Hackear la realidad, los secretos de la criptografía cuántica

Por: Alejandro Massa Varela. 14/11/2024

¿Qué son los qubits y en qué se basa el poder de la computación cuántica? ¿Por qué es teóricamente imposible copiar su información con exactitud? ¿Qué es el "teorema de la no clonación" y por qué es la clave de la seguridad de la criptografía cuántica?

La conocida como "criptografía cuántica" es lo más novedoso en tecnología para preservar y ocultar información. Se basa en el hecho de que el estado de los mensajes cifrados de la computación cuántica no se pueden copiar sin colapsarse o corromperse también.

El *Grupo de Física Fundamental* fue una iniciativa de estudiantes del *Laboratorio Lawrence Berkeley* con un interés en común por descubrir posibles puntos de encuentro entre la mecánica cuántica y el misticismo oriental, las experiencias con drogas psicodélicas y fenómenos parapsicológicos como la telepatía. Precisamente su mayor iniciativa consistió en poner a prueba si una persona podía recibir mensajes de otra de una manera semejante al "entrelazamiento" de entidades cuánticas como los fotones. Otro tipo de influjo a distancia o "no local" denominado "visión remota". A pesar de recibir fondos de la CIA, esta investigación sería tachada de pseudocientífica.

Sin embargo, en su libro *Cómo los hippies salvaron la física*, el profesor del MIT e historiador de la ciencia David Kaiser asegura que, aunque este experimento estudiantil fue un completo fracaso, las preguntas radicales de su planteamiento han sido clave para algo tan importante como el "teorema de la no clonación", el principio básico de la actual criptografía cuántica.

El padre teórico de la computación cuántica, el estadounidense Richard Feynman, pronosticó a mediados del siglo XX que, conforme los componentes electrónicos fueron alcanzando escalas nanométricas, hoy pueden diseñarse ordenadores cada vez más potentes. Esta profecía sobre el estado de la informática le valió el Premio Nobel de física en 1956. En palabras de Seth Lloyd, profesor de ingeniería mecánica

y sistemas cuánticos en el MIT:

No podríamos construir computadoras cuánticas a menos que el universo fuera cuántico y computacional. Podemos construir esas máquinas porque el universo almacena y procesa información en el ámbito cuántico. Cuando construimos computadoras cuánticas, estamos secuestrando esa computación subyacente para que haga las cosas que queremos: cálculos pequeños y o no. Estamos hackeando el universo.

En la escala cuántica, los objetos parecen no adquirir estados estables y definitivos, sino “susceptibles”. De esto da cuenta el famoso experimento del físico inglés Thomas Young, en el que se hace pasar un fotón de luz a través de una pantalla con dos pequeñas rendijas, produciéndose un “patrón de interferencia” en forma de onda. Sin embargo, cuando esto intenta observarse con un detector cuántico, el patrón desaparece. Esta es la conocida como “superposición”, la simultaneidad como onda y como partícula del fotón, o que “exista” un sistema cuántico en todos los estados posibles previo a que una medición “colapse” el sistema en un estado.

Un “bit” es la unidad informática básica de las primeras computadoras. Codifica datos en binario y puede tomar los valores 0 o 1. Pero en la computación cuántica, un “qubit” como unidad de información, a diferencia de un bit, aprovecha la superposición y puede tomar simultáneamente ambos valores, lo que le permite llevar a cabo cálculos complejos de manera mucho más eficiente y rápida, un beneficio indispensable para la comunicación a alta velocidad.

Propuesto en 1982 por los físicos William Wootters y Wojciech Zurek, el teorema de la no clonación establece que un qubit colapsa siempre que se le intenta copiar. Es imposible medirlo y no perturbarlo, lo que implica que sea inviable obtener una copia o un clon exacto. Y si bien es posible duplicar un bit, no se puede replicar un qubit debido la superposición.

El teorema de no la clonación es la base de la criptografía cuántica como forma de comunicación ultrasegura. El intento de interceptar y copiar un mensaje de un ordenador cuántico alteraría los qubits, algo que asegura que cualquier acción intrusa no pueda pasar desapercibida. Y el principio de no clonación también asegura la integridad de los cálculos cuánticos.

LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ

Fotografía: Pijama surf. computación y criptografía cuánticas, Zuplexpai.

Fecha de creación
2024/11/14