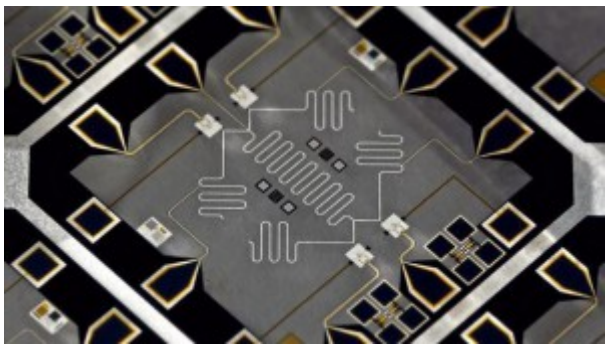
Demuestran que 15 es igual a 3×5 casi la mitad de las veces



Investigadores crean un procesador cuántico, prototipo de una tecnología que puede revolucionar la informática.

La seguridad de las transacciones bancarias o de las compras «online» puede estar en jaque. Los sistemas de cifrado que las protegen caerían derrotados en cuestión de minutos ante los «ordenadores cuánticos». Piezas de una tecnología aún en pañales, pero que prometen revolucionar lo que se puede y no se puede hacer con un ordenador.

Un grupo de investigadores de la Universidad de Santa Bárbara (California) ha desarrollado un «procesador cuántico» capaz de descomponer el número 15 en sus factores –los números primos cuya multiplicación da como resultado esa cifra– (3 y 5). Aunque no parece una proeza, no era tan fácil. Todavía no está muy claro cómo –o si se puede– desarrollar plenamente la computación cuántica.

Aunque descomponer el 15 en factores es sencillo y rápido, hacerlo con números gigantes –de 500 o 600 dígitos– es harina de otro costal. La edad del universo –más de 13.000 millones de años– no sería tiempo suficiente para que un ordenador actual pudiese llevar a cabo el reto.

El proceso contrario –encontrar el resultado de multiplicar una serie de números primos–, sin embargo, es fácil y

rapidísimo. En esta propiedad matemática –lo fácil que es en un sentido y lo difícil que es en el otro– se basan la mayoría de métodos de cifrado que se usan en la actualidad. Depende de ella, por tanto, la seguridad digital del mundo entero.

En teoría, los ordenadores cuánticos serían capaces de factorizar –descomponer– números gigantes en apenas minutos. El procesador cuántico desarrollado por estos científico, que han publicado sus resultados en la revista Nature Physics, es un pequeño paso más en esta dirección. «Un ordenador cuántico puede resolver este problema miles de billones de veces más rápido que un ordenador clásico», explicó Erik Lucero, investigador principal.

«Lo importante es que los conceptos utilizados para factorizar este número (15) se mantienen a la hora de factorizar otros más grandes», dijo Andrew Cleland, colaborador en los experimentos. «Sólo necesitamos hacer un procesador mucho más grande. No será fácil, pero el camino está claro».

Criptografía cuántica

¿Y qué pasará con la seguridad digital si consigue desarrollar ordenadores cuánticos? ¿Qué reemplazará los sistemas de cifrado actuales? La respuesta, explicó Lucero, está en la «criptografía cuántica». «No sólo es más difícil de romper, , sino que además te permite saber si alguien la ha intervenido. Imagina alguien pinchando una llamada de teléfono, pero que cada vez que intenta escuchar, el audio empeora mucho. Con criptografía cuántica, si alguien intenta extraer información, esto cambia el sistema, por lo que tanto el emisor como el receptor pueden saberlo».

La criptografía cuántica, por su parte, está más desarrollada y avanzada que la computación cuántica. De hecho, ya tiene un cierto uso en una aplicación denominada Quantum Key Distribution (QKD).

Sólo la mitad de las veces

Los investigadores eligieron el 15 porque «es el número más pequeño que cumple las condiciones para probar el algoritmo de Shor: es el producto de dos números primos y no es par». El algoritmo de Shor es un método matemático de factorización de números utilizando ordenadores cuánticos.

«Tras repetir el experimento 150.000 veces, mostramos que nuestro procesador cuántico dio con la respuesta adecuada algo menos de la mitad de las veces», explicó Lucero. «Lo máximo que se puede esperar del algoritmo de Shor es obtener la respuesta correcta un 50% de las veces, por lo que nuestros resultados son básicamente los que podíamos esperar».

El próximo paso, afirmó Lucero, es pasar de unos pocos elementos cuánticos a cientos, luego miles y después millones. «Ahora que sabemos que 15 es igual a 3×5, podemos empezar a pensar en cómo factorizar números más grandes y —permítanme la osadía— prácticos», aseguró.

fuente:abc