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.