# the BIG BELL TEST

## Fichas Didácticas

www.thebigbelltest.org
@TheBellsters

ICFO 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, Protection
ICREA

# Índex



# Material Adicional

### Material Impreso

Dossier para el público general: https://cloud.icfo.es/owncloud/index.php/s/sEYFFVgVUfAJ2MF

### Material Audiovisual

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

Vídeo Promocional (Inglés): https://vimeo.com/184480786

Vídeo Promocional (Catalán): https://vimeo.com/185292887

Vídeo Promocional (Castellano): https://vimeo.com/185292940

# EL BIG Bell Test en el aula

## FICHA 1: EL AZAR Y CÓMO USAR EL JUEGO DEL BBT EN EL AULA

### Azar y probabilidad

### Conceptos elementales de estadística: población, media, distribución estadística, medidas de dispersión.

### Funciones elementales de Excel: filtros y gráficos.

### Azar y probabilidad

El azar es un componente fundamental de la física cuántica. **En esta unidad os recomendamos el** excelente material creado por Joan Jarreño sobre el azar y la probabilidad en una entrada de su blog precisamente dedicada al **BIG Bell Test,** que podéis encontrar aquí: http://calaix2.blogspot.com.es/2016/10/latzar-te-patrons.html

### Estadística con el videojuego del **BIG Bell Test** en el aula.

El videojuego del **BIG Bell Test** es el portal para contribuir a los experimentos del 30 de noviembre.

Se puede jugar en cualquier momento, pero estaremos contribuyendo al experimento en tiempo real si jugamos en cualquiera de las 48 horas en que es el 30 de noviembre en algún punto del planeta.

Es decir, el día 30 de noviembre, tus alumnos pueden contribuir tantas veces como quieran, desde móviles, tabletas u ordenadores. No hace falta registrarse, pero es recomendable, por los motivos que verás a continuación.

Se puede contribuir en cualquiera de las dos versiones de la plataforma: el Quick Bell Test o el BIG Bell Quest, ambas en www.thebigbelltest.org/contribute.

El BIG Bell Quest, la versión gamificada, es la que hemos desarrollado para motivar la participación, no solo porque incluya una estética y una historia, sino porque incentiva la competición, entre individuos o grupos, y además nos permite crear una actividad de aula, que explicamos a continuación.

1. Ve a www.thebigbelltest.org/quest

2. Regístrate (puedes entrar como invitado, pero entonces perderás los datos de cada misión, y no podrás tener un nombre de usuario identificable). Al registrarte, no es necesario introducir el e-mail, es solo recomendable, por si alguna vez pierdes la contraseña para volver a entrar a la web.

3. **Crea un Evento**. En tu perfil de usuario, localiza la casilla "Evento" y elige un nombre significativo para el. Por ejemplo tu nombre, o el de tu clase seguido del nombre de tu centro.

4. Di a tus alumnos que se registren en el juego, pero dales el nombre del Evento **una vez están todos en el aula**.

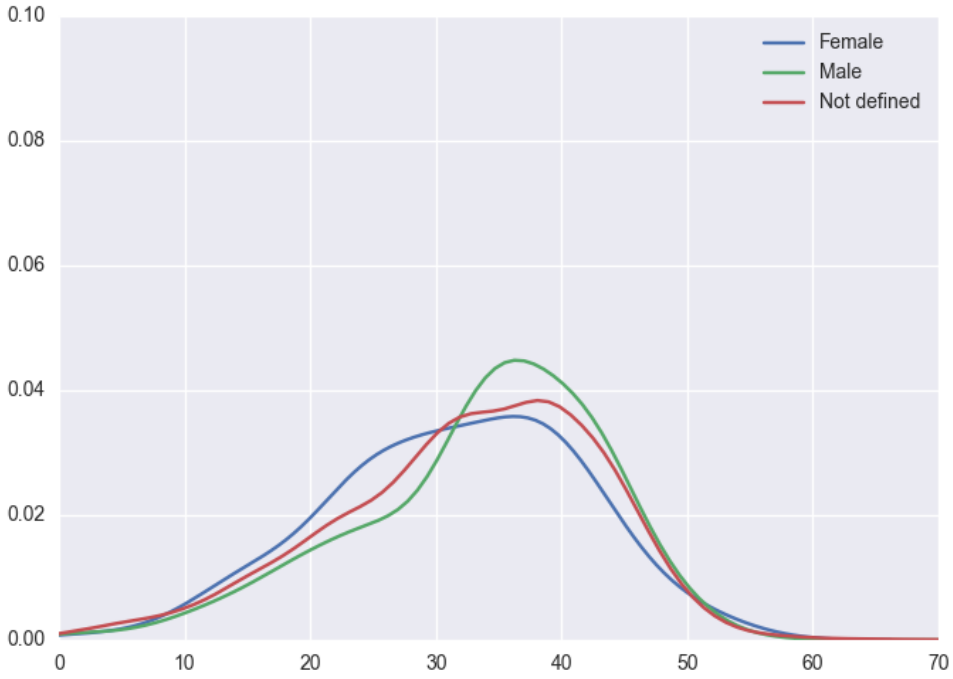
5. Una vez todos registrados, y todos habiendo elegido el mismo nombre para el Evento (ojo con las mayúsculas), empieza el juego. **Los alumnos han de jugar una misión o varias** (según tú consideres). Quizá puedes darles tres minutos, o cinco, para jugar. Cuando haya pasado el tiempo, han de dejar el móvil en las mesas. No te olvides de participar!

6. Ve a **www.thebigbelltest.org/radarevent** La página te pedirá un nombre de Evento, introduce el que has creado antes. Saldrá entonces la clasificación, por aleatoriedad y por puntos, de la clase.

7. Te puedes bajar esa **clasificación en Excel**, y hacer el gráfico de la distribución. ¿Qué forma tiene? ¿Es una gaussiana? ¿Tiene varios picos? ¿Es muy dispersa? Puedes utilizarla para trabajar los conceptos de media y medidas de dispersión. Al fin y al cabo tienes una población y un conjunto de valores (la aleatoriedad de cada uno). A medida que juguéis, podéis ver si la distribución cambia, si la media se acerca a algún punto, si la dispersión baja, etc.

8. Los alumnos pueden bajarse los datos y **trabajar correlaciones extra**. Por ejemplo ¿Hay diferencia entra las distribuciones si diferenciamos los chicos de las chicas? ¿Se mantienen estas diferencias en otras clases? ¿Y si comparamos las distribuciones entre diferentes grupos de amigos? ¿Los alumnos que tocan un instrumento son más o menos aleatorios, comparados con los demás? Si lo hacemos varios días seguidos, ¿podemos ver mejoría en los datos? Los alumnos pueden pensar otras correlaciones.

A continuación, os presentamos los resultados que hemos obtenido nosotros al estudiar el efecto del género sobre la aleatoriedad. ¿Obtenéis algo similar?



# La física cuántica

## INTRO

En esta serie de prácticas, tus alumnos aprenderán que:

1. en la física cuántica, las cosas no siempre se comportan como estamos **acostumbrados** y cuáles y de dónde vienen esas propiedades fundamentalmente nuevas y características de la cuántica.

2. la comunidad científica se ha dedicado con interés, y a veces dividida, a la **interpretación** de las sorprendentes predicciones de la física cuántica

3. las paradojas y aparentes sinsentidos de la física cuántica pueden ser aprovechados para generar **tecnologías** que superan las limitaciones de las tecnologías clásicas

4. el hecho de que la física cuántica sea tan difícil de comprender hace que la sociedad no está familiarizada con ella y pueda absorber mensajes erróneos por parte de sectores **pseudocientíficos**

5. la **generación a la que pertenecen** entenderá la física cuántica mejor que cualquier otra pasada, incluídos sus inventores. Ellos vivirán en una sociedad que tendrá que ir asumiendo cada vez más el paradigma cuántico, igual que antes se asumió el heliocéntrico.

6. Qué es el **BIG Bell Test**, qué harán los científicos, y por qué es importante que participemos.

# FICHA 2 - PRIMEROS CONCEPTOS

## Actividad 1 (Deberes para casa + discusión en clase)

Una posible manera de empezar es pedir a los estudiantes como deberes para casa buscar "cuántico" en internet, y encontrar una entrada, un punto concreto que les llame mucho la atención.

Al día siguiente, han de explicar a toda la clase qué han seleccionado y por qué. Ha de ser breve. No han de tratar de entender qué han leído, sino explicar por qué les sorprende, o precisamente qué no han entendido.

Es posible que algunos hablen de las propiedades extrañas de la cuántica, otros de aplicaciones como el ordenador cuántico, o la criptografía, y otros de cosas aún más extrañas como la meditación cuántica, la sanación cuántica, y pseudociencias similares.

Esta primera práctica nos servirá para:

- Introducir la física cuántica como una teoría científica que explica las leyes que obedecen los objetos más pequeños, como átomos, electrones, fotones, etc., que tiene un extraordinario poder explicativo y predictivo pero que de la misma manera es extraordinariamente antiintuitiva e imposible de conciliar con nuestra manera de entender el mundo.

- Decir que a pesar de ser incomprensibles, las propiedades de las partículas cuánticas sirven para generar tecnologías nuevas con capacidades imposibles de alcanzar para las tecnologías cla´sicas (ordenadores rapidísimos, transacciones de información seguras 100%...)

- Alertar que como la física cuántica es tan difícil de integrar en nuestra manera habitual de entender el mundo y parece desafiar nuestro sentido común, hay muchas personas lo aprovechan para inventarse todo tipo de "conexiones extrañas" como la consciencia cuántica, el desdoblamiento cuántico, la curación cuántica. Es importante que la sociedad se empiece a acercar a la cuántica, a qué significa y qué implica, para evitar caer en este tipo de engaños y confusiones. Además, es posible que la sociedad tenga mucho que decir sobre las nuevas tecnologías **cuánticas.**

Ejemplos de sitios que abusan de los "misterios cuánticos":

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

Sea lo que sea lo que signifique "Scientific Counciousness", ningún grupo de investigación científico ha podido demostrar que la consciencia tenga que ver algo con la física cuántica.

http://www.quantumenergywellness.com/

El término "quantum energy" no tiene ningún sentido, y no lo utiliza ningún científico.

http://medicinacuantica.cl/

Aquí incluso utilizan los vídeos muy buenos de Dr. Quantum para explicar sus conexiones entre medicina y cuántica.

Entonces puedes hacer un resumen de las tecnologías cuánticas que están ahora en desarrollo o en práctica (en la bibliografía hemos seleccionado algunas). A lo largo de las siguientes fichas nos fijaremos en una muy sugerente, la criptografía cuántica, que nos servirá de entorno para explicar las propiedades cuánticas fundamentales.

## FICHA 3 : EL PROBLEMA DE COMPATIR LLAVES SEGURAS

### (Actividades para explicar qué es la criptografía)

### Se trabaja la aritmética modular.

### Se puede relacionar con los alfabetos.

Empecemos por un pequeño juego. Nos vamos a enviar mensajes secretos.
(Aquí tienes más actividades de criptografía clásica, por si te parecen interesantes.)

Se juega por parejas. Si hay un número impar de alumnos, un grupo puede ser de tres.

Cada alumno tiene que coger una palabra de siete letras, y tiene que cifrarla según el cifrado César, es decir, sustituyendo cada letra de la palabra por la que se encuentra a K (el número K es la clave y la han de decidir ellos.) posiciones a la derecha de ella en el alfabeto.

- Dependiendo de cómo quieras hacerlo, la clave la comparten o no. O sea, a la hora de descifrar el mensaje, el alumno descifrador puede actuar como receptor normal (sabe qué es K) o como espía (ha de ir probando muchas K posibles).

-Y dependiendo del nivel de los alumnos, pueden usar la rueda de Cesar https://inventwithpython.com/cipherwheel/ (muy fácil), o hacer ellos el trabajo de escribirse el alfabeto e ir contando posiciones, o sustituir cada letra por un número y hacer la suma módulo 27 (contamos 27 letras, sin ll ni ch).

- ¿Qué significa sumar módulo 27? Lo podemos explicar mediante un ejemplo. Un buen ejemplo son las horas del día. Si queremos saber qué hora será dentro de 30 horas, tendremos que sumar módulo 24, porque no hay más que 24 horas en un día.

Cuando el estudiante haya cifrado la palabra, la pasa a su compañero, quien a su vez ha de darle la suya. Ahora ellos tendrán que descifrarse mutuamente. Si uno termina de cifrar antes de que el otro, puede empezar a cifrar otra palabra. Así, además, prevenimos que cifren muy fácil (K pequeño), o muy difícil (K grande), porque no querrán estar mucho tiempo cifrando y que el compañero les pase muchos deberes.

Gana quien descifre antes todas las palabras que tiene encima de la mesa.

Casi mejor si el profesor preselecciona las palabras y les da unas cuantas a cada uno. Además, para hacerlo más fácil, pueden dejarse sin cifrar algunas letras, señalando que esas no hace falta cifrarlas.

**Ahora vamos a ver qué pasa si el receptor no sabe la clave de encriptación, o la ha perdido u olvidado. ¿Puede descifrar su mensaje? O lo que es lo mismo, entonces ¿Puede un espía descifrar un mensaje que no tiene la clave?**

Se puede hacer una ejercicio en la pizarra para todos. La estrategia del espía o del receptor despistado que ha perdido la clave, es ir probando K=1, K=2, K=3, ...

Para incentivar la respuesta, en la pizarra podemos descifrar una palabra fácil, Alabama con K=2, sin decirlo a los alumnos (quedaría CNCDCOC). Y entonces ver que en cuanto sacas una letra (la A), ya tienes muchas pistas para descifrar. Si además sabemos que es el nombre de una ciudad de América, pues otra ventaja más. Es decir, si el espía tiene contexto, su tarea es relativamente fácil.

¿Cómo podríamos hacerlo más difícil para el espía? Una manera de hacerlo más difícil (y de hecho es imposible de descifrar!) es dar a cada palabra un K distinto, en lugar del mismo desplazamiento para todas las letras.

Les haces una prueba para que descifren una con un K distinto para cada letra. Les resultará imposible y verán rápido por qué. Este método se llama el cifrado Vernam.

Ahora vienen las consideraciones:

- La clave de encriptación no es un número, sino una secuencia de números (uno para cada letra)

- ¡La clave es tan larga como el mensaje!

- Como a cada número corresponde una letra del alfabeto, la clave de encriptación puede ser también una secuencia de letras

- Un alfabeto tiene 27 letras, es un poco farragoso hacer sumas módulo 27. ¿Y si nos pasamos a un alfabeto con dos letras? ¿Y si las "letras" son 0 y 1?

## Actividad:

- El profesor escribe un "mensaje" en ceros y unos (puede ser una cosa inventada, puede ser una palabra en código ASCII, si quiere explicar qué es, pero algo no muy largo).

- Entonces pide a los alumnos que inventen cada uno una clave de cifrado. Cada alumno ha de inventar la que quiera, aleatoriamente.

- Los alumnos han de sumar módulo 2 la clave que han inventado al mensaje. Tienen un mensaje encriptado.

- De nuevo, sumar módulo 2 consiste en saltar al 0 una vez pasas del 1. Las operaciones quedarían así: 0+0=0 ; 0+1=1 ; 1+0=1 ; 1+1=0

- Dos alumnos salen a la pizarra. Cada uno escribe su mensaje encriptado totalmente distinto. El profesor les pide que sumen a su mensaje encriptado su clave de encriptación. A los dos (si o hacen bien) les ha de salir el mensaje original.

## - (Profundización - deberes opcionales para casa):

- ¿Qué pasa si pruebo todas las posibles combinaciones para descifrar un mensaje? Como hacíamos en la primera actividad, que íbamos probando K=1, K=2, hasta dar con el mensaje

(¡Si hacemos eso, obtendremos todos los posibles mensajes de esa longitud!)

- ¿Qué pasa si uso dos veces la misma clave en dos mensajes diferentes?

(Si hacemos eso, los mensajes pueden ser la clave el uno del otro. Por eso este método se llama el one time pad)

## Conclusiones:

- La clave de cifrado es entonces una secuencia de ceros y unos tan larga como el mensaje.

- Es importante que sea una secuencia aleatoria, es decir, que no tenga ningún sentido, para que un espía no pueda imaginársela.

- El emisor y el receptor del mensaje deben estar seguros de tener la misma clave de cifrado, la misma secuencia, para cifrar y descifrar. Es decir, tienen que compartir la clave.

- !!!El emisor y receptor del mensaje tienen que compartir la clave sin que el espía la robe!!!

- **Si** el emisor y el receptor del mensaje comparten una secuencia de verdad aleatoria (que el espía no tenga manera de inferir) y **si** de verdad el espía no la puede conseguir de ningún modo (interceptándola sin que se enteren emisor y receptor), entonces este método es **100% seguro**.

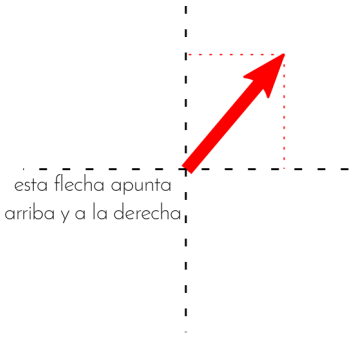
Ahora, una vez hemos entendido que si somos capaces de que el emisor y el receptor de un mensaje cifrado **compartan** la clave de cifrado tenemos comunicación segura, es la hora de entender siguiendo la ficha 3 a continuación, cómo la cuántica lo consigue. Cualquier otro método es falible, el espía siempre puede hackear tu sistema, si tiene un súper ordenador y es muy listo y tiene recursos para espiar todos los posibles canales.

## FICHA 4: CUÁNTICA: LA COMUNICACIÓN MAS SEGURA

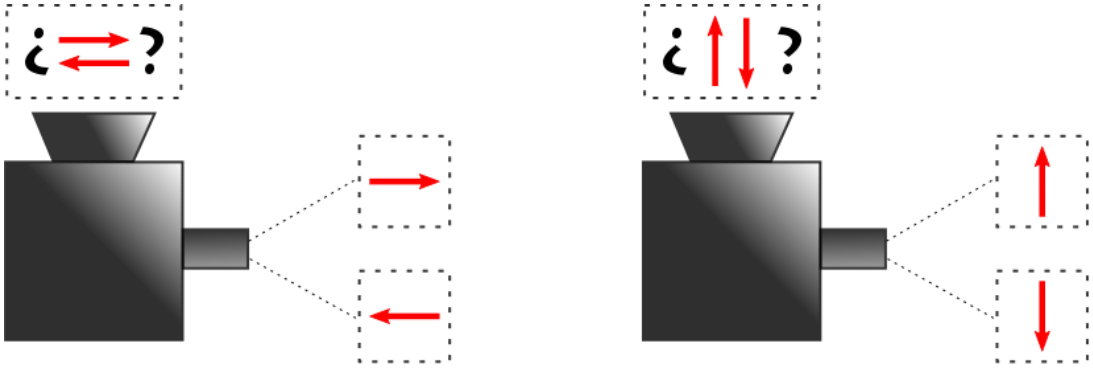
### Principio de Incertidumbre de Heisenberg
### Estado colapsado
### Azar

Para entender cómo con las partículas cuánticas seremos capaces de compartir esta clave de forma súper segura, hay que entender qué tiene de especial el mundo cuántico frente al clásico.

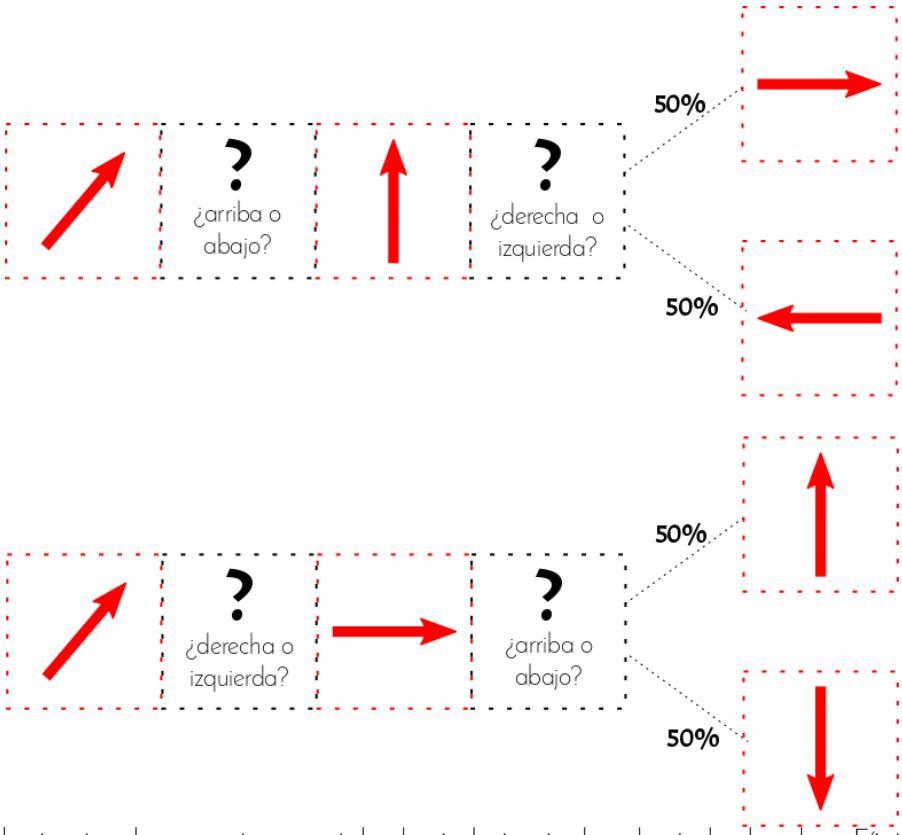
$|\uparrow\rangle$ Para un objeto cuántico (átomo, electrón, fotón) no es posible tener todas sus propiedades definidas al mismo tiempo.
Por ejemplo, dibuja una flecha. Si miras esta flecha puedes saber si apunta hacia la parte de arriba de la pizarra o hacia la parte de abajo, y también puedes saber si apunta hacia la derecha de la pizarra o hacia la izquierda. (Y puedes decir un montón de cosas más de la flecha, ir apuntándolas en una lista cada vez más grande, que la diferencia de cualquier otra flecha.) Si un compañero quiere saber cómo es la flecha te puede hacer preguntas: "¿apunta arriba o abajo?" y luego "¿apunta hacia la derecha o la izquierda?" y tú le puedes ir contestando consecutivamente como si estuvierais jugando al *¿Quién es quién?* de las flechas.




Sin embargo, si nos imaginamos la flecha con la que jugáis es una partícula cuántica, encontramos un problema al plantear la segunda pregunta. Podemos saber si la flecha apunta hacia arriba o hacia abajo, pero entonces ya no podemos saber si apunta hacia la izquierda o hacia la derecha. Y viceversa, podemos saber si apunta a la derecha o a la izquierda, pero entonces no sabremos nada de si apunta arriba o abajo. Esto es consecuencia del **principio de incertidumbre de Heisenberg,** que nos dice que existen preguntas incompatibles, cuyas respuestas no podemos saber a la vez. Es como si la flecha estuviera dentro de una caja negra imposible de abrir con un mecanismo que permite solo una pregunta a la vez.



|↑⟩ ¿Y cómo evita la cuántica que sepamos la respuesta a las dos preguntas? Pues porque en el momento en que la partícula responde, su estado **colapsa** a la respuesta que ha dado. Si la partícula nos responde "arriba" o "abajo", se queda apuntando hacia arriba o hacia abajo, y ya no sabemos




nada de si antes de preguntar apuntaba hacia la izquierda o hacia la derecha. Fíjate que una consecuencia de esto es que el orden de las preguntas puede cambiar la respuesta final, como en la siguiente figura, al contrario que en el *¿Quién es Quién?* de arriba. En el momento en que la flecha responde arriba, entonces se "olvida" de si apuntaba a la derecha o a la izquierda, y se queda apuntando hacia arriba. Entonces, ¿Qué pasa ahora si alguien llega y le pregunta si apunta a la derecha o a la izquierda? Pues, y aquí llega otra sorpresa, si a una partícula que está en un estado definido arriba/abajo (por ejemplo, arriba) se le pregunta si apunta derecha/izquierda, entonces la partícula, forzada a responder en esos términos, el 50% de las veces dice derecha y el 50 % de las veces dice izquierda. Es decir, **la cuántica es una fuente de azar genuino**.

|↑⟩ **(Nota)** La orientación de la flecha, que es el estado en que está la partícula cuántica, se puede describir en términos arriba/abajo o izquierda/derecha. No las dos cosas a la vez. El mismo estado se puede describir en esas dos bases. Por ahora nos quedamos aquí. Aún no hablaremos de superposición (de esto se habla en la ficha 4). Un estado puede ser arriba, puede ser abajo, pero también cualquier superposición de ellos. Esto por ahora no lo necesitamos.

Estas propiedades de la física cuántica (las preguntas incompatibles, el azar y el colapso al hacer una medida) pueden parecer una desventaja a la hora de saber completamente cómo es una partícula, pero podemos utilizarlas a nuestro favor para **garantizar 100% la seguridad** de la criptografía. Os explicamos por qué.

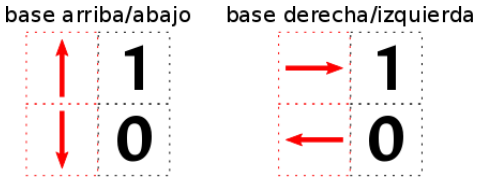
Ya hemos visto en la ficha 2, que una de las mejores maneras para enviar mensajes seguros es que el emisor (Alice) y el receptor (Bob) compartan una clave secreta de cifrado, una lista de ceros y unos aleatorios (clave en el estilo one-time pad).

Ahora veremos cómo Alice y Bob pueden obtener esa lista de 0s y 1s a partir de las propiedades de una partícula cuántica (que vamos a entender siempre como la flecha cuántica que describimos antes).

Alice prepara una flecha en cada caja y se las envía a Bob, que hace una pregunta a cada caja.

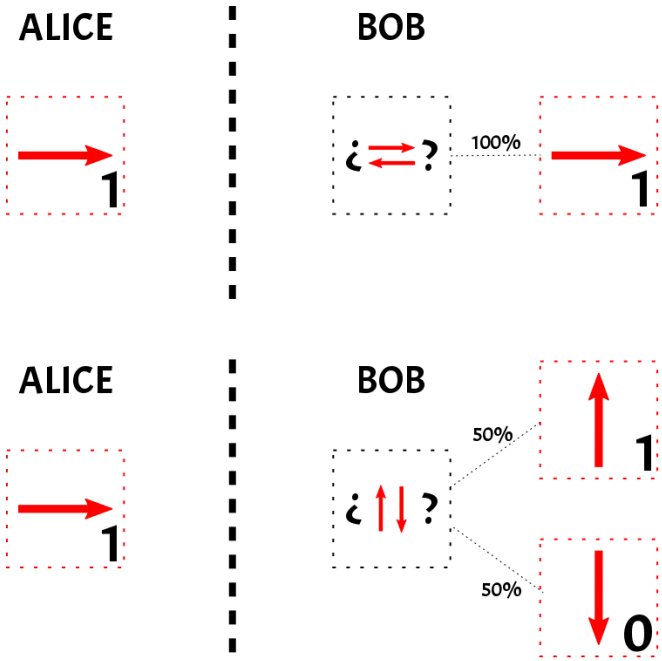
### Paso 1: Lógica del código

Alice y Bob se ponen de acuerdo para asociar 0 ó 1 con cada una de las dos respuestas posibles a cada una de las dos preguntas básicas.



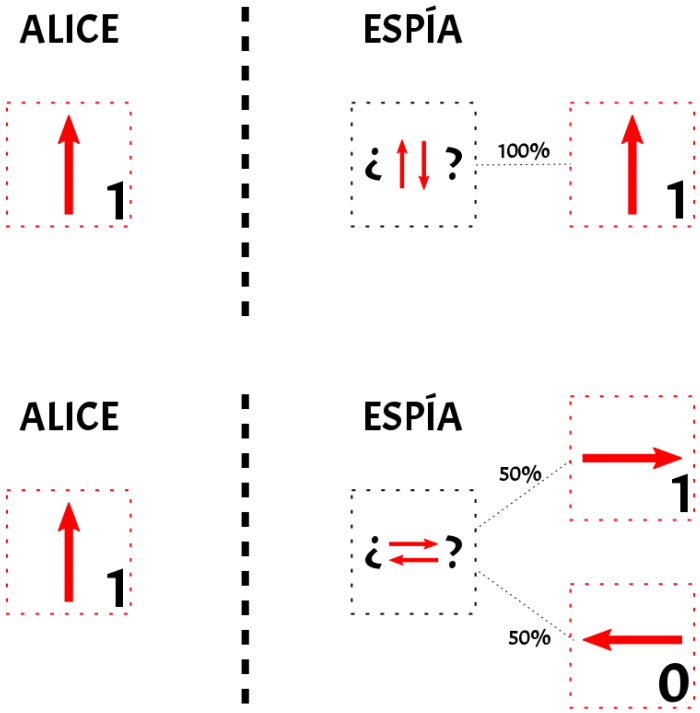

### Paso 2: compartir una partícula

Alice prepara su primera flecha para que corresponda a un **1** en la base derecha/izquierda, por ejemplo, y la envía a Bob. **Pero aquí está el punto importante:** Bob no sabe qué pregunta tiene que hacerle a la caja. ¡Cómo no lo sabe, a veces puede obtener un 0!



Esto puede parecer una desventaja, pero es lo que hace la clave segura, porque tampoco ningún espía podría apoderarse de la clave.

Por ejemplo, si Alice envía su 1 en base arriba/abajo, y el espía lo mide en base derecha/izquierda, entonces verá uno 50% de las veces derecha (1) y el 50% de las veces izquierda (0) ¡Si el espía necesita el contenido de TODAS las cajas, seguro que no tiene tanta suerte como para dar con todas!




(Por cierto, escoger qué preguntas hacer a las partículas es justo lo que haréis vosotros (los *Bellsters*) el 30 de noviembre.)

## Paso 3: compartir la clave

Esto es lo que se llama el Protocolo BB84.

Imaginad que el mensaje tiene 2000 caracteres. Entonces necesitamos una clave, una secuencia aleatoria de 2000 ceros y unos.

Alice elige al azar cómo preparar sus partículas y envía a Bob digamos 5000 partículas, que – como hemos dicho – es como si fuesen cajitas numeradas. 1, 2, 3, ... 5000.

Bob recibe las cajitas, y las va mirando, decidiendo también al azar qué pregunta hacerles (arriba/abajo o derecha/izquierda).

Como hemos visto en el paso 2, no siempre van a coincidir. ¿Cómo comprueban cuándo han coincidido?

Se llaman por teléfono y eligen algunas cajitas al azar: la 37, la 135, la 250, la 500, la 700, la 1234, 3021...

1) Alice le dice a Bob como ha preparado las flechas, es decir:
    - qué base ha asignado a cada caja de las seleccionadas al azar
    - qué valor ha puesto en cada caja: 0 ó 1.
2) Bob separa las cajas en las cuales él y Alice han utilizado la misma base y comprueba si el valor 0 ó 1 que le ha comunicado Alice coincide.
3) Si los números coinciden, entonces se puede decir que no hay espía. Si no coinciden, es que tiene que haber un espía en el medio que ha hecho medidas sobre las flechas y las ha hecho colapsar en otra base. (Recuerda que si un espía se interpone, con 50% de probabilidad cambiará el resultado de cada caja!).

Si concluyen que hay espía, abortan la comunicación.

Si no lo hay, entonces construyen la clave. Simplemente Alice le dice a Bob qué base ha elegido por cada partícula, Bob comprueba en cuáles coincide y se lo dice. Alice y Bob se han comunicado las bases públicamente, ¡pero solo ellos pueden saber la clave compuesta por los ceros y unos!

Y vuestros estudiantes pueden preguntar:

1. ¿Cómo se codifica la información en los fotones?

2. La física cuántica dice que en ciertas condiciones las cosas no están definidas antes de mirarlas (por ejemplo si la fleca apunta hacia arriba, no está definido si apunta a la derecha o a la izquierda) y cuando las miramos, deciden al azar cómo ser (la flecha decide al azar si apunta a la derecha o la izquierda)¿No es raro? ¿Se aceptó así de fácil en la comunidad?

Ficha 5 (Próximamente): Einstein contra la cuántica: La paradoja EPR y el Test definitivo de Bell.

## FICHA 5: POLARIZACIÓN Y SUPERPOSICION

**Polarización**
**Superposición clásica y cuántica**
**Suma vectorial**
ACTIVIDAD EXTRA : **Interferencia**

### ¿Clásico o cuántico?

Las actividades que proponemos aparecen en algunas páginas web como ejemplos de experimentos de física cuántica que se pueden hacer en casa. En realidad, es muy complicado observar propiedades cuánticas con materiales caseros, porque las propiedades cuánticas de las partículas pequeñas son muy delicadas y es muy complicado poderlas observar en ausencia de las condiciones estrictas que se pueden encontrar en un laboratorio.

Los **experimentos** que proponemos aquí – en realidad – se pueden explicar fácilmente con la **óptica clásica** (polarización e interferencia) que se estudia en la escuela secundaria. De todas maneras, nos parece interesante proponerlos en este contexto porque pueden llevar a conclusiones sorprendentes cuando se hace el **experimento mental** de reflexionar sobre cómo se pueden reproducir estos efectos si pensamos que la luz está compuesta de partículas cuánticas individuales, los **fotones**.

¡Pero esto no nos tiene que parecer algo lejano del trabajo que hacen los físicos! El experimento mental es una herramienta que los científicos han utilizado a lo largo de los siglos para resolver problemas difíciles de poner a prueba experimentalmente con la tecnología de la época: ejemplos célebres son el barco de Galileo, el demonio de Maxwell, la paradoja de los gemelos o el gato de Schrödinger.

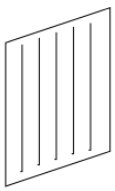
### Actividad 1. Polarización

**Material:** 3 polarizadores lineales

PASO 1. UN POLARIZADOR

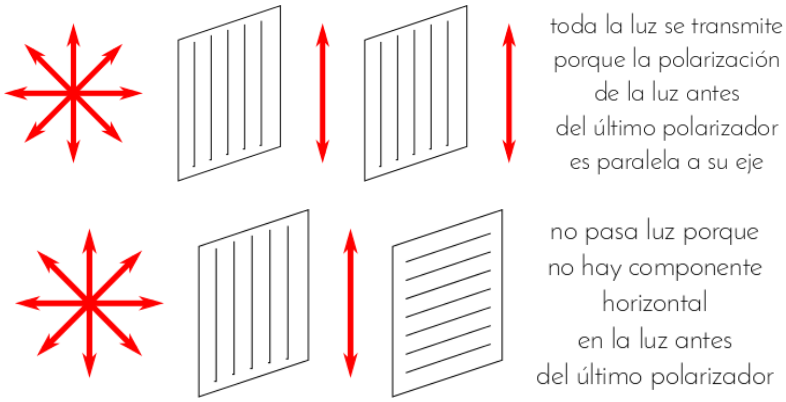
La **polarización** de la luz se describe como un **vector**. El **polarizador** actúa como un filtro y **proyecta** la polarización de la luz incidente sobre el eje del polarizador.

la luz del sol
o de una bombilla
no está polarizada



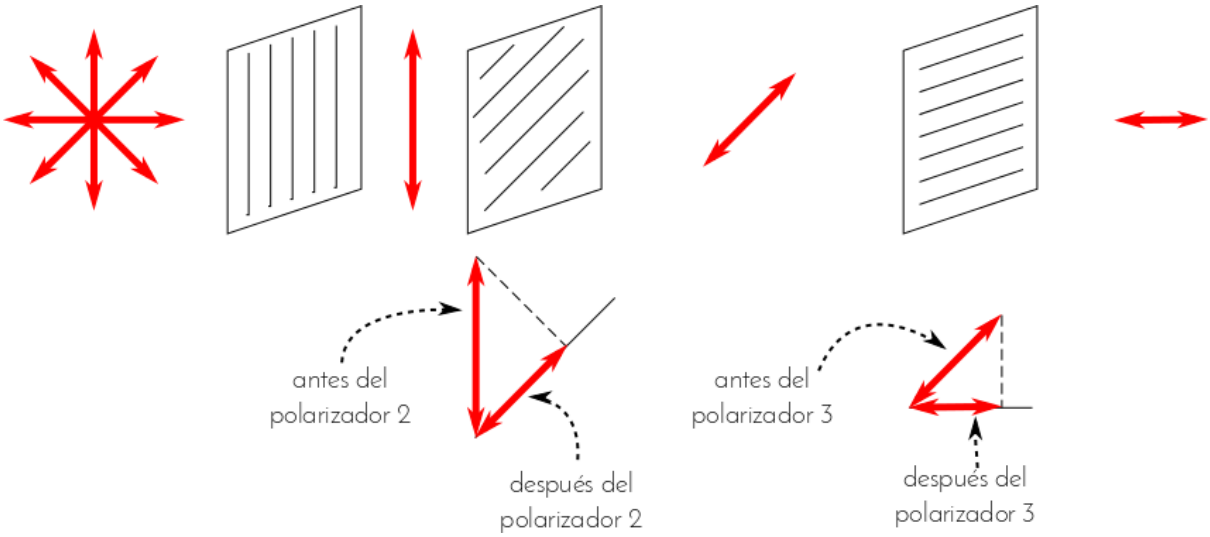
solo se transmite
la componente paralela
al eje del polarizador

Paso 2: DOS polarizadores




PASO 3: TRES POLARIZADORES

Utilizando los dos polarizadores cruzados del paso 2, añadimos un tercer polarizador en el medio a un ángulo de 45º con el horizontal. ¿Qué pasa?




La luz pasa a través del sistema de polarizadores, ¡a pesar de que el polarizador 1 y 3 estén cruzados! Podemos entender esto gracias a las propiedades de los vectores: después de cada polarizador se transmite la componente paralela al eje del polarizador.

EXPERIMENTO MENTAL

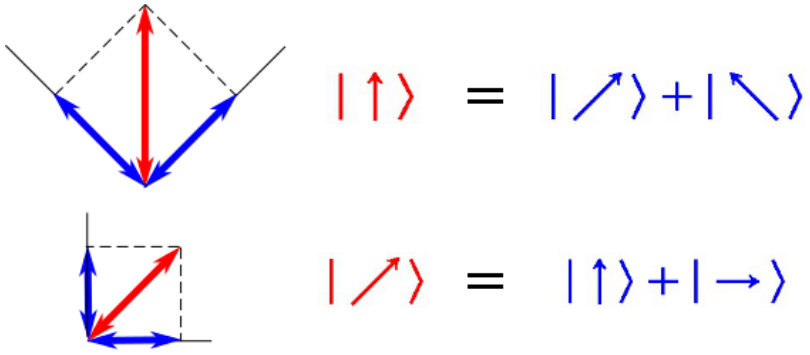
¿Funcionaría esto también si interpretásemos la luz como compuesta de partículas individuales llamadas **fotones**?
Podríamos decir que cada fotón tiene su propia polarización: por ejemplo, en la luz no polarizada hay muchos fotones y cada uno tiene polarización distinta, así que en media la polarización es nula. Cuantos más fotones en una dirección de polarización, más largo será el vector correspondiente a esa dirección.

Sabemos que los fotones no interactúan entre ellos, así que deberíamos obtener el mismo resultado enviando muchos fotones a la vez (como en nuestro experimento) o enviando solo un fotón a la vez.

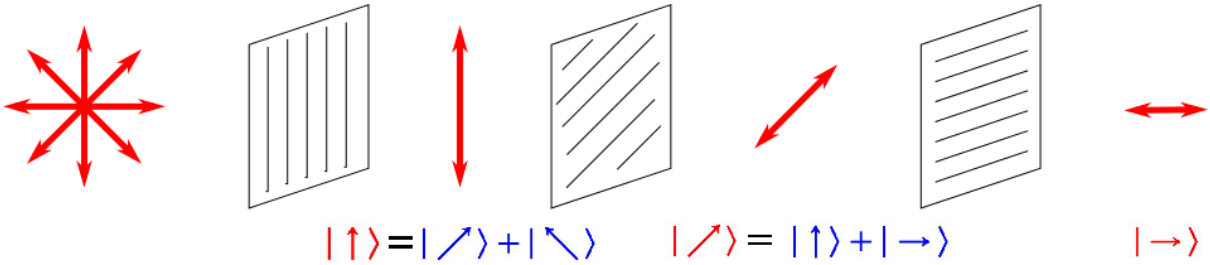
¿Pero cómo va a dar lo mismo si enviamos nada más que un fotón a la vez? Nuestra intuición nos dice que, si el fotón puede pasar a través del primer polarizador, no debería poder pasar a través del segundo porque su polarización no está paralela a la del segundo polarizador.

Para explicar el experimento de los tres polarizadores desde el punto de vista cuántico, tenemos entonces que recordar que la polarización se porta como un vector. Pero – como un fotón nada más puede tener una polarización – tendremos que asumir que los estados (en este caso la polarización) del fotón (y en general de las partículas cuánticas) se sumen como si fuesen vectores. Esto se llama **principio de superposición**.

Por ejemplo, un fotón vertical es la superposición de un fotón con polarización a +45° y de uno a -45°, como en la siguiente figura. De la misma manera, el fotón a 45° es la superposición de un fotón vertical y de uno horizontal.




En el caso cuántico, el polarizador tiene el efecto de quitar el fotón de la superposición y hacerlo "colapsar" en uno de los dos estados, en particular, el que tenga polarización paralela al eje del polarizador.




**Nota:** en la ficha 3 también utilizamos una flecha para explicar las propiedades de la física cuántica, pero la describimos de manera diferente que la polarización. En la ficha 3, los estados posibles de la flecha involucran **dirección y sentido** de la flecha (arriba, abajo, derecha, izquierda), mientras aquí consideramos solo la **dirección** (vertical, horizontal, +45°, -45°).

Para saber más: http://www.informationphilosopher.com/solutions/experiments/dirac_3-polarizers/

## Actividad extra: Interferencia

Podemos utilizar polarizadores para destruir y volver a crear patrones de interferencia como en el experimento descrito aquí: https://www.scientificamerican.com/slideshow/a-do-it-yourself-quantum-eraser/

Podéis encontrar los materiales necesarios para realizar este experimento aquí: https://www.scientificamerican.com/article/a-do-it-yourself-quantum-2007-05/

Si hacemos el experimento mental de hacer este experimento con un fotón a la vez, obtenemos lo que se llama **quantum eraser**.

## BIBLIOGRAFÍA


### Sobre implementaciones recientes de la criptografía cuántica:

New Scientist

Nature Photonics

Historia interactiva de la Criptografía (material hecho en ICFO para exposición Top Ciencia de CosmoCaixa)

### Sobre Einstein y sus problemas con la cuántica

Está la luna realmente ahí?

### Una gran introducción a los fenómenos cuánticos

Física cuántica: Interferencias, Correlaciones y Realidad, por Valerio Scarani

### Quantum Manifesto - A New Era of Technology