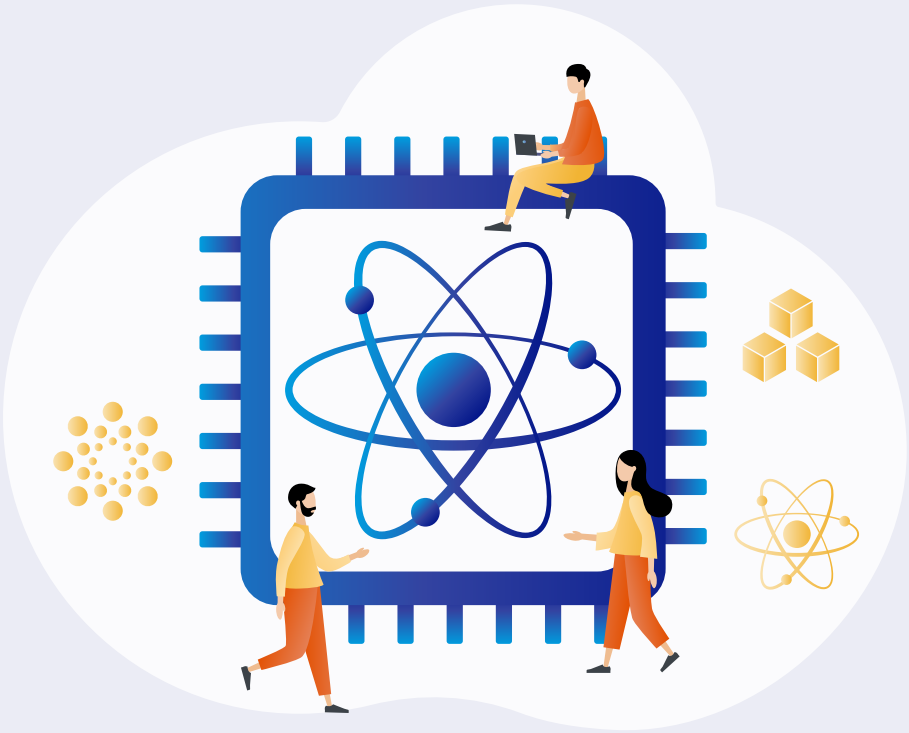
ICFO

LA CRIPTOGRAFIA QUÀNTICA A L'AULA



ICFO Maciej Lewenstein Quantum School for Teachers

Patronat

Generalitat de Catalunya

UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH

Fundació Privada CELLEX

Fundació Privada MIR-PUIG

Centre Cerca

Institució CERCA Centres de Recerca de Catalunya

Membre de

BIST Barcelona Institute of Science and Technology

Distinció

EXCELENCIA SEVERO OCHOA 2020 - 2023

Amb el suport de

Gobierno de España Ministerio de Economía y Competitividad

Unió Europea Fons Europeu de Desenvolupament Regional

QUANTUMCAT

Fundació Catalunya La Pedrera

Ajuntament de Barcelona

ECOP European Centres for Outreach in Photonics

ICFO Maciej Lewenstein Quantum School for Teachers

LA CRIPTOGRAFIA QUÀNTICA A L'AULA

Estem al principi de la segona revolució quàntica: moltes tecnologies emergents basades en els principis poc intuïtius de la física quàntica prometen portar beneficis a la societat en molts camps diferents, com per exemple el de les comunicacions i de la seguretat informàtica. Per això, és important que les **noves generacions estiguin familiaritzades amb la física quàntica**, perquè puguin entendre millor el món en què viuran i quins avantatges els ofereix, fugint de les promeses pseudocientífiques. La ciència i la tecnologia avancen més ràpidament que el currículum escolar, però això no vol dir que els alumnes hagin d'esperar a arribar a la universitat per conèixettr els últims avenços tecnològics: en aquest document hem recollit algunes **activitats que es poden traslladar fàcilment a l'aula** per introduir alguns conceptes relatius a una de les tecnologies quàntiques més madures: la criptografia quàntica.

Índex

1 Introducció a la Criptografia

La majoria de la gent no coneix la criptografia i la seva importància a les nostres vides. Aquesta activitat permet apropar-se a aquest fascinant món.

OBJECTIUS

Entendre la importància de la criptografia a la nostra vida.

PREPARACIÓ

Els alumnes busquen de manera individual notícies d'actualitat o informació sobre criptografia.

ACTIVITAT

En petits grups els alumnes tracten de respondre a les següents preguntes i després comparteixen les seves troballes amb la resta de la classe:

- És important la criptografia a la nostres vides? Per què?
- Com podries enviar un missatge a un/a company/a, sense que la resta de la classe s'adoni del contingut del missatge? Pensa en exemples que potser has vist en pelis, llibres o escape rooms.

CONCEPTES IMPORTANTS

Al dia d'avui, és fàcil accedir a moltíssimes dades gràcies al núvol i a les xarxes de comunicacions: per això, és crucial poder protegir les informacions més delicades (com per exemple les dades personals, sanitàries o financeres) d'ulls indiscrets.

Cada vegada que comprem per internet o amb la targeta, estem enviant les nostres dades bancàries i no volem que hi hagi cap espia que pugui obtenir aquestes informacions.

La **criptografia** és doncs una **eina fonamental per un món digital** com el nostre, perquè ens permet enviar i rebre dades de forma segura.

2 Codi de Substitució

Una manera senzilla de xifrar un missatge que potser ha sorgit a l'activitat precedent és substituir les lletres del missatge amb altres segon una regla establerta. Aquesta activitat permet treballar amb un codi de substitució i entendre les seves principals característiques.

OBJECTIUS

- Xifrar i desxifrar missatges amb un xifrat de substitució
- Entendre el principal límit d'un xifrat de substitució

ACTIVITAT

- Proposa als alumnes de desxifrar els següents missatges (en català):

"erhxz oz ulglmrxz" – "oz oofn vh fgro" [1]

on hem substituït cada lletra amb una altra segon una regla senzilla.

Pots suggerir que es concentrin en les paraules curtes com "oz" i "vh" i pensar en les paraules de dues lletres més comunes en català o també en la paraula "oofn" (no hi ha moltes paraules que comencin amb dues lletres iguals. No és important que desxifrin els missatges sencers, sinó entendre que els patrons de l'idioma que estem fent servir (e.g. hi ha poques lletres que poden aparèixer dues vegades al principi de paraules curtes) ens donen pistes per desxifrar el missatge.

Per xifrar els missatges precedents, vam fer servir uns dels codis de substitució més antics: el **codi Atbash**, que va ser utilitzat fins i tot a la Bíblia. Consisteix a substituir la primera lletra de l'alfabet per l'última, la segona per la penúltima, i així successivament. Les substitucions es poden resumir en aquesta taula:

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
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

- Els alumnes desxifren els missatges amb l'ajuda de la taula de conversió.
- Els alumnes intenten escriure el nom de l'escola amb aquest xifrat i controlen que el resultat coincideixi.

CONCEPTES IMPORTANTS

- Un codi criptogràfic transforma el missatge de manera que sigui fàcil d'entendre només si es coneix el codi.
- Idealment, els espies que no coneixen el codi no haurien de poder esbrinar el contingut del missatge. Tot i això, un codi de substitució manté els patrons de l'idioma i amb missatges suficientment llargs és possible recuperar al menys parcialment el codi.

[1] Solucions: "visca la fotonica" i "la llum es util".

3 Claus Criptogràfiques

Ja des de les societats més antigues, les persones han ideat mètodes per intercanviar-se informació sense que els adversaris sabessin el contingut dels missatges. Aquesta activitat permet explorar els principis bàsics de la criptografia a través d'un parell d'aquests mètodes antics: el codi Atbash i el codi Cèsar.

OBJECTIUS

- Entendre què és una clau criptogràfica.
- Xifrar i desxifrar missatges amb un xifrat senzill.

PREPARACIÓ: MATERIALS

- Paper, llapis
- Cartolina i tisores (opcionals, per a la roda del xifrat Cèsar)

ACTIVITAT

El general romà Juli Cèsar va fer servir un sistema molt senzill per encriptar els missatges dirigits a les seves tropes: substituir cada lletra per la que està tres llocs més enllà a l'alfabet. D'aquesta manera, escriuria una D en lloc de cada A, una E en lloc de cada B, una F en lloc de cada C, etc.

Les substitucions es poden resumir a aquesta taula:

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
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

- Els alumnes intenten escriure el nom de l'escola amb aquest xifrat i controlen que el resultat coincideixi.
- Discussió: quin codi és més difícil de desxifrar, el codi Atbash (presentat a l'activitat precedent) o el codi Cèsar?
- Discussió: una vegada que l'espia hagi esbrinat el codi, podem modificar un dels codis precedents de manera senzilla per generar un altre codi?

Encara que Cèsar sempre substituïa cada lletra per la que quedava 3 posicions més enllà, es poden crear moltes variacions senzilles, escollint la lletra que quedi X places més enllà. Això és una **clau criptogràfica**: obtindràs un missatge diferent depenent de la clau que facis servir.

- Quantes claus possibles hi ha usant codi Cèsar?[2]
- Cada alumne tria un valor X entre 0 i 26, i xifra una de les frases de l'activitat 2 segons la clau corresponent. Comparen els resultats: desxifrar el missatge es torna més complicat? Es podrien fer servir les mateixes estratègies que van fer servir per desxifrar les frases de l'activitat 2?
- Els alumnes tracten de desxifrar el següent missatge[3]:

"bfly slrtd lnlmle, otrfpd pw yzx op wl epgl lgtl lw oznpye"

Per fer-ho més ràpidament, els alumnes poden construir una roda de cartolina seguint el model que trobeu aquí (https://crypto.interactive-maths.com/uploads/1/1/3/4/11345755/shift.pdf) o fer servir la versió virtual que trobeu a aquest enllaç: https://inventwithpython.com/cipherwheel/.

Aquesta activitat és una adaptació de l'activitat "shift" d'aquesta pàgina web:
https://crypto.interactive-maths.com/downloadable-resources.html
Hi trobaràs més activitats interessants sobre criptografia (en anglès).

CONCEPTES IMPORTANTS

Les clau criptogràfiques permeten obtenir combinacions diferents amb una regla general (codi criptogràfic). Un codi que permeti múltiples claus és doncs més flexible i convenient.

[2] Solució: 26, tantes com les lletres de l'alfabet. Comptem també la clau A->A que transforma el missatge en un idèntic (que no és gaire útil per enviar missatges criptogràfics).

[3] Solució: "Quan hagis acabat, digues el nom de la teva avia al docent" Clau: X=15

4 Clau aleatòria: el Codi Vernam

Les activitats precedents ens han mostrat que és possible esbrinar part del missatge quan els codis preserven els patrons típics de l'idioma que estem emprant.
Una solució podria ser fer servir idiomes molt poc coneguts: per exemple, durant la segona guerra mundial, els Estats Units van utilitzar sistemes de xifrat basats en els idiomes d'algunes tribus natives americanes[4], com per exemple els Navajos.
Una altra possibilitat és fer servir l'atzar per amagar els patrons de la llengua.
En aquesta activitat veurem com l'atzar pot jugar un paper important a la criptografia.

OBJECTIUS

- Entendre que l'atzar contribueix a crear claus més segures.
- Xifrar i desxifrar fent servir claus aleatòries.
- Xifrar i desxifrar fent servir el sistema binari.

ACTIVITAT

El codi Vernam és un dels codis de substitució més difícil de desxifrar, perquè es canvia la regla de substitució per a cada lletra.

- Els alumnes xifren una de les frases de l'activitat 2 fent servir el codi Vernam: per cada lletra, generen un número aleatori[5] X entre 0 i 26 i substitueixen la lletra amb la que queda X places més enllà. Per anar més ràpidament, poden treballar en grups i dividir-se el treball.
- Els alumnes comparen els missatges que acaben de xifrar entre ells: tenen alguna cosa en comú? Podrien fer servir les mateixes estratègies que van fer servir per desxifrar les frases de l'activitat 2?
- Quantes claus diferents creuen que es poden crear amb aquest codi?

Fer servir l'alfabet pot ser una mica complicat quan es treballa amb claus aleatòries: xifrar i desxifrar es torna molt més senzill si fem servir el **sistema binari**, que és el que es fa servir en totes les comunicacions digitals, on cada missatge - des de texts fins i tot a imatges i vídeos - es converteix en una seqüència de 0 i 1.
Els alumnes proven de xifrar i desxifrar el missatge

01010001

que correspon al número 81 en el sistema binari i a la lletra Q en el codi ASCII, un dels estàndards per a convertir lletres en seqüències de 0 i 1.

- Cada alumne genera una clau de xifrat segons el codi Vernam, és a dir, generant un número aleatori entre 0 i 1 per a cada xifra de la seqüència. Poden fer servir per exemple una moneda.

Exemple: la clau és 11100101

[4] Per saber-ne més, mira aquí: https://en.wikipedia.org/wiki/Code_talker

[5] Podeu fer servir aquest generador de nombres aleatoris: https://www.random.org/sequences/

- Per xifrar el missatge, han de sumar[6] mòdul 2 el missatge a la clau: obtindran una seqüència encriptada. Ex:

Missatge	0	1	0	1	0	0	0	1
Clau	1	1	1	0	0	1	0	1
Missatge xifrat	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**0**

- Els alumnes proven d'intercanviar-se els missatges xifrats i a desxifrar-los: és una tasca fàcil?
- Ara els alumnes que s'havien intercanviat els missatges intercanvien també la clau: per desxifrar és suficient tornar a sumar la clau al missatge xifrat com al següent exemple:

Clau	1	1	1	0	0	1	0	1
Missatge xifrat	1	0	1	1	0	1	0	0
Missatge	**0**	**1**	**0**	**1**	**0**	**0**	**0**	**1**

CONCEPTES IMPORTANTS

- Les claus aleatòries augmenten significativament la seguretat dels missatges, ja que amaguen els patrons de la llengua que podrien donar indicis als espies.
- Una clau aleatòria ha de ser tan llarga com el missatge.
- Hi tantes claus com el nombre de missatges possibles de la mateixa longitud, doncs per missatges suficientment llargs, la tasca de desxifrar-los provant totes les claus no és viable.
- Per poder compartir informació de manera segura, és important que l'emissor i el receptor comparteixin la clau.
- Si la clau és de veritat aleatòria (de manera que l'espia no pugui inferir-la d'alguna altra manera), la comunicació serà veritablement segura.

[6] Quan se suma mòdul 2, es poden fer servir només 0 i 1, doncs has de fer servir de nou el 0 quan passes de l'1. Les operacions possibles quedarien així: 0 + 0 = 0; 0 + 1 = 1 + 0 = 1; 1 + 1 =0.

5 El secret d'una bona clau és no reutilitzar-la

Les claus aleatòries ens permeten generar missatges molt complicats de desxifrar, però amb algunes condicions. Amb aquesta activitat descobrireu un límit important de les claus aleatòries.

OBJECTIUS

- Entendre que reutilitzar les claus per diferents missatges redueix la seguretat de les comunicacions

MATERIALS I PREPARACIÓ

- Fulls d'acetat transparent per impressores
- Impressora

Imprimeix les pàgines 19-21 d'aquest document en fulls d'acetat transparent. En cada pàgina hi ha dues còpies de la mateixa imatge. Pots distingir les diferents imatges pel text que hi ha a sota a la dreta ("Imatge 1", "Imatge 2", "Clau"). Cada alumne hauria de tenir una còpia de cada imatge.

ACTIVITAT

Seguir les passes descrites a la pàgina 22.

CONCEPTES IMPORTANTS

- Si fem servir la mateixa clau per xifrar missatges diferents, una espia podria deduir part dels missatges originals només a partir dels missatges xifrats, tot i no tenir-ne la clau. Per això, utilitzar **una clau diferent per a cada missatge** és fonamental per garantir-ne la seguretat.
- El problema d'enviar informació segura es redueix doncs al problema de **compartir la clau de manera segura**. Per això en criptografia es parla normalment de mètodes de distribució de clau, que permeten compartir les claus de manera segura entre emissor i receptor.
- Els mètodes de distribució de clau que es fan servir actualment, com per exemple el protocol RSA, estan basats normalment en problemes matemàtics que siguin fàcils de resoldre en un sentit (per l'emissor i el receptor ha de ser fàcil xifrar i desxifrar el missatge) però molt difícil en el sentit oposat (per l'espia el problema ha de ser tan complicat que els ordinadors més potents trigarien massa temps per resoldre'l). Un d'aquests problemes és la factorització: multiplicar dos nombres grans és una tasca ràpida, però trobar els dos factors prims d'un nombre molt gran és una tasca complexa, on el temps per completar-la creix de manera exponencial amb el nombre de xifres del nombre a factoritzar.
- La seguretat dels actuals protocols criptogràfics depèn doncs de la tecnologia que tenim a l'abast.

6 Física quàntica: superposició i mesura

Gràcies a la física quàntica, és possible crear protocols per compartir claus aleatòries que siguin segurs independentment de la tecnologia present (o futura) que es pugui emprar. Amb aquesta activitat, introduïm els conceptes de superposició i mesura quàntiques que utilitzarem a l'activitat següent per a construir un protocol de criptografia quàntica.

OBJECTIUS

- Entendre com funciona la polarització i els filtres polaritzadors del punt de vista clàssic.
- Familiaritzar-se amb els conceptes de superposició i mesura en un context de física quàntica.

MATERIALS

1 polaritzador lineal per a cada alumne (si no en tens, pots trobar-los al Kit Fotònic de l'ICFO – https://s.ic.fo/kitfotonic; alternativament, pots fer servir ulleres de sol que tinguin lents polaritzades)

ACTIVITAT

PAS 1: UN POLARITZADOR

Els alumnes miren a través del polaritzador: què observen?
La llum és una ona electromagnètica i la seva polarització és el pla en què oscil·la l'ona[7].
La polarització de la llum es descriu com un vector. El polaritzador actua com un filtre i projecta la polarització de la llum incident sobre l'eix del polaritzador, com es veu a la Figura 1.

PAS 2: DOS POLARITZADORS

Els alumnes treballen en parelles i posen un polaritzador davant l'altre. Què observen? Què canvia si canvien l'angle entre els polaritzadors?

A les Figures 2 i 3 pots observar què passa quan la polarització està alineada o perpendicular al polaritzador.

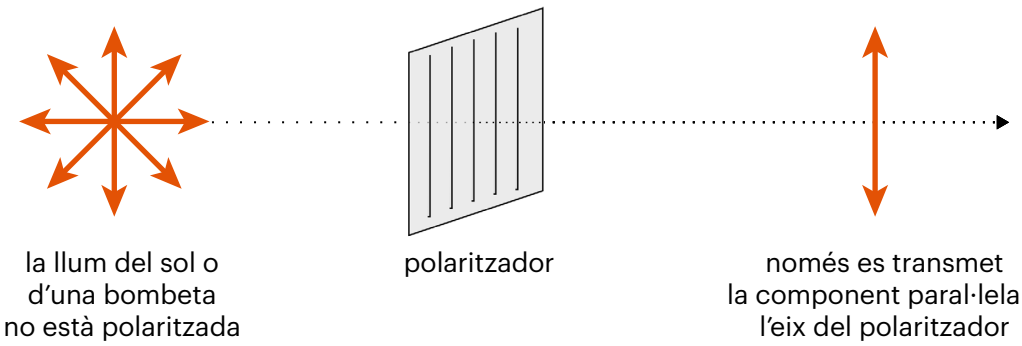


Figura 1

[7] Podeu explicar la polarització movent les mans amb moviment ondulatori primer en un pla vertical i després en un pla horitzontal.

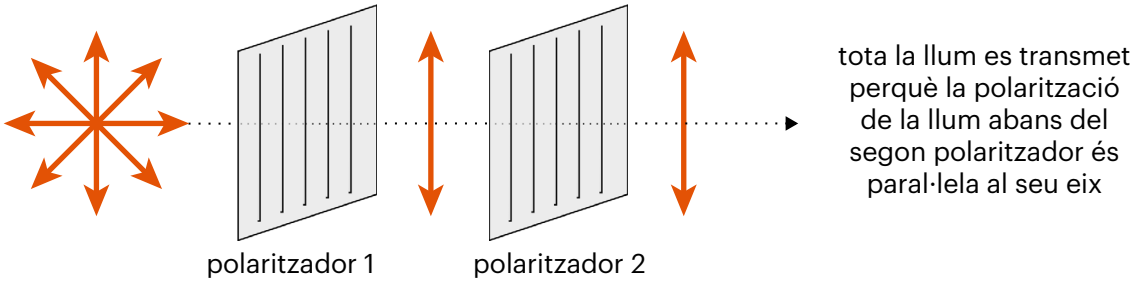


Figura 2

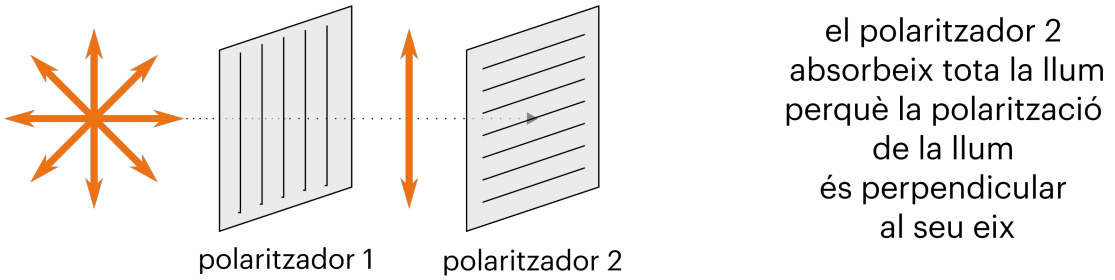


Figura 3

PAS 3: TRES POLARITZADORS

Utilitzant els dos polaritzadors creuats com a la Figura 3, els alumnes afegeixen un tercer polaritzador al mig formant un angle de 45º amb l'horitzontal. Què passa?

La llum passa a través del sistema de polaritzadors, tot i que els polaritzadors 1 i 3 estan creuats! Podem entendre això gràcies a les propietats dels vectors: després de cada polaritzador es transmet la component paral·lela a l'eix del polaritzador i la perpendicular es queda absorbida.

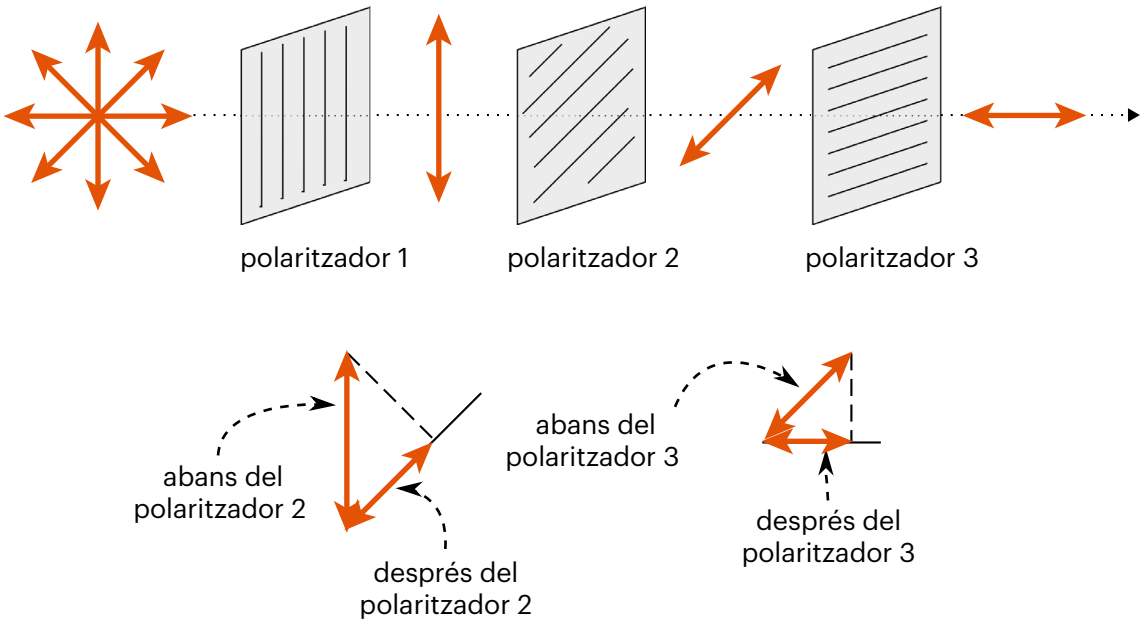


Figura 4

PAS 4: EXPERIMENT MENTAL

Imaginem que reduïm la intensitat de la font de llum que estem fent servir. Si la reduïm fins a tenir tan poca llum que només passa un fotó[8] a la vegada a través de cada polaritzador, el resultat de l'experiment seria igual?

Podríem dir que cada fotó té la seva pròpia polarització: per exemple, en la llum no polaritzada hi ha molts fotons i cadascú té una polarització diferent, així que de mitjana la polarització és nul·la. Com més fotons en una direcció de polarització, més llarg serà el vector corresponent a aquesta direcció.

Sabem que els fotons no interactuen entre ells, i per tant hauríem d'obtenir el mateix resultat enviant molts fotons a la vegada (com en el nostre experiment) que enviant-ne un de sol.

Què passa doncs quan un fotó individual amb una polarització establerta passa per un polaritzador? Podem seguir raonant amb els vectors com als passos precedents? Pot passar només una part d'un fotó?

CONCEPTES IMPORTANTS

EXPERIMENTS MENTALS

És molt complicat observar propietats quàntiques en absència de les condicions estrictes que es poden trobar en un laboratori.

Els experiments que proposem aquí - en realitat - es poden explicar fàcilment amb l'òptica clàssica (polarització com a vectors) que a vegades s'arriba a estudiar a l'escola secundària. De tota manera, és interessant proposar-los en aquest context perquè poden portar a conclusions sorprenents quan es fa l'experiment mental de reflexionar sobre com es poden reproduir aquests efectes si pensem que la llum està composta per partícules quàntiques individuals, els fotons.

Però això no ens ha de semblar una cosa llunyana de la feina que fan els físics! L'experiment mental és una eina que els científics han utilitzat al llarg dels segles per resoldre problemes difícils de posar a prova experimentalment amb la tecnologia de l'època: exemples cèlebres són el vaixell de Galileu, el dimoni de Maxwell, la paradoxa dels bessons o el gat de Schrödinger.

SUPERPOSICIÓ QUÀNTICA

Per explicar l'experiment dels tres polaritzadors des del punt de vista quàntic, hem de recordar que la polarització es comporta com un vector. Per exemple, com es pot veure a la següent figura, un fotó vertical és la superposició d'un fotó amb polarització a +45º i d'un a -45º. De la mateixa manera, el fotó a 45º és la superposició d'un fotó vertical i d'un horitzontal.

[8] Podem definir un fotó com la component més petita en que podem dividir la llum.

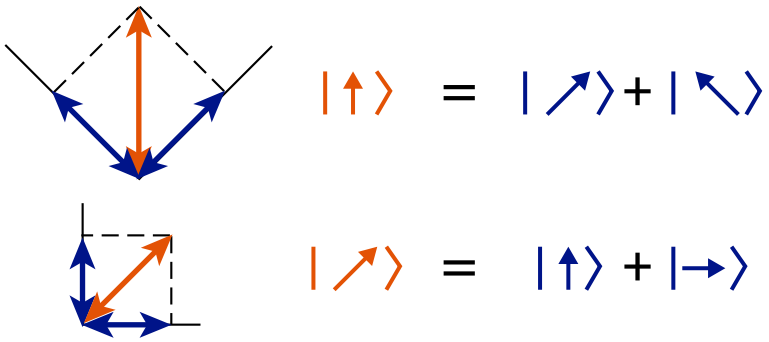


Figura 5

En general, **els possibles estats dels objectes quàntics es poden representar com a vectors**, inclosos els que en el món clàssic se solen representar com a quantitats escalars. La suma dels vectors dels estats quàntics es diu **superposició quàntica**: d'aquí sorgeixen propietats que desafien la nostra intuïció que fan que sembli que un objecte pugui estar en dos estats a l'hora. Per exemple, al vídeo sobre Superposició del Quantum Tour (http://www.quantumtour.icfo.eu/Quantum-World), el camí que segueix el fotó es pot representar com un vector i això fa que hi hagi una superposició quàntica entre els possibles camins. En el cas dels polaritzadors, es crea una **superposició entre dos possibles estats de polarització** del fotó.

MESURA SOBRE OBJECTES QUÀNTICS

En el cas quàntic, el polaritzador té l'efecte de treure el fotó de la superposició i fer-ho "col·lapsar" en un dels dos estats, en particular, el que tingui polarització paral·lela a l'eix del polaritzador.

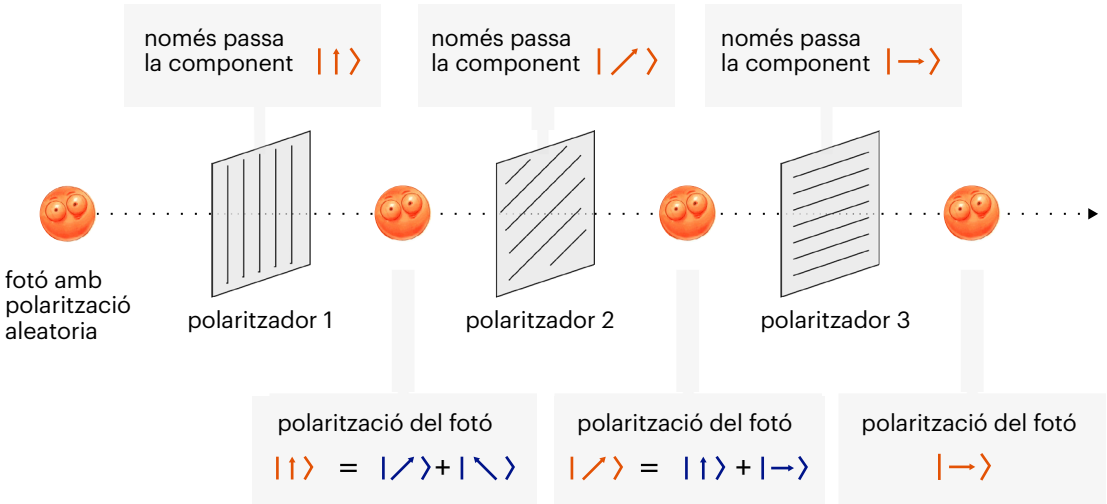


Figura 6

Mesurar un objecte quàntic pot canviar l'estat de l'objecte: hem vist a la Figura 6 que es pot transformar un fotó vertical amb dues mesures. A més, l'**ordre en què fem les mesures canvia el resultat**: si canviéssim l'ordre dels últims dos polaritzadors, tots els fotons quedarien absorbits pel polaritzador horitzontal com a la Figura 2. Això és conseqüència del **principi d'incertesa de Heisenberg**, que ens diu que hi ha mesures incompatibles, de les quals no podem conèixer els resultats alhora. Pots trobar unes explicacions més detallades al vídeo sobre Mesura del Quantum Tour (http://www.quantumtour.icfo.eu/Quantum-World) o a aquesta pàgina: https://www.informationphilosopher.com/solutions/experiments/dirac_3-polarizers/

7 Criptografia Quàntica

Richard Feynman deia que la superposició quàntica és l'únic misteri de la física quàntica. La veritat és que només entenent què és la superposició i com és afectada per les mesures podem entendre el primer protocol de física quàntica, el BB84, que deu el seu nom a les inicials dels científics que el van dissenyar (Charles Bennet i Gilles Brassard) i a l'any en que el van publicar (1984).

OBJECTIUS

- Entendre que les propietats quàntiques permeten compartir claus aleatòries de manera segura
- Entendre que la criptografia quàntica proporciona més seguretat que els protocols criptogràfics actuals

PREPARACIÓ

Imprimir la fitxa per alumnes que es troba a la pàgina 23.

ACTIVITAT

L'Alice vol compartir informació de manera segura amb en Bob, sense que l'Eve pugui saber què s'estan comunicant. Gràcies a les activitats precedents, sabem que seria ideal que puguin compartir una clau aleatòria i que la facin servir (una sola vegada!) per xifrar el missatge. L'Alice i en Bob ho aconseguiran seguint els passos descrits pel protocol BB84. Nota que totes les comunicacions entre l'Alice i el Bob podran ser públiques (podrien fins i tot posar-les a posts a les xarxes socials!): les propietats de la física quàntica asseguraran que la clau estigui protegida!

PAS 1: ESTABLIR EL CODI

L'Alice i el Bob es posen d'acord per associar "0" i "1" a quatre estats de polarització dels fotons com a la Taula 1.

Taula 1

Base +		Base x	
↑	0	↖	0
→	1	↗	1

PAS 2: L'ALICE PREPARA ELS SEUS FOTONS

L'Alice envia un fotó a la vegada cap al Bob. Cada vegada tria de manera aleatòria quin dels quatre estats de polarització establerts (↑, →, ↖ , ↗) enviar.

PAS 3: EL BOB DETECTA ELS FOTONS

El Bob no sap en quin estat de polarització estarà el fotó que li enviarà l'Alice. Per a cada fotó decideix mesurar en una de les bases possibles, la base + o la base x.

Segon les regles de la superposició i de la mesura sobre objectes quàntics que hem observat a l'activitat precedent, si la base triada pel Bob coincideix amb la de l'estat del fotó, el Bob obtindrà un resultat que coincideix amb el bit (0 o 1) que correspon a l'estat enviat per l'Alice. Per exemple, si l'Alice envia un 0 mitjançant un fotó ↑, el Bob veurà un 0 amb 100% de probabilitat si el mesura amb la base + com a la Figura 7.

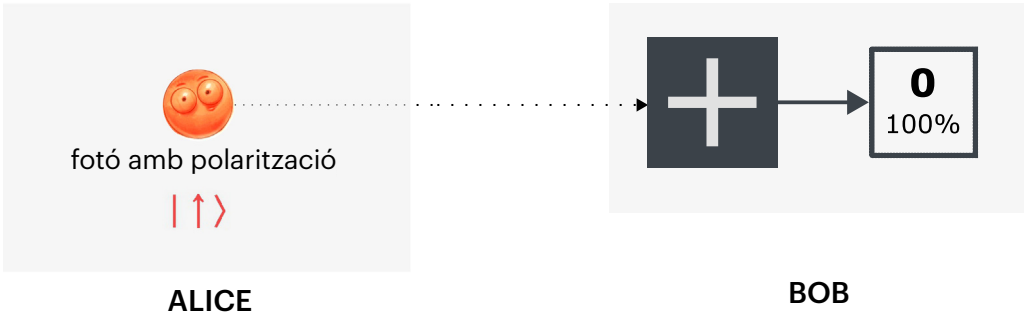


Figura 7

D'altra banda, si la base triada pel Bob no coincideix amb la de l'estat del fotó, el Bob obtindrà un resultat completament aleatori. Per exemple, si l'Alice envia un 0 mitjançant un fotó ↑, el Bob veurà 0 amb 50% de probabilitat i 1 amb 50% de probabilitat si el mesura amb la base x com a la Figura 8.

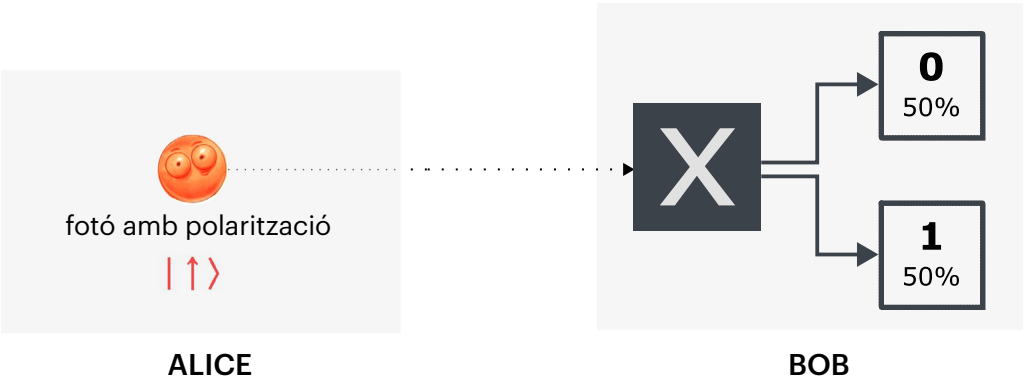


Figura 8

PAS 4: L'ALICE I BOB S'ENVIEN MOLTS FOTONS

L'Alice i el Bob repeteixen els passos 2 i 3 moltes vegades, aproximadament el doble del nombre de bits que té el missatge que voldran xifrar.

A la Taula 2 es troben els estats del fotons enviats per l'Alice i les bases escollides pel Bob pels primers 10 fotons: els alumnes omplen les columnes buides i comparen els resultats entre ells[9]. Quan el resultat de la mesura de Bob és aleatori, poden tirar una moneda i posar 0, si surt cara, i 1, si surt creu.

[9] Solucions: Alice – bit: 0100010111; Alice – base: +x++x+xx++; Bob – bit: 01????0?11 (els punts interrogatius ? corresponen als valors aleatoris; seran 0 o 1 segon el que surti de la moneda a cada alumne)

#fotó	Alice: estat del fotó	Alice: bit (0 o 1)	Alice: base del fotó (+ o x)	Bob: base de la mesura	Bob: bit (0 o 1)
1	↑			+	
2	↗			x	
3	↑			x	
4	↑			x	
5	↖			+	
6	→			x	
7	↖			x	
8	↗			+	
9	→			+	
10	→			+	

Taula 2

PAS 5: COMPARAR LES BASES

L'Alice i el Bob es comuniquen públicament quines bases corresponen a cada fotó i descarten els casos en que les dues bases no coincideixen, perquè corresponen a un resultat aleatori pel Bob. Les xifres que li queden constitueixen la **clau**: gràcies a les propietats estranyes de la física quàntica, Alice i Bob poden per fi comunicar-se de manera segura!
Quina és la clau compartida en aquest cas? [10]

PAS 6: L'EVE INTERCEPTA ELS FOTONS

A més de permetre la distribució segura de claus criptogràfiques, aquest protocol ens permet **detectar la presència d'espies** que intenten interceptar la clau.

Abans d'enviar-se un missatge xifrat amb la clau que acaben d'obtenir, envien un altre grup de fotons per controlar que ningú els estigui espiant.

L'aleatorietat del resultat de la mesura en el cas en que les bases no coincideixen juga a favor nostre i ens permet revelar la presència d'un intrús. Com en el cas dels tres polaritzadors de l'activitat 6, afegir un element al mig pot canviar significativament el resultat final.

L'Eve vol espiar la comunicació entre l'Alice i el Bob: per fer-ho, té una màquina idèntica a la del Bob que li permet mesurar els fotons en dues bases possibles (+ i x). Com el Bob, l'Eve desconeix en quina base l'Alice enviarà els fotons i tria les bases de manera aleatòria per cada fotó.

[10] Solució: 01011

Si la base triada per l'Eve coincideix amb la de l'estat del fotó (com en la Figura 9), l'Eve obtindrà un resultat que coincideix amb el bit que correspon a l'estat enviat per l'Alice i haurà obtingut informació útil per inferir la clau. Per exemple, si l'Alice envia un 0 mitjançant un fotó ↑ , l'Eve veurà un 0 amb 100% de probabilitat si el mesura amb la base + i el Bob veurà el mateix resultat (0) que hauria vist sense la presència de l'Eve.

Figura 9

D'altra banda, si la base triada per l'Eve no coincideix amb la de l'estat del fotó (com en la Figura 10), l'Eve obtindrà un resultat completament aleatori. A més, **el fotó es quedarà en la base de la mesura de l'Eve**, així que el fotó que rebrà el Bob serà diferent del que va enviar l'Alice. Per exemple, si l'Alice envia un 0 mitjançant un fotó ↑, l'Eve veurà 0 amb 50% de probabilitat i 1 amb 50% de probabilitat si el mesura amb la base X. Després de la intervenció de l'Eve, depenent del resultat de la mesura, el fotó que rebrà el Bob estarà en l'estat ↖ o ↗. Això fa possible que el Bob obtingui un valor diferent de 0 encara que hagi escollit la mateixa base que l'Alice.

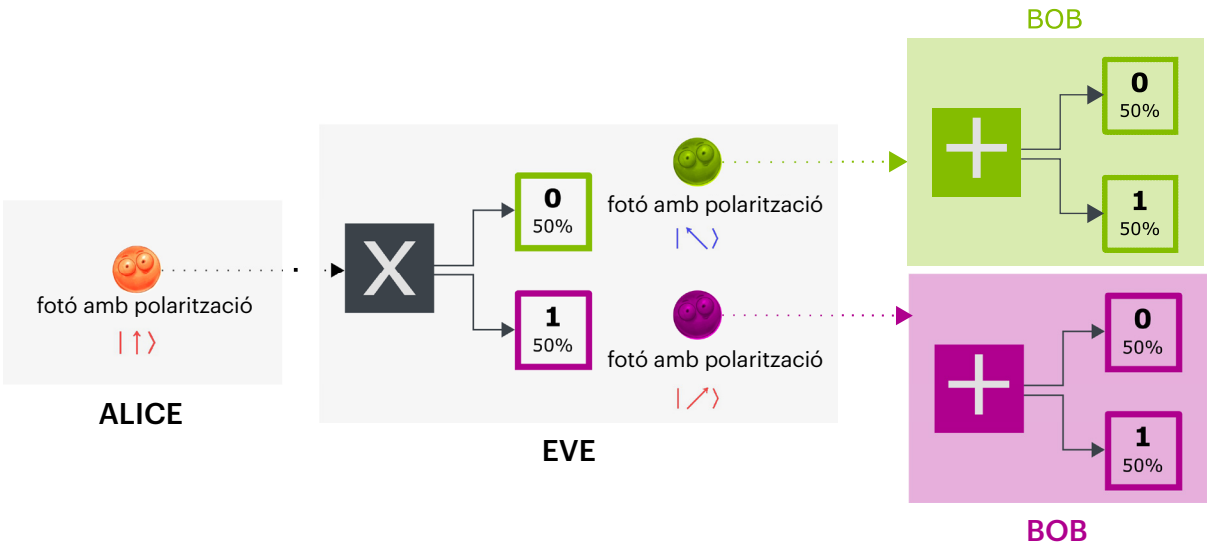


Figura 10

En els casos proposats a la Taula 3, l'Alice i el Bob haurien d'obtenir sempre els mateixos resultats perquè trien les mateixes bases. Els alumnes omplen la Taula 3, observant quin efecte té la presència de l'Eve sobre els resultats observats pel Bob[11]. Com al pas 4, quan el resultat de la mesura de l'Eve o del Bob hauria de ser aleatori, tiren una moneda i posen 0 si surt cara i 1 si surt creu.

[11] Solucions: Alice – bit: 0100010111; Alice – base del fotó: +x++x+xx++; Eve – bit: 0?0??101?1 (els punts interrogatius ? corresponen als valors aleatoris: seran 0 o 1 segon el que surti de la moneda a cada alumne); Bob – bit: 0¿0¿¿101¿1 (els punts interrogatius ¿ corresponen als valors aleatoris: seran 0 o 1 segon el que surti de la moneda a cada alumne)

#fotó	Alice: estat del fotó	Alice: bit (0 o 1)	Alice: base del fotó (+ o x)	Eve: base de la mesura	Eve: bit (0 o 1)	Bob: base de la mesura	Bob: bit (0 o 1)
1	↑			+		+	
2	↗			+		x	
3	↑			+		+	
4	↑			x		+	
5	↖			+		x	
6	→			+		+	
7	↖			x		x	
8	↗			x		x	
9	→			x		+	
10	→			+		+	

Taula 3

PAS 7: DETECTAR ESPIES

El Bob i l'Alice segueixen el protocol descrit al pas 5 per obtenir la clau:

- L'Alice i en Bob obtenen la mateixa clau? Per què?
- La base escollida per l'Eve afecta el resultat de la mesura d'en Bob?

Per detectar la presència d'un espia, l'Alice i el Bob poden comunicar-se les bases i els bits corresponents a un grup de fotons: si veuen que en algun cas els bits no corresponen, tot i que les bases que havien seleccionat eren iguals, vol dir que hi havia una espia interceptant les seves comunicacions. Hauran doncs d'esperar-se o canviar mètode de comunicació per evitar que el seu missatge pugui ser interceptat.

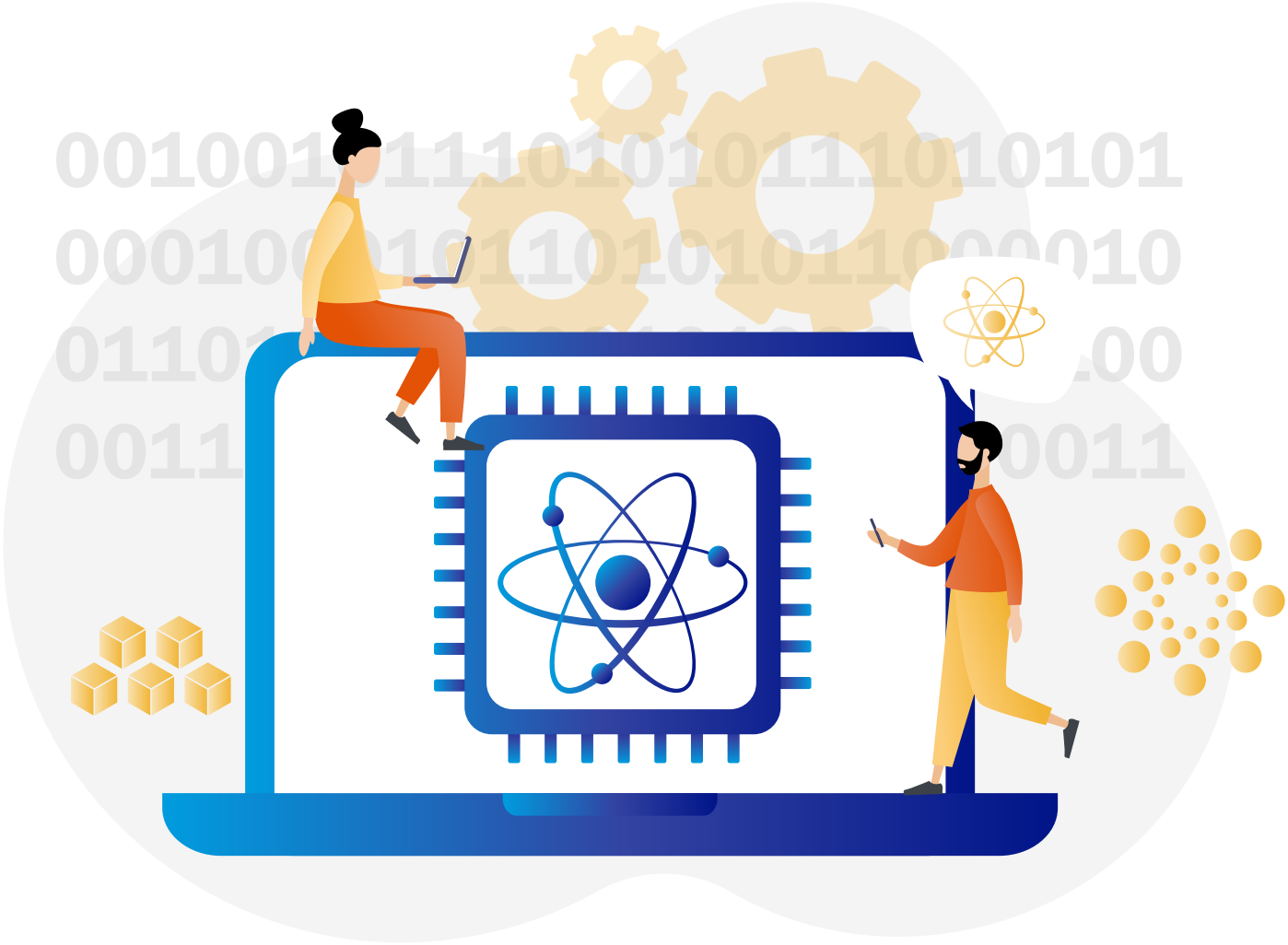
És difícil dur a terme aquesta activitat a l'escola amb llum i elements òptics perquè requereix materials prou cars com làmines d'ona, però podeu aprofitar el simulador que trobeu aquí (https://lab.quantumflytrap.com/lab/bb84) o contactar amb nosaltres (organitzem regularment sessions per realitzar aquest experiment amb grups petits d'estudiants - https://outreach.icfo.eu/tdr/).

CONCEPTES IMPORTANTS

- En aquesta activitat hem treballat amb la polarització dels fotons, com a l'activitat precedent, però els mateixos raonaments es poden aplicar a qualsevol sistema quàntic que tingui dos possibles estats en dues bases diferents.
- Gràcies a la superposició i als efectes de la mesura en el món quàntic, l'Alice i el Bob poden **compartir de manera segura una clau criptogràfica sense haver de comunicar-se-la** (i tenir el perill que algú la intercepti).
- En el protocol BB84 i en els altres protocols de criptografia quàntica, la **seguretat de la transmissió és garantida per les propietats de la física quàntica**: això és molt diferent dels protocols actuals, on la seguretat està basada en els límits tecnològics actuals i pot ser posada en discussió per avenços futurs.
- Amb la criptografia quàntica tenim la possibilitat de **poder detectar si la nostra comunicació és interceptada** per algú abans d'enviar-nos el missatge.

8 Fitxes pels alumnes

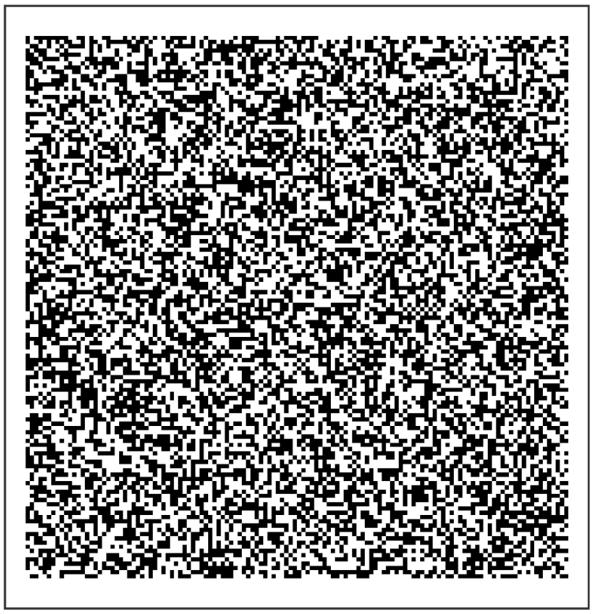
A les pàgines següents es troben fitxes que pots imprimir per poder posar fàcilment a la pràctica les activitats proposades a classe.



El secret d'una bona clau és no reutilitzar-la

IMATGE 1

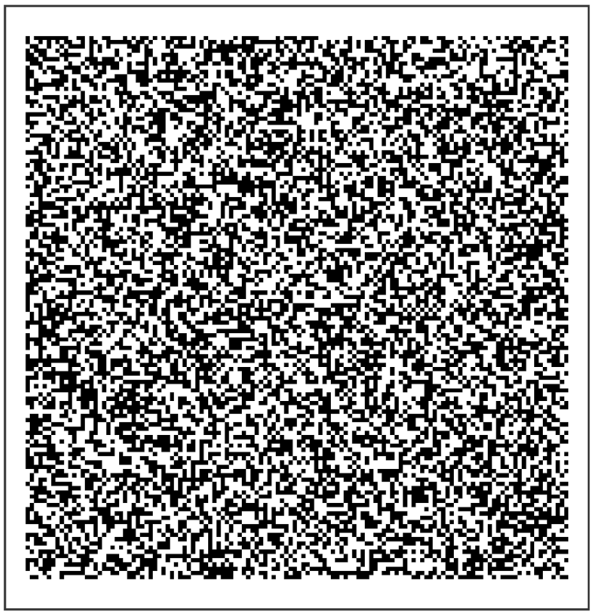
ICFO Maciej Lewenstein Quantum School for Teachers



outreach.icfo.eu
outreach@icfo.eu

imatge 1

ICFO Maciej Lewenstein Quantum School for Teachers



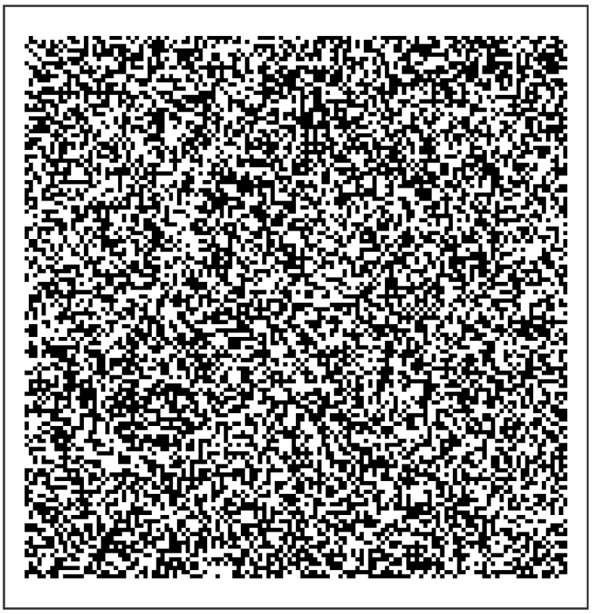
outreach.icfo.eu
outreach@icfo.eu

imatge 1

El secret d'una bona clau és no reutilitzar-la

IMATGE 2

ICFO Maciej Lewenstein Quantum School for Teachers



outreach.icfo.eu
outreach@icfo.eu

imatge 2

ICFO Maciej Lewenstein Quantum School for Teachers

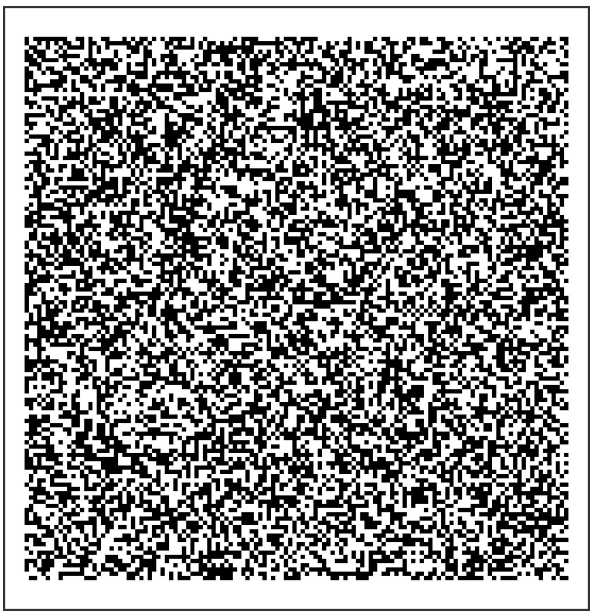
outreach.icfo.eu
outreach@icfo.eu

imatge 2

El secret d'una bona clau és no reutilitzar-la

CLAU

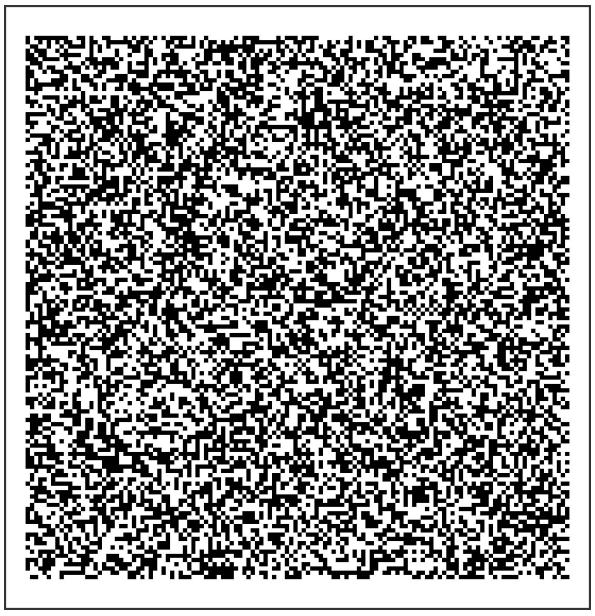
ICFO Maciej Lewenstein Quantum School for Teachers



outreach.icfo.eu
outreach@icfo.eu

clau

ICFO Maciej Lewenstein Quantum School for Teachers



outreach.icfo.eu
outreach@icfo.eu

clau

ICFO

ICFO Maciej Lewenstein Quantum School for Teachers

El secret d'una bona clau és no reutilitzar-la

Pas 1

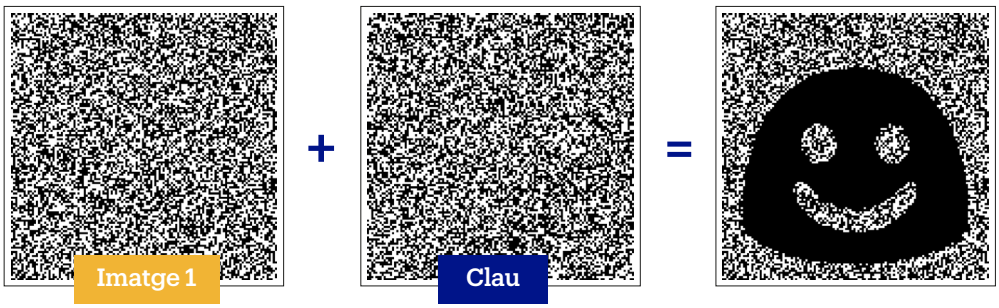
Imatge 1

Imatge 2

Aquestes imatges són xifrades: les hem generat sumant mòdul 2 (*) el valor de cada píxel de les imatges originals al valor de cada píxel de la clau.

(*) Suma de mòdul 2: 0+0=1+1=0; 0+1=1+0=1

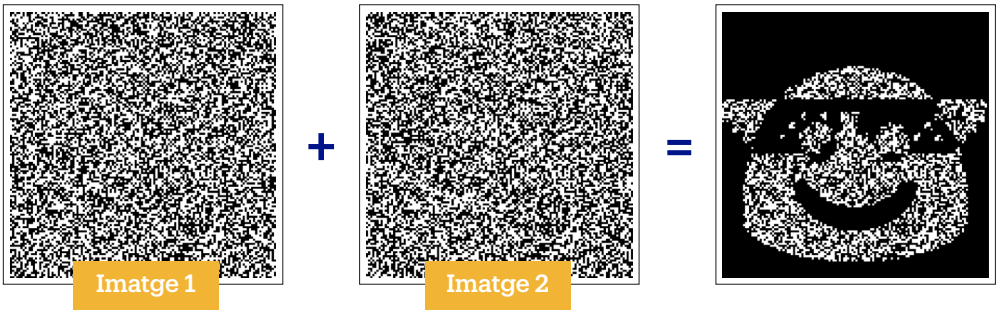
Pas 2



La clau és una imatge feta de píxels amb valors aleatoris. Posa la clau a sobre de les imatges fent coincidir els requadres exteriors per a descobrir les imatges originals.

Pas 3

Creus que aquesta és una manera segura per amagar el contingut de les imatges? Penses que qui no tingui la clau trigarà molt a desxifrar les imatges? Prova de superposar les dues imatges, sense fer servir la clau:



Si envies dos missatges fent servir la mateixa clau, es pot esbrinar part del missatge de manera molt fàcil. Per aquesta raó, **és important fer servir les clau criptogràfiques una sola vegada!**

Criptografia quàntica

CODI

Base +		Base x	
↑	0	↖	0
→	1	↗	1

ALICE I BOB

#fotó	Alice: estat del fotó	Alice: bit (0 o 1)	Alice: base del fotó (+ o x)	Bob: base de la mesura	Bob: bit (0 o 1)
1	↑			+	
2	↗			x	
3	↑			x	
4	↑			x	
5	↖			+	
6	→			x	
7	↖			x	
8	↗			+	
9	→			+	
10	→			+	

ALICE, BOB I EVE

#fotó	Alice: estat del fotó	Alice: bit (0 o 1)	Alice: base del fotó (+ o x)	Eve: base de la mesura	Eve: bit (0 o 1)	Bob: base de la mesura	Bob: bit (0 o 1)
1	↑			+		+	
2	↗			+		x	
3	↑			+		+	
4	↑			x		+	
5	↖			+		x	
6	→			+		+	
7	↖			x		x	
8	↗			x		x	
9	→			x		+	
10	→			+		+	