

the BIG BELL TEST



Fitxes Didàctiques

www.thebigbelltest.org

@TheBellsters

ICFO^R

The Institute
of Photonic
Sciences

A member of **BIST** Barcelona Institute of
Science and Technology



Generalitat
de Catalunya



UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

Fundació Privada
CELLEX

Fundació Privada
MIR-PUIG

Fundació
Catalunya
La Pedrera



EXCELENCIA
SEVERO
OCHOA
2016 - 2019



AXA
Research Fund
Through Research. Protector

ICREA

Índex

- Fitxa 1 L'atzar, la probabilitat i com fer servir el joc del **BIG Bell Test** a l'aula
- Fitxa 2 Física quàntica: Primers conceptes
- Fitxa 3 El problema de compartir claus segures
- Fitxa 4 Quàntica - La comunicació més segura
- Fitxa 5 Polarització i Superposició

Material Addicional

Material Imprès

Dossier pel públic general: <https://cloud.icfo.es/owncloud/index.php/s/sEYFFVgVUfAJ2MF>

Material Audiovisual

Video-instruccions del videojoc del **BIG Bell Test**: <https://vimeo.com/user57186692>

Video Promocional (Anglès): <https://vimeo.com/184480786>

Video Promocional (Català): <https://vimeo.com/185292887>

Video Promocional (Castellà): <https://vimeo.com/185292940>

El joc del BBT a l'aula

FITXA 1: L'ATZAR I COM FER SERVIR EL JOC DEL BBT A L'AULA

Atzar i probabilitat

Conceptes elementals d'estadística: població, mitjana, distribució estadística, mesures de dispersió.

Funcions elementals d'Excel: filtres y gràfiques.

Azar y probabilidad

L'atzar és un component fonamental de la física quàntica. **En aquesta unitat us recomanem** l'excel·lent material creat per Joan Jarreño sobre l'atzar i la probabilitat en una entrada del seu bloc precisament dedicada al **BIG Bell Test**, que podeu trobar aquí: <http://calaix2.blogspot.com.es/2016/10/latzar-te-patrons.html>

Estadística amb el videojoc del BIG Bell Test

El videojoc del **BIG Bell Test** és el portal per contribuir als experiments del 30 de novembre.

Es pot jugar en qualsevol moment, però estarem contribuint a l'experiment en temps real si juguem en qualsevol de les 48 hores en què és el 30 de novembre en algun punt del planeta.

És a dir, el dia 30 de novembre, els alumnes poden contribuir tantes vegades com vulguin, des de mòbils, tauletes o ordinadors. No cal registrar-se, però és recomanable, pels motius que veuràs a continuació.

Es pot contribuir en qualsevol de les dues versions de la plataforma: El Quick Bell Test o el BIG Bell Quest, totes dues a www.thebigbelltest.org/contribute.

El BIG Bell Quest, la versió gamificada, és la que hem desenvolupat per motivar la participació, no només perquè inclogui una estètica i una història, sinó perquè incentiva la competició, entre individus o grups, i a més a més ens permet crear una activitat d'aula, que expliquem a continuació.

1. Vés a www.thebigbelltest.org/quest
2. Registra't (pots entrar com a convidat, però llavors perdràs les dades de cada missió, i no podràs tenir un nom d'usuari identificable). No cal introduir l'e-mail, és només recomanable, per poder tornar a entrar al web si alguna vegada perds la contrasenya.
3. **Crea un Esdeveniment.** En el teu perfil d'usuari, localitza la casella "Esdeveniment" i tria un nom significatiu. Per exemple el teu nom, o el de la teva classe seguit del nom del teu centre.
4. Digues als teus alumnes que es registrin en el joc, però dóna'ls el nom de l'Esdeveniment un cop estiguin **tots a l'aula**.

Fitxes didàctiques per a la presentació a l'aula del BIG Bell Test

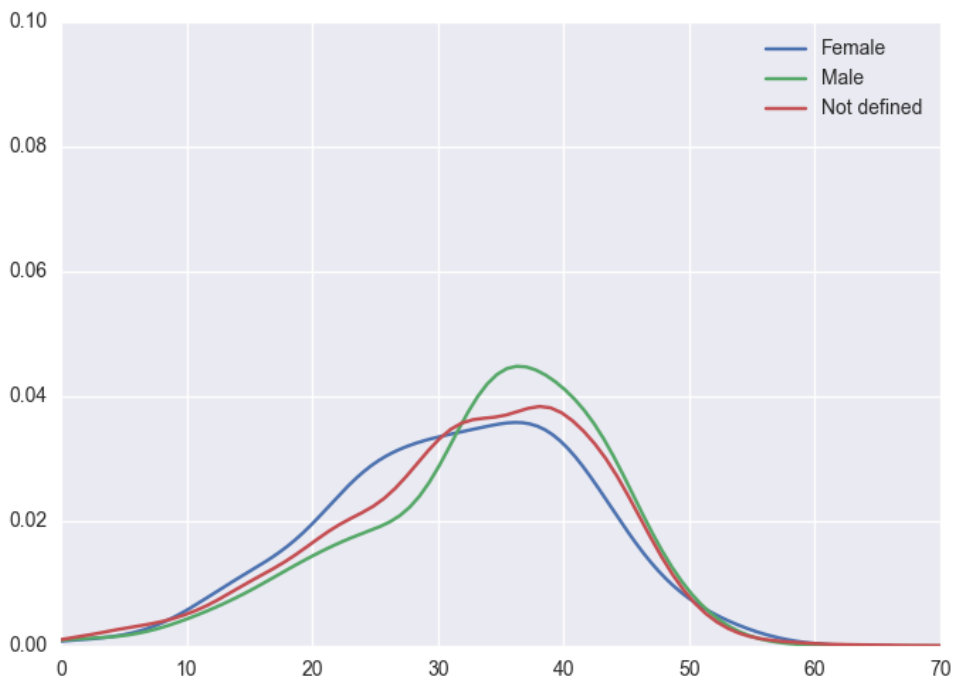
5. Una vegada tots registrats, i tots havent triat el mateix nom per al Esdeveniment (compte amb les majúscules!), comença el joc. Els alumnes han de jugar una missió o diverses (segons tu consideris). Potser pots donar-tres minuts, o cinc, per jugar. Quan hagi passat el temps, han de deixar el mòbil a les taules. **No oblidis participar-hi!**

6. Vés a www.thebigbelltest.org/radarevent La pàgina et demanarà un nom d'Esdeveniment, introdueix el que has creat abans. Sortirà llavors la classificació, per aleatorietat i per punts, de la classe.

7. Et pots baixar aquesta **classificació en Excel**, i fer el gràfic de la distribució. Quina forma té? ¿És una gaussiana? Té diversos pics? És molt dispersa? Pots utilitzar-la per treballar els conceptes de mitjana i mesures de dispersió. Al cap i a la fi tens una població i un conjunt de valors (l'aleatorietat de cada un). A mesura que jugueu, podeu veure si la distribució canvia, si la mitjana s'acosta a algun punt, si la dispersió baixa, etc.

8. Els alumnes poden baixar les dades i treballar altres correlacions extra. Per exemple: Hi ha diferència entra les distribucions si comparem els nois amb les noies? Es mantenen aquestes diferències en altres classes? I si comparem les distribucions entre diferents grups d'amics? Els alumnes que toquen un instrument són més o menys aleatoris, comparats amb els altres? Si ho fem diversos dies seguits, podem veure millora en les dades? Els alumnes poden pensar altres correlacions.

A continuació, us presentem els resultats que hem obtingut nosaltres en estudiar l'efecte del gènere sobre l'aleatorietat. ¿Obteniu una cosa semblant?



La física quàntica

INTRO

En aquesta sèrie de pràctiques, els teus alumnes aprendran que:

1. en la física quàntica, les coses no sempre es comporten tal i com estem **acostumats**, i també quines són i d'on vénen les **propietats fonamentalment noves** i característiques de la quàntica que la fan tan especial.
2. la comunitat científica s'ha dedicat amb interès, i de vegades dividida, a la **interpretació** de les sorprenents prediccions de la física quàntica.
3. les paradoxes de la física quàntica poden ser aprofitades per **generar tecnologies** que superen les limitacions de les tecnologies clàssiques.
4. el fet que la física quàntica sigui tan difícil de comprendre fa que la societat no estigui familiaritzada amb ella i aleshores pugui absorbir missatges erronis per part de sectors **pseudocientífics**.
5. la generació a la qual pertanyen els teus alumnes entendrà la física quàntica millor que qualsevol altra passada, inclosos els seus inventors. Ells viuran en una societat que haurà d'anar assumint cada vegada més el **paradigma quàntic**, de la mateixa manera que abans es va assumir el heliocèntric, per exemple
6. Què és el **BIG Bell Test**, què faran els científics, i per què és important que hi participem.

FITXA 2 - PRIMERS CONCEPTES

Activitat 1 (Deures per a casa + discussió a classe)

Una possible manera de començar és demanar als estudiants com a deures per a casa anar a buscar "quàntic" a internet, i trobar-hi una entrada, un punt concret que els cridi molt l'atenció.

L'endemà, han d'explicar a tota la classe breument què han seleccionat i per què. No han de tractar d'entendre què han llegit, sinó explicar per què els ha sorprès.

És possible que alguns parlin de les propietats estranyes de la quàntica, altres d'aplicacions com ara l'ordinador quàntic, o la criptografia quàntica, i altres de coses encara més estranyes com la meditació quàntica, la sanació quàntica, i pseudociències similars.

Aquesta primera pràctica ens servirà per:

- Introduir la física quàntica com una teoria científica composta per les lleis que obeeixen els objectes més petits, com àtoms, electrons, fotons, etc., amb un extraordinari poder explicatiu i predictiu però alhora extraordinàriament anti-intuïtiva i impossible de conciliar amb la nostra manera d'entendre el món.

- Mencionar que tot i ser incomprensibles, les propietats de les partícules quàntiques serveixen per generar tecnologies noves amb capacitats impossibles d'assolir per a les tecnologies clàssiques (ordinadors rapidíssims, transaccions d'informació segures 100% ...)

- Alertar que com que la física quàntica és molt difícil d'integrar en la nostra manera habitual d'entendre el món i sembla desafiar el nostre sentit comú, hi ha molts que ho aprofiten per inventar-se tot tipus de "connexions estranyes" com ara la consciència quàntica, el desdoblament quàntic, la curació quàntica, de les que hem de fugir. És important que la societat es comenci a acostar a la quàntica, a què significa i què implica, per evitar caure en aquest tipus d'enganyos i confusions. A més, és possible que la societat tingui molt a dir sobre les veritables noves tecnologies quàntiques.

Exemples de llocs que parlen dels "misteris quàntics":

<http://www.quantumworldvision.com/scio/>

Segui el que sigui el que signifiqui "Scientific Consciousness", cap grup de recerca científic ha pogut demostrar que la consciència tingui a veure alguna cosa amb la física quàntica.

Fitxes didàctiques per a la presentació a l'aula del BIG Bell Test

<http://www.quantumenergywellness.com/>

El terme "quantum energy" no té cap sentit, i no el fa servir cap científic.

<http://medicinacuantica.cl/>

Aquí fins i tot utilitzen els vídeos molt bons de Dr. Quantum per explicar les seves connexions entre medicina i quàntica.

Aleshores pots fer un resum de les tecnologies quàntiques que estan ara en desenvolupament o en pràctica (en la bibliografia hem seleccionat algunes). En la propera fitxa ens fixarem en una de molt atractiva, la criptografia quàntica, que ens servirà com a contexte per explicar les propietats quàntiques fonamentals.

FITXA 3 : EL PROBLEMA DE COMPATIR CLAUS SEGURES

(Activitats per explicar què és la criptografia)

Es treballa l'aritmètica modular.

Es pot relacionar amb el ús dels alfabetos.

Comencem per un petit joc. Ens enviarem missatges secrets.

([Aquí](#) tens més activitats de criptografia clàssica, per si et semblen interessants.)

Es juga per parelles. Si hi ha un nombre imparell d'alumnes, un grup pot ser de tres.

Cada alumne ha d'agafar una paraula de set lletres, i ha de xifrar-segons el [xifrat César](#), és a dir, substituint cada lletra de la paraula per la que es troba a K (el nombre K és la clau i l'han de decidir ells) posicions a la dreta d'ella a l'alfabet.

-Depenent de com vulguis fer-ho, la clau la comparteixen o no. O sigui, a l'hora de desxifrar el missatge, l'alumne desxifrador pot actuar com a receptor normal (sap què és K) o com espia (ha d'anar provant moltes K possibles).

-Depenent del nivell dels alumnes, poden utilitzar la roda de Cesar <https://inventwithpython.com/cipherwheel/> (molt fàcil), o fer ells la feina d'escriure l'alfabet i anar comptant posicions, o substituir cada lletra per un nombre i fer la suma mòdul 27 (comptem 27 lletres, sense ll ni ch).

Quan l'alumne hagi xifrat la seva paraula, la passa al seu company, qui al seu torn ha de donar-li la seva paraula xifrada. Ara ells hauran de descriptarse mútuament. Si un d'ells acaba de xifrar abans que l'altre, pot començar a xifrar una altra paraula. Així, a més, prevenim que xifren molt fàcil (K petit), o molt difícil (K gran), perquè no voldran estar molt temps xifrant i que el company els passi molts deures.

Guanya qui desxifri abans totes les paraules que té a sobre de la taula.

Gairebé millor si el professor preselecciona les paraules i els dona unes quantes a cada un. A més, per fer-ho més fàcil, poden deixar-se sense xifrar algunes lletres i dir quines són.

Ara veurem què passa si el receptor no sap la clau d'enciptació, o l'ha perdut o oblidat. Pot desxifrar el seu missatge? O el que és el mateix, pot un espia desxifrar un missatge si no té la clau?

Fitxes didàctiques per a la presentació a l'aula del BIG Bell Test

Es poden fer a la pissarra un parell d'exemples per a tots, per consolidar els procediments. L'estratègia de l'espia o del receptor despistat que ha perdut la clau, és anar provant $K = 1$, $K = 2$, $K = 3$, ...

Per incentivar la resposta, a la pissarra podem desxifrar una paraula fàcil, Alabama amb $K = 2$, sense dir-ho als alumnes (quedaria CNCDCOG). I llavors veure que quan treus una lletra (l'A), ja tens moltes pistes per desxifrar. Si a més sabem que és el nom d'una ciutat d'Amèrica, ja que un altre avantatge més. És a dir, si l'espia té context, la seva tasca és relativament fàcil.

Com podríem fer-ho més difícil per l'espia? Una manera de fer-lo més difícil (i de fet és impossible de desxifrar!) És donar a cada paraula un K diferent, en lloc del mateix desplaçament per a totes les lletres.

La manera de fer-ho més difícil per tant és donar a cada paraula un K diferent, en lloc del mateix desplaçament per a totes.

Els fas una prova perquè desxifrin una paraula amb un K diferent per a cada lletra. Els resultarà impossible i veuran ràpid per què. Aquest mètode es diu el [xifrat Vernam](#).

Ara vénen les consideracions:

- La clau d'encryptació no és un nombre, sinó una seqüència de nombres
- La clau és tan llarga com el missatge!
- Com a cada número correspon una lletra de l'alfabet, la clau d'encryptació pot ser també una seqüència de lletres
- Un alfabet té 27 lletres, és una mica complicat fer sumes mòdul 27. I si ens passem a un alfabet amb dues lletres? I si les "lletres" són 0 i 1?

Activitat:

- El professor escriu un "missatge" en zeros i uns (pot ser una cosa inventada, pot ser una paraula en codi ASCII, si vol explicar què és, però alguna cosa no molt llarg).
- Llavors demana als alumnes que inventin cadascun una clau de xifrat. Cada alumne ha d'inventar la que vulgui, aleatòriament.
- Els alumnes han de sumar mòdul 2 la clau que han inventat al missatge. Tenen un missatge encriptat.
- De nou, sumar mòdul 2 consisteix a saltar al 0 un cop passes del 1. Les operacions quedarien així: $0 + 0 = 0$; $0 + 1 = 1$; $1 + 0 = 1$; $1 + 1 = 0$
- Dos alumnes surten a la pissarra. Cada un escriu el seu missatge encriptat totalment diferent. El professor els demana que sumin al seu missatge encriptat la seva clau d'encryptació. Als dos (si o fan bé) els ha de sortir el missatge original.

- (Aprofundiment - deures opcionals):

- Què passa si provo totes les possibles combinacions per desxifrar un missatge? Com fèiem a la primera activitat, que anàvem provant $K = 1$, $K = 2$, fins a trobar el missatge

(Si fem això, obtindrem tots els possibles missatges d'aquesta longitud!)

- Què passa si ús dues vegades la mateixa clau en dos missatges diferents?

(Si fem això, els missatges poden ser la clau l'un de l'altre. Per això aquest mètode es diu el [one time pad](#))

Conclusions:

- La clau de xifrat és llavors una seqüència de zeros i uns tan llarga com el missatge.

- És important que sigui una seqüència aleatòria, és a dir, que no tingui cap sentit, perquè un espia no pugui imaginar-.

- L'emissor i el receptor del missatge han d'estar segurs de tenir la mateixa clau de xifrat, la mateixa seqüència, per xifrar i desxifrar. És a dir, han de compartir la clau.

- L'emissor i receptor del missatge han de compartir la clau sense que l'espia la robi !!!

- Si l'emissor i el receptor del missatge comparteixen una seqüència de veritat aleatòria (que l'espia no tingui manera d'inferir) i si de veritat l'espia no la pot aconseguir de cap manera (interceptándola sense que s'assabentin emissor i receptor), llavors aquest mètode és 100% segur.

Ara, un cop hem entès que si som capaços que l'emissor i el receptor d'un missatge xifrat comparteixin la clau de xifrat tenim comunicació segura, és l'hora d'entendre seguint la fitxa **4** a continuació, com la quàntica ho aconsegueix. Qualsevol altre mètode és fal·lible, l'espia sempre pot hackejar el teu sistema, si té un súper ordinador i és molt llest i té recursos per espia tots els possibles canals.

FITXA 4: QUÀNTICA: LA COMUNICACIÓ MES SEGURA

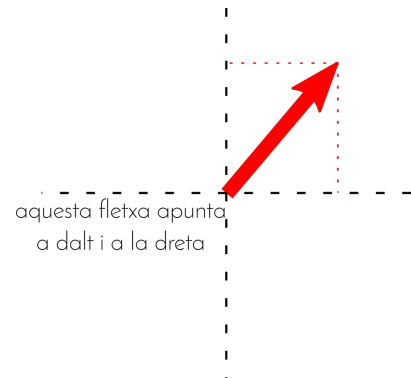
Principi d'Incertesa de Heisenberg

Estat colapsat

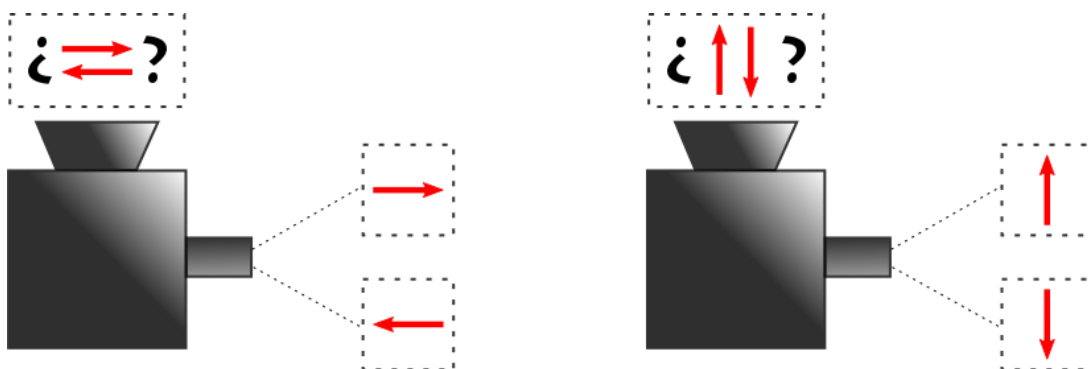
Atzar

Per entendre com amb les partícules quàntiques serem capaços de compartir aquesta clau de forma súper segura, cal entendre què té d'especial el món quàntic enfront del clàssic.

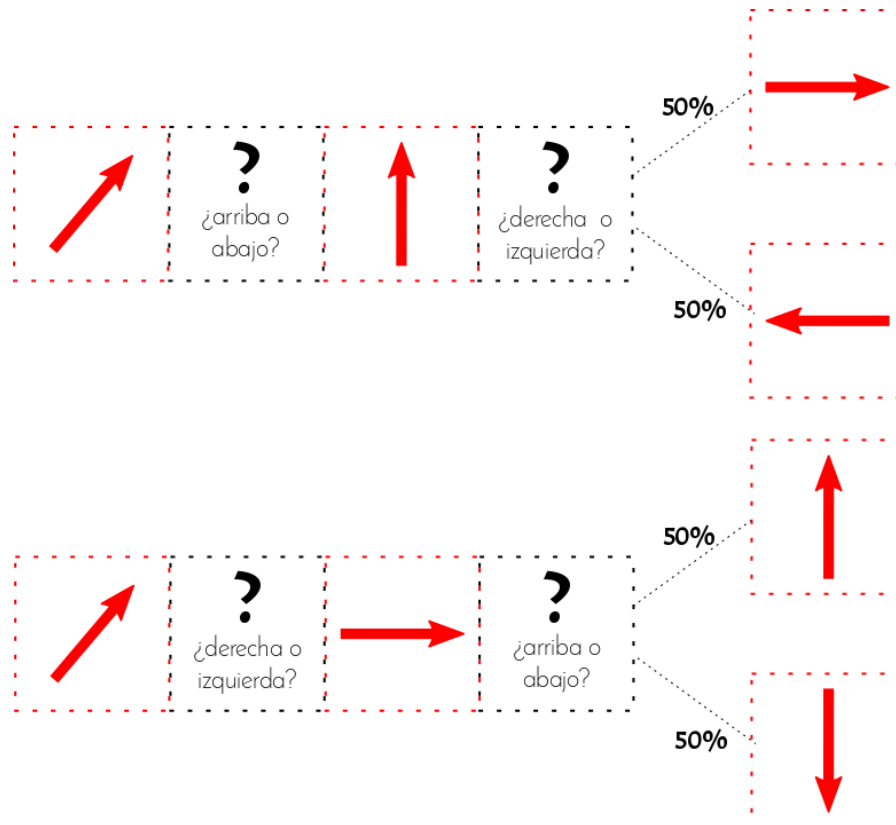
1) Per a un objecte quàntic (àtom, electró, fotó) no és possible tenir totes les seves propietats definides al mateix temps. Per exemple, dibuixa una fletxa. Si mires aquesta fletxa pots saber si apunta cap a la part de dalt de la pissarra o cap a la part de baix, i també pots saber si apunta cap a la dreta de la pissarra o cap a l'esquerra. (I pots dir un munt de coses més de la fletxa, anar apuntant-se en una llista cada vegada més gran, que la diferència de qualsevol altra fletxa.) Si un company vol saber com és la fletxa et pot fer preguntes: "¿apunta dalt o avall?" i després "¿apunta cap a la dreta o l'esquerra?" i tu li pots anar contestant consecutivament com si estiguéssiu jugant al *Qui és qui?* de les fletxes.



No obstant això, si ens imaginem la fletxa amb la qual jugueu és una partícula quàntica, trobem un problema en plantejar la segona pregunta. Podem saber si la fletxa apunta cap amunt o cap avall, però llavors ja no podem saber si apunta cap a l'esquerra o cap a la dreta. I viceversa, podem saber si apunta a la dreta o a l'esquerra, però llavors no sabrem res de si apunta amunt o avall. Això és conseqüència del **principi d'incertesa de Heisenberg**, que ens diu que hi ha preguntes incompatibles, les respostes no podem saber alhora. És com si la fletxa estigués dins d'una caixa negra impossible d'obrir amb un mecanisme que permet només una pregunta alhora.



11) I com evita la quàntica que sapiguem la resposta a les dues preguntes? Doncs perquè en el moment en què la partícula respon, el seu estat col·lapsa a la resposta que ha donat. Si la partícula ens respon "a dalt" o "baix", es queda apuntant cap amunt o cap avall, i ja no sabem res de si abans de preguntar apuntava cap a l'esquerra o cap a la dreta. Fixa't que una conseqüència d'això és que l'ordre de les preguntes pot canviar la resposta final, com en la següent figura, al contrari que en el *Qui és Qui?* d'abans. En el moment en que la fletxa respon a dalt, llavors s' "oblida" de si apuntava a la dreta o a l'esquerra, i es queda apuntant cap amunt. Llavors, què passa ara si algú arriba i li pregunta si apunta a la dreta o a l'esquerra? Doncs, i aquí arriba una altra sorpresa, si a una partícula que està en un estat definit dalt / baix (per exemple, a dalt) se li pregunta si apunta dreta / esquerra, llavors la partícula, forçada a respondre en aquests termes, el 50% de les vegades diu dreta i el 50% de les vegades diu esquerra. És a dir, **la quàntica és una font d'atzar genuí**.



(Nota) L'orientació de la fletxa, que és l'estat en què està la partícula quàntica, es pot descriure en termes dalt / baix o esquerra / dreta. No les dues coses alhora. El mateix estat es pot descriure en aquestes dues bases. Per ara ens quedem aquí. Encara no parlarem de superposició (d'això es parla la fitxa 5). Un estat pot ser a dalt, pot ser baix, però també qualsevol superposició d'ells. Això per ara no ho necessitem.

Aquestes propietats de la física quàntica (les preguntes incompatibles, l'atzar i el col·lapse quan es fa una mesura) poden semblar un desavantatge a l'hora de saber completament com és una partícula,

Fitxes didàctiques per a la presentació a l'aula del BIG Bell Test

però podem utilitzar-les al nostre favor per garantir 100% la seguretat de la criptografia. Us expliquem per què.

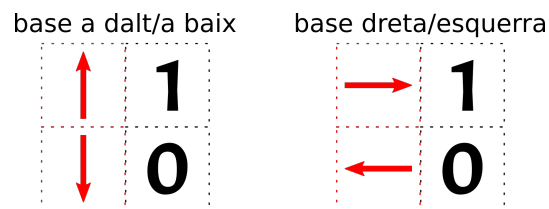
Ja hem vist en la fitxa **3**, que una de les millors maneres per enviar missatges segurs és que l'emissor (Alice) i el receptor (Bob) comparteixin una clau secreta de xifrat, una llista de zeros i uns aleatoris (clau en l'estil one-time pad).

Ara veurem com Alice i Bob poden obtenir aquesta llista de Os i 1s a partir de les propietats d'una partícula quàntica (que anem a entendre sempre com la fletxa quàntica que descrivim abans).

Alice prepara una fletxa a cada caixa i les envia a Bob, qui a la seva vegada fa una pregunta a cada caixa.

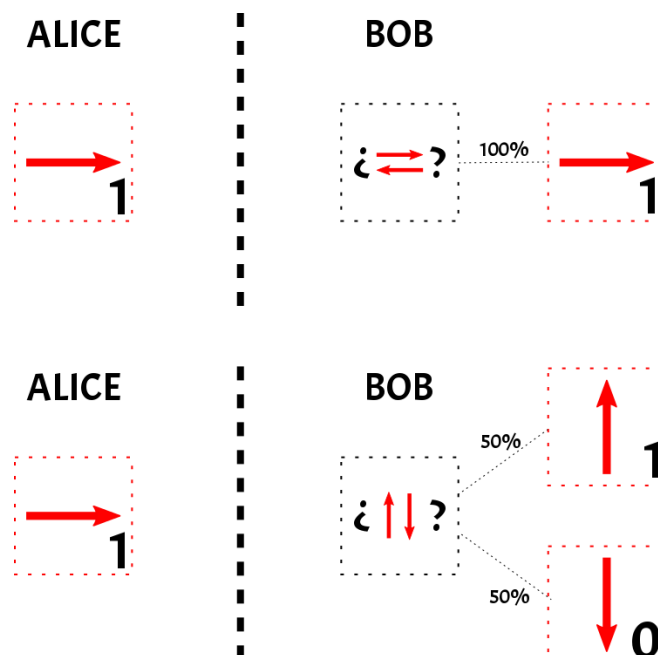
Pas 1: Lògica del codi

Alice i Bob es posen d'acord per associar 0 o 1 amb cadascuna de les dues respostes possibles a cadascuna de les dues preguntes bàsiques.



Pas 2: compartir una partícula

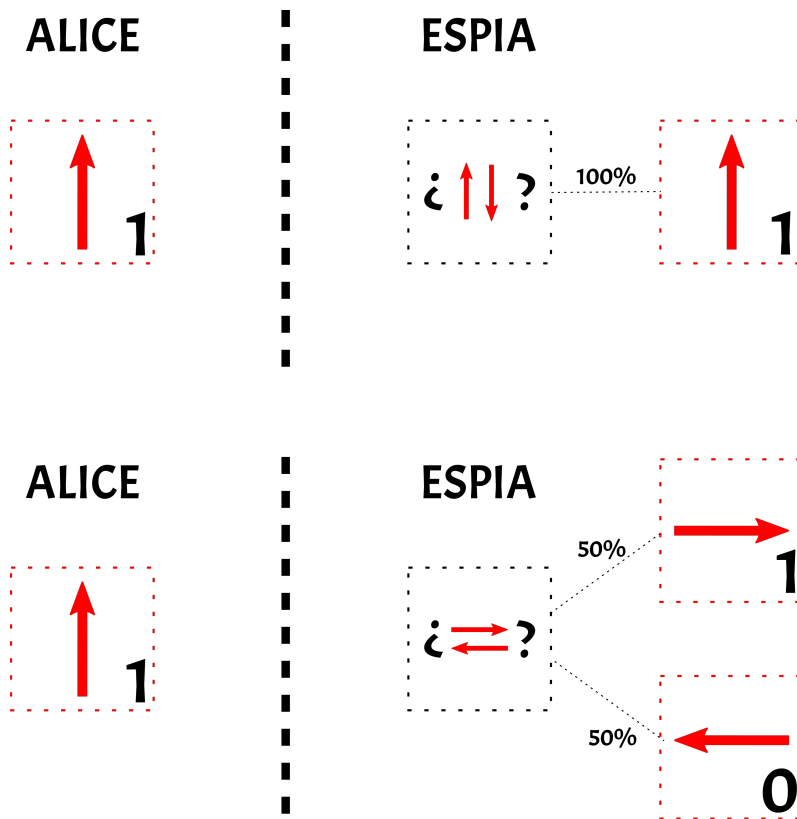
Alice prepara la seva primera fletxa perquè correspongui a un 1 a la base dreta / esquerra, per exemple, i l'envia a Bob. **Però aquí hi ha el punt important:** Bob no sap què pregunta ha de fer-li a la caixa. Com no ho sap, de vegades pot obtenir un 0!



Fitxes didàctiques per a la presentació a l'aula del BIG Bell Test

Això pot semblar un desavantatge, però és el que fa la clau segura, perquè tampoc cap espia podria apoderar-se de la clau.

Per exemple, si Alice envia el seu 1 en base dalt / baix, i l'espia el mesura en base dreta / esquerra, llavors veurà 50% de les vegades dreta (1) i el 50% de les vegades esquerra (0). Si l'espia necessita el contingut de TOTES les caixes, segur que no té tanta sort com per donar amb totes!



(Per cert, escollir quines preguntes fer a les partícules és just el que fareu vosaltres (els Bellsters) el 30 de novembre.)

Pas 3: compartir la clau

Això és el que s'anomena Protocol BB84.

Imagineu que el missatge té 2000 caràcters. Llavors necessitem una clau, una seqüència aleatòria de 2000 zeros i uns.

Fitxes didàctiques per a la presentació a l'aula del BIG Bell Test

Alice tria a l'atzar com preparar les seves partícules i envia a Bob diguem 5000 partícules, que - com hem dit - és com si fossin capsetes numerades. 1, 2, 3, ... 5000.

Bob rep les capsetes, i les va mirant, decidint també a l'atzar quina pregunta fer-los (a dalt / a baix o dreta / esquerra).

Com hem vist en el pas 2, no sempre van a coincidir. Com comproven quan han coincidit?

Es diuen per telèfon i trien algunes capsetes l'atzar: la 37, la 135, la 250, la 500, la 700, la 1234, 3021...

- 1) Alice li diu a Bob com ha preparat les fletxes, és a dir:
 - quina base ha assignat a cada caixa de les seleccionades a l'atzar
 - quin valor ha posat en cada caixa: 0 o 1.
- 2) Bob separa les caixes en les quals ell i Alice han utilitzat la mateixa base i comprova si el valor 0 o 1 que li ha comunicat Alice coincideix.
- 3) Si els números coincideixen, llavors es pot dir que no hi ha espia. Si no coincideixen, és que ha d'haver un espia en el mig que ha fet mesures sobre les fletxes i les ha fet col·lapsar en una altra base. (Recorda que si un espia s'interposa, amb **25%** de probabilitat canviarà el resultat de cada caixa!)

Si conclouen que hi ha espia, avorten la comunicació.

Si no n'hi ha espia, llavors construeixen la clau. Simplement Alice li diu a Bob quina base ha triat per cada partícula, Bob comprova en quines coincideix i l'hi diu. Alice i Bob s'han comunicat les bases públicament, però només ells poden saber la clau composta pels zeros i uns!

I els vostres estudiants poden preguntar:

1. Com es codifica la informació en els fotons?
2. La física quàntica diu que en certes condicions les coses no estan definides abans de mirar (per exemple si la fleca apunta cap amunt, no està definit si apunta a la dreta oa l'esquerra) i quan les mirem, decideixen l'atzar com ser (la fletxa decideix a l'atzar si apunta a la dreta o l'esquerra) ¿No és estrany? ¿Es va acceptar així de fàcil a la comunitat?

Fitxa **6** (Properament): Einstein contra la quàntica: La paradoxa EPR i el Test definitiu de Bell.

FITXA 5: POLARITZACIÓ I SUPERPOSICIÓ

Polarització

Superposició clàssica i quàntica

Suma vectorial

ACTIVIDAD EXTRA: Interferència

¿Clàssic o quàntic?

Les activitats que proposem apareixen en algunes pàgines web com a exemples d'experiments de física quàntica que es poden fer a casa. En realitat, és molt complicat observar propietats quàntiques amb materials casolans, perquè les propietats quàntiques de les partícules petites són molt delicades i és molt complicat poder-les observar 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 i interferència) que s'estudia a l'escola secundària. De tota manera, ens sembla interessant proposar 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 de partícules quàntiques individuals, els **fotons**.

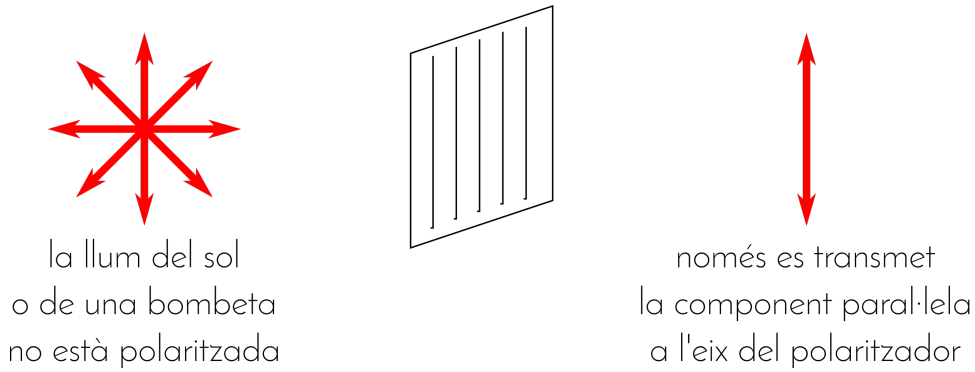
Però això no ens ha de semblar una cosa llunyana de la feina que fan els físics! L'experiment mental és una eina que els científics han utilitzat al llarg dels segles per resoldre problemes difícils de posar a prova experimentalment amb la tecnologia de l'època: exemples cèlebres són el vaixell de Galileu,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

Activitat 1. Polarització

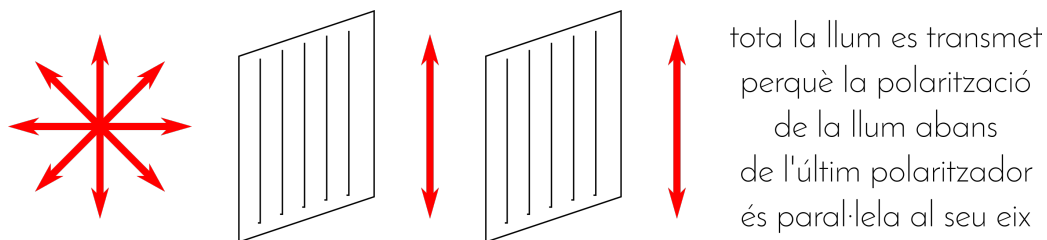
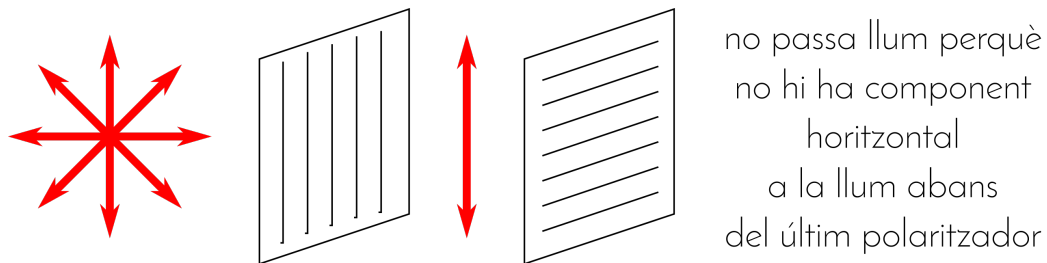
Material: 3 polaritzadors lineals

PAS 1. UN POLARITZADOR

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.

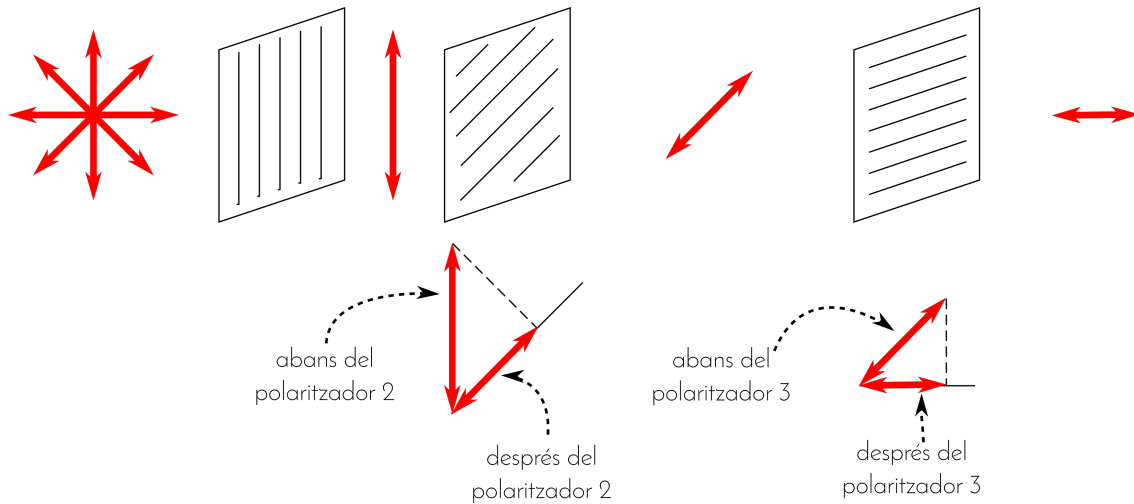


PAS 2: DOS POLARITZADORS



PAS 3: TRES POLARITZADORS

Utilitzant els dos polaritzadors creuats del pas 2, afegim un tercer polaritzador **al mig** a un angle de 45° amb l'horitzontal. Què passa?



La llum passa a través del sistema de polaritzadors, ¡tot i que el polaritzador 1 i 3 estiguin 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.

EXPERIMENT MENTAL

Funcionaria això també si interpretéssim la llum com composta de partícules individuals anomenades fotons?

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

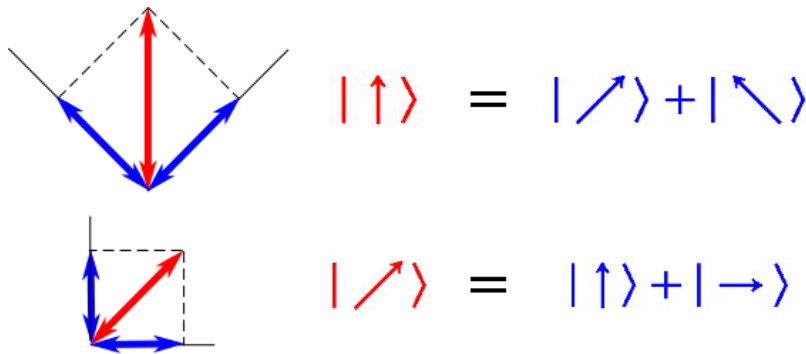
Sabem que els fotons no interactuen entre ells, i per tant hauríem d'obtenir el mateix resultat enviant molts fotons a la vegada (com en el nostre experiment) que enviant-ne un de sol.

Però com va a donar el mateix si enviem res més que un fotó alhora? La nostra intuïció ens diu que, si el fotó pot passar a través del primer polaritzador, no hauria de poder passar a través del segon perquè la seva polarització no està paral·lela a la del segon polaritzador.

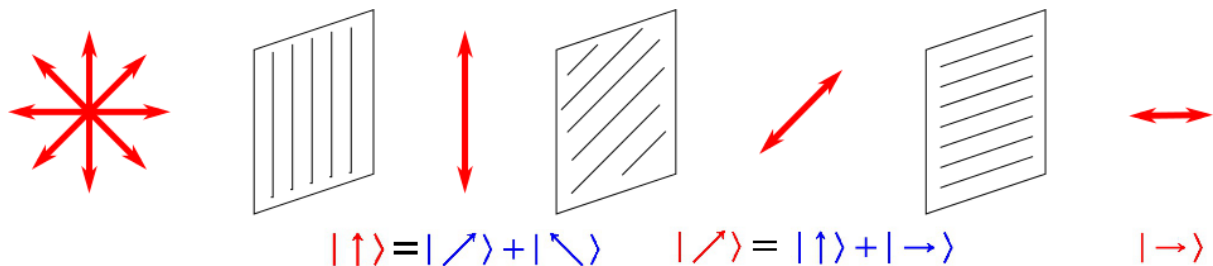
Per explicar l'experiment dels tres polaritzadors des del punt de vista quàntic, tenim llavors de recordar que la polarització es **comporta** com un vector. Però - com un fotó només pot tenir una polarització - haurem d'assumir que els estats (en aquest cas la polarització) del fotó (i en general de les partícules quàntiques) es sumen com si fossin vectors. Això es diu **principi de superposició**.

Fitxes didàctiques per a la presentació a l'aula del BIG Bell Test

Per exemple, un fotó vertical és la superposició d'un fotó amb polarització a $+45^\circ$ i d'un a -45° , com en la següent figura. De la mateixa manera, el fotó a 45° és la superposició d'un fotó vertical i d'un horitzontal.



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.



Nota: en la fitxa 3 també fem servir una fletxa per explicar les propietats de la física quàntica, però la descrivim de manera diferent que la polarització. A la fitxa 3, els estats possibles de la fletxa involucren direcció i sentit de la fletxa (amunt, avall, dreta, esquerra), mentre aquí considerem només l'adreça (vertical, horitzontal, $+45^\circ$, -45°).

Per saber més: http://www.informationphilosopher.com/solutions/experiments/dirac_3-polarizers/

Actividad extra: Interferencia

Podem utilitzar polaritzadors per destruir i tornar a crear patrons d'interferència com en l'experiment descrit aquí:

<https://www.scientificamerican.com/slideshow/a-do-it-yourself-quantum-eraser/>

Podeu trobar els materials necessaris per realitzar aquest experiment aquí:

<https://www.scientificamerican.com/article/a-do-it-yourself-quantum-2007-05/>

Si fem l'experiment mental de fer aquest experiment amb un fotó a la vegada, obtenim el que s'anomena **quantum eraser**.

BIBLIOGRAFÍA

Sobre implementacions recents de criptografia quàntica

Review en **New Scientist**

Artículo en **Nature Photonics**

Elecciones suizas en 2007

Història interactiva de la criptografia quàntica
(material fet per l'ICFO per a l'exposició Top Ciència del CosmoCaixa)

Sobre Einstein i els seus problemes amb la quàntica

Is the moon really there?

Una gran introducción a los fenómenos cuánticos.

Física cuántica: Interferencias, correlaciones y realidad, Valerio Scarani

Quantum Manifesto - A new era of technology

