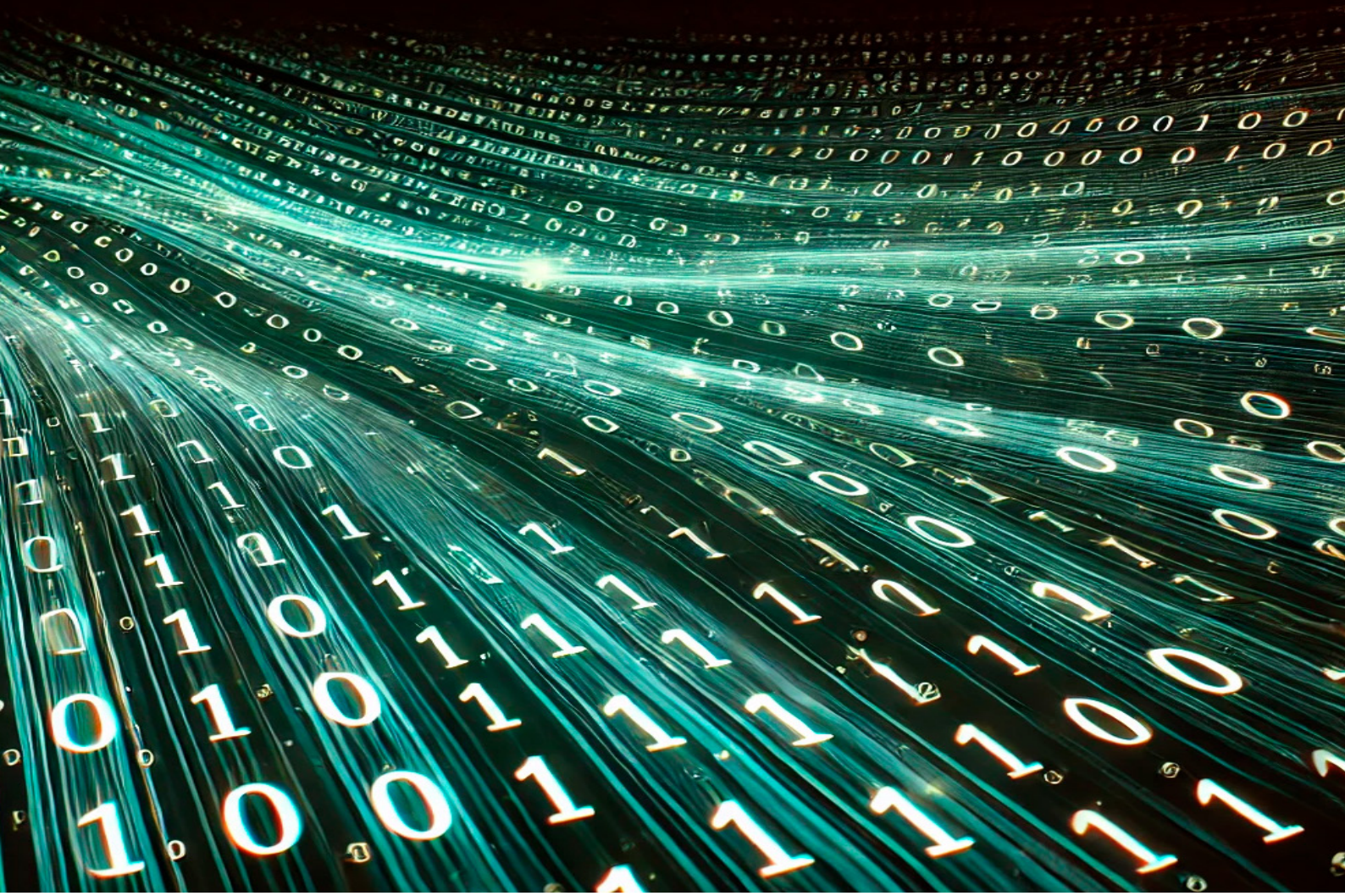
REVELACIONES CUÁNTICAS: EL PODER DE LA MECÁNICA CUÁNTICA PARA DESCIFRAR NUESTROS SECRETOS MEJOR GUARDADOS

Felipe Tejo Lazo
Dr. En Ciencias con mención en Física



Descubre cómo los enigmas del universo cuántico no sólo desafían nuestra comprensión del mundo, sino que también prometen revolucionar la tecnología, la computación y la seguridad digital en maneras que apenas comenzamos a entender.

La Mecánica Cuántica, una de las ramas más fascinantes y menos intuitivas de la física, surgió en la primera mitad del siglo XX como una necesidad de explicar fenómenos que el marco clásico, es decir, la física de nuestro entorno cotidiano no podía resolver. Científicos como Max Planck, Niels Bohr, Albert Einstein, y Erwin Schrödinger, entre otros, desarrollaron conceptos revolucionarios que desafiaban la percepción ordinaria del espacio, el tiempo y la materia. Este desarrollo no solo transformó nuestra comprensión del universo a nivel microscópico, sino que también sentó las bases para tecnologías que hoy están al borde de transformar radicalmente nuestra sociedad.

¿Qué es la Mecánica Cuántica?

La mecánica cuántica estudia las propiedades de las partículas a niveles atómicos y subatómicos, donde las leyes de la física clásica ya no aplican de la misma forma. En este universo, partículas como electrones y fotones no exhiben los mismos comportamientos que se observan en los objetos cotidianos con los que interactuamos diariamente. A modo de ejemplo, en nuestro entorno macroscópico, los objetos poseen ubicaciones precisas; por ejemplo, usted se encuentra en un lugar específico del mundo leyendo este artículo, y no en otro lugar. No obstante, en el mundo atómico, la posición de una partícula no está definida antes de observarla y lo más que podemos determinar es la probabilidad de encontrarla en una posición u otra. Este panorama cambia una vez que realizamos la medición de la partícula, momento en el cual su posición se define en un sitio determinado.

En este contexto, uno de los principios fundamentales de la Mecánica Cuántica, es el principio de superposición. La superposición cuántica es un concepto fundamental que puede parecer contraintuitivo respecto al mundo que observamos, pero es esencial para entender el desarrollo de la mecánica cuántica y sus aplicaciones en nuevas tecnologías. En un nivel básico, la superposición cuántica nos dice que las partículas subatómicas, como los electrones o los fotones, no se encuentran en un estado definido y la determinación de su estado se define una vez que se realiza su medición. A menudo se dice erróneamente que estos objetos pueden existir en múltiples estados simultáneamente, lo cual es resultado de tratar de atribuir características clásicas a sistemas cuánticos, algo que resulta incompatible.

Para hacerlo más comprensible, utilicemos la siguiente analogía: imagine una moneda que está siendo lanzada al aire. En el mundo clásico, la moneda puede caer mostrando cara o cruz. Sin embargo, mientras está girando en el aire podríamos decir que la moneda no se encuentra en un estado bien definido. No es exactamente cara ni tampoco cruz, hasta que cae y observamos el resultado. En el mundo cuántico, los objetos pueden experimentar este tipo de existencia dual o múltiple, manteniendo una indeterminación de su estado hasta que se realiza su medición. Sí bien, el ejemplo de la moneda no es rigurosamente correcto, al tratarse de un objeto macroscópico, nos permite obtener una idea básica de lo que ocurre en el universo de los átomos.

Computación Cuántica

Los actuales computadores, a pesar de su complejidad y la capacidad de realizar miles de millones de operaciones por segundo, en su nivel más básico, trabajan únicamente con dos estados: encendido y apagado, representados por los dígitos binarios 0 y 1. Cada uno de estos dígitos se llama "bit", que es la unidad más pequeña de datos en computación. El código binario es la forma en que los computadores leen y comprenden las instrucciones; todo, desde procesar texto hasta mostrar imágenes y videos, se traduce a una serie de ceros y unos. Cuando se escribe una letra en su teclado, esta acción se convierte en una señal eléctrica que representa un código binario específico; por ejemplo, la letra "A" puede ser 01000001 en binario. Esta señal binaria se envía al procesador del computador, que interpreta el código y decide qué hacer con él, como mostrar la letra "A" en la pantalla. El código binario también se usa para almacenar información; cuando guardas un documento, el computador traduce el contenido a binario y lo almacena en el disco duro en forma de ceros y unos. La razón principal por la que los computadores utilizan binario es su simplicidad y confiabilidad, ya que los circuitos electrónicos pueden estar fácilmente en uno de dos estados: alto voltaje (1) y bajo voltaje (0), permitiendo operar de manera rápida y eficiente, reduciendo la posibilidad de errores.

En contraste, los computadores cuánticos del futuro funcionarán con qubits. Los qubits son unidades de información más avanzadas los cuales pueden representar no solo los estados 0 y 1, sino también cualquier superposición cuántica de estos estados. Por ejemplo, un qubit puede estar en un estado que es una combinación de 0 y 1 simultáneamente, hasta que se mide. Cuando se mide, el qubit colapsa a uno de los dos estados clásicos (0 o 1) con una cierta probabilidad.

Otro aspecto fundamental que proviene de los principios de la Mecánica Cuántica es que los qubits pueden experimentar el fenómeno de entrelazamiento cuántico. Básicamente, esto significa que el estado de un qubit puede depender del estado de otro, sin importar la distancia entre ellos. Este fenómeno, descrito por Einstein como "acción espeluznante a distancia", permite que los computadores cuánticos realicen operaciones complejas a una velocidad increíblemente rápida, ya que los qubits entrelazados actúan de manera coordinada.

Esta capacidad de los qubits de existir en estados superpuestos y de entrelazarse con otros qubits les permitirá realizar muchos cálculos simultáneamente, potenciando una capacidad de procesamiento exponencialmente superior a la de los computadores clásicos actuales. Por ejemplo, un computador cuántico equipado con varios qubits puede resolver cálculos que serían prácticamente imposibles para un computador clásico. Esta revolucionaria capacidad hace que los computadores cuánticos sean muy prometedores para aplicaciones en criptografía, optimización de problemas y simulaciones científicas donde se requieren cálculos complejos y masivos.

Nuestros secretos al descubierto

En el mundo de las comunicaciones digitales vía internet, resguardar la seguridad de nuestra información es fundamental. En este contexto, la criptografía —el arte de codificar mensajes— es fundamental para resguardar la información. A modo de ejemplo, consideremos una actividad que hoy por hoy resulta imprescindible en nuestro día a día y que practicamos de forma cotidiana: la comunicación vía internet con nuestro banco. El Físico español José Ignacio Latorre, en su libro Cuántica Tu Futuro en Juego [1], utiliza la siguiente analogía para explicar este proceso: un mensaje, un cofre y una llave. Lo explico a continuación.

Imaginemos que el banco tiene un cofre muy especial. La única forma de abrir este cofre es utilizando una llave única que consiste en dos números primos muy grandes (un número primo es un número que sólo es divisible por 1 y por sí mismo, ejemplo: 2, 3, 5, 7 …). Estos dos números, cuando se multiplican, forman la llave pública —el cofre— mientras que los números individuales se guardan en secreto como la llave privada.

Paso a Paso en la Criptografía Moderna

Paso 1: Generación de Claves:

- El banco elige dos números primos secretos y los multiplica.

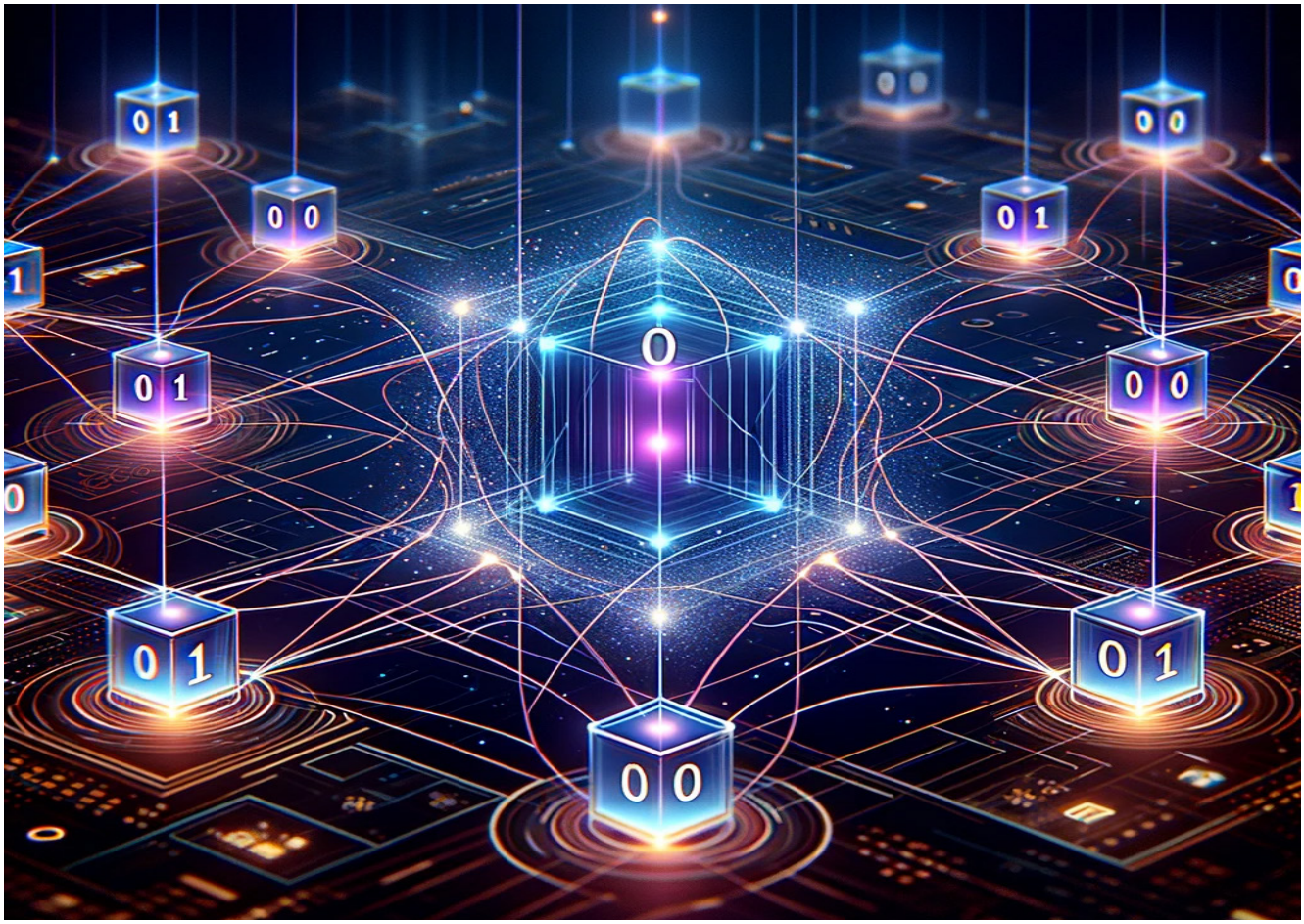


Figura 1

Representación artística creada por IA de un arreglo de qubits en un procesador cuántico, donde cada qubit posee la capacidad de mantener estados de superposición y entrelazamiento cuántico.

- El resultado de esta multiplicación es un número enorme que se convierte en la llave pública.

Paso 2: Comunicación de la Clave:
- El banco mantiene en secreto los dos números primos originales y solo envía el producto de estos (la llave pública) al usuario.

Paso 3: Codificación y Envío de Mensajes:
- El usuario utiliza esta llave pública para codificar su mensaje.
- Una vez codificado, el mensaje se envía de vuelta al banco.

Paso 4: Descodificación del Mensaje:
- El banco usa sus dos números primos secretos para descodificar el mensaje.

Esta es la forma en que compartimos nuestra información secreta con la sociedad actual cuando usamos internet. Este método, conocido como RSA (por las iniciales de sus creadores, Ron Rivest, Adi Shamir, y Leonard Adleman), es ampliamente utilizado debido a su solidez matemática. La clave de su seguridad radica en que, aunque la llave pública (el producto de dos números primos) es conocida por todos, factorizarla —es decir, descomponerla en sus factores primos originales— es extremadamente difícil con la tecnología actual.

Imaginemos que un ladrón obtiene la llave pública. Aunque conozca el número resultante, sin los dos números primos originales, no puede descifrar el mensaje. Factorizar un número grande, como los que se usan en RSA, es tan difícil que se estima que llevaría más tiempo del que el universo ha existido hasta ahora usando tecnología actual. Es decir, la forma de descifrar un mensaje no es un problema en sí mismo, sino que los tiempos necesarios para hacerlo son extremadamente extensos.

Sin embargo, la llegada anticipada de la computación cuántica podría cambiar este escenario. Los computadores cuánticos prometen la capacidad de factorizar estos grandes números de manera eficiente, lo que podría hacer vulnerables todos los sistemas de criptografía actuales como el RSA.

Aunque la computación cuántica aún se encuentra en una fase experimental, la historia nos ha demostrado que el avance científico es implacable. Las teorías que en su momento parecían meras especulaciones han dado paso a innovaciones tecnológicas que han transformado el curso de la humanidad y modificado profundamente nuestras interacciones sociales. Aún es incierto cuándo los primeros computadores cuánticos comerciales estarán disponibles o cuál será su costo. Sin embargo, si algo podemos anticipar con certeza es que, al alcanzar este hito, el mundo tal como lo conocemos experimentará una transformación radical. Este progreso nos invita a reflexionar sobre el poder de la ciencia y la tecnología para moldear nuestro futuro, subrayando la importancia de seguir explorando los límites del conocimiento humano.

[1] Latorre, J. I. (2017). Cuántica: Tu futuro en juego (3ª ed.). Ariel.
[2] Hürter, T. (2022). Tiempo de Incertidumbre: Los brillantes y oscuros años de la física (1951-1945). TusQuets Editores.
[3] Sabin, C. (2020). Verdades y mentiras de la física cuántica. CSIC, Catarata.