UTN FACULTAD REGIONAL MENDOZA
UNIVERSIDAD TECNOLÓGICA NACIONAL

Teorema de no clonación
e
influencia en el entrelazamiento cuántico

Parte III

Dr. Ing. Ernesto Gandolfo Raso
egandolfo@frm.utn.edu.ar

Criptografía Cuántica

Ya hablamos acerca del *Verschränkung*, el entrelazamiento cuántico. Conocimos entonces a los adorables –y a veces mortales– *cuantejos*, criaturas de naturaleza cuántica sobre los que realizamos algunas observaciones un tanto surrealistas. A pesar de que el entrelazamiento supone una unión entre sistemas físicos (como dos cuantejos) que no está sometida a límites de velocidad ni se ve entorpecida por barrera física alguna, eso *no significa* que podamos utilizarlo para transmitir información de manera instantánea: no podemos usar un par de cuantejillos para informarnos el uno al otro, por ejemplo, de si queremos ir al cine o no instantáneamente.

Pero eso no quiere decir que la naturaleza cuántica del Universo no pueda ser utilizada para transmitir información de formas insospechadas y utilísimas; simplemente significa que hay matices que debemos tener en cuenta. En este artículo trataremos de cómo comunicarnos de una forma que, si la cuántica no fuera real, sería imposible. Hablaremos sobre **criptografía cuántica**.

La manera más típica de resolver el problema es que la información que debo enviarte (que es muy sencilla, básicamente "sí" o "no") esté *encriptada* o *cifrada*, es decir, que sea un mensaje en clave. Podríamos habernos visto esta mañana, por ejemplo, y haber acordado la siguiente clave: si esta noche te llamo y te digo que "*la rana croa*", es que este personaje NO viene. Si, por el contrario, te digo que "*la rana salta*", es que SI viene a verme. Incluso si alguien tiene acceso de algún modo a nuestra conversación telefónica, no puede saber si esta persona viene mañana o no: el único con la información necesaria para descifrar el mensaje (el único con la clave) eres tú, con lo que nuestro problema está resuelto. Hemos utilizado una **clave privada**.

Podríamos incluso enviarnos mensajes mucho más complejos que “la persona viene” o “la persona no viene”, porque podríamos asociar “la rana salta” a un 1 binario, y “la rana croa” a un 0 binario. Cualquier mensaje puede ser reducido a ceros y unos –empleando el morse, caracteres ASCII o cualquier otro sistema similar–, con lo que nuestra clave de la rana es mucho más versátil de lo que pudiera parecer en un principio. Naturalmente, nuestra clave es algo tan primitivo que, si la usásemos para hablar todos los días, tarde o temprano alguien conseguiría descifrarla simplemente detectando estructuras o repeticiones en los mensajes; pero estoy seguro de que comprendes que, complicando la clave lo suficiente, podría llegar a ser muy difícil descifrarla.

La limitación fundamental de este sistema de clave privada debería ser obvia: requiere **que nos pongamos de acuerdo en una clave privada** que nadie más puede saber. Salvo que nos veamos en persona, seguros de que absolutamente nadie más nos está escuchando, *¿cómo diablos te comunico la clave?* No hay manera de que pueda transmitirte la clave por teléfono, porque si lo hago abiertamente, alguien podría estar escuchando, y si lo hago con un mensaje cifrado, *¿cómo te paso la clave?*

Tampoco puedo enviarte una carta, ni mandar un mensajero.

Esta limitación ha sido superada por sistemas más modernos de **clave pública**. En ellos, no compartimos la misma clave, sino que tú tienes una y yo otra, pero con un detalle ingeniosísimo que los hace utilísimos y que sería imposible sin una propiedad curiosa de muchos procesos matemáticos, como *la descomposición en factores primos*.

En estos sistemas, cada uno de los dos tenemos una clave propia que no comunicamos absolutamente a nadie – no, *ni siquiera el uno al otro*. A continuación, generamos a partir de esta clave privada una segunda clave, la clave pública, utilizando un algoritmo matemático prefijado. El *quid* de la cuestión está aquí: en matemáticas, existen algunos procesos que son triviales en un sentido *pero horriblemente complicados en el contrario*, y el algoritmo que empleemos debe ser uno de esos procesos.

Así, yo puedo producir una clave pública a partir de mi clave privada sin complicación alguna, pero si alguien tiene mi clave pública, es dificilísimo que consiga obtener mi clave privada. La cuestión está en que para cifrar un mensaje hace falta simplemente la clave pública: una vez así cifrado, la única manera de volver a descifrarlo es utilizando también la clave privada. Es decir, a diferencia del sistema anterior, ahora hay una **asimetría** entre ambos procesos (una asimetría que aparece por esa dificultad diferente en algunos algoritmos matemáticos en uno y otro sentido): *cifrar un mensaje es sencillo*, *descifrarlo es complicadísimo*. Puedo incluso publicar mi clave en el periódico, para que todo el mundo la vea… y todo el mundo podría enviarme mensajes cifrados, pero sólo yo podría leerlos. Es como si pudieras dar a todo el mundo una llave para *meter* cartas en tu buzón, pero sólo tú tuvieras una segunda llave con la que *sacar* cartas del buzón.

De modo que supongamos que quiero enviarte un mensaje acerca de los planes de la persona que viene a visitarme para la próxima semana. Lo primero que hago es llamarte por teléfono, para darte mi clave pública y que tú hagas lo mismo, y no nos importa que alguien pueda estar escuchando, porque no pueden obtener nuestras claves privadas a partir de la pública sin cálculos matemáticos absurdamente complejos. A continuación, utilizo tu clave pública para encriptar el mensaje que te voy a mandar (no uso mi clave absolutamente para nada). Una vez que lo hago, nadie puede descifrar ese mensaje sin tener además la clave privada… de hecho, como yo no la tengo, una vez he encriptado el mensaje para ti *¡ni siquiera yo puedo descifrarlo!* Por supuesto, no me hace falta, porque tengo el mensaje original sin cifrar.

Finalmente, te envío el mensaje así cifrado con tu clave pública. Incluso si alguien detecta el mensaje, como no tienen tu clave privada, no pueden descifrarlo: sólo tú, cuando lo recibes y utilizas tu clave privada, puedes saber que la semana que viene esta persona ha decidido ir al zoo. Podrías a continuación contestar a mi mensaje, cifrarlo con mi clave pública, y sólo yo sería capaz de descifrarlo. Y hemos conseguido esto *sin disponer en ningún momento de un canal de comunicación a prueba de escuchas*, y sin vernos en persona – una maravilla.

Porque el sistema, como cualquier sistema criptográfico, no es perfecto. Fíjate que he dicho que el algoritmo matemático es muy sencillo en un sentido y muy difícil en el otro… *pero "muy difícil" no es "imposible"*. Alguien con la suficiente capacidad de cálculo siempre puede, con tiempo, obtener inevitablemente mi clave privada a partir de la pública.

Lo único que nos protege en este caso es que, si la clave es larga y el algoritmo complejo, pueden hacer falta años para descifrarla salvo que alguien tenga capacidades de cálculo absolutamente sobrehumanas.
Pero todo este lío de la clave privada y la pública podría resolverse empleando nuestro primer sistema de clave privada, mucho más sencillo, simplemente si consiguiéramos una cosa: **ponernos de acuerdo en la clave privada sin que nadie más pueda saberla**, incluso sin vernos en persona. Y es aquí donde entra en juego la mecánica cuántica, los estados, las superposiciones, etc.

Vamos a empezar empleando los adorables cuantejillos. Pero, para ello, tenemos que ser más cuidadosos en su descripción, porque algunos de los aspectos más sutiles de la mecánica cuántica son clave en el asunto de la encriptación, con lo que no podemos utilizar el mismo tipo de cuantejos que utilizamos al hablar del entrelazamiento.

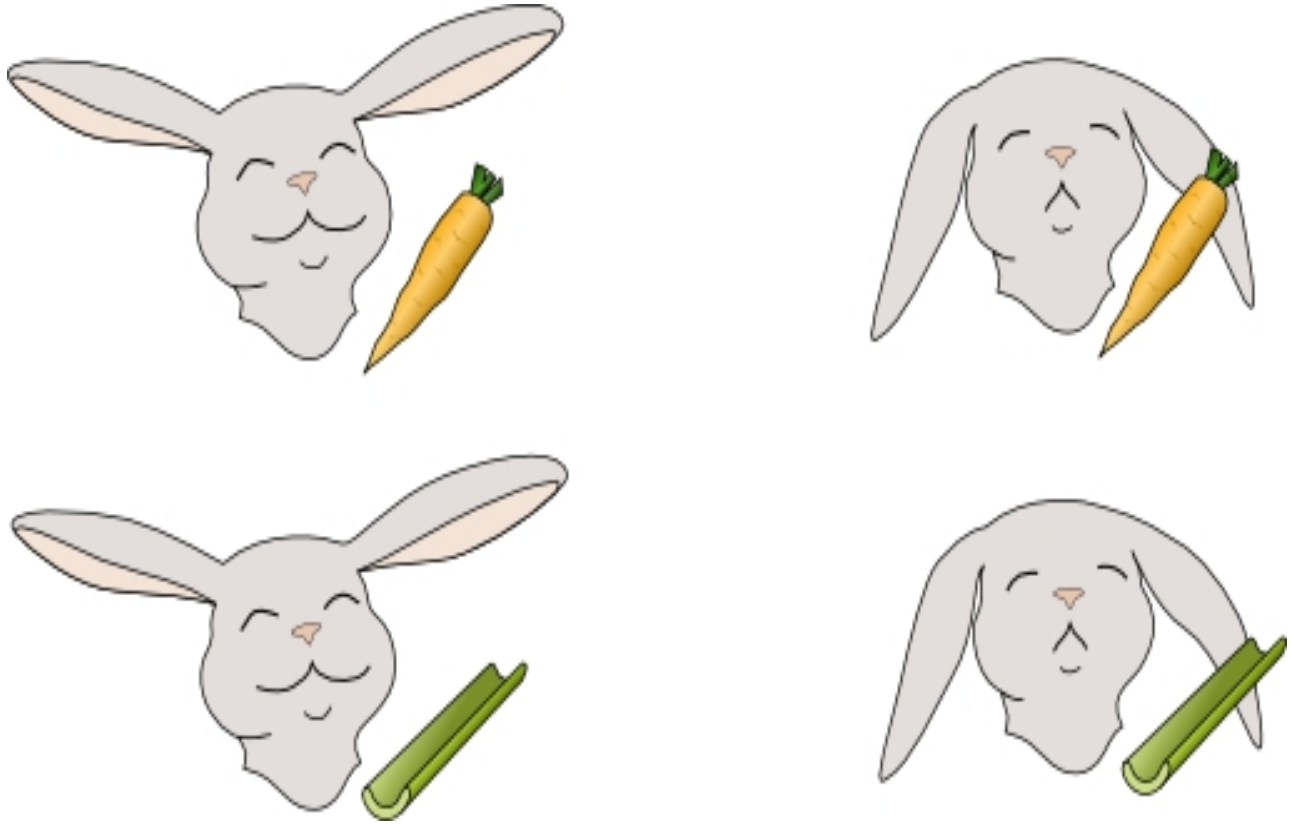
La clave para entender por qué la criptografía cuántica es útil es recordar que **al realizar una observación sobre un sistema lo modificamos irremediablemente**. Cuando detectamos un fotón, por ejemplo, es porque ese fotón ha impactado contra algún detector… con lo que ese fotón ya no existe.

De modo que los cuantejos que usaremos hoy en nuestra comunicación se comportan del siguiente modo: antes de que nadie realice cualquier medición sobre ellos, son de un color especial, inconfundible y cuántico – el color *octarino*. Pero, en cuanto un observador interacciona con el cuantejillo, éste se vuelve de un vulgar color gris como cualquier conejo normal y se echa a dormir. Una analogía más exacta sería decir que, cuando interaccionas con un cuantejo, éste muere y desaparece. De modo que los cuantejos simplemente cambian de color y se dan una siesta.

Puesto que, además, vamos a tener que mandarnos cuantejos el uno al otro unas cuantas veces, sería recomendable no emplear las variedades angelical y diabólica, porque tarde o temprano podría haber un accidente. Supongamos que existen cuatro tipos de cuantejos diferentes (para el primer ejemplo que utilizaré nos bastarían dos, pero luego nos harán falta los otros, de modo que creo que es mejor que los definamos todos ahora.

A algunos cuantejos les encantan las zanahorias más que cualquier otra cosa. Dales una zanahoria y son el ser más feliz del Universo. Estos amantes de las zanahorias tienen su opuesto en los cuantejos que las odian a muerte: si les acercas una zanahoria les has arruinado el día. Llamemos a la primera subespecie **zanahoriófilos**, y a los segundos **zanahoriófobos**.

También hay otras dos subespecies de cuantejos que tienen apetencias opuestas por el apio. Los cuantejos **apiófilos** se zampan esta verdura en cuanto se la enseñas, pero los **apiófobos** reaccionan de manera extrema y opuesta a ellos, rechazando el apio.



Las cuatro subespecies de cuantejos, tras enseñarles las verduras correspondientes.

Todos estos cuantejillos son tan predecibles en lo que respecta a la verdura que les importa *como impredecibles respecto al resto de verduras*. Si le enseñas un apio a un cuantejo zanahoriófilo, por ejemplo, es igualmente probable que se lance a por el apio y lo devore con fruición que lo rechace. No hay manera de saber cuál va a ser su reacción hasta que le enseñas el apio; y lo mismo sucede, por poner otro ejemplo, si le enseñas una zanahoria a un cuantejo apiófobo. Tal vez se disguste y la rechace, o tal vez –con igual probabilidad– sonría y se coma la zanahoria con gran placer.

Dicho de otra manera, un cuantejo zanahoriófilo es, expresado en términos de apio, una superposición de estados igualmente probables:

$$\frac{1}{\sqrt{2}}|\text{apiófilo}\rangle+\frac{1}{\sqrt{2}}|\text{apiófobo}\rangle$$

Al enseñarle el apio, el cuantejo se colapsa a uno de los dos autoestados, pero no hemos obtenido información sobre lo que realmente lo definía (si le gustaba la zanahoria o no), porque no hemos realizado la pregunta correcta.
Y, en cualquiera de los casos, antes de enseñar una zanahoria a un cuantejo (es decir, antes de realizar una observación sobre él para determinar su tipo) el cuantejo es de color octarino, *pero tras realizar la medición, el cuantejo se vuelve gris y se pone a dormir*.

De modo que, por un lado, es evidente cuándo un cuantejo se ha enfrentado a una verdura, y una vez eso ha sucedido, el cuantejo no sirve para nada en lo que a verduras se refiere, porque se ha ido a dormir.

Supongamos también que es posible producir pares de cuantejos entrelazados: uno zanahoriófilo junto a uno zanahoriófobo, o uno apiófilo junto a uno apiófobo.

¿Cómo podríamos comunicarnos la clave privada utilizando cuantejos sin que nadie pueda enterarse de ella y sin vernos en persona?

Vamos a emplear los cuantejos para describir los dos sistemas fundamentales de criptografía cuántica, el **protocolo BB84** y el **protocolo E91**, así nombrados por las iniciales de sus diseñadores y el año de su creación. Sin embargo, aunque el primero es anterior históricamente al segundo, vamos a estudiarlos al revés, simplemente porque el E91 es conceptualmente más fácil de entender a partir de nuestro artículo anterior, mientras que el BB84 es más retorcido.
Una manera muy sencilla de poner nuestra clave en común de forma segura es que yo produzca un *par de cuantejos entrelazados*, uno amante de las zanahorias y otro que las odie. Yo me quedo con uno de los dos (da igual cuál), y tú te llevas el otro en una caja a tu casa. Tanto tu cuantejo como el mío son de color octarino, porque nadie ha interaccionado con ellos aún: nadie les ha enseñado una zanahoria ni apio.

Esa tarde, le enseño a mi cuantejo una zanahoria, y pueden pasar dos cosas: o bien se abalanza sobre ella y se pone a comer vorazmente, o bien muestra cara de disgusto y la rechaza. Supongamos, para seguir con nuestro ejemplo concreto, que mi cuantejo pone cara triste y se niega a comer la zanahoria. Al mismo tiempo, su color cambia y deja de ser octarino, para ser gris, puesto que he interaccionado con él, y se pone a dormir.

Y también al mismo tiempo yo puedo estar *absolutamente seguro* de que el cuantejo que te has llevado es un cuantejo zanahoriófilo, lo contrario del mío.

Es *esencial* que entiendas una cosa. Yo no he presentado ninguna verdura a tu cuantejo: nadie lo ha hecho aún. Por lo tanto, aunque mi cuantejo es ahora gris, *el tuyo sigue siendo octarino*, y lo será hasta que vea alguna verdura. Como se ha dicho antes, si los cuantejos fueran fotones, al realizar la medición sobre el mío éste dejaría de existir, pero el tuyo seguiría existiendo. Este cambio en la observación es fundamental para entender la utilidad de nuestro sistema de comunicación más tarde, porque puedo saber con exactitud el tipo de tu cuantejo sin modificarlo en modo alguno.

De modo que, esa noche, puedo llamarte por teléfono y decirte lo siguiente: "*Si tu cuantejo es zanahoriófilo, nuestra clave es 1. Si es zanahoriófobo, nuestra clave es 0*". Y tú puedes colgar, enseñar una zanahoria a tu cuantejo y saber cuál es la clave, sin que yo te la haya dicho por teléfono, con lo que si alguien está escuchando la conversación no tiene ni idea de cuál es la clave.

Antes de nada, también para enviar una clave más larga bastaría con que no te llevaras un cuantejo en una caja, sino *una serie de cajas ordenadas del 1 en adelante*, y que luego hiciéramos lo mismo de antes pero más veces. Así tendríamos una serie de ceros y unos que constituirían nuestra clave de comunicación.

Pero *¿y si no podemos reunirnos en ningún momento?* Porque, si podemos hacerlo, no nos hacen falta cuantejos: nos decimos la clave de palabra y punto. Pero entonces no hemos ganado nada respecto al sistema tradicional de clave privada.
Supongamos, por tanto, que tú vives en una ciudad y yo en otra, y que podemos enviarnos paquetes por una empresa de mensajería. Nuestro problema, claro está, es que no sabemos qué puede pasar a los paquetes que enviamos por el camino, o si alguien va a registrarlos o no. *¿cómo te envío la clave privada utilizando cuantejos sin que nadie pueda verla?*

La clave es, claro está, el hecho de que **la medición del sistema lo modifica**, y es imposible ignorar que ha sido modificado. Podemos utilizar el sistema de antes: te voy enviando cuantejos en cajas, uno detrás de otro, a través de la empresa de mensajería. Si el mensajero es de fiar no hay problema, y todo funciona exactamente como antes. Si el mensajero es un espía, la única manera que tiene de descifrar la clave es ir abriendo las cajas y enseñando una zanahoria a cada cuantejo. Incluso aunque luego los vuelva a meter en sus cajas y te los entregue, cuando llegue la hora de que tú hagas la prueba enseñándoles una zanahoria… *¡los cuantejos no serán octarinos, porque alguien ya les ha enseñado una verdura!* De modo que, esa noche, antes de que nos pongamos de acuerdo como antes, tú me avisarás de que nuestra comunicación ha sido interceptada por un espía y que no vale.

De este modo, el principio de incertidumbre se confabula con nosotros, no para que podamos evitar la intercepción del mensaje, sino **para que podamos saber que se ha producido la intercepción** antes de poner en común la información secreta.

Lo único que tenemos que hacer entonces es cambiar de empresa de mensajería al día siguiente y volver a empezar, y así hasta que alguna vez recibas cuantejos octarinos, pongamos la clave en común y todos nuestros problemas estén resueltos.

Como ves, el sistema funciona empleando dos fenómenos cuánticos: el *entrelazamiento*, por el que estoy seguro de cómo es tu cuantejo si conozco el mío, y el *principio de indeterminación*, por el que podemos saber si alguien ha interaccionado con tu cuantejo, puesto que inevitablemente lo modifica.

Este sistema de encriptación, en la realidad, se realiza con **pares de fotones entrelazados** con polarizaciones determinadas, y se denomina **protocolo E91**; fue desarrollado en 1991 por Artur Ekert.

Sin embargo, hay un punto débil en este plan si el enemigo es lo suficientemente inteligentes… y tienen sus propias fuentes de cuantejos.

El mensajero puede abrir una caja y enseñar una zanahoria al cuantejo número 1. Si resulta que es zanahoriófobo, el mensajero se apunta este dato. No puede seguir enviando el cuantejo a tu casa, porque ha dejado de ser octarino para ser gris… pero puede preparar un nuevo cuantejo zanahoriófobo, meterlo en la caja y enviártelo. *¿Cómo puede hacer eso?*

Por ejemplo, creando un par de cuantejos zanahoriófilo-zanahoriófobo y enseñando una zanahoria a uno de ellos.

Si resulta ser zanahoriófilo, mete al otro en la caja y te lo envía: es, con total seguridad, zanahoriófobo, y sigue siendo octarino porque nadie le ha enseñado una verdura. Si ese par de cuantejos no funciona porque el que él detecta es el zanahoriófobo, crea otros hasta que haya suerte y obtenga el resultado que necesita.

El problema es que si este intermediario es listo, puede enviarte sus propios cuantejos y quedarse con los míos, de modo que ambos pensemos que todo ha ido bien y esa noche nos pongamos de acuerdo en la clave… y, si nuestra línea telefónica está pinchada, la hayamos delatado al enemigo. Por cierto, esto no se produce en la realidad con el protocolo E91 porque, en el caso de los fotones entrelazados, existen maneras de detectar el hecho de que los fotones que recibes ya no están entrelazados con nada, con lo que sabrías que el mensajero es un enemigo.

Pero la potencia tremenda de la cuántica basta para que, *incluso si este sistema no funcionase por esa razón*, pudiéramos emplear otro que no fuera vulnerable de ese modo. Ese otro sistema es el **protocolo BB84**, desarrollado en 1984 por Charles Bennett y Gilles Brassard, y no utiliza en absoluto cuantejos entrelazados. Como he dicho antes, es más enrevesado que el de Ekert, de modo que vayamos paso a paso, con un ejemplo muy concreto, para que se pueda comprender en qué se basa este protocolo, primero sin mensajero espía y luego con él.

En primer lugar, preparo unos cuantos cuantejos al azar de las cuatro subespecies posibles: zanahoriófilos, zanahoriófobos, apiófilos y apiófobos. Puedo hacer esto de diversas maneras, por ejemplo creando pares de cuantejos entrelazados y determinando uno de ellos (mostrándole la verdura correspondiente), y luego metiendo el otro cuantejo del par en la caja, todavía octarino. Utilicemos un ejemplo concreto: preparo cinco cuantejos de los cuatro tipos al azar, que resultan ser (1) zanahoriófilo, (2) apiófobo, (3) apiófobo, (4) zanahoriófobo y (5) apiófilo.

En el dibujo muestro la verdura al lado del cuantejo, pero eso no quiere decir que haya una verdura cerca, sino simplemente de qué tipo de cuantejo se trata:

Mensaje preparado por mí.

A continuación, te envío los cuantejos en cajas numeradas del 1 al 5. Por ahora, como he dicho, imaginemos que el mensajero no es un espía y que recibes los cuantejos como te los mando. De modo que recibes en tu casa cinco cajas numeradas, abres la primera caja y te encuentras, claro está, con un adorable cuantejo octarino.

Aquí está la clave de la diferencia con el protocolo E91: *¿qué haces, le enseñas una zanahoria o le enseñas un apio?* Tienes que elegir una verdura, y una vez que lo hagas el cuantejo se volverá gris, se irá a dormir y no servirá para nada más. Si eliges la verdura que se corresponde con esa subespecie de cuantejo, el animal hará lo que corresponde a su subespecie, pero si eliges la verdura incorrecta, el cuantejo actuará al azar, comiendo o rechazando la verdura con igual probabilidad. Y no tienes manera de saber qué subespecie es… de modo que le enseñas la verdura que te dé la gana.

Supongamos que enseñas al cuantejo una zanahoria. Como el cuantejo (1) es zanahoriófilo, se lanza a por la zanahoria, la devora, se vuelve gris y se va a dormir.
Tú, desde luego, no tienes manera de saber si esto ha sucedido porque es un cuantejo zanahoriófilo, o porque es de una de las dos subespecies de cuantejo sensibles al apio que ha reaccionado al azar, pero puedes apuntar lo que ha sucedido **[(1) zanahoria: se la ha comido]**.
Con el segundo cuantejo haces lo mismo: le enseñas una zanahoria. Pero el cuantejo (2) es apiófobo, con lo que su reacción a la zanahoria es aleatoria. Imaginemos, por ejemplo, que se abalanza sobre ella feliz y contento y se la come, se vuelve gris y se va a dormir.
Una vez más, no sabes cuál es su subespecie, pero apuntas el resultado: **[(2) zanahoria: se la ha comido]**.

Y lo mismo haces con los demás; supongamos que los resultados que obtienes son **[(3) apio: lo ha rechazado]**, **[(4) apio: se lo ha comido]**, **[(5) apio: se lo ha comido]**.

Recapitulemos lo que ha sucedido hasta ahora; aquí tienes los cuantejos que he mandado yo, lo que le has enseñado a cada uno y el resultado en cada caso:

Una vez más, tú sabes sin duda lo que has enseñado a cada cuantejo y la reacción del cuantejo, pero no de qué tipo de cuantejo se trata. Pero por fin llegamos al final del proceso – el momento en el que hablamos por la noche por teléfono, sabiendo que la línea telefónica puede estar pinchada, con lo que tenemos que ser cuidadosos con la información que compartimos.

"Al primer cuantejo le enseñé una zanahoria", me dices tú.

"*Buena elección*", respondo yo. *"Entonces no tienes duda de qué tipo de cuantejo se trata"*

Y tú apuntas en tu libreta: **Cuantejo (1): zanahoriófilo**.

¿Ves lo maravilloso del sistema de Bennet y Brassard? Tú no me has dicho en ningún momento qué resultado has obtenido, simplemente qué experimento has realizado. Si alguien está escuchando la conversación, sabrá que el primer cuantejo es zanahoriófilo o zanahoriófobo, pero no cuál de los dos.
A continuación, me dices: *"Al segundo cuantejo también le enseñé una zanahoria"*.
Yo sé, claro está, que el segundo cuantejo era apiófobo, de modo que no tengo manera de saber cómo reaccionó ante la zanahoria, pero es que **me da exactamente igual**.
"No, este no sirve para nada", respondo. *"Es la verdura equivocada"*. Con lo que el segundo cuantejillo no nos ha servido para nada.
Y tú apuntas en tu libreta:

Cuantejo (1): zanahoriófilo.

"Al tercero le enseñé un apio", sigues tú. Y yo, naturalmente, respondo: *"Buena elección"*, con lo que tú, sabiendo que ese cuantejo rechazó el apio, escribes en tu libreta:

Cuantejo (3): apiófobo.

"Al cuarto le enseñé también un apio", continúas. Pero yo respondo *"No, no vale para nada"*, porque sé que el cuantejo (4) era zanahoriófobo. Así que tú no apuntas nada.

"Al quinto y último le mostré, una vez más, un apio", sigues tú. Y yo respondo *"Bien hecho, entonces éste nos sirve"*… y tú apuntas, sabiendo que se comió el apio:

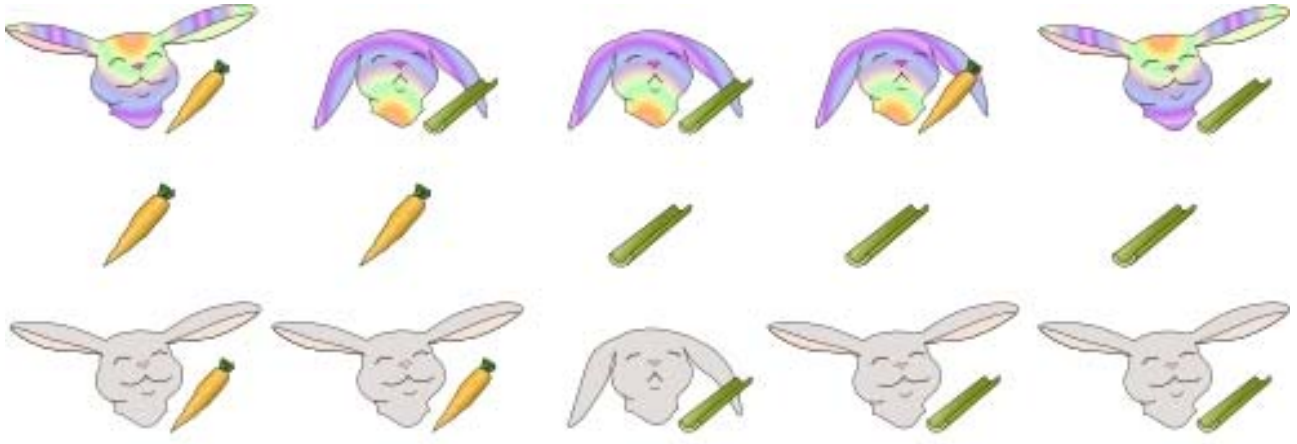
Cuantejo (5): apiófilo.

Y entonces, como último paso, quedamos en la siguiente clave:

los cuantejos -*filos* (zanahoriófilos o apiófilos) son "unos", y los -*fobos* (zanahoriófobos o apiófobos) son "ceros".

Ambos sabemos, entonces, que la clave, compuesta de tres dígitos, correspondientes con los tres cuantejos que nos han valido, es **101**. *Y nadie que esté escuchando nuestra conversación tiene manera alguna de saberlo.*

Aquí tienes el resultado final. Observa cómo sólo utilizamos, para nuestra clave, los cuantejos en los que acertaste en la elección de verdura, e ignoramos aquéllos en los que utilizamos verduras diferentes:



1 - 0 - 1

Ah, pero *¿y si el mensajero que te envió los cuantejos hizo lo mismo que en el ejemplo anterior, reemplazando mis cuantejos por otros idénticos tras enseñarles una verdura para saber cuáles son?* Aquí es donde se pone de manifiesto la verdadera genialidad de este sistema criptográfico.

Sigamos con el mismo ejemplo de arriba y los mismos cuantejos, y supongamos que tú realizas exactamente las mismas elecciones que antes. El mensajero **es esta vez un espía** de los enemigos, abre la caja número 1, y se encuentra con un adorable cuantejo octarino. Pero él, igual que tú, no sabe qué verdura debe enseñarle… *tiene que elegir una al azar*.

Supongamos que le muestra, por ejemplo, una zanahoria. El cuantejo (1), que es zanahoriófilo, se la come con fruición, se vuelve gris y se echa a dormir, con lo que al espía ya no le sirve. Pero el espía, que no es tonto, prepara un cuantejo zanahoriófilo y octarino, lo mete en la caja y te la envía. Cuando tú abres la caja, sucede exactamente lo mismo que en el ejemplo de arriba: le enseñas una zanahoria, se la come, etc. En este caso, todo ha sucedido en tu casa igual que sucedió cuando no había espía, y no tienes manera de saber que alguien ha interceptado nuestro cuantejo.
Pero –y ésta es la clave del asunto– *esto sólo ha sucedido porque el espía ha acertado en la elección al azar de la verdura*.

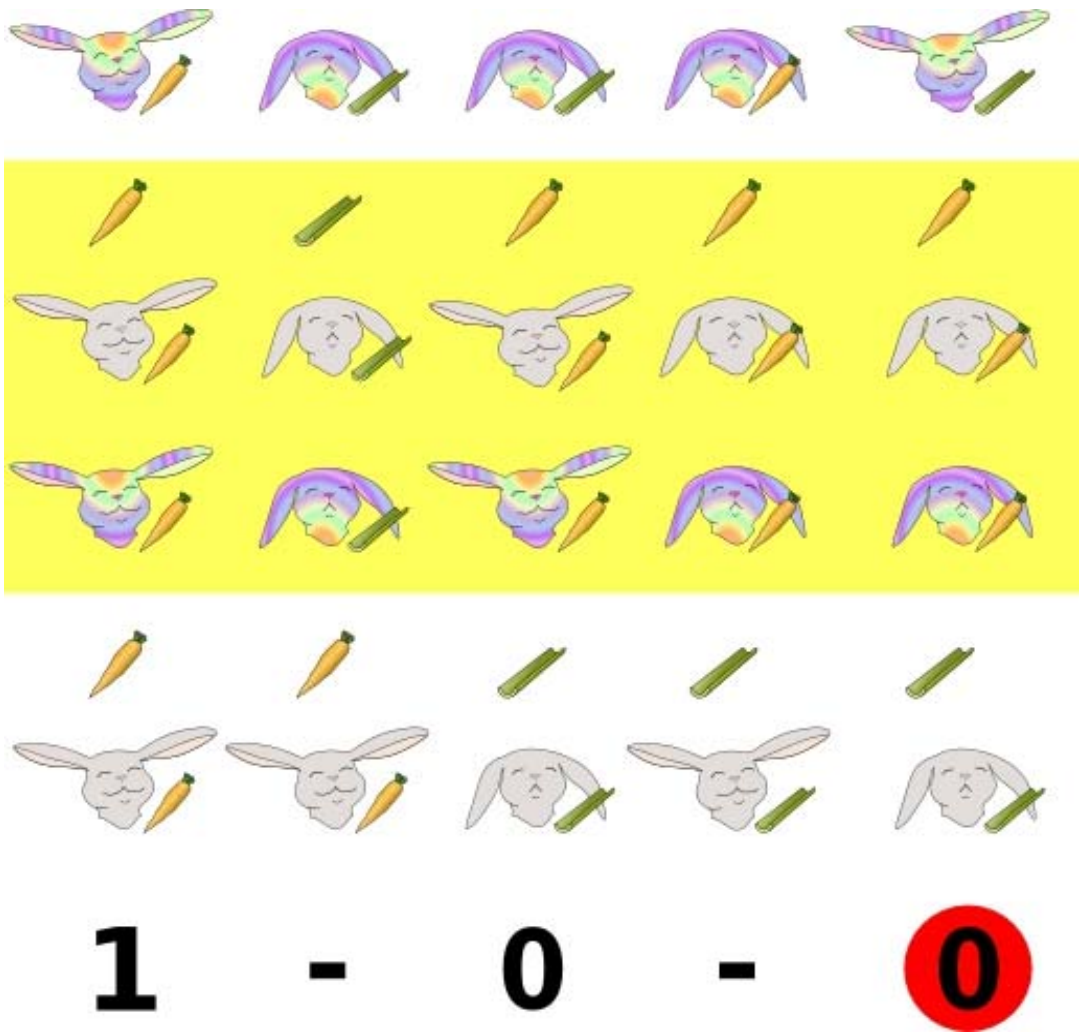
Lo que haga el espía con los cuantejos (2) y (4) es irrelevante, porque cuando me digas la verdura que has escogido en cada caso te diré que no nos sirve e ignoraremos esos cuantejos, que no pasarán a formar parte de nuestra clave privada, pero para seguir con nuestro ejemplo, imaginemos que acierta en ambos casos en la elección de la verdura, con lo que te envía cuantejos idénticos a los míos. Lo importante es qué sucede en los cuantejos que sí vamos a acabar utilizando, el (3) y el (5).

Supongamos que al cuantejo (3) el espía le muestra una zanahoria. Aquí el espía ha cometido un error con la verdura (algo que sucederá un 50% de las veces, claro). El cuantejo (3) era apiófobo, con lo que reaccionará al azar ante la zanahoria – supongamos que se la come. Entonces, el espía prepara un cuantejo octarino zanahoriófilo, *¡algo diferente de lo que envié yo!*

Esto no significa que, necesariamente, detectemos el problema. Cuando ese cuantejo "falsificado" te llegue, tú harás lo mismo de antes: le presentarás un apio. Pero el cuantejo falso es zanahoriófilo, con lo que un 50% de las veces se comerá el apio que le ofreces, y el otro 50% de las veces lo rechazará. Si lo rechaza, entonces habrá sucedido exactamente lo mismo que cuando no había espía y no podremos saber que algo malo ha sucedido, pero si se lo come, el espía se habrá delatado.

Supongamos que el espía tiene suerte y el cuantejo rechaza, muy triste, el apio que le ofreces. Apuntarás en tu libreta exactamente el mismo dato de antes, cuando no había espía. Finalmente, supongamos que al quinto cuantejo el mensajero espía le ofrece una zanahoria (una vez más, un error, pues el cuantejo es apiófilo). El cuantejo rechaza la zanahoria, con lo que el espía te envía un cuantejo octarino zanahoriófobo… y cuando tú lo recibes, le presentas un apio. Pero esta vez el espía tiene mala suerte: el cuantejo falso, zanahoriófobo, se pone a llorar y no se come el apio, con lo que apuntas **[(5) apio: lo ha rechazado]**. En este caso algo ha cambiado respecto al caso en el que no había espía, y esto será el talón de Aquiles de la estrategia del espía, como veremos en un momento.

Aquí tienes la recapitulación de lo que ha sucedido, con la interferencia del espía encuadrada en amarillo. Se ha marcado en rojo el dígito de la clave que no coincide con el que se obtuvo antes de la aparición del espía:



Nuestra conversación telefónica sería exactamente igual que antes y, si no hacemos nada que no hiciéramos entonces, no habría manera de detectar al espía. Como verás, el único caso en el que algo ha cambiado en tus observaciones a causa de la interferencia del espía es el quinto cuantejo (en el caso anterior se comió el apio, como debe ser, pero esta vez lo ha rechazado)… pero eso no es algo que nos digamos por teléfono. Tú seguirás diciendo que le mostraste un apio, y yo responderé *"Excelente, buena elección"*. Sin embargo, yo consideraré ese dígito de la clave un 1 (pues el cuantejo (5) era apiófilo), mientras que tú considerarás que es un 0 (puesto que tu cuantejo, que era falso, no se comió el apio). Mi clave es 101, como antes, pero tú crees que es 100, debido a la injerencia del maldito enemigo. El último dígito, como está marcado arriba, no coincide en nuestras claves.

Pero existen maneras sencillas de que nos demos cuenta, simplemente teniendo un poco de cuidado. La más sencilla de todas es ésta: una vez acaba nuestra conversación telefónica y **antes de enviar información secreta** te envío un mensaje cifrado de prueba, como por ejemplo: "*¿Hay algún espía escuchando esto?*"

Pero yo encripto el mensaje con la clave "101"… y tú tratas de descifrarlo con una **clave incorrecta**. En vez de obtener el mensaje correcto, recibirás un sinsentido parcial o total, por ejemplo "*¿Hsy slgún espís escuchsndo esto?*" Automáticamente sabrás que alguien ha interferido el mensaje, me llamas por teléfono, me dices que la clave no vale y empezamos todo el proceso otra vez, con una empresa de mensajería más de fiar.

Naturalmente, puedes pensar que es posible que el espía tenga suerte todas las veces. Al fin y al cabo, para que nos demos cuenta de que un cuantejo fue interceptado, tiene que tener mala suerte al elegir la verdura (50% de las veces), y además yo tengo que elegir la verdura correcta (un 50% de las veces), con lo que, en media, sólo uno de cada cuatro cuantejos será susceptible de ser revelado como uno falso. Y en nuestro ejemplo así ha sido, más o menos: un error detectable en cinco cuantejos.

Pero la solución es muy fácil: no usamos cinco cuantejos, **usamos cien**. Por mucha suerte que tenga el individuo, la probabilidad de que *absolutamente ninguno* de los cuantejos que modifica sean detectados es de un 75% por cuantejo, es decir, para cien cuantejos, 0,75100 en este caso. Sí, *¡elevado a cien!* ¿Quieres más seguridad que eso?

La segunda manera, un poco más elaborada, es que no empleemos todos los cuantejos en los que coinciden nuestras verduras para la clave, sino que **sacrifiquemos unos cuantos para comparar resultados**. Si, por ejemplo, usamos un total de 1000 cuantejos, de los cuales nos resultan útiles 500, podemos dejar 100 de ellos como prueba, y emplear los otros 400 (que siguen siendo secretos) como clave. De los 100 que compartimos abiertamente, si no hay espía, coincidirán todos –con lo cual los hemos descartado simplemente para estar seguros, pero podemos usar el resto con confianza–, mientras que si hay espía, unos 25 de esos 100 no coincidirán entre sí, con lo que sabremos que hay un espía y tendremos que volver a empezar. En cuanto alguno de los dígitos que compartamos sea "rojo", como en el dibujo de arriba, sabemos que los enemigos están al acecho.

Como ves, el protocolo BB84 no hace uso del entrelazamiento como el E91, pero sí del principio de incertidumbre – con él, podemos estar seguros con una probabilidad aplastante, si usamos los suficientes cuantejos, de que nadie ha interferido la comunicación de nuestra clave. Y, como siempre, no se trata de un sistema absolutamente seguro, porque existe la posibilidad –por baja que sea– de que alguien haya tenido suerte al interceptar cuantejos. Pero ningún sistema criptográfico es seguro al 100%.

Vamos con los aspectos más teóricos de todo el asunto, porque la base es la misma que con los cuantejos.
En primer lugar, la clave de los cuantejos zanahoriófilos, apiófobos y demás es que hemos usado estados cuánticos **incompatibles entre sí**: se trata de autoestados de las variables "amor por las zanahorias" y "amor por el apio".
En el caso de los sistemas reales de criptografía cuántica, como he dicho al principio, se utilizan fotones. En el caso de los fotones se emplean autoestados de la polarización, por ejemplo, polarización vertical u horizontal (equivalente a zanahoriófilo y zanahoriófobo), y polarización sudeste-noroeste o sudoeste-nordeste (equivalente a apiófilo y apiófobo).

Dos pares de estados perpendiculares entre sí, de modo que si realizas la prueba "incorrecta" (apio para un cuantejo al que le importan las zanahorias o al revés, polarización vertical-horizontal para un fotón polarizado sudoeste-nordeste, etc.) existe un 50% de probabilidad de un resultado u otro, ya que se trata de una superposición de estados. En segundo lugar, las limitaciones reales hacen que estos sistemas –como cualquier sistema criptográfico, por otro lado– no sean perfectos. Si tú y yo nos comunicamos la clave enviando fotones polarizados a través de un cable de fibra óptica, **es casi imposible que absolutamente todos los fotones que te envío te lleguen bien**, incluso si no hay espía.

Por lo tanto, si seguimos un criterio tan radical como el del ejemplo de arriba (si un solo resultado es imposible, suponemos que hay un espía), nunca nos pondríamos de acuerdo en la clave, pues siempre va a llegarte una señal con algo de ruido, aunque no haya espía. Pero, si aceptamos cierto nivel de inconsistencia en los resultados, *¿en qué punto sabemos si hay un espía, y cómo de seguros estamos?*

Además, **en la realidad es casi imposible enviar fotones uno a uno**: suelen enviarse cortos "chorros" de fotones en el mismo estado de polarización, y es imposible saber cuántos van a salir en cada uno exactamente. Alguien puede detectar un solo fotón del chorro –disminuyendo muy ligeramente la intensidad del chorro, pero dejando varios fotones en él–, y así realizar una observación sobre él sin que ni tú ni yo seamos capaces de saber que alguien ha interceptado nuestra comunicación.

Pero, como digo, ningún sistema criptográfico es inviolable. Con una calidad de la señal muy buena y muy pocos fotones por cada pulso, es posible conseguir niveles de seguridad muy altos.

De hecho estas cosas no son elucubraciones de un puñado de científicos locos, sino que la criptografía cuántica se emplea en la realidad y existen incluso empresas que venden sistemas comerciales de encriptación por estos protocolos.
En 2006 se envió una clave empleando pares de fotones entrelazados –es decir, el protocolo E91 de Ekert– a través del aire entre las islas de La Palma y Tenerife, a lo largo de nada más y nada menos que 144 kilómetros. El mismo año se realizó un experimento empleando el protocolo BB84 de Bennet y Brassard, a través de un cable de fibra óptica de 148,7 km. Y se han empleado comunicaciones con criptografía cuántica para enviar datos electorales en Suiza, datos bancarios en Austria, etc. No es barato, pero ya está funcionando – y no sería posible sin la cuántica.

Finalmente, una de las limitaciones inherentes a los sistemas como el de la imagen es que no vale cualquier cable de fibra óptica. En las conexiones "normales", la señal se amplifica en varios puntos de la conexión, ya que se atenúa según avanza por el cable. Pero en el caso de la comunicación encriptada como hemos descrito, la **amplificación no puede producirse**, porque sería detectada en el otro extremo como un "espía". Con lo que no se han logrado comunicaciones a enormes distancias (aunque 148 km no está nada mal), y no vale utilizar los cables de fibra óptica normales: los fotones del mensaje encriptado, al no estar amplificados, serían engullidos por todo el resto de comunicaciones normales –amplificadas.