0101010101010101010101
0101010101010101010101
0101010101010101010101

CRIPTOGRAFIA QUÀNTICA

INS Salvador Vilaseca

2n BAT C

2014

ÍNDEX

1. PRÒLEG

He decidit fer aquest treball de recerca perquè volia tocar un tema que encara resta molt desconegut en la societat en què vivim i és molt més important del que ens pensem. Quan escoltem la paraula física ens imaginem Newton o algun físic antic, calculant trajectòries i velocitats, tot d'una forma perfecta, matemàtica i sobretot predictible. El que la majoria de persones no sap és que aquesta física no és l'expressió real del nostre univers. No, no vivim a l'univers de les coses impossibles, vivim en un univers on sembla que tot és possible.

Normalment la societat ha adquirit la física quàntica com quelcom estrany, rar i gens interessant. En realitat la física quàntica explica el funcionament del nostre univers i la veritable visió de les coses i si no s'entén és perquè no es pot fer servir la lògica racional i tradicional per entendre-la. Al igual que quan parlem sobre física la gent se'n pot fer una idea més o menys aproximada, per importància i transcendència, quan parléssim de física quàntica la gent també hauria de tenir mitjanament clar què és.

A més aquest tema m'apassiona, des que els meus pares als 9 anys, em van regalar una novel·la que explicava conceptes de física quàntica, anomenat *La clave secreta del universo* de Stephen Hawking i la seva filla Lucy.

Trobo convenient tractar aquest tema en una de les branques més noves de la física com seria la criptografia quàntica.

2. INTRODUCCIÓ

El meu treball de recerca ha estat elaborat amb l'ajuda de la UAB (Universitat Autònoma de Barcelona concretament el campus de Bellaterra).

Hi vaig anar durant l'estiu a fer unes pràctiques sobre l'efecte fotoelèctric* que té relació amb la primera part d'aquest treball. Més tard, durant el curs, vaig continuar-hi estant en contacte per entendre conceptes, resoldre dubtes, elaborar els experiments mentals i els exemples. Aquests dos últims mencionats són inèdits i han estat pensats expressament per aquest treball de recerca amb l'ajuda de: Ramon Muñoz Tapia, el tutor que em portava el treball de recerca des de la universitat i me n'ha corregit els conceptes.

Aquest treball de recerca tracta sobre la criptografia quàntica, però vaig pensar que entrar directament al tema sense tenir coneixement dels seus components seria com començar una casa per la teulada. Li he volgut donar molta importància a la física quàntica i per això una part important del treball parla sobre les seves principals característiques, una primera introducció necessària per trencar la lògica tradicional i agafar una mentalitat més amplia. També he trobat important repassar una mica el desenvolupament de la criptografia al llarg del temps i la forma com ha anat evolucionant. Si expliqués la criptografia quàntica sense parlar de la criptografia clàssica podríem entendre alguns fenòmens quàntics però també és necessari entendre la base de la criptografia convencional, ja que es parteix des d'aquest punt.

A continuació , explico el perquè d'aquest títol del treball de recerca: "criptografia" perquè és essencial tenir uns conceptes bàsics per poder entendre els diferents processos de funcionaments i "quàntica" perquè és precisament la característica especial que fa que aquesta forma criptogràfica tingui un valor afegit; ja que funciona amb unes regles totalment diferents que les de qualsevol altre mètode criptogràfic, funciona amb les lleis dels àtoms i les partícules.

Un cop han quedat delimitats aquests dos conceptes m'he posat a explicar el funcionament de la pròpia criptografia quàntica, amb l'esperança d'aconseguir explicar de manera entenedora la base del seu funcionament .

A cada apartat del treball hi he afegit un vídeo curt perquè sigui més entenedor que amb un clic és pot visionar s'hi s'està connectat a Internet, a la vegada està gravat en el suport informàtic lliurat.

Finalment hi ha un glossari i dues entrevistes personals a dos investigadors.

3. CARACTERÍSTIQUE QUÀNTIQUES

La física quàntica expressa unes manifestacions molt diferents en la naturalesa de les partícules i dels cossos més diminuts en comparació de la física clàssica.
La física quàntica es manifesta en totes les entitats de l'univers, però on es pot apreciar més és en les entitats més petites que formen la matèria. Bàsicament es poden distingir quatre apartats que expliquen el funcionament i les peculiaritats de la física quàntica: -Dualitat ona corpuscle.

-Principi d'incertesa de Heisenberg.

-Superposició.

-Entrellaçament quàntic.

És possible entendre les seves característiques però no es poden comprendre amb la lògica normal. Com va dir un gran físic:

"It is safe to say that nobody understands quantum mechanics".
Es pot afirmar amb seguretat que ningú entén la física quàntica".

Richard Feynman.

3.1. Dualitat ona-corpuscle

Una de les apassionants particularitats de la física quàntica és la dualitat ona-corpuscle. Consisteix en la capacitat de comportar-se de forma corpuscular o de forma ondulatòria en diferents circumstàncies. Es podria definir com l'expressió de dues característiques d'una realitat interna més profunda (fig. 2.1.). Només ho poden experimentar les partícules subatòmiques*[1], àtoms i certes molècules ja que com més gran sigui l'entitat més dificultat hi ha perquè es pugui manifestar la dualitat.

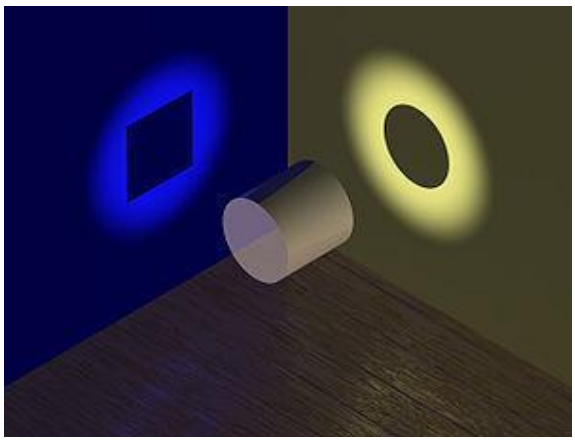


Fig. 2.1. Imatge il·lustrativa de la dualitat ona-corpuscle, on podem veure com un fenomen es pot percebre de dues maneres diferents obtenint una realitat més profunda.

[1] Totes les paraules amb asterisc estan explicades al glossari. Únicament s'ha posat l'asterisc quan sorgeix el concepte per primera vegada.

Abans que aparegués aquest concepte, es creia que existien partícules i ones per separat. Cada entitat tenia les seves característiques definides, es pensava que la llum tenia caràcter ondulatori i la matèria, caràcter corpuscular.

Les ones es consideren entitats extenses, que ocupen zones, poden coexistir més de dues ones en una mateixa zona de l'espai. Si tirem dues pedres a la superfície d'un llac, les ones resultants de l'impacte s'entrellacen. En canvi, les partícules tenen una naturalesa localitzada en una zona concreta de l'espai, de manera que en un mateix punt no hi poden haver dues partícules alhora. Aquests dos conceptes en la física clàssica són totalment incompatibles, és a dir, no es poden manifestar els dos en una mateixa entitat.

En els inicis de la física quàntica van començar a sorgir obstacles i contradiccions, aquestes s'oposaven a les idees clàssiques. Les ones i partícules eren entitats diferents i pertanyien a la llum i a la matèria respectivament. Un dels obstacles que va sorgir va ser l'efecte fotoelèctric, teoria presentada per Einstein el 1905, ja que fins aleshores s'havia pensat que la llum era una ona i aquesta teoria demostrava que l'energia de les ones electromagnètiques* estava quantitzada*, és a dir l'energia dels electrons en l'àtom està restringida a determinats valors característics. Aquest impediment no preocupava a Einstein; al igual que en la superfície de l'aigua s'hi poden observar ones, en realitat l'aigua està formada per petites molècules. Ell considerava que la llum estava formada per petits corpuscles però aquests, a gran escala, interaccionaven entre si i produïen l'efecte d'ones.

El dubte va sorgir quan es va constatar que aquets efectes ondulatoris no són causats per la interacció d'una gran quantitat de partícules, com passa amb les ones de l'aigua. Es va observar que encara que s'enviés partícula a partícula, seguien mantenint els efectes quàntics* de dualitat ona-corpuscle.

Per entendre millor aquesta apartat:

http://www.youtube.com/watch?v=VTfZ-6h6R-0 [2] (video 1)

3.1.1Experiment de la doble escletxa

L'experiment de la doble escletxa és una de les millors maneres de poder comprendre la dualitat ona-corpuscle i apreciar la importància de l'observador*.

Imaginem-nos que tenim una paret amb dues escletxes verticals paral·leles i al darrera de la paret hi ha una pantalla d'impactes on queden marcats tots els cops que rep. Si ens posem a xutar pilotes de futbol contra la paret, podrem observar com les pilotes

[2] Per vídeos més llargs i explicació més complexa consultar Webgrafia o suport informàtic.

que passen per les escletxes xoquen en la pantalla d'impactes formant una única franja, i si se'n xuten moltes al final es distingiran dues franges paral·leles (esquerra fig. 2.2.).

Si fem aquest experiment amb una ona produïda a la superfície de l'aigua, de manera que la paret amb la doble escletxa i l'aigua estiguin situades perpendicularment, quan l'ona passi per la doble escletxa es formaran dues ones que tindran el seu centre al començament de cada escletxa. Aquestes ones s'interferiran entre elles de manera que quan els màxims de cada ona es trobin se sumaran i quan un màxim d'una ona i un mínim de la altra es trobin s'anul·laran. A la pantalla de detecció hi podrem observar un patró d'interferència provocat per les dues ones en entrar en contacte (dreta fig. 2.2.).

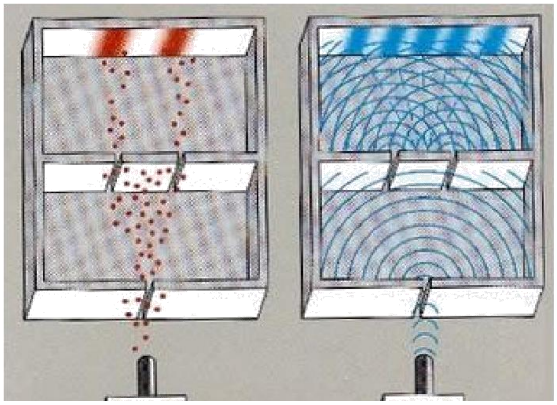


Fig. 2.2. Resultats que en teoria s'haurien de complir si llancem partícules (a l'esquerra) i ones (a la dreta) a través d'una doble escletxa.

Si fem aquest experiment amb partícules microscòpiques,com els fotons, aparentment podem pensar que s'haurien de comportar com les pilotes de futbol, repartint-se en dues franges a la pantalla del darrere; però, quan fem l'experiment llançant les partícules a través de dues escletxes i mirem la pantalla, sorprenentment hi podem observar un patró d'interferència com en les ones de l'aigua. Com hem dit anteriorment, es podria pensar que les partícules interactuen entre elles i nosaltres podem observar aquestes interaccions en forma d'ona.

Quan els científics van tenir la tecnologia necessària, van decidir llançar les partícules una a una contra la doble escletxa i així evitar que interferissin entre elles. Al començament es podia observar com a la pantalla del darrere les partícules xocaven d'una forma aleatòria i aparentment sense sentit, però en esperar-se una estona van poder observar que aquests xocs anaven formant un patró d'interferència (fig. 2.3.).

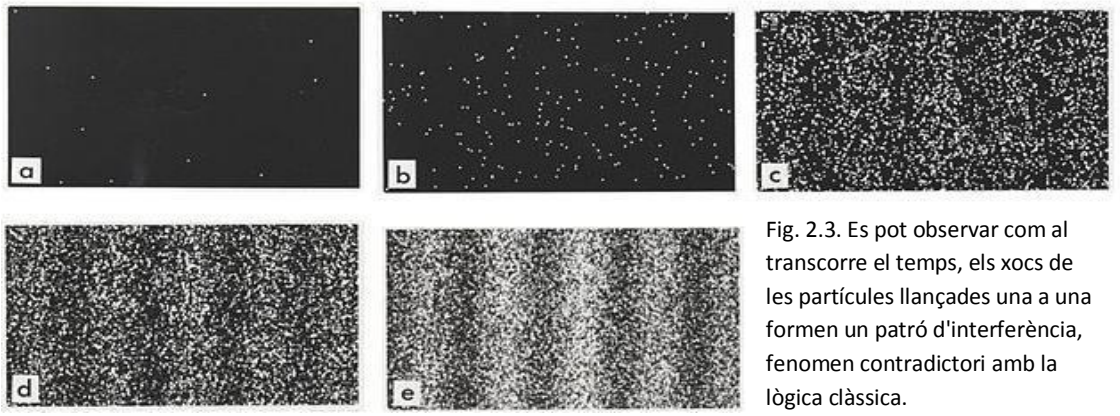


Fig. 2.3. Es pot observar com al transcorre el temps, els xocs de les partícules llançades una a una formen un patró d'interferència, fenomen contradictori amb la lògica clàssica.

Sorpresos per aquesta descobriment, els científics van voler ''observar[3]'' com les partícules podien interactuar amb elles mateixes per comportar-se com una ona. Van col·locar aparells per mesurar les partícules abans de passar per la doble escletxa, però sorprenentment quan intentaven veure per on passaven les partícules, aquestes es comportaven com les pilotes de futbol i marcaven dues franges a la pantalla d'impactes[4] (fig. 2.4.). Aquesta és una demostració que en la física quàntica l'observador juga un paper clau i pràcticament sempre determina els resultats obtinguts.

També van provar de tapar una de les dues escletxes i van observar, en la pantalla del darrere, que el patró d'interferència desapareixia i només s'observava com les partícules xocaven formant una línia vertical corresponent a l'escletxa oberta.

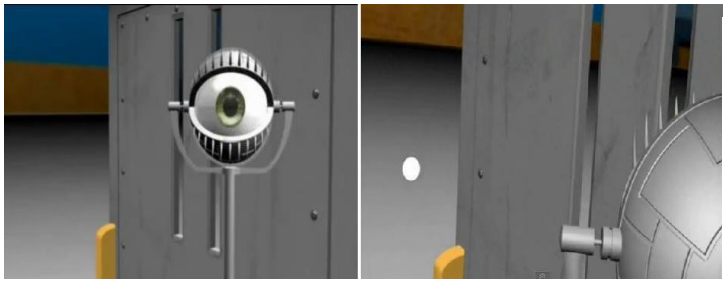


Fig. 2.4. L'ull representa l'acte de mesurar/observar per on passen les partícules quan creuen la doble escletxa. Pel simple fet d'observar s'altera el comportament de les partícules i llavors deixen de crear el patró d'interferència.

Per entendre aquest fenomen podem imaginar que una partícula agafa tots els camins que la poden portar fins a la pantalla de xocs i alhora no els agafa[5], de manera que pot passar pel primer forat, pel segon, per darrere teu, per Alfa Centauri... Es pot entendre que una partícula quan està desplaçant-se cap a la pantalla és com un sistema amb moltes possibilitats i com que passa per les dues escletxes alhora s'interfereix ella

[3] Aquesta observació no succeeix físicament sinó experimentalment, és a dir interpretant els resultats dels experiments

[4] Aparentment és com si la partícula sabes quan és observada i quan no.

[5] Aquesta explicació acceptada completament avui en dia va ser proposada per Richard Feynman a traves dels Diagrames de Feynman , aquests són considerats un dels instruments més importants de la física moderna.

mateixa i actua com una ona (fig. 2.5.). En l' apartat sobre la superposició aquest fenomen es podrà entendre millor.

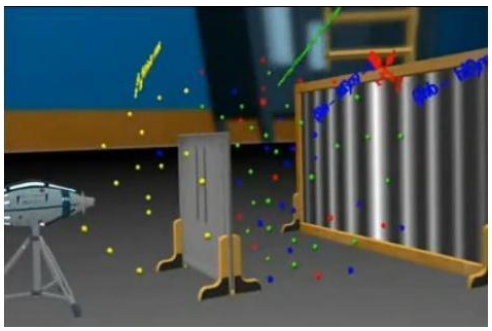


Fig. 2.5. Quan les partícules no són observades passen per tots els camins possibles per arribar a la pantalla de xocs interferint-se entre elles mateixes.

3.2. Principi d'incertesa de Heisenberg

Des dels temps de Newton el determinisme ha estat la forma de pensament més popular sobre el comportament del nostre univers. Segons el determinisme, pensament creat a través de les equacions de Newton, es creia que si sabies les velocitats, posicions i les forces que experimentava un sistema determinat es podia calcular el seu passat i predir el seu desenvolupament futur.

Aquest fet observat des d'un punt de vista objectiu pot resultar lògic, si tu tires una pilota contra el terra sabent les forces que se li apliquen: les velocitats que té i la seva posició, pots predir com es comportarà. Segons aquest concepte, tenint els suficients coneixements de l'estat de totes les partícules de l'univers i una velocitat de càlculs pràcticament instantània, podríem calcular el passat i el futur de tot l'univers!

Aquesta idea pot semblar seductora, ja que en teoria donaria resposta a totes les qüestions que tenim sobre l'univers: en el passat en el present i en el futur. Però si es pot calcular tot el que ha passat i passarà, llavors es poden predir també les accions humanes. Això demostraria que la llibertat que sentim és merament una il·lusió, de manera que encara que ens pensem que podem decidir les nostres accions i comportaments futurs, en realitat estem determinats per les lleis de la física. Segons el determinisme, aquesta sensació de llibertat pròpia de la raó i del pensament humà existeix a causa de la complexitat del cervell, ja que el determinisme afirma que amb els medis necessaris per calcular totes les reaccions del cervell d'una persona, en un moment determinat, es podrien calcular les seves accions futures (fig. 2.6.).

Fig. 2.6. Segons el determinisme fins i tot el pensament i el comportament humà es podrien predir, fet que limita bastant el nostre concepte de llibertat

A principis del segle XX ,amb l'aparició de la física quàntica, van sorgir molts conceptes impactants que trencaven amb aquest pensament classicista que defensava un univers predictible. Un d'aquests conceptes va ser el principi d'incertesa de Heisenberg. El principi d'incertesa de Heisenberg ens explica que no es poden conèixer dues característiques d'una partícula alhora. Per tant, si intentem mesurar exactament la velocitat d'una partícula, en un moment determinat, no podrem saber la seva posició i si intentem conèixer la seva posició concreta ens resultarà impossible poder determinar-ne la seva velocitat. També es pot intentar conèixer les dues magnituds alhora però llavors obtindrem una informació molt inexacta de les dues. A mesura que s'intenta reduir la incertesa en una de les magnituds* mesurades, podem observar com la incertesa en l'altra magnitud augmenta proporcionalment a la disminució de la primera. Aquest principi és aplicable no només a la posició i a la velocitat, es pot aplicar a totes les magnituds que siguin conjugades (posició - moment, energia - temps, etcètera). Aquesta característica de la física quàntica trenca amb el determinisme, segons el qual totes les magnituds d'una partícula, objecte, sistema...; sempre són conegudes, ben definides i a partir de les quals es pot conèixer com s'han desenvolupat i com es desenvoluparan. Si només podem conèixer una magnitud exacta i les altres són incertes, no es pot predir el futur ni el passat ja que es regeixen per possibilitats.
Segons la teoria clàssica, la pertorbació produïda per la medició es pot reduir tant com es vulgui[6], però la teoria quàntica fixa un límit inferior a aquesta pertorbació, ja que l'energia està quantitzada i no pot ser arbitràriament petita.
Per entendre millor aquesta apartat:
http://www.youtube.com/watch?v=y3v61_hklF8 (video 2)
http://www.youtube.com/watch?v=JhxfK1pLI88 (vídeo 3 curt de càlcul)

3.2.1 Fenomen de difracció

Per poder entendre millor el concepte explicaré un experiment d'incertesa sobre la posició i la velocitat anomenat fenomen de difracció. Quan una ona d'una longitud determinada passa per una escletxa, deixa de passar recta i es desvia en un cert angle, el sinus del qual és proporcional al quocient entre la longitud d'ona i l'amplitud de l'escletxa[7].
Si l'escletxa és molt més ampla que la longitud d'ona que hi passa, aquesta segueix la

[6] Evidentment aquesta es reduirà a través del màxim de mesures preses.

[7] Per entendre millor aquesta relació:
http://www.sc.ehu.es/sbweb/fisica/ondas/difraccion/difraccion.html (al final d'aquesta pàgina web hi ha un complement JAVA interactiu per experiments propis)

mateixa direcció que tenia inicialment, sense eixamplar-se. En canvi, si la longitud d'ona és més gran que l'amplitud de l'escletxa, aquesta escletxa més augmentarà l'amplitud de l'ona (fig. 2.7.).

Això es produeix pel principi d'incertesa de Heisenberg. Quant menor és la incertesa en la posició (més estreta és la escletxa), major és la incertesa en la velocitat (l'angle de sortida pot ser més ample).

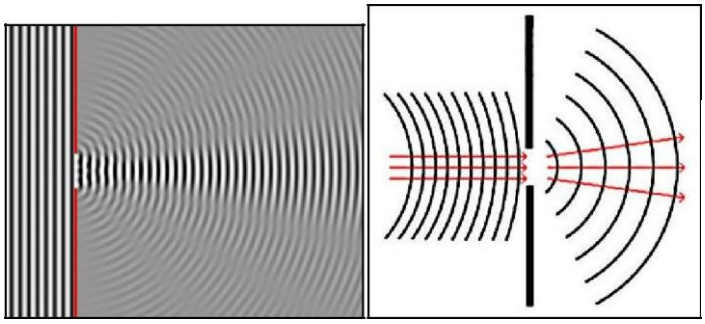


Fig. 2.7. Clara representació del fenomen de difracció. Es pot observar com l'angle de sortida de les ones en passar per l'escletxa és major a causa del principi d'incertesa de Heisenberg.

Un concepte erroni, que es podria adoptar per intentar explicar el principi d'incertesa de Heisenberg, és pensar que les partícules tenen unes característiques concretes i ben definides en tot moment. Però que al mesurar una magnitud, per exemple la velocitat, necessàriament es produeix una pertorbació en la seva posició, fet que fa impredictible la seva posició en el moment que mesurem la seva velocitat i a l'inrevés. Aquesta explicació no reflecteix realment el comportament de la naturalesa i impedeix que sorgeixi la part fascinant de la física quàntica.

La conclusió real que s'extreu d'aquest principi és que abans que es mesuri cap característica d'una partícula no existeix una realitat concreta. Nosaltres en observar col·lapsem una possibilitat d'una de les magnituds mesurables de la partícula, de manera que creem aquella realitat.

3.2.2 Efecte túnel

Una altra peculiaritat és la incertesa en el temps i l'energia, quan major sigui la precisió amb què es mesura l'energia inicial i final d'un salt[8] , menor serà la precisió amb què es podrà mesurar el moment en que s'ha produït el salt.

Una de les conseqüències de la incertesa entre temps i energia és l'efecte túnel. Gràcies a l'efecte túnel les partícules poden travessar barreres d'energia*(també anomenades de potencial) que clàssicament seria impossible que ho fessin. En el cas quàntic hi ha una certa possibilitat que la partícula passi la barrera d'energia, si el temps necessari és menor que la constant de Planck* dividida per l'energia que

[8] Aquests salts fan referència al pas d'un electró des d'una òrbita a una altra en un àtom*.

necessita la partícula per superar la barrera[9].

L'efecte túnel és molt important en molts processos relacionats amb les reaccions químiques ja que explica com passar la barrera d'energia i formar diversos compostos. L'efecte túnel de la física quàntica pot arribar a permetre velocitats de reacció deu mil vegades més ràpides que la física clàssica. També explica la desintegració alfa de nuclis radioactius, les partícules dels quals travessen la barrera de la força nuclear forta* per escapar del nucli (fig. 2.8.).

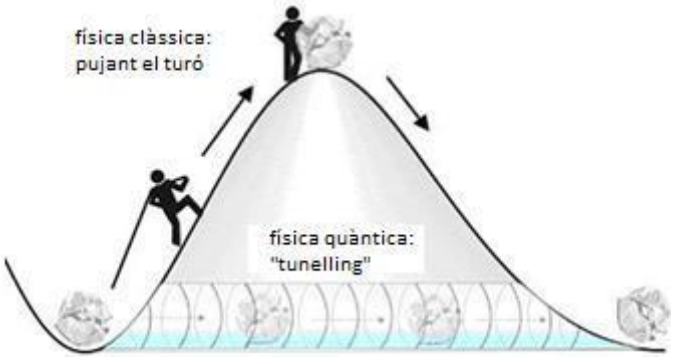


Fig. 2.8. Representació de l'energia necessària per transportar una partícula mitjançant la física clàssica i la física quàntica segons el principi d'incertesa de Heisenberg.

3.3. Superposició

Com hem pogut observar en l'apartat anterior, l'univers es regeix per l'Indeterminisme. Les magnituds d'una partícula no poden ser totalment arbitràries sinó que estan quantitzades i hi ha possibilitats de trobar diferents valors per a cada una de les magnituds de la partícula, de manera que no es pot conèixer el seu valor exacte en mesurar-les. L'Indeterminisme real de la física quàntica succeeix quan l'observador col·lapsa una de les possibilitats d'un sistema, ja que el valor que s'obté és totalment aleatori i impredictible.

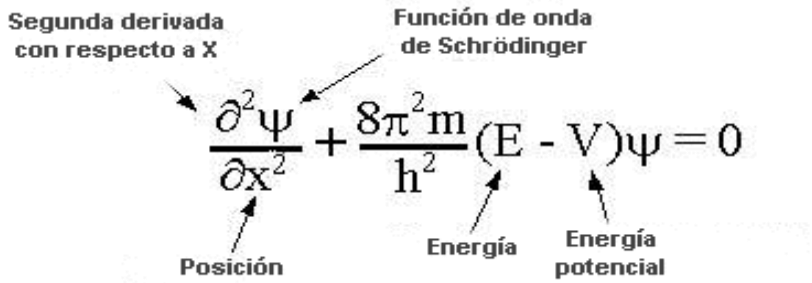
S'anomena funció d'ona un sistema que té unes possibilitats de tenir diferents valors, per exemple, una partícula que no està sent observada i té algunes possibilitats que les seves magnituds tinguin uns determinats valors. El 1927 Max Born va proposar que la funció d'ona estava relacionada amb la probabilitat de trobar un sistema* en un cert estat, de manera que en efectuar una observació s'obtingui un valor concret dins d'un conjunt de valors possibles, normalment coneguts anteriorment. Aquesta visió de Born es pot interpretar de dues maneres: alguns físics com Einstein acceptaven la física quàntica com una descripció incompleta de la naturalesa i creien que li faltaven alguns valors interns que farien que la física quàntica fos determinista, de manera que aquestes probabilitats serien degudes al desconeixement dels comportaments reals de les partícules; d'altra banda, Neils Bohr defensava que la física quàntica estava

[9] Aquesta relació s'entén amb el segon vídeo d'aquest apartat sobre l'incertesa de Heisenberg

completa i que realment es regia per probabilitats, una idea difícil d'assimilar que trencava amb el pensament de l'època[10].

Erwin Schrödinger va ser un físic nascut a finals del segle XIX, les seves aportacions van ser crucials en el desenvolupament de la física quàntica, a causa de l'equació de Schrödinger* que descriu la funció d'ona, és a dir, explica com es comporta una partícula quan no és observada. Aquesta equació, va jugar un dels papers centrals en el desenvolupament de la física quàntica, no explica la manera com la funció d'ona es col·lapsa i passa de ser un cúmul de possibilitats a un valor exacte en el moment en què és observada; sinó que la solució general de l'equació de Schrödinger és una suma de les solucions particulars corresponents a uns estats propis del sistema, a cadascun dels quals correspon un valor d'una certa magnitud física.

Cada una de les solucions particulars va multiplicada per una funció numèrica en què el seu quadrat està relacionat amb la probabilitat de trobar el valor corresponent de la magnitud en efectuar la medició.



Podem pensar que aquesta probabilitat de les magnituds d'un sistema descrit per l'equació de Schrödinger és degut a la falta d'informació i que en realitat les magnituds estan sempre definides, però com que no podem obtenir el seu valor directament, només podem accedir a uns valors pròxims. Si fos així, la física quàntica estaria incompleta.

Si acceptem que la física quàntica és totalment completa, implica que la realitat és molt més sorprenent del que ens pensem ja que en aquest cas quan no estem observant, com descriu la equació de Schrödinger, hi ha certes possibilitats per a cada magnitud d'un sistema, de manera que cap valor està definit, tots existeixen alhora i nosaltres només podem conèixer els possibles valors que podem trobar en observar i les possibilitats que tenen cadascun d'aquests valors de ser observats. Aquest fet explica el comportament ondulatori de les partícules que passen per una doble escletxa; com que quan viatgen a través de la doble escletxa i no són observades, agafen tots els camins possibles de manera que una mateixa partícula passa per les

[10] Aquests dos arguments són els que van portar als famosos debats entre Einstein (determinsista) y Bhor (indeterminista) , al 1925 ; un dels debats va ser durant el conveni de Solvay al 1927.

dues escletxes alhora i s'interfereix ella mateixa.
Una forma d'entendre millor la superposició és imaginar-nos que hi ha molts universos paral·lels i en cada un d'aquests universos la partícula que es dirigeix cap a la doble escletxa agafa un dels camins possibles (fig. 2.9.). A cada univers tindrem un camí diferent per on ha passat la partícula. Si ajuntem tots els universos, la partícula estarà passant per tots els camins possibles, de manera que estarà en un estat de superposició.

Fig. 2.9. . Conjunt de possibles universos en què la partícula tindria un comportament/trajectòria diferent, aquests universos es troben en una superposició i només quan observem en col·lapsem un dels possibles.

Per entendre millor aquesta apartat:
http://www.youtube.com/watch?v=ae4fgtwgc8Q (video 4)

3.3.1 El gat de Schrödinger

Schrödinger i Einstein es van negar a acceptar l'indeterminisme. Creien que la natura es regia pel determinisme i que els conceptes que sorgien de la física quàntica eren erronis i esbojarrats. Per intentar explicar les excentricitats de la física quàntica, van idear per separat un seguit de jocs mentals perquè la gent pogués entendre l'estrany que era la física quàntica.
Schrödinger ,al 1935, va publicar un problema mental que es va fer molt famós anomenat el gat de Schrödinger. Explicava com hauria de ser la naturalesa en realitat si la física quàntica fos completa. El gat de Schrödinger consisteix en un gat que es troba a l'interior d'una capsa tancada i totalment opaca. A l'interior de la capsa hi ha un sistema que si s'activa trencarà una ampolla plena de verí, de manera que el gat morirà. El sistema consisteix en un fotó* que viatja en línia recta fins que es troba en una bifurcació de dos camins; si el fotó agafa el camí de la dreta activarà el sistema de la capsa i el gat morirà, en canvi si el fotó passa pel camí de l'esquerra no passarà res.
Si aquest sistema funcionés amb pilotes, depenent del camí que agafés la pilota, el gat es moriria o seguiria viu, però com que ho estem fent amb fotons les coses són més interessants: segons la física quàntica es formarà una superposició, de manera que el fotó passarà pels dos camins alhora, fet que comporta que el gat estarà viu i mort al mateix temps (fig. 2.10.). No serà fins que nosaltres obrim la capsa que la funció d'ona

es col·lapsarà i trobarem el gat viu o mort.

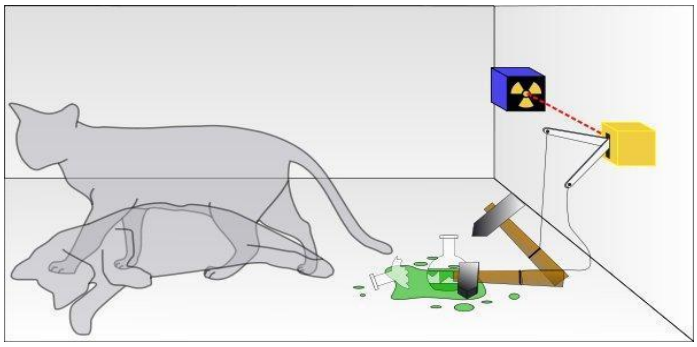


Fig. 2.10. Es pot apreciar la superposició dels dos estats, en què el gat es troba viu i mort alhora.

En la realitat, si féssim l'experiment, el gat no podria entrar en una superposició a causa dels fenòmens de descoherència en no ser una entitat microscòpica[11], però sí que la seva vida o mort seria aleatòria i dependria del camí que agafés la partícula.

3.3.2 Els daus quàntics

Si agafem un dau, el posem dins d'un cubilet, el remenem i el posem contra el terra, de manera que el dau ja estigui quiet però no el podem veure perquè hi ha el cubilet al damunt, en teoria encara que nosaltres no puguem mirar el dau, ell ja tindrà una de les seves cares a la part superior i en mirar veurem quina és (fig. 2.11.). (Sistema clàssic)

Fig.2.11. Quan remenem el cubilet i després l'aixequem per veure el número del dau, ens apareix un valor clar en una de les seves cares.

Si tinguéssim un dau quàntic, després de remenar-lo, quan estigués quiet però tapat pel cubilet, la cara superior del dau no estaria determinada, es trobaria en una superposició de totes les cares possibles que té el dau i nosaltres, en aixecar el cubilet i mirar, col·lapsaríem la funció d'ona i observaríem un valor concret per a la cara superior (fig. 2.12.). (Sistema quàntic)

[11]Com hem establert anteriorment la física quàntica únicament té validesa a nivell microscòpic.

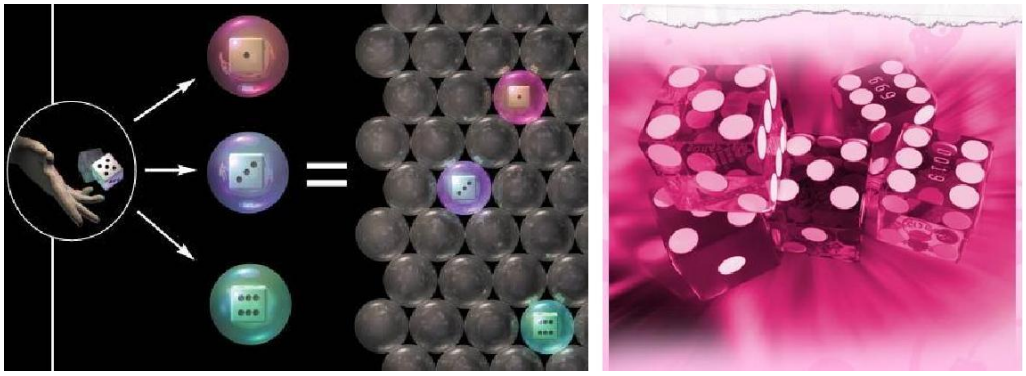


Fig. 2.12. Si existissin uns daus quàntics, quan no els miréssim es trobarien en una superposició de totes les cares possibles, i en mirar col·lapsaríem una de les possibilitats i veuríem una de les cares

3.4. Entrellaçament quàntic

Tracto l'entrellaçament quàntic en últim lloc perquè és en el que es necessiten utilitzar més característiques de la física quàntica per poder-lo comprendre. A més és una de les parts més apassionants i a partir de les quals se'n poden obtenir més aplicacions pràctiques.

Explicaré cinc experiments, els quatre primers necessaris per a poder entendre l'últim que és un estat GHZ[12] (Greenberger–Horne–Zeilinger state)[13], un tipus de desigualtat de Bell. Al final aconseguirem entendre i demostrar l'entrellaçament quàntic i a més es podrà comprovar matemàticament com amb la física clàssica no es poden explicar els diferents fenòmens observats, de manera que la física quàntica va més enllà.

Al final de cada experiment hi haurà dues explicacions, una que intentarà interpretar el que s'observa des d'un punt de vista clàssic, com si fóssim uns científics en un laboratori i intentéssim explicar el que veiem en els experiments. L'altra descripció parlarà sobre les observacions des d'un punt de vista quàntic, que avui en dia sabem que és el cert.

Tots els experiments que realitzarem a continuació són simplificacions d'experiments que s'han reproduït fàcilment als laboratoris, de manera que tot el que s'explica està demostrat.

Aquests experiments s'han fet expressament per aquest treball per ampliar la ment del lector cap una visió més quàntica i menys tradicional de la física. Estan simplificats ja que es fan amb diagrames i per entendre conceptes deixant de banda tota la part

[12] En l'àmbit de la teoria de la informació quàntica, és un cert tipus d'estat quàntic enredat que implica almenys tres subsistemes (partícules). Va ser estudiat per primera vegada per D. Greenberger, MA Horne i Anton Zeilinger en 1989. S'han adonat de les propietats extremadament no clàssiques de l'estat.

[13] Daniel M. Greenberger, Michael A. Horne, Anton Zeilinger (2007), *Going beyond Bell's Theorem*

matemàtica amb càlcul de matrius, anàlisis de probabilitat, etc.

Per entendre millor aquest apartat:

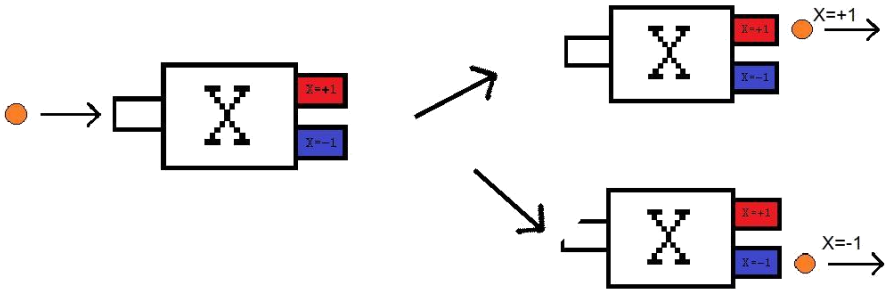
http://www.youtube.com/watch?v=fZkkl4n2CrQ (video 5)

3.4.1- Observable

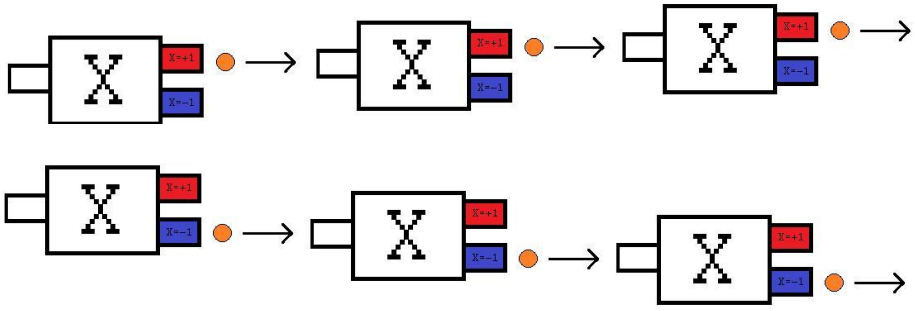
Tenim unes partícules taronges amb totes les característiques iguals.

També tenim uns detectors que mesuren una de les magnituds d'aquestes partícules. Els detectors tenen una entrada i dos sortides.

Fem passar aquestes partícules per un detector que mesura la magnitud X, com que només te dues sortides, si la partícula surt per dalt significarà que el seu valor per la magnitud X serà +1 i si surt per baix serà -1.



Posem un seguit de detectors idèntics que mesuren la mateixa magnitud. Si en el primer detector la partícula taronja surt per dalt (X=+1) i ho observem, en els següents aparells seguirà sortint sempre per dalt (X=+1). Si la partícula surt per baix (X=-1) en el primer detector, en la resta també seguirà sortint per baix (X=-1).

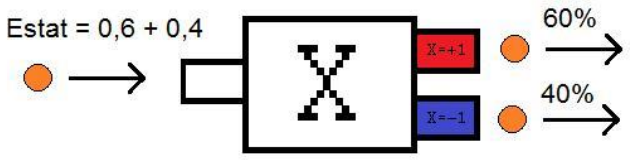


Interpretacions:

- Des del punt de vista clàssic es pot pensar que la partícula té un valor per la magnitud X, de manera que sempre sortirà per dalt en el cas que sigui X=+1 o per baix en el cas que sigui X=-1.
- Quànticament podem explicar-ho dient que la partícula abans que entri en el primer detector no té cap valor definit per a X, es troba en una superposició dels dos valors alhora. Quan passa per el detector es col·lapsa la funció d'ona i s'expressa un valor concret (X=+1 o X= -1). Quan mirem per on surt pel primer detector, com que estem observant-la no pot tornar a superposar-se, de manera que es manté el valor de X que s'ha col·lapsat en el primer detector, per tant en la resta de detectors seguirà marcant aquest valor.

3.4.2- Probabilitats

Si tenim una font de partícules taronges i sabem que hi ha un 60% de probabilitats que les partícules siguin X=+1 i un 40% de que siguin X=-1, efectivament quan passin per un detector un 60% sortiran per dalt (X=+1) i un 40% per baix (X=-1).



Interpretacions:

- Clàssicament és lògic que si el 60% de les partícules que surten de la font són X=+1 i el 40% són X=-1, quan posem un detector sortiran amb les mateixes proporcions.
- Explicat des del punt de vista quàntic, les partícules que surten de la font tenen un 60% de probabilitats que quan siguin observades i es col·lapsi la funció d'ona es determinin donant X=+1 i un 40% de que esdevinguin X=-1. I si no són observades no es pot preveure el resultat.

3.4.3- Element de realitat

Segons la física quàntica una partícula no té unes característiques definides, som nosaltres els que definim les característiques en observar-les. De manera que nosaltres creem la realitat en el moment de mirar el que passa en el sistema que prèviament no estava definit, era com un cúmul de possibilitats i nosaltres en observar aquest sistema que, parlant d'espai, es podria trobar potencialment en molts llocs, col·lapsem una de les possibilitats de la partícula i l'observem en un punt concret, hem creat una realitat que no existia.

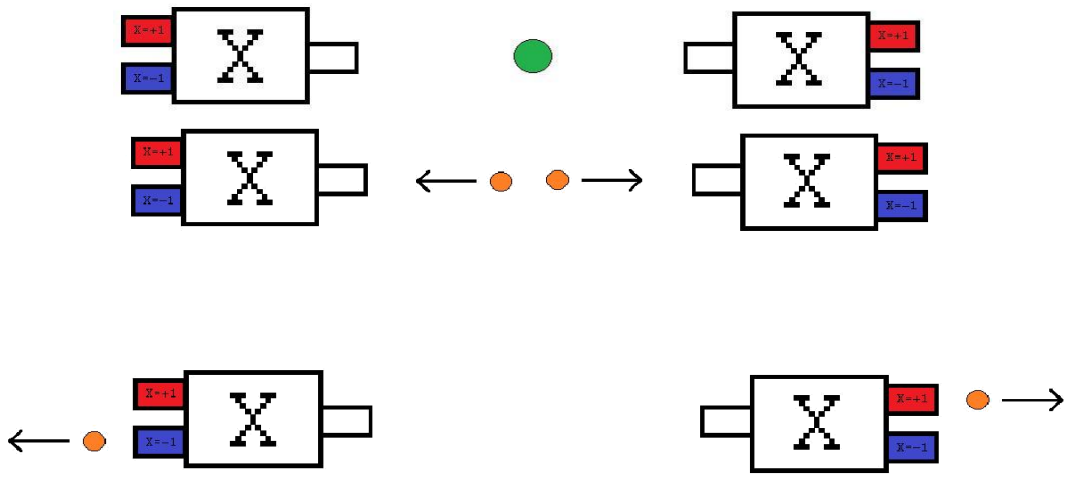
Einstein i altres científics s'oposaven a les característiques indeterminants de la física quàntica, ells defensaven que els objectes tenen unes propietats definides com per exemple velocitat, posició..., independentment de si les observem o no, de manera que pensaven que si ningú les observa seguirien mantenint les mateixes qualitats i característiques pròpies.

3.4.3.1La paradoxa d' Einstein, Podolsky i Rosen

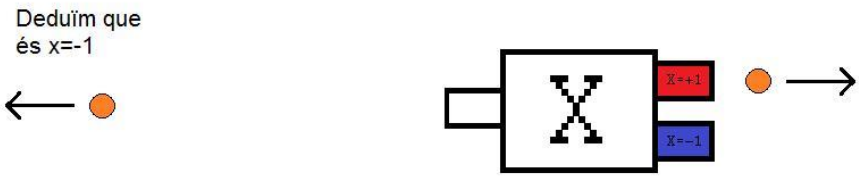
Aquests científics deterministes volien demostrar que les partícules tenen unes característiques definides i fixes.
Es van imaginar un sistema format per dues partícules idèntiques emeses simultàniament, amb velocitats iguals i sentits oposats, per exemple, dos fotons emesos per un àtom. La igualtat de les seves velocitats i els seus sentits oposats no és quelcom excepcional, vénen donades per les lleis de conservació de moment lineal i angular. Segons aquestes condicions si mesurem la velocitat d'una de les partícules despreses, podríem conèixer la de l'altra, i si mesurem la posició d'una també coneixeríem la de l'altra. De manera que si hi ha dos observadors per a cada partícula i un mesura la velocitat i l'altre mesura la posició, podríem conèixer alhora dues característiques de les partícules, fet que es contradiu amb el principi d'incertesa de Heisenberg. Einstein suposa que com que absolutament res de res pot viatjar més ràpid que la velocitat de la llum, les partícules prèviament tindrien una posició i velocitat definides ja que si cada partícula les adquirís en el moment del mesurament, llavors l'altra partícula instantàniament hauria de determinar-se i adquirir posició o velocitat, depenent del que es mesuri en la primera. Seria una acció que aniria en contra de la relativitat ja que en teoria hauria de ser instantània i com sabem res no viatja més ràpid que la llum.
Quan en un sistema es pot conèixer alguna qualitat d'una de les partícules que el formen sense pertorbar-la de cap manera, es diu que el sistema té un element de realitat. En la paradoxa d' Einstein, Podolsky i Rosen, sabent el valor d'alguna de les magnituds d'un dels fotons es pot conèixer el de l'altra fotó sense pertorbar-lo de cap manera, de manera que aquest sistema té un element de realitat.
Interpretem d'una forma més senzilla la paradoxa d' Einstein, Podolsky i Rosen:
Tenim unes partícules verdes.

Aquestes partícules es poden desintegrar cada una en dues de taronges. La suma del valor de X de les partícules taronges que surten de la partícula verda és X=0, de

manera una de les partícules taronges tindrà un valor de X=+1 i l'altra de X=-1.

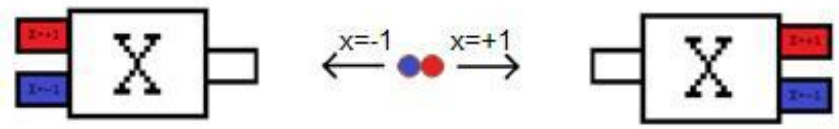


Segons la paradoxa d' Einstein, Podolsky i Rosen, sabent la magnitud X d'una de les partícules ja podrem conèixer el valor de l'altra. Si mesurem una i ens dóna X=+1, l'altra necessàriament ha de ser X=-1



Interpretacions:

- Segons la física clàssica tots aquests sistemes han de tenir localitat, és a dir, les partícules taronges d'alguna manera hagut de posar-se d'acord sobre el seu valor de X quan estaven en contacte o haver-se comunicat quan s'estaven separant. L'única condició és que quan estaven separades no poden haver-se comunicat ni rectificat els seus estats en un temps inferior al que tardaria la llum en arribar de l'una a l'altra. Això és una conseqüència de la relativitat d'Einstein.



- L'única manera d'explicar aquest fet des d'un punt de vista quàntic és que les partícules d'alguna manera estan connectades en tot moment. No tenen un valor determinat en el moment de formar-se per la desintegració de la partícula verda, ni quan s'estan separant. En el moment en què una de les partícules és mesurada i es col·lapsa un dels dos valors de X en que es pot manifestar, determina instantàniament el valor que tindrà l'altra partícula, estiguin a tres metres o a punts remots de la

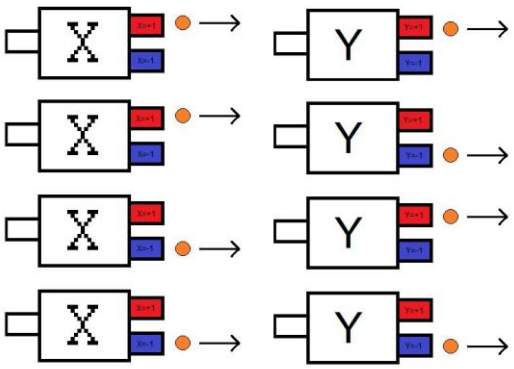
galàxia. Això és l'entrellaçament.

A partir del sisè experiment es podrà demostrar realment que les partícules estan entrellaçades. Amb la informació que tenim en aquest punt encara no es pot demostrar que les partícules estiguin entrellaçades realment i si fóssim uns científics fent aquests experiments en un laboratori el més fàcil seria pensar de la manera clàssica i dir que les partícules s'han posat d'acord quan estaven juntes, és a dir, que tenien localitat.

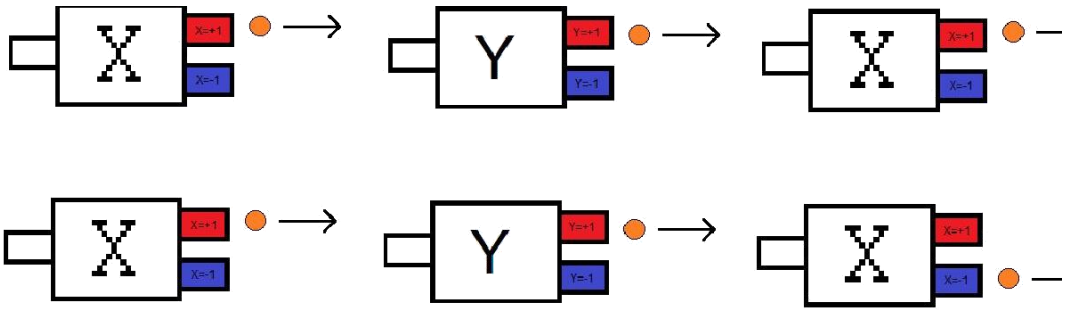
3.4.4- Incompatibilitat d'observadors

Col·loquem dos detectors de magnituds diferents en línia, per exemple, el primer de la magnitud X i el segon de la magnitud Y. Quan hi fem passar partícules taronges pels dos detectors, com que mesuren magnituds diferents lògicament poden haver-hi quatre opcions:

Primera opció: X=+1 , Y=+1
Segona opció: X=+1 , Y=-1
Tercera opció: X=-1 , Y=+1
Quarta opció: X=-1 , Y=-1



Ara posem tres detectors en línea de manera que el primer i el tercer mesurin la magnitud X i el segon mesuri la magnitud Y. En els dos detectors primers la partícula es comportarà com s'explica en el principi de l'experiment 5. Però en el tercer detector, que torna a mesurar la magnitud X, la partícula pot passar per dalt (X=+1) o per baix (x=-1)!



Interpretacions:

- Amb la lògica clàssica ja comencen a sorgir problemes ja que si en el primer detector, que mesura la magnitud X surt per la sortida de dalt, en el tercer també hauria de

sortir per la mateixa sortida ja que en teoria les propietats de les partícules es mantenen. Tot i aquests obstacles, encara es pot pensar que el segon detector, que mesura la magnitud Y ,ha afectat la partícula d'alguna manera i ha fet que canviï la seva magnitud X. També es pot pensar que existeixen unes variables ocultes, diferents processos que poden haver afectat la partícula i per falta d'informació desconeixem com funcionen.

- Quànticament podem explicar-ho dient que la partícula quan passa pel primer detector se li col·lapsa un valor per la magnitud X, quan passa per la segona màquina es determina un dels dos valors per a la magnitud Y però torna a trobar-se en un estat d'incertesa per a la magnitud X, de manera que en passar per la tercera màquina poden expressar-se els dos valors de la magnitud X.

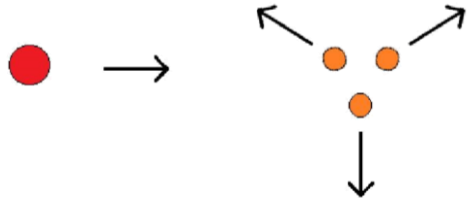
3.4.5- Estat GHZ. El fi de l'element de realitat i la no-localitat

John S. Bell va ser un físic important que treballava en la física de partícules teòriques i també en el disseny d'acceleradors al CERN(Conseil Européen pour la Recherche Nucléaire) .

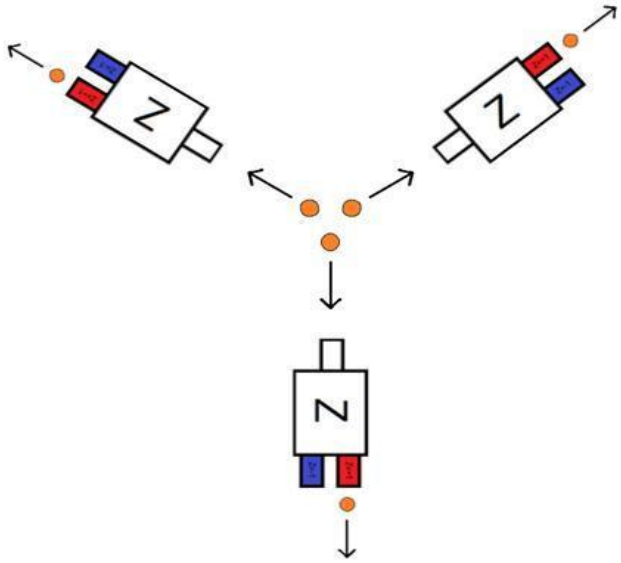
En sorgir aquestes idees sobre les variables ocultes com a últim recurs per defensar la física clàssica, John S. Bell va presentar un estudi que demostrava matemàticament que en els experiments descrits en la paradoxa d'Einstein Podolsky i Rosen no hi havia localitat. És a dir que cap explicació clàssica podia descriure els experiments plantejats.

Aquestes demostracions matemàtiques que desmenteixen qualsevol interpretació clàssica d'aquests experiments s'anomenen desigualtats de Bell. L'experiment que desenvoluparem a continuació és un tipus de desigualtat de Bell anomenada estat GHZ. És la forma més fàcil de demostrar la no-localitat i com clàssicament no es pot descriure el comportament real.

En aquest experiment tindrem un nou tipus de partícules de color vermell que es poden desintegrar en tres de taronges formant un estat GHZ. Quan una partícula vermella es desintegra, les tres taronges que sorgeixen s'allunyen entre si amb angles de 120º.

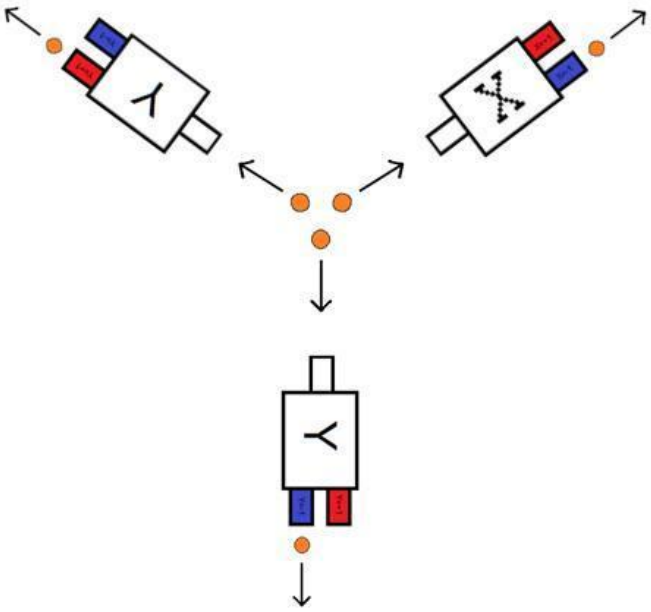


Col·loquem tres detectors per a la magnitud Z, de manera que a cada un hi entri una de les partícules taronges despreses de la desintegració d'una partícula vermella. En aquest cas o totes sortiran per dalt (Z=+1) o per baix (Z=-1).



Podem observar que amb aquest sistema seguim tenint element de relatat. Si coneixem el valor d'una del es partícules, seguirem coneixent el valor de les altres sense fer-les passar per cap detector.

Ara posem un detector X i dos de Y i hi fem passar partícules taronges.



Si fem la prova moltes vegades podrem observar com només ens poden sortir un seguit de resultats:

X1	Y2	Y3
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

En aquest cas concret si ens hi fixem bé encara podem trobar un element de realitat.

Es pot comprovar que la multiplicació dels resultats que donen cada una de les configuracions és igual a +1. Si sabem les mesures de dues partícules podem saber el valor de la tercera.

Exemple:

Si sabem que:

$$X_1 = -1$$

$$Y_2 = -1$$

Fent una senzilla equació:

$$X_1 \cdot Y_2 \cdot Y_3 = +1$$

$$-1 \cdot -1 \cdot Y_3 = +1$$

$$Y_3 = +1$$

El fet que en aquest sistema la multiplicació dels resultats sigui +1 és merament casualitat i només podem saber que realment en totes les combinacions dona +1 si els detectors estan en aquesta combinació ja que s'ha observat després de veure tots els resultats obtinguts.

Ara col·loquem diferents detectors en unes posicions concretes i podem observar que també donen elements de realitat per separat:

Y1	X2	Y3
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

Y1	Y2	X3
+1	+1	+1
+1	-1	-1
-1	+1	-1
-1	-1	+1

X1	X2	X3
-1	-1	-1
-1	+1	+1
+1	-1	+1
+1	+1	-1

Y1 · Y2 · X3 = +1

Y1 · X2 · Y3 = +1

X1 · X2 · X3 = -1

Si les quatre equacions que descriuen els elements de realitat fossin certes, la multiplicació de les quatre també hauria de concordar i donar una igualtat.

Calculem-ho a veure què passa:

$$X_1 \cdot Y_2 \cdot Y_3 = +1$$
$$Y_1 \cdot X_2 \cdot Y_3 = +1$$
$$Y_1 \cdot Y_2 \cdot X_3 = +1$$
$$\underline{X_1 \cdot X_2 \cdot X_3 = -1}$$
$$X_1^2 \cdot Y_1^2 \cdot X_2^2 \cdot Y_2^2 \cdot X_3^2 \cdot Y_3^2 = -1$$
$$+1 \neq -1$$

Interpretacions:

- Des del punt de vista clàssic no es pot descriure el que s'observa ja que segons aquestes operacions no hi ha localitat.

- Com podem veure es produeix una desigualtat ja que mai +1 serà igual a -1. Així queda demostrat que amb la física clàssica no es pot descriure aquest experiment i que realment les partícules estan entrellaçades. Quan les tres partícules se separen i es dirigeixen cap als detectors no tenen cap valor definit i el fet de col·lapsar-ne alguna, depenent del sistema, implica que instantàniament es determinin les altres, independentment de la distància i el temps.

Més endavant, quan la tecnologia ho va permetre, es van dur a terme un seguit d'experiments que van acabar de demostrar l'entrellaçament de les partícules. Quan les partícules s'estaven separant van canviar els detectors d'una forma aleatòria amb un temps prou curt per impedir que les partícules es comuniquessin a una velocitat inferior a la de la llum. El que va passar és que les partícules en entrar pels detectors canviats van donar la resposta correcta per a cada detector, s'havien corregit instantàniament. Estaven entrellaçades.

4. BREU DESCRIPCIÓ DE LA CRIPTOGRAFIA

Des de fa milers d'anys la humanitat ha tingut la necessitat de transmetre informació d'una forma segura. Des de l'antiga Grècia , passant per l'edat mitjana, l'època moderna i l'actualitat, la informació ha esdevingut un element cada cop mes crucial i poderós i és per això que amb ella, la criptografia també ha evolucionat moltíssim.
La criptografia és com un joc perillós on hi intervenen bàsicament dos personatges:
Els criptògrafs, encarregats d'ocultar els missatges que es volen enviar, empescant-se un munt de maneres per evitar que ningú pugui aconseguir llegir la informació que contenen, a excepció de la persona a qui van destinats i els criptoanalistes que són totalment el contrari dels criptògrafs i intenten totes les maneres d'extreure la informació amagada en els missatges que envien els criptògrafs. Tant els criptoanalistes com els criptògrafs posseeixen una gran imaginació per a poder practicar nous mètodes de xifratge i desxiframent respectivament.
Al llarg de la historia de la criptografia aquests dos personatges han anat millorant els seus mètodes de tal manera que s'intentaven superar els uns als altres: hi havia èpoques en què els missatges eren totalment segurs i aparentment no es podien desxifrar, però llavors els criptoanalistes aconseguien un nou mètode per desxifrar el missatge i durant un temps semblava que les comunicacions eren insegures i així, successivament fins ara, que pot ser que els criptògrafs hagin guanyat el joc.
Al llarg del temps s'han anat desenvolupant milers de formes d'ocultar un missatge, algunes molt poc segures, altres que han tardat segles a desxifrar-les, però totes les escriptures secretes es poden separar en dos grups:

- Primerament hi ha la criptografia, que és l'art d'ocultar un missatge canviant la seva estructura a partir d'algun patró, amb el qual es pot tornar a invertir aquest canvi i tornar a obtenir el text pla o descodificat.
- Una segona forma d'ocultar missatges és l'esteganografia, que consisteix a ocultar el missatge físicament. En aquest cas el missatge està amagat però si algú el troba el podrà llegir perfectament ja que no s'ha alterat la seva estructura.

Molts cops aquestes dues tècniques s'han fusionat per intentar aconseguir una major seguretat. D'aquesta manera, en cas que el missatge fos interceptat, també hauria de ser desxifrat per a poder-ne obtenir la informació.

4.1. La xifra de substitució monoalfabètica

En els inicis de la criptografia s'utilitzaven uns mètodes que comparats amb els actuals

eren molt bàsics i elementals però com tota matèria, primer es comença en un estat simple i cada cop es va desenvolupant més i va augmentant la seva dificultat.
Independentment de la complexitat del mètode criptogràfic que s'utilitzi, pràcticament totes les formes de criptografia funcionen de la mateixa forma. Primerament hi ha el missatge que es vol enviar, que es pot anomenar text pla, ja que encara no s'ha alterat de cap manera. L'emissor, que té el missatge, tria una clau i a través d'un algorisme criptogràfic, una sèrie de passos i maneres mitjançant les quals aplica la clau al text pla, xifra el missatge. Un cop el missatge ja està xifrat, l'emissor l'envia cap al receptor. Quan el missatge arriba al receptor, com que té la mateixa clau que ha utilitzat l'emissor per xifrar el missatge, només s'ha d'aplicar la clau amb l'algorisme criptogràfic invers al que ha utilitzat l'emissor. Un cop fet tot el procediment, el receptor aconseguirà el missatge original que tenia l'emissor (fig. 3.2.).

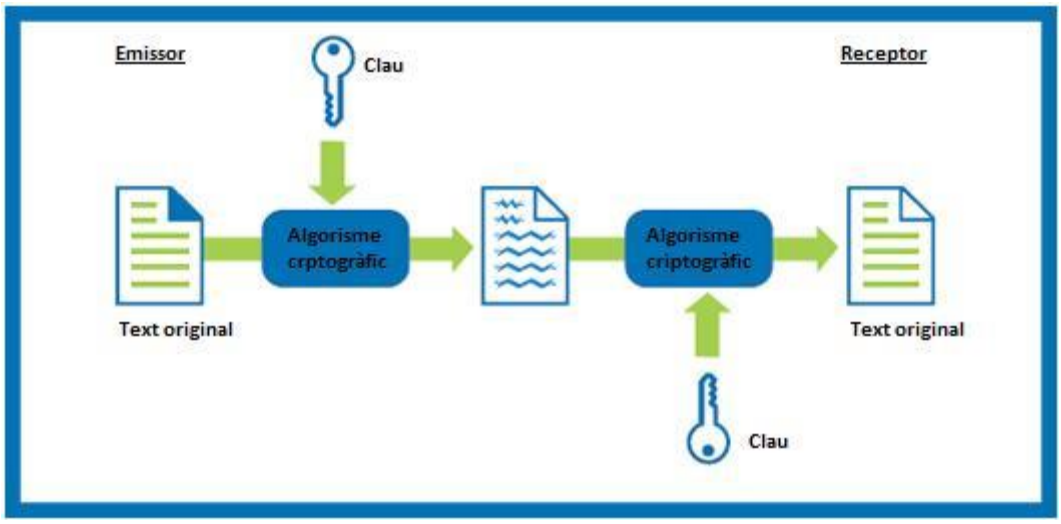


Fig. 3.2. En la majoria de processos criptogràfics, la clau s'aplica sobre el text pla d'una certa manera (algorisme criptogràfic) per a obtenir el text xifrat. Per desxifrar-lo simplement es necessita la clau i invertir l'algorisme criptogràfic que se li havia aplicat.

El primer ús documentat d'una forma de criptografia amb propòsits militars apareix a *La guerra de les Gàl·lies,* de Juli Cèsar. Cèsar utilitzava moltíssim la criptografia per enviar missatges d'una forma aparentment segura. L'emperador simplement substituïa cada lletra del missatge amb la lletra que està tres llocs més endavant en l'alfabet. Els criptògrafs sovint pensen en termes com alfabet pla, l'alfabet que s'utilitza per escriure el missatge original, i en alfabet xifrat, les lletres que substitueixen les de l'alfabet pla. Quan l'alfabet pla es col·loca sobre l'alfabet xifrat, queda clar que l'alfabet xifrat ha estat mogut tres posicions, és per això que aquesta forma de substitució s'anomena xifra de canvi del Cèsar o simplement xifra del Cèsar. Una xifra és qualsevol forma de substitució criptogràfica en que cada lletra es canvia per una altra lletra o símbol.

Alfabet pla :	a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabet xifrat	D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Text pla : veni, vidi, vici

Text xifrat : YHQL, YLGL, YLFL

La xifra del Cèsar aplicada a un missatge curt es pot observar com no ofereix molta seguretat ja que és bastant fàcil desxifrar-la i obtenir el text pla.

La xifra del Cèsar només té 26 possibilitats ja que només es basa en córrer l'alfabet algunes posicions. En canvi, si l'emissor utilitza un algorisme de substitució més general, que permeti que l'alfabet xifrat sigui qualsevol combinació de l'alfabet pla, i no només que es corrin algunes posicions, llavors hi ha 400.000.000.000.000.000.000.000.000 possibles claus entre les quals es pot escollir. Des del punt de vista de l'enemic, si el missatge és interceptat i es coneix l'algorisme (tipus de canvis que s'han aplicat al text pla), encara li queda la terrible feina de revisar totes les claus possibles. Si un agent enemic fos capaç de revisar una clau per segon li portaria aproximadament un bilió de cops la vida de l'univers en revisar totes elles i desxifrar el missatge.

Alfabet pla : a b c d e f g h i j k l m n o p q r s t u v w x y z
Alfabet xifrat : J L P A W I Q B C T R Z Y D S K E G F X H U O N V M

Text pla : et tu, brute?

Text xifrat : WX XH, LGHXW?

L'avantatge d'aquest tipus de xifra, anomenada xifra de substitució monoalfabètica, radica que és fàcil de posar en pràctica i ofereix un alt nivell de seguretat. Per l'emissor és fàcil definir la clau, que realment consisteix a determinar l'ordre de les 26 lletres de l'abecedari xifrat i a l'enemic li serà pràcticament impossible per l'anomenat ''atac per la força bruta'', que és anar comprovant una per una totes les claus possibles.

4.1.1 Desxiframent de la xifra de substitució monoalfabètica

Els àrabs van ser els que van inventar el criptoanàlisi, la ciència de desxifrar un missatge sense conèixer la clau. Els criptoanalistes àrabs van aconseguir trobar un mètode per desxifrar la xifra de substitució monoalfabètica, la qual havia restat invulnerable durant molts segles. El criptoanàlisi no podia ser inventat fins que una civilització hagués aconseguit un nivell suficientment sofisticat d'erudició en vàries disciplines, incloses les matemàtiques, l'estadística i la lingüística. La civilització musulmana va esdevenir el bressol del criptoanàlisi.

Al Kindi va ser l'autor de 290 llibres de medicina, astronomia, matemàtiques, lingüística

i música. El seu tractat més important, que no va ser descobert fins el 1987, es titulava *Sobre el desxiframent de missatges criptogràfics*. Tot i que conté debats sobre estadística, fonètica i sintaxis aràbiga, el revolucionari sistema de criptoanàlisi d'Al Kindi està comprès en la primera pàgina del seu llibre:

> *Una manera de resoldre un missatge xifrat, si sabem amb quina llengua està escrit, és trobar un text pla diferent escrit en la mateixa llengua i que sigui prou llarg per omplir al voltant d'una pagina, llavors comptar quantes vegades apareix cada lletra. A la lletra que aparegui amb més freqüència l'anomenarem <<primera>>, a la següent en freqüència l'anomenarem <<segona>>, la següent <<tercera>>, i així successivament fins que haguem cobert totes les lletres que apareguin en el text.*
>
> *Després observem el text xifrat que volem resoldre i classifiquem els seus símbols de la mateixa manera. Trobarem el símbol que apareix amb més freqüència i el substituirem amb la forma de la lletra <<primera>> de la mostra del text pla, el següent símbol el substituirem per la forma de la lletra <<segona>>, i el següent en freqüència el canviarem per la forma de la lletra <<tercera>>, i així successivament, fins que haguem cobert tots els símbols del criptograma que vulguem resoldre.*

L'explicació d'Al Kindi és més fàcil d'entendre des del punt de vista de l'alfabet anglès. En primer lloc és necessari examinar un fragment de text anglès normal, potser més d'un, per establir la freqüència de cada lletra de l'abecedari. En anglès la lletra més freqüent és la **e**, seguida de la **t** i després la **a** i així successivament. Un cop fet això s'ha d'examinar el text xifrat i examinar la freqüència de cada lletra. Si la lletra més corrent en el text xifrat es, per exemple, la **J**, llavors sembla probable que substitueixi la **e**. I si la segona lletra més freqüent és la **P**, probablement substituirà la **t**, i així successivament. La tècnica d'Al Kindi, coneguda com anàlisis de freqüència, demostra que no és necessari revisar cada una dels billons de claus potencials, sinó que és possible revelar el contingut d'un missatge codificat simplement analitzant la freqüència dels caràcters. Tot i els avantatges que aporta el nou mètode d'Al Kindi, no es pot aplicar sempre incondicionalment. La llista estàndard de freqüències que obtenim d'un o diversos textos plans és només una mitjana i no correspondrà exactament a les freqüències de cada text. En general és probable que els textos curts es desviïn significativament de les freqüències normals i si tenen menys de cent paraules, el seu desxiframent serà molt difícil.

Molts cops pot passar que la freqüència dels textos llargs que vulguem desxifrar

tampoc coincideixi a la perfecció amb la freqüència que nosaltres tenim. En aquest cas s'ha d'anar jugant amb les lletres la freqüència de les quals sigui més alta, per anar desxifrant el missatge poc a poc. Per exemple, pot ser que la lletra amb freqüència més alta d'un text xifrat sigui la **N** i que no representi la **e**, podria representar la **t** o la **a**, que darrere la **e** són les lletres més freqüents. Es tracta d'anar provant les diferents lletres i deduir quin valor correspon a cadascuna.

4.2. La xifra de substitució polialfabètica o xifra Vigenère

Durant segles, la xifra de substitució monoalfabètica simple era prou forta per assegurar els secrets. El desenvolupament de l'anàlisi de freqüència, primer en l'Aràbia i després a Europa va destruir la seva seguretat. En aquest punt, en el combat entre criptògrafs i criptoanalistes, estava clar que aquests últims portaven les de guanyar. Qualsevol persona que enviava un missatge codificat havia d'acceptar que un desxifrador enemic expert podria interceptar i desxifrar els seus més valuosos secrets.
Els criptògrafs havien de donar un pas més i inventar una xifra més sòlida, quelcom que pogués despistar els criptoanalistes. Aquesta xifra no va sorgir fins a finals de segle XV. Finalment el que va descobrir aquesta nova xifra va ser Blaise de Vigenère, un diplomàtic francès nascut el 1523. Al principi, el seu interès en la criptografia era merament pràctic i es relacionava amb el seu treball de diplomàtic. Després, a l'edat de trenta-nou anys ja havia acumulat prou fortuna per abandonar la seva carrera i dedicar la seva vida a l'estudi.
La força de la xifra Vigenère, en honor a l'home que la va inventar, radica en què no utilitza un alfabet, sinó 26 alfabets xifrats diferents per a codificar un sol missatge. El primer pas de la codificació és crear el que s'anomena un quadre Vigenère (fig. 3.4.). Es tracta d'un alfabet pla seguit de 26 alfabets xifrats, de manera que cadascun d'ells comença amb la següent lletra que l'anterior. D'aquesta forma, la línia 1 representa un alfabet xifrat amb un canvi del Cèsar d'una posició, la qual cosa significa que es podria utilitzar per posar en pràctica una xifra de canvi del Cèsar en què cada lletra del text pla és substituïda per la lletra següent de l'alfabet. De manera similar, la línea 2 representa un alfabet xifrat amb un canvi del Cèsar de dues posicions, i així successivament. La línia superior del quadre en minúscules representa les lletres del text pla. Es podria codificar cada lletra del text pla segons un dels 26 alfabets xifrats. Per exemple, si s'utilitza l'alfabet xifrat número 2 llavors la lletra **a** es codifica com **C**, però si s'utilitza l'alfabet xifrat número 12, llavors la **a** es codifica com **M**.
Si l'emissor només utilitzés un dels alfabets xifrats per codificar tot un missatge, realment es tractaria d'una simple xifra del Cèsar, la qual cosa seria un forma de codificació molt dèbil, fàcilment desxifrable per un criptoanalista enemic. En canvi, en

la xifra Vigenère s'utilitza una línia diferent del quadre Vigenère (un alfabet xifrat diferent) per xifrar les diferents lletres del missatge. D'aquesta manera, l'emissor podria xifrar la primera lletra segons la línia 5, la segona segons la línia 19...

Text pla	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
8	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
9	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Fig. 3.4. Quadre Vigenère, necessari per xifrar i desxifrar missatges a través del mètode Vigenère.

Per desxifrar el missatge, el receptor a qui va dirigit necessita saber quina línia del quadre Vigenère ha estat utilitzada per codificar cada lletra, de manera que hi ha d'haver un sistema acordat per canviar de línia. Això s'aconsegueix utilitzant una paraula clau. Per il·lustrar com s'utilitza una clau amb el quadre Vigenère per xifrar un missatge curt xifrarem la frase **tropes al turó est**, utilitzant la clau BLANC. Per començar, es lletreja la clau sobre el missatge, repetint-la les vegades que sigui necessari fins que cada lletra del missatge quedi associada amb una lletra de la clau. Per xifrar la primera lletra, **t**, s'ha de començar per identificar la lletra clau que hi ha sobre ella, **B**, que al seu torn defineix una línia particular en el quadre Vigenère. La línia que comença per **B**, la línia 1, és l'alfabet xifrat que s'utilitzarà per trobar la lletra que substituirà la **t** del text pla. Observem on es creua la columna que comença per **t** amb la línia que comença per **B** i resulta ser la lletra **U**. Per tant, a aquella lletra **t** del text pla la representa la lletra **U** en el text xifrat.

Clau : B L A N C B L A N C B L A N C

Text pla : T r o p E s a l t u R O e S t

Text xifrat : U C O C G T L L G W S Z E F V

Per codificar la segona lletra del missatge, **r**, repetim el procés. La lletra clau que hi ha

sobre la **r** és la **L**, de manera que la codificarem mitjançant una línia diferent del quadre Vigenère. Per codificar la **r** observem on es creua la columna que comença per **r** amb la línia que comença per **L**, i resulta ser la lletra **C**. D'aquesta manera, a aquella lletra **r** del text pla li correspon la **C** del text xifrat. Cada lletra de la clau indica un alfabet xifrat determinat del quadre Vigenère.

El gran avantatge de la xifra Vigenère és que resulta inexpugnable per l'anàlisi de freqüència d'Al Kindi. Per exemple, un criptoanalista que aplica l'anàlisi de freqüència a un text xifrat, generalment comença identificant la lletra més corrent en el text xifrat i assumeix que a aquella lletra li pertany la lletra més corrent d'aquell idioma. Però en realitat la lletra més corrent del text xifrat pot representar moltes lletres del text pla.

A més a més de ser invulnerable a l'anàlisi de freqüència, la xifra Vigenère té un número enorme de claus. L'emissor i el receptor poden acordar de fer servir qualsevol paraula del diccionari, qualsevol combinació de paraules, fins i tot crear paraules. Un criptoanalista seria incapaç de buscar totes les claus perquè el nombre d'opcions és simplement massa gran.

A causa de la solidesa i garantía de seguretat semblaria natural que la xifra Vigenère hagués estat adoptada ràpidament pels secretaris de xifres de tot Europa. Per contra, els secretaris de xifres semblaven haver rebutjat la xifra Vigenère. Aquest sistema, aparentment perfecte, es mantindria pràcticament ignorat durant els dos segles següents.

4.2.1El desxiframent de la xifra Vigenère

Les formes tradicionals de xifra de substitució, les que ja existien abans de la xifra Vigenère, s'anomenen xifres de substitució monoalfabètica perquè utilitzaven només un alfabet xifrat en cada missatge. La naturalesa polialfabètica de la xifra Vigenère és el que li dóna la seva força, però també fa que sigui molt més complicada de fer servir.

Apart de l'extra de dificultat que suposava utilitzar aquesta xifra, al llarg del temps es va anar implantant i popularitzant. Aquesta extensió es deu a l'alta seguretat que proposava i a l'extensió del mètode d'anàlisi de freqüències. No va ser fins els segle XIX que es va aconseguir trencar aquesta xifra quasi perfecta.

La figura més fascinant del criptoanàlisi del segle XIX és Charles Babbage(fig. 3.5.), l'excèntric geni britànic més conegut per desenvolupar el precursor de l'ordinador modern. Mentre que la majoria de criptoanalistes havien perdut tota esperança en arribar a desxifrar la xifra Vigenère, a Babbage el va animar a intentar el desxiframent un intercanvi de cartes amb John Brock Thwaites, un dentista amb un innocent concepte de les xifres.

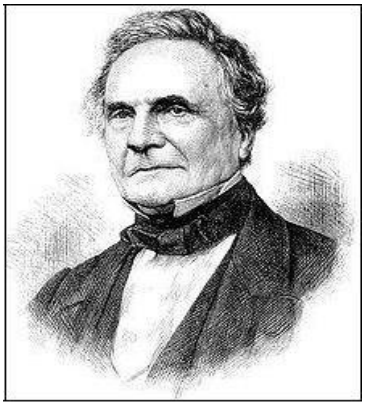


Fig. 3.5. Imatge de Charles Babbage, polifacètic geni que va contribuir en molts avenços, els més significatius en el camp de la criptografia i en desenvolupar el primer concepte d'ordinador.

Desxifrar una xifra difícil es similar a escalar la cara molt escarpada d'una muntanya. El criptoanalista busca qualsevol sortint o escletxa per trobar la més lleugera ajuda. En una xifra monoalfabètica, el criptoanalista s'agafaria a la freqüència de les lletres. En la polialfabètica xifra de Vigenère, les freqüències estan molt més equilibrades perquè es canvia entre diferents alfabets xifrats. Per això a primera vista, la muntanya sembla impossible d'escalar.

Recordem que la gran força de la xifra Vigenère és que la mateix lletra serà codificada de moltes maneres diferents. Per exemple, si la paraula clau és **KING**, llavors cada lletra del text pla pot estar potencialment codificada de quatre maneres diferents, perquè la clau té quatre lletres. Cada lletra de la clau defineix un alfabet xifrat diferent en el quadre Vigenère.

De manera similar, paraules senceres seran desxifrades de maneres diferents: la paraula **the**, per exemple, podria ser codificada com **DPR**, **BUK**, **GNO** o **ZRM**, depenent de la seva posició amb relació amb la clau. Tot i que això dificulta moltíssim el criptoanàlisi, tampoc fa que sigui impossible. La informació important que s'ha d'extreure és que si només hi ha quatre maneres de codificar la paraula **the**, i el missatge original conté varis casos de la paraula **the**, llavors és altament provable que alguna de les quatre codificacions possibles es repeteixin en el text xifrat.

Babbage es va adonar que aquest tipus de repetició li proporcionava una molt bona ajuda per poder escalar la muntanya de la xifra Vigenère. Va aconseguir definir una sèrie de passos que qualsevol criptoanalista podria executar per desxifrar la fins llavors *chiffrre indéchiffrable*. La primera fase del criptoanàlisi de Babbage és buscar seqüències de lletres que apareguin més d'un cop en el text xifrat. Aquestes repeticions poden sorgir de dues formes diferents. La més provable és que la mateixa seqüència de lletres del text pla hagin estat codificades utilitzant la mateixa part de la clau. Com alternativa, existeix la possibilitat que dues seqüències diferents del text pla hagin estat codificades usant diferents parts de la clau, resultant per casualitat en una seqüència idèntica en el text xifrat. Si ens limitem a les seqüències llargues, llavors podem descartar la segona possibilitat i en aquest cas, només considerarem les

seqüències repetides que tinguin quatre lletres o més.

A més a més d'utilitzar-se per codificar el text pla i convertir-lo en text xifrat, la clau la fa servir també el receptor per desxifrar el text xifrat i tornar-lo a convertir en text pla. Per això, si poguéssim identificar la clau, desxifrar el text seria molt fàcil. En aquest pas encara no tenim prou informació per començar a extreure la clau.

En aquest punt, un cop tenim uns quants fragments repetits de text xifrat, s'ha d'intentar buscar la llargària de la clau. Aquest procés és bastant complex i pot resultar molt entretingut, però bàsicament es tracta de buscar els espais entre les diferents repeticions en el text xifrat.

Si sabem l'espai que hi ha entre les diferents repeticions del text xifrat, es pot trobar el divisor comú entre el nombre de lletres que tenen els espais de les repeticions. El divisor comú dels espais dels fragments repetits equival a la llargària de la clau. Per exemple, si tenim quatre tipus de repeticions i l'espai de la primera és de 95 lletres, la segona 5, la tercera 20 i la quarta 120, podem deduir que l'únic divisor comú és el número 5, de manera que la clau utilitzada per xifrar aquell text tindrà cinc lletres.

Un cop ja coneixem la llargada de la clau, el següent pas és decidir quines són exactament les seves lletres. Ara anomenarem la clau L1-L2-L3-L4-L5, de forma que L1 representi la primera lletra de la clau i així successivament. El procés de codificació hauria començat codificant la primera lletra del text pla segons la primera lletra de la clau, L1. La lletra L1 proporciona un determinat alfabet xifrat del quadre Vigenère, però a l'hora de codificar la segona lletra utilitzarem l'alfabet xifrat que ens marqui L2. La tercera lletra del text pla serà codificada segons L3, la quarta segons L4 i la cinquena segons L5. Tot i això, la sisena lletra del text pla seria codificada un altre cop com L1 i el cicle es repetiria.

Sabem que una de les línies del quadre Vigenère , definida per L1, proporciona l'alfabet xifrat per codificar les lletres 1ª, 6ª, 11ª, 16ª..., del missatge. Per tant, podríem utilitzar l'anàlisi de freqüència per deduir l'alfabet xifrat en qüestió. Un cop es fa l'anàlisi de freqüència de les lletres que pertanyen a L1, es compara aquest amb l'anàlisi de freqüència d'un text pla. Com que els alfabets del quadre Vigenère són alfabets normals moguts unes quantes posicions, si comparem el lloc on es troben les freqüències més altes i baixes de les lletres que pertanyen a L1 i les freqüències d'un text pla, podrem deduir quin alfabet del quadre Vigenère és.

Un cop tenim aquesta informació ja sabrem el valor de la primera lletra de la clau, L1 i totes les paraules que xifrava L1. D'aquesta manera es pot seguir trobant L2, L3... fins que la clau sigui fàcilment deduïble o en cas contrari trobar totes les paraules de la clau. Un cop tenim la clau ja només ens falta desxifrar el missatge com ho faria el receptor del missatge.

4.3. La criptografia en els ordinadors: l'últim pas abans de la criptografia quàntica

A mesura que van anar sorgint els ordinadors i la informàtica va començar a guanyar importància, la criptografia va passar a un nivell superior i va ser transcendent en tots els nivells de la societat. Abans que sorgissin els ordinadors, la criptografia era una eina bàsicament utilitzada pels governs, sobretot la part militar, i en les comunicacions entre gent de gran poder i importància. També pot ser que la gent normal utilitzés mètodes criptogràfics, però era una minoria i només ho utilitzaven en casos excepcionals.

Amb l'arribada dels ordinadors, va començar a ser un problema les transmissions d'informació a través de la xarxa. Pot ser que no existís un Internet com el coneixem avui en dia però es podia establir una comunicació entre dos o més ordinadors i era un perill fer-ho sense un bon mètode criptogràfic.

Utilitzar un ordinador per codificar un missatge és, en gran mesura, molt semblant a les formes convencionals. En realitat, només hi ha tres diferències significatives entre la codificació per ordinadors i la codificació mecànica que constituïa la base de xifres com l'Enigma[14]:

- La primera diferència és que una màquina de xifres mecànica té la limitació del que es pot construir pràcticament, mentre que un ordinador pot imitar una hipotètica màquina de xifres d'immensa complexitat. Per exemple, es pot programar un ordinador per imitar l'acció de cent modificadors girant en diferents sentits. Una màquina mecànica seria impossible de construir en la pràctica.
- La segona diferència és simplement una qüestió de velocitat. L'electrònica pot funcionar molt més ràpidament que els modificadors mecànics: un ordinador programat per imitar la xifra enigma podria codificar un missatge extens en un instant (fig. 3.9.).
- La tercera diferència és que un ordinador modifica números en lloc de les lletres de l'alfabet. Els ordinadors només operen amb números binaris: seqüències d'uns i zeros coneguts com dígits binaris o bits. Per tant, abans de la codificació s'ha de convertir qualsevol missatge en dígits binaris. El protocol més utilitzat per a fer aquesta conversió és l'ASCII (American Standard Code for Information Interchange).

[14] Màquina portàtil per encriptar i desencriptar missatges utilitzada durant la segona guerra mundial pels alemanys.

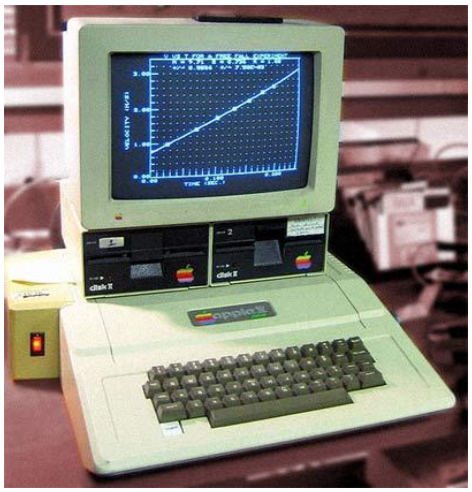


Fig. 3.9. Gràcies als ordinadors, es poden simular moltes formes de criptografia a una velocitat extremadament més gran que hauria de xifrar de forma convencional.

Tot i tractar-se de números, la forma de xifrar els missatges que es volen enviar seguia sent la mateixa. El problema era que pràcticament cap de les xifres del moment oferia una seguretat extremadament alta, de manera que es va decidir utilitzar els avantatges dels ordinadors per trobar algun mètode millor.

Una de les primeres formes de criptografia utilitzada en els ordinadors va ser el sistema Llucifer. Llucifer agafa paquets de 64 bits d'informació i els combina. Un cop estan combinats, a cada paquet li aplica una sèrie de processos, com dividir el paquet en més parts i mesclar-les diferents vegades. El procés s'assembla una mica a amassar un tros de massa de pa. Primer el tros llarg es divideix en trossos més petits i després cadascun dels trossos petits són amassats unes quantes vegades.

El gran problema d'aquest sistema és que la pròpia clau, que ''descrivia'' la forma en com es barrejaven aquests paquets de bits, no podia ser enviada a través dels ordinadors, ja que podia ser interceptada. La clau d'enviar-se de forma convencional, com per exemple una carta o un document. Això limitava moltíssim la transmissió d'informació ja que les comunicacions entre diferents ordinadors eren rapidíssimes però la distribució de la clau era molt lenta. Aquest factor condicionava molt la velocitat de les comunicacions.

En aquest punt el que es necessitava era una forma de xifrar que, a més a més d'oferir una màxima seguretat, es pogués dur a terme sense haver de compartit una clau prèviament. Es van fer molts intents i van haver-hi molts sistemes prometedors però al final el que va triomfar va ser l'algorisme RSA (Rivest, Shamir y Adleman).

4.3.1 L'algorisme RSA

L'algorisme RSA fou descrit el 1977 per **R**on Rivest, Adi **S**hamir i Len **A**dleman a l'Institut de Tecnologia de Massachusetts. Aquesta xifra es basa en les funcions d'una sola via, concretament en àlgebra modular. Aquestes funcions es caracteritzen perquè és molt

fàcil crear-les o obtenir un resultat però és pràcticament impossible desfer el resultat obtingut i obtenir els factors inicials.

Quan s'utilitzen els ordinadors per fer criptografia, normalment l'emissor és anomenat Alice i el receptor Bob i en cas que hi hagués un espia aquest s'anomena Eve.

No explicaré els detalls matemàtics de l'algorisme RSA però el sistema es basa en què l'Alice primer ha de crear una clau pública, la qual publicarà perquè el Bob (i tot el món) puguin utilitzar-la per codificar els missatges dirigits cap a ella. Com que la clau pública és una funció d'una sola via ha de ser virtualment impossible que ningú la pugui invertir i descodificar els missatges que se li envien a l'Alice. Però l'Alice necessita descodificar els missatges que li envien. Per tant, ha de tenir una clau privada, una informació especial que li permeti invertir l'efecte de la clau pública. Per consegüent, només l'Alice té el poder per descodificar els missatges dirigits a ella.

D'aquesta forma, l'Alice primer tria dos nombres primers (que només són divisibles per la unitat o per ells mateixos), per exemple, **p** i **q**. Llavors els multiplica (**p** x **q**) i li dóna un nombre **N**. Gràcies a les operacions modulars, l'Alice només ha de publicar **N** i un altre nombre anomenat **e** (necessari per codificar). El Bob mira quina és la seva clau pública i utilitza aquests dos nombres per codificar el missatge. Quan el missatge ha arribat a l'Alice, utilitza els nombres **p** i **q** per descodificar-lo. Aquest mètode es basa en la simplicitat que hi ha en fer una multiplicació (**p** x **q**) i obtenir **N** però la dificultat és a partir de **N** poder trobar **p** i **q**. L'única manera d'aconseguir-ho és factoritzant (trobar els nombres que multiplicats resulten **N**), un procés molt complex i lent per a les computadores convencionals, ja que cada cop que és més gran el número **N**, la dificultat augmenta exponencialment.

Amb les computadores quàntiques, com que a més de treballar amb zeros i uns, treballen amb els dos valors a la vegada (superposats), es va desenvolupar un procediment anomenat algorisme de Shor, amb el qual es podria factoritzar el nombre **N** molt fàcilment. Des del 1977 fins l'actualitat seguim utilitzant la mateixa tècnica de xifratge, l'algorisme RSA. Els temps estan canviant i pot ser que en un futur no molt llunyà no en tinguem prou amb la RSA, però per sort ja tenim una alternativa molt seductora i perfecta, la criptografia quàntica.

5.CRIPTOGRAFIA QUÀNTICA

Els protocols de criptografia quàntica intenten aconseguir que tant l'emissor com el receptor pugin compartir una determinada clau de forma segura, tant segura que es creu que si es practiquessin els protocols de criptografia quàntica d'una forma perfecta (sense errors experimentals), amb les lleis del nostre univers és impossible aconseguir la informació que l'emissor i el receptor s'estan enviant.

Aquí està la ''màgia'' de la física quàntica, com que pel simple fet d'observar ja s'altera qualsevol estat, si l'espia intenta observar les comunicacions entre l'Alice (emissor) i el Bob (receptor), "destrossarà" la clau que es volien enviar, de manera que se n'adonaran que no comparteixen la mateixa clau i per tant, que els estan espiant.

Els protocols de criptografia quàntica no serveixen per enviar un missatge sencer d'una forma segura i invulnerable, amb ells només es pot enviar la clau. Això passa gràcies que la clau que comparteixen ha de ser aleatòria i per tant, és igual si se'n perden alguns trossos durant la comunicació, fet que passa amb tots els protocols. Si apliquéssim la criptografia quàntica al missatge que es vol enviar, una vegada el Bob hagués passat el missatge que hauria rebut del codi binari a text normal, obtindria un galimaties que no entendria de cap manera; això es deu que durant la comunicació s'eliminen parts i l'estructura del missatge es perdria. Un altre dubte que pot sorgir quan tractem la criptografia quàntica i que causa molta confusió, és quan es tracta aquest camp de manera superficial; és el fet que si amb la criptografia quàntica només podem compartir una clau de forma segura, després com es xifra el missatge? Poden desxifrar-lo tot i que no sapiguem la clau? La resposta és que la criptografia quàntica només s'encarrega de la distribució de la clau de forma totalment perfecta, ja existeix una forma de criptografia que és matemàticament indesxifrable. D'aquesta manera, la criptografia quàntica acaba tancant la gran escletxa que quedava en el món de la criptografia, la distribució de la clau d'una forma totalment segura.

Aquesta forma perfecta de fer criptografia s'anomena la xifra de quaderns d'un sol ús. Tot i que ja es va descobrir en la primera guerra mundial, pràcticament mai no s'ha usat a causa de la incomoditat que comporta. Es tracta d'utilitzar la xifra Vigenère (pàg. 30) però aquest cop, en lloc d'utilitzar una clau formada per una paraula o com a màxim una frase, es crea un seguit de lletres aleatòries, tantes com lletres tingui el text pla, de manera que la clau serà tant llarga com el propi text i mai es repetirà (fig. 4.1.). Després es xifraria el missatge de la forma de sempre, mirant la taula Vigenère i anar transcrivint, igual que amb la xifra Vigenère normal. Es pot imaginar la dificultat que suposa utilitzar aquesta xifra, sobretot quan va sorgir. Només va ser usada per comunicacions entre els presidents dels països més importants. S'utilitzaven uns

quaderns plens de lletres aleatòries per dur-la a terme, d'aquí el seu nom. Fins i tot amb l'arribada dels ordinadors ha estat complicat utilitzar aquesta xifra, ja que la solució pràctica per evitar s'havia de compartir la clau entre l'Alice i el Bob ha estat la RSA, en que la clau de l'Alice és pública i el Bob xifra el missatge amb aquesta, llavors l'Alice amb una clau diferent el desxifra. Però qui sap si ja existeix un mètode ràpid de factoritzar* i si no és així, quan les computadores quàntiques es puguin aplicar pràcticament, aquestes podran fer-ho.

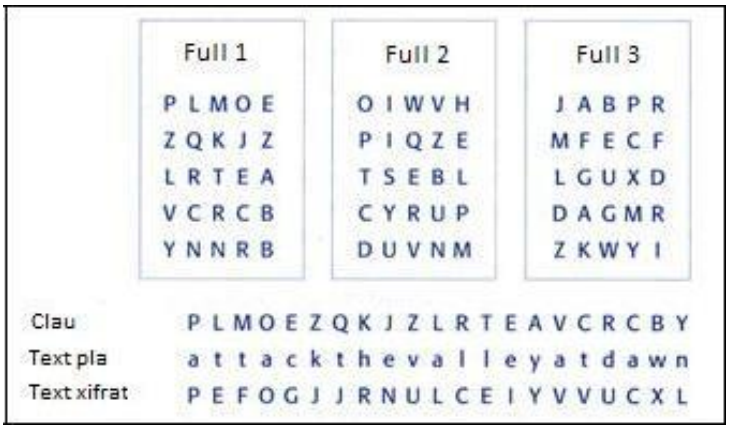


Fig. 4.1. En aquesta imatge podem veure com a cadascuna de les lletres del text pla (attack the valley at dawn) se li assigna una lletra aleatòria. Llavors amb aquesta clau es procedeix a xifrar amb el mètode Vigenère.

Havia de passar la clau, ja sigui físicament o ara a través dels ordinadors, ha estat molt perillós i un risc que sempre s'ha intentat evitar; ara amb la criptografia quàntica la molèstia i el gran perill d'enviar la clau ja ha deixat d'existir i ara no hi ha cap problema per utilitzar la xifra de quaderns d'un sol ús. D'aquesta manera, combinant la criptografia quàntica, per comunicar-se la clau sense problemes i la xifra de quaderns únics, per poder tenir un text impossible de desxifrar sense la clau, sembla que ens apropem a la forma perfecta de criptografia. Potser aquest cop els criptògrafs han guanyat definitivament.

Abans d'introduir el funcionament dels principals protocols d'encriptació quàntica, és molt recomanable entendre l'ignitor o idea inicial que va ajudar que es creés el primer protocol de criptografia quàntica.

Per entendre millor aquest apartat:

http://www.youtube.com/watch?v=HihQ6eIGNAs (video 6)

5.1. Diners quàntics

Primerament, abans de la criptografia quàntica, va sorgir una idea que feia servir els mateixos conceptes i principis de la física quàntica, la qual va ser el pas previ a la criptografia quàntica.

Es podria dir que la base del concepte de criptografia quàntica va sorgir de la idea d'un peculiar personatge anomenat Stephen Wiesner. En aquells moments era un estudiant graduat de la Universitat de Columbia, el seu problema va ser que va tenir una idea

massa avançada per la seva època i pràcticament ningú el va prendre amb seriositat, a més la tecnologia en aquest àmbit estava molt poc desenvolupada.

Wiesner proposava la idea dels diners quàntics que no podien ser falsificats de cap forma, aparentment un gran avantatge. La seva idea es basava principalment en la física dels fotons. Quan un fotó viatja per l'espai vibra; els fotons poden viatjar amb la mateixa direcció però l'angle de vibració de cadascun d'ells pot ser diferent en cada cas. L'angle de vibració dels fotons és conegut amb el nom de polarització del fotó. El Sol o una bombeta generen fotons amb pràcticament totes les polaritzacions possibles, de manera que si miréssim un a un els fotons, en podríem trobar alguns que vibrarien amunt i avall, altres d'un costat a un altre i altres amb angles intermedis. Per simplificar-ho suposarem que els fotons només tenen quatre polaritzacions possibles : (↕ ↔ ↘ ↗).Si posem un filtre (anomenat Polaroid) en un raig de llum, podem assegurar-nos que tots els fotons que passin tindran el mateix angle de vibració, és a dir que tindran la mateixa polarització. Un bon exemple és pensar en una reixa formada per filferros amb una orientació vertical, si deixéssim caure llapis de colors sobre aquesta reixa, uns quants passarien a causa que coincidirien amb l'espai que hi ha entre cada fil ferro, però els llapis que no estiguin alineats amb l'angle correcte no passarien i es quedarien sobre la reixa metàl·lica. Tots els fotons que tinguin el mateix angle de polarització que el filtre Polaroid, per exemple vertical, passaran sense problemes, però aquells que estiguin polaritzats horitzontalment no podran passar i es quedaran atrapats en el filtre (fig. 4.2.).

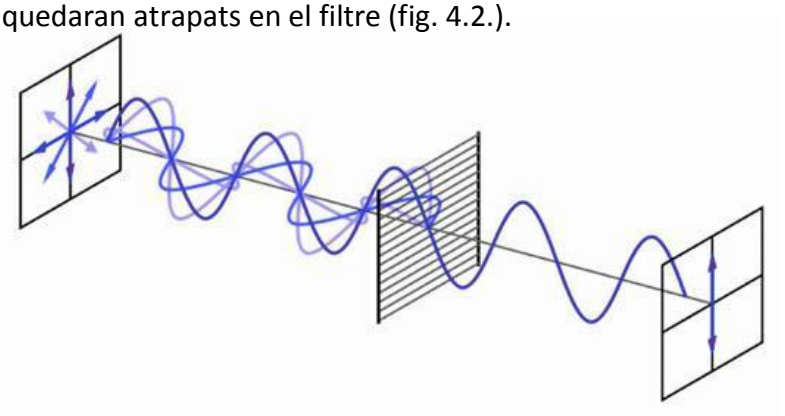


Fig. 4.2. Fotons representats com ones on el pla de l'ona és el pla de polarització dels fotons, podem observar que quan arriben al filtre només passen els fotons que tenen una certa polarització, els altres es queden aturats al filtre.

Com que estem tractant amb partícules molt petites, sorgeixen aspectes quàntics que fan possible el concepte dels diners quàntics. Quan els fotons estan polaritzats diagonalment i han de passar per un filtre vertical, en lloc de quedar-se atrapats com en teoria ho farien els llapis, tenen el 50% de possibilitats de passar o d'aturar-se. Aquest fet es deu que aquests fotons es troben en un dilema quàntic entre passar i no passar, i en trobar-se amb un angle de polarització intermedi entre el vertical i l'horitzontal, les possibilitats de passar i no passar són les mateixes. Un exemple de filtres són les ulleres de sol Polaroid, que només deixen passar la llum amb una certa polarització. Si mirem només per una de les lents, naturalment ho veuríem tot molt

més fosc a causa que la lent bloqueja molts dels fotons que de l'altra manera arribarien als nostres ulls; a més tots els fotons que ens arriben tindran la mateixa polarització. Ara si poguéssim treure l'altra lent de les ulleres i col·locar-la sobre la primera i la féssim girar, hi hauria un moment en què només podríem notar l'efecte d'una lent, de manera que tots els fotons que ens arribarien amb la primera lent sola ara ens arriben amb les dues; això es perquè l'orientació de les dues lents és la mateixa, de manera que tots els fotons que passen per la primera lent també passaran per la segona. Si girem la segona lent 90º tot es tornarà completament fosc (fig. 4.3.). Això és a causa que en aquesta configuració la polarització de la primera lent és perpendicular a la de la segona lent, de manera que tots els fotons que surten de la primera lent es quedaran aturats en la segona, per exemple, si la primera té una orientació vertical, els fotons que passin xocaran quan es trobin la segona lent que tindrà una polarització horitzontal. En canvi, si col·loquem la lent en un angle de 45º arribarà un punt en què la meitat dels fotons que passen per la primera lent passaran per la segona.

Fig. 4.3. Depenent de la forma en què col·loquem diferents filtres Polaroid, podem aconseguir que la llum passi menys o fins i tot que no passi cap fotó. Per exemple, si posem dos filtres Polaroid un davant de l'altre, podem arribar a aconseguir que no passi llum.

Wiesner va pensar a utilitzar la polarització dels fotons per poder crear bitllets que mai no poguessin ser falsificats. La seva idea era que els bitllets tinguessin 20 trampes de llum al seu interior, diminuts sistemes capaços d'atrapar un fotó amb una polarització concreta i mantenir-la. Els bancs podrien utilitzar quatre filtres Polaroid orientats de quatre maneres diferents (↕ ↔ ↘ ↗) per poder omplir les 20 trampes de llum amb una seqüència de 20 fotons polaritzats, de manera que cada bitllet tingués una seqüència de polarització diferent, que el fes únic. Un exemple seria un bitllet que tingués la següent seqüència: ↘ ↕ ↗ ↗ ↔ ↕ ↕ ↘ ↕ ↘ ↔ ↔ ↗ ↔ ↘ ↗ ↔ ↗ ↕ ↕
Aquestes seqüències de polarització quedarien aparentment ocultes dins de les trampes de llum, de manera que no es podrien observar a simple vista en els bitllets. A més a més dels 20 fotons polaritzats, els bitllets tindrien un número de sèrie imprès. Per exemple, aquest bitllet (fig. 4.4.) té el B2801695E. El banc tindria una llista mestra amb les seqüències de polarització de cada bitllet que estigués circulant i el seu número de sèrie corresponent.

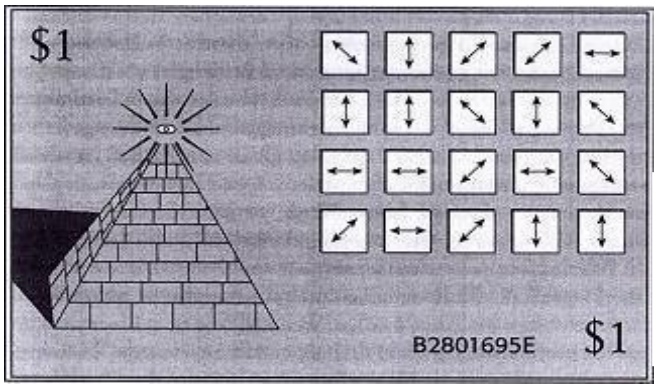


Fig. 4.4. Els bitllets quàntics tindrien 20 trampes de llum ocultes i un número de sèrie, de manera que només el banc pogués conèixer la seva seqüència de polarització i en cas que algú intentés falsificar-los, quan arribessin al banc serien detectats.

Aquests bitllets tenen el gran avantatge que són impossibles de falsificar. Si un falsificador agafés un bitllet fals omplint-lo amb 20 fotons amb polaritzacions aleatòries i li assignés un número de sèrie qualsevol, quan aquest bitllet arribés al banc, com que ells tenen una llista mestra amb totes les seqüències de polarització i el seu corresponent número de sèrie, veurien que la polarització dels fotons d'aquell bitllet no coincidiria amb el número de sèrie assignat. L'única opció que tindria un falsificador seria intentar fer còpies a partir d'un bitllet de mostra però per fer-ho primer necessitaria fer un pas pràcticament impossible, que és alliberar els fotons de les trampes del bitllet genuí per a poder veure les seves polaritzacions i si hipotèticament ho aconseguís, com que ja tindria la informació de la seqüència de polaritzacions, només hauria d'omplir els dos bitllets amb aquella seqüència i procurar que el bitllet fals també tingués el mateix número de sèrie que el bitllet de mostra. La gràcia d'aquest sistema rau en la dificultat per poder determinar la polarització dels fotons que resten tancats en les trampes de llum. L'única manera de determinar la polarització dels fotons és utilitzant un filtre Polaroid. Per precisar la polarització d'un fotó en una trampa de llum en particular, el falsificador selecciona un filtre Polaroid i l'orienta d'una manera particular, posem verticalment (↕). Si casualment el fotó que surt de la trampa de llum està polaritzat verticalment, aquest passarà pel filtre Polaroid vertical i el falsificador suposarà acertadament que es tracta d'un fotó amb una polarització vertical. Si el fotó provinent de la trampa de llum té una polarització horitzontal, quan arribi al filtre Polaroid orientat verticalment no podrà passar, de manera que el falsificador suposarà també acertadament que la polarització d'aquell fotó és horitzontal. El problema apareix quan el fotó que surt de la trampa de llum està polaritzat diagonalment (↘ o ↗) ja que podria passar per el filtre o podria no fer-ho, i en els dos casos el falsificador no podrà identificar la veritable naturalesa del fotó. Recordem que tenim un filtre Polaroid orientat verticalment, de manera que si hi fem passar un fotó orientat diagonalment, a causa de la física quàntica hi ha un 50% de possibilitats que passi, com si fos un fotó amb una polarització vertical i un 50% que no passi, com si fos un fotó amb una polarització horitzontal. D'una altra manera, si el

falsificador decideix orientar el filtre Polaroid diagonalment cap a l'esquerra (↘), podrà detectar correctament tots els fotons que estiguin polaritzats diagonalment, però aquells que tinguin una polarització vertical o horitzontal els confondrà com si tinguessin una polarització diagonal, ja pot ser cap a l'esquerra (↘) com cap a la dreta (↙).

El falsificador hauria d'utilitzar el filtre Polaroid orientat correctament per a cada un dels fotons de les trampes de llum, si no ho aconsegueix llavors obtindrà una seqüència de polarització que no pertany a la d'aquell bitllet. Per exemple, si fa servir un filtre que polaritza diagonalment cap a l'esquerra (↘) per detectar el fotó que surt de la segona trampa de llum del nostre bitllet i el fotó no passa pel filtre, el falsificador pot estar segur que aquell fotó no tenia una polarització diagonal cap a l'esquerra (↘), però no pot saber si era un fotó polaritzat diagonalment cap a la dreta (↙), que realment no hauria passat pel filtre, o si tenia una polarització vertical o horitzontal (↕ o ↔), que tenien un 50% de passar o de quedar bloquejades en el filtre Polaroid.

Un pot pensar que si els falsificadors tenen aquest problema per precisar la seqüència de polarització dels bitllets, també hauria de ser impossible per als bancs poder identificar-los. L'avantatge que tenen els bancs és que ells tenen la llista mestra on hi ha escrites totes les seqüències de polarització i el seu corresponent número de sèrie. Només haurien de mirar a la llista mestra quina seqüència de polarització pertany al número de sèrie del bitllet que volen comprovar. Un cop la tenen, alliberen els fotons de les trampes de llum i com ja saben quina hauria de ser la seva polarització, ja utilitzen els filtres Polaroid adients. En cas que detectin que la seqüència de polaritzacions que hi ha a la llista mestra no és igual a la del bitllet, llavors sabran que aquell bitllet ha estat falsificat. Això és degut que el falsificador mai no pot detectar la seqüència de polarització del bitllet de mostra correctament, la còpia sempre portarà una seqüència incompatible amb el seu número de sèrie i un cop el bitllet arribi al banc, serà detectat. En cas que la seqüència de polarització del bitllet coincideixi amb la de la base de dades del banc, es tornarien a omplir les trampes de llum del bitllet amb els fotons polaritzats correctament i es tornaria a posar en circulació.

Per resumir-ho, els diners quàntics són impossibles de copiar i si un falsificador decideix fer una còpia amb polaritzacions aleatòries, un cop el bitllet arribi al banc, en extreure els fotons i veure que no coincideixen les polaritzacions amb les de la llista podran detectar que aquell bitllet és fals.

Els diners quàntics de Wiesner va ser una idea totalment increïble i original però per desgràcia és pràcticament inviable. Els enginyers encara no han aconseguit crear una tecnologia per poder emmagatzemar fotons amb una determinada polarització al llarg del temps, i si existeix es troba en un estadi molt primari, no per l'ús a gran escala. L'altre inconvenient és que encara que la tecnologia estigués prou desenvolupada per a

poder crear els diners quàntics, seria caríssim posar-la a la pràctica, costaria aproximadament un milió de dòlars protegir cada bitllet americà d'un dòlar. Tot i la inviabilitat que suposen els diners quàntics, aquesta idea utilitzava d'una forma molt original diferents conceptes de la física quàntica. Tot i això, Wiesner a part de rebre una manca de suport per part del director de la seva tesis doctoral, va presentar la idea a diverses revistes científiques, que no hi van parar atenció i van rebutjar la seva idea.

5.2. Protocol BB84

Pot ser que els diners quàntics mai no es portessin a la pràctica però van servir de base i d'inspiració per a crear el primer protocol de criptografia quàntica.

Tot i la poca acceptació de la idea de Wiesner hi havia una persona que compartia el seu entusiasme pels diners quàntics. Es tractava de Charles Benett, que uns anys abans havia estudiat amb ell a la Universitat. Una de les característiques més destacables de la personalitat de Benett era la seva curiositat per tots els aspectes de la ciència. Des de ben petit sabia que volia ser científic i al llarg dels anys aquesta eufòria no va disminuir. Va cursar la carrera de química a la Universitat de Brandeis, en el seu doctorat es va centrar en la química aplicada a la física i després va passar a fer investigacions sobre física, matemàtiques, lògica i finalment informàtica.

Wiesner, conscient dels amplis coneixements del seu amic va decidir enviar-li el seu projecte rebutjat, amb l'esperança que ell pogués apreciar-lo. Benett va quedar immediatament fascinat i el va considerar una de les idees més belles que havia vist mai. Durant la següent dècada va seguir llegint el manuscrit preguntant-se si hi hauria alguna forma de fer d'una idea tan magnifica, també quelcom pràctic. Pot ser que les revistes l'haguessin rebutjat però Benett n'estava obsessionat.

Un dia Benett va comentar aquest concepte amb Gilles Brassard, un amic seu de la Universitat de Montreal. Els dos ja havien col·laborat en diferents investigacions anteriorment i es van posar a discutir un i altre cop sobre les característiques de l'article de Wiesner. Van arribar a la conclusió que el concepte podria ser útil aplicat a la criptografia. Perquè l'Eve (l'espia) pugui interceptar un missatge xifrat entre l'Alice i el Bob primer té que interceptar-lo i d'alguna manera percebre amb exactitud el contingut de la transmissió. Es van preguntar què passaria si un missatge fos representat i enviat mitjançant fotons polaritzats. En teoria l'Eve no podria llegir correctament el missatge xifrat, de manera que no el podria desxifrar. El problema sorgia en que el Bob, el receptor, també havia d'interpretar el missatge i si no el llegia bé, tampoc no podria desxifrar-lo. Finalment van trobar un mètode que es basava a enviar la clau del missatge i no el propi missatge amb fotons polaritzats per tal d'aconseguir una comunicació totalment segura. Van decidir enviar la clau a causa que

aquesta pot ser totalment aleatòria i com veurem al llarg del protocol BB84 s'eliminen parts de la clau creada al principi. Si féssim això amb el missatge, al final s'hauria enviat un missatge incomplet i illegible. La clau que l'Alice vol enviar es troba en el llenguatge binari, és a dir que està formada per un seguit de zeros i uns. Perquè sigui totalment aleatòria, es fa ús d'un qubit*, partícula quàntica que té el 50% de probabilitats de decaure en un estat i el 50% de decaure en un altre. D'aquesta manera depenent dels estats en que decaigui el qubit al llarg del temps es podrà formar la clau, una seqüència de zeros i uns totalment aleatòria.

Primerament, l'Alice i el Bob decideixen establir un sistema de signes en què l'esquema rectilini (+), els fotons polaritzats verticalment (↕) seran interpretats com un bit amb el número 1 i els polaritzats horitzontalment(↔) seran un bit amb el número 0. En l'esquema diagonal (X), els fotons polaritzats diagonalment cap a la dreta (⤢) seran representats com un bit amb el número 1 i els polaritzats diagonalment cap a l'esquerrà (⤡) es representaran com un bit amb el número 0.

* Esquema + : ↕ → 1 ↔ → 0

* Esquema X : ⤢ → 1 ⤡ → 0

Aquest pas es pot dur a terme a través d'un canal convencional (seria molt poc pràctic però un exemple és el telèfon) sense por que l'Eve intercepti aquesta informació, ja que no compromet la seguretat del missatge. Un cop l'Alice té la clau que vol enviar, decideix assignar aleatòriament un esquema de polarització a cada un dels números de la clau. Els esquemes de polarització poden ser el rectilini (+) o el diagonal (X), això significa que si per exemple, el primer número de la clau és un 1 i se li assigna l'esquema diagonal (X), el pla de polarització del fotó que representarà aquest número necessariament tindrà que ser diagonal cap a la dreta (⤢), ja que el primer numero és un 1 i si polaritzéssim el fotó diagonalment cap a l'esquerra (⤡) representa un 0.

Alice

Clau en codi binari	1	0	0	1	0	1	1	0	1	0	0	0	1	1	0	1	0	1	1	0
Esquemes de polarització assignats (aleatoris)	X	+	X	X	+	X	+	X	+	+	X	X	+	X	+	+	+	X	+	+
Plans de polarització corresponents	↗	→	↘	↗	→	↗		↘	↕	→	↘	↘	↕	↗	→	↕	→	↗	↕	→

Canal Quàntic

Bob

Esquemes de polarització assignats (aleatoris)	+	+	X	X	+	+	X	+	+	X	+	+	+	X	X	+	X	X	+	X
Plans de polarització corresponents	→	→	↘	↗	→	↕	↗	↕	↕	↗	→	→	↕	↗	↗	↕	↘	↗	↕	↗
Clau en codi binari resultant	0	0	0	1	0	1	1	1	1	1	0	0	1	1	1	1	0	1	1	1

Al Bob quan li arriben els fotons de l'Alice no sap quin esquema de polarització ha assignat l'Alice per cada fotó que li ha enviat, de manera que assigna a l'atzar esquemes de polarització (+ o X) per a cada un dels fotons que rep. A conseqüència d'això, en la meitat de casos coincidirà l'esquema amb què l'Alice ha decidit polaritzar un fotó i l'esquema que en Bob li assigna i en l'altra meitat l'esquema que ha fet servir l'Alice per enviar el fotó i el que li assigna el Bob quan el rep seran diferents.

En el cas en què el Bob encerti els esquemes de polarització dels fotons que li envia l'Alice sempre obté el valor numèric (0, 1) correcte corresponent a aquell bit* d'informació; això passa aproximadament amb el 50% dels fotons, en la taula són els fotons que tenen els esquemes de polarització de color blau. En el cas que l'esquema de polarització que ha assignat l'Alice no coincideixi amb l'esquema que utilitza el Bob (50% dels casos), com que el fotó que arriba esta polaritzat amb un esquema incompatible amb l'esquema que utilitza el Bob per detectar-lo, en la meitat de casos pot decaure en valor el real que hauria sorgit si hagués estat mesurat correctament i en l'altra meitat de casos és detectat erròniament, de manera que dóna un valor incorrecte de la clau. Això és degut a que quan l'Alice, per exemple, envia un 1 de la clau i al seu corresponent fotó li assigna l'esquema rectilini (+), aquell fotó tindrà una polarització vertical (↕). Quan en Bob rep aquell fotó i li assigna aleatòriament un esquema diagonal (X), està utilitzant un filtre diagonal i com dèiem en l'apartat anterior dels diners quàntics, com que l'esquema no coincideix, segons la física quàntica tant podrà passar representant un valor (per exemple 1) o quedar-se en el filtre marcant un altre valor (per exemple 0), tot és qüestió de possibilitats.

He marcat de color verd tots els números de la clau d'en Bob que coincideixen amb la clau de l'Alice, independentment de si s'han obtingut quan els esquemes de polarització que utilitza en Bob i l'Alice coincideixen o si són fruit de la casualitat quan els esquemes no coincideixen. En Bob aproximadament tindrà un 75% de la clau correcta però un 25% incorrecta.

En aquest punt l'Alice i en Bob tenen claus diferents:

Clau Alice = 10010110100011010110

Clau Bob = 00010111110011110111

Per aconseguir tenir la mateixa clau, en Bob es posa en contacte amb l'Alice per un canal convencional i li diu a l'Alice la sèrie d'esquemes de polarització que ha triat aleatòriament per a cada fotó que li ha enviat l'Alice.

Bob → + + X X + + X + + X + + + X X + X X + X → Alice

Llavors l'Alice li contesta a en Bob els casos en què en Bob no ha escollit el mateix esquema que ella.

Alice → 1, 6, 7, 8, 10, 11, 12, 15, 17, 20 (no coincideixen els esquemes de polarització) →Bob

Un cop saben els esquemes que no coincideixen entre l'Alice i el Bob, eliminen els números corresponents a aquells fotons i finalment tenen els dos la mateixa clau.

Clau compartida (els dos tenen la mateixa) → 0010111111

Com podem comprovar no tots els números que anteriorment he marcat de color verd, és a dir aquells que coincideixen entre la clau d'en Bob i de l'Alice, es mantenen. Només es mantenen els números que s'han obtingut quan l'esquema que ha triat l'Alice i l'esquema que ha escollit el Bob han coincidit (aproximadament el 50%), la resta s'han eliminat. Ara només els falta comprovar si les seves claus coincideixen. Per fer-ho agafen un fragment de la clau, en el nostre cas triarem els tres últims números. Llavors tant l'Alice com el Bob fan públic el mateix fragment de cada una de les seves claus, en aquest cas agafarem els tres números finals.

Fragment Alice → 111

Fragment Bob → 111

Podem comprovar com els dos fragments descoberts són exactament iguals, això significa que no hi ha hagut cap espia i que la connexió és segura. Un cop ho han comprovat eliminen la part de la clau que han publicat i ara ja tenen la clau final amb garanties que és totalment igual i que només la tenen ells dos.

Clau final → 0010111

En la realitat les claus estan compostes per milers de números i quan han de fer pública una part per veure si coincideix acostumen a fer-ho aproximadament amb 70 dígits. Amb la nostra demostració seria bastant fàcil que els fragments de claus que s'ensenyen coincidissin encara que tinguéssim un espia, però si es fa amb una

quantitat tant gran de dígits com en la realitat, les possibilitats que coincideixin són pràcticament nul·les.

5.2.1 BB84 amb observador

Fins ara he explicat com funcionaria el protocol BB84 en el cas que ningú ens estigués espiant, però precisament la gràcia dels protocols d'encriptació quàntica és la seva absoluta seguretat, per tant, anem a veure què passa si hi tenim un espia (anomenat Eve) entre l'Alice i el Bob. Com hem dit abans l'Alice primerament assigna aleatòriament un esquema de polarització (+ o X) a cada un dels números o bits de la clau. Després polaritza el fotó que contindrà la informació d'un bit de la clau depenent del número i de l'esquema de polarització que se li hagi assignat.

Alice

Clau en codi binari	1	0	0	1	0	1	1	0	1	0	0	0	1	1	0	1	0	1	1	0
Esquemes De polarització assignats (aleatoris)	X	+	X	X	+	X	+	X	+	+	X	X	+	X	+	+	+	X	+	+
Plans de polarització corresponents	⤢	↔	↘	⤢	↔	⤢	↕	↘	↕	↔	↘	↘	↕	⤢	↔	↕	↔	⤢	↕	↔

Canal

quàntic

Eve

Esquemes De polarització assignats (aleatoris)	+	+	X	X	+	+	X	+	+	X	+	+	+	X	X	+	X	X	+	X
Plans de polarització corresponents	↔	↔	↘	⤢	↔	↕	⤢	↕	↕	⤢	↔	↔	↕	⤢	⤢	↕	↘	⤢	↕	⤢
Clau en codi binari resultant	0	0	0	1	0	1	1	1	1	1	0	0	1	1	1	1	0	1	1	1

Canal

quàntic

Bob

Esquemes De polarització assignats	+	X	X	X	+	X	+	X	+	X	+	X	+	+	+	X	+	X	X	+

(aleatoris)																				
Plans de polarització corresponents	↔	↘	↘	↗	↔	↗	↔	↗	↕	↗	↔	↘	↕	↔	↕	↘	↕	↗	↘	↔
Clau en codi binari resultant	0	0	0	1	0	1	0	1	1	1	0	0	1	0	1	0	1	1	0	0

L'espia anomenat Eve vol conèixer la clau i per fer-ho han d'intentar interceptar la informació que envia l'Alice cap el Bob, analitzar-la i després tornar a enviar aquesta informació cap el Bob, d'aquesta manera en teoria no es detectaria la seva presència i l'Eve podria obtenir la clau. Si l'Alice i el Bob s'estiguessin comunicant per un canal clàssic, per exemple el telèfon, l'Eve se'n sortiria però com que l'Alice i el Bob es comuniquen per un canal quàntic, enviant-se qubits (fotons polaritzats), les coses canvien: l'Eve intercepta el missatge i procedeix igual que el Bob. Per fer-ho menys complicat he fet coincidir els resultats de la Eve amb els resultats que ha obtingut el Bob quan no hi havia cap espia. Podem veure com primer assigna aleatòriament un esquema de polarització per a cada fotó que intercepta i obté una clau amb el 75% d'encerts i el 25% d'errors (aproximadament), de moment tot igual que amb el Bob.

El moment complicat arriba quan l'Eve ha d'enviar la informació que ha obtingut cap al Bob. Com que l'Eve no té tota la informació correcta, quan li enviï al Bob ja li estarà enviant qubits erronis. Per fer-se una idea, quan no hi ha espia al Bob ja li costa mesurar correctament els fotons que li envia l'Alice, que estan polaritzats correctament, i no els encerta tots. Imaginem la dificultat addicional si l'Eve li està enviant la seva clau, que ja té una part incorrecta. D'aquesta manera l'error del Bob augmenta encara més.

Posem que un cop s'han enviat la clau, amb l'Eve espiant, les claus de l'Alice, l'Eve i en Bob són:

Clau Alice = 10010110100011010110

Clau Eve = 00010111110011110111

Clau Bob = 00010101110010101100

Llavors, sense que l'Alice ni el Bob sàpiguen que han estat espiats, procedeixen a comunicar-se per un canal convencional. El Bob li diu els seus esquemes que ha assignat als fotons que li arribaven, que en teoria havien de ser de l'Alice però en realitat provenien de l'Eve.

Bob → + X X X + X + X + X + + + X + X X + → Alice

Llavors l'Alice li contesta al Bob els casos en què el Bob no ha escollit el mateix esquema que ella.

Alice → 1, 2, 10, 11, 14, 16, 19 (no coincideixen els esquemes de polarització) → Bob

Aquest procés no ajuda gens a l'Eve, tant l'Eve com el Bob han triat aleatòriament uns esquemes per a cada fotó que els arriba, per tant la seqüència d'esquemes que tria l'un i l'altre és diferent. L'Alice comunica amb un canal convencional (que pot ser espiat) els

esquemes en que el Bob s'ha equivocat, però com que l'Eve s'haurà equivocat amb uns esquemes diferents que els del Bob, no li serveix de res aquesta informació. Un cop saben els esquemes que no coincideixen entre l'Alice i el Bob, eliminen els números corresponents a aquells fotons i en teoria haurien de tenir la mateixa clau.

Clau Alice → 0101101010010

Clau Bob → 0101011011110

En aquest moment decideixen compartir un fragment de la clau per comprovar si tenen la mateixa clau o si hi ha hagut un espia que hagi pogut alterar la informació. Decideixen compartir els tres últims dígits:

Fragment Alice → 010

Fragment Bob → 110

En aquest punt l'Alice i el Bob se n'adonen que hi havia un intrús. Pel simple fet d'estar interceptant i enviant informació l'Eve ha alterat la informació i ha provocat que al final les claus de l'Alice i del Bob siguin diferents. Això passa gràcies que la comunicació es produeix en un canal quàntic, en què pel simple fet de mesurar ja s'altera la informació que s'envia. En la majoria de fotons no passa res però quan realment s'enxampa ''in fraganti'' l'Eve és quan per casualitat primer l'esquema que tria l'Alice per polaritzar un fotó i el que tria l'Eve aleatòriament no coincideixen però el Bob torna a triar l'esquema que l'Alice havia triat i llavors es crea una contradicció. Com que l'esquema de l'Alice i en Bob són iguals, quan es comuniquin els esquemes que no coincideixen, no s'eliminaran els números a què pertanyen aquells esquemes, però com que el Bob rep els fotons de l'Eve i el seu esquema era diferent, el Bob pot mesurar un nombre que no era l'original. En la taula els esquemes de color blau que ha triat el Bob són els que coincideixen amb els de l'Alice i es pot observar com tot i coincidir amb l'esquema amb l'Alice el bit és incorrecte (números en vermells), això provoca que la clau final sigui diferent, per tant, que se n'adonin que intenten espiar-los.

5.3. Protocol SARG04

El protocol SARG04 és un dels mes recents que s'han creat, es va idear el 2004 i presenta diverses millores respecte del BB84. Aquest protocol va ser fruit de la col·laboració entre Valerio Scarani, Antonio Acín (treballa actualment al ICFO a Barcelona), Grégoire Ribordy i finalment Nicolas Gisin (entrevista pàg. 66).

El protocol és bastant més robust i presenta diferents avantatges respecte Del protocol BB84:

- Com que el bit es troba xifrat en l'esquema i no en el pla de polarització el protocol és més resistent als atacs PNS (Photon Number Splitting). Aquest atac és possible quan per falta de precisió experimental s'envien dos fotons en lloc d'un sol,

llavors l'Eve pot agafar-ne un i deixar passar l'altre i així no alterar alguns resultats del Bob. El protocol BB84 és més vulnerable a aquest tipus d'atacs que el SARG04. Nosaltres només tocarem els atacs amb fotons individuals ja que l'atac PNS és més complex.

- El SARG04 aconsegueix menys errors en els bits que s'envien. Aquests errors anomenats soroll de fons es produeixen a causa que és pràcticament impossible dur a terme aquests protocols d'una forma ideal i sempre hi ha factors que afecten la transmissió.
- Com més lluny és la comunicació, més errors es produeixen en la clau fins arribar a un punt que el protocol ja no és factible. Amb el SARG04 la distància efectiva és major que la del BB84.

En aquest cas l'Alice crea una clau en llenguatge binari (formada per zeros i uns) totalment aleatòria, al igual que amb el protocol BB84. Per fer-ho, el millor és utilitzar un qubit i així aconseguirà una clau totalment aleatòria.

Un cop l'Alice té la clau aleatòria en codi binari, decideix assignar un esquema de polarització per a cada bit. A diferència del protocol BB84 en què l'Alice triava els esquemes de polarització aleatòriament i els assignava a cada bit, en el protocol SARG04 depenent del valor del bit s'assignaria l'esquema rectilini (+) o diagonal (x). L'Alice decideix que els bits amb el número 1 de la clau els pertocarà l'esquema diagonal (X) i als bits que siguin un 0 se'ls hi assignarà l'esquema rectilini (+).

Bit: 1 ➔ X

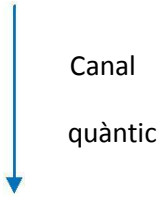
Bit: 0 ➔ +

Un cop ha assignat els esquemes a cadascun dels bits envia un fotó polaritzat amb un dels plans de l'esquema que li ha tocat. Per exemple, si un fotó ha de representar el bit 0 serà polaritzat amb un dels dos plans de l'esquema rectilini (+), el pla vertical (↕) u horitzontal (↔).

L'elecció dels esquemes no és aleatòria ja que depèn del bit de la clau que s'està enviant, però els plans amb què es polaritza el fotó poden ser aleatoris, mentre que siguin els de l'esquema que li pertoca.

Alice

Clau de l'Alice	0	0	0	0	0	1	1	0	1
Esquemes corresponents	+	+	+	+	+	X	X	+	X
Plans de polarització (aleatoris)	↕	↕	↕	↕	↔	⤢	↘	↕	↘



Bob

Esquemes De polarització assignats (aleatoris)	+	X	X	X	X	X	+	X	+
Plans de polarització resultants	↕	⤢	↘	↘	↘	⤢	↕	⤢	↔

El Bob al principi com que no sap com estan polaritzats els fotons que li envia l'Alice decideix assignar aleatòriament un esquema de polarització a cadascun dels fotons que li arriben i conseqüentment obté una seqüència de plans de polarització per a cada fotó. Quan el Bob encerta l'esquema de polarització els plans amb què l'Alice ha enviat un bit i el Bob l'ha detectat seran els mateixos. Si el Bob no encerta l'esquema de polarització li sortirà un pla de polarització corresponent a l'esquema que ha utilitzat i no sabrà si ho ha fet correctament o si s'ha equivocat d'esquema. En aquest punt el Bob no sap si els resultats que té són correctes (és pràcticament impossible que ho siguin) i no té prou informació per continuar. Un cop al Bob li han arribat tots els fotons, l'Alice decideix publicar una part de la informació sobre la clau que ha enviat. L'Alice declara públicament un estat S per a cada fotó polaritzat que ha enviat. Els estats que declara l'Alice poden ser públics, de manera que tothom el pot observar ja que no representen cap perill. Aquests estats poden ser quatre:

S++ → {↕, ⤢}

S-- → {↔, ↘}

S+- → {↕, ↘}

S-+ → {↔, ⤢}

D'aquesta manera per a cada fotó que ha enviat poden haver-hi dues possibilitats. Es pot pensar que és poc útil ja que cadascuna pertany a un esquema de polarització diferent però en realitat és una informació molt valuosa per al Bob. L'Alice declara cada un dels estats depenent del pla de polarització del fotó que envia, si envia un fotó amb una polarització vertical, per aquell fotó podrà declarar públicament l'estat S++ o S+- ja que els dos contemplen la possibilitat del pla vertical.

Alice

Clau de l'Alice	0	0	0	0	0	1	1	0	1
Esquemes corresponents	+	+	+	+	+	X	X	+	X
Plans de polarització (aleatoris)	↕	↕	↕	↕	↔	↗	↘	↕	↘
Estat que declara públicament	S++	S++	S++	S++	S-+	S-+	S+-	S+-	S+-

Canal quàntic

Bob

Esquemes de polarització assignats (aleatoris)	+	X	X	X	X	X	+	X	+
Plans de polarització resultants	↕	↗	↘	↘	↘	↗	↕	↗	↔
Bits que pot saber a partir del que l'Alice declara	?	?	0	0	0	?	?	0	1

Amb els estats que ha declarat l'Alice, el Bob pot saber el valor d'alguns bits de la clau. Només podrà saber el bit exacte en els fotons que hagi triat l'esquema de polarització contrari al de l'Alice i li hagi sortit el pla de polarització del fotó també contrari. Per exemple, l'Alice vol enviar un bit, com que aquest és un 0 li assigna un esquema rectilini (+), l'envia amb el pla de polarització vertical (↕) i decideix declarar l'estat S++. Llavors el Bob tria aleatòriament l'esquema diagonal (X) per mesurar aquell fotó i li resulta que té un pla de polarització vertical cap a l'esquerra (↘). Com que l'Alice ha declarat l'estat S++, els dos únics plans amb què aquell fotó podria estar polaritzat són el vertical o el diagonal cap a la dreta (↕ o ↗) i com que el Bob ha mesurat amb l'esquema diagonal i li ha donat el contrari que el pla diagonal del S++, llavors pot estar segur que el pla d'aquell fotó serà vertical, de manera que l'Alice li haurà assignat l'eix rectilini, i per tant serà un 0.

Si el pla de polarització que mesura el Bob coincideix amb un dels plans de l'estat S que

declara l'Alice, llavors el Bob no podrà saber si el seu resultat és correcte o si en realitat el fotó estava polaritzat amb l'esquema contrari al seu i aquest al ser mesurat per el Bob amb un esquema contrari s'ha decantat cap al valor que ha obtingut. En aquest punt el Bob es comunica amb l'Alice per un canal convencional, sense por que ningú els escolti i li diu els bits que no sap, ja que pot haver-hi més d'una possibilitat.

Bob ➔ 1,2,6,7 (els desconec) ➔ Alice

Ara només han d'eliminar els bits que el Bob desconeix i finalment podran compartir una clau totalment idèntica i segura.

Clau Alice ➔ 00001

Clau Bob ➔ 00001

Al igual que en el protocol BB84 ara tocaria que tant l'Alice com el Bob publiquessin un fragment de la clau per poder comprovar que la transmissió s'ha efectuat correctament i que no hi havia cap espia. Un cop comprovat això llancen el fragment publicat i ja poden començar a enviar-se informació d'una forma segura.

5.3.1 SARG04 amb observador

Ara observarem el que passaria si mentrestant l'Alice i el Bob s'intenten enviar la clau a través del protocol SARG04 un espia anomenat Eve decideix ''escoltar'' la conversa. Primerament al igual que abans l'Alice crea una clau aleatòria en codi binari, assigna uns esquemes de polarització depenent del valor dels bits i envia fotons amb un dels dos plans de polarització de l'esquema que li pertoca a cadascun. Un cop ho ha fet declara els estats S[15] per a cada fotó que ha enviat.

Alice

Clau de l'Alice	0	0	0	0	0	1	1	0	1
Esquemes corresponents	+	+	+	+	+	X	X	+	X
Plans de polarització (aleatoris)	↕	↕	↕	↕	↔	⤢	↘	↕	↘
Estat que declara públicament	S++	S++	S++	S++	S-+	S-+	S+-	S+-	S+-

Canal quàntic

[15] Aquests estats fan referència a la conversió explicats a la pàgina 51.

Eve

Esquemes De polarització assignats (aleatoris)	+	X	X	X	X	X	+	X	+
Plans de polarització resultants	↕	⤢	⤡	⤡	⤡	⤢	↕	⤢	↔
Bits que pot saber a Partir del Que l'Alice declara	?	?	0	0	0	?	?	0	1

Canal

quàntic

Bob

Esquemes De polarització assignats (aleatoris)	+	X	X	+	+	X	+	+	X
Plans de polarització resultants	↕	⤢	⤡	↔	↕	⤢	↕	↔	⤢
Bits que pot saber a Partir del Que l'Alice declara	?	?	0	1	1	?	?	1	0

En aquest cas l'Eve, que està atenta a les comunicacions entre l'Alice i el Bob, intenta interceptar els fotons que envia l'Alice i intenta enviar els mateixos fotons que ha interceptat cap al Bob. Com hem vist en el protocol BB84 les coses no són tan fàcils per als espies que intenten aconseguir informació d'un canal quàntic. Per simplificar-ho he fet que els resultats que obté l'Eve siguin els mateixos que obtenia el Bob quan no hi havia un espia. Un cop s'ha produït la transmissió amb espia, el Bob comunica els bits que no coneix a l'Alice per aconseguir tenir la mateixa clau:

Bob → 1,2,6,7 (els desconec) → Alice

No hi ha perill si l'Eve els està escoltant ja que els bits que l'Eve desconeix no són els mateixos que els que el Bob desconeix, de manera que a l'Eve no li serveix per res aquesta informació.

En teoria en aquest punt l'Alice i el Bob haurien de tenir la mateixa clau però en intervenir l'Eve en la comunicació, com que és un canal quàntic i en observar ja s'alteren els resultats, les claus que obtenen al final són diferents.

Clau Alice → 00001

Clau Bob → 01110

En aquest punt, l'Alice i el Bob compartirien un fragment de clau i se n'adonarien que no coincideixen, per tant hi havia un espia que ha alterat els resultats.

5.4. Protocol Eckert91

El protocol d'encriptació Eckert91 tot i que és dels més complicats de realitzar i té moltes limitacions per poder-lo portar a la pràctica utilitza una característica de la física quàntica que els altres protocols no fan servir. Aquest protocol utilitza l'entrellaçament quàntic per transmetre la informació de l'Alice cap al Bob (fig. 4.5.).

Des de sempre si s'ha volgut enviar informació s'ha hagut de fer a través d'algun medi, per ones electromagnètiques, quelcom escrit en un full de paper, a través d'impulsos elèctrics...

Això canvia totalment en aquest protocol ja que només s'han d'enviar fotons entrellaçats i, essencialment, no s'ha d'enviar la clau de l'Alice cap al Bob.

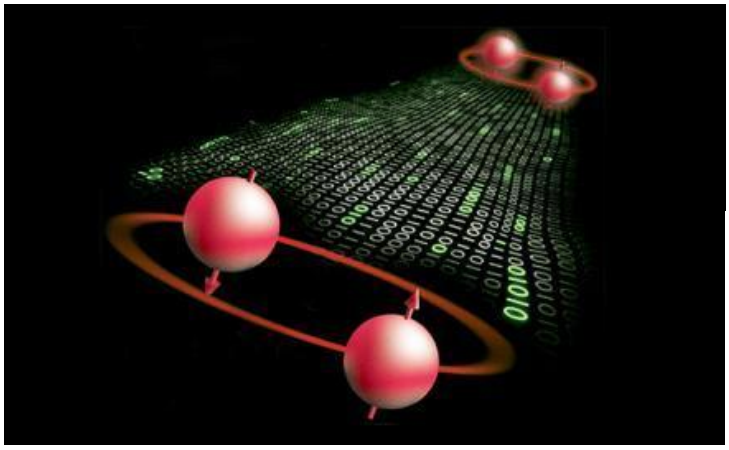


Fig. 4.5. Gràcies a la física quàntica es poden dur a terme successos com l'entrellaçament o la teletransportació quàntica, que amb la física clàssica era inimaginable que poguessin portar-se a terme.

Primerament tenim l'Alice i el Bob a una certa distancia, cadascú al seu laboratori. En aquest moment, des d'una tercera posició s'envien fotons entrellaçats. De cada parell de fotons entrellaçats, un dels fotons va cap a l'Alice i l'altre cap al Bob. L'Alice i el Bob, que ja estaven pendents dels fotons els mesuren, com que estaven entrellaçats el que mesura un serà el contrari que el que mesura l'altre.

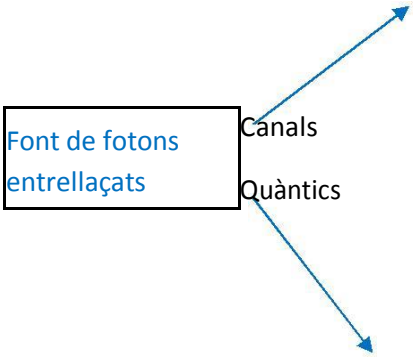
En aquest protocol s'agafen els mateixos valors que el BB84. En l'esquema rectilini (+) el pla vertical correspon un 1 i l'horitzontal un 0. En l'esquema diagonal (X) el pla horitzontal cap a la dreta representa un 1 i el que va cap a l'esquerra un 0.

L'Alice i el Bob assignen esquemes de polarització de forma aleatòria per a cada fotó

que els arriba. Si els esquemes escollits per l'Alice i el Bob coincideixen, llavors es complirà l'entrellaçament. En cas que l'Alice i el Bob no tinguin els mateixos esquemes per al mateix parell de fotons, sorgiran errors en la comunicació. Això és degut que si, per exemple, l'Alice mesura un dels fotons entrellaçats amb un detector rectilini, llavors si el Bob mesurés l'altre fotó que està entrellaçat amb el mateix detector rectilini li sortiria un valor contrari al que li ha donat a l'Alice (a causa de l'entrellaçament). Però si el Bob mesura l'altre fotó entrellaçat amb un detector diagonal, com que no han mesurat la mateixa magnitud de la mateixa forma, no es produirà l'entrellaçament i el Bob tindrà un 50% de possibilitats que mesuri diagonal cap a la dreta i un 50% més de que sigui cap a l'esquerra.

Alice

Esquemes De polarització Que utilitza l'Alice (aleatoris)	X	X	+	+	+	X	+	X	+	X
Plans de polarització resultants	↘	↗	↕	↔	↔	↘	↕	↘	↕	↘
Clau en Codi binari resultant	0	1	1	0	0	0	1	0	1	0



Bob

Esquemes De polarització Que utilitza El Bob (aleatoris)	X	X	X	X	+	+	+	X	X	X
Plans de polarització resultants	↗	↘	↗	↗	↕	↔	↔	↗	↗	↗
Clau en Codi binari resultant	1	0	1	1	1	0	0	1	1	1

Un cop tenen tots els fotons detectats un dels dos ha d'invertir els seus resultats. Això és degut que com que estan entrellaçats, si a l'Alice li dóna un 1, el Bob tindrà un 0, ja que al mesurar un dels fotons entrellaçats, determina el valor de l'altre, fent que sigui el contrari del primer.
La clau que comparteixen és:
Clau Alice = 0110001010
Clau Bob = 1011100111 → Inverteix els seus valors = 0100011000
Quan els dos ja tenen una clau, l'Alice li comunica al Bob els esquemes de polarització que ha utilitzat i el Bob li comunica a l'Alice els esquemes que no han coincidit.
Alice → X X + + + X + X + X → Bob
Bob → 3, 4, 6, 9 (no coincideixen) → Alice
Ara si tot ha sortit bé els dos ja compartirien una mateixa clau.
Clau final = 010100
Per comprovar-ho publiquen un tros de clau, de manera que si els dos fragments no són iguals sabran que algun espia ha alterat els resultats fent que aquells fotons que reben ja no siguin els entrellaçats, fet que provoca errors. En cas que coincideixin els dos fragments de claus, treuen el fragment compartit i ja poden començar a intercanviar missatges de forma segura.

5.5. Aplicacions de la criptografia quàntica

5.5.1. Els inicis de la criptografia quàntica

Des que es van desenvolupar els primers protocols* de criptografia quàntica fins que es va aconseguir demostrar-los experimentalment van passar uns quants anys. Al principi els sistemes i la tecnologia estaven molt poc desenvolupats i el nivell de qualitat i la distància en què es podien dur a terme eren molt baixos però es va anar desenvolupant i millorant la tecnologia fins aconseguir un grau de precisió en la distribució de clau per via quàntica molt bo.
Un dels primers i més destacables experiments en criptografia quàntica va ser l'experiment de la Venus de Willendorf. Es tractava d'enviar-se a través de criptografia quàntica la clau de la imatge xifrada de la Venus de Willendorf. La clau era bàsicament una plantilla de la mateixa resolució que la Venus (49984 bits de longitud).
Aquesta imatge o plantilla, formada per un seguit de píxels aleatoris sense cap sentit aparent, se superposava amb la imatge de la Venus i aquesta quedava xifrada, de manera que només si es tornava a aplicar la plantilla (clau) sobre la Venus xifrada es podria tornar a veure el seu contingut. Podem observar en la imatge (fig. 4.6.) que en la Venus desxifrada hi ha diversos errors o píxels mal col·locats. Aquestes alteracions

es van produir a causa dels errors sorgits quan es va enviar la clau amb criptografia quàntica, concretament amb el protocol BB84. Va ser una de les primeres imatges la clau de les quals va ser enviada a través de criptografia quàntica, de manera que els errors es van produir perquè la criptografia quàntica estava molt poc desenvolupada pràcticament.

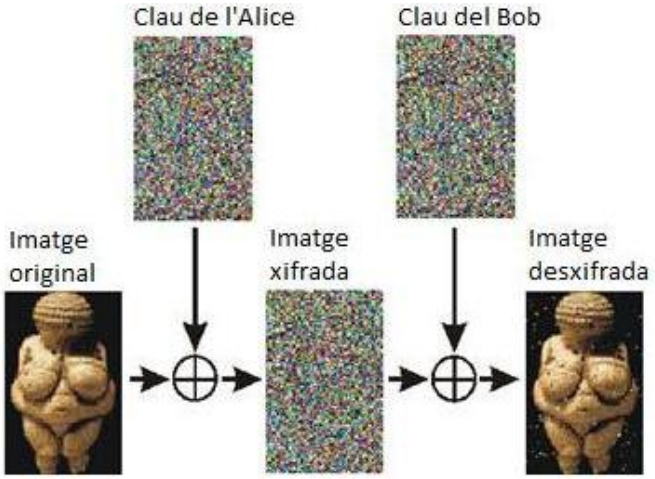


Fig. 4.6. Primera imatge en què es va utilitzar la criptografia quàntica amb el protocol BB84.

En l'exemple de la Venus es pot apreciar molt bé la importància que té canviar de clau cada cop que s'inicia una comunicació a través d'algun protocol de criptografia quàntica. Si l'Eve intercepta una imatge xifrada que l'Alice s'envia amb el Bob no passa res, però si l'Alice li envia una segona imatge xifrada amb la mateixa clau que la primera, l'Eve amb les dues imatges xifrades, el repetir-se el patró, ho tindrà molt fàcil per revelar el seu contingut. És per això que és tan important crear una clau nova abans d'enviar-se qualsevol cosa.

5.5.2 La criptografia quàntica en l'actualitat

Avui en dia el procés està molt més perfeccionat i el nombre d'errors que es produeixen és molt més baix. La criptografia quàntica ha passat de ser un experiment practicable al laboratori a tenir ja sortides comercials. Tot i que està en una fase molt prematura molts bancs (sobretot els suïssos) ja l'utilitzen per transmetre informació confidencial amb un nivell de seguretat mai vist. A part dels bancs, el govern suís ja transmet els resultats de les seves votacions utilitzant criptografia quàntica.
Actualment una de les empreses que treballa amb sistemes de criptografia quàntica és ID Quantique (fig. 4.7.). Aquesta empresa té la seu a Ginebra i treballa desenvolupant i venent aparells per fer criptografia quàntica. La major demanda que té és dels propis bancs del país i un dels membres principals és Nicolas Gisin, un dels desenvolupadors del protocol SARG04 (entrevista pàg. 66).

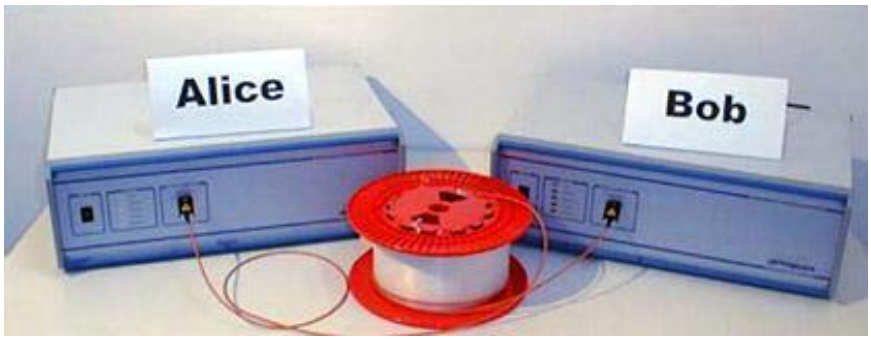


Fig. 4.7. Aparells comercialitzats per ID Quantique per poder establir comunicacions a través de criptografia quàntica.

A part d'ID Quantique, ja hi ha altres empreses que es dediquen al mateix. Amb la velocitat en què avança la tecnologia i la necessitat de seguretat creixent, cada cop s'està implementant més aquesta forma de criptografia i en ser un mercat creixent, cada cop tindrem més empreses que tocaran aquest camp.

5.5.3La criptografia quàntica en el futur

Tot i que s'aniran desenvolupant els mètodes de criptografia quàntica actuals i augmentarà el nombre d'empreses que ho comercialitzin, un dels moments més importants per a la criptografia quàntica serà quan s'aconsegueixi dur a terme sense cables. Actualment encara es poden millorar les comunicacions per cable de la criptografia quàntica però hi ha un límit. Utilitzant la criptografia quàntica de la millor manera no es pot aspirar que s'implementi mai a un nivell mundial ja que tindria una distància útil de pocs centenars de quilòmetres i només ho utilitzarien empreses que treballen amb informació molt important, però no arribaria al gran públic.

Quan aconseguim dur-ho a terme sense cables podrem utilitzar satèl·lits i passar d'unes desenes o centenars de quilòmetres a tot el món (fig. 4.8.). En aquest punt serà quan realment s'expandeixi la criptografia quàntica ja que es podrà aplicar al mateix nivell que la criptografia que s'utilitza avui en dia, que és l'algorisme RSA.

Cada cop que enviem o rebem qualsevol cosa per Internet o els canals que ens arriben per la televisió de pagament, venen xifrats amb l'algorisme RSA. Si la criptografia quàntica es pot implantar utilitzant satèl·lits, totes aquestes comunicacions que realitzem de forma habitual estaran xifrades de la millor forma existent.

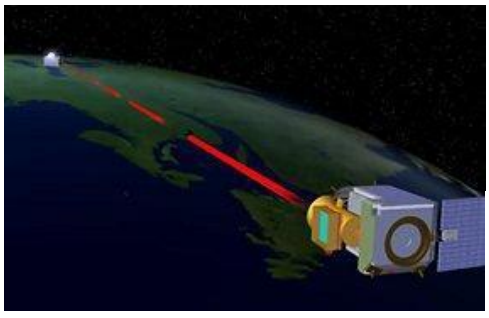


Fig. 4.8. Si s'aconsegueix fer criptografia quàntica amb satèl·lits es podria transmetre per tot el món amb una seguretat mai vista.

Ja hi ha diversos grups de treball que ho investiguen i es creu que en uns quans anys es podrà aconseguir. Tot apunta que en uns anys o dècades aquesta tecnologia serà accessible i tindrà una gran importància en la nostra societat.

6. ENTREVISTES

Aquestes entrevistes són de font pròpia igual que les fotografies que les acompanyen.

6.1.1 Entrevista a Sonia Fernández-Vidal

* Sonia Fernández-Vidal és una escriptora i divulgadora científica, nascuda el 8 de març de 1979 a Barcelona. Doctora en Òptica i Informació Quàntica per la Universitat Autònoma de Barcelona, va contribuir l'any 2003, a través del CERN, en el projecte LHC. L'any 2005 va viatjar a Los Álamos i va col·laborar amb la divisió teòrica de Los Álamos National Lab LANL en un projecte sobre la decoherència i la informació quàntica. També va contribuir l'any 2006 en un projecte europeu sobre computació quàntica a través de l'Institut de Ciències Fotòniques ICFO. A partir de 2009 va treballar com a docent i investigadora a la Universitat Autònoma de Barcelona. També ha fet xerrades de divulgació científica per a persones no especialitzades.
Així mateix, és l'autora del llibre La porta dels tres panys (La Galera 2011), una novel·la de divulgació científica destinada tant a nens com a adults que va mantenir-se a la llista dels més venuts a Espanya durant mesos, esgotant edicions mes a mes, i venent-se els drets del llibre a 11 idiomes
El seu darrer llibre, Quantic Love (La Galera 2012) també ha col·locat la Sònia a les llistes dels llibres més venuts a Espanya, amb una segona edició després d'un mes del seu llançament i amb 40.000 llibres a llibreries en menys de dos mesos.

-En quin moment et vas adonar que el que t'agradava era la física i què va fer que t'hi decantessis?
- Me'n vaig adonar quan estava a l'institut, quan vaig fer física per primera vegada. Des de petita sempre m'havia agradat molt la ciència i sempre intentava buscar les respostes de les coses i sabia que volia ser científica però no sabia molt bé el què. EN descobrir la física me'n vaig adonar que aquesta em donava resposta a tots els dubtes que tenia. La física semblava que em donava les respostes fins que vaig descobrir el que era la física quàntica, que et desmunta el ''castell de cartes'' de totes les respostes i et suscita encara més misteri i més preguntes i m'hi vaig quedar enganxada de seguida.

- Podries explicar les teves primeres passes? Com vas viure aquest canvi d'estudiant a fer recerca científica?

- Vaig fer la carrera de física a la UAB i parlant de fer el canvi d'estudiant a recerca científica, jo vaig anar al CERN quan estava a punt d'acabar la carrera. Vaig decidir anar a fer una primera prova del que era fer recerca de tot allò que estava estudiant. Penso que va ser una experiència extraordinària que recomano molt, per exemple el CERN organitza uns programes per a Summer Students per a gent que està fent la carrera de física.

- Tenies previst anar a treballar a llocs de recerca fora d'Espanya tant importants com el CERN o el Laboratori Nacional de los Álamos? Com et van sorgir les oportunitats?

- En realitat no m'ho imaginava quan vaig començar però una cosa que s'ha de tenir clar és que les oportunitats s'han de buscar. Moltes vegades pensem que a nosaltres no ens agafarien mai però hem de trencar amb aquesta barrera i fer totes les sol·licituds que es puguin ja que el no ja el tens i no tens res a perdre. Per exemple, jo vaig anar a fer un curs d'acceleradors de partícules a una universitat d'Estats Units i tot i que estava pensat per a gent d'allà, em vaig atrevir a demanar-ho i em van acceptar.
Les coses existeixen però les has de buscar. La qüestió és buscar les oportunitats i no pensar mai que no t'ho donaran. I no t'has de preocupar per si treus bones o males notes, a la majoria de llocs et demanen un currículum de les coses que has fet, i clar, cada cop que fas més coses va sumant.

- Quan estaves a l'estranger, quines diferències vas veure respecte d'Espanya en els àmbits de treball, recerca ...

- Hi ha moltes diferències però n'hi ha dues de destacables:
La primera és que quan vaig estar treballant a Suïssa, al CERN, des de les condicions econòmiques al lloc on estava eren molt millors.
La segona és que a l'hora de fer recerca, vaig trobar mes diferencia entre Europa i els Estats Units ja que a Europa la recerca és bastant piramidal, el cap o el més antic és el que en sap i tu quan ets estudiant estàs a la part més baixa, en canvi als Estats Units vaig veure que la recerca era molt més horitzontal. A Los Álamos fèiem una cosa anomenada quantum lunch, que consistia que dinàvem tots junts i mentrestant menjàvem algú exposava la seva feina. Això ho fèiem amb tot el departament de teòrica de Los Álamos i recordo que en aquestes reunions hi havia post docs i investigadors que feien unes preguntes de coses que se suposava que ja s'havien de saber i jo em sorprenia al veure com s'atrevien en preguntar allò. Ells no tenen aquesta por ja que no temen fer preguntes encara que siguin bajanades, de manera que si ets nou pots preguntar el que vulguis encara que sigui alguna tonteria que no es riuran de

tu, fins i tot et veuran una miqueta més atrevit.

- Haver treballat a tants llocs creus que t'ha canviat la forma de poder veure el món i les persones?
- Sí però per molts aspectes, el primer perquè quan et mous en ambients internacionals canvia la teva perspectiva del món i la manera de tractar la gent. A més a més crec que la física quàntica et dóna una perspectiva diferent per veure com funciona el món, per exemple, tu i jo estem aquí asseguts i el saber que aquesta taula és un 99,99% buida doncs sí que fa que paris a pensar-hi, parafrasejant Shakespeare '' hi ha més coses al cel i a la terra de les coses que et pots imaginar'' i crec que aquestes coses filosòficament et canvien.

- Què va ser el que va fer que decidissis començar a escriure llibres?
- Jo ja havia fet algunes xerrades de divulgació sobre el que era la física quàntica per a no científics, com per exemple gent de lletres i persones que no tenien res a veure amb el món de la ciència. En una d'aquestes xerrades vaig coincidir amb el Francesc Miralles que és un escriptor molt reconegut i em va dir: - Sonia per què totes aquestes xerrades que expliques no les fas amb format de llibre, així podries arribar a molta més gent. Jo vaig pensar que de llibres de divulgació científica ja n'hi han molts i si mai escrivís un llibre ho faria precisament per a la gent que no llegiria mai un llibre de divulgació científica, ho faria com si fos un conte per a nens, de manera que els grans també s'atrevissin a llegir-lo i així va néixer tota aquesta aventura.

- Com creus que la física quàntica s'ha estès per la societat, creus que és ben coneguda?
- Crec que encara no és ben coneguda, penso que la física quàntica encara és com un sinònim de coses rares. Hi ha dos problemes, el primer és que no l'hem sabut divulgar bé, potser des dels mateixos científics i també s'ha utilitzat i manipulat molt per pretendre explicar molta pseudociència, és a dir, se n'està fent un mal ús i un abús. Però jo penso que aquestes coses passen perquè ara s'estan exposant i hi ha una miqueta un *boom* de gent que vol saber el que és la física quàntica. Per exemple, quan es va descobrir la radioactivitat, els alquimistes estaven d'allò més contents , la transmutació de la matèria! La radioactivitat et diu que un àtom pot decaure i convertir-se en un altre, i era el que els alquimistes portaven dient des de feia segles. Suposo que és un pas normal i que l'única manera de combatre aquesta confusió és divulgant-la. En el moment en què els nens petits hi estiguin tant acostumats, potser perquè la computació o la criptografia quàntica ja s'utilitzin, aquests problemes ja no hi seran. Crec que de moment no és molt coneguda però comença a filtrar-se i la millor

manera d'evitar les confusions i les relacions estranyes és precisament explicant-la més, llavors aquesta fama ja passarà. Fixa't bé que la física quàntica té una part que és molt filosòfica, té explicacions molt *heavies* sobre el que és la realitat, amb la qual cosa és molt fàcil fer connexions de vegades massa dràstiques i, tot i que s'ha de ser molt prudent quan es parla de filosofia i ciència, crec que és bo establir ponts entre la filosofia i la física quàntica i s'ha d'animar a fer-ho.

- Tornant enrere, podries parlar sobre què tracta el teu doctorat i quina és la teva especialització?
- Em vaig doctorar en informació quàntica però més específicament vaig treballar amb òptica quàntica. En el meu treball d'òptica quàntica intentava aconseguir desenvolupar dispositius que podien ser utilitzats per qualsevol tipus de protocol d'informació quàntica. Sobretot el que feia jo era treballar la llum i els àtoms de manera quàntica, és a dir, treballava molt la interacció entre la matèria i la llum però des del punt de vista de la física quàntica perquè normalment s'hi treballa molt des del punt de vista semi-clàssic ja que la llum de vegades s'agafa d'una forma quàntica però amb l'àtom només s'hi treballa en primera quantització. Utilitzava els dos conceptes de manera quàntica amb la qual cosa feia aquest estudi sobre la interacció entre la llum i la matèria. Per exemple jo treballava els condensats de Bose-Einstein amb una interacció quàntica amb la llum.

- Què és el que et fascina més de la física quàntica?
- Sobretot que posa a prova la teva lògica constantment perquè quan creus que ja ho has entès, te n'adones que no has entès res. Penso que són més fascinants les preguntes que et desperta que no pas les respostes que et dóna i inevitablement et porta fins als límits d'allò que pots comprendre i a vegades és inevitable no fer aquest pas i tenir unes discussions cientifico-filosòfiques molt interessants.

- Aparentment si sorgeixen les computadores quàntiques poden portar problemes en els temes de desxiframent de dades, creus que si la criptografia i les computadores quàntiques sorgissin alhora podrien suposar la solució l'un de l'altre?
- S'aniran adaptant, pensa que per exemple, en criptografia quàntica, ID Quantique és una empresa que va sorgir a la universitat de Ginebra i ja s'està comercialitzant.
No crec que arribi a ser un problema social ja que els protocols d'encriptació quàntica són bastant fàcils d'aplicar ja que amb fibra òptica ja ho pots fer. En canvi, per aconseguir una computadora quàntica necessitaries una sala enorme, de manera que no hi ha perill que arribi un *hacker* amb un portàtil i ho utilitzi, abans ja s'haurà solucionat el problema d'encriptació. A més a més a la computació quàntica encara li

falta molt, abans haurem de passar per els simuladors quàntics que permeten simular estats quàntics i això ja seria un avanç.

- Creus que dintre d'uns quants anys la física quàntica guanyarà importància i passarà a ser quelcom habitual en les nostres vides, des del punt de vista acadèmic respecte al coneixement d'aquesta i domèstic a nivell d'aplicacions pràctiques?

- Domèstic ja ho és tot i que no en siguem conscients ja que gracies a la física quàntica funcionen els microones, les portes dels supermercats s'obren, els punters laser funcionen, podem tenir transistors... Sense el coneixement que tenim de la física quàntica no podríem haver desenvolupat tota aquesta tecnologia.

El que passa és que ara arribarà el que a mi m'agrada anomenar ``una segona revolució quàntica´´ quant a tecnologia, és a dir, la primera revolució quàntica tecnològica va ser la que he anomenat abans, per exemple, poder fer un làser, tenir un microones, els transistors... Quan comencem a parlar sobre criptografia, teletransportació o computació quàntica és quelcom que impacta més en la gent i comença a fer-se mes popular. Penso que quan tot això arribi a un nivell domèstic, arribarà acompanyat amb un coneixement, que tot i que sigui sense voler, serà molt més avançat i molt més difós del que és la física quàntica. Penso que avui en dia ja s'hauria d'estar explicant i en la meva opinió crec que la física quàntica ja s'hauria d'ensenyar des de les escoles als nens petits, no les matemàtiques, però si que a un nen li pots explicar l'estructura de la matèria amb els quarks i les partícules fonamentals. Jo amb el llibre de *La porta dels tres panys* he anat a fer xerrades de física quàntica a nens de nou anys i els he explicat la dualitat ona-partícula, l'efecte fotoelèctric, la superposició i els he ensenyat el vídeo de la doble escletxa; lògicament ells no et sabran agafar les matemàtiques però jo el que pretenc és que comencin a familiaritzar-se amb aquest llenguatge, per exemple, et pot venir un nen de 9 anys i dir-te els noms de les partícules fonamentals, és a dir, ja tenir-ho normalitzat per quan després ho estudiïn no hagin de començar de zero. Penso que si la gent conegués més aquestes coses pensarien que la ciència és mes divertida ja que seguim explicant la mateixa ciència que fa 100 anys.

- Com recomanes que ha d'actuar algú que té moltes ganes d'entrar en aquest món, com hauria de començar...

- Jo recomano que alhora que estudies, segueixis llegint coses de divulgació científica ja que si et fiques directament amb la part més abstracta, les matemàtiques i estudiar-ho tot, de vegades perds de vista la perspectiva. Per exemple, està molt bé estudiar termodinàmica però aquestes equacions que de vegades no te les tradueixen saber entendre que són les equacions que t'expliquen com neixen, evolucionen i arriben a

morir les estrelles, això li dona un toc de passió al que estàs fent. Sinó, pot arribar un punt en el qual et perds, i a mi em va passar. Vaig arribar a un punt en què estava estudiant la carrera i vaig veure que no era el que m'imaginava, has de combinar les lectures que t'estimulen de manera que a allò que estàs fent li puguis trobar una explicació i així trobar-li el sentit. Pensa que estudiar física és molt dur en el sentit que t'hi has d'esforçar molt i l'única manera d'aconseguir esforçar-t'hi és gaudir del que estàs fent.

6.2. Entrevista a Nicolas Gisin

Interview with Nicolas Gisin (anglès)

* Professor Nicolas Gisin was born in Geneva, Switzerland, in 1952. After a master in physics and a degree in mathematics, he received his Ph.D. degree in Physics from the University of Geneva in 1981 for his dissertation in quantum and statistical physics.
After a post-doc at the University of Rochester, NY, he joint a start-up company, Alphatronix, dedicated to fiber instrumentation for the telecommunication industry.
In 1988 an opportunity to join the Group of Applied Physics at the University of Geneva as head of the optics section brought him back to the academic life. At the time the optics section was entirely devoted to support of the Swiss PTT (now Swisscom). In order to get a critical mass and stability, the optics section under the impulse of Prof. N. Gisin started two new research directions, one in optical sensors, one in quantum optics. The telecom and the sensing activities led to many patents and technological transfers to Swiss and international industries. Several products had and still have a commercial success. The quantum optics activities are more basic research oriented. The main theme is to combine the large expertise of the group in optical fibers with basic quantum effects. More recently, the demonstration of quantum cryptography and of long distance quantum entanglement received quite a lot of attention as well from the international scientific community as from the press “grand public”.
In 2009, he was awarded the First Biennial John Stewart Bell Prize for Research on Fundamental Issues in Quantum Mechanics and their Applications.

- I have read The Code Book by Simon Singh, a book about cryptography. The last part

of the book talks about quantum cryptography. This book was published 12 years ago, in 2000 and says that the maximum distance that a key can be send using quantum cryptography is 15 km because at more distances the ''sound'' or errors caused by the system are too high. I know that nowadays the results of the Swiss elections are sent by using quantum cryptography. How do you think that the practical application of quantum cryptography has changed from its beginnings?

- Quantum cryptography has changed a lot since this book and today the longest distance of commercial quantum cryptography or quantum key distribution is about 70km and the longest that has been demonstrated in the lab is 250km, however, there is a limit. I mean this 250 km with a few improvements maybe we will go to 300km but we shall not go to 500km or longer distances, it's just impossible, there is a limit.

- What are the main problems of quantum cryptography today?

- I think that the main problems are two. The first is the financial aid because not all but most of the commercial customers are banks and the banks haven't money and even the Swiss banks have no money so that's why we are really having a bad time.
There is another reason that slows down the quantum key distribution, is that the classical cryptographers, the specialists of classical cryptography don't like quantum because they don't understand it so they tend to underestimate it because they are afraid that they would lose their job if we go to a technology that they don't understand. And it's also true that many of my physicists colleagues oversell quantum cryptography, so between both that oversell and underestimate there is a big gap. And that will take time to fill because there are still a lot of progress to be done but a lot has happened yet.

- Maybe today quantum cryptography is not very famous but do you think that it will take a lot of transcendence in the future? How do you see it in the future?

- Yes, I think so. I think that it will continue to roll but I think by the next five years the development will be slow, because of these psychological problems of the classical cryptographers and because the situation of the banks. So it's going slowly but it's going and I'm sure that If we late a few decades ahead, if we locate in a relativity far future I'm sure that quantum cryptography and more general quantum technologies will become available. It's a natural trans, we go to smaller things, look at your little recorder here, to make something that small you have to get the electronics closer and closer at to the quantum domain. We don't know how many billions of transistors are in that and every time we make thinks smaller and compact so we are going to the quantum, moreover, everyone wants security, we always talk about security, so I think these quantum technologies have a great future.

- Is possible to share a key by quantum cryptography through the air in a level that it can be useful, like using the satellites to do it?
- Yes, I am not working in this but there are people working in that in Europe, especially in Vienne and there are also people working in that in China, Japan and in US. Now there is a little race between these three or four who will be the first to do a quantum key distribution between a satellite and the earth and I bet it will be the Chinese because their motivation is also political so they want to be the first. Japanese too are very interested but I guess for the Chinese. And I think that's going to happen very soon, in a few years I guess we'll have such a demonstration.

- What are the principal advantages of the SARG04 protocol on the BB84 protocol?
- Most of the implementations of quantum key distributions don't use a single photons, in the theory we should use a single photon, a single qubit, but no one uses that commercially, what people uses is a device that makes that most of the bits are empty, if it's empty we don't lose any information, sometimes there is one photon, so that is fine, and sometimes there are two photons or more, it's rare having two photons or more but it happens. Of course If you have two photons or more you could imagine that the adversary, Eve, can take one of these photons and let the other one go and that is called photon number splitting attack and this attack is quite efficient on the BB84 protocol and the SARG protocol has the advantage of being more robust in that. But there are now even better protocols than resist this photon number splitting attack, there is one that is called decoy-state and the decoy-state protocol is actually the most robust to this photon number splitting attack.

- Is now SARG04 protocol being used instead of the BB84? Has SARG04 protocol replaced BB84 protocol?
- Both are used. For instance in the long distances that I mentioned before is used SARG.

-How you and your team had this idea? How this type of ideas that break with all known come?
- Actually you need a combination of several things. It's very important to have people with a lot of experience and a kind of global view, like myself and others, but there is also equally and extremely important to have students that at the beginning don't have much experience but to them you give a relatively appreciated topic and of course you need good students that will bend work full time, you know, they are 25 years old typically like that, and they work full time on some problem and they are

bright persons. Moreover there must be a good environment, with students and also with some more advanced post-docs. These different lines, the students, the post docs and the professors and researchers, it really matter to get the good combination between these people to get the good ideas, and the ideas don't come just thinking by yourself in your bath or wherever, ideas come mostly by talking, so people should talk and work a lot together and also is important the way how you develop and work in the lab. So progress has mostly to do with interaction between the human beings of different categories because you need ones that they are working daily on the same problem with a lot of persistence but you also need someone who organizes what type of questions we shall address.

- How did you started in this world? Did you know from the first moment that you wanted to dedicate to this fascinating work?

- No because when I was a high school student I didn't know anything about quantum first and I didn't even really understand the difference between physics and mathematics, so it was not clear to me in that time. After my high school I even went for two years travelling around the world and I did a lot of interesting things but no studies, and it's only two years after finishing high school that I decided that I wanted to have studies and because I didn't really know what studies I wanted to do I did physics and mathematics. I did both and It's only when studying that I understood the importance of physics and It's only then when I discovered quantum physics, however, I have to say since I started discovering quantum physics that I really realized how fascinating that is but even not that time and even I didn't know of course quantum cryptography, because that was not known and was not even invented at that time anyway, but I didn't even know about non locality, entanglement, this very important concepts of today because most of them were rarely known and our professors didn't teach them and our professors didn't know much about it, so I actually think that I learned doing my PhD, so I discovered this kind of things and then, once I discovered that, entanglement, non locality... then I knew that physics was what I wanted to do. When even after knowing that this was what I wanted to do, Is not easy to know what you want to do, so then I actually worked for a long time also in classical optical communications, optical fibers, this kind of things and It is only once I was getting more permanent at the university, you know, climbing the hierarchy that I could decide to do quantum cryptography and I think it was in the early nineties when I decided to do that and it had immediately a big effect because I was one of the few persons who at the same time, understanding the theory and mastering optical fibers and combining these two I was the first to do quantum cryptography over significant distances and that had a big impact on the entire community.

- In what are you working now? Are coming important discoveries?
- My team is organized in four groups, four directions. One still works with QKD and single photon detectors and their aim is making QKD more reliable, faster, longer distances, better electronics, optics, software… so it's a part which is pretty engineering. Although you need ideas, basic ideas, it's very technical. And then if you really want to go beyond this four or five hundred kilometers limit which I mentioned what you need is something called quantum repeater. For a quantum repeater you need several things, you need quantum teleportation but you also need quantum memories, so we are working a lot in quantum teleportation and quantum memories to develop these quantum repeaters, this is a second activity which is maybe the most important today. We have two more groups; one is doing quantum communication, everything which is not quantum repeaters, so you have a lot of possibilities and things to do. The last group is a theory group and they deal with the theory of non-locality, so non-locality is something that is intellectually very fascinating.

Entrevista a Nicolas Gisin (català)

* El professor Nicolas Gisin va néixer a Ginebra, Suïssa, el 1952. Després d'obtenir un màster en física i un graduat en matemàtiques, va rebre el seu doctorat en física per la Universitat de Ginebra el 1981, per la seva dissertació en física quàntica i estadística.
Després d'un post doctorat a la Universitat de Rochester, Nova York, es va a unir a una companyia emergent, Alphatronix, dedicada a l'instrumental per treballar amb fibra òptica i a la indústria de les telecomunicacions.
El 1988 li va sorgir una oportunitat per unir-se al grup de física aplicada a la Universitat de Ginebra com el cap de la secció d'òptica, això el va tornar a portar a la vida acadèmica. La secció d'òptica va ser totalment desenvolupada per donar suport al servei de telecomunicacions suís (avui en dia Swisscom). Per tal d'aconseguir certa estabilitat, dues noves direccions, una en sensors òptics i l'altra en òptica quàntica. Les telecomunicacions i les activitats de detecció portaren moltes patents i molta transferència de tecnologia per a Suïssa i les indústries internacionals. Diversos productes van tenir i encara tenen èxit comercial. Les activitats d'òptica quàntica estan

orientades més en la recerca. L'objectiu és combinar la gran perícia del grup en fibra òptica amb bàsics efectes quàntics. Més recentment, la demostració de la criptografia quàntica i l'entrellaçament quàntic a llarga distància han rebut molta atenció tant de la comunitat científica internacional com de la premsa ''gran públic''.
El 2009, Nicolas Gisin va ser guardonat amb el premi John Stewart Bell per la recerca en els temes fonamentals de la mecànica quàntica i les seves aplicacions.

- He llegit Els Codis Secrets de Simon Singh, un llibre sobre criptografia. La darrera part del llibre parla sobre la criptografia quàntica. Aquest llibre va ser publicat fa 12 anys, el 2000 i diu que la màxima distància que una clau pot ser enviada fent servir la criptografia quàntica són 15km perquè a més distancia el ''soroll'' o errors causats pel sistema són massa alts. Sé que avui en dia els resultats de les eleccions Suïsses són enviats fent servir la criptografia quàntica.
Com creu que ha canviat l'aplicació pràctica de la criptografia quàntica des dels seus començaments?
- La criptografia quàntica ha canviat molt des que va sorgir aquest llibre i avui en dia la distància comercial més llarga de la criptografia quàntica o distribució quàntica de la clau és d'uns 70km i la més llarga que s'ha demostrat al laboratori és de 250km, tot i això, hi ha un límit. Aquests 250km amb millores potser arriben a 300km però segurament no arribarem als 500km o distàncies més llargues, és impossible, hi ha un límit.

- Quins creu que són els principals problemes de la criptografia quàntica en l'actualitat.
- Crec que hi ha dos principals problemes. El primer és l'ajuda financer; no tot, però la majoria de consumidors comercials són els bancs i els bancs no tenen diners, fins i tot els bancs suissos no tenen diners i és per això que tots estem realment patint uns mals moments, però hi ha una altra raó que intenta tirar a terra la criptografia quàntica: els criptògrafs clàssics. Als especialistes en criptografia clàssica no els i agrada la criptografia quàntica perquè no l'entenen; per tant, ells intenten devaluar-la ja que tenen por de perdre la feina si anem cap a una tecnologia que no entenen. També és cert que molts col·legues meus, que són físics, elogien massa la criptografia quàntica, per tant entre aquests que sobrevaloren i infravaloren, hi ha una gran bretxa. I es tardarà temps a omplir-la, perquè tot i que hi ha molts progressos per fer, n'hi ha que ja estan fets.

- Potser avui en dia la criptografia quàntica no és molt famosa però creu que guanyarà importància en el futur? Com la veu en el futur?
- Sí, ho penso. Crec que continuarà desenvolupant-se però crec que per als següents

cinc anys el desenvolupament serà lent a causa d'aquests problemes psicològics dels criptògrafs clàssics i per la situació dels bancs. Per tant, va lent però està anant i estic segur que si esperem unes quantes dècades, si esperem a un relativament futur llunyà estic segur que la criptografia quàntica i més en general la tecnologia quàntica estaran a l'accés del consumidor. És una transició natural en què cada cop anem cap a coses més petites. Mira la teva petita gravadora aquí, per fer quelcom tan petit has de fer que l'electrònica estigui cada cop més junta fins arribar als dominis quàntics. No sabem quants bilions de transistors conté al seu interior i cada cop que fem coses més petites i compactes ens estem apropant cap a la quàntica, d'altra banda, tothom vol seguretat, nosaltres sempre parlem sobre la seguretat, per tant, crec que la criptografia quàntica tindrà un molt bon futur.

- És possible intercanviar una clau a través de la criptografia quàntica a un nivell que pugui ser útil, com per exemple utilitzant satèl·lits?
- Si, jo no hi estic treballant però hi ha gent que hi treballa a Europa, especialment a Viena i també hi ha gent treballant-hi a la China, Japó i Amèrica. Ara hi ha una petita cursa entre aquests tres o quatre que seran els primers que faran criptografia quàntica entre un satèl·lit i la terra. Jo aposto per la China ja que la seva motivació és també política, per tant, ells volen ser els primers. Els japonesos també hi estan molt interessats però crec que seran els xinesos. Penso que això passarà molt aviat, en uns pocs anys crec que ja tindrem una demostració.
- Quins són les principals avantatges del protocol SARG04 davant del BB84?
- La majoria d'implementacions de la distribució quàntica de la clau no utilitzen fotons sols, en teoria hauríem d'utilitzar fotons sols, un sol qubit, però ningú ho utilitza comercialment. El que la gent utilitza és un procés en què la majoria de casos els bits estan buits, si està buit no perdem informació, de vegades hi ha un fotó, que està bé, però de vegades hi ha dos fotons o més, és estrany tenir dos o més fotons però passa. És evident que si tens dos fotons o més pots imaginar que l'adversari, l'Eve, podria agafar un dels fotons i deixar que l'altre segueixi el seu camí i això s'anomena PNS (photon number splitting attack), hi ha un protocol anomenat decoy-state que és el més robust davant l'atac PNS.

- Actualment s'utilitza el protocol SARG04 en lloc del protocol BB84? El SARG04 ha reemplaçat el BB84?
- Els dos són utilitzats. Però per les distàncies llargues que he mencionat abans s'utilitza el SARG.

- Com vostè i el seu equip van tenir aquesta idea? Com es tenen aquestes idees que

trenquen amb tot el conegut?

- En realitat es necessita una combinació de diverses coses. És molt important tenir gent amb molta experiència, amb un tipus de visió global, com jo mateix i d'altres. Però també és igual i extremadament important tenir estudiants que al principi no tenen molta experiència i a ells els proporciones un tema determinat, per descomptat que necessites bons estudiants, que estiguin moltes hores treballant, ja saps, acostumen a tenir uns 25 anys i ells treballen tot el temps en algun problema i són persones brillants. D'altra banda hi ha d'haver-hi un bon ambient, amb estudiants i també alguns més avançats com post docs.

Aquestes línies diferents, els estudiants, els post docs i els professors i investigadors és molt important de tenir la bona combinació entre aquesta gent perquè sorgeixin les bones idees. Les idees no només sorgeixen pensant un mateix al lavabo o a qualsevol lloc, les idees bàsicament sorgeixen parlant, per tant, la gent hauria de parlar i treballar molt en equip i també és important la forma com es desenvolupa i es treballa al laboratori. Per tant, el progrés es fa amb la interacció entre els éssers humans de diferents categories perquè necessites uns que estiguin treballant dia a dia en el mateix problema amb molta persistència però també necessites algú que organitzi com han d'anar adreçades les qüestions que es plantegen.

- Com va començar en aquest món? Sabia des del principi que es volia dedicar al que fa actualment?

- No perquè quan era un estudiant de batxillerat primerament no sabia res de la quàntica i tampoc entenia realment la diferència entre la física i les matemàtiques, per tant, en aquell moment no ho tenia clar. Després del batxillerat vaig estar dos anys viatjant per tot el món i vaig fer moltes coses interessants però estudis no. És només dos anys després d'acabar el batxillerat que vaig decidir que volia tenir estudis i com que no tenia molt clar quins estudis volia fer vaig fer física i matemàtiques. Vaig fer els dos i va ser només quan vaig estudiar-ho que vaig descobrir la importància de la física i de la física quàntica. Tot i això he de dir que des que vaig començar a descobrir la física quàntica i vaig descobrir com fascinant era no va ser exactament llavors, en aquell moment no coneixia totes les seves característiques, com la criptografia quàntica, perquè llavors no era coneguda i pràcticament no estava ni inventada, però tampoc coneixia la no-localitat, entrellaçament..., tots aquests conceptes tan importants avui en dia, ja que la majoria d'ells eren estranyament coneguts i el nostre professor no sabia molt d'aquests temes i crec que realment vaig aprendre quan vaig fer el meu doctorat, llavors vaig descobrir aquest tipus de coses com entrellaçament, no-localitat... Llavors va ser quan vaig saber que la física era el que volia fer. No és fàcil saber el que un vol fer i llavors encara que vaig estar treballant durant molt de temps

en comunicacions per òptica clàssica, fibra òptica i aquest tipus de coses. Només va ser quan vaig començar a agafar més permanència a la universitat, ja saps, escalant posicions en la jerarquia, quan vaig poder decidir fer criptografia quàntica. Crec que va ser a principis dels noranta quan vaig decidir-ho i immediatament va tenir un gran impacte perquè jo era una de les poques persones que al mateix temps, entenent la teoria també dominava les fibres òptiques i combinant aquestes dos parts vaig ser el primer en fer criptografia quàntica en unes distàncies significatives i això va tenir un gran impacte en la comunitat.

- En què treballa ara? Falta poc per què sorgeixin descobriments importants?

- El meu equip esta organitzat en quatre grups, quatre direccions. Un encara treballa amb QKD (quantum key distribution) i detectors de fotons aïllats; el seu objectiu és aconseguir una QKD més accessible, ràpida, a unes distàncies més llargues, amb una millor electrònica, òptica, software... és un grup on es necessita molta enginyeria. Tot i que necessites idees, idees bàsiques, és molt tècnic. Llavors si vols arribar més lluny d'aquests quatre o cinc cents quilòmetres que he mencionat abans el que es necessita és un repetidor quàntic. Per tenir un repetidor quàntic es necessiten diverses coses, necessites la teletransportació quàntica i també memòries quàntiques, per tant, estem treballant molt en teletransportació i memòries quàntiques per desenvolupar aquests repetidors quàntics, aquesta és una segona activitat, potser la més important actualment.

Tenim dos grups més; un es dedica a les comunicacions quàntiques, qualsevol cosa que no siguin repetidors quàntics, per tant tenen moltes possibilitats i coses a fer.

L'últim grup és un grup teòric i tracten la teoria de la no-localitat, la qual és molt fascinant intel·lectualment.

7. EPÌLEG

A partir del llarg procés de recerca i estructuració de la informació he pogut arribar a les següents conclusions, tot i que totes no es reflecteixen directament en aquest treball, em semblen més importants:

-Referent a la física quàntica:

1 - Les partícules subatòmiques* , existeixen en un estat potencial obert a totes les possibilitats fins que nosaltres les alterem en observar o mesurar-les i en aquell moment es converteixen en alguna cosa real .

2 - També que tot en l'univers està fet del mateix material bàsic . Al nostre nivell més fonamental , els éssers vius incloent l'ésser humà , som paquets d'energia quàntica , intercanviant informació constantment en un mar d'energia inextingible .

3- La interferència es dóna entre dos conjunts d'ones o de partícules , és a dir les crestes d'un dels conjunts d'ones poden coincidir amb les valls d'un altre conjunt . En aquest cas els dos conjunts s'anul·len mútuament en lloc de conjuminar-se en una ona més intensa .

4-La interferència a més, es pot produir amb partícules a causa de la dualitat* (ona - partícula) introduïda per la mecànica quàntica* . Aquesta deducció és molt important perquè permet l'existència dels camps* interferents .

5- Acceptar els models no com la realitat, sinó com la millor representació de la mateixa en un determinat moment. Això ens obre la ment, perquè ens fa pensar els models no com definits i determinats, sinó com una evolució constant.

-Referent a criptografia quàntica:

El principal avantatge de la criptografia quàntica és que a diferència que en tots els mètodes de criptografia convencionals, la seguretat de la criptografia quàntica no depèn de la capacitat de còmput de l'adversari sinó que està garantida en forma absoluta per les lleis de la física quàntica. Un altre gran avantatge que ofereix és la seva capacitat única per detectar escoltes. I tot i que encara quedi molt per fer en matèria d'investigació fins que sigui un mètode aplicable a gran escala, la criptografia quàntica és un salt importantíssim en matèria de seguretat.

Respecte a la dificultat de realitzar el treball, puc dir que la recerca d'informació no ha estat tan fàcil com m'esperava. Sobretot, el més complicat ha estat a l'hora d'explicar els conceptes i intentar obrir la ment cap a la física quàntica, que com que es comporta únicament en el món microscopi no es correspon amb la lògica racional de la nostra vida diària. També m'ha semblat dificultós alhora d'organitzar tots els apartats, temes i sintetitzar la informació. Tot i que al començament l'explicació de conceptes no donava els seus fruits ja que les paraules emprades no eren les més adients i em feia un embolic, poc a poc amb l'ajuda dels tutors i l'entrevistada he anat reunint els elements de diverses fonts diferents que m'ha ajudat a donar-li un sentit més profund al treball.

Personalment , als inicis del treball no sabia ben bé com idear-lo i no trobava la manera de fer alguna cosa més pràctica. Però una vegada he assolit certs coneixements del tema sobre la criptografia quàntica, a base de consultar fonts d'informació, el treball s'ha anat fent més amè i m'han començat a sorgir idees de caire més pràctic.

A través de les entrevistes i amb el meu tutor de la universitat, he pogut observar i entendre de més a prop el funcionament i l'impacte de la física quàntica a la nostra societat, així com també el treball que fan els físics relacionats en criptografia quàntica al dia a dia.

Cal destacar que s'han presentat dificultats alhora de realitzar una pràctica completament experimental durant el curs. Bàsicament per dos motius. El primer es deu al fet que intentar realitzar una pràctica en física quàntica ha estat impossible per la falta de la maquinària, el seu preu costós així com també el gran nivell de coneixement necessaris per fer els carregosos càlculs i saber-los interpretar correctament. Així que he omplert aquesta mancança amb la realització d'experiments mentals i exemples per poder entendre millor tant els principis de la física quàntica com els diferents protocols en criptografia quàntica.

8.GLOSSARI

Aquest glossari conté paraules que no han estat assenyalades amb asterisc però que es troben a les entrevistes o en les mateixes definicions. Aquestes definicions són per a qui únicament coneix la física més elemental.

accelerador de partícules: Aparells que utilitzen camps electromagnètics per accelerar partícules subatòmiques amb càrrega elèctrica fins a velocitats molt properes a la de la llum.

àtom: És la part més petita que forma part d'un sistema químic. És la mínima quantitat d'un element químic que presenta les mateixes propietats de l'element. Està format per electrons, protons i neutrons.

barrera d'energia: És un problema de model mono-dimensional (un a dimensió) que permet demostrar el fenomen de l'efecte túnel.

bit: És l'acrònim Binary digit ('dígit binari'). Un bit és un dígit del sistema de numeració binari.

camp: És l'assignació d'una quantitat a cada punt de l'espai. Aquesta quantitat pot ser escalar i llavors es parla de *camps escalars* (és a dir, simplement s'assigna un número a cada punt de l'espai) o vectorial i es parla de *camps vectorials* (és a dir, assignem un vector: mòdul, direcció i sentit). Un exemple de camp escalar podria ser la temperatura: a cada punt de l'espai li podem associar un valor numèric que és la temperatura d'aquell punt. Un exemple de camp vectorial és el camp gravitatori: a cada punt de l'espai assignem un vector que indica la magnitud, la direcció i el sentit de la força gravitatòria que experimentaria una massa unitària.

camp electromagnètic: És un camp produït per la presència d'objectes carregats elèctricament. Aquest camp s'estén indefinidament a través de l'espai i afecta el comportament dels objectes.

camp magnètic: És una entitat física generada per la presència de càrregues elèctriques en moviment (com ara els corrents elèctrics), o bé per la presència de partícules quàntiques amb espín, i que exerceixen una força sobre les altres càrregues que es mouen sota la seva influència.

constant de Planck Pedra angular del principi d'incertesa - . el producte de la incertesa en la posició per la incertesa en la velocitat i per la massa ha de ser més gran que la constant de Planck - . És representada pel símbol h.

dualitat Correspondència entre teories aparentment diferents que condueixen als mateixos resultats físics.

efecte fotoelèctric: Fenomen en què són expulsats electrons d'una superfície metàl·lica quan aquesta és exposada a la llum.

efectes quàntics: Són els resultats que s'obtenen a través de les lleis que determinen la física quàntica.

electró: Partícula amb càrrega negativa que gira al voltant dels nuclis atòmics.

energia quantitzada: energia quantitzada: Significa que l'energia dels electrons en l'àtom està restringida a determinats valors característics. És a dir, l'energia pren valors discrets i no continus. Ja que segons el que va postular Planck que l'emissió de radiació electromagnètica es produeix en forma de "paquets" o "quants" d'energia (fotons). Això vol dir que la radiació no és contínua, és a dir, els àtoms no poden absorbir o emetre qualsevol valor d'energia, sinó només uns valors concrets.

equació de Schrödinger: Equació que regeix l'evolució de l' Funció d' ona en la teoria quàntica.

mecànica quàntica: Teoria desenvolupada a partir del principi quàntic de Planck i del principi d'incertesa d'Heisenberg.

espín: Propietat interna de les partícules Elementals relacionada però no idèntica a la va conèixer quotidiana de rotacions.

físio nuclear: Procés en què un nucli es trenca en dos o més nuclis menors , alliberant energia.

força electromagnètica: Força entre partícules amb càrregues elèctriques del mateix signe (o de signes oposats).

força nuclear forta: És la més intensa de les quatre interaccions fonamentals de la naturalesa , i la que té abast més curt . Manté units els quarks per formar protons i neutrons , i aquestes partícules unides entre si per formar els nuclis atòmics.

fotó: Quant de llum , el paquet més petit del camp electromagnètic.

funció d'ona(Ψ): És una forma de descriure l' estat físic d'un sistema de partícules. Usualment és una funció complexa i de quadrat integrable de les coordenades espacials de cadascuna de les partícules. Les propietats esmentades de la funció d'ona permeten interpretar-la com una funció quadràtica integrable.

freqüència: En una ona, és el nombre de cicles complets per segon.

fusió nuclear: Procés en què dos nuclis xoquen i s'uneixen per formar un nucli més gran i més pesat.

longitud d'ona: Distància entre dues crestes o dues valls consecutives d'una ona.

magnitud: És qualsevol propietat natural que pot ser quantificada a partir de la mesura o del càlcul matemàtic, els possibles valors s'expressen en forma d'un número i, generalment, una unitat de mesura.

neutró: Partícula sense càrrega , semblant al Protó , que constitueix gairebé la meitat de les partícules que formen nuclis atòmics . Està format per tres quarks (dos cap avall i un cap amunt).

observador: Persona o instrument que mesura propietats físiques d'un sistema.

ones electromagnètiques: Són ones que es propaguen a l'espai amb un component elèctric i un component magnètic. Aquests dos components oscil·len en angles rectes respecte ells i respecte a la direcció de propagació, i són en fase entre ells.

partícula elemental: Partícula que no pot ser subdividida.

partícules subatòmiques: És una unitat bàsica constituent de la matèria que per si sola no conserva les propietats d'un element químic. Poden formar part dels àtoms, que sí que conserven aquestes propietats.

protó: Partícula de càrrega positiva , molt semblant al neutró , que constitueix aproximadament la meitat de la massa dels nuclis atòmics . Està formada per tres quarks (dos amunt i un avall) .

protocol: Conjunt de procediments destinats a estandarditzar un comportament humà o sistemàtic artificial enfront d'una situació específica.

protocol criptogràfic: Protocol abstracte o concret que realitza funcions relacionades amb la seguretat, aplicant mètodes criptogràfics.

quants: Unitat indivisible en què les ones poden ser absorbides o emeses.

quark: És un tipus de partícula elemental, i un component fonamental de la matèria. Es caracteritzen per tenir una càrrega elèctrica fraccionària (+2/3, o -1/3; -2/3, o +1/3 els antiquarks) així com la càrrega de color, és a dir, la magnitud activa en la força nuclear forta.

qubit: És un sistema quàntic amb dos estats propis i que pot ser manipulat arbitràriament. És a dir, es tracta d'un sistema que només pot ser descrit correctament mitjançant la mecànica quàntica.

sistema: És qualsevol conjunt d'elements en interacció. També s'entén un sistema com un grup de parts en interacció que funcionen com un tot i que és distingible del seu entorn a través d'uns límits o fronteres reconegudes.

9.BIBLIOGRAFIA I WEBGRAFIA

Bibliografia

FERNÁNDEZ-VIDAL, Sònia., *Quantic love*, La Galera, Barcelona, 2012.

FERNÁNDEZ-VIDAL, Sònia., *La porta dels tres panys*, La Galera, Barcelona, 2010.

FERNÁNDEZ-VIDAL, Sònia .,La màgia de la física quàntica, 1990.

HAWKING, S. W., MLODINOW, L. , *El gran disseny*, Crítica, Barcelona, 2011.

HAWKING, S. W., *El universo en una cáscara de nuez*, Crítica, Barcelona, 2001.

HAWKING, S. W., Los *sueños de los que está hecha la materia*, Crítica, Barcelona, 2011.

JOU, D., Introducción *al mundo quántico*, Pasado y Presente, Barcelona, 2012.

LINDLEY, D., *Incertidumbre*, Ariel, 2010.

FEYNMAN, R. P., ¿Qué te importa lo que piensen los demás?, Alianza Editorial, Madrid, 2011.

KAKU, M., *La física del futuro*, Debate, 2011.

SINGH, S., *Los códigos secretos*, Debate, 2000.

DELIGORGES, S., *El mundo cuántico*,Alianza Univ., 1990.

FERRERO, M., FERNÁNDEZ-RAÑADA, A.,SÁNCHEZ-GÓMEZ, *Fundamentos de Física Cuántica. Curso de verano de El Escorial*, Complutense, Madrid, 1996.

.V.A.A.;*Misterios de la Física Cuántica*, Investigacóón y Ciencia, Temas 10, 1997.

MOORE, W.; *ErwinSchrödinger: una vida,* Cambridge Univ. Press, Cambridge, 1996.

NAVARRO, L., ed.; *El siglo de la Física*,Tusquets, 1992.

NEUMAN, J. von; *Fundamentos matemáticos de la Mecánica Cuántica*, Consejo Superior de Investigaciones Científicas, Madrid, 1991.

PAIS, A.; *Subtle is the Lord...-The science and the life of Albert Einstein*, Oxford Univ., Oxford, 1982.

PAIS, A.; *Niels Bohr's Times, in Physics, Philosophy and Polity*, Clarendon, Oxford, 1991.

REALE, G., ANTISERI, D.; *Historia del pensamiento filosófico y científico*, 3 vols., Herder, Barcelona, 1992.

SELLERI,F., *Quantum Mechanics Versus Local Realism. The Einstein-Podolsky-Rosen Paradox*, Plenum, New York, 1988.

SKALAR, Lawrence; *Filosofía de la Física*, Alianza Edit., Madrid, 1994.

BLACK, D., *Redes de computadoras: Protocolos, normas e interface.* Macrobit Editores, México,1990.

CABALLERO, Pino, *Seguridad informática: técnicas criptográficas*, Alfaomega, México.

DALTABUIT, Enrique,*La seguridad de la información,* Limusa, México.

FUSTER Sabater, Amparoi altres .,*Técnicas criptográficas de protección de datos,* Alfaomega, México,

LÓPEZ , María Jaquelina, *Criptografía*, UNAM, Facultad de Ingeniería, México,2009.

LÓPEZ , María Jaquelina, QUEZADA ,Cintia, *Fundamentos de seguridad informática*, UNAM, Facultad de Ingeniería ,México.

MENEZES, J. i altres .*Handbook of Applied Cryptography* Boca Raton, Florida.

PASTOR, José, i altres. *Criptografía digital : fundamentos y aplicaciones*, Prensas Universitarias de Zaragoza, Zaragoza.

Webgrafia

Vídeos

Historia de la física quàntica, youtube,
http://www.youtube.com/watch?v=RC8uRPlHgqs
Redes 94: La incertidumbre del universo cuántico - física cuántica, youtube,
http://www.youtube.com/watch?v=7sSiYXwyuiw
Redes 146: Física que causa perplejidad - física cuántica , youtube,
http://www.youtube.com/watch?v=o__ZgfSh1AM
García, J., Vídeo teletransportació quàntica, raconet, http://ciencia.raconet.cat/?p=86 Kjlg74,
Michio Kaku: La revolucion cuántica, youtube,
http://www.youtube.com/watch?v=nMjeUekseqE
Más allá del Cosmos - Un Salto Cuántico
http://www.youtube.com/watch?v=UYM_rdvgQWw
Las leyes de la Mecánica cuántica, youtbe,
http://www.youtube.com/watch?v=bghsPrJ7nDg&list=PL19E9CD3672699CB3
Documental sobre física cuántica y sus postulados en Español, youtube,
http://www.youtube.com/watch?v=kxF46NetyHc
Las Revoluciones en la visión del Mundo Físico La explicación cuántica. (conferencia)
http://www.youtube.com/watch?v=ki6ey4yC8iE
Seminario de introducción a la Computación y Criptografía Cuántica 1 (conferencia)
http://www.youtube.com/watch?v=3zsg3DGfWFg
Seminario de introducción a la Computación y Criptografía Cuántica 2 (conferencia)
http://www.youtube.com/watch?v=sW11m1JzXDs
Seminario de introducción a la Computación y Criptografía Cuántica 3 (conferencia)
http://www.youtube.com/watch?v=T723gMJmp_s
Científicos de Frontera - Ignacio Cirac (entrevista aquest increïble científic català)

http://www.youtube.com/watch?v=FSkmAUHBEkk

http://www.youtube.com/watch?v=6K3JRwNeFEM (Redes)

La Mecánica Cuántica y sus aplicaciones: el ordenador cuántico.

http://www.youtube.com/watch?v=O9TA2faf6nw

Vídeo protocol BB84, youtube, http://www.youtube.com/watch?v=UVzRbU6y7Ks

Escrits

Quantiki, http://www.quantiki.org/wiki/Main_Page

Wikipedia, Sonia Fernández-Vidal,

http://ca.wikipedia.org/wiki/Sonia_Fern%C3%A1ndez-Vidal

Gap-optique, Nicolas Gisin,

http://www.gapoptique.unige.ch/wiki/members:nicolas_gisin

Gaussianos, protocolo de distribución de clave, http://gaussianos.com/criptografia-protocolo-de-distribucion-de-clave-bb84

http://www.oberlin.edu/physics/dstyer/StrangeQM/history.html

http://www3.hi.is/~hj/QuantumMechanics/quantum.html

http://walet.phy.umist.ac.uk/QM/LectureNotes/ (un petit compendi de física quàntica, només per físics)

http://theory.uwinnipeg.ca/physics/quant/index.html (un altre compendi de física quàntica, més assequible que l'anterior)

http://phys.educ.ksu.edu/ ("The Visual Quantum Mechanics project" ; fantàstic link on es pot veure la simulació de l'experiment del Frank-Hertz, jugar amb l'espectre de l'hidrogen i observar l'efecte Zeeman)

http://en.wikipedia.org/wiki/Basics_of_quantum_mechanics

http://en.wikipedia.org/wiki/Quantum_mechanics (Nota: la wikipedia pot contenir errors i imprecisions: ha de ser llegida, com qualsevol text, en guàrdia. Però, crec, que és un bon intent, en algunes àrees, de divulgació, i conté nombrosos enllaços útils).

http://www.ciencia-hoy.retina.ar/hoy28/fisica02.htm

http://www.qubit.it/links/homelinks.html (En aquesta pàgina hi ha molts links, des dels coneixements teòrics de la física quàntica fins aplicacions interactives).