UNIVERSIDAD ALFONSO X EL SABIO

ESCUELA POLITÉCNICA SUPERIOR

GRADO EN INGENIERÍA MATEMÁTICA

TRABAJO DE FIN DE GRADO

Computación Cuántica aplicada a la Criptografía

Rubén Nogueras González

Junio de 2025

Índice

Índice de figuras

1. Objetivos

- Comprender la necesidad de la mecánica cuántica en la física clásica.
- Entender los fundamentos matemáticos de la mecánica cuántica, incluyendo álgebra lineal y espacios de Hilbert.
- Aprender las diferencias, ventajas y desventajas entre un ordenador cuántico y uno tradicional.
- Analizar el papel que juegan las puertas cuánticas en la manipulación de estados, y por lo tanto en algoritmos cuánticos.
- Explicar los distintos principios básicos de la criptografía cuántica para garantizar la seguridad de los nuevos sistemas.
- Aprender el concepto de teleportación cuántica como mecanismo eficiente y seguro para la transmisión de información.

2. Introducción Histórica a la Mecánica Cuántica

La computación cuántica es un nuevo sistema de computación, en el que nos apoyamos en las propiedades de los sistemas cuánticos para mejorar distintos paradigmas de la computación clásica. Esto lo hacemos mediante el uso del *qubit*, la unidad básica de información cuántica, a diferencia de la información clásica que se centra en el *bit* como unidad minima de información. La principal ventaja de los *qubits* es que, además de albergar información binaria (0 o 1), podemos obtener una mezcla de ambos estados (esto se conoce como el principio de superposición cuántica, que ya veremos en los próximos capítulos), de manera que podemos obtener algoritmos cuánticos que no pueden ser modelizados mediante *bits*, reduciendo en muchos casos la complejidad de algoritmos clásicos tradicionales, lo que mejora el rendimiento y eficiencia de nuestros computadores.

Para explicar esto de la mejor manera posible, nos remontamos a los orígenes de la física cuántica, a finales del siglo *XIX* y principios del siglo *XX*, cuando se pensaba que la física clásica era el foco global para explicar todos los fenómenos que suceden a nuestro alrededor, hasta que con el resultado de ciertos experimentos se comenzó a ver una relación entre el comportamiento de las ondas y las partículas, rompiendo completamente con los principios de la física clásica.

En primer lugar, vamos a comenzar explicando qué es un cuerpo negro, esto es un cuerpo que absorbe toda la radiación emitida sobre él, sin reflejar nada de lo que le llega. Esto se puede imaginar como una cavidad isotérmica con un orificio por el que se aproxima cierta radiación, de manera que permanezca en su interior. Además, suponemos que dicha cavidad se encuentra en equilibrio térmico, es decir, a una temperatura constante, de manera que la radiación que permanece dentro de ella se transforma en energía, obligando a emitir radiación hacia el exterior, sin tener nada que ver con la radiación que entra por el orificio.

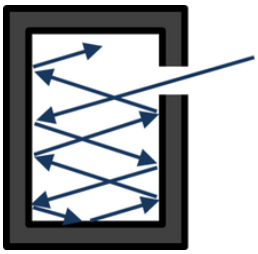

Figura 1: Ilustración del cuerpo negro

La física clásica es incapaz de explicar la radiación emitida por un cuerpo negro en función de la longitud de onda, hasta que la explicación de este fenómeno vino de la mano de *Max Planck* en el siglo *XX*, el cual establece que la energía liberada por el cuerpo negro se emite en pequeños paquetes, llamados *cuantos de energía*. Esta energía es proporcional a una pequeña constante, la constante de Planck, de manera que la energía emitida por el cuerpo negro no es continua, sino que toma un valor discreto que ha de ser múltiplo de dicha constante por su frecuencia de onda, rompiendo completamente con la física de la época y dando el nacimiento a un nuevo campo de la física, la mecánica cuántica.

$$E = h\nu \tag{1}$$

Siendo h la denominada *constante de Planck*, la cual alcanza un valor de $6{,}62607015 \times 10^{-34}\,\mathrm{J}\cdot\mathrm{s}$, y siendo ν la frecuencia. Esta energía o intensidad que libera el cuerpo la podemos medir, en función de su longitud de onda, obteniendo la siguiente gráfica:

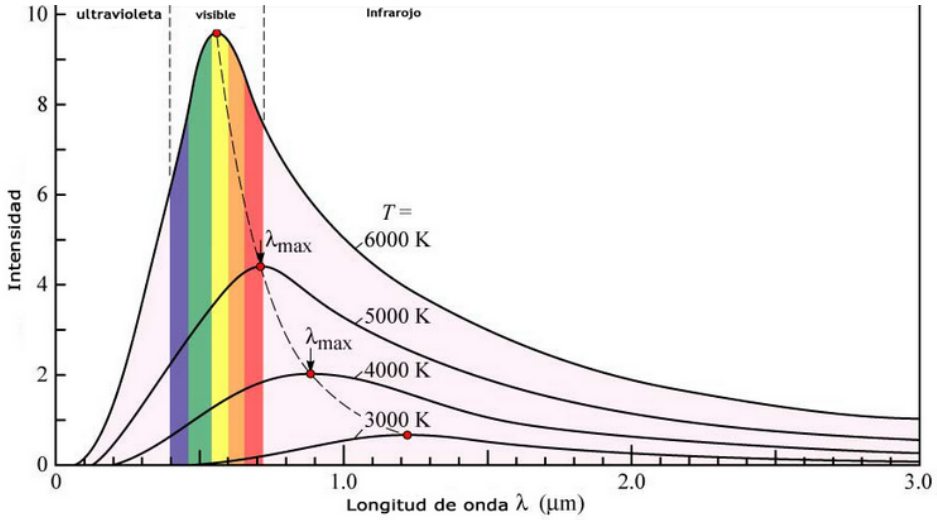

Figura 2: Catástrofe del ultravioleta

Podemos observar que a diferentes temperaturas (longitudes de onda) llegamos a diferentes curvas. La física clásica intentaba predecir estas curvas mediante ciertos modelos, que, aunque se ajustaban correctamente en distintas zonas de la gráfica, no se acercaban ni mucho menos a la realidad. Un ejemplo de esto es la catástrofe del ultravioleta, como

resultado de no ajustarse correctamente en la zona ultravioleta, en la que la intensidad de la energía tendía a infinito como resultado de otros modelos, en lugar de tender a cero como propuso *Max Planck*, formulando una ecuación que describe perfectamente la Figura 2:

$$B_\nu(T) = \frac{2h\nu^3}{c^2} \frac{1}{e^{\frac{h\nu}{k_B T}} - 1} \tag{2}$$

Donde h es la *constante de Planck*, ν la frecuencia de la radiación, c la velocidad de la luz en el vacío, k_B la *constante de Boltzmann*, T la temperatura, y e como base de los logaritmos naturales. No obstante, esta teoría cuántica fue primeramente descartada por los físicos de la época, al establecer que la energía no es un valor continuo sino discreto, hasta que con la llegada del efecto fotoeléctrico de *Albert Einstein* todo comenzó a cobrar sentido.

A finales del siglo XIX, en 1888, se presenta el efecto fotoeléctrico, definido por *Heinrich Hertz*, que consiste en la emision de electrones (fotoelectrones) al incidir luz sobre un metal, actuando como cátodo, los cuales se recogen en un ánodo, generando corriente en un circuito. Dicha luz suele ser ultravioleta, aunque en algunos casos puede ser visible.

Previamente al experimento, se plantearon varias hipótesis en base a la física clásica de la época:

- El aumento de la intensidad de la luz incrementaría la energía cinética de los fotoelectrones emitidos.
- A mayor frecuencia mayor intensidad de corriente en el circuito.

Los resultados de dicho experimento fueron sorprendentes, ya que se observó que la energía cinetica de los electrones que poseen el cátodo no dependen de la intensidad de la luz, sino de su frecuencia, y adicionalmente se pudo ver que a mayor intensidad de luz mayor intensidad de corriente. Más tarde, en 1905, se presentó un artículo, ciertamente atrevido teniendo en cuenta los recursos de la época, que resolvía todos estos problemas.

Albert Einstein presentó su hipótesis para el efecto fotoeléctrico, basándose en los resultados del experimento de *Planck*, aclarando que la luz no se comporta como una onda, sino que está compuesta de pequeñas partículas, llamadas *fotones*, cuya energía depende de su frecuencia, como ya propuso *Max Planck* en Ecuación 1, rompiendo de nuevo con los principios de la física clásica.

En dicha hipótesis se establece la necesidad de una frecuencia mínima, denominada frecuencia umbral, para que el efecto fotoeléctrico tenga lugar, la cual depende del material del que esté construido el cátodo. Por lo que si la frecuencia de los *fotones* emitidos por el haz de luz es menor a esta frecuencia umbral, no se produce corriente en el circuito, por muy intensa que sea la luz. De esta manera, si la frecuencia es mayor o igual a la umbral, los *fotoelectrones* se trasladarán hacia el ánodo al ser expulsados del núcleo de sus átomos, generando energía cinética y por lo tanto, intensidad de corriente en el circuito. Esto lo podemos razonar con la siguiente ecuación:

$$E_e = E_{ionizacion} + E_{cinetica} \tag{3}$$

Esta ecuación tiene sentido visto lo anterior, de manera que la energía de los electrones del cátodo ha de ser igual a su *energía de ionización* (o también conocido como *trabajo de extracción*), la cual es la cantidad de energía necesaria para que se produzca el efecto fotoeléctrico, sumado a su *energía cinética*. Por la explicación vista anteriormente, sabemos que dicha *energía de ionización* depende de la *frecuencia umbral* ν_0, y con la ecuación de la energía de *Planck* (Ecuación 1), además de conocer la *energía cinética* de una partícula, podemos desarrollar la Ecuación 3:

$$h\nu = h\nu_0 + \frac{1}{2}m_e v_e^2$$

Donde *h* es la *constante de Planck*, ν es la *frecuencia*, ν_0 es la *frecuencia umbral*, m_e es la masa del electrón, y v_e la velocidad del electrón, en este caso al cuadrado.

Estos son solo dos de los múltiples experimentos con soluciones extrañas para los físicos clásicos de aquella época, en los que, como hemos visto, el comportamiento de ciertos fenómenos, teóricamente imaginados como funciones de onda, se comportan como partículas. También se da el fenómeno contrario, experimentos planteados como partículas pero que son razonados mediante funciones de onda. Esto se definió con el nombre de *dualidad onda-corpúsculo*.

Más tarde, tras estudiar a fondo las bases de la mecánica cuántica propuesta por *Max Planck* y *Albert Einstein*, *Louis de Broglie* propuso en su tesis doctoral, en *1924*, que no solo la luz tiene un carácter ondulatorio, sino que toda partícula material, como los electrones, tienen una naturaleza ondulatoria, cuya longitud de onda λ es:

$$\lambda = \frac{h}{p} \tag{4}$$

Donde *p* se refiere al *momento lineal* de la partícula, lo cual podemos expresar como $p = m \cdot v$, siendo *m* la masa, y *v* la velocidad de la partícula. Tras el razonamiento de *Broglie* en *1924*, surge la *función de onda* en una dimensión, la cual describe el comportamiento las partículas con carácter ondulatorio:

$$\varphi(x,t) = e^{i(px-Et)/\hbar} \tag{5}$$

Siendo *i* la unidad imaginaria, $\hbar$ la *constante de Planck normalizada* y *x* y *t* las coordenadas de posición y tiempo de la partícula. Sin embargo, todavia no se conocia su significado fisico con total exactitud. No fue hasta que con el experimento de la doble rendija de *Clinton Davisson* y *Lester Germer* sobre electrones en *1927* (aunque *Thomas Young* lo propuso en *1801*, sobre un haz de luz, demostrando su naturaleza ondulatoria) que se confirmó la hipótesis de *De Broglie*. Como su propio nombre indica, dicho experimento consiste en una superficie opaca con dos rendijas, detrás de la cual colocamos un detector de partículas para poder percibir el comportamiento de los electrones o fotones que pasan a través de ambas rendijas. Según la física clásica, se espera que las partículas pasen a través de las rendijas en forma de línea recta, como lo haría cualquier objeto. Sin embargo, esto no sucede así en el contexto de la mecánica cuántica.

Al realizar el experimento, podemos observar un patrón de interferencias en la pantalla de detección situada detrás de las rendijas, el cual es muy similar al patrón que siguen las ondas cuando se superponen unas con otras. Efectivamente, las ondas asociadas a cada partícula se superponen unas con otras como se reveló en el experimento, no obstante, cuando observamos estas partículas mediante el detector, se comportan como una partícula clásica, cambiando su comportamiento, de manera que podemos ver por qué rendija cruzó la partícula. Este fenómeno se conoce como *colapso de función de onda*, y existen muchas teorías que intentar explicar esto, siendo la más famosa la *intepretación de Copenhage*, en la que se establece que la observación de la partícula produce un colapso de su función de onda, determinando su estado correspondiente a la medición.

Matemáticamente, podemos expresar la superposición de ondas como una superposición de estados, esto es:

$$\varphi(x,t) = \varphi_1(x,t) + \varphi_2(x,t) + \cdots + \varphi_n(x,t), \qquad \forall n \in \mathbb{N} \setminus \{0\} \tag{6}$$

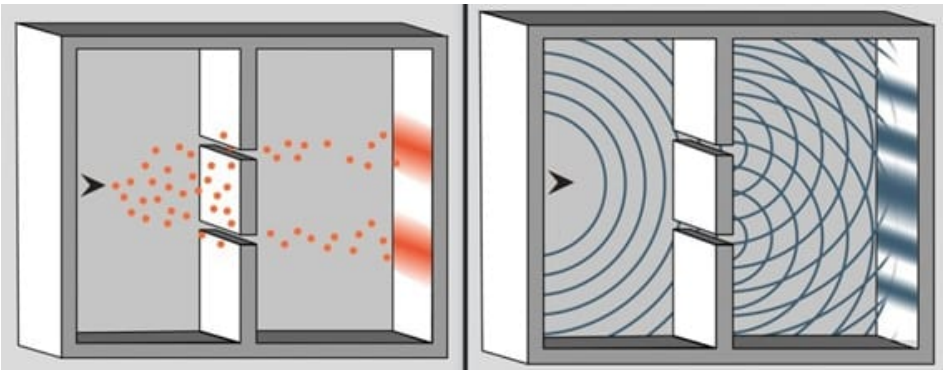

Figura 3: Experimento de la doble rendija

Adicionalmente, surgieron ciertas dudas relacionadas con la naturaleza de la función de onda. Es lógico preguntarse que, si las partículas están definidas por funciones de onda, ¿Dónde están realmente las partículas? Ya que una partícula no puede estar en varios puntos a la vez, ha de estar en un único punto. Es aquí cuando entró *Max Born*, quien sugiere que $|\varphi(x,t)|^2$ no es simplemente el cuadrado del módulo de la función de onda, sino que es una función de probabilidad, de manera que

$$|\varphi(x,t)|^2 \tag{7}$$

Representa la probabilidad de encontrar una partícula en una determinada posición. Esto tuvo una importancia bastante profunda en la mecánica cuántica de la época y en la física en general, ya que las únicas ideas de probabilidad estaban relacionadas a sistemas de incertidumbre, como el lanzamiento de una moneda. De esta manera se concluyó en la probabilidad como uno de los principales focos de la física y de la comprensión de las partículas subatómicas.

3. Ecuación de Schrödinguer

3.1. El Espacio de Hilbert

4. Álgebra Lineal y Puertas Cuánticas

4.1. Estados Cuánticos

4.1.1. Esfera de Bloch

4.2. Producto Escalar

4.2.1. Ortonormalidad

4.3. Puertas Cuánticas

4.4. Producto Tensorial

5. Errores Cuánticos

5.1. Decoherencia

5.2. Shor Code

6. Entrelazamiento Cuántico

6.1. Estados de Bell

6.2. Codificación Superdensa

7. Teleportación Cuántica

8. Algoritmos Cuánticos

8.1. Oracles Cuánticos

8.2. Algoritmo de Grover

8.3. Algoritmo de Shor

9. Estado del Arte

La empresa líder en computación cuántica es, hasta la fecha y sin duda alguna, IBM, la cual ofrece a nuestra disposición distintas páginas web en las que podemos ejecutar circuitos cuánticos y ver su comportamiento de la manera más real posible. El desarrollo del circuito se hace a través de *Python* mediante su librería destinada a la computación cuántica *Qiskit*, y una vez lo hemos completado, tenemos distintas opciones de configuración para la ejecución del circuito.

Por otra parte, si la programación en *Python* no es nuestro punto fuerte, tenemos a nuestra disposición la interfaz gráfica para el desarrollo de circuitos cuánticos de IBM, Quantum Composer. Con esta herramiento web podemos crear circuitos cuánticos con el sistema *drag and drop* sobre puertas cuánticas o qubits, de manera que se genera el correspondiente código equivalente al circuito cuántico creado y se ejecuta en un emulador o sistema cuántico, además de

que podemos visualizar el estado y la fase correspondiente en la *esfera de Bloch*, y un histograma con las probabilidades de los estados a los que puede colapsar el circuito.

De la misma manera que IBM, Amazon ha desarrollado su propia plataforma para la ejecución de circuitos cuánticos, la cual está basada nuevamente en *Python*, con la diferencia de que usamos la librería relacionada con su propio producto, *Braket*. Este producto incluye ciertas ventajas sobre el producto de IBM, como que permite la combinación de computación cuántica y clásica, aunque como vimos anteriormente, todo circuito clásico se puede expresar como un circuito cuántico. Tambień podemos encontrar productos de otras empresas para la simulación y ejecución de circuitos cuánticos, como Google o Azure, pero no dejan de ser, junto con el producto de Amazon, competidores de la solución presentada por IBM, la cual fue la primera en salir públicamente al mercado con su plataforma IBM Quantum Experience, lanzada en *2016*.

No obstante, la computación cuántica tiene muchos problemas, relacionados precisamente con la naturaleza de las partículas subatómicas, las cuales son muy sensibles al ruido causado por el exterior, lo que hace que se produzcan muchos fallos en los circuitos y que, por lo tanto, los computadores cuánticos actuales no sean tolerantes a fallos (*fault-tolerant*), de manera que los errores se acumulan muy rápidamente y sin la capacidad de ser revertidos con la tecnología cuántica hasta el momento. Sin embargo, Microsoft ha hecho un hallazgo que puede convertirse en la revolución del siglo, mucho más allá que el desarrollo de la inteligencia artificial en estos últimos años.

Microsoft ha anunciado el lanzamiento de *Majorana 1*, la primera unidad de procesamiento cuántico (QPU) con qubits topológicos, qubits que almacenan informacion cuántica de manera más estable y robusta, de manera que es mucho menos susceptible a errores cuánticos, que es uno de los principales problemas de este campo de la física y la tecnología, siendo una de las principales motivaciones para Microsoft construir el primer ordenador cuántico con tolerancia a fallos en los próximos años.

La clave de este gran avance ha sido el desarrollo de materiales topoconductores, los cuales permiten la superconductividad topológica, un estado de la materia que hasta este descubrimiento solo existía en la teoría. Este tipo de materiales se crean con arseniuro de indio y aluminio, de manera que cuando se enfrían prácticamente al cero aboluto y se sintonizan con campos magnéticos, se forman nanocables superconductores topológicos con modos cero de Majorana (MZM) en sus extremos, de manera que aumentan la estabilidad y se reducen los errores en comparación con los qubits tradicionales.

Así es como se ha desarrollado el primer qubit topológico del mundo, y se plantea tener un chip cuántico con más de un millón de qubits y tolerante a fallos en unos años, y no en unas décadas como se planteaba anteriormente, dando un gran paso en la computación cuántica práctica y probablemente uno de los mayores hitos de este campo.

10. Bibliografía

TFG Silvia Rodriguez
https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_silvia_rodriguez.pdf

Investigacion Computacion Cuantica –>Seguridad informatica, redes informaticas, IA, etc.
https://rua.ua.es/dspace/bitstream/10045/124691/1/Estudio_de_la_computacion_cuantica_en_los_diferent_Claramunt_Carriles_Sergio.pdf

Universidad de Murcia –>Schrodinguer, Hamiltoniano, Oscilador armonico, Atomo de Hidrogeno
https://webs.um.es/gustavo.garrigos/tfg/MarinMunoz_Diego_TFG_julio2021.pdf

TFG Pablo –>Algoritmo de Grover y otros algoritmos
https://rodin.uca.es/bitstream/handle/10498/27218/tfg_pablo.pdf?sequence=1&isAllowed=y

TFM –>Schrodinguer e interpretacion probabilistica de la funcion de onda
https://repositorioinstitucional.buap.mx/server/api/core/bitstreams/fb9bfe95-7945-404d-a
content

Universidad Autonoma de Madrid –>Interpretacion probabilistica de la funcion de onda e introduccion al atomo de hidrogeno
https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_luis_sanchez.pdf

TFG –>Espacios de Hilbert y su relacion con la mecanica cuantica
https://idus.us.es/server/api/core/bitstreams/4c49766a-cdfc-4d72-9acf-f62761db63fb/content

Claudia Mielgo –>El sistema cuantico es un espacio de Hilbert, y funciones de onda
https://matematicas.uam.es/~fernando.chamizo/supervision/TFG/past/memoirs/TFG_claudia_mielgo.pdf

Algebra Lineal –>Algebra lineal, espacios de Hilbert y criptografia cuantica
https://repositorio.ual.es/bitstream/handle/10835/9810/VILLASANA%20ALCARAZ%2C%20MARIA%20DEL%20MAR.pdf

Roberto Gonzalez –>Sistema Bineario e introduccion a los qubits
https://oa.upm.es/69234/1/TFG_ROBERTO_GONZALEZ_RIVAS.pdf

Por que un ordenador cuantico?
https://zaguan.unizar.es/record/76803/files/TAZ-TFG-2018-3072.pdf

Radiacion del cuerpo negro
https://www.fisicacuantica.es/la-radiacion-del-cuerpo-negro/

https://weblab.deusto.es/olarex/cd/kaernten/BBR_ES_new_27.09.2013/distribucin_de_la_energa.html

https://www.quimicafisica.com/teoria-cuantica/la-radiacion-del-cuerpo-negro.html

Efecto Fotoeléctrico
https://es.khanacademy.org/science/ap-chemistry/electronic-structure-of-atoms-ap/bohr-model-hydrogen-ap/a/photoelectric-effect

https://www.quimicafisica.com/teoria-cuantica/el-efecto-fotoelectrico.html

Experimento de la Doble Rendija
https://www.fisicalab.com/apartado/cantidad-movimiento#google_vignette

https://www.dciencia.es/fisica-cuantica-el-experimento-de-la-doble-rendija/

https://mecanicosvalencia.es/max-born-mecanica-cuantica/

Majorana
https://news.microsoft.com/source/latam/noticias-de-microsoft/microsoft-presenta-majoran