Universidad Internacional de la Rioja (UNIR)

Escuela Superior de Ingeniería y Tecnología

Máster en Computación Cuántica

Mecánica Cuántica (CCFF)

Protocolos cuánticos de seguridad y cifrado

Actividad de la asignatura

presentada por:

Miguel Aliende García,

Daniel Casado Faulí,

Sergio Jiménez Fernández,

Jorge Parra Palacios

Profesor: Jenaro Gallego Gómez

Fecha: 8 de Enero de 2024

Índice de contenidos

Índice de figuras

Resumen

Este trabajo se enfoca en los protocolos de transmisión de clave cuántica (QKD), un área fundamental en la criptografía cuántica. Se expondrán algunos de los protocolos más importantes e interesantes. Para garantizar la confidencialidad de las comunicaciones, estos protocolos se basan en los principios fundamentales de la mecánica cuántica, como el entrelazamiento cuántico, teorema de no clonación, entre otros. La comprensión de estos protocolos contribuye a la creación de nuevos sistemas seguros en el campo de la criptografía cuántica.

Palabras Clave: criptografía cuántica, clave, protocolos, seguridad.

Abstract

This paper focuses on quantum key distribution protocols (QKD), a fundamental area in quantum cryptography. Some of the most important and interresting protocols will be presented. To garantee the confidentiality of communications, these protcols are based on the fundamentals principles of quantum mechanics, such as quantum entanglement, the non-cloning theorem, among others. The undestanding of these protocols contributes to the creation of new secure systems in the field of quantum cryptography.

Palabras Clave: quantum cryptography, key, protocol, security

1. Introducción

A lo largo de la historia, se ha buscado proteger la confidencialidad de la información a través de sistemas de encriptado. Uno de los primeros sistemas de encriptado es el conocido como César, se dice que lo usaba Julio Cesar en sus campañas.

Durante muchos años se han ingeniado numerosos mecanismos para cifrar mensajes, pero durante la segunda guerra mundial se dio un cambio de paradigma. Se inventaron maquinas de cálculo que permitían cifrar y descifrar mensajes de manera rápida y segura, la maquina de cifrado más famosa posiblemente sea la maquina alemana Enigma. Posteriormente, surgieron los primeros algoritmos de criptografía simétrica (una sola clave) y asimétrica (una clave para cifrar y otra para descifrar). La seguridad de estos protocolos está basada en la dificultad computacional de resolver ciertos problemas matemáticos como la factorización de números naturales o calcular la intersección de una recta con una elipse en poco tiempo.

El desarrollo de la teoría cuántica, supuso la aparición de algoritmos cuánticos que pueden ser capaces de resolver estos problemas matemáticos en tiempo polinómico si se ejecutan en una maquina cuántica lo suficientemente potente. Puesto que con esta premisa la mayoría de sistemas de encriptado podrían verse comprometidos, la criptografía cuántica surge para contrarrestar esta posible vulnerabilidad. La gran ventaja de los algoritmos de encriptación cuántica es que su seguridad no depende de la capacidad de resolver un problema, si no que se basa en principios fundamentales de la mecánica cuántica como el principio de incertidumbre y el entrelazamiento cuántico entre otros.

La motivación que trataremos de afrontar con este documento es ser capaces de distinguir los diferentes protocolos de distribución de clave cuántica (QKD), que precisamente, toman ventaja de los conceptos de la criptografía cuántica.

Para cumplir con dicho objetivo, recurriremos a la clasificación entre protocolos *Prepare & Measure* (PM) y *Entanglement Based* (EB). Partiendo de esta división, comenzaremos por definir los protocolos de cada tipo (Capítulo 2). Una vez definidos, para poder compararlos, tomaremos un enfoque en dos niveles (Capítulo 3): un primer nivel con dos partes con las diferencias entre los protocolos (Sección 3.1); y, en el segundo nivel, dar una comparación más general entre las dos clases de protocolo (PM y EB) (Sección 3.2).

2. Protocolos QDK

Durante este capítulo expondremos los protocolos de distribución de clave cuántica más importantes. Explicaremos el funcionamiento de estos protocolos, así como sus fortalezas y debilidades para después compararlos.

2.1. *Prepare & Measure*

En esta sección presentaremos los protocolos del tipo PM, que son los primeros protocolos QDK. Estos protocolos se centrar en medir estados en superposición.

2.1.1. Protocolo BB84

El protocolo BB84, desarrollado por Bennett y Brassard (1984), fue el primer protocolo de distribución de clave cuántica y además uno de los más influyentes, ya que muchos protocolos de distribución de clave cuánticas son mejoras del BB84. Este protocolo utiliza principios de la mecánica cuántica como el principio de incertidumbre (Heisenberg, 1927) y el teorema de no clonación (Wootters y Zurek, 1982) para maximizar la seguridad frente a escuchas.

El escenario de este protocolo entre dos interlocutores, Alice (emisor) y Bob (receptor) utiliza dos canales de comunicación, uno cuántico, generalmente unidireccional (de Alice a Bob), y otro clásico, bidireccional y público. Como se explica detalladamente en el apéndice A.1, en este protocolos y en el resto de protocolos PM, los qubits son los estados de polarización de los fotones.

Funcionamiento BB84

En esta sección explicaremos de una manera sencilla y sin entrar en detalles complejos como funciona el protocolo BB84. Este protocolo tiene 4 fases bien definidas: distribución de clave, reconciliación de base, corrección de errores y amplificación de seguridad.

1. Distribución de clave

1. Alice genera una cadena aleatoria de N bits y los codifica asignando la base rectilínea ($\{|0\rangle, |1\rangle\}$) al bit 0 y la base diagonal ($\{|+\rangle, |-\rangle\}$) al bit 1 . Utilizando la misma nomenclatura que A.1, la secuencia 010011 quedaría:

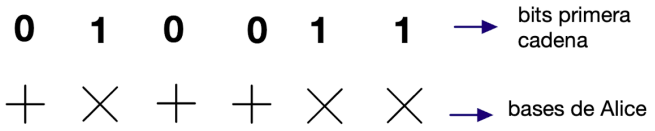


Figura 2.1: Fase 1 BB84. Fuente: Elaboración Propia.

2. Alice vuelve a generar otra cadena aleatoria de N bits. A cada uno de estos bits le asigna un estado propio de la base que ha elegido para cada bit en la cadena anterior. Por ejemplo si el primer bit es un 1 y en la cadena anterior teníamos un 0 (base rectilínea) a ese 1 le vamos a asignar el estado vertical, o en notación de Dirac $|1\rangle$, si hubiésemos tenido un 0, le asignaríamos el estado $|0\rangle$. De esta manera, si la segunda cadena aleatoria es 100101, le asignamos estos estados:

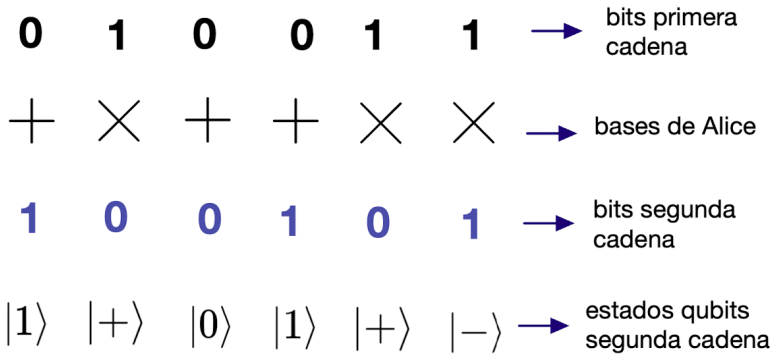


Figura 2.2: Fase 2 BB84. Fuente: Elaboración Propia.

3. Alice le envía a Bob esos qubits por el canal cuántico.

4. Bob genera una cadena de N bits aleatorios, y al igual que Alice, le asocia a cada bit una base rectilínea si es un 0 o una base diagonal si es un 1. Si la cadena aleatoria de Bob es 000101, entonces el resultado se muestra en la Figura 2.3.

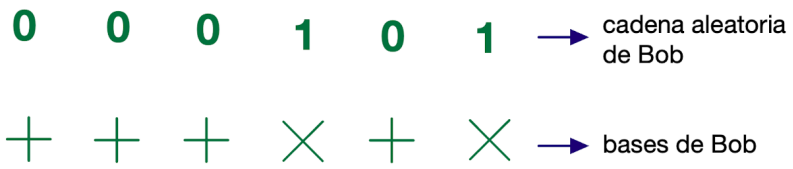


Figura 2.3: Fase 3 BB84. Fuente: Elaboración Propia.

5. Ahora Bob va a medir los qubits enviados por Alice utilizando estas bases aleatorias, por lo tanto, el resultado de la medición será correcto solo en aquellos qubits que la base de Alice y Bob coinciden, para nuestro el ejemplo este sería el resultado de la medición de Bob:

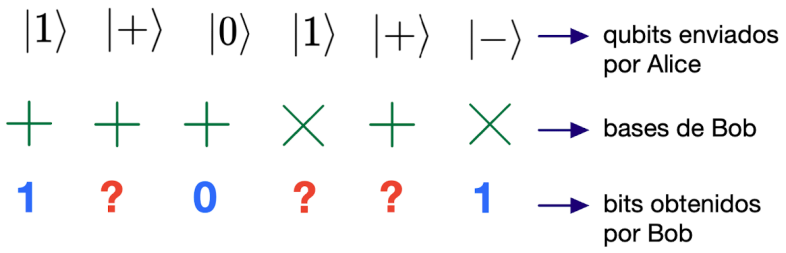


Figura 2.4: Fase 4 BB84. Fuente: Elaboración Propia.

2. Reconciliación de bases Una vez Bob ha recibido y medido los qubits de Alice, lo que deben hacer es poner en común las bases y Alice le dirá a Bob cuales de los qubits ha medido correctamente, para ello siguen los siguientes pasos:

1. Bob le dice a Alice públicamente la serie de bases que ha utilizado.
2. Alice le responde a Bob públicamente con las bases que fueron elegidas correctamente, y por lo tanto los bits medidos con esas bases será iguales para ambos. Los podemos ver en la figura 2.5:
3. En este punto, tanto Alice como Bob saben cuales son aquellos bits que tienen en común y esta será su calve, en este caso "101"

En este punto, ya se ha intercambiado la clave utilizando sistemas de información cuánticos. Hemos visto que Alice y Bob en ningún momento se intercambian las cadenas

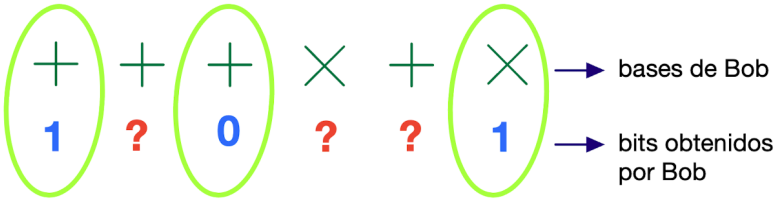


Figura 2.5: Fase 5 BB84. Fuente: Elaboración Propia.

de bits, únicamente las bases.

3. Corrección de errores En este punto ya se ha intercambiado la clave de manera segura, pero antes debemos asegurarnos de que no haya habido errores debido a la presencia de ruido, o como ya veremos más adelante, errores provocados por la presencia de "espias".

1. Alice envía a Bob una lista de posiciones junto a su valor, para estimar la tasa de error en la comunicación con Bob.

2. Si la tasa de error supera cierto umbral, la comunicación se aborta y se tiene que repetir todo el proceso. Por el contrario si la tasa de error es inferior a dicho umbral, el intercambio de la clave ha sido un existo.

4. Amplificación de privacidad Una de las características más importantes de este tipo de protocolos, es que son capaces de detectar si un intruso ha interceptado los mensajes de Alice y luego los reenvía a Bob.

Ahora tenemos el mismo escenario que al principio, pero vamos a introducir a un intruso que intercepta los mensajes de Alice y se los reenvía a Bob, llamémosle Eve. Eve va a interceptar los qubits que Alice envía a Bob y los va a medir con una secuencia de bases aleatoria.

La gran ventaja que de los protocolos de distribución de clave cuántica es que utilizan principios de la mecánica cuántica para maximizar la seguridad. En este caso, Eve, al no tener la secuencia de bases con las que ha codificado Alice, al hacer la medición, el resultado obtenido no tiene porque ser correcto, sólo si se da la casualidad de que las bases aleatorias de Alice y Eve coinciden. No sólo eso, además, debido al principio de incertidumbre y el principio de no clonación, Eve modificará el estado de los qubits que le ha enviado Alice,

y por lo tanto, los qubits que le reenvía a Bob no son los mismos que ha emitido Alice.

De está manera, en el punto 2.1.1 Alice y Bob se darán cuenta de que la tasa de error es alta debido a la presencia de Eve y abortarán el protocolo.

Características del protocolo BB84

En esta sección recopilaremos y describiremos las características del protocolo BB84, puntos débiles, fuertes, etc.

Se trata de un protocolo, que como hemos visto, utiliza fotones para para representar los bits de información, esto supone una ventaja respecto a otros protocolos que utilizan sistemas cuánticos más complejos. Utiliza 4 estados cuánticos distintos representados en dos bases ortonormales.

Es el protocolo más sencillo en lo que al proceso de comunicación se refiere. Si bien utiliza propiedades cuánticas para detectar espías de manera eficiente, es vulnerable a otro tipo de ataques activos.

Como otros protocolos similares, se enfrenta a retos como el comportamiento en presencia de ruido, incluyendo un mecanismo de detección de errores y a la aparición de efectos como atenuación, dispersión, etc al aumentar la distancia de comunicación.

2.1.2. Protocolo B92

Fue propuesto por primera vez de la mano de Bennett (1992) y el principal objetivo era tratar de simplificar el protocolo BB84 (en cuyo diseño y propuesta también participó). También es conocido por algunos autores como protocolo "Two-States" (Gisin et al., 2002).

De forma muy resumida, este protocolo permite el intercambio de claves de manera ciertamente segura empleando, en lugar de cuatro estados (dos pares de estados ortogonales), únicamente dos estados no ortogonales.

La idea clave de la que parte Bennett (1992) proviene de otro trabajo del que fue partícipe (Bennett et al., 1992), y se trata de una equivalencia entre el uso de una pareja EPR entrelazada para la comunicación y el uso de estados no entrelazados y no ortogonales.

De este modo, el protocolo B92 escuda la clave bajo la afirmación de que, si no se

perturba uno de los dos estados no ortogonales es imposible extraer información (Bennett, 1992). Dicho de otro modo, se basa en la imposibilidad de decidir entre dos estados no ortogonales sin ningún tipo de interacción con los qubits.

Para este, se requiere, del mismo modo que en el protocolo BB84, de un canal clásico y un canal cuántico, además de, claro está, de un emisor (Alice) y un receptor (Bob).

Funcionamiento B92

Veamos a continuación como aprovecha los estados no ortogonales para la distribución de claves. En esta subsección, explicaremos las fases de distribución y de reconciliación de base, sin pararnos en la corrección de errores ni amplificación de seguridad, puesto que las mismas técnicas aplicadas en BB84, pueden ser usadas también en B92.

Para esta explicación, aunque en el paper original de Bennett (1992) se utilicen estados genéricos ($|u_0\rangle$ y $|u_1\rangle$), utilizaremos un enfoque basado en fotones así como un ejemplo.

1. Distribución de clave

1. Alice crea de forma aleatoria una cadena de N bits que utilizará para decidir que polarización aplicar a los fotones que enviará a Bob. Por ejemplo, si el valor de un bit es 1 aplicará la polarización diagonal $+45°$ (estado $|+\rangle$), mientras que si el valor es 0 aplicará la polarización horizontal H (estado $|0\rangle$) (Elboukhari et al., 2010). Nótese en la Figura 2.6 que no son ortogonales.

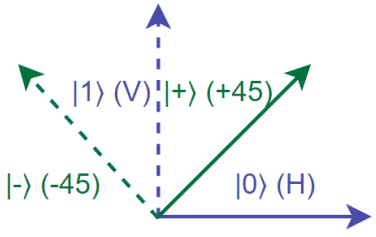


Figura 2.6: Representación vectorial de estados no ortogonales. Fuente: Elaboración Propia.

   Siguiendo el ejemplo, si la cadena de Alice es 101100, la sucesión de estados a enviar será $|+\rangle, |0\rangle, |+\rangle, |+\rangle, |0\rangle, |0\rangle$.

2. Alice le envía a Bob dicha sucesión mediante el canal cuántico.

3. Bob también creará de forma aleatoria una cadena de N bits que le servirá para decir en que bases medirá los fotones recibidos. De modo que, volviendo al ejemplo, si el valor de un bit es 0, aplicará una medición rectilínea (base $\{|0\rangle, |1\rangle\}$, $+$), y si el valor es 1, la medición será diagonal (base $\{|+\rangle, |-\rangle\}$, $\times$) (Elboukhari et al., 2010).

   Continuando con el ejemplo, si la cadena de Bob es 000101, la sucesión de mediciones será $+, +, +, \times, +, \times$.

4. Entonces Bob puede proceder a medir los fotones que Alice le envió en la base que le indique su cadena. En la Figura 2.7 podemos ver los posibles valores que Bob puede obtener de cada medición en función de la base que le toque y del valor que Alice codificó en los fotones.

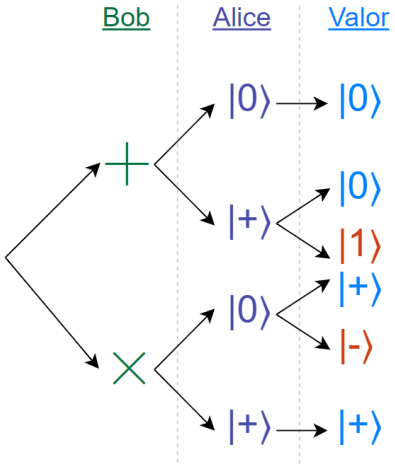


Figura 2.7: Árbol de posibilidades para las posibles salidas de la medición de los fotones. Fuente: Elaboración Propia.

Volviendo a nuestro ejemplo, si Alice envió la secuencia $|+\rangle, |0\rangle, |+\rangle, |+\rangle, |0\rangle, |0\rangle$ y Bob resultó que medía siguiendo el orden $+, +, +, \times, +, \times$, un posible resultado de la medición sería $|1\rangle, |0\rangle, |1\rangle, |+\rangle, |0\rangle, |-\rangle$.

2. Reconciliación de bases Una vez que Bob ha medido todos los fotones que Alice le envió, es momento de que reconcilien bases. Pero, a diferencia del protocolo BB84, no se comunican las bases directamente, pues, dado que el *vocabulario* de la clave se sabe que es $|0\rangle$ y $|+\rangle$, si se dijeran las bases por el canal clásico, Eve podría deducir directamente los valores de esta.

El proceso entonces es el siguiente:

1. Bob se pone en contacto con Alice a través del canal clásico y le dice en cuales de las posiciones de la cadena que le mandó obtuvo como resultado $|1\rangle$ o $|-\rangle$.

2. Una vez Bob ha terminado su comunicación, se descartan el resto de estados.

   Una pregunta que nos puede surgir llegados a este punto es, ¿por qué se quedan con los que tuvieron valores que ni pertenecían al vocabulario inicial? Y la respuesta está en que, el objetivo principal de estos algoritmos es buscar una correlación entre los valores medidos (los cuánticos) y la información a enviar (clásica).

   Supongamos entonces que utilizamos los valores del *vocabulario* y hagamos la labor de Bob en este punto: ¿qué valor me habrá querido mandar Alice sabiendo que he obtenido un $|0\rangle$?, es decir, ¿que correlación hay entre el valor $|0\rangle$ y el valor que me quiso mandar Alice?.

   Apoyándonos en la Figura 2.7, la respuesta es que no lo podemos saber, porque existen dos posibles caminos para llegar al estado $|0\rangle$ (y lo mismo con el $|+\rangle$). Mientras que, si nos hacemos la misma pregunta pero con el valor $|1\rangle$, si que puedo saber con total seguridad que Alice me quiso mandar un $|+\rangle$, aunque eso implique que haya escogido una base errónea en la medición. Esto se suele expresar como $Alice = 1 - Bob$.

3. Finalmente, la clave obtenida con este protocolo serían los valores correspondientes con el mapeo definido. En nuestro ejemplo, nos tendríamos que quedar con los valores en las posiciones 1, 3 y 6, que, por lo que explicamos anteriormente, podemos interpretar (véase de nuevo Figura 2.7) que en dichas posiciones Alice quería mandar los estados $|+\rangle, |+\rangle, |0\rangle$, y, de acuerdo con el mapeo inicial, la clave final sería 110.

Como mencionamos anteriormente, el protocolo puede ser extendido con las etapas de reconciliación de la información y amplificación de privacidad, lo que haría que se modificara más la clave final.

Características del protocolo B92

Expongamos ahora algunos puntos fuertes y débiles de este protocolo en concreto. Y es que, su ventaja es reducir el número de estados necesarios para intercambiar información, pasando de cuatro estados (BB84) a solamente dos (no ortogonales).

A priori, este punto fuerte puede verse como una mejora a la hora de interpretar la información que se envía [1]. Pero, si recordamos el funcionamiento del algoritmo, a la hora de traducir estados a bits (véase la Figura 2.7) solo dos de esas seis ramas son realmente útiles (las que desembocan en $|1\rangle$ y en $|+\rangle$). Esto implica una eficiencia relativamente baja en el sentido de generar la clave.

2.1.3. Protocolo de seis estados

El protocolo de seis estados o SSP(*six-state protocol*) propuesto por primera vez por Bruß (1998) y estudiado y analizado posteriormente por Bechmann-Pasquinucci y Gisin (1999), se trata de una generalización del protocolo BB84, descrito en la sección 2.1.1.

El funcionamiento del protocolo es el mismo que el BB84, pero utilizando seis estados en vez de cuatro, en tres bases ortogonales en vez de en dos. En el protocolo BB84 teníamos la base $\{|0\rangle, |1\rangle\}$, con los estados que hemos llamado horizontal y vertical, y la base $\{|+\rangle, |-\rangle\}$, con los estados diagonal y anti-diagonal. La propuesta del protocolo SSP es añadir otros dos estados en una base ortonormal adicional, esta base es $\{|+i\rangle, |-i\rangle\}$. Estos estados representados en la esfera de Bloch quedarían así:

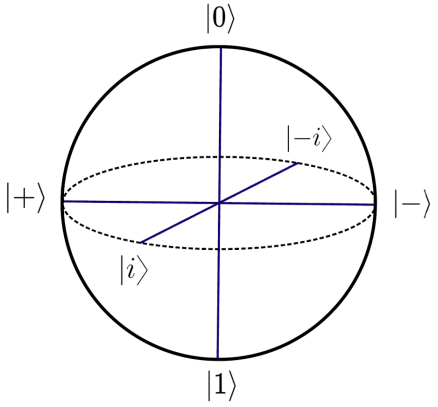


Figura 2.8: Representación esfera de Bloch de estados SSP. Fuente: Elaboración Propia.

Por lo tanto en el protocolo SSP, cuando Alice codifica los qubits, utiliza otra base más que en el BB84. De la misma manera para Bob, realizará las mediciones con tres bases aleatorias.

Respecto a la seguridad de SSP, se ha demostrado que es seguro para tasas de error de

[1] Puesto que en vez de cuatro opciones, simplemente hemos de considerar dos

hasta el 12,7 % (Lo, 2001). Una mejora de este protocolo es usar la técnica de purificación de entrelazamiento bidireccional, lo que hace que SSP sea seguro con tasas de error de hasta el 26,4 % (Gottesman y Lo , 2003). La técnica de purificación de entrelazamiento bidireccional también puede ser aplicada a BB84 y mejora la tasa de error a la que este es seguro.

2.1.4. Protocolo SARG04

Este protocolo surge del riesgo que existe de un tipo de ataques denominados PNS (*photon number splitting attack*) es decir ataques por separación del número de fotones, que hacen vulnerable al protocolo BB84. Este riesgo se da cuando en este protocolo se usan pulsos de láser atenuados (lo que es el uso más práctico), en lugar de envío de fotones individuales. Al trabajar con pulsos atenuados se establecen envíos con un número medio de fotones, algo que permitiría bloquear alguno de ellos y con ello obtener información completa sobre la clave compartida.

El protocolo SARG04, propuesto por vez primera por Scarani, Acin, Ribordy y Gisin en 2004 (Scarani et al., 2004), y surge como modificación del protocolo BB84 de cara a prepararlo para los citados tipos de ataque PNS. En este caso el hardware del protocolo BB84 no cambia, sino que lo hace únicamente el protocolo en una forma diferente para decodificar la información.

Siguiendo para el caso indicado del protocolo BB84 de la figura del intruso denominado Eve, la forma en la cual se puede realizar un ataque consiste en establecer un sistema de conteo de fotones, de manera que si Eve detecta que en el envío de un pulso láser van varios fotones, almacena uno para medirlo y deja que el resto llegue a Bob sin realizar medición. En el caso de que se midiese un solo fotón individual , el pulso quedaría bloqueado, lo cual haría posible conocer la intrusión de Eve.

Una vez indicado el riesgo del protocolo BB84, la modificación del mismo se lleva a cabo a partir de la fase de reconciliación de bases en el canal público, dando lugar así al protocolo SARG04.

Funcionamiento SARG04

La modificación que se introduce en el protocolo BB84 consiste en que en la fase de reconciliación, Alice no revela públicamente la base que ha utilizado sino que anuncia una pareja de estados no ortogonales de los cuatro posibles $\{|0\rangle, |+\rangle\}, \{|0\rangle, |-\rangle\}, \{|1\rangle, |+\rangle\}, \{|1\rangle, |-\rangle\}$.

De forma que uno de los estados de la pareja sea el estado del qubit que ha transmitido. De esta manera solo Alice conoce la base que ha usado para elaborar el estado. Bob llevará a cabo la medida sobre ambos estados, de manera que si solo es compatible con uno de ellos, el bit será válido, anunciando públicamente. De otra manera si es compatible con ambos estados la información se descarta.

Dado que las fases del protocolo se asemejan bastante con los anteriores, condensaremos las etapas de distribución de claves y reconciliación de la información con este ejemplo (Arranz-Díez, 2022):

1. Alice envía el estado $|0\rangle$ y publica la pareja $\{|0\rangle, |+\rangle\}$.

2. En el caso de que Bob mida en la base rectilínea, el resultado será $|0\rangle$. Puesto que $\langle 0|+\rangle = \frac{1}{\sqrt{2}} \neq 0$, este resultado es compatible con el estado $|+\rangle$ y Bob no puede distinguir con seguridad entre los dos.

3. Sin embargo, si Bob mide con la base diagonal puede obtener los dos estados, $|+\rangle$ y $|-\rangle$ con la misma probabilidad, con lo cual es nuevamente compatible con ambos estados del par $\{|0\rangle, |+\rangle\}$, así que se descartaría. Sin embargo si se tiene como resultado $|-\rangle$, como $\langle +|-\rangle = 0$ el estado inicial solo puede ser el $|0\rangle$. En este caso Bob anuncia que cual de los estados es y con ello conoce el bit enviado por Alice.

Características del protocolo SARG04

Como punto fuerte destacaremos que gracias a esta corrección en el protocolo BB84, la seguridad frente a ataques de tipo PNS es mucho más robusta.

Como punto débil los bits en común identificados se reducen a solo el 25 % frente al 50 % que obtiene el BB84, lo cual hace aumentar la seguridad en detrimento de la eficiencia del sistema.

2.2. *Entaglement Based*

Una vez explicados los cuatro protocolos de la clase anterior, pasamos a explicar los protocolos EB, que aprovechan la propiedad cuántica del entrelazamiento.

2.2.1. Protocolo E91

Este debe su nombre a Arthur Ekert, el cual, en el año 1991 y de forma independiente a los desarrollos del BB84 (Gisin et al., 2002), dio con una manera de implementar la distribución cuántica de claves pero con una idea diferente respecto a BB84 (Ekert, 1991).

De hecho, uno de los principales atractivos de este protocolo es que recurre al teorema de Bell (solución de la paradoja EPR, en concreto a la inecuación propuesta por Clauser et al. (1969)) para la detección de intrusos en la conversación.

De forma muy resumida, E91 utiliza permite la comunicación cuántica mediante la medición simultánea de Alice y Bob sobre estados entrelazados, generando así la clave.

Funcionamiento E91

Nuevamente, del mismo modo que los protocolos PM, también necesitamos un canal cuántico y un canal clásico para la implementación. Aunque también es necesario introducir una fuente o central que se encarga de proveer tanto a Alice como a Bob de fotones con estados concretos entrelazados que permitan la comunicación (Nikolina, 2007).

Aunque en el resto de protocolos hemos empleado una explicación basada en fotones, para este caso, utilizaremos el ejemplo expuesto en el propio artículo original. En este se emplean partículas de spin-$\frac{1}{2}$, debido a que tienen ciertas propiedades especiales.

1. Distribución de clave

1. La fuente generará pares de partículas de spin-$\frac{1}{2}$ entrelazadas formando un singlete (*singlet*).

   La peculiaridad del estado singlete es que supone una anti-correlación entre los estados de las partículas. Esto formalmente, en notación de Dirac, se traduce como el

estado:

$$\left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(|\uparrow\downarrow\rangle + |\downarrow\uparrow\rangle\right) \tag{2.1}$$

Notar la correspondencia con uno de los cuatro estados de Bell, resultado del entrelazamiento entre dos partículas.

2. Una vez se han generado todos los entrelazamientos procede a mandar una partícula del par EPR a Alice y la otra a Bob. De este modo, ya tenemos una "conexión virtual", por denominarlo de algún modo.

3. Entonces, Alice y Bob comienzan a realizar mediciones, eligiendo como base de las mediciones una entre tres opciones que cada uno tiene.

   La disposición que propone Ekert en su artículo viene dada por dos conjuntos de ejes $A_i, B_i, \forall i = 1, 2, 3$, de modo que cada eje se define por los ángulos $\phi_1^A = 0, \phi_2^A = \frac{\pi}{4}, \phi_3^A = \frac{\pi}{2}$ y $\phi_1^B = \frac{\pi}{4}, \phi_2^B = \frac{\pi}{2}, \phi_3^B = \frac{3\pi}{4}$. Las bases formadas por estos ejes se puede ver de forma gráfica en la Figura 2.9.

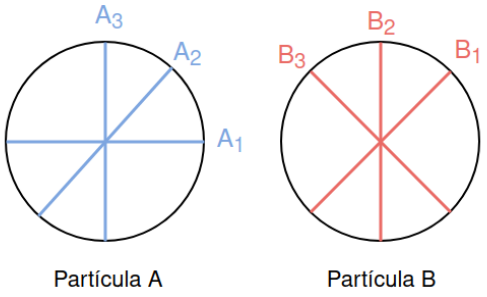


Figura 2.9: Bases A_i y B_i para la medición de las partículas de spin-$\frac{1}{2}$. Fuente: Elaboración Propia.

De este modo, Alice y Bob irán midiendo las partículas eligiendo una base aleatoria entre el conjunto A y B respectivamente, sin establecer ningún acuerdo entre ellos.

2. Reconciliación de bases Una vez ambos han terminado de medir individualmente todas las partículas entrelazadas que le envió la central, es momento de reconciliar las bases.

1. Alice y Bob se comunican a través del canal clásico las bases en las que realizaron las mediciones, generando así dos grupos: (i) las mediciones en las que las bases

coincidían, concretamente los casos (A_3, B_2) y (A_2, B_1), y (ii) mediciones con bases que no coinciden.

2. Entonces, deciden descartar aquellas partículas en las cuales las mediciones no fueron las adecuadas, es decir, aquellos casos en los que uno o ambos participantes utilizaron la base que no correspondía.

3. Finalmente, la clave se formará a partir de la anti-correlación establecida previamente entre los estados de las partículas $|\uparrow\rangle$ y $|\downarrow\rangle$.

Posteriormente, como en el resto de protocolos, tiene cabida la aplicación de diferentes técnicas de reconciliación de la información y amplificación de privacidad.

3. Amplificación de privacidad Llegados a este punto, nos puede surgir una pregunta más que razonable: Si descartamos las mediciones en las bases incorrectas, ¿para qué queremos tres bases?¿no sería mejor quitar una base de cara a la complejidad del protocolo?

La respuesta es que esa base *extra* tiene su función: detectar posibles intrusos mediante la aplicación del teorema de Bell y la desigualdad CHSH Clauser et al. (1969).

El proceso es el siguiente:

1. Alice y Bob comunican mediante el canal clásico los valores obtenidos de las mediciones del segundo grupo, es decir, las que se realizaron de forma incorrecta (involucrando ahora esta base *extra*).

2. Con esta información, calculan una magnitud, denominada S y que, según Clauser et al. (1969), la mecánica cuántica requiere que $S = 2\sqrt{2}$.

3. En función del valor obtenido de S, si se cumple o no el requisito, se puede llegar a la conclusión de que hay alguien perturbando la comunicación, luego, deciden abortar. Si no se da, pueden dar la comunicación como exitosa.

Características del protocolo E91

De nuevo, tratemos de destacar algunas características que supongan puntos fuertes y débiles respecto a este protocolo.

En primer lugar, puesto que se pasa en la propiedad del entrelazamiento, si logramos que las partículas o qubits de Alice y Bob estén máximamente entrelazados, a la hora de medir, los resultados estarán máximamente correlacionados (Renner et al., 2005).

Por tanto, introduciendo una etapa de purificación de entrelazamiento en la central incrementaríamos la eficiencia a la hora de obtener la clave.

Aunque, precisamente el entrelazamiento es una cuchilla de doble filo, ya que, de haber mucho ruido en la comunicación empeoraría la calidad del entrelazamiento. Y, por tanto, perdemos eficiencia a la hora de generar la clave.

2.2.2. Protocolo BBM92

El protocolo BBM92 fue propuesto por Charles H. Bennett, Gilles Brassard y N. David Mermin (Bennett et al., 1992) como extensión a la propuesta de Artur Ekert del protocolo E91, pero dónde se comparten 2 qubits entrelazados en un estado de Bell en vez de transmitir un solo qubit. Este protocolo en concreto fue muy relevante ya que se demostró que un observador externo no podría obtener información sobre los pares EPR distribuidos ya que no hay ninguna información definida previamente a la medición de los estados enviados, y se podría al mismo tiempo detectar posibles escuchas o redireccionamientos de información fácilmente.

Funcionamiento BBM92

Igual que en el protocolo E91, se requerirá de un canal clásico y un canal cuántico para transmitir la información entre el emisor y el receptor, así como la fuente o central que se encarga de proveer tanto a Alice como a Bob con uno de los dos fotones entrelazados del par EPR.

1. Distribución de clave Una de las principales diferencias entre el protocolo E91 y el BBM92 aparece en la distribución de las claves y en las bases utilizadas para las mediciones.

1. Alice y Bob comparten un conjunto N de pares de fotones entrelazados previamente a partir de una entidad central, de manera similar al protocolo E91, en el estado

$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\leftrightarrow\rangle + |\updownarrow\updownarrow\rangle)$ o el estado $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\updownarrow\rangle - |\updownarrow\leftrightarrow\rangle)$ (pudiendo utilizarse dos bases $|x\rangle$ e $|y\rangle$ cuales quiera siempre que sean ortogonales) (Waks et al. , 2002)

2. Alice y Bob escogerán cada uno, de manera aleatoria dos bases complementarias no ortogonales, el conjunto horizontal-vertical (conjunto base $+$) o el conjunto de bases diagonales (conjunto base $\times$), para cada uno de los fotones. Este conjunto de bases diagonales, en nuestro caso, serían las bases:

$$\begin{aligned} |+\rangle &= \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle + |\updownarrow\rangle) \\ |-\rangle &= \frac{1}{\sqrt{2}}(|\leftrightarrow\rangle - |\updownarrow\rangle) \end{aligned} \tag{2.2}$$

2. Reconciliación de bases

1. Alice y Bob se transmiten, a través de un canal clásico, las bases que han escogido para cada medición del conjunto N de fotones.

2. Una vez conocidas las bases escogidas por el otro, Alice y Bob deben de descartar todas aquellas medidas realizadas con bases diferentes, quedándose solo con aquellas que escogieron la misma base (proceso denominado "sifting") (Waks et al. , 2002).

3. Se convierte el resultado de la medición entonces a bits ($\leftrightarrow/|+\rangle = 0$ y $\updownarrow/|-\rangle = 1$). En el caso de que el estado inicial de superposición escogido fuera $|\phi^+\rangle$, ambas bases tienen resultados de medición correlacionados con respecto al estado de superposición inicial:

$$\left|\phi^+\right\rangle = \frac{1}{\sqrt{2}}(|\leftrightarrow\leftrightarrow\rangle + |\updownarrow\updownarrow\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle) \tag{2.3}$$

4. Por lo tanto, se considerará como clave resultante el propio valor de los bits medidos, ya que ambos resultados deberían ser los mismos (aunque posteriormente se revisará esto en la corrección de errores). En el caso de haber utilizado como estado de superposición inicial $|\psi^-\rangle$, tal y como se explicó en el Apartado 2.2.1, al existir una anti-correlación en las medidas, es necesario invertir uno de los bits medidos, por convenio el bit resultado de la medición del receptor, en este caso el de Bob. A esta clave resultante se le denomina la "clave cruda. De esta, solo el 90 % de los bits

se utilizarán como **clave final**, mientras que un 10 % de los bits se utilizarán para detectar y realizar corrección de errores (Erven , 2002).

Se puede ver un esquema resumen de este proceso en la Figura 2.10

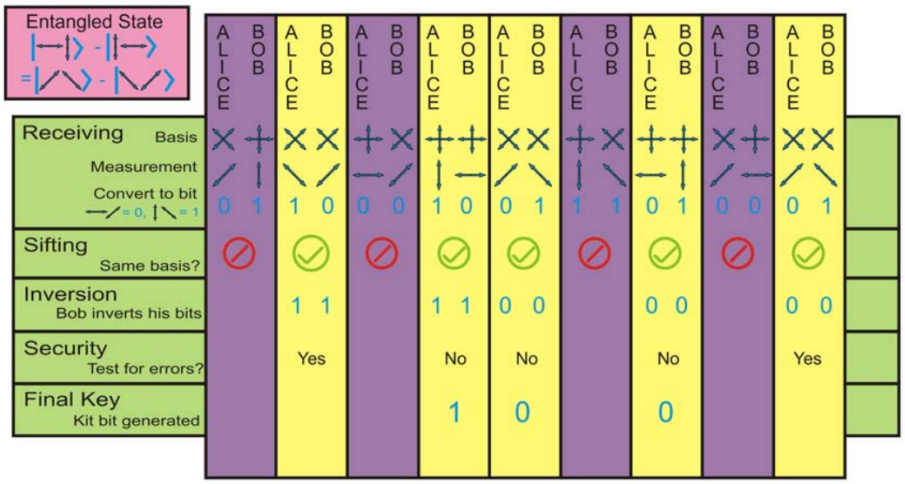


Figura 2.10: Esquema del protocolo BBM92 considerando el estado inicial de superposición $|\psi^-\rangle$, con todo el proceso explicado a partir de sus etapas: elección de bases, "sifting, conversión a bits, detección de errores y creación de clave final. Fuente: (Erven , 2002)

3. Amplificación de privacidad Para detectar si un actor externo, en nuestro Eve, está interceptando las comunicaciones, se utiliza el 10 % de bits de la clave cruda para computar el porcentaje de errores de bits (QBER).

La detección de espionaje se basa en lo siguiente:

1. Supongamos que Eve intercepta el fotón de Bob. Eve debe elegir entre una de las dos bases posibles para poder medir este fotón. Por lo tanto, Eve tiene un **50 % de probabilidades de escoger la misma base que Alice** escogió

   a) Caso 1: Eve coincide en la elección de bases respecto a Alice. Entonces, Eve obtendrá la misma medición que habría obtenido Bob. Por lo tanto, si Eve transmite el fotón medido a Bob, él obtendrá el mismo resultado igualmente, ya que utiliza la misma base, por lo que no se podría detectar esta escucha

   b) Caso 2: Eve escoge la base contraria a Alice. En este caso, Eve enviaría a Bob un fotón resultante que se encontraría en superposición respecto a la base de

Bob (misma probabilidad de medir un estado u otro). Por lo tanto, Bob mediría correctamente el fotón resultante con el mismo valor que Alice un 50 % de las veces.

Por lo tanto, si calculamos la probabilidad total de que Bob obtenga una medición distinta a Alice utilizando la misma base si Eve se encuentra escuchando las transmisiones es de: $0{,}5x0{,}5 = 0{,}25 = 25\,\%$. Por lo tanto, si del conjunto de bits que se utiliza como test, hay más de un 25 % de error, podemos decir que claramente está siendo escuchada la transmisión, teniendo entonces que abortar y reiniciar la comunicación. Se muestra un esquema gráfico de esta demostración en la Figura 2.11.

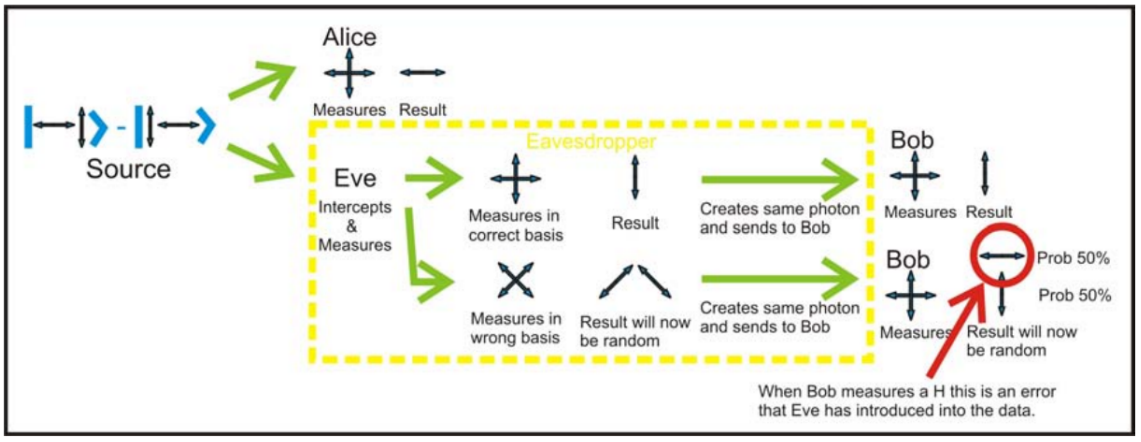


Figura 2.11: Diagrama dónde se muestra un ejemplo de las diferentes casuísticas posibles en el caso de que Eve estuviera espiando las comunicaciones entre Alice y Bob y como estos serían capaces de detectarlo. Fuente: (Erven , 2002)

Una vez entendido el concepto y, para ser más específicos, la fórmula genérica para el cálculo del ratio ideal (considerando que no hay ningún agente interceptando la señal) dependen también del medio que se utilice para las comunicaciones y la calibración de los dispositivos. Es por ello que los márgenes de porcentajes más comunes de QBER utilizados son de 11 % como límite mínimo y 14.6 % como límite máximo (Hjelme et al. , 2011) (siempre que sea un valor menor al 25 %, por las razones explicadas anteriormente y en el esquema de la Figura 2.11).

Características del protocolo BBM92

Este protocolo comparte muchas de las propiedades del E91, entre ellas la de utilizar estados entrelazados, lo que permite una mayor seguridad ya que no existe una información compartida previa a la medición, lo que hace que cualquier intermediación pueda modificar el resultado y, por lo tanto, ser detectable.

Una de las principales características de este protocolo basado en entrelazamiento, comparado con E91, es que al estar midiendo utilizando únicamente 2 bases (H/V y $+/-$), no se incumple la inecuación CHSH (Clauser et al., 1969) ($|S| \leqslant 2$), lo que permite no violar las desigualdades de Bell y, por lo tanto, ofrece menos errores en la preparación de los estados o menos perdida de partículas. (Erven , 2002).

También, si comparamos con protocolos como en BB84, este protocolo permite transmitir a distancias más lejanas sin perder la potencia de la señal (debido a que no se debe de hacer correcciones para evitar ataques de separación de fotones y los estados entrelazados ofrecen una menor decoherencia en su transmisión) (Waks et al. , 2002).

3. Comparación

Como se mencionó en la introducción de esta actividad, para realizar la comparación entre los protocolos utilizaremos un enfoque en dos niveles. De este modo, las dos primeras secciones de este capítulo están dedicadas al primer nivel (enfocados en los protocolos *per se*) y, en la última sección, "subiremos" el punto de vista y nos centraremos al segundo nivel donde compararemos las dos clases a nivel estructural.

3.1. Comparación entre los protocolos

En esta primera sección, como ya se ha mencionado, trataremos de comparar los seis protocolos explicados anteriormente. Para ello, hemos extraído un conjunto de propiedades que utilizaremos a modo de marco/plantilla para comparar los protocolos entre sí. En lo que queda de sección analizaremos cada propiedad del marco protocolo a protocolo.

Propiedad cuántica

Como ya hemos mencionado, una de las principales características de los protocolos de distribución de clave cuántica es que se aprovechan de propiedades de la mecánica cuántica. La división que se hace de los protocolos entre PM y EB se basa en la propiedad cuántica que cada protocolo utiliza.

Todos los protocolos PM utilizan la propiedad de superposición cuántica, donde un qubit puede estar en varios estados a la vez. Esta característica es muy importante para la codificación de información en sistemas cuánticos, ya que ofrece muchísimas más posibilidades que la codificación clásica.

Como su propio nombre indica, los protocolos EB se basan en la propiedad de entrelazamiento cuántico, que dice que dos partículas se pueden encontrar instantáneamente correlaciones sin importar la distancia entre ellas. Esta propiedad se aprovecha en ciertos protocolos para transmitir información de forma más segura y eficiente que los sistemas clásicos.

Ambos tipos de protocolos se aprovechan del teorema de no clonación, que imposibilita la creación de copias idénticas de un estado cuántico, lo que aumenta la seguridad en las comunicaciones.

Número de estados y bases

Otra clasificación que podemos hacer es respecto al numero de estados y de bases que utiliza cada protocolo para codificar y medir la información. Tenemos ejemplos de protocolos que usan dos, cuatro o seis estados y dos o tres bases.

Los protocolos como el B92 que utiliza dos estados, sacrifican capacidad de representación de información compleja y algo de seguridad respecto a protocolos de cuatro estados, a cambio de una mayor simplicidad en la implementación y menos complejidad en la corrección de errores cuánticos.

Por otro lado, tenemos protocolos como el six-state que utilizan seis estados en tres bases. En este caso, el resultado es que aumenta la complejidad y se pierde un poco de eficiencia comparado con protocolos de cuatro estados, pero a cambio, se consigue una mayor riqueza en la codificación y se mejora la seguridad.

Respecto al protocolo E91 podemos destacar que, pese a que se requieran tres bases para su implementación, solo dos (cuatro estados) son realmente utilizadas exclusivamente para comunicación. Mientras que la base restante se destina a la detección de terceros.

Por último, el caso más común que son protocolos de cuatro estados y dos bases, como el conocido BB84. Con lo que hemos contado de los otros tipos de protocolos, podríamos considerar los de cuatro estados como los más equilibrados.

Detección de presencia

Como hemos visto, los protocolos de distribución de clave cuántica son capaces de detectar escuchas y abortar la comunicación cuando detectan espías. Para esto, se sirven de propiedades cuánticas aunque hay ciertas diferencias entre ellos.

La mayoría de protocolos que hemos visto utilizan el QBER (*Quantum Bit Error Rate*) para detectar espías. Una aplicación se muestra en Lizama-Pérez et al. (2016) en el que lo utilizan para contrarrestar ataques de interceptación y reenvío (IR e IRFS) con BB84.

En general, se calcula este parámetro y si es mayor que determinado umbral quiere decir que los errores en la transmisión son notables, bien por ruido, o por la presencia de espías. Por lo tanto, cuando se supera dicho umbral se aborta el protocolo.

Por otro lado, tenemos el protocolo E91 a modo de excepción, que para este propósito utiliza el teorema de Bell y la inecuación CHSH. De manera similar a los otros protocolos,

este calcula una magnitud (S) y la utiliza como umbral.

Eficiencia (*key rate*)

Una medida de la eficiencia de los protocolos es el *key rate*. Nos dice a qué ratio somos capaces de crear una clave más o menos segura. Existen varios tipos y varias variables. Tratemos de identificar la eficiencia de los protocolos comparándolos con otro.

Comenzando con BB84, según Watanabe et al. (2006) (fig. 2, pág. 10) observamos un *key rate* prácticamente lineal en función del ratio de error, y con un máximo de 1 en el caso ideal. Esto no ocurre con el B92, que depende del ángulo de rotación θ entre bases (Coles et al., 2016) (fig. 6, pág. 7). Además, en Muskan et al. (2023) (fig 3, pág. 15) compara dos casos de cada uno en un par de casuísticas y resulta que el BB84 es más eficiente.

Mizutani et al. (2014) compara el *key rate* de SARG04 con BB84 respecto a la distancia (concretamente sus generalizaciones MDI[1]) en varios escenarios (fig. 4a, pág. 5 y fig. 6, pág 6) y concluimos que tienen valores parecidos, siendo ligeramente mejor el BB84.

Cabe destacar también el estudio de Goyal et al. (2014) en el que, puesto que E91 y six-state tienen tres bases, analizan la eficiencia de ambos (fig. 2, pág. 2). La conclusión es que ambos tienen eficiencias muy similares pese a ser de diferente tipo, aunque, el six-state es ligeramente mejor.

Dentro de los EB, si comparamos BBM92 con E91, de nuevo Muskan et al. (2023) (fig. 5, pág. 16) realiza un estudio de dos aplicaciones de cada uno en varios escenarios y (en ambas) resulta más eficiente BBM92.

Reconciliación de base

Si analizamos la forma que cada protocolo tiene de llevar a cabo esta etapa podemos encontrar algunas diferencias. Como nota previa, en la Tabla 3.1 nos referiremos a la base elegida arbitrariamente como χ.

Por un lado, ambos protocolos EB requieren que tanto Alice como Bob midan simultáneamente en bases arbitrarias para, posteriormente quedarse sólo con los pares EPR tal que ambos midieron en las mismas bases.

[1]Las adaptaciones MDI (*Measurement Device Independent*) son versiones de los protocolos QKD que atribuyen la tarea de medición a otra tercera entidad (Mizutani et al., 2014).

De manera similar encontramos BB84 y SS, en los cuales, en esta etapa, nos quedaremos con aquellos fotones/qubits que Bob midió en la misma base que Alice utilizó para codificar inicialmente.

Por otro lado, encontramos peculiaridades en B92, que mantiene sólo los estados que dieron como resultado de la medición de Bob $|1\rangle$ o $|-\rangle$; y en SARG04, en el que Alice el estado original junto con otro de la otra base para que Bob lo mantenga si el resultado de su medición es compatible con solo uno de ellos[2].

Ataque PNS

Excepto por el protocolo SARG04, dónde el emisor no publica sus bases directamente, el resto debe de protegerse de alguna manera a los ataques PNS o de separación de fotones. En estos ataques, Eve puede recoger cierto número de fotones y solo reenviar el resto a Bob para obtener información parcial de la clave.

No obstante, para ataques del tipo PNS, dónde Eve no reenvía la información a Bob, en el resto de protocolos es necesario añadir una capa de seguridad extra aplicando lo que se denomina "estados señuelo" (*decoy state*) (Hoi-Kwong et al. , 2005), dónde se envían un número de fotones extra con unas características de intensidad diferentes al resto. En el caso de que Eve extrajera estos paquetes de fotones, Bob podría detectar la omisión de los mismos y, por lo tanto, saber que hay una intervención de las comunicaciones.

Esta medida preventiva, igualmente, no protege las comunicaciones de manera tan eficiente como el SARG04, lo que la diferencia respecto a los otros cinco protocolos (respecto a esta característica).

Habiendo terminado de exponer las siete características definidas para la identificación y comparación de los protocolos, se ha resumido toda esta explicación en la Tabla 3.1.

3.2. Comparación de clases

Ampliando un poco el punto de vista de la comparación, tratemos de dar con una distinción a nivel de tipo en lugar de a nivel de protocolo. Podemos ver este punto como un escalón más arriba en la escala de abstracción y poder así encontrar peculiaridades no

[2]Podemos decir que es una generalización con cuatro permutaciones del árbol de decisiones que vimos en B92 (Figura 2.7).

ligadas exclusivamente con implementaciones.

Quizá, el aspecto más diferenciador que podemos encontrar a este nivel es la manera de crear la clave, es decir, sobre quién recae la responsabilidad de formar una primera instancia de la clave.

En este sentido, los PM son unidireccionales, es decir, la responsabilidad recae únicamente sobre el emisor (Alice), de modo que el receptor (Bob) simplemente se limita a medir y, posteriormente, ponerse de acuerdo y dar con la versión final de la clave (que variará en función de las etapas que se apliquen tras la reconciliación de bases).

Mientras que, en los EB la clave no se conoce hasta que no termina la ejecución del protocolo. Ni Alice ni Bob saben cual es la clave inicialmente[3], simplemente se dedican a medir partículas, fotones o qubits que reciben de una central.

Podemos, por tanto, decir que la diferencia entre los protocolos PM y EB es el canal cuántico: uno es unidireccional y el otro se puede entender como dos canales unidireccionales que provienen de una central.

Aunque, por fundamental que pueda parecer esta diferencia, existe una conexión que permite definir los protocolos de tipo PM en forma de EB. Esto se debe a que, desde el punto de vista de la privacidad, como mencionamos a lo largo del Capítulo 2, el principal objetivo es encontrar una correlación entre estados cuánticos y bits clásicos (Bae, 2007).

[3]A no ser que uno de los dos tome también el papel de central.

	Prepare & Measure				*Entanglement-Based*	
Característica	**BB84**	**B92**	**SS**	**SARG04**	**E91**	**BBM92**
Propiedad cuántica	Superposición	Superposición	Superposición	Superposición	Entrelazamiento	Entrelazamiento
Número estados	4	2	6	4	4	4
Número bases	2	2	3	2	3	2
Detección presencia	QBER	QBER	QBER	QBER	Inecuación CHSH	QBER
Eficiencia	Aprox. lineal	Peor que BB84	Mejor que E91	Peor que BB84	Peor que BBM92, SS	Mejor que E91
Reconciliación base	$\chi^A_{cod} = \chi^B_{med}$	$\{\|1\rangle, \|-\rangle\}$	$\chi^A_{cod} = \chi^B_{med}$	Pares	$\chi^A_{med} = \chi^B_{med}$	$\chi^A_{med} = \chi^B_{med}$
Ataques PNS	Decoy state	Decoy state	Decoy state	Robusto	Decoy state	Decoy state

Tabla 3.1: Tabla comparativa global entre los seis protocolos con las características mencionadas. Fuente: Elaboración Propia.

4. Conclusiones

En este último capítulo, destacaremos algunas conclusiones interesantes que hemos podido obtener con la realización de esta actividad, así como el cumplimiento del objetivo mediante la estructura propuesta.

Comenzando con algunas ideas interesantes que pudimos obtener, la primera de ellas es que BB84 supuso un referente fundamental para los protocolos posteriores de la clase PM. Es por esto por lo que, tanto a la hora de explicar los protocolos así como de compararlos, BB84 ha estado muy presente y ha sido un punto clave para el objetivo de esta actividad.

Otro punto relevante es cómo consiguen aplicar conceptos y aprovechar teorías de la mecánica cuántica para lograr establecer una comunicación lo más segura posible. Más concretamente, nos referimos (entre otros) a casos como el de E91, que aprovecha el teorema de Bell para la detección de intrusos, o el de B92, que directamente utiliza como premisa fundamental la imposibilidad de distinguir entre estados no ortogonales.

De cara a nuestra motivación inicial, la definición de un marco compuesto por siete características nos ha permitido obtener (o al menos intentarlo) una visión más fundamental pero a la vez detallada de cada protocolo mediante el estudio de dichas propiedades. Y, lo que es más interesante, este nos sirve como un mecanismo para identificar un protocolo en base a un subconjunto de sus atributos (que variará en función del protocolo).

Veamos esto con un ejemplo en el que tratamos de identificar el protocolo six-state. Si comprobamos sus atributos en la Tabla 3.1 vemos que, sólo con fijarnos en que usa tres bases (o lo que es lo mismo, seis estados) y que se enmarca en la clase PM, ya podríamos identificarlo unívocamente.

Esto, junto con el análisis comparativo entre clases (que aporta una visión más global y abstracta) y las definiciones de cada uno de los protocolos, nos ha permitido satisfacer nuestra motivación inicial a la vez que obtener un conjunto sólido de conocimientos acerca de QKD.

Por último, uno de los aspectos más importantes que hemos aprendido es la importancia de la securización del envío y recepción de la información en una tecnología que, aunque se presupone segura por el hecho de estar basada en principios de la mecánica cuántica

y que hace casi imposible la clonación de información, tiene ciertas vulnerabilidades que han de mejorarse, demostrarse y perfeccionarse. No solamente por el hecho de que sea parte del desarrollo tecnológico de los sistemas de información cuántica, sino que además nos va en ello la protección de la privacidad de la información en general, con los riesgos que conlleva, dado que los sistemas actuales de información basados en sistemas clásicos de encriptación ya tienen fecha de caducidad por la amenaza en sí mismo que supone la computación cuántica y por la más que probada capacidad de ruptura de las claves de encriptación en los sistemas clásicos.

Bibliografía

Bennett, C. H. (1992) Quantum Cryptography Using Any Two Nonorthogonal States. *Physical Review Letters, 68*(21), 3121-3124. https://doi.org/10.1103/PhysRevLett.68.3121

Bennett, C. H., Brassard, G. y Mermin, N. D. (1992) Quantum cryptography without Bell's theorem. *Physical Review Letters, 68*(5), 557-559. https://doi.org/10.1103/PhysRevLett.68.557

Ekert, A. K. (1991) Quantum cryptography based on Bell's theorem. *Physical Review Letters, 67*(6), 661-663. https://doi.org/10.1103/PhysRevLett.67.661

Elboukhari, M., Azizi, M. y Azizi A. (2010) Achieving unconditional security by quantum cryptography. https://www.researchgate.net/publication/228669847_Achieving_unconditional_security_by_quantum_cryptography?enrichId=rgreq-e2a462d26a240f0258b884f972cabb7d-XXX&enrichSource=Y292ZXJQYWdlOzIyODY2OTg0NztBUzoxMDE1MTMzMDk0NTg0MzdAMTQwMTIxNDA2NzMxMg%3D%3D&el=1_x_3&_esc=publicationCoverPdf

Gisin, N., Ribordy, G., Tittel, W. y Zbinden, H. (2002) Quantum cryptography. *Reviews on Modern Physics, 74*(1), 145-195. https://doi.org/10.1103/RevModPhys.74.145

Clauser, J. F., Horne, M. A., Shimony, A. y Holt, R. A. (1969) Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letter, 23*(15), 880-884. https://doi.org/10.1103/PhysRevLett.23.880

Nikolina, I. (2007) The Ekert Protocol. *Journal of Phy334, 1*, 1-4. https://api.semanticscholar.org/CorpusID:5553232

Renner, R., Gisin, N. y Kraus, B. (2005) An information-theoretic security proof for QKD protocols. *Physical Review A, 72*(1), 012332. https://doi.org/10.1103/PhysRevA.72.012332

Scarani, V., Acín, A., Ribordy, G. y Gisin, N. (2004). Quantum Cryptography Protocols Robust against *Photon Number Splitti*ng Attacks for Weak Laser Pulse Implementations.

Physical Review Letters, 92(5), 057901. https://doi.org/10.1103/PhysRevLett.92.057901

Arranz-Díez, J. M. (2022). *Prueba de concepto de criptografía cuántica.* [TFG, Universidad de Valladolid]. https://uvadoc.uva.es/bitstream/handle/10324/58297/TFG-G6043.pdf?sequence=1

Lizama-Pérez, L. A., Mauricio-López, J. y De Carlos-López, E. (2016). Quantum Key Distribution in the Presence of the Intercept-Resend with Faked States Attack. *Entropy 2017, 19*(4). https://doi.org/10.3390/e19010004

Coles, P. J., Metodiev, E. M. y Lütkenhaus, N. (2016). Numerical approach for unstructured quantum key distribution. *Nature Communications, 7*, 11712. https://doi.org/10.1038/ncomms11712

Watanabe, S., Matsumoto, R. y Uyematsu, T. (2006). *Security of quantum key distribution protocol with two-way classical communication assisted by one-time pad encryption.* arXiv. https://doi.org/10.48550/arXiv.quant-ph/0608030

Muskan, Meena, R. y Banerjee, S. (2023). *Analysing QBER and secure key rate under various losses for satellite based free space QKD.* arXiv. https://doi.org/10.48550/arXiv.2308.01036

Goyal, S., Ibrahim, A. H., Roux, F. S., Konrad, T. y Forbes, A. (2014). *Experimental orbital angular momentum based quantum key distribution through turbulence.* arXiv. https://doi.org/10.48550/arXiv.1412.0788

Mizutani, A., Tamaki, K., Ikuta, R., Yamamoto, T. e Imoto, N. (2014). Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol. *Scientific Reports, 4*, 5236. https://doi.org/10.1038/srep05236

Bae, J. (2007). *Entanglement and Quantum Cryptography.* [Tesis, Universitat de Barcelona]. Dipòsit Digital. https://diposit.ub.edu/dspace/bitstream/2445/35495/1/JB_THESIS.pdf

Bennett, C. H. y Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science, 560*, 7-11. https://doi.org/10.1016/j.tcs.2014.05.025

Heisenberg, W. (1927). Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Zeitschrift für Physik, 43*, 172–198. https://doi.org/10.1007/BF01397280

Wootters, W. y Zurek, W. (1982). A single quantum cannot be cloned. *Nature, 299*, 802–803. https://doi.org/10.1038/299802a0

Bruß, D. (1998). Optimal Eavesdropping in Quantum Cryptography with Six States.*Physical Review Letters, 81*, 3018-3021. https://link.aps.org/doi/10.1103/PhysRevLett.81.3018

Bechmann-Pasquinucci, H., Gisin, N. (1999). Incoherent and Coherent Eavesdropping in the 6-state Protocol of Quantum Cryptography. *Physical Review A, 59* , 4238-4248. https://doi.org/10.1103/PhysRevA.59.4238

Lo, H. K. (2001). Proof of unconditional security od six-state quantum ket distribution scheme. *Quantum Information and Computation, 1*, 81-94. https://doi.org/10.48550/arXiv.quant-ph/0102138

Gottesman, D. y Lo, H. K. (2003). Proof of security of quantum key distribution with two-way classical communications. *IEEE Transactions on Information Theory, 49*, 457-475. https://doi.org/10.1109/TIT.2002.807289

Hjelme, D. R., Lydersen, L. y Makarov, V. (2002). Quantum cryptography. arXiv. https://doi.org/10.48550/arXiv.1108.1718

Waks, E., Zeevi, E. y Yamamoto, Y. (2002). Security of quantum key distribution with entangled photons against individual attacks. *Physical Review A, 65*, 052310. https://doi.org/10.1103/PhysRevA.65.052310

Lo, H. K., Ma, X. y Chen, K. (2005). Decoy State Quantum Key Distribution. *Physical Review Letters, 23*(94). https://doi.org/10.1103/physrevlett.94.230504

Erven, C. (2007). On Free Space Quantum Key Distribution and its Implementation with a Polarization-Entangled Parametric Down Conversion Source. *University of Waterloo.* https://uwspace.uwaterloo.ca/handle/10012/3021

A. Apéndices

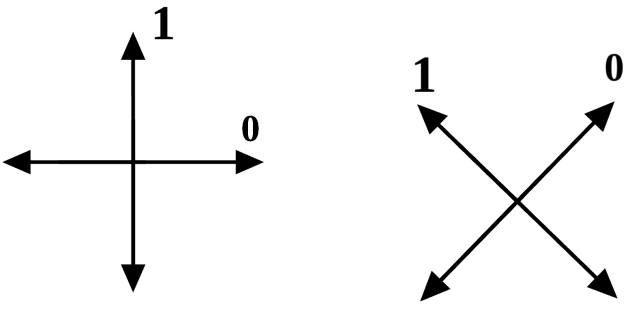
A.1. Fotones polarizados como qubits

Los qubits en este caso serán los estados de polarización de fotones. El utilizar fotones facilita mucho la implementación en laboratorio de este protocolo.

La polarización de cada fotón es modulada por el emisor, pudiendo tener polarización rectilínea o diagonal. Si medimos la polarización de un fotón con polarización rectilínea obtendremos el estado horizontal o el vertical, si hacemos lo mismo a un fotón con polarización diagonal, obtendremos los estados diagonal o anti-diagonal. A cada uno de estos estados, en cada tipo de polarización le asignaremos un 0 o un 1.

Para obtener el resultado de medición correcto es necesario conocer como se ha polarizado el fotón, y al medir utilizar la base correcta correspondiente a cada tipo de polarización. Vamos a describir las bases y los estados usando notación de Dirac, de este modo la base rectilínea estará formada por los vectores estado $\{|0\rangle, |1\rangle\}$, mientras que la base diagonal será: $\{|+\rangle, |-\rangle\}$.

El protocolo BB84 se basa en que si medimos un fotón con polarización rectilínea, utilizando una base diagonal o el caso contrario, el resultado obtenido no va a ser siempre correcto, ya que estamos haciendo la medición con la base equivocada. Vamos definir de manera gráfica estas bases para facilitar la explicación del protocolo:



(a) Base rectilínea $\{|0\rangle, |1\rangle\}$ (b) Base diagonal $\{|+\rangle, |-\rangle\}$

Figura A.1: Bases protocolo BB84. Elaboración propia.