Resum

Aquest treball s'enfoca a estudiar un nou camp emergent de la criptografia, la criptografia quàntica, que promet protegir amb una eficàcia del 100% dels ordinadors quàntics. Explora superficialment la història de la criptografia, des dels seus inicis fins a l'actualitat. Profunditza en la idea de criptografia clàssica, i estudia els conceptes de la física quàntica fonamentals per poder aplicar la criptografia quàntica. Presenta dues entrevistes a experts, un informàtic i un investigador en un grup d'investigació d'informació quàntica, i realitza una simulació clàssica del protocol BB84 de la criptografia quàntica, mostrant el seu funcionament. També realitza una comprovació d'efectivitat amb algorismes quàntics mitjançant l'ordinador quàntic superconductiu del Centre per a la Informació i Biologia Quàntica, a Osaka, Japó.

El treball recalca que, encara que sobre paper, l'eficàcia de la criptografia quàntica sigui molt propera al 100%, a la realitat hi ha altres factors que alteren aquesta probabilitat fent, actualment, impossible una comunicació tan segura amb aquest mètode. Els factors que disminueixen aquesta probabilitat són: un petit percentatge teòric de 7.89x10^-31, completament negligible; un percentatge referent a les limitacions actuals de mantenir un estat quàntic en moviment per grans distàncies, calculat d'aproximadament d'un 7,2%; i una possibilitat no calculable, l'espionatge clàssic (com per exemple suplantació d'identitat) i l'error humà.