STORMSHIELD

ARTÍCULOS DE OPINIÓN

CIBERSEGURIDAD Y CUÁNTICA: CUIDADO CON LAS SIMPLIFICACIONES

Fabien Thomas
Chief Technology Officer, Stormshield

Quantum System One de IBM, Quantum AI de Google, Azure Quantum de Microsoft, Qian Shi de Baidu... Desde finales de la década de 2010, la computación cuántica ha cobrado cada vez más importancia, tanto en términos de protección como de amenazas para la seguridad informática. A largo plazo, esta revolución informática podría debilitar considerablemente los sistemas de seguridad basados en el cifrado; es decir, la gran mayoría... La amenaza cuántica, un nuevo reto para la ciberseguridad. Se impone una comprensión del fenómeno para evitar las ideas preconcebidas.

Prólogo: para garantizar la legibilidad de este documento, no detallaremos aquí los algoritmos de Grover y Shor ni todos los matices de los qubits (estables, noisy, annealing y demás...). Nuestros lectores nos lo agradecerán.

LAS PROMESAS DE LA POTENCIA DE LA COMPUTACIÓN CUÁNTICA

De la informática tradicional al ordenador cuántico

Aunque la computación cuántica es fascinante, también es un tema extremadamente complicado de entender. Tras esta fachada, se esconden multitud de incertidumbres, resumidas en la famosa cita atribuida al físico Richard Feynman: «*Creo que puedo afirmar sin temor a equivocarme que nadie entiende la mecánica cuántica*». Un paradigma que ha de tenerse en cuenta al leer este documento. «*Cuando se trata de cuántica, no hay que intentar entenderla por intuición*», añade Yvan Vanhullebus, Technical Leader de Stormshield, *dado que nuestra intuición se basa en nuestras experiencias pasadas y no está en absoluto entrenada en la cuántica. Tanto es así que hoy parece más fácil explicar lo que NO es la cuántica...* ».

«Cuando se trata de cuántica, no hay que intentar entenderla por intuición, dado que nuestra intuición se basa en nuestras experiencias pasadas y no está en absoluto entrenada en la cuántica. Tanto es así que hoy parece más fácil explicar lo que NO es la cuántica...»

Yvan Vanhullebus, Technical Leader de Stormshield

Se trata de un tema complicado que interesa especialmente al mundo de **la ciberseguridad, ya que la computación cuántica podría revolucionar la informática tal y como la conocemos en la actualidad.** ¿Cómo? Gracias al «salto cuántico»; es decir, a la posibilidad de beneficiarse de una potencia de cálculo optimizada y poder así realizar operaciones matemáticas complejas que antes eran imposibles. Como explica Yvan Vanhullebus: «*El ordenador cuántico utiliza las propiedades de la materia a una escala infinitamente pequeña para realizar en pocos minutos ciertos cálculos que con los ordenadores actuales más potentes se tardaría al menos varios miles de años.*

La informática cuántica está estrechamente vinculada al desarrollo de una nueva unidad: el bit cuántico o «*qubit*». Una unidad que, como se explica en la mayoría de los artículos, puede tomar dos valores (denotados como 0 o 1), así como tener ambos valores al mismo tiempo, lo que permitiría calcular todos los valores simultáneamente. «***Sin embargo, en realidad, no funciona así: nos acercamos más a la realidad de la física cuántica hablando de probabilidades***», tal como explica Yvan Vanhullebus, tomando como referencia el cómic *The Talk* , de Scott Aaronson y Zach Weinersmith.

Aplicaciones deseadas de la informática cuántica

Numerosos actores se han embarcado en una carrera tecnológica para alcanzar la supremacía cuántica. **Pero, ¿qué es exactamente la supremacía cuántica?** Este es el punto en el que un cálculo cuántico sobre un problema dado será más rápido que su equivalente informático. Aunque algunos actores explican periódicamente que han

alcanzado esta supremacía cuántica, el paso a la verdadera era de la computación cuántica aún está lejos. En esta carrera de superordenadores, los anuncios han corrido a cargo de actores privados como Google, IBM y Baidu , cada uno de los cuales ha divulgado numerosas veces sus avances (más o menos experimentales) en este ámbito. **¿Quién ha logrado entonces la supremacía cuántica?** No hay consenso entre los expertos en la materia, sobre todo porque no todos los *qubits* son iguales... Las cantidades de *qubits* en los distintos anuncios a veces pueden sorprender, ya que no siempre representan lo mismo... Ya en 2019, Google anunció que había logrado esta supremacía cuántica antes que los investigadores chinos en 2021, pero en ambos casos, los resultados se pusieron en tela de juicio. Entre los 54 qubits del procesador Sycamore de Google y los 433 del procesador Osprey de IBM, la carrera de *qubits* está en marcha y en pleno apogeo.

Los actores públicos no se quedan atrás en esta carrera tecnológica. En Estados Unidos, la NSA lleva años interesada en el sector cuántico (en 2014 gastó sus primeros 80 millones de dólares en un programa llamado *Owning The Net*). Por su parte, Europa tiene previsto invertir al menos 4500 millones de euros en tecnologías cuánticas de aquí a 2027. En enero de 2021, el Gobierno francés hizo público un presupuesto de 1800 millones de euros para tecnologías cuánticas. «*Un presupuesto importante, pero inferior a las inversiones chinas y estadounidenses*», afirma **Noël Chazotte,** Product Manager de Stormshield. *Si tenemos en cuenta que las cantidades mencionadas son 25 000 millones de dólares en el caso de Estados Unidos y 50 000 millones en el de China, Europa no tiene la misma escala*... ».

«Europa tiene previsto invertir al menos 4500 millones de euros en tecnologías cuánticas de aquí a 2027. En enero de 2021, el Gobierno francés hizo público un presupuesto de 1800 millones de euros para tecnologías cuánticas.»

Y es que hay mucho en juego: se trata de dominar una tecnología que se perfila como revolucionaria. Simular el funcionamiento del universo o el comportamiento de la materia a nivel molecular, encontrar nuevos planetas habitables, predecir mejor la meteorología, crear medicamentos capaces de tratar importantes enfermedades como el cáncer o el Alzheimer, así como luchar contra el fraude bancario y, en general, mejorar la seguridad de los sistemas de información... las aplicaciones son numerosas y afectan a numerosos sectores industriales. Sin embargo, aunque las promesas de esta industria son impresionantes, **la computación cuántica también supone una nueva amenaza para el sector de la ciberseguridad.**

LAS NUEVAS AMENAZAS DE LA INFORMÁTICA CUÁNTICA

Una ciberamenaza... ¿para el Estado?

Antes de dar crédito a los informes sobre una amenaza cibercriminal cuántica, esta podría ser ante todo geopolítica. «*Está claro que el primer Estado que gane la carrera por dominar la tecnología cuántica ostentará la supremacía frente a los demás*», explica **Arnaud Dufournet**, Chief Marketing Officer de TheGreenBow. *Al igual que las potencias nucleares, habrá potencias cuánticas en el mundo. En la actualidad, este puesto se lo disputan China y Estados Unidos. Por tanto, para que los actores no gubernamentales, como los ciberdelincuentes, dispongan de esta arma, hará falta aún más tiempo*. **¿El ordenador cuántico se convertiría entonces en una nueva palanca para el espionaje industrial y gubernamental, o incluso para la desestabilización geopolítica?** Sería tentador responder que sí, ya que muchos países se toman muy en serio esta cuestión de seguridad nacional. En un discurso público inusual del responsable del MI6, el servicio secreto británico, expresó su preocupación por el hecho de que ciertos «*rogue states*» o Estados malintencionados se estuvieran posicionando en el ámbito cuántico con vistas a futuros conflictos.

«Está claro que el primer Estado que gane la carrera por dominar la tecnología cuántica ostentará la supremacía frente a los demás. Al igual que las potencias nucleares, habrá potencias cuánticas en el mundo.»

Arnaud Dufournet, Chief Marketing Officer de TheGreenBow

Esta amenaza latente o el uso malicioso de la cuántica reside en el ataque a las claves de cifrado asimétricas. Llevaría al colapso de todos los sistemas de información basados en el cifrado e incluso se conoce como «apocalipsis cuántico», expresión tomada de un artículo de la BBC ampliamente difundido. ¿En qué consiste? En el caso de las empresas, la seguridad de sus sistemas de información dejaría de estar garantizada de la noche a la mañana. Una perspectiva muy real, según **Ilyas Khan** , de la empresa *Quantinuum*, y **Harri Owen**, de la empresa Post Quantum, entrevistados por la BBC: «*Todo lo que hacemos hoy en Internet, desde las compras online a las operaciones bancarias, está cifrado. Sin embargo, una vez que un ordenador cuántico en funcionamiento sea capaz de descifrar estas claves, podría crear la posibilidad de vaciar cuentas bancarias o carteras de criptoactivos, así como vulnerar los sistemas de defensa nacionales*.

Una ciberamenaza ya presente

Entonces, ¿cuál es la naturaleza de las nuevas vulnerabilidades provocadas por el advenimiento de la era cuántica? Se refieren casi exclusivamente a la seguridad de las infraestructuras criptográficas, que podría verse socavada por la potencia de la computación cuántica, lo que podría hacer fracasar los actuales sistemas criptográficos asimétricos (RSA, ECC, etc.). Las posibles consecuencias son la suplantación de servidores u otras entidades implicadas en intercambios electrónicos o el descifrado de

datos. **¿Hasta el punto de descifrar una clave RSA-2048 en menos de 24 horas?** Esta era la cuestión planteada en el «*Informe sobre la cronología de la amenaza cuántica*» publicado en 2021, con una proyección a lo largo de los próximos 30 años. Entre una proyección a 5 y 30 años, incluso las visiones pesimistas aumentan del 2 % al 80 %. A finales de diciembre de 2022, un equipo de investigadores universitarios chinos anunció en una publicación que habían sido capaces de descifrar el algoritmo RSA-2048 utilizando un ordenador cuántico. Sin embargo, esta comunicación pública plantea ciertos interrogantes: ¿se trata de un avance tecnológico real o de una advertencia a los países occidentales? Aún no tenemos la respuesta.

No obstante, estos futuros ataques pueden prepararse sobre los datos actuales: en su aviso de abril de 2022, la agencia francesa ANSSI menciona **el caso de los ciberataques retroactivos denominados «*store now, decrypt later attack*»**, si bien también se conocen como «*hack now, decrypt later*», «*harvest now, decrypt later*», «*capture now, decrypt later*»... La técnica consiste en registrar en la actualidad una importante cantidad de datos y comunicaciones cifradas con el objetivo de descifrarlos más adelante, una vez dominada la tecnología cuántica. «*Estados Unidos ya ha visto este tipo de ataques dirigidos a los datos con una vida útil muy larga, que pueden afectar a sus infraestructuras y datos militares*», afirma Arnaud Dufournet. Antes de planificar : «*En el sector bancario, siempre será interesante disponer de datos sobre las condiciones y los importes de determinadas operaciones estratégicas. En el sector de la defensa, la información sobre submarinos será válida durante décadas. Sin embargo, también en el sector de la energía, el automóvil, los secretos industriales ya hay una necesidad urgente de protegernos porque los Estados empiezan a almacenar datos en previsión de poder descifrarlos. «En el sector médico francés también se plantea la cuestión* —añade Yvan Vanhullebus— *ya que la ley estipula que un establecimiento sanitario (ya sea público o privado) puede conservar una historia clínica durante 20 años. De forma segura, por supuesto*».

«En su dictamen de abril de 2022, la Agencia Nacional francesa de Seguridad de los Sistemas de Información (ANSSI) menciona el caso de los ciberataques retroactivos conocidos como «store now, decrypt later attack». La técnica consiste en registrar en la actualidad una importante cantidad de datos y comunicaciones cifradas con el objetivo de descifrarlos más adelante, incluso años después, una vez dominada la tecnología cuántica.»

Por último, las criptomonedas, incluida la popular bitcóin, también podrían ver corrompida su infraestructura en contra de su reputación de tecnología infalsificable. De acuerdo con algunos investigadores de la Universidad de Sussex en el Reino Unido, un ordenador cuántico con 13 millones de qubits podría piratear la blockchain de bitcóin en tan solo 24 horas. Entonces, sería posible secuestrar las transacciones y vaciar de activos los monederos digitales. Otras investigaciones son menos alarmistas y explican que se tardará una o dos décadas más en desarrollar esta capacidad. En el estado actual de desarrollo, el pirateo de la red bitcóin por un ordenador cuántico sigue siendo una teoría.

LA NECESIDAD DE ADAPTAR LOS PRODUCTOS DE SEGURIDAD

Una transición gradual hacia la criptografía poscuántica

La futura desaparición de los actuales algoritmos de seguridad de datos frente a la computación cuántica, ¿marca el ocaso del cifrado? «*Si todo el sector no reacciona de forma concertada, sí*» —señala Yvan Vanhullebus antes de matizar esta idea de obsolescencia programada de los sistemas de cifrado— *No hay alternativa real: los algoritmos, protocolos y sistemas tendrán que evolucionar*». Esta evolución requiere el desarrollo de algoritmos matemáticos capaces de resistir los ataques clásicos y los futuros ataques cuánticos. Al igual que ciertos algoritmos de cifrado simétrico: si se considera que el algoritmo AES128 podría vulnerarse por un futuro ordenador cuántico, este se consideraría debilitado, pero seguiría siendo bastante resistente. En Estados Unidos, esta perspectiva de seguridad nacional se toma muy en serio. En 2015, el físico canadiense Michele Mosca presentó los resultados de su investigación en el ámbito cuántico e introdujo el teorema que llevaría su nombre: el teorema de Mosca. Con miras a responder a la pregunta «¿cuándo debemos preocuparnos por la cuántica?», teorizó lo que se convertiría en uno de los preceptos de la mecánica cuántica. Si la suma del tiempo durante el cual los datos cifrados deben permanecer seguros (X) y el tiempo necesario para reequipar la infraestructura existente con una solución de seguridad cuántica a gran escala (Y) es mayor que el tiempo necesario para construir un ordenador cuántico a gran escala u otros avances pertinentes (Z), hay motivos para preocuparse.

De hecho, **todo el universo de la ciberseguridad debe ahora acelerar su transición hacia un mundo poscuántico**. Se perfilan diversos ejes de interés. Por un lado, la criptografía poscuántica, cuyo objetivo es estudiar nuevos problemas matemáticos subyacentes a los protocolos de cifrado, para hacerlos más resistentes a los ataques que posibilitaría la aparición de ordenadores cuánticos a gran escala. Por otro, la criptografía cuántica, que modifica el soporte físico de la información apoyándose en las nuevas tecnologías cuánticas. La criptografía poscuántica es, para la ANSSI, «*la forma más prometedora de protegerse frente a la amenaza cuántica*». Sin embargo, la posición de esta agencia francesa es más prudente que la de su homóloga estadounidense, la NSA, que presiona para que se adopten cuanto antes las tecnologías poscuánticas. En un dictamen exhaustivo sobre la migración a la criptografía poscuántica publicado en su web en abril de 2022, la agencia francesa aconseja que la industria avance gradualmente hacia algoritmos poscuánticos. Un mecanismo híbrido que tiene así la ventaja de combinar «*los cálculos de un algoritmo de clave pública precuántico reconocido y de un algoritmo poscuántico adicional*» y de «*beneficiarse a la vez de la fuerte garantía de resistencia del primero frente los atacantes clásicos y de la resistencia conjeturada del segundo frente a los atacantes cuánticos*». Por su parte, los editores, ¿tendrán que evolucionar también sus protocolos de cifrado para adaptarse al cifrado poscuántico? Para Noël Chazotte, esta transición tendrá que producirse, si bien existe una gran incógnita: ¿cuál es el calendario de despliegue? ¿Y con qué algoritmos? «*En este tema, solo podemos estar de*

acuerdo con la ANSSI: el ámbito aún no ha alcanzado la madurez. Es imposible predecir cómo se comportarán los algoritmos poscuánticos dentro de cinco años —señala—. El algoritmo *SIKE* por *ejemplo, fue durante mucho tiempo una auténtica promesa en el ámbito de lo cuántico antes de que se revelara su vulnerabilidad a un ataque clásico en el verano de 2022 por investigadores belgas...*».

Distribución cuántica de claves para aplicaciones específicas

Existen alternativas al cifrado poscuántico, pero son menos prometedoras porque se limitan a aplicaciones específicas. Este es el caso de la (QKD por sus siglas en inglés), un conjunto de protocolos para distribuir una clave de cifrado entre dos interlocutores a distancia, garantizando al mismo tiempo la seguridad de la transmisión gracias a las leyes de la física cuántica y de la teoría de la información. Se trata de una familia de métodos basados en principios físicos, no matemáticos como en el caso de la criptografía habitual, que permite a dos interlocutores establecer un «secreto común» (una clave) para dialogar. La QKD suele destacarse por establecer comunicaciones confidenciales con integridad, es decir, no modificables por un atacante. Para ello se necesitan dos canales: uno con propiedades físicas controladas (una fibra óptica o un enlace directo al aire libre) sin ningún dispositivo que interactúe con la información transportada, y un enlace de red convencional.

Por tanto, la QKD depende totalmente de las características físicas de los canales que utiliza, lo que hace que su despliegue a gran escala sea «complejo y costoso», según el criterio de la ANSSI. Además, la agencia francesa considera que la distribución cuántica de claves no es «*la vía evolutiva natural de las comunicaciones seguras*». Esto se debe a que la falta de una línea directa entre dos puntos obliga a los usuarios a negociar claves por tramos en una ruta formada por varios nodos, lo que requiere la confianza en estos intermediarios. Se trata de «*un gran paso atrás con respecto a los actuales métodos de negociación de claves de extremo a extremo*», señala la autoridad. Así, esta tecnología solo podría utilizarse para aplicaciones muy especializadas.

De la teoría a la industrialización

La era de la computación cuántica no ha hecho más que empezar y los retos que plantea ya son numerosos. La vigilancia activa, la anticipación, la agilidad y la adaptación a esta nueva amenaza son ahora brújulas esenciales para abarcar la informática cuántica y la ciberseguridad. Por un lado, la carrera tecnológica hacia el ordenador cuántico es compleja y costosa. Las inversiones presupuestarias, del orden de varias decenas de miles de millones de euros, constituyen un obstáculo importante. La necesidad de protección criptográfica frente a los ataques cuánticos es compleja y costosa. Para Yvan Vanhullebus, «*aunque ya se ha alcanzado la fase teórica, aún quedan grandes pasos por dar antes de llegar a la era de su industrialización*». La normalización de los primeros algoritmos fue una de ellas, pero, por reciente que sea, aún se necesita tiempo

para evaluar realmente su solidez. Paralelamente, también será necesario elaborar otras normas para su uso en un contexto híbrido, tal como recomienda la ANSSI. En la actualidad, también se plantea la cuestión con respecto a los componentes de hardware, que por su propia naturaleza tienen una inercia real. «*Es un tema que en Stormshield hemos afrontado con total seriedad desde sus inicios*» —explica Yvan Vanhullebus—. *En el caso de nuestros cortafuegos Stormshield Network Security, por ejemplo, ya estamos integrando los últimos TPM Infineon, el único componente TPM del mercado que ofrece protección poscuántica* ».

Es importante que todos los actores de la ciberseguridad den los pasos necesarios ahora para anticiparse a la era de la computación cuántica y la criptografía poscuántica. **¿El objetivo? No ser víctimas, sino actores de esta gran evolución tecnológica**. En este contexto, Europa busca su lugar.