# RESUM

Aquest treball de recerca ofereix una anàlisi exhaustiva dels fonaments de la física quàntica i la seva aplicació pràctica en el camp de la criptografia moderna, centrant-se específicament en el protocol BB84. La hipòtesi principal estableix que mitjançant la simulació computacional d'aquest protocol és possible detectar eficaçment intercepcions en la transmissió de claus quàntiques, ja que qualsevol intent d'espionatge introdueix alteracions mesurables i quantificables en la clau secreta compartida entre els usuaris.

El marc teòric desenvolupat examina en profunditat conceptes quàntics essencials com el principi d'incertesa de *Heisenberg, la superposició d'estats i el fenomen entrellaçament quàntic, tots els pilars fonamentals que garanteixen la seguretat del protocol BB84. Aquests principis físics asseguren que qualsevol mesurament no autoritzat sobre el sistema quàntic modifiqui inevitablement l'estat dels qubits transmesos, deixant així una petjada detectable de l'intent d'intercepció.

La part pràctica es materialitza a través d'una simulació desenvolupada en Python que recrea meticulosament totes les etapes del protocol: des de la generació i codificació dels qubits fins a la seva transmissió, mesurament i posterior processament. El model incorpora de manera realista la possible intercepció per part d'un espia extern, denominat Eva, cosa que permet quantificar l'impacte de les seves accions sobre la integritat de la comunicació.

Els resultats obtinguts a través de múltiples simulacions confirmen contundentment la hipòtesi inicial, demostrant que quan Eva intercepta els qubits transmesos, la taxa d'error en la clau resultant experimenta un increment significatiu i mesurable. El protocol estableix criteris precisos, determinant que si aquesta taxa d'error supera un llindar de l'11%, la clau ha de ser immediatament descartada per considerar-se compromesa. Aquesta recerca evidencia la viabilitat operativa del protocol BB84 per a assegurar comunicacions en entorns hostils, destacant la seva directa dependència de les propietats fonamentals de la mecànica quàntica i la seva

capacitat per a prioritzar la seguretat absoluta sobre consideracions operatives o d'eficiència en la distribució de claus criptogràfiques.