Capítulo 3
Ordenadores cuánticos

1. Quanta y bits

1.1 Física cuántica

En 1900, el físico Max Planck propuso una teoría para explicar la radiación generada por un cuerpo calentado a cierta temperatura. En esta teoría, la energía no se transfiere de forma continua, sino en pequeños paquetes de energía llamados cuantos. En 1905, Albert Einstein retomó el concepto de cuantos de energía en un artículo en el que explicaba el efecto fotoeléctrico, por el que un cuerpo que recibe luz emite electrones. Sobre esta base, muchos otros científicos, entre ellos Niels Bohr, Louis de Broglie, Paul Dirac, Erwin Schrödinger, Wolfgang Pauli, Werner Heisenberg, Max Born, Satyendra Nath Bose y Enrico Fermi, contribuyeron al desarrollo de la física cuántica, que permite describir y predecir fenómenos a escala de átomos y partículas subatómicas. A partir de los años 50, la física cuántica hizo posibles muchas innovaciones tecnológicas como los transistores, los láseres, las células fotovoltaicas y las imágenes por resonancia magnética (IRM). La física cuántica experimentó una nueva fase de desarrollo en los años 80, conocida como la segunda revolución cuántica, cuando los científicos consiguieron aislar objetos cuánticos (átomos, electrones, fotones e iones), manipularlos y medirlos individualmente.

La física cuántica tiene dos propiedades sorprendentes y contradictorias. La primera es la superposición de estados cuánticos. De hecho, es posible que un objeto cuántico se encuentre en un estado superpuesto. Mientras que en la física clásica un objeto estaría en el estado A o en el estado B, en la física cuántica un objeto puede estar en una superposición de los estados A y B. La segunda propiedad es igual de sorprendente: dos objetos cuánticos pueden estar entrelazados. En este caso, sus estados cuánticos están vinculados independientemente de la distancia que los separa.

1.2 El ordenador cuántico

La idea de un ordenador que pudiera aprovechar las desconcertantes propiedades de la física cuántica surgió en los años 80, cuando físicos como Paul Benioff, Richard Feynman y David Deutsch propusieron diseñar ordenadores que utilizaran esas características para simular sistemas físicos cuánticos o realizar cálculos. En los años 90, cuando la computación cuántica todavía era puramente teórica, los matemáticos crearon algoritmos cuánticos y demostraron sus ventajas sobre los que se ejecutaban en ordenadores convencionales.

En un ordenador convencional, la información se almacena y procesa en forma de bits. En un momento dado, un bit solo puede tener un valor, 0 o 1. En un ordenador cuántico la unidad fundamental de información es el bit cuántico, o cúbit. Estos cúbits son implementados por objetos cuánticos en estado de superposición. Un cúbit puede tener simultáneamente el valor 0 y el valor 1, con, cuando se mide, una cierta probabilidad de estar en estado 0 y una cierta probabilidad de estar en estado 1. Esto permite diseñar algoritmos en los que un conjunto de cúbits superpuestos se somete a una sucesión de operaciones lógicas implementadas físicamente sometiendo los objetos cuánticos subyacentes a láseres o microondas. Estas operaciones se denominan puertas cuánticas. El paso por una puerta cuántica modifica el estado de los cúbits manteniendo la superposición de estados. Al final del cálculo se realizan mediciones en los cúbits, que los hacen salir de su estado de superposición y dan el resultado final. El principio de un algoritmo cuántico es aplicar operaciones sobre los cúbits para hacerlos converger, manteniendo la superposición, hacia estados que proporcionan los valores esperados al final de la ejecución del programa. Algunos algoritmos cuánticos son probabilísticos, lo que significa que deben ejecutarse varias veces para obtener un resultado suficientemente preciso.

La principal ventaja del ordenador cuántico es que puede resolver ciertos problemas mucho más rápido que los ordenadores convencionales. Hay problemas que pueden resolverse en teoría, pero no en la práctica. Se han ideado algoritmos para encontrar soluciones a estos problemas, pero los tiempos de cálculo en un ordenador convencional aumentan exponencialmente con el tamaño del problema. Un ejemplo es el del viajero comercial que tiene que pasar por N ciudades y solo quiere pasar una vez por cada una de ellas. Si el problema es pequeño, el ordenador puede ejecutar el algoritmo en unos segundos o minutos. Pero si el problema es grande, el tiempo de cálculo se vuelve desmesurado, tardando años o incluso decenas, cientos, miles o millones de años, aunque intervenga un gran número de ordenadores muy potentes. Pero algunos de estos problemas pueden resolverse mediante algoritmos cuánticos que pueden ejecutarse en pocos segundos, minutos u horas. Una aplicación muy prometedora es la simulación de moléculas grandes, que podría dar lugar a importantes avances en química y farmacología. También podrían resolverse problemas complejos de optimización en ámbitos como la logística, el transporte o las redes de comunicaciones o de distribución de energía.

Sin embargo, los principios de funcionamiento de un ordenador cuántico tropiezan con numerosas y desalentadoras dificultades prácticas. Los cúbits se implementan mediante objetos físicos utilizando diferentes técnicas: circuitos superconductores, átomos, iones, electrones y fotones. El estado de superposición cuántica de estos objetos es muy frágil y desaparece con extrema rapidez como consecuencia de las interacciones con su entorno. Este fenómeno se denomina decoherencia. En el momento de escribir este libro, el tiempo de coherencia de los cúbits en los ordenadores cuánticos es del orden de una milésima de segundo, lo que limita el número de operaciones que pueden realizar los algoritmos. Para aumentar este tiempo de coherencia, los cúbits se mantienen a temperaturas extremadamente bajas, muy cercanas al cero absoluto, lo que reduce las perturbaciones pero requiere dispositivos de refrigeración complejos y restrictivos. Otro obstáculo es la tasa de error observada en las operaciones realizadas con los cúbits, que también puede restringir el número de puertas cuánticas que pueden utilizarse. Para tener en cuenta estas condiciones, se han desarrollado algoritmos de corrección de errores que permiten obtener cúbits lógicos a partir de varios cúbits físicos. La ventaja es que los cúbits lógicos tienen tasas de error mucho más bajas que los cúbits físicos. El inconveniente es que se necesita un gran número de cúbits físicos para obtener un solo cúbits lógico.

El número de cúbits de un ordenador cuántico se ha convertido en un marcador de la madurez de la tecnología de los distintos fabricantes. Los prototipos de ordenadores cuánticos han pasado de unos pocos cúbits en la década del año 2000 a alrededor de un centenar en el momento de escribir estas líneas. Las empresas que trabajan en ordenadores cuánticos, como Google, Microsoft, IBM, Intel y Rigetti, prevén un rápido aumento del número de cúbits en los próximos años. En mayo de 2022, IBM prometió un ordenador cuántico con más de 4.000 cúbits para 2025. Pero los problemas técnicos que hay que resolver son espinosos, hay un componente de efecto publicitario y es especialmente difícil predecir cuándo verá la luz un ordenador cuántico con varios miles o incluso millones de cúbits, con tasas de error suficientemente bajas y tiempos de coherencia suficientemente largos.

1.3 Distribución cuántica de claves

La física cuántica permite realizar otras proezas que a menudo se confunden erróneamente con el ordenador cuántico. Los protocolos criptográficos de distribución de claves (QKD, *Quantum Key Distribution*), como BB84, utilizan las leyes de la física cuántica para garantizar la transferencia segura de datos entre dos partes a través de fotones. Estas leyes establecen que es imposible medir un cúbit sin hacer que abandone su estado superpuesto y que es imposible clonar o copiar un cúbit en su estado superpuesto. Si un adversario quiere espiar el intercambio entre el emisor y el receptor, tiene que interceptar y medir el estado cuántico de los fotones para obtener la clave. El protocolo está diseñado para que esta medición genere errores, que pueden ser detectados por las dos partes legítimas. También es imposible que el atacante clone un fotón antes de medirlo. Por tanto, las partes que deseen intercambiar secretos como claves criptográficas deben estar equipadas con dispositivos especializados conectados por un enlace capaz de transportar objetos cuánticos, como los fotones, y por un enlace de comunicación convencional. Otros protocolos QKD, como el E91, se basan en el entrelazamiento cuántico. Este tipo de tecnología ya está madura, con equipos disponibles comercialmente e instalaciones operativas entre sitios sensibles separados por algunas decenas de kilómetros, principalmente en el sector bancario.

1.4 Redes de comunicación cuántica

Un campo de investigación relacionado son las redes de comunicación cuántica, que permiten transmitir claves criptográficas y otros tipos de datos sensibles de forma segura entre varios dispositivos. También podrían enviar cúbits entre dos dispositivos y permitir que varios ordenadores cuánticos intercambien cúbits. Estas infraestructuras se basan en el principio del teletransporte de estados cuánticos, que se consigue utilizando fotones entrelazados. Para disponer de una red real que transporte cúbits a lo largo de miles de kilómetros y entre varios nodos necesitamos implantar equipos como repetidores o routers de confianza.

Se está investigando el diseño de redes cuánticas que no requieran ese tipo de equipamiento, a pesar de las leyes y limitaciones físicas (imposibilidad de medir un cúbit en estado superpuesto, imposibilidad de clonar un cúbit, tiempo de decoherencia del cúbit, pérdida de fotones durante la transmisión, interoperabilidad, etc.). Existen prototipos de redes cuánticas formadas por unas decenas de nodos y se están realizando experimentos de comunicaciones cuánticas entre estaciones terrestres y satélites.

2. La espada de Damocles cuántica

2.1 El algoritmo de Shor

En 1995, Peter Shor, un matemático que trabajaba en los legendarios Bell Labs, publicó un artículo [1] en el que describía un método para factorizar números en sus factores primos utilizando un ordenador cuántico. En aquel momento no existía ningún prototipo de ordenador cuántico. El algoritmo de cifrado asimétrico RSA se había creado diecisiete años antes y TLS/SSL, el protocolo de seguridad web que hace un uso extensivo de la criptografía asimétrica, acababa de emerger con Internet para el público en general.

La seguridad de los algoritmos de cifrado asimétrico como el RSA se basa en el hecho de que en la práctica es imposible determinar la clave privada a partir de la clave pública. Un número extraído de la clave pública tendría que ser factorizado, es decir, habría que encontrar los dos números primos de los que este número es el producto. Los tiempos de ejecución de los mejores algoritmos de factorización en un ordenador convencional aumentan de forma subexponencial, lo que significa que los tiempos de cálculo aumentan muy rápidamente con el tamaño del número a factorizar. Cualquiera puede descifrar una clave RSA de 256 bits en su ordenador personal, pero el último récord es una clave RSA de 829 bits descifrada en febrero de 2020 tras 3 meses de cálculo en varios cientos de procesadores.

Descifrar claves RSA de 2.048 o 4.096 bits utilizando un algoritmo de factorización en un ordenador convencional requeriría tiempos de cálculo increíblemente largos. En cambio, el tiempo de ejecución del algoritmo de Shor aumenta polinómicamente con el tamaño del número a factorizar, es decir, mucho más lentamente, lo que permite descifrar claves privadas de algoritmos asimétricos basados en números primos como RSA. El algoritmo de Shor también hace vulnerables los algoritmos basados en el problema del logaritmo discreto, como Diffie-Hellman, un algoritmo de intercambio de claves, y los basados en curvas elípticas, como ECDSA.

Por lo tanto, el algoritmo de Shor es una amenaza para la criptografía asimétrica. Peter Shor sabía lo que implicaba su trabajo, porque menciona a RSA como uno de los objetivos potenciales de su algoritmo. Entre ellos se encuentran los algoritmos de firma electrónica utilizados en procesos de autenticación, pago o certificación de documentos, y los algoritmos de intercambio de claves simétricas que luego se utilizan para cifrar datos o establecer canales de comunicación seguros. Estos algoritmos criptográficos están presentes en un gran número de protocolos y herramientas de seguridad, como TLS/SSL, que protege los flujos hacia sitios web, SSH, que se utiliza para la administración de servidores, y las VPN, que permiten el acceso remoto a redes corporativas. A modo de ejemplo, los analistas estiman que hay 200 millones de sitios web activos en todo el mundo, de los cuales alrededor del 80 % están protegidos por TLS/SSL. La utilización del algoritmo de Shor para descifrar claves privadas podría comprometer la seguridad de empresas y autoridades públicas, ciudadanos y consumidores, objetos y terminales conectados, medios de pago, operaciones de firma y archivo de documentos, etc.

La amenaza no se limita a los procesos y flujos. Los datos almacenados de forma cifrada también se ven afectados, así como los datos cifrados que un atacante podría haber recogido a la espera de descifrarlos.

Un estudio de 2002 [2] estimó que se necesitarían 2N+3 cúbits para ejecutar el algoritmo de Shor en un número de N bits, lo que corresponde a 4.099 cúbits para descifrar una clave RSA de 2.048 bits. Pero se trata de cúbits lógicos, sin errores. Se necesitan muchos más cúbits físicos para que los algoritmos cuánticos funcionen correctamente. Varios equipos de investigadores propusieron formas de descifrar una clave RSA de 2.048 bits y lograron mil millones de cúbits físicos en 2012, 230 millones en 2017 y 170 millones en febrero de 2019. En diciembre de 2019, un estudio [3] llegó a una estimación de 20 millones de cúbits físicos y un tiempo de ejecución del algoritmo de 8 horas. En 2021, un artículo [4] presentó una arquitectura de ordenador cuántico basada en una estructura tridimensional de cúbits que permitiría a un algoritmo Shor adecuado descifrar una clave RSA de 2.048 bits en 177 días utilizando 13.436 cúbits físicos.

Todavía queda mucho camino por recorrer entre la teoría y la práctica. En 2001, unos investigadores consiguieron factorizar el número 15 implementando el algoritmo de Shor en un ordenador cuántico experimental. En 2019, un equipo [5] que utilizaba un ordenador cuántico IBM con 16 cúbits fue capaz de factorizar los números 15 y 21 con bastante facilidad. Para el número 35, solo el 14 % de los intentos dieron el resultado correcto, debido a las altas tasas de error durante la ejecución del programa. Utilizando otro algoritmo llamado *Variational Quantum Factoring*en un ordenador cuántico, los investigadores [6] consiguieron factorizar el número 1.099.551.473.989 a finales de 2020. A finales de 2022, un equipo [7] afirmó haber factorizado el número 261.980.999.226.229 utilizando otro algoritmo, denominado *Quantum Approximate Optimization Algorithm*, en un ordenador cuántico con 10 cúbits físicos. Los investigadores afirman que este método requeriría 372 cúbits físicos para descifrar una clave RSA de 2.048 bits, pero los expertos creen que no es seguro que su algoritmo funcione correctamente para unos tamaños de clave similares.

La cuestión es saber cuándo los avances en los ordenadores cuánticos, el aumento del número de cúbits disponibles y la reducción de las tasas de error, o incluso la creación de nuevos algoritmos que requieran menos cúbits, permitirán descifrar una clave privada. Las estimaciones de los analistas son muy amplias y oscilan entre diez y cincuenta años antes de que llegue el Q-day o día Q, como lo llaman algunos. A corto plazo, los avances de los ordenadores cuánticos serán muy visibles porque los fabricantes competirán en los efectos publicitarios. Pero a más largo plazo, los estados más poderosos serán sin duda menos comunicativos sobre la capacidad de sus servicios de inteligencia para construir o adquirir tales máquinas, y sobre el tiempo que les separa de un ordenador cuántico capaz de aplicar el algoritmo de Shor o cualquier otro algoritmo capaz de descifrar claves asimétricas.

2.2 El algoritmo de Grover

El ordenador cuántico no es la única amenaza para la criptografía asimétrica. Otro algoritmo, creado en 1996 por Lov Grover, también investigador de los Bell Labs, podría debilitar la criptografía simétrica, que utiliza una sola clave para cifrar y descifrar datos. El algoritmo de Grover puede acelerar la resolución de problemas cuando es necesario buscar un valor concreto en una lista de valores sin ordenar, basándose en el concepto de oráculo. Se trata de una función que dice si un dato de la lista es el que se busca o no (y no debe confundirse con los oráculos que se encuentran en el mundo de la blockchain). Mientras que, en un ordenador convencional, el tiempo de ejecución de un algoritmo de búsqueda de este tipo aumenta linealmente con el tamaño de la lista en la que hay que buscar el valor, el algoritmo de Grover es capaz de encontrar el valor con un número de operaciones equivalente a la raíz cuadrada del tamaño de la lista.

Si se quiere descifrar una clave simétrica con un ordenador convencional, hay que probar todos los valores posibles de la clave, lo que corresponde, para una clave de N bits, a 2 elevado a N intentos. Con el algoritmo de Grover, para una clave simétrica, serían necesarias 2 elevado a N/2 operaciones, lo que significa que, para la criptografía simétrica, el uso de un ordenador cuántico equivale a dividir por 2 el tamaño de las claves. El cifrado con una clave de 256 bits correspondería, en términos de seguridad, al cifrado con una clave de 128 bits en un mundo precuántico.

Los algoritmos de huella criptográfica también se ven amenazados por el algoritmo de Grover. El objetivo de un atacante sería encontrar un valor que genere un determinado hash. Entonces el oráculo tiene que calcular un hash a partir del valor probado y compararlo con el hash buscado. En este caso, el tiempo de ejecución del algoritmo de Grover aumenta con la raíz cuadrada del tamaño de la lista. Por lo tanto, la robustez de un algoritmo hash en un mundo postcuántico es equivalente a la de un algoritmo con un tamaño hash dividido por 2 en comparación con la era precuántica. Un algoritmo hash que genere un hash de 256 bits correspondería, en términos de robustez, a un hash de 128 bits. Existen casos especiales en los que el atacante no desea determinar un contenido que produce un hash determinado, sino obtener colisiones de hash, es decir, dos contenidos que generan el mismo hash. En este caso, utilizar el algoritmo BHT cuántico [8], derivado del algoritmo de Grover, equivaldría a dividir el tamaño del hash por 3 en lugar de por 2.

Tanto en el caso de los algoritmos de cifrado simétrico como en el de las huellas criptográficas, el algoritmo criptográfico que se quiere romper debe implementarse como un oráculo en el ordenador cuántico, lo que requiere cúbits y puertas cuánticas adicionales respecto a los necesarios para el algoritmo de Grover. Por eso, los investigadores llevan años diseñando oráculos que utilizan cúbits y puertas cuánticas para implementar distintos algoritmos de cifrado simétrico o de huella criptográfica. En el momento de escribir este libro, los oráculos más optimizados requieren algo más de 2.500 cúbits para el algoritmo de cifrado simétrico AES256 [9] y algo menos de 3.000 cúbits para el algoritmo criptográfico de huella criptográfica SHA256 [10]. El coste de estos oráculos en términos de puertas cuánticas es muy elevado. Estas condiciones aumentan la dificultad de ejecutar el algoritmo de Grover en condiciones reales en un ordenador cuántico para descifrar una clave simétrica o un hash.