LA AMENAZA CUÁNTICA

CF. YOANN GUGLIELMETTI – FUERZAS SUBMARINAS,
MARINE NATIONALE, FRANCIA

SUMARIO

El término "amenaza cuántica" se utiliza a menudo para describir la amenaza potencial que supone la computación cuántica para la seguridad de la información. Debido a sus propiedades intrínsecas muy específicas, los ordenadores cuánticos podrían ser capaces de realizar ciertos cálculos increíblemente más rápido que los superordenadores convencionales. De este modo, podrían suponer una grave amenaza para los actuales protocolos de cifrado, que se basan en ciertas dificultades computacionales de los ordenadores clásicos para garantizar su inviolabilidad. El objetivo de este artículo es describir brevemente el funcionamiento de estos ordenadores y los protocolos de cifrado utilizados hoy en día. A continuación, un análisis crítico caracteriza el riesgo asociado a esta amenaza y las posibles contramedidas. Por último, se ofrece una visión global de los principales actores para indicar las principales iniciativas en curso y cómo los competidores en esta carrera cooperan y actúan para ser el ganador, es decir, el que consiga desarrollar un ordenador con prestaciones suficientes para suponer una amenaza real para los protocolos de cifrado actuales.

Palabras clave: QKD (Quantum Key Distribution), post-cuántica, criptografía, informática cuántica.

ABSTRACT

The term "quantum threat" is often used to describe the potential threat to information security posed by quantum computing. Indeed, due to very specific intrinsic properties, quantum computers could be capable of performing certain calculations incredibly faster than conventional supercomputers. In so doing, they could pose a major threat to current encryption protocols, which rely for their inviolability on certain computational difficulties for classical computers. The purpose of this article is to briefly describe the operation of these computers and the encryption protocols used today. A critical analysis then characterizes the risk associated with this threat and possible countermeasures. Finally, an overview of the main players is given to indicate the main initiatives underway and how the competitors in this race cooperate and act to be the winner, that is, the one who

manages to develop a computer with sufficient performance to pose a real threat to current encryption protocols.

Key words: QKD (Quantum Key Distribution), post-quantum, cryptography, quantum computing.

INTRODUCCIÓN

La física cuántica es una rama de la física especialmente difícil de comprender por la falta de analogía entre los fenómenos microscópicos que describe y el mundo macroscópico en el que vivimos. En los años 70 y 80, los progresos realizados a lo largo del siglo XX permitieron vislumbrar la posibilidad de utilizar las propiedades muy específicas de las partículas atómicas para crear un nuevo tipo de ordenador potencialmente muy prometedor y mucho más potente que los ordenadores convencionales. Durante mucho tiempo, esta idea permaneció confidencial y restringida a un reducido número de académicos, pero el descubrimiento en los años 90 de dos algoritmos que sólo podían utilizarse en ordenadores cuánticos iba a actuar como catalizador en el desarrollo de esta tecnología. Estos algoritmos debilitaban teóricamente la credibilidad, en términos de inviolabilidad, de los protocolos de cifrado que se venían utilizando desde hacía más de 10 años.

Desde entonces, la inversión ha aumentado considerablemente y las iniciativas gubernamentales en forma de estrategias o planes nacionales han sido especialmente importantes en los últimos 5 años. Sin embargo, tras estos anuncios se esconden realidades técnicas y obstáculos tecnológicos especialmente importantes, aunque las amenazas convencionales no hayan desaparecido. En primer lugar, se presentarán los fundamentos de la física cuántica necesarios para comprender el funcionamiento de estos ordenadores, junto con un breve repaso de la historia de los protocolos de cifrado y descifrado. A continuación, se hará un repaso de las principales iniciativas en curso y se pondrá al día sobre el despliegue de ordenadores cuánticos en todo el mundo. Por último, se presentará un análisis crítico de la amenaza y las posibles contramedidas.

PANORAMA HISTÓRICO...

...de la física cuántica

La física cuántica surgió como respuesta a los problemas planteados por ciertas observaciones que no encajaban con las teorías clásicas de la física. Esta nueva rama de la física ha conducido a una revisión fundamental de nuestra

comprensión de la materia, pero la ha hecho menos accesible, en la medida en que muchos de los principios descubiertos no tienen equivalente en el mundo a nuestra escala: el mundo microscópico es radicalmente diferente del macroscópico. Entre estos importantes principios figuran, por ejemplo:

- **El principio de superposición**: un objeto cuántico puede encontrarse en una combinación de estados al mismo tiempo (un estado puede ser una posición, una característica física, etc.). Esta superposición se anota mediante una notación especial, que para un sistema con dos estados superpuestos da: |Estado 1> + |Estado 2>.
- **Reducción del paquete de ondas**: tras una medición, el objeto cuántico, que puede haber estado previamente en un estado de superposición, ve este estado completamente reducido al que se ha medido.
- **Entrelazamiento cuántico**: se dice que dos objetos cuánticos que forman un sistema enlazado, independientemente de la distancia que los separe, y que presentan estados cuánticos que dependen el uno del otro, están entrelazados.

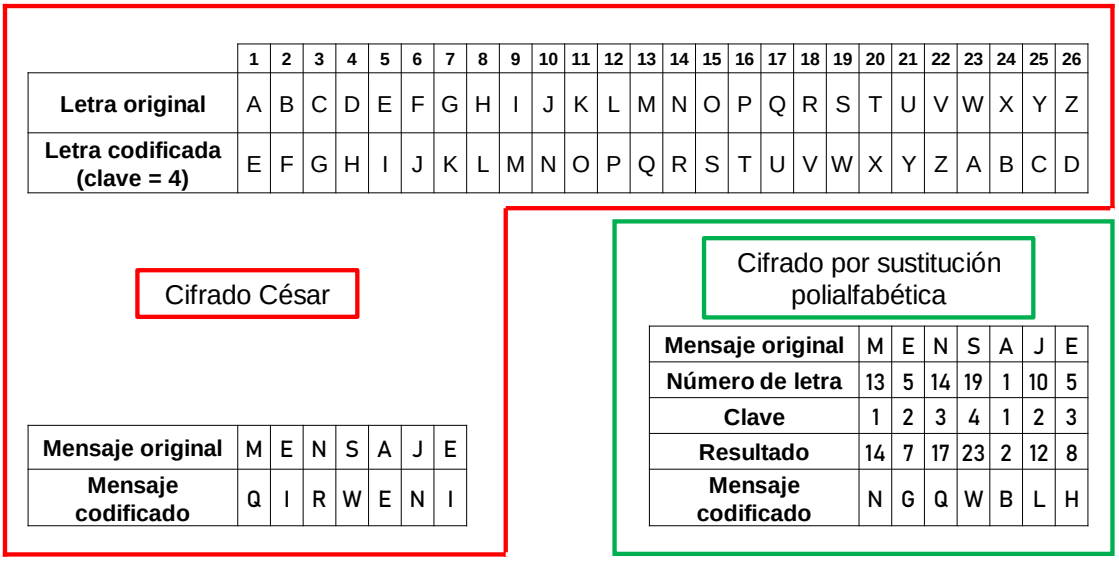
Estos principios son difíciles de visualizar porque **están ligados a probabilidades**, mientras que nuestro entorno cotidiano es más determinista.

Sin embargo, los avances logrados en este campo han tenido repercusiones tecnológicas muy reales. La física nuclear, las imágenes médicas por resonancia magnética, los relojes atómicos (esenciales para todas las mediciones de precisión, como la determinación de la posición por GPS), los láseres, los semiconductores (base de todos los chips electrónicos) y ciertos sensores de alta precisión se han desarrollado gracias a la comprensión que proporciona la mecánica cuántica. Los ordenadores cuánticos, aunque siguen siendo principalmente instrumentos de investigación, son una de las tecnologías en desarrollo. Otra aplicación es la distribución cuántica de claves (QKD, Quantum Key Distribution), que es la más desarrollada y conocida. En teoría, permite a dos partes establecer una clave compartida con total seguridad, sin riesgo de interceptación por un tercero. Este proceso es seguro porque se basa en principios físicos y no en las capacidades informáticas del adversario. Por tanto, ofrece lo que se conoce como "**seguridad incondicional**".

... de la encriptación

El principio básico de la encriptación es transformar un mensaje claro en una secuencia de caracteres indescifrables. Para lograrlo, se aplican operaciones de transformación reversibles. Si el método de transformación es único, el resultado final será variable y dependerá de un parámetro, llamado **clave**, que hace posible esta variabilidad. Por ejemplo, el cifrado más sencillo es el código César. Consiste en desplazar las letras de un mensaje un número fijo conocido por el

destinatario y el emisor (por ejemplo, para un desplazamiento de 4, A se convierte en E, B en F, etc.). **Este número es, en este caso, la clave**. La simplicidad de este sistema es también su debilidad: una vez conocido el método, bastan unos pocos intentos para descifrar el mensaje. Es lo que se conoce como ataque de fuerza bruta. Posteriormente, este método de cifrado se hizo más complejo introduciendo una clave más larga con un desplazamiento variable. Por ejemplo, si la clave es 1234, la primera letra del mensaje a cifrar se desplaza 1 letra (utilizando el método del código César), la segunda 2, y así sucesivamente. A continuación, se repite el proceso: la 5ª letra se desplaza 1 letra, la 6ª 2 letras y así sucesivamente. Este método produce mensajes más difíciles de descifrar, pero su interés histórico radica en que **el ataque de este código sentó las bases del criptoanálisis actual**, que utiliza ciertas operaciones matemáticas y estadísticas sobre el mensaje cifrado.



	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
Letra original	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Letra codificada (clave = 4)	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Mensaje original	M	E	N	S	A	J	E
Mensaje codificado	Q	I	R	W	E	N	I

Mensaje original	M	E	N	S	A	J	E
Número de letra	13	5	14	19	1	10	5
Clave	1	2	3	4	1	2	3
Resultado	14	7	17	23	2	12	8
Mensaje codificado	N	G	Q	W	B	L	H

Figura 1. Ejemplo de utilización del cifrado César y de la sustitución polialfabética. Fuente: Elaboración propia.

Durante el siglo XX, el cifrado (generalmente militar) también evolucionó. Tras abandonar más o menos el cifrado manual, laborioso y poco eficaz, se utilizaron máquinas de tecnología electromecánica, como la famosísima Enigma de la Segunda Guerra Mundial, antes de pasar a las máquinas digitales. La complejidad del descifrado se basaba tradicionalmente en **el número de combinaciones posibles para generar un número muy elevado de claves** de cifrado -varios millones de millones en el caso de Enigma, por ejemplo- a partir de unos pocos ajustes en la máquina. La llegada del ordenador cambió todo esto, con el desarrollo del primer ordenador programable diseñado específicamente para descifrar las comunicaciones del Eje durante la Segunda Guerra Mundial. Por tanto, los métodos de cifrado tuvieron que evolucionar.

En los años 70 surgió el **cifrado asimétrico**. Se trata de un sistema de cifrado que utiliza **dos claves separadas pero vinculadas** matemáticamente: una **clave pública** (disponible para todo el mundo) y una **clave privada**. La clave pública se utiliza para cifrar los datos, mientras que la privada sirve para descifrarlos. Este principio resuelve el problema de la confidencialidad durante el intercambio de claves, uno de los puntos débiles de los anteriores métodos de cifrado, llamados simétricos. Poco después aparecieron nuevos protocolos. **Su inviolabilidad se basa en la complejidad computacional de ciertas operaciones matemáticas**. El cifrado RSA combina estos dos principios y ofrece la ventaja de un nivel de seguridad escalable: la longitud de las claves recomendadas aumenta con el rendimiento de los superordenadores, que, a medida que aumenta su potencia de cálculo, son capaces de realizar cada vez más rápidamente las operaciones matemáticas que garantizan la seguridad del cifrado. Por estas razones, este método de cifrado sigue siendo uno de los más utilizados en la actualidad. Sin embargo, **la historia demuestra que ningún método es infalible**: con el tiempo, la tecnología acaba permitiendo un ataque de fuerza bruta, se encuentra un fallo en el protocolo de cifrado que facilita el descifrado o un error humano en la aplicación de los protocolos de cifrado reduce su eficacia de forma temporal o permanente. Igualmente, **el intercambio de claves siempre ha sido un problema**, sea cual sea la época(Singh, 1999).

LA INFORMÁTICA CLÁSICA/CUÁNTICA Y SUS PRINCIPIOS DE FUNCIONAMIENTO

Aunque se trata de máquinas muy complejas, es posible modelizar el funcionamiento de un ordenador moderno en términos sencillos. Podemos resumir su funcionamiento diciendo que procesa la información en forma de **bits sucesivos**, con valor 0 ó 1, que se representan mediante variaciones de la corriente eléctrica (dos valores distintos de tensión eléctrica). Estos bits se agrupan en paquetes llamados **registros** y luego se manipulan según algoritmos cuya finalidad es producir un resultado a partir de una entrada. En resumen, un ordenador puede reducirse a un dispositivo que transforma bits de entrada en bits de salida. Sin embargo, esta manipulación está limitada por el número de bits a procesar (cuanto mayor es el número, más bits se necesitan para codificarlo) y la velocidad de procesamiento, que determinan, entre otras cosas, la potencia de cálculo del ordenador.

El **qubit, equivalente cuántico del bit**, es un objeto cuántico que utiliza determinadas propiedades físicas. A menudo se utiliza el espín, una propiedad física frecuentemente asociada a la rotación de una partícula sobre sí misma,

pero sin equivalente real a escala macroscópica. El espín de un electrón, por ejemplo, puede servir de base para la constitución de un qubit. Como su espín es +1/2 o -1/2, el qubit puede caracterizarse por estos dos valores. También puede estar en un **estado superpuesto** de |1/2> + |-1/2>.

En la práctica, es posible crear registros de qubits, como en la informática convencional. Por ejemplo, con 2 qubits, se pueden crear 4 registros diferentes, (1/2,-1/2), (-1/2,-1/2), (-1/2,1/2) y (1/2,1/2). En términos más genéricos, hay 2^n registros para n qubits. Pero, a diferencia de la informática clásica, es posible diseñar un registro cuántico que sea una superposición de los cuatro registros posibles: |1/2,-1/2> + |-1/2,-1/2> + |-1/2,1/2> + |1/2,1/2>.

La idea del ordenador cuántico surgió a finales de los años 70, cuando se exploró el principio de **superposición de registros cuánticos**. La idea básica es utilizar un registro de estados superpuestos para realizar una serie de operaciones, como en un ordenador clásico. Sin embargo, mientras que el ordenador clásico tiene que procesar los 4 registros del ejemplo anterior uno tras otro y en 4 etapas, el ordenador cuántico puede procesar los 4 registros en una sola etapa. Es como si ejecutara 4 **operaciones en paralelo**. Es este principio teórico básico el que, cuando los registros están formados por un gran número de qubits, permite procesar cantidades masivas de información en una sola operación, mientras que un ordenador convencional procesaría estos datos secuencialmente. La principal diferencia reside en la forma en que se llevan a cabo estas operaciones. En un ordenador convencional, las operaciones internas se reducen a modificaciones realizadas en la corriente eléctrica a través de componentes electrónicos. En un ordenador cuántico, todo depende de la tecnología utilizada, ya que los qubits pueden estar formados por fotones o electrones, por ejemplo. La radiación electromagnética, los láseres y los dispositivos ópticos pueden utilizarse para manipular estos qubits. En consecuencia, el ordenador cuántico no es universal, porque sus algoritmos no son necesariamente de la misma naturaleza que los de los ordenadores clásicos. También por esta razón los ordenadores cuánticos han sido durante mucho tiempo relativamente poco comunes. En los años 90, dos importantes innovaciones en algoritmos aceleraron considerablemente el interés por esta tecnología. Se trata de los **algoritmos de Shor y Grover**, que llevan el nombre de sus descubridores (*Les Ordinateurs Quantiques*, 2017).

El algoritmo de Shor se utiliza para **factorizar números enteros en un producto de dos números primos**. Por poner un ejemplo sencillo, sirve para calcular que 15 es el producto de 3 y 5. Resulta que la complejidad matemática de esta operación aumenta exponencialmente con el número de cifras del número a factorizar. Por tanto, se considera que, con las recomendaciones actuales sobre la longitud de la clave de cifrado RSA, el tiempo necesario para factorizar con un superordenador los números utilizados como claves puede alcanzar fácilmente

varios miles (o incluso millones) de años con los mejores algoritmos disponibles actualmente. En cambio, el algoritmo de Shor no crece exponencialmente, sino logarítmicamente. Una estimación muy aproximada (Aaronson, 2008) es que, para números de unos cientos de dígitos n, el tiempo de cálculo del mejor algoritmo de factorización crecerá en $2^{\sqrt[3]{n}}$, mientras que el algoritmo de Shor lo hará en $\log n$. Esto puede dar lugar a ganancias considerables: cuanto mayor sea el número, mayor será la diferencia entre ambos, como se muestra en la figura siguiente.

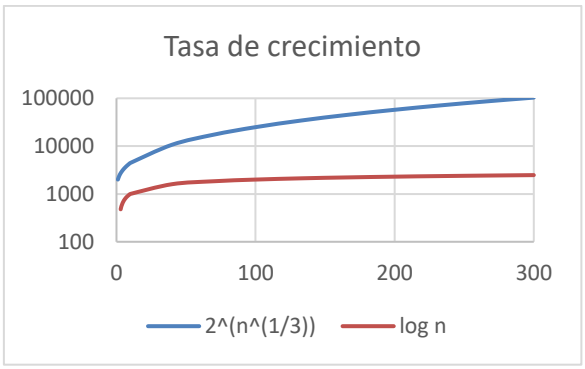


Figura 2. Tasa de crecimiento de la complejidad temporal (con coeficiente arbitrario, escala logarítmica): factorización en computación cuántica o clásica. Fuente: Elaboración propia.

El algoritmo de Grover es **un algoritmo de búsqueda** que puede funcionar eficazmente en una base de datos sin ordenar. Por ejemplo, buscar un valor concreto en una lista que contenga N valores requerirá como máximo N pasos. El algoritmo de Grover, por su parte, necesitará como máximo $\sqrt{N}$ pasos, lo que de nuevo representa una ganancia para los números más grandes. Da la casualidad de que **estos dos algoritmos son de especial interés para los ataques de fuerza bruta y el criptoanálisis** de los métodos de cifrado actualmente en uso, y es por ello que han actuado como catalizador en el desarrollo tecnológico de los ordenadores cuánticos.

PRINCIPALES INICIATIVAS EN CURSO EN EUROPA Y EN EL MUNDO

En la medida en que las demostraciones tecnológicas han demostrado que el concepto de ordenador cuántico es válido, y debido a la ventaja tecnológica que puede conferir tanto en informática como en el campo de la inteligencia, un gran número de países se han dedicado a este tema. En **los últimos 5 años**, los países más desarrollados han anunciado una serie de iniciativas y proyectos, tanto gubernamentales como privados, para desarrollar la informática cuántica.

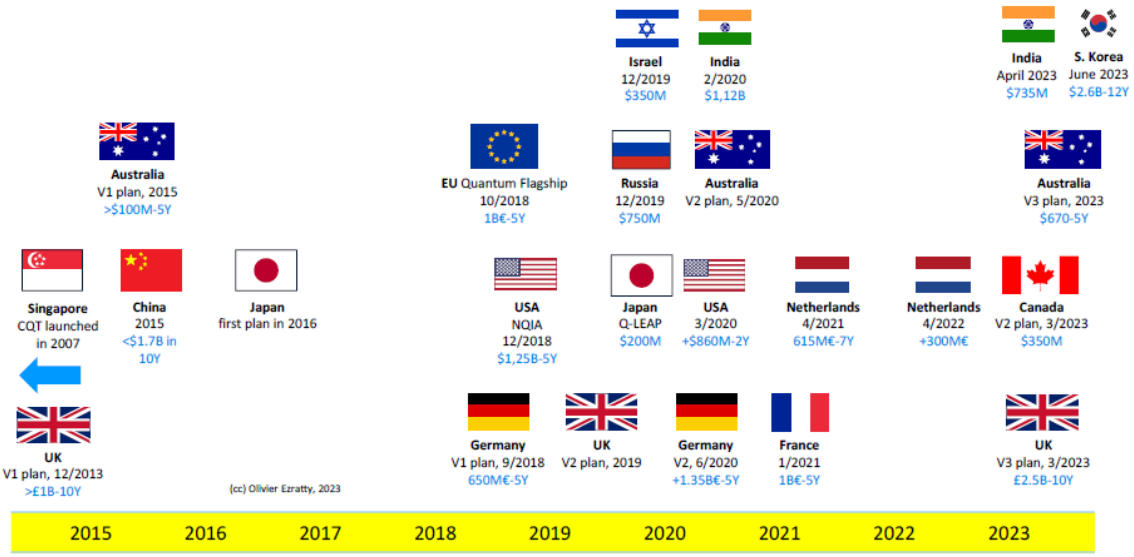


Figura 3. Planes nacionales de iniciativas cuánticas que sólo incluyen financiación pública, de 2007 a 2023. Fuente: (Ezratty, 2024, p. 1115).

En la actualidad, Estados Unidos, China y la Unión Europea en su conjunto (cada país de la UE puede tener sus propias estrategias y proyectos nacionales) son los 3 líderes en estos proyectos de desarrollo. Existen varios tipos de ordenadores cuánticos con dos tipos principales: el **ordenador cuántico digital** (también llamado *gate-level quantum computer*) y el **ordenador cuántico analógico** o *quantum annealer* (Krelina, 2021).

Europa en general

Para que los investigadores de la UE puedan trabajar en las plataformas de computación cuántica escalable más prometedoras, el proyecto OPENSUPERQ, que forma parte de la *European Quantum Technology Flagship*, ha permitido construir un sistema de computación cuántica competitivo a escala mundial basado en circuitos integrados superconductores (objetivo de 50-100 qubits). A partir de marzo de 2023, el proyecto evolucionará hasta convertirse en OPENSPERQPLUS, con un objetivo de 1.000 qubits para el verano de 2026. El sistema tiene su sede en la institución nacional de investigación Forschungszentrum de Jülich (Alemania).

La Unión Europea, a través de la *European High-Performance Computing Joint Undertaking*[1] (EuroHPC JU) ha seleccionado seis sitios en toda Europa en octubre de 2022 para acoger y operar las primeras computadoras cuánticas de Europa (European High-Performance Computing Joint Undertaking, 2022).

[1] Esta entidad de la UE, creada en 2018, tiene como objetivo coordinar los esfuerzos de los miembros de la UE en supercomputación.

Por último, la tecnología de *quantum annealer* está siendo desarrollada por el proyecto AVaQus (*Annealing-based VAriational QUantum processorS*), en el que participan 5 centros de investigación y 3 *startups*. Todo el proyecto está coordinado por el Institut de Física d'Altes Energies (IFAE) de Barcelona.

Alemania, España y Francia

Alemania destaca con dos tipos de ordenadores cuánticos. En primer lugar, un *quantum annealer* operado por el Forschungszentrum Jülich en colaboración con D-Wave, con más de 5.000 qubits, el mayor hasta la fecha. Alemania también ha instalado el primer ordenador cuántico superconductor de Europa, el Q *system one* de IBM, con 27 qubits. España también se está posicionando con un ordenador cuántico IBM de 127 qubits en San Sebastián y un otro integrado en el superordenador MareNostrum 5 del *Barcelona Supercomputing Center*, que comenzará con 5 qubits en 2023 y aspira a alcanzar los 30 qubits a finales de 2025 como parte del programa ***Quantum Spain***. En Francia, la Euro HPC JU ha anunciado que pronto se construirá un ordenador cuántico fotónico que ofrecerá hasta 10 qubits y se acoplará al superordenador Joliot-Curie.

EE.UU.

En Estados Unidos, IBM anunció 1.121 qubits en diciembre de 2023, con una ambiciosa hoja de ruta para alcanzar entre 10.000 y 100.000 qubits después de 2026 y el objetivo final de **superar el millón de qubits**. Google ha logrado la "**supremacía cuántica**" (es la etapa a partir de la cual las computadoras cuánticas realizan cálculos mucho más rápidamente que sus contrapartes clásicas) con Sycamore (*La Suprématie Quantique de Google*, 2019), un procesador de 53 qubits, y aspira a alcanzar el millón de qubits a finales de la década. Microsoft se centra en los qubits topológicos para lograr una mayor estabilidad, mientras que Amazon ofrece servicios cuánticos a través de Braket, conectando a los usuarios con ordenadores de D-Wave, Rigetti e IonQ. Las fuerzas armadas estadounidenses, están muy implicadas en la financiación y el desarrollo de ordenadores cuánticos y protocolos QKD para comunicaciones seguras, incluso para la US Navy (Ezratty, 2024).

OTAN

La OTAN no dispone de un ordenador cuántico, pero ha anunciado en 2022 que abrirá un centro de investigación sobre física cuántica como parte del sistema de aceleración de la innovación de la alianza.

China

En 2020, Benyuan Wuyuan lanzó el primer ordenador cuántico superconductor de China. Ese mismo año, el prototipo de ordenador cuántico fotónico *Jiuzhang*

alcanzó la supremacía cuántica, el segundo después de Google. En 2021, se anunció el ordenador cuántico *Zuchongzhi 2* con 66 qubits superconductores, del que se afirmaba que era un millón de veces más rápido que el Sycamore de Google y 10 millones de veces más rápido que el superordenador más potente del mundo. En 2023 contaba con 176 qubits. Los resultados anunciados para estos dos modelos **se basan en cálculos muy específicos**.

En cuanto a la comunicación, desde 2016 se utiliza un satélite (Micius) para realizar una serie de pruebas de transmisión de claves mediante QKD. Se trata del proyecto QUESS (*Quantum Experiments at Space Scale*). Tras validar las comunicaciones a una estación, en 2020 se llevaron a cabo comunicaciones a dos estaciones separadas por más de 1.000 km, batiendo los récords de distancia de las transmisiones terrestres por fibra óptica (del orden de cien km o más).

Como en Estados Unidos, los BATX participan en parte. Baidu presentó su primer ordenador cuántico en 2022, llamado Qian Shi, capaz de procesar hasta 10 qubits superconductores. Alibaba ha lanzado varios proyectos cuánticos, incluido un servicio de computación cuántica en la nube, como Amazon, con 11 qubits. Sin embargo, en 2023, Alibaba cerró su laboratorio de computación cuántica para volver a centrar su investigación en la IA. Tencent no tiene un ordenador cuántico, pero ha puesto en marcha el Tencent Quantum Lab en Shenzhen, dedicado a la investigación científica de la computación cuántica. Por último, no hay información pública disponible sobre la implicación de Xiaomi en la computación cuántica.

Actualmente se considera que China, junto con EE.UU., lidera la carrera tecnológica en computación cuántica.

¿DE QUÉ TIPO DE AMENAZA ESTAMOS HABLANDO?

No obstante, esta tecnología está limitada actualmente por dos grandes retos:

- **La corrección de errores cuánticos**: los qubits son muy sensibles a las perturbaciones de su entorno y pueden perder fácilmente su estado de superposición (este fenómeno se denomina decoherencia) cuando no se han completado las operaciones matemáticas que se les aplican. Una forma de sortear este problema es crear qubits lógicos, considerados perfectos, a partir de qubits físicos. La proporción puede llegar a ser de 10.000 qubits físicos por un solo qubit lógico (Krelina, 2021).

- **La necesidad intrínseca de disponer de un gran número de qubits**: en el caso concreto de la utilización del algoritmo de Shor, se requiere un ordenador con unos 2×n qubits perfectos para factorizar un número de n bits (Boudot et al., 2020), es decir, varios millones o incluso miles de millones de qubits en la actualidad.

Estos 2 factores explican por qué algunos fabricantes tienen una hoja de ruta que incluye un aumento del número de qubits disponibles en el futuro, y no sólo hacerlos más fiables. Otra razón relacionada es que **el número de qubits es un factor clave en la potencia de cálculo de un ordenador cuántico**, aunque no es el único.

La siguiente figura muestra dónde se encuentran actualmente los principales ordenadores cuánticos en servicio. Muchos están aún en un rango que puede **simularse en ordenadores convencionales** o superordenadores. En cuanto a los que están más allá (por encima de los 40 o 50 qubits), también podemos ver que todavía se encuentran en áreas en las que el error es demasiado grande para hacerlos realmente útiles. Existen al menos dos áreas de desarrollo tecnológico: NISQ (*Noisy Intermediate-Scale Quantum*) y FTQC (*Fault-Tolerant Quantum Computer*). Los NISQ son útiles para validar el funcionamiento de ciertos algoritmos cuánticos, pero son incapaces de hacer funcionar aquellos que no son tolerantes a errores. Para ello pueden utilizarse los FTQC, que tratan de corregir los errores automáticamente durante el cálculo.

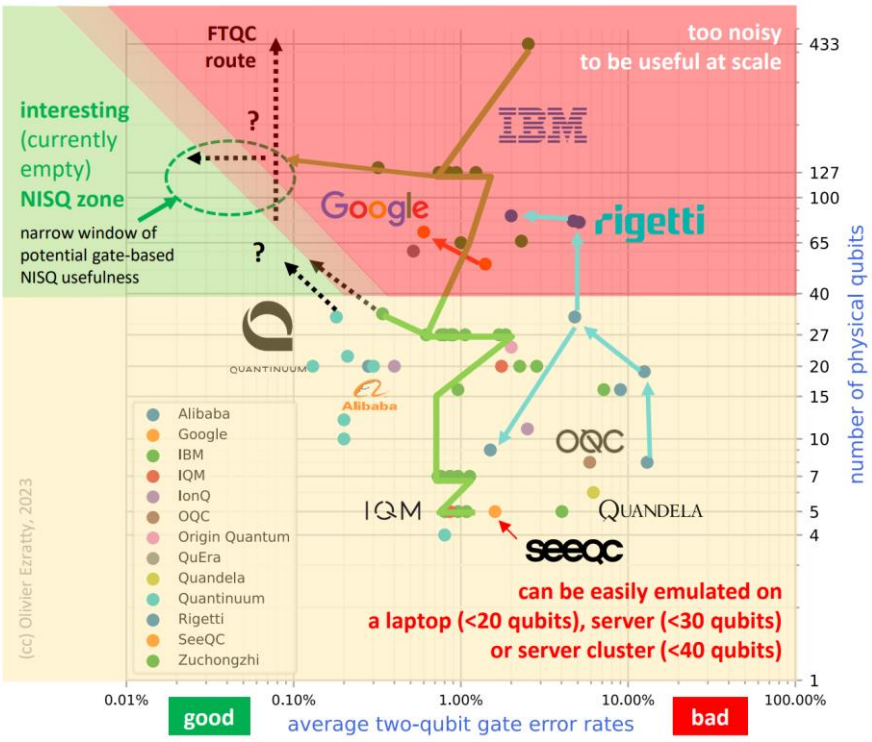


Figura 4. Fidelidad de puerta de dos qubits y número de qubit para los sistemas de computación cuántica disponibles a partir de enero de 2024. Fuente: (Ezratty, 2024, p. 257).

En definitiva, los ordenadores cuánticos aún no tienen aplicaciones realmente prácticas, a excepción de algunos cálculos en el campo de la química cuántica o en algunos problemas concretos de optimización.

Por tanto, la cuestión de la amenaza no es qué, sino más bien cuándo estará disponible un ordenador cuántico capaz de romper los métodos de cifrado actualmente en uso, conocido como CRQC (*Cryptographically Relevant Quantum Computer*). Según un panel de expertos competentes, la mayoría consideraba extremadamente improbable que esto ocurriera en un plazo de 5 años, pero que era **muy probable que sucediera en un plazo de 30 años**. Entre los dos, para el periodo de 15-20 años, es el momento crucial en el que empieza a aparecer entre los expertos más optimistas el hecho de que es extremadamente probable. Estos datos pueden verse en la siguiente figura.

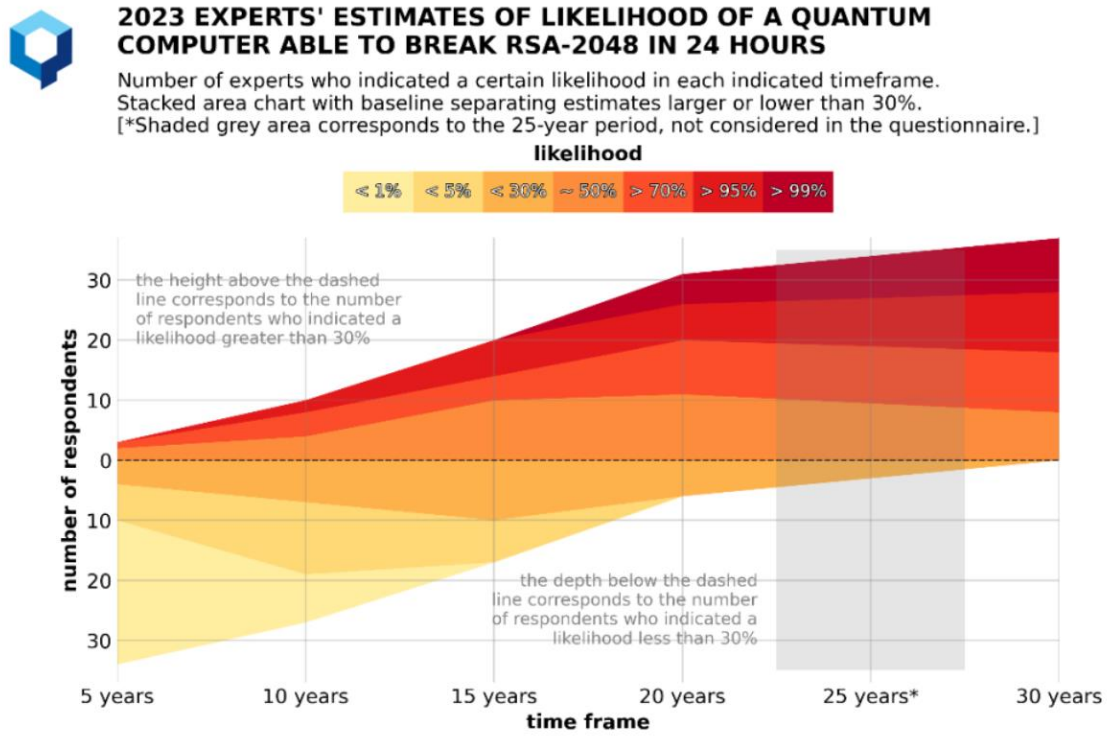


Figura 5. Probabilidad de que un CRQC sea capaz de romper el RSA-2048 en 24 horas - para varios periodos, de 5 a 30 años, panel de 37 expertos. Fuente: (Mosca and Piani, 2023).

Aunque la amenaza no sea inminente, esto no significa que no sea una amenaza. El problema de *"store now, decrypt later"* es el hecho de que la información cifrada hoy puede almacenarse y descifrarse más tarde utilizando ordenadores cuánticos. Para mitigar el riesgo que supone un CRQC, los informes hacen hincapié en **la necesidad de migrar a herramientas criptográficas resistentes**. El tiempo de migración será diferente para cada organización, pero un cambio de este tipo requiere un tiempo de transición significativo y debe hacerse de forma meditada para evitar introducir vulnerabilidades adicionales o

errores de implementación. Además del tiempo necesario para realizar un CRQC y del tiempo de migración, la urgencia de la transición para una organización determinada depende de otro parámetro: el tiempo durante el cual los datos deben permanecer seguros. Esto es especialmente cierto en el caso de las fuerzas armadas, donde cierta información debe mantenerse en secreto durante varias décadas. Este concepto, conocido como desigualdad de Mosca, se ilustra en la siguiente figura.

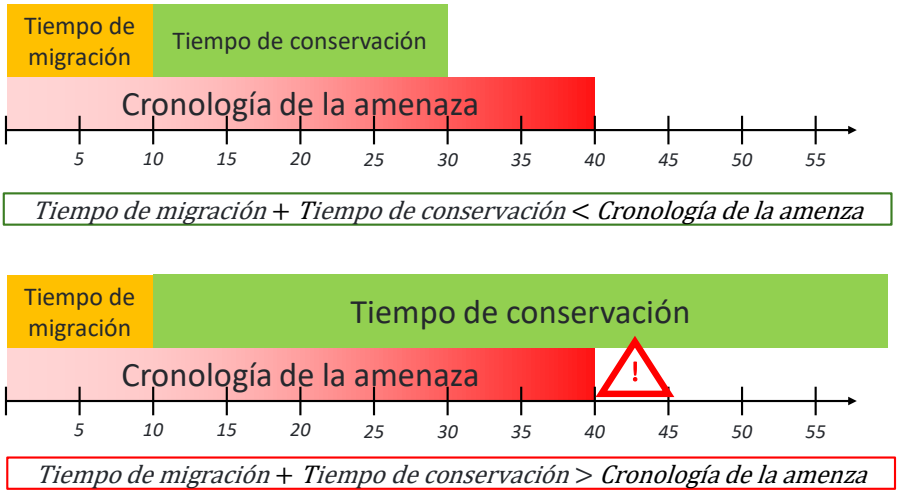


Figura 6. Desigualdad de Mosca: en la parte superior, el tiempo de migración y el tiempo de conservación son compatibles con la llegada de la CRQC, en la parte inferior (el tiempo antes de la desclasificación es de 50 años) no lo son. Fuente: Elaboración propia según (Mosca and Piani, 2023).

Así pues, aunque la inversión puede haberse visto impulsada durante un tiempo por el hype tecnológico (Smith III, 2020) y es probable que esta moda se agote, es importante tener en cuenta que la amenaza es muy real, no necesariamente inmediata, **sino estrechamente vinculada al tiempo de conservación de la información confidencial**. Además, el entusiasmo por la tecnología cuántica tiende a eclipsar las amenazas tradicionales, que no han desaparecido. En definitiva, los grandes Estados implicados en la carrera lo hacen por prestigio y mimetismo, ya sea para uso militar o no.

Contramedidas

Frente a la amenaza cuántica, se están estudiando contramedidas, como los **algoritmos post-cuánticos**, diseñados para resistir los ataques de los ordenadores cuánticos (Krelina, 2021). Algunos de ellos se encuentran actualmente en fase de competición y en las etapas finales de certificación por parte de las autoridades estadounidenses.

La implementación de **protocolos QKD será una herramienta adicional** que se utilizará, cuando esté suficientemente madura y proporcione una ventaja

sobre los sistemas actualmente en uso. Salvo en algunos casos concretos, actualmente pueden utilizarse para la "defensa en profundidad[2]" (ANSSI, 2022).

Por último, es crucial **no descuidar el personal y el hardware**, ya que los errores humanos y las vulnerabilidades del hardware pueden comprometer la seguridad independientemente de la solidez de los algoritmos utilizados, como la historia ha demostrado en numerosas ocasiones.

CONCLUSIÓN

A lo largo de este resumen hemos tratado en primer lugar de establecer los fundamentos de la computación y la criptografía cuánticas con el fin de poner las bases para comprender y contextualizar el campo de estudio, es decir, la amenaza cuántica. Una amenaza en el sentido de la que representan los ordenadores cuánticos para la seguridad de la información. Esta amenaza se basa en una serie de innovaciones y desarrollos de gran actualidad destinados a poner en práctica los descubrimientos algorítmicos teóricos realizados durante los años noventa. Un gran número de iniciativas gubernamentales y del sector privado están en marcha, sobre todo en los últimos 5 años. La evidencia es que la amenaza está realmente justificada, que se está tomando muy en serio y que la investigación que se está llevando a cabo para hacer frente a esta amenaza está teniendo un impacto mucho más amplio.

Sin embargo, no es más que una nueva amenaza que no ha sustituido ni disminuido a las demás, y hasta la fecha se mantiene en un nivel de peligrosidad muy inferior al de las amenazas actuales. Su efecto retroactivo es, de hecho, lo que debería motivar la inversión y la investigación para contrarrestar sus efectos potenciales. Ya existen medidas, incluidos algunos de los viejos principios de la seguridad de la información y la criptografía, u otras más recientes con distintos niveles de madurez. Otras están a punto de aplicarse. Se mire como se mire, esta amenaza tiene el mérito de haber dado un impulso a la investigación en criptografía, un campo que requiere una innovación constante, porque la historia

[2] Este concepto, que tiene su origen en la ingeniería de fortificaciones militares, se ha desarrollado ampliamente en el contexto de la energía nuclear civil. Su principio es que los accidentes son inevitables y acabarán ocurriendo (no existe el riesgo cero). Por tanto, según esta lógica, hay que adoptar una serie de medidas que no se detengan en las normas de aplicación, sino que partan del diseño de los sistemas, su fabricación, la formación del personal y lleguen hasta el momento en que se produce el accidente, planificando de antemano las medidas de mitigación para limitar las consecuencias. Más que un enfoque, es un paradigma de gestión de la seguridad.

nos demuestra que ningún código puede resistir para siempre los ataques de quienes quieren penetrar en sus secretos.

(4490)

BIBLIOGRAFÍA

ANSSI (2022) *ANSSI views on the Post-Quantum Cryptography transition*, *ANSSI*. Disponible en: https://www.ssi.gouv.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/ [Consultado: 11 septiembre 2023].

European High-Performance Computing Joint Undertaking (2022) Selection of six sites to host the first European quantum computers - European Commission, The European High Performance Computing Joint Undertaking. Disponible en: https://eurohpc-ju.europa.eu/selection-six-sites-host-first-european-quantum-computers-2022-10-04_en [Consultado: 10 diciembre 2023].

Ezratty, O. (2024) Understanding Quantum Technologies 2023. Sixth edition-2023-v6.8. Autopublicación. Disponible en: https://www.oezratty.net/wordpress/2023/understanding-quantum-technologies-2023/ [Consultado: 6 marzo 2024].

Krelina, M. (2021) 'Quantum technology for military applications', EPJ Quantum Technology, 8(1), pp. 1–53. Disponible en: https://doi.org/10.1140/epjqt/s40507-021-00113-y.

La Suprématie Quantique de Google (2019). ScienceEtonnante. Disponible en: https://www.youtube.com/watch?v=KaRd_eB2qOA [Consultado: 11 septiembre 2023].

Louapre, D. (2019) 'La suprématie quantique – Science étonnante', ScienceEtonnante, 4 Octubre. Disponible en: https://scienceetonnante.com/2019/11/05/la-suprematie-quantique/ [Consultado: 11 septiembre 2023].

Les Ordinateurs Quantiques (2017). ScienceEtonnante. Disponible en: https://www.youtube.com/watch?v=bayTbt_8aNc [Consultado: 11 septiembre 2023].

Louapre, D. (2017) 'Les ordinateurs quantiques – Science étonnante', ScienceEtonnante, 3 Marzo. Disponible en: https://scienceetonnante.com/2017/04/07/les-ordinateurs-quantiques/ [Consultado: 11 septiembre 2023].

Mosca, M. and Piani, M. (2023) *2023 Quantum Threat Timeline Report*. Report. Toronto: Global Risk Institute in financial Service, p. 67. Disponible en: https://globalriskinstitute.org/publication/2023-quantum-threat-timeline-report/ [Consultado: 7 Abril 2024].

Singh, S. (1999) Histoire des codes secrets : De l'Egypte des Pharaons à l'ordinateur quantique. Paris: JC Lattès.