CRIPTOGRAFIA QUÀNTICA

Xavier Luis Santos
2023-2024
Física
Jesús González Ortuño /
Gisela García Bardají
INS Puig Castellar
15/11/2024

“If you think you understand quantum mechanics, you don't understand quantum mechanics.”

Richard Feynman (1918-1988), premi Nobel de Física al 1965.

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.

Resumen

Este trabajo se enfoca en estudiar un nuevo campo emergente de la criptografia, la criptografia cuántica, que promete proteger con una eficacia del 100% de los ordenadores cuánticos. Explora superficialmente la historia de la criptografia, desde sus inicios hasta la actualidad. Profundiza en la idea de criptografia clásica, y estudia los conceptos fundamentales de la física cuántica para poder aplicar la criptografia cuántica. Presenta dos entrevistas a expertos, un informático y un investigador en un grupo de investigación de información cuántica, y realiza una simulación clásica del protocolo BB84 de la criptografia cuántica, mostrando su funcionamiento. También realiza una comprobación de efectividad con algoritmos cuánticos mediante el

ordenador cuántico superconductor del Centro para la Información y Biología Cuántica, en Osaka, Japón.

El trabajo recalca que, aunque sobre papel, la eficacia de la criptografia cuántica sea muy próxima al 100%, en la realidad hay otros factores que alteran esta probabilidad haciendo, actualmente, imposible una comunicación tan segura con este método. Los factores que disminuyen esta probabilidad son: un pequeño porcentaje teórico de $7.89x10^{-31}$, completamente negligible; un porcentaje en lo referente a las limitaciones actuales de mantener un estado cuántico en movimiento por grandes distancias, calculado de aproximadamente de un 7,2%; y una posibilidad no calculable, el espionaje clásico (como por ejemplo suplantación de identidad) y el error humano.

Abstract

This paper focuses on studying a new emerging field on cryptography, the quantum cryptography, which promises to protect with 100% efficiency from quantum computers. It explores superficially the history of cryptography, from its beginnings to the present day. It delves into the idea of classical cryptography, and studies the fundamental concepts of quantum physics in order to apply quantum cryptography. It features two interviews with experts, a computer specialist and a researcher in a quantum information research group, and performs a classical simulation of the BB84 protocol of quantum cryptography, showing how it works. It also performs an effectiveness check with quantum algorithms using the superconducting quantum computer at the Center Information and Quantum Biology in Osaka, Japan.

The paper emphasizes that, although on paper, the effectiveness of quantum cryptography is very close to 100%, in reality there are other factors that alter this probability, making it currently impossible to communicate so securely with this method. The factors that decrease this probability are: a small theoretical percentage of $7.89x10^{-31}$, completely negligible; a percentage regarding the current limitations of maintaining a quantum state in motion over long distances, calculated to be approximately 7.2%; and a non-calculable possibility, classical espionage (such as identity supplanting) and human mistakes.

Índex

1. Introducció

Aquest treball es centra envers un tema encara en desenvolupament, la criptografia quàntica. Moltes vegades, si escoltes alguna cosa sobre el tema, el que et queda clar primerament és que és un mètode de comunicació, com les paraules, que té unes normes a seguir per aconseguir l'enteniment d'ambdós parlants; si investigues una mica més veus que es diu que és un mètode indesxifrable i 100% segur, on no cap possibilitat d'espionatge ni d'adulteració de la informació. Aquest treball té com a motivació investigar més que és la criptografia quàntica i respondre a la pregunta: és avui dia la criptografia quàntica un mitjà de comunicació 100% segur?

Per resoldre aquests dubtes faré primerament un repàs per la història de la criptografia, investigarem i profunditzarem en la criptografia tradicional, repassarem els conceptes bàsics de la física quàntica i buscarem aplicacions tant actuals com futures en aquesta nova tecnologia.

Per poder comprovar de primera mà el procés de treballar amb informació quàntica, aprofitaré una de les sessions que m'ofereix el programa Bojos per la Ciència, de la Fundació Catalunya La Pedrera[1], on es treballen tant teòricament com pràcticament molts camps de la ciència, al meu cas, serà una sessió sobre el pas del BIT al QBIT, és a dir, de la informació tradicional que tenim a un ordinador domèstic, escrita en codi binari, al QBIT, el nou sistema d'informació quàntica.

Per últim, intentarem respondre tant a la pregunta plantejada inicialment com a preguntes que hagin sortit durant el procés d'investigació, concloent amb una reflexió final sobre l'avenç d'aquesta nova tecnologia i posant una mirada en el seu futur.

[1] Bojos per la Ciència. Fundació Catalunya La Pedrera [Consultat: 06 de maig de 2024]. Disponible a: https://www.fundaciocatalunya-lapedrera.com/es/bojos-ciencia

2. Hipòtesi

Intentaré respondre a la pregunta “És realment la criptografia quàntica 100% segura?” formulant la meva hipòtesi, més endavant, a les conclusions, corroboraré o refutaré aquesta hipòtesi.

Amb els coneixements que tinc sobre el tema abans d’investigar i de fer la sessió experimental, crec que la criptografia quàntica sí que és 100% segura perquè els QBITS (els BITs quàntics) aleatoritzen el seu missatge en ser llegits i, en cas d'haver-hi algun error de seguretat, el receptor s’adonaria immediatament. Afegint-hi l’encriptació estàndard al missatge i missatges amb nombres aleatoris al principi de cada comunicació, es pot fer un sistema a prova d’espionatge.

3. Marc teòric

A través d'aquest apartat faré una recerca envers la criptografia i la quàntica, per després enllaçar aquests dos conceptes i arribar a la criptografia quàntica. Començarem per fer un breu repàs per la història de la criptografia, un pas molt important per poder entendre la importància que té actualment un sistema segur per transmetre informació.

3.1. Història de la criptografia

La criptografia, l'art de codificar missatges per mantenir la seva seguretat, té una llarga història que es remunta a milers d'anys. Des dels mètodes més simples fins als sistemes quàntics actuals, la criptografia ha evolucionat constantment, però el ritme d'aquest progrés ha estat desigual, amb un avanç molt accelerat en els darrers 100 anys.

3.1.1. Antiguitat: Els Primers Sistemes de Criptografia

Les primeres formes de criptografia es remunten a les antigues civilitzacions. Un dels exemples més antics és l'escítala lacedemònia (segle V a.C.)[2], utilitzada pels espartans per enviar missatges secrets. Es tractava d'un bastó on es col·locava una tira de cuir o pergamí amb el missatge xifrat, que només podia llegir-se enrotllant-la al bastó correcte.

Figura 1: Escítala. Extreta de Wikimedia Commons.

[2] Schneider, J. (2024, 30 setembre). Breve historia de la criptografia. *IBM*. Consultat el 9 de novembre de 2024, de https://www.ibm.com/mx-es/think/topics/cryptography-history

Un altre exemple clàssic és el xifratge de Cèsar (segle I a.C.), utilitzat per Juli Cèsar. En aquest sistema, les lletres del missatge original es desplaçaven un nombre de posicions en l'alfabet. Encara que senzill, aquest mètode garantia una capa de seguretat bàsica per a les comunicacions militars.

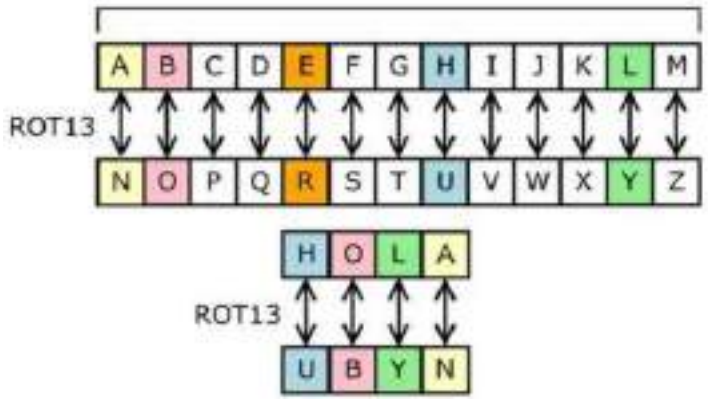

Figura 2: Exemple ROT13. Extreta del blog de Daviticblog.

Aquests primers sistemes eren rudimentaris i fàcils de trencar, però proporcionaven prou seguretat per a les necessitats de l'època. La criptografia es limitava a un cercle reduït de persones, normalment per a aplicacions militars o polítiques, i els mètodes de desxifrat sovint depenien de la destresa humana.

3.1.2. Edat Mitjana i Renaixement: Les Primeres Innovacions

Durant l'Edat Mitjana, la criptografia es va seguir utilitzant, principalment en l'àmbit militar i diplomàtic[3]. Ramon Llull, al segle XIII, va ser un dels primers en teoritzar sobre sistemes de xifratge més complexos, i el seu treball va influir en la criptografia europea dels segles posteriors[4].

Un avanç important va arribar amb l'algorisme de substitució polialfabètic, desenvolupat per Leon Battista Alberti al segle XV. Aquest sistema utilitzava múltiples alfabets de substitució, codificant dues lletres com a una sola, fent que el xifratge fos més difícil de trencar. Alberti va ser també pioner en l'ús de dispositius mecànics per ajudar en el xifratge, una innovació important en la criptografia[5].

[3] Aparicio, J. I. (2020, 10 setembre). *Criptografía en la Alta Edad Media*. Historia del Condado de Castilla. Consultat el 10 de novembre de 2024, de https://www.condadodecastilla.es/blog/criptografia-en-la-alta-edad-media/

[4] Col·legi Oficial d'Enginyeria Informàtica de Catalunya. (2019, 11 abril). *Ramon Llull, patró dels informàtics: per què?* COEINF. Consultat el 10 de novembre de 2024, de https://enginyeriainformatica.cat/ramon-llull-patro-dels-informatics-per-que /

[5] Carbajo, J. L. T. (s. d.). *Alberti | Criptografía clásica*. Consultat el 10 de novembre de 2024, de https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto11.html

DE POLYGRAPHIE. 167

Table recte de transpoſition.

a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&
b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a
c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b
d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c
e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d
f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e
g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f
h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g
i	k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h
k	l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i
l	m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k
m	n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l
n	o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m
o	p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n
p	q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o
q	r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p
r	s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q
s	t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r
t	u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s
u	x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t
x	y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u
y	z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x
z	&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y
&	a	b	c	d	e	f	g	h	i	k	l	m	n	o	p	q	r	s	t	u	x	y	z

Figura 3: Taula de transposició polialfabètica. Extreta de Todolibroantiguo.

Malgrat tots aquests avenços, la criptografia continuava sent utilitzada principalment per reis, diplomàtics i militars. El ritme de progrés era relativament lent, ja que les comunicacions estaven limitades i els sistemes de xifratge només s'aplicaven a un petit nombre de missatges.

3.1.3. Segles XVII-XIX: L'Era de la Criptografia Militar

A mesura que les guerres europees es van intensificar, la necessitat de comunicacions segures va augmentar. Al segle XIX, l'ús de la criptografia en la diplomàcia i la guerra es va estendre considerablement. Durant la Guerra Civil Nord-americana, per exemple, ambdós bàndols van utilitzar codis per mantenir les seves comunicacions segures[6].

Al mateix temps, matemàtics com Friedrich Kasiski van començar a desenvolupar mètodes per desxifrar els sistemes de xifratge més sofisticats, com el de substitució polialfabètic[7]. Això va conduir a una cursa entre els creadors de sistemes de xifratge i els experts en trencar-los, un tema recurrent en la història de la criptografia.

3.1.4. Segle XX: El Naixement de la Criptografia Moderna

El segle XX va suposar una revolució per a la criptografia, especialment durant les dues guerres mundials. Un dels exemples més famosos és la màquina Enigma, utilitzada per l'exèrcit alemany durant la Segona Guerra Mundial. Aquesta màquina utilitzava rotors per crear codis increïblement complexos, però gràcies a l'esforç d'Alan Turing i el seu equip de criptògrafs a Bletchley Park, els Aliats van aconseguir trencar aquest codi creant la primera màquina programable, cosa que va ser fonamental per al desenllaç de la guerra[8].

---

[6] *Overview of Civil War Codes and Ciphers*. (s. d.). Consultat el 10 de novembre de 2024, de https://cryptiana.web.fc2.com/code/civilwar0.htm

[7] Fuensanta, J. R. S. (s. d.). *Cifrados polialfabéticos - criptohistoria*. Consultat el 10 de novembre de 2024, de https://www.criptohistoria.es/polialfabeticos.html

[8] Sadurní, J. M. (2024, 17 juny). Alan Turing, el arma secreta de los aliados. *historia.nationalgeographic.com.es*. https://historia.nationalgeographic.com.es/a/alan-turing-arma-secreta-aliados_16352

Figura 4: Rèplica de màquina Enigma. Extreta de National Geographic.

Després de la guerra, la criptografia va continuar evolucionant, però el veritable canvi va arribar amb l'era de la computació. El desenvolupament de l'algorisme RSA el 1977 per Rivest, Shamir i Adleman va ser un dels moments clau[9]. Aquest sistema de criptografia asimètrica va permetre per primera vegada que dues persones intercanviessin missatges de manera segura sense necessitat de compartir una clau prèviament.

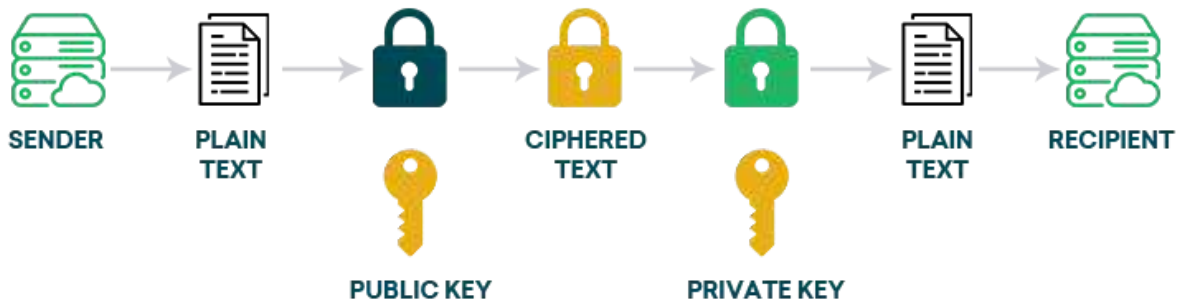

Figura 5: Criptografia de clau pública. Extreta de ClickSSL.

[9] *RSA (Rivest, Shamir y Adleman)*. (s. d.). Cyberzaintza. Consultat el 10 de novembre de 2024, de https://www.ciberseguridad.eus/ciberglosario/rsa-rivest-shamir-y-adleman

El segle XX va veure també la creació de l'Advanced Encryption Standard (AES), un dels algorismes més segurs i utilitzats actualment[10], i la introducció de nous conceptes, com la criptografia de clau pública.

3.1.5. Segle XXI: La Criptografia en l'Era Digital i la Criptografia Quàntica

En l'era d'internet, la criptografia s'ha convertit en una peça clau de les comunicacions digitals. Les transaccions bancàries, els correus electrònics, les xarxes socials i altres formes de comunicació utilitzen criptografia per garantir la privadesa i la seguretat de les dades. Amb l'arribada dels ordinadors quàntics[11], es planteja la possibilitat de trencar els sistemes actuals de xifratge, i això ha donat lloc a la criptografia quàntica, un camp emergent que es basa en les lleis de la mecànica quàntica per crear sistemes de seguretat teòricament inviolables[12].

3.2. Què és la criptografia?

Ara que ja sabem una mica sobre la seva història i orígens, profunditzarem més per entendre la criptografia, exemplificarem uns quants mètodes senzills i comprovarem la seguretat d'aquests mètodes no quàntics, que anomenarem "clàssics".

Abans de començar a definir el concepte de criptografia hem de saber que no funciona si els dos comunicadors no s'han vist abans, és a dir, que han de pactar quin mètode d'encriptació utilitzaran, perquè si envies el teu mètode de descodificació juntament amb el missatge qualsevol persona que sàpiga una mica sobre criptografia sabrà com desencriptar-ho.

Per començar, una bona definició general de la criptografia seria: La criptografia és la ciència que estudia l'encriptació i desencriptació de missatges, és a dir, codificar i

[10] *AES*. (s. d.). NFON AG. Consultat el 10 de novembre de 2024, de https://www.nfon.com/es/get-started/cloud-telephony/lexicon/base-de-conocimiento-destacar/aes

[11] Xu, T. (2024, 8 febrer). *Cryptographers are racing against quantum computers*. Built In. Consultat el 10 de novembre de 2024, de https://builtin.com/articles/post-quantum-cryptography

[12] Schneider, J., & Smalley, I. (2024, 30 agost). What is quantum cryptography? *IBM*. Consultat el 10 de novembre de 2024, de https://www.ibm.com/topics/quantum-cryptography

descodificar missatges per augmentar la seguretat d'aquests i que cap persona que no siguin l'emissora i la receptora sàpiguen que diu el missatge[13].
Ara bé, aquest concepte és molt gran i comprèn molts mètodes, per poder entendre millor l'encriptació i desencriptació de missatges posaré un exemple de comunicació encriptada.

3.2.1. Posem en pràctica la criptografia clàssica

Per posar en pràctica aquesta mecànica d'encriptació i desencriptació en posarem en aquesta situació, l'Alice vol enviar un missatge a en Bob[14], aquest missatge conté el següent text: "El codi secret és 2773".

L'Alice no vol que cap persona excepte en Bob sàpiga el codi, i com que vol enviar el missatge per correu no pot assegurar que no hi hagi cap espia. Per tant, l'Alice encriptarà el missatge de manera que només es pugui saber que diu tenint un codi de desencriptació específic. L'Alice i en Bob van pactar que utilitzarien el mètode de codificació cèsar[15] amb un desplaçament de 5 lletres cap a la dreta.

Com s'ha mencionat a l'apartat 3.1.1., el mètode d'encriptació Cèsar consisteix en desplaçar el missatge X vegades a l'abecedari, normalment cap a la dreta. Si la desplacem 5 vegades (ROT5) la A passa a ser la F, la B la G i així successivament. Els números els situem després de l'abecedari per fer el desplaçament, per tant, després de la Z va el 0 i després del 9 torna la A.

El missatge inicial ("El codi secret és 2773"), una vegada passat per la codificació queda així: "Jp htin xjhwjy jx 7cc8", completament ilegible i lliure de mirades indiscretes. Això si, una persona amb coneixements de desencriptació pot arribar a endevinar quina clau utilitzen (en aquest cas ROT5), ja que el xifrat cesar es un dels

[13] *¿Qué es la criptografía?* (2020, 20 novembre). Kaspersky. Consultat el 10 de novembre de 2024, de https://www.kaspersky.es/resource-center/definitions/what-is-cryptography

[14] *Alice y Bob*. (2023, 29 setembre). Wikipedia, la Enciclopedia Libre. Consultat el 10 de novembre de 2024, de https://es.wikipedia.org/wiki/Alice_y_Bob

[15] dCode. (s. d.). *Cifrado César*. Consultat el 10 de novembre de 2024, de https://www.dcode.fr/cifrado-cesar?__r=1.129bfa8fcc6dd2f9029fdfd510213cb0

més senzills i simples, però ens ve bé per entendre aquesta mecànica d'encriptació, desencriptació, clau, etc.

3.2.2. Mètodes avançats

Cal mencionar que hi existeixen molts altres mètodes més avançats i segurs, que s'utilitzen en informàtica i que no són desxifrables per un sol individu, però sí per una màquina. Per exemple la criptografia de clau pública[16], en la que hi ha dues claus, una pública per xifrar un missatge i una altra privada per desxifrar-lo, això resol el problema de la criptografia de clau privada (com la Cèsar), en la que ambdós costats han de saber la clau abans i després d'enviar-la.

3.3. Què és la quàntica?

Abans de profunditzar en el concepte de la criptografia quàntica, ens vindrà molt bé repassar algunes propietats de la quàntica que són vitals pel funcionament de la nova criptografia.

3.3.1. Orígens de la quàntica

A finals del segle XIX, la física clàssica havia aconseguit explicar pràcticament tot fenomen observable i, per tant, molts científics de l'època pensaven que el camp de la física s'havia acabat i quedaven únicament per resoldre petits detalls sense gaire importància. Tant és així que William Thomson, més conegut com Lord Kelvin, va fer una conferència a l'any 1900 on afirmava que la física estava gairebé completa, i que només quedaven dos problemes que ell va anomenar "dos petits núvols al cel clar de la física"[17].

Es tractava del problema del cos negre i de l'efecte fotoelèctric. Aquests dos petits núvols van revolucionar la física i va obrir les portes del que ara coneixem com física quàntica[18].

---

[16] *Public key encryption*. (2024, 24 juny). GeeksforGeeks. Consultat el 10 de novembre de 2024, de https://www.geeksforgeeks.org/public-key-encryption/

[17] Passon, O. (2021). *Kelvin's clouds* [Article]. https://arxiv.org/pdf/2106.16033

[18] Sabadell, M. Á. (2024, 28 juny). *Así nació la teoría física más perfecta jamás creada*. Muy Interesante. Consultat el 10 de novembre de 2024, de https://www.muyinteresante.com/ciencia/60562.html

3.3.1.1. El problema del cos negre

El primer problema per resoldre és el problema de la radiació del cos negre, un objecte idíl·lic que absorbeix tota la radiació que rep i, en resposta, emet radiació segons la temperatura a la que es trobi[19]. Si utilitzem la física clàssica per estudiar aquest fenomen, un cos negre hauria d'emetre energia infinita a freqüències altes, això es coneix com a catàstrofe ultraviolada[20].

Max Planck va resoldre aquest problema l'any 1900, proposant que l'energia no s'emet de forma contínua sinó "quantitzada" en paquets. Aquest va ser el naixement de la física quàntica, amb el concepte del "quàntum" d'energia. Planck va proposar que l'energia de la radiació estava quantificada, amb E=hv, on h és la constant de Planck i v és la freqüència de la radiació[21].

3.3.1.2. L'efecte fotoelèctric

L'efecte fotoelèctric era l'altre "petit detall" que quedava sense resoldre, consisteix en que quan la llum és rebuda per un metall, aquest allibera electrons. Segons la física clàssica, la intensitat d'aquesta llum determinava l'energia dels electrons alliberats, però els experiments demostraven que només depenia de la freqüència d'aquesta llum i no pas de la seva intensitat[22]. A l'any 1905, utilitzant la idea de Planck de "quantitzar" energia, Albert Einstein va proposar que la llum no era només una ona continua, sinó partícules discretes anomenades fotons. Cada fotó tenia una energia proporcional a la seva freqüència i només els fotons amb suficient energia (freqüència) podien alliberar els electrons del metall.

Aquesta explicació va marcar una de les primeres aplicacions directes de la mecànica quàntica i va fer guanyar a Einstein el Premi Nobel de Física el 1921[23].

---

[19] *La radiación del cuerpo negro*. (2019, 5 febrer). Física Cuántica En la Red. Consultat el 10 de novembre de 2024, de https://www.fisicacuantica.es/la-radiacion-del-cuerpo-negro/

[20] *Catástrofe ultravioleta*. (s. d.). Luz-Wiki. Consultat el 10 de novembre de 2024, de https://luz.izt.uam.mx/wikis/mediawiki/index.php/Catastrofe_ultravioleta

[21] Rami Arieli. (s. d.). *Fotones y diagramas de energía*. LEQ. Consultat el 10 de novembre de 2024, de https://www.um.es/LEQ/laser/Ch-2/F2s2p1.htm

[22] *Photoelectric effect | Definition, Examples, & Applications*. (2024, 25 octubre). Encyclopedia Britannica. Consultat el 10 de novembre de 2024, de https://www.britannica.com/science/photoelectric-effect

[23] ¿Qué hizo Albert Einstein para ganar el Premio Nobel? (2024, 10 març). *Clarín*. https://www.clarin.com/internacional/hizo-albert-einstein-ganar-premio-nobel_0_fjDU1EWY2B.html?srsltid=AfmBOoofZ0JCnujeFPSCdUniYRo4UHxFd9wuCy1fKc_-PwGz2Ec-m7xo

3.3.2. Les bases de la quàntica

La física clàssica és l'estudi d'una partícula o cos, com una pilota, i el seu estat ens descriu els valors concrets de variables com la velocitat, la posició, la temperatura… Aquests valors concrets es poden representar amb punts en un espai abstracte unidimensional, com per exemple la temperatura.

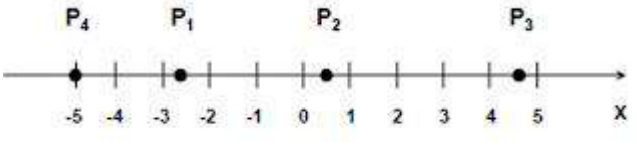

Figura 6: Punts en un espai unidimensional. Extreta de Geometriaanalitica5d.

A la quàntica, aquesta partícula no pot definir el seu estat (velocitat, posició, temperatura…) amb un punt, sinó que ha de fer-ho amb un vector en un espai abstracte bidimensional que anomenem "Espai de Hilbert"[24].

Pensem en un sistema senzill com l'espín d'un electró[25], que només pot tenir dos estats possibles: "espín cap amunt" i "espín cap avall". Podem imaginar aquests dos estats com dos vectors en un espai bidimensional. Però en lloc de tenir només dos estats possibles, un electró pot estar en una superposició d'aquests dos estats (una combinació dels dos), i això es representa per un vector que no està ni totalment "cap amunt" ni totalment "cap avall", sinó en algun punt intermedi.

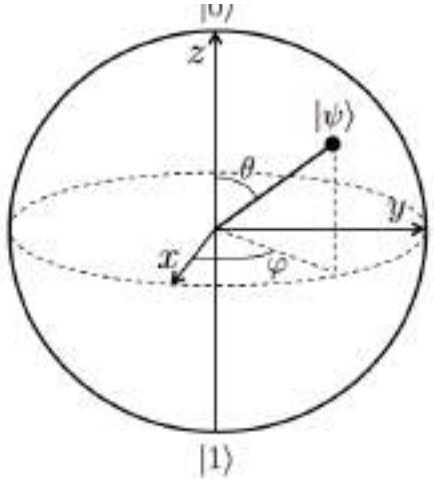

Figura 7: Vectors d'un estat quàntic. Extreta de ResearchGate.

[24] *Hilbert Space*. (2024, 6 novembre). Wikipedia. Consultat el 10 de novembre de 2024, de https://en.wikipedia.org/wiki/Hilbert_space

[25] *Electron spin*. (s. d.). Consultat el 10 de novembre de 2024, de http://hyperphysics.phy-astr.gsu.edu/hbasees/spin.html

Aquest vector es representa normalment amb la notació de Dirac: $|\psi\rangle$[26] i s'anomena estat quàntic.

3.3.3. Les lleis de la quàntica

Hem mencionat la superposició al punt 3.3.2. i en aquest punt, l'explicarem amb les altres lleis fonamentals de la quàntica.

3.3.3.1. Principi de superposició

El principi de superposició diu que un sistema quàntic pot estar en múltiples estats al mateix temps. Això vol dir que, abans de mesurar-lo, una partícula en un estat quàntic no es troba en un estat concret, sinó en una combinació de tots els estats possibles[27]. Aquesta superposició es representa mitjançant un vector d'estat (com vam veure abans).

Aquest principi és la base de la criptografia quàntica, on els Qbits poden estar en superposició d'1 i 0 alhora, a diferència dels bits clàssics que només poden ser o 1 o 0; el que ens dona un valor incert que permet aquesta seguretat, com veurem més endavant.

3.3.3.2. Entrellaçament quàntic

L'entrellaçament quàntic passa quan dues partícules queden entrellaçades, de manera que el seu estat quàntic està connectat. Això vol dir que, fins i tot si les dues partícules se separen a grans distàncies, el que li passi a una partícula afecta immediatament l'altra, independentment de la distància[28].

3.3.3.3. Principi d'incertesa de Heisenberg

El principi d'incertesa de Heisenberg diu que és impossible conèixer amb precisió absoluta certs parells de propietats d'una partícula (en estat quàntic) al mateix temps. El cas més famós és el de la posició i la velocitat. Com més precisament

---

[26] Téllez, A. M. (s. d.). *La notación bra-ket de Dirac*. Consultat el 10 de novembre de 2024, de https://la-mecanica-cuantica.blogspot.com/2009/08/la-notacion-bra-ket-de-dirac.html

[27] *Principio de superposición de estados.* (s. d.). Consultat el 10 de novembre de 2024, de https://web.ua.es/pt/cuantica/docencia/qce/teoria/node17.htm

[28] González, A. C. (s. d.). *Entrelazamiento: el mayor misterio de la física cuántica*. The Conversation. Consultat el 10 de novembre de 2024, de https://theconversation.com/entrelazamiento-el-mayor-misterio-de-la-fisica-cuantica-192075

coneixes la posició d'una partícula, menys precisament pots conèixer el seu moment (o velocitat), i viceversa[29].

Aquest principi explica per què no podem predir el comportament exacte d'una partícula, sinó només probabilitats, i juga un paper clau en el funcionament de l'aleatorietat en el nostre protocol quàntic BB84.

3.3.3.4. Quantificació d'energia

En la mecànica quàntica, l'energia no és contínua com en la física clàssica. L'energia d'un sistema es troba en valors quantificats, anomenats "quants". Això vol dir que les partícules, com els electrons en un àtom, no poden tenir qualsevol quantitat d'energia, sinó només certs valors concrets. Aquests electrons només poden orbitar el nucli en certs nivells d'energia específics. Quan un electró salta d'un nivell a un altre, emet o absorbeix una quantitat d'energia concreta en forma de llum (un fotó)[30].

Aquesta idea de l'energia quantificada és fonamental per explicar el funcionament dels nostres Qbits, ja que són en si "quants" concrets.

3.3.3.5. Dualitat ona-partícula

La dualitat ona-partícula diu que les partícules com els electrons i els fotons poden comportar-se tant com partícules (amb massa, ocupant un lloc concret) com ones (distribuïdes en l'espai, sense un lloc precís)[31].

A l'experiment de la doble escletxa, realitzat per primera vegada el 1801 per Thomas Young[32], si envies electrons un per un a través de dues escletxes, es comporten com a ones i formen un patró d'interferència (com les ones en l'aigua). Però si intentes mesurar per quina escletxa passa cada electró, es comporten com partícules i només passen per una escletxa, destruint el patró d'interferència. Això passa per

---

[29] *Heisenberg's uncertainty principle*. (2023, 30 gener). Chemistry LibreTexts. Consultat el 10 de novembre de 2024, de https://chem.libretexts.org/Bookshelves/Physical_and_Theoretical_Chemistry_Textbook_Maps/Supplemental_Modules_(Physical_and_Theoretical_Chemistry)/Quantum_Mechanics/02._Fundamental_Concepts_of_Quantum_Mechanics/Heisenberg%27s_Uncertainty_Principle

[30] *La cuantización de la energía*. (2024, 10 abril). Física Cuántica En la Red. Consultat el 10 de novembre de 2024, de https://www.fisicacuantica.es/la-cuantizacion-de-la-energia/

[31] *The wave-particle duality of photons*. (s. d.). Photon Terrace. Consultat el 10 de novembre de 2024, de https://photonterrace.net/en/photon/duality/

[32] Verde, A. P. (2022, 19 desembre). *El experimento de la doble rendija de Young y su explicación*. Astrométrico | la Web de Antonio Pérez Verde. Consultat el 10 de novembre de 2024, de https://astrometrico.es/2020/05/18/experimento-doble-rendija-explicacion/

que al mesurar les partícules les fem col·lapsar, és a dir, que les fem definir-se en un punt específic, fent que es comportin com partícules discretes.

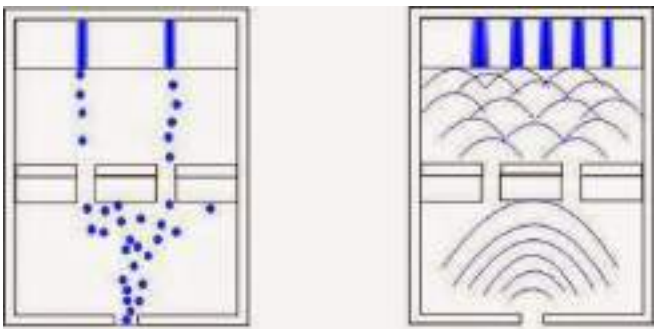

Figura 8: Experiment de la doble escletxa. Extreta de Steemit.

3.3.4. Superposició quàntica en una imatge

Per clarificar el concepte de superposició quàntica, essencial per entendre la criptografia quàntica, analitzarem una imatge que ho exemplifica a la perfecció.

Figura 9: Il·lustració “Kaninchen und Ente” (Ànec i Conill), publicada a *Fliegende Blätter* al 1892.

Aquesta famosa il·lusió òptica alemanya[33] presenta una imatge ambigua en la qual es poden percebre dues figures: un ànec o un conill, depenent de com s'observi.

Aquest fenomen és rellevant per al nostre estudi perquè ofereix una analogia visual potent amb el concepte de superposició quàntica. Igual que la imatge de l'ànec i el conill, que pot representar dues formes alhora fins que l'observador en determina

[33] Hase oder Ente? Was Sie sehen, verrät viel über Ihre Kreativität. (2022, 5 mayo). *FOCUS*. https://www.focus.de/panorama/optische-taeuschung-hase-oder-ente-was-sie-sehen-verraet-viel-ueber-ihre-kreativitaet_id_94477185.html

una, en el món quàntic una partícula pot existir en diversos estats simultàniament. Només quan s'observa, aquesta "decideix" en quin estat es manifesta, de manera similar a com l'observació de la imatge defineix si es veu un ànec o un conill.

3.3.5. Bombes Elitzur-Vaidman

L'experiment de les bombes d'Elitzur-Vaidman mostra com és possible detectar la presència d'una bomba extremadament sensible sense fer-la explotar, utilitzant els principis de la mecànica quàntica[34]. Aquest experiment es basa en la capacitat d'un fotó de seguir diversos camins simultàniament gràcies a la superposició quàntica.

Imagina que tens una bomba que explota al més mínim contacte, però vols saber si està activa sense que exploti. Per aconseguir-ho, es fa passar un fotó a través d'un interferòmetre de Mach-Zehnder[35], que divideix el fotó en dos camins, posant-ho en un estat quàntic, on el fotó és a dos camins alhora:

- Camí 1: Passa per la bomba.
- Camí 2: Evita la bomba.

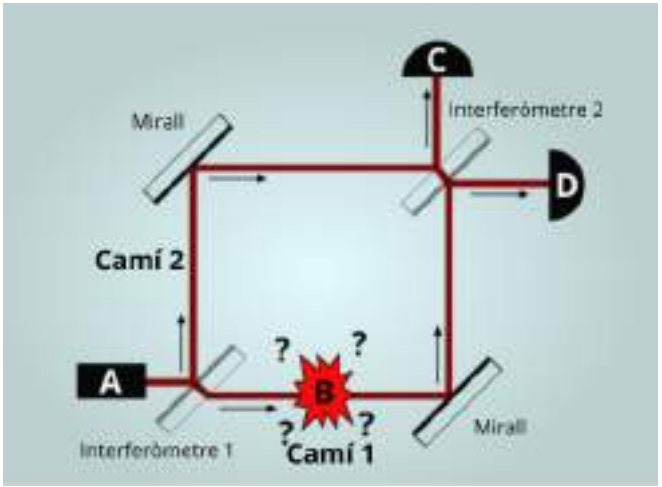

Figura 10: Esquema bombes Elitzur-Vaidman. Adaptada de Wikimedia Commons.

La idea és que si la bomba és activa, pot alterar el comportament del fotó i permetre que detectem la seva presència sense haver interaccionat directament amb ella.

---

[34] *The Elitzur–Vaidman Bomb-Testing method*. (2013, 25 agost). Azimuth. Consultat el 10 de novembre de 2024, de https://johncarlosbaez.wordpress.com/2013/08/24/the-elitzur-vaidman-bomb-testing-method/

[35] *Interferòmetre de Mach-Zehnder*. (2022, 11 juny). Viquipèdia. Consultat el 10 de novembre de 2024, de https://ca.wikipedia.org/wiki/Interfer%C3%B2metre_de_Mach-Zehnder

Suposem que utilitzem un fotó per a l'experiment, i estudiem dues situacions:

- La bomba és defectuosa (no explota, encara que hi passi el fotó).
- La bomba és activa (pot explotar si el fotó la toca).

Cas 1: La Bomba és Defectuosa

Si la bomba és defectuosa, el fotó pot viatjar sense cap interferència i segueix el seu camí normal dins de l'interferòmetre. Quan els dos camins es recombinen, les ones del fotó interfereixen i, gràcies al fet que les ones es combinen constructivament en C i destructivament en D (recordem la dualitat ona partícula), el fotó acaba sempre en un únic detector, el C.

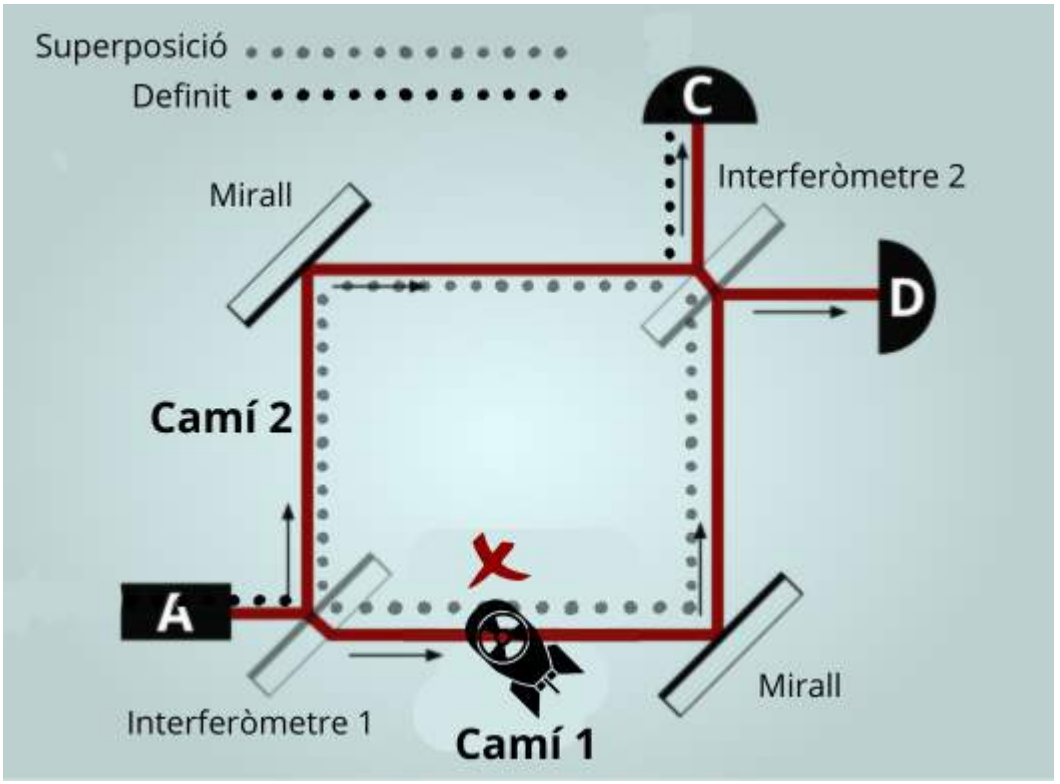

Figura 11: Cas on la bomba és defectuosa. Adaptada de Wikimedia Commons.

Això vol dir que si la bomba és defectuosa, el fotó segueix el patró esperat i només serà detectat en Detector C. No hem après res sobre la bomba, ja que es comporta com si no hi fos.

Cas 2: La Bomba és Activa

Quan la bomba és activa el fotó xoca amb la bomba i s'ha de definir en el camí 1 o 2, hi ha dues possibilitats:

1. El fotó col·lapsa en el camí 1, la bomba explota.

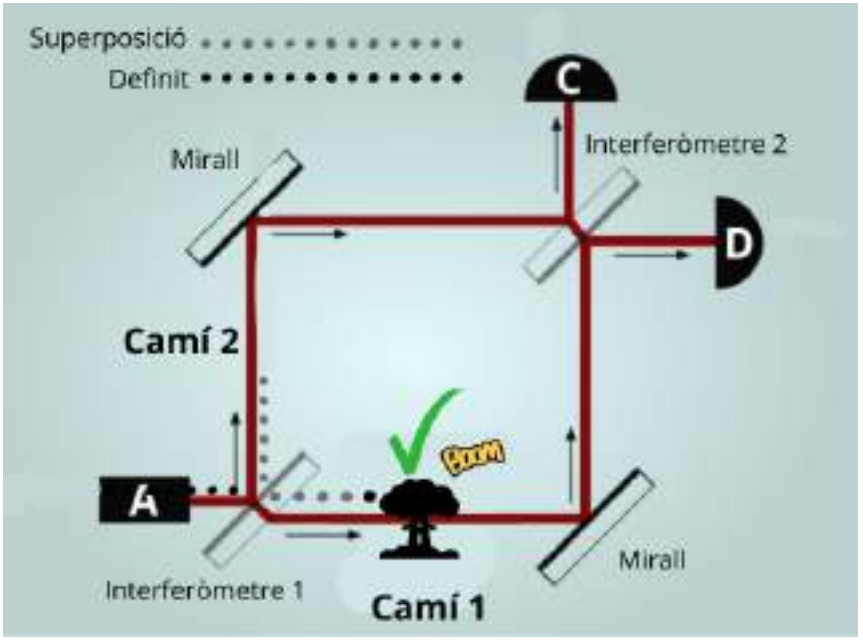

Figura 12: Cas on la bomba explota. Adaptat de Wikimedia Commons.

2. El fotó col·lapsa en el camí 2 i evita la bomba.

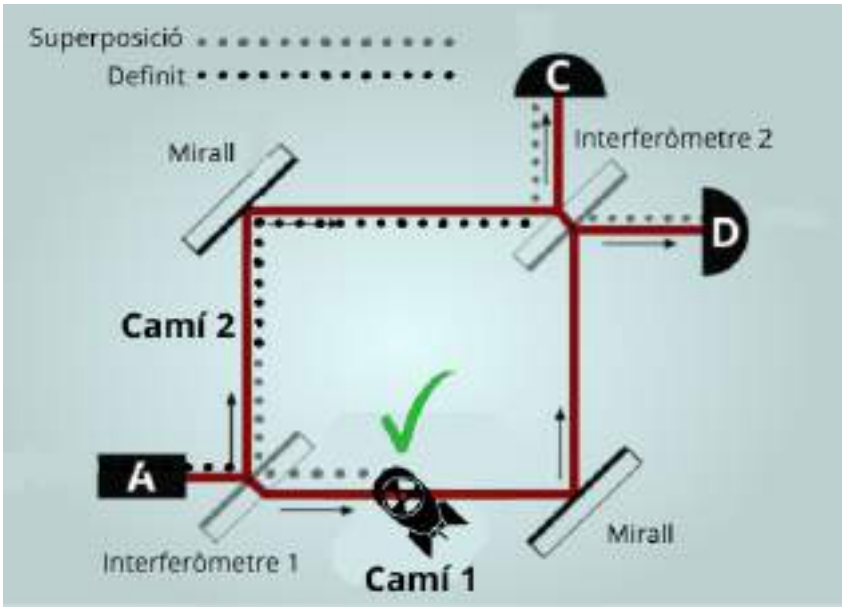

Figura 13: Cas on la bomba és activa i no explota. Adaptat de Wikimedia Commons.

El fet que la bomba estigui activa trenca la interferència quàntica. Això altera la distribució de probabilitats, i ara el fotó pot acabar tant en el Detector C com en el Detector D si ha col·lapsat en 2. Si es detecta en Detector D, podem concloure que la bomba és activa sense haver-la fet explotar. Pot ser detectada al detector D, ja que abans d'arribar als detectors (com es veu a l'esquema), hi ha un altre interferòmetre de Mach-Zehnder, que fa que hi hagi un 50% de probabilitats de què passi per un camí o altre.

Les taules de probabilitats són:

Taules 1 i 2: Probabilitats de l'experiment Elitzur-Vaidman.

	Bomba activa
Detector A	0.5*0.5=0.25 (25%)
Detector B	0.5*0.5=0.25 (25%)
Bomba explota	0.5 (50%)

	Bomba defectuosa
Detector A	1 (100%)
Detector B	0 (0%)
Bomba explota	0 (0%)

En aquest cas, el fotó té un 25% de probabilitat d'acabar en Detector D (ja que té un 50% de col·lapsar en 2 i, seguidament, un altre 50% d'anar a D), cosa que ens indica que la bomba està activa sense haver-hi interaccionat directament. També hi ha un 25% de probabilitat que el fotó es detecti en Detector C, com en el cas anterior, però en aquest cas no podem concloure res sobre l'estat de la bomba. A més hi ha una probabilitat del 50% que la bomba s'accioni, explotant el nostre laboratori, per això es considera un experiment mental.

Per tant, l'experiment d'Elitzur-Vaidman ens mostra que, en el món quàntic, podem obtenir informació sobre un sistema sense interaccionar directament amb ell. Utilitzant la mecànica quàntica, i gràcies a la probabilitat d'interferència quàntica, podem detectar si la bomba és activa simplement observant en quin detector es troba el fotó. Si es detecta al Detector D, sabrem que la bomba està activa, però sense fer-la explotar, la qual cosa resulta impossible des d'un punt de vista clàssic.

3.3.6. Preguntes “còmodes” i “incòmodes”

L'experiment de les bombes d'Elitzur-Vaidman exemplifica com podem obtenir informació sobre un sistema quàntic sense interaccionar-hi directament. Això ens porta a distingir entre preguntes còmodes i preguntes incòmodes (termes no científics) dins de la física quàntica, i aquesta distinció també és clau en la criptografia quàntica.

En el context quàntic, les preguntes còmodes es refereixen a situacions en què es mesura una partícula quàntica seguint la base correcta de mesura. Això permet obtenir informació sobre el sistema sense alterar el seu estat[36]. Per exemple, si una partícula està en superposició respecte a la seva posició i mesurem la seva velocitat, obtindrem el resultat correcte sense afectar a la posició d’aquesta. Aquest tipus de mesura és segur i no altera el sistema, proporcionant-nos informació "còmoda".

D'altra banda, les preguntes incòmodes sorgeixen quan fem la mesura d’allò que està en superposició. En aquest cas, el fet de mesurar la posició d'una partícula quàntica respecta la seva posició altera l'estat d’aquesta[36]. Això fa que la partícula col·lapsi a un nou estat i perdem la informació original. Aquesta mesura és "incòmoda" perquè no només no encertem la informació, sinó que també modifiquem l'estat quàntic de la partícula.

En relació amb la criptografia quàntica, veurem que depenent de quina base escullis per mesurar la polarització d’un fotó, aquest col·lapsarà o no. Es tractarà de preguntes “còmodes” i “incòmodes”

3.4. Criptografia quàntica

La criptografia quàntica és un sistema de seguretat en les comunicacions basat en els principis de la mecànica quàntica. A diferència dels mètodes clàssics de criptografia, que es fonamenten en problemes matemàtics difícils de resoldre (com la factorització de nombres grans[37]), la criptografia quàntica utilitza les propietats

[36] *Medición en la mecánica cuántica*. (2024, 18 setembre). Wikipedia. Consultat el 10 de novembre de 2024, de https://es.wikipedia.org/wiki/Medici%C3%B3n_en_la_mec%C3%A1nica_cu%C3%A1ntica

[37] *Taller de Criptografia*. (s. d.). Expediente 1. Consultat el 10 de novembre de 2024, de https://www.ugr.es/~aquiran/cripto/expedien/exped001.htm

intrínseques de les partícules quàntiques, com els fotons, per garantir la seguretat de la informació.

El principal avantatge de la criptografia quàntica és que ofereix una seguretat inquebrantable gràcies a dos conceptes fonamentals:

1. Superposició quàntica: Les partícules, com els fotons, poden existir en múltiples estats simultàniament fins que són observades. En el context de la criptografia quàntica, això permet crear claus de seguretat que són inaccessibles fins que són llegides.
2. Principi d'incertesa de Heisenberg: Un altre aspecte clau és que qualsevol intent de mesurar l'estat d'una partícula quàntica altera inevitablement aquest estat. Això significa que, si algú intenta interceptar la clau quàntica durant el seu enviament, aquesta serà immediatament alterada, i els dos usuaris (el transmissor i el receptor) s'adonaran de l'atac.

La implementació més coneguda de la criptografia quàntica és el protocol BB84, desenvolupat per Charles Bennett i Gilles Brassard el 1984[38]. Aquest protocol permet l'intercanvi de claus segures entre dos usuaris mitjançant fotons. Si es detecta qualsevol interferència durant la transmissió, la clau s'abandona i se'n crea una de nova, assegurant la seguretat de la comunicació.

En resum, la criptografia quàntica no es basa en la dificultat matemàtica, sinó en les lleis fonamentals de la física. Això la converteix en un sistema teòricament invulnerable als atacs informàtics convencionals, incloent-hi els futurs ordinadors quàntics, que podrien trencar els sistemes de criptografia clàssics en qüestió de minuts. Tot i que encara està en desenvolupament, la criptografia quàntica representa un avenç revolucionari en la seguretat de les comunicacions.

[38] Fran. (2007, 17 gener). *Criptografia: Protocolo de distribución de clave BB84*. Gaussianos. Consultat el 10 de novembre de 2024, de https://www.gaussianos.com/criptografia-protocolo-de-distribucion-de-clave-bb84/

3.4.1. Clàssic o quàntic: les diferències entre un bit i un qbit

Un dels aspectes més fonamentals per entendre la criptografia quàntica és la diferència entre el bit clàssic, que és la unitat bàsica d'informació en la computació tradicional, i el Qbit, que és la unitat d'informació de la computació quàntica.

Un bit[39] és la unitat bàsica d'informació en la computació clàssica i només pot tenir dos valors: 0 o 1. Cada operació en un ordinador clàssic es basa en aquestes dues opcions, que representen els dos estats possibles en un sistema binari.

Per exemple, si tenim 8 bits, podem representar 256 combinacions diferents de 0s i 1s (2^8), però cada bit només pot estar en un dels dos estats en qualsevol moment.

Per altra banda, un Qbit[40] és la unitat bàsica d'informació en un sistema quàntic. A diferència d'un bit clàssic, un Qbit pot estar en múltiples estats simultàniament gràcies a la superposició quàntica. Això significa que un Qbit no només pot ser 0 o 1, sinó també qualsevol combinació dels dos estats alhora.

Un qbit pot estar en una superposició d'estats 0 i 1. Això vol dir que, fins que no sigui mesurat, el qbit existeix en una barreja de tots dos estats. Només en el moment de la mesura col·lapsa en un dels dos.

Imagina una moneda que pots llençar. Un bit és com una moneda que ja ha caigut i es troba en una cara (cara o creu), mentre que un Qbit és com una moneda que està girant en l'aire: encara no saps si serà cara o creu fins que no la miris, però mentre gira, pot estar en una barreja dels dos estats.

[39] *¿Qué es un Bit?* (2020, 28 setembre). JVS Informática Blog. Consultat el 10 de novembre de 2024, de https://www.jvs-informatica.com/blog/glosario/bit/

[40] Voorhoede, D. (s. d.). *What is a qubit?* Quantum Inspire. Consultat el 10 de novembre de 2024, de https://www.quantum-inspire.com/kbase/what-is-a-qubit/

3.4.2. El canal de comunicació quàntic

Per poder fer qualsevol intercanvi d'informació, en qualsevol àmbit, es necessita un canal.

En el cas de la criptografia quàntica, necessitem un canal on puguin passar els nostres Qbits, en forma de fotons polaritzats en el cas del protocol BB84.

Com que els Qbits no poden ser llegits sense alterar-los, el canal ha d'estar completament aïllat per evitar qualsevol interferència o pèrdua d'informació. Això significa que l'aire no és una opció adequada. Per sort, hi ha un medi que compleix aquests requisits i que ja s'utilitza àmpliament en les telecomunicacions modernes: la fibra òptica.

Què és la polarització de la llum?

La polarització de la llum és el fenomen pel qual les ones de llum oscil·len en una sola direcció o pla[41]. Normalment, la llum natural (com la del Sol) es compon d'ones que vibren en totes direccions perpendiculars al seu trajecte. Però quan la llum està polaritzada, aquestes vibracions s'alineen en un sol pla.

Una de les maneres més senzilles de polaritzar la llum és amb l'ús de filtres polaritzadors[42]. Aquests filtres només permeten el pas de les ones que vibren en una direcció específica i bloquegen les altres. Per exemple, un filtre polaritzador orientat verticalment només deixarà passar les ones que oscil·len verticalment, bloquejant les que oscil·len horitzontalment. Si s'utilitzen dos filtres polaritzadors orientats perpendicularment entre si, bloquejaran tota la llum que intenti travessar-los.

Com funciona la fibra òptica?

La fibra òptica és un material, generalment fet de vidre o plàstic, que funciona gràcies al principi de la reflexió total interna[43]. Quan un raig de llum (o un fotó) entra

[41] *Introduction to Polarization*. (s. d.). Edmund Optics. Consultat el 10 de novembre de 2024, de https://www.edmundoptics.es/knowledge-center/application-notes/optics/introduction-to-polarization/

[42] *Polarizing filters*. (2020, 18 juny). Science World. Consultat el 10 de novembre de 2024, de https://www.scienceworld.ca/resource/polarizing-filters/

[43] *Total internal reflection*. (s. d.). Consultat el 10 de novembre de 2024, de http://hyperphysics.phy-astr.gsu.edu/hbasees/phyopt/totint.html

en el nucli de la fibra i arriba a la vora entre el nucli i el revestiment (també de vidre o plàstic, però amb un índex de refracció diferent), si l'angle és prou pronunciat, el raig es reflecteix en lloc de travessar el revestiment. Això permet que la llum viatgi llargues distàncies sense escapar-se del nucli, mantenint-se confinada dins la fibra.

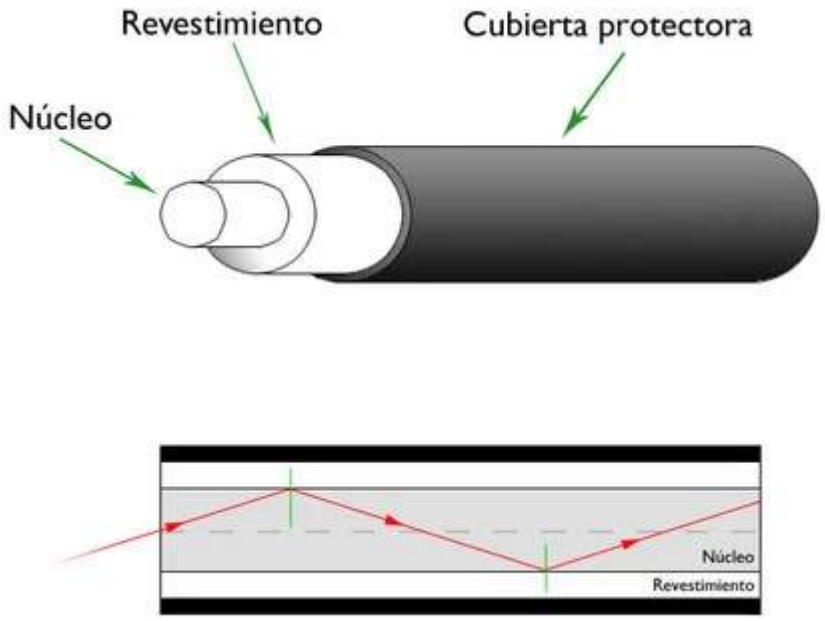

Figura 14: Funcionament fibra òptica. Extreta de XatakaHome.

Aquest fenomen fa que els fotons enviats a través de la fibra òptica es moguin d'un punt a un altre amb molt poca pèrdua, sense interaccions amb l'exterior, cosa que la converteix en el medi ideal per transportar Qbits.

Per comprovar aquest principi, hem dut a terme un petit experiment que simula el funcionament de la fibra òptica. Pots trobar els detalls al següent apartat.

Mitjançant una fibra òptica perfecta, podem enviar fotons un a un de manera segura i sense que interaccionin amb res. Això és molt important per mantenir la seguretat de les comunicacions en criptografia quàntica.

3.4.3. Fibra òptica

Per exemplificar el funcionament de la fibra òptica, faré un experiment molt senzill que tothom pot realitzar amb una moneda, un got i aigua.

L'experiment consisteix a posar una moneda sota el got, i mirant el got des del costat o des de dalt, veiem la moneda. Si emplenem el got d'aigua la moneda no es veurà des dels costats sinó que solament des de dalt, tal com passa amb la fibra òptica.


Figures 15 i 16: Got buit (esquerre) i got ple (dreta).

Podem observar la moneda a la primera imatge, amb el got buit, i no la podem veure a la segona imatge, amb el got ple d'aigua. Pots consultar un vídeo de la realització als apèndixs.

3.4.3. Intercanvi de claus

Com he mencionat anteriorment, la criptografia quàntica (especialment el protocol BB84) es basa en l'intercanvi segur de claus, un procés que permet generar un codi binari que només coneixen els dos comunicants amb una certesa gairebé absoluta. Aquesta clau es fa servir per encriptar un missatge binari, que després es pot enviar per un canal no segur. És indiferent quin canal s'utilitzi per enviar el missatge, ja que aquest només es pot desxifrar correctament amb la clau compartida.

Fins i tot si un tercer intentés interceptar el missatge i intentar desxifrar-lo mitjançant força bruta (provar totes les combinacions possibles), només aconseguiria generar totes les possibles variacions del missatge amb el mateix nombre de dígits, però sense la clau correcta, cap d'aquestes variacions seria útil. Això es deu al fet que el codi binari resultant només és interpretable per aquells que tenen la clau.

La generació d'aquesta clau quàntica es basa, naturalment, en els principis fonamentals de la mecànica quàntica, com la superposició i el principi d'incertesa de Heisenberg, que garanteixen que qualsevol intent d'intercepció sigui detectat immediatament.

Per a una explicació pràctica més detallada, pots consultar l'apartat 4.2, on es presenta una simulació molt propera a la realitat que mostra el procés de generació d'aquesta clau mitjançant un experiment pràctic.

3.4.4. Xifratge del missatge

Per tal d'enviar el missatge a través d'un canal no quàntic i no segur (que pot ser des d'un correu electrònic fins a una publicació a qualsevol xarxa social), cal encriptar-lo de manera que només qui conegui la clau pugui entendre el missatge real.

Generem la clau com s'ha explicat a l'apartat anterior. Sabem que aquesta clau només és coneguda per l'Alice i el Bob i, per tant, codificarem el missatge utilitzant-la.

- Exemple d'encriptació amb XOR

Suposem que la clau generada té 8 dígits (en la pràctica, la clau sol ser molt més llarga, preferiblement de la mateixa longitud que el missatge, però per a aquest exemple utilitzarem 8 dígits). Aquesta clau és aleatòria i no té cap significat en si mateixa. Imaginem que la clau generada és: 00101101

També suposem que el nostre missatge és un codi de seguretat d'un cadenat, que en aquest cas és 3658. Per codificar aquest codi, primer el convertirem a binari utilitzant el sistema BCD[44] (Binary-Coded Decimal), on cada dígit decimal es converteix en el seu equivalent binari de quatre dígits: 3658 → 0011 0110 0101 1000

[44] *What is BCD?* (2023, 30 novembre). Consultat el 10 de novembre de 2024, de https://store.omron.co.nz/knowledge-base/what-is-bcd?srsltid=AfmBOoqPU7nmjZgNptgfj5pNxW12JyFwzwMeFOz9T93oQZZFa6i_vnoR

Ara codificarem aquest missatge utilitzant l'operació lògica binària XOR[45]. El XOR (o "Exclusive OR") funciona comparant dígit a dígit la clau amb el missatge. Si els dígits són iguals, el resultat és 0; si són diferents, el resultat és 1. Si la clau no és prou llarga, simplement es repeteix fins a completar la longitud del missatge.

- Operem

Taula 3: Operació XOR de codificació.

	Dígit 1	Dígit 2	Dígit 3	Dígit 4
Codi cadenat	0011	0110	0101	1000
Clau generada	0010	1101	0010	1101
Resultat	0001	1011	0111	0101

Aquest nou codi (0001 1011 0111 0101) és el missatge encriptat, que es pot enviar pel canal no segur. Només Bob, que té la mateixa clau, podrà desxifrar-lo aplicant de nou l'operació XOR per recuperar el codi original.

- Desxifrat del missatge

Per desxifrar el missatge, Bob aplica la mateixa operació XOR al codi encriptat utilitzant la mateixa clau:

[45] Jacabrera. (2024, 8 febrer). *Compuerta lógica XOR*. iElectel. Consultat el 10 de novembre de 2024, de https://ielectel.com/compuerta-logica-xor/

Taula 4: Operació XOR de descodificació.

	Dígit 1	Dígit 2	Dígit 3	Dígit 4
Codi encriptat	0001	1011	0111	0101
Clau generada	0010	1101	0010	1101
Resultat	0011	0110	0101	1000

El resultat és el codi original en BCD: 0011 0110 0101 1000, que es tradueix novament en 3658.

Aquest procés garanteix que, fins i tot si algú intercepta el missatge, no podrà desxifrar-lo sense la clau correcta.

3.4.5. Criptografia post-quàntica

La criptografia quàntica, com ja s'ha mencionat anteriorment, s'utilitza principalment per protegir les nostres dades davant de l'amenaça dels futurs ordinadors quàntics, que seran capaços de trencar els mètodes criptogràfics actuals, com ara els basats en la factorització de nombres grans.

Ara bé, per què necessitem utilitzar fotons polaritzats per protegir la informació? No seria possible adaptar els sistemes criptogràfics actuals per resistir als ordinadors quàntics?

La resposta és: sí, és possible. Es poden dissenyar sistemes de criptografia basats en problemes matemàtics que, fins i tot per a un ordinador quàntic, serien molt difícils de resoldre. A aquest tipus de criptografia se l'anomena criptografia post-quàntica[46]. El nom no es refereix a una criptografia que ve després de la criptografia quàntica, sinó que fa referència a la criptografia que s'utilitzarà després de l'aparició dels ordinadors quàntics.

[46] Clyde, R., & Gillis, A. S. (2023, 5 abril). *post-quantum cryptography*. Search Security. Consultat el 10 de novembre de 2024, de https://www.techtarget.com/searchsecurity/definition/post-quantum-cryptography

La criptografia post-quàntica no es basa en la física quàntica, sinó en la millora dels mètodes criptogràfics clàssics. Això significa que utilitza problemes matemàtics encara més complexos que la factorització de nombres grans, com un problema de xarxes, que consisteix a trobar el vector no zero més curt dins d'una xarxa per protegir les dades[47]. Tot i que encara es troba en fase de recerca i desenvolupament, és una de les solucions proposades per resistir els atacs dels ordinadors quàntics.

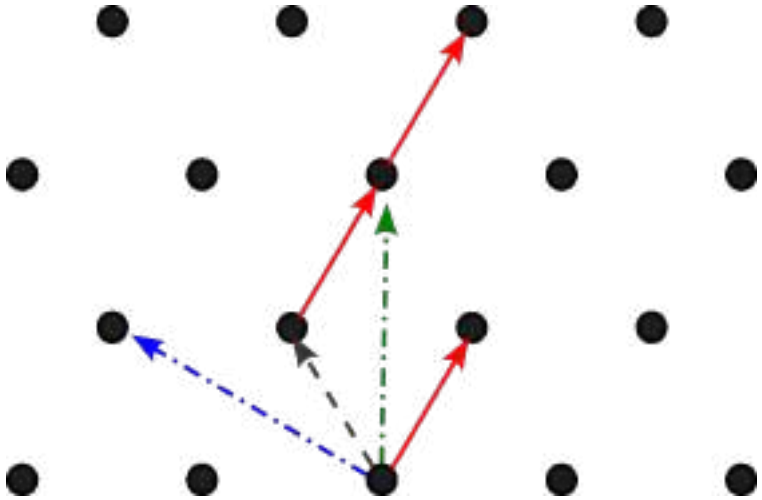

Figura 17: Problema de xarxes. Extreta de Redhat.

No obstant, aquest treball se centra en la criptografia quàntica, però és important esmentar la criptografia post-quàntica, ja que, tot i funcionar de manera diferent, ambdues tecnologies tenen el mateix objectiu: protegir les dades en un futur on els ordinadors quàntics siguin capaços de desxifrar els sistemes actuals.

3.5. Futures aplicacions

Per aquesta part del meu treball, centrada en el futur de la criptografia quàntica, he tingut l'oportunitat de realitzar dues entrevistes a experts de camps relacionats amb la informàtica i la física quàntica. La primera entrevista és amb l'Oscar Torrente, professor d'informàtica a l'Institut Puig Castellar, i la segona amb el Pere Mujal Torreblanca, doctor en Física per la Universitat de Barcelona i actual investigador al grup de Quantum Information Theory (QIT) de l'Institut de Ciències Fotòniques (ICFO)[48].

[47] Bernstein, D., Lange, T. Post-quantum cryptography. *Nature* 549, 188–194 (2017). https://doi.org/10.1038/nature23461
[48] ICFO. (2022, 13 juny). *Interest | ICFO*. https://www.icfo.eu/interest/105/quantum-information-theory/11/

Aquests dos perfils ofereixen perspectives complementàries sobre el futur de la criptografia quàntica. Mentre que el professor Torrente pot aportar una visió enfocada en les aplicacions pràctiques i els reptes tecnològics, el doctor Mujal Torreblanca, des de la seva experiència en la recerca teòrica, pot aprofundir en les possibilitats i límits de les tecnologies quàntiques a llarg termini.

L'objectiu final d'aquestes entrevistes és comparar ambdues perspectives i intentar fer una predicció sobre com evolucionarà la criptografia quàntica en un futur pròxim.

3.5.1. Entrevista a professor d'informàtica

L'entrevista amb l'Oscar Torrente, professor d'informàtica a l'Institut Puig Castellar de Santa Coloma de Gramenet, va tenir un to més informal del que havia planejat inicialment. Es va dur a terme en un entorn públic amb cert soroll ambiental, la qual cosa va fer impossible registrar l'àudio de la conversa.

No obstant això, vaig poder prendre notes detallades de les seves respostes per tal de capturar el seu punt de vista i incloure'l en aquest treball. A continuació, presento les seves idees i la seva opinió entorn la criptografia quàntica.

L'Oscar creu que la criptografia quàntica no és del tot necessària tenint un bon desenvolupament de la criptografia post-quàntica, ja que aquesta ja fa el treball de protegir les nostres comunicacions de l'arribada dels ordinadors quàntics, amb l'avantatge que utilitza el mateix tipus de tecnologia que la criptografia actual, fent més fàcil la seva integració. Encara que no descarta la idea de tindre un canal de criptografia quàntica per a comunicacions molt importants de nivell internacional.

En conclusió, l'Oscar dona una visió una mica contrària al desenvolupament d'aquesta nova tecnologia, ja que creu que amb la criptografia post-quàntica donarà la suficient protecció contra els ordinadors quàntics i, per tant, un canvi de paradigma en l'estil de criptografia, afegint-hi el cost elevat que té implementar-la, és innecessari.

3.5.2. Entrevista a investigador postdoctoral del QIT

L'entrevista amb en Pere Mujal Torreblanca, investigador del grup de Quantum Information Theory (QIT) de l'Institut de Ciències Fotòniques (ICFO), es va realitzar a les instal·lacions del mateix institut. Aquesta entrevista es va poder enregistrar en àudio, disponible a l'apèndix del treball.

A continuació, presento els punts més rellevants de l'entrevista.

Amb el Pere vam conversar sobre del grup de treball QIT, enfocant el tema a la subvenció que reben per fer les investigacions. Va recalcar que sobretot les fonts eren o europees o fonts obtingudes de beques, amb molt poc percentatge de la indústria privada.

Vam profunditzar en el grup de recerca sobre la criptografia quàntica del QIT, sobre què estudia i quines limitacions actuals hi ha. En general, aquest grup estudia nous mètodes i protocols més eficients, ja que el protocol BB84 té bastants manqueses en posar-ho en pràctica. A més va mencionar un experiment que es va fer aproximadament fa dos anys en què van connectar un cable de fibra òptica des de l'ICFO fins a un radi de 2 km i van passar fotons en estat quàntic. La tassa d'error dels fotons era molt baixa i acceptable per a establir una comunicació amb criptografia quàntica.

Profunditzant en la comparació de la quàntica amb la post-quàntica, el Pere opina que la criptografia quàntica és una bona tecnologia capaç de protegir la informació més sensible en termes governamentals o internacionals, encara que és conscient que la criptografia post-quàntica pot assolir el mateix resultat, creu que una combinació de les dues podria ser ideal, baixant encara més la petita tassa d'error que puguin tenir aquests dos mètodes.

En conclusió, el Pere ofereix un punt de vista esperançador sobre el futur de la criptografia quàntica, destacant el seu potencial per protegir comunicacions confidencials, tot i que el seu ús encara es limitarà a àmbits on realment valgui la pena invertir grans recursos econòmics. A més, el Pere no descarta la rellevància de la criptografia post-quàntica i, de fet, proposa la combinació de tots dos mètodes com a estratègia per augmentar la seguretat.

4. Marc pràctic

4.1. Computació quàntica

Per mesurar el grau de fiabilitat que té actualment un sistema quàntic, com per exemple un ordinador quàntic o fotons en superposició, he enviat un programa a l'ordinador quàntic superconductiu del Centre per a la Informació i Biologia Quàntica, a Osaka, Japó[49].

Aquest programa és un algorisme format per portes lògiques quàntiques conegut com algorisme de Grover[50]. En aquest cas, el programa sempre donarà, en teoria, la sortida 11.

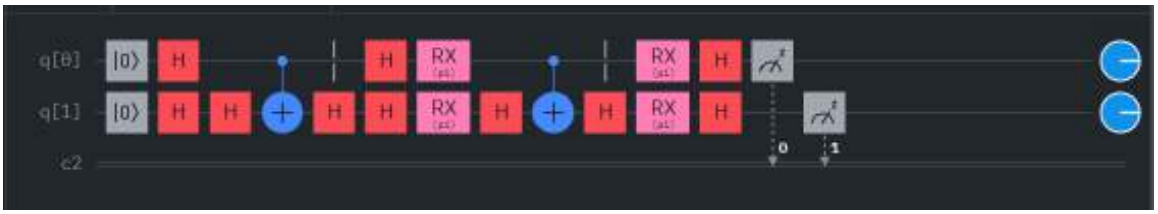

Figura 18: Algorisme de Grover. Captura de pantalla del programa IBM Quantum Computing.

Amb un càlcul teòric, en % sobre 1024 intents, el 100% de les vegades la sortida és 11:

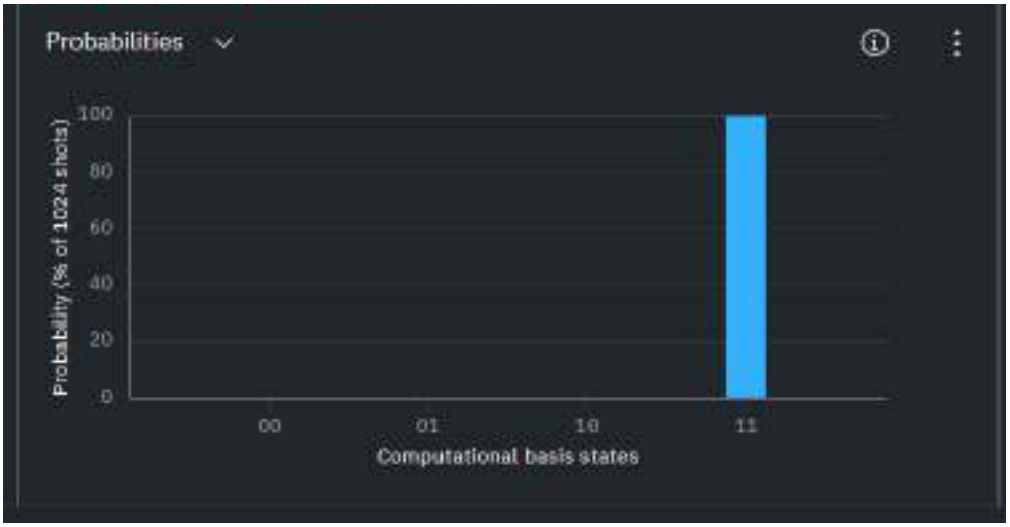

Figura 19: Probabilitat teòrica per a la sortida de l'algorisme de Grover. Captura de pantalla del programa IBM Quantum Computing.

[49] *About Us | QIQB: Center for Quantum Information and Quantum Bilogy, Osaka University*. (s. d.). https://qiqb.osaka-u.ac.jp/en/about-us/

[50] *Grover's algorithm.* (s. d.). IBM Quantum Learning. Consultat el 10 de novembre de 2024, de https://learning.quantum.ibm.com/course/fundamentals-of-quantum-algorithms/grovers-algorithm

Posem en pràctica aquest programa, executant-lo 1000 vegades, per comprovar el percentatge d'error sobre el càlcul teòric.

Podem comprovar com (mostrat a la següent imatge) no sempre, experimentalment, aquest programa ens dona la sortida 11. Això passa per errors dins de la computació quàntica, ja que una mínima variació de temperatura pot interferir dràsticament en el resultat.

El nombre de vegades que la sortida ens dona 11 és de 923 vegades, sobre 1000 intents. Això vol dir que un 92,8% de les vegades, l'ordinador quàntic ha funcionat amb normalitat, i que un 7,2% de les vegades, l'ordinador ha fallat.

Havent trigat 3s en executar el programa 1000 vegades, podem deduir que per programes senzills com aquest no suposen gaire problema, ja que l'executem moltes vegades i agafem el resultat que més s'apropi probabilísticament a l'esperat.

No obstant, amb la criptografia quàntica no passa el mateix, ja que cada Qbit compta per la generació de la clau (recordem que, com que van numerats, amb la sola pèrdua d'un fotó, descoordinaríem les bases corresponents).

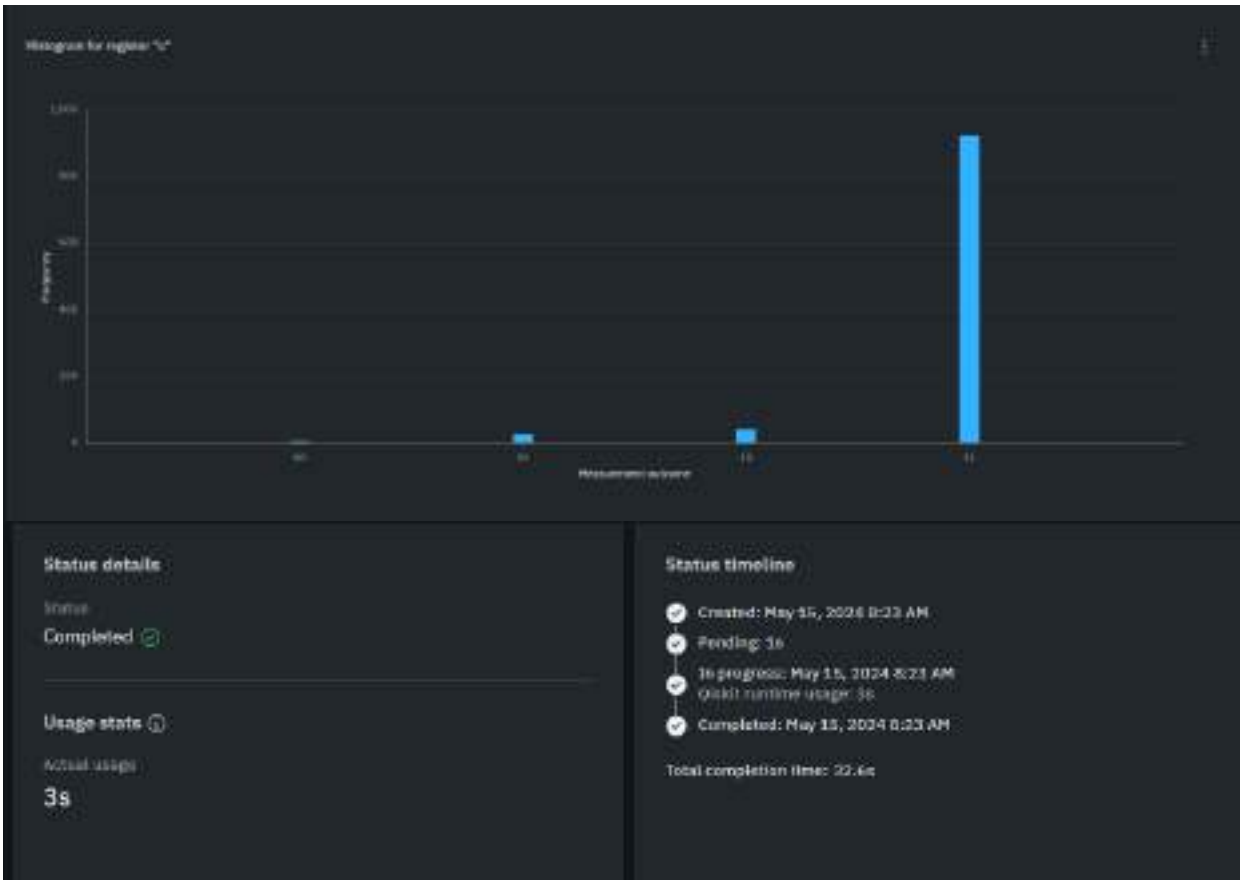

Figura 20: Resultats reals de l'algorisme de Grover. Captura de pantalla del programa IBM Quantum Computing.

Per tant, aquesta comprovació ens fa veure que, encara que sobre paper, la criptografia quàntica és perfecta, encara té bastants errors que resoldre.

4.2. Criptografia quàntica

Per tal d'entendre millor com es genera la clau de la criptografia quàntica, realitzarem una simulació. Els recursos necessaris per generar paquets d'un sol fotó i detectar la seva polarització són actualment molt difícils d'aconseguir i tenen un cost elevat. Per això, utilitzarem una simulació simplificada on la llum polaritzada es representa amb molts fotons alhora, i els participants de la simulació seran persones que actuen com a màquines que automatitzen el procés. Aquesta simulació es basa en una idea extreta del programa "Bojos per la Física" de la Fundació La Pedrera, la qual he adaptat per al meu treball de recerca.

La simulació implementa el protocol BB84, un dels protocols més coneguts en criptografia quàntica. Aquest protocol permet l'intercanvi de bits (que es representen

com paquets de fotons a gran escala) per establir una clau de xifrat segura i intercanviar missatges xifrats a través de canals no segurs.

Per poder mostrar la seguretat antiespionatge del protocol BB84, repetirem la simulació amb un espia, que simularà l'aleatorització dels Qbits després de haver estat llegits amb una base errònia.

4.2.1. Materials i entorn

Els materials necessaris per realitzar aquesta simulació són:

- Una font de llum
- 5 filtres polaritzadors de 5x5 cm
- 1 filtre polaritzador de 10x10 cm
- Dues ulleres sense vidres (per col·locar els filtres polaritzadors)
- Papers i 2 bolígrafs
- 5 participants

L'entorn de la simulació ha de ser un espai fosc, tot i que no cal que sigui completament negre. L'important és evitar fonts de llum directa. També és recomanable que l'espai sigui silenciós per evitar malentesos o errors en la comunicació entre els participants.

4.2.2. Preparació

Abans de fer la simulació com a tal hem de preparar els materials i revisar que tot funcioni bé.

Les ulleres han de tenir filtres polaritzadors col·locats en quatre angles diferents: 90º, 0º, 45º i 135º. Cada espai destinat a les lents de les ulleres tindrà un filtre diferent (mostrat a les imatges respectivament).

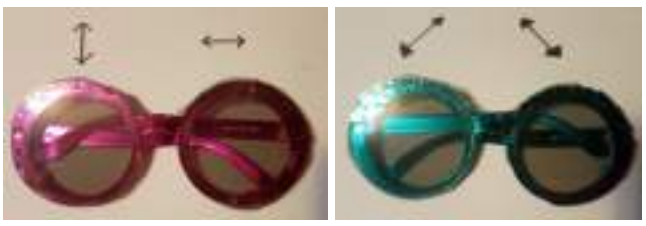

Figura 21: Ulleres amb filtres polaritzadors.

Per assegurar-nos que els filtres estan correctament alineats, superposarem un filtre polaritzador sobre un altre amb una polarització contrària. Si els filtres estan ben col·locats, la llum haurà de ser completament bloquejada, opacant la visió (mostrat a les imatges).

Figura 22, 23, 24 i 25: Comprovació de filtres polaritzadors.

Si no hi ha cap error s'hauria d'opacar el filtre analitzat, com a les imatges.

Es preparen dues taules idèntiques, una per a cada comunicador (Alice i Bob). Cadascun apuntarà els resultats obtinguts durant la simulació, registrant la base (representada per "+" o "x") i el bit corresponent (0 o 1). Aquestes taules hauran de tenir tantes fileres com bits es vulguin enviar durant la simulació.
Un exemple de taula sense emplenar i emplenada, respectivament.

Taules 5 i 6: Exemples de taules Alice i Bob; sense emplenar i emplenades, respectivament.

BASE	BIT

BASE	BIT
+	0
×	0
×	1
+	0

Per últim, hem de trobar un lloc que ofereixi els requisits per realitzar la simulació, la meva elecció és una aula de l'Institut Puig Castellar a la tarda, quan és buit.

4.2.3. La simulació

Un cop tenim tot el material preparat i les taules a punt, el següent pas és definir els rols de cada participant i establir com es representarà cada angle de polarització mitjançant bits.

En la simulació, hi ha cinc rols diferents, cadascun amb una funció específica:

1. Alice: l'Alice (l'emissor) és el participant encarregat de generar i enviar els BITs (representant els Qbits) utilitzant la font de llum i els filtres polaritzadors. Aquest rol simula l'emissió de fotons en una base polaritzada, que escull aleatòriament entre les bases rectes (0º o 90º) o diagonals (45º o 135º).

2. Receptor perpendicular: el receptor perpendicular mesura els fotons enviats per l'Alice utilitzant una base recta, és a dir, 0º o 90º. Intenta detectar la polarització dels fotons segons la base que escull, però si la seva base no coincideix amb la de l'Alice, aleatoritza el resultat.

3. Receptor diagonal: aquest receptor mesura els fotons utilitzant una base diagonal, és a dir, 45º o 135º. Igual que amb la base perpendicular, la seva mesura pot no coincidir amb la de l'Alice i generar una aleatorietat.

4. Bob: el Bob és el participant que genera les bases aleatòries dels receptors, és a dir, escull aleatòriament qui rep cada bit, si el receptor perpendicular o el diagonal. A més anota els resultats a la taula prèviament preparada.

5. Espia: l'espia intenta interceptar els bits durant la transmissió. Mesura els fotons amb una base aleatòria, i les seves accions poden alterar la informació, fent que l'Alice i el Bob detectin la presència d'un espia si hi ha discrepàncies als resultats.

Els rols van ser assignats de manera aleatòria, per tal de simular un entorn de comunicació i seguretat més natural.

En aquesta simulació, els angles de polarització dels filtres es representen com a bits, seguint el protocol BB84. Els bits es defineixen de la següent manera:

- Base recta:
    - 0º es representa amb el bit 0.
    - 90º es representa amb el bit 1.
- Base diagonal:
    - 45º es representa amb el bit 0.
    - 135º es representa amb el bit 1.

Ara que ho hem posat tot en ordre i tothom sap el que ha de fer, començarem. La primera simulació es farà sense espia. A continuació una fotografia feta just abans de començar la simulació:

Figura 26: Escenari de la simulació. Alice (dreta) i Bob (esquerra).

4.2.3.1. Simulació sense espía

1. Selecció de bases i bits:
    - L'Alice escull aleatòriament les bases que utilitzarà per enviar els bits (base recta: 0º o 90º; o base diagonal: 45º o 135º). La quantitat de bases escollides ha de coincidir amb el nombre de bits que es volen comunicar. En aquesta simulació vam utilitzar 10 bits.
    - A més, selecciona també de manera aleatòria els bits (0 o 1) que vol enviar, sense necessitat de tenir cap significat concret, ja que l'objectiu és generar una clau aleatòria per xifrar un missatge.
    - Paral·lelament, el Bob escull bases aleatòriament per a cada bit que ha de rebre.

Les taules van quedar així:

Alice

nº	Base	Bit
1	+	1
2	+	0
3	+	0
4	x	1
5	x	1
6	x	0
7	+	0
8	+	1
9	+	0
10	x	0

Bob

nº	Base	Bit
1	x	
2	x	
3	x	
4	+	
5	+	
6	x	
7	+	
8	+	
9	x	
10	x	

Taules 7 i 8: Eleccions de bases i bits abans de la transmissió.

Podem notar que, com les bases de l'Alice i d'en Bob s'han generat aleatòriament, n'hi ha que no coincideixen; seran els bits que descartarem.

2. Enviament dels bits:
    - L'Alice comença a enviar els bits utilitzant una llanterna amb un filtre polaritzador segons la base que ha seleccionat per a cada bit.
    - El Bob indica quin receptor ha de rebre el bit en funció de la base seleccionada aleatòriament:
        - Si ha escollit una base recta, el receptor perpendicular serà qui hagi de rebre el bit.
        - Si ha escollit una base diagonal, el receptor diagonal serà l'encarregat de rebre el bit.
3. Recepció dels bits:
    - Quan el receptor rep el bit, pot observar tres situacions diferents:
        - Si veu la llum només per l'ull dret, comunica al Bob que ha rebut un bit 1.
        - Si veu la llum només per l'ull esquerre, comunica al Bob que ha rebut un bit 0.
        - Si veu la llum per tots dos ulls, vol dir que la mesura és incerta i, per tant, comunica un bit aleatori (0 o 1). Aquest és el cas en què les bases no coincideixen, i en realitat, seria el Qbit el que col·lapsaria en un estat aleatori.
    - Aquest procés es repeteix tantes vegades com bits es vulguin enviar, i l'Alice canvia de base per a cada bit.

La taula de l'Alice no canvia, ja que únicament envia les dades, però la del bob ja té plena la columna de bit, i queda així:

Taula 9: Bits rebuts pel Bob.

nº	Base	Bit
1	x	1
2	x	1
3	x	1
4	+	0
5	+	0
6	x	1
7	+	1
8	+	1
9	x	1
10	x	0

4. Comparació de les bases:
    - Quan tots els bits han estat enviats, tant l'Alice com el Bob publiquen les bases que han utilitzat per a cada bit.
    - Les bases de l'Alice es comparen amb les bases escollides pel Bob. Si les bases no coincideixen, els bits corresponents es descarten, ja que són aleatoris. Per exemple, si al bit número 3 l'Alice ha triat una base recta i el Bob ha utilitzat una base diagonal, aquest bit es considera invàlid i no forma part de la clau.
    - Els bits en què les bases de l'Alice i el Bob han coincidit es conserven, i aquests formen la clau secreta.

En la nostra simulació, queda així:

Alice Bob

Taules 9, 10 i 11: Comparacions bases Alice i Bob.

nº	Base	Bit
1	+	0
2	+	0
3	+	1
4	x	0
5	x	0
6	x	1
7	+	1
8	+	1
9	+	0
10	x	0

nº	Base	Bit
1	x	1
2	x	1
3	x	1
4	+	0
5	+	0
6	x	1
7	+	1
8	+	1
9	x	1
10	x	0

La base coincideix?
No
No
No
No
No
Si
Si
Si
No
Si

Un cop s'ha completat l'enviament i recepció dels bits, l'Alice i el Bob comparteixen una clau secreta, formada pels bits en què les bases escollides han coincidit. El nombre de bits d'aquesta clau pot variar, ja que depèn del nombre de vegades que les bases han estat les mateixes.

En aquest cas, la clau seria: 1110

En un intercanvi de claus real, per assegurar-se que no hi ha hagut cap espia interceptant el procés de transmissió, es realitza una comprovació pública. Aquesta comprovació consisteix a publicar els primers dígits de la clau secreta i comparar-los

entre l'Alice i el Bob. Per exemple, si hem generat una clau de 1000 dígits, comparem els primers 100.

- Si els 100 primers dígits coincideixen vol dir que la transmissió ha estat segura, i no hi ha hagut cap interferència. Així, es pot concloure que no hi ha hagut cap espia i que la clau generada és vàlida per a xifrar missatges. Aquesta seguretat no ha estat del 100%, però és molt elevada, al següent punt 4.2.3.2. s'explica el perquè.
- Si hi ha discrepàncies en alguns dels 100 primers dígits entre l'Alice i el Bob indicaria un possible error durant la comunicació o la presència d'un espia que ha intentat interceptar el missatge. Això es deu al fet que un espia, en intentar mesurar els bits sense conèixer les bases correctes, alteraria inevitablement els bits, ja que mesurar un fotó amb la base incorrecta altera la seva polarització i el resultat esdevé aleatori, com passa quan l'Alice i el Bob utilitzen bases diferents.

En cas de detectar discrepàncies, l'emissor i el receptor haurien de descartar la clau i repetir el procés de transmissió, ja que no es pot garantir que la clau sigui segura.

4.2.3.2. Simulació amb espia

En aquesta simulació, l'espia intenta interceptar els bits enviats col·locant un filtre polaritzador aleatòriament al feix de llum, sense conèixer la base utilitzada per l'Alice. L'espia, per tant, ha de triar una base de forma aleatòria. Aquest acte d'intentar mesurar els bits provoca les següents situacions:

1. Cas en què l'espia encerta la base de l'Alice

   Si l'espia, per casualitat, tria la mateixa base que l'Alice, el bit transmès no es veu alterat.

   En aquest cas, la llum passa pel filtre polaritzador de l'espia sense modificar la seva polarització, i el receptor encara pot veure correctament el bit enviat.

   Com que no hi ha cap alteració, el bit no es veu afectat i el receptor rebrà el mateix resultat que en una transmissió sense espia. Això significa que, en aquest cas, no es detecta cap discrepància entre l'emissor i el receptor.

2. Cas en què l'espia tria una base incorrecta

Si l'espia tria una base diferent de la que ha utilitzat l'Alice, la situació canvia. Quan la llum arriba al filtre de l'espia, aquesta es veu polaritzada incorrectament o bloquejada, alterant el seu estat original.

Si la base de l'espia no coincideix amb la de l'Alice, el resultat es torna aleatori. Per tant:

- Si la llum passa pel filtre equivocat, arriba alterada al receptor.
- Si la llum no passa, el receptor no rep cap informació clara i, com a resultat, el receptor aleatoritza el bit que comunica al Bob.
- El Bob rep informació aleatòria, i això es reflecteix en la clau secreta final, introduint errors que no hi serien en una transmissió sense espia.

Quan l'espia interfereix en la transmissió, els bits que ha interceptat tenen una alta probabilitat d'error (un 50% per cada bit). Això provoca que quan es comparen les bases entre l'emissor i el receptor, apareguin discrepàncies en els bits corresponents.

Aquesta alteració és detectable gràcies a la publicació i comparació dels primers bits de la clau secreta. Si aquests bits no coincideixen entre l'emissor i el receptor, és un indicador clar que hi ha hagut una interferència o un error, i la presència d'un espia és molt probable.

En l'exemple on es publiquen 100 bits, l'espia té un 50% de probabilitats d'alterar el missatge per a cada bit, per tant, la probabilitat que llegeixi tots els bits i no alteri cap és de 0.5100 = 7.89x10-31 o 0,00000000000000000000000000000789%, una xifra completament absurda, que es compara amb llençar 100 vegades una moneda estàndard i que totes surti cara o que guanyis el primer premi de la loteria "El Gordo" 10 vegades seguides.

Si es detecten moltes d'aquestes discrepàncies, l'emissor i el receptor poden descartar la clau generada i repetir la transmissió, garantint que només utilitzen una clau segura.

4.2.4. Conclusions de la simulació

En aquesta simulació, hem explorat la criptografia quàntica a través d'una simulació clàssica del protocol BB84. La simulació ha permès entendre com funciona la transmissió i generació de claus quàntiques.

Una de les principals conclusions que es pot extreure és la capacitat del sistema quàntic per detectar qualsevol intent d'interferència o espionatge. La mateixa naturalesa de la física quàntica, simulada aquí amb l'aleatorització dels receptors, fa que qualsevol mesura no autoritzada sobre els Qbits alteri el seu estat, fent que les discrepàncies en la clau siguin evidents. Això garanteix que els participants puguin saber si la clau generada és segura o no, cosa que no es pot aconseguir amb els sistemes clàssics.

5. Conclusions

Per concloure aquest treball, podem afirmar que la hipòtesi inicial és parcialment incorrecta.

La hipòtesi esmenta que la seguretat de la criptografia quàntica és del 100%, quan al transcurs del treball hem comprovat el contrari.

Primerament, sobre el paper, teòricament, l'eficàcia no és del 100% sinó que s'apropa molt, i encara que podem negligir aquest petit percentatge, la hipòtesi no ho té en compte.

Experimentalment, hem comprovat com l'eficàcia dels sistemes quàntics a la realitat tampoc és del 100%, ja que hi ha moltes interferències, com la temperatura. Amb un 7,2% d'error, no podem afirmar de cap manera una eficàcia del 100%

A més, mitjançant les entrevistes, hem vist un punt de vista nou sobre l'eficàcia de la criptografia quàntica: l'error humà. Pot donar-se el cas en què, en un futur, el fet de generar la clau i compartir-la funcioni al 100% (o un valor molt proper), però mai es donarà el cas en què l'ésser humà sigui perfecte, per tant, es poden donar situacions clàssiques d'espionatge, com la suplantació d'identitat.

Per tant, no afirmem que l'eficàcia d'aquest mètode d'encriptació és del 100% per tres raons, una petita probabilitat d'error en el mateix concepte, una probabilitat d'error actual, que pot millorar i una probabilitat d'error que sempre ha existit i sempre existirà sigui com sigui encriptació de dades.

Amb aquest treball he descobert dos camps que em fascinen, el de la criptografia i el de la quàntica. He après a seguir la metodologia de fer un treball científic i he tingut enriquidores converses amb experts en el tema.

Crec que aquesta investigació no ha arribat pas al final, ja que encara queda molt per investigar al ser un camp en un desenvolupament actual. Jo continuaria investigant sobre la post-quàntica, per a poder formar la meva pròpia preferència entre quàntica i post-quàntica. A més podria ser interessant trobar els límits que té el protocol BB84 i si n'hi han protocols més preparats encara per a l'arribada dels ordinadors quàntics.

6. Agraïments

En primer lloc, m'agradaria agrair als meus tutors, Jesús González Ortuño i Gisela García Bardaji, per haver sabut guiar-me en tot moment i donar-me idees i inspiracions claus pel desenvolupament d'aquest treball. Gràcies a Yolanda Moneo per ajudar-me a fixar el tema d'aquest treball abans que ens assignin cap tutor. Gràcies també a Ana Justo per ser la meva tutora durant una setmana entre la transició entre Jesús i Gisela.

Gràcies a la fundació Catalunya La Pedrera per donar-me l'oportunitat de participar en el programa Bojos per la Física, que ha suposat una gran font d'informació per a l'elaboració d'aquest treball.

També m'agradaria agrair a l'Oscar Torrente i al Pere Mujal Torreblanca, per oferir-se a ajudar-me a enfocar el futur de la criptografia quàntica mitjançant entrevistes.

Per últim, però no menys important, gràcies a la meva família i amics, per donar-me suport moral durant totes les etapes del treball i ajudar-me a realitzar la simulació.

7. Bibliografia i webgrafia

S'ha decidit citar en format APA pel fet que és el format estàndard en papers científics.

About Us | QIQB: Center for Quantum Information and Quantum Bilogy, Osaka University. (s. d.). https://qiqb.osaka-u.ac.jp/en/about-us/

AES. (s. d.). NFON AG. Consultat el 10 de novembre de 2024, de https://www.nfon.com/es/get-started/cloud-telephony/lexicon/base-de-conocimiento-destacar/aes

Alice y Bob. (2023, 29 setembre). Wikipedia, la Enciclopedia Libre. Consultat el 10 de novembre de 2024, de https://es.wikipedia.org/wiki/Alice_y_Bob

Aparicio, J. I. (2020, 10 setembre). *Criptografia en la Alta Edad Media*. Historia del Condado de Castilla. Consultat el 10 de novembre de 2024, de https://www.condadodecastilla.es/blog/criptografia-en-la-alta-edad-media/

Carbajo, J. L. T. (s. d.). *Alberti | Criptografia clásica*. Consultat el 10 de novembre de 2024, de https://joseluistabaracarbajo.gitbooks.io/criptografia-clasica/content/Cripto11.html

Catastrofe ultravioleta. (s. d.). Luz-Wiki. Consultat el 10 de novembre de 2024, de https://luz.izt.uam.mx/wikis/mediawiki/index.php/Catastrofe_ultravioleta

Clyde, R., & Gillis, A. S. (2023, 5 abril). *post-quantum cryptography*. Search Security. Consultat el 10 de novembre de 2024, de https://www.techtarget.com/searchsecurity/definition/post-quantum-cryptography

Col·legi Oficial d'Enginyeria Informàtica de Catalunya. (2019, 11 abril). *Ramon Llull, patró dels informàtics: per què?* COEINF. Consultat el 10 de novembre de

2024, de https://enginyeriainformatica.cat/ramon-llull-patro-dels-informatics-per-que/

Daniel J. Bernstein, & Tanja Lange. (2016). *Post-quantum cryptography shielding us against quantum-computer fallout* [Tesis, University of Illinois at Chicago and Technische Universiteit Eindhoven]. https://doi.org/10.1038/nature23461

dCode. (s. d.). *Cifrado César*. Consultat el 10 de novembre de 2024, de https://www.dcode.fr/cifrado-cesar?__r=1.129bfa8fcc6dd2f9029fdfd510213cb0

Electron spin. (s. d.). Consultat el 10 de novembre de 2024, de http://hyperphysics.phy-astr.gsu.edu/hbasees/spin.html

Fran. (2007, 17 gener). *Criptografia: Protocolo de distribución de clave BB84*. Gaussianos. Consultat el 10 de novembre de 2024, de https://www.gaussianos.com/criptografia-protocolo-de-distribucion-de-clave-bb84/

Fuensanta, J. R. S. (s. d.). *Cifrados polialfabeticos - criptohistoria*. Consultat el 10 de novembre de 2024, de https://www.criptohistoria.es/polialfabeticos.html

González, A. C. (s. d.). *Entrelazamiento: el mayor misterio de la física cuántica*. The Conversation. Consultat el 10 de novembre de 2024, de https://theconversation.com/entrelazamiento-el-mayor-misterio-de-la-fisica-cuantica-192075

Grover's algorithm. (s. d.). IBM Quantum Learning. Consultat el 10 de novembre de 2024, de https://learning.quantum.ibm.com/course/fundamentals-of-quantum-algorithms/grovers-algorithm

Hase oder Ente? Was Sie sehen, verrät viel über Ihre Kreativität. (2022, 5 mayo). *FOCUS*. https://www.focus.de/panorama/optische-taeuschung-hase-oder-ente-was-sie-sehen-verraet-viel-ueber-ihre-kreativitaet_id_94477185.html

Heisenberg's uncertainty principle. (2023, 30 gener). Chemistry LibreTexts. Consultat el 10 de novembre de 2024, de https://chem.libretexts.org/Bookshelves/Physical_and_Theoretical_Chemistry_Textbook_Maps/Supplemental_Modules_(Physical_and_Theoretical_Chemistry)/Quantum_Mechanics/02._Fundamental_Concepts_of_Quantum_Mechanics/Heisenberg%27s_Uncertainty_Principle

Hilbert Space. (2024, 6 novembre). Wikipedia. Consultat el 10 de novembre de 2024, de https://en.wikipedia.org/wiki/Hilbert_space

ICFO. (2022, 13 juny). *Interest | ICFO*. https://www.icfo.eu/interest/105/quantum-information-theory/11/

Interferòmetre de Mach-Zehnder. (2022, 11 juny). Viquipèdia. Consultat el 10 de novembre de 2024, de https://ca.wikipedia.org/wiki/Interfer%C3%B2metre_de_Mach-Zehnder

Introduction to Polarization. (s. d.). Edmund Optics. Consultat el 10 de novembre de 2024, de https://www.edmundoptics.es/knowledge-center/application-notes/optics/introduction-to-polarization/

Jacabrera. (2024, 8 febrer). *Compuerta lógica XOR*. iElectel. Consultat el 10 de novembre de 2024, de https://ielectel.com/compuerta-logica-xor/

La cuantización de la energía. (2024, 10 abril). Física Cuántica En la Red. Consultat el 10 de novembre de 2024, de https://www.fisicacuantica.es/la-cuantizacion-de-la-energia/

La radiación del cuerpo negro. (2019, 5 febrer). Física Cuántica En la Red. Consultat el 10 de novembre de 2024, de https://www.fisicacuantica.es/la-radiacion-del-cuerpo-negro/

Medición en la mecánica cuántica. (2024, 18 setembre). Wikipedia. Consultat el 10 de novembre de 2024, de https://es.wikipedia.org/wiki/Medici%C3%B3n_en_la_mec%C3%A1nica_cu%C3%A1ntica

Overview of Civil War Codes and Ciphers. (s. d.). Consultat el 10 de novembre de 2024, de https://cryptiana.web.fc2.com/code/civilwar0.htm

Passon, O. (2021). *Kelvin's clouds* [Article]. https://arxiv.org/pdf/2106.16033

Photoelectric effect | Definition, Examples, & Applications. (2024, 25 octubre). Encyclopedia Britannica. Consultat el 10 de novembre de 2024, de https://www.britannica.com/science/photoelectric-effect

Polarizing filters. (2020, 18 juny). Science World. Consultat el 10 de novembre de 2024, de https://www.scienceworld.ca/resource/polarizing-filters/

Principio de superposición de estados. (s. d.). Consultat el 10 de novembre de 2024, de https://web.ua.es/pt/cuantica/docencia/qce/teoria/node17.htm

Public key encryption. (2024, 24 juny). GeeksforGeeks. Consultat el 10 de novembre de 2024, de https://www.geeksforgeeks.org/public-key-encryption/

¿Qué es la criptografia? (2020, 20 novembre). Kaspersky. Consultat el 10 de novembre de 2024, de https://www.kaspersky.es/resource-center/definitions/what-is-cryptography

¿Qué es un Bit? (2020, 28 setembre). JVS Informática Blog. Consultat el 10 de novembre de 2024, de https://www.jvs-informatica.com/blog/glosario/bit/

¿Qué hizo Albert Einstein para ganar el Premio Nobel? (2024, 10 març). *Clarín*. https://www.clarin.com/internacional/hizo-albert-einstein-ganar-premio-nobel_0_fjDU1EWY2B.html?srsltid=AfmBOoofZ0JCnujeFPSCdUniYRo4UHxFd9wuCy1fKc_-PwGz2Ec-m7xo

Rami Arieli. (s. d.). *Fotones y diagramas de energía*. LEQ. Consultat el 10 de novembre de 2024, de https://www.um.es/LEQ/laser/Ch-2/F2s2p1.htm

RSA (Rivest, Shamir y Adleman). (s. d.). Cyberzaintza. Consultat el 10 de novembre de 2024, de https://www.ciberseguridad.eus/ciberglosario/rsa-rivest-shamir-y-adleman

Sabadell, M. Á. (2024, 28 juny). *Así nació la teoría física más perfecta jamás creada*. Muy Interesante. Consultat el 10 de novembre de 2024, de https://www.muyinteresante.com/ciencia/60562.html

Sadurní, J. M. (2024, 17 juny). Alan Turing, el arma secreta de los aliados. *historia.nationalgeographic.com.es*. https://historia.nationalgeographic.com.es/a/alan-turing-arma-secreta-aliados_16352

Schneider, J. (2024, 30 setembre). Breve historia de la criptografia. *IBM*. Consultat el 9 de novembre de 2024, de https://www.ibm.com/mx-es/think/topics/cryptography-history

Schneider, J., & Smalley, I. (2024, 30 agost). What is quantum cryptography? *IBM*. Consultat el 10 de novembre de 2024, de https://www.ibm.com/topics/quantum-cryptography

Taller de Criptografia. (s. d.). Expediente 1. Consultat el 10 de novembre de 2024, de https://www.ugr.es/~aquiran/cripto/expedien/exped001.htm

Téllez, A. M. (s. d.). *La notación bra-ket de Dirac*. Consultat el 10 de novembre de 2024, de https://la-mecanica-cuantica.blogspot.com/2009/08/la-notacion-bra-ket-de-dirac.html

The Elitzur–Vaidman Bomb-Testing method. (2013, 25 agost). Azimuth. Consultat el 10 de novembre de 2024, de https://johncarlosbaez.wordpress.com/2013/08/24/the-elitzur-vaidman-bomb-testing-method/

The wave-particle duality of photons. (s. d.). Photon Terrace. Consultat el 10 de novembre de 2024, de https://photonterrace.net/en/photon/duality/

Total internal reflection. (s. d.). Consultat el 10 de novembre de 2024, de http://hyperphysics.phy-astr.gsu.edu/hbasees/phyopt/totint.html

Verde, A. P. (2022, 19 desembre). *El experimento de la doble rendija de Young y su explicación*. Astrométrico | la Web de Antonio Pérez Verde. Consultat el 10 de novembre de 2024, de https://astrometrico.es/2020/05/18/experimento-doble-rendija-explicacion/

Voorhoede, D. (s. d.). *What is a qubit?* Quantum Inspire. Consultat el 10 de novembre de 2024, de https://www.quantum-inspire.com/kbase/what-is-a-qubit/

What is BCD? (2023, 30 novembre). Consultat el 10 de novembre de 2024, de https://store.omron.co.nz/knowledge-base/what-is-bcd?srsltid=AfmBOoqPU7nmjZgNptgfj5pNxW12JyFwzwMeFOz9T93oQZZFa6i_vnoR

Xu, T. (2024, 8 febrer). *Cryptographers are racing against quantum computers*. Built In. Consultat el 10 de novembre de 2024, de https://builtin.com/articles/post-quantum-cryptography

8. Apèndixs

Entrevista Pere Mujal Torreblanca (30:50):
https://drive.google.com/file/d/13brLLjQdUGryqsoco1RfmdMX9Zx4NK03/view?usp=sharing

Experiment got simulant fibra òptica:
https://drive.google.com/file/d/1yC3Zn1wiFKHo5M9hfbYlYsV3fMzBxCLW/view?usp=sharing

Simulació protocol BB84:

https://drive.google.com/file/d/1pc768Dza0-BFRnGxt5X0KCMR0T6EKTh0/view?usp=sharing