Mientras que cada bit, su contraparte en las computadoras digitales, representa un valor de cero o uno, los qubits representan tanto cero como uno (o alguna combinación de ambos) al mismo tiempo, un fenómeno llamado superposición. El entrelazamiento cuántico es una conexión especial entre pares o grupos de elementos cuánticos, mientras que cambiar el estado de un elemento afecta a otros elementos entrelazados instantáneamente, independientemente de la distancia entre ellos. Este es un fenómeno tan contraintuitivo que Albert Einstein se burló del entrelazamiento como "acción espeluznante a distancia" (Macmillan, 1971). Al enredar qubits, el número de estados representados aumenta exponencialmente, lo que permite explorar una gran cantidad de posibilidades al instante y realizar cálculos paralelos en una escala que está fuera del alcance de las computadoras tradicionales. Gracias a la superposición y el entrelazamiento, agregar solo unos pocos qubits adicionales en pleno funcionamiento puede conducir a saltos exponenciales en la potencia de procesamiento.

Teóricamente, las computadoras cuánticas pueden superar a las computadoras tradicionales actuales (y futuras), la llamada "supremacía" cuántica o ventaja cuántica. Es posible modelar los estados de las computadoras cuánticas con las computadoras tradicionales, pero los recursos necesarios para ello aumentan exponencialmente. Un qubit puede tener valores de cero y uno al mismo tiempo y se puede modelar con dos bits lógicos tradicionales, cada uno con valores de cero o uno. Para dos qubits, se necesitan cuatro bits tradicionales; para tres qubits, ocho bits, etc. Para modelar una computadora cuántica con 54 qubits, se necesitarían 254 = 18,014,398,509,481,984, que es aproximadamente 18 cuatrillones de bits de memoria lógica tradicional. A finales de 2019, solo había una supercomputadora en el mundo que tenía una memoria tan grande: la supercomputadora Summit (OLCF-4) desarrollada por IBM para el Laboratorio Nacional Oak Ridge. Para modelar una computadora cuántica con 72 qubits, se necesitarían 272, alrededor de 5 sextillones de bits. Esto se puede lograr, por ejemplo, apilando 262 mil supercomputadoras tipo Summit. Una computadora cuántica de 100 qubits requeriría más bits que todos los átomos del planeta tierra, y una computadora de 280 qubits requeriría más bits que todos los átomos en el universo conocido. Estos ejemplos numéricos ilustran el poder exponencial de las computadoras cuánticas.

Las computadoras cuánticas no solo son más poderosas, sino que también son fundamentalmente diferentes de las computadoras digitales de hoy. Requieren diferentes algoritmos e infraestructura para resolver problemas matemáticos existentes y nuevos. Para fines ilustrativos, algunas tareas computacionales complejas podrían compararse con un laberinto (por ejemplo, encontrar la ruta más rápida entre dos ciudades o la cadena de suministro más eficiente). Este laberinto tiene multitud de caminos que no conducen a ninguna parte y solo uno que conduce a la salida. La computadora tradicional trata de resolver este problema de la misma manera que podríamos tratar de escapar de un laberinto: probando todos los pasillos posibles y volviendo a los callejones sin salida hasta que finalmente encontremos la salida. Esto puede llevar mucho tiempo. Pero la superposición permite a una computadora cuántica probar todos los caminos posibles a la vez (es decir, el paralelismo cuántico). Esto reduce drásticamente el tiempo necesario para encontrar la solución, la llamada aceleración cuántica.

La aceleración cuántica depende, entre otras cosas, de los problemas computacionales y de los algoritmos utilizados. Los algoritmos de Grover y Shor son los dos algoritmos cuánticos más conocidos. Producen una aceleración polinómica y una aceleración exponencial, respectivamente, sobre sus contrapartes clásicas (Kothari, 2020). Una aceleración polinómica es cuando una computadora cuántica resuelve un problema en el tiempo T, pero una computadora clásica necesita tiempo T2. Por ejemplo, el algoritmo de Grover puede resolver un problema en una computadora cuántica con 1,000 pasos que tomaría 1,000,000 de pasos en una computadora clásica. Este tipo de algoritmos se pueden usar para los llamados problemas NP-completos, descritos como la búsqueda de una aguja en un pajar exponencialmente grande (por ejemplo, encontrar claves simétricas y funciones hash). Una aceleración exponencial es donde una computadora cuántica toma tiempo T pero una computadora clásica toma tiempo 2T. Si T es 100, hay una gran diferencia entre 100 y 2100, más que todos los átomos del planeta tierra. Este tipo de algoritmos incluye el algoritmo de Shor, que puede romper claves asimétricas (públicas). Estas impresionantes aceleraciones son uno de los aspectos más prometedores y convincentes de las computadoras cuánticas.

Motivados por su poder potencial, investigadores de empresas tecnológicas líderes están desarrollando prototipos funcionales de ordenadores cuánticos. En 2019, los ingenieros de Google utilizaron su máquina cuántica alimentada por el procesador Sycamore de 54 qubits, que tenía 53 qubits funcionando en ese momento, para realizar una tarea de cálculo específica en solo 200 segundos, mientras que estimaron que la supercomputadora digital más potente disponible en ese momento tardaría 10,000 años en ejecutar esa tarea. Los ingenieros de Google lo presentaron como prueba de la "supremacía" cuántica, que es la confirmación de que las computadoras cuánticas pueden realizar tareas prácticamente imposibles para las computadoras tradicionales (Arute et al., 2019). Un equipo de investigación competidor de IBM cuestionó las afirmaciones de Google, mientras promovía sus propias computadoras cuánticas. IBM afirma que las estimaciones de Google son inexactas, y que la computadora más rápida del mundo, Summit, construida por IBM, podría modificarse para obtener los mismos resultados en aproximadamente 3 días (Pednault et al., 2019), aunque no lo han demostrado en la práctica. Consolidando las afirmaciones de ventaja cuántica, en diciembre de 2020 un equipo de investigadores de la Universidad de Ciencia y Tecnología de China en Hefei anunció que su computadora cuántica de fotones, llamada Jiuzhang, realizó en 200 segundos un cálculo que en una de las supercomputadoras más poderosas del mundo tardaría 2.500 millones de años en completarse (Zhong et al., 2020). Es importante destacar que llevaron a cabo la tarea en una computadora cuántica fotónica que funcionaba a temperatura ambiente.

Además, muchas otras empresas tecnológicas, desde líderes de la industria hasta nuevas empresas y universidades, están trabajando en computadoras cuánticas, lo que aumenta la probabilidad de un gran avance. A partir de enero de 2021, IBM ha desplegado 28 computadoras cuánticas para uso público y comercial a través de sus servicios en la nube. En septiembre de 2020, IBM lanzó una hoja de ruta para producir un dispositivo de más de 1,000 qubits llamado Quantum Condor para fines de 2023.Efectivamente, significa duplicar o triplicar el número de codos en la computadora cuántica cada año. Microsoft y Amazon también han lanzado versiones beta de servicios en la nube de computación cuántica, Microsoft Azure y AWS Bracket, impulsados por proveedores como 1Qbit, Rigetti, IonQ y D-Wave. En todo el mundo, hay al menos 87 proyectos conocidos en marcha para construir sistemas cuánticos utilizando diferentes tecnologías centrales.**5**

Para cosechar los beneficios de la computación cuántica, los investigadores necesitan construir máquinas cuánticas que computen con tasas de error más bajas. La superposición y el entrelazamiento son estados frágiles. La interacción de los qubits con el entorno produce errores de cálculo. Cualquier perturbación o ruido externo, como el calor, la luz o las vibraciones, inevitablemente saca los qubits de su estado cuántico y los convierte en bits regulares. Las computadoras clásicas también son propensas a errores computacionales aleatorios, aunque en tasas mucho más bajas. Al emplear redundancia, los procesos de corrección de errores permiten a las computadoras clásicas producir cálculos prácticos y sin errores. Sin embargo, tales técnicas no son aplicables a la física cuántica debido al principio de no clonación: es físicamente imposible copiar el estado de ejecución de un qubit.

En 1994, Peter Shor propuso un código teórico de corrección de errores cuánticos, logrado mediante el almacenamiento de la información de un qubit en un estado altamente entrelazado de varios qubits. Este esquema utiliza muchos qubits ordinarios para crear una sola entidad libre de errores: los primeros se denominan qubits físicos, mientras que los segundos como qubits lógicos. Pero simplemente agregar más qubits podría no aumentar el rendimiento de una máquina. La frecuencia de los errores en qubits delicados y sus operaciones, causadas por ruidos, tiende a aumentar a medida que se conectan más qubits. IBM ha desarrollado el concepto de volumen cuántico para medir el progreso en la computación cuántica, que ajusta el número de qubits, entre otras cosas, para la tasa de error y la calidad de la conectividad entre qubits.**6** IBM espera que el volumen cuántico se duplique con creces cada año. Los dispositivos cuánticos de hoy en día tienen tasas de error que son demasiado altas, que son uno de los problemas más apremiantes para las computadoras cuánticas.

La carrera para construir mejores computadoras cuánticas se está intensificando, con empresas que utilizan diferentes tecnologías. Es posible clasificar la comunidad de hardware de computación cuántica temprana en dos categorías o tipos generales. En primer lugar, las computadoras cuánticas basadas en las puertas cuánticas y los circuitos cuánticos son las más similares a nuestras computadoras clásicas actuales basadas en puertas lógicas.**7** La otra gran familia de ordenadores cuánticos son los ordenadores cuánticos analógicos. Estas computadoras cuánticas manipulan directamente las interacciones entre qubits sin dividir estas acciones en operaciones de puerta. Las máquinas analógicas más conocidas son los analizadores cuánticos. Algunos recocidos cuánticos experimentales ya están disponibles comercialmente, el ejemplo más destacado es el procesador D-Wave, con más de 5.000 qubits. Esta máquina ha sido fuertemente probada en laboratorios y empresas de todo el mundo, incluyendo Google, LANL, Texas A&M, USC. Las empresas también están utilizando varias estrategias para implementar qubits físicos. Por ejemplo, Alibaba, IBM, Google, D-Wave y Rigetti usan qubits superconductores, IonQ usa qubits de iones atrapados, mientras que Xanadu y la Universidad de Ciencia y Tecnología de China están desarrollando computadoras cuánticas fotónicas.

En el futuro previsible, se espera que las computadoras cuánticas complementen, no reemplacen, a las computadoras clásicas. Si bien las computadoras cuánticas de escritorio están muy lejos, el público ya puede tener acceso a la computación cuántica a través de servicios en la nube proporcionados por compañías como IBM y D-Wave. Las personas pueden usar sus computadoras clásicas para realizar cálculos en computadoras cuánticas y recibir los resultados en sus computadoras clásicas. En un futuro cercano, las aplicaciones cuánticas probablemente serían híbridas, ya que las tecnologías de computación cuántica y clásica tienen fortalezas complementarias (Academias Nacionales de Ciencias, 2019).

III. BENEFICIOS POTENCIALES DE LA COMPUTACIÓN CUÁNTICA

Las computadoras cuánticas pueden transformar el sistema financiero, ya que pueden resolver muchos problemas considerablemente más rápido y con mayor precisión que las computadoras clásicas más poderosas. La simulación, la optimización y el aprendizaje automático (ML) son tres áreas en las que las computadoras cuánticas pueden tener una ventaja sobre las computadoras clásicas (Bouland et al. 2020; Egger et al., 2020; y Orus et al. 2019):

• Simulaciones: métodos basados en Monte Carlo. El uso de simulaciones por parte del sector financiero es omnipresente. Por ejemplo, los métodos Monte Carlo se utilizan para fijar el precio de los instrumentos financieros y gestionar los riesgos. Sin embargo, las simulaciones de Monte Carlo son computacionalmente intensivas, lo que a menudo conduce a compensaciones entre precisión y eficiencia. La computación cuántica podría realizar simulaciones como la gestión de precios y riesgos casi en tiempo real, sin la necesidad de tomar suposiciones poco realistas para simplificar los modelos.

• Optimización de modelos. Las instituciones financieras hacen una miríada de cálculos de optimización todos los días. Por ejemplo, para determinar la mejor estrategia de inversión para una cartera de activos, asignar capital, administrar efectivo en redes de cajeros automáticos o aumentar la productividad. Algunos de estos problemas de optimización son difíciles, si no imposibles, para las computadoras tradicionales de abordar. Las aproximaciones se utilizan para resolver los problemas dentro de un marco de tiempo razonable. Las computadoras cuánticas podrían realizar optimizaciones mucho más precisas en una fracción del tiempo sin la necesidad de usar aproximaciones.

• Métodos de aprendizaje automático (ML), incluidas las redes neuronales y el aprendizaje profundo. Las instituciones financieras están utilizando cada vez más ML. Los ejemplos incluyen estimar el nivel de riesgo de los préstamos mediante la calificación crediticia y detectar fraudes al encontrar patrones que se desvían del comportamiento normal. Sin embargo, tales tareas de ML se enfrentan a la maldición de la dimensionalidad. El tiempo necesario para entrenar un algoritmo de ML en computadoras clásicas aumenta exponencialmente con el número de dimensiones consideradas. Incluso si la computadora clásica puede manejar estas tareas, tomaría demasiado tiempo. Las computadoras cuánticas tienen el potencial de superar a los algoritmos clásicos al acelerar las tareas de ML (aceleración cuántica), lo que les permite abordar análisis más complejos al tiempo que aumentan la precisión.

Más allá de las finanzas, la computación cuántica tiene el potencial de ser un catalizador para el descubrimiento científico y la innovación. Una aplicación importante de la computación cuántica es para modelos de física de partículas, que a menudo son extraordinariamente complejos y requieren grandes cantidades de tiempo de computación para la simulación numérica. Las computadoras cuánticas permitirían el modelado de precisión de las interacciones moleculares y la búsqueda de configuraciones óptimas para las reacciones químicas. Pueden transformar áreas como el almacenamiento de energía, la ingeniería química, la ciencia de materiales, el descubrimiento de fármacos y vacunas, la simulación, la optimización y el aprendizaje automático. Específicamente, esto permitiría el diseño de nuevos materiales, como baterías livianas para automóviles y aviones, o nuevos catalizadores que puedan producir fertilizantes de manera más eficiente, un proceso que hoy representa más del 2 por ciento de las emisiones de carbono del mundo (Martinis y Boixo, 2019). Las computadoras cuánticas también podrían mejorar los pronósticos meteorológicos, optimizar las rutas de tráfico y las cadenas de suministro, y ayudarnos a comprender mejor el cambio climático.

Más allá de la computación, las tecnologías cuánticas dan lugar a nuevas formas de transmisión, almacenamiento y manipulación de datos. Las redes cuánticas pueden transmitir información en forma de qubits entrelazados entre procesadores cuánticos remotos casi instantáneamente (teletransportación cuántica) y de forma segura utilizando la distribución de claves cuánticas (QKD). Hasta hace poco, tales redes podían funcionar solo en condiciones de laboratorio, pero los experimentos confirmaron su viabilidad para comunicaciones seguras a larga distancia (Boaron et al., 2018). Además, los datos podrían transmitirse de forma inalámbrica a través de satélites cuánticos en el espacio. Científicos en China pudieron transmitir datos utilizando un satélite cuántico lanzado en 2016 entre una estación terrestre móvil en Jinan (en el noreste de China) y una estación fija en Shanghai. El banco ICBC y el Banco Popular de China están utilizando QKD basado en satélites para el intercambio de información entre ciudades distantes, como Beijing y Urumqi en el extremo noroeste.**8** **9** En los Países Bajos, un equipo de la Universidad Tecnológica de Delft está construyendo una red que conecta cuatro ciudades con tecnología cuántica. Han demostrado que puede enviar partículas cuánticas entrelazadas a largas distancias.**10** En los Estados Unidos, un consorcio de importantes instituciones liderado por Caltech ha demostrado una teletransportación cuántica sostenida y de alta fidelidad a largas distancias. Lograron la teletransportación exitosa de qubits a través de 44 kilómetros de fibra en dos bancos de pruebas: Caltech Quantum Network y Fermilab Quantum Network.**11**

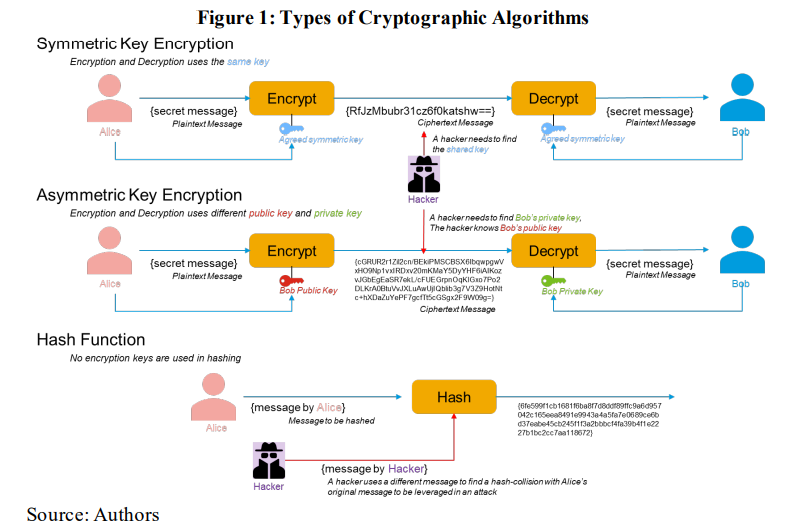
Otro lugar prometedor son los dispositivos de detección cuántica. Se han reportado avances en radar cuántico, imágenes, metrología y navegación, lo que permitiría una mayor precisión y sensibilidad. Por ejemplo, la medicina ha comenzado a cosechar los beneficios de los sensores cuánticos, revolucionando la detección y el tratamiento de enfermedades. En los Estados Unidos, la Agencia de Proyectos de Investigación Avanzada de Defensa (DARPA) está ejecutando el programa quantum-Assisted Sensing and Readout (QuASAR). Basándose en técnicas de control y lectura establecidas de la física atómica, tiene como objetivo desarrollar un conjunto de dispositivos de medición que puedan encontrar aplicación en las áreas de imágenes biológicas, navegación inercial y sistemas robustos de posicionamiento global.**12**

IV. RIESGOS POTENCIALES DE LA COMPUTACIÓN CUÁNTICA

Si bien la computación cuántica tiene un tremendo potencial para beneficiar a la sociedad, trae nuevos riesgos y desafíos. El poder de cómputo masivo de las máquinas cuánticas amenaza la criptografía moderna, con implicaciones de gran alcance para la estabilidad financiera y la privacidad. Las computadoras cuánticas pueden resolver lo que se conoce en la teoría de la complejidad como problemas matemáticos difíciles exponencialmente más rápido que las supercomputadoras clásicas más poderosas, lo que potencialmente hace que los principales estándares criptográficos de hoy en día sean obsoletos. En particular, la computación cuántica tiene el potencial de hacer que la criptografía asimétrica (criptografía de clave pública) sea obsoleta, al tiempo que reduce la fuerza de otras claves criptográficas y hashes.

La criptografía actual se basa en tres tipos principales de algoritmos: claves simétricas, claves asimétricas (públicas) y funciones hash algorítmicas, o hashing (consulte los anexos III y IV para obtener más descripciones). Estos algoritmos criptográficos, en su mayor parte, han tenido la ventaja de mantener la seguridad necesaria para proteger los datos, proporcionar comprobaciones de integridad y firmas digitales. Por lo general, se consideran seguros e irrompibles con el hardware y las técnicas de criptoanálisis más avanzadas de la actualidad que utilizan computadoras convencionales.

Con el cifrado de clave simétrica, un atacante necesita encontrar la clave secreta compartida entre el emisor y el receptor para descifrar el mensaje cifrado como se muestra en la Figura 1 (panel superior).**13** Por el contrario, con el cifrado de clave pública, el atacante necesita encontrar la clave privada de los receptores, conociendo su clave pública, para descifrar el mensaje (panel central). Los algoritmos de cifrado asimétrico se utilizan ampliamente para proteger las comunicaciones a través de Internet. Los ataques exitosos contra estos algoritmos criptográficos estándar comprometerían las conexiones seguras, poniendo en peligro la seguridad de la banca, el comercio electrónico y otros servicios. Con las funciones hash (panel inferior), un atacante intentaría encontrar una colisión de hash para hacer coincidir el resumen de salida con una entrada diseñada y diferente, lo que permitiría producir resúmenes de autenticación falsificados para transacciones o documentos.



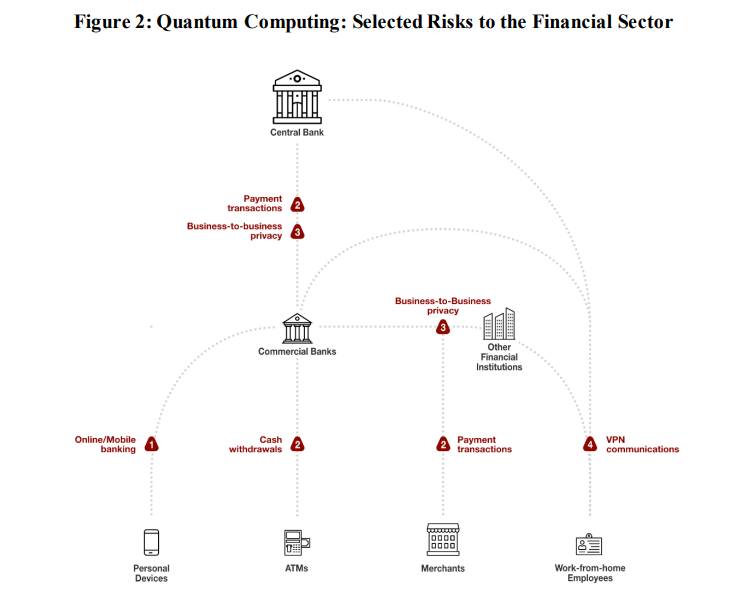
Los riesgos de la computación cuántica varían según los tipos de algoritmos criptográficos:

• Se cree que la criptografía simétrica, bajo ciertas condiciones, es resistente a la cuántica. Los estándares de seguridad actuales recomiendan el uso del algoritmo AES con claves de 256 bits para el cifrado simétrico. Conocido como AES 256, este algoritmo es ampliamente utilizado para múltiples propósitos, como proteger sitios web de Internet o redes inalámbricas. Un atacante tendría que probar 2256 combinaciones para romper una clave AES de 256 bits utilizando la fuerza bruta, un esfuerzo que requeriría un lapso de tiempo de más de 7 mil millones de años para ser ejecutado por una supercomputadora clásica, la mitad de la edad actual del universo (CISA, 2019). Una computadora cuántica puede reducir la complejidad de romper la clave de cifrado simétrica a la mitad, por ejemplo, mediante el uso del algoritmo de Grover (Grassl et al., 2015). Sin embargo, todavía tendría que funcionar durante millones de años para romper una sola clave AES utilizando métodos conocidos. Esto lleva a la mayoría de los expertos a creer que ese algoritmo es resistente a la cuántica por ahora, al igual que otros métodos de cifrado simétrico de naturaleza similar.

• También se cree que las funciones de hash son resistentes a la cuántica en determinadas condiciones. El hashing genera códigos únicos de tamaño fijo de acuerdo con entradas arbitrarias. Se utilizan para validar información y se aprovechan en varios métodos criptográficos para diversos fines, como validar información o generar códigos de autenticación. Su novedad proviene de la cuasi imposibilidad de revertirlos. Dado un código hash determinado, tomaría miles de años producir entradas que generen el mismo código (esto se llama ataque de colisión). Al igual que con la criptografía simétrica, utilizando el algoritmo de Grover, una computadora cuántica podría reducir el tiempo para revertir una función hash de 2n a 2n/2, siendo n el número de bits utilizados para la salida hash. Por lo tanto, las funciones hash más largas como la familia SHA-3, que generalmente generan salidas de 256 bits, se consideran cuánticas seguras y se espera que permanezcan como estándares aprobados por ahora.

• Las claves públicas (o asimétricas), sin embargo, pueden volverse obsoletas con la computación cuántica. Teóricamente, una computadora cuántica en pleno funcionamiento puede romper una clave asimétrica en unas pocas horas mediante el uso del algoritmo de Shor y las optimizaciones relacionadas (Gidney et al., 2019). Además, los investigadores creen que los avances en computación cuántica alcanzarán un nivel de optimización que permitiría a las computadoras cuánticas romper las claves públicas actuales en menos tiempo del que se tarda en generarlas utilizando computadoras digitales (Monz et al, 2016 y Anschuetz et al, 2018).

Los protocolos críticos detrás de los datos digitales y la seguridad de la comunicación del sector financiero dependen en gran medida de la criptografía de clave pública. En la era de Internet, las claves públicas tienen como objetivo lograr servicios de seguridad críticos que sustenten el sector financiero. Estos incluyen (Burr y LyonsBurke, 1999): (i) autenticación/autorización (la capacidad de corroborar la identidad de una parte que originó datos particulares, transacción o participa en un protocolo); (ii) privacidad/confidencialidad (la capacidad de garantizar que personas no autorizadas no puedan acceder a datos protegidos); y (iii) integridad (la capacidad de saber que los datos no han sido alterados). Por ejemplo, los certificados digitales y las firmas digitales de hoy en día se basan en claves asimétricas. Estos servicios de seguridad críticos que apoyan al sector financiero se verían comprometidos por una computadora cuántica suficientemente potente, amenazando la información confidencial administrada y comunicada por las instituciones financieras y los bancos centrales. En pocas palabras, un atacante que puede falsificar firmas puede gastar efectivamente los fondos de otras personas o hacerse pasar por cualquier entidad.





La Figura 2 muestra algunos impactos potenciales de las computadoras cuánticas en los diferentes protocolos de comunicación utilizados por el sistema financiero:

1. Banca en línea / móvil. Usando una computadora cuántica, un atacante puede comprometer las claves públicas para los protocolos estándar de Internet y espiar cualquier comunicación entre los usuarios y las instituciones financieras. Además, un atacante puede comprometer los esquemas de autenticación y autorización, ya sea un token de sesión o un sistema financiero basado en clave pública para producir transacciones falsificadas. Además, en el caso de las monedas digitales del banco central (CBDC) y las redes blockchain, los atacantes pueden extraer claves de billetera válidas de los registros disponibles públicamente, otorgándoles la capacidad de apropiarse de los créditos y tokens de los usuarios.

2. Transacciones de pago y retiros de efectivo. Los cajeros automáticos están conectados a través de redes privadas. Esto facilita a los atacantes acceder a las conexiones que dependen del cifrado de clave pública y utilizar los mismos lugares aplicables a la banca en línea o móvil para falsificar transacciones.

3. Privacidad de empresa a empresa. Las redes corporativas punto a punto también utilizan el cifrado de clave pública para crear canales seguros, autenticar y autorizar intercambios de datos entre empresas. Al comprometer dichos canales, los atacantes tendrían acceso completo a la información que, una vez capturada, les permitiría puntos de entrada fáciles para invadir las redes internas corporativas, al hacerse pasar por usuarios o servidores a través de ataques man-in-the-middle. Al falsificar certificados, por ejemplo, los atacantes podrían agregar sus propios recursos a la red empresarial. Otra forma de ataques puede ser registrar los datos cifrados disponibles ahora y descifrarlos una vez que una computadora cuántica esté disponible, lo que les permite revelar secretos comerciales actuales en el futuro, por ejemplo.

4. Comunicaciones VPN. Las conexiones VPN son utilizadas por el personal de las instituciones financieras para trabajar desde casa y para acceder a los recursos internos y sensibles de la organización. Dichas conexiones suelen utilizar el cifrado de clave pública para autenticar el negocio y las estaciones de trabajo que serían vulnerables a los mismos problemas que las conexiones de empresa a empresa.

Otras aplicaciones que se basan en la criptografía de clave pública incluyen activos digitales populares basados en blockchain como Bitcoin o Ethereum y aplicaciones web protegidas por contraseña. El más conocido de estos protocolos es HTTPS, utilizado por el 96 por ciento de los sitios web de Internet (Informe de Google, 2020). Por lo tanto, la computación cuántica es una amenaza existencial para muchos sectores empresariales que dependen de la criptografía asimétrica para sus operaciones diarias (ETSI, 2020).

Si bien la capacidad de usar claves más largas hace que el cifrado simétrico y el hashing cuántico sean seguros hoy en día, no son inmunes a los avances adicionales en la computación cuántica. A medida que el campo de la computación cuántica se investiga y comprende ampliamente, nuevos esquemas y algoritmos surgen continuamente. El algoritmo de Shor, por ejemplo, se ha mejorado varias veces desde su inicio, principalmente para reducir sus requisitos de procesamiento. Se crean nuevos algoritmos y análisis que disminuyen significativamente la capacidad de hardware cuántico necesaria para resolver problemas que van más allá del ámbito de las supercomputadoras clásicas (Cade, 2020). Por lo tanto, es razonable suponer que, a medida que avanza la investigación, se descubrirían nuevos algoritmos para apuntar a las funciones avanzadas de criptografía simétrica y hash criptográfica de hoy en día y convertirlas en obsoletas, como en el caso de la criptografía de clave pública.

Lograr un entorno cuántico seguro requerirá una mentalidad diferente por parte de los gobiernos, las empresas y los individuos. Más del 50 por ciento de las organizaciones, incluidas las agencias gubernamentales, admiten ejecutar software obsoleto.**14** Las experiencias pasadas con el reemplazo del estándar de cifrado de datos (DES) y varias funciones hash (SHA-1, MD5) sugieren que se necesita al menos una década para reemplazar un algoritmo criptográfico ampliamente implementado (Academias Nacionales de Ciencias, 2019). Es probable que la migración a algoritmos resistentes a la cuántica sea mucho más compleja que las experiencias anteriores, dado el uso ubicuo de claves públicas. Por lo tanto, incluso si todos los proveedores de productos hicieran que su software fuera resistente a la cuántica, las organizaciones públicas y privadas por igual necesitarían un enfoque diferente para la gestión de la obsolescencia. Esto sería aún más complicado y costoso para los sistemas heredados que ya no tienen actualizaciones de software emitidas por sus fabricantes.

V. EL CAMINO A SEGUIR

Estamos en el umbral de la era de la computación cuántica. Las computadoras cuánticas pueden acelerar el proceso de descubrimiento científico, desde el diseño de nuevos materiales para baterías más eficientes hasta la creación de mejores medicamentos y vacunas. Las computadoras cuánticas también podrían transformar el sistema financiero, ya que resolverían muchos problemas considerablemente más rápido y con mayor precisión que las supercomputadoras clásicas más poderosas. Aprovechar el potencial de las computadoras cuánticas también requerirá nuevos enfoques y algoritmos. Esto incluye el desarrollo de nuevos esquemas de corrección de errores, la creación de nuevos lenguajes de programación, la formación de comunidades de usuarios potenciales y el desarrollo de estándares comunes para garantizar la interoperabilidad entre los diferentes enfoques de computación cuántica y las comunicaciones.

Las computadoras cuánticas también pueden causar interrupciones sustanciales, incluido el socavamiento de la estabilidad financiera. Un riesgo importante de la computación cuántica se relaciona con los algoritmos de cifrado existentes que podrían quedar obsoletos, especialmente los algoritmos de clave pública ampliamente utilizados. La historia del criptoanálisis está llena de historias de advertencia sobre la criptografía percibida e irrompible que se ha vuelto obsoleta por las nuevas tecnologías (Anexo II). La carrera ya ha comenzado a desarrollar nuevos estándares y algoritmos de cifrado cuánticos seguros. Por ejemplo, en los Estados Unidos, el Instituto Nacional de Estándares y Tecnología (NIST) está organizando una competencia para un algoritmo de cifrado cuántico seguro, con el objetivo de anunciar un ganador para 2024 (NIST, 2020). Si las computadoras cuánticas completamente funcionales se convierten en una realidad antes o poco después de eso, las organizaciones (empresas y gobiernos) tendrían una ventana estrecha para mitigar este riesgo. En Europa, el Instituto Europeo de Normas de Telecomunicaciones (ETSI) está encabezando el despliegue de normas de seguridad cuántica (ETSI, 2015, 2017, 2020). Estos trabajos se incorporan a las actividades de otros organismos normativos, como la Unión Internacional de Telecomunicaciones (UIT) y el Grupo de Trabajo sobre Ingeniería de Internet (IETF).

Mientras esperan estándares de resistencia cuántica, los reguladores del sistema financiero pueden desempeñar un papel importante al crear conciencia de la comunidad financiera sobre los riesgos y desafíos actuales y futuros. En primer lugar, las instituciones financieras deben desarrollar planes para migrar la criptografía actual a algoritmos resistentes a la cuántica. ETSI (2020) ha esbozado un marco de acciones que una organización debe tomar para permitir la migración a un estado criptográfico seguro cuántico. El marco comprende tres etapas: (i) compilación de inventarios, (ii) preparación del plan de migración y (iii) ejecución de la migración:

• Compilación de inventarios. Una organización no puede planificar la migración sin un conocimiento previo de sus activos que la computación cuántica afectaría. Por lo tanto, la primera etapa de la migración es identificar el conjunto de activos criptográficos (tanto hardware como software) y los procesos en el sistema. El marco requeriría la gestión del proceso institucional, la asignación de un presupuesto y la rendición de cuentas. Los costos podrían ser significativos, incluidos los financieros, temporales, organizativos y para provisiones técnicas.

• Elaboración del plan migratorio. El plan de migración determinaría si un activo identificado en la etapa 1 se migrará o retirará, ya que algunos activos pueden quedar obsoletos a través del rediseño. La secuenciación de la migración es importante dada la interdependencia de los activos. Si se requiere compatibilidad con versiones anteriores durante la migración, la aplicación tendrá que admitir algoritmos clásicos y cuánticos seguros. Esto se puede lograr mediante el uso de algoritmos clásicos individuales y cuánticos seguros, o mediante el uso de algoritmos híbridos dependiendo de la agilidad criptográfica existente. Por ejemplo, en noviembre de 2020, IBM anunció planes para agregar criptografía cuántica segura a sus servicios en la nube, además de los estándares actuales.**15** Las disposiciones para la agilidad criptográfica deben considerarse para cualquier criptografía nueva o actualizada. Si se encuentra una vulnerabilidad en el algoritmo cuántico-seguro, puede ser necesario cambiar a uno diferente, aunque a veces la vulnerabilidad puede abordarse con parches y actualizaciones. Garantizar la agilidad criptográfica facilitará estas actualizaciones.

• Ejecución de migración. El papel de esta etapa es implementar el plan de migración de la etapa 2 contra el inventario de la etapa 1. Esta etapa también incluye la gestión de la mitigación. Un elemento clave de la gestión de la mitigación es la realización de ejercicios para simular y probar el plan de migración para determinar su viabilidad. Estos ejercicios son importantes, ya que pueden descubrir elementos de inventario faltantes (es probable que el inventario esté incompleto).

Este marco supone una migración ordenada y planificada. Sin embargo, la disponibilidad inmediata de una computadora cuántica viable que se utiliza para atacar claves públicas podría requerir una transición inmediata a una criptografía cuántica segura. En este caso, una migración de emergencia podría requerir la ejecución simultánea rápida de las medidas clave descritas anteriormente.

Dado el ritmo de las innovaciones y la incertidumbre sobre cuándo estarán disponibles los estándares de seguridad cuántica, las instituciones financieras deben desarrollar agilidad criptográfica. Esta es una propiedad que permite cambiar o actualizar sin problemas los algoritmos o parámetros criptográficos para mejorar la resiliencia general de la ciberseguridad en el futuro. A largo plazo, puede ser necesario implementar métodos criptográficos cuánticos para reducir los riesgos de ciberseguridad.

Más allá de la estabilidad financiera, la computación cuántica plantea importantes riesgos de privacidad, y los reguladores deben trabajar con expertos de la industria para comprender estos riesgos. Regulaciones como la Ley Gramm-Leach-Bliley de los Estados Unidos (Gramm-Leach, 1999) o el Reglamento General de Protección de Datos de los Estados Unidos (GDPR, 2018) ya guían la protección de la información, pero pueden requerir un mayor escrutinio para garantizar un cifrado resistente a la cuántica del intercambio y almacenamiento de datos. Es importante destacar que, dado que las computadoras cuánticas representan riesgos retroactivos, el momento de actuar es ahora.

El FMI tiene un papel importante que desempeñar en la sensibilización de sus miembros sobre los riesgos para la estabilidad financiera de las computadoras cuánticas y la promoción de normas y prácticas de seguridad cuántica. A nivel multilateral, el FMI debería alentar a los países miembros a colaborar estrechamente en la elaboración de normas y protocolos comunes para garantizar la interoperabilidad. A nivel bilateral, debería alentar a las autoridades nacionales a desarrollar planes de migración de cifrado en la vigilancia del sector financiero, por ejemplo, como parte del diálogo sobre cómo garantizar la resiliencia operativa de las instituciones financieras, los mercados y la infraestructura.

**ANEXO I. GLOSARIO DE TÉRMINOS TÉCNICOS UTILIZADOS EN EL DOCUMENTO**

**El criptoanálisis** estudia el mensaje secreto cifrado (texto cifrado) para obtener la mayor cantidad de información posible sobre el mensaje original.

**La criptografía** es la ciencia de la transmisión de información secreta a través de canales públicos. Un sistema criptológico realiza transformaciones en un mensaje, el texto plano, y utiliza una clave para hacerlo ininteligible, produciendo una nueva versión del mensaje, el texto cifrado. Para revertir el proceso, el sistema realiza transformaciones inversas para recuperar el texto plano, descifrando el texto cifrado (Dooley, 2018).

**La agilidad criptográfica** (o agilidad criptográfica) es la propiedad que permite cambiar o actualizar algoritmos o parámetros criptográficos. Si bien no es específica de la computación cuántica, la agilidad criptográfica facilitaría la defensa contra las computadoras cuánticas al permitir la sustitución de los algoritmos de clave pública vulnerables a la cuántica de hoy en día con algoritmos resistentes a la cuántica.

**HTTPS (Hypertext Transfer Protocol Secure)** es un protocolo de comunicación web utilizado entre dispositivos de red para una comunicación segura. Cifra tanto la información que un usuario envía a un sitio web como la información que el sitio web envía de vuelta, por ejemplo, información de tarjetas de crédito, extractos bancarios y correo electrónico.

**El recocido cuántico** es un proceso para encontrar el mínimo global de una función objetiva dada sobre un conjunto dado de soluciones candidatas (estados candidatos), mediante un proceso que utiliza fluctuaciones cuánticas. Encuentra un tamaño mínimo absoluto / longitud / costo / distancia desde dentro de un conjunto posiblemente muy grande, pero sin embargo finito de posibles soluciones utilizando la computación basada en la fluctuación cuántica en lugar de la computación clásica.

**La computación cuántica** es el uso de un modelo no clásico de computación. Mientras que los modelos tradicionales de computación como la máquina de Turing o el cálculo Lambda se basan en representaciones clásicas de la memoria computacional, un cálculo cuántico podría transformar la memoria en una superposición cuántica de posibles estados clásicos. Una computadora cuántica es un dispositivo que podría realizar dicho cálculo.

**El entrelazamiento cuántico** es una etiqueta para el fenómeno físico observado que ocurre cuando un par o grupo de partículas se genera, interactúa o comparte proximidad espacial de tal manera que el estado cuántico de cada partícula del par o grupo no se puede describir independientemente del estado de las demás, incluso cuando las partículas están separadas por una gran distancia.

**La puerta cuántica** es un circuito cuántico básico que opera en un pequeño número de qubits. Son los bloques de construcción de los circuitos cuánticos, como lo son las puertas lógicas clásicas para los circuitos digitales convencionales.

**La distribución de claves cuánticas (QKD)** es un método de comunicación segura que implementa un protocolo criptográfico que involucra componentes de la mecánica cuántica. Permite a dos partes producir una clave secreta aleatoria compartida conocida solo por ellos, que luego se puede usar para cifrar y descifrar mensajes.

**La mecánica cuántica** (también conocida como física cuántica, teoría cuántica, modelo mecánico de ondas o mecánica matricial) es una teoría fundamental en física que describe la naturaleza en las escalas más pequeñas, incluidas las atómicas y subatómicas.

**La superposición cuántica** es un principio fundamental de la mecánica cuántica, donde un sistema está en más de un estado a la vez. Afirma que, al igual que las ondas en la física clásica, dos (o más) estados cuánticos cualesquiera se pueden sumar ("superpuestos") y el resultado será otro estado cuántico válido; y a la inversa, que cada estado cuántico puede representarse como una suma de dos o más estados distintos.

**La "supremacía" cuántica** está demostrando que un dispositivo cuántico programable puede resolver un problema que las computadoras clásicas prácticamente no pueden (independientemente de la utilidad del problema). En comparación, la ventaja cuántica más débil es demostrar que un dispositivo cuántico puede resolver un problema más rápido que las computadoras clásicas. El uso del término "supremacía" ha sido controvertido, y la ventaja cuántica ahora se usa a menudo para ambas descripciones.**16**

**Qubit o bit cuántico** es la unidad básica de la información cuántica. Es la versión cuántica del bit binario clásico. Un qubit es un sistema mecánico cuántico de dos estados (o dos niveles), uno de los sistemas cuánticos más simples que muestra la peculiaridad de la mecánica cuántica. Permite que el qubit esté en una superposición coherente de ambos estados/niveles simultáneamente, una propiedad que es fundamental para la mecánica cuántica y la computación cuántica.

**La clave simétrica** es un enfoque en criptografía cuando se debe usar la misma clave para descifrar o cifrar un mensaje. La criptografía asimétrica utiliza un par de claves relacionadas, cuando una se utiliza para cifrar una carga útil y la otra para descifrarla. En la criptografía de clave pública, los usuarios publican una de las claves, la clave pública, y mantienen la otra en secreto, la clave privada. Luego, se usa la clave pública para cifrar el mensaje y se necesita la clave privada para descifrarlo.

**ANEXO II. UNA BREVE HISTORIA DEL CIFRADO, EL CRIPTOANÁLISIS Y LAS COMPUTADORAS DIGITALES**

**Cifrado y criptoanálisis**

Desde la antigüedad, la criptografía ha sido una carrera entre aquellos que intentan mantener secretos y adversarios que intentan descubrirlos. Los primeros ejemplos de cifrados de transposición se remontan al menos al año 485 a.C., cuando los soldados griegos envolvían una tira de papiro alrededor de un bastón, un escil, escribían un mensaje a lo largo de su longitud y enviaban el papiro. Los receptores podían descifrar mensajes envolviéndolos alrededor de otro escil del mismo grosor. En este caso, la forma del personal representaba la clave de cifrado. El primer registro histórico conocido de cifrado de sustitución es del Imperio Romano: se cree que el emperador Julio César envía mensajes cifrados al orador Cicerón reemplazando cada letra por su tercera siguiente en el alfabeto. El cifrado César fue roto ya en el siglo 7 por criptógrafos árabes, que documentaron las técnicas de criptoanálisis, la ciencia de deshacer cifrados (Singh, 1999). En "A Manuscript on Deciphering Cryptographic Messages", el filósofo al-Kindī observó que cada idioma tiene una frecuencia característica de letras y secuencias y que al capturarlos utilizando textos de muestra de ese idioma, el criptoanalista podría descifrar cualquier mensaje.

Las sustituciones simples se volvieron obsoletas en la década de 1700 debido a la proliferación de Cámaras Negras, oficinas mantenidas por las naciones europeas para romper cifrados y recopilar inteligencia. A medida que Black Chambers industrializó el criptoanálisis, los criptógrafos se vieron obligados a adoptar sustituciones más elaboradas recurriendo a métodos poli alfabéticos. En lugar de referirse a un solo alfabeto para el cifrado, los criptógrafos cambiarían entre dos alfabetos para elegir símbolos de reemplazo. El cifrado Vigenère, que se cree que es el primer método poli alfabético y también llamado Le Chiffre Indéchiffrable, se describió por primera vez en 1553 y siguió siendo popular hasta que se rompió en el siglo 19.

La Primera Guerra Mundial intensificó la necesidad de secreto. La radio había aportado nuevas capacidades sobre el terreno, como la coordinación de tropas a larga distancia. Sin embargo, las olas abiertas también permitieron a los enemigos escuchar las comunicaciones. Cada nación utilizó sus propios métodos de cifrado. Algunos, como el cifrado Playfair utilizado por los británicos, permanecieron intactos durante la guerra; otros, como el ADFGVX alemán, se rompieron. En el período posterior a la Primera Guerra Mundial, las máquinas se convirtieron en la solución lógica para el aumento del volumen de material a descifrar. Varios dispositivos criptográficos mecánicos se inventaron en el período anterior a la Segunda Guerra Mundial, como el dispositivo de cifrado M-94 utilizado por el ejército de los Estados Unidos; el C-36 del ejército francés; y el Enigma del Ejército Alemán (Dooley, 2018). Además, se inventaron varios dispositivos para romper su cifrado. Para romper Enigma, Alan Turing, uno de los inventores de la computadora digital, creó Bombes para el centro de operaciones secreto británico. Colossus, la primera computadora programable basada en el diseño de Turing, permitió a los británicos romper el cifrado Lorenz, que protegía las comunicaciones del alto mando alemán. La marina de los Estados Unidos construyó máquinas analógicas totalmente automáticas para romper el cifrado del dispositivo Purple de Japón.

Después de la Segunda Guerra Mundial, las computadoras digitales dominaron la criptografía. Mientras que los dispositivos mecánicos están sujetos a limitaciones físicas, las computadoras operan a una velocidad mucho mayor y codifican números, no letras, dando acceso a un gran conjunto de nuevas operaciones. A principios de la década de 1960, el transistor reemplazó al tubo de vacío en los circuitos digitales para computadoras y, a fines de esa década, se inventó Internet, iniciando la era digital actual. A principios de la década de 1970, las computadoras estuvieron disponibles para los clientes comerciales, lo que exigía capacidades de secreto de los proveedores. A medida que los ciudadanos comunes se convirtieron en usuarios de computadoras, la criptografía se hizo necesaria, por ejemplo, para permitir transacciones con tarjeta de crédito o transmisión de información personal a través de redes públicas. Apareció una plétora de nuevos esquemas criptográficos, lo que llevó a la Oficina Nacional de Estándares de los Estados Unidos a intervenir en 1973 y abrir una competencia pública para elegir un estándar criptográfico para los Estados Unidos. El cifrado Lucifer de IBM, renombrado Data Encryption Standard (DES), fue elegido como el estándar oficial de Estados Unidos en 1977. Después de que DES se rompió en una competencia pública en 1997, fue reemplazado como estándar por Triple-DES en 1999, y se retiró cuando NIST adoptó el Estándar de Cifrado Avanzado (AES) a principios de la década de 2000.

Hasta mediados de la década de 1970, todos los métodos criptográficos utilizaban claves simétricas: la misma clave debe usarse para descifrar o cifrar un mensaje. Por lo tanto, para usar criptografía, los remitentes y receptores tenían que compartir claves por adelantado, una cuestión complicada de logística. Whitfield Diffie, Martin Hellman y Ralph Merkle resolvieron el problema en 1976. El intercambio de claves Diffie-Hellman permitió a dos partes acordar una clave secreta utilizando un canal público. El trío creó efectivamente la criptografía asimétrica, mediante la cual las operaciones se asocian con un par de claves relacionadas: cuando una se usa para cifrar una carga útil, la otra la descifra y viceversa. Dos años más tarde, Rivest, Shamir y Adleman ampliaron el concepto con criptografía de clave pública, mediante la cual los usuarios publican una de las claves, la clave pública, y mantienen la otra en secreto, la clave privada. Los métodos asimétricos permitieron nuevas aplicaciones. Por ejemplo, las personas pueden reclamar su identidad mostrando un mensaje de texto plano y el cifrado producido por su clave privada, que podría verificarse descifrando el cifrado utilizando su clave pública. La criptografía asimétrica (incluida RSA), también conocida como criptografía de clave pública, es ampliamente utilizada en Internet, incluso por el sistema financiero, para intercambios de claves, firmas digitales, no repudio y autenticación. Las claves públicas y privadas también sustentan las monedas digitales y las tecnologías blockchain.

La criptografía asimétrica o de clave pública es la más vulnerable a la computación cuántica. Las ventajas potenciales de las computadoras cuánticas se hicieron evidentes a principios de la década de 1980, cuando Richard Feynman señaló dificultades esenciales para simular sistemas mecánicos cuánticos en computadoras clásicas, y sugirió que construir computadoras basadas en los principios de la mecánica cuántica nos permitiría evitar esas dificultades (Nielsen, 2010). La idea se refinó a lo largo de la década de 1980. En 1994, Peter Shor publicó un algoritmo que permitiría realizar la factorización primo mucho más rápido cuando se utilizan propiedades cuánticas. Como los números primos se utilizan en el núcleo de la mayoría de los métodos de criptografía asimétrica, el algoritmo de Shor utilizado en las computadoras cuánticas podría hacer que la mayoría de la seguridad de Internet sea inválida.

Si bien la computación cuántica representa una amenaza para la seguridad de Internet, la mecánica cuántica también puede proporcionar criptografía irrompible. En la década de 1980, los investigadores de IBM propusieron una nueva forma de aprovechar la polarización de fotones para realizar la distribución de claves. Mediante el uso de las leyes de la física, la distribución de claves cuánticas (QKD) puede volverse impenetrable porque los espías no pueden interceptar las comunicaciones sin interferir con ellas. Tales sistemas experimentales se han implementado desde la década de 1990, pero están muy lejos del uso comercial.

**Computadoras digitales**

El origen de las computadoras clásicas se remonta a francia del siglo 17. En la pequeña ciudad de Clermont-Ferrand, Blaise Pascal construyó la primera máquina que permitió a la humanidad manipular números realizando mecánicamente las cuatro operaciones aritméticas básicas. La capacidad humana para hacer matemáticas fue mejorada nuevamente en 1822 por el Difference Engine de la polímata inglés Charles Babbage. Podía tabular funciones polinómicas, lo que permitía la aproximación mecánica de cálculos complejos como funciones logarítmicas o trigonométricas. Babbage también diseñó una computadora de propósito general, la Máquina Analítica. Sin embargo, el proyecto fue terminado debido a problemas de ingeniería y financiación, y nunca se construyó un motor de trabajo en la vida útil de Babbage. Las siguientes máquinas notables en la historia fueron los analizadores diferenciales, computadoras analógicas que utilizan mecanismos de rueda y disco para realizar la integración de ecuaciones diferenciales. El primer analizador diferencial construido en el MIT por Vannevar Bush en 1931 jugó un papel particularmente importante en la historia para inspirar a uno de los estudiantes graduados de Bush, Claude Shannon. En 1938, inventó los circuitos digitales para su tesis de maestría (Shannon, 1938), demostrando que las operaciones matemáticas complejas pueden realizarse haciendo funcionar la electricidad a través de configuraciones específicas de componentes electrónicos.

El trabajo de Shannon se complementó con la tesis doctoral de Alan Turing. Surgió como respuesta al desafío producido por David Hilbert y Sir Bertrand Russel en la década anterior, el problema de Entscheidungs, o el problema de la detención: los matemáticos deben buscar un algoritmo para probar si alguna afirmación es verdadera en un sistema. La Máquina de Turing era un dispositivo imaginario compuesto por un mecanismo que mueve una cinta infinita hacia adelante y hacia atrás, escribe símbolos en ella y lee símbolos grabados. La tesis de Church-Turing luego establece que este dispositivo puede calcular cualquier función en números naturales siempre que exista un método efectivo para obtener su valor. Y, a la inversa, que tal método existe solo si el dispositivo puede calcular esa función.

Por lo tanto, la ingeniería se encontró con las matemáticas: para cuando Claude Shannon inventó los circuitos digitales, Turing acababa de diseñar el plano matemático de una computadora de propósito general. Los circuitos resultantes, las computadoras digitales completas de Turing, eran capaces de calcular todas las funciones que la máquina imaginaria puede calcular. Mientras que el Coloso, un secreto de guerra construido por la inteligencia británica para romper las comunicaciones de Hitler, fue el primero en la historia, las computadoras modernas se basan en la arquitectura diseñada dentro de un equipo dirigido por John Von Neumann, utilizado por primera vez en EDVAC (Electronic Discrete Variable Automatic Computer) de 1949. Los dispositivos digitales contemporáneos son dispositivos turing-completos generalmente compuestos de unidades de procesamiento (por ejemplo, CPU), dispositivos de almacenamiento (por ejemplo, RAM / ROM y unidades de disco) y mecanismos de entrada y salida (por ejemplo, teclado y video). Las computadoras de escritorio y los teléfonos inteligentes siguen este mismo diseño.

Una vez inventado el diseño, la ingeniería avanzó enormemente en acelerar cada uno de sus componentes. Por ejemplo, los tubos de vacío eran componentes prominentes de las CPU en las primeras máquinas, necesarios por su capacidad singular para controlar la dirección del flujo de electrones a través de sus terminales. Sin embargo, los tubos presentaron varios desafíos relacionados con la durabilidad y la confiabilidad. Fueron reemplazados por transistores inventados en la década de 1940, que a su vez fueron reemplazados por circuitos integrados a lo largo de la década de 1960. Desde entonces, el rendimiento y el tamaño de las computadoras digitales han sido dictados por la tecnología de fabricación de circuitos integrados. Desde la década de 1960, tales tecnologías nos han permitido duplicar el número de componentes en cada circuito integrado cada 18 meses, según lo previsto por Gordon Moore de Intel en 1965, la llamada ley de Moore. Tal avance, por ejemplo, es la razón por la que pudimos agrupar toda la potencia informática utilizada en la cápsula de aterrizaje lunar del Apolo 11 en 1969 en un solo dispositivo a principios de la década de 2010. Saltos similares ocurrieron para otros componentes, generando cosas como pantallas plegables delgadas como papel o dispositivos del tamaño de una cabeza de alfiler que pueden almacenar enciclopedias enteras.

Sin embargo, dado que tales máquinas son máquinas de Turing en su núcleo, también están sujetas a las limitaciones de la máquina de Turing. Uno de ellos es su incapacidad para abordar ciertos problemas matemáticos, los llamados problemas NP-Hard. El más infame de ellos es el problema del agente de ventas itinerantes: calcular la ruta más corta a través de una serie de ciudades y visitar cada una exactamente una vez. Las computadoras digitales pueden calcular soluciones para configuraciones pequeñas, aproximadamente comparando todas las rutas posibles entre sí. A medida que crece el tamaño del problema, los matemáticos inventaron algoritmos heurísticos para encontrar soluciones razonables sin pasar por todas las posibilidades, pero no hay certeza de que se encuentre el camino óptimo.

Como cada problema de NP-Hard es equivalente al agente de ventas itinerante, desbloquear su solución pondría en marcha un nuevo universo de posibilidades, para muchas optimizaciones. Esta es la clave que tienen las computadoras cuánticas.

**ANEXO III. ALGORITMOS CRIPTOGRÁFICOS MODERNOS Y SUS VULNERABILIDADES A LAS TECNOLOGÍAS ACTUALES**

La criptografía actual se basa en tres tipos principales de algoritmos: claves simétricas, claves asimétricas (públicas) y funciones hash algorítmicas, o hashing. En el Apéndice IV se enumeran los algoritmos principales actuales y pasados.

El algoritmo AES es actualmente el estándar aceptado para el cifrado de clave simétrica. El NIST lo seleccionó en 2001 para reemplazar el antiguo estándar (Triple-DES). Aunque múltiples publicaciones introdujeron nuevos esquemas de criptoanálisis que intentaban socavar el AES, la comunidad criptográfica demostró que eran ineficaces. Por ejemplo, Biryukov y otros (2010) esbozaron un ataque efectivo contra variaciones específicas de AES, lo que reduce la fuerza del cifrado. Sin embargo, tales ataques se consideraron poco prácticos y se descartaron como una no amenaza para los algoritmos de cifrado AES.

El algoritmo RSA, un estándar popular para el cifrado asimétrico (clave pública), se utiliza ampliamente para proteger la confidencialidad y la firma digital. El algoritmo RSA ha sido resistente a las técnicas de criptoanálisis desde su publicación en 1977, a pesar de varios intentos de desafiar su fuerza. Anteriormente se sugirió que cierto conocimiento del mensaje de texto plano, bajo condiciones específicas, podría debilitar el cifrado (Durfee, 2002). Sin embargo, los algoritmos RSA siguen siendo resistentes. Aunque algunos esquemas se pueden usar para reducir el tiempo y la memoria necesarios para romper el cifrado de clave pública, hasta ahora se ha demostrado que los tamaños de clave adecuados y las mejores prácticas hacen que la criptografía de clave pública sea resistente a los ataques informáticos clásicos. Una computadora digital tardaría miles de millones de años en romper la clave RSA de 2.048 bits estándar actual (CISA, 2019).

Las funciones hash algorítmicas se vieron afectadas temporalmente por el criptoanálisis, pero el progreso reciente restauró su efectividad. En 2005, el matemático Lenstra demostró un ataque de hashcollision17 contra una de las funciones de hashing más utilizadas llamada MD5 (Lenstra et al, 2005). Otros investigadores demostraron más tarde que una computadora de escritorio decente equipada con un procesador gráfico (GPU) barato podría encontrar una colisión de hash en menos de un minuto. El algoritmo MD5 fue retirado oficialmente por el NIST en 2011. Sin embargo, todavía se usa ampliamente a pesar de sus debilidades conocidas, lo que demuestra el problema duradero con el reemplazo de sistemas heredados. El NIST organizó un concurso para crear el siguiente estándar para la función hash algorítmica llamada SHA-3 para superar el avance del criptoanálisis que socava MD5 y las versiones anteriores de los algoritmos SHA. Si bien hay algunas debilidades posibles,18 SHA-3 fue seleccionado en 2015 y se convirtió en el estándar aprobado (Morawiecki et al, 2014). Además, casi cualquier algoritmo criptográfico se puede fortalecer aumentando sus tamaños de clave, pero eso requeriría más potencia de procesamiento y, por lo tanto, aumentaría los costos de ejecución del algoritmo, lo que a menudo lo haría prohibitivamente caro.

Más allá del algoritmo de cifrado en sí, una clase diferente de ataques estudia los sistemas exógenos. Los ataques de canal lateral se dirigen al software, firmware y hardware utilizados para implementar el algoritmo de cifrado. Las vulnerabilidades de software y hardware suelen ser más fáciles de encontrar y explotar en comparación con romper las técnicas matemáticas subyacentes del algoritmo de cifrado. Las vulnerabilidades, o errores, son el resultado de errores de implementación durante las fases de desarrollo. Sin embargo, algunas vulnerabilidades pueden ser el resultado de un mal uso o una configuración incorrecta de las bibliotecas criptográficas. La vulnerabilidad Heartbleed (CMU, 2014) fue un ejemplo devastador de una vulnerabilidad descubierta en OpenSSL, una biblioteca criptográfica ampliamente utilizada para asegurar la comunicación de red. (Lazar et al., 2014) informaron que el 17 por ciento de las vulnerabilidades en las bibliotecas criptográficas publicadas por CVE19 entre 2011 y 2014 fueron errores cometidos durante las fases de desarrollo, mientras que el 83 por ciento restante estaba relacionado con el mal uso o la configuración incorrecta por parte de las aplicaciones de alojamiento.

**ANEXO IV. PRINCIPALES ALGORITMOS CRIPTOGRÁFICOS**

|  |  |  |
| --- | --- | --- |
| **Algoritmos Simétricos** | **Descripción** | **Estado de Criptoanálisis** |
| 1. Enigma | El Enigma fue una máquina de cifrado construida por la Alemania nazi para cifrar / descifrar mensajes durante la Segunda Guerra Mundial. | El cifrado enigma fue roto en 1932 por la Oficina de Cifrado polaca con la ayuda de los aliados franceses y británicos. El Enigma tenía varios procedimientos mal diseñados que hicieron posible la ingeniería inversa. Los británicos utilizaron la máquina Bombe para ayudar a romper mensajes cifrados al descifrar permuta-ciones (Tang et al, 2018) |
| 2. DES | El estándar de cifrado de datos fue desarrollado en la década de 1970 por IBM. Una versión de la misma fue publicada oficialmente como estándar federal de los Estados Unidos en 1977. El tamaño de la clave DES era de 56 bits. | DES fue descifrado en 1998 por la Electronic Frontier Foundation mediante la construcción de una máquina llamada EFF DES cracker y la fuerza bruta de la clave DES donde la máquina tardó 3 días en encontrar la clave de cifrado (EFF, 1999). |
| 3. Triple-DES | Triple Data Encryption Standard (Triple DES) o TDEA (Triple Data Encryption Algorithm) se introdujo en 1995 debido a la creciente preocupación de la fuerza de DES para resistir ataques de fuerza bruta. Triple-DES todavía está aprobado por el gobierno de los Estados Unidos para proteger datos confidenciales no clasificados, pero bajo ciertas condiciones (utilizando tres claves distintivas con cierta longitud de clave). | Los nuevos esquemas de criptoanálisis, como el ataque meet-in-the-middle, demostraron ser efectivos para reducir la fuerza de la clave Triple-DES, considerando que alguna variación del algoritmo era insegura. El NIST está dejando de usar Triple-DES para fines de 2023 (NIST, 2019). |
| 4. AES | Advanced Encryption Standard fue seleccionado en el programa NIST de 1997 para desarrollar un reemplazo de DES. AES fue introducido en 2001 por el NIST y tenía tamaños de clave de 128, 192 y 256 bits con 10, 12 y 14 rondas respectivamente. | A principios de la década de 2000, algunos criptoanalistas propusieron formas de romper el estándar, pero la comunidad de criptografía demostró que eran ineficaces. En 2009 se introdujo un nuevo ataque de canal lateral que redujo ligeramente la fuerza clave AES. Biryukov et al. (2010) presentaron un ataque efectivo a claves AES de 192 y 256 bits reduciendo sus fortalezas a claves de 176 y 22.9 bits respectivamente |
| 5. Twofish | Uno de los cinco finalistas de AES en el programa NIST de 1997 para desarrollar un reemplazo a DES. Si bien tiene una estructura similar a DES, se ha demostrado que Twofish es eficiente con el uso de la memoria y la velocidad de cifrado / descifrado de mensajes en comparación con otros algoritmos simétricos. | Moriai, et al. (1999) presentaron un criptoanálisis diferencial truncado del cifrado de bloques en Twofish reduciendo el número de rondas a 5 de una permutación aleatoria que requiere un texto plano conocido. El mismo año Ferguson (1999) presentó un ataque diferencial imposible rompiendo 6 rondas de la versión de clave de 256 bits utilizando 2256 pasos que es más rápido que una búsqueda exhaustiva. |

|  |  |  |
| --- | --- | --- |
| **Algoritmos Asimétricos** | **Descripción** | **Estado de Criptoanálisis** |
| 1. Diffie-Hellman | Diffie-Hellman es uno de los primeros métodos de intercambio de clave pública. Nombrado en honor a Whitfield Diffie y Martin Hellman que lo publicaron, este algoritmo se consideró un gran avance en criptografía, ya que permitía a las partes intercambiar mensajes seguros a través de un canal de comunicación no confiable (Diffie et al, 1976). | Se sabe que el intercambio de claves Diffie-Hellman es susceptible a los ataques man-in-the-middle. Las nuevas variaciones de Diffie-Hellman han abordado este problema. Sin embargo, Heninger (2015) discute un método para realizar precálculos para un número primo que puede debilitar el estándar y hacerlo menos seguro de lo que se cree. |
| 2. ElGamal | ElGamal es un cifrado de clave asimétrica basado en el logaritmo discreto (El Gamal, 1985) y el intercambio de claves Diffie-Hellman. ElGamal es ampliamente utilizado en el sistema de cifrado de correo electrónico Pretty Good Privacy (PGP) y GNU Privacy Guard (GPG), entre otros. | Los enfoques de criptoanálisis contra ElGamal se introdujeron en Allen (2008). Sin embargo, los autores admiten que estos ataques son efectivos contra el algoritmo en ciertas condiciones de selección de longitud y clave y se pueden evitar configurando los criptosistemas. |
| 3. Rivest– Shamir– Adleman (RSA) | Desarrollado y publicado por Rivest-Shamir-Adleman en 1977, este algoritmo se deriva de la dificultad de factorizar grandes enteros que son el producto de dos grandes números primos. RSA es ampliamente utilizado para el establecimiento de claves, así como para generar y verificar firmas digitales. | Inicialmente, los ataques propuestos eran para escenarios en los que se utiliza el mismo texto sin formato con diferentes claves públicas (diferente destinatario) con acceso al texto cifrado. Johan Håstad encontró una mejora del ataque donde el texto plano no tiene que ser el mismo, sino con una relación lineal entre los mensajes de texto plano. Don Coppersmith más tarde mejoró este ataque para ganar algunas eficiencias (Durfee, 2002). Sin embargo, la selección adecuada de la longitud y el seguimiento de las mejores prácticas confirman la fuerte seguridad de RSA. |
| 4 Elliptic Curve Digital Signature Algorithm (ECDSA) | ECDSA requiere claves de cifrado más pequeñas en comparación con otros algoritmos de cifrado asimétrico. Además, el tiempo de ejecución de ECDSA para cifrar/descifrar mensajes es más rápido que otras claves asimétricas, y este algoritmo requiere menos espacio de almacenamiento y ancho de banda de transmisión. | Los esquemas propuestos para reducir la fuerza de ECDSA incluyen el algoritmo de Pohlig-Hellman, Rho de Pollard y el algoritmo Rho de Pollard paralelizado más efectivo. Sin embargo, las mejores prácticas en aleatorización y selección de claves considerarían estos algoritmos ineficaces (Johnson et al, 2001). |
| 5 Super-singular Isogeny Key Exchange (SIDH) | En los esfuerzos por desarrollar un algoritmo criptográfico asimétrico (clave pública) de seguridad cuántica, SIDH se desarrolló sobre la base de la dificultad conjeturada de encontrar isogenias entre curvas elípticas supersingulares. Está motivado por el desarrollo de un algoritmo cuántico de tiempo subexponencial para construir isogenias entre curvas elípticas (De Feo et al., 2011). | Galbraith et al. (2016) afirman que ciertos ataques contra SIDH, como los ataques de canal lateral y de falla, pueden reducir la fuerza clave. Los autores creen que la industria verá más literatura e investigación en los criptoanálisis de SIDH en un futuro cercano a medida que se vuelva más popular y ampliamente adoptado. |

|  |  |  |
| --- | --- | --- |
| **Funciones Hash** | **Descripción** | **Estado de Criptoanálisis** |
| 1. MD5 | Esta función hash criptográfica fue desarrollada por el criptógrafo Ronald Rivest del Laboratorio de Ciencias de la Computación del MIT. La función MD5 produce un resumen hash largo de 128 bits. Se convirtió en un estándar RFC # 1321 en 1991 y fue ampliamente utilizado para verificaciones de integridad, así como hash de contraseñas, entre otras funciones sensibles. | Lenstra et al. (2005) demostraron un ataque de hashcollision al generar dos claves públicas con el mismo resumen de hash MF5. Por lo tanto, MD5 se considera una función hash débil y ya no se utiliza para funciones de seguridad críticas. |
| 2. SHA-1 | Una función hash criptográfica desarrollada y diseñada en 1995 por la NSA. La función SHA-1 produce un resumen hash de 160 bits con más rondas que MD5. SHA-1 fue ampliamente utilizado entre los principales navegadores web con certificados SSL. | En 2017, un grupo de investigadores demostró un ataque de colisión completa contra SHA-1 (Stevens et al., 2017). SHA-1 fue obsoleto por el NIST en 2011. |
| 3. SHA-2 | Una función hash criptográfica desarrollada y diseñada en 2001 por la NSA. La función hash SHA-2 puede producir diferentes tamaños de resumen 224, 256, 384 o 512 bits con 64 u 80 rondas. SHA-2 reemplazó SHA-1 con certificados SSL entre otros protocolos seguros como SSH, PGP e IPSec. | A lo largo de los años, los criptógrafos han propuesto ataques contra SHA-2 que reducen las variaciones específicas del algoritmo, lo que debilitó la fuerza de SHA-2. Dobraunig et al. (2016) utilizaron criptoanálisis diferencial, además de sofisticadas herramientas de búsqueda para maximizar la efectividad con SHA-512/224 y SHA512/256. SHA-2 sigue siendo un estándar válido y es ampliamente utilizado. |
| 4. SHA-3 (Keccak) | El último miembro del Algoritmo Hash Seguro seleccionado a través de la competencia NIST 2007 que se completó en 2015. SHA-3 (originalmente llamado KECCAK) no es una variación de su predecesor (Sha2, SHA-1 o MD5). El algoritmo de SHA-3 es estructuralmente diferente y se basa en una función de esponja criptográfica (Bertoni et al., 2007). La función hash SHA-3 puede producir diferentes tamaños de resumen 224, 256, 384 y 512. | Morawiecki et al. (2014) describen un ataque de preimagen basado en criptoanálisis rotacional para reducir las rondas del algoritmo contra la variación SHA-3 de 512 bits, lo que puede reducir ligeramente el tiempo y la memoria necesarios para romper este algoritmo. |

1. Nos gustaría agradecer, sin implicaciones, a Andreas Bauer, Sonja Davidovic, Davide Furceri, Dong He y Herve Tourpe por sus útiles comentarios y sugerencias sobre versiones anteriores del documento; y Mariam Souleyman por su excelente asistencia administrativa y editorial.

2. Macmillan (1971, p. 158).

3. En la literatura sobre computación cuántica, las computadoras que procesan información de acuerdo con las leyes clásicas de la física se conocen como computadoras clásicas, a diferencia de las computadoras cuánticas. En este artículo, utilizamos los términos computadoras clásicas, convencionales, digitales y tradicionales indistintamente.

4. Estos riesgos se conocen como ataques de "cosechar ahora, descifrar más tarde".

5. "Principios de incertidumbre: comercialización de computadoras cuánticas". —The Economist, 26 de septiembre de 2020.

6. "Abarrotando más poder en un dispositivo cuántico". —Blog de investigación de IBM, 4 de marzo de 2019.

7. Si bien el objetivo final es construir computadoras cuánticas totalmente corregidas de errores, un objetivo intermedio es construir aplicaciones comerciales prácticas de computadoras cuánticas ruidosas de escala intermedia (NISQ). Actualmente el ruido está presente tanto en los quantumannealers como en los tipos de máquinas NISQ, lo que limita la complejidad de los problemas que pueden resolver.

8. China alcanza un nuevo hito en las comunicaciones cuánticas basadas en el espacio, —Scientific American, 25 de junio de 2020.

9. China ha desarrollado la primera estación satelital cuántica móvil del mundo, NewScientist, 10 de enero de 2020.

10. Unhackable internet, MIT Technology Review, 2 de abril de 2020.

11. Investigadores logran una teletransportación cuántica sostenida y de alta fidelidad, Phys.org, 29 de diciembre de 2020.

12 <https://www.darpa.mil/program/quantum-assisted-sensing-and-readout>.

13. El criptoanálisis, el análisis del mensaje secreto cifrado (texto cifrado) para obtener la mayor cantidad de información posible sobre el mensaje original, estudia los algoritmos, las matemáticas y las técnicas para descubrir los mensajes secretos. Al explotar las debilidades en los métodos de cifrado subyacentes, se puede aprender mucho sobre el mensaje original sin conocer la clave secreta (véase el anexo III).

14. "Miles de organizaciones ejecutan la mayoría de sus computadoras en sistemas operativos obsoletos, casi triplicando las posibilidades de una violación de datos." —BitSight.

15 <https://newsroom.ibm.com/2020-11-30-IBM-Cloud-Delivers-Quantum-Safe-Cryptography-and-Hyper-Protect-Crypto-Services-to-Help-Protect-Data-in-the-Hybrid-Era>

16. En lugar de 'supremacía' usa 'ventaja cuántica': Nature, 10 de diciembre de 2019.

17. En un ataque de colisión de hash, un atacante intenta encontrar dos entradas al algoritmo hash que producirían el mismo valor de hash. Cuando se encuentra una colisión de este tipo, las funciones hash algorítmicas se consideran inseguras.

18. Describen un ataque de preimagen basado en criptoanálisis rotacional que redirige las rondas del algoritmo contra la variación sha-3 de 512 bits. Como resultado, se requeriría menos tiempo y memoria para encontrar una colisión de hash.

19. Las vulnerabilidades y exposiciones comunes (CVE) son un esfuerzo de la comunidad internacional de ciberseguridad para mantener una lista de identificadores comunes para vulnerabilidades de ciberseguridad conocidas públicamente.