Las amenazas a la seguridad

Seguro que has leído más de una vez que la computación cuántica representará un reto importante para la seguridad porque podrá romper los sistemas de cifrado, y, de paso, las firmas digitales, *blockchain*, las criptomonedas y los contratos inteligentes. ¿Cómo estar preparado?

[ILUSTRACIÓN: DANIEL MONTERO GALÁN]

A día de hoy nadie sabe cuándo existirá un ordenador cuántico con la suficiente capacidad (diseño y cúbits[1]) para romper la criptografía usada actualmente. Cuando Google proclamó que había conseguido la supremacía cuántica en2019 afirmó que para romper RSA se necesitarían 4.096 cúbits. En 2019 el chip Sycamore de Google tenía 52 cúbits, pero para añadir cúbits hay que hacerlo sin incrementar la temperatura, así que cada vez es más difícil añadir cúbits sin que pierdan la coherencia.

¿Y entonces por qué la empresa D-Wave dice que tiene 5.000 cúbits? Hay que diferenciar entre cúbits lógicos y cúbits físicos. Como es tan difícil añadir cúbits (lógicos) se añaden muchos cúbits (físicos) para corregir errores y obtener un cúbit (lógico), así que la próxima vez que veas un número de cúbits pregúntate si son lógicos o físicos.

La criptografía postcuántica

En definitiva, mi opinión es que se tardarán décadas en poder romper la criptografía actual con un ordenador cuántico.

Para que un algoritmo criptográfico se estandarice se prueban varios a la vez durante años. Desde 2015, el NIST[2] tiene el proyecto *Post Quantum Cryptography* (PQC) para estandarizar un nuevo algoritmo criptográfico que sea resistente a un posible futuro ordenador cuántico. Desde junio de 2021, están en la ronda tres donde hay siete finalistas y ocho candidatos alternativos[3].

Antes de seguir, es necesario aclarar que los ataques con ordenadores cuánticos o criptografía postcuántica tienen aplicación en comunicaciones militares o gubernamentales. No en los sistemas usados por empresas y particulares, que son muy débiles.

¿La criptografía necesita un ordenador cuántico para ser rota? NO

Para entender por qué las comunicaciones nunca han sido seguras —sin necesitar ordenadores cuánticos— hay que analizar varios aspectos. El primero, el legal. La legislación en los países occidentales permite que un juez ordene que se descifren los mensajes cifrados. WhatsApp, Telegram, el correo electrónico, lo que escuchan los asistentes de voz... todo está sujeto al escrutinio de la justicia. Todas las empresas de tecnología tienen que guardar los mensajes durante años. Y abrirlos si un juez se lo pide.

Cifrar consiste en desordenar los bits siguiendo un algoritmo de cifrado (por ejemplo, T-DES, AES, RSA o

curvas elípticas) y una clave (que es el parámetro que debe mantenerse secreto). Así que el cifrado es tan seguro como secreta sea la clave.

La amenaza de los ordenadores cuánticos a los sistemas criptográficos actuales es un engaño para que creas que el cifrado que utilizas hoy es seguro

En el cifrado simétrico como Triple-DES o AES, la misma clave se utiliza para cifrar y para descifrar. Es más rápido, pero tiene un problema. ¿Cómo el emisor —que ha cifrado— manda al receptor la clave —para descifrarlo—? Porque si la capturan en el camino —o legalmente tiene que existir una clave de recuperación—, la clave deja de ser secreta.

El cifrado asimétrico (RSA o curvas elípticas) se diseñó para resolver el problema. Hay dos claves: una para cifrar (pública) y otra para descifrar (privada). Solo es necesario compartir la pública, y la privada no hay que enviarla entre emisor y receptor. Así que el emisor cifra el mensaje con la clave pública del receptor (y solo el receptor puede descifrarlo). Por ejemplo, tu DNI electrónico tiene una clave pública y otra privada (que nunca sale del chip). Y son seguras siempre porque se han generado dentro del chip y nunca salen fuera del chip, ni el dueño del DNI las conoce nunca.

La fuerza bruta o probar todas las claves hasta que la encuentres

Si el algoritmo es seguro —se ha probado durante años— y la clave secreta, la única forma de romper el cifrado es probando todas las posibles claves. A esto se le llama ataque por fuerza bruta. Las claves RSA actuales suelen ser de 2.048 o de 4.096 bits (de ahí que Google dijera que necesitan 4.096 cúbits para romper RSA). Y, por eso, si existiera un ordenador cuántico que probara en paralelo todas las posibles claves podría encontrar el secreto.

Una clave de 4.096 bits tiene 2^{4096} posibles valores o aproximadamente 10^{1234} . Así que la seguridad se llama computacional porque no habría suficiente materia ni tiempo en el universo para probarlas todas. Ya veremos si la coherencia cuántica encuentra algún día las claves.

Los números aleatorios

Hoy en día, las claves de cifrado se generan aleatoriamente —no confundir con una contraseña que elige el usuario—. Y ahí está la trampa. Si no tienes un buen generador de números aleatorios, tus claves puede que no tengan 4.096 bits independientes.

Imagina un dado de seis caras que fuera perfecto, y que la probabilidad de que salga cualquier cara es la misma: 1/6. Es perfectamente aleatorio y, sin embargo, solo son seis números así que los puedo probar todos.

Si tenemos una clave que tiene digamos 32 bits aleatorios y el resto calculados en función de los primeros, no tendríamos 2^{4096} posibilidades, sino 232 = 4.000 millones y fácilmente atacable por fuerza bruta. Tradicionalmente, se ha dicho siempre que solo los generadores de números aleatorios por *hardware* son buenos. Incluso hay generadores cuánticos de números aleatorios. Pero antes o después habrá un conversor A/D que recortará el número de bits y limitará el número de claves a probar.

La computación cuántica solo podrá aumentar la seguridad. Disminuirla no se puede

La verdadera aplicación de un ordenador cuántico será verificar si una clave es realmente aleatoria o no. Si los 4.096 bits son independientes. Y parece que eso ya lo hace el chip de 52 cúbits de Google.

Por cierto, para generar números aleatorios (por *software*) de longitud larga, lo mejor es usar RSA. Utilizando un texto al azar cifrado con una clave al azar se debe generar un numero aleatorio (estás aumentando el desorden, en eso consiste cifrar) de modo que estás generando un resultado más aleatorio que con el que empezaste (siempre que al final olvides el texto y la clave de partida). Lo interesante sería pasar un número aleatorio así generado por el verificador cuántico de Google. Si el resultado no es aleatorio verificable, es que el método RSA también tiene trampas en su diseño (lo desconozco).

¿Y necesito ordenadores cuánticos para romper *blockchain*, la firma digital, los contratos inteligentes? Tampoco.

Aquí la trampa está en las funciones *hash*. Tú no firmas un documento, firmas un *hash* del documento. ¿Qué es un *hash*? Es un resumen del documento generado con algoritmos como SHA256 a SHA512, (o los que no deberían utilizarse como MD-5 o SHA-1). Haces un resumen usando todos los bits del documento y acabas teniendo solo 256 bits. Si cambias un solo bit del documento, cambia el *hash*. Así que en teoría firmar el *hash* sería equivalente a firmar el documento.
Pero lo que siempre se olvida es que los *hashes* tienen colisiones. No puedes resumir infinitos documentos en un número finito de bits. Habrá infinitos documentos que den el mismo *hash*. Si alguien (por ejemplo, la NSA4) supiera cómo generar colisiones (documentos que den el mismo *hash*, y habrá infinitos) podría decir que el documento firmado no fue el original, sino otro que daba el mismo *hash*. No hay que olvidar que las funciones *hash* estándar SHAxx fueron diseñadas por la NSA.

La seguridad la determina el punto más débil de la cadena

Edward Snowden desveló en 2013 muchos de los programas de espionaje de la NSA. Algunos incluyen la instalación de troyanos en los ordenadores de todo el mundo. Así no hay que atacar los mensajes cifrados. La NSA puede leerlos incluso antes de que se cifren.

En mi opinión, la amenaza de los ordenadores cuánticos a los sistemas criptográficos actuales es una cortina de humo para que creas que el cifrado que utilizas hoy es seguro.

Y partiendo de esta situación, estoy seguro de que la computación cuántica solo podrá aumentar la seguridad

—disminuirla no se puede—. Puede que sea buena idea guardar alguno de los candidatos que no ganen el PQC. Así evitaríamos volver a usar todo el mundo en el futuro el mismo algoritmo estándar de cifrado postcuántico.

Así que, lo siento, el mundo está lleno de trileros. Y el juego es ¿dónde está la bolita?

Fernández Lara, C. (2021): "La computadora del futuro de Google que parece bote de basura", en *Forbes*. Disponible en: https://forbes.co/2021/08/26/tecnologia/la-computadora-del-futuro-de-google-que-parece-bote-de-basura/
Sec Lab (2020): "La computación cuántica y el 'futuro de la criptografía': la criptografía post-cuántica", en *BBVA Next Technologies*. Disponible en: https://www.bbvanexttechnologies.com/pills/la-computacion-cuantica-y-el-futuro-de-la-criptografia-la-criptografia-post-cuantica/
Snowden, E.: *Continuing Ed – With Edward Snowden*. Disponible en: https://edwardsnowden.substack.com
Wikipedia: Revelaciones sobre la red de vigilancia mundial (2013-2015). Disponible en: https://es.wikipedia.org/wiki/Revelaciones_sobre_la_red_de_vigilancia_mundial_(2013-2015)