NOVA BCU

Disrupción de la computación cuántica en el sistema financiero.

Documento técnico acompañante.

BANCO CENTRAL DEL URUGUAY

Contenido

Introducción

Este documento, que acompaña a "*Disrupción de la computación cuántica en el sistema financiero y de pagos:* Principales conceptos, impacto esperado y propuesta de abordaje para autoridades financieras", busca complementar la información relativa a la computación cuántica, ofreciendo un recorrido sobre sus principales fundamentos con el fin de que el lector interesado pueda lograr una mayor comprensión de la disciplina, y que esto contribuya a un abordaje más informado por parte de las autoridades financieras. Si bien este documento no pretende ser exhaustivo ni demasiado riguroso en el trasfondo técnico y científico de la computación cuántica, dos referencias bibliográficas resultaron fundamentales al momento de elaborarlo: el libro "*Quantum Computation and Quantum Information: 10th Anniversary Edition*" de Nielsen y Chuang (2000), y el libro "*Introduction to Classical and Quantum Computing*" de Wong (2023).

En el presente documento se estructura en cuatro grandes secciones: Principales fundamentos de la computación cuántica, Computación cuántica y ciberseguridad: amenazas y oportunidades, Desarrollo de la computación cuántica en los proveedores de servicios y Modelos de procesamiento híbridos.

La primera sección introduce los fundamentos de la computación cuántica, explicando cómo la física cuántica ha dado origen a esta nueva forma de procesamiento de información. Se destacan conceptos clave como la superposición, el entrelazamiento y la interferencia cuántica, que permiten a los cúbits realizar cálculos de manera exponencialmente más eficiente que los bits clásicos. Además, se presenta el Algoritmo de Shor (1994), que amenaza la criptografía actual, y el Algoritmo de Grover (1994), que acelera la búsqueda en grandes volúmenes de datos. Adicionalmente, se analizan las diversas tecnologías utilizadas para implementar cúbits, incluyendo superconductores, iones atrapados, átomos fríos y fotones, evaluando su estabilidad, escalabilidad y eficiencia operativa en la construcción de computadoras cuánticas.

En la segunda sección, se examinan los riesgos que la computación cuántica representa para la seguridad digital. Se explica cómo el algoritmo de Shor puede comprometer la criptografía asimétrica, incluyendo RSA y ECC, y cómo el algoritmo de Grover afecta la seguridad de la criptografía simétrica. Se introduce el Teorema de Mosca (2015), que advierte sobre la urgencia de la transición a criptografía post-cuántica, y el fenómeno "Harvest Now, Decrypt Later", que alerta sobre la recopilación masiva de datos cifrados para su eventual descifrado cuando la computación cuántica sea lo suficientemente avanzada. También se presentan innovaciones como la distribución cuántica de claves (QKD), la generación cuántica de números aleatorios (QRNG) y la firma digital cuántica.

En la tercera sección, se abordan los avances tecnológicos en computación cuántica y los principales desarrolladores de hardware cuántico. Se analizan las arquitecturas de varios procesadores cuánticos, destacando el volumen cuántico y la fidelidad de operación como métricas clave para evaluar su rendimiento. Se comparan los enfoques de computación cuántica universal basada en compuertas y el recocido cuántico (quantum annealing), utilizado principalmente para problemas de optimización.

Finalmente, en la cuarta sección se explica cómo la computación cuántica aún no ha alcanzado la madurez suficiente para reemplazar completamente la computación clásica, por lo que se están desarrollando modelos híbridos que combinan ambas tecnologías. Se presentan algunos casos de uso, y se describen las plataformas de computación cuántica en la nube que facilitan la integración de modelos híbridos en infraestructuras existentes.

Por último, se realizan unos breves comentarios finales.

Principales fundamentos de la computación cuántica

A continuación, se presentan algunos de los elementos centrales que vuelven a la física cuántica una disciplina con enorme potencial para la computación, el cálculo y el procesamiento de datos.

Se intentará darle un abordaje desde los conceptos primarios de la física cuántica, pasando por la relación en los fundamentos teóricos de la computación clásica y la cuántica, y culminando con las características de la computación cuántica que hacen a su enorme potencial.

De la física cuántica a la computación cuántica

La física cuántica es la rama de la ciencia que estudia el comportamiento y las propiedades fundamentales de la materia y la energía a escalas extremadamente pequeñas, como los átomos y las partículas subatómicas. Sus principios, como la superposición, el entrelazamiento cuántico y la dualidad onda-partícula, han revolucionado la comprensión del universo y han dado lugar a aplicaciones innovadoras, incluida la computación cuántica.

Mientras que la física cuántica abarca todas las teorías, principios y fenómenos relacionados con el comportamiento de las partículas a escala subatómica, donde las leyes de la física clásica no son aplicables, la mecánica cuántica constituye una rama específica encargada de describir y modelar matemáticamente el comportamiento de partículas como electrones, fotones y átomos, utilizando conceptos fundamentales como el principio de incertidumbre de Heisenberg, la dualidad onda-partícula y el colapso de funciones de onda. Ésta se enfoca principalmente en el desarrollo de ecuaciones y herramientas formales, como la ecuación de Schrödinger, para predecir y explicar el comportamiento de sistemas físicos a nivel microscópico.

Por otro lado, la computación cuántica es un campo de conocimiento interdisciplinario que combina la informática y la física cuántica para desarrollar una nueva generación de computadoras capaces de resolver problemas que están más allá del alcance de las computadoras clásicas.

A diferencia de las computadoras tradicionales, que utilizan bits clásicos (0 o 1), las computadoras cuánticas utilizan cúbits, los cuales pueden existir en estados de superposición (0 y 1 simultáneamente) y pueden estar entrelazados con otros cúbits, lo que permite procesar información de manera exponencialmente más eficiente.

Asimismo, la teoría de la computación estudia los límites y capacidades de los modelos de cómputo para resolver problemas mediante algoritmos. Uno de sus ejes principales es la complejidad computacional, que mide la cantidad de recursos (como tiempo y memoria) necesarios para ejecutar un algoritmo. Existen problemas que requieren una cantidad prohibitiva de recursos en los modelos clásicos de cómputo, lo que los hace inabordables a gran escala, algo que no siempre es un punto negativo, ya que en el campo de la criptografía esta propiedad es de suma importancia y permite considerar ciertos algoritmos como seguros. Sin embargo, algunos de estos problemas clásicamente intratables pueden resolverse en tiempos razonables utilizando algoritmos cuánticos, lo que amplía significativamente el horizonte del cálculo eficiente.

Abordando la teoría de la computación, la Máquina de Turing Cuántica es un modelo teórico que extiende el concepto fundamental de la Máquina de Turing clásica (ver Recuadro 1) al ámbito de la mecánica cuántica. Como es de esperar, en lugar de operar con estados discretos de 0 y 1, este modelo utiliza cúbits y permite que el sistema esté en una superposición de múltiples estados simultáneamente. Gracias a este principio, la Máquina de Turing Cuántica puede explorar múltiples

soluciones en paralelo, acelerando significativamente la resolución de ciertos problemas computacionales. Un concepto fundamental es que todo algoritmo cuántico puede ser representado y expresado en términos de una Máquina de Turing Cuántica, lo que establece un marco formal para la computación cuántica.

Recuadro 1. Máquina de Turing

Una Máquina de Turing es un modelo teórico de computación creado por Alan Turing en 1936, diseñado para representar el proceso de ejecución de algoritmos de forma abstracta. Consiste en una cinta infinita dividida en celdas, un cabezal que puede leer y escribir símbolos en dichas celdas, un conjunto finito de estados y una tabla de transición que define las reglas de operación. A partir de estas reglas, la máquina puede modificar los símbolos, cambiar de estado y mover el cabezal hacia la izquierda o derecha, con el objetivo de simular cualquier cálculo computacional. Este modelo es fundamental en la teoría de la computación, ya que establece los límites de lo que es computable y es la base de conceptos clave como la decidibilidad, la complejidad algorítmica y la Tesis de Church-Turing, que sostiene que cualquier problema resoluble mediante un algoritmo puede ser simulado por una Máquina de Turing.

Programación y algoritmos cuánticos

Desde la perspectiva del contenido de las aplicaciones, la programación cuántica es el desarrollo de software específicamente diseñado para ejecutarse en computadoras cuánticas. Dado que estas máquinas operan bajo principios radicalmente distintos a los sistemas clásicos, los lenguajes y paradigmas de programación cuántica pueden y deben aprovechar fenómenos como la interferencia cuántica, superposición y el entrelazamiento. Consecuentemente, un algoritmo cuántico es un procedimiento computacional optimizado para computadoras cuánticas, diseñado para explotar las propiedades fundamentales de la mecánica cuántica. En ese sentido, a diferencia de los algoritmos clásicos, los algoritmos cuánticos pueden procesar múltiples soluciones simultáneamente y pueden emplear la interferencia cuántica para reforzar los resultados correctos y cancelar los incorrectos.

Si bien todo algoritmo clásico puede ser expresado en términos de un algoritmo cuántico, la verdadera ventaja de la computación cuántica radica en su capacidad para resolver problemas de manera exponencialmente más rápida en comparación con las computadoras clásicas.

Los algoritmos cuánticos pueden clasificarse en distintas categorías en función de sus principios matemáticos y su aplicabilidad a problemas específicos. A continuación, se presentan las principales clases de algoritmos cuánticos junto con ejemplos destacados.

Algoritmos cuánticos basados en Transformadas de Fourier Cuánticas

Estos algoritmos utilizan la Transformada de Fourier Cuántica (QFT), que es una generalización cuántica de la Transformada de Fourier Discreta. Esta técnica es clave en problemas relacionados con la periodicidad, factorización y logaritmos discretos.

- Algoritmo de Factoreo de Shor
    - Problema que resuelve: descomposición de un número entero en sus factores primos.
    - Principio: utiliza la QFT para encontrar la periodicidad de una función modular, lo que permite calcular factores primos de grandes números en tiempo polinomial.
    - Aplicaciones: criptografía, particularmente en la ruptura de RSA. Más adelante será detallado en profundidad en este informe.
- Algoritmo del Logaritmo Discreto
    - Problema que resuelve: cálculo del logaritmo discreto en un grupo finito.
    - Principio: se basa en la QFT para encontrar la estructura periódica del logaritmo discreto en grupos cíclicos.

    - Aplicaciones: ataques a sistemas criptográficos basados en logaritmos discretos, como Diffie-Hellman y ECC.
- Problema del Subgrupo Oculto (HSP, Hidden Subgroup Problem)
    - Problema que resuelve: determinar subgrupos ocultos en estructuras algebraicas.
    - Principio: utiliza la QFT para detectar periodicidades en funciones que ocultan información estructural.
    - Aplicaciones: factorización, logaritmo discreto, problemas en grupos abelianos y no abelianos.

Algoritmos de búsqueda y optimización cuántica

Estos algoritmos aprovechan la superposición y la interferencia cuántica para acelerar búsquedas en espacios no estructurados.

- Algoritmo de Búsqueda de Grover
    - Problema que resuelve: búsqueda en bases de datos no estructuradas.
    - Principio: reduce el número de operaciones requeridas para encontrar un elemento en una lista desordenada de N elementos de $O(N)$ en la computación clásica a $O(\sqrt{N})$.
    - Aplicaciones: criptografía (ataques de búsqueda inversa), problemas de optimización combinatoria. También será detallado más adelante en este documento.
- Algoritmos Cuánticos de Optimización (QAOA y VQE)
    - Problema que resuelven: minimización de funciones objetivo en problemas de optimización combinatoria.
    - Principio: se basan en heurísticas cuánticas, como el Quantum Approximate Optimization Algorithm (QAOA) y el Variational Quantum Eigensolver (VQE), que combinan técnicas clásicas y cuánticas.
    - Aplicaciones: finanzas, logística, diseño de materiales, inteligencia artificial.

Algoritmos basados en simulación cuántica

Aprovechan la capacidad de los sistemas cuánticos para simular sistemas físicos de manera más eficiente que los métodos clásicos.

- Simulación de Sistemas Cuánticos
    - Problema que resuelve: modelado de moléculas y materiales cuánticos.
    - Principio: utiliza cúbits para representar directamente estados cuánticos de sistemas físicos, evitando la necesidad de aproximaciones costosas en supercomputadoras clásicas.
    - Aplicaciones: química cuántica, física del estado sólido, desarrollo de nuevos materiales y fármacos.
- Algoritmos de Monte Carlo Cuántico
    - Problema que resuelve: simulación de sistemas probabilísticos complejos.
    - Principio: utiliza técnicas de interferencia cuántica para acelerar métodos estocásticos, reduciendo el número de muestras requeridas para obtener estimaciones precisas.
    - Aplicaciones: finanzas, climatología, mecánica estadística.

Algoritmos cuánticos de aprendizaje automático

Buscan aprovechar la computación cuántica para acelerar tareas de machine learning.

- Support Vector Machines Cuánticas (QSVM)
    - Problema que resuelve: clasificación de datos de alta dimensión.
    - Principio: utiliza circuitos cuánticos para encontrar hiperplanos de separación óptimos con menor costo computacional que las SVM clásicas.

    - Aplicaciones: análisis de datos, reconocimiento de patrones.
- Redes Neuronales Cuánticas (QNNs)
    - Problema que resuelve: entrenamiento de redes neuronales con grandes volúmenes de datos.
    - Principio: emplea cúbits y puertas cuánticas para modelar funciones de activación y pesos neuronales.
    - Aplicaciones: inteligencia artificial cuántica, análisis de big data.

Objetos cuánticos y cúbits en la computación cuántica

Un objeto cuántico es cualquier entidad que sigue las leyes de la mecánica cuántica. A diferencia de los sistemas clásicos, los objetos cuánticos pueden exhibir fenómenos únicos como superposición, entrelazamiento y dualidad onda-partícula. Ejemplos de objetos cuánticos incluyen electrones, fotones, átomos, iones y cuasipartículas en materiales superconductores.

Un cúbit (bit cuántico) es la unidad fundamental de información en computación cuántica. Aunque todo cúbit es un objeto cuántico, no todos los objetos cuánticos son cúbits, ya que un cúbit debe cumplir ciertas condiciones que permitan su control y manipulación para procesamiento de información. Los cúbits presentan las siguientes características fundamentales que serán detalladas más adelante:

- **Superposición**: un cúbit puede existir en una combinación de los estados $|0\rangle$ y $|1\rangle$ simultáneamente, hasta que es medido.
- **Entrelazamiento**: dos o más cúbits pueden correlacionarse de manera que medir uno afecta instantáneamente al otro, sin importar la distancia entre ellos.
- **Interferencia Cuántica**: los estados de los cúbits pueden sumarse y restarse, permitiendo el diseño de algoritmos cuánticos eficientes.

Tecnologías utilizadas para representar cúbits

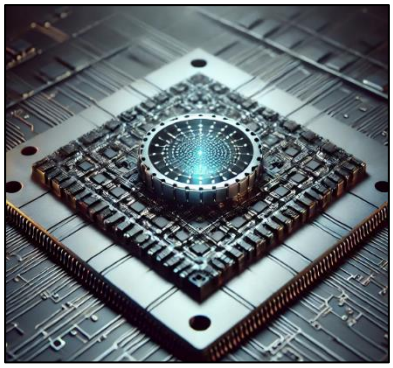
Diferentes sistemas físicos pueden ser utilizados para representar y manipular cúbits. Cada tecnología tiene ventajas y desafíos en términos de estabilidad, escalabilidad y facilidad de control. A continuación, se detalla brevemente las tecnologías más utilizadas.

Cúbits superconductores

Basados en circuitos superconductores que operan a temperaturas cercanas al cero absoluto (Clarke y Wilhelm, 2008). Son los más utilizados actualmente ya que son bastante escalables, la velocidad de operación en las compuertas es veloz, y son compatibles con tecnología ya existente. Sin embargo, el requerir estar a muy bajas temperaturas, sumado a otros elementos, hace que tengan un alto consumo energético.

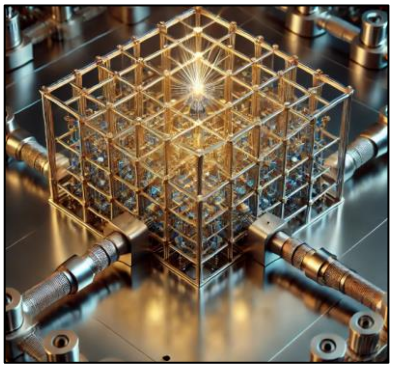
Spin de silicio

Usa el spin de electrones en materiales semiconductores como el silicio (Pla et al., 2012), permitiendo compatibilidad con tecnologías clásicas de semiconductores, lo cual es una gran ventaja para la integración y escalabilidad. Además, no tienen tanto costo energético. Sin embargo, tiene desafíos operativos y técnicos que otras tecnologías no presentan, además de tiempos de operación más lentos.



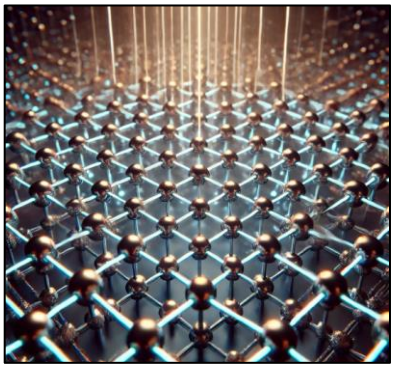
Iones atrapados

Cúbits formados por iones individuales dentro de campos electromagnéticos y manipulados con láseres (Kielpinski et al., 2002). Son altamente estables, por lo que se mantiene la coherencia por largo tiempo, y tienen una alta fidelidad operativa, no siendo necesaria una gran corrección de errores. Además, todos los cúbits de un sistema pueden interactuar entre sí. Sin embargo, esto hace que tengan una escalabilidad e integración limitada.



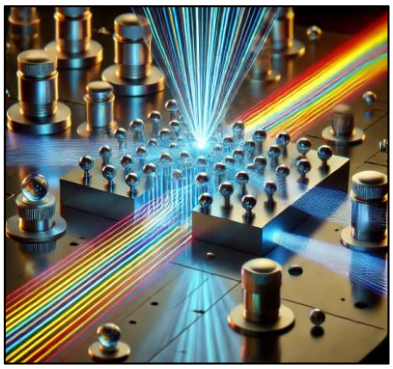
Átomos fríos/neutrales

Se utilizan átomos enfriados a temperaturas extremas y manipulados con luz láser (Henriet et al., 2020). Presentan una escalabilidad natural y una conectividad controlable, además de ser fáciles de operar en diversas compuertas y mantener una aceptable coherencia. De todos modos, requieren de tecnología compleja para el enfriado y para los láseres, y su operativa se puede volver algo compleja para manejar las redes ópticas.



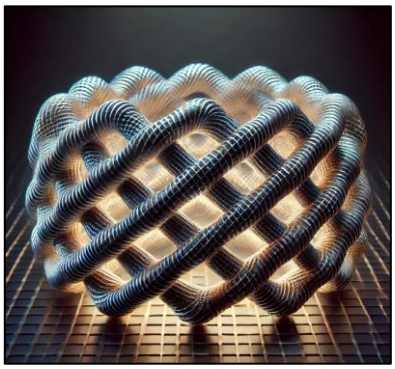
Fotónicos

Usa la polarización de fotones como cúbits (Slussarenko y Pryde, 2019), lo que permite una computación basada en luz con baja interferencia ambiental, lo cual contribuye a mantener una alta coherencia. Además, al operar a la velocidad de la luz, las operaciones y transmisiones de información se hacen rápidamente. Esto también las hace ideales para la comunicación cuántica. Sin embargo, la tecnología para su operativa es muy compleja.



Cúbits topológicos

Se basan en el movimiento colectivo de cuasipartículas exóticas en materiales cuánticos (Merali, 2019) Presentan una mayor robustez natural contra errores y mantienen un buen tiempo de coherencia. Su sólida base matemática da un marco conceptual robusto para su uso. Es una de las tecnologías que está más en fase experimentales, aunque Microsoft recientemente publicó el primer chip con esta tecnología (Bolgar, 2025).



Evaluación de cúbits

Para comprender mejor el potencial de una computadora cuántica existen algunas métricas claves en la evaluación de los cúbits que las componen, por ejemplo, la cantidad de cúbits y su tiempo de vida.

Cantidad de cúbits

El número total de cúbits en un sistema cuántico es una métrica básica, pero no suficiente para evaluar su capacidad computacional. Se debe considerar que un mayor número de cúbits no garantiza un mejor rendimiento si estos tienen altos errores de decoherencia o baja fidelidad en sus operaciones, por lo tanto, la calidad de los cúbits (coherencia, fidelidad, conectividad) es tan importante como la cantidad.

Tiempo de vida del cúbit

Indica cuánto tiempo un cúbit puede retener su estado antes de decaer. Esto es crucial en tecnologías de cúbits sintéticos (superconductores, semiconductores), donde los cúbits solo permanecen coherentes por microsegundos o milisegundos. En sistemas de iones atrapados o átomos neutrales, el tiempo de vida es mucho mayor, limitándose solo por la capacidad experimental de mantener los átomos atrapados.

Actualmente, la investigación en computación cuántica busca desarrollar cúbits con mayor estabilidad, menor error y mayor conectividad. Los desafíos clave incluyen:

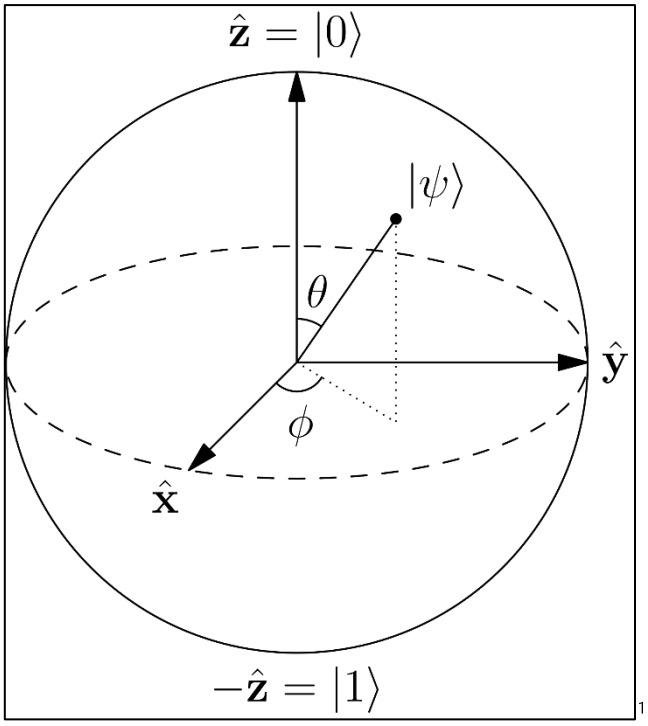
- **Escalabilidad:** aumentar el número de cúbits manteniendo su calidad y controlabilidad.
- **Corrección de errores cuánticos:** implementar códigos de corrección que mitiguen los efectos de la decoherencia.
- **Integración con tecnologías clásicas:** mejorar la compatibilidad entre arquitecturas cuánticas y sistemas actuales de procesamiento.

Esfera de Bloch

La Esfera de Bloch es una representación geométrica utilizada para visualizar el estado de un cúbit. Los estados $|0\rangle$ y $|1\rangle$ corresponden a los polos norte y sur de la esfera. Estos son los estados clásicos de la computación actual. Por otro lado, los estados de superposición se representan como puntos en la superficie de la esfera, definidos por dos ángulos θ y ϕ:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$

De esta manera, la Esfera de Bloch facilita en gran medida la visualización de las rotaciones cuánticas, interferencias y el impacto de la decoherencia, proporcionando una herramienta conceptual clave para facilitar el diseño de algoritmos cuánticos.



[1]

Propiedades fundamentales de la computación cuántica

Superposición cuántica

En la computación clásica, un bit puede tomar un único valor en un instante dado: 0 o 1. En cambio, un cúbit, gracias a la superposición cuántica, puede existir en una combinación de múltiples estados simultáneamente. A modo de ejemplo, puede considerarse una brújula tradicional que solo apunte al norte o sur (bits clásicos). Un cúbit, en cambio, puede señalar cualquier dirección (de una esfera), representando infinitos estados posibles hasta que se mida.

Matemáticamente, un cúbit puede representarse como $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, donde α y β son amplitudes de probabilidad que determinan la probabilidad de obtener 0 o 1 al medir el cúbit. Consecuentemente, la superposición permite que una computadora cuántica realice cálculos en múltiples estados simultáneamente, proporcionando un potencial de aceleración exponencial en ciertos algoritmos.

[1] Archivo: Bloch Sphere.svg. (2023, 28 de noviembre). Wikimedia Commons. Obtenido el 13 de febrero de 2025 a las 13:51 https://commons.wikimedia.org/w/index.php?title=File:Bloch_Sphere.svg&oldid=825786851.

Recuadro 2. Superposición en el caso de la "moneda giratoria"

La superposición cuántica se puede explicar a través de una metáfora usando una moneda giratoria.

Supongamos que se hace girar rápidamente una moneda sobre una mesa. Mientras gira, la moneda parece estar en dos estados al mismo tiempo, cara y cruz, porque no se puede determinar cuál lado se mostrará hasta que la moneda deje de girar y se apoye uno de sus lados sobre la mesa. En ese instante, la moneda se "decide" y se detiene en un resultado específico.

En el mundo cuántico, esta metáfora representa la superposición: una partícula, como un cúbit en una computadora cuántica, puede existir en múltiples estados simultáneamente, como si estuviera "girando". Solo cuando se mide, el sistema colapsa y muestra un único estado, parecido a cuando la moneda deja de girar.

Esta capacidad de "estar en múltiples lugares o estados a la vez" es lo que permite que las computadoras cuánticas realicen ciertos cálculos mucho más rápido que las computadoras clásicas.

Entrelazamiento

El entrelazamiento es una propiedad fundamental de la mecánica cuántica donde dos o más cúbits están correlacionados de manera no clásica.

Cuando dos cúbits están entrelazados, el estado de uno depende instantáneamente del otro, sin importar la distancia que los separe. Esto significa que, si se mide el primer cúbit y se obtiene cierto valor, el segundo cúbit siempre colapsará a un valor determinado, según el diseño del experimento. Por ejemplo, si se tienen dos partículas entrelazadas, y el diseño del experimento hace que giren en sentidos opuestos en su entrelazamiento, si medimos una de ellas y vemos que está girando hacia arriba, sabremos que la otra estará girando hacia abajo.

Esto genera las siguientes consecuencias importantes:

- Los cúbits entrelazados comparten propiedades cuánticas, como la correlación de fase[2] y la polarización[3].
- Se describen mediante una única función de onda, y realizar una medición de uno afecta instantáneamente al otro.
- Es la base para tecnologías cuánticas avanzadas como la teletransportación cuántica, la criptografía y los circuitos cuánticos altamente eficientes.

[2] Se refiere a la relación coherente entre las fases cuánticas de los cúbits en un sistema entrelazado.
[3] Hace alusión a la orientación de propiedades físicas fundamentales (como el spin en partículas o el estado de polarización en fotones) que pueden usarse para codificar información.

Recuadro 3. Los "guantes del entrelazamiento"

Supongamos que se tiene un par de guantes, uno derecho y otro izquierdo, y se decide separarlos. Se pone un guante en una caja y lo enviamos a un amigo en la otra punta del mundo, mientras uno se queda con la otra caja.

Estos guantes tienen una propiedad especial: hasta que uno no abre su caja, no se sabe si se tiene el guante derecho o el izquierdo. Sin embargo, en el momento exacto en que uno abre su caja y ve su guante (por ejemplo, el derecho), automáticamente y de forma instantánea, el otro amigo sabrá que tiene el guante izquierdo, sin importar la distancia entre ambos.

En el mundo cuántico, este fenómeno es mucho más extraño, porque no es simplemente que el segundo objeto "descubre" su estado después de que el primero es observado. En realidad, ambos guantes (o cúbits) existen en una combinación de posibilidades simultáneamente hasta que uno es observado. Una vez que uno de los cúbits se mide, el otro cúbit adopta instantáneamente un valor correspondiente, como si existiera una conexión invisible y directa entre ambos.
Este "vínculo especial" es lo que hace del entrelazamiento cuántico una propiedad crucial en la computación cuántica y en la comunicación segura.

El Teorema del no-clonado, la teletransportación cuántica, y el internet cuántico

El teorema del no-clonado establece que no es posible copiar un estado cuántico desconocido de forma exacta.

Mientras que, en los sistemas clásicos, cualquier dato puede copiarse sin modificar su estado original, en los sistemas cuánticos, cualquier intento de copiar un cúbit desconocido alterará su estado debido a que es necesario medirlo antes de copiarlo, lo que hace imposible la duplicación exacta.

Esto es relevante dado que, por ejemplo, en la criptografía cuántica la imposibilidad de copiar estados cuánticos garantiza la seguridad en protocolos como BB84 para distribución de claves cuánticas (Bennett y Brassard, 2014)[4]. Además, la seguridad de la información en el contexto cuántico se basa en que cualquier intento de espionaje o interferencia colapsa el estado cuántico, alertando a los participantes de la comunicación y protegiendo de esta manera la privacidad de la información tratada.

Por otro lado, la teletransportación cuántica permite la transferencia del estado cuántico de una partícula a otra partícula diferente, sin que haya un desplazamiento físico de la partícula original. Para ello, primero se establece entrelazamiento entre dos partículas separadas. Luego se mide el estado de la partícula original junto con una de las partículas entrelazadas. Posteriormente, la información de la medición se transmite clásicamente a la ubicación de la segunda partícula. Por último, usando esta información, se aplica una transformación cuántica a la segunda partícula, haciendo que adopte el estado exacto de la partícula original. Es importante considerar que el estado cuántico original se destruye en el proceso, evitando la duplicación de información cuántica (en conformidad con el teorema del no-clonado). Además, el estado cuántico nunca existió físicamente entre las dos ubicaciones, sino que se reconstruyó en la nueva ubicación a partir de la información transmitida. Es relevante destacar que no se transporta materia, solo información cuántica.

[4] Se detalla sobre esto más adelante en el documento.

De manera práctica, esto ha sido logrado experimentalmente con fotones, iones atrapados, espines y cúbits superconductores. En 2012, investigadores de la Universidad de Viena y la Universidad de Waterloo lograron teletransportar el estado de un fotón a lo largo de 143 km entre dos de las Islas Canarias, utilizando estaciones terrestres y satélites (Ma et al., 2012). De manera más reciente, en 2020 investigadores chinos lograron teletransportar información cuántica desde la Tierra a un satélite en órbita a más de 1.200 km (Yin et al., 2020).

Su desarrollo es de suma importancia, dado que permitiría desplegar redes de comunicación cuántica seguras, así como implantar computación cuántica de manera distribuida, permitiendo la transferencia de estados cuánticos entre diferentes cúbits de una arquitectura computacional.

Esto último fue desarrollado por investigadores de la Universidad de Oxford recientemente, donde se logró, por primera vez, distribuir cálculos cuánticos entre dos módulos de iones atrapados interconectados fotónicamente, separados por dos metros (Main et al., 2025). Mediante entrelazamiento remoto, se teletransportó de manera determinista una puerta controlada-Z (CZ) y se ejecutó el algoritmo de búsqueda de Grover.

Asimismo, también permitiría desarrollar un internet cuántico, que no es más que una red de comunicación que -a diferencia del internet clásico- no solo transmite información binaria, es decir, bits, sino que permite la transmisión de estados cuánticos. Se basa en la distribución de entrelazamiento cuántico entre diferentes nodos de la red, permitiendo la transmisión segura de información mediante protocolos de criptografía cuántica y el uso de la teletransportación cuántica.

Interferencia cuántica

La interferencia cuántica es un fenómeno relacionado con la naturaleza dual de las partículas, las cuales pueden comportarse tanto como partículas clásicas como ondas. Este efecto se observa cuando diferentes caminos o estados cuánticos se superponen, produciendo un patrón de interferencia que refleja las probabilidades de diferentes resultados en un experimento.

Un ejemplo clásico es el experimento de la doble rendija, en el que partículas como electrones o fotones se envían hacia una pantalla con dos rendijas. Cuando no se observa cuál rendija atraviesa cada partícula, se forma un patrón de interferencia caracterizado por franjas alternadas de alta y baja intensidad, similar al patrón producido por ondas de luz. Este resultado indica que cada partícula, en términos cuánticos, existe en una superposición de haber atravesado ambas rendijas simultáneamente, generando interferencia entre las probabilidades asociadas a cada camino posible. Este fenómeno es una manifestación directa de la superposición de estados cuánticos y pone de relieve la diferencia fundamental entre la mecánica cuántica y la intuición clásica. En un sistema clásico, las partículas solo pueden tomar un camino específico, y no se produciría ningún patrón de interferencia. Sin embargo, a nivel cuántico, la interferencia se produce porque las amplitudes de probabilidad asociadas a diferentes caminos se combinan de forma constructiva o destructiva, dependiendo de sus fases relativas.

Como previamente se comentó, en los algoritmos cuánticos se utilizan estados superpuestos para explorar simultáneamente múltiples soluciones de un problema. Aquí se está aprovechando, a su vez, la interferencia constructiva para amplificar las probabilidades de las respuestas correctas y la destructiva para cancelar las incorrectas. Esto es clave para lograr una aceleración exponencial en los cálculos cuánticos.

Recuadro 4. La interferencia de las olas en el estanque

Supongamos que se lanza una piedra al agua desde un lado de un estanque. Al hacerlo, se forman olas circulares que se expanden desde el punto donde cayó la piedra. Luego, se lanza otra piedra desde el otro lado del estanque. Ahora, dos conjuntos de olas se expanden y, en algún momento, se encuentran en el centro del estanque.

Cuando estas olas se cruzan, ocurre lo siguiente:
- En algunos puntos, las olas se refuerzan, es decir, las crestas de ambas olas se encuentran, creando olas más grandes.
- En otros puntos, las olas se cancelan, cuando una cresta se encuentra con un valle, haciendo que el agua quede en calma.

Este fenómeno es similar a lo que ocurre con las partículas cuánticas, como los electrones o los fotones, que pueden comportarse como ondas. Cuando estas partículas viajan por diferentes caminos, sus "ondas de probabilidad" se combinan. Dependiendo de cómo se alineen estas ondas, pueden reforzar o cancelar ciertas probabilidades. Esto es lo que se conoce como interferencia cuántica y es fundamental para el funcionamiento de algoritmos cuánticos.

Coherencia y decoherencia

La coherencia es la propiedad que permite que un sistema cuántico mantenga su superposición y entrelazamiento a lo largo del tiempo. Esta mide cuánto tiempo un cúbit puede permanecer en un estado cuántico sin ser perturbado por su entorno.

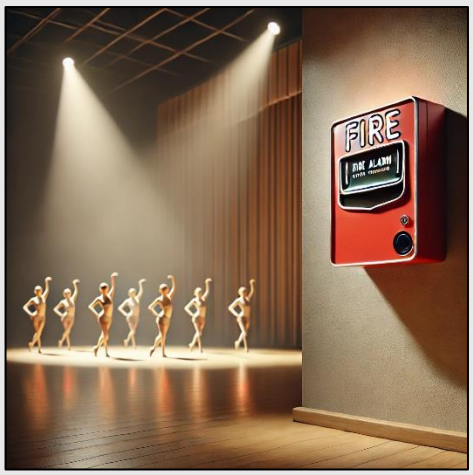
Es un factor de suma relevancia, ya que la computación cuántica requiere mantener la coherencia el tiempo suficiente para completar operaciones lógicas antes de que los cúbits pierdan su información cuántica. En la actualidad, se están investigando materiales y técnicas para prolongar la coherencia, como el uso de cúbits superconductores, iones atrapados y cúbits topológicos.

Por otro lado, la decoherencia es el proceso por el cual un sistema cuántico pierde su estado cuántico debido a interacciones con el entorno, colapsando a un estado clásico definido ($|0\rangle$ o $|1\rangle$). Esto puede deberse, por ejemplo, a la interacción con fluctuaciones electromagnéticas y ruido térmico, o al acoplamiento con el entorno externo, lo que puede verse como perturbaciones en la Esfera de Bloch.

Recuadro 5. La sincronización de un cuerpo de baile como ejemplo de coherencia

La coherencia y la decoherencia cuántica se pueden entender usando la metáfora de un grupo sincronizado de bailarines.

Supongamos que estamos viendo un grupo de bailarines sobre un escenario, todos perfectamente sincronizados. Cada uno de ellos representa un cúbit en un sistema cuántico, y sus movimientos están en perfecta armonía, creando una bella coreografía. Esta sincronización es la coherencia cuántica: todos los cúbits mantienen una relación precisa entre sus estados, lo que permite realizar cálculos y operaciones complejas.



Ahora, supongamos que, de repente, comienza a sonar una alarma de incendio en el teatro. Los bailarines se ven perturbados por este elemento externo, y poco a poco, pierden la coordinación. Algunos se equivocan de paso o comienzan a moverse en direcciones diferentes. Esta pérdida de sincronización es la decoherencia cuántica, donde los cúbits, al interactuar con su entorno, pierden la conexión que les permite funcionar como un sistema cuántico cohesivo. Incluso puede que terminen la coreografía de manera abrupta, en una situación que no era la final esperada (lo que en el mundo cuántico sería colapsar a un estado no final).

En resumen, la coherencia es el estado ideal en el que un sistema cuántico puede mantener sus propiedades cuánticas, mientras que la decoherencia es la interrupción de ese estado debido a ruidos o interferencias externas.

Medición en mecánica cuántica y colapso de la función de onda

La medición cuántica es el proceso de observar un estado cuántico, lo que inevitablemente altera dicho estado. Antes de la medición, un sistema cuántico puede existir en una superposición de múltiples estados posibles, pero al medirlo, el sistema colapsa a un único resultado definido, representado como un bit clásico (0 o 1 en el caso de un cúbit).

El concepto de colapso de la función de onda es fundamental en la mecánica cuántica. La función de onda describe matemáticamente el estado de un sistema cuántico y codifica la información sobre las probabilidades de distintos resultados posibles. Gracias a su naturaleza ondulatoria, esta función permite explicar fenómenos cuánticos como la interferencia y la difracción.

La función de onda $\psi(x,t)$ describe la probabilidad de encontrar una partícula en una posición y con un momento determinado. Su cuadrado, $|\psi(x,t)|^2$, representa la densidad de probabilidad de encontrar la partícula en una determinada posición en el espacio.

Al momento de realizar una medición, el sistema transita instantáneamente desde su superposición cuántica a un estado definido, destruyendo la información sobre los otros posibles resultados.

Matemáticamente, si un cúbit está en la superposición $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$,

tras la medición, colapsará a $|0\rangle$ o $|1\rangle$ con probabilidades $|\alpha^2|$ y $|\beta^2|$, respectivamente.

Una confusión común en la computación cuántica es asumir que, dado que la medición introduce elementos probabilísticos, toda la computación cuántica es inherentemente aleatoria. Sin embargo, esto no es cierto. Hasta el momento de la medición, el sistema evoluciona de manera completamente determinista (siguiendo la ecuación de Schrödinger). Como se detalló previamente, los algoritmos

cuánticos pueden aprovechar interferencias constructivas y destructivas para amplificar los resultados correctos y cancelar los incorrectos, asegurando que las mediciones finales produzcan resultados útiles con alta probabilidad. Por ejemplo, en el algoritmo de Shor, utilizado para la factorización de números primos, el uso de la Transformada de Fourier Cuántica permite aumentar la probabilidad de obtener el resultado correcto, a pesar de la aleatoriedad inherente en la medición final.

Además, el tipo de medición que se realice afecta los resultados:

- En la mecánica clásica, cualquier medición de una propiedad siempre da el mismo resultado.
- En la mecánica cuántica, ciertas propiedades no pueden ser medidas simultáneamente con precisión absoluta, debido al Principio de Incertidumbre de Heisenberg[5].
- La medición de una propiedad puede influir en el resultado de otra, ya que las bases de medición pueden ser incompatibles.

Antes de la medición, la función de onda contiene todas las posibles configuraciones del sistema cuántico. Sin embargo, cuando se mide una propiedad, como la posición o el espín, la función de onda colapsa a un único valor, y las otras posibilidades dejan de existir en términos observables. Este fenómeno plantea preguntas fundamentales sobre la naturaleza de la realidad, y ha dado lugar a diversas interpretaciones de la mecánica cuántica, como la interpretación de Copenhague y la interpretación de los mundos múltiples.

[5] El Principio de Incertidumbre de Heisenberg dice que es imposible medir con precisión y simultáneamente dos propiedades complementarias de una partícula cuántica, como su posición y su momento lineal. Cuanto más exacta es la medición de una de estas propiedades, mayor es la incertidumbre en la medición de la otra. Esto no se debe a limitaciones tecnológicas, sino a la naturaleza fundamental del mundo cuántico, donde las partículas se describen como ondas de probabilidad.

Recuadro 6. La interpretación de Copenhague y la de los mundos múltiples

La interpretación de Copenhague es una de las explicaciones más conocidas y aceptadas acerca del significado de la mecánica cuántica, formulada principalmente por Niels Bohr y Werner Heisenberg en la década de 1920. Según esta interpretación, los sistemas cuánticos no tienen propiedades definidas hasta que son observados o medidos. Esto implica que las partículas, como electrones o fotones, se describen por una función de onda que contiene todas las posibles propiedades del sistema, como su posición o momento. Sin embargo, estas propiedades permanecen en un estado de superposición hasta que ocurre una medición, momento en el cual la función de onda "colapsa" y el sistema adopta un valor específico.

Tiene los siguientes principios fundamentales.

- Superposición cuántica: un sistema puede existir en múltiples estados posibles simultáneamente, descritos por una función de onda.

- Colapso de la función de onda: la función de onda colapsa en un estado único cuando se realiza una medición, lo que determina el resultado observado.

- Indeterminación: no es posible predecir con certeza el resultado de una medición, solo es posible calcular la probabilidad de los resultados posibles.

- Complementariedad: algunas propiedades, como la posición y el momento, no pueden ser medidas simultáneamente con precisión ilimitada (principio de incertidumbre de Heisenberg).

Por otro lado, la interpretación de los mundos múltiples (o interpretación de Everett) es una propuesta alternativa en la mecánica cuántica (considerada excesivamente especulativa por algunos sectores de la academia), formulada por el físico Hugh Everett III en 1957. Esta interpretación sugiere que cada vez que ocurre un evento cuántico, el universo se ramifica en múltiples universos paralelos, donde se materializan todos los posibles resultados del evento. A diferencia de la interpretación de Copenhague, no existe un colapso de la función de onda; en su lugar, la función de onda evoluciona de manera continua y determinista, y cada uno de sus posibles resultados corresponde a un universo distinto.

Esta tiene sus propios principios fundamentales.

- Existencia de múltiples universos: cada vez que se realiza una medición cuántica, el universo se divide en versiones paralelas, donde cada resultado posible ocurre en una de esas ramas.

- Función de onda universal: la función de onda describe no solo el sistema cuántico, sino el estado de todo el universo. Esta función nunca colapsa, sino que evoluciona de acuerdo con la ecuación de Schrödinger.

- Observadores en universos paralelos: un observador solo puede percibir una de las posibles ramas del universo, lo que explica por qué se observa un resultado específico en una medición.

Procesamiento de cúbits

Una Unidad de Procesamiento Cuántico (QPU) es el equivalente cuántico de una Unidad de Procesamiento Central (ampliamente conocida por su sigla, CPU) en la computación clásica. Contiene cúbits, circuitos cuánticos y el soporte necesario para realizar cálculos cuánticos. Las QPUs aprovechan los fenómenos cuánticos antes mencionados para realizar cálculos de manera más eficiente en ciertas tareas específicas.

Las QPUs suelen incluir:

- Cúbits físicos: los elementos físicos que representan los bits cuánticos, como los ya comentados iones atrapados, superconductores, o fotones.
- Circuitos de control y lectura: infraestructura que permite manipular y medir los estados cuánticos de los cúbits.
- Corrección de errores cuánticos: técnicas para mitigar los errores generados por el ruido y la decoherencia cuántica.

Circuitos cuánticos

Los circuitos cuánticos son una secuencia organizada de compuertas lógicas cuánticas aplicadas sobre uno o varios cúbits. Estos circuitos representan algoritmos cuánticos y, en la práctica, se ejecutan en una QPU. Cada circuito puede incluir múltiples operaciones cuánticas, que transforman el estado de los cúbits según principios de la mecánica cuántica. Por otro lado, una compuerta cuántica es la unidad básica de procesamiento en un circuito cuántico. Recibe uno o más cúbits de entrada, los procesa mediante una transformación unitaria y genera uno o más cúbits de salida. Estas transformaciones se representan geométricamente en la Esfera de Bloch (estos cambios pueden verse como rotaciones en distintos ejes {X, Y, Z}, que modifican la fase del cúbit). Las compuertas cuánticas pueden modificar la probabilidad de colapso de los cúbits a estados clásicos, 0 o 1, y pueden generar efectos como interferencia cuántica y entrelazamiento.

Algunos ejemplos de compuertas cuánticas son:

- Hadamard (H): coloca un cúbit en superposición entre los estados 0 y 1.
- Pauli-X (X): equivalente a un NOT clásico, invierte el estado de un cúbit.
- CNOT: una compuerta de dos cúbits que introduce entrelazamiento cuántico.

Velocidad de compuerta

La velocidad de compuerta es el tiempo que toma una operación cuántica en ejecutarse. Cada compuerta tiene un tiempo de ejecución característico, y la suma de todos estos tiempos dentro de un algoritmo cuántico debe ser menor que el tiempo de coherencia del cúbit para que el cálculo sea útil. En otras palabras, si el tiempo total de ejecución de un algoritmo cuántico supera el tiempo de coherencia, los resultados se degradarán debido a errores cuánticos.

Ruido en computación cuántica

Atado al concepto anteriormente mencionado de decoherencia, el ruido se refiere a cualquier interacción no deseada entre la QPU y su entorno, o cualquier imperfección dentro del propio sistema cuántico. Debido a la extrema sensibilidad de los cúbits, cualquier perturbación externa (como vibraciones, fluctuaciones electromagnéticas o variaciones térmicas) puede alterar su estado cuántico, causando decoherencia y reduciendo la fidelidad de los cálculos cuánticos. A medida que se añaden más cúbits en una QPU, el impacto del ruido crece, dificultando la estabilidad de los sistemas cuánticos.

Corrección de errores cuánticos

Para lograr tolerancia a fallos, se utilizan códigos de corrección de errores cuánticos, que permiten detectar y corregir errores sin colapsar el estado cuántico.

Algunas técnicas clave incluyen:

- Código de Shor: primer código de corrección de errores cuánticos, que usa 9 cúbits físicos para almacenar 1 cúbit lógico protegido contra ruido.
- Código de superficie: considerado uno de los métodos más prometedores, ya que usa múltiples cúbits físicos para representar un cúbit lógico con tolerancia a fallos y requiere tasas de error inferiores al 1%.
- Corrección de errores topológicos: técnicas avanzadas que permiten mitigar errores con estructuras de cúbits organizadas en topologías específicas.

El desafío radica en que la corrección de errores cuánticos requiere un número significativamente mayor de cúbits físicos por cada cúbit lógico. Por ejemplo, para obtener un cúbit lógico estable, podrían necesitarse entre 100 y 1000 cúbits físicos dependiendo de la tecnología utilizada.

Tipos de computadoras cuánticas según sus capacidades

Era NISQ (Noisy Intermediate-Scale Quantum)

La era NISQ (Computación Cuántica Intermedia y Ruidosa) representa la primera fase de la computación cuántica práctica, en la cual nos encontramos actualmente. Fue definida por Preskill (2018) y describe el estado actual del hardware cuántico.

Cuando se habla de era NISQ, se refiere a dispositivos de escala intermedia, es decir, computadoras cuánticas con entre decenas y cientos de cúbits, que no son lo suficientemente grandes ni estables como para implementar algoritmos cuánticos con corrección de errores completa. Además, tienen una presencia de ruido significativa, ya que los cúbits actuales tienen tiempos de coherencia limitados y las operaciones cuánticas aún sufren errores debido a la interferencia ambiental y fallos en la manipulación de los cúbits.

Aunque los dispositivos NISQ no pueden ejecutar algoritmos cuánticos de tolerancia a fallos, han logrado demostrar ventaja cuántica en problemas específicos (por ejemplo, en simulación de materiales y optimización).

La siguiente etapa de la computación cuántica llegará cuando se logre corrección de errores cuánticos a gran escala, permitiendo cálculos cuánticos tolerantes a fallos. Para ello, se requieren mejoras en tres áreas clave:

1. Más cúbits: aumentar la cantidad de cúbits en las QPUs.
2. Cúbits de mayor calidad: menor afectación ante ruido y mejorar la fidelidad de las operaciones.
3. Corrección de errores cuánticos: implementar códigos de corrección de errores eficientes sin comprometer la capacidad de cómputo.

Computadora cuántica escalable, tolerante a fallos y basada en compuertas universales

El concepto de una computadora cuántica escalable, tolerante a fallos y basada en compuertas universales representa el objetivo final del desarrollo de la computación cuántica al día de hoy. Este sistema ideal sería capaz de ejecutar cualquier algoritmo cuántico sin que los errores cuánticos afecten significativamente los resultados. Para lograrlo, la computación cuántica debe cumplir con tres características clave: estar basada en compuertas universales, tener tolerancia a fallos, y ser escalable.

En primer lugar, una computadora cuántica "basada en compuertas universales" significa que puede ejecutar cualquier cálculo cuántico posible mediante la combinación de un conjunto finito de operaciones básicas, conocidas como compuertas cuánticas, que, como se explicó previamente, se encuentran en la QPU. La capacidad de operar con compuertas universales es crucial para garantizar que la computadora pueda ejecutar cualquier algoritmo (a diferencia de los quantum annealers comentados a continuación), desde simulaciones de sistemas físicos hasta algoritmos de optimización y criptografía.

Asimismo, como ya fue detallado, las computadoras cuánticas están propensas a errores causados por factores como el ruido, la interferencia externa y la decoherencia, debido a la fragilidad de los estados cuánticos. Para superar este obstáculo, es necesario implementar corrección de errores cuánticos como los descritos anteriormente.

Finalmente, la escalabilidad implica que el sistema puede ser ampliado a un gran número de cúbits manteniendo la coherencia y la eficiencia operativa. Como previamente se comentó, los cúbits son altamente susceptibles a errores debido al ruido ambiental y la decoherencia cuántica, por lo tanto, una computadora cuántica escalable debe incorporar mecanismos que permitan añadir más cúbits sin que el sistema se vuelva inestable o ingobernable.

Quantum Annealers

Un quantum annealer es un tipo de computadora cuántica no universal, diseñada específicamente para resolver problemas de optimización combinatoria mediante un proceso llamado recocido cuántico (quantum annealing). A diferencia de los procesadores cuánticos basados en compuertas lógicas que se describieron previamente, los quantum annealers no pueden ejecutar cualquier algoritmo cuántico; en cambio, están optimizados para encontrar la solución óptima en problemas donde hay muchas posibles configuraciones y se busca la mejor opción. Este proceso de quantum annealing busca encontrar la configuración de menor energía en un sistema.

A modo de ejemplo, cualquier problema de optimización puede representarse como un sistema físico donde cada solución posible corresponde a un estado energético. El objetivo del quantum annealer es encontrar el estado de menor energía, que representa la solución óptima al problema. Por ejemplo, puede ser usado para la optimización financiera en la asignación óptima de portafolios de inversión considerando múltiples variables y restricciones de riesgo, o en el modelado de estrategias de negociación y optimización de carteras en mercados volátiles.

A pesar de su potencial, los quantum annealers tienen limitaciones en comparación con las computadoras cuánticas universales, ya que no pueden ejecutar cualquier algoritmo cuántico, dependen de formulaciones específicas del problema ya que deben representarse en términos de estados energéticos, y, para la inversión que representan, a día de hoy brindan una limitada ventaja cuántica dado que los algoritmos clásicos de optimización procesados en supercomputadoras aún pueden competir con el rendimiento de los quantum annealers.

Supremacía cuántica[6]

La supremacía cuántica es un hito en la computación cuántica que se refiere al punto en el que una computadora cuántica puede realizar un cálculo que sería inviable para una supercomputadora clásica en un tiempo razonable. A lo largo de las últimas décadas, este concepto ha evolucionado desde una idea teórica hasta demostraciones experimentales realizadas por distintas instituciones y empresas tecnológicas.

[6] También conocida como “ventaja cuántica”, para evitar utilizar el término “supremacía” por sus posibles connotaciones (Preskill, 2019).

El concepto de supremacía cuántica fue introducido también por Preskill (2012). Se definió como el umbral en el que las computadoras cuánticas superan a los sistemas clásicos en ciertas tareas computacionales específicas. En el momento en que se acuñó esta definición, las computadoras cuánticas aún no contaban con suficientes cúbits coherentes ni con tiempos de coherencia suficientemente largos para superar a las computadoras clásicas. Sin embargo, los avances en la fabricación de cúbits, las mejoras en la corrección de errores y el desarrollo de algoritmos cuánticos comenzaron a acelerar la llegada de este hito que algunas empresas o laboratorios dicen haber batido.

Algunos hitos centrales en la evolución de la supremacía cuántica

2000 - 2009

- Primeras computadoras cuánticas son diseñadas e implementadas.
- Cuentan con a lo sumo cinco cúbits.
- Se implementan de manera experimental los primeros algoritmos cuánticos en estas infraestructuras incipientes.
- Aparecen también los primeros quantum annealers.

2010 - 2014

- Se sientan las bases para el "boson sampling", modelo cuántico basado en fotones que marca un antes y un después en el potencial de procesamiento de las computadoras cuánticas.
- Empresas como D-Wave Systems comienzan a comercializar computadoras cuánticas.
- El físico teórico John Preskill acuña el término de "supremacía cuántica" en 2012.

2015 - 2019

- Compañías como Google e IBM anuncian programas de hardware cuántico, con planes para alcanzar la supremacía cuántica.
- Se simulan más de 50 cúbits en supercomputadoras cuánticas.
- Pese a dudas planteadas por otras empresas, Google anuncia que alcanzó la supremacía cuántica en 2019, con su procesador Sycamore de 53 cúbits.

2020 - 2024

- Equipo chino con su procesador Jiuzhang basado en fotones anuncia que alcanza la supremacía cuántica en 2020.
- El mismo equipo, en 2021, presenta Zuchongzhi, procesador cuántico superconductivo de 66 cúbits, postulando que superaba a Sycamore.
- Xanadu informa en 2022 haber desarrollado procesador cuántico con fotones, con aceleraciones 50 millones de veces superior a experimentos anteriores.
- En 2024, D-Wave Systems reporta que su quantum annealer supera a métodos clásicos para resolver un problema en particular, alcanzando la supremacía cuántica en ello.

Criterio de DiVincenzo

El criterio de DiVincenzo establece las condiciones necesarias para construir una computadora cuántica universal. Fue propuesto por DiVincenzo (2000), definiendo los siguientes cinco requisitos fundamentales para la implementación de la computación cuántica:

1) *Sistema físico escalable y bien definido de cúbits*

La tecnología cuántica debe poder manejar múltiples cúbits sin que las interacciones entre ellos se vuelvan caóticas o incontrolables. Cada cúbit debe estar claramente definido, con estados cuánticos distinguibles. Además, es fundamental que el sistema pueda expandirse a cientos o miles de cúbits sin que se degraden las propiedades cuánticas, algo que implica mejoras tanto en hardware como en técnicas de control.

2) *Capacidad de inicializar el sistema en un estado bien definido*

Antes de realizar cualquier cálculo, los cúbits deben poder ser preparados en un estado base conocido, generalmente el estado $|0\rangle$. Esto garantiza que las operaciones posteriores partan de un estado controlado y eviten errores acumulativos. La inicialización debe ser rápida y reproducible, permitiendo múltiples ejecuciones del mismo cálculo. Por ejemplo, en circuitos superconductores, esto se logra enfriando los cúbits a temperaturas cercanas al cero absoluto.

3) *Tiempo de coherencia suficientemente largo*

Los cúbits deben mantenerse en un estado cuántico coherente el tiempo suficiente para completar las operaciones necesarias, es decir, el tiempo de coherencia debe ser significativamente mayor que el tiempo de ejecución de las puertas lógicas. Como se detalló, la decoherencia es el proceso mediante el cual los cúbits pierden sus propiedades cuánticas debido a la interacción con el entorno. Minimizar esta interacción requiere entornos altamente controlados, como cámaras de vacío, enfriamiento criogénico y aislamiento de ruidos electromagnéticos.

4) *Conjunto universal de puertas cuánticas*

Para que un sistema cuántico sea capaz de realizar cualquier operación, debe implementarse un conjunto de puertas lógicas universales. Estas incluyen puertas de un cúbit, como la puerta Hadamard (H), la puerta X (NOT cuántico) y la puerta Z, así como puertas de dos cúbits, como la puerta CNOT. La combinación de estas puertas permite ejecutar cualquier algoritmo cuántico. Es crucial que estas puertas tengan alta fidelidad para evitar errores durante el cálculo.

5) *Capacidad de medir los cúbits de forma fiable*

Al final del proceso, es necesario medir los estados cuánticos de los cúbits. La medición debe ser precisa y reproducible, lo que implica una probabilidad muy alta de obtener el resultado correcto. Además, en sistemas cuánticos, la medición colapsa el estado cuántico, por lo que debe realizarse en el momento adecuado para no interrumpir el cálculo. En superconductores, la medición se realiza con resonadores acoplados a cada cúbit, detectando el estado $|0\rangle|$ o $|1\rangle$.

Criterios adicionales para la comunicación cuántica

Además de los cinco criterios anteriores, DiVincenzo (2000) propuso dos requisitos adicionales para la comunicación cuántica:

6) Conversión de cúbits entre almacenamiento y transmisión

En una red cuántica, los diferentes nodos de procesamiento cuántico deben poder compartir estados cuánticos, especialmente mediante el entrelazamiento. Esto permite operaciones no locales, donde cúbits en diferentes ubicaciones colaboran en un mismo cálculo. Esta capacidad es fundamental para la comunicación cuántica segura, como la distribución de claves cuánticas. Esto se logra, por ejemplo, con el uso de fotones como mediadores de información entre sistemas de iones atrapados.

7) Intercambio de cúbits entre diferentes ubicaciones

Los cúbits locales (como los de estado sólido o iones atrapados) deben ser convertidos en cúbits voladores, típicamente fotones. Los fotones son ideales para la transmisión de información cuántica porque pueden viajar grandes distancias sin interactuar demasiado con el entorno. Sin embargo, es crucial que esta conversión mantenga la coherencia y el entrelazamiento del estado cuántico. Una vez que los cúbits voladores llegan a su destino, deben ser detectados de manera eficiente para recuperar la información cuántica. Los detectores de fotones únicos, por ejemplo, deben ser altamente sensibles y rápidos, con tasas de error muy bajas. Esto es esencial para mantener la fidelidad en la transmisión de estados cuánticos. Esto viene siendo estudiado, por ejemplo, en los experimentos de teletransportación cuántica en China con satélites cuánticos como Micius (Lu et al., 2022).

Computación cuántica y ciberseguridad: amenazas y oportunidades

Riesgos para la criptografía clásica

La robustez de los algoritmos criptográficos actuales radica en que la computación clásica no tiene el suficiente poder de procesamiento requerido para quebrarlos. El potencial poder de procesamiento de las computadoras cuánticas y la consecuente reducción en el orden de complejidad para hallar soluciones a problemas matemáticos, hacen que esta robustez criptográfica sea perdida.

En este apartado, se describen dos algoritmos cuánticos ampliamente conocidos, que son capaces de quebrar la criptografía asimétrica y reducir la fortaleza de la criptografía simétrica.

Adicionalmente, se presenta una ecuación fundamental para la criptografía post-cuántica, conocida como Teorema de Mosca.

Algoritmo de Shor

El algoritmo de Shor, desarrollado por Peter Shor (1994), es uno de los avances más significativos en la computación cuántica, ya que proporciona una forma eficiente de factorizar números enteros grandes y resolver el problema del logaritmo discreto. Estos problemas matemáticos son la base de la seguridad en la mayoría de los esquemas de criptografía asimétrica utilizados actualmente, como RSA (Rivest-Shamir-Adleman), DSA (Digital Signature Algorithm), y ECC (Elliptic Curve Cryptography).

Si bien la computación clásica requiere tiempo exponencial para resolver estos problemas en números suficientemente grandes, el algoritmo de Shor permite una solución polinómica en una computadora cuántica potente, lo que compromete por completo la seguridad de estos esquemas criptográficos.

La mejor estrategia actual usa algoritmos como la Criba General del Cuerpo de Números (GNFS, General Number Field Sieve), que tiene una complejidad de $\exp(O\left((\log N)^{1/3}(\log\log N)^{2/3}\right))$. Esto significa que, para números extremadamente grandes, el tiempo requerido para factorizarlos crece de

manera exponencial, lo que hace que, a modo de ejemplo, la seguridad de RSA sea viable con tamaños de clave suficientemente grandes (como es el caso de largos de 2048 o 4096 bits).

El algoritmo de Shor cuenta de dos etapas, primero se hace una reducción del problema a la búsqueda del período, utilizando un valor entre 1 y el valor a factorizar N; y luego, en el segundo paso, se hace uso de la Transformada de Fourier Cuántica explotando las propiedades de superposición. Este algoritmo reduce la complejidad del problema a $O((\log N)^3)$, lo que implica que la factorización se vuelve polinómica y, por lo tanto, factible en tiempos razonables si se dispone de una computadora cuántica con suficientes cúbits. Como consecuencia, por ejemplo, cualquier número utilizado en RSA puede ser factorizado rápidamente en una computadora cuántica sin importar el tamaño.

La siguiente tabla ilustra sobre aproximados en tiempos de factorización:

Bits de RSA	**GNFS (Estimación en Computación Clásica)**	**Shor (Computación Cuántica con suficientes cúbits)**
512 bits	Horas o días (con supercomputadora)	Segundos
1024 bits	Meses o años	Minutos
2048 bits	Siglos	Horas
4096 bits	Prácticamente imposible	Días

El algoritmo de Shor rompe, por ejemplo, los siguientes esquemas criptográficos asimétricos:

Nombre del algoritmo	**Algoritmo matemático**	**Uso principal**	**Observaciones**
RSA	Factorización de enteros	Cifrado y firma digital	Uno de los algoritmos más utilizados en la actualidad
Rabin	Factorización de enteros	Cifrado	Similar a RSA, pero con menos adopción práctica
DSA	Logaritmo discreto	Firma digital	Definido como parte del estándar DSS
DSS	Logaritmo discreto	Firma digital	Estándar que incluye DSA, RSA y ECDSA
Diffie-Hellman	Logaritmo discreto	Intercambio de claves	Protocolo clásico para el establecimiento de claves seguras
ElGamal	Logaritmo discreto	Cifrado y firma digital	Base para varios sistemas de firma digital
Schnorr	Logaritmo discreto	Firma digital	Precursor de otros algoritmos como EdDSA
X.509	Logaritmo discreto	Certificados de clave pública	Utilizado en la infraestructura de claves públicas (PKI)
ECDSA	Logaritmo discreto en curvas elípticas	Firma digital	Más eficiente que DSA con claves más cortas
ECDH	Logaritmo discreto en curvas elípticas	Intercambio de claves	Utilizado en protocolos como TLS para asegurar la comunicación
ECIES	Logaritmo discreto en curvas elípticas	Cifrado integrado	Proporciona cifrado y autenticidad simultáneamente
EdDSA	Logaritmo discreto en curvas elípticas	Firma digital	Más eficiente y seguro frente a fallas en la implementación

De todos modos, el algoritmo de Shor ha sido solamente probado en pequeños números en laboratorios con computadoras cuánticas, por ejemplo, factorizando 15, 21 y 35 (Amico et al., 2019). Asimismo, existe cierto recelo sobre la validez de estos experimentos, dado que partían de conocer los factores de antemano, algo que en realidad no sucede (Smolin et al., 2018). Todavía no existe una

computadora cuántica con la capacidad de romper criptografía real debido a la gran cantidad de cúbits requeridos. Se estima que se requieren al menos 6000 cúbits lógicos estables para factorizar claves RSA de 2048 bits (representando un número de 617 cifras) de manera efectiva, requiriéndose, asimismo, millones de cúbits físicos para lograr un sistema escalable y con corrección de errores (Gidney y Ekerå, 2021).

Por otro lado, pese a que se ha logrado factorizar números de cinco (Dattani y Bryans, 2014), seis (Li et al., 2017) y hasta siete cifras (Dash et al., 2018) usando otros mecanismos, estos fueron casos particulares, sin capacidad de generalización, y sin riesgo real para la criptografía clásica. De igual manera ocurrió cuando se planteó que con 372 cúbits físicos se podría romper RSA de 2048 bits (Yan et al., 2022).

Algoritmo de Grover

El algoritmo de Grover (1996) es un algoritmo cuántico diseñado para acelerar la búsqueda en bases de datos no estructuradas y resolver problemas de búsqueda en general. Su importancia en el ámbito de la criptografía radica en que reduce drásticamente el tiempo requerido para ataques de fuerza bruta contra algoritmos de cifrado simétrico y funciones hash.

Los algoritmos de cifrado simétrico, como AES (Advanced Encryption Standard), se basan en la premisa de que probar todas las claves posibles es inviable debido a su alto costo computacional. Mientras que en una computadora clásica un ataque de fuerza bruta contra un cifrado de n bits tiene una complejidad de $O(2^n)$, ya que hay 2^n claves posibles, en una computadora cuántica con el algoritmo de Grover la complejidad se reduce a $O(2^{n/2})$. Esto significa que el nivel de seguridad efectivo de una clave de tamaño n se reduce a la mitad en términos de resistencia a ataques de fuerza bruta, por lo que una clave de 128 bits dejaría de ser mínimamente segura al representar la misma fortaleza que una clave de 64 bits en la actualidad. Otros tamaños de clave mayores, si bien continuarían brindando garantías de seguridad, podrían dejar de ser óptimos a largo plazo.

Los tiempos aproximados para quebrar AES según el largo de las claves se detallan en la siguiente tabla:

Tamaño de clave	Tiempo con computadoras clásicas	Tiempo con computadoras cuánticas (Grover)	Seguridad
AES-40	Minutos	Segundos	Inseguro
AES-56 (DES)	Horas a días	Minutos	Inseguro
AES-64	Días a semanas	Horas	Inseguro
AES-80	Meses a años	Días	Inseguro
AES-128	$\sim 10^{18}$ años	$\sim$6 meses	Mínimamente seguro
AES-192	$\sim 10^{37}$ años	$\sim 10^{6}$ años	Seguro
AES-256	$\sim 10^{54}$ años	$\sim 10^{18}$ años	Muy seguro

Por otro lado, a continuación, se presenta un resumen de algoritmos simétricos afectados por este algoritmo:

Nombre del algoritmo	Algoritmo matemático	Uso principal	Observaciones
AES	Combinación de operaciones algebraicas (cajas S, permutaciones, XOR)	Cifrado	Una clave de 256 bits ofrece una seguridad equivalente a 128 bits
Triple DES	Feistel, permutaciones y sustituciones	Cifrado	Ya considerado obsoleto por sus vulnerabilidades conocidas
SHA-256	Funciones hash (compresión y expansión)	Integridad y firma digital	Sigue siendo resistente, pero puede requerir funciones hash de mayor tamaño en el futuro
HMAC	Basado en funciones hash (SHA, MD5)	Autenticación de mensajes	Depende de la función hash subyacente, como SHA-256
Blowfish	Redes de Feistel, operaciones XOR, cajas S	Cifrado	Clave máxima de 448 bits, aunque suele usarse con claves más cortas
Twofish	Redes de Feistel, matrices de dispersión	Cifrado	Diseño basado en mejorar aspectos de Blowfish
ChaCha20	Cifrado de flujo (operaciones XOR, rotaciones)	Cifrado	Alta eficiencia en sistemas de hardware limitado

En líneas generales, el algoritmo de Grover puede entenderse en cuatro pasos, que van desde crear una superposición cuántica y diseño de una función de oráculo para distinguir claves correctas, hasta la aplicación de un operador cuántico para lograr una amplificación de amplitud con el fin de reforzar la probabilidad de la clave correcta al momento del paso final de medición del sistema.

El mismo ya ha sido implementado en varias ocasiones, por ejemplo, con 3 cúbits (Figgatt et al., 2017), con la misma cantidad de cúbits usando la infraestructura de IBM (AbuGhanem, 2024), en esta infraestructura pero con 4 cúbits (Mandviwalla et al., 2018), usando 4 cúbits pero con otra tecnología (Mehta, 2024), utilizando 5-6 cúbits(Vemula, 2022), en esquemas más complejos como en la encriptación homomórfica (Fernández y Martín-Delgado, 2024), y para buscar en bases de datos estructuradas o no (Sun y Wu, 2024).

Teorema de Mosca y "Harvest Now, Decrypt Later"

El Teorema de Mosca, propuesto por Michele Mosca (2015), es un marco conceptual que describe la urgencia de migrar a la criptografía post-cuántica debido al avance de la computación cuántica. Se centra en el tiempo necesario para que ésta sea capaz de romper la criptografía actual y el tiempo requerido para reemplazar y actualizar los sistemas criptográficos. Este teorema plantea una triple desigualdad temporal, que evalúa la seguridad de la información en función de tres variables clave: $X + Y > Z$, donde:

- X: Tiempo que la información cifrada debe permanecer segura. Ejemplo: datos gubernamentales, registros financieros o secretos industriales que deben mantenerse seguros durante 10, 20 o incluso 50 años.
- Y: Tiempo necesario para migrar los sistemas criptográficos a soluciones resistentes a la computación cuántica. En grandes organizaciones y gobiernos, este proceso puede tomar entre 5 y 10 años (o más inclusive).
- Z: Tiempo estimado hasta que una computadora cuántica suficientemente poderosa pueda romper la criptografía actual (RSA, ECC, AES-128, y otros detallados precedentemente).

Si la suma del tiempo que los datos deben mantenerse seguros (X) y el tiempo requerido para la migración (Y) es mayor que el tiempo estimado para que las computadoras cuánticas rompan los sistemas criptográficos (Z), entonces existe un riesgo de exposición de datos sensibles antes de que los sistemas puedan ser protegidos.

Este teorema advierte sobre dos amenazas principales relacionadas con la computación cuántica: el fenómeno conocido como "Harvest Now, Decrypt Later" y el largo tiempo que toma migrar sistemas informáticos, sobre todo en organizaciones grandes o del sector público.

Harvest Now, Decrypt Later

Este concepto, que en español se traduce como “Almacenar Ahora, Descifrar Después”, se basa en que actores malintencionados podrían estar recopilando y almacenando un gran volumen de datos cifrados con algoritmos vulnerables como los previamente comentados. El fin de esto es que, cuando una computadora cuántica suficientemente potente esté disponible, estos actores podrán descifrar rápidamente estos datos recolectados y acceder a información confidencial.

A continuación, se brindan más detalles del proceso.

1. **Recolección de datos cifrados:**
    a. Los atacantes capturan grandes volúmenes de información cifrada en tráfico de red, bases de datos, archivos almacenados y comunicaciones seguras.
    b. Fuentes comunes incluyen VPNs, correos electrónicos, chats cifrados, documentos legales y financieros, información militar, transacciones bancarias, accesos a bases de datos cifradas (por ejemplo, conteniendo contraseñas), etc.
    c. La recolección se realiza de manera masiva, sin que la víctima lo sepa.
2. **Almacenamiento a largo plazo:**
    a. La información recolectada se guarda en bases de datos hasta que la tecnología cuántica avance lo suficiente.
    b. Los atacantes no necesitan entender los datos en el momento de la recolección; simplemente los almacenan con la expectativa de que serán útiles en el futuro.
3. **Descifrado con computación cuántica:**
    a. Una vez que una computadora cuántica con capacidad suficiente esté disponible, los atacantes usarán algoritmos como el de Shor para romper la criptografía utilizada, extrayendo información previamente recolectada.
    b. Esto permitirá descifrar información confidencial y clasificada, comprometiendo la seguridad de datos antiguos pero que aún sean relevantes.

Recuadro 7. Ejemplo práctico del Teorema de Mosca: banco comercial

Un banco comercial utiliza actualmente algoritmos RSA para proteger sus transacciones internacionales. Hoy, la infraestructura no cuenta con soporte para criptografía post-cuántica. Según estimaciones, podría tomarles 5 años (Y) implantar nuevas tecnologías (sistemas, bases de datos, dispositivos de red, etc.) que utilicen criptografía post-cuántica.

Por otro lado, investigadores han estimado que computadoras cuánticas podrían estar disponibles con capacidad para romper RSA en 10 años (Z). Sin embargo, el banco planea utilizar sus datos y sistemas actuales durante los próximos 15 años (X).

Aquí se cumple $X + Y = 20$, mientras que $Z = 10$, lo que significa que:

$$\boldsymbol{X + Y = 20 > 10 = Z}$$

Conclusión:

El banco comercial corre el riesgo de que la información relacionada a sus transacciones internacionales sea descifrada en un futuro cercano, aun cuando esa información ya no esté en uso operativo.

Criptografía cuántica y otras oportunidades

Más allá de la criptografía resistente a la computación cuántica (que en la actualidad está basada en la complejidad matemática y se desarrolla para ser ejecutada en computadoras clásicas), esta tecnología emergente tiene la capacidad de brindar nuevas oportunidades para la innovación criptográfica a partir de la naturaleza misma de la física y la mecánica cuántica.

Sin embargo, cabe destacar que estas innovaciones cuánticas aún se encuentran en etapa de desarrollo en la mayoría de los casos, y que sus costos se mantienen muy elevados para su acceso a gran escala.

A continuación, se presentan algunos ejemplos de potenciales innovaciones.

Distribución cuántica de claves (QKD)

La distribución cuántica de claves es una tecnología basada en los principios de la mecánica cuántica que permite a dos partes generar y compartir una clave secreta utilizada para cifrar y descifrar información. Lo más importante de este método es que garantiza la seguridad absoluta de la clave, siempre y cuando se respeten ciertas condiciones físicas.

La seguridad de la distribución cuántica de claves se basa en dos principios fundamentales de la mecánica cuántica. En primer lugar, el principio de la no clonación establece que es imposible copiar o duplicar un estado cuántico desconocido sin alterar dicho estado. Esto impide que un espía pueda interceptar las claves sin dejar rastros de su presencia. Por otro lado, el principio de la medición dice que cuando se mide un estado cuántico, este se ve perturbado. Si se intenta interceptar los cúbits, causará alteraciones detectables, permitiendo identificar que la seguridad ha sido comprometida.

Existen diversos protocolos diseñados para la distribución cuántica de claves. Los más conocidos son BB84 y E91, creados en 1984 y 1991 respectivamente.

Adicionalmente, este esquema de distribución de claves puede extenderse a más de dos participantes, en lo que se conoce comúnmente en la literatura como “Conference Key Agreement”, y en términos más generales, a la criptografía cuántica multipartita.

Generación cuántica de números aleatorios (QRNG)

La Generación Cuántica de Números Aleatorios es un método que utiliza fenómenos cuánticos para generar secuencias de números aleatorios verdaderamente impredecibles. A diferencia de los generadores clásicos de números aleatorios, que dependen de algoritmos matemáticos y semilla inicial (y por lo tanto se consideran "pseudoaleatorios"), los QRNG se basan en propiedades físicas cuánticas que no pueden ser replicadas ni predichas con certeza, ya que surgen de fenómenos físicos no deterministas.

Por ejemplo, si un fotón en superposición es enviado a través de un divisor de haz, tiene un 50% de probabilidad de ser detectado en un camino u otro. Esta medición proporciona un bit aleatorio. Un camino puede representar el valor 0, y el otro puede representar el valor 1.

Firma digital cuántica

La firma digital cuántica combina los principios de la mecánica cuántica con las técnicas de criptografía para autenticar documentos y transacciones de manera segura.

A diferencia de las firmas digitales tradicionales (basadas en algoritmos como RSA o ECDSA), las firmas cuánticas son resistentes a los ataques de computadoras cuánticas.

Asimismo, la firma digital cuántica mantiene las tres propiedades fundamentales de las firmas digitales clásicas: autenticidad, integridad y no repudio.

Criptografía cuántica basada en protocolos de compromiso

La criptografía cuántica basada en protocolos de compromiso es un enfoque que utiliza principios de la mecánica cuántica para garantizar compromisos criptográficos seguros. Estos protocolos son fundamentales en escenarios donde dos partes desean garantizar que una de ellas se comprometa a un valor sin revelarlo de inmediato, manteniendo la integridad y confidencialidad del proceso hasta que se deba revelar dicho valor.

Los compromisos criptográficos clásicos, como los basados en funciones de hash o cifrado asimétrico, dependen de supuestos de seguridad matemática, como la dificultad de factorizar números grandes (RSA) o resolver problemas de logaritmos discretos (ECDSA), funciones que, como fue detallado, se volverían obsoletas una vez que sea accesible la computación cuántica. Para enfrentar esta amenaza, los protocolos de compromiso cuántico se basan en fenómenos físicos, lo que ofrece seguridad independiente de los avances en computación cuántica.

Comunicación directa segura cuántica (QSDC)

La comunicación directa segura cuántica es un método avanzado de comunicación que permite enviar mensajes de manera directa y segura, sin necesidad de compartir claves criptográficas separadas (lo cual suele ser un factor de riesgos en todo mecanismo criptográfico o comunicación cifrada de información).

A diferencia de los métodos convencionales, que dependen de la distribución de claves cuánticas, este método ofrece una solución en la que el mensaje completo se transmite a través de un canal cuántico, garantizando seguridad basada en los principios de la mecánica cuántica dado que ningún atacante puede interceptar mensajes sin ser detectado.

Desarrollo de la computación cuántica en los proveedores de servicios

Los procesadores cuánticos, abarcan una variedad de dispositivos desarrollados por diferentes proveedores, cada uno con arquitecturas y enfoques particulares.

Es importante destacar que la comparación entre estos procesadores es compleja debido a las diferencias en sus arquitecturas y enfoques. El número de cúbits físicos no siempre refleja el rendimiento real del procesador, el cual se evalúa mejor mediante métricas como el volumen cuántico, la fidelidad de las puertas lógicas y la tasa de operaciones por segundo.

A continuación, se destacan algunos de los proveedores y procesadores más relevantes:

Procesadores cuánticos basados en circuitos

Los procesadores cuánticos basados en circuitos son una de las principales arquitecturas para computación cuántica, donde los cálculos se realizan a través de circuitos cuánticos compuestos por una secuencia de puertas cuánticas aplicadas a un conjunto de cúbits. Estos procesadores son análogos a los procesadores clásicos basados en circuitos lógicos, pero utilizan principios de la mecánica cuántica para realizar operaciones que no son posibles en la computación tradicional.

Existen dos modos principales en los procesadores cuánticos basados en circuitos. Por un lado, el modo de circuito cerrado, donde el cálculo completo se ejecuta y luego se mide el resultado en un contexto cuántico. El otro modo es el de circuito híbrido, el cual combina cálculos cuánticos y clásicos, donde el procesador cuántico ejecuta subrutinas específicas y el procesador clásico controla el flujo del algoritmo. Este modelo se detalla más en la siguiente sección.

Las principales tecnologías utilizas incluyen cúbits superconductores, iones atrapados, fotones cuánticos, y cúbits topológicos.

Algunos proveedores y procesadores destacados son:

Proveedor	Procesador	Cúbits	Tecnología	Lanzamiento
IBM	Heron r2[7]	156	Superconductores	2024
Google	Willow[8]	105	Superconductores	2024
Rigetti	ANKAA-3[9]	82	Superconductores	2024
IonQ	Forte[10]	36	Trampas de iones	2023
Quantinuum	H2[11]	56	Trampas de iones	2023

Procesadores cuánticos basados en recocido cuántico (Quantum Annealing)

Los procesadores cuánticos basados en recocido cuántico representan una arquitectura cuántica diseñada específicamente para resolver problemas de optimización, búsqueda en grandes espacios de soluciones y ciertos tipos de simulaciones, como fue comentado en la primera sección de este

[7] Ver Gambetta y Mandelbaum (2024).
[8] Ver Neven (2024).
[9] https://qcs.rigetti.com/qpus
[10] https://ionq.com/quantum-systems/forte
[11] www.quantinuum.com/products-solutions/quantinuum-systems/system-model-h2

documento. Este tipo de procesador difiere en su enfoque respecto a los procesadores cuánticos universales, ya que no utiliza puertas lógicas cuánticas en la misma forma, sino que emplea la mecánica cuántica para encontrar el mínimo global en problemas complejos.

El recocido cuántico es una técnica inspirada en el proceso físico de "temple" o "recocido" térmico, que consiste en calentar un material y luego enfriarlo lentamente para eliminar defectos en su estructura. En el ámbito cuántico, el proceso utiliza fluctuaciones cuánticas, en lugar de variaciones de temperatura, para guiar un sistema hacia un estado fundamental (o de energía mínima).

Sin embargo, esta tecnología no sirve para procesadores cuánticos universales, ya que no permite ejecutar algoritmos cuánticos generales (como el de Shor o Grover).

Uno de los principales desarrolladores de procesadores de recocido cuántico es D-Wave Systems, que ha desarrollado varias generaciones de máquinas de recocido cuántico, como la serie D-Wave 2000Q y Advantage, con más de 5000 qubits[12].

Procesadores cuánticos analógicos

Los procesadores cuánticos analógicos representan una aproximación a la computación cuántica diferente a la de los procesadores digitales, los cuales se basan en la ejecución de puertas lógicas cuánticas secuenciales. Los procesadores cuánticos analógicos no implementan algoritmos generalizados, sino que emplean la evolución continua de un sistema cuántico para simular o resolver un problema físico o matemático específico, donde un sistema físico cuántico es configurado para imitar otro sistema cuya dinámica es demasiado compleja para ser modelada con métodos clásicos. Entre las técnicas analógicas más comunes se incluyen el recocido cuántico, el procesamiento adiabático y las simulaciones de modelos cuánticos específicos, como los modelos de Ising o Hubbard.

Un proveedor de estos es QuEra, con su procesador Aquila[13], basado en átomos neutros con 256 cúbits.

Otros proveedores de servicios relacionados a la computación cuántica

Más allá de los previamente nombrados, existen otros proveedores de estos servicios (muchos de los cuales se han asociado con los anteriores), entre los que se encuentran:

- **Amazon Braket:** Computación cuántica en la nube, a través de proveedores de hardware.
- **Annealing Cloud Web:** Quantum Annealer en la nube.
- **Atos:** Varios servicios a través de su compañía Eviden.
- **Azure Quantum:** Computación cuántica en la nube, a través de proveedores de hardware.
- **AQT:** Servidores cuánticos comerciales de 20 cúbits para centros de procesamiento datos privados, y también acceso a recursos en la nube.
- **ColdQuanta:** Proveedor de computadoras cuánticas para laboratorios y otros centros nacionales.
- **IQM Quantum Computers**: Proveedor de computadoras cuánticas para laboratorios y otros centros nacionales, que también ofrece acceso en la nube.
- **Xanadu:** Computación cuántica en la nube y librería de software PennyLane.

[12] www.dwavesys.com/solutions-and-products/systems
[13] www.quera.com/aquila

Finalmente, son muchos los laboratorios, centros nacionales, universidades, entre otros, que se encuentran realizando investigación de punta en la temática, construyendo sus propios prototipos y contribuyendo al desarrollo de la tecnología cuántica.

Procesamiento cuántico en instalaciones propias

Si bien es válido plantear la alternativa de si conviene utilizar proveedores en la nube o tener servidores propios en instalaciones propias para el procesamiento de la computación clásica, al referirse al procesamiento cuántico la pregunta carece de sentido, a menos que sea necesario un extraordinario poder de cómputo o si se cuenta con un presupuesto limitado.

Tener infraestructura propia tiene ventajas como el control total del hardware y software a utilizar, administración total de la seguridad y privacidad, disminución de latencias en el acceso al hardware, y la no dependencia de terceras partes. Sin embargo, los costos que conlleva diseñar, procurar, implementar y mantener una infraestructura de computación cuántica son prácticamente inviables para la mayoría de las organizaciones. Además, es una tecnología que se encuentra en franca evolución, por lo que la escalabilidad, estandarización entre componentes y obsolescencia actual de la tecnología usada representarían obstáculos importantes.

De todas maneras, están apareciendo proveedores de servidores cuánticos comerciales, como el caso de AQT[14] mencionado previamente.

Modelos de procesamiento híbridos

La computación cuántica aún no es lo suficientemente avanzada para reemplazar la computación clásica en todos los ámbitos, pero los enfoques híbridos son una forma práctica y eficiente de maximizar sus capacidades.

En un modelo híbrido, que han sido propuestos ya desde principios de siglo (Lloyd, 2003), las tareas de un problema se dividen entre:

- **Procesadores clásicos:** encargados de realizar cálculos estándar, gestionar la lógica general del programa y coordinar las operaciones.
- **Procesadores cuánticos:** encargados de resolver partes específicas del problema donde la computación cuántica tiene ventaja.

Este trabajo en conjunto entre las dos tecnologías brinda algunas de ventajas al aprovechar lo mejor de ambos mundos, por ejemplo, permite integrar el poder de procesamiento de la computación cuántica con sistemas tradicionales sin necesidad de sustituir por completo las infraestructuras actuales. También se mitigan las limitaciones actuales de la computación cuántica, como la decoherencia y los errores de cúbits, ya que los modelos clásicos ayudan a detectar y corregir errores.

Se destacan algunos proyectos de la industria como el de Terra Quantum y Thales Group, que utilizaron esta modalidad de trabajo para hacer más eficiente la operativa de los satélites, en particular en lo referido al planeamiento de misiones para su administración (Rainjonneau, 2023), los desarrollos híbridos involucrando supercomputadoras de IBM (Mandelbaum y Sitdikov, 2024), así como trabajos de investigación académica en farmacéutica(Li et al., 2024), ciencia de materiales (Nie

[14] www.aqt.eu/products/marmot

et al. 2024), y en la resolución de problemas NP-completos, como el algoritmo de Grover (Sinitsyn y Yan, 2023).

Por otro lado, algunos proveedores de modelos híbridos comerciales son Microsoft Azure[15] y Amazon Braket (Natu et al., 2024).

Comentarios finales

La computación cuántica combina los principios de la informática y la física cuántica para desarrollar una nueva generación de computadoras capaces de resolver problemas que exceden las capacidades de los sistemas clásicos. A diferencia de las computadoras tradicionales, que operan con bits clásicos, las computadoras cuánticas utilizan cúbits, la unidad fundamental de información cuántica. Los cúbits poseen propiedades únicas, como la superposición, el entrelazamiento y la interferencia cuántica, que permiten procesar información de manera exponencialmente más eficiente.

La seguridad de los algoritmos criptográficos actuales se basa en la incapacidad de la computación clásica para resolver ciertos problemas matemáticos en tiempos razonables. Sin embargo, el poder de procesamiento de las computadoras cuánticas, junto con su capacidad para reducir drásticamente la complejidad de estos cálculos, compromete esta seguridad.

El algoritmo de Shor representa uno de los avances más significativos en computación cuántica, ya que permite factorizar números enteros grandes y resolver el problema del logaritmo discreto en tiempo polinómico. Estas funciones son la base de la seguridad en la mayoría de los sistemas de criptografía asimétrica, como RSA, DSA y ECC, utilizados en cifrado, firma digital, intercambio de claves y certificados digitales. Una computadora cuántica suficientemente potente podría quebrar estos esquemas, poniendo en riesgo su confiabilidad.

Por otro lado, el algoritmo de Grover está diseñado para optimizar la búsqueda en bases de datos no estructuradas y acelerar el tiempo necesario para ataques de fuerza bruta contra cifrados simétricos y funciones hash. Esto afecta la seguridad de algoritmos ampliamente utilizados, como AES para cifrado y SHA-256 para firma digital e integridad de datos, los cuales deberán adaptarse para resistir ataques cuánticos.

En los últimos años, distintos proveedores han impulsado avances en procesadores cuánticos basados en circuitos, recocido cuántico (quantum annealing), procesamiento analógico y servicios en la nube. Dado que el alcance práctico de estas tecnologías sigue siendo limitado, también se están desarrollando modelos híbridos que combinan la computación clásica y cuántica para maximizar su eficiencia y aplicabilidad.

Tal como pudo verse, si bien la computación cuántica aún se encuentra en una fase temprana y no representa una amenaza inmediata, su avance es acelerado y su impacto potencial es significativo, por lo que anticiparse a los cambios que traerá esta tecnología es crucial. En este sentido, es fundamental que los distintos actores comiencen a prepararse mediante la adopción de estrategias de migración hacia criptografía post-cuántica, el fortalecimiento de los sistemas actuales y el impulso a la investigación en soluciones seguras. La transición será un desafío progresivo, pero una planificación temprana permitirá mitigar los riesgos y garantizar la continuidad y confianza en los sistemas del futuro.

[15] https://learn.microsoft.com/en-us/azure/quantum/hybrid-computing-integrated

Referencias

AbuGhanem, M. (2024). Comprehensive characterization of three-qubit Grover search algorithm on IBM's 127-qubit superconducting quantum computers. *Scientific Reports, 15*, 1281. https://doi.org/10.1038/s41598-024-80188-6

Amico, M., Saleem, Z. H., y Kumph, M. (2019). An experimental study of Shor's factoring algorithm on IBM Q. *Physical Review A, 100*(1), 012305. https://doi.org/10.1103/PhysRevA.100.012305

Bennett, C. H., y Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science, 560*(Part 1), 7-11. https://doi.org/10.1016/j.tcs.2014.05.025

Bolgar,C. (2025, 19 de febrero). Microsoft's Majorana 1 chip carves new path for quantum computing. *Microsoft News Center*. https://news.microsoft.com/source/features/innovation/microsofts-majorana-1-chip-carves-new-path-for-quantum-computing/

Clarke, J., Wilhelm, F. Superconducting quantum bits. Nature 453, 1031–1042 (2008). https://doi.org/10.1038/nature07128

Dash, A., Sarmah, D., Behera, B. K., y Panigrahi, P. K. (2018). Exact search algorithm to factorize large biprimes and a triprime on IBM quantum computer. *arXiv preprint* arXiv:1805.10478. https://arxiv.org/abs/1805.10478

Dattani, N. S., y Bryans, N. (2014). Quantum factorization of 56153 with only 4 qubits. *arXiv preprint* arXiv:1411.6758. https://arxiv.org/abs/1411.6758

DiVincenzo, D. P. (2000). *The Physical Implementation of Quantum Computation*. Fortschritte der Physik, 48(9-11), 771-783. https://doi.org/10.1002/1521-3978(200009)48:9/11<771::AID-PROP771>3.0.CO;2-E

Fernández, P., y Martin-Delgado, M. A. (2024). Implementing the Grover algorithm in homomorphic encryption schemes. *Physical Review Research, 6*(4), 043109. https://doi.org/10.1103/PhysRevResearch.6.043109

Figgatt, C., Maslov, D., Landsman, K.A. *et al.* Complete 3-Qubit Grover search on a programmable quantum computer. *Nat Commun* 8, 1918 (2017). https://doi.org/10.1038/s41467-017-01904-7

Gambetta, J., y Mandelbaum, R. (2024). *IBM Quantum delivers on performance challenge made two years ago*. IBM Quantum Computing Blog. https://www.ibm.com/quantum/blog/qdc-2024

Gidney, C., y Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum, 5*, 433. https://doi.org/10.22331/q-2021-04-15-433

Grover, L. K. (1996). A fast quantum mechanical algorithm for database search. *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, 212–219. https://doi.org/10.1145/237814.237866

Henriet, L., Beguin, L., Signoles, A., Lahaye, T., Browaeys, A., Reymond, G.-O., y Jurczak, C. (2020). *Quantum computing with neutral atoms*. Quantum, 4, 327. https://doi.org/10.22331/q-2020-09-21-327

Kielpinski, D., Monroe, C. y Wineland, D. Architecture for a large-scale ion-trap quantum computer. Nature 417, 709–711 (2002). https://doi.org/10.1038/nature00784

Li, W., Yin, Z., Li, X., Ma, D., Yi, S., Zhang, Z., Zou, C., Bu, K., Dai, M., Yue, J., Chen, Y., Zhang, X., y Zhang, S. (2024). A hybrid quantum computing pipeline for real world drug discovery. *Scientific Reports, 14*,16942. https://doi.org/10.1038/s41598-024-67897-8

Li, Z., Dattani, N. S., Chen, X., Liu, X., Wang, H., Tanburn, R., Chen, H., Peng, X., y Du, J. (2017). High-fidelity adiabatic quantum computation using the intrinsic Hamiltonian of a spin system: Application

to the experimental factorization of 291311. *arXiv preprint* arXiv:1706.08061. https://arxiv.org/abs/1706.08061

Lloyd, S. (2003). Hybrid Quantum Computing. In: Braunstein, S.L., Pati, A.K. (eds) Quantum Information with Continuous Variables. Springer, Dordrecht. https://doi.org/10.1007/978-94-015-1258-9_5

Lu, C.-Y., Cao, Y., Peng, C.-Z., y Pan, J.-W. (2022). Micius quantum experiments in space. *Reviews of Modern Physics, 94*(3), 035001. https://doi.org/10.1103/RevModPhys.94.035001

Ma, X.-S., Herbst, T., Scheidl, T., Wang, D., Kropatschek, S., Naylor, W., Wittmann, B., Mech, A., Kofler, J., Anisimova, E., Makarov, V., Jennewein, T., Ursin, R., y Zeilinger, A. (2012). Quantum teleportation over 143 kilometres using active feed-forward. *Nature*, 489, 269–273. https://doi.org/10.1038/nature11472

Main, D., Drmota, P., Nadlinger, D.P. *et al.* Distributed quantum computing across an optical network link. Nature 638, 383–388 (2025). https://doi.org/10.1038/s41586-024-08404-x

Mandelbaum, R., y Sitdikov, I. (2024). Demonstrating a true realization of quantum-centric supercomputing. *IBM Quantum Computing Blog*. https://www.ibm.com/quantum/blog/supercomputing-24

Mandviwalla, A., Ohshiro, K., y Ji, B. (2018). Implementing Grover's algorithm on the IBM quantum computers. *2018 IEEE International Conference on Big Data (Big Data)*, 2531-2537. https://doi.org/10.1109/BigData.2018.8622457

Mehta, S., Bhallamudi, V. P., Arige, S., y Dixit, T. (2024). Implementation of Grover's Algorithm based on Quantum Reservoir Computing. *In 2024 5th International Conference for Emerging Technology (INCET)* (pp. 1-5). IEEE.

https://www.researchgate.net/publication/379656234_Implementation_of_Grover's_Algorithm_based_on_Quantum_Reservoir_Computing

Merali, Z. (2019). *John Preskill explains "quantum supremacy"*. Quanta Magazine. https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/

Mosca, M. (2015). *Cybersecurity in an era with quantum computers: Will we be ready?* Cryptology ePrint Archive, Report 2015/1075. International Association for Cryptologic Research. Retrieved from https://eprint.iacr.org/2015/1075

Natu, S., Hyatt, K., Heim, B., Shabtai, E., Khalate, P., y Chen, T. (2024). Advancing hybrid quantum computing research with Amazon Braket and NVIDIA CUDA-Q. *AWS Quantum Technologies Blog*. https://aws.amazon.com/es/blogs/quantum-computing/advancing-hybrid-quantum-computing-research-with-amazon-braket-and-nvidia-cuda-q/

Neven, H. (2024). *Introducing Willow, our next-generation quantum chip*. Google. https://blog.google/technology/research/google-willow-quantum-chip/

Nie, X., Zhu, X., Fan, Y., Long, X., Liu, H., Huang, K., Xi, C., Che, L., Zheng, Y., et al. (2024). Self-consistent determination of single-impurity Anderson model using hybrid quantum-classical approach on a spin quantum simulator. *Physical Review Letters, 133*(14), 140602. https://doi.org/10.1103/PhysRevLett.133.140602

Nielsen, M. A., y Chuang, I. L. (2000). *Quantum Computation and Quantum Information*. Cambridge University Press.

Physics World. (2004). *Superconducting quantum bits*. Physics World.

Pla, J., Tan, K., Dehollain, J. et al. A single-atom electron spin qubit in silicon. Nature 489, 541–545 (2012). https://doi.org/10.1038/nature11449

Preskill, J. (2012). Quantum computing and the entanglement frontier. *arXiv preprint* arXiv:1203.5813. https://arxiv.org/abs/1203.5813

Preskill, J. (2018). Quantum computing in the NISQ era and beyond. *Quantum*, 2, 79. https://doi.org/10.22331/q-2018-08-06-79

Preskill, J. (2019). Why I called it 'quantum supremacy'. Quanta Magazine. https://www.quantamagazine.org/john-preskill-explains-quantum-supremacy-20191002/

Rainjonneau, S., Tokarev, I., Iudin, S., Rayaprolu, S., Pinto, K., Lemtiuzhnikova, D., Koblan, M., Barashov, E., Kordzanganeh, M., Pflitsch, M., y Melnikov, A. (2023). Quantum algorithms applied to satellite mission planning for Earth observation. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing, 16*, 7062–7075. https://doi.org/10.1109/JSTARS.2023.10155128

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124-134. https://doi.org/10.1109/SFCS.1994.365700

Sinitsyn, N. A., y Yan, B. (2023). Topologically protected Grover's oracle for the partition problem. *Physical Review A, 108*(2), 022412. https://doi.org/10.1103/PhysRevA.108.022412

Slussarenko, S., y Pryde, G. J. (2019). *Photonic quantum information processing: A concise review.* Applied Physics Reviews, 6(4), 041303. https://doi.org/10.1063/1.5115814

Smolin, J., Smith, G. y Vargo, A. Oversimplifying quantum factoring. *Nature* 499, 163–165 (2013). https://doi.org/10.1038/nature12290

Sun, Y., Wu, LA. Quantum search algorithm on weighted databases. *Sci Rep* 14, 30169 (2024). https://doi.org/10.1038/s41598-024-81701-7

Vemula, D. R., Konar, D., Satheesan, S., Kalidasu, S. M., y Cangi, A. (2022). A scalable 5,6-qubit Grover's quantum search algorithm. *arXiv preprint* arXiv:2205.00117. https://arxiv.org/abs/2205.00117

Wong, T. (2023). *Introduction to Classical and Quantum Computing* (4ª ed.). Rooted Grove. https://www.thomaswong.net/introduction-to-classical-and-quantum-computing-1e4p.pdf

Yan, B., Tan, Z., Wei, S., Jiang, H., Wang, W., Wang, H., Luo, L., Duan, Q., Liu, Y., Shi, W., Fei, Y., Meng, X., Han, Y., Shan, Z., Chen, J., Zhu, X., Zhang, C., Jin, F., Li, H., Song, C., Wang, Z., Ma, Z., Wang, H., y Long, G.-L. (2022). Factoring integers with sublinear resources on a superconducting quantum processor. *arXiv preprint* arXiv:2212.12372. https://arxiv.org/abs/2212.12372

Yin, J., Li, YH., Liao, SK. *et al.* Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature* 582, 501–505 (2020). https://doi.org/10.1038/s41586-020-2401-y