uc3m | Universidad Carlos III de Madrid

Grado en ingeniería en tecnologías de telecomunicación

2020 - 2021

Trabajo Fin de Grado

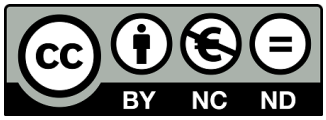
"Comunicaciones cuánticas"

Julio Nevado Delgado

Tutor

Luis Enrique García Muñoz

julio de 2021, Leganés



Esta obra se encuentra sujeta a la licencia Creative Commons **Reconocimiento - No Comercial - Sin Obra Derivada**

ABSTRACT

The present essay aims to revise the current situation of quantum technologies and approach them in a practical way.

We will first study the theory underlying quantum mechanics in order to fully understand the developments included in the Development chapter. Next, a glance at most useful applications of quantum mechanics will be taken. Those applications involve quantum computing and quantum networking, both aiming to be game changing in nowadays life. Also we will get to know which countries and organizations are investing harder in the research and development of quantum technologies.

Next we will get into the most practical part of the essay which will be split. First the set-up and tests made over a quantum key distribution system will be explained. Second, the development and operation of a quantum communications emulator which will allow us to compare the performance of a quantum communications system and a classical one under different conditions.

Finally, gathering both, the performance of the emulator and the QKD set-up along with current state of quantum technologies I will lend my perspective on this technologies. I will analyse the achievements that could be made as well as the issues we will have to overcome.

Palabras clave: quantum, computing, network, communications, key, QKD

DEDICATORIA

A mi pareja, familia y amigos por el apoyo siempre incondicional.

A mi tutor, Luis Enrique García, por su tiempo y dedicación.

A ISDEFE por el apoyo económico y la confianza depositada en mí.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1. MOTIVACIÓN

La empresa ISDEFE (Ingeniería de Sistemas para la DEFensa de España), interesada en nuevas tecnologías, nos contactó en mayo de 2019 para un proyecto de consultoría acerca del estado de la criptografía cuántica en aquel momento. Parte de este proyecto inicial, que comenzó en julio de 2019, fue el montaje de un *set-up* de demostración de distribución cuántica de claves (QKD).

Debido a mi interés por seguir formándome en este ámbito y a la satisfacción por parte de ISDEFE con el trabajo realizado, el contrato se prolongó hasta el presente, pero abordando otras áreas de las tecnologías cuánticas.

En primer lugar, de la mano de mi tutor PhD. Luis Enrique García Muñoz, obtuve los conocimientos básicos en relación a comunicaciones cuánticas como modulaciones cuánticas, estados coherentes, etc. Todos estos conceptos será cubiertos en el capítulo de introducción.

En segundo lugar, tras haber adquirido todos los conocimientos necesarios, procedimos a desarrollar un emulador de un sistema cuántico de comunicaciones que, por medio de las matemáticas, nos permite comprobar como serían las prestaciones de un sistema cuántico en diversas condiciones de atenuación y temperatura mediante la transmisión de imágenes además de poder comparar estas prestaciones con las proporcionadas por un sistema clásico de comunicaciones. Este emulador, como se detallará mas adelante, también aceptará la entrada de audios para emular la transmisión.

El presente informe refleja el trabajo realizado desde julio de 2019 hasta la fecha, cubriendo tanto las partes teóricas en materia de criptografía y comunicaciones como las partes más prácticas.

2. INTRODUCCIÓN

En el capítulo de introducción se conocerá la base teórica necesaria para poder comprender de la mejor manera posible todos aquellos conceptos utilizados en el capítulo de desarrollo. Además, se analizará el estado del arte de las tecnologías cuánticas, poniendo el foco sobre las comunicaciones pero también sobre otros temas muy interesantes como la criptogafía o la computación. Finalmente, se llevará a estudio la situación de las tecnologías cuánticas a nivel mundial cubriendo qué empresas las están utilizando en la práctica, si es que las hay, y qué países y organizaciones están invirtiendo más dinero en su desarrollo.

2.1. Base matemática

2.1.1. Espacios vectoriales, espacios de Hilbert y bases

Un espacio vectorial V es un conjunto de elementos (vectores) sobre el cual se definen dos operaciones, como vemos en [1]:

- Suma.
- Producto por un escalar.

Estas operaciones, además, deben cumplir con una serie de propiedades, de nuevo en [1]:

1. El espacio vectorial es cerrado respecto a la suma. Es decir, la suma de dos vectores $\vec{x}$ e $\vec{y}$ tambien pertenece al espacio vectorial V.
2. Conmutativa de la suma: $\vec{x} + \vec{y} = \vec{y} + \vec{x}$.
3. Conmutativa del producto: $a\vec{x} = \vec{x}a$ donde a es un escalar.
4. Asociativa de la suma: $(\vec{x} + \vec{y}) + \vec{z} = \vec{x} + (\vec{y} + \vec{z})$.
5. Asociativa del producto: $a(\vec{x} + \vec{y}) = a\vec{x} + a\vec{y}$.

6. Existencia del elemento nulo, tal que al sumarlo a un vector el resultado sea el mismo vector.

7. Existencia del elemento opuesto, de tal manera que al sumar un vector con su opuesto el resultado es el elemento nulo del conjunto.

8. El producto por un escalar es cerrado, es decir, el vector resultante de multiplicar un vector por un escalar también pertenece al espacio vectorial.

Por su parte, una base B del espacio vectorial V es un subconjunto de elementos de V que son linealmente independientes y cuya combinación lineal puede generar cualquier vector de V. Además, el número de elementos de la base B (su cardinalidad) debe ser igual a la dimensión de V.

Si, por ejemplo, V es un espacio en $2D$, la base B tendrá dos elementos $\vec{x}$ e $\vec{y}$ ($B = \{\vec{x}, \vec{y}\}$) cuya combinación lineal puede generar un vector cualquiera $\vec{z}$ de V ($\vec{z} = c_1\vec{x} + c_2\vec{y}$, con c_1 y c_2 escalares).

Finalmente, un espacio de Hilbert H es un espacio vectorial complejo que cumple según [2]:

- Se define el producto interior, como el producto matricial de un bra y un ket.
- Es completo.

2.1.2. Matrices

En este trabajo, los autovectores y autovalores van a ser elementos tremendamente importantes. Por ello, es muy conveniente definirlos:

Diremos que un vector $\vec{x}$ es un autovector de una matriz M cuando el resultado del producto $M\vec{x}$ es un vector $\vec{y}$ que no es más que el vector $\vec{x}$ multiplicado por un escalar λ, al que llamamos autovalor asociado al autovector $\vec{x}$. Además, puede haber varios autovectores asociados al mismo autovalor.

Para calcular los autovalores de un operador M planteamos la siguiente ecuación, tal y como se hace en [2]:

$$det(M - \lambda I_H) = 0$$

Esta ecuación podrá representarse como:

$$(\lambda - \lambda_0)^{p_0}(\lambda - \lambda_1)^{p_1} \cdots (\lambda - \lambda_i)^{p_i} = 0$$

donde los λ_i son los autovalores **distintos** del operador y p_i su multiplicidad.

Las matrices que nos van a interesar pueden ser de tres tipos, de acuerdo con [2]:

- Hermíticas: Decimos que una matriz M es hermítica cuando coincide con su hermítica. Es decir, si $M = M^*$, donde * indica la matriz transpuesta y conjugada elemento a elemento. Estas matrices, tienen la propiedad de que los autovectores asociados a autovalores distintos son ortogonales, es decir, su producto interior es 0. Además, todos sus autovalores son reales.

- Unitarias: Decimos que una matriz M es unitaria si M por su hermítica M^* es la matriz identidad. Es decir, si $MM^* = I$. Tienen la propiedad de que todos sus autovalores tienen módulo 1.

- Normales: Son matrices que cumplen que $MM^* = M^*M$. Evidentemente, tanto matrices hermíticas como unitarias son normales.

Otro de los conceptos utilizados acerca de matrices es su rango. El rango de una matriz nos permite averiguar las filas o columnas que son linealmente independientes.

2.1.3. Traza de un operador

El operador traza va a tener una importancia enorme en el presente trabajo ya que será la clave para modelar las medidas cuánticas de manera matemática.

Como veremos, un operador de un espacio de Hilbert H se define respecto a los elementos de una base B. Por ello, un mismo operador tendrá distintas representaciones matriciales dependiendo de la base elegida. Para calcular la traza de un operador necesitamos conocer la base respecto a la que se define como podemos ver en la siguiente fórmula, obtenida de [2], con M un operador cualquiera:

$$Tr[M] = \sum_i \langle b_i | M | b_i \rangle$$

donde $|b_i\rangle$ y $\langle b_i|$ son los elementos de la base como vector fila y columna, respectivamente. La traza tiene las siguientes propiedades, analizadas en la misma publicación:

- La traza del operador M es independiente de la base B respecto a la que se define. Evidentemente, si definimos M respecto a una base distinta, su expresión matricial cambiaría al igual que cambiarían los vectores $|b_i\rangle$ de la fórmula anterior, por lo que la traza del operador sería constante.

- La traza es lineal: $Tr[mM + nN] = mTr[M] + nTr[N]$, con m y n escalares.

- Podemos calcular la traza a partir de los autovalores del operador como: $Tr[M] = \sum_i p_i \lambda_i$. Donde λ_i son los autovalores **distintos** del operador y p_i su multiplicidad.

2.1.4. "Singular Value Descomposition" (SVD)

La SVD de una matriz será algo crucial en el cálculo de probabilidades teóricas. Tal y como tenemos disponible en [2], una matriz puede descomponerse en el producto de tres matrices:

$$M = U\Sigma V^* = \sum_i \sigma_i |u_i\rangle \langle v_i|$$

donde U y V son matrices unitarias y la matriz Σ es diagonal y contiene los valores singulares de M, σ_i, que son no negativos ($\sigma_i \geq 0$).

Si retiramos las filas y columnas de Σ_i para los que $\sigma_i = 0$ y retiramos los ket $|u_i\rangle$ (columnas) de U y los bras $\langle v_i|$ (filas) de V correspondientes a esos valores singulares, tendremos lo que conocemos como SVD reducida, y la cual se representa con los subíndices r:

$$M = U_r \Sigma_r V_r^*$$

Lo podemos ver también de manera gráfica a continuación, en la figura 2.1.

$$A = U\Sigma V = \begin{bmatrix} a & \cdots & b \\ \vdots & \ddots & \vdots \\ c & \cdots & d \end{bmatrix} \begin{bmatrix} e & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 0 \end{bmatrix} \begin{bmatrix} f & \cdots & g \\ \vdots & \ddots & \vdots \\ h & \cdots & i \end{bmatrix}$$

$$A = U_r \Sigma_r V_r = \begin{bmatrix} a & \cdots \\ \vdots & \ddots \\ c & \cdots \end{bmatrix} \begin{bmatrix} e & \cdots \\ \vdots & \ddots \end{bmatrix} \begin{bmatrix} f & \cdots & g \\ \vdots & \ddots & \vdots \end{bmatrix}$$

Fig. 2.1. Descomposición en valores singulares reducida

La SVD es muy útil para, entre otras cosas, calcular raíces de una matriz. Por ejemplo,

si tenemos la matriz A cuya SVD es:

$$U\Sigma V^*$$

podríamos obtener, siguiendo la teoría desarrollada en [2], $A^{-\frac{1}{2}}$ como:

$$U\Sigma^{-\frac{1}{2}}V^*$$

donde $\Sigma^{-\frac{1}{2}}$ indica la raíz de los valores singulares de A contenidos en la matriz Σ.

2.1.5. Procesos de Poisson

Los procesos de Poisson nos permiten caracterizar estadísticamente la ocurrencia de una serie de eventos. Es decir, nos permiten, por ejemplo, caracterizar la probabilidad de que lleguen 3 coches a un parking o de que lleguen 5 fotones a un fotodetector.

Un proceso de Poisson viene caracterizado por la intensidad del proceso, $\lambda(t)$ que se define como:

$$\lambda(t) = \lim_{h\to 0^+} \frac{P[n(s, s+h] = 1]}{h}$$

que nos indica la probabilidad de que un evento ocurra en un instante de tiempo infinitesimal, de acuerdo a lo expuesto en [3].

Un proceso de Poisson tiene una media de llegadas en un intervalo $n(s, t]$ caracterizada por:

$$\Lambda = E[n(s, t]] = \int_s^t \lambda(s)ds$$

Un proceso de Poisson que nos será muy útil de aquí en adelante es el de la potencia instantánea, caracterizado como:

$$p(t) = \sum (hv)\delta(t)$$

La intensidad de este proceso de Poisson que caracteriza la potencia instantánea se relaciona con la potencia media como:

$$\lambda(t) = \frac{1}{hv}P(t)$$

Por lo tanto, a partir de la potencia promedio $P(t)$ del proceso, podemos calcular su media:

$$\bar{n} = E[n(0, T]|\lambda(t)] = \int_0^T \lambda(t)dt = \frac{1}{hv}\int_0^T P(t)dt$$

2.1.6. Envolvente compleja

Si tenemos una señal paso banda $v(t)$ que se encuentra alrededor de la frecuencia v se define su envolvente compleja, al igual que expone Cariolaro [3], como $c_v(t)$ tal que:

$$v(t) = Real\{c_v(t)e^{j2\pi vt}\}$$

donde $c_v(t)$ equivale a:

$$c_v(t) = 2v_+(t)e^{-j2\pi vt}$$

siendo $v_+(t)$ uno de los 2 modos obtenidos al calcular la transformada de Fourier de una señal paso banda (estas señales estarán alrededor de la frecuencia v y de la frecuencia $-v$).

Siguiendo el mismo ejemplo utilizado por Cariolaro [3] la señal:

$$v(t) = A_0 cos(2\pi vt + \phi)$$

puede descomponerse como:

$$\frac{A_0}{2}e^{j2\pi vt+\phi} + \frac{A_0}{2}e^{-j2\pi vt-\phi}$$

donde $v_+(t)$ sería:

$$v_+(t) = \frac{A_0}{2}e^{j2\pi vt+\phi}$$

y por tanto la envolvente compleja sería:

$$c_v(t) = 2v_+(t)e^{-j2\pi vt} = 2\frac{A_0}{2}e^{j2\pi vt+\phi}e^{-j2\pi vt} = A_0e^{\phi}$$

A partir de ella podemos recuperar la señal original $v(t)$:

$$v(t) = Real\{A_0e^{\phi}e^{j2\pi vt}\} = Real\{A_0e^{j2\pi vt+\phi}\} = A_0cos(2\pi vt + \phi)$$

La envolvente compleja es muy útil puesto que está relacionada con la potencia promedio de la señal como:

$$P_0 = |c_v(t)|^2 = |A_0e^{\phi}|^2 = A_0^2$$

2.2. Base teórica

2.2.1. Estados y medidas cuánticas

El primer paso para poder comprender la mecánica cuántica es dejar a un lado lo que conocemos acerca de mecánica clásica. Las “reglas” que rigen los estados y sistemas

cuánticos son tan distintas que tratar de tender puentes entre la mecánica clásica y la cuántica es, en la mayoría de casos, inútil. En otras palabras, rara vez tratar de buscar un explicación a por qué algo ocurre de una determinada manera en este "mundo" cuántico nos permite llegar a buen puerto.

La base de esta gran diferencia son los conceptos de estado y medida, cuya desemejanza es abismal. Mientras que en un sistema clásico realizar una medida implica unívocamente conocer su estado, en un sistema cuántico ésto **no** es así. La manera más común de explicar ésto es el *spin* de un electrón tal y como hacen Susskind y Friedman [4], en quienes nos vamos a inspirar para explicar esta diferencia entre la mecánica clásica y la cuántica.

Si imaginamos el *spin* como una flecha que tiene el electrón en su superficie, podemos intentar llevar a cabo una medida que nos diga el valor de ese *spin* en una dirección determinada. Preparamos ese *spin* sobre el eje z como se ve en la figura 2.2.

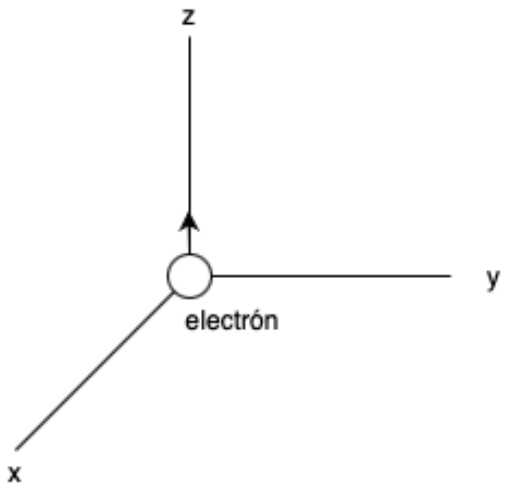


Fig. 2.2. Electrón en un sistema de coordenadas

Para la medida, se supone un aparato que nos da el valor de la componente del *spin* en la dirección marcada por el aparato. Si ponemos el aparato en la dirección y sentido del eje **z** positivo y medimos, obtendremos siempre 1 (el *spin* está sobre la dirección que medimos y en el mismo sentido de la medida). Si damos la vuelta al aparato y medimos en la dirección $-z$, obtendremos un -1, es decir, la dirección del aparato, pero en sentido opuesto. Por ahora los resultados son los esperados.

El problema ocurre cuando en lugar de medir sobre la dirección del eje z, lo hacemos

sobre cualquier otra dirección, como por ejemplo la del eje y. Al estar el *spin* preparado sobre el eje z, el resultado obtenido de la medida debería ser 0, pues la componente del *spin* en esa dirección es nula. No obstante, al medir obtendremos 1 o -1 con la misma probabilidad. Si volvemos a preparar el *spin* sobre z y medimos sobre y, volveremos a obtener 1 o -1 con la misma probabilidad. Si repetimos esta secuencia de primero preparar el *spin* y luego medir sobre y obtendremos una secuencia con tantos 1 como -1. Sin embargo, si preparamos el *spin* en la direccion del eje z positivo y realizamos dos medidas seguidas sobre el eje y positivo, obtendremos dos valores iguales, $+1$ ó -1, pero el mismo. Es decir, el estado que define el *spin* es un estado cuya medida sobre el eje y puede arrojar $+1$ ó -1 indistintamente, pero tras una medida, ese estado se transforma en otro que, al medir sobre el eje y da siempre el mismo valor. En otras palabras, **el hecho de medir un estado cuántico implica de manera general modificarlo**, como afirmaron Susskind y Friedman en [4].

Por esto es por lo que decimos que una medida cuántica es de por sí aleatoria. Además, como ya se ha dicho, no tiene sentido alguno buscar una explicación lógica a por qué ocurre esto. Por ello, se tratará de comprender de manera estadística qué ocurre, con el objetivo de predecir el comportamiento de estos sistemas.

Estados cuánticos

La notación que vamos a utilizar para representar un estado cuántico es de la notación de *Dirac*, consistente en bras ($\langle a|$, representados como vectores fila) y kets ($|a\rangle$, representados como vectores columna). La relación entre bras y kets es muy sencilla. Para obtener el ket de un bra solamente hay que transponer el bra y hacer el conjugado elemento a elemento. Para obtener el bra de un ket, la operación es la misma.

$$|a\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}, \ \langle a| = (a_1^*, a_2^*)$$

No obstante, para que $|a\rangle$ pueda representar el estado de un sistema cuántico deben darse dos condiciones, tal y como se afirma en [5].

En primer lugar, $|a\rangle$ debe pertenecer al espacio de estados del sistema cuántico, que será un espacio de Hilbert H.

La segunda condición que debe cumplir un ket (o un bra) para poder representar el

estado de un sistema cuántico es que ese ket debe estar normalizado, es decir, que su norma al cuadrado sea 1. Para el ejemplo anterior, esta condición se cumpliría si:

$$|a_1|^2 + |a_2|^2 = 1$$

Además, vamos a representar estos kets (o bras) respecto a una base B del espacio de Hilbert H. Por ejemplo, para el caso inicial del *spin*, si tenemos la base $B = |1\rangle, |-1\rangle$ un ket cualquiera $|x\rangle$ podría expresarse como

$$|x\rangle = \sqrt{\frac{3}{4}}|1\rangle + \frac{1}{2}|-1\rangle$$

donde se cumple la condición de normalización:

$$\left|\sqrt{\frac{3}{4}}\right|^2 + \left|\frac{1}{2}\right|^2 = \frac{3}{4} + \frac{1}{4} = 1$$

y donde cada uno de los coeficientes (en módulo) al cuadrado nos da la probabilidad de, al medir, obtener un valor u otro. Es decir, para el coeficiente del estado $|1\rangle$, tendremos:

$$\left|\sqrt{\frac{3}{4}}\right|^2 = \frac{3}{4} = 0{,}75$$

En otras palabras, para el estado anterior, la probabilidad de al medir obtener 1 es 0,75 y la de obtener -1 es 0,25.

Además, siguiendo la teoría de [5], los estados cuánticos pueden ser puros o mixtos. Un sistema se encuentra en un estado puro cuando sabemos con total seguridad el estado en el que se encuentra. En este caso, el estado del sistema podría representarse por un único ket: $s = |\Psi\rangle$.

Por su parte, un estado mixto o ambiguo es aquel donde no tenemos un único estado, sino que tenemos un serie de posibles estados en los que podría encontrarse nuestro sistema y las probabilidades de cada uno de esos estados. En este caso el estado de un sistema, s, estará representado por:

- $S = \{|\Psi_0\rangle, |\Psi_1\rangle, .., |\Psi_N\rangle\}$, el conjunto de N posibles estados en los que se puede encontrar el sistema.
- $P = \{p_0, p_1, ..., p_N\}$, las probabilidades de encontrarse en cada uno de esos N posibles estados.

Una forma muy útil de representar los estados mixtos es utilizar operadores densidad, que podemos calcular como:

$$\rho = \sum_{i=0}^{N} p_i \left|\Psi_i\right\rangle \left\langle\Psi_i\right|$$

Es evidente que un estado puro también podría representarse como operador densidad:

$$\rho = \left|\Psi\right\rangle \left\langle\Psi\right|$$

donde hemos eliminado el sumatorio, ya que sólo hay un estado posible que, evidentemente tiene probabilidad 1, tendiendo cualquier otro estado probabilidad 0.

No debemos confundir el hecho de tener un estado puro con tener una medida sin aleatoriedad. Es decir, podemos tener un estado puro y para diferentes medidas sobre ese mismo estado puro obtener distintos resultados. Para el ejemplo anterior del estado:

$$\left|x\right\rangle = \sqrt{\frac{3}{4}} \left|1\right\rangle + \frac{1}{2} \left|-1\right\rangle$$

sabemos con total certeza el estado en que nos encontramos, no obstante, el resultado de la medida es aleatorio como hemos podido comprobar.

En cualquier caso, si calculamos la traza de un operador densidad (ya sea de un estado puro o mixto), el resultado es siempre 1, lo que nos permitirá determinar si las representaciones matriciales utilizadas en el emulador del capítulo de Desarrollo constituyen una buena aproximación de un operador de densidad.

Operadores de medida

Como hemos visto al comienzo de la sección 2.2.1, en un sistema cuántico los conceptos de estado y medida son bien diferentes a sus equivalentes clásicos. El hecho de que la medida sobre un mismo estado cuántico pueda arrojar cada vez distintos resultados no deja de ser inquietante, especialmente si vamos a aplicar estas medidas al ámbito de las comunicaciones donde serán la base de la decisión.

Para poder interpretar estas medidas, la mejor opción es recurrir a la estadística, ya que nos ayudará a evitar cometer el error de interpretar de manera clásica estos conceptos. Por ello, en esta sección hablaremos de los operadores de medida.

Un operador sobre un espacio de Hilbert H es una aplicación que, dado un vector $\left|x\right\rangle$ de H devuelve otro vector $\left|y\right\rangle$ que también pertenece a H. Los operadores se representan

en forma matricial. Esta representación matricial debe hacerse respecto a una base B del espacio de Hilbert H. Por ende, un mismo operador de H podría tener diferentes representaciones matriciales como se dijo en el apartado 2.1.3.

Los operadores de medida más genéricos son los sistemas POVM (*Positive Operator-Valued Measurement*), que representamos como $\{Q_i,\ i \epsilon M\}$, donde M es el alfabeto de los posibles resultados de las medidas. Estos sistemas de operadores deben cumplir, siempre según [5], las siguientes condiciones:

- Ser semidefinidos positivos. Es decir, los autovalores de cada operador Q_i deben ser no negativos.
- Dar una resolución completa de la identidad del espacio de Hilbert H. En otras palabras, que $\sum_i Q_i$ sea igual al operador identidad sobre el espacio H, I_H. Es decir, que si hacemos la suma de todos los operadores del sistema POVM el resultado es un nuevo operador que, al aplicarse a un ket $|x\rangle$ cualquiera, devuelve ese mismo ket $|x\rangle$
- Ser operadores hermíticos, es decir, cada operador debe ser igual a su hermítitco: $Q_i = Q_i^*$, donde recordemos Q_i^* es la matriz Q_i transpuesta y conjugada elemento a elemento.

Estos operadores Q_i nos van a ser extremadamente útiles, pues, a partir del estado en el que se encuentra nuestro sistema (ya sea puro o mixto) vamos a poder caracterizar estadísticamente los posibles resultados obtenidos de las medidas.

Si partimos de un estado cuántico representado por el operador densidad ρ, la probabilidad de obtener de la medida m el resultado j se define muy fácilmente mediante el operador traza, según [5], como:

$$p[m = j|\rho] = Tr[\rho Q_j]$$

Podemos ver como esta ecuación es válida tanto para estados mixtos como para estados puros ya que, como sabemos, ambos pueden representarse mediante operadores densidad.

2.2.2. Distribución cuántica de claves (QKD)

Cuando queremos tener comunicaciones seguras, necesitamos una clave con la que cifrar los datos. No obstante antes de poder cifrar los datos, es necesario primero generar la clave y segundo hacerla llegar a cada uno de los extremos de la comunicación.

En cuanto a la distribución de claves, hay numerosos protocolos muy extendidos que funcionan muy bien como es el caso de los protocolos *Diffie-Hellman*, RSA o ElGamal. No obstante, estos protocolos suelen basar su seguridad en la resolución de un problema matemático muy complejo, como puede ser la factorización de un gran número o el cálculo de un logaritmo discreto. Este nivel de seguridad suele ser más que suficiente para las capacidades computacionales de los equipos de hoy en día. No obstante, el avance tecnológico en general, y los ordenadores cuánticos en particular, podrían llegar a tener la capacidad computacional suficiente para romper estos algoritmos, dejándolos inservibles.

Una solución a esta amenaza son los algoritmos de criptografía postcuántica [6] que son algoritmos clásicos pero que son capaces de resistir ataques que pudiesen venir de ordenadores cuánticos futuros. Otra solución, que es la que trataremos en este apartado, es la distribución cuántica de claves o QKD (*Quantum Key Distribution*) por sus siglas en inglés.

La distribución cuántica de claves aprovecha los principios de la mecánica cuántica para, simultáneamente, crear la clave y hacerla llegar de manera segura a ambos extremos de la comunicación. Hay numerosos protocolos de distribución cuántica de claves. Nosotros nos centraremos en el protocolo BB84, que es uno de los más simples, y concretaremos en su variante *efficient*.

Protocolo BB84

El protocolo BB84 hace uso del teorema de no-clonación. Según [7], este teorema nos dice que, de manera general, no podemos clonar un estado cuántico debido a que el simple hecho de medirlo lo va ha modificar, de tal manera que no podremos replicarlo.

Como se explica en [8], en este protocolo se usarán dos bases, la base + y la base $\times$. En cada una de estas bases, podremos codificar los estados $|0\rangle$ y $|1\rangle$, que representaremos como $|0^+\rangle$ y $|1^+\rangle$ para la base + y como $|0^\times\rangle$ y $|1^\times\rangle$ para la base $\times$. Estos estados se inferirán

en un fotón mediante un polarizador. Es decir, polarizaremos un fotón de una forma u otra en función del bit a transmitir y de la base a utilizar.

Además, los estados pertenecientes a una misma base son ortogonales, es decir, si recibimos los estados $|0^+\rangle$ ó $|1^+\rangle$ y medimos en base +, obtendremos **siempre** 0 ó 1, respectivamente (asumiendo que el canal no introduce errores). ídem si recibimos $|0^\times\rangle$ y $|1^\times\rangle$ y medimos en base $\times$.

Pero, ¿qué ocurre si recibimos un estado polarizado en una base y medimos respecto a la otra? En este caso, el resultado de la medida será 0 ó 1 aleatoriamente, es decir, $p(m = 0|\rho) = p(m = 1|\rho) = 0{,}5$.

El extremo transmisor (Alice) elige una secuencia aleatoria de bits y, para cada uno de ellos, elige la base a transmitir. Es decir, si el primer bit que Alice quiere transmitir es 0, deberá elegir si transmitir el estado $|0^+\rangle$ ó $|0^\times\rangle$. Si el segundo fuese 1, debería elegir entre $|1^+\rangle$ ó $|1^\times\rangle$, y así para el resto de bits que componen la secuencia.

Por su parte, el receptor (Bob), elegirá para cada fotón recibido una base u otra para medir. Para el ejemplo de los dos primeros fotones transmitidos por Alice, si Bob decidiese medir ambos utilizando la base +, la medida del primero arrojaría un 0, mientras que la del segundo daría 0 ó 1 de manera aleatoria, al 50 %.

Tras el intercambio de todos los fotones, Alice y Bob intercambiarían por un canal clásico las bases utilizadas para cada fotón y descartarían aquellas transmisiones en las que usaron bases opuestas ya que la medida de Bob habría sido aleatoria y por tanto no aportaría información. Los bits restantes, formarían lo que se conoce como *raw key*.

A continuación, ambos extremos intercambiarían por ese canal clásico alguno de los bits de la *raw key*. La elección de los bits intercambiados depende del protocolo BB84 utilizado.

BB84 *efficient*

Para el protocolo BB84 *efficient* (que es el que emplearemos en el emulador), se intercambian los bits transmitidos por fotones polarizados en base $\times$. Para los bits intercambiados, ambos extremos calculan la BER. Si esta tasa de error está por encima de de lo esperado (no se espera una tasa de error 0 ya que puede haber errores debidos a la distor-

sión del canal) la comunicación se aborta pues se asume la presencia de un espía. Si esa BER está dentro de los márgenes establecidos, se asume que no hay ninguna anomalía y, tras eliminar de la *raw key* los bits intercambiados, obtenemos la conocida como *shifted key*, que será la utilizada para cifrar los datos. Como para los bits de la *shifted key* ambos han utilizado las mismas bases, ambos deberían tener los mismos bits. Evidentemente, algunos de estos bits podrían diferir debido a errores del canal. No obstante, podría llevarse a cabo un mecanismo de corrección de errores.

Presencia de un espía

Si existiese un espía (Eve) que interceptase los fotones intercambiados por Alice y Bob, éste tambien debería elegir para cada fotón que intercepta que base va a utilizar para leerlo y para polarizar otro fotón que transmitirá a Bob. La elección de la base podría ser aleatoria puesto que Alice y Bob aún no han intercambiado sus bases (recordemos que lo hacen tras la transmisión de todos los fotones) y por lo tanto no sabe ni que base está utilizando Alice para polarizar cada fotón ni que base utilizará Bob para medir cada fotón.

El espía, haría una medida sobre cada fotón recibido con la base elegida para después polarizar un nuevo fotón con el bit medido y con la misma base utilizada en la medida. Este nuevo fotón lo transmitiría a Bob.

Tras la transmisión de todos los fotones, Alice y Bob también intercambian las bases utilizadas y generarían la *raw key*. A continuación, intercambiarían algunos de los bits de la *raw key* y calcularían la BER. Para los bits de la *raw key*, Alice y Bob han utilizado la misma base como sabemos. En cuanto a la base del espía, pueden pasar dos cosas:

- Eve utiliza la misma base que Alice y Bob: en este caso, Eve mide el bit que Alice codificó en el fotón y se lo transmite a Bob que, como utiliza la misma base que Alice y Eve, vuelve a medir el bit que Alice codificó.
- Eve utiliza la base opuesta a Alice y Bob: en este caso, Eve mediría aleatoriamente 0 ó 1 y transmitiría lo medido a Bob que, al utilizar la base opuesta a Eve, mediría también aleatoriamente 0 ó 1. Desglosamos las posibles medidas en la figura 2.3, suponiendo que Alice transmitió un 0, por ejemplo.

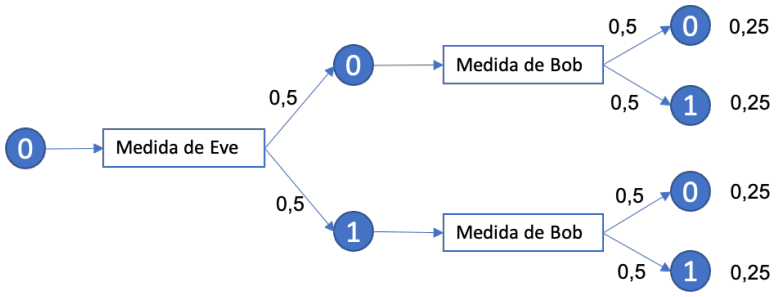


Fig. 2.3. Desglose de probabilidades de la distribución cuántica de claves cuando Eve utiliza base opuesta

Podemos ver que hay un 50 % de posibilidades de que Bob mida 0 (lo mismo que transmitió Alice) y evidentemente un 50 % de medir 1. Es decir, en la mitad de los casos Eve generaría un bit erróneo.

Si asumiésemos un canal ideal, que no introdujese errores, Alice y Bob esperarían que todos los bits intercambiados concordasen pero, debido al efecto de Eve, la mitad serían erróneos. Ésto, incrementaría notablemente la BER y haría saltar las alarmas de Alice y Bob que, con casi total seguridad, abortarían la distribución de claves debido a la sospecha de un espía.

Si el canal no fuese ideal, los bits erróneos causados por Eve podrían camuflarse con el error que se espera que introduzca el canal (ya no se espera una tasa de error 0). Sin embargo, el efecto del espía es tan grande que, a no ser que el canal fuese tan malo que la probabilidad de error esperada se acercase al 50 %, sería extremadamente difícil que pasase desapercibido.

2.2.3. Canales ópticos

Los dos canales ópticos a considerar serán canales de fibra óptica y espacio libre. Estos canales introducirán una atenuación que inicialmente se modelará en potencia. No obstante, nosotros adaptaremos esta atenuación a nuestras señales transmitidas para cada uno de los casos clásico y cuántico.

Sistema clásico

En un sistema clásico introduciremos el efecto de la atenuación en potencia sobre la envolvente compleja.

En primer lugar, sabemos que la atenuación en potencia implica que:

$$P_{rx} = P_{tx} A_F$$

La potencia y la envolvente compleja se relacionan mediante el cuadrado como se vio en el apartado 2.1.6:

$$P_0 = |V_0|^2$$

La envolvente compleja transmitida es igual al producto entre la envolvente compleja propia del láser y el símbolo transmitido. Esto es:

$$C_i V_0$$

y la potencia transmitida vendrá dada por:

$$P_{tx,i} = |C_i V_0|^2 = |C_i|^2 V_0^2$$

donde hemos podido eliminar el módulo de V_0 al ser un número real.

Como C_i representa al símbolo y es por tanto complejo, podemos introducir toda la atenuación sobre V_0 (real) sin modificar el símbolo:

$$P_{rx,i} = |C_i V_r|^2 = |C_i|^2 V_r^2$$

Por otro lado, si trabajamos en potencia tendremos:

$$P_{rx,i} = P_{tx,i} A_F = |C_i|^2 V_0^2 A_F$$

Igualando ambas expresiones llegamos a:

$$|C_i|^2 V_r^2 = |C_i|^2 V_0^2 A_F$$

que, eliminando el factor común que es el símbolo C_i, llegamos a que:

$$V_r^2 = V_0^2 A_F$$
$$V_r = V_0 \sqrt{A_F}$$

Sistema cuántico

En el emulador desarrollado se modelará la atenuación introducida por el canal como una pérdida del número promedio de fotones. Esto se demuestra siguiendo el siguiente razonamiento:

1. Energía de un fotón: $E_{foton} = h \cdot v$ [Julios] (donde h es la constante de Planck y v la frecuencia a la que vibra el fotón).
2. Potencia: $1Watt = 1[\frac{Julio}{segundo}]$.
3. Para un estado cuántico γ tenemos que $|\gamma|^2$ son $[\frac{fotones}{simbolo}]$.
4. Por tanto, si hacemos $|\gamma|^2 \cdot \frac{h \cdot v}{T_s}$ tenemos $[\frac{fotones}{simbolo} \cdot \frac{Julios}{\frac{segundo}{simbolo}}] = [fotones \cdot \frac{Julios}{segundo}] = [Watt]$, es decir, la potencia transmitida por cada estado cuántico (donde T_s es el periodo de símbolo).
5. Como la atenuación calculada es en potencia, tendríamos que $P_{rx} = |\gamma|^2 \cdot \frac{h \cdot hv}{T_s} \cdot atenuacion$.
6. Esto equivaldría a una transmisión con menos fotones ya que $|\gamma \cdot \sqrt{atenuacion}|^2 = |\gamma|^2 \cdot atenuacion$.
7. $\gamma' = \gamma \cdot \sqrt{atenuacion}$

Por lo tanto, para cada estado coherente determinado por el complejo γ, su estado atenuado correspondiente no será más que multiplicarlo por la raíz de la atenuación, teniendo así el estado determinado por:

$$\gamma \sqrt{A_F}$$

Fibra óptica

El canal de fibra óptica clásico se modelará como una atenuación en potencia, que vendrá dada, de acuerdo con [3], por la expresión:

$$A_F = 10^{-0,1 \alpha D(km)}$$

donde:

- α es la atenuación característica de la fibra, que se medirá en $\frac{dB}{km}$. Un valor muy típico, que será el que utilicemos en el emulador, es $\alpha = 0{,}2\frac{dB}{km}$.
- D es la longitud de la fibra. Como es lógico, a mayor distancia mayor será la atenuación.

Espacio libre

La atenuación en el espacio libre vendrá dada, según [3], por la fórmula:

$$G_T(\frac{\lambda}{4\pi d})^2 G_R$$

donde:

- λ es la longitud de onda de los fotones.
- d es la distancia del enlace.
- G_T y G_R serán las ganancias de transmisor y receptor, respectivamente.

2.2.4. Ruido térmico

El número de fotones de ruido térmico, al que en sucesivos apartados nos referiremos como N, viene dado por la siguiente fórmula utilizando la teoría en [9]:

$$N = \frac{1}{e^{\frac{hv}{kT_0}} - 1}$$

donde:

- $h = 6{,}626 \cdot 10^{-34}$ es la constante de Planck.
- $k = 1{,}38 \cdot 10^{-23}$ es la constante de Boltzmann.
- T_0 es la temperatura a la que se encuentra la fibra óptica.
- v es la frecuencia a la que vibra el fotón.

La fórmula anterior nos permite calcular el número de fotones que en promedio radia el medio al calentarse a la frecuencia v.

A pesar de que los fotones de señal vibrarán a una determinada frecuencia v, los fotones de ruido radiados por el medio que nos afecten no corresponderán únicamente a esa frecuencia v de los fotones de señal, sino a todo el ancho del canal que estemos utilizando. Por lo tanto, la fórmula empleada en la práctica se transforma a partir de la anterior como:

$$N = \int_{v_{min}}^{v_{max}} \frac{1}{e^{\frac{hv}{kT_0}} - 1} dv$$

donde v_{min} y v_{max} son las frecuencias mínima y máxima, respectivamente, del canal físico del medio.

2.2.5. Sistemas de comunicaciones

Como bien sabemos, un sistema de telecomunicaciones es aquel que nos permite transmitir información de una localización espacial a otra, ya sea por medio de cable o aire. No obstante, la forma en la que hacemos llegar esta información de un extremo a otro varía en gran medida dependiendo de la naturaleza del sistema empleado. En siguientes apartados, analizaremos estas diferencias para sistemas de comunicaciones clásicos y cuánticos. Para modelar estos sistemas, haremos uso de la notación y los desarrollos presentes en [9], [10], [11] y [12].

Antes de eso, explicaremos algunos de los muchos parámetros de mérito disponibles para los sistemas de telecomunicaciones que nos permitirán analizar de manera objetiva el rendimiento de cada sistema y llevarlos a comparación.

BER

La BER, *bit error rate* o probabilidad de error de bit es uno de esos parámetros de calidad objetivos que nos permiten ver cómo de bueno es un sistema. La BER es el cociente entre el número de bits erróneos y el número total de bits transmitidos:

$$BER = \frac{num_{bits,err}}{num_{bits,tx}}$$

Lo vemos con un ejemplo en la siguiente tabla:

Número de bits transmitidos	Número de bits erróneos	BER
1000	0	0
1000	1	0,001
1000	100	0,1
1000	500	0,5
1000	1000	1

TABLA 2.1. EJEMPLO DEL CÁLCULO DE LA BER

Como podemos ver, la BER es un parámetro muy fácil de calcular y con el que podemos ver rápidamente como está funcionando nuestro sistema. Las tasas de error típicas en sistemas de comunicaciones están en torno a $10^{-8}/10^{-9}$.

Probabilidad de error de símbolo

La probabilidad de error de símbolo (normalmente representada como P_e) es un parámetro muy similar a la BER. Como veremos a continuación, la información a transmitir, los bits, se modulan dando lugar a lo que conocemos como símbolos. La modulación nos permite transmitir la información de manera más fiable o a mayor velocidad. La probabilidad de error de símbolo se calcula de igual manera que la BER pero a nivel de símbolo, es decir:

$$P_e = \frac{num_{simb,err}}{num_{simb,tx}}$$

La diferencia la encontramos en que en un símbolo, en función de la modulación utilizada, podremos transmitir varios bits.

Sistemas de comunicaciones clásicos sin ruido térmico

El esquema de un sistema clásico de comunicaciones puede verse en la figura 2.4.

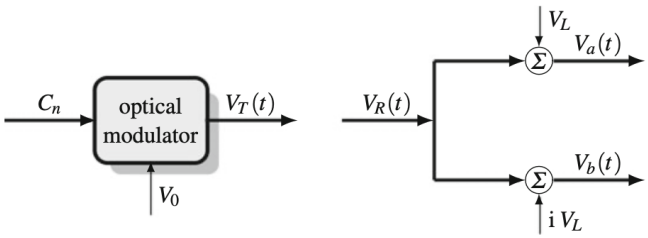


Fig. 2.4. Esquema general de un sistema de comunicaciones clásico [10]

Transmisor

Este esquema se formula en términos de envolventes complejas por simplicidad.

C_n es un valor complejo que depende de los datos a transmitir, de los bits a transmitir. En el apartado ”modulaciones clásicas” veremos como se obtiene.

El complejo C_n se modula mediante un láser de amplitud V_0, formando la envolvente compleja $V_T(t)$ y se transmite mediante el canal óptico al receptor. $V_T(t)$ se obtiene a partir de C_n y V_0 como [10]:

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

Donde:

- $h(t)$ es un pulso de duración T, puede ser por ejemplo una ventana cuadrada, que iremos desplazando a intervalos de longitud T, donde en cada intervalo se representará un símbolo. Normalmente este pulso estará normalizado en energía.
- V_0 es la amplitud de $h(t)$. Nos permitirá emular una transmisión de más o menos potencia.
- C_n es el símbolo correspondiente a cada intervalo. Nos permite introducir sobre la señal $V_0 h(t)$ la información a transmitir.

V_0 es la amplitud que introduce el láser y dependerá del número de fotones promedio que emita el láser, N_0. Es muy importante porque nos permitirá la comparación entre un sistema cuántico, determinado en parte por N_s que es el número promedio de fotones que emite el láser en un periodo de símbolo. Obtenemos V_0 como [10]:

$$V_0 = \sqrt{\frac{N_0}{H}} = \sqrt{\frac{N_0}{\frac{T}{h\nu}}}$$

donde:

- T: periodo de símbolo.
- h: constante de planck ($6{,}626 \cdot 10^{-34}$).
- v: es la frecuencia a la que vibra el fotón.

V_0, N_0 y N_s se relacionan como:

$$N_s = \frac{1}{M} \sum_{i \epsilon M} |C_0|^2 |\sqrt{H} V_0|^2 = \frac{1}{M} \sum_{i \epsilon M} |C_0|^2 N_0$$

donde al factor $\frac{1}{M} \sum_{i \epsilon M} |C_0|^2$ lo llamaremos, como veremos en el apartado del sistema cuántico, factor de forma μ_M.

Por lo tanto, podemos representar la amplitud del láser V_0 en función únicamente de N_s (asumiendo fijos v y T) como:

$$V_0 = \sqrt{\frac{N_s}{\mu_M H}}$$

Receptor

Por su parte, el receptor recibe una versión distorsionada de $V_T(t)$:

$$V_R(t) = \sum_{n=-\infty}^{\infty} C_n V_R h(t - nT)$$

Como podemos ver, hemos incluido **toda** la atenuación en el factor V_0, convirtiéndolo en el factor V_R. Esta envolvente compleja $V_R(t)$ es necesario demodularla para obtener los bits estimados. La demodulación, puede hacerse de manera homodina o heterodina. Optamos por la modulación homdina ya que sus prestaciones son mejores.

Como se puede ver en la imagen 2.4, la señal óptica recibida se divide en dos caminos. Por el camino "a", la señal $V_R(t)$ se mezcla con un láser de amplitud V_L, formando:

$$V_a(t) = V_R(t) + V_L$$

En el camino "b", se mezcla con un láser de amplitud jV_L (la imagen utiliza *i* como unidad imaginaria), haciendo:

$$V_b(t) = V_R(t) + jV_L$$

Para que la detección tenga éxito, el valor V_L debe ser mucho mayor que V_R ($V_L \gg V_R$).

No obstante, como vamos a considerar "fotoconteo" y el "fotoconteador" va a operar independientemente en cada intervalo de duración T, podemos asumir que en cada uno de esos intervalos, las envolventes complejas $V_a(t)$ y $V_b(t)$ son constantes, es decir, se convierten en V_a y V_b respectivamente (para un intervalo de duración T dado).

En ambos caminos, en cada uno de esos intervalos de duración T, los fotoconteadores harán una medida del número de fotones recibidos en dicho intervalo siendo estas medidas n_a para el camino "a" y n_b para el camino "b". Combinamos ambas medidas en un complejo z de tal manera que podamos decidir el símbolo estimado en base a un único valor, al igual que se hace en [10]:

$$z = n_a + in_b$$

Evidentemente, para decidir el símbolo recibido debemos definir unos umbrales respecto a los cuales podamos decidir. Para ello, se calcula el número medio de fotones recibidos en el camino "a" ($\bar{n}_a$) y en el "b" ($\bar{n}_b$) para cada símbolo dado C_n. Si combinamos estas medias igual que se hizo con las medidas de los "fotoconteadores" en un único número complejo como $\bar{n}_a + j\bar{n}_b$ tendremos el símbolo medio recibido para el símbolo transmitido C_n. Si calculamos el símbolo medio recibido para todos los posibles símbolos transmitidos, tendremos la constelación de símbolos recibidos o, como nos referiremos a ella, constelación recibida. Cada símbolo de la constelación recibida se corresponderá biunívocamente con un símbolo de la constelación de símbolos transmitidos.

Para calcular las medias ($\bar{n}_a$) y ($\bar{n}_b$), al modelarse éstas como procesos de Poisson, únicamente debemos recordar la teoría desarrollada en el apartado 2.1.5. Para un símbolo complejo genérico $C_n = A_n + iB_n$, las medias serían:

- $\bar{n}_a = 2\sqrt{N_L N_R}A_n + N_L$
- $\bar{n}_b = 2\sqrt{N_L N_R}B_n + N_L$

Podemos llegar a estos resultados aplicando la teoría del apartado 2.1.5. Por ejemplo, para el camino "a", si asumimos que en el intervalo $(0, T]$ la envolvente compleja es constante, tenemos el siguiente desarrollo:

1. Envolvente compleja en el camino "a": $V_R(t) + V_L = C_n V_R + V_L$

2. La potencia del proceso de Poisson es: $P(t) = |C_n V_R + V_L|^2 = |(A_n V_R + V_L + jB_n V_R)|^2 = (A_n V_R)^2 + 2A_n V_R V_L + V_L^2 + (B_n V_R)^2$

3. Como hemos impuesto la condición $V_L \gg V_R$, aproximamos la potencia a: $P(t) = V_L^2 + 2A_n V_R V_L$

4. A partir de la potencia, obtenemos la intensidad del proceso de Poisson como: $\lambda(t) = \frac{1}{h\nu} P(t) = \frac{1}{h\nu}(V_L^2 + 2A_n V_R V_L)$

5. Con la intensidad, podemos calcular fácilmente la media: $\bar{n_a} = \int_0^T \frac{1}{h\nu}(V_L^2 + A_n V_R V_L)dt = \frac{T}{h\nu}(V_L^2 + 2A_n V_R V_L) = HV_L^2 + 2A_n \sqrt{H} V_R \sqrt{H} V_L = N_L + 2A_n \sqrt{N_R N_L}$

Donde como hemos visto antes, $HV_0^2 = N_0$, en este caso tenemos $\sqrt{H}V_R$ y $\sqrt{H}V_L$ que son $\sqrt{N_R}$ y $\sqrt{N_L}$, respectivamente.

Para el camino "b" el desarrollo es prácticamente idéntico:

1. Envolvente compleja en el camino "b": $V_R(t) + jV_L = C_n V_R + jV_L$

2. La potencia del proceso de Poisson es: $P(t) = |C_n V_R + jV_L|^2 = |A_n V_R + jB_n V_R + jV_L|^2 = (A_n V_R)^2 + (B_n V_R)^2 + 2B_n V_R V_L + V_L^2$

3. Como hemos puesto la condición $V_L \gg V_R$, aproximamos la potencia a: $P(t) = V_L^2 + 2B_n V_R V_L$

4. A partir de la potencia, obtenemos la intensidad del proceso de Poisson como: $\lambda(t) = \frac{1}{h\nu} P(t) = \frac{1}{h\nu}(V_L^2 + 2B_n V_R V_L)$

5. Con la intensidad, podemos calcular fácilmente la media: $\bar{n_a} = \int_0^T \frac{1}{h\nu}(V_L^2 + B_n V_R V_L)dt = \frac{T}{h\nu}(V_L^2 + 2B_n V_R V_L) = HV_L^2 + 2B_n \sqrt{H} V_R \sqrt{H} V_L = N_L + 2B_n \sqrt{N_R N_L}$

Las varianzas en ambos caminos serían igual a las medias. Ésto es algo propio de las variables de Poisson.

Por lo tanto, el símbolo medio sería $\bar{n} = 2\sqrt{N_L N_R} C_n + (1 + j)N_L$. Como podemos ver, cada símbolo de la constelación recibida depende únicamente de las partes real (A_n) y compleja (B_n) de un símbolo de la constelación de símbolos transmitidos. De ahí esa relación biunívoca entre los símbolos de ambas constelaciones de la que hablamos.

Así, una vez tenemos la constelación de símbolos recibidos, para cada medida de los "fotoconteadores", en cada periodo T estimaremos el símbolo recibido como:

$$z = n_a + jn_b$$

para el cual buscaremos el símbolo de la constelación de estados recibidos más cercano. Una vez elegido, el símbolo más cercano se corresponderá con uno solo de los símbolos transmitidos y, por lo tanto, con una única secuencia de bits.

Sistemas de comunicaciones clásicos con ruido térmico

En esta sección consideramos el mismo sistema de comunicaciones clásico pero ahora cuando es afectado por el ruido térmico.

Como el ruido térmico nos afectará en el canal óptico, la parte del transmisor es idéntica al caso sin ruido.

En cuanto al receptor, lo que ocurrirá es que la señal recibida tendrá una mayor distorsión, por lo que el número de fotones medidos variará.

Por lo tanto para un símbolo C_n, el rango de valores en los que oscilarán las medidas de los "fotoconteadores" cuando el sistema se ve afectado por el ruido térmico será distinto (y en general mayor) al rango en el que oscilan las medidas del "fotoconteador" cuando consideramos un sistema ideal en cuanto a ruido térmico. Por ello, debemos modificar las medias de los símbolos que forman la constelación recibida. En presencia de ruido térmico, ya no trabajamos con variables de Poisson sino con variables aleatorias de Laguerre, que tienen la forma [9]:

$$p_n(k|\gamma) = \frac{N^k}{(N+1)^{k+1}} exp(-\frac{N_\gamma}{N+1}) L_k(-\frac{N_\gamma}{N(N+1)})$$

donde:

- N_γ es el número de fotones de señal, y se corresponde con la media calculada para el caso sin ruido ($2\sqrt{N_L N_R} A_n + N_L$, para el camino "a" por ejemplo).
- N es el número de fotones de ruido térmico.

La media de una variable de Laguerre se puede ver a continuación:

- $\bar{n}_a = N_{\gamma,a} + N = 2\sqrt{N_L N_R} A_n + N_L + N$
- $\bar{n}_b = N_{\gamma,b} + N = 2\sqrt{N_L N_R} B_n + N_L + N$

A pesar de que modificamos la constelación recibida de acuerdo a las medidas esperadas de los "fotoconteadores", es previsible un error mayor ya que el ruido térmico no sólo hace aumentar la media de las medidas sino su varianza. Es decir, en presencia de ruido térmico la disparidad de las medidas para un mismo símbolo será claramente mayor que en su ausencia.

La varianza de una variable de Laguerre se define como:

- $var(n)_a = \bar{n}_a + 2N_{\gamma,a}N + N^2$
- $var(n)_b = \bar{n}_b + 2N_{\gamma,b}N + N^2$

Donde vemos que ya no es igual a su media (como ocurría en variables aleatorias de Poisson) sino que es igual a su media más un factor $2N_\gamma N + N^2$.

Para entender por qué esto es así, pensemos que debido a la emisión del láser, nosotros únicamente conocemos los fotones emitidos en promedio y ésto va a ser fuente de error ya que igual nosotros estamos esperando diez fotones, pero solo se emiten ocho que son los que se miden. Si ahora tenemos dos fuentes de fotones promedio (el láser y la fibra que se calienta) esa fluctuación será mayor. Por ejemplo, imaginemos que en un periodo de símbolo esperamos diez fotones de señal (láser) y dos de ruido térmico (fibra) pero debido a la emisión de fotones, en realidad se emiten seis de señal y uno de ruido térmico. El "fotoconteador" mediría ocho fotones cuando en realidad se esperan doce, algo más de la mitad.

Modulaciones clásicas

Para finalizar los sistemas de comunicaciones clásicos, hablaremos de las modulaciones, de como se obtiene un símbolo genérico C_n a partir de los datos de entrada que consideraremos (como prácticamente siempre ocurrirá) que son bits. Puesto que en el emulador del capítulo de desarrollo sólo se emplea la modulación PSK, ésta será la única que se explique.

Lo primero que debemos hacer es generar la constelación de símbolos transmitidos. Una constelación de símbolos depende de un parámetro, M, que es el orden de la modulación. Es decir, el número de símbolos de la modulación.

Para generar los símbolos de una M-PSK debemos utilizar la siguiente ecuación:

$$e^{j\frac{2\pi}{M}l}$$

donde l tomará valores desde 0 hasta $M-1$. Cada uno de esos M posibles valores originará un símbolo.

Para una 2-PSK o BPSK, l tomará valores 0 ó 1. Los símbolos que tendremos serán:

- $l = 0 \rightarrow e^{j\frac{2\pi}{2}0} = e^0 = 1$
- $l = 1 \rightarrow e^{j\frac{2\pi}{2}1} = e^{j\pi} = -1$

Vemos en la siguiente imagen los estados posibles para una BPSK.

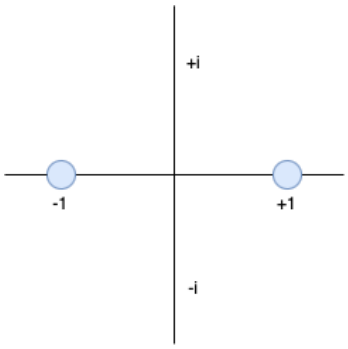


Fig. 2.5. Símbolos de una BPSK en el plano complejo

Para una 4-PSK o QPSK, l tomará valores 0, 1, 2 ó 3. Los símbolos que tendremos serán:

- $l = 0 \rightarrow e^{j\frac{2\pi}{4}0} = e^0 = 1$
- $l = 1 \rightarrow e^{j\frac{2\pi}{4}1} = e^{j\frac{\pi}{2}} = j$
- $l = 2 \rightarrow e^{j\frac{2\pi}{4}2} = e^{j\pi} = -1$
- $l = 3 \rightarrow e^{j\frac{2\pi}{4}3} = e^{j\frac{3\pi}{2}} = -j$

Vemos en la siguiente imagen los estados posibles para una QPSK.

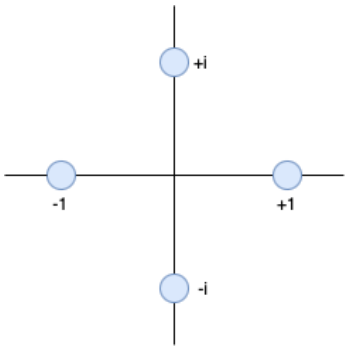


Fig. 2.6. Símbolos de una QPSK en el plano complejo

Sistemas de comunicaciones cuánticos

El esquema para un sistema de comunicaciones cuántico se muestra en la figura 2.7.

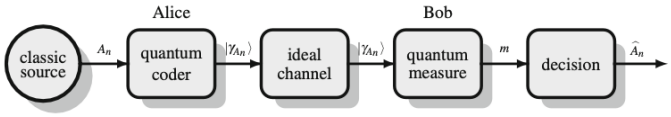


Fig. 2.7. Esquema general de un sistema de comunicaciones cuántico [10]

Estados coherentes

Antes de comenzar a analizar las distintas partes del sistema de comunicaciones cuántico, se explicarán los estados coherentes ya que son aquellos estados utilizados para modelar la transmisión puesto que representan la radiación coherente de un láser.

Un estado coherente se define, según [10], en un espacio de Hilbert H de dimensión infinita respecto a una base formada por los denominados "fock states". Los "fock states" (también denominados "number states") son estados cuánticos representados por $|n\rangle$ donde "n" indica el número **exacto** de fotones asociado a ese estado. Por ejemplo, el "number state" $|2\rangle$ lleva asociados dos fotones. Además, los "fock states" son ortogonales, es decir

$$\langle n_i | n_k \rangle = \delta_{ik} = \begin{cases} 1, & i = k \\ 0, & i \neq k \end{cases}$$

Como sabemos, el número de elementos que forman una base de un espacio de Hilbert H debe ser igual a su cardinalidad (la dimensión del espacio). Por lo tanto, como el espacio

de Hilbert utilizado es de dimensión infinita, la base formada por los "fock states" tendrá infinitos elementos.

Dicho esto, un estado coherente se define según [10] como:

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

donde α es un número complejo que caracteriza completamente el estado $|\alpha\rangle$ y cuyo módulo al cuadrado nos da el número **promedio** de fotones asociados al estado dado.

Finalmente, calculamos el producto interior entre dos estados coherentes (definidos por α y β) siguiendo el desarrollo en [10]:

$$\langle\beta|\alpha\rangle = (e^{-\frac{1}{2}|\beta|^2} \sum_{m=0}^{\infty} \frac{(\beta^m)^*}{\sqrt{m!}} \langle m|)(e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle) = e^{-\frac{1}{2}(|\beta|^2-|\alpha|^2)} \sum_{m=0}^{\infty}\sum_{n=0}^{\infty} \frac{(\beta^m)^*}{\sqrt{m!}} \frac{\alpha^n}{\sqrt{n!}} \langle m|n\rangle$$

Como hemos visto, los "fock states" son ortogonales, por lo que el producto interior $\langle m|n\rangle$ siempre es 0 excepto cuando $m = n$. Por tanto, la expresión anterior queda:

$$e^{-\frac{1}{2}(|\beta|^2-|\alpha|^2)} \sum_{n=0}^{\infty} \frac{(\beta^n)^*}{\sqrt{n!}} \frac{\alpha^n}{\sqrt{n!}} = e^{-\frac{1}{2}(|\beta|^2-|\alpha|^2)} \sum_{n=0}^{\infty} \frac{(\beta^*\alpha)^n}{n!} = e^{-\frac{1}{2}(|\beta|^2-|\alpha|^2)} e^{\beta^*\alpha} = e^{-\frac{1}{2}(|\beta|^2-|\alpha|^2)+\beta^*\alpha}$$

Es decir, el producto interior de dos estados coherentes es una exponencial que depende de α y de β. Por lo tanto, al tratarse de una exponencial, podemos afirmar que dos estados coherentes **nunca** son ortogonales. Esto tendrá importantes consecuencias como veremos a continuación.

Transmisor

Como vemos, al igual que en el sistema clásico, a la entrada del modulador tenemos un símbolo C_n que es un valor complejo calculado de manera similar a como acabamos de ver para el caso clásico.

La diferencia principal es que la salida del modulador no se modela con envolventes complejas como se hacía con $v_T(t)$ en la figura 2.4 sino que lo hacemos con $\left|\gamma_{C_n}\right\rangle$, un ket que representa un estado cuántico asociado al símbolo C_n.

El ket $\left|\gamma_{C_n}\right\rangle$ representa un estado coherente que, como acabamos de ver, tiene la forma:

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

Si recordamos, un estado coherente se define respecto a la base formada por los *number states* y el parámetro α nos permite caracterizar por completo el estado coherente. Lo que se hace es, cuando el modulador recibe el símbolo complejo C_n genera el estado $\left|\gamma_{C_n}\right\rangle$ que no es más que un estado coherente con $\alpha = C_n$.

Así, si el símbolo a transmitir es $C_n = +j$, el estado $|\gamma\rangle$ transmitido sería:

$$|\gamma\rangle = |\alpha\rangle_{\alpha=+j} = e^{-\frac{1}{2}|j|^2} \sum_{n=0}^{\infty} \frac{j^n}{\sqrt{n!}} |n\rangle$$

Receptor

Como, de momento, no consideramos el ruido térmico, el estado que tendremos a la entrada del receptor también será un estado puro, al que denominaremos $\left|\tilde{\gamma}_{C_n}\right\rangle$.

En el receptor se realizará una medida sobre $\left|\tilde{\gamma}_{C_n}\right\rangle$ que, como ya sabemos, arrojará un resultado con una cierta aleatoriedad. Para, dado este estado, averiguar en que proporción obtendremos unos resultados u otros, recurriremos a los operadores de medida. Si tenemos una modulación BPSK, tendremos dos posibles resultados de la medida 0 ó 1 y, por lo tanto, tendremos dos operadores de medida Q_0 y Q_1. La probabilidad de a partir del estado $\left|\tilde{\gamma}_{C_n}\right\rangle$ la medida "m" sea 0 ó 1 vendrá determinada por la traza de la siguiente forma:

$$p(m = i|\tilde{\gamma}_{C_n}) = Tr[\rho Q_i] = Tr\left[\left|\tilde{\gamma}_{C_n}\right\rangle\left\langle\tilde{\gamma}_{C_n}\right| Q_i\right] = \left\langle\tilde{\gamma}_{C_n}\right|Q_i\left|\tilde{\gamma}_{C_n}\right\rangle$$

No obstante estamos utilizando estados coherentes y, como hemos demostrado anteriormente, dos estados coherentes nunca son ortogonales. Esto implica que al medir estos estados el resultado nunca será determinista. En otras palabras, aunque en el demodulador tengamos el mismo estado generado en el transmisor, nunca tendremos que la probabilidad de obtener un resultado u otro sea 1 ó 0.

Sistemas de comunicaciones cuánticos con ruido térmico

Cuando consideramos el ruido térmico en nuestro sistema de comunicaciones, el estado que llega al demodulador ya no es un estado puro como ocurría antes, sino un estado mixto, que representaremos en forma de operador densidad.

Como sabemos, el estado coherente transmitido está determinado por un único valor complejo C_n, el símbolo. Para obtener matemáticamente el operador densidad que tendremos en el demodulador podemos hacer uso de la siguiente ecuación obtenida de [9]:

$$\rho_{\gamma_{C_n}} = \sum_{h=0}^{\infty}\sum_{k=0}^{\infty} \frac{N^k}{(N+1)^{k+1}} \sqrt{\frac{h!}{k!}} (\frac{\gamma^*_{C_n}}{N})^{k-h} e^{-\frac{|\gamma_{C_n}|^2}{N+1}} L_h^{k-h}(-\frac{\gamma^*_{C_n}}{N(N+1)})$$

donde:

- N es el numero promedio de fotones de ruido térmico.
- $L_h^{k-h}(-\frac{\gamma^*_{C_n}}{N(N+1)})$ es el polinomio de Laguerre de grado h y parámetro $k-h$ evaluado en el punto $x = -\frac{\gamma^*_{C_n}}{N(N+1)}$

Una vez tenemos el estado cuántico a la entrada del demodulador representado por el operador densidad $\rho_{\gamma_{C_n}}$ lo único que falta es la medida. De nuevo, la volvemos a definir de manera matemática. En este caso, quedaría caracterizada únicamente mediante la traza:

$$p(m = i|\rho_{\gamma_{C_n}}) = Tr[\rho_{\gamma_{C_n}} Q_i]$$

Debido al ruido térmico, mientras que a la salida del transmisor tenemos un estado puro, a la entrada del receptor este estado puro se habrá transformado en un estado abstracto (mixto). Si, como hemos visto para el caso sin ruido, dos estados coherentes nunca serán ortogonales y por lo tanto la medida será de por sí aleatoria, ahora añadimos una distorsión más y es que ya no vamos a estar en un estado concreto, sino que vamos a poder estar en un conjunto de estados cada uno con una probabilidad.

Modulaciones cuánticas

De nuevo, como sólo utilizaremos en el emulador la constelación PSK con órdenes $M = 2$ y $M = 4$, éstas serán las únicas explicadas en detalle.

Para obtener el complejo C_n que caracteriza al estado cuántico transmitido debemos seguir un procedimiento muy similar a como hicimos para los sistemas clásicos.

En primer lugar, debemos generar la constelación PSK utilizando de nuevo la fórmula $e^{j\frac{2\pi}{M}l}$. A la constelación generada la llamaremos constelación PSK estándar.

No obstante, la constelación creada a partir de la ecuación $2e^{j\frac{2\pi}{M}l}$ también es una PSK. De manera general, podemos escribir cualquier constelación PSK como:

$$\Delta e^{j\frac{2\pi}{M}l}$$

En palabras, multiplicando la constelación que hemos denominado estándar por un factor Δ. Podemos elegir qué PSK utilizar gracias al parámetro N_s.

N_s indica el número de fotones que en promedio emite el láser por símbolo. Si sabemos que el módulo al cuadrado del complejo α indica el número de fotones promedio asociados a ese estado coherente y que para el estado coherente transmitido α tomará el valor del símbolo a transmitir, podemos calcular N_s como [10]:

$$N_s = \frac{1}{M}\sum_{i\epsilon M}|\gamma_i|^2$$

Expresando cada símbolo γ_i como su símbolo de la constelación normalizada ($\bar{\gamma}_i$) multiplicado por el factor Δ obtenemos:

$$N_s = \frac{1}{M}\sum_{i\epsilon M}|\bar{\gamma}_i|^2\Delta^2$$

De este modo, N_s está determinado por:

- $\frac{1}{M}\sum_{i\epsilon M}|\bar{\gamma}_i|^2$. A esta parte lo denominamos factor de forma (μ_M) y depende **únicamente** de la constelación estándar. Como en una PSK todos los símbolos se encuentran sobre una circunferencia de radio unidad, tendremos $|\bar{\gamma}_i|^2 = 1^2 = 1$ sea cual sea el símbolo $\bar{\gamma}_i$. Por ello, si tenemos M símbolos cuyo modulo al cuadrado es 1, el sumatorio daría como resultado M y, como dividimos el sumatorio entre M, podemos concluir que una constelación PSK **siempre** tiene $\mu_M = 1$.
- Δ

Con el desarrollo anterior, obtenemos

$$N_s = \mu_M\Delta^2 = \Delta^2$$

Pudiendo, por tanto, elegir la constelación utilizada como:

$$const = \sqrt{N_s}\cdot const_{base}$$

Es decir, modificando el parámetro N_s elegimos la constelación PSK utilizada.

2.2.6. Obtención de operadores de medida

Para un sistema cuyos símbolos transmitidos y recibidos pertenecen a un alfabeto A con M símbolos, la probabilidad de acierto de símbolo de un sistema se define como:

$$P_a = \frac{1}{M} \sum_{i \epsilon A} Tr[\rho_i Q_i]$$

donde $Tr[\rho_i Q_i]$ como sabemos indica la probabilidad de, para un símbolo i representado por el operador densidad ρ_i, medir el símbolo correcto. Evidentemente, la probabilidad de error de símbolo no será más que

$$P_e = 1 - P_a$$

El objetivo de esta sección es, por tanto, encontrar el conjunto de operadores de medida $(Q_i, i \epsilon A)$ que maximicen (minimicen) la probabilidad de acierto P_a (la probabilidad de error P_e).

No obstante, tal y como se dice en [11], optimizar estos operadores densidad para obtener la mínima probabilidad de error posible es algo extremadamente costoso ya que debemos encontrar varias matrices de dimensiones considerables lo que implica la búsqueda de un gran número de valores, que no siempre es posible. Sólo se considerará la optimización en algunos casos, como por ejemplo sistemas binarios o sistemas que utilizan constelaciones que cumplen la GUS donde el número de valores que hay que encontrar es menor.

Para el resto de casos, el método empleado será la suboptimización que, con un coste menor, nos permite obtener probabilidades de error muy cercanas a las óptimas y, en algunos casos, iguales a las óptimas.

Factores de un operador

Un factor de un operador Γ es un vector o matriz de elementos complejos γ tal que multiplicando ese factor por su hermítico (recordemos, transpuesto y conjugado elemento a elemento) obtenemos el operador Γ de la forma:

$$\Gamma = \gamma \gamma^*$$

Por ejemplo, para un operador densidad que representa un estado puro sabemos que:

$$\rho = |\gamma\rangle \langle\gamma|$$

por tanto, su factor sería $\gamma = |\gamma\rangle$ ya que:

$$\rho = \gamma\gamma^* = |\gamma\rangle (|\gamma\rangle)^* = |\gamma\rangle \langle\gamma|$$

donde hemos hecho uso de que, como vimos en las primeras líneas del capítulo, el bra de un ket no es más que el transpuesto y conjugado elemento a elemento del ket.

No obstante, para un estado mixto, el factor no sería un vector sino que sería una matriz de dimensiones *nxr*, donde *n* es la dimensión del espacio de Hilbert en el que se define el estado (pudiendo ser infinita). Por su parte, *r* es el rango del operador densidad.

Matrices de interés

Definimos aquí algunas matrices que serán utilizadas a continuación. Seguiremos, como de costumbre, la notación utilizada en [11].

En primer lugar, tenemos la matriz de estados y la matriz de medida, las cuales tienen la siguiente forma para estados puros:

- Matriz de estados: $\Gamma = [|\gamma_0\rangle, |\gamma_1\rangle, \cdots, |\gamma_M\rangle]$ de dimensiones nxM, donde n es la dimensión del espacio de Hilbert utilizado (pudiendo ser infinita) y M es el orden de la constelación (el número de estados que la forman).
- Matriz de medida: $M = [|\mu_0\rangle, |\mu_1\rangle, \cdots, |\mu_M\rangle]$, también de dimensiones nxM

También existe una definición para estados mixtos en términos de factores:

- Matriz de estados: $\Gamma = [\gamma_0, \gamma_1, \cdots, \gamma_M]$, siendo sus dimensiones nxH con H la suma de las columnas de los factores. Es decir, si veíamos que cada factor tenía dimensiones nxr, tendremos $H = r_0 + r_1 + \cdots + r_M$
- Matriz de medida: $M = [\mu_0, \mu_1, \cdots, \mu_M]$, con dimensiones nxH.

Otras dos matrices que también utilizaremos en el apartado de suboptimización son:

- Matriz de Gram: $G = \Gamma^*\Gamma$
- Operador de Gram: $T = \Gamma\Gamma^*$
- Matriz de producto mixto: $B = M^*\Gamma$

Geometria simétrica uniforme (GUS)

La geometría simétrica uniforme o GUS por sus siglas en inglés("Geometrically Uniform Symmetry") es una propiedad que poseen ciertas constelaciones de estados. Para que una constelación cumpla la GUS, deben cumplirse dos propiedades que, según [11], son:

- $|\gamma_i\rangle = S^i |\gamma_0\rangle$. Es decir, que todos los estados de la constelación puedan obtenerse a partir de un estado $|\gamma_0\rangle$ aplicando i veces un operador S.
- $S^M = I_H$. Es decir, que aplicando M veces (el número de estados de la constelación) el operador S a un estado obtengamos de nuevo ese mismo estado (equivalente a aplicar el operador identidad, I_H)

Estas condiciones pueden extenderse a estados mixtos de la misma forma tal y como se indica en la misma publicación:

- Aplicado a operadores densidad: $\rho_i = S^i \rho_0 (S^i)^*$.
- Aplicado a los factores de los operadores densidad: $\gamma_i = S^i \gamma_0$.

Podemos ver que el punto referente a operadores densidad es equivalente al punto anterior ya que:

$$\rho_i = \gamma_i (\gamma_i)^* = S^i \gamma_0 (S^i \gamma_0)^*$$

que recordando las propiedades de las matrices donde:

$$(AB)^* = B^* A^*$$

tenemos:

$$\rho = S^i \gamma_0 \gamma_0^* (S^i)^* = S^i \rho_0 (S^i)^*$$

Las constelaciones con la GUS son extremadamente útiles como veremos a continuación.

Operadores de medida óptimos en constelaciones binarias

Obtener los operadores de medida óptimos en una constelación binaria es el caso más sencillo ya que únicamente debemos optimizar un operador puesto que se debe cumplir que:

$$Q_0 + Q_1 = I_H$$

La probabilidad de acierto vendrá dada por:

$$P_a = \frac{1}{2}\sum_{i\epsilon A} Tr[\rho_i Q_i] = \frac{1}{2}Tr[\rho_0(I_H - Q_1)] + \frac{1}{2}Tr[\rho_1 Q_1]$$

que, aprovechando que la traza es lineal y que la traza de un operador densidad es 1, obtenemos

$$\frac{1}{2}Tr[\rho_0] + \frac{1}{2}Tr[(\rho_1 - \rho_0)Q_1] = \frac{1}{2} + \frac{1}{2}Tr[(\rho_1 - \rho_0)Q_1] = \frac{1}{2} + \frac{1}{2}Tr[DQ_1]$$

donde hemos llamado D al operador $\rho_1 - \rho_0$.

Para el desarrollo siguiente, nos inspiramos una vez más en el trabajo realizado por Gianfranco Cariolaro en [11].

Debemos buscar el operador Q_1 que maximice la probabilidad de acierto anterior. Dado que el primer término es constante, podemos centrarnos únicamente en el término $Tr[DQ_1]$. Descomponiendo D en autovalores y autovectores, obtenemos:

$$D = \sum_k x_k |x_k\rangle \langle x_k|$$

Si introducimos esta formulación de D en el término a maximizar tenemos:

$$Tr[\sum_k x_k |x_k\rangle \langle x_k| Q_1]$$

que debido a la linealidad de la traza es equivalente a:

$$\sum_k x_k Tr[|x_k\rangle \langle x_k| Q_1]$$

Si recordamos, la expresión $Tr[|x_k\rangle \langle x_k| Q_1] = Tr[\rho_{x_k} Q_1]$ representa la probabilidad de, dado un estado puro $|x_k\rangle$, obtener 1 en la medida. Por lo tanto, al ser una probabilidad, debe ser mayor o igual que 0.

Por otro lado, x_k representa los autovalores de D, que pueden ser tanto positivos como negativos. Por ello, el término $\sum_k x_k Tr[|x_k\rangle \langle x_k| Q_1]$ será máximo si $Tr[|x_k\rangle \langle x_k| Q_1] = 0$

cuando $x_k < 0$ y $Tr[|x_k\rangle\langle x_k| Q_1] = 1$ cuando $x_k > 0$ de tal manera que en el sumatorio en k únicamente sumamos valores positivos.

Para que $Tr[|x_k\rangle\langle x_k| Q_1]$ sea 1, Q_1 debe ser $|x_k\rangle\langle x_k|$ ya que tendríamos:

$$Tr[|x_k\rangle\langle x_k|x_k\rangle\langle x_k|] = Tr[|x_k\rangle\langle x_k|] = 1$$

ya que $\langle x_k|x_k\rangle = 1$ debido a la condición de normalización y $|x_k\rangle\langle x_k|$ es el operador densidad que representa al estado cuántico $|x_k\rangle$ y, como sabemos, un operador densidad tiene traza unidad.

Por ello, debemos concluir que el operador Q_1 debe tener la forma:

$$\sum_{x_k>0} |x_k\rangle\langle x_k|$$

Al tratar con operadores hermíticos, como los autovectores asociados a distintos autovalores son ortogonales ($\langle x_j|x_i\rangle = 0$ si $i \neq j$), tendríamos para un autovalor negativo x_{-k} (los que queremos eliminar):

$$Tr\left[|x_{-k}\rangle\langle x_{-k}| Q_1 \right] = Tr\left[|x_{-k_1}\rangle\langle x_{-k_1}| \left(|x_{k_2}\rangle\langle x_{k_1}| + |x_{k_2}\rangle\langle x_{k_2}| + ... \right) \right] =$$
$$Tr\left[|x_{-k_1}\rangle\langle x_{-k_1}|x_{k_1}\rangle\langle x_{k_1}| + |x_{-k_1}\rangle\langle x_{-k_1}|x_{k_2}\rangle\langle x_{k_2}| + ... \right] =$$
$$Tr[0 + 0 + ...] = 0$$

donde los productos interiores tales como $\langle x_{-k_1}|x_{k_1}\rangle$ harían que la traza fuese 0 debido a la ortogonalidad.

Finalmente, una vez se ha obtenido el operador de medida Q_1, obtener Q_0 es muy sencillo puesto que debe cumplirse:

$$Q_0 = I_H - Q_1$$

ya que, como vimos en el apartado 2.2.1, los operadores de un sistema POVM deben dar una especificación completa de la identidad en el espacio de Hilbert H.

Operadores de medida óptimos en constelaciones con la GUS

La obtención de operadores de medida para constelaciones que cumplen con la GUS es otro de los casos “sencillos”. No obstante, a diferencia del caso binario, el desarrollo

no es tan simple y se necesita hacer uso de técnicas software como CSP ("convex semidefinite programming"). Por ello, únicamente se hace una mención a estos casos de interés.

La razón por la que la optimización es más sencilla es por que si la constelación cumple la GUS, se ha demostrado en [11] que existe un conjunto de operadores de medida óptimos que también cumplen la GUS, es decir, que:

$$Q_i = S^i Q_0 (S^i)^*$$

Es decir, en lugar de tener que buscar el conjunto de M operadores únicamente es necesario encontrar un único operador (igual que acabamos de ver para el caso binario), lo que reduce drásticamente la complejidad del problema.

Suboptimización SRM

Finalmente, llegamos a la suboptimización. Éste es un método que no nos permite encontrar los operadores de medida que minimizan la probabilidad de error pero que ofrecen una probabilidad de error muy cercana a la mínima. Por ello, constituyen una gran aproximación. Además, en algunos casos, la suboptimiación ofrece soluciones óptimas como para constelaciones con la GUS.

Para la suboptimización, nos basaremos en los desarrollos disponibles en [12].

De los distintos métodos de suboptimización existentes, utilizaremos el método SRM (*Square Root Measurement*). Este método no busca encontrar los operadores de medida que minimicen la probabilidad de error sino aquellos que minimicen el error cuadrático.

Si definimos el ket error como:

$$|e\rangle = |\gamma_i\rangle - |\mu_i\rangle$$

debemos buscar los vectores de medida $|\mu_i\rangle$ que minimicen el error cuadrático:

$$\varepsilon = \sum_i \langle e_i | e_i \rangle = \sum_i (\langle \gamma_i | - \langle \mu_i |)(|\gamma_i\rangle - |\mu_i\rangle)$$

Podríamos por tanto pensar que la mejor opción es tomar los vectores de medida como $|\mu_i\rangle = |\gamma_i\rangle$ teniendo así $\varepsilon = 0$. No obstante esto no es posible debido al teorema de Kennedy.

El teorema de Kennedy nos dice que, para una constelación que está determinada por estados puros (las que vamos a utilizar lo están), los operadores de medida óptimos son elementales. Un operador elemental es aquel que tiene la forma:

$$Q_i = |\mu_i\rangle \langle\mu_i|$$

Además, esos kets $|\mu_i\rangle$ han de ser ortogonales, es decir, se cumple que:

$$\langle\mu_i|\mu_j\rangle = \begin{cases} 0 & , \text{si } i \neq j \\ 1 & , \text{si } i = j \end{cases}$$

Por lo tanto, no podemos elegir $|\mu_i\rangle = |\gamma_i\rangle$ ya que los kets de estado $|\gamma_i\rangle$ son estados coherentes que nunca son ortogonales tal y como se demostró algunos apartados atrás.

Lo que nos queda es obtener la matriz de medida, de tal manera que podamos obtener los vectores de medida $|\mu_i\rangle$ (factores de medida μ_i) a partir de los cuales obtener los operadores de medida Q_i como $|\mu_i\rangle \langle\mu_i|$ para estados puros ($\mu_i\mu_i^*$ para estados mixtos)

Podemos obtener la matriz de medida M de tres formas:

- SVD de la matriz Γ
- Matriz de Gram
- Operador de Gram

SVD de la matriz de estados Γ

Sabemos del apartado 2.1.4 que podemos hacer una descomposición en valores singulares (reducida) de una matriz y representarla de la forma:

$$\Gamma = U_r \Sigma_r V_r^*$$

A partir de esa SVD, la matriz de medida se obtiene muy fácilmente, siempre según [12], como:

$$M = U_r V_r^*$$

Matriz de Gram G

Podemos obtener la matriz de medida M a partir de la matriz de estados y de la matriz de Gram, de nuevo de acuerdo con [12], como:

$$M = \Gamma G^{-\frac{1}{2}}$$

Donde el exponente $-\frac{1}{2}$ indica la raiz inversa de la matriz de Gram.

El cálculo de la raíz inversa de una matriz es muy sencillo a partir de su SVD como se vio en el apartado 2.1.4.

Podemos demostrar que la expresión anterior desemboca en la misma expresión vista para el caso de la SVD de Γ:

$$M = \Gamma G^{-\frac{1}{2}} = \Gamma(\Gamma^*\Gamma)^{-\frac{1}{2}}$$

$$M = (U_r\Sigma_r^2 V_r^*)(V_r\Sigma^{-1}U_r^*)(U_r\Sigma^{-1}V_r^*)$$

$$M = U_r\Sigma_r^2\Sigma_r^{-2}V_r^*$$

$$M = U_r V_r^*$$

Donde hemos hecho uso de las SVD, de la raíz de una matriz y del hecho de que las matrices de la SVD de una matriz son unitarias (implica que $AA^* = A^*A = I$) como se vio en los apartados 2.1.4 y 2.1.2.

Operador de Gram T

La aproximación del operador de Gram nos permite obtener la matriz de medida como [12]:

$$M = T^{-\frac{1}{2}}\Gamma$$

Una vez más, podemos llegar a la misma expresión que con la SVD de la matriz de estados como demostramos a continuación:

$$M = T^{-\frac{1}{2}}\Gamma = (\Gamma\Gamma^*)^{-\frac{1}{2}}\Gamma$$

$$M = (U_r\Sigma_r^{-1}V_r^*)(V_r\Sigma_r^{-1}U_r^*)(U_r\Sigma_r^2V_r^*)M = U_r\Sigma_r^2\Sigma_r^{-2}V_r^*$$

$$M = U_r V_r^*$$

De nuevo, hacemos uso de las propiedades de la SVD y de las matrices unitarias.

Lo interesante de esta aproximación es que a partir del operador de Gram, podemos obtener cada vector de medida a partir de cada vector de estado como:

$$|\mu_i\rangle = T^{-\frac{1}{2}} |\gamma_i\rangle$$

Ídem para estados mixtos, donde cada factor de un operador de medida se relaciona con un factor de estado como:

$$\mu_i = T^{-\frac{1}{2}} \gamma_i$$

Obtención de probabilidades teóricas

Para obtener las fórmulas que nos permiten acceder a las probabilidades de error teóricas, necesitamos hacer uso de la matriz B o la matriz de producto mixto.

Como hemos visto al inicio de esta sección, esta matriz se calcula como:

$$B = M^* \Gamma$$

No obstante, nos será mas útil si la descomponemos en forma de factores:

$$B = [\mu_0^*, \mu_1^*, \cdots, \mu_M^*]^T [\gamma_0, \gamma_1, \cdots, \gamma_M]$$

Es decir, la submatriz b_{ji} se obtiene multiplicando como los factores μ_j y γ_i, como:

$$b_{ji} = \mu_j^* \gamma_i$$

Donde, la probabilidad de medir el estado j habiendo transmitido el estado i se calcula de manera muy sencilla, tal y como se afirma en [12], a partir de la anterior submatriz:

$$p(j|i) = Tr[b_{ji}^* b_{ji}]$$

Gracias a lo anterior, podemos obtener la probabilidad de acierto teórica como:

$$P_a = \sum_i Tr[b_{ii}^* b_{ii}]$$

y por lo tanto la probabilidad de error teórica como:

$$P_e = 1 - P_e = 1 - \sum_i Tr[b_{ii}^* b_{ii}]$$

2.3. Estado actual de las tecnologías cuánticas

En esta sección se analizarán las actuales líneas de investigación y aplicaciones de las tecnologías cuánticas (computación y redes) así como que países y organizaciones están invirtiendo más fuertemente en ellas.

2.3.1. Internet cuántico

Hoy en día la vida sin internet parece impensable. No obstante, hace no tanto, internet no era más que un proyecto de investigación. Actualmente las redes de comunicaciones cuánticas parecen estar en ese mismo punto. A pesar del largo camino que queda por delante, son muchas las personas que creen que una red totalmente cuántica al estilo de internet es posible. Al contrario de lo que se pudiese pensar, este internet cuántico no se imagina como un sustituto del internet actual sino como una red que abra la puerta a un sinfín de aplicaciones irrealizables hoy en día.

Esto es lo que modelan Wehner et al. en [13], quienes nos indican algunos ejemplos de estas futuras aplicaciones como por ejemplo votaciones ultra-seguras en elecciones o una mayor sincronización entre relojes además de los ya mencionados protocolos de distribución cuántica de claves. En esta misma publicación, ante la ausencia de un criterio global común, se modela la red como la conjunción de tres elementos bien diferenciados:

- Canales cuánticos.
- Terminales u ordenadores cuánticos.
- Repetidores cuánticos.

Los cuales en su conjunto, tal y como se indica en el propio artículo, presentan dificultades claras.

Los canales cuánticos (fibra óptica o espacio libre) atenúan el estado cuántico transmitido al igual que hacen con las señales físicas transmitidas en las comunicaciones clásicas. No obstante, en un sistema cuántico no podemos introducir un repetidor donde tomamos la señal a la entrada y transmitimos una copia de la misma amplificada a la salida tal y como hacemos en los sistemas de comunicaciones clásicos. Esto se debe al teorema de

no clonación, que como vimos anteriormente nos dice que es imposible copiar un estado cuántico ya que el propio hecho de medir el estado a la entrada lo modificaría, por lo que no sabríamos a ciencia cierta el estado recibido y por consiguiente no podríamos duplicarlo. Es evidente que los dispositivos que hagan esta tarea en las redes cuánticas deben diseñarse de una manera radicalmente opuesta a como se plantean en las comunicaciones clásicas.

Otro de los problemas en el artículo dado es el desarrollo de ordenadores cuánticos potentes que sean capaces de preparar y medir varios qubits (hasta ahora nos hemos referido a ellos como estados cuánticos) de manera simultánea. Ésta es la línea seguida por Caleffi et al. [14], quienes descomponen en su artículo el reto de crear una red cuántica global en tres pasos claros donde analizan además las principales dificultades de cada una de estas etapas:

1. Interconectar varios procesadores dentro de una misma computadora cuántica. Se plantea la necesidad de desarrollar protocolos de "routing" y direccionamiento para este propósito. No obstante, tal y como se nos indica en el artículo, los distintos procesadores están siempre en el mismo lugar, por lo que los protocolos a desarrollar no parecen el mayor reto en el internet cuántico.

2. Interconectar varios ordenadores cuánticos dentro de una misma organización. Como es lógico pensar, dentro de una organización ya no tendremos una topología de red fija, por lo que será necesario diseñar otros protocolos de direccionamiento y encaminamiento ("routing") algo más complejos. Además, en esta red organizacional aparecerán nodos con distintas funcionalidades y cuyas interacciones también será necesario gestionar.

3. Interconectar redes cuánticas de distintas organizaciones entre sí. Se indica como principal desafío la heterogeneidad de las redes, las cuales al estar operadas por distintas organizaciones puede generar dificultades debido al uso de diferentes protocolos entre ellas.

2.3.2. Computación cuántica

La computación cuántica representa otro de los principales atractivos de las tecnologías cuánticas. Aprovechando las leyes y propiedades de la mecánica cuántica, los ordenadores cuánticos son capaces de resolver problemas que serían inimaginables utilizando ordenadores tradicionales.

Algunos de los ejemplos más importantes de aplicaciones de la computación cuántica son:

- Factorización de grandes números.
- Aprendizaje automático cuántico.
- Generación de números verdaderamente aleatorios.

No obstante, tal y como exponen Orus et al. [15], la computación cuántica aún debe enfrentarse a una gran cantidad de dificultades.

Una de esas dificultades, según el artículo dado, es le decoherencia cuántica que es un fenómeno que hace que, debido a la interacción con su entorno, un qubit en superposición colapse a un único estado antes de la propia medida. Ésto limita las operaciones que puede hacer un ordenador cuántico con un qubit ya que, si no se realizan los suficientemenete rápido, la superposición de estados se desvanecerá. Ésto dificulta el desarrollo de ordenadores cuánticos.

No obstante, siempre según Orus et al., tenemos dos opciones para sobreponernos a la decoherencia. En primer lugar podemos hacer corrección de errores codificando el estado cuántico en más de un qubit aunque para que esto funcione, las puertas cuánticas que componen un ordenador cuántico deben tener una tasa de error muy pequeña. En segundo lugar utilizar los algoritmos NISQ (*Noisy Intermediate-Scale Quantum*), que son capaces de ofrecer mejores prestaciones que los ordenadores clásicos incluso con la presencia de decoherencia cuántica.

Factorización de grandes números

Uno de los grandes atractivos de la mecánica cuántica es la factorización de grandes números en tiempos claramente inferiores a los alcanzables por los ordenadores clásicos. Para ello, es muy común hacer uso del algoritmo de Shor, creado por Peter Shor, el cual nos ofrece una complejidad logarítmica dependiente del número de bits del número factorizado ($O(log(n))$) [16]. Sin embargo, el algoritmo de Shor ha sido utilizado para factorizar números hasta el 21 en la actualidad, por lo que de momento no ha habido una aplicación realista del algoritmo. No obstante, hay gran cantidad de artículos que muestran, de manera teórica, la clara ventaja de este algoritmo frente al más eficiente de los algoritmos clásicos.

Por ejemplo, en el artículo de Van Meter et al [17] se incluye una gráfica que muestra esta comparativa entre algoritmos clásicos y cuánticos la cual, vemos a continuación.

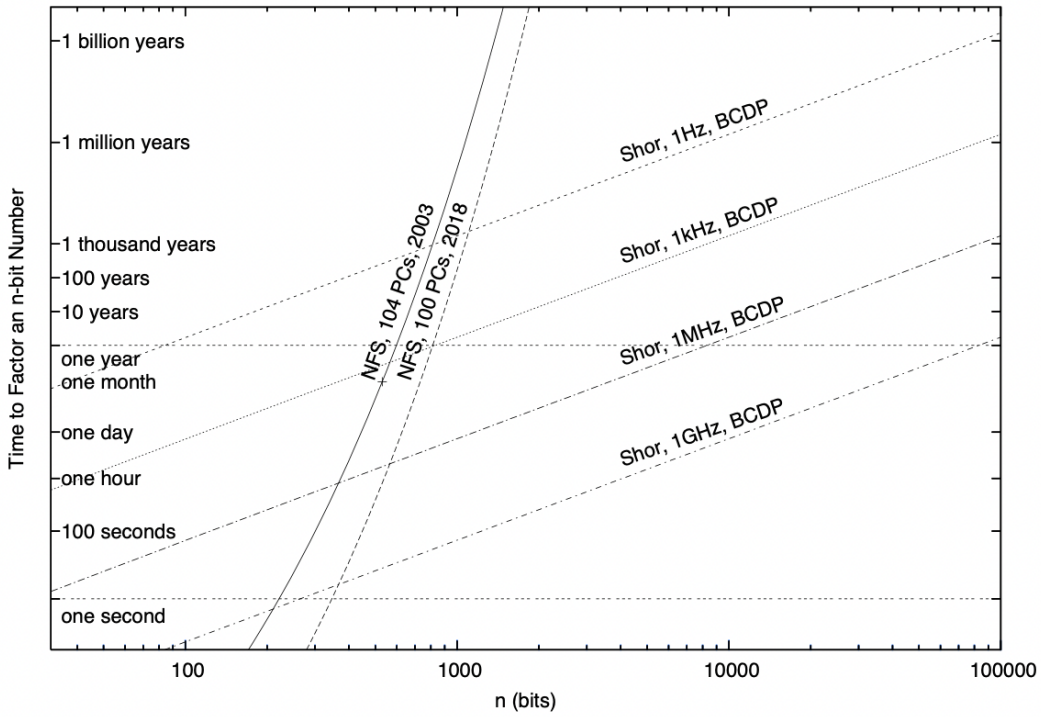


Fig. 2.8. Comparativa de algoritmos de factorización clásicos vs algoritmo de Shor [17]

Podemos ver que para un número de 1000 bits, los algoritmos clásicos tradarían más de 1 billón de años mientras que el algoritmo de Shor iría desde unos 50 segundos hasta 1000 años aproximadamente (dependiendo de la configuración utilizada).

Queda clara por tanto la gran oportunidad ofrecida, de manera teórica, por los algoritmos cuánticos frente a los clásicos. Por ello, parece algo lógico seguir la investigación en esta línea con el objetivo de poner estos mecanismos en práctica en aplicaciones realistas.

Aprendizaje automático cuántico

Una de las tareas más interesantes que puede llevar a cabo un computador cuántico es el QML (*Quantum Machine Learning*).

Tal y como explican Biamonte et al. en Nature [18] esto se debe a la capacidad de los ordenadores cuánticos de poder llevar a cabo operaciones como resolución de sistemas ecuaciones lineales en espacios de 2^n dimensiones o el cálculo de transformadas de fourier en tiempo polinómico en n.

Además, el artículo nos ofrece una tabla que nos indica el incremento de velocidad respecto a su contraparte clásica.

Method	Speedup	Amplitude amplification	HHL	Adiabatic	qRAM
Bayesian inference[106,107]	$O(\sqrt{N})$	Yes	Yes	No	No
Online perceptron[108]	$O(\sqrt{N})$	Yes	No	No	Optional
Least-squares fitting[9]	$O(\log N)$*	Yes	Yes	No	Yes
Classical Boltzmann machine[20]	$O(\sqrt{N})$	Yes/No	Optional/ No	No/Yes	Optional
Quantum Boltzmann machine[22,61]	$O(\log N)$*	Optional/No	No	No/Yes	No
Quantum PCA[11]	$O(\log N)$*	No	Yes	No	Optional
Quantum support vector machine[13]	$O(\log N)$*	No	Yes	No	Yes
Quantum reinforcement learning[30]	$O(\sqrt{N})$	Yes	No	No	No

Fig. 2.9. Aceleración de algoritmos cuánticos respecto a los clásicos [18]

La base para la resolución de sistemas de ecuaciones en espacios 2^n dimensionales es el algoritmos HHL, que tal y como podemos leer en el mismo artículo de Nature nos permite encontrar el $|x\rangle$ que resuelve:

$$A\,|x\rangle = |y\rangle$$

si A es cuadrada y todos sus autovalores son distintos de 0 y donde asumimos que A es hermítica.

En el caso de que A no sea cuadrada o tenga autovalores 0, el algoritmos HHL nos permite encontrar aquel ket $|x\rangle$ que hace mínima la expresión

$$|A\,|x\rangle - |y\rangle\,|$$

PCA cuántico

El PCA cuántico consiste en tomar los vectores de datos disponibles v_j y mapearlos a un estado cuántico $\left|v_j\right\rangle$.

Una vez hecho esto, obtenemos el operador densidad de todos los estados cuánticos obtenidos como:

$$\rho = \frac{1}{N}\sum_j \left|v_j\right\rangle\left\langle v_j\right|$$

Una vez obtenido ese operador densidad, según el mismo artículo de Nature [18], se calcula la exponenciación del operador densidad seguido del algoritmo de estimación de fase con el objetivo de obtener los autovalores y autovectores del operador densidad, consiguiendo expresar cada vector de datos en la forma:

$$\sum_k v_k\,|c_k\rangle\,|\hat{e}_k\rangle$$

donde $|c_k\rangle$ son las componentes principales de un vector de datos v cualquiera.

Support Vector Machines cuánticas

Una SVM es un método que lo que hace es encontrar un hiperplano capaz de separar varias categorías de tal manera que cada categoría este presente de manera única a cada lado del hiperplano.

En las SVM cuánticas el primer paso es, como en cualquier otro caso, introducir en el ordenador cuántico la información clásica. Una vez hecho esto, según [18], es necesario aplicar de nuevo *quantum phase estimation* (para obtener autovalores y autovectores) y el algoritmo HHL para invertir una matriz que será la que caracterice le hiperplano.

Segun el propio artículo disponible en Nature, encontrar el SV de N vectores nos lleva $\sqrt{\frac{N}{s}}$ iteraciones.

Generación de números verdaderamente aleatorios

La mecánica cuántica nos ofrece una solución a este problema aunque a priori puede parecer algo relativamente sencillo.

A veces acostumbramos a pensar que nuestros ordenadores son capaces de cualquier cosa, pero esto realmente no es así y la obtención de números aleatorios es una de esas tareas que son incapaces de acometer. Los ordenadores son máquinas deterministas que, para unas mismas entradas, generan unas mismas salidas. Cuando empleamos códigos que generan números aleatorios, aunque para nosotros puede parecerlo ya que cada vez obtenemos un resultado distinto, en realidad no es así, puesto que el ordenador puede coger como entrada un valor de su reloj interno por ejemplo, que cambia constantemente, por lo que el resultado también cambia constantemente.

Otra de las formas en las que suelen actuar los ordenadores convencionales es con una secuencia con un determinado periodo y, pasado ese periodo, los números "aleatorios" generados comienzan a repetirse.

Los ordenadores cuánticos nos ofrecen una alternativa para ello ya que, generando un estado en superposición, se puede conseguir que el resultado de la medida sea completamente aleatorio.

2.4. Aplicaciones más importantes de las tecnologías cuánticas hasta la fecha

2.4.1. Elecciones en Ginebra (2007)

En las elecciones federales de 2007, Ginebra fue pionera en el uso de tecnologías cuánticas al usar un protocolo de distribución cuántica de clave para hacer llegar los votos de los centros de conteo hasta la central donde se almacenaban. Ésto lo cuenta la empresa IDQuantique en su web [19] que, fue la encargada de proporcionar la tecnología necesaria. Además, según la propia empresa, sabemos que esta instalación se realizó con su dispositivo *Cerberis*, que era el encargado de asegurar el enlace. *Cerberis* proporcionaba

seguridad tanto de manera clásica con cifrado AES-256 como de manera cuántica utilizando la distribución cuántica de claves para llevar la clave de cifrado AES-256 a ambos extremos. Vemos un esquema de la instalación en la siguiente imagen.

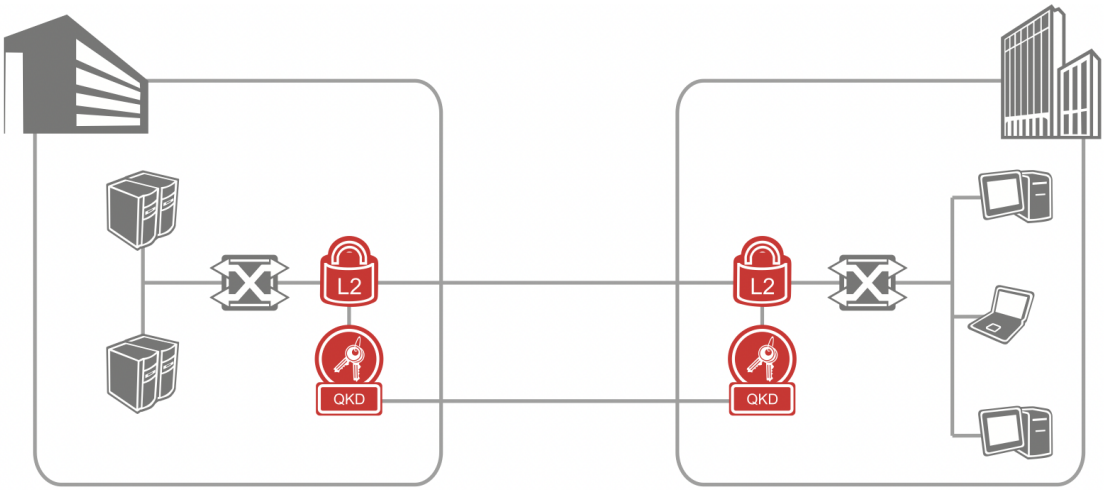


Fig. 2.10. Esquema de la instalación llevada a cabo por IDQuantique [20]

2.4.2. Satélite Micius (2016)

Una de las más famosas y recientes aplicaciones de las tecnologías cuánticas es el satélite Micius.

Según Yin et al. [21] el satélite fue lanzado en 2016 y desde entonces ha llevado a cabo una serie de experimentos.

Entre los que se comentan en el artículo anterior está la distribución de dos fotones entrelazados a dos ubicaciones terrestres separadas por 1200km. Se demostró que a esta distancia las partículas seguían estando entrelazadas.

También se implementó un protocolo de distribución cuántica de claves entre el satélite y una estación terrena así como la teleportación (la cual permite replicar un estado cuántico en otra ubicación con la ayuda de un canal clásico, pero **no** permite conocer el estado teleportado) de un estado cuántico al satélite.

Sin embargo, probablemente el uso más interesante de este satélite fue la videoconferencia llevada a cabo entre la academia de ciencias austriaca y la academia de ciencias china, separadas por 7600km utilizando las claves intercambiadas cuánticamente gracias a Micius en un protocolo VPN estándar. La conferencia duró alrededor de hora y media

según Amy Nordum en IEEE Spectrum [22]

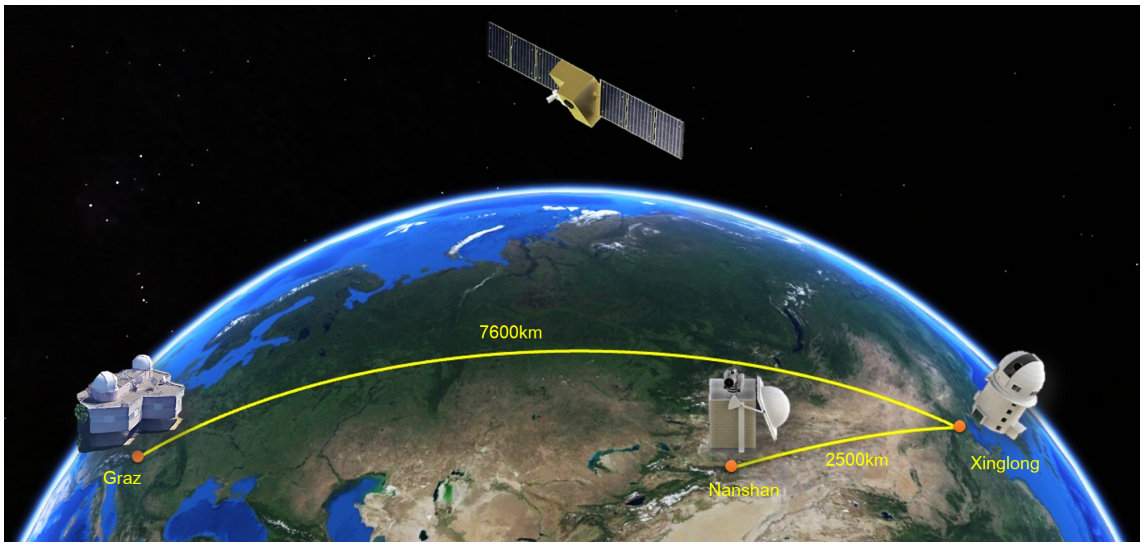


Fig. 2.11. Esquema de la transmisión entre China y Austria [23]

Podemos ver en la imagen anterior una conexión entre la estación terrena china en Xinglong hasta Nanshan. Esta conexión es terrestre y se realizó porque era en Nanshan donde estaban los participantes chinos en la videollamada.

2.5. Financiación de las tecnologías cuánticas

En esta sección se analizarán que países u organizaciones están apostando más fuertemente en el desarrollo de las tecnologías cuánticas. Este estudio se dividirá en, probablemente, los cuatro principales actores en esta materia:

- Union Europea.
- Estados Unidos.
- China.
- Reino Unido.

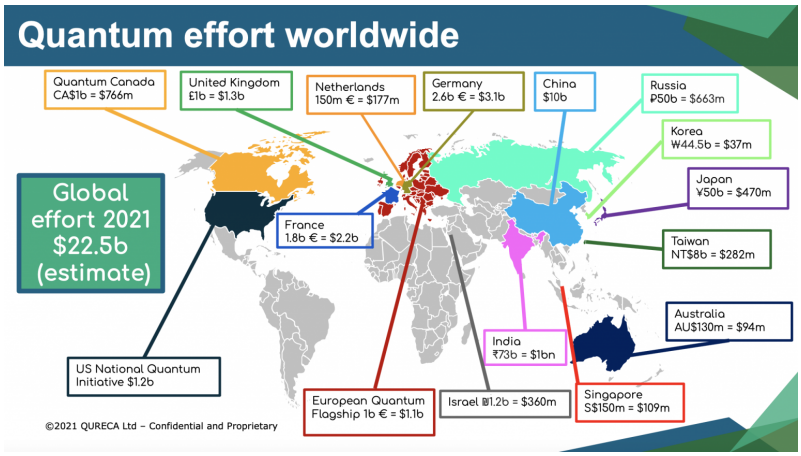


Fig. 2.12. Inversión estimada por regiones según QURECA [24]

2.5.1. Unión Europea

Al igual que en otras muchas áreas, la Union Europea tiene en marcha planes de financiación relativos a tecnologías cuánticas. De esta manera queda patente la gran importancia que tienen las aplicaciones de la mecánica cuántica en el futuro tecnológico de la Unión.

Esta iniciativa, denominada *Quantum Flagship*, si inició en 2018 con un presupuesto inicial de 1 billón de euros y con una duración prevista de más de 10 años, siempre según la propia pagina web que la UE ha habilitado para este *Quantum Flagship* [25]. En esta misma página web se indica que el principal objetivo es el de tener una red cuántica para (al igual que se dijo algunos apartados atrás) tener una capacidad de cómputo sin precedentes así como comunicaciones ultra seguras y una gran precisión en labores de sincronización y de medida.

Según la mencionada página, *Quantum Flagship* consiste, actualmente, en 24 proyectos de diferentes áreas como computación, comunicación o sensado y metrología.

2.5.2. Estados Unidos

De manera similar al *Quantum Flagship* de la UE, Estados Unidos también puso en marcha en 2019 un instrumento financiero, la *National Quantum Initiative*, con el objetivo de mantener a EEUU como uno de los líderes en el desarrollo de lo que denominan QIS, *Quantum Information Science*, es decir, todo aquello relacionado con la mecánica

cuántica y sus aplicaciones.

Se puede ver en el programa emitido por el NIST [26] el presupuesto para el año fiscal (FY) 2019 y para los años 2020 y 2021.

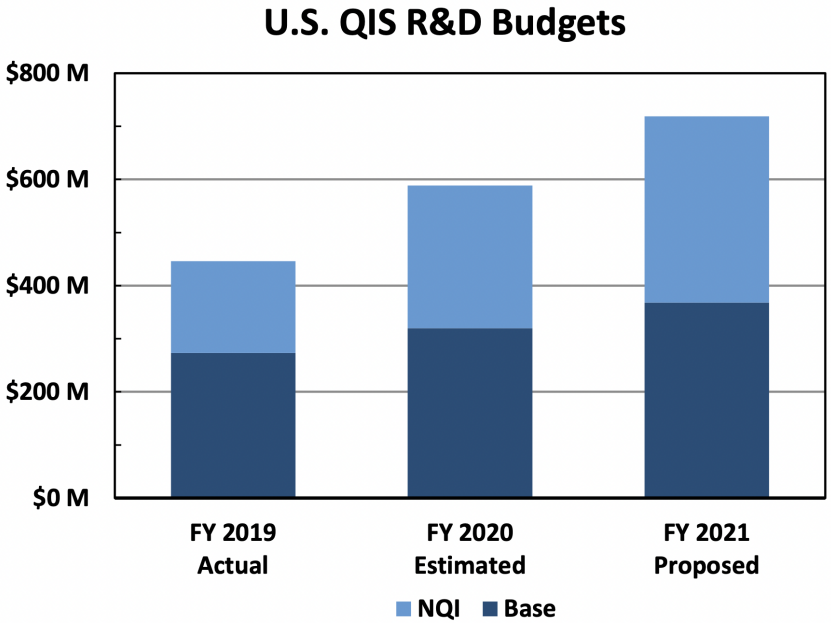


Fig. 2.13. Presupuesto para la investigación y el desarrollo en QIS [26]

Como podemos ver, el presupuesto es creciente en los años sucesivos. Además, se divide en lo que denominan como "*base*", que es lo dedicado por el gobierno de EEUU para unas líneas estratégicas básicas en lo referente a QIS; y lo que denominan como "*NQI*", que son los proyectos avalados por el programa a los que se da financiación, la financiación "atribuible" a NQI.

Estados Unidos focaliza su inversión en QIS en 5 áreas:

- *Quantum Sensing and Metrology* (QSENS): Estudia el uso de mecánica cuántica en lo referente a sensado y medida.
- *Quantum Computing* (QCOMP): Se centra en el estudio de los qubits así como en algoritmos y software para ordenadores cuánticos.
- *Quantum Networking* (QNET): Este área busca el despliegue de redes cuánticas y la búsqueda de nuevas aplicaciones que puedan surgir a partir de ellas.
- *Quantum Advancement* (QADV): Investigan aplicaciones para las que las tecnologías cuánticas puedan ser útiles.

- *Quantum Technology* (QTECH): Desarrollo de la infraestructura necesaria para la puesta en marcha de las tecnologías cuánticas. También se involucra en la solución de los peligros que pueda suponer el desarrollo de estas tecnologías sobre los sistemas actuales.

De nuevo, el propio programa emitido por el NIST nos proporciona una gráfica donde podemos ver la proporción de cada una de estas áreas en el presupuesto total visto en la anterior gráfica.

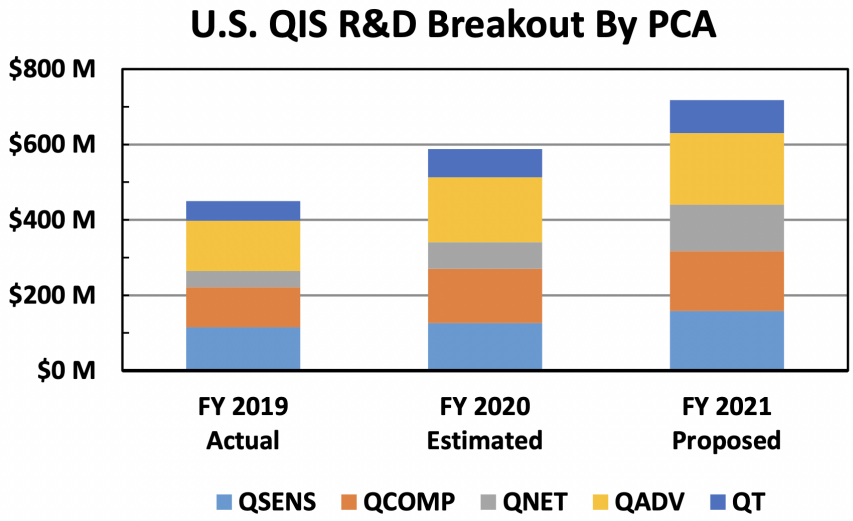


Fig. 2.14. Presupuesto para la investigación y el desarrollo en QIS (por áreas) [26]

Podemos ver como el principal área de inversión es el *Quantum Advancement* puesto que se busca en primer lugar averiguar la utilidad de todo aquello en lo que se investiga.

Tras esto, podemos ver que las dos áreas con mayor crecimiento en el periodo 2019 – 2021 son la computación y el *networking*, dejando patente que, con el paso de los años, la importancia que están tomando es creciente.

Recordemos que esta gráfica también recoge la inversión en QIS de EEUU por otros medios fuera de *Quantum Initiative*.

2.5.3. China

Obtener datos tan clarividentes con China al igual que hemos hecho con la Unión Europea y Estados Unidos es más complejo debido a la introvertida actitud del país asiático.

No obstante, se sabe que China tiene el objetivo de situarse como lider en tecnologías cuánticas, por lo que en lo que se conoce como “plan de 5 años” donde se incluye la mejora de la infraestructura cuántica y la creación de un laboratorio dedicado a tecnologías cuánticas (con una inversión inicial de 1000 millones de euros), tal y como podemos leer en el artículo de Elsa B. Kania [27].

No obstante, podemos tener alguna noción de la importancia de las tecnologías cuánticas para china en el articulo de Elizabeth Gibney en la revista Nature [28] donde encontramos la siguiente imagen.

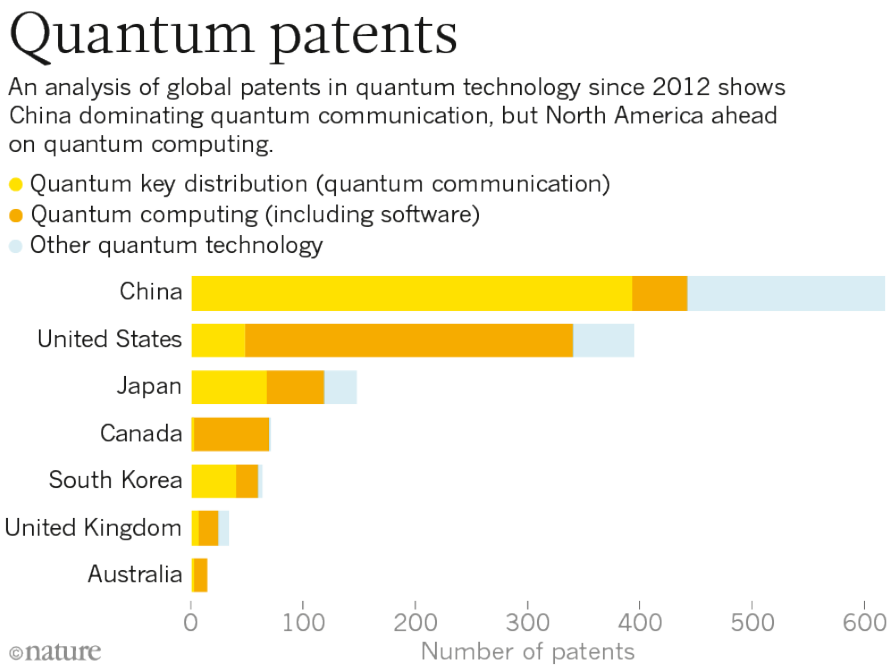


Fig. 2.15. Patentes por país en 2019 [28]

Podemos apreciar dos cosas muy interesantes. En primer lugar, el líder indiscutible en cuanto a número de patentes es China seguido de Estados Unidos. En segundo lugar, vemos que la mayoría de patentes Chinas son relacionadas con los sistemas de distribución cuántica de claves (QKD), es decir, tienen como objetivo la seguridad más que tener una mayor capacidad computacional que el resto de países.

2.5.4. Reino Unido

Reino Unido es otro de los países que más decididamente esta apostando por el desarrollo de las tecnologías cuánticas.

El Reino Unido puso en marcha en el año 2014 su NQTP (*National Quantum Technology Programme*) de 5 años de duración (hasta 2019) como indican Knight y Walmsley en su artículo [29].

NQTP tuvo un presupuesto inicial de 380 millones del libras. Una porción de este presupuesto se destinó a cuatro líneas de investigación bien marcadas y denominadas en el artículo antes citado como "hubs". Estos "hubs" de investigación, de los que formaban parte tanto universidades como organismos estatales o empresas privadas, son:

- Escáner.
- Sensado y medida.
- Comunicaciones.
- Computación y simulación.

El desglose de esos 380 millones de libras puede verse en la siguiente imagen.

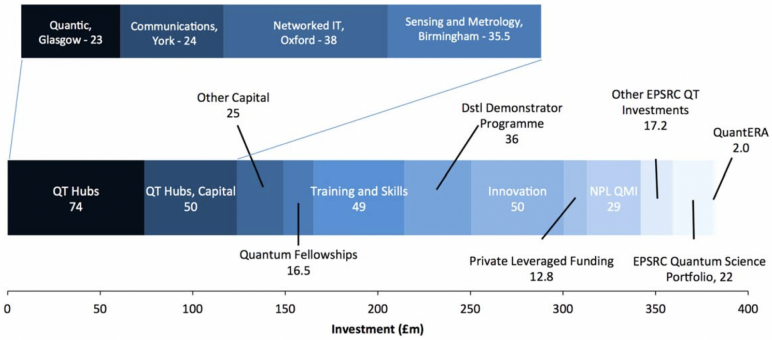


Fig. 2.16. Distribución de fondos del NQTP [29]

Tal y como indican Knight y Walmsley, todo lo anterior concierne a la primera fase del NQTP. La segunda fase, comenzó a finales de 2019 y forma parte del ISCF (*Industrial Strategy Challenge Fund*). De este fondo la parte destinada a tecnologías cuánticas es una dotación alrededor de 153 millones de libras.

3. OBJETIVOS

En el capítulo de desarrollo se cubrirán dos partes bien diferenciadas, cada una de las cuales nos pemitirá alcanzar una serie de objetivos relativos a la formación en las tecnologías cuánticas.

Sistema de distribución cuántica de clave

En primer lugar se expondrá el montaje y funcionamiento de un sistema de distribución cuántica de claves de la empresa THORLABS. Este montaje nos permitirá alcanzar los siguientes objetivos:

- Familiarizarnos con el montaje de un sistema básico de distribución cuántica de claves.
- Conocer los componentes más esenciales de un sistema cuántico.
- Afianzar los conocimientos teóricos previamente adquiridos mediante su constatación con la realidad.

Emulador de un sistema cuántico de comunicaciones

Tras analizar los componentes y el funcionamiento del sistema de QKD, llegará el turno de del emulador de un sistema cuántico de comunicaciones. Este emulador nos permitirá:

- Mejorar nuestro nivel de programación en MATLAB, software que se ha sido muy utilizado durante el grado.
- Ser capaces de, a partir de unos conocimientos teóricos previos, trasponerlos a un código funcional que los aplique.
- Ver, de manera cualitativa mediante imágenes y audios, el efecto que tienen agentes externos como la atenuación o el ruido térmico a una comunicación cuántica y clásica.
- Conocer las vulnerabilidades y fortalezas de los sistemas de comunicaciones cuánticos y clásicos.

- Reforzar los conocimientos referentes a sistemas clásicos desde un punto de vista diferente al abordado en los estudios de grado.

4. DESARROLLO

Tras la introducción teórica anterior, llegamos a la parte central de este trabajo, que consta de dos secciones bien diferenciadas como se acaba de ver:

- Un kit de distribución cuántica de claves.
- El emulador de un sistema de comunicaciones cuánticas.

4.1. Kit de distribución cuántica de claves

Para esta parte se realizó el montaje del *"Quantum Cryptography Kit"* de THORLABS como el que se muestra a continuación. Este montaje formó parte de una beca cursada en la Universidad Carlos III de Madrid por lo que se realizó junto a una compañera de la misma universidad.

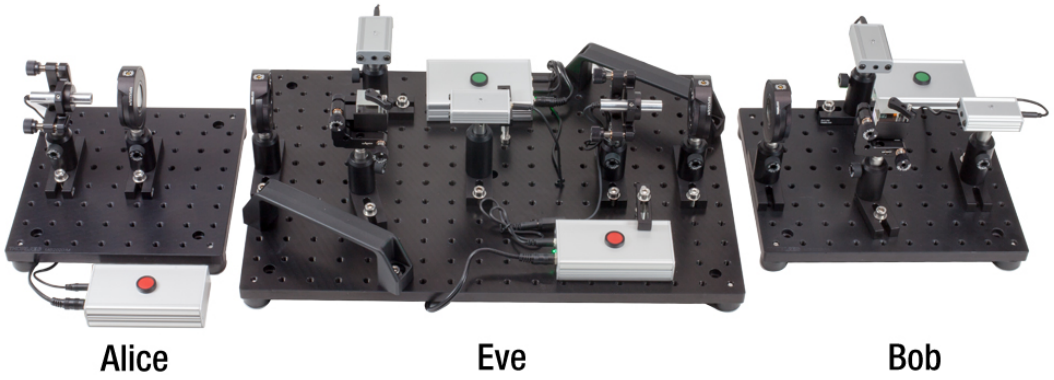


Fig. 4.1. Kit de distribución cuántica de claves [30]

Cabe destacar que no se trata de una transmisión puramente cuántica debido a que el láser empleado no es capaz de generar un **único** fotón. No obstante, el número de fotones generados es tan reducido que podremos apreciar los efectos de la mecánica cuántica sin problema alguno.

En esta sección se analizarán, en primer lugar, el conjunto de componentes del kit, explicando tanto sus características como la función que tienen cada uno de los elementos.

Para terminar, se mostrarán los resultados de las pruebas realizadas así como los principios de la mecánica cuántica que han podido ser comprobados.

4.1.1. Componentes del kit

Los componentes que conforman el kit de distribución cuántica de claves son:

- *Lasers*
- Polarizadores
- *Beamsplitters* o divisores de haz
- Detectores
- Pulsadores

Se explicará el funcionamiento de cada uno de estos elementos en sendos apartados.

Lasers

Los *lasers* son los elementos del kit que proporcionan los fotones. No obstante, estos fotones aún no han pasado por el polarizador, por lo que aún no transportan información.

Los *lasers* empleados son los *CPS635R-C2*, de 1,2mW. Estos *lasers* son de clase 2, que son aquellos que emiten en longitudes de onda correspondientes al espectro visible, concretamente los utilizados son $\lambda = 635nm$ (recordemos que el espectro visible va desde los $400nm$ hasta los $700nm$). Para utilizar este tipo de láser no son necesarias gafas de protección. No obstante, si es altamente recomendable tener cierta precaución porque, aunque poco probable, podrían producirse daños en el ojo.

Podemos ver el láser utilizado en las figuras 4.2 y 4.3.

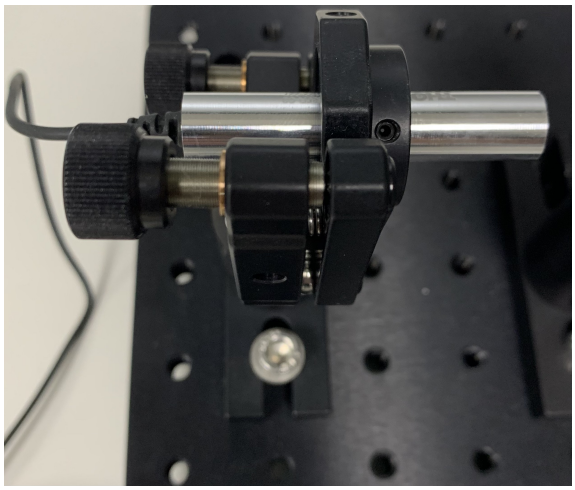


Fig. 4.2. *Laser* utilizado

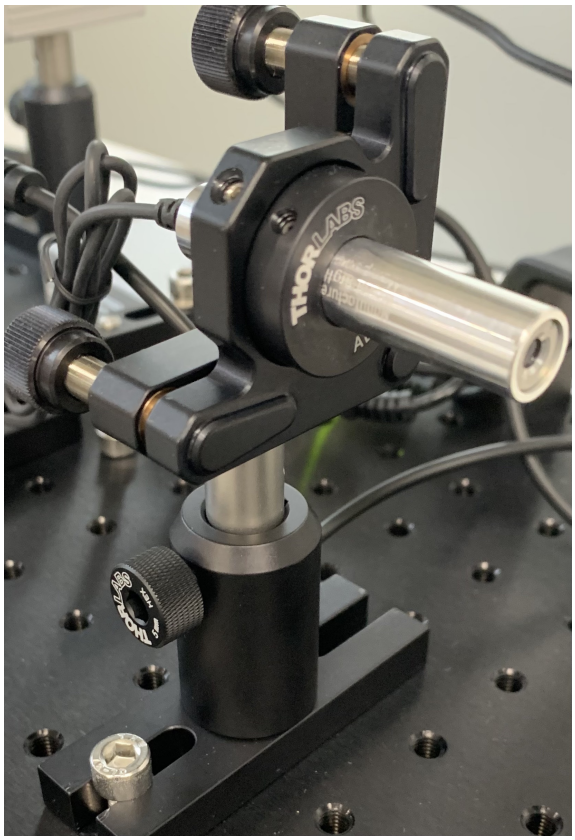


Fig. 4.3. *Laser* utilizado

Polarizadores

Los polarizadores son cristales que nos permiten inferir en los fotones transmitidos la información, los bits, que queremos enviar al otro extremo. Utilizamos láminas $\frac{\lambda}{2}$.

Los fotones generados por el láser no están polarizados, es decir, vibran, oscilan, en todas direcciones. Lo que hace el polarizador es únicamente dejar pasar una de esas direcciones, de tal manera que se polariza.

En función de la dirección que dejamos pasar, podemos elegir entre base "+" o base "×" y entre bit "0" ó bit "1". Para poder elegir la dirección, la lámina polarizadora se monta en una estructura que nos permite girarla. Podemos verlo a continuación.

Fig. 4.4. Lente polarizadora

Girando la estructura podemos polarizar los fotones de las siguientes formas:

- 0: Polarización en base "+". Se corresponde con el bit "0".
- 90: Polarización en base "+". Se corresponde con el bit "1".
- -45: Polarización en base "×". Se corresponde con el bit "0".
- 45: Polarización en base "×". Se corresponde con el bit "1".

Una lente idéntica se utiliza para elegir la base en la que queremos hacer la medida en el receptor. Para ello, al igual que cuando el objetivo es polarizar, montamos la lámina en una estructura que nos permitirá girarla para decidir si queremos medir en base "+" o en base "×". Podemos verlo a continuación.

Fig. 4.5. Lente receptora

Vemos como ahora únicamente tenemos dos posibles posiciones:

- 0: Medida en base "+".
- −45: Medida en base "×".

Beamsplitters o divisores de haz

El *beamsplitter* recibe cada conjunto de fotones y los direcciona a un detector u otro en función del estado cuántico de los fotones. Por ejemplo, si el estado de los fotones es

puro y representa un “0” con probabilidad 1, el beamsplitter dejará pasar los fotones. En cambio, si este estado es también puro pero representa un “1” (también con probabilidad 1), el *beamsplitter* reflejará los fotones a 90°.

De manera general, si en el polarizador y en la lente receptora utilizamos la misma base, el *beamsplitter* será capaz de discernir perfectamente entre “0” ó “1”, es decir, la probabilidad de medir un estado será 1 y la de medir el otro 0. No obstante, si las bases utilizadas son distintas, el estado que llega al divisor de haz es un estado en el que la probabilidad de obtener el bit “0” es 0,5 y la de obtener el bit “1” es 0,5. En otras palabras, aleatoriamente obtendremos “0” ó “1”. Veremos este efecto en la sección 4.1.2, correspondiente al experimento llevado a cabo con este kit.

Detectores

Los detectores nos permiten averiguar el estado medido. El *beamsplitter* dirige los fotones a un detector u otro y el que los recibe se ilumina. Lo vemos en la imagen 4.6.

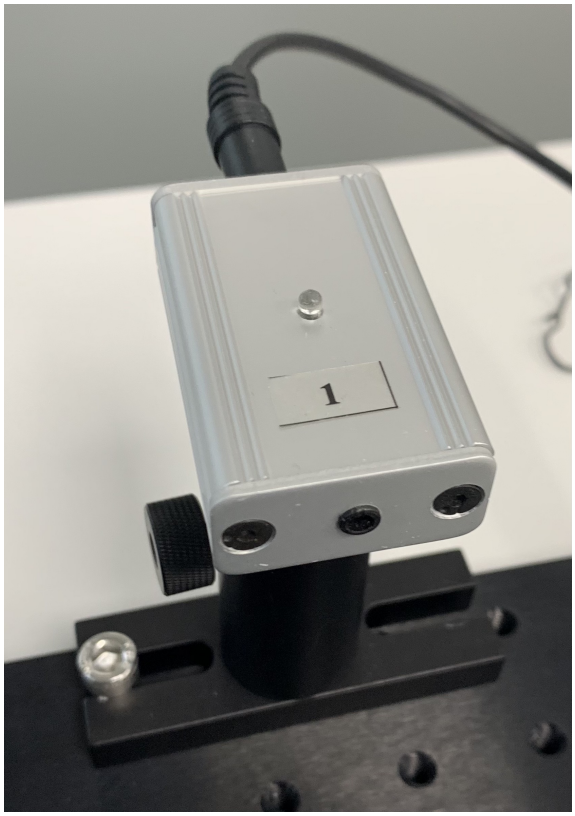


Fig. 4.6. Detector de fotones

Pulsadores

Simplemente nos permiten hacer que el láser emita fotones. Podemos hacer una pulsación corta o una larga.

Si hacemos una pulsación corta, el láser genera un haz de corta duración que nos permitirá emular la transmisión de un fotón.

La pulsación larga, por su parte, provoca un haz continuo que se utilizará primordialmente para ajustar y calibrar los componentes con el objetivo de que el haz que genera el láser entre correctamente en la apertura del detector.

4.1.2. Experimento con el kit de distribución cuántica de claves

Para llevar a cabo este experimento, el primer paso es, evidentemente, el montaje. El kit montado se muestra en la imagen 4.7.

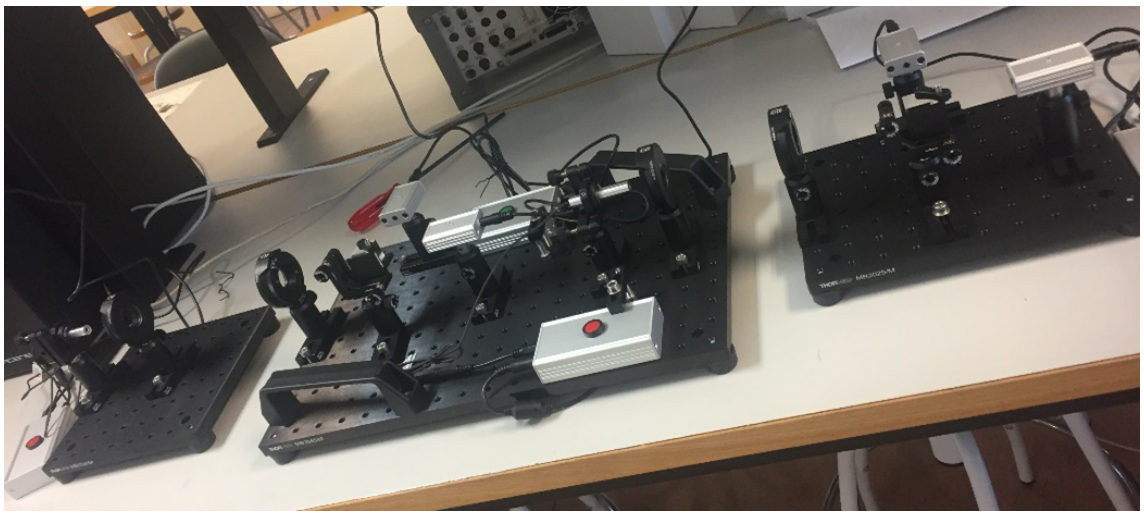


Fig. 4.7. Kit de distribución cuántica de claves (montado por nosotros)

Para este experimento, el transmisor elige diez bits aleatorios. Estos diez bits, serán transmitidos diez veces, para lo que cada una de las partes legítimas deberá elegir diez conjuntos de diez bases cada uno. Además, introduciremos una tercera parte, un espía, el cual utilizará siempre el mismo conjunto de bases y que se situará entre los extremos legítimos.

En la siguiente imagen, mostramos los conjuntos de bases elegidos por el extremo

transmisor, al que llamaremos Alice.

ALICE	1	2	3	4	5	6	7	8	9	10
BASIS 1	+	+	+	X	X	+	X	+	X	X
BASIS 2	+	X	+	X	X	X	+	+	X	X
BASIS 3	+	+	X	+	+	+	X	X	X	+
BASIS 4	+	X	X	+	X	+	+	X	X	+
BASIS 5	+	X	X	+	+	X	+	X	X	+
BASIS 6	+	+	X	+	+	X	X	+	X	+
BASIS 7	+	+	X	+	X	X	X	+	X	X
BASIS 8	+	X	X	+	X	+	X	+	+	+
BASIS 9	+	X	X	+	+	+	+	+	X	+
BASIS 10	+	X	X	X	X	+	X	X	X	X
BITS	1	0	0	1	1	1	1	0	1	0

Fig. 4.8. Conjuntos de bases utilizados por Alice y secuencia de bits transmitidos

Como podemos ver, Alice transmite los mismos diez bits utilizando diez conjuntos distintos de bases.

En la siguiente gráfica tenemos el conjunto de bases utilizado por el espía, al que llamaremos Eve, y los bits leídos en cada una de las diez transmisiones.

EVE	1	2	3	4	5	6	7	8	9	10
BASIS	X	X	+	X	+	+	+	+	X	X
READ 1	0	0	0	1	1	1	1	0	1	0
READ 2	0	0	0	1	0	1	1	0	1	0
READ 3	0	0	1	1	1	1	0	1	1	1
READ 4	0	0	1	1	0	1	1	0	1	0
READ 5	1	0	0	0	1	0	1	1	1	1
READ 6	0	0	0	1	1	0	1	0	1	1
READ 7	1	0	1	1	1	1	1	0	1	0
READ 8	1	0	0	0	0	1	1	0	1	1
READ 9	1	0	0	0	1	1	1	0	1	0
READ 10	1	0	1	1	0	1	1	0	1	0

Fig. 4.9. Conjunto de bases utilizado por Eve y secuencia de bits leídos en cada transmisión

En cada una de las transmisiones, el espía toma los diez bits leídos con su propio set de bases y, utilizando este mismo set de bases, los transmite al otro extremo legítimo, al que llamaremos Bob. Se representan en esta tabla a color verde o rojo aquellos casos

en los que Alice y el espía Eve utilizan bases distintas. Al utilizar bases distintas, hemos visto en la introducción que las medidas deberían ser 50 % correctas 50 % erróneas. Si analizamos caso a caso, podemos ver, por ejemplo, que para el primer bit donde se utilizan bases distintas siempre, la mitad de las medidas son correctas (verde) y la mitad erróneas (rojo). Además, si contamos todos los casos correctos y erróneos, llegamos a 30 medidas correctas y 24 erróneas de los 54 casos donde las bases elegidas difieren ($p_{acierto} = 0{,}55, p_{error} = 0{,}45$). Si bien no estamos justo en ese equilibrio 50 - 50, estas medidas nos demuestran como verdaderamente cuando las bases utilizadas son distintas, las medidas obtenidas son aleatorias. Además, podemos ver como aquellos casos en los que Alice y Eve utilizan la misma base, el bit medido por Eve es **siempre** el que Alice codificó.

Por último, en la siguiente imagen mostramos, para cada una de las diez transmisiones, el conjunto de bases utilizado y los bits leídos por el extremo receptor, Bob.

BOB	1	2	3	4	5	6	7	8	9	10
BASIS 1	X	X	+	+	X	+	X	+	+	+
READ 1	0	0	0	1	0	1	0	0	1	0
BASIS 2	X	X	X	+	+	X	+	+	+	+
READ 2	0	0	1	1	0	0	1	0	1	0
BASIS 3	X	+	X	+	+	+	X	X	+	X
READ 3	0	0	0	1	1	1	1	0	1	1
BASIS 4	+	+	X	+	+	X	X	X	X	+
READ 4	0	0	0	0	0	0	0	0	1	0
BASIS 5	X	+	X	X	X	+	X	+	X	X
READ 5	1	0	0	0	0	0	1	1	1	1
BASIS 6	+	+	+	X	+	X	X	+	X	X
READ 6	1	1	0	1	1	1	1	0	1	1
BASIS 7	X	X	X	+	+	+	+	X	+	X
READ 7	1	0	1	0	1	1	1	0	0	0
BASIS 8	X	X	+	+	X	+	X	+	X	+
READ 8	1	0	0	0	1	1	1	0	1	0
BASIS 9	+	+	+	X	X	+	X	+	+	X
READ 9	1	0	0	0	1	1	0	0	0	0
BASIS 10	+	X	X	+	X	X	X	X	+	+
READ 10	0	0	1	1	0	1	1	0	1	1

Fig. 4.10. Conjuntos de bases utilizado por Bob y secuencia de bits leídos en cada transmisión

Para cada una de las transmisiones, Alice y Bob intercambiarían sus bases (por un canal clásico), seleccionando aquellas en las que ambos han utilizado la misma. Estos casos aparecen coloreados en la imagen anterior en azul, verde o naranja.

Los casos marcados en azul son aquellos en los que tanto los extremos legítimos (Alice y Bob) como el espía (Eve) han utilizado la misma base. En estos casos, el bit que codifica Alice es el mismo que Bob lee ya que, a pesar de existir un nodo intermedio, las bases utilizadas son las mismas y por lo tanto no se introduce aleatoriedad tal y como se explicó en la introducción.

Los casos verdes o naranjas son aquellos en los que Eve tiene una base distinta a Alice y Bob. Dentro de ellos, se marcan en verde aquellos casos en los que el bit codificado en el fotón transmitido por Alice difiere del leído por Bob mientras que los naranjas indican que Bob lee el mismo bit que Alice codificó en el fotón.

Los casos verdes son, por tanto, aquellos que hacen posible que Alice y Bob puedan descubrir la presencia del espía ya que ambos utilizan la misma base pero el bit que tienen es distinto, por lo que se dan cuenta de que entre ellos hay una aleatoriedad que, a priori, no debería existir gracias a la elección de bases.

Evidentemente, para tener la posibilidad de detectar a Eve, Alice y Bob deberían intercambiar, además de las bases, algunos de los bits transmitidos. Los bits que además de las bases se intercambian dependen del protocolo de distribución cuántica de claves empleado. En el capítulo de introducción ya se definieron algunos de estos protocolos.

4.2. Emulador de un sistema de comunicaciones cuántico

En este emulador, tomaremos una entrada y la manipularemos emulando su transmisión por un sistema de comunicaciones. No obstante, esta manipulación será doble. Por un lado, las modificaciones llevadas a cabo serán acordes a la mecánica clásica (emulador de un sistema clásico de comunicaciones). Por otro lado, estas modificaciones serán fieles a la mecánica cuántica (emulador de un sistema cuántico de comunicaciones).

En la última fase de la emulación, se mostrará al usuario la misma entrada, pero con la distorsión que se obtendría en los receptores de cada sistrema para que éste pueda comparar de manera subjetiva como afectan parámetros como el ruido térmico a cada uno

de los sistemas. Además, se mostrará por pantalla como parámetro de calidad objetivo la tasa de error obtenida para cada uno de los sistemas con el propósito de complementar de una manera equidistante la percepción inicial del usuario tras el análisis de ese "payload" de salida ya mencionado previamente.

Por ello, comenzaremos la sección con una breve explicación del código desarrollado. Analizaremos en primer lugar las entradas y salidas del programa para después mostrar los diagramas de flujo que lo rigen, donde podremos ver de manera sencilla la lógica del mismo.

Finalizaremos el desarrollo con algunas ejecuciones que nos permitirán comprobar el correcto funcionamiento del emulador. Para ello, compararemos los resultados obtenidos con resultados derivados de otras publicaciones contrastadas. También se extraerán, a la vista de estas ejecuciones, algunas conclusiones referentes a sistemas de comunicaciones clásicos y cuánticos.

4.2.1. Entradas y salidas

El programa desarrollado es capaz de tener en cuenta un número considerable de parámetros de entrada. En la imagen siguiente, se muestra la interfaz gráfica que permite al usuario introducir estos parámetros y lanzar la ejecución, así como la evolución de la BER en tiempo real mientras el código se ejecuta y un resumen con las tasas de error obtenidas para cada sistema al final de la transmisión.

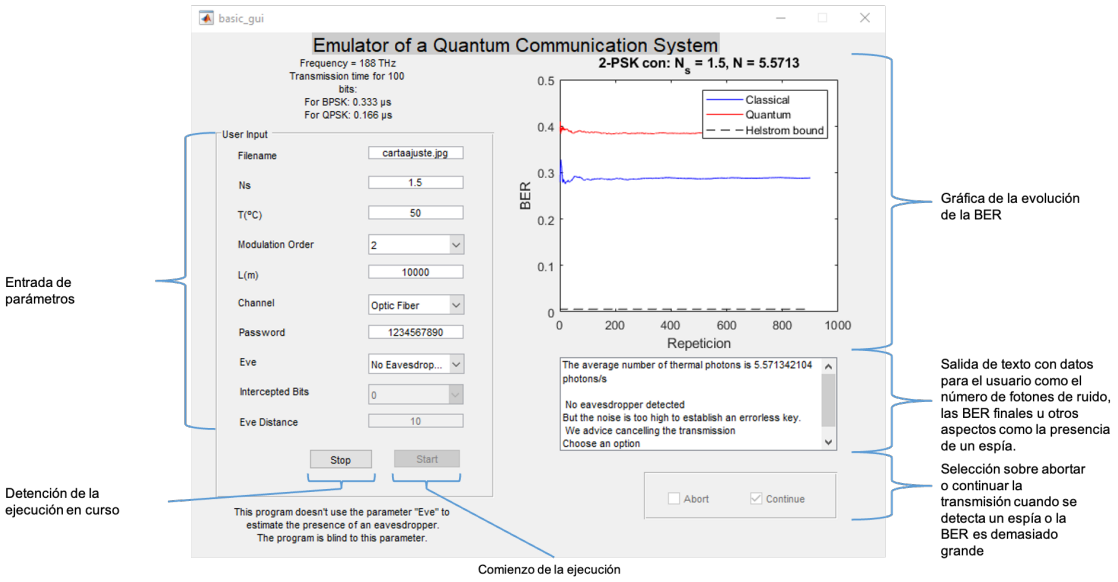


Fig. 4.11. Interfaz gráfica del emulador desarrollado

En cuanto a la gráfica de la BER, mostramos la tasa de error de bit de ambos sistemas durante la ejecución del emulador. Para ello, se calcula al final de cada repetición (conjunto de 100 bits) la tasa de error con todos los bits transmitidos hasta el momento (tanto los bits de la repetición actual como los de repeticiones pasadas). Podemos ver como al comienzo de la ejecución las BER de ambos sistemas oscilan mucho mientras que, a medida que avanza el numero de bits transmitidos, comienzan a converger. Ésto se debe a que, evidentemente, cuando el número de bits transmitidos es pequeño, el efecto que tiene un bit erróneo sobre la BER será mucho mayor que cuando hemos transmitido muchos bits con anterioridad. Podemos verlo en números a continuación:

- 100 bits transmitidos y 1 erróneo: $BER = \frac{1}{100} = 0{,}01$
- 1.000.000 bits transmitidos y 1 erróneo: $BER = \frac{1}{1{,}000{,}000} = 0{,}000001$

Además de las BER, se muestra el límite de *Helstrom* que nos dice lo mejor que lo podemos hacer, la menor tasa de error que podemos obtener.

En esta sección se analizarán cada uno de los parámetros de entrada así como las limitaciones que puedan tener sus posibles valores.

Entrada o "payload"

La entrada, "payload" o carga útil es la información sobre la que vamos a emular la transmisión. Puede ser tanto una imagen como un audio. Evidentemente, al ser la modalidad de este trabajo escrita es inviable añadir audios, por lo que para las simulaciones realizadas al final de este capítulo únicamente se utilizarán imágenes. Sin embargo, se explicará como se lleva a cabo la conversión a unos y ceros tanto de imágenes como de audios.

Es necesario tener en cuenta que la duración de la simulación dependerá en gran medida de la resolución de la imagen que utilicemos, o de la duración si queremos trabajar con un audio como entrada.

Es decir, si tomamos una imagen con resolución $1920x1080$ (píxeles), tendremos $1920 \cdot 1080 = 2073600$ valores de rojo, 2073600 valores de verde y 2073600 valores de azul (descomponemos la imagen como RGB), por lo que tendríamos en total 6220800 valores a transmitir. Además, como veremos más tarde, representamos cada valor con 6 bits, por lo que deberíamos iterar 373248 veces (en cada iteración transmitimos cien bits del sistema clásico y otros cien bits del sistema cuántico). Si, en otro caso, utilizásemos una imagen con resolución $200x149$, las iteraciones se reducirían drásticamente hasta 5364, aproximadamente 70 veces menos que en el caso anterior. Por lo tanto, debemos tener cuidado con la imagen introducida porque, si no se presta atención a ésto, el programa podría estar en ejecución durante horas o incluso días.

Número de fotones de señal (N_s)

El número de fotones de señal N_s indica el número de fotones que en media emite nuestra fuente (un *láser* típicamente) durante un periodo de símbolo. Decimos en media porque un láser no emite fotones de manera equiespaciada en el tiempo.

Si, por ejemplo, estuviésemos empleando un periodo de símbolo $T = 1\ segundo$ y un valor $N_s = 1\ \frac{fotones}{simbolo}$, los fotones podrían emitirse como se muestra en la figura 4.12:

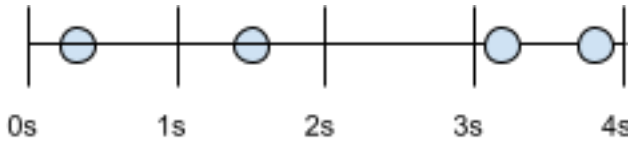


Fig. 4.12. Posible emisión de los fotones por parte del láser

Como ya hemos dicho este número de fotones es un promedio, el cual se cumple puesto que tenemos: $N_s = \frac{4 fotones}{4 segundos} = 1 \frac{foton}{segundo}$.

Es decir, los fotones no tienen por qué emitirse con un equiespaciado de 1 segundo exacto como se muestra en la figura 4.13:

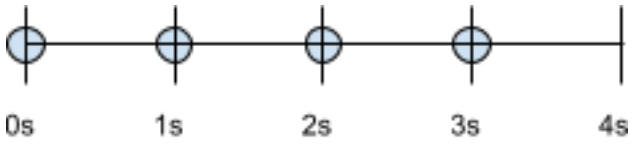


Fig. 4.13. Emisión no real de los fotones por parte del *láser*

Temperatura (T)

La temperatura (en $°C$) a la que trabajemos va a ser el parámetro que más nos va a permitir "jugar" a la hora de comparar ambos sistemas puesto que va a ser lo que determine la cantidad de ruido térmico que los afecta. Se van a aceptar valores de temperatura que van desde $-273{,}15°C$ (correspondientes a $0K$, la mínima temperatura posible) hasta $50°C$, donde ambos sistemas ya se encuentran saturados de ruido térmico.

Distancia del enlace (L)

La distancia del enlace va a determinar la atenuación introducida por el mismo, independientemente de si seleccionamos un canal de espacio libre o un canal de fibra óptica. En función de la atenuación y del ruido térmico, recomendaremos al usuario abortar la comunicación si la distorsión prevista es demasiado grande como para establecer una clave mutua entre ambos extremos sin errores. Por ello, no establecemos un limite superior a la distancia del enlace, será el usuario quien, a pesar de unas condiciones de transmisión desfavorables, decida si continuar o abortar la transmisión.

En cuanto al límite inferior, mientras que la transmisión sobre fibra no tiene (eviden-

temente, no permitimos valores negativos de distancia) para la transmisión en espacio libre sí se ha introducido una distancia mínima. Ésto se debe a que la atenuación en este tipo de canal (ver sección 2.2.3) aumenta con el cuadrado de la distancia, por lo que si permitiésemos distancia $0m$, tendríamos una potencia recibida infinita, lo cual no es simulable.

Debido a que en el canal en espacio libre la atenuación crece muy rápidamente, es necesario el uso de antenas que nos ofrezcan una ganancia que permita recorrer mayores distancias. Por ello, hemos empleado unas antenas de $1{,}5mm$ y $2mm$ de diámetro (lo cual no sería realizable en la práctica puesto que sería imposible alinearlas) cuyas ganancias permiten compensar la atenuación del espacio libre derivada de la transmisión a $10m$ de distancia. Ésta va a ser nuestra distancia mínima al trabajar con este canal. Ésto se debe a que una menor distancia implicaría que tenemos ganancia en la transmisión, lo que se modela como una transmisión empleando más fotones.

El problema viene de que la matriz que corresponde a un operador densidad que representa un estado cuántico tiene originalmente dimensión infinita y por tanto, para poder trabajar con estas matrices, debemos aproximarlo a una dimensión finita. Si trabajamos con un número pequeño de fotones (por ejemplo hasta 5 como se hace en el emulador) una matriz $30x30$ es suficiente para representar un operador densidad. No obstante, si quisiésemos representar el operador densidad correspondiente a un estado cuántico con $N_s = 30$ necesitaríamos una matriz de dimensiones aproximadamente $300x300$, lo que haría el código excesivamente pesado y lento. Por ello, si no se impusiese un límite inferior, podría darse una transmisión equivalente a emplear $N_s = 10$ (o valores superiores, claro), que haría que los resultados obtenidos del emulador no fuesen fiables al ser las matrices demasiado pequeñas y, por tanto, dejando de ser una buena aproximación.

Canal

La entrada “Canal” nos permite indicar si preferimos trabajar con un canal de fibra óptica o si por el contrario preferimos hacerlo en uno de espacio libre.

Espía

Nos permite indicar si queremos emular la presencia de un espía durante la distribución cuántica de claves. Tenemos tres opciones:

- "No eavesdropper": El intercambio de fotones durante el establecimiento de la clave de la comunicación está libre de espías. Los fotones salen de un extremo y llegan al otro sin pasar por un tercero ajeno a la comunicación.
- "Random": Existe un tercero que intercepta todos o una porción de los fotones intercambiados durante la distribución cuántica de claves. Como es aleatorio, éste alternará aleatoriamente entre base "+" y base "×" al medir el estado de cada fotón interceptado.
- "Best": En este caso también existe un espía que trata de "robar" bits de la clave, pero ahora siempre va a utilizar la base "+". Se denomina "Best" porque es lo mejor que le podría ocurrir a los extremos legítimos de cara a detectar que están siendo espiados. Esto se debe a que estará introduciendo mayor aleatoriedad ya que siempre que ambos extremos utilicen base "×" podrá ser detectado (tendrá base opuesta a ellos **siempre**) mientras que si el espía alterna entre las dos bases posibles habrá veces en las que éste esté utilizando base "×" también y por lo tanto en esos casos no tendrá efecto sobre la BER. Hay que destacar además que esta estrategia permitirá al espía obtener una mayor parte de la clave puesto que siempre va a medir en base "+" (Recordemos que estamos usando el protocolo BB84 *efficient*, explicado en 2.2.2).

Además, si decidimos emular la presencia de un espía, podemos indicar si queremos que intercepte todos los fotones intercambiados o sólo una porción de ellos, pudiendo elegir entre tres opciones:

- 0,1: interceptar aleatoriamente el 10 % de los fotones intercambiados.
- 0,5: interceptar aleatoriamente el 50 % de los fotones intercambiados.
- 1: interceptar el 100 % de los fotones intercambiados.

La opción de que el espía pueda no interceptar la totalidad de los fotones intercambiados sino una parte de ellos es muy interesante de cara a intentar robar la información de una comunicación. Como ya se ha explicado, cuando ambos extremos han empleado la base "×" para un mismo fotón éstos intercambian qué bit corresponde a ese fotón. Tras hacer esto para cada partícula se calcula la BER y, si está por encima de un determinado umbral, se avisa al usuario. Evidentemente cuantos más bits intercepte el espía mayor será la tasa de error obtenida, por lo que podría interceptar una parte de los fotones y simplemente dejar pasar el resto tratando de reducir su efecto sobre la BER y pudiendo pasar desapercibido. Es cierto que en este caso no tendría posibilidad de acceder a la totalidad de la clave, pero podría, a partir de la porción "robada" y los mensajes intercambiados, reconstruir la clave por completo.

Podemos ver la comparación entre entre ambas modalidades de espionaje y el efecto que tiene no interceptar todos los fotones sobre las veces que el espía es detectado en la figura 4.14, donde en este caso ambos extremos eligen sus bases de manera aleatoria, esto es, 50 % base "+" 50 % base "×" .

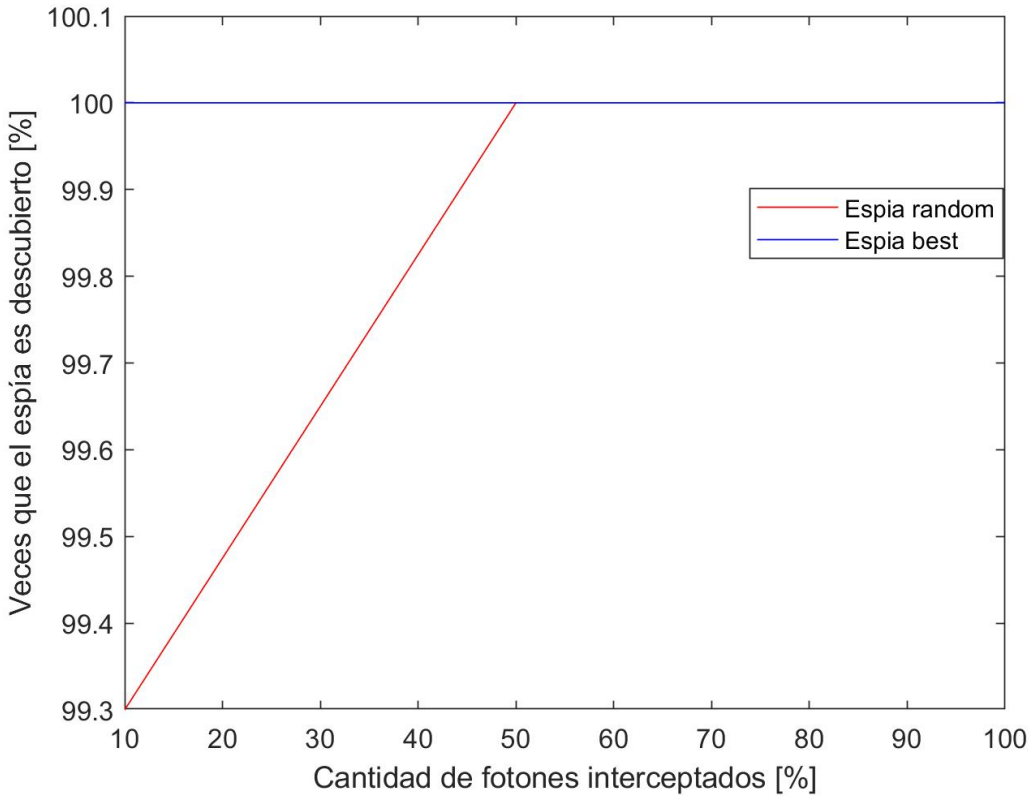


Fig. 4.14. Detección de espías vs. bits interceptados

Podemos ver que la diferencia es mínima, de un 0,7 %, pero demuestra lo comentado anteriormente.

4.2.2. Lógica del programa

En esta sección se mostrará la lógica de funcionamiento del emulador. Por simplicidad, en primer lugar se incluye un diagrama de flujo que refleja la lógica general del emulador y, en los apartados siguientes, los diagramas de flujo de aquellos procesos coloreados en la lógica general.

Esquema general

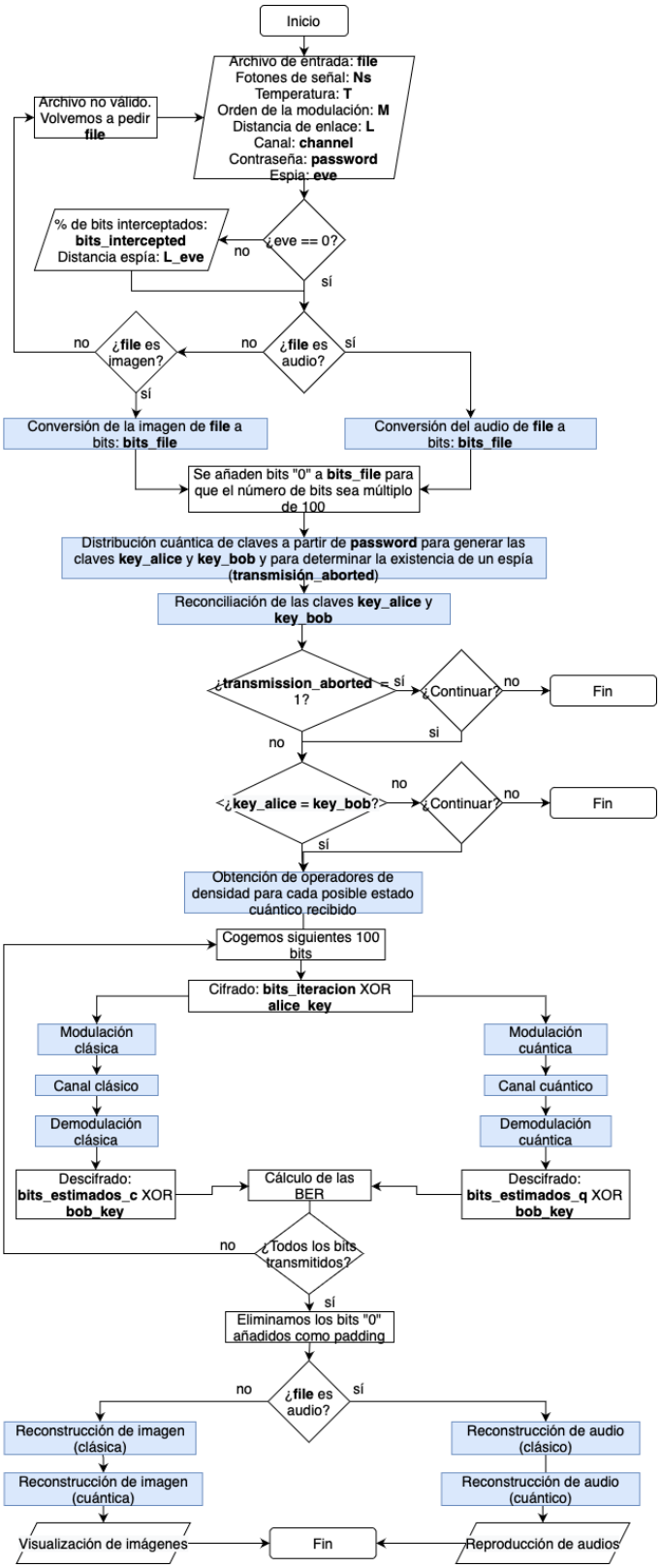


Fig. 4.15. Lógica general del emulador

Conversion de la imagen de "file" a bits

En la figura 4.16 podemos ver la lógica que sigue el emulador para convertir la imagen con nombre "file" a un vector de bits.

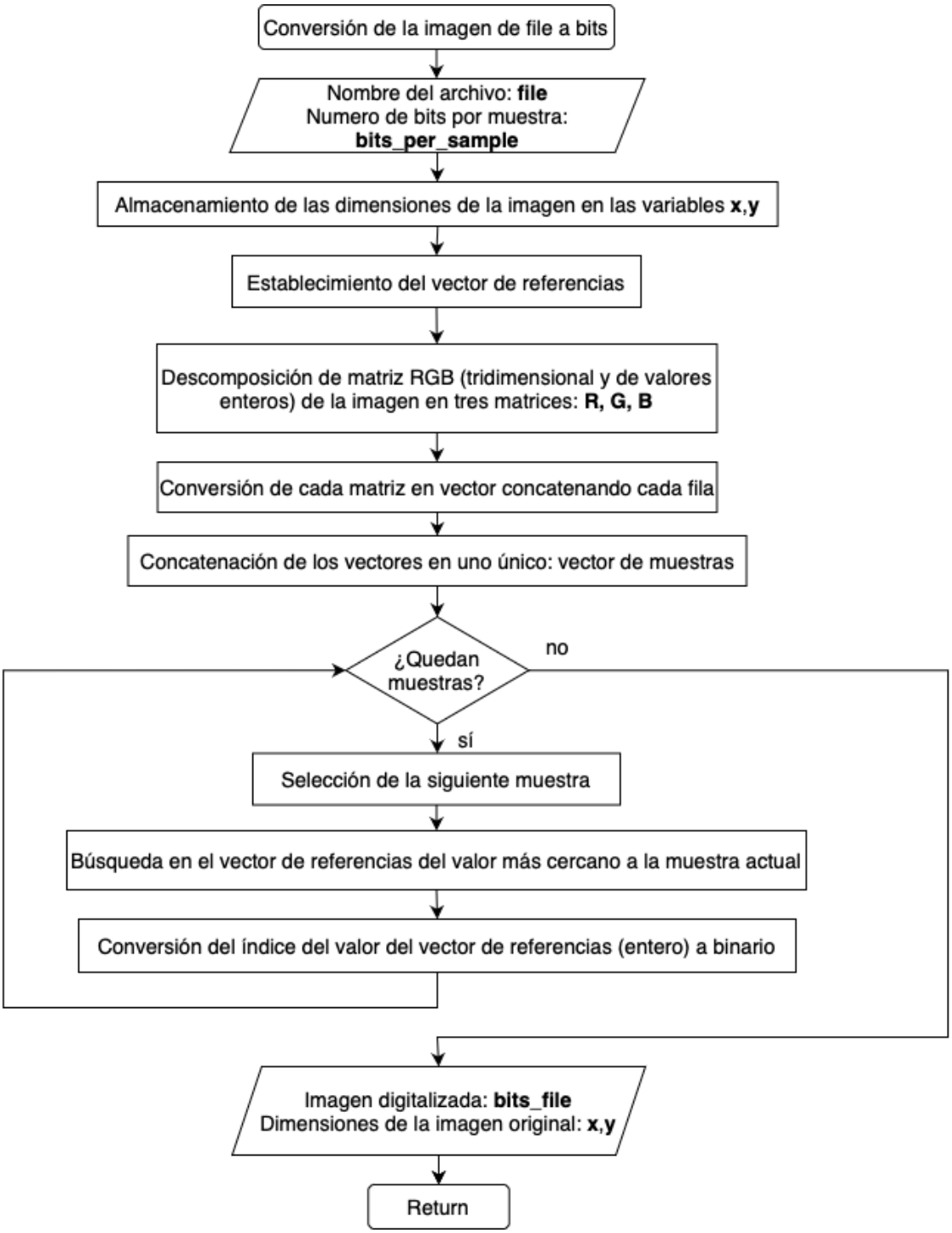


Fig. 4.16. Lógica de la conversión imagen - bits

En primer lugar, debemos almacenar las dimensiones de la imagen ($pixeles_{altura} x pixeles_{anchura}$)

para poder reconstruir la imagen correctamente tras la transmisión. Estas dimensiones se almacenan, como se puede ver en el diagrama de flujo, en las variables x e y.

En cuanto al establecimiento del vector de referencias, lo que hacemos es crear un vector cuyo primer valor es 0 y su último elemento vale 255 (cada muestra de la imagen leída es un entero de 8 bits) y donde el resto de elementos están equiespaciados y redondeados al entero de 8 bits más cercano (los valores equiespaciados en sí podrían no ser enteros) de tal manera que el vector obtenido tiene $2^{bits\_per\_sample}$ muestras enteras.

Con ello vamos a poder codificar en binario el índice de cada valor de la imagen (o el del más próximo) en el vector de referencias empleando un número menor de bits y mejorando así el tiempo de ejecución de nuestro código. En la práctica utilizaremos $bits\_per\_sample = 6$, de tal manera que el vector de referencias tendrá $2^{bits\_per\_sample} = 2^6 = 64$ posibles valores, por lo que cada una de las muestras de la imagen podrá ser codificada con sólo 6 bits.

Para terminar con la lógica de la conversión imagen - bits, se muestra en la siguiente imagen este mismo proceso de una manera más gráfica.

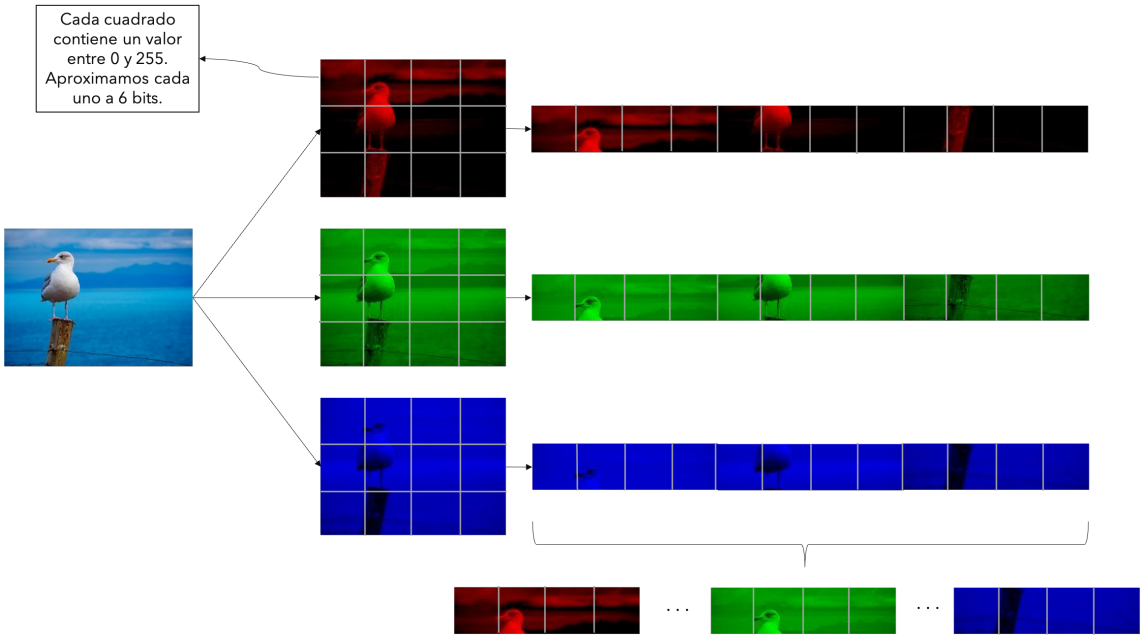


Fig. 4.17. Digitalización de una imagen

Es necesario aclarar que esos “cuadrados” son únicamente una representación, es decir, en la ejecución del código las porciones en las que se dividirá la imagen serán mucho más pequeñas.

Una vez hemos obtenido el vector que vemos en la parte inferior derecha de la figura 4.17, buscamos para cada "cuadrado" (cada uno es un único valor) el valor más próximo a él en el vector de referencias para, a continuación, hacer la conversión del índice de ese elemento del vector de referencias a binario, siendo la concatenación de los bits de cada muestra los bits a transmitir.

A modo de ejemplo, si el primer elemento del vector de muestras obtenido tuviese valor 130, buscaríamos en el vector de referencias qué elemento es más próximo a 130, obteniendo en este caso 129, que se encuentra en la posición 32 (si numeramos desde 0). Por tanto, la primera muestra de la imagen se codificaría como 100000_2.

Las salidas de la conversión imagen - bits serán la secuencia de bits obtenida y las dimensiones de la imagen original (x,y).

Conversión del audio de "file" a bits

En la figura 4.18 podemos ver la lógica que sigue el emulador para convertir el archivo de audio con nombre "file" a un vector de bits.

Como se puede apreciar en el diagrama de flujo, obtenemos los valores del audio haciendo un muestreo a una frecuencia f_s marcada por MATLAB. Para reducir la cantidad de valores obtenidos, lo que hacemos es un remuestreo con parámetros a y b, donde lo que se consigue es un vector con $\frac{a}{b}$ muestras por cada una del original. Es decir, si al leer el audio obtenemos diez muestras y los parámetros del remuestreo son son $a = 1$, $b = 5$ el nuevo vector de muestras contendrá dos valores.

En las ejecuciones del código los parámetros de remuestreo son $a = 1$ y $b = 10$. Al contrario de lo que se pudiese pensar, las muestras remuestreadas no tienen por qué coincidir con alguna de las originales ya que en el remuestreo existe una etapa de filtrado que puede hacerlas cambiar. En el contexto del ejemplo anterior esto quiere decir que las dos muestras obtenidas no tienen por qué ser dos de las diez originales.

Además, podemos ver que en la digitalización del audio también se genera un vector de referencias. La diferencia es que en este caso es necesario hacerlo (en el caso anterior lo hacíamos con el único objetivo de transmitir menos bits), ya que las muestras que obtenemos al leer el audio no son valores enteros (como sí lo son los índices del vector de

referencias) y, evidentemente, son necesarios para poder codificarlos en binario.

Para obtener este vector de referencias procedemos de igual manera que en la conversión imagen - bits, la única diferencia estará en que no será necesario redondear los valores del vector para obtener elementos enteros puesto que las muestras del audio tampoco son enteras.

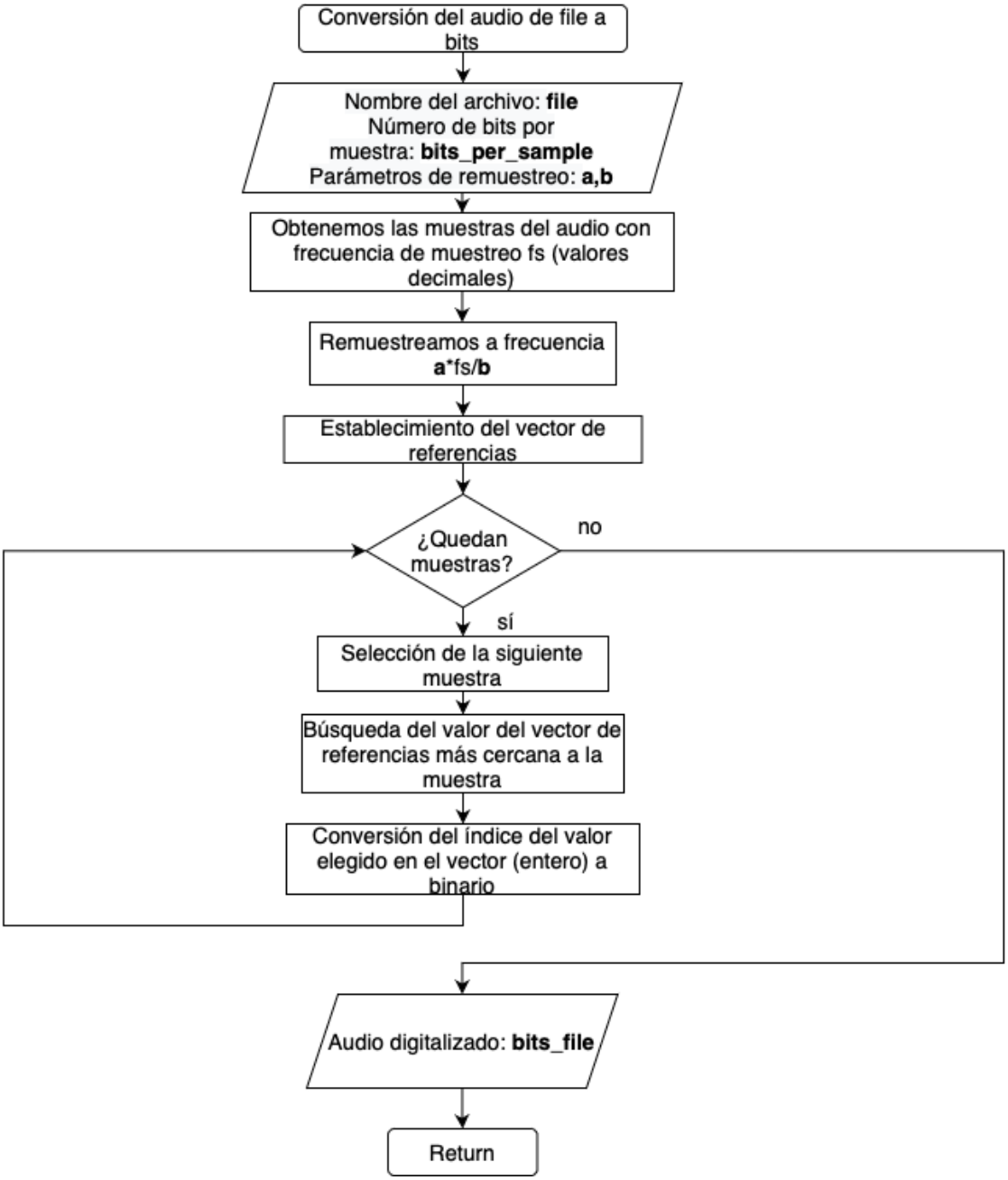


Fig. 4.18. Lógica de la conversión audio - bits

Una vez obtenidas tanto muestras como vector de referencias, podemos ver que el proceder es idéntico al de cuando la entrada es una imagen. Buscamos para cada muestra

el valor del vector de referencias más próximo a ella y codificamos en binario su índice, la posición (numerando desde 0), de este elemento. Una vez hecho esto para todas las muestras, los bits a transmitir serán la concatenación de los bits obtenidos para cada muestra.

Quantum Key Distribution (QKD)

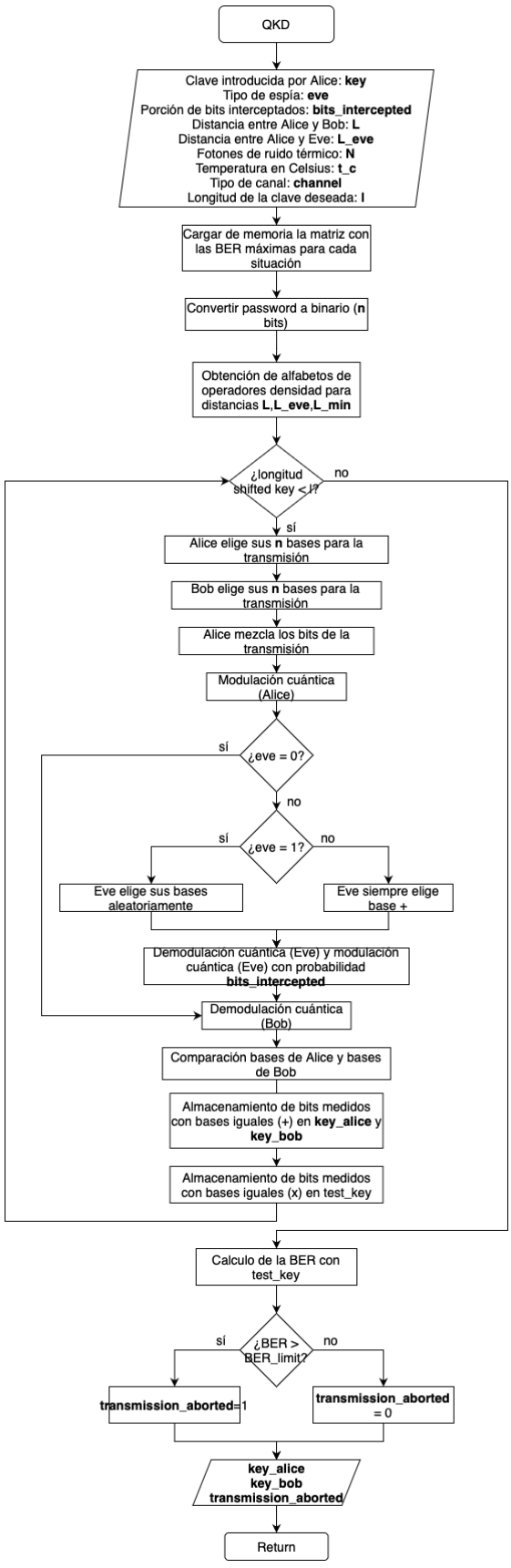


Fig. 4.19. Lógica del sistema cuántico de distribución de claves

La lógica del QKD se corresponde estrechamente con la teoría expuesta en el apartado 2.2.2 de la introducción.

Es necesario aclarar que en cada transmisión los bits iniciales son los mismos pero se hace una permutación pseudoaleatoria para no transmitirlos siempre en el mismo orden. No obstante, como no siempre los mismos bits pasan a formar parte de la *raw key* (solo se seleccionan aquellos para los que las bases de Alice y Bob coinciden), no sería estrictamente necesario hacer esa permutación inicial.

Además, utilizaremos unos operadores densidad u otros en función de la situación:

- Si $eve = 0$: Bob recibe los operadores densidad obtenidos para la distancia L.
- Si $eve = 1$: Con probabilidad $bits\_intercepted$, Eve recibe los operadores densidad obtenidos para la distancia entre Alice y Eve (L_{eve}) mientras que, para Bob, los estados cuánticos recibidos se representan mediante los operadores densidad calculados con L_{min} (asumimos canal ideal entre Eve y Bob). Con probabilidad $1 - bits\_intercepted$ Eve no actua y Bob recibe los estados cuánticos especificados por la distancia L.

Reconciliación de claves

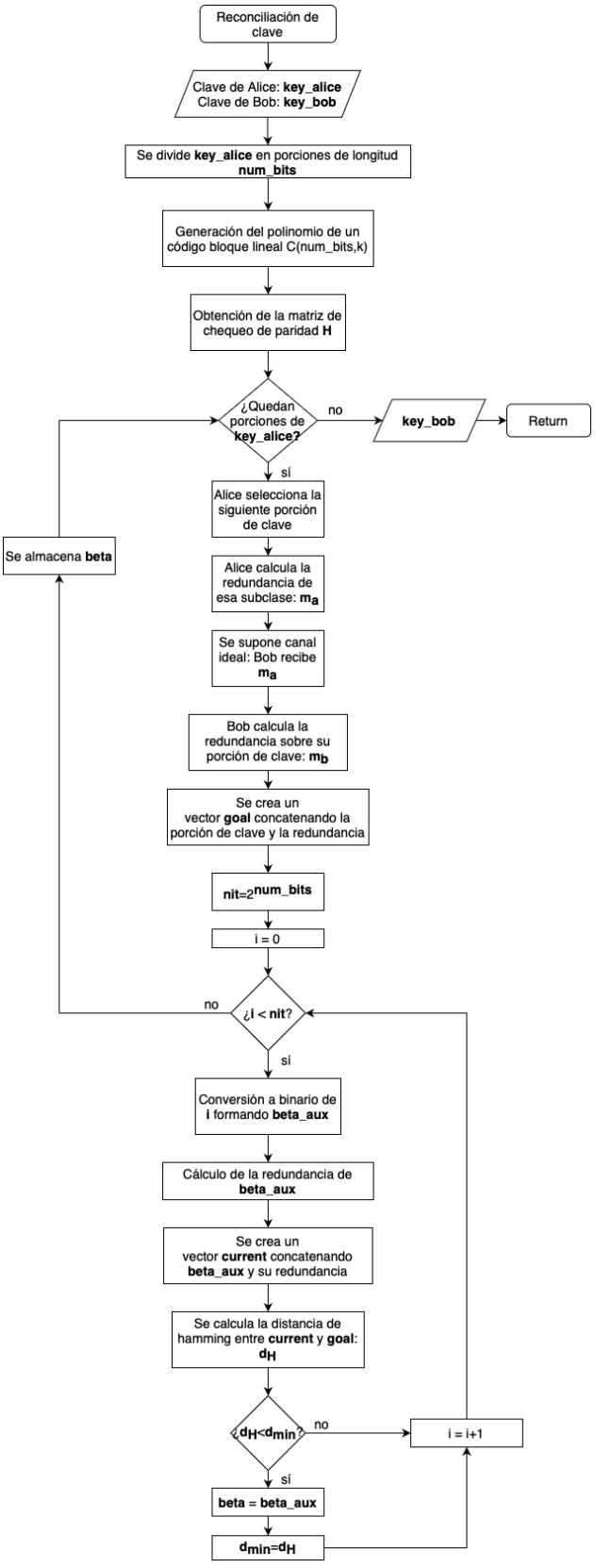


Fig. 4.20. Lógica de la reconciliación de clave

Debemos aclarar que en la lógica anterior, $C(num\_bits, num\_bits + k)$ indica un código bloque lineal en el que a partir de palabras de num_bits bits creamos palabras con $num\_bits + k$ bits.

Ademas, vemos como Bob recibe m_A idéntico al calculado por Alice. Esto se debe a que en la reconciliación de clave se asume un canal ideal sin errores y en ausencia de espías

Por último, *key_bob*, la clave "reconciliada" de Bob se forma por la concatenación de todas las "Beta" almacenadas.

Obtención de los operadores densidad de cada posible estado cuántico recibido

En la imagen de la figura 4.21 tenemos la lógica del emulador a la hora de obtener los posibles estados cuánticos recibidos a la salida del canal cuántico.

Podemos ver que lo primero que hacemos tras leer las entradas es, en función del orden de modulación, obtener la secuencia de bits que generará todos los posibles estados cuánticos ($bits\_alfabeto$). Si tenemos una modulación binaria ($M = 2$) sólo tendremos dos estados cuánticos que se corresponderán, evidentemente, con el bit "0" el primero y con el bit "1" el segundo (secuencia de bits "01"). Por otra parte, cuando tenemos una modulación cuaternaria ($M = 4$), cada estado cuántico codificará dos bits de manera simultánea, lo que hace que los bits que nos generan los cuatro posibles estados son "00", "01", "10", "11" (secuencia de bits "00011011").

El siguiente paso es calcular la atenuación introducida por el canal, ya estemos utilizando un canal de fibra óptica o un canal de espacio libre. Podemos ver que esta atenuación es calculada de manera idéntica a como se explicó en la sección 2.2.3 de la introducción.

Una vez tenemos la secuencia $bits\_alfabeto$ y la atenuación del canal, modulamos la secuencia $bits\_alfabeto$. El resultado será una secuencia de M números complejos, los símbolos, cuyo módulo al cuadrado recordemos que nos dirá el número de fotones que en promedio emitirá el láser en un periodo de símbolo para ese símbolo concreto. No obstante, al trabajar con modulaciones PSK, todos estos posibles números complejos están sobre una circunferencia, por lo que sus módulos serán iguales y por tanto el láser

emitirá el mismo número de fotones en promedio para cada estado, para cada símbolo.

Tras esto, para obtener la constelación de estados recibidos (sin tener en cuenta aún el ruido térmico) simplemente multiplicamos cada uno de estos estados (números complejos) por la atenuación. Ésto se debe a que en este emulador se modela la atenuación en potencia como una pérdida en el número de fotones promedio tal y como se estudió en el capítulo de introducción en la sección 2.2.3.

Una vez tenemos estos "nuevos" estados cuánticos producto de la atenuación del canal sólo nos queda "introducir" el efecto del ruido térmico. Para ello lo único que tenemos que hacer es crear los operadores densidad definidos por los complejos anteriores (γ') y por el número promedio de fotones de ruido (N) según se vio en las secciones 2.2.4 y 2.2.5.

Finalmente, la salida de esta función serán los operadores densidad calculados, los cuales constituyen el abanico completo de operadores que se podrían obtener a la entrada del demodulador.

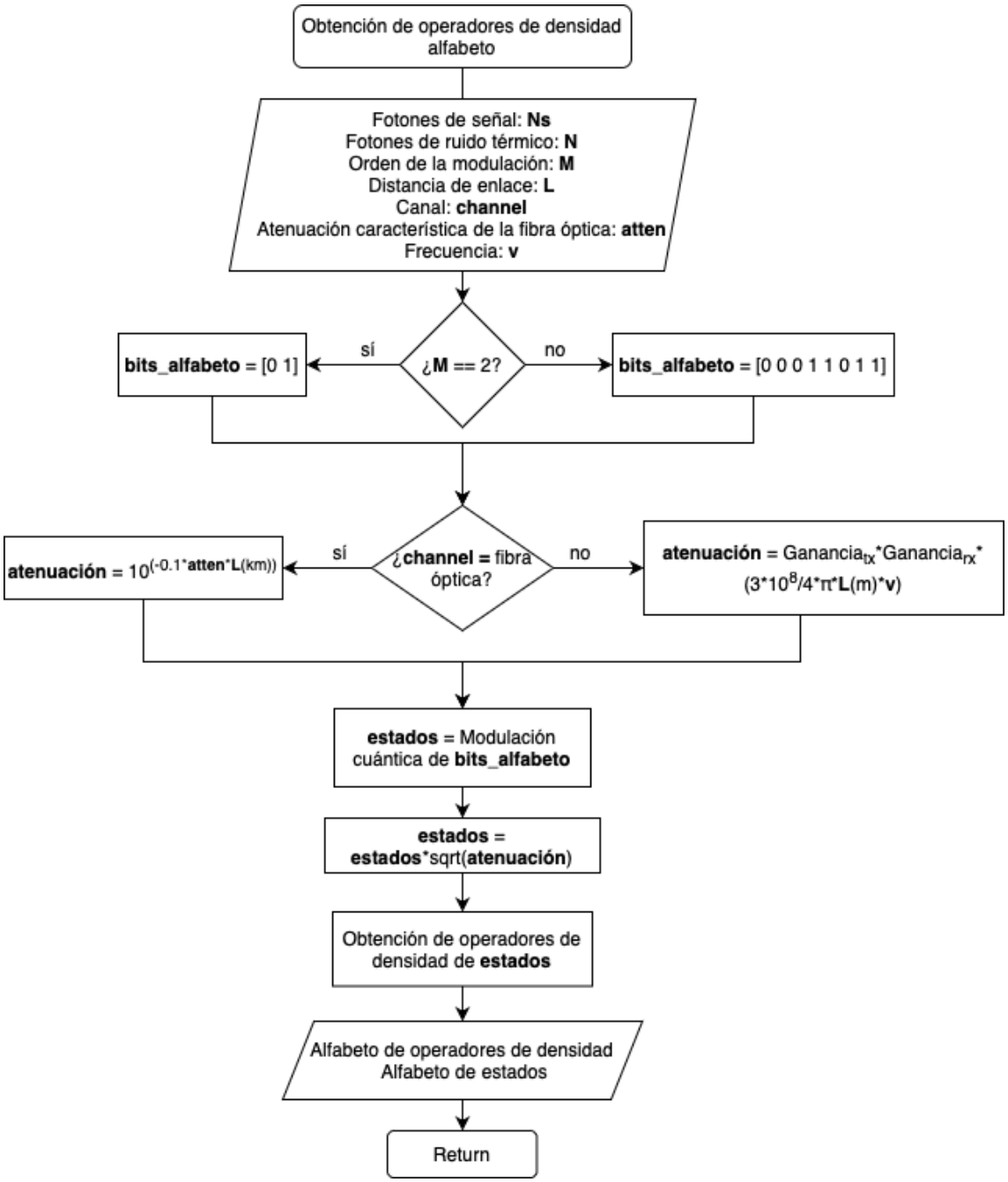


Fig. 4.21. Lógica de la obtención de los posibles operadores densidad

Modulación clásica

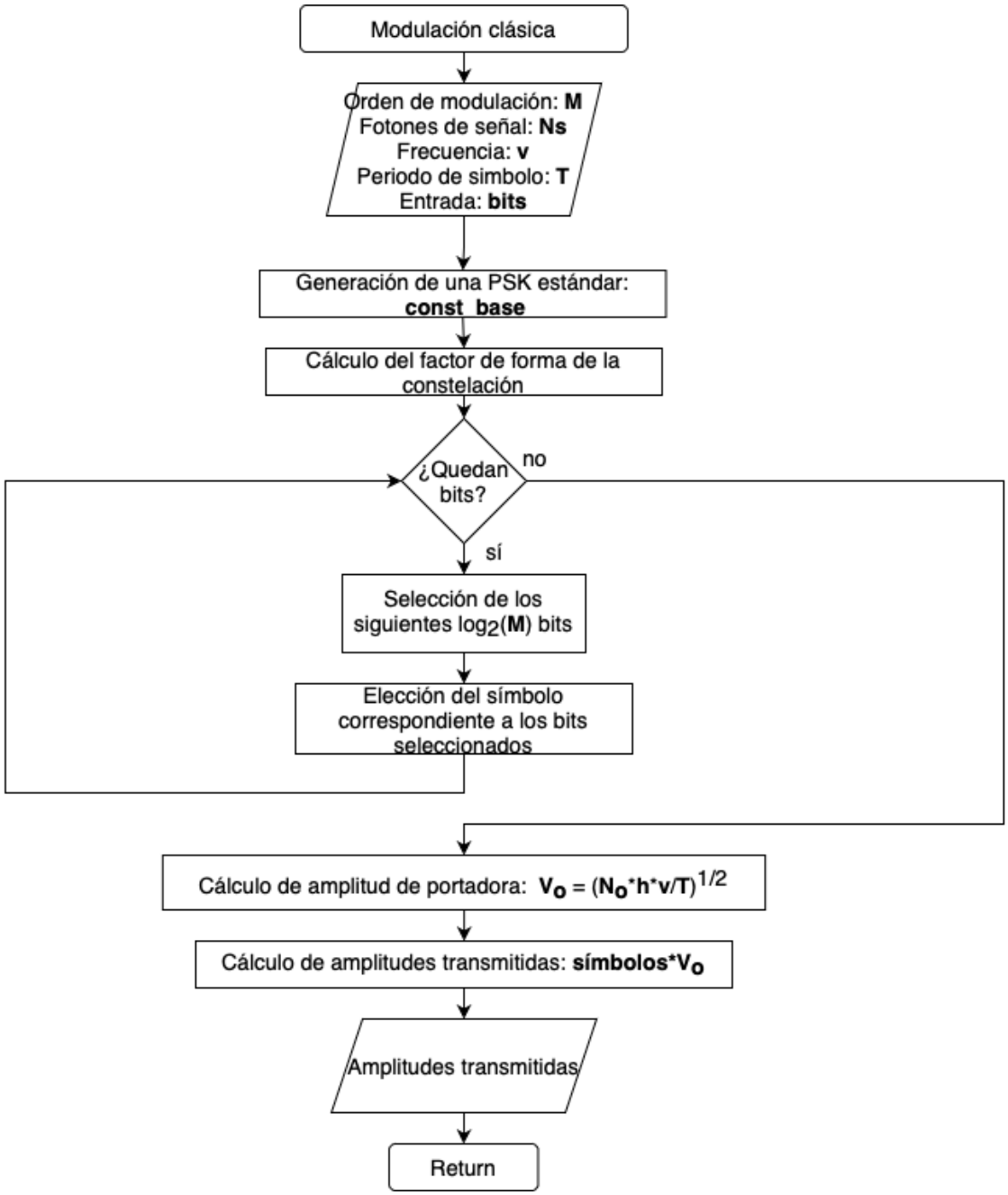


Fig. 4.22. Lógica de la modulación clásica

A la hora de modular de manera clásica, lo primero que hacemos es obtener una constelación PSK estándar, donde los símbolos se encuentran todos en una circunferencia de radio unidad.

Una vez tenemos esta constelación base, estándar, es necesario ir tomando los bits y, en función de su valor, asignar el escalar complejo correspondiente para obtener una

secuencia con los símbolos a transmitir. El número de bits seleccionados cada vez dependerá del orden de modulación. Si se emplea una modulación BPSK, los bits se tomarían de uno en uno, mientras que si se tratase de una QPSK, cada símbolo representaría dos bits de manera simultánea. De manera general, tomaremos los bits en grupos de $log_2(M)$ bits. (Si $M = 2$, $log_2(2) = 1$; si $M = 4$, $log_2(4) = 2$)

Una vez obtenida esta PSK estándar se obtienen las amplitudes de la onda que transmitiríamos para cada símbolo. Como vimos en la sección 2.2.5 de la introducción, primero calculábamos el factor de forma μ_M, después el número de fotones promedio de la portadora N_0 y finalmente la amplitud de la portadora como $V_0 = \sqrt{\frac{hv}{T} \cdot N_0}$. Terminamos de modular de manera clásica calculando el valor complejo transmitido simplemente multiplicando cada símbolo por la amplitud de portadora.

Ejemplo: $M = 4$ (QPSK), bits "00", $N_s = 1{,}5$, $v = 188THz$, $T = 3{,}33ns$

1. Obtenemos la constelación QPSK estándar formada por los símbolos $1, j, -1, -j$.
2. A los bits "00" les correspondería el símbolo 1.
3. Se calculan los fotones promedio de la portadora como $N_0 = \frac{N_s}{\mu_M} = \frac{1{,}5}{1} = 1{,}5$.
4. Se calcula la amplitud de la portadora como $V_0 = \sqrt{\frac{hv}{T} \cdot N_0} = \sqrt{\frac{6{,}626 \cdot 10^{-34} \cdot 188 \cdot 10^{12}}{3{,}33 \cdot 10^{-9}} \cdot 1{,}5} = 7{,}487 \cdot 10^{-6}$.
5. Se calcula el valor complejo "transmitido" $Valor_{tx} = simbolo \cdot V_0 = 7{,}487 \cdot 10^{-6}$.

Canal clásico

La lógica del canal clásico queda plasmada en la figura 4.23. Se trata de una de las funciones más sencillas del emulador. Únicamente calcula la atenuación de manera idéntica a como se explicó en la sección 2.2.3 y multiplica su raíz (recordemos que la envolvente compleja y la potencia se relacionan con la raíz) a cada uno de los valores complejos obtenidos de la modulación clásica resultando en los valores complejos recibidos ($valores_{rx}$).

Continuando el ejemplo del apartado anterior, donde obtuvimos $valor_{tx} = 7{,}487 \cdot 10^{-6}$, si tuviésemos un canal de $10km$ de fibra óptica cuya atenuación característica es $0{,}2[\frac{dB}{km}]$:

1. Se obtiene la atenuación como: $atenuacion = 10^{-0{,}1 \cdot 0{,}2 \cdot 10} = 0{,}63$

2. Se calcula el valor recibido como $valor_{rx} = \sqrt{atenuacion} \cdot valor_{tx} = \sqrt{0{,}63} \cdot 7{,}487 \cdot 10^{-6} = 5{,}945 \cdot 10^{-6}$

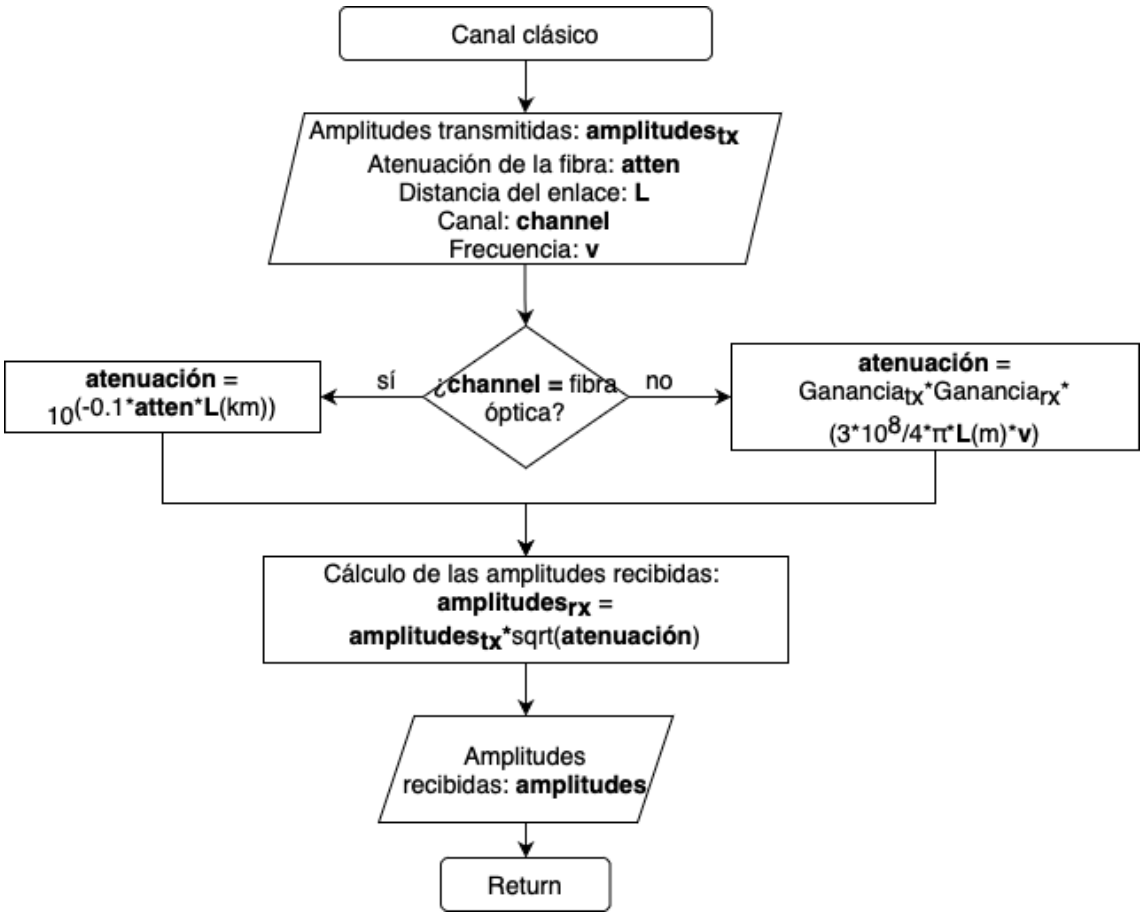


Fig. 4.23. Lógica del canal clásico

Demodulador clásico

La lógica del demodulador clásico apenas necesita de explicación adicional, puesto que simplemente es necesario seguir la explicación teórica de la demodulación coherente vista en la introducción.

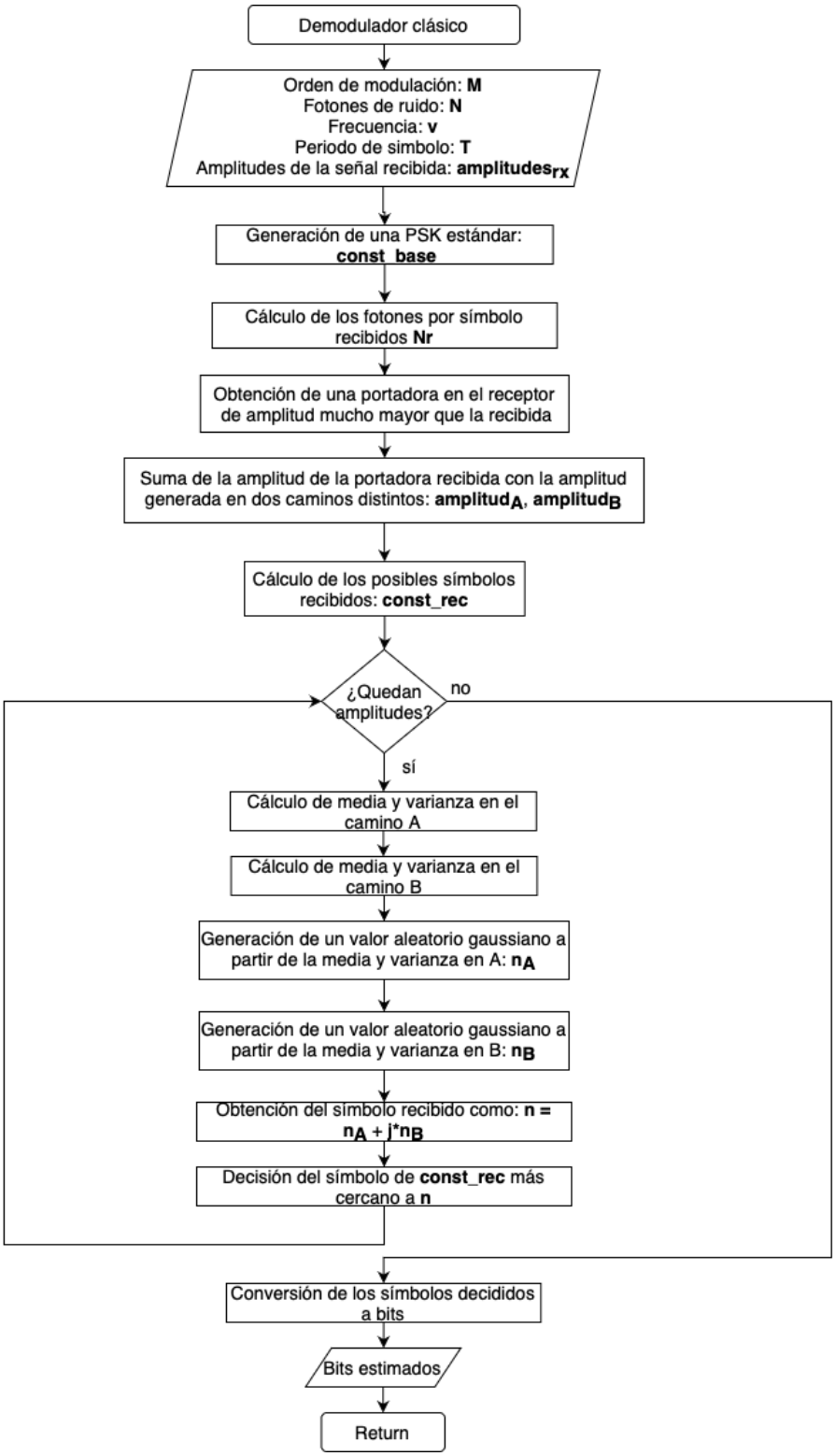


Fig. 4.24. Lógica de la demodulación clásica

Modulación Cuántica

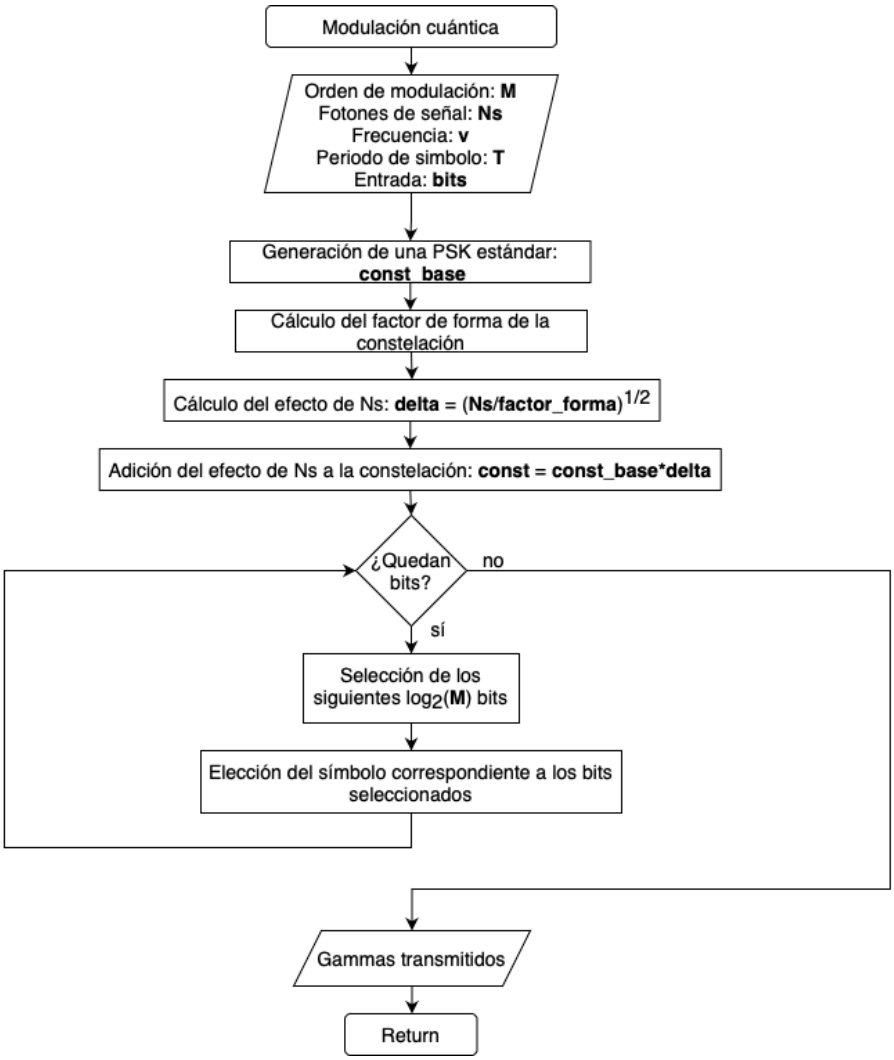


Fig. 4.25. Lógica de la modulación cuántica

La lógica de la modulación cuántica es muy similar a la de la modulación clásica. La principal diferencia es que la salida del modulador van ser simplemente los símbolos de una constelación PSK **no** estándar en lugar de las amplitudes de la señal transmitida para cada símbolo.

Lo primero que hacemos es, al igual que en la modulación clásica, generar una constelación PSK estándar, que como ya se explicó en la introducción significa que $\Delta = 1$, es decir que todos los símbolos se encuentran en una circunferencia de radio unidad y por tanto para cada símbolo tenemos $|\gamma|^2 = 1[\frac{fotones}{simbolo}]$. Esta constelación PSK evidentemente dependerá del orden de modulación empleado al igual que en el caso clásico.

A continuación, es necesario generar una nueva constelación que ya tenga en cuenta el efecto del N_s introducido como parámetro por el usuario, la constelación no estándar de la que estamos hablando. Como vimos en la introducción (2.2.5) debemos multiplicar la constelación base por un factor Δ que deriva de N_s y del factor de forma de la constelación, μ_M, como $\Delta = \sqrt{\frac{N_s}{\mu_M}}$. Como en una PSK el factor de forma es $\mu_M = 1$, obtenemos $\Delta = \sqrt{N_s}$.

Por tanto la constelación de los valores complejos que determinan cada posible estado cuántico transmitido quedaría como $const = const_{base} \cdot \sqrt{N_s}$

Una vez tenemos esta constelación, simplemente debemos ir tomando los bits a modular y asignar los símbolos correspondientes en función de su valor. Igual que en la modulación clásica debemos tomar más o menos bits en función del orden de la modulación, número de bits que seguirá estando determinado por la expresión $log_2(M)$.

La salida del modulador cuántico será la secuencia de valores complejos obtenidos de esa asignación bits - símbolo. Cada uno de estos valores complejos determinará por completo un único estado cuántico.

Canal cuántico

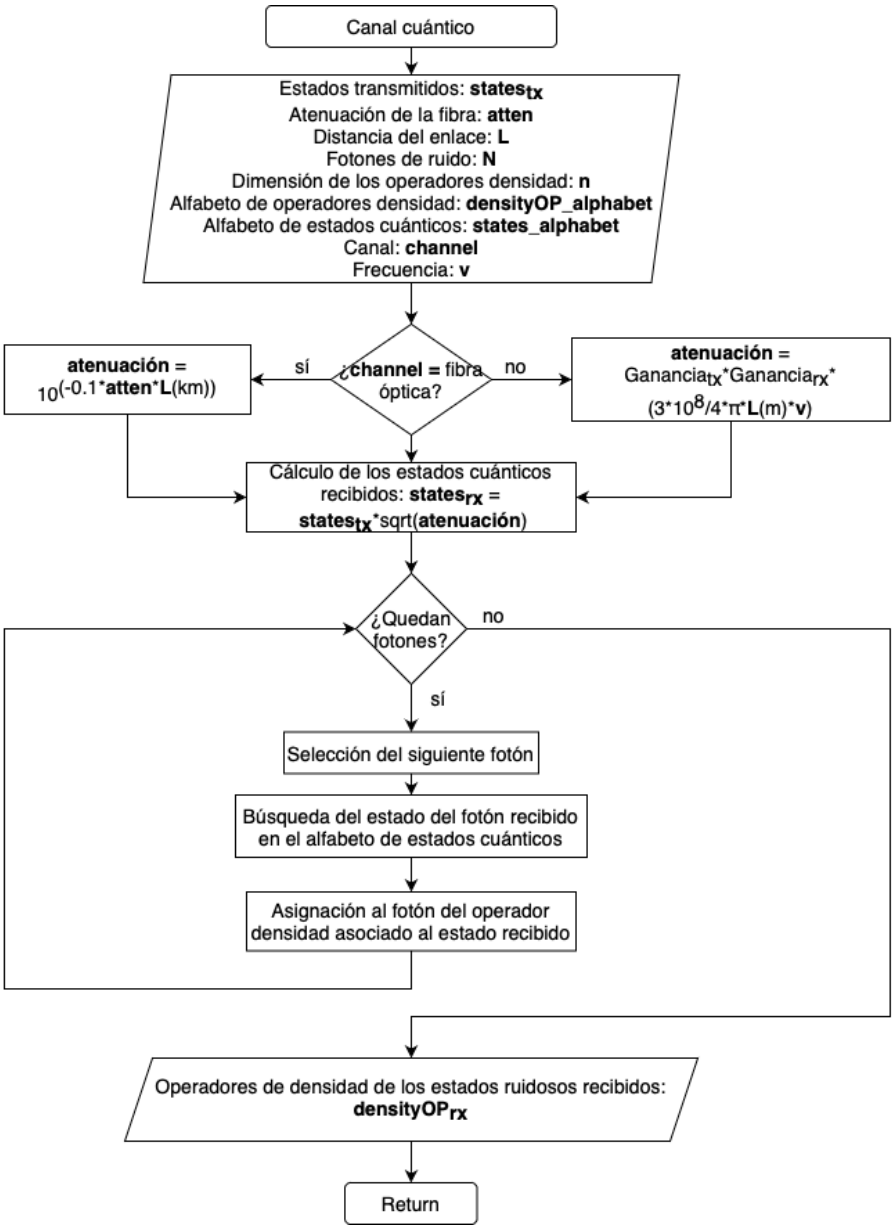


Fig. 4.26. Lógica del canal cuántico

En el canal cuántico, al igual que se hizo en el cálculo de los posibles operadores densidad recibidos, lo primero es calcular la atenuación que introduciría el canal, dependiendo de si se elige trabajar en un canal de espacio libre o de fibra óptica. Una vez tenemos la atenuación, obtenemos lo que en el diagrama de flujo se llama $states_{rx}$, es decir, los valores complejos que representarían a cualquier posible estado cuántico en el demodulador.

Una vez tenemos esta secuencia de valores complejos recibidos, $states_{rx}$, para cada uno de ellos buscamos su operador densidad correspondiente en el alfabeto que tenemos como entrada. Iteramos para cada valor complejo hasta tener una secuencia, pero de operadores densidad en este caso.

Se podría haber omitido el alfabeto de operadores densidad y, a partir de cada valor complejo y del número de fotones promedio de ruido térmico, haber calculado cada posible operador densidad. El problema de este proceder es que el cálculo de un operador densidad es lo más costoso computacionalmente del emulador y, siguiendo este esquema, para cada valor complejo que sale del modulador cuántico deberíamos hacer el cálculo de un operador densidad. Ésto habría ralentizado enormemente las ejecuciones del código, lo que no tendría sentido ya que tendremos únicamente dos (BPSK) o cuatro (QPSK) operadores densidad distintos. Es decir, estaríamos constantemente calculando las mismas matrices.

Por el contrario, con el proceder actual, se calculan los posibles operadores densidad **una única vez** y en función del valor complejo de $states_{rx}$ introducimos en la secuencia de operadores densidad uno u otro, teniendo así un programa mucho más eficiente computacionalmente. Se muestra en la siguiente figura la asignación de operadores densidad de manera gráfica.

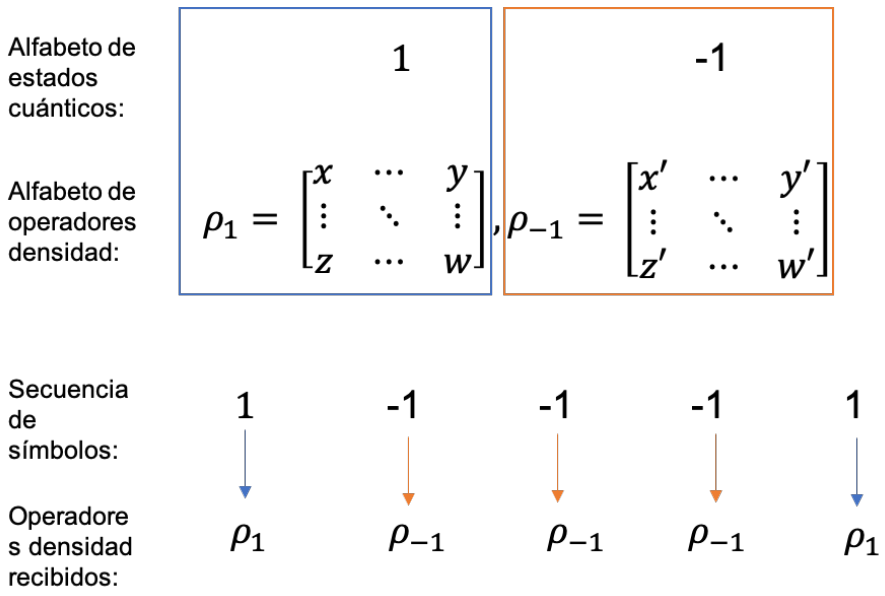


Fig. 4.27. Asignación de operadores densidad

Como ya hemos dicho, el resultado del canal cuántico sería una secuencia operadores

densidad, matrices como ya se ha dicho, que representarían cada posible estado cuántico en el receptor y donde ya se han tenido en cuenta tanto los efectos de la atenuación del canal, como los efectos del ruido térmico.

Demodulador Cuántico

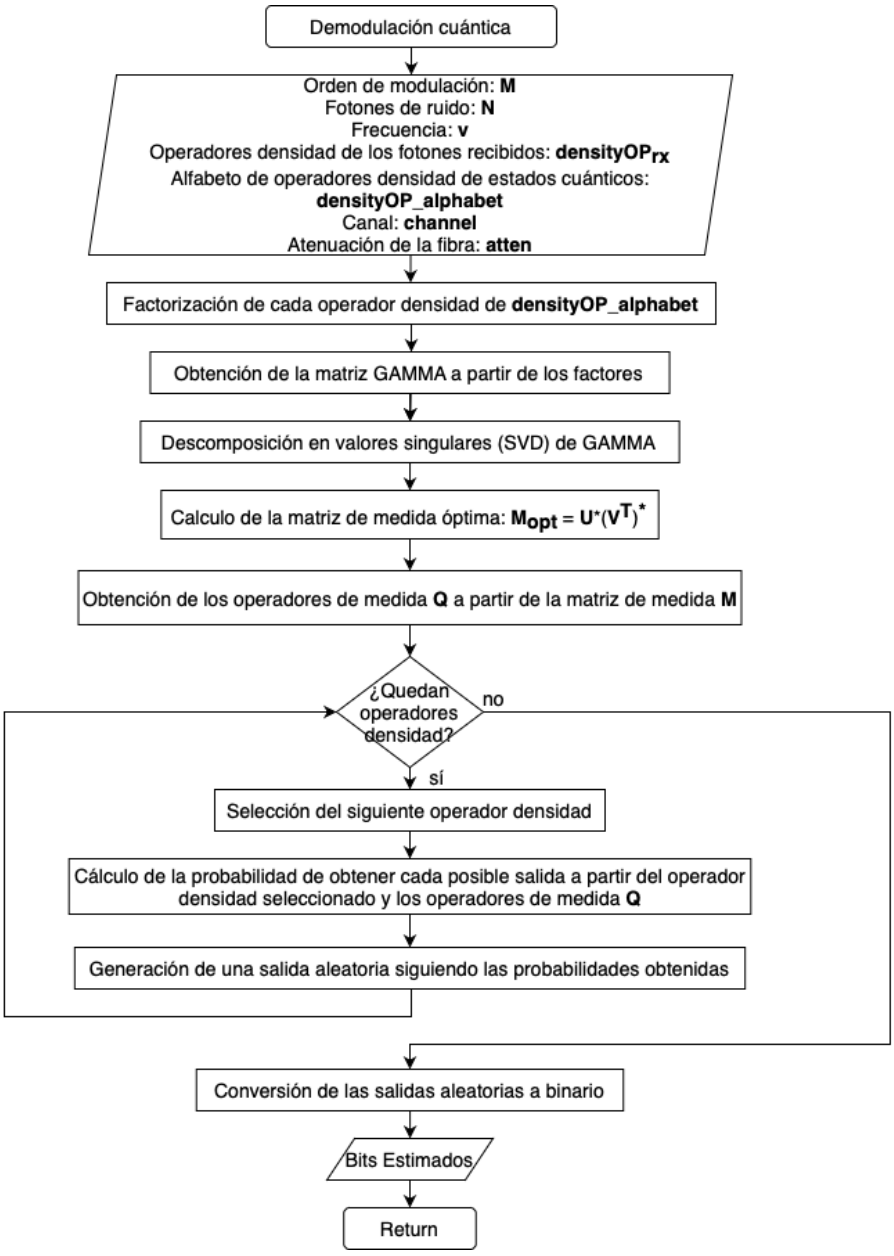


Fig. 4.28. Lógica del demodulador cuántico

Al igual que en el demodulador clásico, no es preciso detallar mucho el diagrama de flujo pues únicamente es necesario seguir la explicación teórica del apartado 2.2.5.

Unicamente se aclara que la parte “Generación de una salida aleatoria siguiendo las probabilidades obtenidas” consiste en, a partir de los operadores de medida Q_i y los operadores densidad recibidos ρ_j calcular las probabilidades como se vio anteriormente:

$$p(i|j) = Tr[\rho_j Q_i]$$

A modo de ejemplo si utilizamos una modulación cuaternaria, tendremos 4 operadores densidad:

$$Q_0, Q_1, Q_2, Q_3$$

Si obtenemos un operador densidad ρ_i, podríamos obtener las siguientes probabilidades:

- $p_0 = Tr[\rho_i Q_0] = 0{,}1$
- $p_1 = Tr[\rho_i Q_1] = 0{,}2$
- $p_2 = Tr[\rho_i Q_2] = 0{,}1$
- $p_3 = Tr[\rho_i Q_3] = 0{,}6$

Utilizando la función *randsrc* de MATLAB, obtendríamos un 0 con probabilidad 0,1, un 1 con probabilidad 0,2, un 2 con probabilidad 0,1 y un 3 con probabilidad 0,6. En función de el valor aleatorio obtenido, tendríamos unos bits estimados u otros.

Reconstrucción de imágenes

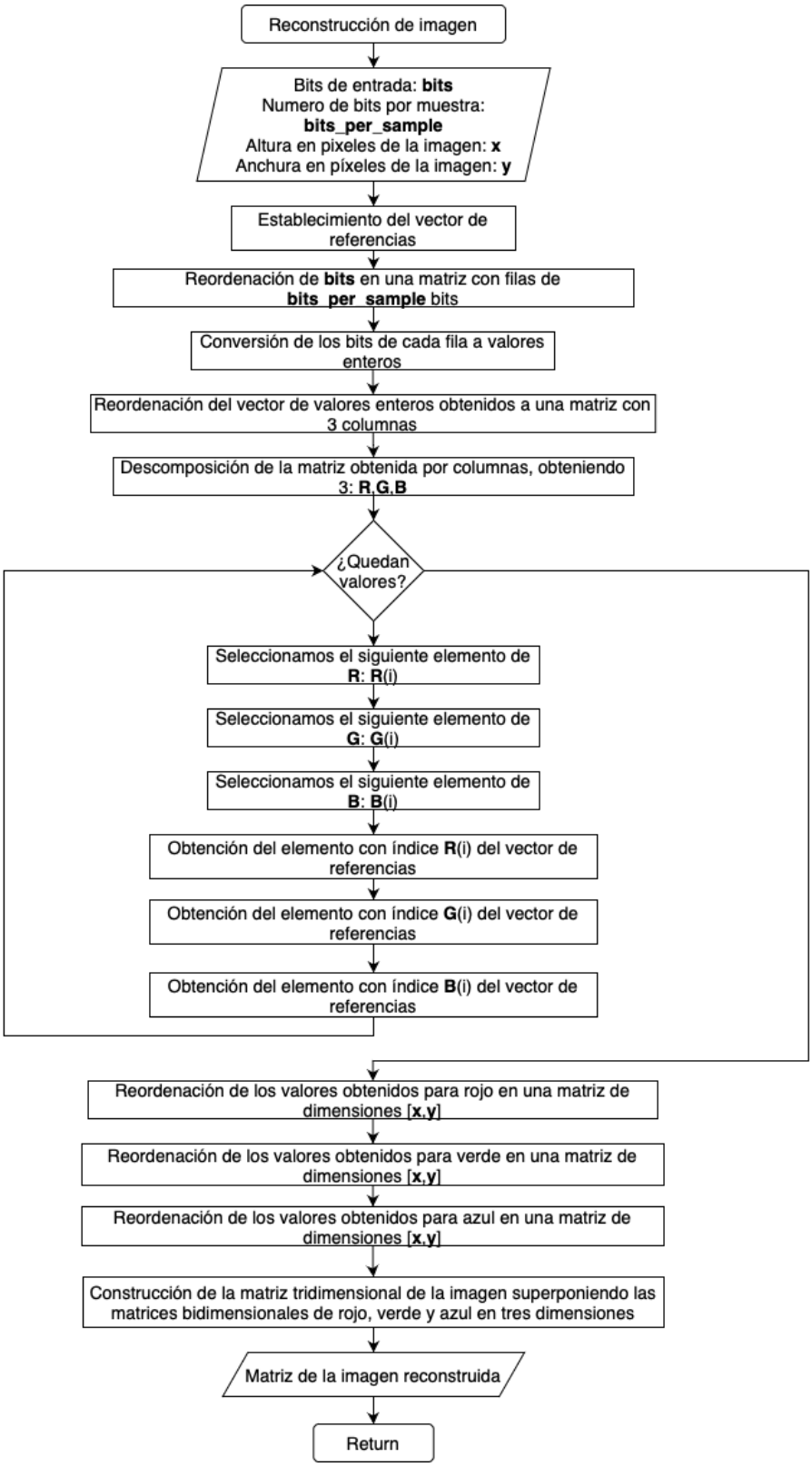


Fig. 4.29. Lógica de la reconstrucción de imágenes

En primer lugar, debemos volver a generar el mismo vector de referencias que obtuvimos en la conversión imagen - bits.

Al reconstruir la imagen es evidente que debemos recorrer los pasos de la conversión imagen - bits pero en sentido opuesto. Por tanto, como lo último que hicimos fue convertir los índices de los valores en el vector de referencias a binario, lo que hacemos es reordenar la secuencia de bits estimados en una matriz con $bits\_per\_sample$ columnas (bits). El siguiente paso es claro, convertir cada fila (un valor binario de 6 bits, que es el bits_per_sample que utilizamos) a enteros, de tal manera que habremos obtenido la secuencia estimada de índices del vector de referencias.

Volvemos a llevar a cabo una "reordenación" de este nuevo vector de valores en una matriz con tres columnas, donde cada una se corresponderá con la secuencia de valores para cada uno de los tres colores primarios de la imagen: rojo (R), verde (G) y azul (B).

Una vez hemos obtenido las tres secuencias anteriores, tomamos de uno en uno los valores de cada vector ($R(i)$, $G(i)$, $B(i)$). Para cada uno de estos valores, buscamos y almacenamos en un nuevo vector el elemento del vector de referencias con el índice $R(i)$ para rojo, $G(i)$ para verde y $B(i)$ para azul.

El resultado de estas iteraciones serán tres nuevos vectores, donde cada uno contendrá ya las muestras (no índices) de cada color primario.

El último paso es convertir estos vectores en matrices con las mismas dimensiones que la imagen original $[x, y]$, dimensiones que obtuvimos de la conversión imagen - bits. Una vez obtenidas estas matrices, la imagen estimada es generada (utilizando las pertinentes funciones de MATLAB).

Reconstrucción de audios

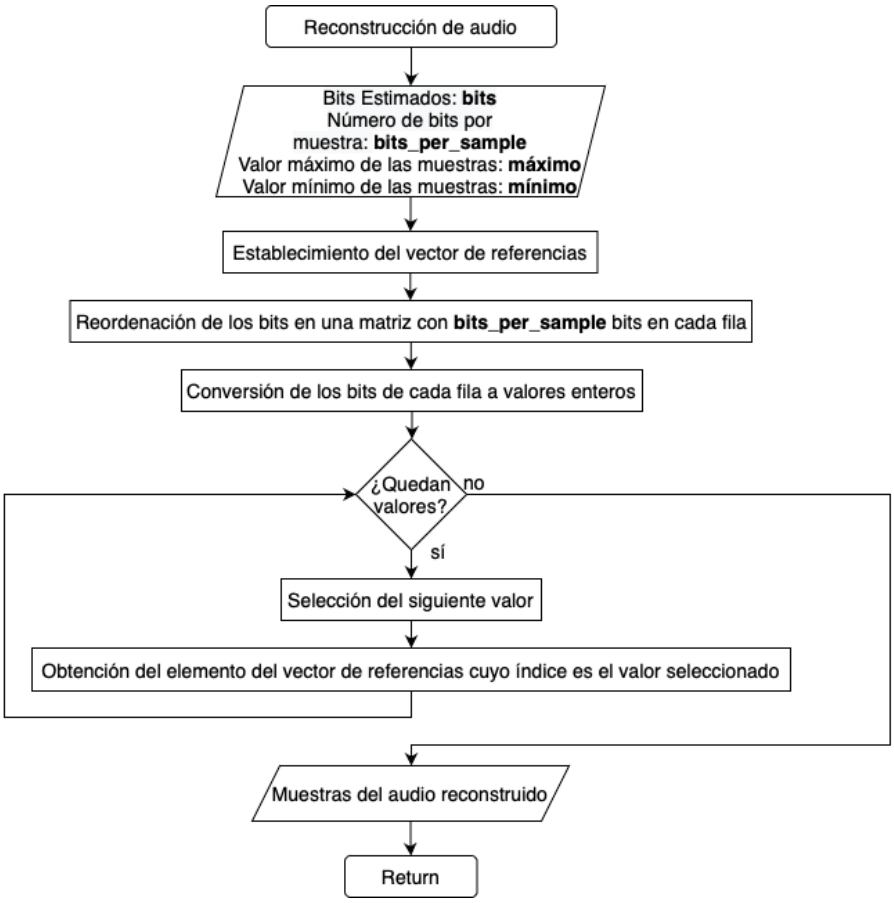


Fig. 4.30. Lógica de la reconstrucción de audios

En primer lugar, es evidente que debemos volver a obtener el mismo vector de referencias.

Tras esto, reordenamos la secuencia de bits estimada en una matriz con *bits_per_sample* columnas para posteriormente hacer la conversión de los bits de cada fila a un valor entero.

Una vez tenemos esta secuencia de valores enteros, la cual representa los índices estimados del vector de referencias, para cada índice estimado, almacenamos en un nuevo vector el valor del vector de referencias con el índice dado.

Tras repetir esto para toda la secuencia de índices estimados, tendremos la secuencia de muestras del audio reconstruido, las cuales serán la salida de la reconstrucción.

4.2.3. Análisis del emulador

Una vez analizadas las entradas y salidas y la lógica del emulador, se procede a estudiar diversas ejecuciones del mismo. Para ello, se utilizará la carta de ajuste de la figura 4.31 y la gaviota de la figura 4.32, ambas mostradas a continuación.

Fig. 4.31. Imagen utilizada en las ejecuciones [31]

Fig. 4.32. Imagen utilizada en las ejecuciones

Efecto del ruido térmico en sistemas de comunicaciones clásico y cuántico sobre una modulación BPSK

En primer lugar, se analizará el efecto del ruido térmico de manera aislada. Para ello, se considerará un canal de fibra óptica ideal en cuanto a atenuación (sería equivalente utilizar un canal de espacio libre de 10m, que como ya se ha dicho en la sección 4.2.1 en el apartado "Distancia del enlace", es la distancia a la que las antenas compensan la atenuación). Se fijarán tanto el número de fotones promedio por símbolo en $N_s = 1{,}5$ como el orden de la modulación en $M = 2$ (modulación BPSK). Tampoco se emulará la presencia de un espía durante el intercambio cuántico de clave.

Por tanto, las únicas distorsiones tenidas en cuenta serán la propia de la medida cuán-

tica (para el sistema cuántico), el ruido shot (para el sistema clásico) y el ruido térmico (para ambos sistemas). Será la temperatura el único parámetro que cambiará en las sucesivas ejecuciones de la presente sección, que como ya es sabido, determinará el número promedio de fotones de ruido térmico, N.

Con el fin de entender como afecta el ruido térmico al sistema clásico y al sistema cuántico, se emularán cuatro casos:

1. Caso sin ruido: $T = -200°C$, donde la temperatura es tan baja que el valor de N puede aproximarse a 0.

2. Caso con ruido térmico bajo: $T = 0°C$. La temperatura sigue siendo baja, pero no lo suficiente como para poder despreciar N.

3. Caso con ruido térmico: $T = 20°C$. El ruido térmico comienza a tener un efecto considerable en la transmisión.

4. Caso con saturación de ruido térmico: $T = 50°C$. El ruido térmico domina sobre los fotones promedio de señal.

Para cada uno de los casos anteriores, se analizará en primer lugar la evolución de la BER resultante de la ejecución con el objetivo de tener una noción cuantitativa de la misma. Terminaremos cada caso con la visualización de las imágenes obtenidas para completar esa visión objetiva que ofrece la BER con una visión personal del usuario acerca de la calidad de las imagenes.

Caso sin ruido: $T = -200°C$

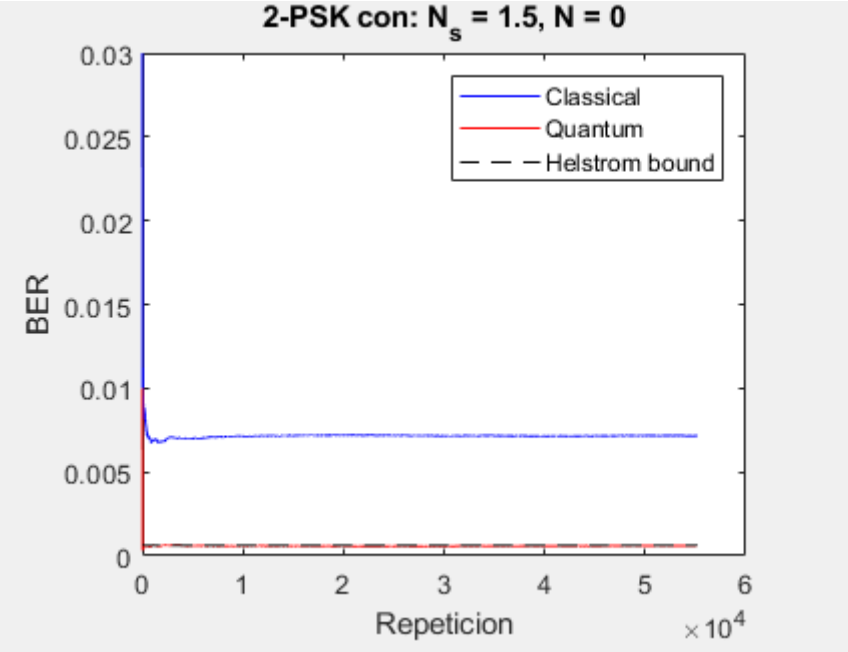


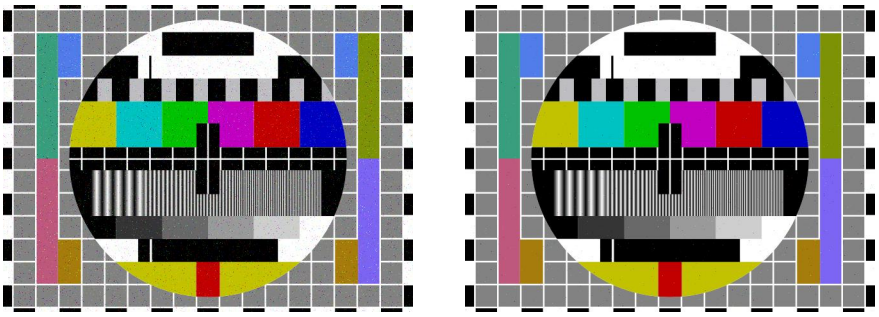
Fig. 4.33. Evolución de la BER para $-200°C$

Como ya se ha explicado, en esta gráfica se muestran la evolución de la BER para el sistema clásico (azul), para el sistema cuántico (rojo) y el límite de *Helstrom*.

Lo primero que es necesario advertir es la ventaja del sistema cuántico frente al clásico, de aproximadamente un década (10^{-3} *vs* 10^{-4}). Cuando se comparan las tasas de error de diferentes sistemas se utilizan las décadas como medida, lo que nos da una noción de que la ventaja del sistema cuántico frente al clásico en estas condiciones es algo a tener en cuenta.

Además de esto, se ve como el rendimiento del sistema cuántico en términos de tasa de error alcanza el límite de *Helstrom* que, como se indicó en el capítulo primero, dice lo mejor que puede hacerlo un sistema de comunicaciones cuántico. También se decía que únicamente se iba a poder alcanzar esta tasa de error en ausencia de ruido térmico, que es el caso actual, por lo que, de momento, el emulador es fiel al desarrollo teórico presente en el apartado de introducción.

Como se prometió, para finalizar el análisis del caso sin ruido, se muestran las imágenes obtenidas de esta ejecución.



(a) (b)

Fig. 4.34. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para $-200°C$

(a) (b)

Fig. 4.35. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para $-200°C$

Los bits erróneos se muestran por medio de píxeles discordantes dentro de la imagen, los puntos que podemos ver en las imágenes anteriores (por ejemplo, azul claro sobre azul oscuro para el ejemplo de la figura 4.35) y que si comparamos con la original (figura 4.32), no aparecen. Si se miran las imágenes, rápidamente se puede ver como ese número de pixeles discordantes (y por tanto de bits erróneos) es claramente mayor en las imágenes transmitidas de manera clásica. Ésto apoya lo expuesto anteriormente cuando sólo se había mostrado la evolución de la probabilidad de error.

Caso con ruido térmico bajo: $T = 0°C$

El siguiente paso es incrementar la temperatura hasta los $0°C$, obteniendo las tasas de error que se muestran en la imagen 4.36.

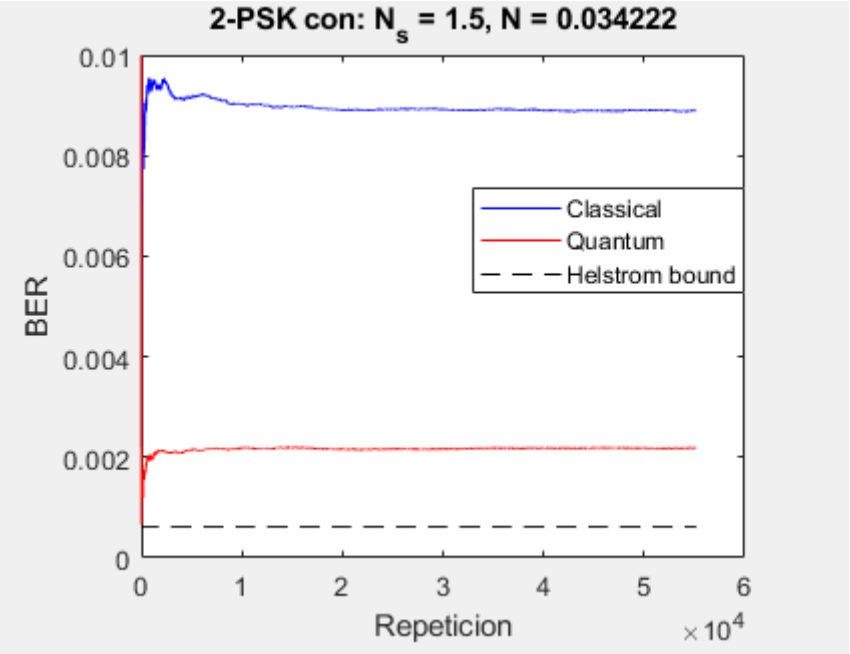
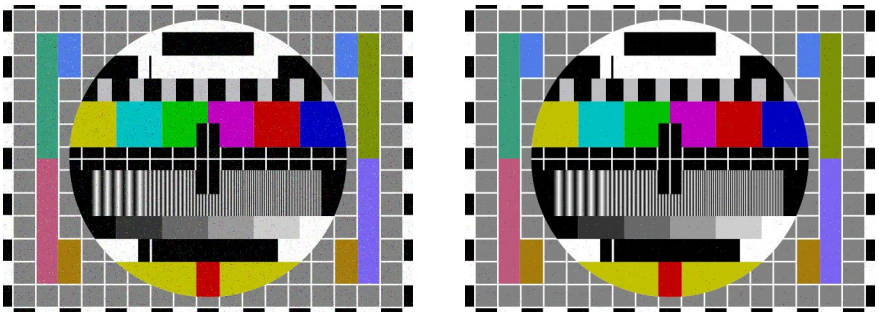


Fig. 4.36. Evolución de la BER para 0°C

Sólo con pasar del caso donde el ruido térmico es despreciable al caso en el que el ruido térmico es muy pequeño pero no despreciable se puede ver algo que, como se comprobará más adelante, se va a convertir en tendencia. Nos referimos a cómo el sistema cuántico se ha aproximado al sistema clásico. Ésto se refleja en la tasa de error del sistema cuántico, que se ha situado en el mismo orden de magnitud que el sistema clásico y al que el paso de $N = 0$ a $N = 0{,}03456$ apenas ha afectado.

Como se indicó en el apartado anterior, la comparación entre las tasas de error de diferentes sistemas de comunicaciones iba a hacerse en términos de décadas y, en este caso, la diferencia ya está por debajo de una década, por debajo de una unidad de medida de tasa de error.

Otro cambio significativo respecto al caso sin ruido está en que la tasa de error del sistema cuántico ya no termina convergiendo al límite de *Helstrom* debido a la presencia del ruido térmico. En el caso anterior, se tenía que la BER del sistema cuántico oscilaba alrededor del límite de *Helstrom* para acabar convergiendo a él, mientras que ahora todas esas pequeñas oscilaciones hasta que la tasa de error converge están siempre por encima de este límite.



(a) (b)

Fig. 4.37. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para $0°C$

(a) (b)

Fig. 4.38. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para $0°C$

Si se comparan de nuevo las imágenes obtenidas para cada sistema, se aprecia aún una clara superioridad del sistema cuántico frente al clásico.

Ésto puede parecer incoherente con lo expresado anteriormente acerca de la comparación entre ambos sistemas. Es necesario entender que aunque se utilicen décadas para comparar probabilidades de error, una tasa de error cuatro veces mas pequeña (como es el caso de la tasa del sistema cuántico respecto al clásico) sigue siendo una diferencia importante a nivel cualitativo, ya que implica cuatro veces menos bits erróneos en las imágenes cuánticas que en las clásicas y, por consiguiente, un número notablemente menor de píxeles discordantes, que es lo que se puede ver en las imágenes.

Caso con ruido térmico: $T = 20°C$

Si se aumenta la temperatura hasta los $20°C$, obtenemos la BER de la imagen 4.39.

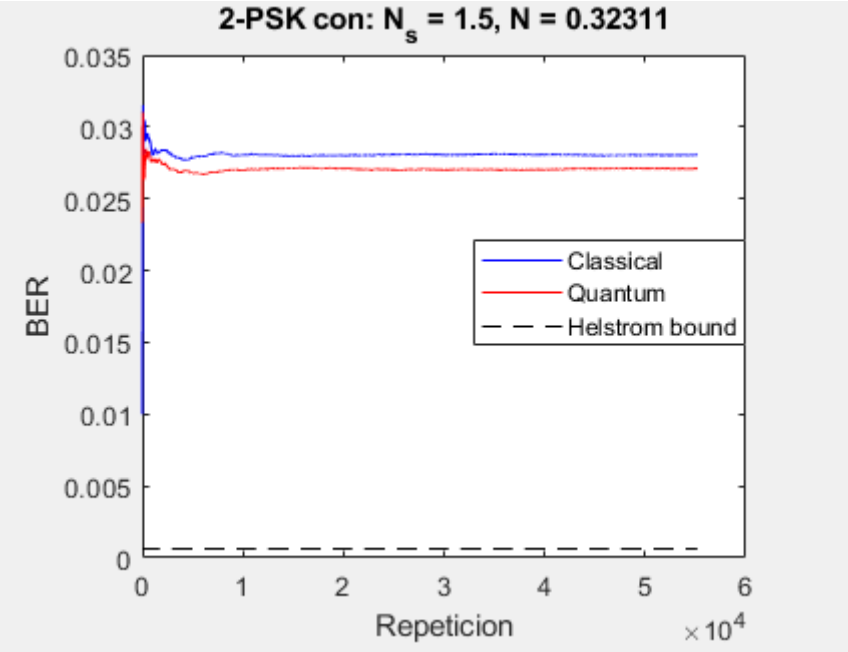
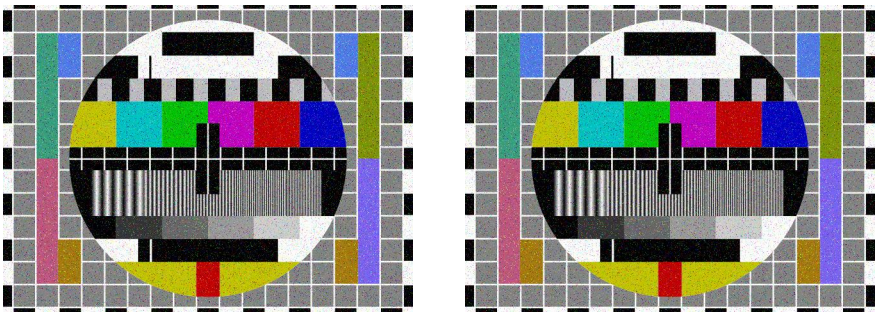


Fig. 4.39. Evolución de la BER para 20°C

Se puede ver como lo que se prometía en el apartado anterior acerca de la tendencia que iba a tener el sistema cuántico de empeorar su rendimiento y acercarse al clásico se consuma. En este caso no sólo el sistema cuántico se acerca al clásico en términos de probabilidad de error sino que se igualan, es decir, el sistema cuántico deja de suponer una ventaja frente al clásico.

Si en el apartado anterior se decía que no se podía hablar, de manera cuantitativa, de una gran ventaja del sistema cuántico al ser la diferencia menor de una década, en este caso ésto se acentúa aún más al no solamente estar ambas probabilidades de error en la misma década, sino en la misma centésima, diferenciándose en apenas algunas milésimas.

Una vez más se finaliza la comparación mostrando las fotografías para su contraste.



(a) (b)

Fig. 4.40. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para $20°C$

(a) (b)

Fig. 4.41. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para $20°C$

Se puede ver como ahora es prácticamente imposible diferenciar si una imagen clásica tiene más o menos píxeles erróneos que su contraparte cuántica. Ésto se debe a que, como se ha visto en la gráfica de la tasa de error, ambos sistemas ofrecen, en estas condiciones de ruido térmico, unas prestaciones prácticamente idénticas.

Caso con saturación de ruido térmico: $T = 50°C$

Toda vez que se ha visto como las prestaciones de ambos sistemas tendían a igualarse a medida que incrementaba la temperatura y por lo tanto el ruido térmico, se saturarán ambos sistemas con ruido térmico, para lo cual se impondrá una temperatura extremadamente alta. Se muestra la probabilidad de error obtenida en este caso en la imagen que sigue.

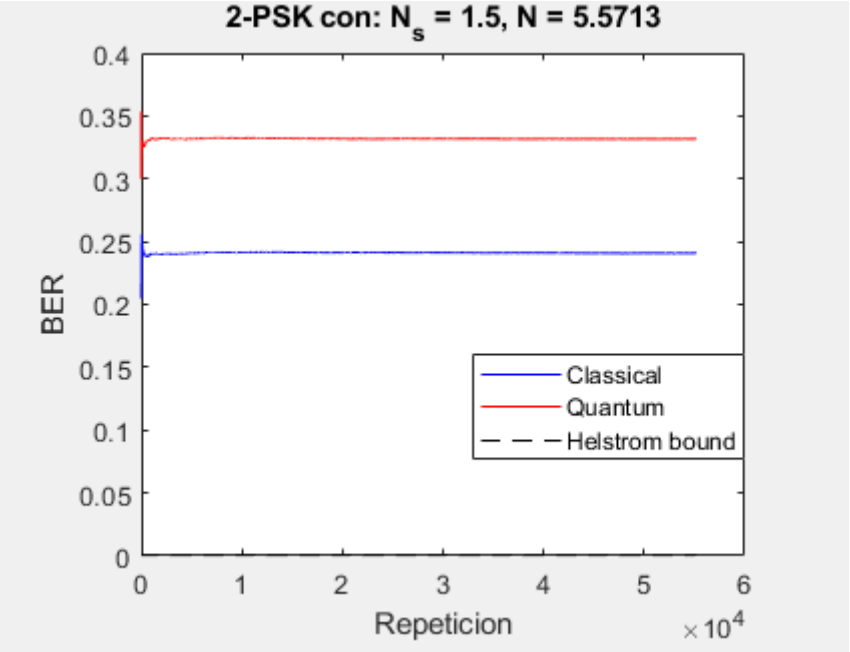
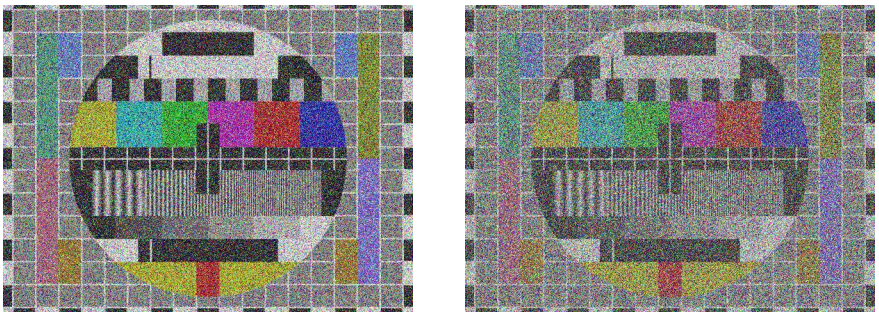


Fig. 4.42. Evolución de la BER para 50°C

Se ve de manera clara que no solamente ese poder que tenía la comunicación cuántica frente a la clásica se diluye por completo como ocurría en el caso anterior, sino que ahora el sistema que es capaz de ofrecer una probabilidad de error de bit menor es el sistema clásico, algo totalmente novedoso atendiendo a los casos analizados anteriormente.

Además, se puede ver como el límite de *Helstrom* queda prácticamente fusionado con el eje de las "Repeticiones", lo que demuestra lo lejos que estamos de esas tasas de error iniciales (donde **sí** alcanzábamos ese límite de *Helstrom*) simplemente por el hecho de incrementar la temperatura de trabajo.



(a) (b)

Fig. 4.43. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para 50°C

(a) (b)

Fig. 4.44. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para $50°C$

Ahora, al visualizar las imágenes recibidas, se advierte rápidamente la gran distorsión que padecen ambos sistemas.

Podemos ver como la temperatura de trabajo es algo tremendamente determinante en el rendimiento de nuestro sistema, hasta el punto de que cuando esta temperatura excede unos determinados límites, prácticamente todo lo recibido es ruido y el demodulador se acerca a hacer decisiones aleatorias, esto es, eligiendo "0" ó "1" al 50 % porque lo recibido apenas aporta información.

Finalmente, en cuanto a la comparativa entre ambos sistemas, podemos ver que a pesar de la gran cantidad de ruido presente en todas las imágenes, las transmitidas a través del sistema clásico parecen tener algo menos de distorsión al igual que se ha visto en la BER.

Contraste de los resultados obtenidos con otras publicaciones

Temperatura	$T = -200°C$	$T = 0°C$
Fotones promedio de ruido	$N = 0$	$N = 0{,}034222$
Sistema clásico	$7{,}152939 \cdot 10^{-3}$	$8{,}900430 \cdot 10^{-3}$
Sistema cuántico	$6{,}200725 \cdot 10^{-4}$	$2{,}193510 \cdot 10^{-3}$

Temperatura	$T = 20°C$	$T = 50°C$
Fotones promedio de ruido	$N = 0{,}32311$	5,5713
Sistema clásico	$2{,}812348 \cdot 10^{-2}$	$2{,}410466 \cdot 10^{-1}$
Sistema cuántico	$2{,}767658 \cdot 10^{-2}$	$3{,}406447 \cdot 10^{-1}$

TABLA 4.1. PROBABILIDADES DE ERROR OBTENIDAS DE LAS FÓRMULAS ANALÍTICAS (TEÓRICAS)

Temperatura	$T = -200°C$	$T = 0°C$
Fotones promedio de ruido	$N = 0$	$N = 0{,}034222$
Sistema clásico	$7{,}155180 \cdot 10^{-3}$	$8{,}895238 \cdot 10^{-3}$
Sistema cuántico	$5{,}938839 \cdot 10^{-4}$	$2{,}182759 \cdot 10^{-3}$

Temperatura	$T = 20°C$	$T = 50°C$
Fotones promedio de ruido	$N = 0{,}32311$	5,5713
Sistema clásico	$2{,}803986 \cdot 10^{-2}$	$2{,}407380 \cdot 10^{-1}$
Sistema cuántico	$2{,}710201 \cdot 10^{-2}$	$3{,}316513 \cdot 10^{-1}$

TABLA 4.2. PROBABILIDADES DE ERROR OBTENIDAS DE LAS EJECUCIONES

En las dos tablas anteriores se recogen las probabilidades de error de bit numéricas para cada uno de los casos emulados tanto de manera analítica, derivadas de las expresiones desarrolladas en el apartado 2.2.6 de la introducción (tabla 4.1); como las reales obtenidas fruto de las ejecuciones anteriores (tabla 4.2). Podemos ver como los valores de ambas tablas tienen una gran semejanza en todos los casos emulados.

Además, utilizando una de las múltiples gráficas ofrecidas por el libro *"Quantum Communications"* de *Gianfranco Cariolario* [9] podemos contrastar la probabilidad de error obtenida por el propio autor con la probabilidad de error resultante de la ejecución del emulador para el caso sin ruido.

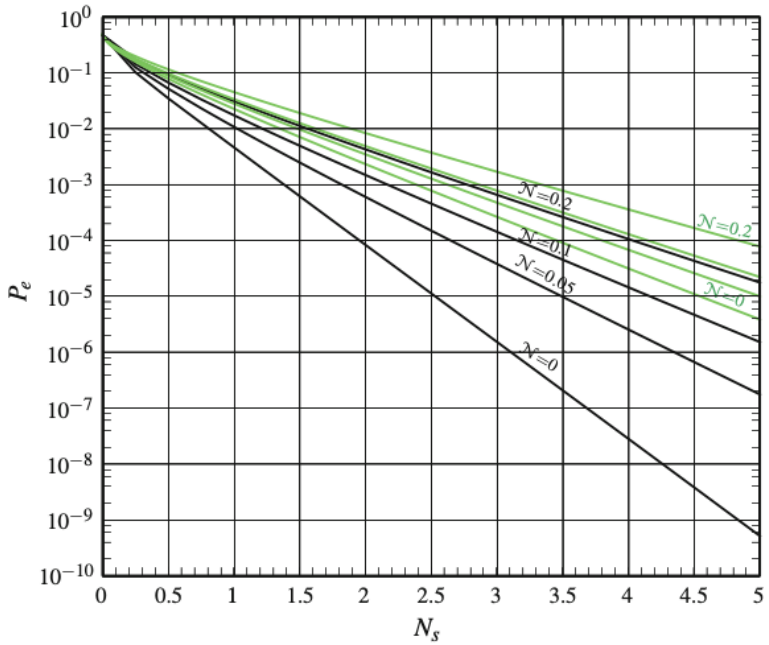


Fig. 4.45. Tasas de error para una modulación BPSK según "Quantum Communications" de Gianfranco Cariolaro [9]

Se puede ver como para el caso sin ruido, el valor desprendido de la gráfica 4.45 para el sistema cuántico es aproximadamente $6 \cdot 10^{-4}$, muy cercana a los $5{,}938839 \cdot 10^{-4}$ del emulador. Asimismo, con las mismas condiciones, el valor de la BER del sistema clásico que aparece en la gráfica está alrededor de $8 \cdot 10^{-3}$ mientras el resultado de la emulación dio $7{,}155180 \cdot 10^{-3}$, también muy cercanos entre sí.

Conclusiones acerca del efecto de ruido térmico sobre una modulación BPSK

A lo largo de las ejecuciones anteriores hemos visto como el sistema cuántico es capaz de ofrecernos tasas de error notablemente inferiores a las alcanzables por el clásico. No obstante, esto no ocurre siempre puesto que como hemos podido comprobar, a medida que crece la temperatura (y en consecuencia, el ruido térmico) las prestaciones de ambos sistemas tienden a igualarse y, llegado a cierto punto, es el sistema clásico el que es capaz de ofrecer una BER mejor.

Por lo tanto, en este apartado se concluye que el sistema de comunicaciones cuántico es capaz de ofrecer tasas de error muy por debajo de las que podría ofrecer un sistema clásico siempre que nos encontremos en una transmisión libre de ruido térmico o, al menos,

siempre que el ruido térmico sea pequeño.

Por su parte, el sistema clásico ha demostrado ser un sistema claramente más robusto frente al ruido térmico. Evidentemente, a medida que aumenta la temperatura el rendimiento del sistema clásico cae, pero lo hace de una manera más lenta, proporcionando tasas de error menores en presencia de mucho ruido térmico en comparación con el sistema cuántico.

Efecto del ruido térmico en sistemas de comunicaciones clásico y cuántico sobre una modulación QPSK

En esta sección llevaremos acabo los mismos ejemplos que en la sección anterior con la diferencia única de que la modulación empleada será una QPSK o 4-PSK. Para ello, sólo será necesario modificar el parámetro de entrada M (orden de la modulación) de $M = 2$ a $M = 4$.

El objetivo es demostrar que las conclusiones surgidas del anterior conjunto de ejecuciones son válidas para otras modulaciones. En otras palabras, que las deducciones anteriores dependen principalmente de la naturaleza del sistema empleado (clásico/cuántico) y no de aspectos variables como la modulación elegida.

Caso sin ruido: $T = -200°C$

Al igual que hicimos con la modulación binaria, comenzamos mostrando la tasa de error. Cabe destacar que al ser una modulación cuaternaria, la BER y la tasa de error de símbolo son diferentes, ya que cada símbolo representa dos bits, por lo que si los dos bits de un símbolo fuesen erróneos, en la BER contabilizaríamos dos fallos, pero en la probabilidad de error de símbolo únicamente sería un elemento erróneo. Dicho esto, lo que mostramos en la gráfica es la BER o tasa de error de **bit**.

Otra gran diferencia es la ausencia del límite de Helstrom, ya que sólo tenemos un límite inferior exacto a la tasa de error para modulaciones binarias. Existen aproximaciones a este límite inferior para modulaciones de órdenes superiores, pero se ha decidido no incluirlas puesto que lo que se muestra, como se ha dicho, son las BER y este límite

aproximado sería en probabilidad de error de **símbolo**.

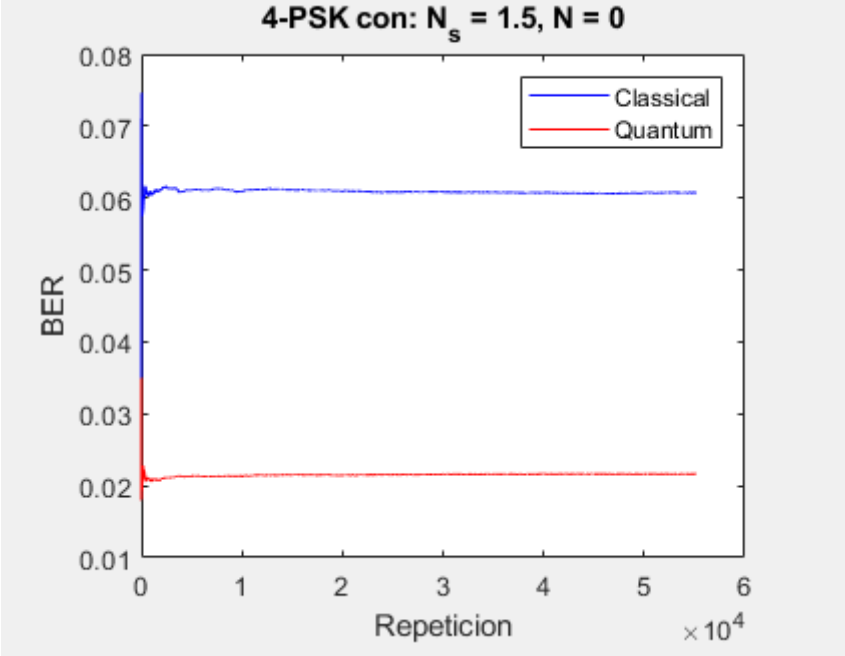
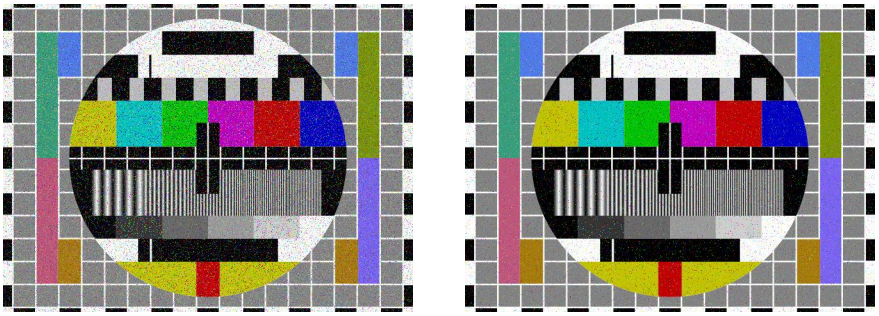


Fig. 4.46. Evolución de la BER para $-200°C(QPSK)$

Observando la gráfica 4.46 se advierten varias cosas. En primer lugar, al igual que ocurría para la modulación binaria, el sistema de comunicaciones regido por la mecánica cuántica parte con ventaja en lo que a BER se refiere. No obstante, vemos que mientras que esta diferencia era de una década en ausencia de ruido para la BPSK, para la modulación cuaternaria esta diferencia inicial es de algo más de media década.



(a) (b)

Fig. 4.47. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para $-200°C$ (QPSK)

(a) (b)

Fig. 4.48. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para $-200°C$ (QPSK)

Si miramos las imágenes obtenidas de estas ejecuciones tenemos que las imágenes transmitidas bajo las reglas clásicas tienen un número notablemente mayor de píxeles erróneos que las cuánticas, correspondiéndose con las tasas de error obtenidas, donde la BER del sistema clásico es aproximadamente tres veces mayor.

Caso con ruido térmico bajo: $T = 0°C$

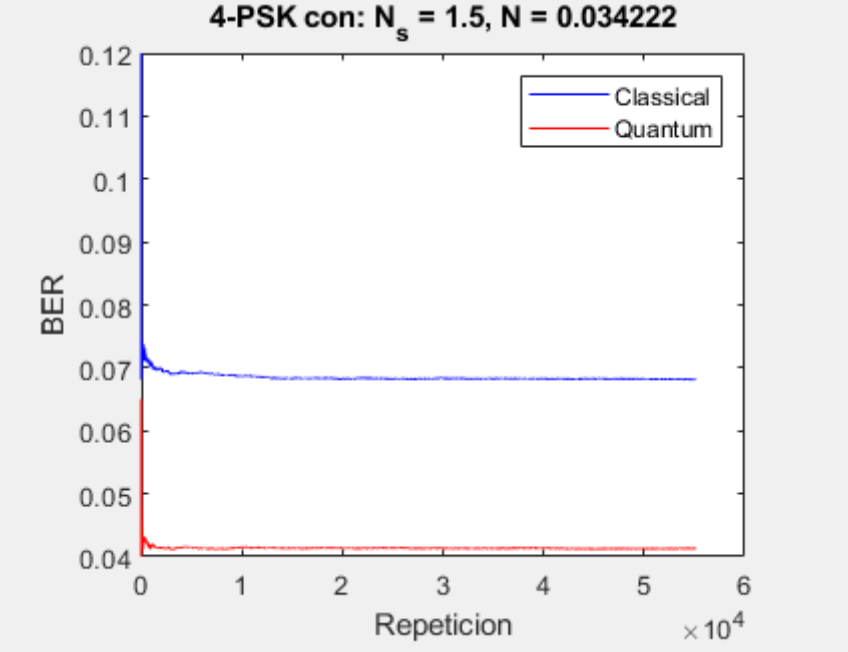
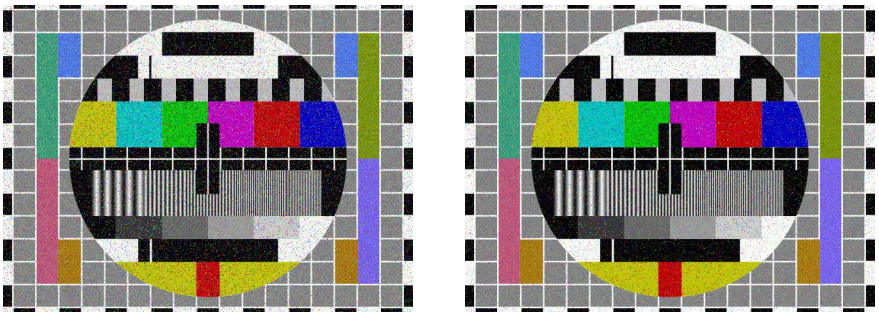


Fig. 4.49. Evolución de la BER para $0°C(QPSK)$

En la gráfica de la figura 4.49 se ve claramente como, de manera idéntica a la modulación con $M = 2$, el sistema cuántico se aproxima en BER al clásico. Por tanto, de momento ocurre lo mismo para la BPSK y para la QPSK.

Visualizamos las imágenes generadas por el código.



(a) (b)

Fig. 4.50. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para $0°C$ (QPSK)

(a) (b)

Fig. 4.51. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para $0°C$ (QPSK)

Caso con ruido térmico: $T = 20°C$

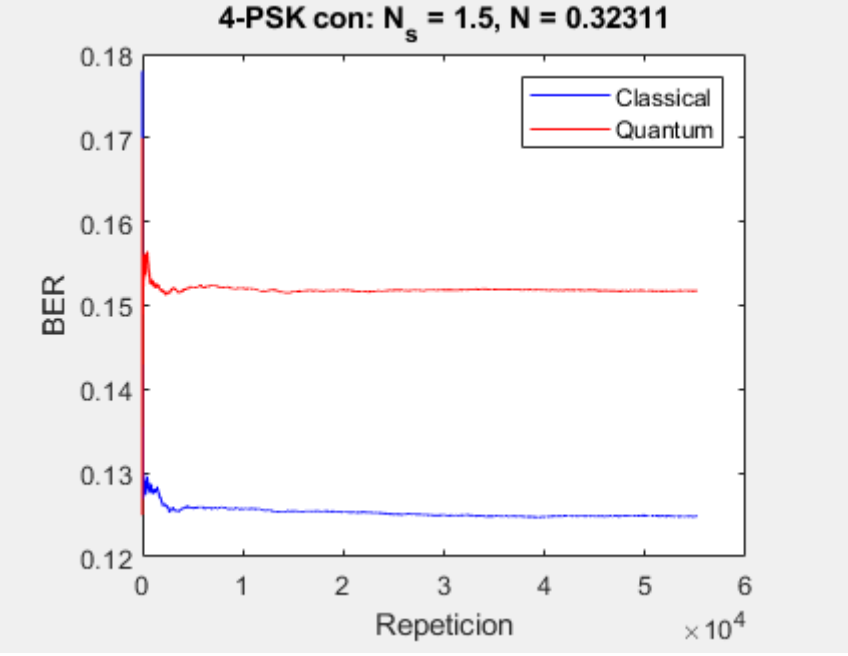


Fig. 4.52. Evolución de la BER para $20°C(QPSK)$

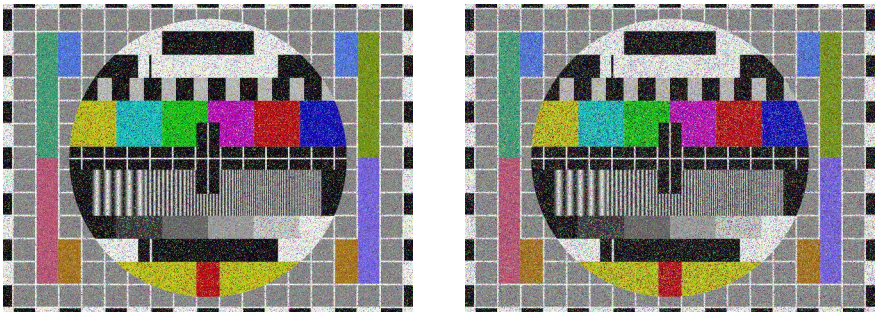
De nuevo, al subir la temperatura de trabajo, la ventaja de las comunicaciones cuánti-

cas decrece. Pero a diferencia del caso binario donde los 20°C hacían que las prestaciones de ambos sistemas se igualasen, utilizando la modulación cuaternaria vemos que no sólo se igualan sino que ya el sistema clásico se va a comportar claramente mejor.

Para cuantificar esto, calculamos los cocientes entre las tasas de error de cada caso:

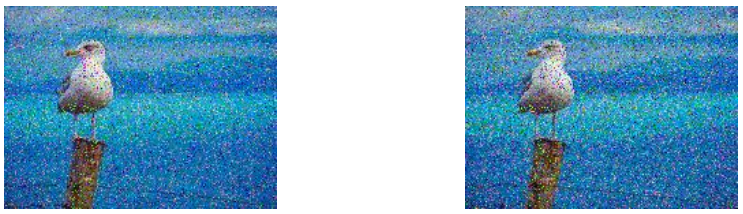
- BPSK: $\eta_{BPSK,20^\circ} = \frac{2{,}710201 \cdot 10^{-2}}{2{,}803986 \cdot 10^{-2}} = 0{,}96$
- QPSK: $\eta_{QPSK,20^\circ} = \frac{1{,}517354 \cdot 10^{-1}}{1{,}247995 \cdot 10^{-1}} = 1{,}21$

Es decir, mientras que para la BPSK el sistema cuántico ofrece una probabilidad de error ligeramente menor que el clásico, para la QPSK es aproximadamente un 20 % mayor.



(a) (b)

Fig. 4.53. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para 20°C (QPSK)



(a) (b)

Fig. 4.54. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para 20°C (QPSK)

Podemos ver, aunque muy ligeramente, algo más de distorsión en las imágenes generadas siguiendo las reglas cuánticas y, si recordamos, cuando visualizamos las imágenes para la 2-PSK y con los mismos 20°C algunos apartados atrás no éramos capaces de distinguir que imagen tenía más calidad.

Caso con saturación de ruido térmico: $T = 50°C$

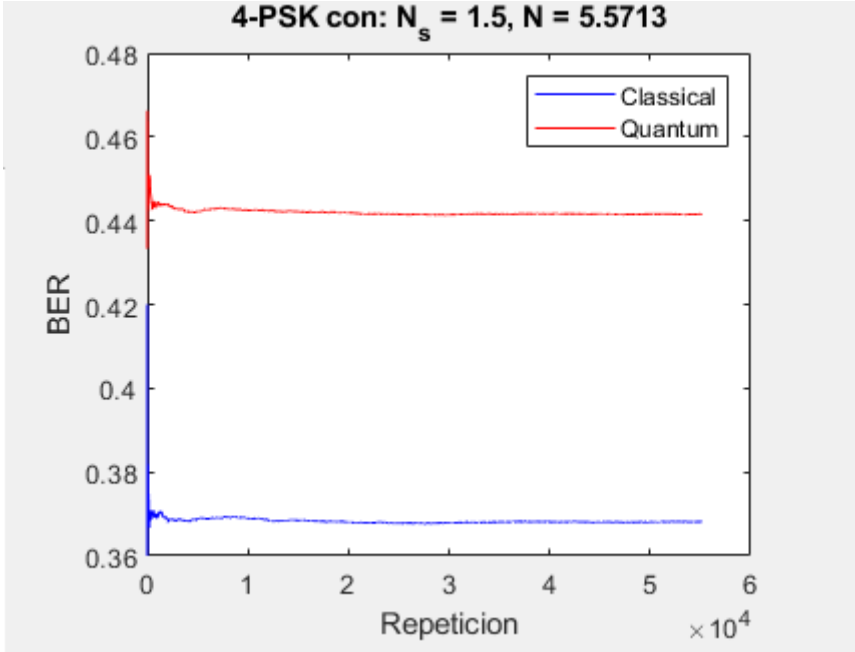
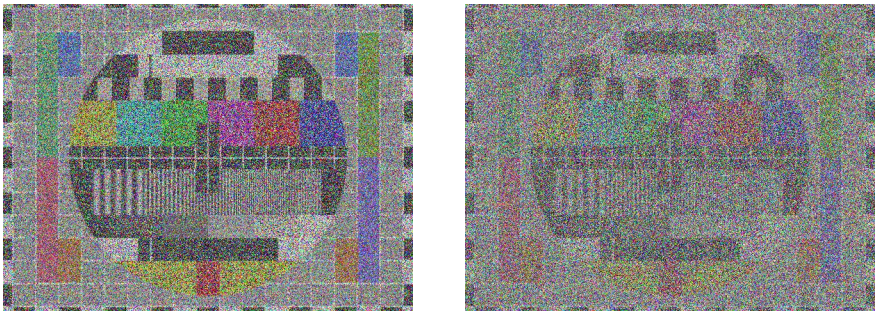


Fig. 4.55. Evolución de la BER para $50°C(QPSK)$

Por último, en saturación de ruido térmico, el sistema cuántico se sigue comportando peor que el sistema clásico, en mayor o menor medida, pero al igual que ocurría con la modulación binaria.

Visualizamos las imágenes a continuación donde se puede apreciar la gran cantidad de ruido que tienen las imágenes, siendo ya clara la mayor distorsión en las imágenes transmitidas de manera cuántica.



(a) (b)

Fig. 4.56. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para $50°C$ (QPSK)

(a) (b)

Fig. 4.57. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para 50°C (QPSK)

Contraste de los resultados obtenidos con otras publicaciones

De manera análoga a como se hizo en la modulación BPSK, se comparan las tasas de error obtenidas con tasas de error teóricas derivadas de expresiones. No obstante, debemos aclarar que estas expresiones analíticas nos dan la probabilidad de error de **símbolo**, por lo que en lugar de las BER mostradas en las gráficas anteriores, debemos utilizar las probabilidades de error de símbolo que también computa el emulador y muestra al usuario por pantalla, pero que no se muestran de manera gráfica.

Al igual que como hicimos anteriormente, se recogen estas probabilidades de error en dos tablas que se muestran a continuación.

Temperatura	$T = -200°C$	$T = 0°C$
Fotones promedio de ruido	$N = 0$	$N = 0{,}034222$
Sistema clásico	$8{,}153127 \cdot 10^{-2}$	$9{,}160584 \cdot 10^{-2}$
Sistema cuántico	$2{,}933889 \cdot 10^{-2}$	$5{,}645809 \cdot 10^{-2}$

Temperatura	$T = 20°C$	$T = 50°C$
Fotones promedio de ruido	$N = 0{,}32311$	5,5713
Sistema clásico	$1{,}691970 \cdot 10^{-1}$	$5{,}233142 \cdot 10^{-1}$
Sistema cuántico	$2{,}082974 \cdot 10^{-1}$	$6{,}485149 \cdot 10^{-1}$

TABLA 4.3. PROBABILIDADES DE ERROR OBTENIDAS DE LAS FÓRMULAS ANALÍTICAS (TEÓRICAS)

Temperatura	$T = -200°C$	$T = 0°C$
Fotones promedio de ruido	$N = 0$	$N = 0{,}034222$
Sistema clásico	$8{,}148688 \cdot 10^{-2}$	$9{,}160786 \cdot 10^{-2}$
Sistema cuántico	$2{,}934192 \cdot 10^{-2}$	$5{,}651844 \cdot 10^{-2}$

Temperatura	$T = 20°C$	$T = 50°C$
Fotones promedio de ruido	$N = 0{,}32311$	5,5713
Sistema clásico	$1{,}691481 \cdot 10^{-1}$	$5{,}230707 \cdot 10^{-1}$
Sistema cuántico	$2{,}081299 \cdot 10^{-1}$	$6{,}426779 \cdot 10^{-1}$

TABLA 4.4. PROBABILIDADES DE ERROR OBTENIDAS DE LAS EJECUCIONES

Atendiendo a estas tablas y tomando los datos sistema a sistema y caso a caso, podemos ver que los resultados obtenidos son muy similares a los esperados de antemano.

Además, al igual que hicimos con la 2-PSK, se compara el caso sin ruido de ambos sistemas con una de las gráficas que están disponibles en el libro *Quantum Communications*.

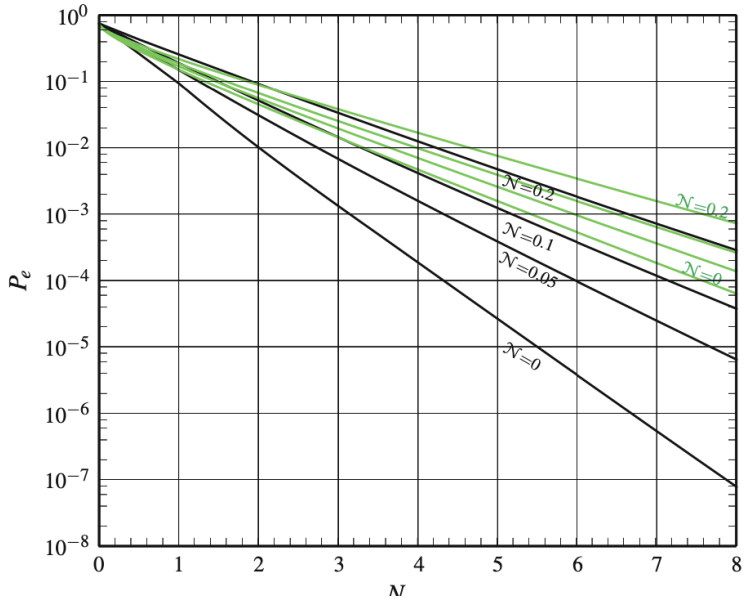


Fig. 4.58. Tasas de error de "Quantum Communications" de Gianfranco Cariolaro para 4-PSK [9]

De esta gráfica, para $N = 0$ podemos extraer unas probabilidades de error de símbolo de $3 \cdot 10^{-2}$ para el sistema cuántico y de $9 \cdot 10^{-2}$ para el clásico, muy cercanas a los $2{,}934192 \cdot 10^{-2}$ y $8{,}148688 \cdot 10^{-2}$ para sistemas cuántico y clásico respectivamente obtenidas de las ejecuciones.

Conclusiones acerca del efecto de ruido térmico sobre una modulación QPSK

Se ha podido comprobar de manera clara como, al igual que ocurrió con la modulación 2-PSK, la modulación 4-PSK comienza con ventaja en términos de BER, que se diluye a medida que aumenta la temperatura y, por tanto, el ruido térmico. Podemos así afirmar que el hecho de que un sistema de comunicaciones cuántico sea más sensible al ruido térmico que uno clásico se debe a la naturaleza de cada sistema, a las reglas que los rigen y no a la modulación empleada.

A pesar de esto, se ha visto como esta evolución de las probabilidades de error en función de la temperatura es distinta para cada modulación. En primer lugar, la ventaja inicial con la que parte el sistema cuántico es claramente menor utilizando una modulación QPSK. Además, con la QPSK, aumentando la temperatura hemos visto como el sistema clásico alcanza en rendimiento al cuántico antes que con la BPSK.

Dicho todo esto, se puede afirmar que a pesar de que no podemos evitar que un sistema de comunicaciones cuántico sea más frágil frente al ruido térmico que uno clásico, la diferencia entre ambos sistemas puede variar en función de la modulación empleada ya que, como se ha visto, una modulación cuaternaria acerca ambos sistemas en cuanto a prestaciones.

Efecto de la atenuación sobre sistemas de comunicaciones clásico y cuántico

De manera análoga a como se hizo unas líneas arriba con el ruido térmico, se aislará el efecto de la atenuación. Para ello, se dejarán como parámetros fijos:

- $N_s = 1{,}5$
- $T = -200$ (caso sin ruido)
- $M = 2$

- Canal = *"Optic fiber"*
- Eve = *"No Eavesdropper"*

Se utilizará un canal de fibra óptica ya que la atenuación crece más lentamente que en un canal de espacio libre, pudiendo así analizar el efecto sobre ambos sistemas de manera más precisa.

El parámetro que no se mantendrá fijo será la distancia del enlace, L, que se irá incrementando hasta que la atenuación sea tan grande que prácticamente se tenga una decisión aleatoria.

Para comparar ambos sistemas, nos centraremos esencialmente en las tasas de error. Obtendremos el cociente entre las tasas de error obtenidas por cada uno de los sistemas con el objeto de comparar su evolución en cada una de las situaciones.

No obstante, también se mostrarán las imágenes obtenidas por si fuera de interés para el lector.

Enlace de 0*km*

Nos encontramos ante el caso sin ruido que se estudió en el análisis del efecto del ruido térmico. A pesar de que las imágenes son idénticas, se muestran de nuevo a continuación para facilitar la comparación entre las distintas situaciones. Únicamente, se recuerda que partimos de una diferencia de aproximadamente una década entre ambos sistemas en el caso en que se considera una fibra óptica ideal en cuanto a atenuación.

Si dividimos las tasas de error obtenidas, tenemos $\eta_{0km} = \frac{2{,}193510 \cdot 10^{-3}}{8{,}900430 \cdot 10^{-3}} = 0{,}24$, es decir, la tasa de error del sistema cuántico es el 24 % de la del sistema clásico.

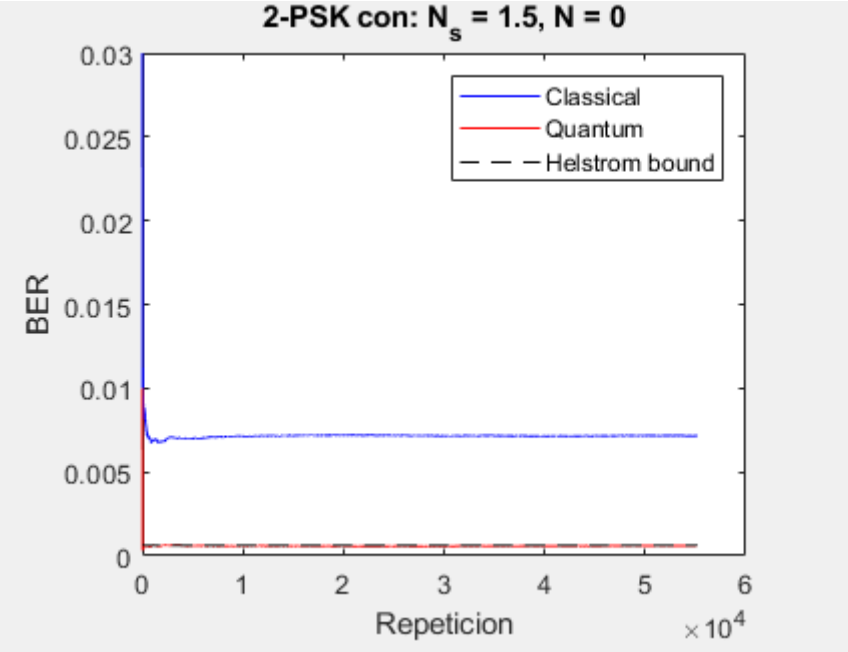
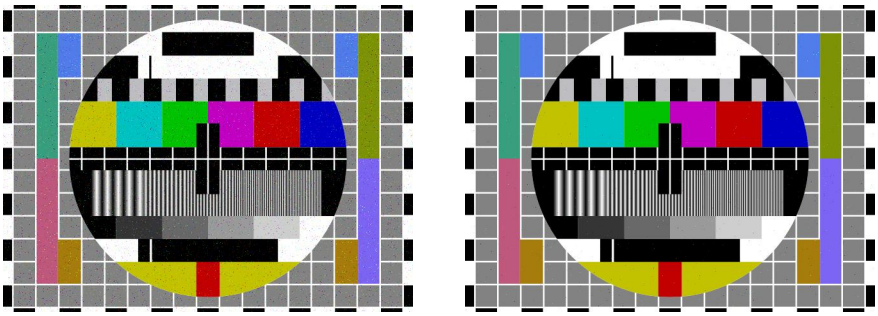


Fig. 4.59. Evolución de la BER para 0*km*



(a) (b)

Fig. 4.60. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para 0*km*

(a) (b)

Fig. 4.61. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para 0*km*

Enlace de 20km

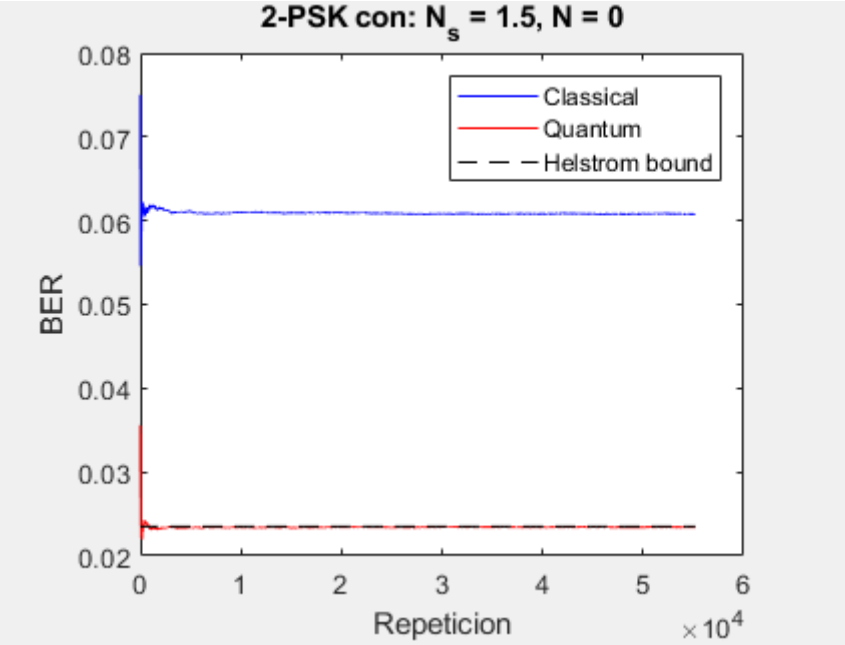


Fig. 4.62. Evolución de la BER para 20*km*

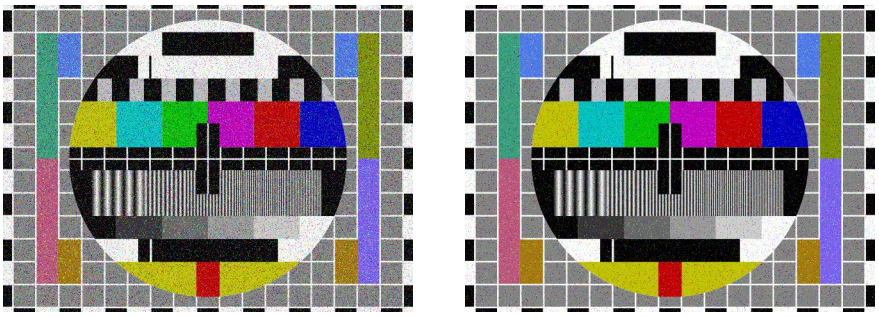
Podemos ver como al considerar la atenuación correspondiente a una fibra de 20km las tasas de error aumentan como es lógico.

Además, se debe aclarar que el sistema cuántico sigue alcanzando el límite de *Helstrom* ya que como se ha dicho, la atenuación se modela como una disminución en el numero de fotones promedio. Por ello, lo que se hace es calcular tal límite para N_r (número de fotones por símbolo recibidos) en lugar de para N_s.

En cuanto a la comparación entre ambos sistemas, se puede ver como se sigue manteniendo la superioridad del sistema cuántico. Si calculamos el cociente de tasas de error con estas condiciones el resultado es $\eta_{20km} = \frac{2{,}342478 \cdot 10^{-2}}{6{,}079516 \cdot 10^{-2}} = 0{,}39$.

Respecto al caso anterior, podemos ver que el sistema cuántico se acerca al clásico, al igual que ocurría cuando incrementábamos la temperatura. Por ello, queda pendiente para el resto de ejecuciones averiguar si de nuevo el sistema cuántico es más sensible, en este caso a la atenuación, o si por el contrario la distancia del enlace afecta por igual a ambos sistemas.

Se muestran las imágenes obtenidas por cada uno de los sistemas.



(a) (b)

Fig. 4.63. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para 20*km*

(a) (b)

Fig. 4.64. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para 20*km*

Enlace de 40*km*

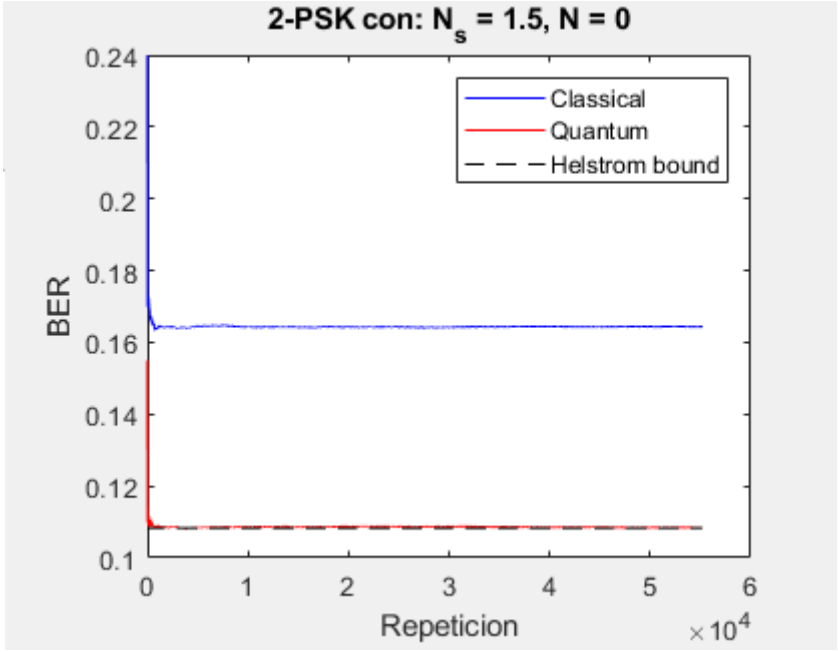
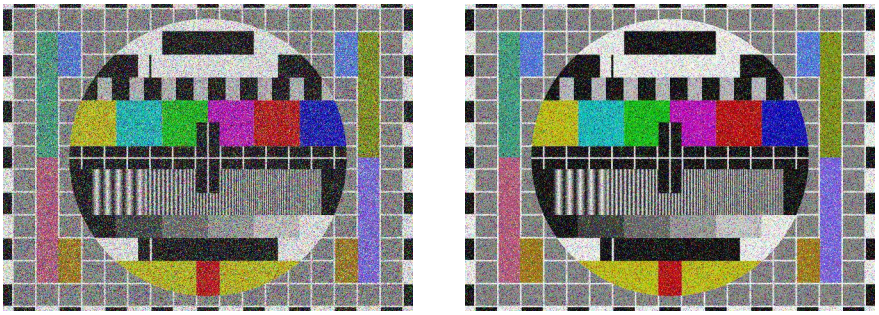


Fig. 4.65. Evolución de la BER para 40*km*

Aumentando la distancia del enlace en otros 20km, hasta situarlo en 40km, las presta-

ciones vuelven a empeorar.

Siguiendo con la lógica de apartados anteriores, calculamos la relación entre ambos sistemas $\eta_{40km} = \frac{1{,}083614 \cdot 10^{-1}}{1{,}643874 \cdot 10^{-1}} = 0{,}67$, donde vemos como a medida que aumentamos la longitud a recorrer más parecidas son las tasas de error de ambos sistemas.



(a) (b)

Fig. 4.66. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para $40km$

(a) (b)

Fig. 4.67. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para $40km$

Enlace de $60km$

Como podemos ver en la gráfica 4.68, la relación entre ambos sistemas para este caso es $\eta_{60km} = \frac{2{,}191254 \cdot 10^{-1}}{2{,}690379 \cdot 10^{-1}} = 0{,}81$. Ambas tasas de error como vemos en la relación anterior se asemejan más y más.

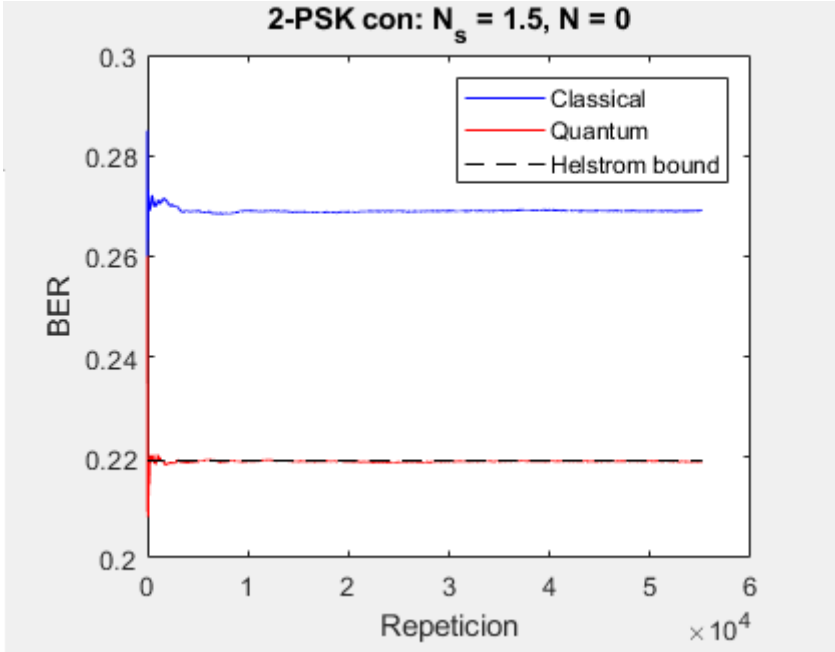
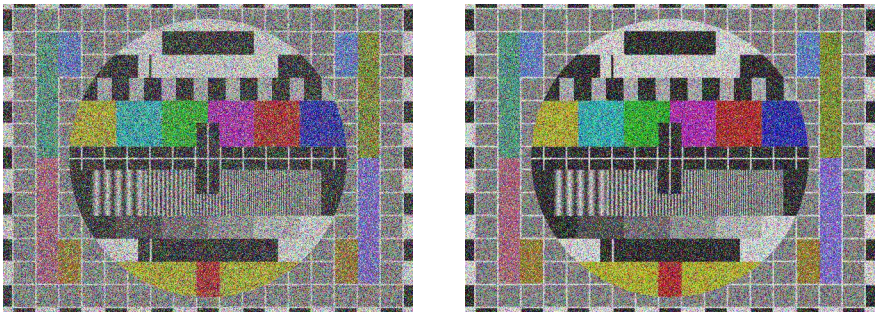


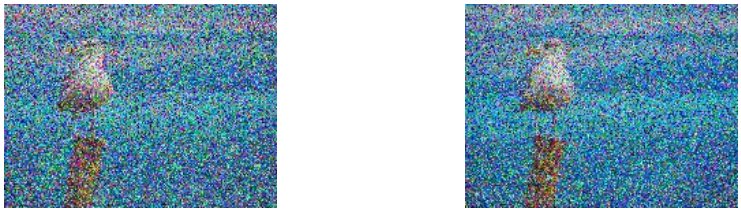
Fig. 4.68. Evolución de la BER para 60*km*

Una vez más, las imágenes resultantes de esta ejecución se muestran a continuación.



(a) (b)

Fig. 4.69. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para 60*km*



(a) (b)

Fig. 4.70. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para 60*km*

Enlace de 80*km*

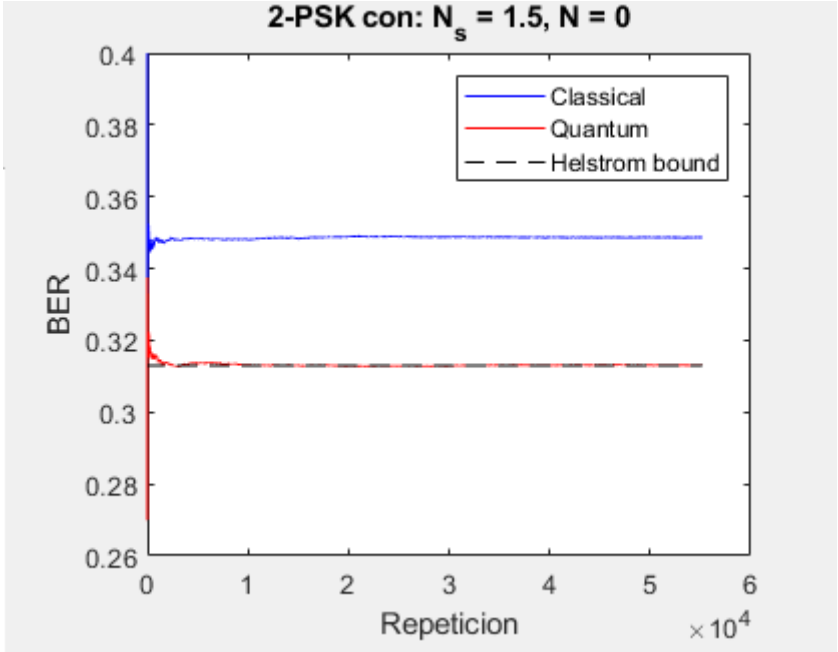
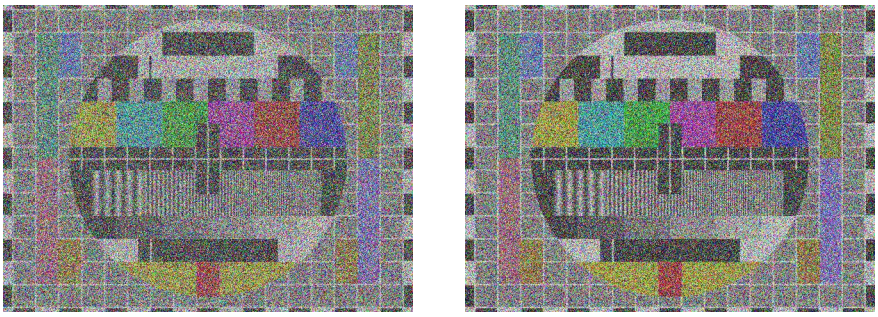


Fig. 4.71. Evolución de la BER para 80*km*

Al separar ambos extremos de la comunicación 80km, una distancia más que considerable, nos situamos ya en tasas de error cercanas a 0,4, rozando una detección aleatoria.

Vemos como, al calcular el coeficiente de tasas de error, se produce un cambio sustancial y es que, en este caso, la aproximación entre ambos sistemas se ralentiza drásticamente. Concretamente, tenemos $\eta_{80km} = \frac{3{,}130114 \cdot 10^{-1}}{3{,}486686 \cdot 10^{-1}} = 0{,}89$.

Si nos fijamos, en los casos anteriores el similitud entre el sistema cuántico y el clásico crecía a razón de entre 0,15 y 0,29. No obstante, para el incremento de 20*km* actual (60km a 80km) ese acercamiento ha sido de 0,08, aproximadamente la mitad que en el menor de los acercamientos anteriores.



(a) (b)

Fig. 4.72. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para 80km

(a) (b)

Fig. 4.73. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para 80km

Enlace de 100km

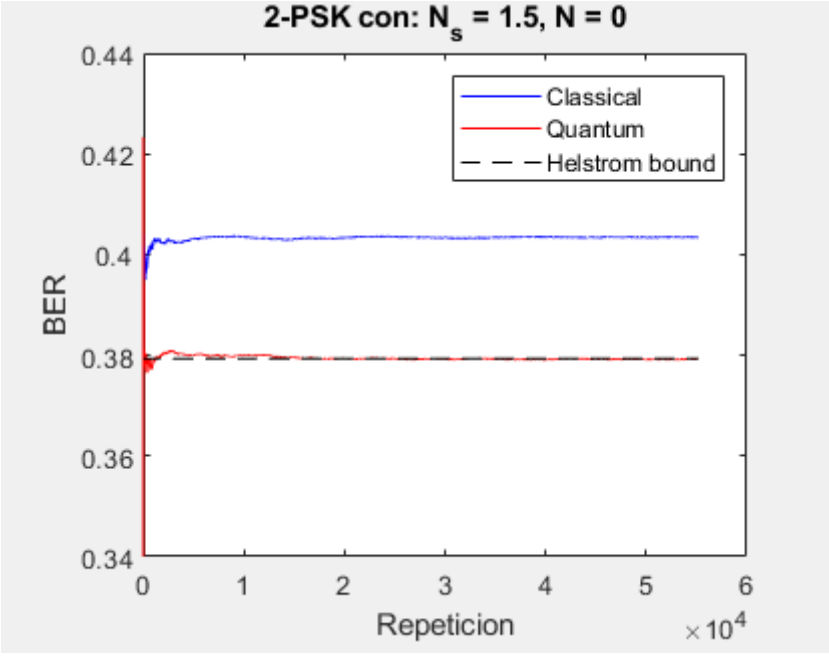
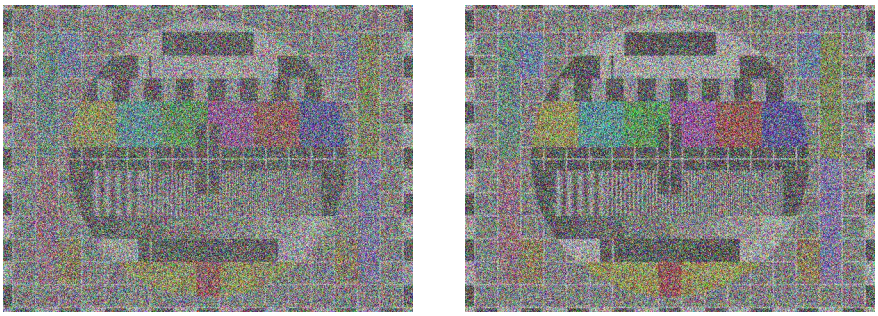


Fig. 4.74. Evolución de la BER para 100km

Volviendo a calcular el coeficiente ya somos capaces dar respuesta a la pregunta plan-

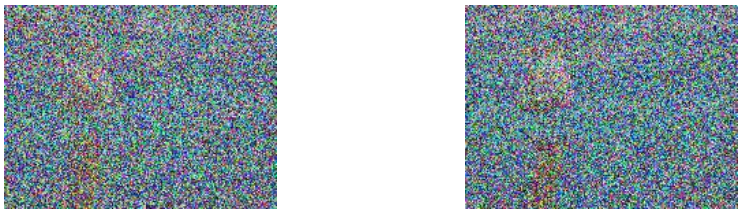
teada algunos apartados atrás. Considerando un canal de $100km$, $\eta_{100km} = \frac{3{,}792560 \cdot 10^{-1}}{4{,}034416 \cdot 10^{-1}} = 0{,}94$. Al igual que ocurrió en el canal de 80km, el acercamiento entre las prestaciones de ambos sistemas vuelve a frenar, creciendo solamente en 0,05.

Podemos ver en las imágenes siguientes una gran cantidad de los píxeles de la imagen recibida son ruidosos.



(a) (b)

Fig. 4.75. Carta de ajuste recibida a través del sistema clásico (a) y cuántico (b) para $100km$



(a) (b)

Fig. 4.76. Gaviota recibida a través del sistema clásico (a) y cuántico (b) para $100km$

Contraste de los resultados obtenidos con valores teóricos

Al igual que para el análisis del efecto del ruido térmico, se organizan tanto tasas de error teóricas como prácticas de las ejecuciones en dos tablas.

Hay que recordar que tras el uso de una modulación cuaternaria, hemos vuelto a una modulación binaria, donde cada bit es un símbolo y por tanto la probabilidad de error de símbolo es igual a la probabilidad de error de bit.

Distancia	$L = 0km$	$L = 20km$	$L = 40km$
Sistema clásico	$8{,}153127 \cdot 10^{-2}$	$6{,}110980 \cdot 10^{-2}$	$1{,}647406 \cdot 10^{-1}$
Sistema cuántico	$2{,}933889 \cdot 10^{-2}$	$2{,}349032 \cdot 10^{-2}$	$1{,}083303 \cdot 10^{-1}$

Distancia	$L = 60km$	$L = 80km$	$L = 100km$
Sistema clásico	$2{,}691836 \cdot 10^{-1}$	$3{,}489274 \cdot 10^{-1}$	$4{,}032480 \cdot 10^{-1}$
Sistema cuántico	$2{,}193031 \cdot 10^{-1}$	$3{,}129802 \cdot 10^{-1}$	$3{,}793300 \cdot 10^{-1}$

TABLA 4.5. PROBABILIDADES DE ERROR OBTENIDAS DE LAS FÓRMULAS ANALÍTICAS (TEÓRICAS)

Distancia	$L = 0km$	$L = 20km$	$L = 40km$
Sistema clásico	$8{,}153127 \cdot 10^{-2}$	$6{,}079516 \cdot 10^{-2}$	$1{,}643874 \cdot 10^{-1}$
Sistema cuántico	$2{,}933889 \cdot 10^{-2}$	$2{,}342478 \cdot 10^{-2}$	$1{,}083614 \cdot 10^{-1}$

Distancia	$L = 60km$	$L = 80km$	$L = 100km$
Sistema clásico	$2{,}690379 \cdot 10^{-1}$	$3{,}486686 \cdot 10^{-1}$	$4{,}034416 \cdot 10^{-1}$
Sistema cuántico	$2{,}191254 \cdot 10^{-1}$	$3{,}130114 \cdot 10^{-1}$	$3{,}792560 \cdot 10^{-1}$

TABLA 4.6. PROBABILIDADES DE ERROR OBTENIDAS DE LAS EJECUCIONES

Al igual que en todos los casos anteriores, las probabilidades de ambas tablas son muy similares, por lo que podemos intuir el correcto funcionamiento del emulador.

Conclusiones acerca del efecto de la atenuación sobre los sistemas clásico y cuántico

Las ejecuciones anteriores demuestran que lo que está ocurriendo no es que la tasa de error del sistema cuántico se acerque a la del sistema clásico porque sea más vulnerable o sensible a la atenuación introducida por el medio, sino que, según aumentamos la longitud del enlace (y por lo tanto, la atenuación), las tasas de error de ambos sistemas comienzan a incrementarse puesto que cada vez la señal recibida se parece menos a la que fue transmitida. El caso límite será cuando la atenuación fuese total, equivalente a una transmisión con $N_s = 0 \ \frac{fotones}{simbolo}$. En este caso, el receptor estaría decidiendo aleatoriamente ya que no tiene nada que le aporte certidumbre sobre lo que se transmitió.

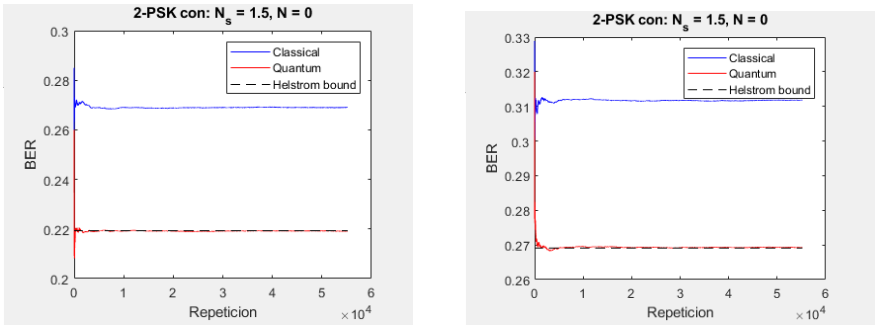
Por lo tanto, no debemos decir que las prestaciones del sistema cuántico se estén acercando a las del sistema clásico, sino que su probabilidad de error se está acercando a 0,5 al igual que la del sistema clásico y es por esto por lo que ambas tasas de error cada vez se parecen más entre sí.

Por todo esto, podemos concluir que el efecto que tiene la atenuación introducida por el medio afectará a ambos sistemas por igual, al contrario que ocurre con el ruido térmico como se demostró en los apartados "Efecto del ruido térmico en sistemas de comunicaciones clásico y cuántico sobre una modulación BPSK" y "Efecto del ruido térmico en sistemas de comunicaciones clásico y cuántico sobre una modulación QPSK"

Canal de espacio libre

En el presente apartado no se pretende analizar cómo afecta la atenuación introducida por un canal de espacio libre a cada uno de los sistemas ya que las conclusiones obtenidas para el canal de fibra óptica son perfectamente extrapolables al presente caso. El objetivo, en cambio, es mostrar al lector cómo la atenuación introducida por el espacio libre es mucho más violenta que la que introduce el canal de fibra óptica.

Para ello, se mostrarán dos ejemplos: el primero de ellos para una distancia de 60km sobre fibra óptica; el segundo, para una distancia de 50m sobre espacio libre.



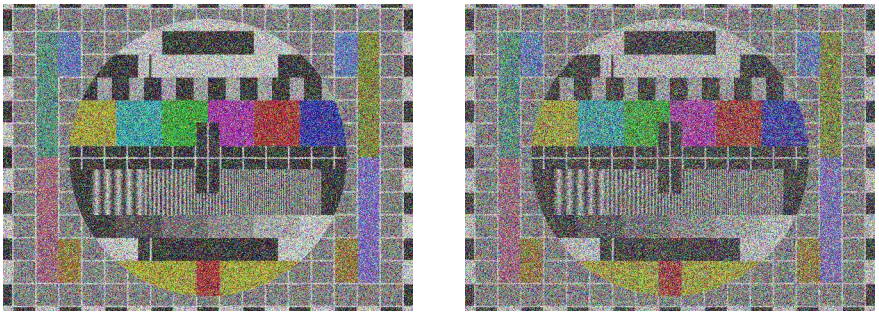
(a) (b)

Fig. 4.77. BER para una transmisión utilizando un canal de fibra óptica de 60km (a) y uno de espacio libre de 50m (b)

Comparando las dos imágenes de la figura 4.77 alertamos como las tasas de error de bit obtenidas para el canal de espacio libre son peores que las del canal de fibra óptica. En otras palabras, incrementar la distancia en 60km desde la no atenuación en fibra óptica

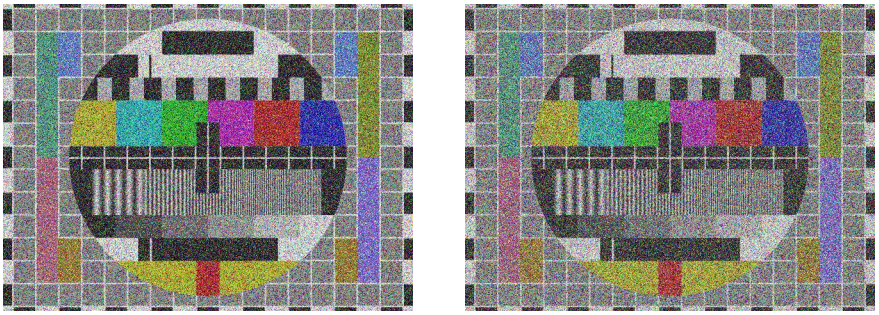
(0m) introduce un menor error que aumentar 40m en espacio libre desde la no atenuación (10m). Así, confirmamos lo manifestado anteriormente: la atenuación introducida por un canal de espacio libre es mucho más agresiva que la introducida por uno de fibra óptica

De hecho, si comparamos las imágenes recibidas con un canal de 60km de fibra óptica y con un canal de 50m de espacio libre (para las antenas utilizadas) nos damos cuenta de que los resultados son muy similares (desde figura 4.78 a figura 4.81), siendo los del canal de espacio libre incluso peores.



(a) (b)

Fig. 4.78. Cartas de ajuste recibidas clásicamente a través de 60km de fibra óptica (a) y 50m de espacio libre (b)

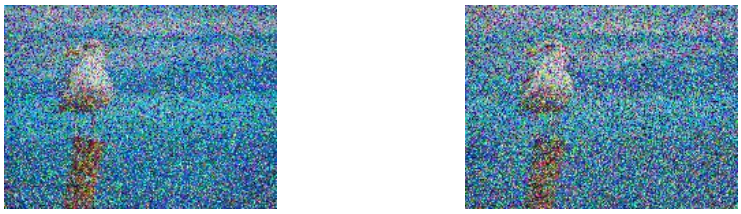


(a) (b)

Fig. 4.79. Cartas de ajuste recibidas cuánticamente a través de 60km de fibra óptica (a) y 50m de espacio libre (b)

(a) (b)

Fig. 4.80. Gaviotas recibidas clásicamente a través de 60km de fibra óptica (a) y 50m de espacio libre (b)



(a) (b)

Fig. 4.81. Gaviotas recibidas cuánticamente a través de 60km de fibra óptica (a) y 50m de espacio libre (b)

Ejemplo del emulador en la zona de interés

A pesar de que las ejecuciones anteriores han sido útiles para poder comprobar como afectan el ruido térmico y la atenuación a los sistemas de comunicaciones clásico y cuántico, la ventaja que en el mejor de los casos es capaz de ofrecer el sistema cuántico no parece abismal (una década) como para invertir en la investigación y el desarrollo que requiere este tipo de comunicaciones. Además, esta ventaja máxima se consigue únicamente en condiciones de ausencia de ruido térmico, que es algo que muy difícil de conseguir en la práctica.

No obstante, esta sensación puede disiparse con la gráfica 4.82.

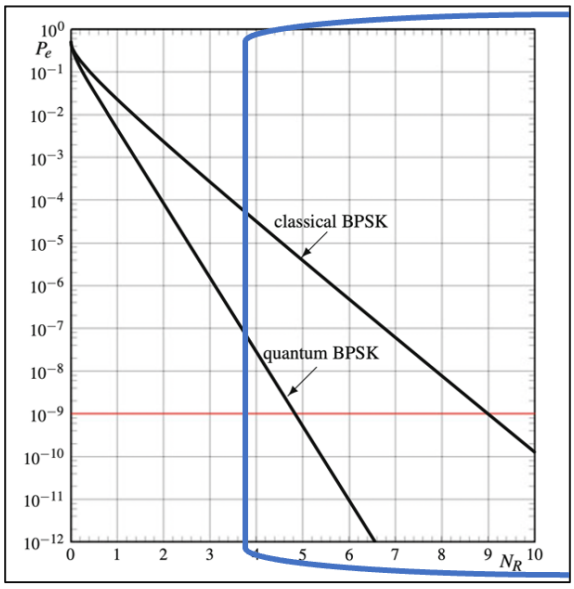


Fig. 4.82. Tasas de error de “Quantum Communications” de Gianfranco Cariolaro [10]

Podemos ver como en la zona en la que trabajamos ($N_s = 1{,}5$) las diferencias entre ambos sistemas son muy pequeñas en comparación con la zona marcada en la imagen ($N_s \geq 4$).

El emulador desarrollado también es capaz de trabajar en esa zona, pero para ello necesitaríamos utilizar una imagen lo suficientemente grande como para obtener una probabilidad de error realista. Por ejemplo, para $N_s = 4$, la tasa de error esperada para el caso sin ruido es de aproximadamente $3{,}5 \cdot 10^{-8}$. Si introdujésemos, por ejemplo, la carta de ajuste utilizada en las ejecuciones anteriores, transmitiríamos 5529600 bits. Si no hubiese ningún bit erróneo, la tasa de error sería 0, por debajo del límite de *Helstrom*, lo que no es correcto. Si por el contrario hubiese un bit erróneo, la tasa de error sería $1{,}8 \cdot 10^{-7}$, claramente por encima del límite de *Helstrom* que en esta situación deberíamos alcanzar. Ésto se debe a que para que las tasas de error obtenidas tengan sentido, la imagen introducida debe ser los suficientemente grande.

Para poder hacer todos los ejemplos en esa zona que hemos denominado de interés, deberíamos utilizar una imagen de unos 100 millones de bits, para lo que el programa necesitaría ejecutarse durante varios días para cada caso analizado. Esta necesidad de capacidad computacional unido a que las ejecuciones con $N_s = 1{,}5$ nos permiten perfectamente evaluar las propiedades de ambos sistemas ha provocado que se haya decidido trabajar con un N_s menor, fuera de la zona de interés.

A pesar de ello, a modo de ejemplo, se incluye una ejecución para $N_s = 4$, de forma que se pueda demostrar el correcto funcionamiento de este emulador también en esta zona. Podemos ver, en la imagen 4.83, la evolución de la BER obtenida.

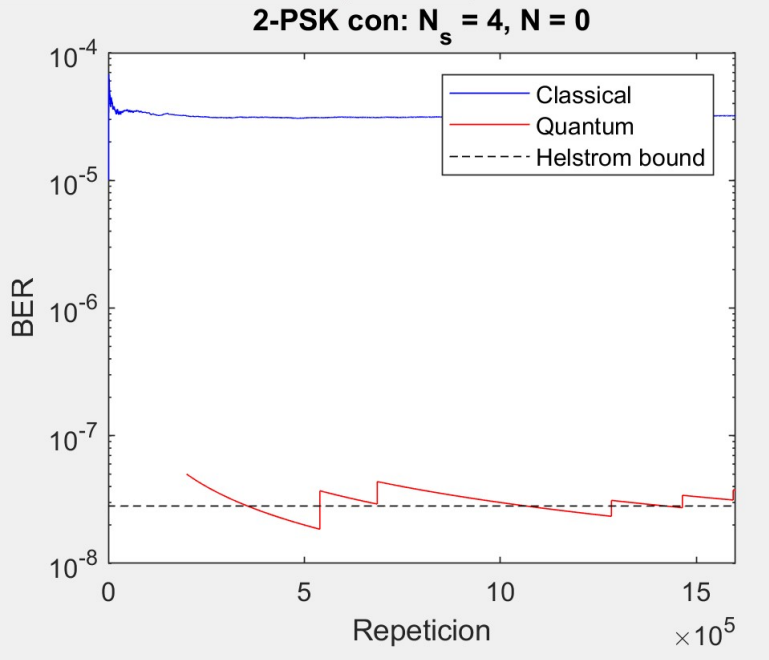


Fig. 4.83. Evolución de la BER obtenida en la zona de interés

Debemos destacar que, para este caso, al ser la diferencia entre ambos sistemas tan grande se ha utilizado una escala logarítmica. Vemos que la tasa de error obtenida para el sistema cuántico es del orden de $3 \cdot 10^{-8}$ mientras que la del sistema clásico se sitúa en unos $3 \cdot 10^{-5}$, tres décadas más alta, una diferencia claramente mayor que la década de diferencia que veíamos en el caso sin ruido para $N_s = 1{,}5$.

Además, si comparamos estas tasas de error con las contenidas en la gráfica 4.82, los resultados son muy similares, ya que de las gráficas obtenemos $3{,}5 \cdot 10^{-8}$ y $3{,}5 \cdot 10^{-5}$ para los sistemas cuántico y clásico respectivamente, muy cercanas a las obtenidas del emulador.

5. CONCLUSIONES

A lo largo del presente trabajo hemos podido conocer numerosas cosas acerca de las tecnologías cuánticas tanto de manera teórica como de manera práctica.

En primer lugar hemos visto solo algunas de la ingente cantidad de aplicaciones de estas tecnologías. Nos hemos centrado en aplicaciones relacionadas con las comunicaciones y la computación, pero existen otros muchos ámbitos como la salud donde también pueden tener un gran impacto en el futuro.

No obstante, también hemos aprendido que las implementaciones actuales con estas tecnologías son mínimas, siendo principalmente experimentales.

Pero no todo acerca de las tecnologías cuánticas nos brindará un mejor futuro y es que hemos hecho hincapié en que también pueden llegar a ser un peligro para los algoritmos criptográficos actuales, puesto que la mayoría de ellos basan su seguridad en complejos problemas matemáticos como la factorización de grandes números o el cálculo de logaritmos discretos. A pesar de que este nivel de seguridad computacional puede ser más que suficiente para los ordenadores actuales, en la introducción se incluyó una comparativa donde podíamos ver como claramente los ordenadores cuánticos eran mucho más eficientes en la realización de estas tareas.

Finalmente el montaje del sistema de distribución cuántica de claves y el desarrollo del emulador nos permitió comprender de mejor manera el funcionamiento de estas tecnologías. En concreto, el emulador nos permitió comprender que aunque los sistemas cuánticos son, en condiciones ideales, capaces de ofrecer tasas de error muy por debajo de lo que lo hacen los sistemas clásicos, estos sistemas son mucho más sensibles al ruido térmico. Ésto implica que en una situación más realista en cuanto a temperatura no podamos aprovechar todas las bondades que nos ofrecen estas tecnologías.

Cabe destacar que unas primeras conclusiones acerca de la comparativa entre sistemas clásicos y cuánticos utilizando este mismo emulador (cuando aún se encontraba en fase de desarrollo) fueron expuestas en los congresos DESEi+D (podemos ver un resumen de lo presentado en [32]) y en el EIE de ingeniería espacial, ambos en 2020.

Por todo lo anterior queda claro que las tecnologías cuánticas tienen un gran potencial para marcar un antes y un después en la vida diaria de todos nosotros debido a las reglas que las rigen y que no tienen contraparte clásica.

No sólo debido a los fenómenos que han sido estudiados en el presente trabajo como la no clonación o la aleatoriedad de las medidas cuánticas es que debemos mirar esperanzados el futuro de las aplicaciones cuánticas. También otros fenómenos como el entrelazamiento cuántico o la teleportación generarán gran interés. El entrelazamiento nos permite, cuando dos fotones están entrelazados, averiguar unívocamente el resultado que obtendríamos al hacer una medida sobre un fotón midiendo sobre el otro. Este fenómeno se mantiene para cualquier distancia que separe a los fotones. Por su parte, la teleportación cuántica nos permite replicar el estado de un fotón en otro fotón a distancia (sin conocer dicho estado) mediante entrelazamiento. A pesar de que la mayoría de implementaciones cuánticas de criptografía y de comunicación utilizan los protocolos, propiedades y leyes abordados en profundidad en este trabajo, son muchos los protocolos desarrollados aprovechando otras características de las tecnologías cuánticas.

Por ello, las tecnologías cuánticas no nos ofrecen un futuro prometedor sólo por lo que hemos podido conocer de ellas gracias a las pequeñas implementaciones actuales y los fundamentos teóricos, sino por todas aquellas particularidades que no tienen un equivalente clásico y que, por lo tanto, aún no se conoce con total certeza la gran cantidad de aplicaciones que podrían llegar a tener.

Además de esas aplicaciones aún inexploradas, debemos tener en cuenta no sólo qué podemos llegar a crear, sino también los beneficios sociales y económicos que pueden derivar de estos avances. De hecho, teniendo en cuenta, por ejemplo, el poder transformador que está teniendo en la actualidad el 5G siendo "únicamente" el nuevo estándar de comunicaciones móviles, el cambio social y económico que podrían traer unas innovaciones tan radicales éstas es inimaginable y, sin duda, muy prometedor.

Sin embargo, a pesar de tener las condiciones necesarias para cambiar nuestra vida por completo también plantean un reto muy complejo que requiere mucho trabajo, tiempo y dinero para poder comprender y utilizar todas sus características de la manera adecuada, además de para descubrir todas las áreas de estudio en las que pueden tener un impacto significativo. Un ejemplo de ésto es el mencionado ruido térmico que, de ser capaces de

reducir su efecto, nos permitiría aprovechar plenamente todas las ventajas ofrecidas por estas tecnologías. Además, esa necesidad de financiación puede atravesar dificultades en un futuro muy cercano debido a la crisis económica que está causando la pandemia del COVID-19 una vez todos los planes de financiación analizados en el apartado 2.5 expiren.

Otro de los problemas a los que se debe hacer frente es a la falta de profesionales altamente cualificados. No obstante, ésto no es un problema único de este campo sino de muchas áreas tecnológicas en general. El incesante avance tecnológico que estamos experimentando en la actualidad hace que la demanda de profesionales con perfiles muy distintos sea en muchos casos mayor que la oferta. Además, son necesarios perfiles muy específicos para el desarrollo de estas tecnologías, por lo que el acceso a esa formación necesaria no siempre es posible.

También es necesario tener en cuenta que no sólo es necesario el desarrollo de las tecnologías cuánticas, sino también de otros sectores como el de la electrónica por ejemplo, los cuales puedan proveer la instrumentación y los avances necesarios para poder acceder a todo el espectro de ventajas que subyacen bajo la mecánica cuántica.

Todo lo anterior hace prever un camino largo y complejo, no sólo hasta estar presentes en la vida cotidiana de la población, sino también hasta poder tener aplicaciones prácticas en entornos profesionales. Los retos son grandes, no obstante la gran inversión que las principales potencias mundiales están haciendo y el desarrollo de otras áreas de la ciencia y la tecnología auguran un futuro muy prometedor de que, en un plazo de 5 a 10 años, podamos ver sus primeras implementaciones 100 % comerciales.

6. APARTADO ECONÓMICO

6.1. Duración trabajo de fin de grado

El trabajo realizado hasta la finalización de este trabajo puede dividirse en tres partes bien diferenciadas:

1. Estudios en criptografía cuántica.
2. Estudios en comunicaciones cuánticas.
3. Desarrollo del TFG.

Estudios en criptografía cuántica

La parte de criptografía cuántica se dividió, a su vez, en:

1. Base teórica: julio 2019 - septiembre 2019.
2. Montaje del sistema cuántico de distribución de claves: septiembre 2019 - octubre 2019.
3. Memoria del trabajo realizado: octubre 2019 - diciembre 2019.

Estudios en comunicaciones cuánticas

La fase de las comunicaciones cuánticas se dividió en:

1. Base teórica: marzo 2020 - julio 2020.
2. Desarrollo del emulador: agosto 2020 - febrero 2021.

Desarrollo del TFG

Finalmente, la escritura del presente trabajo de fin de grado se produjo entre los meses de febrero de 2021 y abril de 2021.

6.2. Presupuesto

El presente trabajo de fin de grado ha generado unos costes en lo referente a:

- Salarios.
- Equipos informáticos.
- Kit de distribución cuántica de clave.

Salarios

El salario mensual percibido desde julio de 2019 (la parte en la que se cubrió el *set-up* de THORLABS) hasta abril de 2021 (fecha de finalización del trabajo de fin de grado) ha sido de 608,83, lo que hace una cantidad total de $22 \cdot 608{,}53 = 13387{,}66$

Equipos informáticos

El ordenador utilizado para realizar el trabajo tiene un PVP de 1449,00

Kit de distribución cuántica de clave

El kit utilizado para el montaje y demostración de un sistema de distribución cuántica de claves es de la marca THORLABS y, según su página web [33], tiene un precio de venta al público de 3224,41.

Presupuesto total

Utilizando las cantidades anteriores, podemos comprobar que el precio valor económico del presente trabajo de fin de grado es de:

$$13387{,}66 + 1449{,}00 + 3224{,}41 = 18061{,}07$$

BIBLIOGRAFÍA

[1] D. C. LAY, "Álgebra lineal y sus aplicaciones," en, 3.ª ed. Pearson, 2007, cap. Espacios Vectoriales, pp. 215-300.

[2] G. Cariolaro, "Quantum Communications," en. Springer, 2015, cap. Vector and Hilbert Spaces, pp. 21-75.

[3] ——, "Quantum Communications," en. Springer, 2015, cap. Introduction to Part II: Quantum Communications, pp. 133-181.

[4] L. Susskind y A. Friedman, "Quantum Mechanics: The Theoretical Minimum," en. Basic Books, 2014, cap. Systems and Experiments, pp. 1-35.

[5] G. Cariolaro, "Quantum Communications," en. Springer, 2015, cap. Elements of Quantum Mechanics, pp. 77-129.

[6] M. Giles, "Explainer: ¿What is post-quantum cryptography?," jul. de 2019. [En línea]. Disponible en: https://www.technologyreview.com/2019/07/12/134211/explainer-what-is-post-quantum-cryptography/.

[7] W. K. Wootters y W. H. Zurek, "The no-cloning theorem," *Physics Today*, vol. 62, n.º 2, pp. 76-77, 2009.

[8] G. Cariolaro, "Quantum Communications," en. Springer, 2015, cap. Applications of Quantum Information, pp. 639-663.

[9] ——, "Quantum Communications," en. Springer, 2015, cap. Quantum Communications Systems with Thermal Noise, pp. 361-420.

[10] ——, "Quantum Communications," en. Springer, 2015, cap. Quantum Communications Systems, pp. 281-359.

[11] ——, "Quantum Communications," en. Springer, 2015, cap. Quantum Decision Theory: Analysis and Optimization, pp. 183-249.

[12] ——, "Quantum Communications," en. Springer, 2015, cap. Quantum Decision Theory: Suboptimization, pp. 251-280.

[13] S. Wehner et al., "Quantum internet: A vision for the road ahead," *Science*, vol. 362, n.º 6412, 2018. [En línea]. Disponible en: https://doi.org/10.1126/science.aam9288.

[14] M. Caleffi et al., "The Rise of the Quantum Internet," *Computer*, vol. 53, n.º 6, pp. 67-72, 2020. [En línea]. Disponible en: 10.1109/MC.2020.2984871.

[15] R. Orús et al., "Quantum computing for finance: Overview and prospects," *Reviews in Physics*, vol. 4, p. 100 028, 2019. DOI: https://doi.org/10.1016/j.revip.2019.100028. [En línea]. Disponible en: https://www.sciencedirect.com/science/article/pii/S2405428318300571.

[16] S. M. Hamdi et al., "A Compare between Shor's quantum factoring algorithm and General Number Field Sieve," en *2014 International Conference on Electrical Engineering and Information Communication Technology*, 2014, pp. 1-6. DOI: 10.1109/ICEEICT.2014.6919115.

[17] T. L. Rodney Van Meter Kohei Itoh, 2006. [En línea]. Disponible en: arXiv:quant-ph/0507023v2.

[18] J. Biamonte et al., "Quantum machine learning," *Nature*, vol. 549, pp. 195-202, sep. de 2017. [En línea]. Disponible en: https://doi.org/10.1038/nature23474.

[19] "IDQ Celebrates 10-Year Anniversary of the World's First Real-Life Quantum Cryptography Installation," IDQuantique, inf. téc., nov. de 2017. [En línea]. Disponible en: https://www.idquantique.com/idq-celebrates-10-year-anniversary-of-the-worlds-first-real-life-quantum-cryptography-installation/.

[20] "Use Case: Government," IDQuantique, inf. téc., 2017. [En línea]. Disponible en: https://marketing.idquantique.com/acton/attachment/11868/f-020f/1/-/-/-/-/Geneva%20Govt_%20DCI%20QKD%20Use%20Case.pdf.

[21] J. Yin et al., "Quantum Science Experiments with Micius Satellite," en *2019 Conference on Lasers and Electro-Optics (CLEO)*, 2019, pp. 1-2. DOI: 10.1364/CLEO_AT.2019.JTu3G.4.

[22] A. Nordrum, "China Demonstrates Quantum Encryption By Hosting a Video Call," *IEEE Spectrum*, oct. de 2017. [En línea]. Disponible en: https://spectrum.ieee.org/tech-talk/telecom/security/china-successfully-demonstrates-quantum-encryption-by-hosting-a-video-call.

[23] S.-K. Liao et al., "Satellite-Relayed Intercontinental Quantum Network," Austrian Academy of Sciences, inf. téc., ene. de 2018.

[24] *Overview on quantum initiatives worldwide*, 2021. [En línea]. Disponible en: https://www.qureca.com/overview-on-quantum-initiatives-worldwide/.

[25] *Introduction to the Quantum Flagship*. [En línea]. Disponible en: https://qt.eu/about-quantum-flagship/introduction-to-the-quantum-flagship/.

[26] S. O. Q. I. S. C. O. Science, "National Quantum Initiative Supplement To The President's FY 2021 Budget," National Science & Technology Council, inf. téc., 2021.

[27] E. B. Kania, "China's Quantum Future," Center for a New American Security, inf. téc., sep. de 2017. [En línea]. Disponible en: https://www.cnas.org/publications/commentary/chinas-quantum-future.

[28] E. Gibney, "Quantum gold rush: the private funding pouring into quantum start-ups," *Nature*, vol. 574, oct. de 2019. [En línea]. Disponible en: https://www.nature.com/articles/d41586-019-02935-4.

[29] P. Knight e I. Walmsley, "UK national quantum technology programme," *Quantum Science and Technology*, vol. 4, n.º 4, sep. de 2019. [En línea]. Disponible en: https://doi.org/10.1088/2058-9565/ab4346.

[30] *Quantum Cryptography Demonstration Kit*, THORLABS, 56 Sparta Avenue, Newton, New Jersey 07860, United States, 2016.

[31] W. Commons, *File:Philips PM5544.svg — Wikimedia Commons, the free media repository*, 2021. [En línea]. Disponible en: https://commons.wikimedia.org/w/index.php?title=File:Philips_PM5544.svg&oldid=530730169.

[32] *VII Congreso Nacional de I+d en Defensa y Seguridad*, Resúmenes, Ministerio de Defensa, nov. de 2020.

[33] 56 Sparta Avenue, Newton, New Jersey 07860, United States: THORLABS. [En línea]. Disponible en: https://www.thorlabs.com/newgrouppage9.cfm?objectgroup_id=9869.