uc3m | Universidad Carlos III de Madrid

Grado en Ingeniería en Tecnologías de Telecomunicación
2020 - 2021

*Trabajo Fin de Grado*

# "Criptografía Cuántica"

Isabel Carnoto Amat

Tutor/es

Luis Enrique García Muñoz

Leganés, septiembre de 2021

# RESUMEN

Actualmente, la mayoría de los mecanismos usados para encriptar información basan su seguridad en la dificultad que supone resolver complejas operaciones matemáticas. Este método podría ser seguro, pero solo bajo la suposición de que la vida útil de la información es más corta que el tiempo que un espía necesita para romper el protocolo de seguridad. Este enfoque es vulnerable ante posibles avances tecnológicos.

La criptografía cuántica, basada en los principios de la mecánica cuántica, ofrece protocolos de seguridad teóricamente seguros. El teorema de no-clonación prohíbe la acción de copiar información cuántica y el hecho de que la monitorización pasiva sea imposible en los sistemas cuánticos permite a los puntos que han establecido la comunicación detectar la presencia de un espía.

El objetivo principal de este trabajo es comparar dos protocolos de distribución de claves cuánticas, el BB84 y BB84 eficiente, y desarrollar un emulador de un sistema de criptografía cuántica para implementar aquel que brinde las mejores prestaciones en términos de eficiencia y capacidad de detección de un espía.

Para lograr este objetivo se utilizó un kit de demostración de claves cuánticas, el cual permite simular el protocolo BB84. Posteriormente, se desarrolló un emulador en MATLAB capaz de simular ambos protocolos, mostrando la eficiencia y probabilidad de detección de cada uno, para distintas longitudes de claves.

Con el protocolo BB84 eficiente, se obtiene una eficiencia mayor que con el BB84 y al aumentar la longitud de la clave se puede seguir incrementando esta eficiencia manteniendo una probabilidad de detección entre un 95% y un 100%, incluso bajo condiciones no ideales.

**Palabras clave: cuántico, criptografía, clave, eficiencia, espía.**

# ABSTRACT

At this present time, most of the mechanisms used for information encryption base their security in the difficulty of solving complex mathematical problems. This method may be secure, but only under the assumption that the life span of the information is shorter than the time an eavesdropper needs to break the security protocol. This approach is vulnerable to possible technological advances.

Quantum cryptography, based on the principles of quantum mechanics, offers security protocols theoretically safe. The non-cloning theorem prohibits the action of copying quantum information and the fact that passive monitorization is impossible in quantum systems allows the communicating parties to detect the presence of an eavesdropper.

The final goal of this project is to compare two quantum key distribution protocols, BB84 and BB84 efficient, and develop an emulator of a quantum cryptography system to implement the one with better benefits in terms of efficiency and ability to detect an eavesdropper.

To accomplish this goal a quantum cryptography demonstration kit was used to simulate the BB84 protocol. Afterwards, an emulator, capable of simulating both protocols, was developed using MATLAB, this one showed the efficiency and detection probability of each one, for different key lengths.

With the protocol BB84 efficient, a higher efficiency can be obtained than with the BB84 protocol and, by increasing the length of the key, this efficiency can be improved maintaining the detection probability between 95% and 100%, even under non-ideal conditions.

**Key words: quantum, cryptography, key, efficiency, eavesdropper.**

# AGRADECIMIENTOS

Me gustaría agradecer a mis padres, por impulsarme a ser mejor cada día y por estar siempre cerca a pesar de la distancia, a Caro y a Nacho, por adoptarme y haber vivido esta carrera conmigo como si también la cursaran, a Raque, por ayudarme a ver más de una perspectiva, a Sav por el apoyo incondicional, y a Rai por no dejar que pase un día sin hacerme reír.

También quiero agradecer a los increíbles amigos que la Carlos III me ha dado por siempre hacerme sentir en familia, aunque yo sea turista.

Por último, quiero agradecer a mi tutor Luis Enrique y a Isdefe, por la oportunidad y el apoyo económico.

# ÍNDICE GENERAL

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# 1. MOTIVACIÓN

La motivación de este proyecto surge del interés de la empresa Isdefe (Ingeniería de Sistemas para la Defensa de España) en la criptografía cuántica.

Dentro del ámbito de la defensa y la seguridad es sumamente importante mantener protegida la información que se intercambia. El principal mecanismo de garantía de la seguridad de la información son los procesos de encriptado, sin embargo, los procesos actuales de criptografía se basan, en su mayoría, en la resolución de complejas operaciones matemáticas, como la factorización en números primos de cifras de gran tamaño. Estos mecanismos son teóricamente vulnerables y sobre todo en la actualidad con el rápido crecimiento de la potencia de los computadores.

Es debido a estas inquietudes por las cuales he trabajado dos años dentro del proyecto de investigación titulado "Convenio de Colaboración para la creación de la Cátedra UC3M-ISDEFE", el cual plantea un salto a la criptografía cuántica ya que, según las propiedades de la física cuántica, esta supone un mecanismo de encriptación de información inmune a intentos de interceptación.

Se busca indagar en los avances de las comunicaciones cuánticas, con la criptografía como punto focal, con el fin de valorar su aplicabilidad en el futuro.

# 2. INTRODUCCIÓN

En este capítulo se comentan los objetivos del trabajo, el marco regulador, inversiones en tecnologías cuánticas, el contenido de la memoria y una introducción teórica con todos los conceptos necesarios para comprender el capítulo de desarrollo del trabajo. En esta introducción también se exponen aplicaciones actuales de la criptografía cuántica.

## 2.1. Objetivos

El objetivo principal de este proyecto es comparar los protocolos BB84 y su variante BB84 eficiente, con el fin de implementar, en un emulador de un sistema de comunicaciones cuántico, también desarrollado, aquel que ofrezca las mejores prestaciones en términos de eficiencia y capacidad de detección de un espía.

Para lograr el objetivo principal es necesario cumplir con los siguientes objetivos parciales:

1. Realizar pruebas usando el "Quantum Cryptography Demonstration Kit" de Thorlabs para entender el funcionamiento del protocolo BB84 de forma práctica.
2. Desarrollar un emulador de un sistema de comunicaciones cuántico teniendo en cuenta los efectos del ruido térmico y atenuación del canal. Validar el correcto funcionamiento de este emulador comparando sus resultados con la bibliografía.
3. Utilizar el emulador para implementar y comparar, mediante simulaciones, los protocolos de distribución de claves cuánticas BB84 y BB84 eficiente, bajo condiciones ideales, con el fin de detectar cuál de ellos ofrece las mejores prestaciones.
4. Implementar el protocolo elegido como óptimo y observar su comportamiento bajo condiciones no ideales.

### 2.2. Marco regulador e inversiones actuales

Actualmente no existen estándares o regulación de los sistemas de criptografía cuántica, esto puede deberse a las limitadas aplicaciones prácticas que existen y a la dificultad y gran cantidad de recursos que se necesitan para llevarlas a cabo.

Sin embargo, sí existen proyectos con la intención de estandarizar algoritmos que puedan ser inmunes a la creciente amenaza que suponen los ordenadores cuánticos.

Aunque es verdad que los avances en criptografía cuántica pueden abrir las puertas a sistemas sumamente seguros, avances en otros ámbitos de las tecnologías cuánticas como los computadores cuánticos representan una amenaza contra los sistemas clásicos de cifrado. Y se teme que este poder computacional se logre antes que la implementación de esquemas cuánticos de cifrado, dejando la información en riesgo de ciberataques.

Por esta razón el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) está trabajando actualmente para establecer los estándares de terminología y rendimiento de los ordenadores cuánticos intentando no perjudicar a la innovación [1].

Aunque muchos expertos afirman que no se espera que los ordenadores cuánticos sean capaces de quebrar los estándares criptográficos actuales sino hasta dentro de al menos 10 años el Instituto Nacional de Estándares y Tecnología (NIST) ya ha comenzado a trabajar en estándares de tecnologías criptográficas postcuánticas, con el objetivo de encontrar los algoritmos que puedan sustituir a la criptografía actual [2].

La criptografía postcuántica hace referencia a algoritmos diseñados para soportar ataques realizados con ordenadores cuánticos [3].

En julio de 2020 NIST anunció los algoritmos seleccionados, de entre todos los que fueron presentados, en la tercera ronda de su proceso de estandarización. Entre los elegidos se encuentran protocolos de establecimiento de claves y algoritmos de firma digital [4].

A continuación, se comentan el interés e inversiones en las tecnologías cuánticas alrededor del mundo. En los últimos años han aumentado significativamente los programas de investigación en distintas áreas de la mecánica cuántica, por lo que se ha incrementado el presupuesto recaudado por parte de financiación tanto pública como privada.

### 2.2.1. Inversiones privadas

En un artículo de *Nature* titulado "Quantum gold rush: the private funding pouring into quantum start-ups" se presenta un análisis de las inversiones en tecnologías cuánticas, entre 2012 y 2018.

Según este análisis, inversores privados han financiado al menos 52 compañías relacionadas con tecnologías cuánticas globalmente. Junto con las inversiones de los distintos gobiernos, grandes compañías, como IBM, Google, Huawei y Alibaba están apurándose a invertir en tecnologías cuánticas.

Los inversores han inyectado dinero en distintos ámbitos, como la computación cuántica, el desarrollo *software*, las comunicaciones cuánticas e incluso el desarrollo de sensores.

Las compañías que desarrollan *hardware* para ordenadores cuánticos son las que han recibido la mayor parte del capital.

Otro campo que recibe gran parte de las inversiones es el desarrollo de *software* cuántico. Aunque aún no exista *hardware* sobre el cual implementarlo, alrededor de 20 compañías recaudaron más de 110 millones de dólares entre 2012 y 2018. Estos algoritmos buscan traducir problemas como la simulación de moléculas u optimización de cadenas de suministros.

Por último, uno de los campos más populares: las comunicaciones cuánticas. La inversión en este campo es difícil de cuantificar debido a que alrededor de la mitad de las compañías que investigan las comunicaciones cuánticas seguras no publicaron el capital recibido.

El análisis muestra que Norte América era el líder en la atracción de capital en ese periodo de tiempo. Sin embargo, no se encuentra todo reservado para Estados Unidos ya que compañías en Canadá han recaudado 243 millones de dólares.

El mayor vacío en el análisis es causado por la falta de información sobre inversiones privadas en China.

En la figura 2.1 se muestra el capital recaudado, a través de inversiones privadas, entre 2012 y 2018 en distintos campos de las tecnologías cuánticas [5].

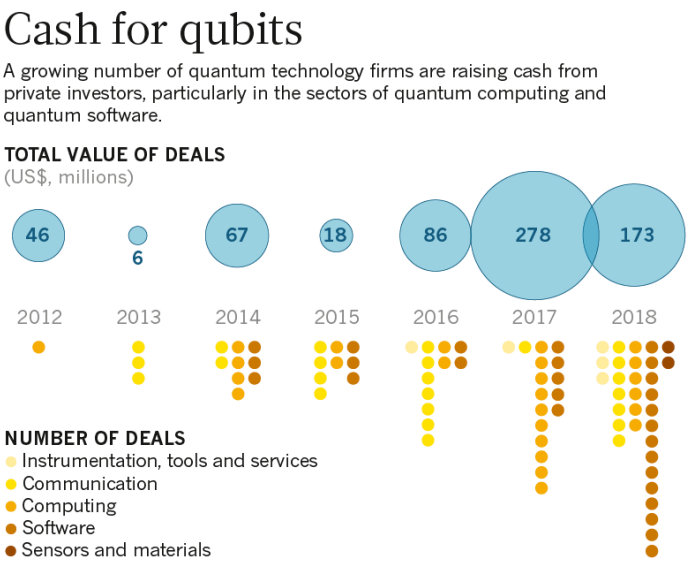


Fig. 2.1. Inversiones privadas entre 2012 y 2018 [5].

### 2.2.2. Financiación pública:

En los últimos años las inversiones en tecnologías cuánticas han aumentado exponencialmente, incrementándose también la financiación pública globalmente [6].

De acuerdo con la consultora McKinsey, en 2015 unas 7000 personas alrededor del mundo, con un presupuesto total de 1.5 billones de dólares, se encontraban investigando tecnologías cuánticas. La distribución de este presupuesto alrededor del mundo se muestra en la figura 2.2 [7].

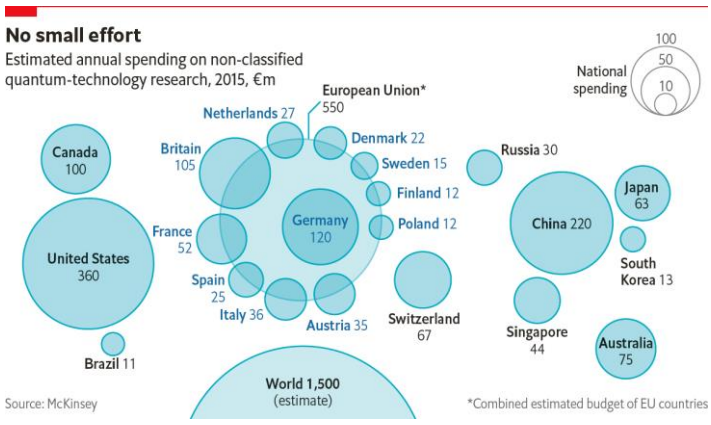


Fig. 2.2. Inversiones públicas en 2015 [7].

Tan solo 6 años después el presupuesto se encuentra ahora alrededor de los 22.5 billones de dólares, según el artículo de QURECA titulado “Overview on quantum initiatives worldwide”. La distribución de este se muestra en el mapa de la figura 2.3 [6].

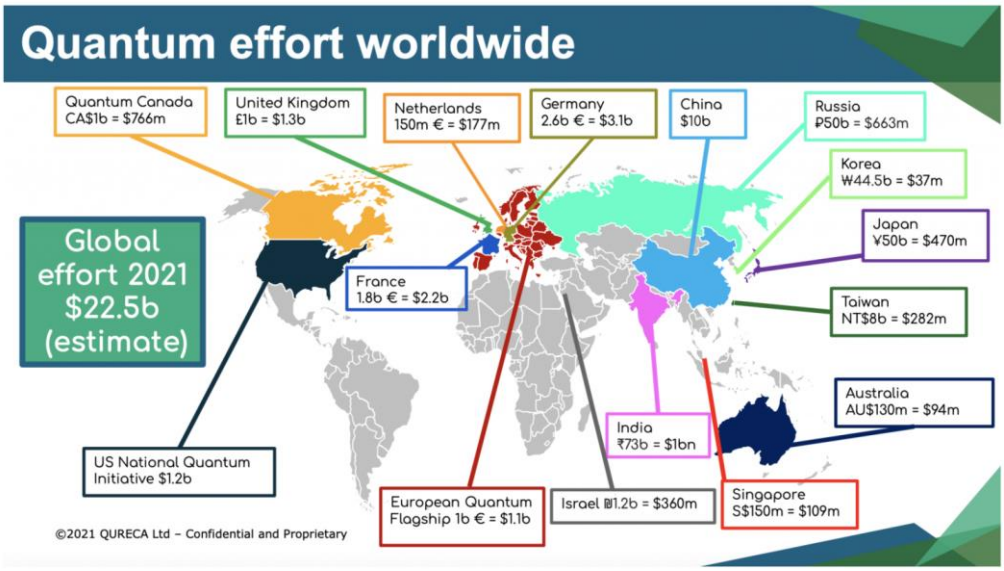


Fig. 2.3. Inversiones públicas actualmente [6].

**Europa**

La Unión Europea lanzó una iniciativa de investigación a largo plazo llamada "Quantum Technologies Flagship", la cual une centros de investigación, compañías y financiación pública con el fin de que Europa alcance un mayor liderazgo científico y excelencia en tecnologías cuánticas.

Esta iniciativa durará 10 años y contará con un presupuesto de 1000 millones de euros. Entre octubre de 2018 y septiembre de 2021 proveerá €132 millones para la financiación de 20 proyectos en las siguientes áreas: simulación cuántica, computación cuántica, comunicaciones cuánticas y meteorología y sensores cuánticos. A continuación, se muestra un desglose de los objetivos que se quieren alcanzar en cada una de las áreas a través de esta iniciativa [8].

- Comunicaciones cuánticas: garantizar la transmisión segura de información y seguridad a largo plazo para la sociedad de la información, a través del uso de recursos cuánticos como protocolos de comunicación.
- Computación cuántica: resolver problemas que están fuera del alcance de los procesadores clásicos utilizando máquinas cuánticas programables.
- Simulaciones cuánticas: entender problemas importantes, como por ejemplo procesos químicos, el desarrollo de nuevos materiales o teorías físicas fundamentales, mapeándolos en sistemas cuánticos controlados.

- Meteorología y sensores cuánticos: alcanzar una mayor sensibilidad, certeza y resolución en las medidas y diagnósticos manipulando objetos cuánticos [9].

**Estados Unidos**

Los programas para investigar cómo la mecánica cuántica podría contribuir con la seguridad nacional comenzaron a finales de la década de los 90.

La iniciativa NQI (National Quantum Initiative Act) presentada en 2018 cuenta con un presupuesto de $1.2 billones de dólares para un plazo de 5 años. Este le permite al gobierno acelerar el desarrollo de tecnologías cuánticas a través de colaboraciones con instituciones académicas y las empresas privadas.

Este presupuesto se dividirá entre el NIST (Instituto Nacional de Estándares y Tecnología), el NSF (Fundación Nacional de Ciencia), centros multidisciplinarios para la investigación cuántica y la educación, el Departamento de Investigación para la Energía y centros nacionales de investigación para la información cuántica.

**China**

Se cree que China es una de las naciones líderes en comunicaciones e información cuántica ya que el país comenzó a invertir en investigación y desarrollo de tecnologías cuánticas a finales de los años 90.

Para el año 2030, China tiene como objetivo tener expandida su infraestructura de comunicaciones cuánticas, haber desarrollado un prototipo de ordenador cuántico y haber construido un simulador cuántico.

Se estima que la inversión realizada por el gobierno chino es de unos $10 billones en tecnologías cuánticas, aunque esta cifra no ha sido confirmada oficialmente [6].

### 2.3. Contenido de la memoria

En este epígrafe se exponen los contenidos de cada capítulo de este trabajo.

- Capítulo 1: Motivación.
  Se exponen las razones que motivaron el desarrollo de este trabajo.
- Capítulo 2: Introducción.
  Se comentan los objetivos, introducción, marco regulador, inversiones actuales, contenido de la memoria y una introducción teórica conformada por una primera aproximación a la mecánica cuántica, una introducción a los conceptos matemáticos, los elementos de la mecánica cuántica, los sistemas de comunicaciones clásico y cuántico y la criptografía cuántica.
- Capítulo 3: Desarrollo.
  Este se divide en dos partes. En la primera se explica el funcionamiento del kit de demostración de criptografía cuántica de Thorlabs y en la segunda se explica el desarrollo y funcionamiento del emulador de criptografía cuántica.
- Capítulo 4: Resultados.
  Se exponen los resultados de los experimentos y simulaciones realizados. Se divide en cuatro partes: experimentos con el kit físico, validación del emulador de comunicaciones cuántico, validación de la implementación de los protocolos BB84 y BB84 eficiente y validación del protocolo óptimo a través de simulaciones en condiciones no ideales.
- Capítulo 5: Conclusiones.
  Se hacen los comentarios finales sobre los resultados obtenidos y objetivos cumplidos. Se exponen también posibles mejoras y ejemplos de trabajos futuros.
- Capítulo 6: Metodología y presupuesto.
  Se comenta el proceso de desarrollo de este trabajo de inicio a fin y se contabiliza el presupuesto necesario para llevarlo a cabo, teniendo en cuenta costes de personal y de materiales.

## 2.4. Introducción teórica

En este epígrafe se expone una introducción teórica con los conceptos necesarios para entender el desarrollo del trabajo.

En primer lugar, se comenta una primera aproximación a la mecánica cuántica, sus conceptos claves y un breve resumen histórico.

Se introducen los conceptos matemáticos y de sistemas de telecomunicaciones, tanto clásicos como cuánticos.

Por último, se explican los principios de la criptografía cuántica, varios protocolos de distribución de claves cuánticas que aplican estos principios y aplicaciones reales de estos en sistemas de criptografía.

### 2.4.1. Primera aproximación a la mecánica cuántica

#### 2.4.1.1. La mecánica cuántica

La mayor diferencia entre la mecánica clásica y la cuántica radica en que las personas se encuentran con ejemplos de la mecánica clásica a diario en la vida cotidiana, conocen cómo se comportan las cosas solo por intuición. La mecánica cuántica estudia cosas tan pequeñas, frías y aisladas que se encuentran completamente fuera del alcance de los sentidos humanos.

Para comprender este mundo cuántico se busca reescribir esta intuición utilizando abstracciones matemáticas. Se puede discutir que la mecánica clásica también utiliza estas abstracciones, sin embargo, las usadas en la mecánica cuántica difieren de estas anteriores por dos razones.

1. Las abstracciones cuánticas son fundamentalmente diferentes a las clásicas. Por ejemplo, el estado de un sistema se representa con distintos objetos matemáticos y sigue una lógica diferente.
2. La relación entre una medida y un estado es completamente diferente. En el caso clásico, se puede realizar una medida para determinar el estado en el que se encuentra un sistema. En el caso cuántico esto es falso. Los estados y medidas se separan como dos cosas diferentes, y la relación entre estos no es intuitiva.

#### 2.4.1.2. El Spin

Las partículas pueden tener múltiples propiedades como: ubicación en el espacio, carga, masa, entre otras.

Un electrón tiene un grado de libertad extra llamado *spin*. Se puede visualizar como una flecha que apunta en alguna dirección. El *spin* es un sistema que puede ser estudiado y es un ejemplo de un sistema simple, el cual se conoce como *qubit*.

Un *qubit*, o bit cuántico, cumple el mismo papel en el mundo cuántico que un bit lógico dentro de un ordenador.

#### 2.4.1.3. Un experimento

A continuación, se comenta un experimento expuesto por Leonard Susskind en [10] que ayuda a entender la gran diferencia entre las medidas en los sistemas clásicos y cuánticos.

En la mecánica clásica, uno de los sistemas deterministas más simples es una moneda. Esta representa un sistema con dos posibles estados: cara (C) o cruz (T).

En mecánica cuántica se considera este sistema (*spin*) como un *qubit*, donde se reemplaza el estado C con $\sigma = +1$ y T con $\sigma = -1$.

Con el fin de exponer qué ocurre cuando se realizan medidas en un sistema cuántico se define un aparato de medida ***M***, el cual interactúa con el *spin* y muestra el valor de $\sigma$. Este aparato ***M*** se define como una caja negra con una ventana donde se muestra el resultado de la medida y con una flecha que indica cómo el aparato se orienta en el espacio. Una representación de ***M*** se muestra en la figura 2.4, mostrando a la izquierda el aparato antes de realizar una medida y a la derecha, después de haberla realizado.

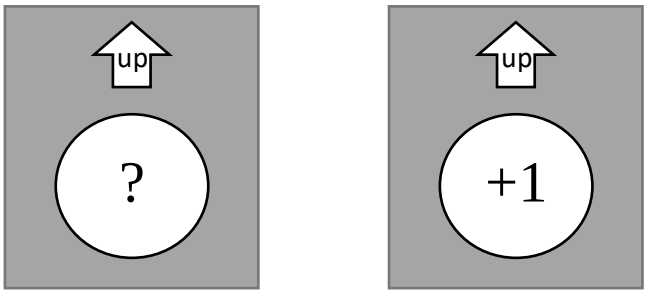


Fig. 2.4. Representación del aparato de medida.

El objetivo de este aparato es determinar el valor del estado $\sigma$, el cual inicialmente es desconocido.

En el primer paso del experimento se apunta el aparato en la dirección del eje z, como se muestra en la figura 2.5.

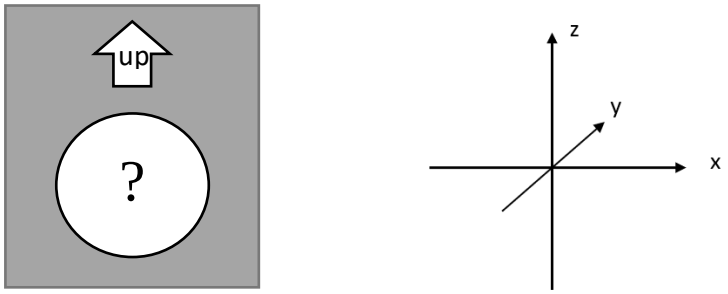


Fig. 2.5 Orientación del aparato de medida en la dirección del eje z.

Se obtiene como resultado de la medida, por ejemplo, $\sigma = +1$. Si la medida se repite múltiples veces con el aparato apuntando en la misma dirección y sin alterar el spin, se obtiene consecutivamente el mismo resultado, $\sigma = +1$, lo que permite corroborar el resultado del experimento.

En otras palabras, la primera medida realizada con $\boldsymbol{M}$ prepara el sistema en uno de los dos estados posibles y las siguientes medidas confirman el estado.

En el siguiente paso del experimento, se prepara el sistema en un estado inicial utilizando el aparato $\boldsymbol{M}$ y se procede a medir de nuevo, pero girando $\boldsymbol{M}$ 180˚, como se muestra en la figura 2.6.

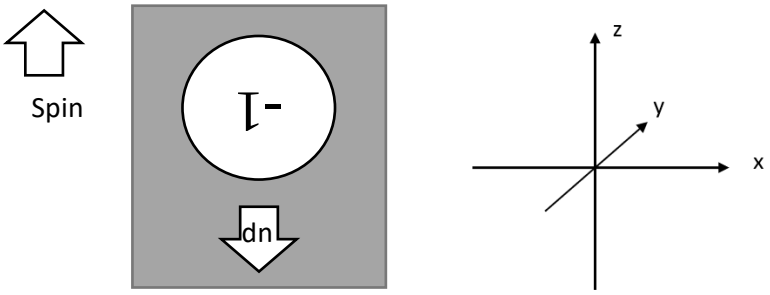


Fig. 2.6. Orientación del aparato de medida en la dirección del eje -z.

Si el estado preparado era $\sigma = +1$, tras la segunda medida se obtiene $\sigma = -1$ y viceversa. A la vista de estos resultados se puede pensar que lo que mide el aparato son las componentes de un vector a lo largo de la dirección marcada en $\boldsymbol{M}$, y que, dependiendo de las direcciones en las que se oriente, se podrían obtener las tres componentes de dicho vector, $\sigma_x,\ \sigma_y,\ \sigma_z$.

Para tratar de comprobar si el *spin* es un vector se usa el aparato $\boldsymbol{M}$ en la dirección del eje z y se prepara el estado como $\sigma = +1$. Ahora se rota el aparato en la dirección del eje x, como se muestra en la figura 2.7, y se realiza la medida de lo que se supone es la componente en x del *spin*, $\sigma_x$.

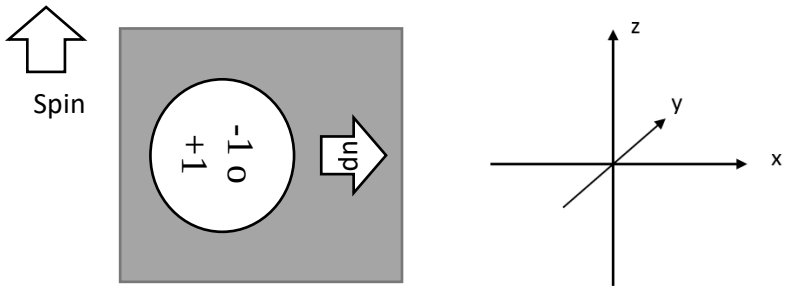


Fig. 2.7. Resultado de la medida en la dirección del eje x.

El resultado esperado de esta medida es $\sigma_x = 0$, ya que se ha comprobado en las dos partes anteriores que, sin en realidad es un vector, este apuntaría en la dirección del eje z. Sin embargo, el aparato ha devuelto el valor $\sigma = +1$ o $\sigma = -1$. Sin importar la dirección en la que se oriente, el aparato solo devuelve $\sigma = \pm 1$.

Para tratar de dar sentido a estos resultados se procede a repetir este último experimento. Se prepara el estado $\sigma = +1$, orientando el aparato hacia el eje z, se coloca $\boldsymbol{M}$ en la dirección del eje x y se mide.

Si se realizan muchas repeticiones se obtiene una secuencia aleatoria de +1 y -1, con probabilidad igual, es decir, en promedio el valor de estas repeticiones es cero.

En conclusión, en mecánica cuántica los sistemas no son deterministas, los resultados de los experimentos son aleatorios, sin embargo, si se realizan suficientes repeticiones, los promedios pueden coincidir con lo que se espera en un sistema clásico.

#### 2.4.1.4. Los experimentos nunca son sutiles

En la mecánica clásica el realizar una medida, pese a que involucra el uso de un aparato o sistema ajeno al que se mide, no altera ningún aspecto del objeto que se mide. Sin embargo, en la mecánica cuántica esta situación es muy diferente. Cualquier interacción capaz de medir algún aspecto del sistema es también capaz de perturbar otro aspecto del mismo sistema.

Esto se puede observar volviendo a los experimentos comentados anteriormente. Si se prepara un estado $\sigma = +1$ en la dirección del eje z y se realizan medidas consecutivas

con el aparato ***M*** orientado también hacia este eje se obtendrá la misma medida sin alterar el resultado. Sin embargo, si se realiza una medida a lo largo del eje x y luego se orienta de nuevo el aparato hacia el eje z, la medida no confirmará el estado preparado originalmente. La medida en la dirección del eje x deja al *spin* en una configuración aleatoria y no hay forma de determinar el valor de *spin* en una medida intermedia sin alterar el resultado final. Esto se puede reescribir como que medir una componente del *spin* destruye la información de otra componente, no se pueden conocer las componentes del *spin* en dos ejes diferentes simultáneamente [10].

#### 2.4.1.5. La madurez de la mecánica cuántica

Fue entre 1920 y 1940 que la mecánica cuántica alcanzó la madurez, avanzando de ser teoría cuántica a mecánica cuántica gracias al trabajo de muchos de los mejores físicos del siglo.

Schrödinger formuló la ecuación fundamental de la mecánica de ondas, la cual es fundamental para la descripción de varios fenómenos de la física molecular, atómica y nuclear.

Heisenberg introdujo el principio de incertidumbre, el cual afirma la imposibilidad de conocer, simultánea y exactamente, parejas de entidades físicas, como la posición y velocidad de una partícula. Mientras más precisamente se conozca la posición de una partícula, menos información se tendrá sobre su velocidad y viceversa.

#### 2.4.1.6. Conceptos clave

La mecánica cuántica presenta una serie de conceptos que pueden incluso parecer contrarios al sentido común y a lo establecido en la física clásica. Estos se han comentado sutilmente en el apartado anterior, sin embargo, a continuación, se definen de forma más explícita:

1. Aleatoriedad: La aleatoriedad es un elemento intrínseco de la mecánica cuántica. Se pueden obtener distintos resultados al medir varias veces un sistema, aunque este empiece siempre con las mismas condiciones iniciales. Esto se debe a que el resultado de cualquier medida es aleatorio y debe ser tratado bajo la teoría de probabilidad.
2. Indeterminación: el procedimiento de medir un sistema lo altera. Esto puede explicarse tomando en cuenta el antes mencionado Principio de Incertidumbre de

Heisenberg, en el cual conocer una de las medidas impide tener conocimiento de otra.

3. Cuantización: los estados de un sistema cuántico pertenecen a un conjunto discreto de niveles de energía.
4. Linealidad y Superposición: aunque los estados pertenecen a un conjunto discreto de valores, estos tienen una naturaleza continua debido a que las funciones de onda son funciones continuas. La combinación lineal de dos funciones de onda $a\psi(x) + b\varphi(x)$, donde a y b son números complejos, es también una función de onda.
5. Entrelazamiento: un par de partículas emitidas por la misma fuente, si se encuentran bajo la condición de entrelazamiento, muestran características correlacionadas que se preservan, aunque estas se alejen una de la otra. Si el estado de una de ellas es medido, el estado de la otra cambia inmediatamente.

#### 2.4.1.7. De la física a las tecnologías de la información

Pese a que el ámbito natural de aplicación de la mecánica cuántica es la física, en los últimos años se ha expandido hacia el área de tecnologías de la información, gracias a su reformulación en distintas aplicaciones como: la computación, la criptografía y las comunicaciones [11].

La motivación de estudiar la información dentro del contexto de la mecánica cuántica surge de la Ley de Moore. Esta expone que la cantidad de transistores dentro de un chip se duplica cada dos años, sin cambiar el tamaño del chip [12]. De no considerarse un límite, la reducción de los componentes continúa infinitamente hasta que se alcanzan las dimensiones atómicas. En esta escala los efectos cuánticos son predominantes.

En el intento de reformular la teoría de información dentro del marco de la mecánica cuántica se encuentran Benioff, Manin y Feynman, quienes expusieron la idea de un computador cuántico. Charles Bennett y Gilles Brassard exploraron la posibilidad de crear sistemas de transmisión de información basados en las leyes de la mecánica cuántica y Arthur Eckert llevó a cabo la misma tarea, pero basándose en la propiedad de entrelazamiento. Este punto marca el nacimiento de la criptografía cuántica

Por último, Peter Shor en 1994, demostró que un ordenador cuántico sería capaz de descomponer un entero en sus factores primos con una complejidad temporal polinómica,

a diferencia de con un ordenador clásico en el que se tiene una complejidad temporal exponencial. Este descubrimiento resultó ser bastante preocupante ya que en la mayoría de los sistemas de criptografía la seguridad recae en la complejidad exponencial que supone descomponer un entero en factores primos. Esto confirmó la importancia de investigar la criptografía cuántica.

### 2.4.2. Introducción matemática

El entorno en el que se desarrolla la mecánica cuántica es los espacios de Hilbert en el campo de los números complejos. Antes de explicar estos es conveniente empezar por los conceptos básicos de espacios vectoriales.

#### 2.4.2.1. Espacio vectorial

Un espacio vectorial ***V*** en el campo de los números complejos es un conjunto no vacío de elementos llamados vectores, para el cual se definen dos operaciones.

1. Adición: la suma de dos vectores pertenecientes al espacio vectorial da como resultado un tercer vector también perteneciente al mismo.
2. Multiplicación por un escalar: al multiplicar un escalar complejo por un vector del espacio se obtiene otro vector también perteneciente al mismo.

#### 2.4.2.2. Subespacio vectorial

Se define como un subconjunto ***S***, no vacío, de un espacio vectorial ***V***, el cual es en sí un espacio vectorial con las mismas operaciones que ***V***.

#### 2.4.2.3. Conjunto generador

Se define como un subconjunto no vacío de ***V*** capaz de generar el subespacio ***S*** a partir de combinaciones lineales de sus vectores [11].

#### 2.4.2.4. Independencia lineal

Un conjunto de vectores es linealmente independiente si ninguno de los vectores puede ser escrito como combinación lineal de los otros [13].

#### 2.4.2.5. Bases

Se define como un subconjunto ***B*** de un espacio vectorial ***V*** constituido por vectores linealmente independientes y capaz de generar dicho espacio ***V***. La dimensión de dicho espacio es igual al número de vectores que tiene la base.

#### 2.4.2.6. Producto interno

Esta operación toma dos vectores de un espacio vectorial ***V*** y da como resultado un número complejo. Se expresa de la siguiente manera:

$$x = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \qquad y^* = [y_1^* \quad y_2^* \quad \dots \quad y_n^*]$$

$$\langle x, y \rangle = \ y^* x = x_1 y_1^* + x_2 y_2^* + \cdots + x_n y_n^* \tag{2.1}$$

#### 2.4.2.7. Espacio de Hilbert

Un espacio de Hilbert ***H*** se define como un espacio vectorial de producto interno completo. Este admite bases ortogonales las cuales permiten generar todo el espacio a través de combinaciones lineales de sus vectores.

#### 2.4.2.8. Notación de Dirac

En la mecánica cuántica, donde se definen los sistemas como espacios de Hilbert, se utiliza la notación de Dirac para representar vectores. Se llama *kets* a los vectores columna y se representan con el símbolo

$$|x\rangle \tag{2.2}$$

Su transpuesto conjugado se llama *bra* y se representa con el símbolo

$$\langle x| = |x\rangle^* \tag{2.3}$$

El producto interno puede expresarse también con esta notación de la siguiente forma:

$$\langle x|y\rangle \tag{2.4}$$

### 2.4.2.9. Operadores lineales

Un operador $\boldsymbol{A}:\boldsymbol{H}\rightarrow\boldsymbol{H}$, desde un espacio de Hilbert $\boldsymbol{H}$ al mismo espacio $\boldsymbol{H}$ es una función que opera sobre un *ket* perteneciente al espacio, por ejemplo $|\alpha\rangle$, y da como resultado otro *ket*, $|\beta\rangle$, también perteneciente, como se muestra en el diagrama de la figura 2.8.


Fig. 2.8. Representación de un operador.

Estos operadores cuentan con propiedades muy parecidas a las de las matrices cuadradas, por lo que es posible asociar a cada operador lineal $\boldsymbol{A}$ una matriz cuadrada $\boldsymbol{A_B}$ de dimensiones coincidentes con las del espacio de Hilbert $\boldsymbol{H}$.

Para realizar esta asociación se fija una base ortonormal $\boldsymbol{B}$ del espacio $\boldsymbol{H}$.

$$B = \{|b_i\rangle, i \in I\} \tag{2.5}$$

Y a través de la relación

$$a_{ij} = \langle b_i|A|b_j\rangle, \qquad |b_i\rangle, |b_j\rangle \in B \tag{2.6}$$

Se pueden definir los elementos $a_{ij}$ de la matriz compleja $A_B = [a_{ij}]$. Esta matriz dependerá de la base $\boldsymbol{B}$ elegida.

Así como se ha determinado la matriz a partir del operador, se puede obtener el operador si se tiene ya la matriz $A_B$. Para esto se debe aplicar la siguiente relación:

$$A = \sum_i \sum_j a_{ij}|b_i\rangle\langle b_j| \tag{2.7}$$

Donde se aplica el producto exterior

$$|b_i\rangle\langle b_j| = \begin{bmatrix} b_{i1} \\ b_{i2} \\ \vdots \\ b_{in} \end{bmatrix} \begin{bmatrix} b_{j1}^* & b_{j2}^* & \dots & b_{jn}^* \end{bmatrix} = \begin{bmatrix} b_{i1}b_{j1}^* & \dots & b_{i1}b_{jn}^* \\ \vdots & & \vdots \\ b_{in}b_{j1}^* & \dots & b_{in}b_{jn}^* \end{bmatrix} \tag{2.8}$$

#### 2.4.2.10. Traza de un operador

Se define como la suma de los elementos de la diagonal de la matriz que representa a dicho operador.

$$Tr[A] = \sum_i \langle b_i|A|b_i\rangle = \sum_i a_{ii} \tag{2.9}$$

La traza del operador es independiente de la base que se haya utilizado, ya que es un parámetro característico del operador.

#### 2.4.2.11. Imagen y rango

La imagen de un operador $\boldsymbol{A}$, definido para un espacio de Hilbert $\boldsymbol{H}$, se define como el conjunto de vectores resultantes de aplicar dicho operador a todos los vectores de $\boldsymbol{H}$. La imagen será un subespacio de $\boldsymbol{H}$.

El rango de un operador será la dimensión de este subespacio vectorial, es decir, la cardinalidad de una base cualquiera que genere dicho subespacio.

#### 2.4.2.12. Autovalores y autovectores

Un autovalor λ de un cierto operador $\boldsymbol{A}$ es un número complejo tal que:

$$A|x_1\rangle = \lambda|x_1\rangle, \qquad |x_1\rangle \in H \quad |x_1\rangle \neq \mathbf{0} \tag{2.10}$$

El vector $|x_1\rangle$ es el autovector correspondiente al autovalor λ. Al conjunto de todos los autovalores de un operador se le llama espectro del operador y el conjunto de autovectores que se corresponden con el mismo autovalor forman un subespacio vectorial llamado autoespacio.

#### 2.4.2.13. Operador adjunto

El operador adjunto de $\boldsymbol{A}$, representado por $\boldsymbol{A}^\dagger$, es una función que opera sobre los *bras*, como por ejemplo $\langle\alpha|$ y $\langle\beta|$, de un espacio de Hilbert $\boldsymbol{H}^\dagger$, asociado a un espacio $\boldsymbol{H}$. Se crea una correspondencia entre cada *ket* perteneciente al espacio $\boldsymbol{H}$ y su *bra* correspondiente, perteneciente a $\boldsymbol{H}^\dagger$. De esta forma cada operador lineal perteneciente a $\boldsymbol{H}$ tiene su correspondiente operador adjunto en $\boldsymbol{H}^\dagger$, según la relación mostrada en la figura 2.9.

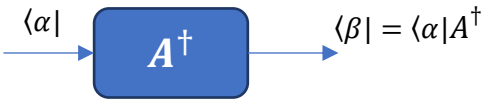


Fig. 2.9. Representación de un operador adjunto.

#### 2.4.2.14. Operadores hermíticos

Un operador ***A***: ***H***→***H*** es hermítico si es igual a su adjunto.

$$A = A^{\dagger} \tag{2.11}$$

Por lo que cualquier matriz asociada a ***A*** será una matriz hermítica, es decir, es igual a su transpuesta conjugada:

$$A_B = [a_{ij}] = [a_{ji}{}^*] = [A_B{}^*]^T \tag{2.12}$$

Una de las propiedades fundamentales de este tipo de operador es que sus autovalores son todos valores reales. Otra característica importante es que los autovectores correspondientes a distintos autovalores son siempre ortogonales, esto trae como consecuencia que los autoespacios de un operador hermítico son ortogonales.

#### 2.4.2.15. Operadores unitarios

Un operador ***U***: ***H***→***H*** es unitario si:

$$UU^* = I_H \tag{2.13}$$

Donde $I_H$ es el operador identidad. Una característica importante es que los autovalores de un operador unitario tienen módulo igual a la unidad.

#### 2.4.2.16. Proyectores

Los proyectores ***P*** son operadores hermíticos sumamente importantes en la mecánica cuántica ya que las medidas se formulan a partir de estos operadores. Los proyectores tienen las siguientes propiedades:

1. Hermíticos: $P = P^{\dagger}$
2. Idempotentes: $P^k = P$, para $k \geq 1$
3. Si *W* es la imagen del operador $P$, un *ket* $|s\rangle$ que pertenezca al subespacio *W* será "inmune" al operador $P$, es decir, $P|s\rangle = |s\rangle$.

4. El espectro de $P$ es siempre $\{0, 1\}$.
5. Semidefinido positivo: $P \geq 0$, es decir, sus autovalores son mayores o iguales a 0.
6. El rango de $P$ y la dimensión del subespacio $W$ vienen dados por la multiplicidad del autovalor 1.
7. La traza de $P$ da el rango del proyector. $Tr[P] = rank(P)$.

Un sistema de proyectores se define como un conjunto de operadores $\{P_i, i \in I\}$ del espacio de Hilbert $\boldsymbol{H}$ que cumple con las siguientes condiciones:

1. Los operadores $P_i$ son proyectores.
2. Son ortogonales por parejas.
3. Su suma es igual a la identidad en $\boldsymbol{H}$. $\sum_i P_i = I_H$.

#### 2.4.2.17. Proyectores elementales

Se puede obtener un sistema de proyectores a partir de una base ortonormal de $\boldsymbol{H}$ $B = \{|b_i\rangle,\ i \in I\}$. Los proyectores elementales $B_i = |b_i\rangle\langle b_i|$ cumplen con los requisitos expuestos anteriormente, son ortogonales por parejas y su suma da como resultado la identidad, $\sum_i B_i = \sum_i |b_i\rangle\langle b_i| = I_H$

#### 2.4.2.18. Teorema de la descomposición espectral

Sea $\boldsymbol{A}$ un operador hermítico en el espacio de Hilbert $\boldsymbol{H}$ y $\{\lambda_i\}, i = 1, 2, \ldots k$ el conjunto de sus distintos autovalores, entonces $\boldsymbol{A}$ puede descomponerse como

$$A = \sum_{i=1}^{k} \lambda_i P_i \tag{2.14}$$

Donde $\{P_i\}$ es un sistema de proyectores.

#### 2.4.2.19. Descomposición en valores singulares (SVD)

La descomposición en valores singulares de una matriz compleja $A$ de dimensiones $m \times n$, viene dada por la siguiente expresión

$$A = UDV^* \tag{2.15}$$

Donde $U$ es una matriz unitaria de dimensiones $m \times n$, $V$ es una matriz unitaria de dimensiones $n \times n$ y $D$ es una matriz diagonal de dimensiones $m \times n$ cuya diagonal se compone de números reales positivos, estos números $d_i$ son los valores singulares de $A$.

También se puede calcular la descomposición en valores singulares reducida según la siguiente expresión

$$A = U_r D_r V_r^* = \sum_{i=1}^{r} d_i |u_i\rangle \langle v_i| \tag{2.16}$$

Donde *r* es el rango de la matriz.

### 2.4.3. Elementos de la mecánica cuántica

En esta sección se comentan tres postulados de la mecánica cuántica, los cuales definen el entorno en el que cualquier sistema físico debe ser descrito, la evolución temporal de dicho sistema y la información que puede ser extraída de este a través de una medida cuántica.

Es importante destacar que estos postulados son abstractos y no dan ninguna explicación sobre como asociar a un sistema físico un espacio de Hilbert.

#### 2.4.3.1. El entorno de la mecánica cuántica

A cada sistema físico cerrado se le debe asociar un espacio de Hilbert $\boldsymbol{H}$ de dimensión apropiada en el campo de los números complejos. En cada instante de tiempo el sistema está completamente descrito por un estado $|\psi\rangle$, dado por un vector unitario de $\boldsymbol{H}$. Para ser unitario, dicho estado debe cumplir con la condición de normalización.

$$\langle \psi | \psi \rangle = 1 \tag{2.17}$$

Debido a la condición de linealidad de los espacios de Hilbert puede ocurrir una superposición de estados, donde, si $|\psi_1\rangle$, $|\psi_2\rangle, \ldots, |\psi_n\rangle$ son estados del espacio $\boldsymbol{H}$, entonces su combinación lineal también es un estado.

$$|\psi\rangle = a_1|\psi_1\rangle + a_2|\psi_2\rangle + \cdots + a_n|\psi_n\rangle \tag{2.18}$$

Siempre que los coeficientes complejos cumplan con la condición de normalización.

$$\sum_i \sum_j a_i^* a_j \langle \psi_i | \psi_j \rangle = 1 \tag{2.19}$$

#### 2.4.3.2. El *qubit*

El *qubit* es uno de los sistemas cuánticos más elementales. Su entorno es un espacio de Hilbert bidimensional, $H = \mathbb{C}^2$, y se define una base utilizando dos vectores ortonormales, $|0\rangle$ y $|1\rangle$.

Un estado genérico de un *qubit* puede expresarse como:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad \alpha, \beta \in \mathbb{C} \tag{2.20}$$

Dado que se cumpla la condición de normalización:

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.21}$$

El *qubit* puede ser comparado con un bit. A los estados del *qubit* $|0\rangle$ y $|1\rangle$ les corresponden los estados 0 y 1 del bit, con la diferencia de que el *qubit* puede encontrarse en una superposición de estados generando infinitos estados posibles, mientras que el bit solo puede encontrarse en dos estados.

#### 2.4.3.3. Estados puros y mixtos

Esta clasificación depende del conocimiento que se tenga del estado del sistema en un instante determinado, este a su vez dependerá del punto de vista del observador.

Cuando el observador conoce el estado del sistema $s = |\psi\rangle \in H$ con seguridad, se dice que es un estado puro. Se puede expresar también como que la probabilidad de que el sistema se encuentre en ese estado es igual a la unidad.

Cuando el observador sabe que el estado en el que se encuentra el sistema pertenece a un subconjunto de $\boldsymbol{H}$, por ejemplo $S = \{|\psi_1\rangle, |\psi_2\rangle, \dots\}$, pero solo sabe el estado específico de forma probabilística, según las probabilidades $p_i := P[s = |\psi_i\rangle]$, se dice que el sistema se encuentra en un estado aleatorio o mixto. Como consecuencia, el estado $s$ del sistema es una variable aleatoria.

Una forma alternativa de describir estos estados es a través del operador de densidad, el cual viene definido por la siguiente ecuación:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{2.22}$$

Este también puede ser utilizado para describir los estados puros, sabiendo que su probabilidad $P[s = |\psi\rangle] = 1$.

$$\rho = |\psi\rangle\langle\psi| \tag{2.23}$$

A continuación, se describen las propiedades de los operadores de densidad:

- Es hermítico, $\rho = \rho^{\dagger}$
- Es semidefinido positivo, $\rho \geq 0$
- Tiene una traza unitaria, $Tr[\rho] = 1$
- $Tr[\rho^2] \leq 1$ y si el sistema se encuentra en un estado puro, $Tr[\rho^2] = 1$

Estos operadores juegan un papel sumamente importante en las comunicaciones. En el extremo transmisor se elige un estado de entre el alfabeto establecido, se define como puro porque es conocido con certeza por el emisor. Si se tiene en cuenta el efecto del ruido térmico en el canal, el estado recibido ya no puede ser descrito como puro por lo que se debe expresar como un operador de densidad.

#### 2.4.3.4. Evolución temporal

La evolución de un sistema cuántico cerrado, es decir, que no se ve influenciado por ningún otro sistema, se encuentra descrita por un operador unitario ***U***. Esta limitación trae como consecuencia que no todas las evoluciones temporales son posibles. Un ejemplo de una acción imposible es la copia o clonación de información [11].

Esto fue demostrado por William Wootters y Woecech Zurek en el teorema de no-clonación, el cual afirma que es imposible crear una copia exacta de un estado cuántico aleatorio desconocido [14].

#### 2.4.3.5. Medidas cuánticas

Los métodos para extraer información de un sistema cuántico vienen descritos por operadores de densidad. En los sistemas de comunicaciones estas medidas se realizan con el fin de extraer la información necesaria para el proceso de decisión.

Es importante recalcar el hecho de que el resultado de dichas medidas es intrínsecamente aleatorio, ya que como se comentó en el experimento del spin, se pueden obtener medidas distintas, aunque se utilice el mismo método de medición sobre dos sistemas preparados de forma idéntica.

#### 2.4.3.6. En términos de estados puros

Una medida cuántica se obtiene a través de un sistema de proyectores $\{\Pi_i, i \in M\}$. $M$ es el alfabeto de todos los posibles resultados de las medidas. Si se mide un sistema que se encuentra en un estado $s = |\psi\rangle$, la probabilidad de que el resultado sea $m = i \in M$ viene dada por

$$p_m(i|\psi) := P[m = i \mid s = |\psi\rangle] = \langle\psi|\Pi_i|\psi\rangle, \qquad i \in M \tag{2.24}$$

Si el resultado es $m = i$, después de la medida el sistema colapsa al estado

$$\left|\psi_{post}^{(i)}\right\rangle = \frac{\Pi_i|\psi\rangle}{\sqrt{\langle\psi|\Pi_i|\psi\rangle}} = \frac{\Pi_i|\psi\rangle}{\sqrt{p_m(i|\psi)}} \tag{2.25}$$

Como el alfabeto *M* es finito, el resultado de la medida *m* se modela como una variable aleatoria discreta.

#### 2.4.3.7. En términos de operadores de densidad

En el caso de que los estados se encuentren descritos en forma de operador de densidad $\rho$, la probabilidad de que el resultado de una medida sea $m = i$, viene dada por

$$P[m = i|\rho] = Tr[\rho\Pi_i], \qquad i \in M \tag{2.26}$$

Donde $\{\Pi_i, i \in M\}$ es un sistema de proyectores. Tras realizar la medida el sistema queda descrito por el siguiente operador de densidad:

$$\rho_{post}^{(i)} = \frac{\prod_i \rho \prod_i}{Tr[\rho \prod_i]} \tag{2.27}$$

#### 2.4.3.8. Medidas con proyectores elementales

Siendo $A = \{|a_1\rangle, |a\rangle, \ldots, |a_M\rangle\}$ una base ortonormal de un espacio de Hilbert de dimensión *M*. Aplicando el producto exterior se obtiene un sistema de proyectores.

$$\Pi_i = |a_i\rangle\langle a_i|, \;\; i = 1, \ldots, M \tag{2.28}$$

La probabilidad de que la medida realizada con estos proyectores elementales dé como resultado $m = i$, cuando el sistema se encuentra en el estado $|\psi\rangle$, es:

$$P[m = i|\psi] = |\langle\psi|a_i\rangle|^2 \tag{2.29}$$

Inmediatamente después de la medida, el estado del sistema colapsa en:

$$|\psi_{post}^{(i)}\rangle = \frac{\Pi_i|\psi\rangle}{|\langle\psi|a_i\rangle|} = \frac{|a_i\rangle\langle a_i|\psi\rangle}{|\langle a_i|\psi\rangle|} = |a_i\rangle\frac{\langle a_i|\psi\rangle}{|\langle a_i|\psi\rangle|} = |a_i\rangle \tag{2.30}$$

El sistema colapsa al estado dado por el *ket* $|a_i\rangle$ ya que la última fracción se reduce a un número complejo de módulo igual a uno.

#### 2.4.3.9. Medidas con observables

En este caso se hará referencia al operador hermítico ***A*** bajo el nombre de *observable.* Un observable combina los proyectores con el alfabeto de medida utilizando el teorema de la descomposición espectral.

Sea ***A*** un observable y $\{a_i, i \in M\}$ el conjunto de sus distintos autovalores. ***A*** puede descomponerse, según el teorema de descomposición espectral, de la siguiente forma:

$$A = \sum_{i \in M} a_i P_i \tag{2.31}$$

Donde $\{P_i, \; i \in M\}$ es un sistema de proyectores. En el caso particular en el que todos los autovalores tengan multiplicidad igual a la unidad, la descomposición se puede expresar en función de proyectores elementales:

$$A = \sum_{i \in M} a_i |a_i\rangle\langle a_i| \tag{2.32}$$

Donde $|a_i\rangle$ son los autovectores de $\boldsymbol{A}$. Por estas propiedades se puede afirmar que el observable $\boldsymbol{A}$ da un sistema de proyectores con el que se pueden realizar medidas cuánticas. La diferencia es que, como ahora el alfabeto está formado por el espectro de $\boldsymbol{A}$, el resultado de cualquier medida será siempre un autovalor del observable.

#### 2.4.3.10. Medidas cuánticas generalizadas (POVM)

En general las medidas cuánticas se hacen utilizando un conjunto de operadores hermíticos, no necesariamente proyectores, los cuales se llaman POVM. Un sistema de POVM $\{Q_i,\ i \in M\}$ se define a partir de las siguientes condiciones impuestas a los operadores $Q_i$:

- Son hermíticos, $Q_i = {Q_i}^\dagger$
- Son semidefinidos positivos, $Q_i \geq 0$
- Su suma es igual a la identidad, $\sum_i Q_i = I_H$

Este sistema constituye una clase más amplia que la de los sistemas de proyectores ya que no es necesario que se cumplan las condiciones de idempotencia ni ortogonalidad, sin embargo, los sistemas de POVM aseguran las mismas probabilidades comentadas anteriormente, tanto para estados puros:

$$P[m = i \mid |\psi\rangle] = \langle\psi|Q_i|\psi\rangle \tag{2.33}$$

Como para estados descritos a través de su operador de densidad:

$$p_m(i|\rho) = P[m = i|\rho] = Tr[\rho Q_i] \tag{2.34}$$

#### 2.4.3.11. Medir un *qubit*

Considerando en este caso un sistema de proyectores elementales $\{\Pi_i, i \in M\}$ cuya base es $B = \{|0\rangle, |1\rangle\}$. La probabilidad de que el resultado de la medida sea $m = i$, para un sistema preparado en un estado $|\psi\rangle$, es igual a $P[m = i|\psi] = |\langle\psi|a_i\rangle|^2$ y el sistema quedará en el estado $|\psi_{post}\rangle = |a_i\rangle$.

Aplicando esto a un *qubit* $|\psi\rangle = a|0\rangle + b|1\rangle$, donde:

$$|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}, \qquad |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}, \qquad \Pi_0 = |0\rangle\langle 0|, \qquad \Pi_1 = |1\rangle\langle 1| \tag{2.35}$$

Se obtiene como resultado de la medida $|0\rangle$ con probabilidad $|a|^2$ o $|1\rangle$ con probabilidad $|b|^2$. Si el resultado de la medida es $m = 0$ el *qubit* colapsa al estado $|\psi_{post}\rangle = |0\rangle$ y si $m = 1$ el *qubit* colapsa $|\psi_{post}\rangle = |1\rangle$.

### 2.4.4. Sistemas de telecomunicaciones

Un sistema de comunicaciones válido tanto para comunicaciones clásicas como cuánticas puede describirse como se muestra en la figura 2.10.

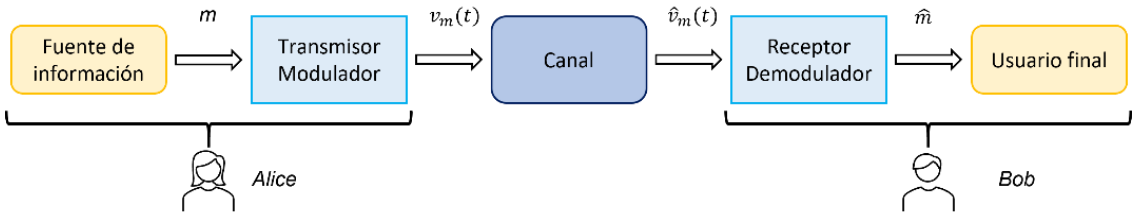


Fig. 2.10. Sistema de comunicaciones.

La fuente de información emite un mensaje $m$, ya sea texto, vídeo, voz, o cualquier otro formato, con el fin de ser enviado a un usuario final que se encuentra a una cierta distancia. El transmisor convierte este mensaje en un estado o una señal $v_m(t)$, como una onda electromagnética, y envía esta señal a través del canal físico. Esta señal se ve afectada por las distorsiones que introduce el canal, como la atenuación y el ruido térmico. Al extremo receptor llega una versión alterada de la señal original transmitida $\hat{v}_m(t)$ y es tarea de este recuperar una réplica del mensaje original $\hat{m}$.

Cuando se trata de sistemas cuánticos, es común llamar al transmisor Alice y al receptor Bob.

#### 2.4.4.1. Transmisión de información analógica

Para transmitir información analógica a través de un sistema digital es necesario aplicar un proceso de muestreo y cuantización.

Se toman muestras de una señal en tiempo continuo a una frecuencia de muestreo igual a al menos el doble del ancho de banda de la señal a muestrear. Se generan una cantidad

finita de niveles entre el valor mínimo y el máximo de la señal y se procede a mapear cada muestra tomada a uno de ellos, siguiendo un criterio de mínima distancia, es decir, a cada muestra se le asignará el valor del nivel que tenga más cerca. Por último, se realiza una conversión a binario para representar el valor de cada nivel con una palabra binaria.

#### 2.4.4.2. Información

El objetivo tanto de las comunicaciones clásicas como de las cuánticas es la transmisión de información clásica.

En el sistema clásico se hace una codificación de clásico a clásico en el transmisor ya que se mapea un símbolo $A$, a una señal física $v_A(t)$. El canal hace el mismo tipo de mapeo ya que a partir de $v_A(t)$ devuelve la versión corrupta $\hat{v}_A(t)$. Por último, el receptor obtiene una réplica del símbolo original $\hat{A}$. Todas las operaciones de este sistema se mantienen dentro del dominio clásico.

En el sistema cuántico no ocurre lo mismo. El transmisor debe ser capaz de preparar tantos estados cuánticos como símbolos tenga el alfabeto a utilizar. Se realiza un mapeo de clásico a cuántico $A \rightarrow \rho_A$ donde $\rho_A$ es el estado cuántico que representa a dicho símbolo. El canal realiza un mapeo de cuántico a cuántico donde se obtiene la versión distorsionada del estado transmitido $\rho_A \rightarrow \hat{\rho}_A$. Para recuperar el símbolo original el receptor debe hacer una medida cuántica para obtener el mapeo de cuántico a clásico $\hat{\rho}_A \rightarrow \hat{A}$.

#### 2.4.4.3. Sistema clásico

En primer lugar, se va a comentar un sistema de comunicaciones clásico funcionando a frecuencias ópticas. Aunque las frecuencias ópticas abarcan desde ultravioleta hasta infrarrojo, una buena parte de las aplicaciones actuales funcionan en el rango de infrarrojo, entre 300GHz y 430THz.

Este tipo de sistemas pueden presentarse utilizando dos escenarios:

1. Considerando la potencia óptica, la cual hace referencia a la potencia óptica promedio $P(t)$.
2. Considerando la potencia óptica instantánea $p(t)$, la cual muestra de forma explícita la presencia de los fotones como cantidades de energía.

#### 2.4.4.4. Considerando potencia óptica promedio

A una cierta frecuencia υ la potencia óptica se calcula según la siguiente ecuación:

$$P(t) = h\upsilon\,\lambda(\mathrm{t}) \tag{2.36}$$

Donde $h = 6{,}626 \times 10^{-34}\ Js$ es la constante de Planck, υ es la frecuencia de trabajo, $h\upsilon$ es la energía de un fotón y λ(t) es la intensidad, dada en fotones por segundo.

Un sistema de comunicaciones clásico sigue el diagrama mostrado en la figura 2.11.

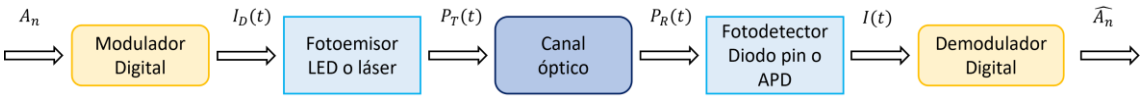


Fig. 2.11. Sistema de comunicaciones clásico.

Se quiere transmitir una secuencia de símbolos $\{A_n\}$. El modulador convierte esta secuencia en una corriente eléctrica $I_D(t)$, esta causa que el LED o láser produzca una potencia óptica $P_T(t)$, la cual se transmite a través de un canal óptico. En el extremo receptor el fotodetector convierte la potencia recibida $P_R(t)$ en una corriente eléctrica $I(t)$. Esta es demodulada para obtener la secuencia original.

Dentro de este escenario se utilizarán transmisiones coherentes donde se aprovecha que la radiación producida por un láser a una frecuencia υ tiene una forma de onda sinusoidal.

$$v_0(t) = V_0 \cos(2\pi\upsilon t + \varphi_0) \tag{2.37}$$

La amplitud de esta da la potencia óptica $P = {V_0}^2$, cuando se normaliza apropiadamente. Uno de los inconvenientes de utilizar las transmisiones coherentes es que se vuelve necesario implementar un láser en el receptor para poder recuperar la portadora sinusoidal.

#### 2.4.4.5. Considerando potencia instantánea

La potencia instantánea permite evaluar de forma explícita los cuantos de energía. Los fotones no llegan al receptor de forma equiespaciada en el tiempo, su llegada ocurre en instantes aleatorios, por lo que resulta conveniente formular estos eventos o llegadas como un proceso de Poisson. Una buena forma de representar una realización de este proceso es a través de un tren de deltas posicionadas en los instantes de llegada.

$$x_\delta(t) = \sum_i \delta(t - t_i) \tag{2.38}$$

El proceso de conteo se realiza integrando esta señal, ya que esto permite obtener el número de llegadas dentro de un intervalo de tiempo.

$$n(s,t] \coloneqq \int_s^t x_\delta(u)du \qquad (s,t]\ \ t > s \tag{2.39}$$

En la figura 2.12 se muestran las llegadas en forma de deltas y el proceso de conteo como funciones escalón de distintas amplitudes.

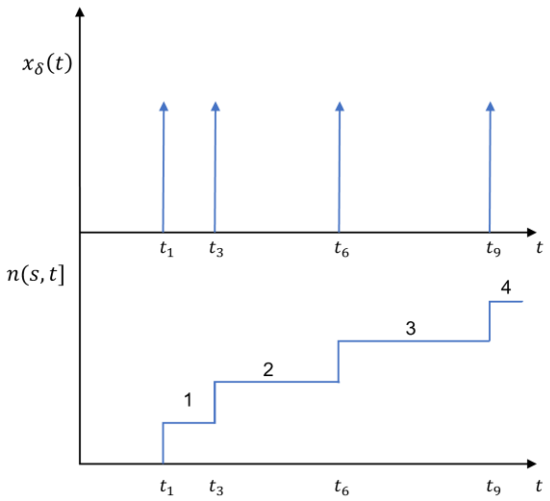


Fig. 2.12. Eventos de un proceso de Poisson y conteo.

Para evaluar la estadística del número de eventos en un intervalo de tiempo arbitrario se debe tener en cuenta que la descripción estadística de un proceso de Poisson se tiene completamente especificada si se conoce su intensidad λ(t).

El número de eventos $n(s,t]$ en un intervalo de tiempo $(s,t]$ es una variable aleatoria de Poisson de media y varianza igual a:

$$\Lambda = E\big[n(s,t]\big] = \int_s^t \lambda(a)da = \ \sigma_n^2 \tag{2.40}$$

Las comunicaciones ópticas se basan en el conteo de fotones en el receptor para poder detectar los diferentes símbolos.

Se considera un contador de fotones ideal que recibe la potencia óptica instantánea de la forma

$$p_R(t) = \sum_i hv\ \delta(t - t_i) \tag{2.41}$$

Y devuelve el número de fotones contados en un intervalo de símbolo. Sabiendo que el conteo de fotones tiene una distribución de probabilidad de Poisson, se puede obtener el número promedio de fotones por símbolo calculando la media

$$N_\gamma = \int_0^T \lambda(t)dt = \frac{1}{hv}\int_0^T P_R(t)dt = \frac{E_T}{hv} \tag{2.42}$$

Donde $E_T$ es la energía óptica en el intervalo (0, T] y $hv$ la energía de un fotón.

#### 2.4.4.6. Envolvente compleja

Una forma eficiente de representar una señal en paso banda es utilizar la envolvente compleja $V(t)$, de forma que la señal a transmitir $v(t)$ se puede expresar de la siguiente manera:

$$v(t) = \Re\{V(t)e^{i\,2\pi\,vt}\} \tag{2.43}$$

La potencia promedio resulta proporcional al módulo al cuadrado de la envolvente y, si se normaliza apropiadamente, se puede expresar directamente como:

$$P(t) = |V(t)|^2 \tag{2.44}$$

De esta representación en forma de envolvente compleja es posible obtener las estadísticas de la potencia promedio $P(t)$ y por ende de la intensidad $\lambda(t)$, la cual brinda, como se ha comentado, la descripción estadística de la llegada de fotones al receptor.

Utilizando este formato el modulador y demodulador, en ausencia de ruido térmico, siguen el esquema mostrado en la figura 2.13.

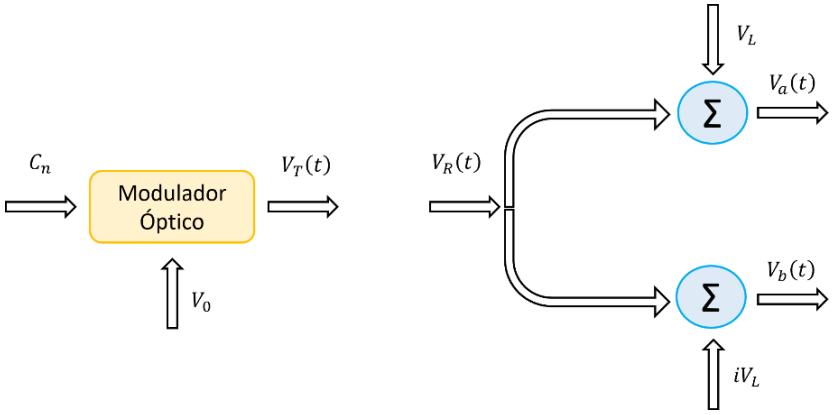


Fig. 2.13. Modulador y demodulador de un sistema clásico en ausencia de ruido térmico.

El modulador toma la secuencia de símbolos $\{C_n\}$, representados por números complejos, y calcula la envolvente compleja de la señal modulada de acuerdo con la siguiente ecuación, la cual se corresponde con la potencia instantánea en el transmisor

$$V_T(t) = \sum_{n=-\infty}^{+\infty} C_n V_0 h(t - nT) \tag{2.45}$$

Donde $V_0$ es la amplitud de la portadora producida por el láser. Si consideramos un único intervalo de tiempo $(0, T)$, la envolvente compleja transmitida es igual a:

$$V_T(t) = C_0 V_0, \qquad 0 < t < T \tag{2.46}$$

En el extremo receptor se recibe una envolvente $V_R(t)$. El demodulador toma esta envolvente compleja y crea dos caminos. Al camino superior se le suma la amplitud $V_L$ y al inferior $iV_L$, donde $V_L$ es la amplitud de la señal introducida por el láser del receptor.

Como resultado, las envolventes complejas obtenidas en cada camino son:

$$V_a(t) = C_0 V_R + V_L, \qquad V_b(t) = C_0 V_R + iV_L \tag{2.47}$$

Donde $V_R$ es la amplitud de la portadora recibida. Esta amplitud será igual a $V_0$ en los casos donde se considere un canal sin atenuación.

El siguiente paso es el conteo de los fotones, el cual dará como resultado dos valores $n_a$ y $n_b$, correspondientes a los dos caminos explicados en la figura 2.13. Se sabe que estos valores son variables de Poisson condicionadas por el símbolo transmitido $C_0$. Sus medias

$\bar{n}_a \coloneqq E[n_a|C_0]$ y $\bar{n}_b \coloneqq E[n_b|C_0]$ se obtienen como se indica en la ecuación 2.42, dividiendo la energía de un periodo de símbolo entre la energía de un fotón.

Para el cálculo de la energía se necesita primero hallar la potencia por lo que se hace uso de la ecuación 2.44, donde esta se obtiene con el módulo al cuadrado de la envolvente compleja

$$P_a = |V_a(t)|^2 = |C_0V_R + V_L|^2 = (A_0V_R + V_L)^2 + (B_0V_R)^2 \tag{2.48}$$

$$P_b = |V_b(t)|^2 = |C_0V_R + iV_L|^2 = (A_0V_R)^2 + (B_0V_R + V_L)^2 \tag{2.49}$$

Donde $C_0 = A_0 + iB_0$.

Como es un valor constante se obtiene la energía multiplicando la potencia por el periodo de símbolo y este resultado se divide entre la energía de un fotón para obtener el número promedio de fotones en cada camino. Si además se considera que la amplitud $V_L$ es mucho mayor que $V_R$, se obtiene

$$\bar{n}_a = \frac{T}{h\nu}\left(2A_0V_RV_L + {V_L}^2\right) \qquad \bar{n}_b = \frac{T}{h\nu}\left(2B_0V_RV_L + {V_L}^2\right) \tag{2.50}$$

Expresando el número de fotones recibidos como $N_R = \frac{T}{h\nu}{V_R}^2$ y el número de fotones aportados por el láser del receptor como $N_L = \frac{T}{h\nu}{V_L}^2$, se puede reescribir la ecuación anterior como

$$\bar{n}_a = 2\sqrt{N_RN_L}A_0 + N_L \qquad \bar{n}_b = 2\sqrt{N_RN_L}B_0 + N_L \tag{2.51}$$

Al componer ambos conteos de fotones en un valor complejo se obtiene la forma estándar de la señal en el punto de decisión y brinda una constelación de valores a recibir con centro en $N_L(i+1)$.

$$z_0 = \bar{n}_a + i\bar{n}_b = 2\sqrt{N_RN_L}C_0 + N_L(i+1) \tag{2.52}$$

Si se realiza, por ejemplo, una modulación BPSK con alfabeto {1, -1} las regiones de decisión son las mostradas en la figura 2.14 [11].

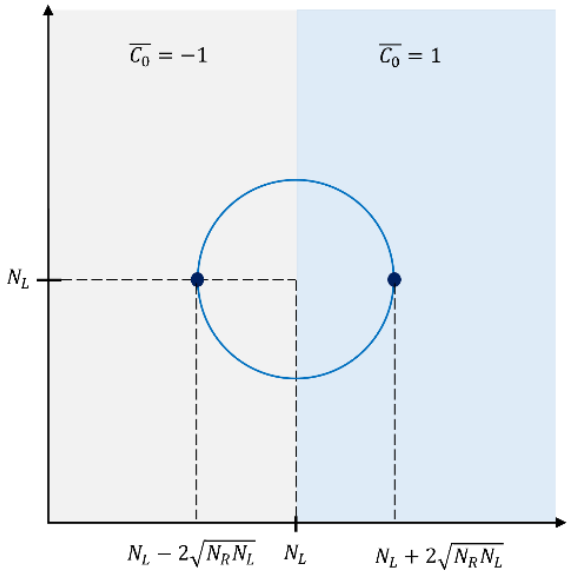


Fig. 2.14. Regiones de decisión para una modulación BPSK.

### 2.4.4.7. Atenuación en la fibra óptica en el sistema clásico

Si se considera el efecto de la atenuación de la fibra óptica se obtiene un valor de $V_R$ distinto de $V_0$. Esta atenuación decrece exponencialmente en función de la distancia *D*. Si se conoce la atenuación $A_F$, expresada en $\frac{dB}{km}$ se puede obtener una relación entre la potencia transmitida y la recibida, de la siguiente manera [15].

$$A_F = \frac{10}{D}\log\left\{\frac{P_{tx}}{P_{rx}}\right\} \quad \rightarrow \quad P_{rx} = P_{tx}\, 10^{-0.1\, A_F\left[\frac{dB}{Km}\right]D[Km]} \tag{2.53}$$

El primer paso es relacionar cada potencia con su amplitud $V_R$ o $V_0$. Esto se hace a través de la relación 2.44 entre la potencia y la envolvente compleja comentada anteriormente. Para un cierto instante de tiempo las envolventes complejas son $V_T(t) = C_0 V_0$ y $V_R(t) = C_0 V_R$, se calcula la potencia como el módulo al cuadrado de cada una

$$P_{rx} = |C_0 V_R|^2 = |C_0 V_0|^2 10^{-0.1\, A_F[\frac{dB}{Km}]D[Km]} = P_{tx}\, 10^{-0.1\, A_F[\frac{dB}{Km}]D[Km]} \tag{2.54}$$

Resolviendo los módulos y despejando las amplitudes se obtiene

$$V_R = V_0 10^{-0.1 A_F[\frac{dB}{Km}]\frac{D}{2}[Km]} \tag{2.55}$$

El valor $A_F$ depende del tipo de fibra óptica y de la frecuencia que se utilice [16]. En la figura 2.15 se pueden observar los distintos valores de este coeficiente de atenuación en función de la longitud de onda.

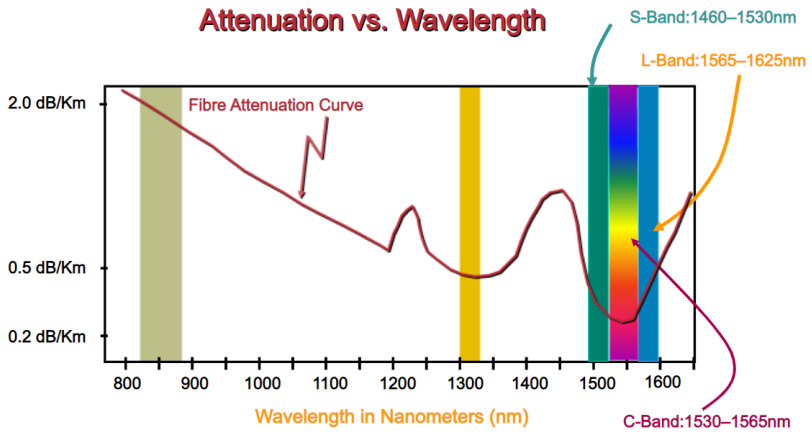


Fig. 2.15. Atenuación en la fibra óptica en función de la longitud de onda [16].

Eligiendo una frecuencia dentro de la ventana de menor atenuación es posible obtener un coeficiente de 0.2 $\frac{dB}{Km}$.

#### 2.4.4.8. Ruido térmico

Un cuerpo en equilibrio térmico produce una radiación electromagnética dentro de un rango de frecuencias y con una intensidad específicos, los cuales dependen únicamente de la temperatura del cuerpo. El punto de máxima intensidad se alcanza a una cierta frecuencia, la cual aumenta a medida que aumenta la temperatura. A temperatura ambiente la radiación se encuentra en la banda infrarroja, mientras que cuando la temperatura supera los 500 ˚C se empiezan a emitir luz visible [17].

En la figura 2.16 se pueden observar las curvas de emisión de cuerpos a distintas temperaturas.

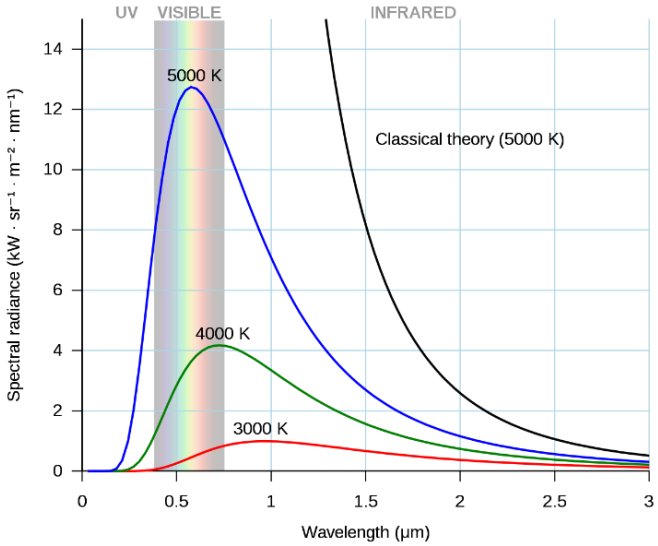


Fig. 2.16. Curvas de emisión [18].

La ley de Planck describe esta radiación electromagnética. La función universal que define esta ley es la densidad de energía espectral

$$u_v(T)dv = \frac{8\pi h v^3}{c^3\left[e^{\frac{hv}{kT}} - 1\right]}dv \tag{2.56}$$

Donde $h$ es la constante de Planck, $v$ es la frecuencia, $k = 1.38 \times 10^{-23}\frac{J}{K}$ es la constante de Boltzmann, $T$ es la temperatura y $c$ es la velocidad de la luz.

Esta ecuación se puede reescribir para definir la energía radiada de la siguiente manera

$$E = \frac{hv}{\left[e^{\frac{hv}{kT}} - 1\right]} \tag{2.57}$$

Y si se divide esta última por la energía de un fotón se puede obtener el número promedio de fotones térmicos radiados por símbolo, para una cierta temperatura $T$ y una frecuencia $v$, como

$$\mathcal{N} = \frac{1}{\left[e^{\frac{hv}{kT}} - 1\right]} \tag{2.58}$$

#### 2.4.4.9. Sistema clásico con ruido térmico

Si se considera el ruido térmico, lo que ocurre es que se modifica la distribución de la llegada de los fotones, esta pasa de ser de Poisson a ser de Laguerre.

El esquema del modulador y demodulador clásico basado en envolvente compleja se mantiene como el que se muestra en la figura 2.13, pero se agrega en cada camino la envolvente compleja del ruido térmico $c_{\eta a}$ y $c_{\eta b}$.

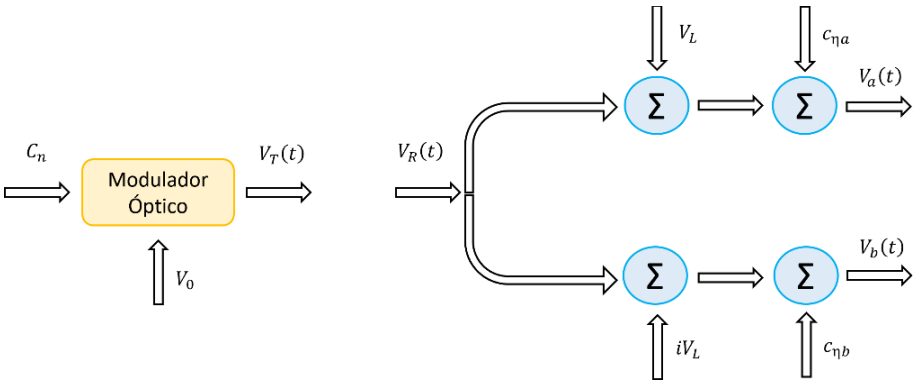


Fig. 2.17. Modulador y demodulador de un sistema clásico en presencia de ruido térmico.

En la salida se obtiene las envolventes complejas correspondientes a cada camino, suponiendo que se realiza la detección del primer símbolo $C_0$ en el intervalo $(0,T]$.

$$V_a(t) = C_0 V_R + V_L + c_{\eta a}, \qquad V_b(t) = C_0 V_R + iV_L + c_{\eta b} \tag{2.59}$$

El número de fotones que se reciben, $n_a$ y $n_b$, en un periodo de símbolo se convierten en variable aleatorias de Laguerre con media y varianza

$$\bar{n}(\gamma) = N_\gamma + \mathcal{N}, \qquad \sigma_n^2(\gamma) = \bar{n}(\gamma) + 2N_\gamma\mathcal{N} + \mathcal{N}^2 \tag{2.60}$$

En este caso, donde se toma en cuenta el ruido térmico, se puede utilizar una aproximación gaussiana. Se muestra a continuación un ejemplo considerando una modulación BPSK.

La señal modulada transmitida en el periodo de símbolo $0 < t < T$ es

$$v_T(t) = \Re C_0 V_0 e^{i2\pi\, \nu t} = V_0 \cos(2\pi\, \nu t + A_0\pi) \tag{2.61}$$

Donde

$$C_0 = e^{iA_0\pi} = \begin{cases} +1 & A_0 = 0 \\ -1 & A_0 = 1 \end{cases} \tag{2.62}$$

En el extremo receptor se obtiene la señal $v_R(t) = V_R \cos(2\pi\, \nu t + A_0\pi)$ y se le añade $V_L \cos(2\pi\, \nu t)$ generada por el láser local, obteniéndose

$$v_R(t) = V_R \cos(2\pi\, \nu t + A_0\pi) + V_L \cos(2\pi\, \nu t) \tag{2.63}$$

De esta señal se calcula la potencia recibida como

$$P_v(t) = V_R^2 + V_L^2 + 2V_R V_L \cos(A_0 \pi) \tag{2.64}$$

Esta potencia se puede convertir en el número de fotones recibidos $N_\gamma(A_0)$ igual que se hizo en la ecuación 2.50 multiplicando por el periodo de símbolo y dividiendo por la energía de un fotón.

$$N_\gamma(A_0) = N_R + N_L + 2\sqrt{N_R N_L}\cos(A_0 \pi) \tag{2.65}$$

Este resultado es el promedio global de fotones recibidos debido a la potencia recibida y a la portadora local. El ruido térmico aporta $\mathcal{N}$ fotones a este promedio.

En conclusión, el número de fotones recibidos tendrá una distribución de Laguerre con las siguientes media y varianza.

$$\bar{n}(A_0) = N_\gamma(A_0) + \mathcal{N}, \qquad \sigma_n^2(A_0) = N_\gamma(A_0) + 2N_\gamma(A_0)\mathcal{N} + \mathcal{N}(\mathcal{N}+1) \tag{2.66}$$

Si se hace una aproximación Gaussiana, se considera que $N_L \gg N_R$ por lo que los valores anteriores se convierten en

$$\bar{n}(A_0) = N_\gamma(A_0) + \mathcal{N}, \qquad \sigma_n^2(A_0) = N_L(2\mathcal{N}+1) \tag{2.67}$$

Este proceso se repite para ambos caminos mostrados en la figura 2.17 y se obtiene

$$z_0 = \bar{n}_a + i\bar{n}_b \tag{2.68}$$

Y se recupera el símbolo según las regiones de decisión mostradas en la figura 2.14.

#### 2.4.4.10. Sistema cuántico sin ruido térmico

En este apartado se procede a explicar el funcionamiento de un sistema de comunicaciones cuántico sin considerar el ruido térmico. Más adelante sí se tomará en cuenta.

En los sistemas cuánticos se utiliza una constelación de *K* estados, donde cada uno representa un símbolo dentro de un alfabeto, este formato es el paralelo a las modulaciones que se utilizan en los sistemas clásicos.

En la figura 2.18 se muestra el diagrama de bloques de un sistema de comunicaciones cuántico para transmisión digital.

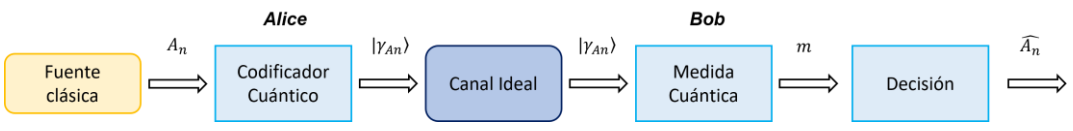


Fig. 2.18. Sistema de comunicaciones cuántico en ausencia de ruido térmico.

Los estados cuánticos son normalmente tratados como estados coherentes de la radiación coherente monocromática emitida por un láser. Estos estados se representan en un espacio de Hilbert de dimensión infinita a través de la base $\{|n\rangle,\ n = 0,\ 1,\ 2 \dots\}$, donde los estados $|n\rangle$ contienen *n* fotones. A esta base se asocia el operador *N* definido como

$$N = \sum_{n=0}^{\infty} n\,|n\rangle\langle n| \tag{2.69}$$

Este operador tiene autovectores $|n\rangle$ con autovalores $n$ y su espectro es $\sigma(N) = \{0,\ 1,\ 2 \dots\}$. A estos estados $|n\rangle$ también se les conoce como estados de Fock.

Un estado coherente genérico se expresa según la siguiente ecuación

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}}\ |n\rangle \tag{2.70}$$

Donde $\alpha$ es una amplitud compleja y su módulo al cuadrado $|\alpha|^2$ es igual al número promedio de fotones en dicho estado.

#### 2.4.4.11. Constelaciones de estados coherentes

Para que Alice pueda transmitir una secuencia de símbolos clásicos de un alfabeto $A$ de K elementos, debe ser capaz de preparar una constelación de K estados coherentes.

Teniendo la constelación de símbolos complejos $C = \{\gamma_0, \gamma_1, \dots, \gamma_{K-1}\}$, se forma la constelación de estados coherentes $S = \{|\gamma_0\rangle, |\gamma_1\rangle, |\gamma_2\rangle, \dots, |\gamma_{K-1}\rangle\}$, con correspondencia uno a uno con los símbolos complejos.

Como se ha mencionado antes, el número promedio de fotones de un estado coherente $|\gamma\rangle$ viene dado por el módulo al cuadrado de su amplitud

$$N_\gamma = |\gamma|^2 \tag{2.71}$$

Cuando se habla de constelación de estados se introduce el número promedio de fotones por símbolo $N_s$. Considerando que los símbolos son equiprobables, el valor $N_s$ se calcula como

$$N_s = \frac{1}{K} \sum_{i \in A} |\gamma_i|^2 \tag{2.72}$$

#### 2.4.4.12. Factores de forma y de escala

La constelación de símbolos complejos $C$ comentada anteriormente se encuentra afectada por un factor de escala asociado a la intensidad de fotones, sin embargo, las modulaciones se suelen expresar en forma normalizada. La constelación normalizada se obtiene dividiendo la constelación original entre el factor de escala Δ, obteniéndose

$$C_0 = \{\bar{\gamma}_0, \bar{\gamma}_1, \dots, \bar{\gamma}_{K-1}\} \tag{2.73}$$

Este factor de escala aparece también en el número promedio de fotones por símbolo $N_s$ como

$$N_s = \frac{1}{K}\sum_{\gamma \in C} |\gamma|^2 = \Delta^2 \frac{1}{K}\sum_{\bar{\gamma} \in C_0} |\bar{\gamma}|^2 = \mu_K \Delta^2 \tag{2.74}$$

Donde

$$\mu_K = \frac{1}{K}\sum_{\bar{\gamma} \in C_0} |\bar{\gamma}|^2 \tag{2.75}$$

Es el factor de forma. En particular, en modulaciones de tipo PSK será igual a la unidad.

#### 2.4.4.13. Atenuación en la fibra óptica en el sistema cuántico

En la ecuación 2.53 se muestra la relación entre la potencia recibida y transmitida debido a los efectos de la atenuación propia de la fibra. En el caso clásico se trató este decremento de potencia como un decremento en la amplitud $V_0$ de la portadora, en el caso cuántico se trata como un decremento en el número promedio de fotones del estado cuántico $|\gamma\rangle$ transmitido.

La potencia de la señal transmitida se expresa como

$$P_{t_x} = hv|\gamma|^2 \tag{2.76}$$

La potencia recibida se calcula como

$$P_{r_x} = hv|\gamma_r|^2 = hv|\gamma|^2 10^{-0.1 A_F[\frac{dB}{Km}] D[Km]} \tag{2.77}$$

Y se despeja la amplitud compleja del estado cuántico para obtener la siguiente ecuación

$$\gamma_r = \gamma 10^{-0.1 A_F \left[\frac{dB}{Km}\right]^{\frac{D}{2}}[Km]} \tag{2.78}$$

#### 2.4.4.14. Decisión cuántica con estados puros

En el emisor, se pueden agrupar los estados coherentes de una constelación en una matriz de estados $\Gamma$, donde

$$\Gamma = [|\gamma_0\rangle, |\gamma_1\rangle, |\gamma_2\rangle, \dots, |\gamma_{K-1}\rangle] \tag{2.79}$$

En el extremo receptor, Bob debe realizar una medida cuántica sobre el estado que recibe, para esto necesita un sistema de operadores de medida $Q_i$ que minimice lo más posible la probabilidad de error.

Como se está considerando primero un sistema con estados puros, los operadores de medida serán elementales, es decir, de la forma $Q_i = |\mu_i\rangle\langle\mu_i|$, por lo que es suficiente con buscar los vectores de medida $|\mu_i\rangle$ que conforman la matriz de medida

$$M = [|\mu_0\rangle, |\mu_1\rangle, \dots, |\mu_{K-1}\rangle] \tag{2.80}$$

Para encontrar estos vectores se aplica una técnica de suboptimización llamada "Square Root Measurement" o SRM, ya que las técnicas de optimización presentan una mayor dificultad.

En SRM se eligen los vectores de medida $|\mu_i\rangle$ intentando que la diferencia $|e_i\rangle$ entre estos y los estados $|\gamma_i\rangle$ sea lo más pequeña posible, como se muestra en la figura 2.19.

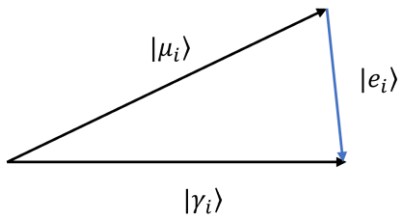


Fig. 2.19. Error entre el vector de medida y los estados.

Se busca específicamente minimizar el error cuadrático, el cual puede calcularse como

$$\varepsilon = Tr[EE^*] = Tr[E^*E] \tag{2.90}$$

Donde $E = \Gamma - M = [|e_0\rangle, |e_1\rangle, \dots, |e_{K-1}\rangle]$

La matriz de medida $M_{opt}$ que minimiza este error se puede calcular como

$$M_{opt} = U_r V_r^* \tag{2.91}$$

Donde $U_r$ y $V_r^*$ se obtienen calculando la SVD reducida de la matriz de estados

$$\Gamma = U_r D_r V_r^* \tag{2.92}$$

Una vez obtenida la matriz de medida se puede calcular la probabilidad de decisión correcta a partir de esta y de la matriz de estados.

$$P_c = \sum_{i \in A} q_i Tr[b_{ii}^* b_{ii}] \tag{2.93}$$

Donde la matriz $B = {M_{opt}}^* \Gamma$.

#### 2.4.4.15. Sistema cuántico con ruido térmico

Considerando ahora el ruido térmico el diagrama de bloques de la figura 2.18 se modifica para incluir los estados mixtos representados a través de operadores de densidad. El nuevo diagrama se muestra en la figura 2.20.

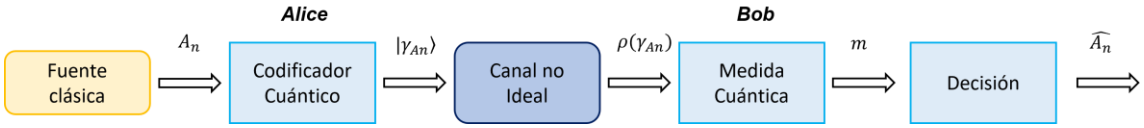


Fig. 2.20. Sistema de comunicaciones cuántico en presencia de ruido térmico.

Al igual que para el caso sin ruido, Alice prepara un conjunto de estados coherente, los cuales son estados puros ya que son conocidos con certeza por ella. Sin embargo, Bob no recibirá los mismos estados puros ya que el ruido térmico elimina esa certeza. Por esta razón se describen los estados utilizando operadores de densidad.

Para calcular el operador de densidad se siguen las siguientes ecuaciones:

$$\rho(\gamma) = \sum_{m=0}^{\infty} \sum_{n=0}^{\infty} R_{mn}(\gamma) |m\rangle\langle n| \tag{2.94}$$

Los coeficientes $R_{mn}(\gamma)$ se calculan como

$$R_{mn}(\gamma) = \begin{cases} \frac{\mathcal{N}^n}{(\mathcal{N}+1)^n}\sqrt{\frac{m!}{n!}}\left(\frac{\gamma^*}{\mathcal{N}}\right)^{n-m} exp\left(-\frac{|\gamma|^2}{\mathcal{N}+1}\right) L_m^{(n-m)}\left(1-\frac{|\gamma|^2}{\mathcal{N}}\right), & m \leq n \\ R_{mn}^*(\gamma), & m > n \end{cases} \quad (2.95)$$

Donde $\mathcal{N}$ es el número promedio de fotones térmicos, $|\gamma|^2$ es el número promedio de fotones del estado, $|n\rangle$ y $|m\rangle$ representan estados de Fock y $L_m^{(n-m)}(x)$ es un polinomio de Laguerre generalizado de grado *m*, cuya expresión es:

$$L_m^{(n-m)}(x) = \sum_{k=0}^{m}(-1)^k \frac{(2m-n)!}{(n-m-k)!\,(n-k)!}x^k \quad (2.96)$$

De estas expresiones se puede verificar que la media del resultado de la medida *m* es:

$$E[m|\rho(\gamma)] = |\gamma|^2 + \mathcal{N} = N_\gamma + \mathcal{N} \quad (2.97)$$

La cual concuerda con el número promedio global de fotones. La varianza de *m* es:

$$\sigma_n^2\big(\rho(\gamma)\big) = N_\gamma + 2N_\gamma\mathcal{N} + \mathcal{N}(\mathcal{N}+1) \quad (2.98)$$

De estas expresiones se puede concluir que el conteo de fotones en un sistema cuántico descrito por un operador de densidad $\rho(\gamma)$ viene dado por una variable aleatoria de Laguerre y esta solo pasa a ser de Poisson en ausencia de ruido térmico.

#### 2.4.4.16. Discretización de operadores de densidad

Para poder trabajar con estos operadores se vuelve necesario realizar un proceso de discretización que permita representar, de forma aproximada, un operador de densidad de dimensión infinita como una matriz cuadrada de dimensión finita $n \times n$, de la siguiente forma:

$$\rho(\gamma) \cong \sum_{h=0}^{n-1}\sum_{k=0}^{n-1} R_{hk}(\gamma)|h\rangle\langle k| \coloneqq R(\gamma) \quad (2.99)$$

Para garantizar que se realiza una buena aproximación se sigue el criterio de la traza. La traza de un operador de densidad debe ser siempre igual a la unidad, por lo que, solo si $Tr[R] \cong 1$ se considera la aproximación como adecuada.

Con esta aproximación se calcula una constelación de operadores de densidad que recoge los posibles estados ruidosos que recibirá Bob.

$$S_\rho = \{\rho_0, \rho_1, \dots, \rho_{K-1}\} \tag{2.100}$$

Donde cada operador se corresponde con uno de los estados coherentes en la constelación

$$S = \{|\gamma_0\rangle, |\gamma_1\rangle, \dots, |\gamma_{K-1}\rangle\} \tag{2.101}$$

#### 2.4.4.17. Decisión en la presencia de ruido térmico

Al igual que en el caso clásico, el objetivo es calcular los operadores de medida $Q_i$ óptimos, es decir, aquellos que minimizan la probabilidad de error.

Para lograr esto se toma cada operador de densidad $\rho_i$, de dimensión $n \times n$, de la constelación $S_\rho$ y se factoriza en un factor $\beta_i$ de dimensión $n \times h_i$, donde $h_i$ es el rango de $\rho_i$.

Suponiendo un operador de densidad genérico $\rho$, su factorización $\rho = \beta\beta^*$ puede obtenerse a través de la EID reducida

$$\rho = Z_h^2 D_h^2 Z_h^2 = \sum_{i=1}^{h} d_i^2 \, |z_i\rangle\langle z_i| \tag{2.102}$$

Donde $D_h^2 = diag[d_1^2, d_2^2, \dots, d_h^2]$ es una matriz diagonal de dimensiones $h \times h$, la cual contiene los autovalores positivos de $\rho$ y $Z_h = [|z_1\rangle \, |z_2\rangle \dots |z_h\rangle]$ tiene dimensiones $n \times h$. El factor se obtiene como $\beta = Z_h D_h$, donde $D_h = \sqrt{D_h^2} = diag[d_1, \dots, d_h]$.

Una vez factorizado cada operador, se compone la matriz de estados como

$$\Gamma = [\beta_0, \beta_1, \dots, \beta_{K-1}] \tag{2.103}$$

Los operadores óptimos de medida $Q_i$ también pueden ser factorizados como $Q_i = \mu_i \mu_i^*$, donde $\mu_i$ son los factores de medida que componen la matriz de medida

$$M = [\mu_0, \mu_1, \dots, \mu_{K-1}] \tag{2.104}$$

Al igual que en el caso de los estados puros esta matriz óptima se puede calcular como

$$M_{opt} = U_r V_r^* \tag{2.105}$$

Donde $U_r$ y $V_r^*$ se obtienen calculando la SVD reducida de la matriz de estados

$$\Gamma = U_r D_r V_r^* \tag{2.106}$$

La probabilidad de decidir correctamente se calcula igual que en la ecuación 2.93.

### 2.4.4.18. Comparación de la probabilidad de error clásica y cuántica para una modulación BPSK

La probabilidad de error se calcula como uno menos la probabilidad de acierto. Tomando para el sistema cuántico la probabilidad de acierto mostrada en la ecuación 2.93, específicamente para una modulación BPSK con símbolos equiprobables, se obtiene una probabilidad de error igual a

$$P_{e\_Q} = 1 - P_c = 1 - \frac{1}{2}\sum_{i\in A} Tr[b_{ii}^* b_{ii}] = 1 - \frac{1}{2}(Tr[b_{11}^* b_{11}] + Tr[b_{22}^* b_{22}]) \quad (2.107)$$

La probabilidad de error para el sistema clásico se obtiene aplicando la función $Q$ a la raíz de la relación señal a ruido $\Lambda$. Para calcular esta probabilidad en la presencia de ruido térmico basta con decrementar dicha relación señal a ruido por el factor $1 + 2\mathcal{N}$, donde $\mathcal{N}$ es el número de fotones térmicos. La expresión final resulta

$$P_{e\_C} = Q\left(\sqrt{\frac{\Lambda}{1+2\mathcal{N}}}\right) = Q\left(\sqrt{\frac{4N_s}{1+2\mathcal{N}}}\right) \quad (2.108)$$

En la figura 2.21 se muestra una comparación de la probabilidad de error de un sistema con modulación BPSK en función del número de fotones por símbolo $N_s$ y para distintos valores de $\mathcal{N}$.

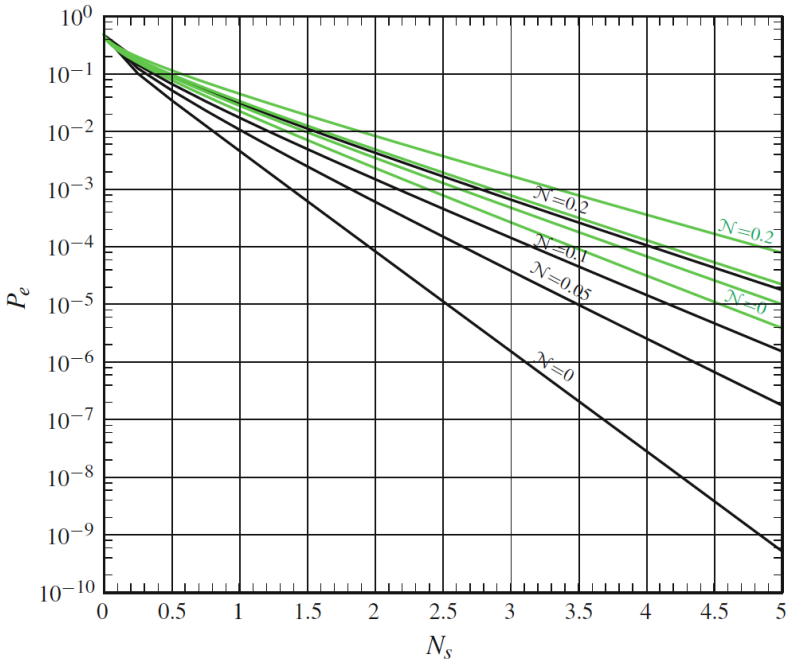


Fig. 2.21. Comparación de la probabilidad de error de un sistema con modulación BPSK en función $N_s$ y de $\mathcal{N}$ [11].

Las líneas verdes representan el sistema clásico y las negras, el cuántico. En la gráfica se puede apreciar la superioridad del sistema cuántico sobre el clásico, sobre todo para valores muy pequeños de fotones térmicos.

#### 2.4.4.19. Límite de Helstrom

Este límite indica la menor probabilidad de error que es posible alcanzar en un sistema cuántico utilizando una modulación BPSK. Para obtenerlo se empieza calculando el operador de decisión $D = \frac{1}{2}(\rho_1 - \rho_0)$, suponiendo un sistema bajo condiciones ideales y una probabilidad a priori equiprobable. La probabilidad de error que se obtiene es

$$P_e = 1 - P_c = 1 - \left(\frac{1}{2} + \sum_{\lambda_k > 0} \lambda_k\right) = \frac{1}{2} - \sum_{\lambda_k > 0} \lambda_k \tag{2.109}$$

Donde $\lambda_k$ son los autovalores del operador $D$ [11].

### 2.4.5. Criptografía

La criptografía busca alterar las representaciones de los mensajes que se desean transmitir con el propósito de volverlos ininteligibles a receptores no autorizados. El objetivo principal de la criptografía es lograr que los mensajes sean confidenciales a través del uso de códigos de cifrado y que solo puedan ser descifrados por el transmisor y receptor, a través de una clave secreta [19].

Actualmente, la criptografía representa el principal mecanismo para proteger la información frente a posibles espías. Para protegerla se utilizan algoritmos criptográficos clásicos que solo son capaces de garantizar que un espía, con limitada capacidad computacional, tiene una baja probabilidad de éxito si realiza un ataque contra un protocolo de seguridad en un tiempo razonable. Esto quiere decir que, si la cantidad de tiempo que el espía necesita para descifrar el protocolo de seguridad es considerablemente mayor que el tiempo de vida útil de la información, entonces se puede decir que el protocolo es seguro.

El problema se encuentra en que estos protocolos no ofrecen seguridad a largo plazo ya que se ven amenazados por posibles avances tecnológicos [11].

Algunos de los algoritmos más usados como el RSA, el cual basa su seguridad en la dificultad computacional de factorizar un entero muy grande [20], pueden llegar a poner

en peligro la seguridad de la información ya que se ha demostrado que son vulnerables ante la computación cuántica gracias a que el algoritmo de Shor es capaz de descomponer en factores un número muy grande en tiempo polinómico [21].

#### 2.4.5.1. Libreta de un solo uso

También conocido como "One-time pad", es un tipo de algoritmo de cifrado el cual toma el texto y lo combina con una clave para cifrarlo, este, en teoría, es indescifrable si la clave cumple con las siguientes condiciones:

- La clave es tan larga como el mensaje.
- La clave se utiliza una sola vez.
- La clave es completamente aleatoria.
- La clave es solo conocida por el emisor y receptor.

Utilizando criptografía clásica se pueden cumplir fácilmente los dos primeros requisitos, sin embargo, el tercer requisito se vuelve complicado ya que los generadores de números aleatorios actuales están basados en algoritmos, por lo que solo dan como resultado cadenas pseudoaleatorias. Si un tercero conociese el algoritmo y la semilla con que se ha cifrado la información, esta estaría en peligro.

La cuarta condición también representa un problema ya que la transmisión clásica de una clave abre las puertas a posibles interceptaciones [22]. En teoría, nada podría evitar que un espía con infinito poder computacional monitorice pasivamente el establecimiento de la clave secreta y decodifique el mensaje que se transmite [23].

#### 2.4.5.2. Criptografía cuántica

Con el objetivo de resolver estos problemas aparece la criptografía cuántica, la cual permite cumplir los últimos dos requisitos utilizando los principios de la mecánica cuántica.

El tercero queda cubierto ya que la física cuántica hace posible la verdadera aleatoriedad, por ejemplo, un único fotón es reflejado o transmitido por un divisor de haz de forma completamente arbitraria [22].

Por último, el cuarto requisito se cumple debido al anteriormente mencionado teorema de la no-clonación. La monitorización pasiva de señales desconocidas transmitidas se encuentra prohibida en la mecánica cuántica debido a que los procesos de medida no son

procesos pasivos ni externos. Un espía que intenta robar información sobre estados cuánticos causará casi siempre alteraciones en las señales cuánticas transmitidas [23].

#### 2.4.5.3. Distribución de claves cuánticas (QKD)

Para que Alice y Bob puedan establecer una clave secreta aleatoria se utilizan protocolos de distribución de claves cuánticas, los cuales se basan en las propiedades de la mecánica cuántica antes mencionadas. A continuación, se comentarán tres de los protocolos más conocidos: el BB84, BB84 eficiente y el de Eckert.

#### 2.4.5.4. Protocolo BB84

En primer lugar, se definen dos bases donde cada una tiene dos polarizaciones de luz, dando como resultado cuatro posibles polarizaciones para cada fotón. Como se muestra en la figura 2.22, la base "+" contiene las polarizaciones 0˚ y 90˚ y la base "×", las polarizaciones -45˚ y 45˚ [22].

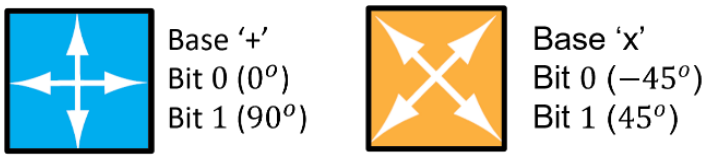


Fig. 2.22. Base "+" y "×" de polarización [22].

Cada base puede utilizarse para representar un '0' binario como 0˚ o -45˚, o un '1' binario como 90˚ o 45˚.

Alice prepara una secuencia de bits aleatoria como clave y tanto Alice como Bob eligen las secuencias de bases, de forma aleatoria y uniforme, que utilizarán para transmitir y medir cada uno de los fotones. Esto quiere decir que la elección de la base es una variable aleatoria y que ambas bases tienen la misma probabilidad de ser escogidas [23].

Alice procede a transmitir cada fotón en la polarización correspondiente a la base escogida y Bob realiza una medida cuántica siguiendo la secuencia de bases que ha elegido. Una vez enviados todos los fotones, Alice y Bob intercambian a través de un canal público las secuencias de bases que han utilizado.

Todos los fotones en los que las bases de Alice y Bob no coincidan son descartados ya que la medida que obtendrá Bob en estos casos será '0' o '1' aleatoriamente. Los restantes, en los que las bases sí coinciden, conforman la clave de cifrado ya que al ser medidos con la misma base con la que han sido polarizados se obtiene la medida correcta el 100% de

las veces [22]. Debido a que las bases son equiprobables y aleatorias, la eficiencia de este protocolo es del 50%, es decir, se descarta la mitad de los bits que son transmitidos [23].

En la figura 2.23 se muestra un ejemplo del establecimiento de clave utilizando este protocolo.

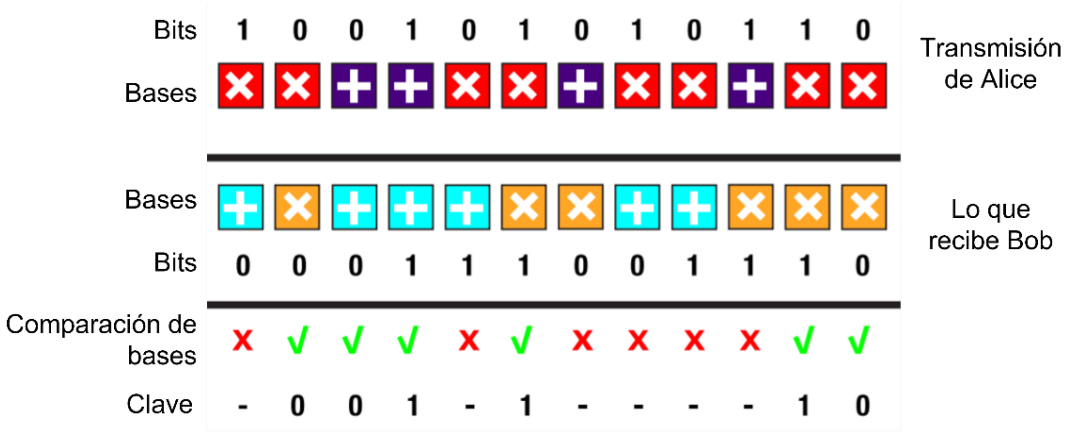


Fig. 2.23. Ejemplo establecimiento de clave, sin espía, con el protocolo BB84 [22].

Este protocolo también implementa un mecanismo que permite detectar la intervención de un espía, al cual se hará referencia como Eva. Eva, al igual que Alice y Bob, elegirá una secuencia de bases de forma aleatoria y uniforme que utilizará para medir los fotones transmitidos por Alice y enviar fotones a Bob. Al terminar de enviar los fotones, Alice y Bob intercambiarán las bases utilizadas, igual que se ha explicado anteriormente, pero, se enviarán también unos cuantos bits de prueba tomados de la secuencia que queda como clave. De no haber un espía, todos los bits de prueba deberían coincidir, pero, en caso de que sí haya un espía, Alice y Bob pueden descubrirlo si aproximadamente el 25% de los bits de prueba comparados son incorrectos. Si se detecta un espía la clave establecida es descartada y el proceso de distribución comienza de nuevo.

Una vez establecida una clave segura Alice procede a encriptar la información realizando una operación XOR entre el mensaje y la clave. Luego, transmite la secuencia resultante utilizando siempre la base "+". Bob mide los fotones recibidos con la base "+" y aplica la misma operación para desencriptar la información [22].

En la figura 2.24 se muestra un ejemplo de este protocolo para 18 bits. Se puede ver que siempre que un fotón es medido con una base distinta a la que se utilizó para polarizarlo se obtiene '0' o '1' aleatoriamente y en los casos donde las bases coinciden se mide correctamente el 100% de las veces. Las flechas verdes indican todos los bits en los que las bases de Alice y Bob coinciden, según la teoría, estos bits deberían coincidir, sin

embargo, debido a la presencia de un espía, que introduce más aleatoriedad, se puede observar que Alice y Bob obtienen bits incorrectos un 30% de las veces, aproximadamente.

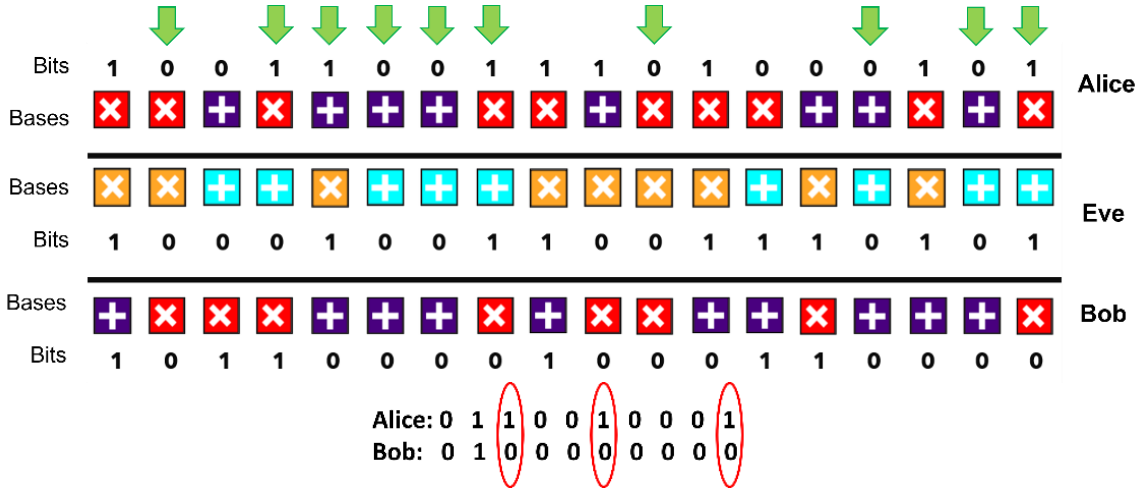


Fig. 2.24. Ejemplo de establecimiento de clave, con espía, con el protocolo BB84.

### 2.4.5.5. Descripción matemática del protocolo BB84

Las cuatro polarizaciones pueden escribirse utilizando la notación de Dirac de la siguiente manera: $|-45°\rangle, |0°\rangle, |45°\rangle, |90°\rangle$.

Los estados pueden representarse como vectores

$$|0°\rangle = \begin{pmatrix}0\\1\end{pmatrix}, \qquad |90°\rangle = \begin{pmatrix}1\\0\end{pmatrix} \tag{2.110}$$

O como combinación lineal

$$\begin{aligned} |45°\rangle &= \frac{1}{\sqrt{2}}|0°\rangle + \frac{1}{\sqrt{2}}|90°\rangle, \qquad |-45°\rangle = \frac{1}{\sqrt{2}}|0°\rangle - \frac{1}{\sqrt{2}}|90°\rangle \\ |0°\rangle &= \frac{1}{\sqrt{2}}|45°\rangle + \frac{1}{\sqrt{2}}|-45°\rangle, \qquad |90°\rangle = \frac{1}{\sqrt{2}}|45°\rangle - \frac{1}{\sqrt{2}}|-45°\rangle \end{aligned} \tag{2.111}$$

Para que Bob pueda realizar las medidas se introducen dos operadores $M_+$ y $M_x$, donde

$$\begin{aligned} M_+ &= |0°\rangle\langle 0°| - |90°\rangle\langle 90°| \\ M_x &= |45°\rangle\langle 45°| - |-45°\rangle\langle -45°| \end{aligned} \tag{2.112}$$

Cuando se miden los estados $|0°\rangle$ y $|90°\rangle$ con el operador $M_+$ se obtiene

$$M_+|0^o\rangle = |0°\rangle\langle 0°|0°\rangle - |90°\rangle\langle 90°|0°\rangle = |0°\rangle$$

$$M_+|90^o\rangle = |0^\circ\rangle\langle 0^\circ|90^\circ\rangle - |90^\circ\rangle\langle 90^\circ|90^\circ\rangle = -|90^\circ\rangle$$

Los resultados obtenidos son los esperados, la medida devuelve el estado inicial multiplicado por un autovalor 1 o -1. El mismo resultado se obtiene cuando se miden los estados $|45^\circ\rangle$ y $|-45^\circ\rangle$ con el operador $M_x$

$$M_x|45^o\rangle = |45^\circ\rangle\langle 45^\circ|45^\circ\rangle - |-45^\circ\rangle\langle -45^\circ|45^\circ\rangle = |45^\circ\rangle$$

$$M_x|-45^o\rangle = |45^\circ\rangle\langle 45^\circ|-45^\circ\rangle - |-45^\circ\rangle\langle -45^\circ|-45^\circ\rangle = -|-45^\circ\rangle$$

Hasta ahora se ha corroborado la teoría explicada por el protocolo para los casos en los que las bases coinciden, pero ¿qué ocurre cuando no coinciden? Como ejemplo se va a medir un fotón en el estado $|0^o\rangle$ con el operador de medida $M_x$

$$M_x|0^o\rangle = |45^\circ\rangle\langle 45^\circ|\left(\frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|-45^\circ\rangle\right) - |-45^\circ\rangle\langle -45^\circ|\left(\frac{1}{\sqrt{2}}|45^\circ\rangle + \frac{1}{\sqrt{2}}|-45^\circ\rangle\right)$$

$$= \frac{1}{\sqrt{2}}|45^\circ\rangle\langle 45^\circ|45^\circ\rangle + \frac{1}{\sqrt{2}}|45^\circ\rangle\langle 45^\circ| - 45^\circ\rangle - \frac{1}{\sqrt{2}}|-45^\circ\rangle\langle -45^\circ|45^\circ\rangle$$

$$- \frac{1}{\sqrt{2}}|-45^\circ\rangle\langle -45^\circ|-45^\circ\rangle$$

$$M_x|0^o\rangle = \frac{1}{\sqrt{2}}|45^\circ\rangle - \frac{1}{\sqrt{2}}|-45^\circ\rangle$$

Con este resultado se puede ver que si se mide el estado $|0^o\rangle$ con el operador $M_x$ se obtendrá $|45^\circ\rangle$ o $|-45^\circ\rangle$ con un 50% de probabilidad, es decir, se obtiene '0' o '1' aleatoriamente. En la figura 2.25 se muestra una tabla resumen de todos los posibles resultados que se pueden obtener cuando Eva intercepta los bits entre Alice y Bob.

| Alice | | Eve | | | Bob | | |
|---|---|---|---|---|---|---|---|
| Basis, Bit | State | Basis | State | State Sent | Basis | State | Measured Bit |
| +, 0 | $\|0°\rangle$ | + | $\hat{M}_+ \|0°\rangle = \|0°\rangle$ | $\|0°\rangle$ | + | $\hat{M}_+ \|0°\rangle = \|0°\rangle$ | 0 |
| | | | | | × | $\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ | 0 or 1 |
| | | × | $\hat{M}_\times \|0°\rangle = \frac{\|45°\rangle}{\sqrt{2}} - \frac{\|-45°\rangle}{\sqrt{2}}$ | $\|45°\rangle$ or $\|-45°\rangle$ | + | $\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ or $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$ | 0 or 1<br>0 or 1 |
| | | | | | × | $\hat{M}_\times \|45°\rangle = \|45°\rangle$ or $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$ | 1<br>0 |
| +, 1 | $\|90°\rangle$ | + | $\hat{M}_+ \|90°\rangle = -\|90°\rangle$ | $\|90°\rangle$ | + | $\hat{M}_+ \|90°\rangle = -\|90°\rangle$ | 1 |
| | | | | | × | $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$ | 0 or 1 |
| | | × | $\hat{M}_\times \|90°\rangle = \frac{\|45°\rangle}{\sqrt{2}} + \frac{\|-45°\rangle}{\sqrt{2}}$ | $\|45°\rangle$ or $\|-45°\rangle$ | + | $\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ or $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$ | 0 or 1<br>0 or 1 |
| | | | | | × | $\hat{M}_\times \|45°\rangle = \|45°\rangle$ or $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$ | 1<br>0 |
| ×, 1 | $\|45°\rangle$ | + | $\hat{M}_+ \|45°\rangle = \frac{\|0°\rangle}{\sqrt{2}} - \frac{\|90°\rangle}{\sqrt{2}}$ | $\|0°\rangle$ or $\|90°\rangle$ | + | $\hat{M}_+ \|0°\rangle = \|0°\rangle$ or $\hat{M}_+ \|90°\rangle = -\|90°\rangle$ | 0<br>1 |
| | | | | | × | $\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ or $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$ | 0 or 1<br>0 or 1 |
| | | × | $\hat{M}_\times \|45°\rangle = \|45°\rangle$ | $\|45°\rangle$ | + | $\hat{M}_+ \|45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle - \frac{1}{\sqrt{2}}\|90°\rangle$ | 0 or 1 |
| | | | | | × | $\hat{M}_\times \|45°\rangle = \|45°\rangle$ | 1 |
| ×, 0 | $\|-45°\rangle$ | + | $\hat{M}_+ \|-45°\rangle = \frac{\|0°\rangle}{\sqrt{2}} + \frac{\|90°\rangle}{\sqrt{2}}$ | $\|0°\rangle$ or $\|90°\rangle$ | + | $\hat{M}_+ \|0°\rangle = \|0°\rangle$ or $\hat{M}_+ \|90°\rangle = -\|90°\rangle$ | 0<br>1 |
| | | | | | × | $\hat{M}_\times \|0°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle - \frac{1}{\sqrt{2}}\|-45°\rangle$ or $\hat{M}_\times \|90°\rangle = \frac{1}{\sqrt{2}}\|45°\rangle + \frac{1}{\sqrt{2}}\|-45°\rangle$ | 0 or 1<br>0 or 1 |
| | | × | $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$ | $\|-45°\rangle$ | + | $\hat{M}_+ \|-45°\rangle = \frac{1}{\sqrt{2}}\|0°\rangle + \frac{1}{\sqrt{2}}\|90°\rangle$ | 0 or 1 |
| | | | | | × | $\hat{M}_\times \|-45°\rangle = -\|-45°\rangle$ | 0 |

Fig. 2.25. Tabla resumen de la descripción matemática del protocolo BB84 [22].

En los casos sombreados en verde Alice, Eva y Bob han elegido las mismas bases por lo que Eva es capaz de leer el bit correctamente y además pasar desapercibida.

Todos los casos sombreados en amarillo son descartados ya que las bases de Alice y Bob no coinciden.

En color azul se muestran los casos en los que, pese a que Eva no tiene la misma base que Alice y Bob, esta logra pasar desapercibida.

Por último, en rojo se muestran los casos donde Alice y Bob tienen la misma base y Eva ha introducido error, por lo que es detectada [22].

#### 2.4.5.6. Protocolo BB84 eficiente

Este protocolo es una variante del BB84 y la principal diferencia es que las bases dejan de ser equiprobables con el objetivo de reducir el porcentaje de bits que son descartados [23].

Se utilizan las mismas dos bases mencionadas anteriormente, la base "+" y la base "×", sin embargo, se hace referencia a ellas como la base mayoritaria y la minoritaria, respectivamente. Esto se debe a que la base "+" tendrá una probabilidad mayor, igual a $p$ y será la utilizada para establecer la clave, y la base "x" tendrá una probabilidad $1 - p$ y se utilizará para detectar al espía [11].

Es importante remarcar la importancia de elegir la probabilidad $p$ adecuadamente, ya que el protocolo se vuelve claramente inseguro si $p = 1$. Sin embargo, el protocolo afirma que para grandes cantidades de fotones este esquema de bases no equiprobables es seguro incluso si la probabilidad de la base minoritaria tiende a cero [23].

El proceso de preparar, transmitir y medir cada fotón es igual al explicado en el protocolo BB84, la diferencia está en que la clave no se establece con todos los bits donde coincidan las bases. Alice y Bob se intercambian por un canal público las bases que utilizaron para medir cada fotón, descartan todos aquellos bits en los que las bases no coinciden y generan dos grupos separados de bits cuyas bases sean iguales. Los bits donde ambos hayan usado la base mayoritaria se utilizarán como clave y en los que coincida la base minoritaria se guardarán como grupo de prueba. Estos bits de prueba se intercambian por el mismo canal público, lo que le permite a Alice y a Bob detectar al espía tras compararlos.

Al igual que en el protocolo anterior, se puede introducir a Eva. Ella puede elegir sus bases con las mismas probabilidades que Alice y Bob ya que este valor puede ser acordado usando un canal público, sin embargo, lo mejor que podría hacer es elegir la base mayoritaria únicamente, ya que esto le asegura medir correctamente todos los bits que se utilizarán en la clave.

Aunque esto parece representar una ventaja para el espía hay que considerar el efecto que tiene esto en los bits que se utilizarán como prueba. La probabilidad de que Eva pase desapercibida observando todos los bits es igual a la probabilidad de que no exista ningún error en los bits donde Alice y Bob hayan utilizado la base minoritaria. Esta es muy baja

ya que Eva ha elegido medir todos los bits con la base mayoritaria, lo que significa que está introduciendo aleatoriedad en cada uno de los bits de prueba.

Una vez establecida la clave con seguridad se procede a cifrar el mensaje y transmitirlo utilizando solo una base [11].

#### 2.4.5.7. Protocolo de Eckert

Este protocolo se basa en el principio de entrelazamiento cuántico. Este afirma que dos partículas pueden entrelazarse de tal manera que al medir una de ellas, el estado opuesto se podrá observar en la otra inmediatamente, sin importar la distancia que las separe. Sin embargo, resulta imposible predecir antes de medir qué estado se observará, por ende, no es posible comunicarse a través de partículas entrelazadas sin utilizar un canal clásico para discutir las observaciones.

El protocolo describe un canal en el cual una fuente emite una pareja de fotones entrelazados, como se muestra en la figura 2.26. Alice y Bob reciben, cada uno, un fotón de la pareja entrelazada y proceden a medirlo utilizando una base aleatoria. A través de canal clásico se intercambian la secuencia de bases que usaron, descartando los resultados obtenidos con bases que no coincidan. Para las medidas en donde utilizaron la misma base Alice y Bob esperan obtener cadenas opuestas, debido al principio de entrelazamiento. Si los resultados obtenidos se interpretan como bits, entonces cada uno tendrá una cadena de bits que será complemento de la otra. Basta con que uno de ellos invierta su clave para obtener la clave secreta compartida.

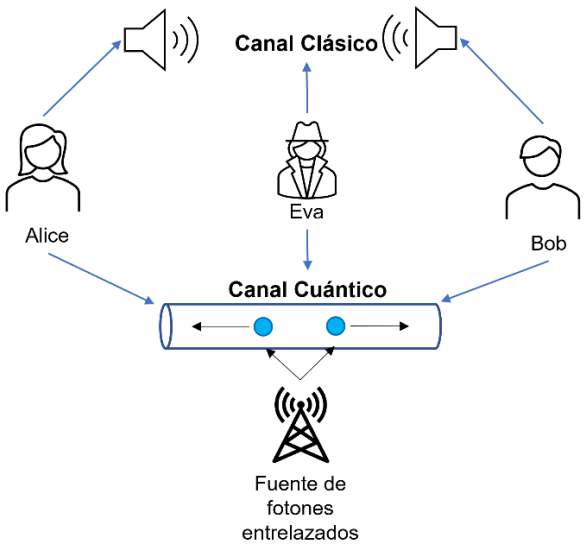


Fig. 2.26. Esquema del protocolo de Eckert.

La detección de un espía se realiza igual que en el protocolo BB84, Alice y Bob se intercambian a través del canal clásico una parte de los bits de la clave secreta, si al compararlos descubren que no hay ningún error se puede decir que no ha habido interceptación y que la clave es segura [24].

### 2.4.6. Aplicaciones actuales de la criptografía cuántica

Actualmente, existen varios ejemplos en el mundo de sistemas que han implementado protocolos de distribución de claves cuánticas para asegurar su información. En este epígrafe se comentarán los siguientes:

1. La red cuántica DARPA.
2. Satélite Micius.
3. Primera red cuántica de tres nodos.

#### 2.4.6.1. Red cuántica DARPA

Esta fue la primera red de distribución de claves cuánticas del mundo, con 10 nodos ópticos entre Boston y Cambridge.

Esta red era compatible con la tecnología de internet estándar (2002-2007) y además era capaz de proveer claves para crear VPNs.

En la primera etapa se diseñó y construyó un sistema completo del protocolo BB84 de distribución de claves cuánticas de dos nodos, Alice y Bob [25]. Para el segundo año ya se había construido la versión de cuatro nodos, agregando a Anna y Boris a los dos nodos anteriores. Esta red permitía conectar a cualquier transmisor con cualquier receptor a través de fibra óptica. En la figura 2.27 se puede ver la localización de los distintos nodos.

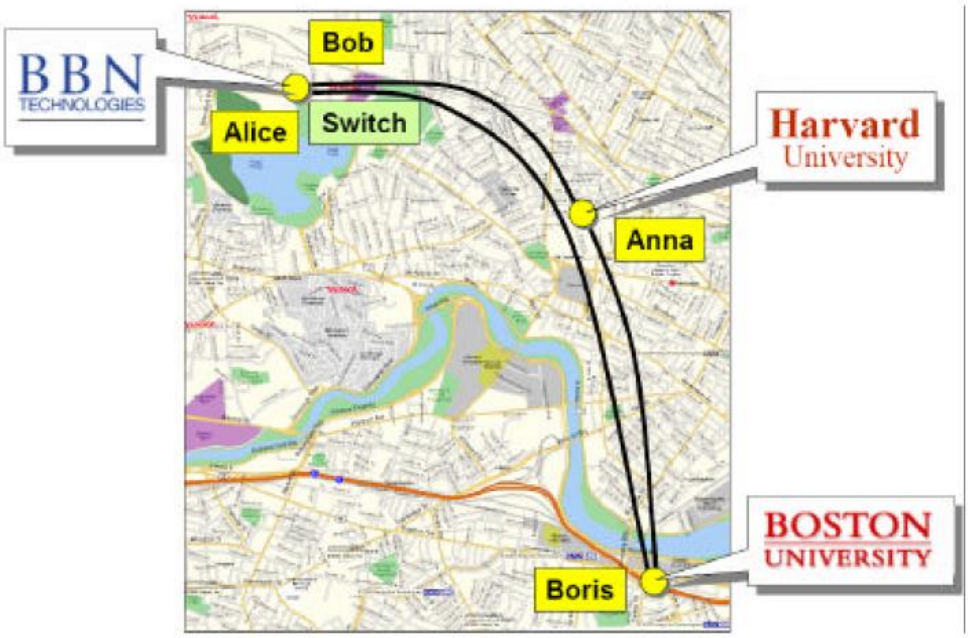


Fig. 2.27. Localización de cuatro nodos de la red DARPA [26].

En los siguientes años se agregaron los otros seis nodos, cuatro de ellos, Ali, Baba, Amanda y Brian, conectados a través de espacio libre y utilizando también el protocolo BB84. Los últimos dos, Alex y Barb, conectados a través de espacio libre se utilizaron para implementar un protocolo basado en entrelazamiento cuántico.

La variedad de protocolos implementados en esta red permitió el estudio de las propiedades de cada uno [25].

#### 2.4.6.2. Satélite Micius

Este satélite fue lanzado en agosto de 2016 como una de las misiones que China planteó en su programa de experimentos cuánticos a escala espacial. En el primer experimento el satélite emitió parejas de fotones entrelazados para ser enviados a dos estaciones receptoras en tierra, una en Delingha y otra en Lijiang, separadas 1200 km. Estas dos estaciones se encuentran localizadas en las montañas del Tibet lo que redujo la cantidad de aire que los fotones tuvieron que atravesar.

Siguiendo un protocolo de distribución de claves cuánticas basado en entrelazamiento estas dos estaciones fueron capaces de establecer una clave de cifrado segura [27]. En la figura 2.28 se muestra un gráfico detallando el experimento.

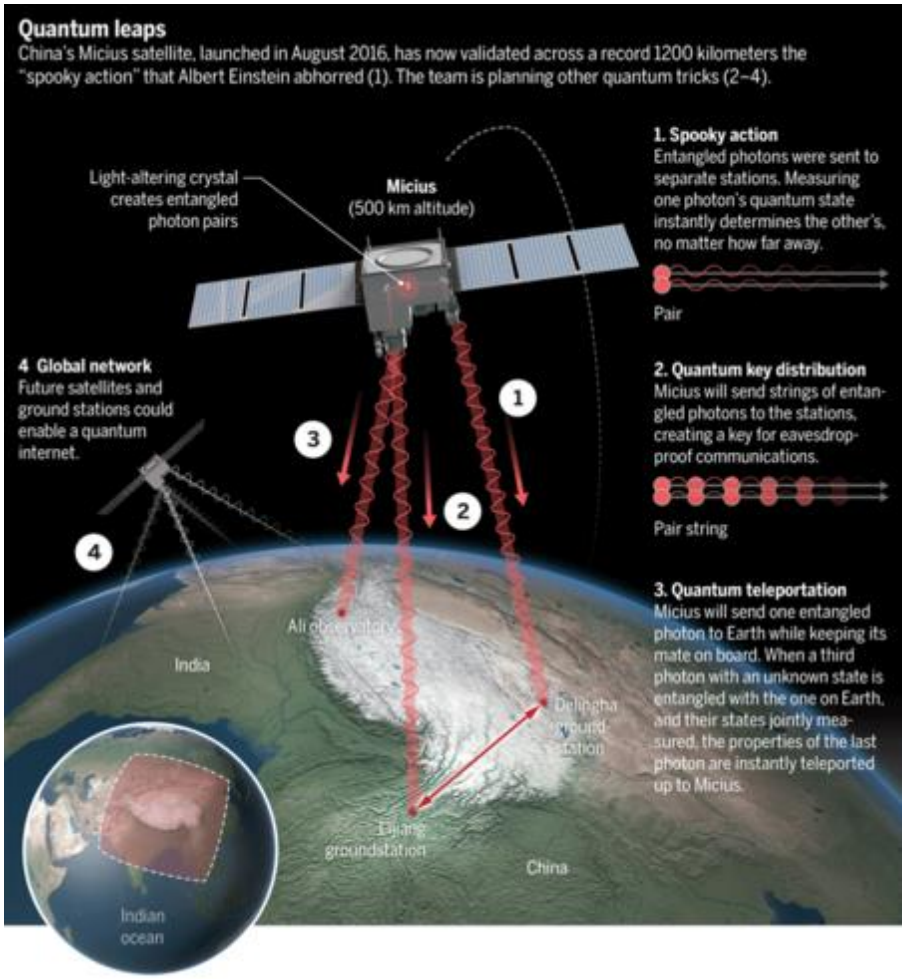


Fig. 2.28. Experimento realizado con el satélite Micius [27].

#### 2.4.6.3. Red cuántica multinodo basada en entrelazamiento cuántico

Investigadores del centro de investigación QuTech en Holanda crearon este sistema formado por tres nodos cuánticos entrelazados como se muestra en la figura.

Esto representa un gran avance hacia la posibilidad de un internet cuántico en el futuro. Pese a que todavía no estaría listo para aplicaciones prácticas, sí muestra una técnica clave que permitirá la conexión de nodos separados a largas distancias.

En esta red de tres nodos cualquier pareja puede obtener *qubits* mutuamente entrelazados. También se demostró que en los tres nodos se pueden colocar *qubits* en un estado de entrelazamiento triple lo que les permite a los tres usuarios compartir información de forma secreta.

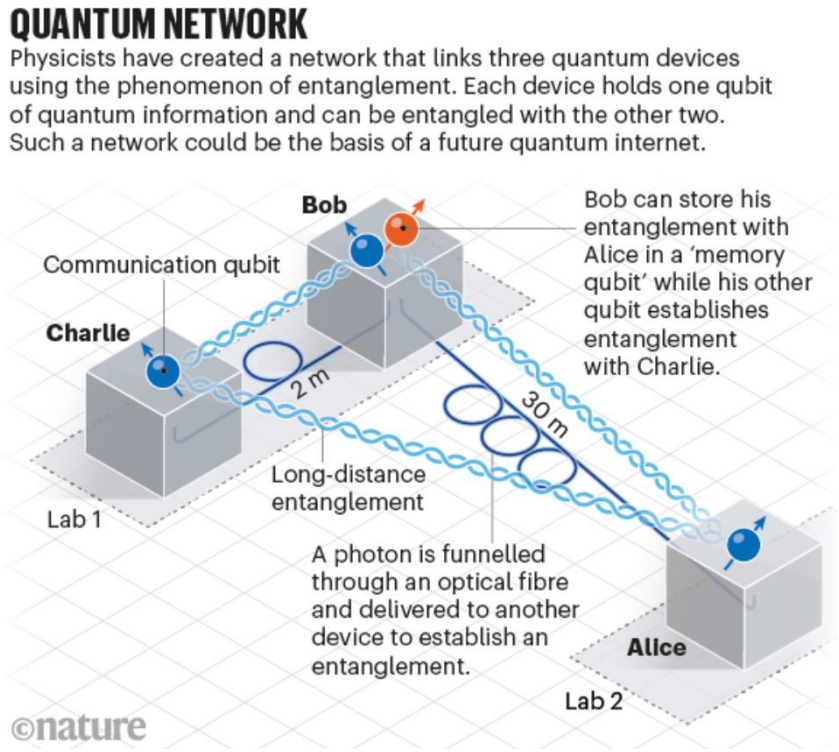


Fig. 2.29. Red cuántica basada en entrelazamiento [28].

Una de las cosas más importantes de esta red es que uno de los tres nodos también se utiliza para guardar información en una especie de "memoria cuántica". Esto se logra utilizando el isotopo no radioactivo carbono-13 como un *qubit* de memoria. Se logró preparar el núcleo de carbono en distintos estados cuánticos específicos, convirtiéndolo en un *qubit* adicional. Estas memorias cuánticas de carbono son capaces de mantener el estado por alrededor de un minuto, lo que en el mundo de las partículas es una eternidad [29].

# 3. DESARROLLO

En este capítulo se expone, en primer lugar, el funcionamiento del kit de demostración de criptografía cuántica, el cual permite comprender el protocolo BB84 de distribución de claves cuánticas.

En la segunda parte, se explica cómo funciona el emulador de un sistema de criptografía cuántica desarrollado.

## 3.1. Kit de demostración de criptografía cuántica

El "Quantum Cryptography Demonstration Kit" de Thorlabs permite simular los principios de la criptografía cuántica. Con él se puede simular el establecimiento de una clave y la detección de un espía descritos en el protocolo BB84.

El aspecto cuántico del protocolo recae en la utilización de una fuente de fotones únicos, donde la información de un bit se codifica en el estado de dicho fotón haciendo que este no pueda ser copiado. Aunque este experimento funciona con un láser de pulsos el funcionamiento es idéntico al que se obtendría con un sistema cuántico, por lo que resulta muy útil para comprender el protocolo.

El esquema de las partes del kit se muestra en la figura 3.1 y, en la figura 3.2, se puede apreciar el montaje real del experimento.

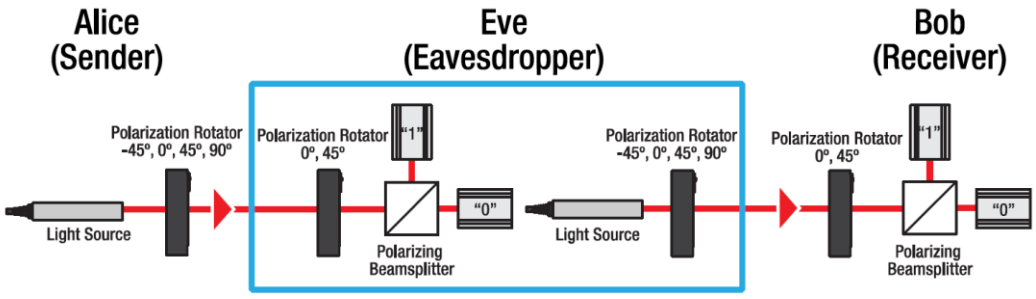


Fig. 3.1. Esquema del kit de demostración de criptografía cuántica [22].

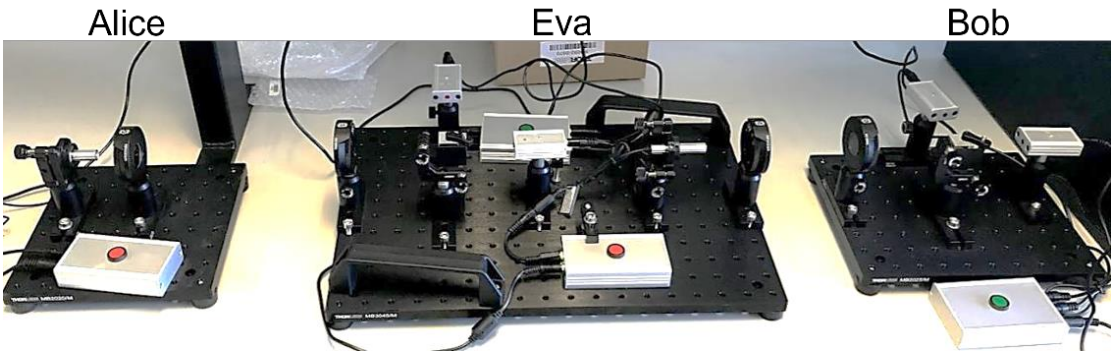


Fig. 3.2. Montaje del kit.

El transmisor, Alice, cuenta con un láser, cuya polarización inicial es horizontal (0°) y un rotador de polarización que le permite seleccionar en qué base transmite cada bit.

El bloque intermedio, Eva, cuenta primero con una parte para medir lo que ha recibido de Alice y luego una para transmitir nuevos bits a Bob. Para medir cuenta con un rotador de polarización, con el que elige si medir en base "+" o en base "×", un cubo divisor de haz que permite la transmisión o reflexión de la luz hacia dos sensores, los cuales indicarán qué bit se ha recibido. En su parte de transmisión cuenta con los mismos componentes que Alice.

El receptor, Bob, cuenta con los mismos componentes que la parte receptora de Eva.

A continuación, se comentan los elementos que componen el experimento y sus funciones:

- Láser: este se encuentra polarizado horizontalmente y tiene dos modos de uso. El primero es el modo de onda continua, el cual facilita la alineación de los otros elementos. El segundo modo, es el de pulsos cortos y es el que se utiliza en la simulación del protocolo. En la figura 3.3 se muestra el láser.

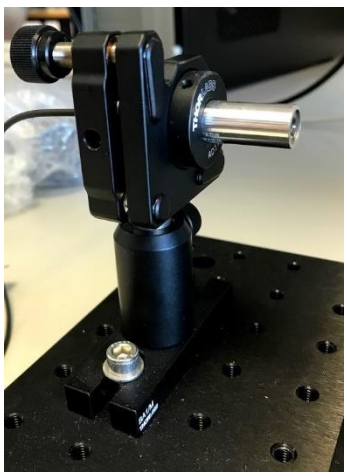

Fig. 3.3. Láser.

- Plato de $\frac{\lambda}{2}$: este plato de cristal hace que la polarización de la luz incidente rote un valor el doble de grande de lo que se rota físicamente. Por ejemplo, si el plato se rota 45˚ la polarización de la luz incidente rotará 90˚. En las figuras 3.4 y 3.5 se muestran los dos tipos de platos de $\frac{\lambda}{2}$ que utiliza el experimento. El primero, sirve para polarizar los fotones antes de transmitirlos en una de las cuatro direcciones, -45˚, 0˚, 45˚ o 90˚. El segundo sirve para rotar la polarización justo antes de recibirlos, si se elige 0˚, se estará usando la base "+" para medir y si se elige 45˚, la base "×".


Fig. 3.4. Plato de polarización de cuatro direcciones.


Fig. 3.5. Plato de polarización de dos direcciones.

- Divisor de haz: este es un cubo divisor de haz, el cual permite el paso de la componente de luz incidente polarizada horizontalmente (0˚) y refleja la componente polarizada verticalmente (90˚). Un fotón que atraviese el divisor representará al bit '0' mientras que el reflejado representa el '1'. En la figura 3.6 se muestra el cubo divisor de haz en su base.

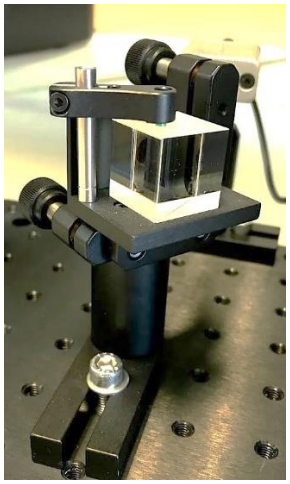

Fig. 3.6. Divisor de haz.

- Sensores: cada parte receptora en el esquema cuenta con dos sensores, uno para indicar que se ha recibido el bit ‘0’ (transmitido) y otro para el ‘1’ (reflejado). Esta indicación se hace mediante un LED que tienen en la parte superior. Los sensores cuentan también con dos modos. En el modo de ajuste, si a ambos sensores llega la misma intensidad de luz se encenderán ambos LEDs. En el modo de medida se encendería solo uno, escogido aleatoriamente. Este efecto es el que permite simular la “decisión” de un único fotón que es transmitido o reflejado por el divisor de haz con un 50% de probabilidad. En la figura 3.7 se muestran los sensores [22].

Fig. 3.7. Sensores.

### 3.1.1. Ejemplos del funcionamiento del kit

Para demostrar que el kit logra simular el protocolo BB84 correctamente se plantean a continuación una serie de ejemplos, mostrados en la tabla 3.1, en ellos se supone que no hay un espía presente.

TABLA 3.1. EJEMPLOS DE TRANSMISIÓN DE BITS ENTRE ALICE Y BOB

| | | | |
|---|---|---|---|
| **Alice** | + | + | + |
| | 0 | 1 | 0 |
| **Bob** | + | + | × |

En el primero Alice transmitirá un ‘0’ en base “+”, es decir una polarización horizontal 0˚ y Bob lo medirá con la misma base. Según lo explicado en el protocolo, Bob debe obtener como resultado el mismo bit ‘0’ transmitido por Alice. En la figura 3.8 se muestra un esquema de lo que ocurre al realizar este ejemplo.

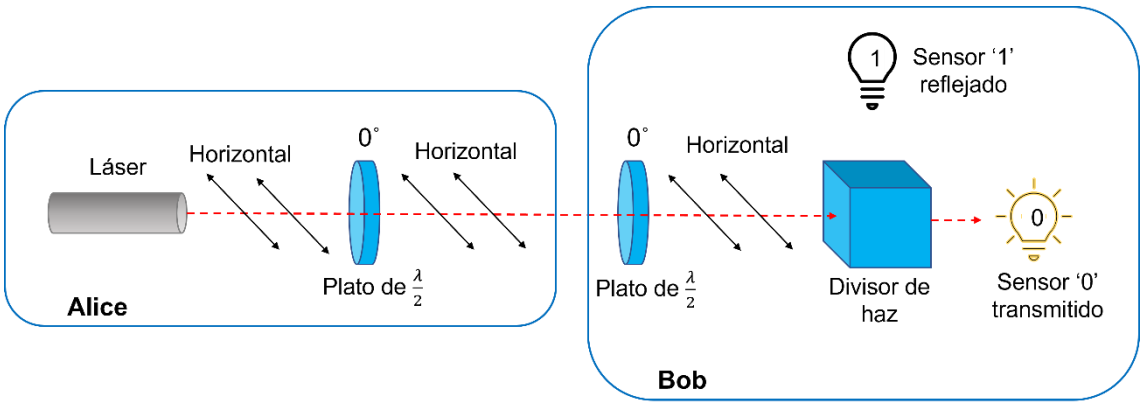


Fig. 3.8. Ejemplo de la transmisión de un ‘0’ en base “+”, medido con base “+”.

La luz inicialmente se encuentra polarizada horizontalmente, al atravesar el plato su polarización no cambia, ya que se ha elegido transmitir un bit ‘0’ en base “+”. Como Bob mide en la misma base la polarización no se ve afectada y al llegar al divisor de haz, lo atraviesa, activando el sensor de bit ‘0’.

El siguiente ejemplo se muestra en la figura 3.9, este solo se diferencia del anterior en que ahora Alice desea transmitir un ‘1’ en vez de un ‘0’.

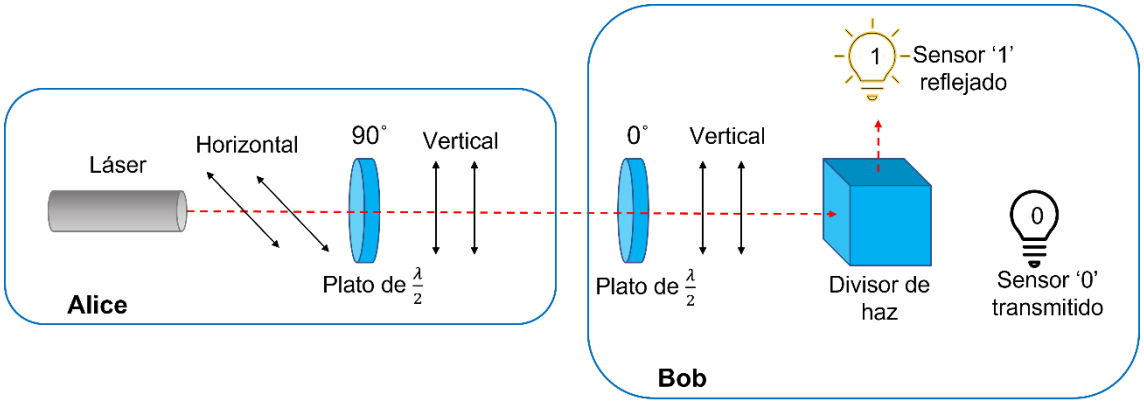


Fig. 3.9. Ejemplo de la transmisión de un '1' en base "+", medido con base "+".

El plato de Alice rota la polarización horizontal del láser 90˚ y el de Bob no la altera. Como la luz incidente en el divisor de haz tiene ahora una polarización vertical, esta es reflejada activando el sensor de bit '1' y dando el resultado correcto.

En el último ejemplo, mostrado en la figura 3.10, Bob medirá el fotón recibido con la base incorrecta por lo que la medida debería ser aleatoriamente '0' o '1'.

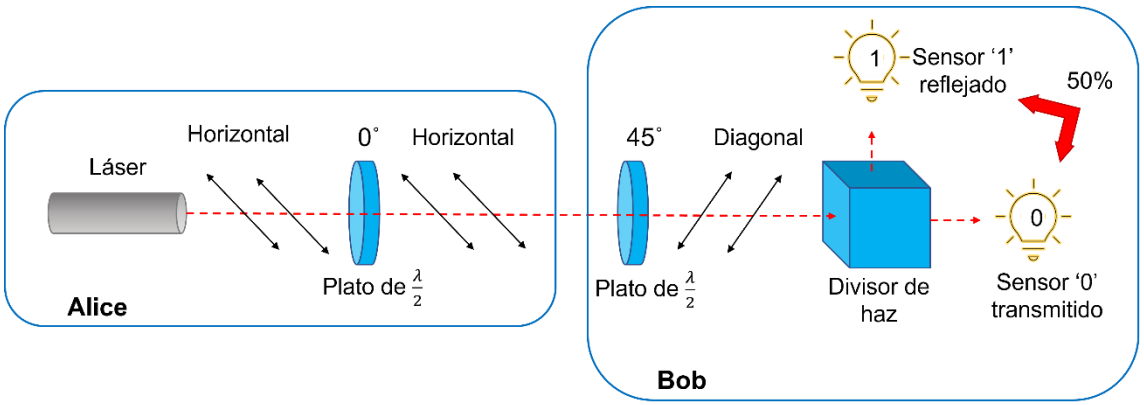


Fig. 3.10. Ejemplo de la transmisión de un '0' en base "+", medido con base "×".

En este caso el plato de Bob rota 45˚ el fotón transmitido por Alice a 0˚, al incidir en el divisor la componente horizontal se transmite mientras que la vertical se refleja, causando que ambos sensores reciban la misma intensidad de luz. En este caso uno de ellos se encenderá aleatoriamente, simulando correctamente el efecto cuántico.

Suponiendo ahora la presencia de un espía se plantean los ejemplos mostrados en la tabla 2.

TABLA 3.2 EJEMPLOS DE TRANSMISIÓN DE BITS ENTRE ALICE Y BOB EN PRESENCIA DE UN ESPÍA

| | | |
|---|---|---|
| **Alice** | + | + |
| | 0 | 0 |
| **Eva** | + | × |
| **Bob** | + | + |

En el primero, Alice transmite un ‘0’ en base “+” (polarización de 0˚), Eva y Bob utilizan la misma base por lo que ambos deberían obtener la medida correcta y Eva debe pasar desapercibida. En la figura 3.11 se muestra el esquema de lo que ocurre.

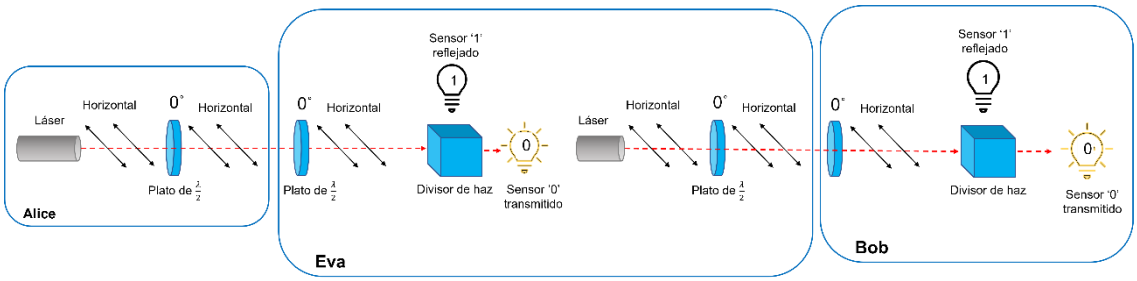


Fig. 3.11. Ejemplo de la transmisión de un ‘0’ en base “+”, medido por Eva y Bob con base “+”.

Como Eva mide la luz recibida utilizando la base “+” el ángulo de polarización no se ve afectado. La luz atraviesa el divisor de haz devolviendo el bit ‘0’. Eva procede a transmitir este bit medido en la base “+” y como Bob cuenta con la misma base de medida también lo lee correctamente.

Cuando Alice y Bob comparen las bases utilizadas no podrán detectar la presencia de Eva en este bit en particular.

En el siguiente ejemplo Alice y Bob se mantienen iguales, pero Eva cambia su base a “×”. En la figura 3.12 se muestra lo que ocurre.

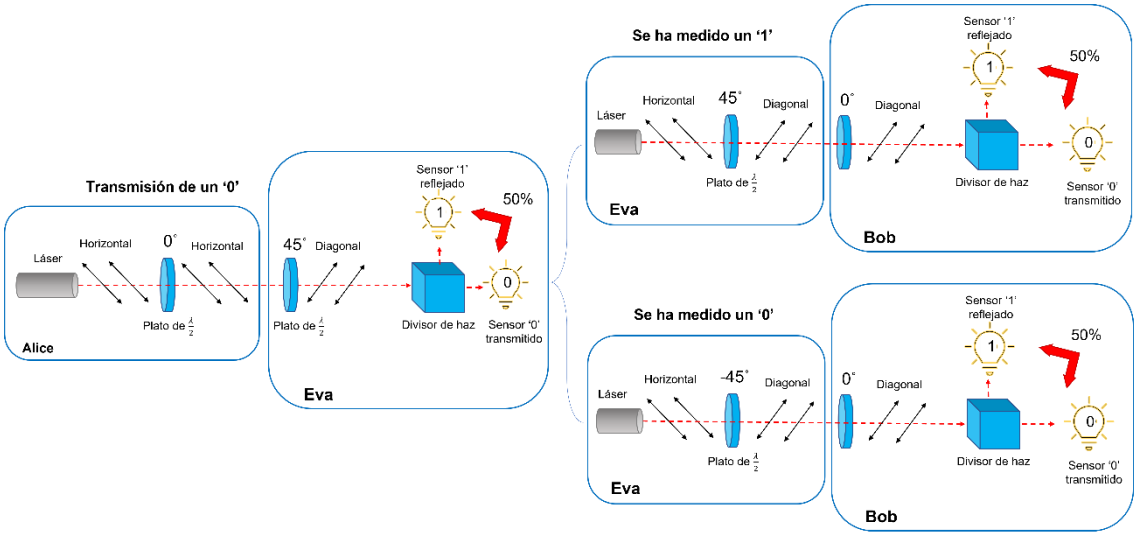


Fig. 3.12. Ejemplo de la transmisión de un '0' en base "+", medido por Eva con base "×" y por Bob con base "+"

Como Eva mide con la base "×" rota la polarización 45°. Cuando esta luz alcanza el divisor de haz, una parte lo atraviesa y otra se refleja encendiendo aleatoriamente uno de los dos sensores.

A partir de ese punto se muestran los esquemas de ambas posibilidades, en el camino superior está el caso en el que Eva haya medido un '1', esta procede a transmitírselo a Bob usando la misma base "×", es decir, polarización de 45°. Como Bob mide con la base "+" no se altera el ángulo de polarización, causando de nuevo que una luz polarizada diagonalmente incida en un divisor de haz, igual que en el caso anterior Bob obtiene '0' o '1' aleatoriamente.

En el camino inferior ocurre lo mismo con la única diferencia que ahora Eva ha medido un '0' y transmite una polarización de -45°.

En el 50% de los casos finales Bob obtendrá el mismo bit que ha sido transmitido por Alice ('0') lo que le permite a Eva pasar desapercibida, sin embargo, en el otro 50% de los casos obtiene un '1' y tras el intercambio de este bit en el grupo de prueba se concluye que un espía ha estado presente en la comunicación.

### 3.2. Emulador de un sistema de criptografía cuántica

En este epígrafe se explica el funcionamiento del emulador. Se comenta la interfaz gráfica, por la cual se introducen los parámetros de trabajo y se reciben los resultados finales, el procesamiento de la imagen o audio introducidos, los componentes de los sistemas clásico y cuántico, modulador, canal y demodulador y ambos protocolos de distribución de claves cuánticas comentados, BB84 y BB84 eficiente.

Antes de comenzar con el funcionamiento de la herramienta es importante comentar las siguientes consideraciones.

1. Se considera que el conteo de fotones en el receptor es ideal, es decir, no se considera como una fuente de error que puedan pasar fotones sin ser contados.
2. Como fuentes de ruido solo se consideran el ruido térmico y la atenuación propia de la fibra óptica. No se toman en cuenta efectos atmosféricos ni ningún otro tipo de distorsión.
3. Aunque la interfaz permite elegir entre una transmisión por fibra óptica o por espacio libre, en este trabajo solo se mostrarán ejemplos utilizando fibra óptica. Esto se debe a que en el espacio libre la atenuación es demasiado grande limitando las simulaciones a distancias muy cortas. Además, introducir ganancias grandes en las antenas para compensar esto implica aumentar las dimensiones de las matrices utilizadas lo cual dificulta el procesamiento.
4. Pese a que la interfaz también permite elegir entre dos tipos de modulación, BPSK y QPSK, en este trabajo se mostrarán ejemplos utilizando solo BPSK. Esto se debe a que en los protocolos BB84 y BB84 eficiente se codifica un solo bit en cada fotón, por lo que resulta más conveniente utilizar una modulación que tenga un bit por símbolo.

### 3.2.1. Funcionamiento general

El programa sigue el diagrama de flujo mostrado en la figura 3.13.

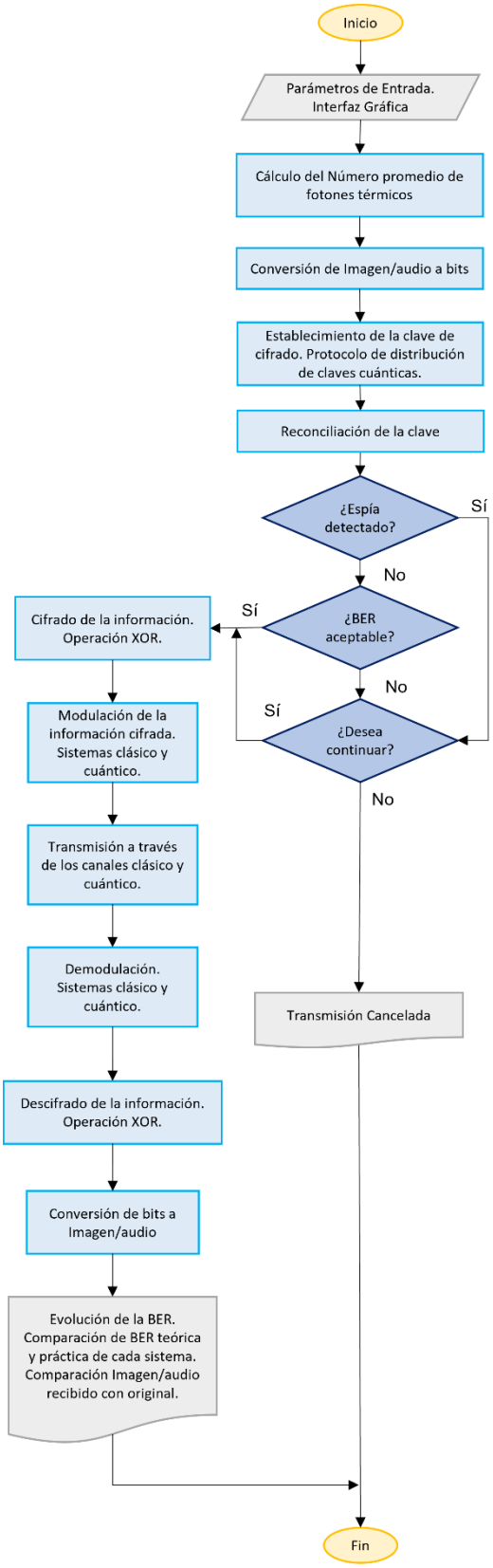


Fig. 3.13. Diagrama de flujo del funcionamiento general del emulador.

En primer lugar, el usuario introduce a través de una interfaz gráfica distintos parámetros de entrada que determinan la información que se quiere cifrar y transmitir, y también algunas condiciones del entorno como la temperatura y si hay presencia de un espía.

Una vez introducidos, la herramienta calcula el número promedio de fotones térmicos en función de la temperatura y convierte la información a cifrar, la cual puede ser una imagen (.jpg) o un audio (.m4a), en una secuencia de bits.

Seguidamente, el programa inicia el proceso de establecimiento de una clave secreta a través de un protocolo de distribución de claves cuánticas.

Una vez seguido el protocolo y generada una clave el programa procede a hacer un proceso de reconciliación de la clave utilizando códigos bloque lineales y chequeo de paridad para poder arreglar cualquier error causado por distorsión en el canal.

Seguidamente el usuario puede obtener alguno de los siguientes tres resultados:

- No se ha detectado un espía. Lo cual significa que se ha establecido una clave de cifrado segura.
- No se ha detectado un espía, pero, el alto nivel de ruido no ha permitido que el emisor y el receptor establezcan una clave sin errores, por lo que se aconseja la cancelación de la transmisión.
- Se ha detectado la presencia de un espía durante el proceso de distribución de claves, por lo que también se recomienda cancelar la ejecución.

Si el resultado obtenido es el primero o el usuario no decide cancelar la transmisión, se procede a cifrar la información a través de una operación XOR con la clave. De obtenerse el segundo o tercer resultado se abrirán dos cuadros de selección donde el usuario podrá decidir si cancelar la transmisión o continuar con ella a pesar de las recomendaciones.

Una vez cifrada la secuencia de bits, esta se transmite a través de los sistemas clásico y cuántico. Se modula, transmite a través del canal respectivo en bloques de 100 bits y demodula en el extremo receptor. Y se vuelve a aplicar la operación XOR para desencriptar la información.

La secuencia recibida y ya desencriptada se procesa para convertirla en una imagen o un audio con el fin de recuperar la información original.

Por último, se muestra al usuario la evolución de la tasa de error de bit para ambos sistemas, la comparación de la imagen o audio recibidos a través de cada canal con el original y las probabilidades de error teóricas y prácticas.

### 3.2.2. Parámetros iniciales

El emulador cuenta con una serie de parámetros iniciales que son opacos al usuario, estos son:

1. Frecuencia de trabajo: 188THz. (Longitud de onda: 1595nm)
2. Atenuación en la fibra óptica: 0.2 $^{dB}/_{km}$
3. Dimensión de vectores (estados) y matrices (operadores de densidad): 30 y 30x30.
4. Tasa: 300 $^{Mb}/_{s}$

El programa cuenta también con una interfaz gráfica que permite al usuario introducir distintos parámetros que serán utilizados en el sistema, al igual que visualizar resultados. Esta se muestra en la figura 3.14.

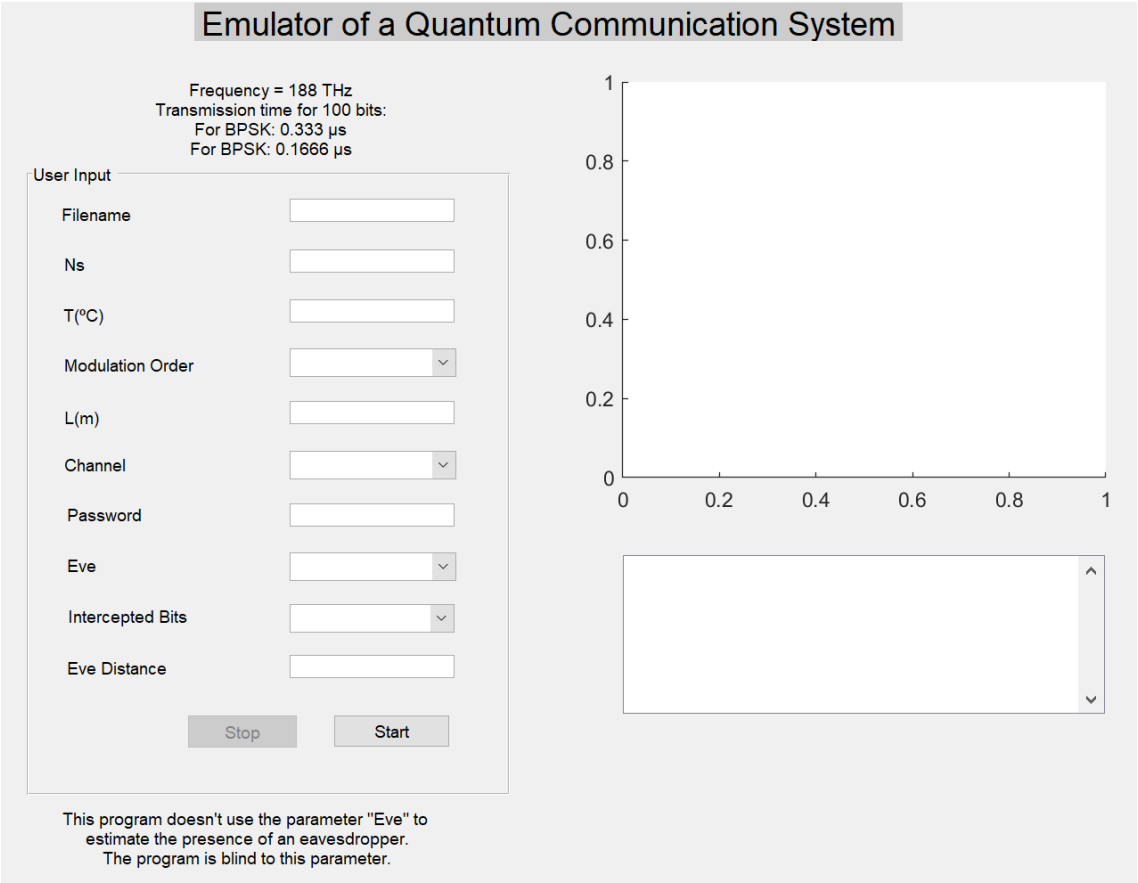


Fig. 3.14. Interfaz gráfica.

### 3.2.3. Parámetros de entrada

**Filename**

El nombre del archivo que se desea cifrar y transmitir. Debe incluirse la extensión correspondiente, ".jpg" o ".m4a".

$\boldsymbol{N_s}$

Es el número promedio de fotones por símbolo. Su valor debe estar entre 1 y 5.

$\boldsymbol{T}$

Es la temperatura, en grados centígrados, del entorno. Sus valores pueden variar entre -200 ˚C y 50 ˚C, con una resolución de 1˚C.

**Modulation order**

Este parámetro permite al usuario elegir la modulación que se utiliza para modular la información en el transmisor. De elegir "2" se selecciona una modulación BPSK, si se escoge "4", una QPSK.

**Channel**

Se elige el tipo de canal que se va a emular tanto para la distribución de claves como para la transmisión de la información cifrada. Se puede elegir entre un canal de fibra óptica o uno de espacio libre.

**L**

Es la distancia en metros entre el transmisor y el receptor. Su rango de valores dependerá del canal de transmisión escogido. Para el canal de fibra óptica el valor mínimo posible es 0 metros y se recomienda como máximo una distancia de 30 km en el caso ideal sin ruido térmico. En el caso de espacio libre la distancia mínima es 10 metros, ya que para este valor no hay atenuación y la ganancia es igual a la unidad. Para una ejecución sin ruido térmico se recomienda no superar una distancia de 15 metros. Para ambas opciones es posible introducir distancias mayores. En particular para el canal de espacio libre unos pocos metros más aumentarán el error significativamente ya que la atenuación decrece muy rápidamente.

**Password**

Es una contraseña de 10 caracteres que será utilizada para generar una clave en el transmisor. Deben ser caracteres ASCII.

**Eve**

Este parámetro permite al usuario elegir entre emular una transmisión con espía o sin él, además puede elegir la secuencia de bases que va a utilizar dicho espía. Entre las opciones de bases están:

- Random: se generará una secuencia de base "+" y base " × ", '0' y '1' respectivamente, con las mismas probabilidades que las bases de Alice y Bob.
- Best: se generará una secuencia de bases que permita espiar la mayor cantidad de información posible. Esta secuencia cuenta únicamente con base "+".

**Intercepted bits**

Indica el porcentaje de bits que el espía intercepta. Las opciones son las siguientes:

- 1: se intercepta el 100% de los bits.
- 0.5: se intercepta el 50% de los bits.
- 0.1: se intercepta el 10% de los bits.

**Eve Distance**

Es la distancia entre el transmisor y el espía. Debe ser menor a la distancia entre emisor y receptor.

### 3.2.4. Parámetros de salida

**Número promedio de fotones térmicos por símbolo**

Resultado que se calcula a partir de la temperatura y se muestra en una ventana de la interfaz gráfica.

**Umbral de ruido**

En los casos donde no se detecta la presencia de un espía, pueden salir dos posibles mensajes. El primero, como se ve en la figura 3.15, se muestra cuando no se ha detectado alteración de los bits y además los niveles de ruido son suficientemente bajos como para que se pueda establecer una clave sin errores entre emisor y receptor, por lo que se procede al cifrado de la información. El segundo, mostrado en la figura 3.16, aparece

cuando, a pesar de no haber detectado a un espía, los niveles de ruido son demasiado altos para establecer una clave sin equivocaciones, por lo que se recomienda cancelar la transmisión y descartar las claves que emisor y receptor hayan establecido.

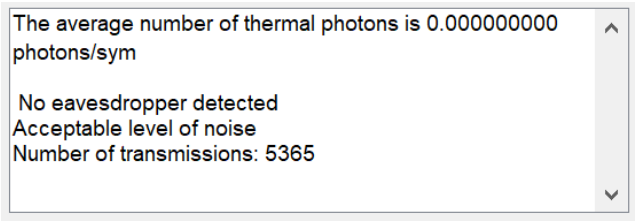


Fig. 3.15. Mensaje de espía no detectado y nivel de ruido aceptable.

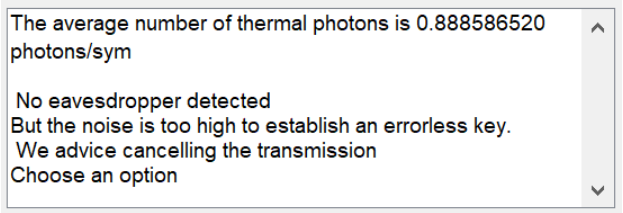


Fig. 3.16. Mensaje de espía no detectado y nivel de ruido demasiado alto.

### Detección de espía

En los casos donde la tasa de error de bit obtenida sea mayor que la esperada se da un aviso al usuario sobre la posible presencia de un espía, como se muestra en la figura 3.17, y se aconseja cancelar la ejecución.

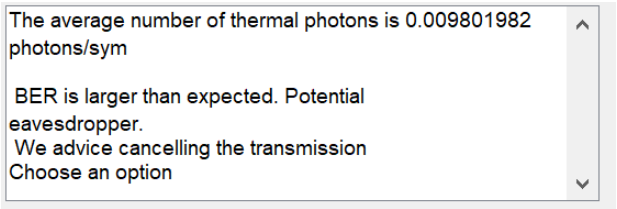


Fig. 3.17. Mensaje de detección de un espía.

### Continuar o cancelar la transmisión

En los casos anteriores donde se haya recomendado cancelar la ejecución aparecerán dos cuadros, como se muestra en la figura 3.18, que permiten al usuario marcar su decisión.

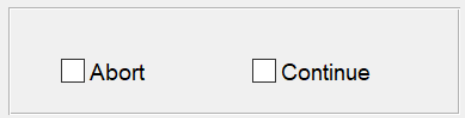


Fig. 3.18. Cuadro para cancelar o continuar con la transmisión.

### Número de transmisiones

Indica la cantidad de paquetes de 100 bits que se van a transmitir.

### Estadísticas

Al finalizar la ejecución se mostrarán los resultados numéricos de ambos sistemas, las probabilidades de error teóricas y prácticas, como se muestra en la figura 3.19.

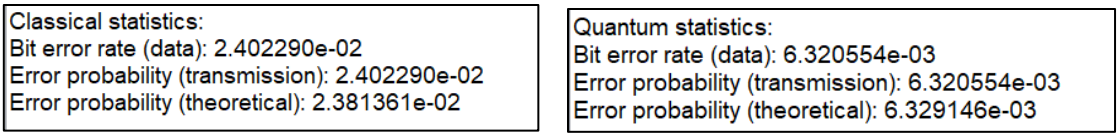


Fig. 3.19. Mensaje con las estadísticas de la transmisión.

### Evolución de la BER

Se muestra una comparación de la tasa de error de bits de ambos sistemas. Cada 100 bits transmitidos, se divide el número total de bits erróneos entre la cantidad total de bits recibidos hasta ese punto. En la gráfica se muestra también el límite de Helstrom, el cual marca la mínima probabilidad de error que se puede obtener en un sistema cuántico cuando se utiliza una modulación BPSK. Un ejemplo se muestra en la figura 3.20.

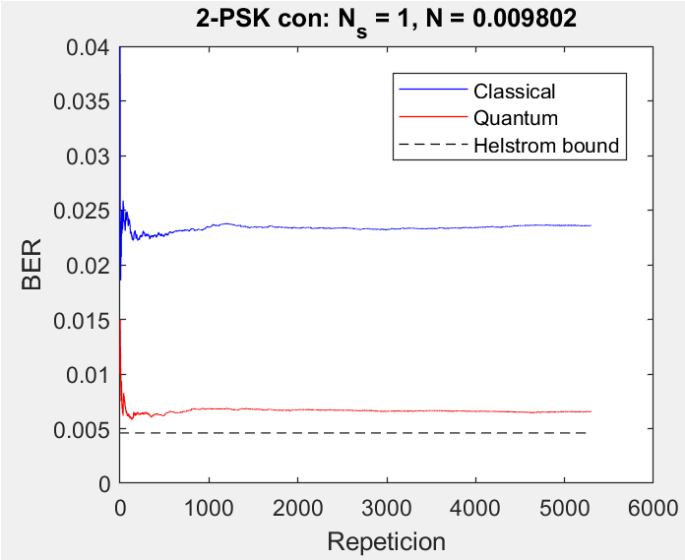


Fig. 3.20. Gráfico de la evolución de la tasa de error de bit.

### Comparación de imágenes o audios

Si se transmitió originalmente una imagen, se abrirá una ventana mostrando una comparación ente la imagen original y las recibidas a través de cada sistema. En el caso de que se haya enviado un audio, se reproducirá primero el original, seguido del recibido

a través del canal clásico y por último el del canal cuántico. Un ejemplo se puede ver en la figura 3.21.

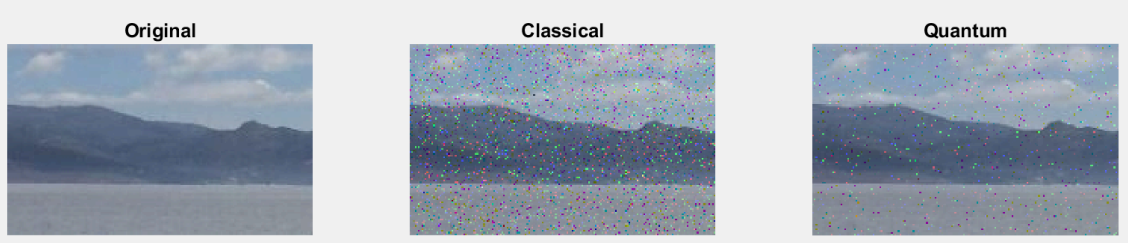


Fig. 3.21. Ejemplo de transmisión de una imagen.

### 3.2.5. Cálculo del número promedio de fotones térmicos

En este bloque se calcula el número promedio de fotones térmicos por símbolo en función de la temperatura introducida. Para este cómputo se utiliza la fórmula (58), sin embargo, la señal se verá afectada no solo por los fotones térmicos radiados dentro del ancho de banda de nuestra señal, sino también por los fotones radiados dentro del ancho de banda del soporte físico, la fibra óptica, a través del cual se transmite la información. De acuerdo con esto, se procede a integrar la ecuación anteriormente mencionada para la temperatura indicada y para el rango de frecuencias del ancho de banda de todo el canal, el cual será del orden de terahercios.

### 3.2.6. Tratamiento de imágenes y audios

Lo primero que hace el programa es identificar el tipo de archivo que se desea transmitir a partir de su extensión. Si es una imagen se busca en la cadena introducida la extensión ".jpg" y si es un audio se busca ".m4a".

Si el archivo es una imagen, se utiliza una función que la lee y la almacena como una matriz de tres dimensiones con el siguiente formato:

$$Imagen = Alto\ x\ Ancho\ x\ 3$$

El alto y el ancho vienen dados en píxeles, mientras que la profundidad se mantendrá constante con valor 3, ya que representa los colores rojo, verde y azul del formato RGB.

Esta matriz es separada en tres, una para cada color, y a su vez estas son reorganizadas en forma de columnas y concatenadas para obtener una única fila de números entre 0 y 255.

La conversión a bits se podría hacer directamente transformando cada valor en un número binario de ocho bits, sin embargo, se busca reducir el número de bits para así disminuir el tiempo de ejecución del programa, por lo que cada valor será representado con 6 bits.

Para realizar esto se crean 64 niveles entre 0 y 255, como se muestra en la figura 3.22. Se toma cada valor de la cadena de bits que se ha obtenido de la imagen y se determina a qué nivel pertenece siguiendo un criterio de mínima distancia. Una vez realizado este muestreo se obtiene una secuencia de valores entre 0 y 63, la cual sí puede ser representada con 6 bits.

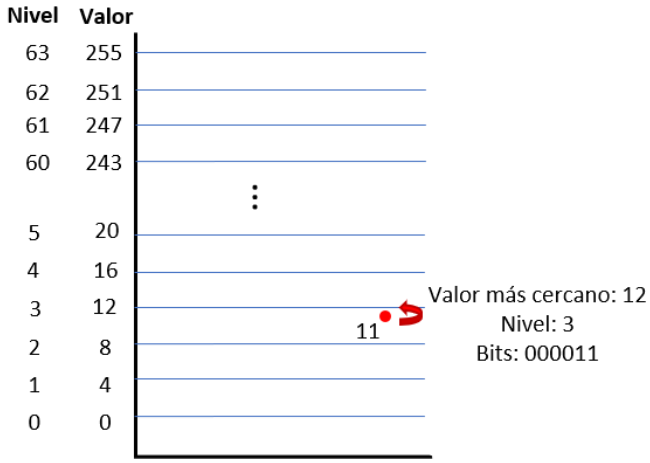


Fig. 3.22. Conversión de los valores RGB a valores dentro de los 64 niveles.

De este proceso es importante guardar las dimensiones de la imagen para poder recuperarla después.

Si el archivo es de audio, se lee y se muestrea a una frecuencia de 8kHz, la cual es la que se utiliza en teléfonos para la digitalización de la voz. En este caso, igual que en el anterior, cada muestra será un valor de 6 bits, lo que da un total de 64 posibles valores.

Una vez muestreada la señal se realiza la cuantificación, se toman los valores máximos y mínimos del audio y se generan 64 niveles equiespaciados entre dichos valores. A partir de aquí el proceso es igual al anterior, se toma cada valor de la señal de audio y se mapea al nivel que se encuentre a menor distancia, como se muestra en la figura 3.23. Una vez obtenida la secuencia de valores ente 0 y 63 se procede a convertir cada uno en un entero de 6 bits.

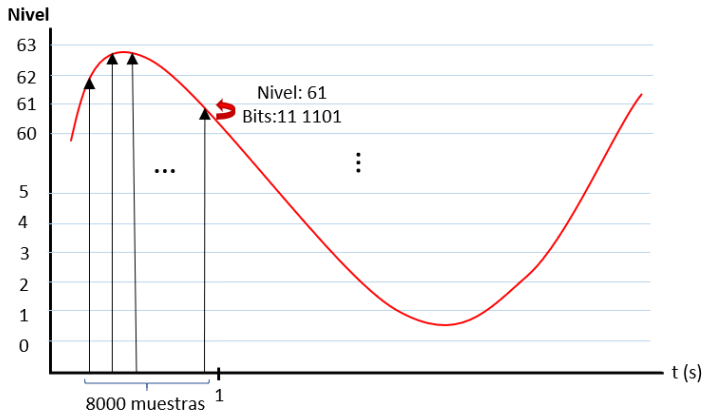


Fig. 3.23. Cuantificación de las muestras del audio.

De este método es importante guardar la frecuencia de muestreo, el valor máximo y mínimo del audio, y el número de bits por muestra con el fin de poder recuperar y reproducir el archivo en el extremo receptor.

Por último, se agregan a la secuencia de bits obtenida, ya sea con una imagen o un audio, una cantidad de bits a '0' de "padding" para que la cadena tenga una longitud múltiplo de 100, ya que la transmisión de la información se realizará en bloques de 100 bits.

### 3.2.7. Sistema clásico

Aunque la transmisión a través del sistema clásico no es el siguiente paso en el diagrama, resulta conveniente explicarlo primero. A partir de sus elementos, modulador, canal y demodulador, se tiene un punto de partida para entender el sistema cuántico más fácilmente.

#### 3.2.7.1. Modulador clásico

El modulador toma una cadena de bits y devuelve la envolvente compleja de la señal a transmitir.

Primero se calcula una constelación BPSK base normalizada, como la que se puede observar en la figura 3.24, y se convierte cada bit en su símbolo correspondiente.

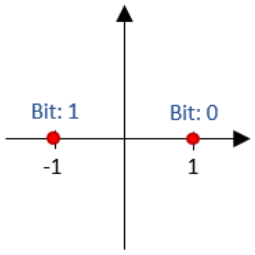


Fig. 3.24. Constelación de la modulación BPSK.

El siguiente paso es el cálculo del factor de forma, aunque este no tendrá ningún efecto ya que para modulaciones de tipo PSK es igual a la unidad.

Ahora se calcula la envolvente compleja. Para ello se debe hallar primero la amplitud de la portadora $V_0$, esto puede hacerse a partir de la potencia óptica la cual se puede calcular, ya que uno de los datos conocidos es el número promedio de fotones por símbolo $N_s$. Siguiendo la ecuación 2.36 y calculando la intensidad de fotones como

$$\lambda(t) = N_s \left[\frac{fotones}{símbolo}\right] R_s \left[\frac{símbolo}{segundo}\right]$$

Donde $R_s$ es la tasa de símbolos por segundo, se obtiene la potencia óptica de la señal. Tomando las ecuaciones 2.44 y 2.61 que relacionan la potencia con la envolvente compleja y la envolvente con la amplitud, respectivamente, se obtiene la siguiente potencia

$$P_{opt} = \left|C_0 V_0 e^{i2\pi\, vt}\right|^2 = hv\lambda(t)$$

Como los módulos de $|C_0|^2$ y $\left|e^{i2\pi\, vt}\right|^2$ son iguales a uno, solo quedaría el módulo de $|V_0|^2$. Considerando esto y despejando $V_0$ se obtiene

$$V_0 = \sqrt{hv\, N_s\, R_s}$$

Por último, se multiplica cada símbolo por la amplitud para obtener la envolvente compleja que se va a transmitir.

$$V(t) = C_0 V_0$$

#### 3.2.7.2. Canal Clásico

Este bloque toma la secuencia devuelta por el modulador y aplica sobre ella la atenuación causada por la fibra óptica.

Para ello se calcula el coeficiente de atenuación en función de la distancia y se multiplica por la secuencia, según la ecuación 2.55, para obtener la envolvente compleja en el extremo receptor.

#### 3.2.7.3. Demodulador Clásico

El demodulador recibe una secuencia de envolventes complejas del canal y, a partir de ella y de la portadora $V_L$ del receptor, realiza el conteo de fotones usando una

aproximación gaussiana, obtiene el símbolo recibido y devuelve una secuencia de bits según las regiones de decisión.

Dividiendo la envolvente recibida entre el módulo de la constelación base se obtiene la amplitud de la señal recibida $V_R$. A partir de esta es posible calcular la potencia recibida y por ende el número promedio de fotones recibidos $N_R$, utilizando la misma ecuación que en el modulador. Como se va a utilizar una aproximación gaussiana, donde se necesita que $N_L >> N_R$, se calcula $N_L = 1000N_R$ y $V_R$ con la misma ecuación con la que se calculó $V_0$.

Para calcular las regiones de decisión que se ven en la figura 2.14, se utilizan los valores obtenidos $N_L$ y $N_R$, y la ecuación 2.52.

El siguiente paso es calcular las envolventes complejas de los caminos A y B, mostrados en la figura 2.17, como se muestra en la ecuación 2.47, ignorando momentáneamente las envolventes causadas por el ruido térmico. Se procede a calcular el número promedio global de fotones recibidos, para cada camino, en función de la potencia de la señal recibida, incluyendo la portadora local. A este valor se le suma el número de fotones térmicos.

Una vez obtenido este valor se siguen las ecuaciones 2.67 para obtener la media $m_{path}$ y varianza $\sigma_{path}^2$ de la variable aleatoria gaussiana. Se utiliza la función *normrnd* de MATLAB para obtener un valor aleatorio con dicha distribución normal para cada camino de la siguiente manera

$$n_a = normrnd(m_a, \sqrt{\sigma_a^2})$$

$$n_b = normrnd(m_b, \sqrt{\sigma_b^2})$$

El símbolo final recibido se compone tomando $n_a$ como su parte real y $n_b$ como su parte imaginaria, como se muestra en la ecuación 2.68. Por último, se convierte cada símbolo recibido en un '0' o '1' según las regiones de decisión. Esto se hace calculando la distancia entre el símbolo y cada punto de la constelación base, asignando el bit de la región que se encuentre a menor distancia.

### 3.2.8. Sistema cuántico

#### 3.2.8.1. Modulador cuántico

Igual que en el caso clásico, este toma una secuencia de bits y devuelve una de símbolos, sin embargo, en este caso los símbolos representan la amplitud compleja del estado cuántico a transmitir. Los pasos que sigue el modulador se muestran en la figura 3.25.

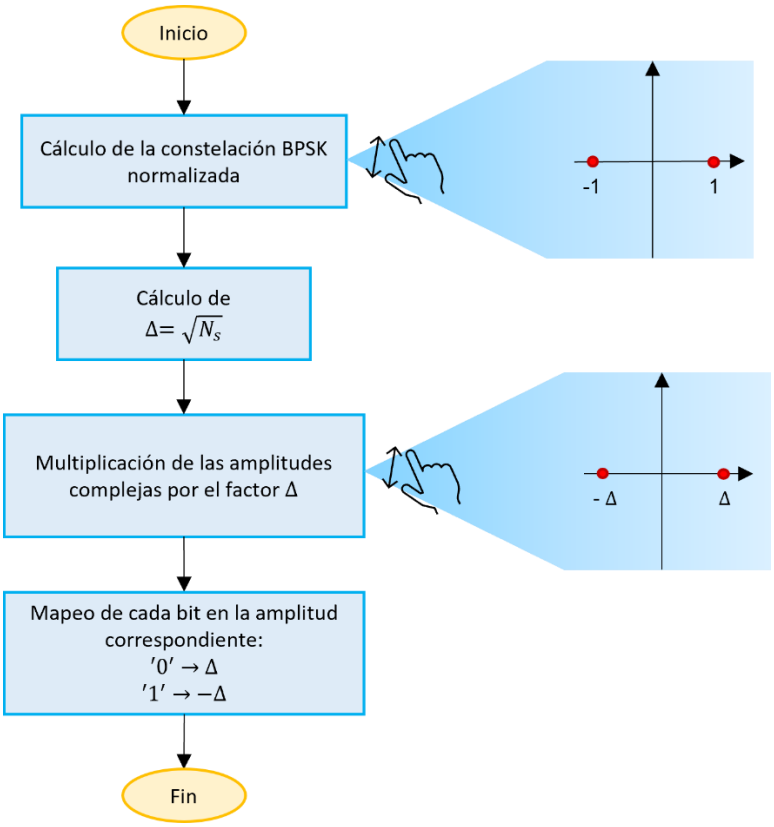


Fig. 3.25. Diagrama de flujo del modulador clásico.

En primer lugar, se calcula una constelación BPSK normalizada y luego se multiplica por la raíz cuadrada del número de fotones por símbolo, $N_s$, para obtener las amplitudes complejas $\Delta$ y $-\Delta$ de los estados $|\Delta\rangle$ y $|-\Delta\rangle$, respectivamente. Esto se calcula de esta forma de acuerdo con la ecuación 2.70 que muestra la fórmula de los estados coherentes, ya que el módulo al cuadrado de la amplitud $|\Delta|^2$ debe ser igual al número de fotones en el estado $N_\gamma = N_s$.

Por último, se mapea cada bit a su amplitud compleja correspondiente.

### 3.2.8.2. Canal cuántico

El canal toma la secuencia de amplitudes complejas, les aplica la atenuación causada por la fibra y el efecto del ruido térmico y devuelve una secuencia de operadores de densidad (estados ruidosos) donde cada uno se corresponde con un símbolo transmitido por Alice.

Para esto se calcula primero la constelación de operadores de densidad que representan los posibles estados, afectados por ruido, que puede recibir Bob utilizando la aproximación de la ecuación 2.99. Este proceso se describe en el diagrama de flujo de la figura 3.26.

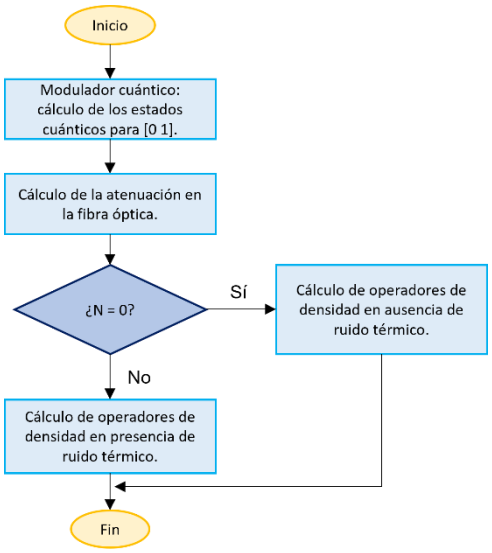


Fig. 3.26. Diagrama de flujo del cálculo de la constelación de operadores recibida por Bob.

En primer lugar, se utiliza el modulador cuántico para obtener las amplitudes complejas, $\Delta$ y $-\Delta$ , de los dos estados posibles, correspondientes con los bits '0' y '1'. Estas amplitudes se multiplican por el mismo coeficiente de atenuación calculado en el canal clásico, siguiendo la ecuación 2.78, para obtener el decremento en potencia causado por la fibra óptica.

Si el número de fotones térmicos es igual a cero se calculan los estados coherentes según la ecuación 2.70 y se aplica el producto externo entre el estado y su traspuesto conjugado para obtener el operador de densidad, siguiendo la expresión 2.23.

En presencia de ruido térmico se calcula primero el número de fotones en cada estado elevando al cuadrado las amplitudes complejas $|\Delta|^2$. Los operadores de densidad se obtienen utilizando la aproximación de la ecuación 2.94 limitando las dimensiones a

30x30. Para aplicar esta fórmula también fue necesario calcular los coeficientes $R_{mn}$ y el polinomio de Laguerre de las ecuaciones 2.95 y 2.96, respectivamente.

Una vez calculada la constelación se procede a mapear cada amplitud compleja recibida del transmisor a su operador de densidad correspondiente, generando la secuencia que llega al receptor.

#### 3.2.8.3. Demodulador cuántico

El demodulador toma la secuencia de operadores de densidad recibidos, realiza una medida cuántica utilizando los operadores de medida y devuelve una cadena de '0' y '1' a partir del resultado de dicha medida. En la figura 3.27 se muestra el diagrama de flujo de este bloque.

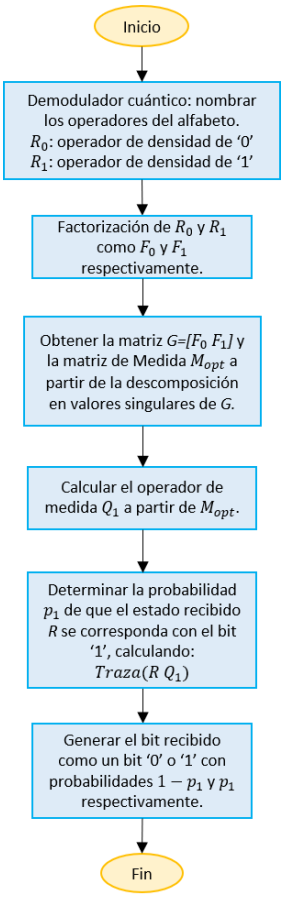


Fig. 3.27. Diagrama de flujo del demodulador cuántico.

El extremo receptor conoce también la constelación de posibles estados ruidosos que fue calculada en el bloque del canal y esta será utilizada para calcular los operadores de medida. En primer lugar, se nombra cada uno de estos operadores de la constelación como $R_0$ y $R_1$. Estos son factorizados, según la expresión 2.102, en los factores $F_0$ y $F_1$.

La matriz de estados se compone concatenando estos factores y, a partir de esta, se calcula la matriz de medida óptima utilizando la descomposición en factores singulares de la ecuación 2.105.

Los dos operadores de medida $Q_0$ y $Q_1$ son calculados a partir de la matriz de medida, tomando los factores de medida $\mu_0$ y $\mu_1$ que la componen (con las mismas dimensiones que $F_0$ y $F_1$) y multiplicándolos por sus transpuestos conjugados de la forma

$$Q_0 = \mu_0\mu_0^* \qquad\qquad Q_1 = \mu_1\mu_1^*$$

Para recuperar la secuencia de bits transmitida se sigue la ecuación 2.26, se toma cada operador de densidad recibido por Bob, se multiplica por el operador de medida $Q_1$ y se calcula la traza de dicho producto. Esto da como resultado la probabilidad $p_1$ de que el operador de densidad medido represente el bit '1'. Para representar esta medida no determinista se utiliza un generador aleatorio de bits donde las probabilidades de obtener '0' o '1' son $1 - p_1$ y $p_1$, respectivamente.

Utilizar un generador aleatorio permite representar de una forma más fiel la aleatoriedad que ocurre cuando se mide un estado cuántico desconocido.

### 3.2.9. ¿Cómo se transmiten Alice y Bob unos bits en el sistema cuántico?

Antes de entrar a explicar el establecimiento de la clave es conveniente dar un ejemplo de cómo se ve la transmisión de los bits '0' y '1', de Alice a Bob, en un canal cuántico.

Se hace la suposición inicial de que el número de fotones por símbolo es igual a uno, $N_s = 1$, ya que en los protocolos se codifica la información de un bit en un único fotón.

Alice utiliza el modulador cuántico para obtener las amplitudes complejas de los estados que desea transmitir. En este caso las amplitudes resultan $1$ y $-1$, respectivamente ya que la raíz cuadrada de $N_s$ es igual a uno. Por ende, los estados que Alice va a transmitir son los siguientes: $|\gamma_0\rangle = |1\rangle$ y $|\gamma_1\rangle = |-1\rangle$.

En el canal se calculan los operadores de densidad que resultarán tras los efectos de la atenuación y el ruido térmico. Como los bits a transmitir conforman el alfabeto, se muestra a continuación cómo se calcula la constelación de operadores de densidad.

La atenuación en potencia causada por la fibra óptica se modela como un decremento en el número promedio de fotones por lo que se multiplican las amplitudes complejas recibidas por un coeficiente de atenuación $\alpha = 10^{-0.1A_F\left[\frac{dB}{Km}\right]\frac{D}{2}[Km]}$ , obteniéndose:

$$|\gamma_0\,\alpha\rangle = |1\cdot\alpha\rangle = |10^{-0.1A_F\left[\frac{dB}{Km}\right]\frac{D}{2}[Km]}\rangle$$

$$|\gamma_1\,\alpha\rangle = |(-1)\alpha\rangle = |-10^{-0.1A_F\left[\frac{dB}{Km}\right]\frac{D}{2}[Km]}\rangle$$

Si se calcula el número de fotones promedio de dichos estados se obtiene:

$$|\gamma_0\alpha|^2 = \left|10^{-0.1A_F\left[\frac{dB}{Km}\right]\frac{D}{2}[Km]}\right|^2 < 1$$

$$|\gamma_1\alpha|^2 = \left|-10^{-0.1A_F\left[\frac{dB}{Km}\right]\frac{D}{2}[Km]}\right|^2 < 1$$

Resultando un número promedio de fotones menor a 1 por símbolo dependiendo de la longitud $D \neq 0$ del enlace y de la atenuación $A_F$ en $\frac{dB}{Km}$.

El segundo efecto del canal es el ruido térmico, el cual se calcula a partir de la temperatura y se expresa como el número promedio de fotones térmicos por símbolo. El efecto de este causa que en el extremo receptor se obtenga una versión ruidosa de los estados originales en forma de operadores de densidad: $\widehat{\rho_1}$ $y$ $\widehat{\rho_{-1}}$. Estos se representan en MATLAB como matrices 30x30 calculadas utilizando las ecuaciones comentadas en la explicación del canal cuántico. Es importante resaltar que la amplitud compleja que se introduce en estas fórmulas no es la original, sino la afectada por el coeficiente de atenuación $\alpha$.

En el receptor, Bob debe medir los operadores recibidos $\widehat{\rho_1}$ $y$ $\widehat{\rho_{-1}}$. Para ello calcula primero los operadores de medida de cada bit, $Q_0$ y $Q_1$ (representados también como matrices 30x30), y multiplica cada operador recibido por uno de ellos, en el caso del código se multiplican por $Q_1$. Calculando la traza de dicho producto se obtiene la probabilidad de que dicho operador medido se corresponda con el bit '1'.

Por ejemplo, si se realiza una ejecución a -200˚, es decir sin ruido térmico, y sin atenuación el resultado de medir $\widehat{\rho_1}$ , el cual representa el bit '0', con $Q_1$ será el siguiente:

$$Tr(\widehat{\rho_1}Q_1) = 0.0046$$

Esto significa que la probabilidad de que $\widehat{\rho_1}$ se corresponda con el bit '1' es del 0,46%. Para finalmente decidir qué bit representa el operador se utiliza el siguiente generador aleatorio

$$bit_{recuperado} = randsrc(1,1,[0\ 1; 1-0.0046\ \ 0.0046])$$

Este devolverá un único número elegido entre ‘0’ y ‘1’ y donde ‘0’ tiene una probabilidad de 99,54% y ‘1’ de 0,46%. La probabilidad de que se decida correctamente ‘0’ es muy alta.

Todo este proceso se muestra como resumen en la figura 3.28.

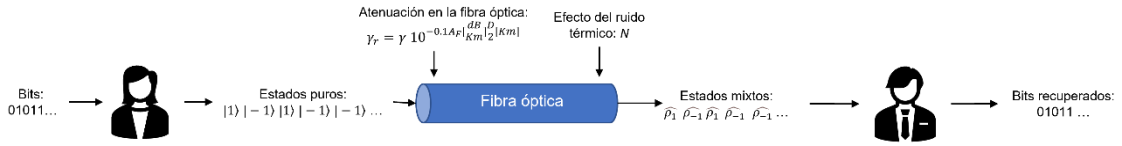


Fig. 3.28. Transmisión de bits de Alice a Bob a través de un canal ruidoso.

### 3.2.10. Protocolo de distribución de claves cuánticas BB84 y BB84 eficiente.

Ahora resulta más fácil comentar los protocolos ya que se han explicado los elementos del sistema cuántico que se utilizarán para el establecimiento de la clave.

Como el protocolo BB84 eficiente es una variante de la versión original en la que se cambian las probabilidades de las bases que utilizan el emisor y receptor para transmitir y medir los fotones, se explicará el funcionamiento del establecimiento de una clave secreta de forma genérica entrando en detalle en las diferencias de estos dos protocolos en los momentos donde sea necesario.

El procedimiento para generar una clave y cifrar el mensaje a transmitir sigue el diagrama de flujo que se muestra en la Figura 3.29.

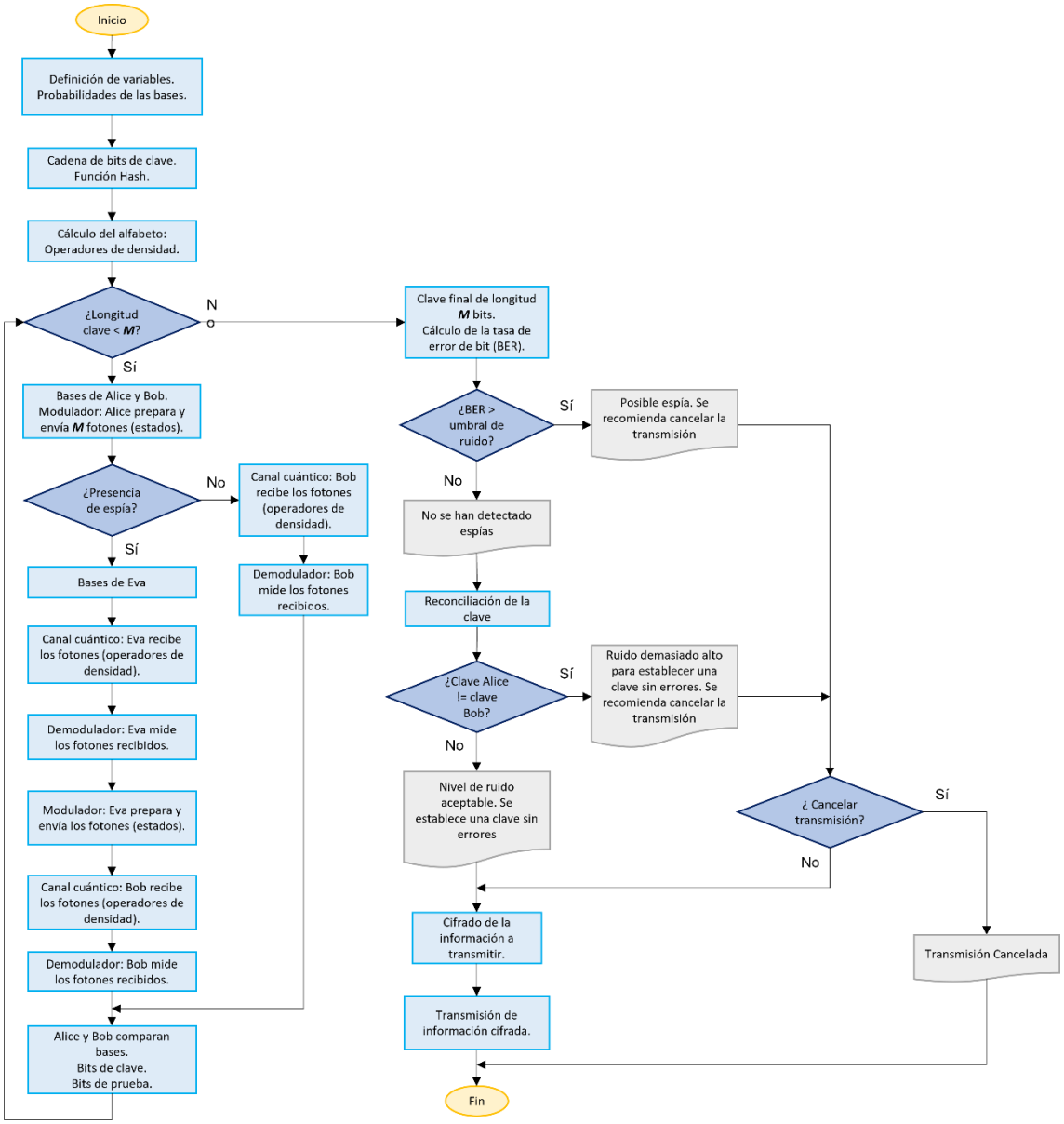


Fig. 3.29. Diagrama de flujo del establecimiento de clave y cifrado.

Lo primero que se hace es definir las variables que se utilizarán a lo largo del proceso de generación de la clave. Se declara el número promedio de fotones por símbolo $N_s$ igual a 1, sin importar el valor introducido por el usuario en la interfaz, ya que cada símbolo, que representa un solo bit, se transmite en la polarización de un solo fotón. También se define desde el inicio la probabilidad de las bases utilizadas, este parámetro varía dependiendo del protocolo seleccionado.

Para el protocolo BB84, ambas bases tienen la misma probabilidad, mientras que en el protocolo BB84 eficiente no. La base '+' tiene una probabilidad *p* y la base 'x' una probabilidad *1-p*, siendo *p* mayor que 0.5. El encontrar el valor de la probabilidad *p* que maximice la eficiencia es uno de los objetivos de este trabajo.

Una vez definidas las probabilidades, Alice debe generar una secuencia de bits que será utilizada como clave. Aunque es verdad que los protocolos establecen que la clave debe ser una secuencia completamente aleatoria, no es posible lograr esto utilizando un ordenador normal, ya que, como se ha comentado, estos son capaces de generar solo secuencias pseudoaleatorias. Con la intención de involucrar al usuario, se toma la clave de diez caracteres introducida a través de la interfaz gráfica, se pasa por una función hash y luego se representa cada carácter en binario, obteniendo una clave de 320 bits de longitud. Como se verá más adelante existe la posibilidad de establecer la longitud de la clave como 10000 bits, en este caso no se toma en cuenta la clave del usuario, sino que se utiliza el generador aleatorio directamente. A partir de este punto se hará referencia al número de bits de la clave como $\boldsymbol{M}$ bits.

El siguiente paso es generar la constelación que se utiliza en la transmisión. Esto se realiza como se ha explicado anteriormente en el canal cuántico.

Es importante comentar que no se calcula solamente una constelación, sino que se calculan tres, una para cada distancia y temperatura establecidas en el programa.

1. Constelación para la comunicación entre Alice y Bob.
2. Constelación para la comunicación entre Alice y Eva.
3. Constelación para la comunicación entre Eva y Bob.

Hacer esta distinción entre las constelaciones es importante porque el utilizar la distancia y temperatura correcta para calcular estos operadores influirá directamente en el cálculo de la matriz de medidas y, por ende, en la probabilidad de error.

La constelación entre Alice y Bob se calcula tomando las distancia y temperatura que fue introducida por el usuario a través de la interfaz gráfica. Es lógico hacerlo de esta forma ya que Alice y Bob, como son los dos puntos que quieren comunicarse, conocen esta información de antemano.

La constelación entre Alice y Eva se calcula también con los datos introducidos por el usuario, debido a que se considera que el espía sabe a qué distancia de Alice se está infiltrando en la comunicación.

La última constelación, entre Eva y Bob se vuelve más complicada. En un entorno real, Bob no tendría conocimiento de la presencia de un espía antes de realizar las pruebas, por lo que no sabría a qué distancia se encuentra. También se vuelve un factor desconocido

lo ruidoso que sería el canal ya que tampoco se conoce como haría llegar Eva los fotones a Bob.

Se podría pensar que una solución realista sería permitir que Bob mida todos los estados que recibe con los operadores que ha calculado a partir de la primera constelación (Alice y Bob) sin embargo, emulándolo matemáticamente no es posible y el resultado serían medidas prácticamente aleatorias.

Se ha tomado la decisión de diseño de simular el canal entre Eva y Bob como ideal, sin ruido térmico ni atenuación y permitiéndole a Bob conocer esta constelación en los casos en los que haya presencia de un espía, con el fin de poder simular correctamente el protocolo.

El calcular las constelaciones fuera de los distintos bloques también reduce significativamente el tiempo de ejecución, ya que permite que tanto el canal como el demodulador puedan recibir los alfabetos por parámetros y así evitan tener que calcular la misma matriz 30 x 30 más de dos veces.

### 3.2.11. Establecimiento de la clave

El siguiente bloque del diagrama hace referencia a la longitud de la clave. Debido a que la eficiencia de ninguno de los dos protocolos de distribución de claves cuánticas es igual al 100%, no es posible establecer una clave de $\boldsymbol{M}$ bits transmitiendo únicamente $\boldsymbol{M}$ fotones, es necesario transmitir una mayor cantidad para compensar los bits que son descartados por Alice y Bob. La cantidad demás que se debe transmitir dependerá de cómo se hacen las pruebas de detección de espías y las probabilidades de las bases en cada protocolo. Por esta razón el programa entra en un bucle en el que se transmiten tantos fotones como sean necesarios hasta obtener una clave de longitud $\boldsymbol{M}$.

Dentro de este bucle es donde se llevan a cabo los pasos descritos de forma teórica en cada protocolo.

Primero, Alice y Bob generan las secuencias de bases que utilizarán. Para el protocolo BB84 se utiliza un generador aleatorio equiprobable de ‘0’ y ‘1’, donde el ‘0’ representa la base ‘+’ y el ‘1’ la base ‘×’. Para el BB84 eficiente se utiliza el mismo generador, pero definiendo las probabilidades de ‘0’ y ‘1’ como $p$ y $1-p$ respectivamente.

Alice utiliza el modulador para obtener la secuencia de estados a transmitir a partir de los bits de la clave.

A continuación, se toman en cuenta las siguientes dos posibilidades:

1. El usuario ha indicado a través de la interfaz gráfica que no se emulará la presencia de un espía.
2. El usuario ha indicado que se emulará la presencia de un espía, indicando el tipo de base y el porcentaje de bits interceptados.

En el primer caso los estados son enviados directamente a Bob a través del canal cuántico.

Bob recibe una secuencia de operadores de densidad los cuales se corresponden con la constelación calculada para una distancia entre Alice y Bob. Bob procede a medir cada uno de los operadores recibidos utilizando el procedimiento descrito en el demodulador cuántico.

En el segundo caso se toma en cuenta la presencia del espía por lo que debe generarse la secuencia de bases "random" o "best", según haya indicado el usuario.

De elegirse "random", se genera una secuencia de bases aleatoria que sigue las probabilidades dadas de cada protocolo. Al elegir "best" se genera la secuencia que permite al espía interceptar la mayor cantidad de información de forma correcta. Este último tipo de espía es utilizado solo en el protocolo BB84 eficiente ya que el BB84 no indica que esto pueda causar ninguna mejora.

Eva recibe los fotones transmitidos por Alice en forma de operadores de densidad, es importante recordar que estos no son los mismos a los operadores de densidad recibidos por Bob ya que Eva y Bob no se encuentran a la misma distancia de Alice, normalmente, por lo que la atenuación para ambos casos será distinta.

Eva usa el demodulador cuántico, de la misma forma que Bob, para recuperar los bits transmitidos originalmente. En todos los casos en los que las bases de Eva y Alice sean diferentes el programa sustituye dichos bits por '0' o '1' de forma aleatoria.

Con el fin de no ser detectada Eva modula los bits que ha medido y se los transmite a Bob como fotones polarizados en la misma base que ha utilizado en el proceso de medición.

En este punto se toma en cuenta el porcentaje de bits interceptados por Eva. Se selecciona aleatoriamente dicho porcentaje de bits de los $\boldsymbol{M}$ que conforman la clave, Bob recibe, para dichos casos, los operadores de densidad transmitidos por Eva y para los bits no alterados por el espía obtiene directamente los operadores de densidad transmitidos por Alice.

Para que Bob puede recuperar los bits correctamente este demodula cada operador de densidad recibido utilizando los operadores de medida correspondientes, basándose en cuáles bits provienen de Alice y cuáles de Eva. Una vez medidos se obtiene la secuencia final de bits.

El siguiente paso, para ambos casos mencionados anteriormente, es la comparación de las bases de Alice y Bob. Los bits para los que las bases sean distintas son descartados y los bits donde las bases coinciden se almacenan como secuencia de clave.

Para detectar la presencia de un espía en el enlace se debe separar esta secuencia en dos grupos, uno que será la clave final de cifrado y otro que servirá como grupo de prueba. El criterio para obtener estos grupos cambia según el protocolo utilizado.

Como se ha mencionado en la descripción teórica, en el protocolo BB84 se toman como bits de prueba una parte de la secuencia clave sin hacer distinción entre las bases '+' o '×'. Este porcentaje de bits de prueba es acordado por Alice y Bob antes del proceso de distribución. En la implementación se decidió tomar el primer 25% de los bits de la clave como grupo de prueba.

En cambio, en el protocolo BB84 eficiente los bits de prueba son aquellos en los que se ha coincidido en la base '×'.

Si la clave final de cifrado no tiene una longitud de $\boldsymbol{M}$ bits, vuelve a comenzar el proceso desde que Alice y Bob definen nuevas bases aleatorias. En estos casos se usa como clave una permutación aleatoria de la contraseña introducida por el usuario, cuando la longitud es 320 bits, o una nueva secuencia aleatoria de 10000, con el fin de no repetir la misma cadena.

Una vez que la clave tenga la longitud deseada, comienza el proceso prueba.

Pese a que el programa tiene conocimiento de la presencia de un espía en el momento de aplicar el protocolo de distribución de claves, ya que es necesario simular la aleatoriedad introducida por dicho espía, el emulador no utiliza dicho conocimiento al momento de decidir y notificar al usuario si lo ha habido o no.

El criterio que se sigue para determinar la presencia de un espía en el proceso de establecimiento de una clave es el siguiente:

Si la tasa de error de bit obtenida durante el proceso de prueba de la clave es mayor que el valor esperado, para una cierta temperatura y distancia especificada, entonces, se concluye que existe la posibilidad de que haya un espía.

En las comunicaciones actuales se utilizan símbolos pilotos, conocidos por transmisor y receptor, para hacer una estimación del canal y determinar de qué forma afecta el medio a cada bit, con el fin de recuperar la información transmitida.

### 3.2.12. Umbral de ruido

Para hacer la estimación del canal cuántico y determinar el umbral que permite detectar la presencia de un espía se realizaron múltiples simulaciones sin espía. Se transmitió una secuencia de bits variando las dos fuentes de errores presentes en el sistema, la temperatura y la atenuación del canal para calcular la tasa de error de bit máxima que se puede obtener cuando no hay un espía presente.

La temperatura fue variada entre -273 ˚C y 50 ˚C, en pasos de un grado, y la atenuación entre 0.01 y 1 en pasos de 0.01. Para cada combinación posible se realizó la transmisión de 320 bits, 20 veces o de 10000 bits, también 20 veces y se almacenó la tasa de error de bit máxima obtenida. Una vez realizadas todas las simulaciones el resultado obtenido fue una matriz de 325x101, donde se almacenan las tasas de error de bit máximas, obtenidas sin presencia de espía, para cada posible combinación de temperatura y atenuación.

El programa avisa de la posible presencia de un espía siempre que el porcentaje de error de bit calculado con el grupo de prueba supere la tasa de error máxima para la temperatura y distancia indicada. Se muestra un mensaje en la interfaz gráfica recomendando cancelar la transmisión y descartar la clave.

### 3.2.13. Reconciliación de la clave

Previo al proceso de reconciliación de la clave ya se conoce si se ha detectado un espía. Esto se hace de esta forma con el fin de evitar enmascarar la presencia del espía eliminando los errores que pueda causar con una reconciliación de clave.

Este proceso se hace porque, hasta ahora se ha considerado que, si Alice y Bob usan las mismas bases y no hay un espía presente, estos deberían obtener una clave igual sin errores. Llevando esto a un escenario más realista se puede ver que el canal cuántico introduce errores debido al ruido térmico y atenuación por lo que las claves podrían diferir, aunque no haya un espía presente.

Por esta razón se utilizan técnicas clásicas como códigos bloque lineales y chequeo de paridad para eliminar la mayor cantidad de errores posibles. En este proceso de hace uso de funciones de Matlab como *cyclpoly* y *cyclgen*, las cuales permiten generar un polinomio de un código bloque lineal y una matriz de chequeo de paridad, respectivamente.

#### 3.2.14. No hay espía, pero el nivel de ruido es muy alto

Cuando el porcentaje de error está por debajo del esperado se indica que no hay presencia de un espía y se procede a comparar las claves de Alice y Bob para determinar si son iguales. Este paso no es parte del protocolo, sin embargo, se ha realizado de esta forma para determinar rápidamente si el canal tiene bajos niveles de ruido. Otra forma de hacerlo sería realizando múltiples ejecuciones y estimando para qué valores de temperatura y distancia se vuelve imposible establecer una clave sin equivocaciones.

Si las claves son distintas, el programa recomienda la cancelación de la ejecución a través de un mensaje en la interfaz gráfica.

#### 3.2.15. Nivel de ruido aceptable

Si tras la reconciliación de claves, estas son iguales significa que el nivel de ruido es aceptable y que se puede utilizar dicha clave para cifrar la información.

#### 3.2.16. Cifrado y descifrado del mensaje

Todo el proceso de distribución de claves cuánticas nos da como resultado una clave de ***M*** bits de longitud. Según los requisitos para lograr un cifrado seguro que se han mencionado, es necesario que la clave tenga la misma longitud que el mensaje y que además cada clave sea utilizada una sola vez (one-time pad), sin embargo, debido al gran tiempo de ejecución que tomaría establecer una clave de unos cientos de miles de bits, se recurre a incumplir el segundo punto, bajo la consideración de que en la simulación el espía no es capaz de descifrar nada sabiendo que la clave se repite. Se toma la clave de ***M*** bits y se concatena tantas veces como sea necesario hasta tener la longitud del mensaje completo.

Una vez que ambas cadenas tienen la misma longitud se aplica una operación XOR para cifrar el mensaje. En el extremo receptor, Bob realiza la misma operación para recuperar el mensaje original. En la figura 3.30 se muestra un ejemplo.

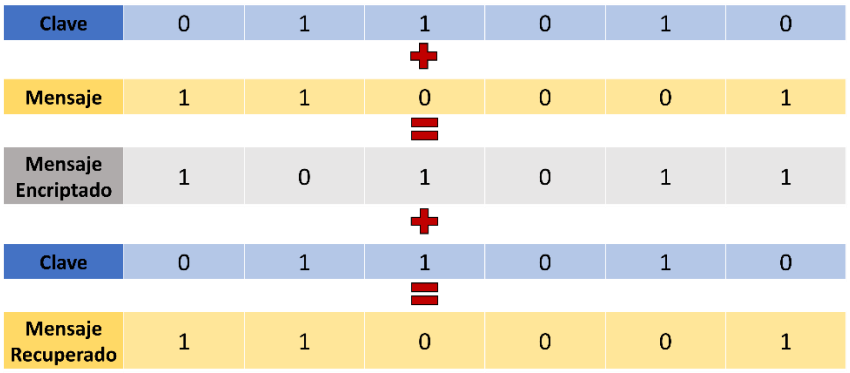


Fig. 3.30. Ejemplo de cifrado y descifrado de un mensaje.

### 3.2.17. Transmisión de la información cifrada

Una vez que se obtiene la clave y se cifra, esta es transmitida en bloques de 100 bits a través del sistema clásico y cuántico. Pasando por sus respectivos componentes, modulador, canal y demodulador como se explicó anteriormente en este capítulo.

En este bloque sí se considera el valor de $N_s$ introducido por el usuario para realizar la transmisión, a diferencia de en el proceso de distribución de claves donde se utilizó $N_s = 1$ para ir acorde al protocolo. Tampoco se calculan varias constelaciones, en este proceso es necesaria solo una, la cual tome la temperatura y distancia entre Alice y Bob, introducidas por el usuario.

Una vez obtenidas las secuencias binarias a la salida de los demoduladores está es descifrada utilizando la clave como se mostró en el subtítulo anterior.

### 3.2.18. Tasas de error

El siguiente paso es calcular la tasa de error obtenida. En este caso, debido a que se consideran solo ejemplos con modulación BPSK, la probabilidad de error y la tasa de error de bit coinciden ya que cada símbolo cuenta con un único bit.

En cada transmisión de 100 bits se van acumulando los bits recibidos erróneamente para calcular al final de la transmisión completa la tasa de error. Estos se obtienen comparando la secuencia original de bits con la recibida.

También se va almacenando un vector con la evolución de esta tasa de error, la cual se calcula dividiendo los bits erróneos obtenidos hasta un instante de tiempo entre el total de bits transmitidos hasta dicho instante.

Al graficar este vector se puede ver como cada vez los valores convergen a la tasa de error total y que para una poca cantidad de bits transmitidos unos pocos bits erróneos pueden disparar la tasa de error.

Las tasas de error teóricas se calculan utilizando las ecuaciones 2.107 y 2.108 para el sistema cuántico y clásico respectivamente.

### 3.2.19. Recuperación de un audio

Se empieza por tomar los valores que fueron guardados en el primer tratamiento del audio, el número de bits por muestra, el máximo y el mínimo del audio original, antes de comenzar la reconstrucción.

Con estos valores se vuelve a construir el vector de niveles que se usa como referencia. Este tendrá 64 niveles entre el valor mínimo y máximo del audio original.

La cadena de bits obtenida se reordena para que cada fila sea un número binario de 6 bits, posteriormente se convierte cada uno en un número entero. Este entero representa el nivel recibido.

Para reconstruir el audio se utiliza el vector de enteros como índice en el vector de referencia, lo que permite recuperar el valor original de las muestras.

### 3.2.20. Recuperación de una imagen

Igual que para el caso del audio se deben tomar los valores iniciales almacenados, en este caso son las dimensiones de la imagen que se va a recuperar.

A partir de aquí se construye un vector con los niveles de referencia, este tendrá 64 niveles entre 0 y 255. El siguiente paso es tomar los bits que se van a reconstruir y reordenarlos, de tal forma que cada fila tenga un número binario de 6 bits.

Estos valores se convierten a números enteros, obteniendo como resultado un vector de valores entre 0 y 63, los cuales representan los distintos niveles de referencia.

Este vector se reordena de nuevo separándolo en 3, uno para cada color RGB (rojo, verde y azul). Utilizando estos como índices dentro del vector de referencia se obtiene un vector de valores de 255 para cada color.

El último paso es ordenar estos vectores como matrices con las dimensiones iguales al ancho y alto de la imagen original y agruparlas en una matriz de tres dimensiones, igual

a la que se obtiene originalmente cuando se lee la imagen. Esta matriz se convierte en una imagen utilizando la función de MATLAB *uint8*.

### 3.2.21. Resultados a través de la interfaz gráfica

Por último, se muestran los resultados a través de la interfaz gráfica. Se muestra la gráfica de la evolución de la tasa de error de bit, comentada anteriormente, para cada sistema para establecer una comparación, como se mostró en la figura 3.20.

Se muestran también las tasas de error final, obtenidas dividiendo la cantidad de bits erróneos entre el total transmitido, comparadas con la tasa de error que se obtiene aplicando las ecuaciones teóricas.

Finalmente, aparece una ventana emergente que mostrará una comparación de las imágenes recibidas a través de ambos sistemas con la original, como se ve en la figura 3.21. O en el caso de un audio se reproducirán primero el original, seguido del recibido a través del clásico y, por último, el recibido a través del cuántico.

# 4. RESULTADOS

En este capítulo se presentan los resultados de los experimentos y simulaciones realizadas para cumplir con los objetivos de este trabajo. El contenido de este se enumera a continuación:

1. Experimentos realizados con el kit de demostración de criptografía cuántica de Thorlabs.
2. Simulación de la transmisión de una imagen utilizando el emulador de un sistema de criptografía cuántica desarrollado y comparación de los resultados obtenidos con los valores esperados mostrados en la introducción teórica.
3. Implementación, validación y comparación de los protocolos BB84 y BB84 eficiente, utilizando el emulador.
4. Implementación del protocolo que brinde las mejores prestaciones en términos de eficiencia y detección de un espía y resultados obtenidos tras someter el sistema a distintos niveles de ruido y atenuación.

## 4.1. Experimentos realizados con el Kit de Thorlabs

Utilizando el kit de demostración de criptografía cuántica se realizaron dos experimentos:

1. Generación de una cadena de bits aleatoria para usar como clave.
2. Establecimiento de una clave secreta y detección de un espía utilizando el protocolo BB84 de distribución de claves cuánticas.

### 4.1.1. Experimento 1: Generación de una cadena aleatoria de bits.

Anteriormente se ha mencionado que gracias a los principios de la mecánica cuántica es posible generar cadenas de bits realmente aleatorias. Una de las formas de lograr esto sería haciendo incidir un único fotón polarizado diagonalmente en un divisor de haz. Este se transmitiría o reflejaría aleatoriamente brindando una cadena de '0' y '1' arbitraria.

El kit permite simular este escenario, pero con el láser de pulsos. Se transmitieron múltiples pulsos de luz con un ángulo de polarización de 45˚ y se midieron en base "+", lo cual no alteró la polarización. Al incidir sobre el divisor se activaron los sensores aleatoriamente generando una secuencia arbitraria de '0' y '1'. En la figura 4.1 se muestra en la primera imagen la polarización de la luz transmitida y en las siguientes se muestran los bits recibidos.

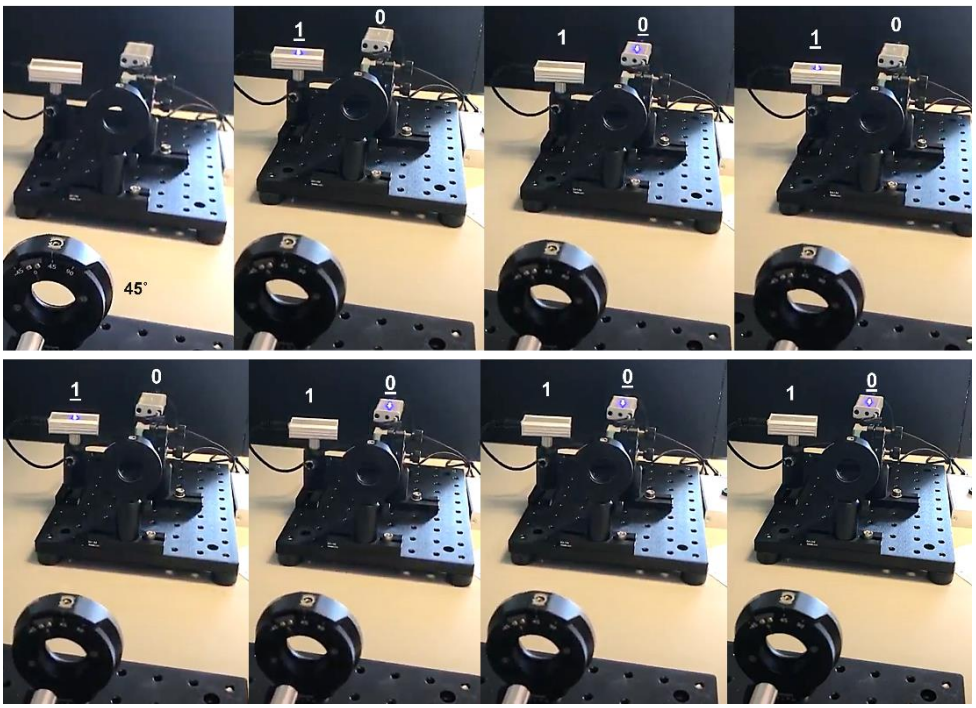


Fig. 4.1. Experimento de generación de una clave aleatoria.

La secuencia obtenida es

| 1 | 0 | 1 | 1 | 0 | 0 | 0 |
|---|---|---|---|---|---|---|

### 4.1.2. Experimento 2: Establecimiento de clave y detección de un espía

Utilizando el método planteado en el experimento anterior se obtuvieron cuatro cadenas de 20 bits que se utilizaron como clave y bases de Alice, Eva y Bob. Para las bases, un '0' significa base "+" y un '1', base "×". Las secuencias obtenidas son las mostradas en la tabla 4.1.

TABLA 4.1. SECUENCIAS ALEATORIAS DE BITS Y BASES OBTENIDAS A TRAVÉS DEL PROCEDIMIENTO DEL EXPERIMENTO 1

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice | × | + | × | + | + | + | × | × | × | + | × | × | + | + | + | × | + | × | × | + |
| | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| Eva | + | + | × | + | × | + | × | × | × | × | + | + | + | × | + | + | × | × | + | × |
| Bob | × | + | + | + | × | + | + | × | × | + | × | + | + | + | × | × | × | + | × | + |

Tras realizar la transmisión de cada bit, Eva y Bob obtienen las cadenas mostradas en la tabla 4.2.

TABLA 4.2. CADENAS DE BITS OBTENIDAS TRAS LA TRANSMISIÓN Y MEDICIÓN

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice | × | + | × | + | + | + | × | × | × | + | × | × | + | + | + | × | + | × | × | + |
| | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| Eva | + | + | × | + | × | + | × | × | × | × | + | + | + | × | + | + | × | × | + | × |
| | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 1 |
| Bob | × | + | + | + | × | + | + | × | × | + | × | + | + | + | × | × | × | + | × | + |
| | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |

Sombreado en verde se muestran todos los eventos aleatorios, causados por bases no coincidentes entre Alice y Eva o Eva y Bob.

Como indica el protocolo, el siguiente paso es que Alice y Bob comparen sus bases a través de un canal público y una vez descartados los bits de bases no coincidentes intercambien algunos bits de prueba para tratar de detectar un posible espía. Debido a que las secuencias de bits son bastante cortas se utilizarán todos los bits elegidos como clave como bits de prueba.

TABLA 4.3. COMPARACIÓN DE LAS BASES UTILIZADAS POR ALICE Y BOB

| | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice | × | + | × | + | + | + | × | × | × | + | × | × | + | + | + | × | + | × | × | + |
| | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 0 | 0 | 0 | 1 | 0 | 1 | 1 | 1 | 0 | 0 |
| Bob | × | + | + | + | × | + | + | × | × | + | × | + | + | + | × | × | × | + | × | + |
| | 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 | 1 |

En la tabla 4.3 se encuentran sombreados en amarillo todos los bits de bases coincidentes. Por último, en la tabla 4.4 se muestra la comparación de los bits para los que las bases coinciden, es decir, los bits de prueba.

TABLA 4.4. COMPARACIÓN DE LA SECUENCIA DE BITS DE PRUEBA

| | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Alice | × | + | + | + | × | × | + | × | + | + | × | × | + |
| | 1 | 0 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 1 | 1 | 0 | 0 |
| Bob | × | + | + | + | × | × | + | × | + | + | × | × | + |
| | 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 | 1 | 0 | 0 | 1 |

En rojo se encuentran marcados los bits que no coinciden entre Alice y Bob. Estos errores ocurren en cuatro de los trece bits, aproximadamente un 30%, el cual es bastante cercano al 25% de error que se espera obtener en presencia de un espía.

### 4.2. Emulador de un sistema de comunicaciones cuántico

Se realizó la transmisión de imágenes a través de los sistemas cuántico y clásico, utilizando una modulación BPSK, para distintos valores del número promedio de fotones por símbolo $N_s$, entre 0.5 y 2.5, y el número promedio de fotones térmicos $\mathcal{N}$, entre 0 y 0.2.

Se busca validar la implementación de este emulador comparando las probabilidades de error para cada combinación de $N_s$ y $\mathcal{N}$ obtenidas a través de simulaciones con la gráfica de la figura 4.2.

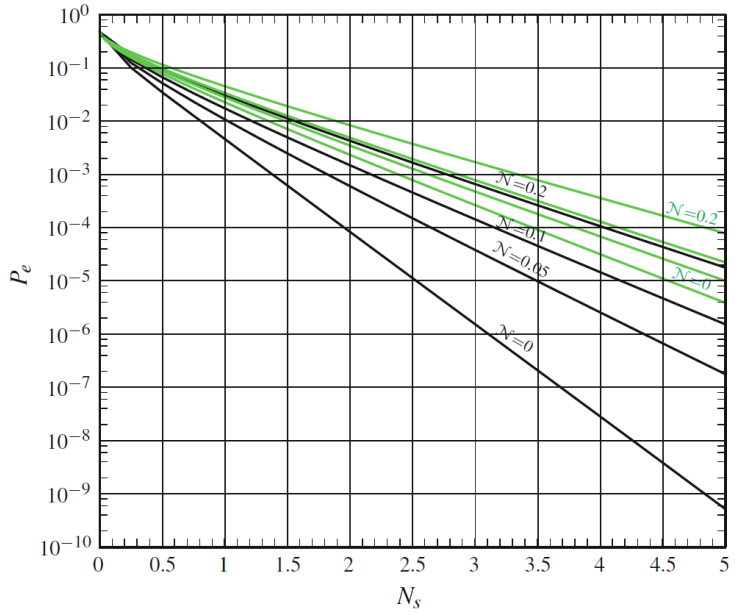


Fig. 4.2. Comparación de la probabilidad de error de un sistema con modulación BPSK en función $N_s$ y de $\mathcal{N}$ [11].

En ella se muestra una comparación de la probabilidad de error obtenida con una modulación BPSK para distintos valores de $N_s$ y $\mathcal{N}$ de un sistema cuántico (color negro) y uno clásico (color verde).

Es importante mencionar que en estas simulaciones no se cifra la información. Tampoco se transmite la misma imagen para todos los casos ya que a medida que la probabilidad de error decrece se necesitan más bits para que esta converja.

Las imágenes transmitidas son las de las figuras 4.3 y 4.4.

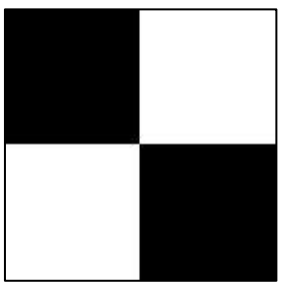

Fig. 4.3. Primera imagen de prueba.

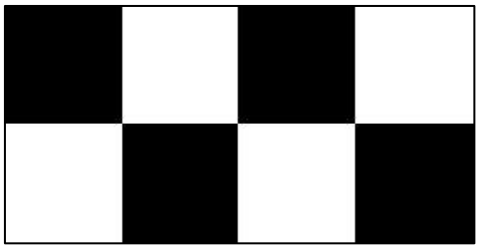

Fig. 4.4. Segunda imagen de prueba.

Estas son imágenes con pocos píxeles para que la ejecución sea rápida. La figura 4.3 tiene unas dimensiones de 139x139 píxeles y la figura 4.4, de 276x139.

En las siguientes 20 figuras se muestra el resultado recibido a través de ambos canales para cada combinación de los valores de $N_s$ y $\mathcal{N}$.

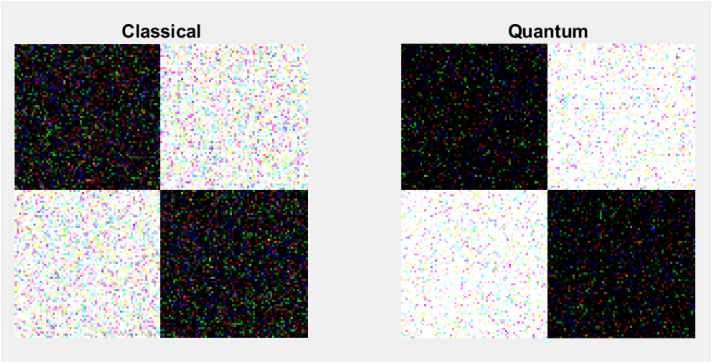


Fig. 4.5. Comparación sistema clásico y cuántico para $N_s = 0.5$ y $\mathcal{N} = 0$

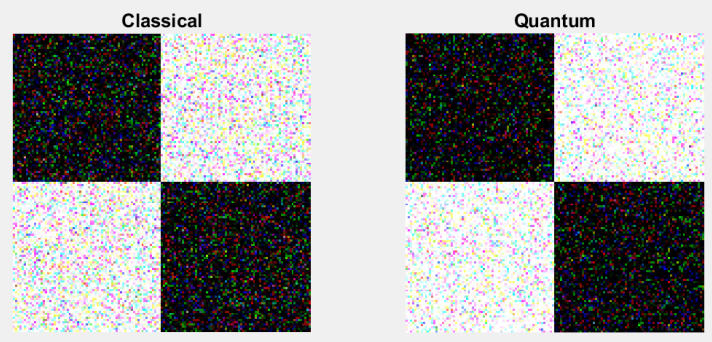


Fig. 4.6. Comparación sistema clásico y cuántico para $N_s = 0.5$ y $\mathcal{N} = 0.05$

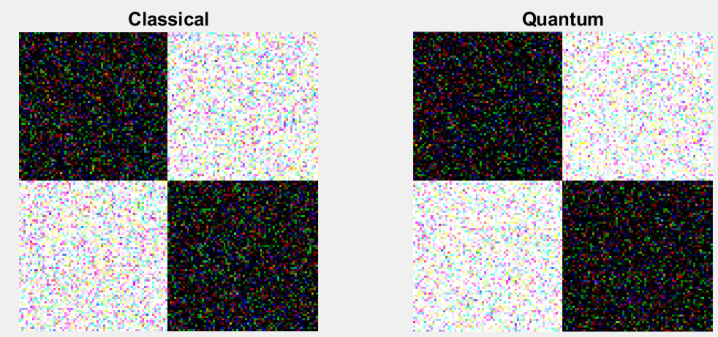


Fig. 4.7. Comparación sistema clásico y cuántico para $N_s = 0.5$ y $\mathcal{N} = 0.1$

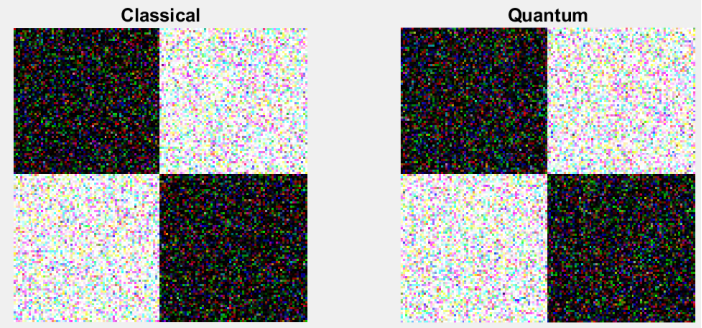


Fig. 4.8. Comparación sistema clásico y cuántico para $N_s = 0.5$ y $\mathcal{N} = 0.2$

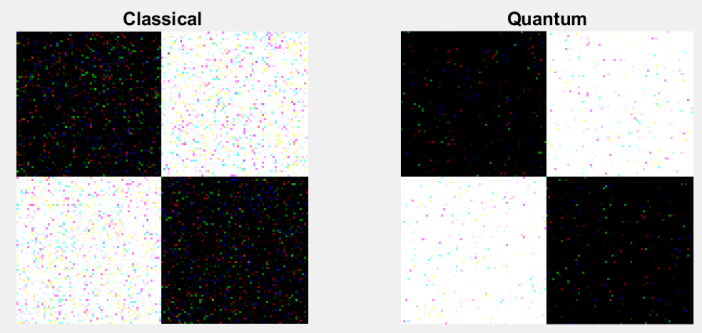


Fig. 4.9. Comparación sistema clásico y cuántico para $N_s = 1$ y $\mathcal{N} = 0$

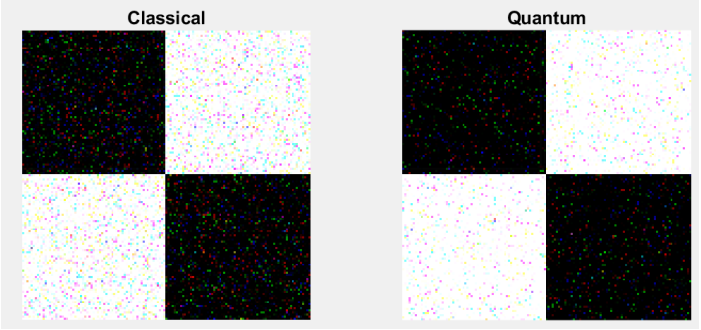


Fig. 4.10. Comparación sistema clásico y cuántico para $N_s = 1$ y $\mathcal{N} = 0.05$

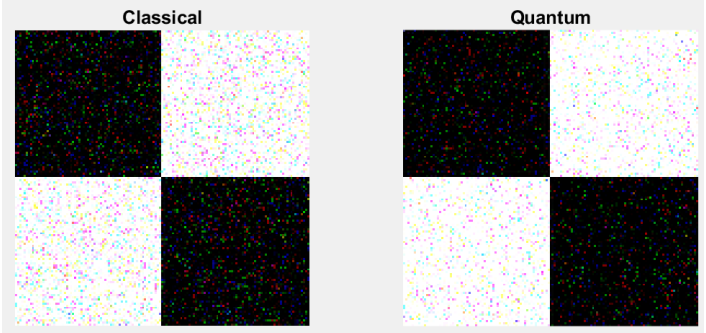


Fig. 4.11. Comparación sistema clásico y cuántico para $N_s = 1$ y $\mathcal{N} = 0.1$

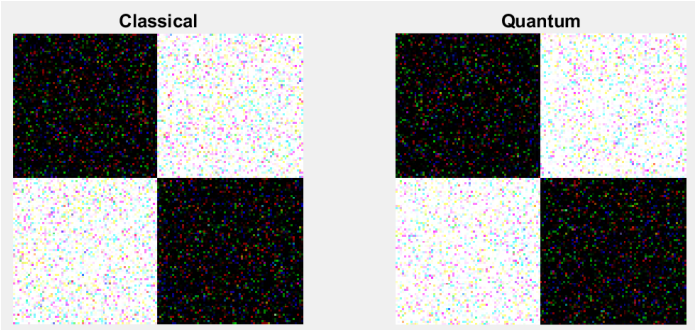


Fig. 4.12. Comparación sistema clásico y cuántico para $N_s = 1$ y $\mathcal{N} = 0.2$

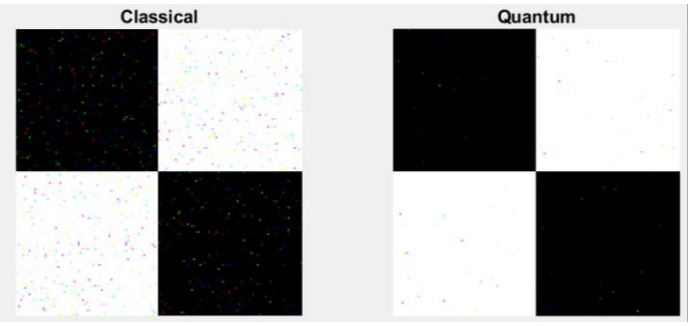


Fig. 4.13. Comparación sistema clásico y cuántico para $N_s = 1.5$ y $\mathcal{N} = 0$

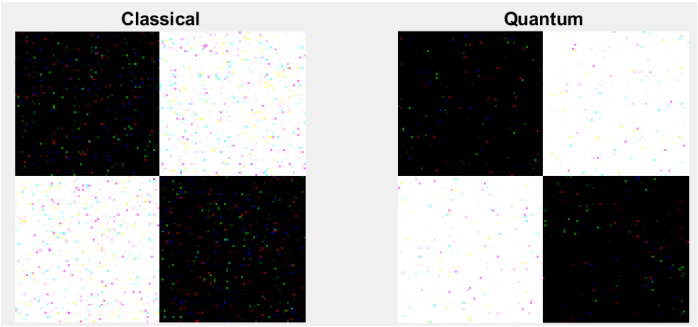


Fig. 4.14. Comparación sistema clásico y cuántico para $N_s = 1.5$ y $\mathcal{N} = 0.05$

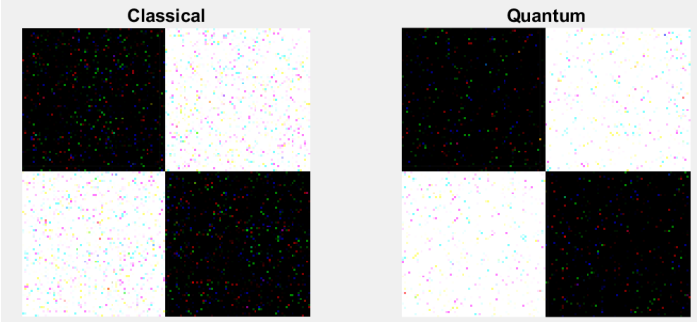


Fig. 4.15. Comparación sistema clásico y cuántico para $N_s = 1.5$ y $\mathcal{N} = 0.1$

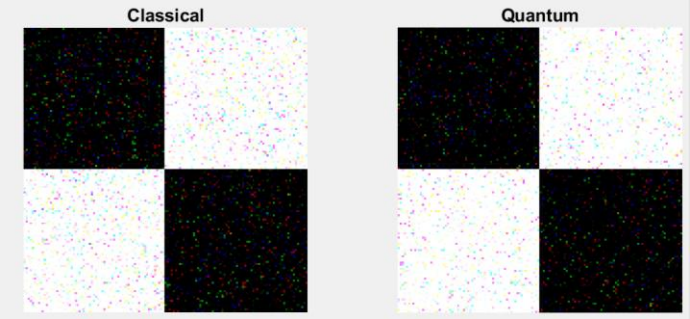


Fig. 4.16. Comparación sistema clásico y cuántico para $N_s = 1.5$ y $\mathcal{N} = 0.2$

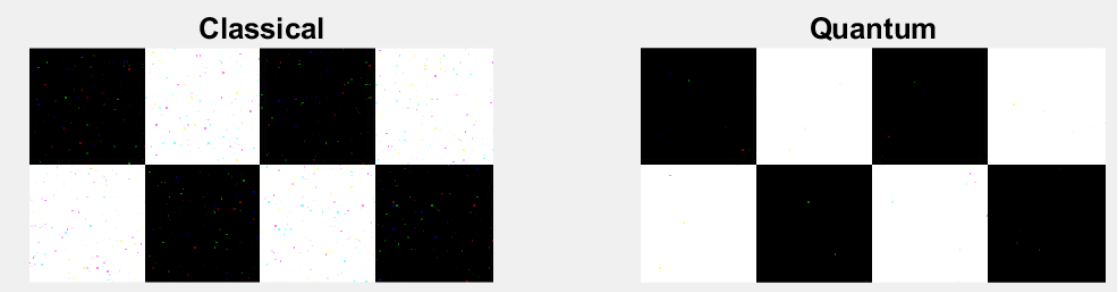


Fig. 4.17. Comparación sistema clásico y cuántico para $N_s = 2$ y $\mathcal{N} = 0$

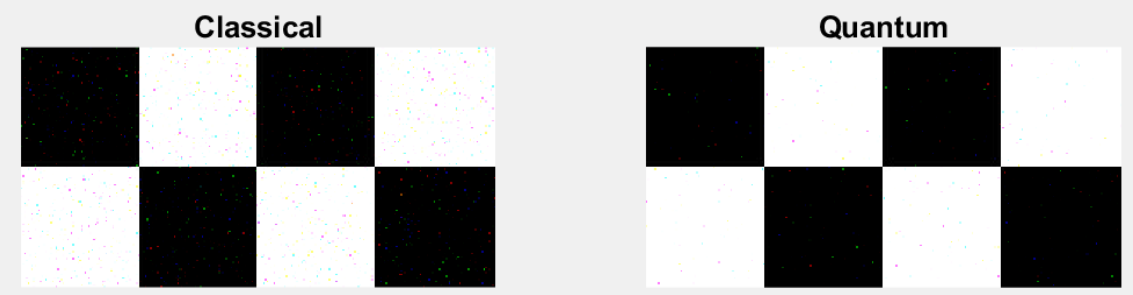


Fig. 4.18. Comparación sistema clásico y cuántico para $N_s = 2$ y $\mathcal{N} = 0.05$

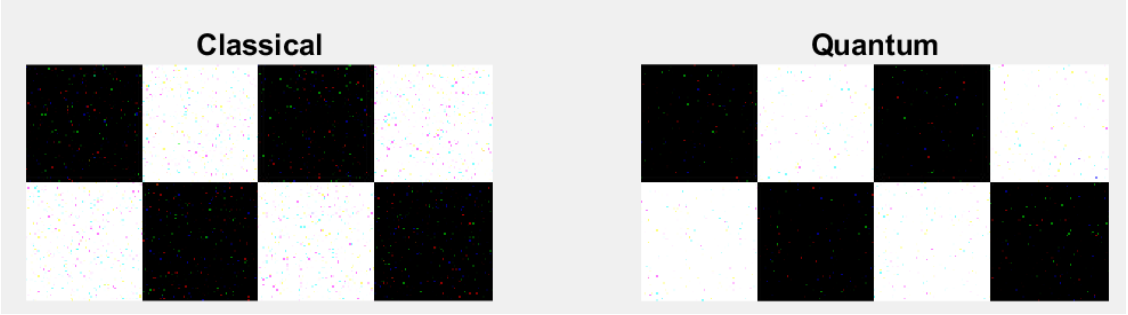


Fig. 4.19. Comparación sistema clásico y cuántico para $N_s = 2$ y $\mathcal{N} = 0.1$

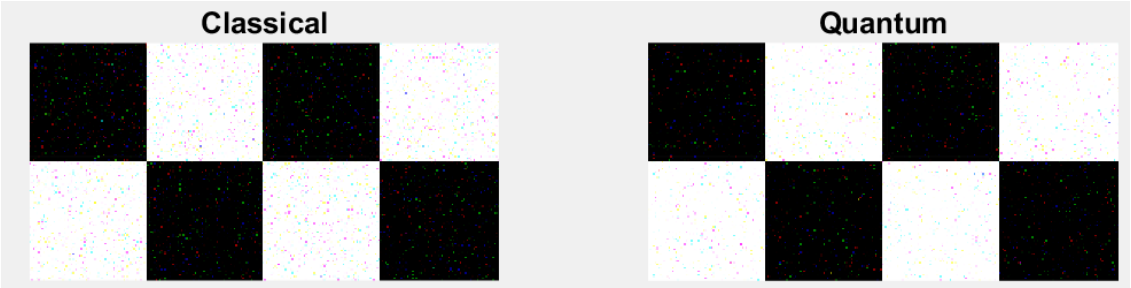


Fig. 4.20. Comparación sistema clásico y cuántico para $N_s = 2$ y $\mathcal{N} = 0.2$


Fig. 4.21. Comparación sistema clásico y cuántico para $N_s = 2.5$ y $\mathcal{N} = 0$


Fig. 4.22. Comparación sistema clásico y cuántico para $N_s = 2.5$ y $\mathcal{N} = 0.05$

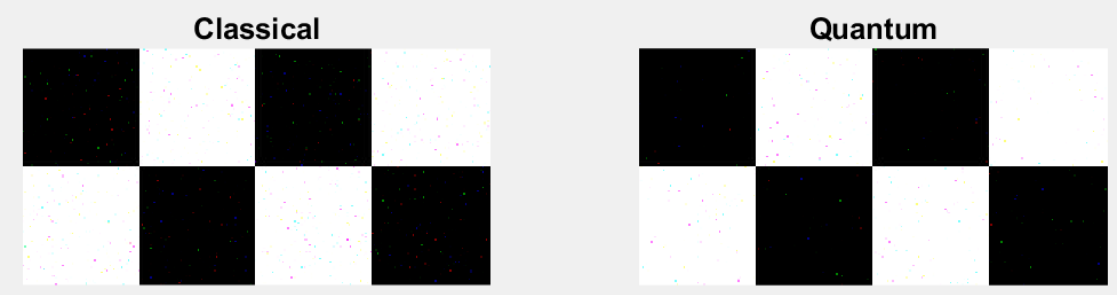


Fig. 4.23. Comparación sistema clásico y cuántico para $N_s = 2.5$ y $\mathcal{N} = 0.1$

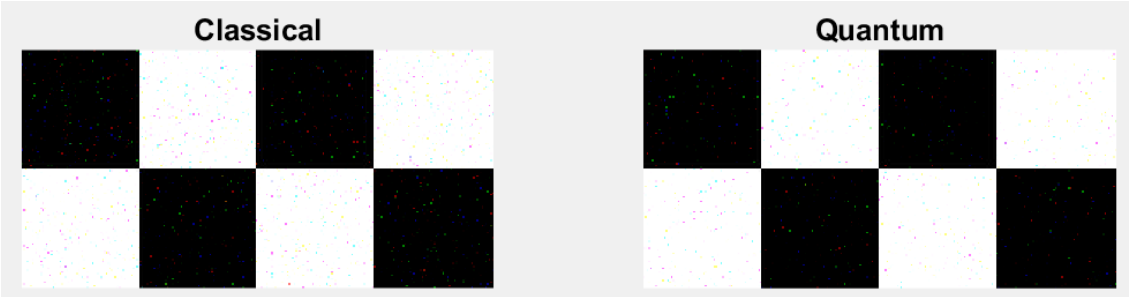


Fig. 4.24. Comparación sistema clásico y cuántico para $N_s = 2.5$ y $\mathcal{N} = 0.2$

Las probabilidades de error devueltas por el emulador al transmitir cada imagen se recopilaron en la tabla 4.5 y se graficaron, como se muestra en la figura 4.25.

TABLA 4.5. PROBABILIDADES DE ERROR PARA CADA IMAGEN TRANSMITIDA A TRAVÉS DE AMBOS SISTEMAS

| **Ns\N** | **0** | | **0.05** | | **0.1** | | **0.2** | |
|---|---|---|---|---|---|---|---|---|
| | **Clásico** | **Cuántico** | **Clásico** | **Cuántico** | **Clásico** | **Cuántico** | **Clásico** | **Cuántico** |
| **0.5** | 7.88e-2 | 3.51e-2 | 8.84e-2 | 6.22e-2 | 9.9e-2 | 8.27e-2 | 1.16e-1 | 1.22e-1 |
| **1** | 2.29e-2 | 4.67e-3 | 2.85e-2 | 1.3e-2 | 3.42e-2 | 2.11e-2 | 4.59e-2 | 3.95e-2 |
| **1.5** | 6.95e-3 | 5.92e-4 | 9.57e-3 | 3.09e-3 | 1.25e-2 | 6.09e-3 | 1.93e-2 | 1.43e-2 |
| **2** | 2.36e-3 | 9.12e-5 | 3.38e-3 | 6.75e-4 | 5.02e-3 | 1.92e-3 | 8.58e-3 | 5.34e-3 |
| **2.5** | 7.94e-4 | 1.23e-5 | 1.38e-3 | 1.88e-4 | 1.89e-3 | 6.94e-4 | 3.71e-3 | 2.14e-3 |

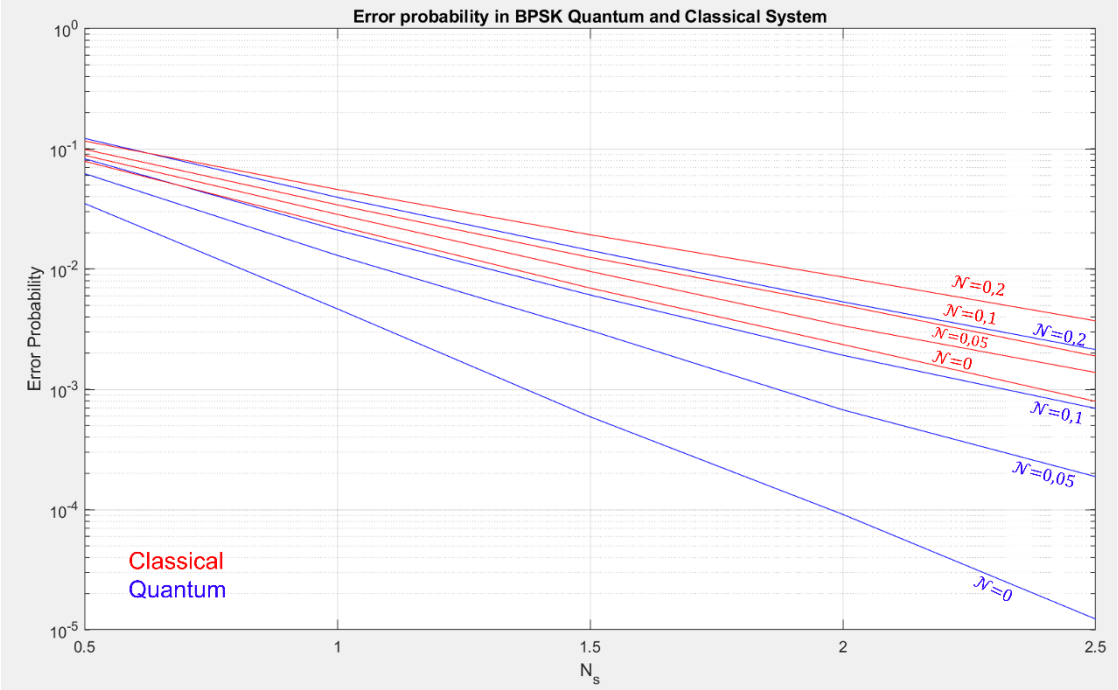


Fig. 4.25. Probabilidad de error en función de $N_s$ para distintos valores de $\mathcal{N}$.

Por último, para establecer una comparación más sencilla de ver se combinaron las gráficas de la figura 4.2 (derecha) y de la figura 4.25 (izquierda) con los mismos límites en los ejes. Esta comparación se muestra en la figura 4.26.

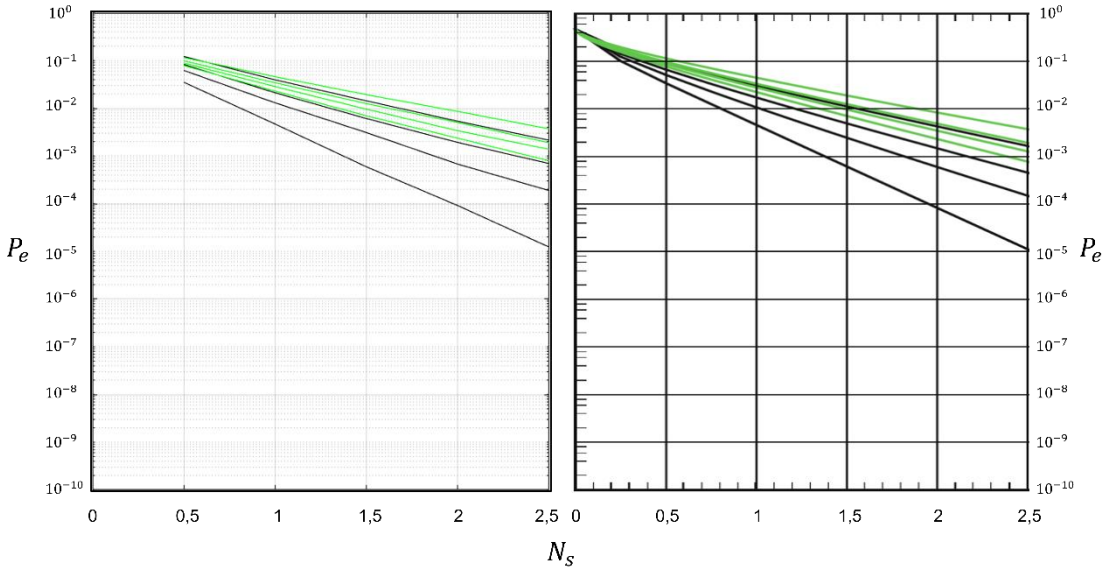


Fig. 4.26. Comparación probabilidad de error teórica y práctica

A partir de esta imagen se puede corroborar que el emulador desarrollado es capaz de simular correctamente la transmisión de información bajo los efectos del ruido térmico ya que brinda una muy buena aproximación a las probabilidades teóricas.

### 4.3. Comparación de los protocolos BB84 y BB84 eficiente.

En esta sección se busca validar el funcionamiento correcto de la implementación de ambos protocolos, a través de simulaciones, comparando los resultados con los que se describen teóricamente o que se consiguen utilizando el kit físico de demostración. Tras validarlos se comparan para elegir aquel que brinde mejores prestaciones en términos de eficiencia y capacidad de detección de un espía.

Al disponer de dos protocolos distintos, se vuelve necesario realizar validaciones diferentes. Se busca validar el correcto funcionamiento del protocolo BB84 demostrando que la máxima eficiencia que se puede obtener es del 50%. Para el protocolo BB84 eficiente, se quiere verificar que su eficiencia puede superar el 50% y que, además, si se aumenta el número de bits de la clave se puede seguir incrementando la eficiencia.

La eficiencia de ambos protocolos puede aumentarse hasta llegar a su máximo valor, sin embargo, esto podría causar inconvenientes en la detección del espía, ya que al reducir la cantidad de bits que se utilizan en el grupo de prueba; bits que siempre son descartados, disminuye la posibilidad de detectar una intervención.

Por esta razón se estudia el aumento de la eficiencia atado a la capacidad de detección del espía.

Se estudian además los efectos de utilizar los siguientes tipos de espías:

- Espía con base “random” que intercepta el 100% de los bits.
- Espía con base “random” que intercepta el 50% de los bits.
- Espía con base “best” que intercepta el 100% de los bits.
- Espía con base “best” que intercepta el 50% de los bits.

Utilizando solo los dos primeros en la validación del protocolo BB84 y todos en el BB84 eficiente. Se busca en particular comprobar que a menor porcentaje de bits interceptados menor será la capacidad de detección y que en los casos donde se compare “best” con “random” se podrá detectar más fácilmente al espía con base “best”.

Por último, es importante mencionar que en las simulaciones se ha considerado el caso ideal, es decir, un canal de fibra óptica de distancia 0 metros a una temperatura de -200 ˚C, con el fin de visualizar solamente los efectos de variar los parámetros de los protocolos y no del entorno.

### 4.3.1. Protocolo BB84

En la tabla 4.6 se muestran los valores teóricos que serán comparados con los obtenidos a través de simulaciones. A continuación de esta se encuentran las fórmulas y consideraciones tomadas para realizar los cálculos.

TABLA 4.6. VALORES TEÓRICOS DEL PROTOCOLO BB84 PARA UNA CLAVE DE 320 BITS

| **Bits de prueba** | | | |
|---|---|---|---|
| **Como porcentaje de la clave** | **Como cantidad de bits** | **Eficiencia calculada teóricamente** | **Bits que es necesario transmitir** |
| 0.25 | 80 | 0.4 | 800 |
| 0.24 | 77 | 0.403 | 794 |
| 0.23 | 74 | 0.406 | 788 |
| 0.22 | 70 | 0.409 | 781 |
| 0.21 | 67 | 0.413 | 775 |
| 0.20 | 64 | 0.416 | 768 |
| 0.19 | 61 | 0.42 | 762 |
| 0.18 | 58 | 0.423 | 756 |
| 0.17 | 54 | 0.427 | 749 |
| 0.16 | 51 | 0.43 | 743 |
| 0.15 | 48 | 0.434 | 736 |
| 0.14 | 45 | 0.438 | 730 |
| 0.13 | 42 | 0.442 | 724 |
| 0.12 | 38 | 0.446 | 717 |
| 0.11 | 35 | 0.45 | 711 |
| 0.10 | 32 | 0.454 | 704 |
| 0.09 | 29 | 0.458 | 698 |
| 0.08 | 26 | 0.462 | 691 |
| 0.07 | 22 | 0.467 | 685 |
| 0.06 | 19 | 0.471 | 679 |
| 0.05 | 16 | 0.476 | 672 |
| 0.04 | 13 | 0.48 | 666 |
| 0.03 | 10 | 0.485 | 660 |
| 0.02 | 6 | 0.49 | 653 |
| 0.01 | 3 | 0.495 | 647 |
| 0 | 0 | 0.5 | 640 |

Los bits teóricos transmitidos se calculan según la siguiente fórmula:

$$B_{tx} \cong 2(Longitud_{Clave} + Porcentaje_{Prueba} \times Longitud_{Clave})$$

Esta fórmula proviene de las siguientes consideraciones:

- $Longitud_{Clave} = 320$.
- Se ha decidido variar el porcentaje de bits de prueba entre 1% y 25%.
- Al multiplicar este porcentaje por la longitud de la clave obtenemos la cantidad de bits que se utilizarán en el proceso de prueba.
- La cantidad total de bits de clave que hay que obtener no es 320, sino la suma de 320 más los bits de prueba, ya que estos últimos serán descartados.
- Debido a que las bases en este protocolo son equiprobables, la probabilidad de que Alice y Bob elijan la misma base es del 50% causando que se descarte siempre un 50% de los bits transmitidos, aproximadamente. Por esta razón se estima que es necesario transmitir al menos el doble de la cantidad total de bits de clave explicada en el punto anterior.

La eficiencia teórica se calcula como:

$$Eff_T = \frac{Longitud_{Clave}}{B_{tx}} = \frac{320}{B_{tx}}$$

Para la validación de este protocolo se programó un bucle en el proceso de distribución de claves cuánticas. Se realizan 200 ejecuciones simulando la presencia de un espía, con bases aleatorias equiprobables. Las primeras 100 con un espía que intercepta el 100% de los bits y en las últimas 100 interceptando solo el 50%.

Para ver cambios en la eficiencia se varía la cantidad de bits que se utiliza en el proceso de detección del espía, ya que estos son siempre descartados y al reducir su cantidad puede aumentarse la eficiencia. De estas ejecuciones se almacena la eficiencia, si se logró detectar la presencia del espía y la cantidad total de bits que fue necesario transmitir para obtener la clave de longitud 320 más los bits utilizados para la detección.

Para poder ver los resultados en gráficas se calcula la media de todas las ejecuciones, obteniéndose un valor de eficiencia, una probabilidad de detección y un total de bits transmitidos para cada porcentaje de prueba.

En la figura 4.27 se comparan los resultados obtenidos en ambas simulaciones.

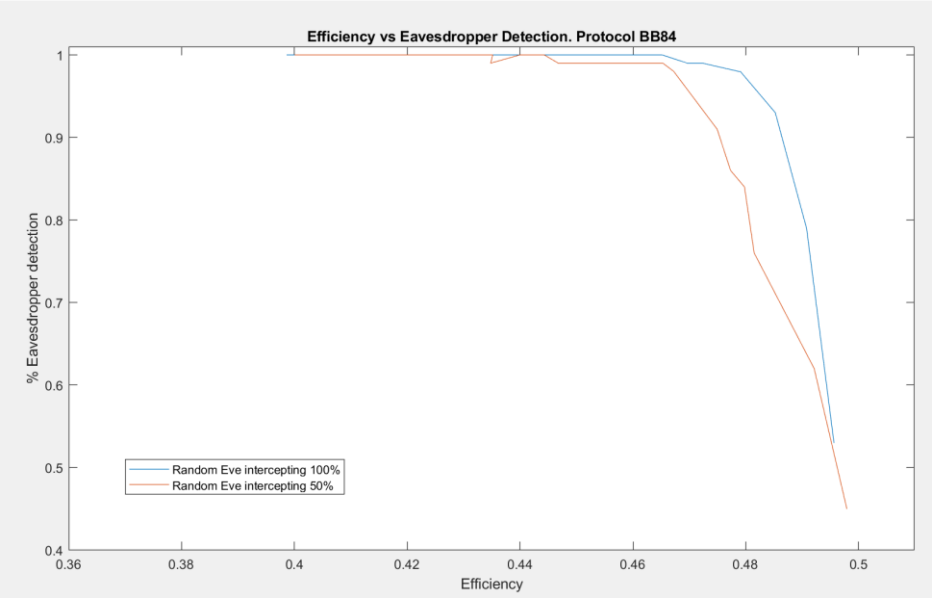


Fig. 4.27. Comparación de la eficiencia y detección entre dos tipos de espías.

Lo primero que se puede apreciar es que no se supera en ningún caso una eficiencia de 50%, lo que concuerda con lo expuesto teóricamente sobre el protocolo.

Comparando los efectos causados por los distintos tipos de espía se observa que hay una mayor capacidad de detección cuando el espía intercepta el 100% de los bits. Se vuelve más fácil detectar a un espía si introduce aleatoriedad a más bits ya que aumenta la probabilidad de que genere un error en los casos donde Alice y Bob tienen bases coincidentes.

En la figura 4.28 se compara la cantidad de bits que es necesario transmitir para cada tipo de espía, con los valores teóricos de la tabla 6.

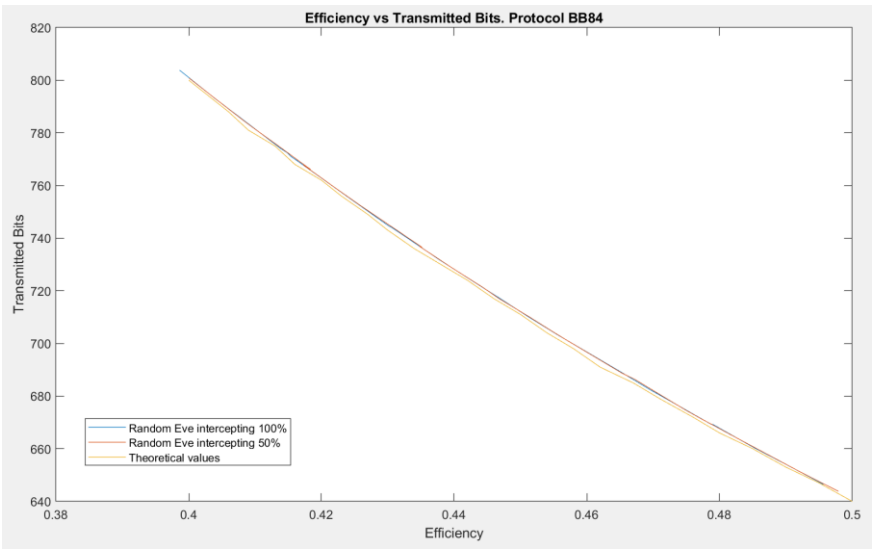


Fig. 4.28. Comparación del número de bits transmitidos con los valores teóricos de la tabla 6.

Debido a que la cantidad de bits transmitidos depende solo de la eficiencia y no del tipo de espía, se observa que tanto para el espía que intercepta el 100% como para el de 50% las cantidades de bits son prácticamente iguales.

En la imagen también se puede apreciar que se obtiene una buena aproximación a los valores teóricos.

### 4.3.2. Protocolo BB84 eficiente con clave de 320 bits

Para este protocolo, igual que para el anterior, se comparan los valores obtenidos a través de las simulaciones con los teóricos que se muestran a continuación en la tabla 4.7.

TABLA 4.7. VALORES TEÓRICOS DEL PROTOCOLO BB84 EFICIENTE PARA UNA CLAVE DE 320 BITS

| Probabilidad base '+' | Probabilidad base 'x' | Cantidad de bits de prueba | Eficiencia calculada teóricamente | Bits que es necesario transmitir |
|---|---|---|---|---|
| 0.7 | 0.3 | 29 | 0.4900 | 654 |
| 0.71 | 0.29 | 27 | 0.5041 | 635 |
| 0.72 | 0.28 | 26 | 0.5184 | 618 |
| 0.73 | 0.27 | 24 | 0.5329 | 601 |
| 0.74 | 0.26 | 22 | 0.5476 | 585 |
| 0.75 | 0.25 | 20 | 0.5625 | 569 |
| 0.76 | 0.24 | 19 | 0.5776 | 555 |
| 0.77 | 0.23 | 17 | 0.5929 | 540 |
| 0.78 | 0.22 | 16 | 0.6084 | 526 |
| 0.79 | 0.21 | 15 | 0.6241 | 513 |
| 0.80 | 0.20 | 13 | 0.6400 | 500 |
| 0.81 | 0.19 | 12 | 0.6561 | 488 |
| 0.82 | 0.18 | 11 | 0.6724 | 476 |
| 0.83 | 0.17 | 10 | 0.6889 | 465 |
| 0.84 | 0.16 | 9 | 0.7056 | 454 |
| 0.85 | 0.15 | 8 | 0.7225 | 443 |
| 0.86 | 0.14 | 7 | 0.7396 | 433 |
| 0.87 | 0.13 | 6 | 0.7569 | 423 |
| 0.88 | 0.12 | 5 | 0.7744 | 414 |
| 0.89 | 0.11 | 4 | 0.7921 | 404 |
| 0.90 | 0.10 | 4 | 0.8100 | 396 |
| 0.91 | 0.09 | 3 | 0.8281 | 387 |
| 0.92 | 0.08 | 3 | 0.8464 | 379 |
| 0.93 | 0.07 | 2 | 0.8649 | 370 |

| | | | | |
|---|---|---|---|---|
| 0.94 | 0.06 | 2 | 0.8836 | 363 |
| 0.95 | 0.05 | 1 | 0.9025 | 355 |
| 0.96 | 0.04 | 1 | 0.9216 | 348 |
| 0.97 | 0.03 | 1 | 0.9409 | 341 |
| 0.98 | 0.02 | 1 | 0.9604 | 334 |
| 0.99 | 0.01 | 1 | 0.9801 | 327 |
| 0.991 | 0.009 | 1 | 0.9821 | 326 |
| 0.992 | 0.008 | 1 | 0.9841 | 326 |
| 0.993 | 0.007 | 1 | 0.9860 | 325 |
| 0.994 | 0.006 | 1 | 0.9880 | 324 |
| 0.995 | 0.005 | 1 | 0.9900 | 324 |
| 0.996 | 0.004 | 1 | 0.9920 | 323 |
| 0.997 | 0.003 | 1 | 0.9940 | 322 |
| 0.998 | 0.002 | 1 | 0.9960 | 322 |
| 0.999 | 0.001 | 1 | 0.9980 | 321 |
| 1 | 0 | 0 | 1 | 320 |

En este caso, la fórmula para calcular los bits que es necesario transmitir es la siguiente:

$$B_{tx} \cong \frac{1}{p_+^2} Longitud_{Clave} = \frac{1}{Eff_T} \times 320$$

Esta fórmula surge de las siguientes consideraciones:

- $Longitud_{Clave} = 320$.
- Debido a que en este protocolo la clave útil se obtiene cuando coincide la base '+', la eficiencia depende de la probabilidad de que Alice y Bob coincidan en dicha base. Esta eficiencia es igual a la probabilidad de la base '+' al cuadrado.
- La parte de la clave utilizada para pruebas está formada por los bits donde Alice y Bob coincidan en la base '×'. Este porcentaje se calcula como la probabilidad de la base '×'al cuadrado.

Para validar la implementación de este protocolo se utilizó el mismo bucle que en el caso anterior. Se realizan 400 simulaciones, 100 para cada tipo de espía.

Para aumentar la eficiencia se varió la probabilidad de la base '+' desde 70% hasta 99% en pasos de 1% y luego de 99,1% hasta 100% en pasos de 0,1%.

De estas ejecuciones se guardan los mismos tres parámetros que en el protocolo anterior y para graficar los resultados se calcula la media de las ejecuciones para obtener un valor

de eficiencia, una probabilidad de detección y un total de bits transmitidos para cada porcentaje de prueba.

En la figura 4.29 se muestra la comparación de los resultados obtenidos de los cuatro tipos de espías utilizados.

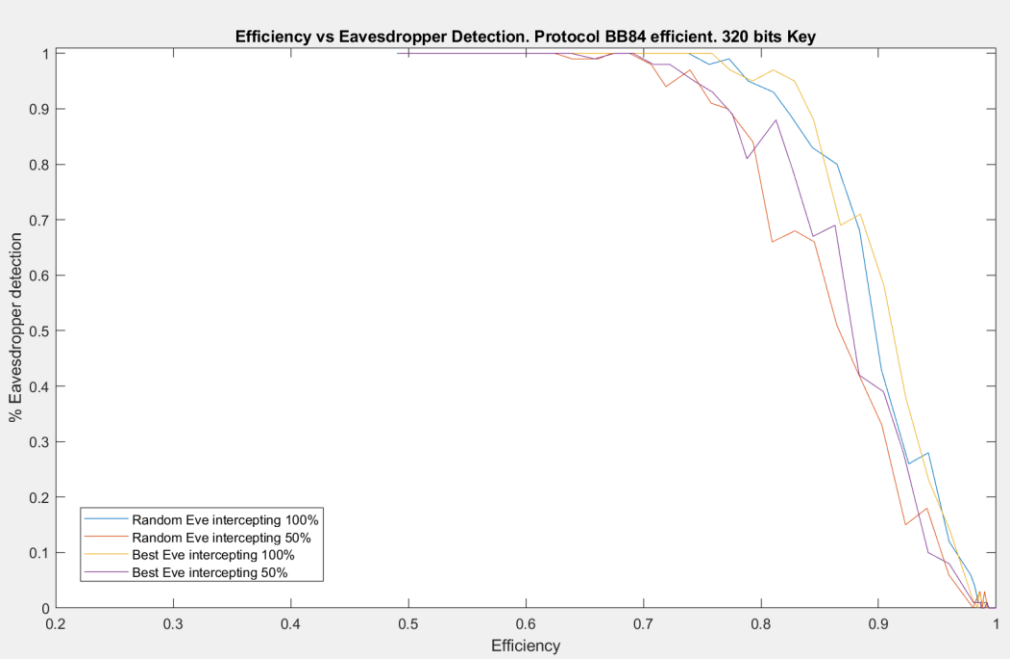


Fig. 4.29. Comparación de la eficiencia y detección entre cuatro tipos de espías.

Lo primero que se puede apreciar es que la eficiencia puede superar el 50%, como se indica teóricamente. Además, se comprueban los valores obtenidos en la tabla ya que el rango va desde 49% hasta el 100%, aproximadamente.

Los casos donde se espía solo el 50% de los bits presentan una capacidad de detección menor a los casos donde se intercepta el 100%. Y comparando los espías “best” con “random”, en la mayoría de los casos hay mayor posibilidad de detectar al espía cuando se usa la base “best”.

Pese a que al utilizar este protocolo se ha logrado superar el umbral del 50%, se ha conseguido llegar la eficiencia como máximo hasta aproximadamente el 64%, en el caso donde se intercepta el 50% de los bits, y hasta un 76%, para el caso de 100% de bits espiados. En la figura 4.30 se pueden apreciar mejor estos valores.

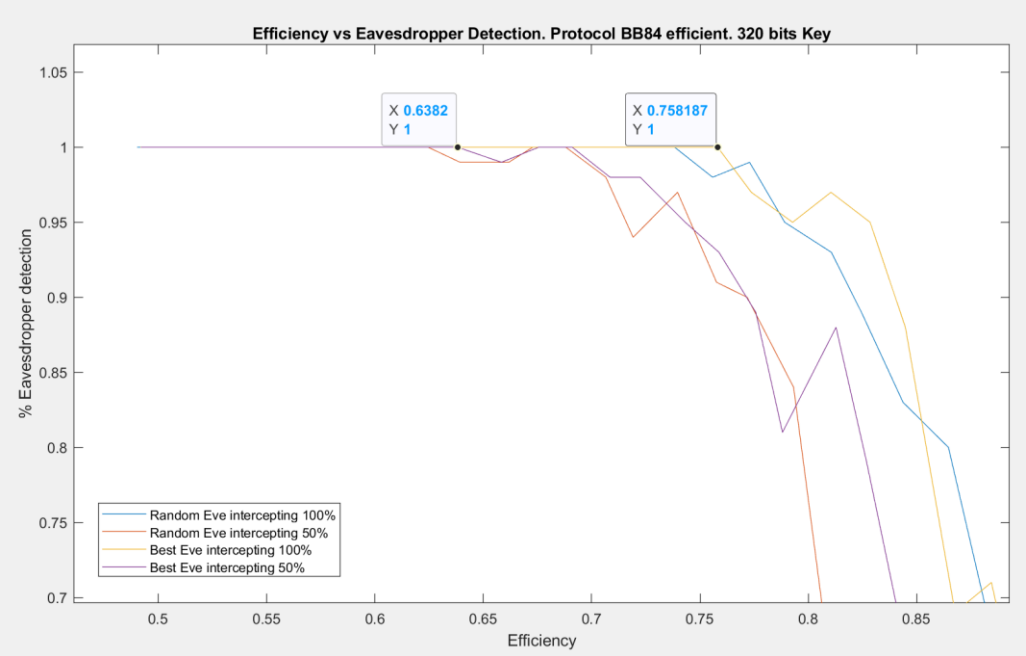


Fig. 4.30. Valores máximos de eficiencia obtenidos para 320 bits de clave.

A continuación, se comparan los bits que fue necesario transmitir para cada tipo de espía para poder establecer la clave de 320 bits con los valores mostrados en la tabla 7. Los resultados se muestran en la figura 4.31.

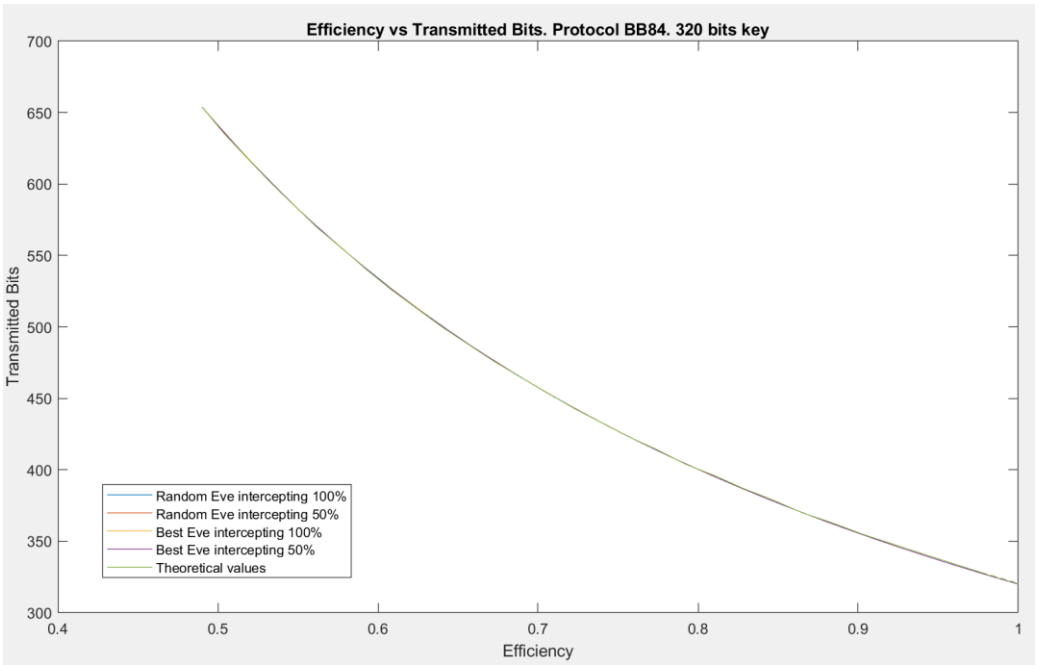


Fig. 4.31. Comparación del número de bits transmitidos con los valores teóricos de la tabla 7.

Nuevamente, como la cantidad de bits solo depende de la eficiencia y no de la capacidad de detección, se obtienen los mismos rangos de valores para los cuatro tipos de espías.

También, se observa que coinciden estos valores con los calculados teóricamente en la tabla.

En la figura 4.32 se muestra una comparación de la cantidad de bits que es necesario transmitir entre ambos protocolos.

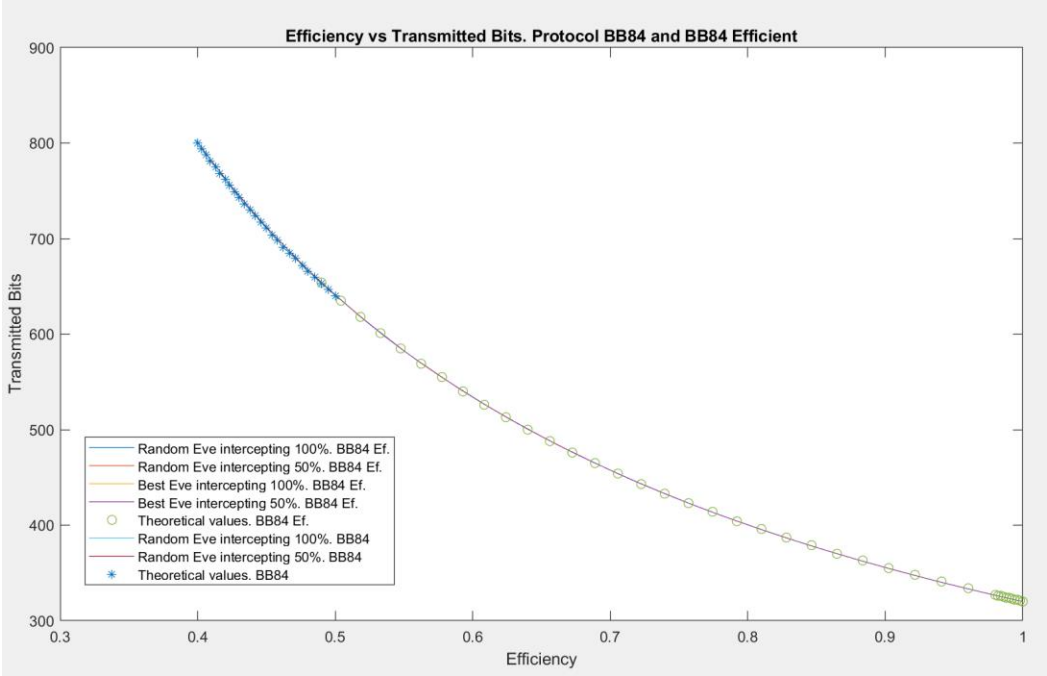


Fig. 4.32. Comparación de la cantidad de bits transmitidos entre el protocolo BB84 y el BB84 eficiente.

En esta última se puede apreciar que para establecer una contraseña de la misma longitud el protocolo BB84 eficiente necesita transmitir, en todos los casos, menos bits que el protocolo BB84.

### 4.3.3. Protocolo BB84 eficiente con clave de 10000 bits

En este protocolo también se comparan los valores obtenidos a través de las simulaciones con los que se muestran en la siguiente la tabla 4.8.

TABLA 4.8. VALORES TEÓRICOS DEL PROTOCOLO BB84 EFICIENTE PARA UNA CLAVE DE 10000 BITS

| Probabilidad base '+' | Probabilidad base 'x' | Cantidad de bits de prueba | Eficiencia calculada teóricamente | Bits que es necesario transmitir |
|---|---|---|---|---|
| 0.7 | 0.3 | 900 | 0.4900 | 20409 |
| 0.71 | 0.29 | 841 | 0.5041 | 19838 |
| 0.72 | 0.28 | 784 | 0.5184 | 19291 |
| 0.73 | 0.27 | 729 | 0.5329 | 18766 |

| | | | | |
|---|---|---|---|---|
| 0.74 | 0.26 | 676 | 0.5476 | 18262 |
| 0.75 | 0.25 | 625 | 0.5625 | 17778 |
| 0.76 | 0.24 | 576 | 0.5776 | 17314 |
| 0.77 | 0.23 | 529 | 0.5929 | 16867 |
| 0.78 | 0.22 | 484 | 0.6084 | 16437 |
| 0.79 | 0.21 | 441 | 0.6241 | 16024 |
| 0.80 | 0.20 | 400 | 0.6400 | 15625 |
| 0.81 | 0.19 | 361 | 0.6561 | 15242 |
| 0.82 | 0.18 | 324 | 0.6724 | 14873 |
| 0.83 | 0.17 | 289 | 0.6889 | 14516 |
| 0.84 | 0.16 | 256 | 0.7056 | 14173 |
| 0.85 | 0.15 | 225 | 0.7225 | 13841 |
| 0.86 | 0.14 | 196 | 0.7396 | 13521 |
| 0.87 | 0.13 | 169 | 0.7569 | 13212 |
| 0.88 | 0.12 | 144 | 0.7744 | 12914 |
| 0.89 | 0.11 | 121 | 0.7921 | 12625 |
| 0.90 | 0.10 | 100 | 0.8100 | 12346 |
| 0.91 | 0.09 | 81 | 0.8281 | 12076 |
| 0.92 | 0.08 | 64 | 0.8464 | 11814 |
| 0.93 | 0.07 | 49 | 0.8649 | 11563 |
| 0.94 | 0.06 | 36 | 0.8836 | 11318 |
| 0.95 | 0.05 | 25 | 0.9025 | 11081 |
| 0.96 | 0.04 | 16 | 0.9216 | 10851 |
| 0.97 | 0.03 | 9 | 0.9409 | 10629 |
| 0.98 | 0.02 | 4 | 0.9604 | 10413 |
| 0.99 | 0.01 | 1 | 0.9801 | 10204 |
| 0.991 | 0.009 | 1 | 0.9821 | 10183 |
| 0.992 | 0.008 | 1 | 0.9841 | 10162 |
| 0.993 | 0.007 | 1 | 0.9860 | 10142 |
| 0.994 | 0.006 | 1 | 0.9880 | 10122 |
| 0.995 | 0.005 | 1 | 0.9900 | 10102 |
| 0.996 | 0.004 | 1 | 0.9920 | 10081 |
| 0.997 | 0.003 | 1 | 0.9940 | 10061 |
| 0.998 | 0.002 | 1 | 0.9960 | 10041 |
| 0.999 | 0.001 | 1 | 0.9980 | 10021 |
| 1 | 0 | 0 | 1 | 10000 |

Para validar la implementación de este protocolo se utilizó el mismo bucle que en el caso anterior. Se realizan 200 simulaciones, 50 para cada tipo de espía.

Las probabilidades de las bases se comportan de igual forma que en el caso con 320 bits de clave. También se almacenan los mismos tres parámetros.

En la figura 4.33 se muestra la comparación entre los cuatro tipos de espía utilizados.

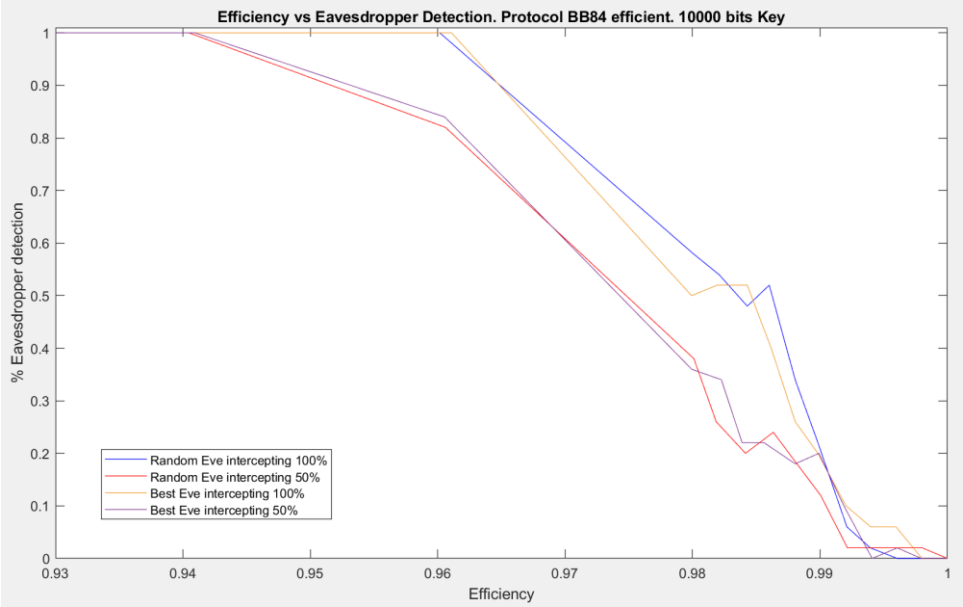


Fig. 4.33. Comparación de la eficiencia y detección entre cuatro tipos de espías.

Igual que en el caso anterior se observa como al utilizar el protocolo BB84 eficiente se logra superar la eficiencia de 50%, sin embargo, la mayor diferencia con el caso de menos bits es la eficiencia que se logra alcanzar con un 100% de probabilidad de detección de un espía.

Para cualquiera de los cuatro tipos de espía se puede obtener una eficiencia de hasta 94% con una tasa de 100% de detección, lo que concuerda con lo expuesto teóricamente respecto a que al aumentar la longitud de la clave se puede aumentar significativamente la eficiencia del protocolo.

Se puede apreciar también que cuando se intercepta el 100% de los bits la capacidad de detección es mayor. El uso de la base “best” también brinda una mayor posibilidad de detectar al espía.

Por último, se hace la comparación de la cantidad de bits que es necesario transmitir en cada caso en la figura 4.34.

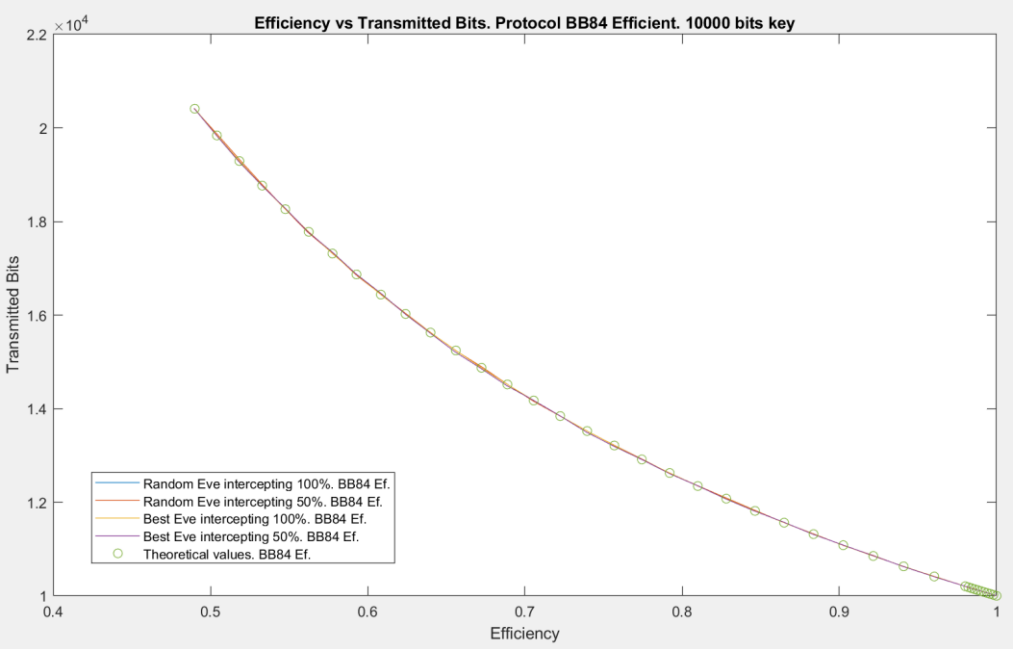


Fig. 4.34. Comparación del número de bits transmitidos con los valores teóricos de la tabla 8.

Como nuevamente estos valores no dependen del porcentaje de intervención del espía se obtienen curvas prácticamente iguales. Se grafica también la secuencia de valores calculados teóricamente y se corrobora que los resultados obtenidos a través de la simulación son correctos.

Con los resultados obtenidos hasta este momento se puede decir que la implementación de los protocolos es correcta ya que siguen las pautas descritas teóricamente sobre la eficiencia.

Tras evaluar los resultados obtenidos se puede concluir que el protocolo BB84 eficiente ofrece mejores prestaciones que el protocolo BB84 original.

A continuación, se busca la probabilidad de la base '+' que ofrece la mayor eficiencia y posibilidad de detección para cada caso.

En el caso de utilizar una clave de longitud 320 se obtienen los valores mostrados en la figura 4.35.

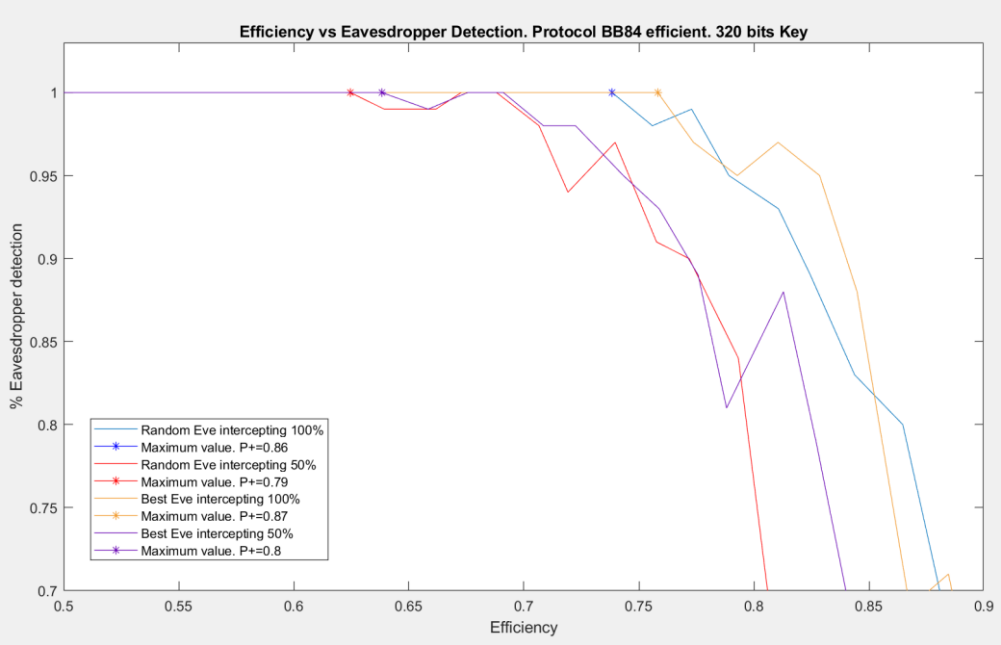


Fig. 4.35. Probabilidad de la base '+' de la eficiencia máxima para una clave de 320 bits.

En este caso se tomaría la probabilidad de la base '+' cercana al valor máximo obtenido cuando el espía intercepta el 50% de los bits, es decir, alrededor del 79% - 80%. La razón de esto es que si se toma una probabilidad mayor y el espía solo intercepta un 50% de los bits, la cual es una cantidad significativa de información, la probabilidad de que pase desapercibido aumenta.

En la gráfica de la figura 4.36 se muestran los valores máximos obtenidos, ahora para una clave de 10000 bits.

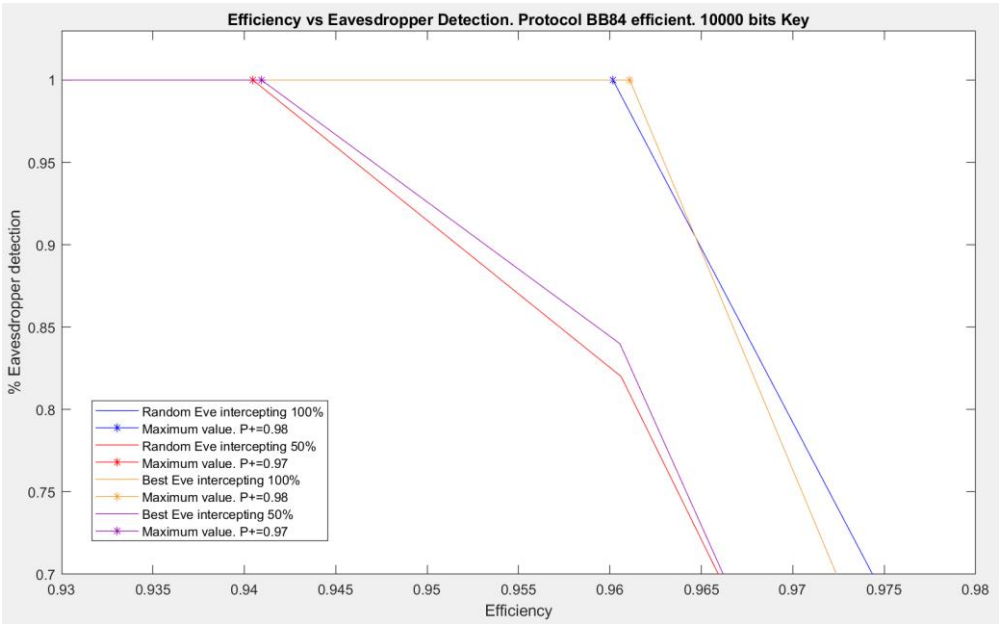


Fig. 4.36. Probabilidad de la base '+' de la eficiencia máxima para una clave de 10000 bits.

Comparando la eficiencia de ambos casos está claro que el protocolo BB84 eficiente con una clave de 10000 bits presenta mejores prestaciones por lo que se implementará dicho protocolo utilizando dicha longitud de clave. Se toma como probabilidad de la base "+" un 97% correspondiente con el espía que intercepta el 50% de los bits. Este se toma por la misma razón mencionada anteriormente, tomar una probabilidad mayor podría perjudicar la detección de un espía que intercepta el 50%.

### 4.4. Protocolo BB84 eficiente con $p^+ = 0.97$ bajo distorsión.

Una vez implementado el protocolo elegido con sus respectivos parámetros (probabilidad de la base mayoritaria igual al 97%), se presentan los resultados de simulaciones realizadas bajo los efectos del ruido térmico y la atenuación del canal, con el fin de determinar si bajo condiciones distintas de las ideales los parámetros elegidos siguen brindando las mejores prestaciones.

La eficiencia teórica con estos parámetros se calcula como:

$$Ef_T = p_+^2 = 0.97^2 = 0.9409$$

Se espera que todas las eficiencias prácticas se encuentren alrededor de este valor ya que estas solo dependen de la probabilidad de la base mayoritaria.

Inicialmente se variará únicamente la temperatura, despreciando la atenuación del canal, y se documentarán los resultados de simular un espía de base "random" que intercepte el 100%, 50% e incluso un caso particular de 10% de los bits de la clave. Se calculará, tras múltiples ejecuciones, la eficiencia media y la capacidad de detección en cada caso. Para casos donde no se detecte un espía, pero el ruido térmico sea muy alto se espera que el emulador indique que es imposible establecer una clave sin errores.

Por último, se variará tanto la temperatura como la distancia para cada porcentaje de bits espiados. Se utilizarán 3 temperaturas (-200$^\circ C$, -20$^\circ C$ y 0$^\circ C$) y dos distancias (1km y 10km). Se documentarán los mismos resultados que en el caso anterior.

Se utiliza un espía de bases "random" ya que este es el más difícil de detectar. Los resultados se muestran en la tabla 4.9.

TABLA 4.9. EFICIENCIA Y PROBABILIDAD DE DETECCIÓN EN FUNCIÓN DE LA TEMPERATURA Y EL PORCENTAJE DE BITS INTERCEPTADOS POR EL ESPÍA

| **% Espía** / **$^{\circ}C$** | 100% | | 50% | | 10% | |
|---|---|---|---|---|---|---|
| | **Eficiencia** | **Detección** | **Eficiencia** | **Detección** | **Eficiencia** | **Detección** |
| **-200$^{\circ}C$** | 94,139% | 100% | 94,136% | 100% | 94,013% | 70% |
| **-40$^{\circ}C$** | 94,151% | 100% | 94,069% | 100% | 94,073% | 80% |
| **-20$^{\circ}C$** | 94,097% | 100% | 94,082% | 100% | 94,042% | 60% |
| **0$^{\circ}C$** | 94,098% | 100% | 94,187% | 100% | 94,15% | 65% |
| **20$^{\circ}C$** | 94,263% | 100% | 94,059% | 95% | 94,158% | 50% |
| **30$^{\circ}C$** | 94,123% | 100% | 94,094% | 95% | 94,107% | 50% |

En la tabla 9 se puede apreciar que por debajo de los $0^{\circ}C$, un espía que intercepte el 100% o 50% de los bits tiene un 100% de probabilidad de ser detectado. Incluso para el caso especial de 10% de bits interceptados el porcentaje se mantiene por encima del 60%.

Al aumentar más la temperatura se puede ver que la detección del espía que intercepta solo el 50% disminuye.

En esta tabla 4.10 se puede observar que para temperaturas por debajo de $0^{\circ}C$ y una distancia de hasta 10km la capacidad de detección de un espía se mantiene en 100% para espías que intercepten el 100% y 50% de los bits. Si se interceptan solo el 10% la probabilidad de detección se mantiene por encima del 65%.

TABLA 4.10. EFICIENCIA Y PROBABILIDAD DE DETECCIÓN EN FUNCIÓN DE LA TEMPERATURA, DISTANCIA Y EL PORCENTAJE DE BITS INTERCEPTADOS POR EL ESPÍA

| **% Espía** / **$^{\circ}C$ / km** | **100%** | | **50%** | | **10%** | |
|---|---|---|---|---|---|---|
| | **Eficiencia** | **Detección** | **Eficiencia** | **Detección** | **Eficiencia** | **Detección** |
| **-200$^{\circ}C$ / 1km** | 94,115% | 100% | 94,132% | 100% | 94,119% | 80% |
| **-200$^{\circ}C$ / 10 km** | 94,041% | 100% | 94,238% | 100% | 94,043% | 70% |
| **-20$^{\circ}C$ / 1 km** | 94,196% | 100% | 94,104% | 100% | 94,137% | 75% |
| **-20$^{\circ}C$ / 10 km** | 94,097% | 100% | 94,051% | 100% | 94,096% | 65% |
| **0$^{\circ}C$ / 1 km** | 94,223% | 100% | 94,079% | 100% | 94,016% | 70% |
| **0$^{\circ}C$ / 10 km** | 94,074% | 100% | 94,124% | 100% | 94,134% | 75% |

En todos los casos la eficiencia se mantiene alrededor del 94% como era de esperar, ya que este parámetro depende solo de la probabilidad de la base mayoritaria.

# 5. CONCLUSIONES

En este capítulo se exponen los comentarios finales sobre el desarrollo de este trabajo, comentando los objetivos cumplidos, posibles mejoras y los trabajos que se podrían realizar en un futuro.

## 5.1. Objetivos

Como se comenta en el epígrafe 2.1 el objetivo principal de este proyecto era comparar los protocolos BB84 y BB84 eficiente con el fin de implementar, en un emulador de un sistema de criptografía cuántica, también desarrollado, aquel que ofrezca las mejores prestaciones en términos de eficiencia y capacidad de detección de un espía.

Para lograr este objetivo una serie de objetivos parciales se fueron alcanzando.

En los epígrafes 4.1.1 y 4.1.2 se muestran los resultados de los dos experimentos realizados con el kit de demostración. Ambos brindan resultados coherentes con lo expuesto en la explicación teórica.

En el epígrafe 4.2 se validó la implementación del emulador de comunicaciones cuánticas transmitiendo dos imágenes y comparando las probabilidades de error obtenidas con las teóricas descritas en la bibliografía. Se obtuvieron también los resultados esperados.

En el 4.3 se valida la implementación de ambos protocolos a través de compararlos con las descripciones teóricas y se concluye que el protocolo BB84 eficiente, utilizando una clave de 10000 bits de longitud, brinda las mejores prestaciones. Permite alcanzar una eficiencia de aproximadamente 94% para una probabilidad de detección del 100% si se utiliza una probabilidad de base mayoritaria igual a 97%.

Por último, en el epígrafe 4.4 se realizan simulaciones para comprobar la eficiencia y capacidad de detección del protocolo bajo los efectos de ruido térmico y la atenuación de la fibra óptica para distintos porcentajes de interceptación.

Si el espía intercepta todos los bits la capacidad de detección del protocolo es siempre del 100%. A medida que decrementa el número de bits también se le hace más difícil al emulador distinguir entre la presencia de un espía y los efectos del ruido.

Por debajo de los $0^{\circ}C$ la capacidad de detección se mantiene en el 100% para los espías de 100% y 50%. Y aun con un porcentaje de interceptación del 10% la probabilidad de detección se mantiene por encima del 60%.

La eficiencia de este protocolo puede seguir incrementándose si se aumenta la longitud de la clave, lo que lo hace muy superior al protocolo BB84 y sumamente útil para los establecimientos de claves.

A la vista de esto se puede concluir que se ha cumplido el objetivo principal, se ha desarrollado un emulador de un sistema de criptografía cuántica y se ha implementado, exitosamente, un protocolo de distribución de claves cuánticas que brinda unas prestaciones muy superiores al otro protocolo estudiado y que, además, permite mejorar estas incrementando la longitud de su clave.

### 5.2. Mejoras

Una de las posibles mejoras sería implementar el canal entre Eva y Bob de una forma más realista. Para esto sería necesario estudiar cómo se podrían calcular las respectivas constelaciones de operadores de densidad de cada uno, de forma que se pueda seguir emulando el protocolo sin causar aleatoriedad, pero, considerando también que el canal no es ideal y que Bob desconoce la distancia a la que se encuentra Eva.

Otra posible mejora sería permitir la transmisión de archivos de otros formatos, como por ejemplo vídeos.

### 5.3. Trabajos futuros

Uno de los proyectos que podría resultar interesante en el futuro es el de implementar en el emulador un protocolo basado en entrelazamiento.

En todas las aplicaciones actuales de la criptografía cuántica comentadas se utilizaba este protocolo para establecer las claves. La implementación de este se diferenciaría de los otros dos en que se necesita un tercer punto, Charlie, que hace el papel de fuente de

fotones. Este representa un tercero, en una comunicación entre dos puntos, que desconoce la clave final establecida. Esto significa que una misma fuente de fotones puede ser utilizada por múltiples comunicaciones sin poner en peligro la seguridad de la información.

# 6. METODOLOGÍA Y PRESUPUESTO

En este capítulo se detallan los pasos que se siguieron para lograr realizar este trabajo y el presupuesto, contabilizando los costes de personal y de materiales.

## 6.1. Metodología

Debido a la gran complejidad que supone el tema en sí, el primer paso consistió en obtener los conceptos básicos sobre la mecánica cuántica y cómo se puede hacer uso de sus propiedades para proteger la información. Esto se llevó a cabo a través de clases dictadas en julio de 2019 por mi tutor PhD. Luis Enrique García Muñoz, dentro de la beca de colaboración con Isdefe y de la consulta de libros, principalmente el libro de Susskind y Friedman (2014): *Quantum Mechanics. The Theoretical Mínimum. What You Need to Know to Start Doing Physics.*

Tras afianzar los conceptos básicos, se procedió a estudiar y documentar el interés actual por las tecnologías cuánticas. Se investigaron distintas aplicaciones como la criptografía, computación, software e incluso sensores y el interés de los países y empresas en ellas, al igual que presupuestos y programas de desarrollo de estas tecnologías alrededor del mundo.

También se realizaron experimentos utilizando el "Quantum Cryptography Demonstration Kit" de Thorlabs que permite simular el protocolo BB84 de distribución de claves cuánticas.

Con el fin de adquirir conocimientos más profundos sobre las comunicaciones cuánticas en sí se procedió a estudiar el libro de Gianfranco Cariolaro (2015): *Quantum Communications.* A partir de los conocimientos teóricos adquiridos con este libro se comenzó a desarrollar un emulador de un sistema de comunicaciones cuántico en septiembre de 2020.

Este trabajo recoge todo lo que se ha aprendido desde julio de 2019 a través de presentar un emulador de un sistema de comunicaciones cuántico capaz de emular un protocolo de

distribución de claves cuánticas al igual que brindar una comparación entre la transmisión de información a través de un sistema clásico y uno cuántico.

## 6.2. Presupuesto

### 6.2.1. Costes del personal

Para llevar a cabo este trabajo han sido necesarias dos personas: la autora Isabel Carnoto Amat y el tutor PhD. Luis Enrique García Muñoz. Los costes totales se calculan a continuación:

Sueldo de la autora por parte de la empresa Isdefe por contrato de $17^{h}/_{semana}$:

- Desde julio de 2019 hasta diciembre de 2019: $564{,}81^{€}/_{mes}$.
- Desde septiembre 2020 hasta febrero 2021: $608{,}83^{€}/_{mes}$.
- Desde marzo 2021 hasta agosto 2021: $622{,}12^{€}/_{mes}$

El coste resulta:

$$Coste = 6meses \times (564{,}81 + 608{,}83 + 622{,}12)\,^{€}/_{mes} = 10.774{,}56€$$

Coste del asesoramiento por parte del tutor durante el periodo de tiempo que tomo redactar este trabajo:

- Desde febrero 2021 hasta agosto 2021: 50 horas por $60^{€}/_{hora}$

El coste resulta:

$$Coste = 50horas \times 60\,^{€}/_{hora} = 3.000€$$

El coste total del personal resulta:

$$Coste_{Total} = 3.000€ + 10.774{,}56€ = 13.774{,}56€$$

### 6.2.2. Coste de los materiales

En las primeras etapas de la beca se utilizó el "Quantum Cryptography Demonstration Kit" de Thorlabs para realizar experimentos, el coste de este equipo es de 3.224,41€ de acuerdo con su página web [22].

Tanto este trabajo como el emulador fueron desarrollados utilizando un ordenador portátil HP Elite x2 con un procesador Intel Core m5-6Y57 a 1.10-1.51 GHz, de 8GB de memoria RAM.

Se ha utilizado el coeficiente de amortización de equipos electrónicos encontrado en la Agencia Tributaria para calcular el coste del uso del material con la siguiente ecuación [30]:

$$Coste = Precio \times Coeficiente \times \frac{Meses\ de\ uso}{12\ meses} = 1.679{,}00 \times 0.2 \times \frac{12}{12} = 335{,}8€$$

$$Coste_{Total} = 3.224{,}41€ + 335{,}8€ = 3.560{,}21€$$

### 6.2.3. Presupuesto Total

En la tabla 6.1 se muestra un desglose de los costes comentados anteriormente y el presupuesto total.

TABLA 6.1. DESGLOSE DE COSTES Y COSTE TOTAL

| Tipo de coste | Coste |
|---|---|
| Personal | 13.774,56€ |
| Materiales | 3.560,21€ |
| **Total** | 17.334,77€ |

# REFERENCIAS


[1] W. G. Johnson. "Quantum Supremacy and the Regulation of Quantum Technologies". The Regulatory Review. https://www.theregreview.org/2019/12/30/johnson-quantum-supremacy-regulation-quantum-technologies/ (acceso: agosto de 2021).

[2] J. Hsu. "How the United States Is Developing Post-Quantum Cryptography". https://spectrum.ieee.org/how-the-us-is-preparing-for-quantum-computings-threat-to-end-secrecy (acceso: agosto de 2021).

[3] Wikipedia. La enciclopedia Libre. "Criptografía postcuántica". https://es.wikipedia.org/wiki/Criptograf%C3%ADa_postcu%C3%A1ntica (acceso: agosto de 2021).

[4] NIST Computer Security Resource Center. "Post-Quantum Cryptography". https://csrc.nist.gov/Projects/Post-Quantum-Cryptography/Post-Quantum-Cryptography-Standardization (acceso: agosto de 2021).

[5] E. Gibney. "Quantum gold rush: the private funding pouring into quantum start-ups". *Nature*, vol. 574, pp. 22-24, octubre 2019. [En línea]. Disponible en: https://www.nature.com/articles/d41586-019-02935-4 Acceso: agosto de 2021.

[6] QURECA. "Overview on quantum initiatives worldwide – update mid 2021". https://www.qureca.com/overview-on-quantum-initiatives-worldwide/ (acceso: agosto de 2021).

[7] Palmer, J. "Quantum technology is beginning to come into its own". The Economist. https://www.economist.com/node/21717782/sites/all/modules/custom/ec_essay (acceso: agosto de 2021).

[8] European Comission. "Quantum Technologies Flagship". https://wayback.archive-it.org/12090/20210727065330/https://digital-strategy.ec.europa.eu/en/policies/quantum-technologies-flagship (acceso: agosto de 2021).

[9] M.F. Riedel, "The European quantum technologies flagship programme". *Quantum Science and Technology*, vol. 2, junio 2017. [En línea]. Disponible en: https://iopscience.iop.org/article/10.1088/2058-9565/aa6aca/pdf Acceso: agosto de 2021.

[10] L. Susskind y A. Friedman, *Quantum Mechanics*. Nueva York: Basic books, 2014.

[11] G. Cariolaro, *Quantum Communications.* Springer, 2015.

[12] Wikipedia. La enciclopedia Libre. "Ley de Moore". https://es.wikipedia.org/wiki/Ley_de_Moore (acceso: julio 2021).

[13] Wikipedia. La enciclopedia Libre. "Dependencia e independencia lineal". https://es.wikipedia.org/wiki/Dependencia_e_independencia_lineal (acceso: julio 2021).

[14] W. K. Wootters y W.H. Zurek, "A single quantum cannot be cloned". *Nature,* vol. 299, p. 802, 1982. [En línea]. Disponible en: https://www.nature.com/articles/299802a0 Acceso: julio 2021.

[15] Delta EU. "Atenuación en la fibra óptica". https://shopdelta.eu/atenuacion-de-la-fibra%20optica_l6_aid811.html (acceso: julio 2021).

[16] M. Kusuma. (2006). *Optical Fiber Communications* [Presentación de PowerPoint]. Disponible en: https://slideplayer.com/slide/6598468/

[17] Wikipedia. La enciclopedia Libre. "Radiación de cuerpo negro". https://es.wikipedia.org/wiki/Radiaci%C3%B3n_de_cuerpo_negro (acceso: julio 2021).

[18] Wikipedia. La enciclopedia Libre. "Ley de Planck" https://es.wikipedia.org/wiki/Ley_de_Planck (acceso: julio 2021).

[19] Wikipedia. La enciclopedia Libre. "Criptografía" https://es.wikipedia.org/wiki/Criptograf%C3%ADa (acceso: julio 2021).

[20] Wikipedia. La enciclopedia Libre. "RSA". https://es.wikipedia.org/wiki/RSA (acceso: julio 2021).

[21] Wikipedia. La enciclopedia Libre. "Algoritmo de Shor". https://es.wikipedia.org/wiki/Algoritmo_de_Shor (acceso: julio 2021).

[22] THORLABS Discovery. (2017). "Quantum Cryptography Demonstration Kit". https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=9869 (acceso: julio 2021).

[23] H.K. Lo, H. Chau y M. Ardehali. "Efficient Quantum Key Distribution Scheme and a Proof of Its Unconditional Security". *J Cryptology*, vol. 18, pp. 133–165, 2005. [En línea]. Disponible en: https://doi.org/10.1007/s00145-004-0142-y Acceso: julio 2021.

[24] M. Shukla y S. Patel. “Prominent Security of the Quantum Key Distribution Protocol”. *International Journal of Science and Research*, vol. 8, pp. 468-476, 2019. [En línea]. Disponible en: https://www.ijsr.net/archive/v8i7/ART20199396.pdf Acceso: julio 2021.

[25] Wikipedia. “DARPA Quantum Network”. Wikiwand. https://www.wikiwand.com/en/DARPA_Quantum_Network (acceso: agosto de 2021).

[26] C. Elliot, “The DARPA Quantum Network”. *arXiv*, 2004. [En línea]. Disponible en: https://arxiv.org/abs/quant-ph/0412029v1 Acceso: julio 2021.

[27] G. Popkin. “China’s quantum satellite achieves ‘spooky action’ at record distance”. Science. https://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achieves-spooky-action-record-distance (acceso: agosto de 2021).

[28] M. Pompili, *et al.* “Realization of a multimode quantum network of remote solid-state qubits”. *Science*, vol. 372, n. 6539, pp. 259-264, 2021. [En línea]. Disponible en: https://arxiv.org/abs/2102.04471 Acceso: agosto 2021.

[29] D. Castelvecchi. “Quantum Network Is Step Towards Ultrasecure Internet”. *Nature*, vol. 590, pp. 540-541, 2021. [En línea]. Disponible en: https://www.nature.com/articles/d41586-021-00420-5 Acceso: agosto 2021.

[30] Agencia Tributaria. “Tabla de coeficientes de amortización lineal”. https://www.agenciatributaria.es/AEAT.internet/Inicio/_Segmentos_/Empresas_y_profesionales/Empresas/Impuesto_sobre_Sociedades/Periodos_impositivos_a_partir_de_1_1_2015/Base_imponible/Amortizacion/Tabla_de_coeficientes_de_amortizacion_lineal_.shtml (acceso: agosto de 2021).

# ANEXOS

**Anexo A.**

## 1. Introduction

A lot of current ciphering mechanisms base their security in the assumed difficulty of solving complex mathematical operations. These algorithms can become vulnerable against the rapid growth of computer power or future technological breakthroughs.

Quantum cryptography offers ciphering mechanisms that are immune to eavesdropping attempts, thanks to the principles of quantum mechanics.

### 1.1. Objective

The main goal of this project is to compare two quantum key distribution protocols, BB84 and BB84 efficient, with the purpose of implementing, in an emulator of a quantum cryptography system also developed, the one that offers more benefits in terms of efficiency and eavesdropper detection probability. To accomplish this goal the project was divided in four partial goals.

1. Simulation of protocol BB84 on a Quantum Cryptography Demonstration Kit.
2. Developing an emulator of a quantum communications system considering the effects of thermal noise and attenuation.
3. Implementing and comparing the performance of both protocols.
4. Implementing the protocol chosen as optimal and observing its performance under non-ideal conditions.

### 1.2. First approach to quantum mechanics

The biggest difference between quantum and classical mechanics is that people find examples of classical mechanics in their day-to-day life and know how things behave just by intuition. Quantum mechanics studies things so small, cold, and isolated that they are completely out of the range of human senses.

One of the biggest dissimilarities is the relationship between a measurement and a state. A measurement cannot be made to determine the state of a quantum system because these

systems are not deterministic, the results of experiments are inherently random and any interaction capable of measuring some aspect of the system will also disturb another aspect of it.

### 1.3. Key concepts

- Randomness: applying the same measurement several times over a system will give different results, this occurs because the outcome of a measurement is completely random, and it must be treated using the theory of probability.
- Entanglement: a couple of entangled particles emitted from the same source stay correlated even when separated. If the state of one of them is measured, the state of the other one will change immediately.

### 1.4. From physics to information technologies

One thing that motivated the study of information in the context of quantum mechanics was Moore's Law. This law states that the number of transistors in a chip doubles every two years, without increasing the size of the chip. If no limit is set the components will keep reducing their size until reaching atomic dimensions and, at this scale the quantum effects are important. It was in 1994 when Peter Shor proved that a quantum computer would be able to break current security protocols because it could decompose a whole number into its prime factors faster than any classical computer could. This discovery confirmed the importance of researching quantum cryptography.

### 1.5. The environment of quantum mechanics

To each physical system a Hilbert $\boldsymbol{H}$ vector space in the field of complex numbers must be associated. In every instant of time the system is completely described by a quantum stated $|\psi\rangle$ (column vector called *ket*) given by a unitary vector of $\boldsymbol{H}$.

These states can be classified into two categories according to the knowledge of the observer. A state is called pure when the observer knows it with security, $s = |\psi\rangle \in H$, and it's called mixed state when the observer knows that the state belongs to a subset of $\boldsymbol{H}$ but only knows which one is it probabilistically, $p_i := P[s = |\psi_i\rangle]$. This means that the state $s$ is a random variable.

An alternative form to represent quantum states is through density operators, defined according to the following equation: $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$

Pure states can also be described as density operators according to the expression $\rho = |\psi\rangle\langle\psi|$. These operators must meet the following properties:

- Hermitian, $\rho = \rho^{\dagger}$
- Positive semidefinite, $\rho \geq 0$
- Unitary trace, $Tr[\rho] = 1$
- $Tr[\rho^2] \leq 1$ and if the system is in a pure state, $Tr[\rho^2] = 1$

These operators are important in communications because a state affected by thermal noise during transmission is no longer known by the observer and must be represented as a density operator.

### 1.6. Temporal evolution

The evolution of a quantum system is described by a unitary operator. As a consequence, not all temporal evolutions are possible. For example, according to the non-cloning theorem it is impossible to create a copy of an unknown random quantum state.

### 1.7. Quantum measurements

Quantum measurements are made using a set of operators $\{Q_i,\ i \in M\}$ that must meet the following conditions:

- Hermitian, $Q_i = {Q_i}^{\dagger}$
- Positive semidefinite, $Q_i \geq 0$
- Resolution to the identity, $\sum_i Q_i = I_H$

The probability that the result of a measurement *m* is equal to $i \in M$ can be calculated using the following expression: $p_m(i|\rho) = P[m = i|\rho] = Tr[\rho Q_i]$

To calculate these operators a suboptimization technique called "Square Root Measurement" or SRM is used. The goal is to find a measurement matrix $M = [\mu_0, \mu_1, \dots, \mu_{K-1}]$ that minimizes the error probability. To calculate the matrix *M* the reduced single value decomposition of the state matrix $\Gamma = [\beta_0, \beta_1, \dots, \beta_{K-1}]$ must be calculated. And from the matrix *M* the measurement operators are calculated as $Q_i = \mu_i \mu_i^*$.

### 1.8. Classical communications system

The transmitter will use a laser with a sine waveform at optical frequencies to transmit the information. To recover the signal transmitted the receiver will need to use a local

laser with amplitude $V_L$ and apply a photon counting process. Since the arrival of photons occurs in random instants of time it is convenient to model these events as Poisson processes. By dividing the optical energy received in one symbol period by the energy of a single photon, the number of photons per symbol received can be obtained.

The modulator calculates and transmits the complex envelopes of a sequence of complex symbols $\{C_n\}$. For example, in the first time interval the complex envelope is $V_T(t) = C_0 V_0$, where $V_0$ is the amplitude of the laser carrier. The demodulator takes the complex envelope received and creates two paths, path a and path b, adding $V_L$ and $iV_L$ to each one, respectively.

A photon counting process is applied to each path to obtain the average number of photons received as $\bar{n}_a$ and $\bar{n}_b$. The constellation of received values is obtained combining these two values into a complex number $z_0 = \bar{n}_a + i\bar{n}_b$. This constellation gives the decision regions since the symbols are equiprobable.

Under the presence of thermal noise, a complex envelope of the thermal noise must be added to each path. Because of this, the arrival of photons becomes a Laguerre process, and a Gaussian approximation can be used for the photon counting. This process will also result in a series of complex values $z_0 = \bar{n}_a + i\bar{n}_b$. These ones are affected by the thermal noise so the decision regions calculated previously will be used to find an estimate of the original symbol transmitted.

### 1.9. Quantum communications system

In this system the transmitter prepares a constellation of pure states and transmits them through a channel affected by thermal noise and attenuation. The states that reach the receiver are no longer pure because of the distortion of the channel so they are represented as density operators.

The density operators received are calculated using an approximation, since there is no way to work with infinite dimensions. The demodulator uses the SRM technique to calculate the measurement operators and recover a sequence of symbols.

### 1.10. Quantum key distribution (QKD)

The security of quantum cryptography relies on two principles: true randomness and eavesdropper detection.

Quantum physics makes true randomness possible, for example, a single photon is transmitted or reflected by a beam splitter in a completely random way.

Because of the no-cloning theorem an eavesdropper cannot copy the information that is being transmitted, and since passive monitorization is prohibited in quantum mechanics the eavesdropper will cause alterations that can be detected by the transmitter and receiver.

### 1.11. BB84 and BB84 efficient protocols

Protocol BB84 efficient is a variant of the BB84 so firstly, the common processes will be explained and then their main differences will be highlighted.

In QKD is common to call the transmitter, eavesdropper and receiver, Alice, Eve and Bob, respectively.

In the first place, two bases are defined, each one with two light polarizations, which gives four possible photon states. The "+" basis has 0˚ and 90˚, and "×" has -45˚ y 45˚. Each direction represents a bit, '0' as 0˚ or -45˚ and '1' as 90˚ or 45˚.

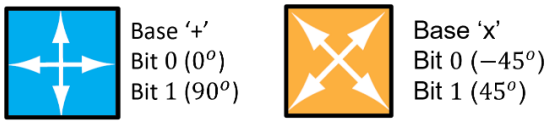


Fig. 1. "+" and "×" polarization bases.

In both protocols Alice chooses a random sequence of bits as the key, and Alice, Eve and Bob choose random sequences of bases too. Alice proceeds to transmit each photon in its corresponding polarization and Bob measures each one with his chosen basis. After the transmission, they exchange through a public channel the sequence of bases they used. They will discard every bit where the bases don't match, because Bob's measurement in these cases will be '0' or '1' randomly. The rest of the bits are saved as the key because, since they were measured with the same basis they were polarized with, the measurement will be correct 100% of the time. Finally, Alice and Bob exchange a sequence of test bits from the key to detect a possible eavesdropper by looking for non-matching bits.

When the eavesdropper is present it measures the photons transmitted by Alice using the chosen bases and then transmits them to Bob using the same bases.

The differences between the protocols are the bases probabilities and the testing bits.

In the BB84 protocol the bases "+" and "×" are uniformly distributed which results in an efficiency of 50%. The testing bits are taken from the key, decreasing the efficiency even more.

In the BB84 efficient protocol the "+" basis has a higher probability; the key bits are the ones where Alice and Bob have used the "+" basis and the testing bits where they have used the "×" basis. By increasing the length of the key and the "+" basis probability the efficiency can be incremented without losing the ability to detect and eavesdropper. In this protocol the efficiency is equal to the square of the "+" basis probability.

## 2. Development

### 2.1. Quantum cryptography demonstration kit

A quantum cryptography demonstration kit from Thorlabs was used to better understand how the BB84 protocol works. The setup of the kit can be seen in figure 2.

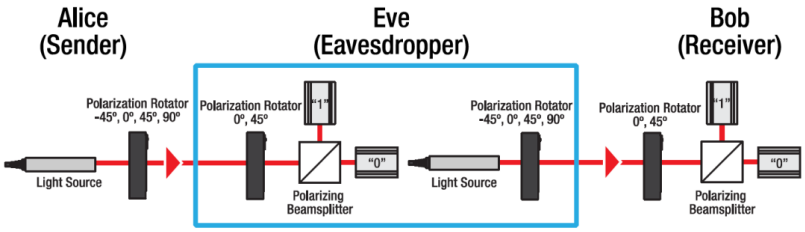


Fig. 2. Quantum cryptography demonstration kit setup.

It uses lasers as photon sources, rotation lenses to polarize the light, beam splitters to reflect or transmit the incident light, and sensors to indicate the bits received. Even though the security of the protocol relies on the use of single photons, this kit allows us to replicate the behavior using a pulse laser.

### 2.2. Emulator of a quantum cryptography system

An emulator was developed to implement and compare the QKD protocols. This program takes a file, introduced by a user, and converts it into a stream of bits. It uses a QKD protocol to stablish a secret key used to cipher the bit stream with an XOR operation. This ciphered message is transmitted through both classical and quantum systems and a comparison between the two is made based on the resemblance of the received file to the original one and the error rate.

The program will let the user know if an eavesdropper was detected, if there is no eavesdropper but the distortion in the channel is too high to stablish an errorless key or if no eavesdropper was detected, allowing the user to decide if they want to continue with the transmission or cancel it in the first two cases.

All the parameters can be introduced by the user in a graphic interface. Some of them are the file name, number of photons per symbol, temperature, length of the channel, fiber optic channel, presence of an eavesdropper and type of spy.

# 3. Results

## 3.1. Quantum cryptography demonstration kit experiments

Two experiments were made using the Thorlabs kit, the first one consisted of measuring light polarized in the "×" basis with the "+" basis. This resulted in a random sequence of 0s and 1s.

The second experiment was the establishment of a key and detection of an eavesdropper. An initial key of 20 bits was sent by Alice, after measuring and discarding a 13 bits key was obtained. These 13 bits were used for testing and the eavesdropper was discover because around 30% of the bits were wrong.

## 3.2. Emulator of a quantum communications system

To validate the correct functioning of the quantum transmission and reception a set of images were transmitted through the quantum and classical systems using a BPSK modulation and varying the number of photons per symbol and the number of thermal photons.

The resulting error probabilities were graphed and compared with the theoretical values shown in Gianfranco Cariolaro's Book: *Quantum communications.* The comparison is shown in figure 3.

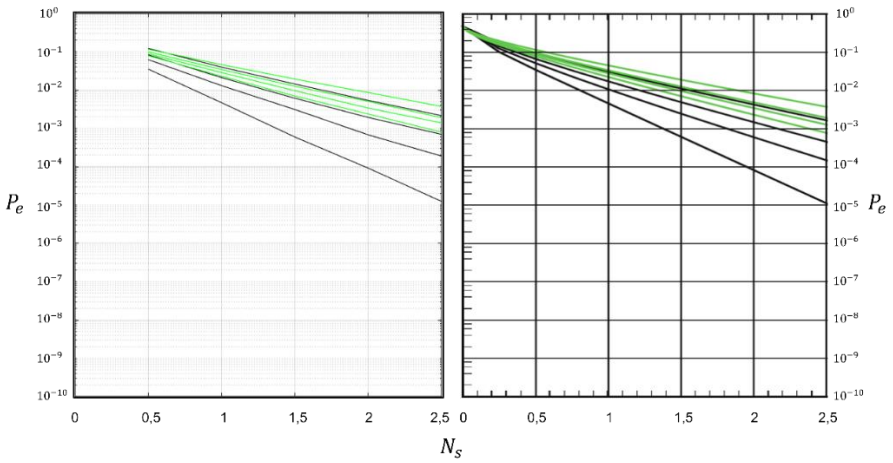


Fig. 3. Error probability comparison.

From this image we can corroborate that the emulator works as expected for the range of values tested.

### 3.3. Comparison between protocols BB84 and BB84 efficient

Three simulations were made in this section to validate the correct implementation of the protocols. Four types of eavesdroppers were used: the first one has random bases and intercepts 100% of the key, the second one has also random bases but intercepts 50% of the key, the third one has only "+" bases and intercepts 100% and the fourth one has only "+" bases but intercepts 50%. These simulations were made under ideal conditions.

#### 3.3.1. BB84 protocol with a key length of 320 bits

Simulations were made using a 320 bits key and the first two types of eavesdroppers. The amount of test bits was varied to see how this would affect the efficiency and detection probability. The results can be seen in figure 4.

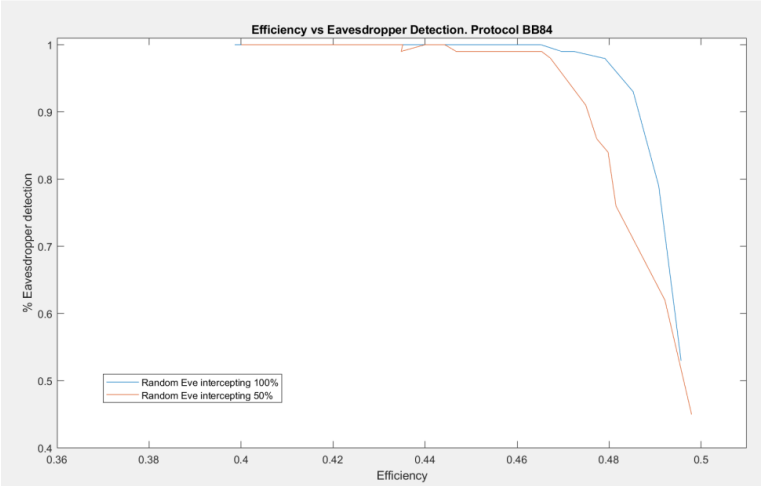


Fig. 4. Comparison of efficiency and detection between two types of eavesdroppers.

From this image we can see that the maximum efficiency is 50%, as expected. We can also observe that it is harder to detect an eavesdropper that intercepts less bits.

#### 3.3.2. BB84 efficient protocol with a key length of 320 bits

Simulations were made using the same 320 bits key as before, but this time the four types of eavesdroppers were compared. To vary the efficiency the probability of the "+" basis was varied. The results are shown in figure 5.

Comparing this figure to the previous one we can see that the efficiency has surpassed 50% without compromising the detection probability, making this protocol superior to the previous one in terms of these two parameters.

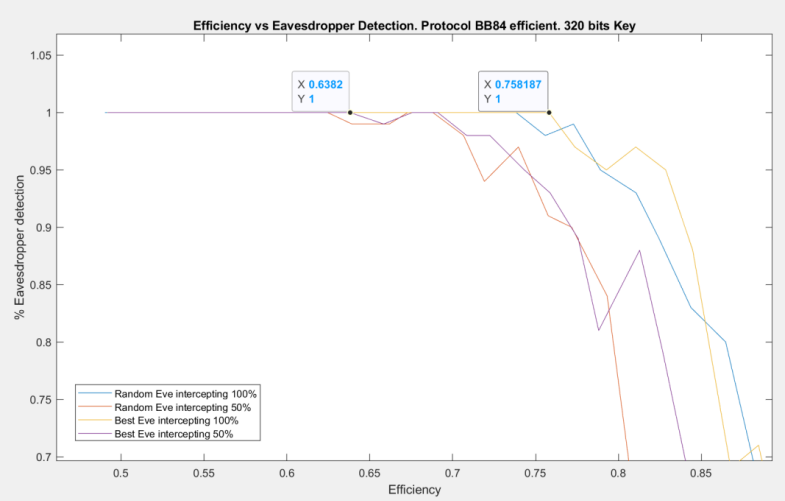


Fig. 5. Maximum efficiency values for 320 bits key for the BB84 efficient protocol.

### 3.3.3. BB84 efficient protocol with a key length of 10000 bits

These simulations are the same as the ones in the previous section but changing the length of the key to 10000 bits. The results can be seen in figure 6.

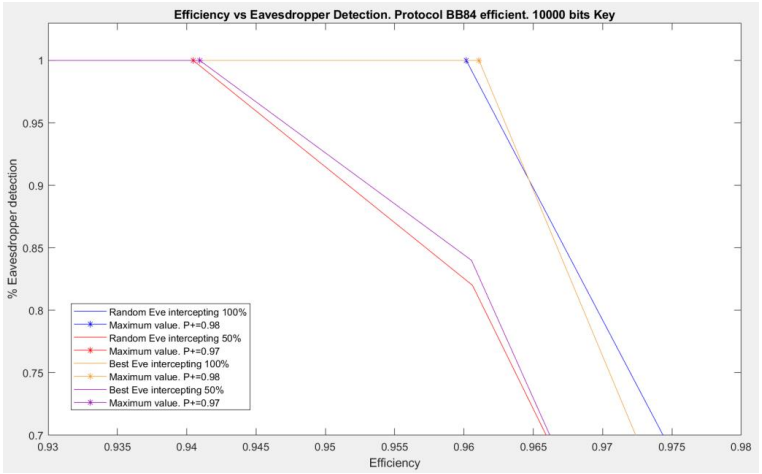


Fig. 6. Maximum efficiency values for 10000 bits key for the BB84 efficient protocol.

This figure shows a significant increase in the efficiency of the protocol when incrementing the length of the key, as stated in the protocol's definition.

After comparing these three results, the protocol chosen was the BB84 efficient, for a key length of 10000 bits and a "+" basis probability of 97%.

### 3.4. BB84 efficient protocol with $p^+ = 0.97$ under non ideal conditions

Several simulations were made under the effects of thermal noise and channel attenuation by varying the temperature and length of the channel.

The expected efficiency was calculated as follows: $Ef_T = p_+^2 = 0.97^2 = 0.9409$.

In the following table the results of the simulations can be seen.

| % Espía / $^{\circ}C$ / km | 100% | | 50% | | 10% | |
|---|---|---|---|---|---|---|
| | **Eficiencia** | **Detección** | **Eficiencia** | **Detección** | **Eficiencia** | **Detección** |
| **-200$^{\circ}C$ / 1km** | 94,115% | 100% | 94,132% | 100% | 94,119% | 80% |
| **-200$^{\circ}C$ / 10 km** | 94,041% | 100% | 94,238% | 100% | 94,043% | 70% |
| **-20$^{\circ}C$ / 1 km** | 94,196% | 100% | 94,104% | 100% | 94,137% | 75% |
| **-20$^{\circ}C$ / 10 km** | 94,097% | 100% | 94,051% | 100% | 94,096% | 65% |
| **0$^{\circ}C$ / 1 km** | 94,223% | 100% | 94,079% | 100% | 94,016% | 70% |
| **0$^{\circ}C$ / 10 km** | 94,074% | 100% | 94,124% | 100% | 94,134% | 75% |

In the table we observe that for temperatures below $0^{\circ}C$ and distances up to 10km the probability of detection is 100% for eavesdroppers intercepting 100% or 50% of the bits. An even for eavesdroppers intercepting only 10% the probability remains above 65%.

## 4. Conclusion

As seen in the results, all the partial goals of the project were accomplished.

In section 3.1 two experiments were performed on the demonstration kit. Both gave results consistent with what was stated in the theoretical explanation.

In section 3.2 the implementation of a quantum communications emulator was validated by comparing the simulation results with the theoretical values.

In section 3.3 the implementation of both protocols was validated and after comparing them it is concluded that the BB84 efficient protocol with a key of 10000 bits brings the best benefits. It allows to reach an efficiency of around 94% with a detection probability of 100% when $p^{+} = 0.97$.

Lastly, in section 3.4 we show that even under non ideal conditions the detection probability is still 100% for eavesdroppers intercepting 100% and 50% of the bits.

The efficiency of the BB84 efficient protocol can be increased even more by incrementing the length of the key which makes it superior to the BB84 protocol and incredibly useful for the establishment of secret keys.