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. Introducción

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 cuando se pensaba que la física clásica era el foco global para resolver todos nuestros problemas, hasta que con el resultado de ciertos experimentos se comenzó a ver una relación entre el comportamiento de las ondas y las partículas.

La física clásica es incapaz de explicar la radiación emitida por un cuerpo negro en función de la longitud de onda. La explicación de este fenómeno físico vino de la mano de *Max Planck* en el siglo *XX*, en el que describía perfectamente el funcionamiento de esta curva (y aqui poner la imagen xd)

Lo primero de todo, un cuerpo negro es un cuerpo que absorbe toda la radiación que le llega, sin reflejar nada de lo que le llega. Esto se puede imaginar como una caja con un orificio por el que se aproxima cierta radiación, de manera que permanezca en su interior.

Si suponemos que dicho cuerpo negro se encuentra en equilibrio térmico, es decir, a una temperatura constante, la radiación que permanece dentro del cuerpo se transforma en energía, obligando al cuerpo negro a emitir radiación hacia el exterior, sin tener nada que ver con la radiación que entra por el orificio.

Esta energía o intensidad que libera el cuerpo la podemos medir, en función de su longitud de onda, obteniendo una gráfica.

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 esta zona, en la que la intensidad de la energía tiende a infinito, en lugar de tender a cero como ya sabemos que ocurre en la realidad.

La solución fue encontrada por *Max Planck* en *1927* (no se si es este año), 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, formulando una ecuación que describe perfectamente la gráfica (referenciar):

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

Esta teoría cuántica fue primeramente rechazada 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 empezó a cobrar sentido.

2. 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 a sus niños –>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 explica bien –>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 xd, 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

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

https://redaccion.org/como-los-fisicos-cuanticos-describen-un-cuerpo-negro/