QUANTUM JAM 2025 – HACKATHON PROMPT

Motivación

Dado que nuestra criptografía clásica de clave pública (RSA, ECC) se ve amenazada por los avances en la computación cuántica, hemos recurrido a nuevos métodos de cifrado para resolver este dilema. La computación cuántica nos ofrece nuevas formas de proteger la información, una de las cuales es la Distribución Cuántica de Claves (QKD). A diferencia de los esquemas basados en factorización, los protocolos QKD utilizan las propiedades únicas de la computación cuántica para generar claves secretas compartidas que los intrusos no pueden interceptar sin ser detectados.

En la década de 1980, Charles Bennett y Gilles Brassard crearon BB84 (Bennett y Brassard, 1984). En BB84, Alice y Bob intercambian qubits en bases aleatorias, los miden y, a continuación, filtran y procesan los resultados de las mediciones para acordar una clave secreta. Cualquier intento de un espía (Eve) de medir los qubits introduce errores detectables.

¡Manos a la obra!

Usando Qiskit, construirán un prototipo de Distribución de Claves Cuánticas BB84 completamente funcional que se ejecutará en hardware cuántico real o simulado. El objetivo es demostrar cómo las partes (Alice y Bob) pueden establecer una clave secreta compartida con seguridad basada en la teoría de la información. La implementación debe incluir la generación de claves de extremo a extremo, procedimientos de medición y “sifting” , y la estimación de la tasa de error para detectar cualquier interferencia. Recopilarán y representarán gráficamente métricas clave e ilustrarán cómo estos valores cambian al introducir ruido. Al comparar el rendimiento en diferentes condiciones, demostrarán la viabilidad práctica de BB84 en las plataformas cuánticas actuales y destacarán la utilidad del enfoque.

Implementarán el protocolo en una notebook de Google Colab, presentando su código de manera informativa. Como extra, pueden explicar los fundamentos de QKD y situarlo en el contexto más amplio del cifrado poscuántico. También pueden comparar BB84 con otro enfoque emergente, explicando cómo estos algoritmos resisten los ataques cuánticos.