Introducción a la criptografía cuántica

Sergio Miguéns Iglesias (*sergio@lonyelon.xyz*)
Pablo González Alonso (*pablo.gonzalez.alonso@rai.usc.es*)

ABSTRACT

Se propone hacer una breve introducción a la criptografía cuántica, su historia, funcionamiento, aplicaciones y perspectivas de futuro. El *paper* dedicará una especial cantidad de tiempo a explicar los conceptos físicos que sirven de base para esta, por ser estos fundamentales para entenderla. Al final del documento se darán, también, unas breves conclusiones con la opinión de los autores sobre el tema de estudio.

Este paper va dirigido a informáticos, por lo que tener conocimientos de criptografía y teoría de la complejidad computacional es altamente recomendable antes de leerlo. Por el contrario, no se requieren conocimientos físicos más allá de los básicos para comprender el presente texto, aunque estos son recomendables.

I. Índice de contenidos

II. Introducción

La criptografía cuántica es la ciencia que aplica los principios físicos de la mecánica cuántica para fines criptográficos. La información cifrada mediante algoritmos criptográficos cuánticos es físicamente imposible de recuperar sin conocer la clave de encriptación, permitiendo un nivel de seguridad mucho mayor a cualquiera de nuestros algoritmos actuales, ya que para romper un cifrado cuántico no sólo haría falta un ordenador potentísimo, si no violar varios principios físicos. Dado que esto es imposible, la criptografía cuántica se alza como un medio extremadamente seguro de comunicación.

La necesidad de este tipo de métodos criptográficos nace de la inminente amenaza que los ordenadores cuánticos suponen para la criptografía moderna. Este tipo de máquinas supondrán no sólo un gran avance en capacidad de cómputo frente a las actuales, sino que además podrán ejecutar algoritmos como el algoritmo de Shor [11], capaz de factorizar números en tiempo polinómico $O((\log N)^2(\log\log N)(\log\log\log N))$. Esta capacidad supondrá la caída de los algoritmos de cifrado asimétrico actuales (*RSA*, *ECDSA*… etc) que basan su seguridad en la dificultad $O(n!)$ del proceso de factorización.

Antes de continuar cabe aclarar un común malentendido: la criptografía cuántica no es criptografía exclusiva para ordenadores cuánticos, esta también puede ser ejecutada por nuestros equipos actuales añadiendo el hardware necesario para ello ya que, como veremos, emplea métodos cuánticos para transportar la información, pero la información en sí puede ser (y es) binaria.

En este documento primero se explicarán los principios físicos sobre los que se sustenta la criptografía cuántica. Tras eso, se hará un breve repaso de la historia de la misma y sus aplicaciones actuales para, después de comentar sus perspectivas de futuro, dar unas conclusiones incluyendo la opinión de los autores sobre este campo. Al final del documento se adjunta una bibliografía con todos los *papers* y libros empleados para la realización de este trabajo.

A. Objetivos de este paper

Se pretende en estas páginas hacer un reporte completo sobre la criptografía cuántica que no se detenga demasiado en los detalles, pero que de una visión general de esta al lector. No es el objetivo de los autores hacer un libro de texto que toque todos los temas en profundidad, como tampoco lo es hacer un breve resumen que no explique casi nada de lo mencionado y cite tres o cuatro puntos clave. El objetivo es claro: que un lector sin muchos conocimientos en este campo pueda terminar de leerlo entendiendo las ideas generales de la criptografía cuántica y sus aplicaciones, tanto presentes como futuras, sin demasiados problemas.

III. Bases físicas de la criptografía cuántica

Mientras que la criptografía clásica utiliza leyes probabilísticas y matemáticas para cifrar la información, la criptografía cuántica utiliza principios de la física como el principio de incertidumbre de Heisenberg para asegurarla, por lo que entender dichos principios es fundamental para poder comprender su funcionamiento. A lo largo de esta sección se estudiarán los principales principios físicos detrás de los métodos criptográficos cuánticos. El lector que quiera profundizar más puede consultar el libro "The Feynman Lectures on Physics" [7].

A. La mecánica cuántica: partículas, ondas e incertidumbre

A nivel fundamental, nuestro universo está compuesto por unidades discretas llamadas cuantos a partir de las cuales se vuelve indivisible. Toda la materia y la energía que nos rodea está compuesta por ellos. Estas unidades mínimas son, que sepamos actualmente, las partículas del modelo estándar de la física.

Estas partículas cuánticas se rigen por unos principios y leyes especiales, aquellos estudiados por la mecánica cuántica. La idea física más importante para entender la criptografía cuántica es la superposición de estados. Esta rige que una partícula cuántica, antes de ser observada, se encuentra en una superposición de todos sus posibles estados definida por su función de onda. Una vez se observa la partícula (interactuando con ella de cualquier manera), sucede un colapso de la función de onda, lo que fuerza la partícula a un estado concreto en vez de la superposición anterior (*Imagen 1*).

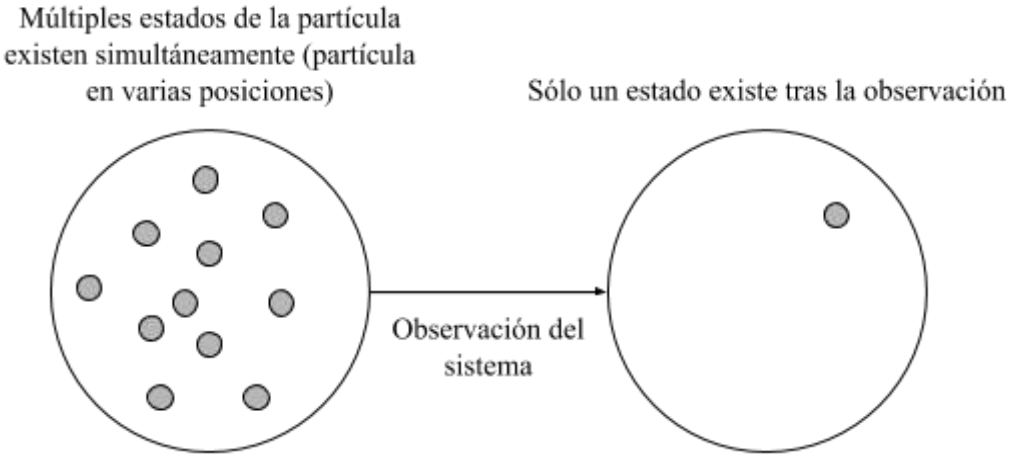

Figura 1: colapso del estado del sistema tras observación.

Tras el colapso del estado es imposible recuperar el conjunto de estados superpuestos antes de la observación. Este fenómeno recibe el nombre de teorema de no clonación [13]. Esto sucede porque, como es natural, para clonar un sistema cuántico es necesario primero medirlo para conocer su estado, pero el medir el sistema provocará un colapso de la función de onda y alterará la realidad de forma que sólo exista uno de los estados superpuestos. Por lo tanto, sólo podemos clonar el estado final y no el original, porque nunca podemos llegar a conocer el primero.

B. El cuanto de la luz: fotones y polarización

La superposición anterior se aplica también a la luz, cuyo cuanto es el fotón. La luz tiene una propiedad muy interesante derivada de ser una onda electromagnética: la polarización. La polarización de la luz es la "inclinación"[1] que esta tiene. Diferentes rayos de luz tienen inclinaciones diferentes. En la *imagen 2* se pueden observar dos ejemplos de luz polarizada: luz polarizada verticalmente y luz polarizada horizontalmente.

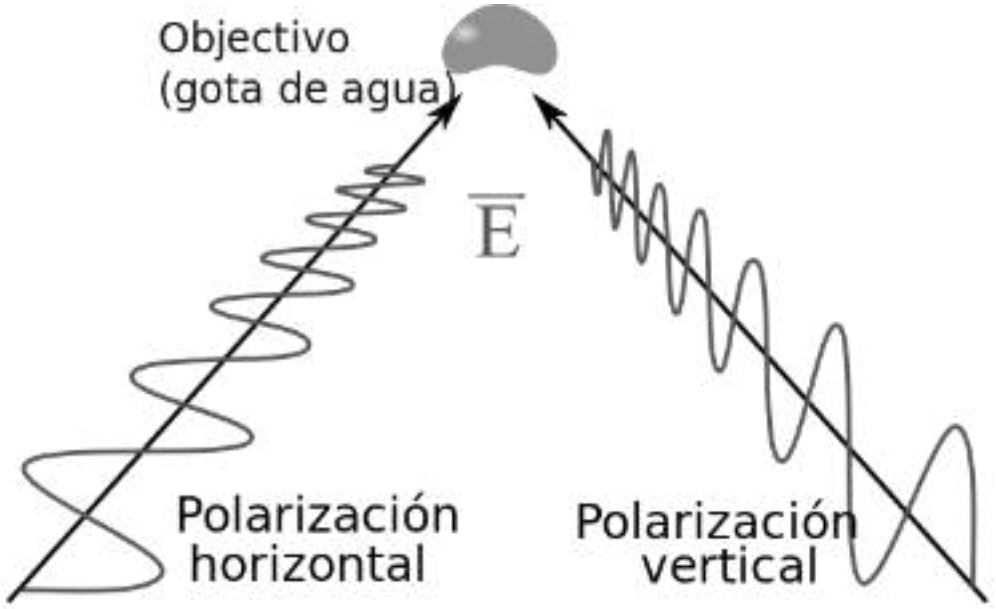

Figura 2: Ejemplos de luz polarizada, fuente: Wikipedia

Cuando la luz es emitida por una fuente luminosa, esta se encuentra en una superposición de todos sus posibles polarizaciones (por ser esta una partícula cuántica). Observar la luz hará que su estado colapse en solo una polarización. Lo interesante es que podemos elegir la polarización a la que colapsará el fotón con un filtro polarizador. Supongamos el siguiente caso (mostrado en la Imagen 3): en el instante (0) la luz se encuentra en una superposición de todas sus posibles polarizaciones (cada línea representa una dirección de polarización). Una vez la onda se encuentra con una lente polarizada vertical en (1) su dirección de polarización es forzada a ser la vertical para poder pasar por la lente, lo que resulta en (2). Dicho ejemplo puede ser observado en la Imagen 3.

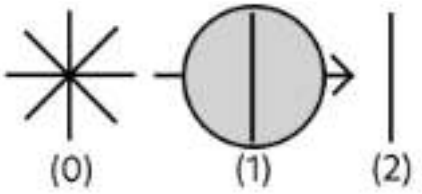

Figura 3: ejemplo de lente polarizada

[1] También existe la polarización circular, pero esta no es relevante para el tema a tratar.

Si la luz salida en (2) pasara ahora por un filtro vertical de nuevo, continuaría con su actual polarización sin problemas, pero la situación sería muy distinta para cualquier otro filtro. Supongamos, por ejemplo, que ahora ese fotón intentara pasar por un filtro polarizado horizontalmente (o en su defecto de forma perpendicular a su polarización actual), dado que la polarización del fotón sería totalmente perpendicular a la de la lente, este tendría un 0% de probabilidades de cruzar (nótese la negrita, hablaremos de probabilidades a continuación). Dicho caso puede ser observado en la Imagen 4.

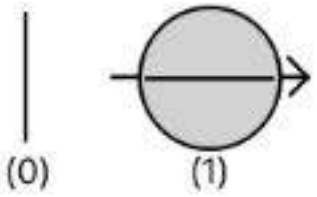

Figura 4: La luz no puede pasar por el filtro

Sin embargo cuando las polarizaciones de la luz y el filtro coinciden, esta si puede pasar a través de él (100% de probabilidad):

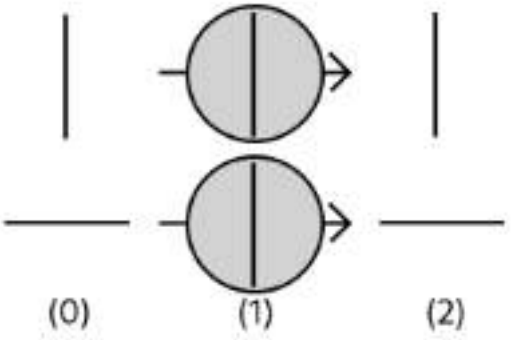

Figura 5: La luz puede pasar los filtros.

Lo que se puede ver es que la probabilidad de que un fotón cruce un filtro polarizado es $cos^2(\theta)$, donde θ es ángulo que forma las polarizaciones de la luz y el filtro. La probabilidad de que el fotón no pase es $sin^2(\theta)$, deducible a partir de la identidad trigonométrica pitagórica.

C. Entrelazamiento cuántico

Además de estar o no polarizados, los fotones pueden estar vinculados entre sí. Esto es una propiedad de todas las partículas cuánticas llamada entrelazamiento cuántico. Dos partículas entrelazadas cuánticamente comparten su estado, de forma que si observamos una, podemos conocer con un 100% de certidumbre el estado de la otra independientemente de la distancia que las separe.

En el caso de los fotones, nos interesa su capacidad para compartir polarizaciones. Si dos fotones están entrelazados y medimos la polarización de uno de ellos, podemos saber que la polarización del otro será igual cuando la midamos.

No se comentará más sobre esta propiedad física, pues con lo anterior es suficiente para entender el resto del documento, aunque se plantea la siguiente pregunta: dado que el entrelazamiento funciona de esa forma ¿No viola eso la relatividad especial de Einstein al estar transmitiendo información de forma instantánea cuando el límite de transmisión de información debería ser la velocidad de la luz?.

IV. Historia de la Criptografía Cuántica

La idea de la criptografía cuántica vio la luz a principios de la década de 1970. Propuesta por *Stephen Wiesner* como "codificación cuántica conjugada", fue rechazada originalmente por la organización *IEEE*, pero acabó siendo publicada en 1983 en *SIGACT News* [13]. La idea inicial proponía almacenar o transmitir dos mensajes codificándolos en dos "observables conjugados", es decir, dos cantidades físicas que podían ser medidas a posteriori. Dichos observables eran la polarización lineal y circular de los fotones, de forma que cualquiera de los dos, pero no ambos (debido al entrelazamiento cuántico), se podrían recibir y decodificar.

Imagen 1: Stephen Wisner jugando al Go. Fuente: mpiwg-berlin

En 1979, *Gilles Brassard* y *Charles H. Bennett* descubrieron cómo aplicar los descubrimientos de *Wiesner* al darse cuenta de que los fotones "estaban destinados" (en sus propias palabras) a transmitir la información y no a almacenarla. Basándose en esto, en 1984 propusieron un método de comunicación segura, considerado el primer protocolo de criptografía cuántica, el **BB84**. Su finalidad era la distribución de claves, permitiendo a dos usuarios generar una clave aleatoria y compartirla de forma segura, dando así luz al primer algoritmo de compartición de claves cuánticas (*QKD*). Para ello, utilizando una serie de filtros de polarización y escogiendo un ángulo con respecto a la vertical (0, 45, 90 o 135 grados), se enviaban fotones preparados en diferentes estados de polarización. Los fotones polarizados en ángulos de 0 y 45 grados representaban el valor binario 0, mientras que los otros dos representaban el valor 1. De esta forma, se podía codificar una secuencia de bits, que se usaría como clave para realizar la comunicación segura mediante un algoritmo clásico.

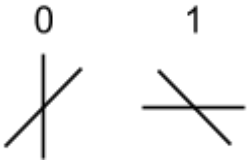

Figura 6: Polarizaciones posibles de la luz en BB84

Este método de comunicación es seguro ya que el receptor de los fotones (o un intruso intentando interceptarlos) ha de disponer de las bases correctas para leerlos. Si por ejemplo se enviara un "1_2" (fotón con polarización de 90º) y el receptor empleara un filtro pensado para leer "0_2"s (45º), este tendría un 27,59%[2] de posibilidades de leer correctamente el bit. Es fácil ver como la probabilidad de acertar en la lectura de fotones para los que no se dispone de la base correcta tiende a 0 con este método, dado que esta decrece exponencialmente:

$$p(n_{fotones}) = p(1_{fotón})^{n_{fotones}}$$

Imagen 2: De derecha a izquierda:Charles Bennett, Gilles Brassard y Peter Shor. Fuente: BBVA

En 1991, *Ekert* diseñó el **protocolo E91** (también llamado EPR) que involucraba las propiedades del entrelazamiento cuántico para la generación de claves [6]. En dicho protocolo, a diferencia del BB84, no existían estados de polarización predefinidos, generando los estados en el momento de la medición. Para ello, a la hora de generar la clave, tanto emisor como receptor comparten varios pares entrelazados de fotones que, al ser medidos, obtienen siempre la misma polarización. De esta forma, se conseguía un método de criptografía puramente cuántico.

Pongamos por ejemplo que Alice quiere mandar un bit a Bob. La polarización vertical de un fotón significará 1, mientras que la horizontal, 0. Lo único que tiene que hacer Alice en este caso es generar dos fotones entrelazados, mandar uno a Bob y, cuando este lo reciba, hacer pasar su propio fotón por un polarizador (en este caso vertical para enviar un 1). Nada más Alice haga pasar su fotón no polarizado por el filtro aplicándole una polarización, el fotón de Bob se polarizará en la misma dirección instantáneamente gracias al entrelazamiento, permitiéndole leer la información que Bob quería transmitirle (el dígito 1).

Este método es resistente a ataques ya que la información no existe durante el proceso de compartición de fotones, solo cuando se realiza la lectura. La única forma de acceder a esta información sería privar a Bob de ella, pues hacer copias de fotones no polarizados es imposible (apartado III).

[2] $\cos^2(45-90)=\cos^2(-45)=0{,}2759$

Imagen 3: Artur Ekert, padre del algoritmo E91. Fuente: Wikipedia

En 1992, *Bennett* creó el protocolo **B92**, teniendo un funcionamiento similar al BB84, pero simplificando el proceso al solo utilizar dos direcciones no ortogonales entre sí para polarizar [1].

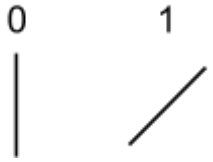

Figura 7: Ejemplo de polarizaciones posibles de la luz en B92

V. Aplicaciones de la criptografía cuántica

Hoy en día la criptografía cuántica tiene una gran variedad de usos, desde el cifrado de comunicaciones hasta la verificación de la geolocalización. En esta sección se describen algunas de sus más destacadas de

A. Comunicaciones seguras

Aunque este sea el uso más básico de la criptografía, no deja de ser el más importante y el motivo por el que esta fue inventada. Como ya se ha explicado anteriormente, mediante la polarización de fotones se pueden cifrar datos binarios y, por lo tanto, se puede enviar un mensaje. El medio utilizado para realizar dicha comunicación son los cables de fibra óptica, los cuales están diseñados especialmente para transmitir luz. Usando la criptografía cuántica se puede realizar tanto comunicaciones en tiempo real (utilizando como un algoritmo de cifrado de flujo) como para enviar mensajes cifrados o, principalmente, realizar intercambios de claves (*QKD*). Esta última aplicación es la principal hoy en día para esta criptografía y será explicada en más detalle a continuación

B. Distribución de claves cuánticas (QKD)

Realizar una comunicación cifrada utilizando únicamente criptografía cuántica conlleva un gran costo y es extremadamente difícil, ya que generar pares únicos de fotones entrelazados como en el algoritmo E91 no es una tarea sencilla. Debido a esto, es preferible utilizar la criptografía cuántica únicamente para realizar el intercambio de claves y realizar la comunicación utilizando un protocolo de cifrado simétrico convencional.

Debido a que los cables de fibra óptica están limitados a una distancia de 200 Km (distancia que se está viendo aumentada recientemente, consultar el subapartado *IV.A*), tanto la comunicación como el intercambio de claves está limitado a dicha distancia. Esta limitación se ha eliminado recientemente gracias al uso del satélite *Micius* [10], el cual tiene una órbita sincrónica a la del sol, por lo que pasa por cada parte de la superficie de la tierra cada día a la misma hora. Para usarlo, una estación terrestre envía la clave que va a ser utilizada para establecer una comunicación cifrada, y, cuando el satélite pasa sobre la estación al que está destinada la clave, se la envía. Además de aumentar el rango de comunicación, también se aumenta la seguridad debido a que, como es natural, es más difícil hackear un satélite en órbita que un cable de fibra óptica.

C. Comunicación entre pares que se desconfían mutuamente

A la hora de establecer una comunicación utilizando criptografía cuántica es imposible saber si el receptor y el emisor del mensaje son quienes dicen ser y, por lo tanto, no tienen motivos para confiar uno en el otro. Para poder realizar comunicaciones entre usuarios que desconfían el uno del otro, se utiliza el protocolo de lanzamiento de monedas, también llamado *quantum coin flipping* [5] inventado por el venezolano Manuel Blum [3] en 1981. Los pasos a seguir para llevar a cabo este proceso son los siguientes:

1. El primer usuario (Alice) escoge una base aleatoria (conjunto de polarizaciones que va a usar eligiendo entre horizontales, diagonales y verticales) y una secuencia de *qubits* aleatorios que cifra con dicha base.
2. Dichos *qubits* cifrados son enviados al segundo usuario (Bob) y este escoge una secuencia de bases de lectura aleatorias para cada fotón. Según la base utilizada, los fotones leídos son almacenados en dos tablas (una para los leídos en diagonal y otra para los rectilíneos).
3. A partir del contenido de dichas tablas, Bob intenta adivinar la secuencia de bases empleadas por Alice y le envía dicha secuencia.
4. Alice comprueba si la secuencia recibida coincide con la generada y envía a Bob su secuencia original, estableciendo la comunicación segura. Si la secuencia es incorrecta, Bob "pierde" el juego.
5. Por último, Bob compara la secuencia recibida con el contenido de sus tablas, si coinciden, significa que ambos usuarios son veraces, ya que Alice está empleando la base prometida.

Este protocolo impide que se produzcan ataques *man-in-the-middle* ya que, en caso de que un tercero intentase leer u obtener información sobre la transmisión, esto es, observar los fotones, provocaría que se alterase inevitablemente la polarización de los mismos (debido a que el sistema ha sido observado, recordemos el principio de no clonación), hecho que sería detectable en los pasos cuatro y cinco.

D. Criptografía cuántica basada en la posición

Un receptor (Alice) puede demostrar su identidad empleando criptografía basada en posición [4]. Para hacer esto se requieren, como mínimo, dos emisores (en este caso Bob y Chuck). El proceso comienza con Alice revelando su posición, a lo que Bob y Cuck responden enviando un *qubit* (fotón) y una base de *BB84*. Es necesario haber cifrado información en ese fotón con la base que se le envía a Alice (mediante los métodos que ya hemos estudiado) y que tanto Bob como Chuck conozcan la información que se ha cifrado, por lo que ambos han de estar en contacto. El fotón y la base se envían de tal forma que la recepción por parte de Alice de ambas sea simultánea, empleando para ello las coordenadas que ella compartió.

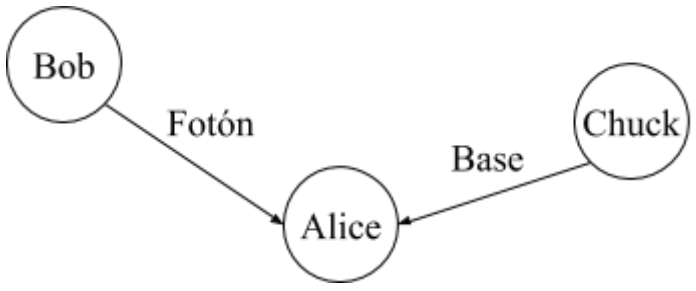

Figura 8: Bob y Chuck envían el fotón y la base a la posición Alice

Una vez Alice ha recibido ambos datos, lee la información contenida en el fotón empleando la base proporcionada por Chuck. Una vez tiene esta información, se la devuelve

a ambos y estos comprueban si es correcta y si Alice realizó el proceso en un tiempo esperable (basándose en su supuesta posición).

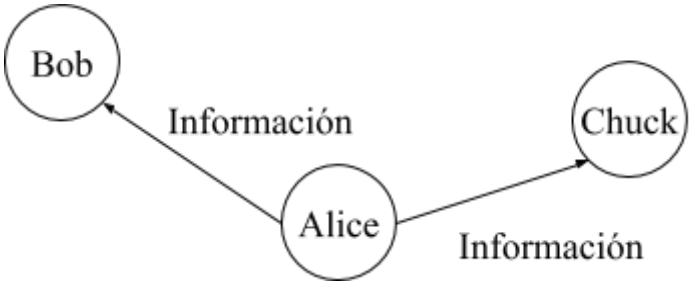

Figura 9: Alice devuelve la información leída a los emisores

Si el proceso termina satisfactoriamente, Bob y Chuck pueden ahora autenticar a Alice basándose en su posición, pues esta ha quedado demostrada. Si Alice intenta, por ejemplo, mentir con su posición haciéndose pasar por otra persona, el retardo causado (ya sea positivo si Alice está lejos o negativo si está cerca de los emisores), así como la diferencia de tiempo entre la recepción del mensaje por parte de ambos delatarán la mentira.

Este proceso sería imposible empleando métodos criptográficos tradicionales, ya que sería vulnerable a ataques *man-in-the-middle*, pero empleando criptografía cuántica este problema se solventa. Pongámonos en los siguientes supuestos en los que dos atacantes (Denny y Evan) se coordinan para atacar el proceso:

- Denny y Evan quieren simplemente interceptar las comunicaciones entre Alice y los dos emisores. Para eso, Denny ha de leer el fotón que Bob ha enviado a Alice, pero al hacerlo sin tener la base necesaria (*Imagen X*), altera su información, delatando que ha habido un ataque. En caso de que Denny espere a recibir la base que Evan ha interceptado (*Imagen X*), quedará delatada por el tiempo que este proceso le ha llevado.

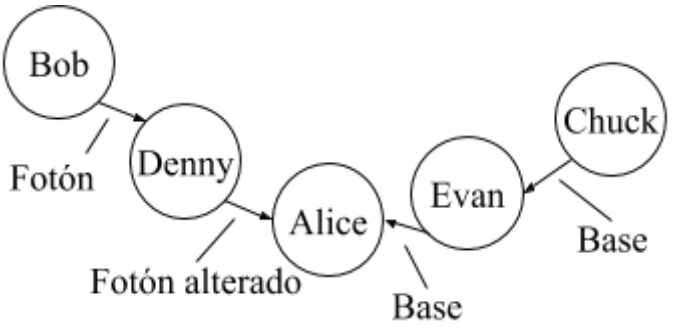

Figura 10: Denny y Evan interceptan la comunicación pero no comparten la base

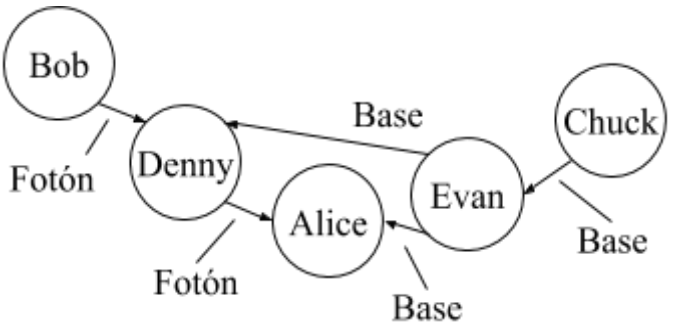

Figura 11: Denny y Evan interceptan la comunicación y comparten la base

- Denny y Evan quieren hacerse pasar por Alice. En este caso se organizan al igual que antes, pero ahora no es necesario enviarle la información de vuelta. Denny y Evan se encuentran entonces en la misma situación que antes: si no comparten la base Denny le enviará información errónea a Bob y Chuck, y si la comparten, los tiempos de envío no corresponderán con los esperados.

Es obvio que para este sistema, a mayor número de fotones enviados y cantidad de emisores capaces de verificar los datos, mejor.

VI. Perspectivas de futuro

El futuro de la criptografía cuántica es, a día de hoy, incierto. Esta incertidumbre se debe al hecho de que, dada su situación actual y a pesar de que esta es posible, no se sabe a ciencia cierta si es deseable o no. A lo largo de esta sección se darán tanto puntos a favor como puntos en contra de la misma, que permitirán al lector sacar sus propias conclusiones.

A. Canal de transmisión

A favor de la criptografía cuántica está el hecho de que el canal necesario para compartir los fotones polarizados ya existe a día de hoy: los cables de fibra óptica. Estos cables están cada vez más instalados en más y más casas a lo largo del mundo, y permitirían hacer una transición bastante sencilla en caso de que esta se vuelva necesaria en un futuro cercano. La única limitación que existe en este aspecto es la longitud de los cables, limitación que cada vez es más insignificante gracias a la gran cantidad de avances que está habiendo en esta materia (recientemente se ha logrado superar la barrera de los 500km de distancia [8]).

Otros medios alternativos de transmisión de claves ya han sido elaborados, tales como el ya mencionado satélite *MICIUS*, capaz de transmitir fotones desde el espacio [10].

B. Lectura de datos: hardware especializado

La aparición de hardware como tarjetas de red cuánticas necesario para obtener las claves tampoco está lejos, recordemos que una vez se ha descifrado la información esta pasa a estar en un formato digital perfectamente compatible con los ordenadores actuales. La traducción de la información contenida en los fotones a señales eléctricas sería trivial, pero las cosas no son tan sencillas cuando se habla de la emisión y recepción de estas partículas.

Una tarjeta de red de este estilo tendría que poder emitir fotones individuales (uno por bit cifrado). Si bien esto no es imposible a día de hoy, sigue siendo algo extremadamente difícil de hacer [14]. Estas tarjetas de red deberían también tener velocidades de emisión iguales o cuya diferencia sea ínfima. Pequeñas diferencias entre la velocidad de emisión y receptor de fotones entre dispositivos podrían suponer pérdidas de información que inutilizarían todo el proceso. En las imágenes siguientes se muestra tanto un sensor (barra negra) cuya velocidad de lectura coincide con la de emisión de la fuente, como otro en el cual estas velocidades no coinciden y la lectura falla.

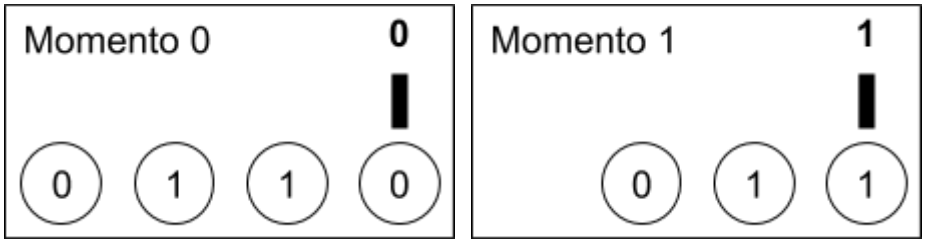

Figura 12: Proceso de lectura correcto: igual velocidad de emisión y lectura

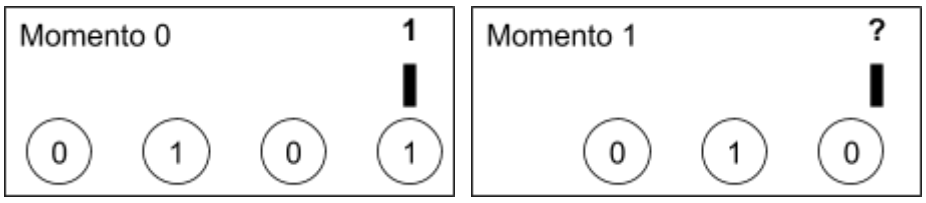

Figura 13: Proceso de lectura fallido: velocidad de emisión y lectura diferentes

C. ¿Es realmente necesaria?

Es preciso plantearse si la criptografía cuántica es realmente necesaria. La respuesta obvia a esta pregunta es un rotundo sí, pero una examinación en profundidad puede hacer que se dude de este hecho.

El motivo principal para dudar es que los ordenadores cuánticos, que se sepa en el presente, no serán un peligro para todos los algoritmos de los que disponemos. Algoritmos como *AES* seguirán siendo seguros en la era cuántica siempre que se usen claves de un tamaño adecuado (≥256 bits). Por otro lado, seguirá siendo increíblemente difícil lograr colisiones en las funciones de *hash* actuales tales como *SHA*. Todos los algoritmos criptográficos que son (o se cree que son) resistentes a ataques con ordenadores cuánticos son llamados algoritmos post-cuánticos o *quantum-safe* [2]. Esta categoría engloba tanto a algoritmos convencionales como a algoritmos cuánticos.

El desarrollo de nuevos algoritmos post-cuánticos es una rama teórica de la informática muy reciente y prometedora, cuyo avance está siendo realizado en paralelo con la criptografía cuántica.

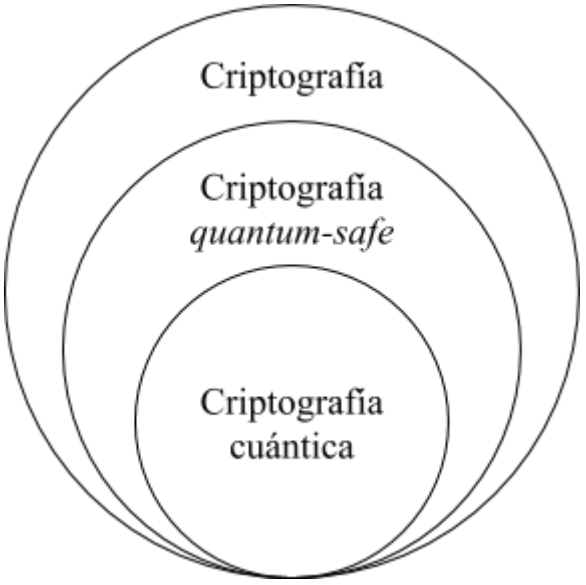

Figura 14: Tipos de criptografía

D. Otras consideraciones

La criptografía cuántica tiene problemas más allá de los expuestos. Uno de ellos es la dificultad para manejar comunicaciones con gran cantidad de pares. Esto sucede porque con

los algoritmos actuales, para cada par de usuarios se ha de crear una clave cuántica (conjunto de polarizadores). Esto no es una tarea sencilla en absoluto y puede terminar con usuarios que manejan cientos de claves cuánticas.

Otro problema es la falta de algoritmos puramente cuánticos. Hoy en día, prácticamente toda la criptografía cuántica se basa en *QKD* (intercambio de claves cuánticas), donde lo que se cifra son las claves, no la información que se desea transmitir. Esto quiere decir que para que un algoritmo criptográfico cuántico sea útil, este ha de sustentarse sobre un algoritmo convencional, por ejemplo usando RSA (o mejor aún, cualquier método basado en curvas elípticas) para cifrar la comunicación y, por ejemplo, B92 para compartir las claves.

Un último problema relacionado con el anterior es que, de por sí, la criptografía cuántica no permite realizar una de las tareas básicas de los algoritmos criptográficos asimétricos modernos: la autenticación de los usuarios. Esta capacidad es la que permite que hoy en día tengamos, por ejemplo, certificados digitales, lo que nos permite comprobar la identidad del emisor de los mensajes. Incluso algoritmos que pretenden solucionar la comunicación entre usuarios que desconfían entre ellos como el *quantum coin-flipping* son, según estudios recientes [9], extremadamente difíciles de implementar.

VIII. Conclusiones

En base a lo visto a lo largo de este texto se puede concluir que la criptografía cuántica es una ciencia que, si bien está aún en desarrollo, ya ha hecho grandes avances y ha logrado progresar desde una rama teórica de la criptografía a una experimental con aplicaciones tan diversas como interesantes. Tanto los avances tecnológicos de los últimos años (sensores y emisores de luz ultra precisos, cables de fibra óptica, tecnología de satélites… etc) como los avances teóricos nos acercan cada vez más a un futuro donde estas técnicas criptográficas puedan ser empleadas de forma común.

Por supuesto, también se han de tener en cuenta los problemas que la criptografía cuántica presenta ya discutidos en el apartado anterior. La opinión de los autores es que todas esas consideraciones harán que muy posiblemente, por lo menos en un futuro cercano, la criptografía cuántica se use sólo con fines militares, pues incluso si llegara el día en el que los ordenadores cuánticos funcionales fueran una realidad, la criptografía post-cuántica podría solucionar la mayoría de problemas que surjan sin la necesidad de modificar el hardware de nuestros actuales *PC*s.

En todo caso, se llegue ésta a emplear o no en un futuro, la criptografía cuántica es una rama de altísimo interés intelectual y una demostración de cómo la ciencia teórica, y concretamente la física cuántica, puede terminar teniendo aplicaciones reales más allá de las pizarras de los laboratorios.

A. Posfacio

Quedaron fuera de este texto, por limitaciones de tiempo y espacio, apartados que hablasen más en detalle de los ordenadores cuánticos y la criptografía post-cuántica, temas muy relacionados con el actual y que realmente aportarían una mejor visión del mismo si fueran explorados en mayor profundidad.

También quedaron fuera del documento la mayoría de expresiones matemáticas y detalles físicos detrás de la criptografía cuántica en un intento de hacer el texto más comprensible, tanto para los lectores como para los escritores del mismo. Esta omisión de información puede ser compensada con la bibliografía que se deja a continuación, donde se listan todas las referencias empleadas a lo largo del texto. Estas referencias son, en muchos casos, más cercanas a libros de texto que a *papers* científicos, y sirven para profundizar en los diversos temas tratados. Los autores recomiendan leer, especialmente, los *papers* de Manuel Blum, que a parte de contener información de altísimo interés, son increíblemente divertidos.

IX. Bibliografía

[1] Bennett, Charles H. “Quantum Cryptography Using Any Two Nonorthogonal States.” *Physical Review Letters*, vol. 68, no. 21, 1992, pp. 3121–3124., doi:10.1103/physrevlett.68.3121.

[2] Bernstein, Daniel J. “Introduction to Post-Quantum Cryptography.” *Post-Quantum Cryptography*, 2009, pp. 1–14., doi:10.1007/978-3-540-88702-7_1.

[3] Blum, Manuel. “Coin Flipping by Telephone a Protocol for Solving Impossible Problems.” *ACM SIGACT News*, vol. 15, no. 1, 1983, pp. 23–27., doi:10.1145/1008908.1008911.

[4] Buhrman, Harry, et al. “Position-Based Quantum Cryptography: Impossibility and Constructions.” *SIAM Journal on Computing*, vol. 43, no. 1, 2014, pp. 150–178., doi:10.1137/130913687.

[5] Döscher, C., y M. Keyl. “An Introduction To Quantum Coin Tossing.” *Fluctuation and Noise Letters*, vol. 02, no. 04, 2002, doi:10.1142/s0219477502000944.

[6] Ekert, Artur K. “Quantum Cryptography Based on Bell’s Theorem.” *Physical Review Letters*, vol. 67, no. 6, 1991, pp. 661–663., doi:10.1103/physrevlett.67.661.

[7] Feynman, Richard P., et al. *The Feynman Lectures on Physics*. Basic Books, 2010. Capítulos "1.1. Atomic mechanics", "1.8. The uncertainty principle" y "17.4. Polarized light".

[8] Lucamarini, M., et al. “Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters.” *Nature*, vol. 557, no. 7705, 2018, pp. 400–403., doi:10.1038/s41586-018-0066-6.

[9] Miller, Carl A. “The Impossibility of Efficient Quantum Weak Coin Flipping.” *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, 2020, doi:10.1145/3357713.3384276.

[10] Sheng-Kai , Liao, et al. “Satellite-Relayed Intercontinental Quantum Network.” *Physical Review Letters*, vol. 120, 19 Jan. 2018, doi:10.1103/PhysRevLett.120.030501.

[11] Shor, P.w. “Algorithms for Quantum Computation: Discrete Logarithms and Factoring.” *Proceedings 35th Annual Symposium on Foundations of Computer Science*, 1994, doi:10.1109/sfcs.1994.365700.

[12] Wiesner, Stephen. “Conjugate Coding.” *ACM SIGACT News*, vol. 15, no. 1, 1983, pp. 78–88., doi:10.1145/1008908.1008920.

[13] Wootters, W. K., y W. H. Zurek. “A Single Quantum Cannot Be Cloned.” *Nature*, vol. 299, no. 5886, 1982, pp. 802–803., doi:10.1038/299802a0.

[14] Zao, Yi. “Quantum Cryptography in Real-Life Applications: Assumptions and Security.” *Universidad De Toronto*, 2009.