¿La informática cuántica pone en riesgo nuestra seguridad digital?

Robin Wilton
Junio de 2020

Física e informática cuánticas

Las computadoras que usamos en la actualidad se basan en valores binarios **("bits")** que representan un valor de 0 o 1. Sin embargo, las computadoras cuánticas utilizan un bit cuántico **("qubit"),** el cual usa una propiedad de las partículas subatómicas para mantener (o **"superponer")** diferentes estados al mismo tiempo. Esto significa que un qubit puede ser 0 y 1 al mismo tiempo. Por lo tanto, una computadora cuántica puede calcular múltiples valores al mismo tiempo, mientras que una computadora clásica no. Esto podría socavar las formas en que usamos el cifrado para asegurar gran parte de nuestra vida digital, desde proteger datos confidenciales como información bancaria hasta mantener la privacidad de nuestras comunicaciones en línea.

Por ejemplo, al intentar resolver problemas con múltiples respuestas posibles, elegir la correcta requerirá estadísticamente varios intentos por parte de una computadora clásica. Sin embargo, si una computadora cuántica puede probar todas las soluciones posibles a la vez, el tiempo que le lleva encontrar la respuesta correcta disminuirá drásticamente. Esto se puede aplicar para atacar las dos formas dominantes de cifrado que se utilizan en la actualidad: **simétrica** y **asimétrica**.

Computadoras cuánticas y cifrado

El **cifrado simétrico** utiliza una clave para "bloquear" los datos y una clave idéntica para "desbloquearlos": como una pequeña caja fuerte. Un método para romper el cifrado simétrico es un "ataque exhaustivo": el atacante prueba todas las claves de descifrado posibles hasta encontrar la correcta.

Se diseñan buenos algoritmos de cifrado simétrico para garantizar, en primer lugar, que *sin la clave*, la forma más eficaz de descifrar los datos sea mediante un ataque exhaustivo. También están diseñados para que la cantidad de claves posibles sea tan grande que un ataque exhaustivo no resulte práctico para una computadora clásica. La cantidad de esfuerzo requerido **(el "factor trabajo")** para montar un ataque exhaustivo se puede cuantificar, en función de la longitud de la clave y los recursos necesarios, como la potencia de cálculo, la memoria, la energía y el dinero. Si las claves son lo suficientemente largas, el número de posibles respuestas incorrectas es tan colosal que el factor trabajo excede los límites prácticos de espacio y tiempo. Puede que la energía no alcance para alimentar suficientes computadoras a fin de que hagan el trabajo, o que no haya suficiente silicio para fabricar suficientes chips de computadora a fin de hacer las computadoras.

Sin embargo, la informática cuántica significaría que se puedan probar muchas claves posibles simultáneamente y, en combinación con nuevas formas de clasificar los resultados[1], reduciría en gran medida el tiempo necesario para encontrar la clave correcta. La reducción es tan grande que es como si hubiera reducido a la mitad la

1 Para obtener más información sobre este aspecto, busque "Algoritmo de Grover" para claves simétricas y "Algoritmo de Shor" para cifrado asimétrico basado en factorización.

longitud de la clave utilizada, reduciendo la dificultad del problema a su raíz cuadrada. Para dar un ejemplo trivial: si la longitud de la clave significa que hay 10.000 claves posibles para probar, reducir a la mitad la longitud de la clave reduciría el factor trabajo a tener que probar solo 100 claves posibles.

El **cifrado asimétrico** utiliza una clave para "bloquear" los datos y una clave diferente para "desbloquearlos", como bloquear un candado. Cualquiera puede cerrar un candado abierto, pero solo la persona que posea la clave o combinación puede volver a abrirlo. Muchos protocolos de comunicación se basan en el cifrado asimétrico, en particular para asegurar un intercambio inicial de claves simétricas entre los socios que se comunican.

El cifrado asimétrico se basa en operaciones matemáticas que son fáciles de realizar en una dirección, pero más difíciles de revertir. Para ilustrarlo: es mucho más fácil calcular 1303 x 1307, que calcular cuáles dos números se deben multiplicar para obtener 1.703.021[2]. Los ataques a este tipo de cifrado se basan en intentar resolver estos problemas matemáticos, en lugar de buscar exhaustivamente una clave. Sin embargo, como en el caso del cifrado simétrico, una combinación de técnicas de clasificación e informática cuántica podría reducir significativamente el tiempo y el esfuerzo necesarios para un ataque.

La informática cuántica no es fatal para el cifrado... todavía

Desafíos prácticos

El número de qubits en una computadora cuántica en funcionamiento ha aumentado a medida que la tecnología mejora, de alrededor de una docena en 2010 a alrededor de 80 en 2019. Pero aún no llega al número necesario para atacar una clave simétrica de 128 bits, y mucho menos una asimétrica de 4096 bits.

En función de una regla general de lo que actualmente se consideran claves "razonablemente fuertes"[3] para cada tipo de algoritmo criptográfico, la siguiente tabla ilustra el número de qubits necesarios.

Tipo de algoritmo	Longitud de una clave "razonablemente fuerte"	Número de qubits requeridos por bit de clave	Total de qubits requeridos
Simétrico (p. ej., AES)	128 bits	1	128
Curva elíptica	256	~9	2304
RSA	3072	2 (más 2 más)	6146

Figura 1: Número de qubits utilizables necesarios para diferentes tipos de algoritmos

Otro desafío es que los qubits tienden a "descomponerse", especialmente a temperatura ambiente. Necesitan mucho enfriamiento y se interrumpen fácilmente por los efectos eléctricos o ambientales, e incluso entre sí. La estabilidad del uso es un problema, y resolverlo cuesta dinero.

Si los mecanismos criptográficos existentes para cifrar y firmar datos son vulnerables a los ataques, entonces también lo son los datos cifrados y firmados usando esas técnicas. También dependemos del cifrado para proteger la autenticación. Ingresar su contraseña para iniciar sesión en un sitio web, introducir su PIN para autorizar una transacción con tarjeta o incluso desbloquear su automóvil de forma remota: todas estas acciones cotidianas están protegidas por mecanismos de cifrado. Sin embargo, se sabe que reemplazar componentes obsoletos o mecanismos inseguros en toda una empresa y una infraestructura de redes es un proceso lento. La migración de un conjunto de algoritmos de cifrado a otro generalmente implica cambios técnicos, operativos y de procedimientos en toda la organización, y compite en materia de prioridad, recursos y presupuestos con las actividades comerciales del día a día.

Si ha estado almacenando archivos de datos cifrados a lo largo de los años, imagine tener que volver a cifrar todos esos archivos con poca antelación, porque el criptoanálisis cuántico ha posibilitado de repente el

2 Nota: Sí, puede multiplicar 1 por 1.703.021 pero aquí no cuentan, porque 1 no es una clave muy útil.

3 Herramienta de comparación de longitud de claves "BlueKrypt": https://www.keylength.com/en/4/

descifrado. O imagine tener que reemplazar las firmas digitales en un archivo de documentos de largo plazo, como títulos de propiedad. O volver a emitir las llaves físicas de todos los automóviles de un modelo en particular.

Si bien la informática cuántica podría debilitar los algoritmos asimétricos populares como RSA y la curva elíptica, las investigaciones están identificando una serie de alternativas cuántico resistentes basadas en otros tipos de problemas matemáticos4.

¿Qué deben hacer los actores?

Es posible que los consumidores no puedan brindar soluciones técnicas, pero debemos comprender los problemas y expresar una opinión informada, dada la oportunidad, a los responsables de la toma de decisiones y los proveedores de servicios.

Dado que la informática cuántica viable tendría el efecto de reducir a la mitad la longitud efectiva de la clave para los algoritmos simétricos, la contramedida obvia para los desarrolladores de productos de cifrado es al menos duplicar la longitud de las claves utilizadas.

Los responsables de la toma de decisiones deben asegurarse de que la tecnología de cifrado se trate como un elemento fundamental de la infraestructura de TI, con la inversión correspondiente en gobernanza, evaluación de riesgos y planificación. Su estrategia debe:

- Supervisar los desarrollos en informática cuántica y cifrado cuántico resistente.
- Incluir tecnología de cifrado en los ciclos regulares de evaluación de riesgos organizacionales.
- Explorar los lineamientos nacionales y regionales correspondientes, como los publicados por el Instituto Nacional de Estándares y Tecnología de los EE. UU. (Selección y validación de algoritmos de cifrado cuántico[5]; orientación sobre mecanismos criptográficos[6]; guía preliminar sobre Cómo prepararse para la criptografía poscuántica[7]).
- Planificar el recifrado de datos en reposo y la repetición de la firma de artefactos firmados de manera digital.[8]
- Maximizar la agilidad de los algoritmos en caso de que se necesite un cambio de algoritmos/tecnología, especialmente con poca antelación.[9]
- Cultivar la capacidad de la organización para actualizar e implementar la tecnología de seguridad conforme a las mejores prácticas.[10]
- Procurar que la tecnología de seguridad reemplazada no pueda persistir en la infraestructura más allá de su período de "uso seguro".

---

4 Este artículo de Wikipedia (en Inglés) señala algunos de los tipos de problemas que se están considerando: https://en.wikipedia.org/wiki/Post-quantum_cryptography

5 Proceso de validación y selección de estándares de algoritmos de cifrado cuántico del NIST (en Inglés). https://csrc.nist.gov/Projects/post-quantum-cryptography/Post-Quantum-Cryptography-Standardization

6 "Pautas para el uso de estándares criptográficos en el gobierno federal: mecanismos criptográficos", Revisado el 1 de marzo de 2020 (en Inglés) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-175Br1.pdf

7 Guía preliminar "Cómo prepararse para la criptografía poscuántica" del NIST (en Inglés) https://csrc.nist.gov/News/2020/draft-nist-cswp-on-getting-ready-for-pqc

8 Cubierto en la guía preliminar del NIST "Cómo prepararse para la criptografía poscuántica"

9 Pautas del IETF sobre la agilidad de los algoritmos (en Inglés): https://datatracker.ietf.org/doc/rfc7696/

10 Artículo de Internet Society sobre "Criptografía para CEOs" (en Inglés): https://www.internetsociety.org/resources/doc/2018/cryptography-ceo-questions-ctos/