Emulador de un sistema de comunicaciones cuántico

Carnoto, Isabel[1, *]; Nevado, Julio[1, *]; Fajardo, Pablo[1]; García, Enrique[1]

[1] Universidad Carlos III de Madrid (UC3M). Avda. Universidad 30, 28911. Leganés.

***** Ambos autores han contribuido por igual; icarnoto@ing.uc3m.es junevado@ing.uc3m.es

.

Resumen: Este artículo presenta un emulador cuántico capaz de comparar la transmisión de información por medio de un sistema de comunicaciones clásico y por medio de un sistema de comunicaciones cuántico. Esta comparación podrá hacerse de manera cuantitativa, por medio de las tasas de error de bit para cada sistema, pero también cualitativamente por medio de la confrontación de dos imágenes, una transmitida bajo las reglas de un sistema clásico, y otra transmitida bajo las reglas de uno cuántico. Estas "transmisiones" se realizarán en función de una serie de parámetros como la temperatura o la potencia de la señal generada, de tal manera que podremos analizar cómo se comportarían los respectivos sistemas reales en distintas situaciones. Como es lógico, antes de comenzar con el estudio del emulador, daremos unas nociones sobre la importancia de las comunicaciones cuánticas y acerca de los conceptos fundamentales que rigen el programa. Finalmente, se expondrán resultados y conclusiones de la comparativa.

Palabras clave: Clave, Comunicación, Cuántico, Emulador, Fotón, Temperatura.

---

1. Introducción

El interés por las comunicaciones cuánticas ha aumentado significativamente en los últimos años debido a la alta fiabilidad que son capaces de proporcionar frente a los sistemas de comunicaciones clásicos [1]. Avances tecnológicos se pueden apreciar, no solo en comunicaciones, sino también en otros ámbitos como la computación cuántica [2].

Empresas como IBM, Google y Microsoft se encuentran en una carrera para alcanzar la supremacía cuántica, intentando crear un ordenador cuántico capaz de resolver problemas que ni las mejores supercomputadoras actuales pueden resolver [3]. En 2018 Huawei, Telefónica y la Universidad Politécnica de Madrid demostraron la aplicación de criptografía cuántica en redes ópticas comerciales [4] y en 2020 científicos de China lograron la

transmisión de un mensaje cifrado con tecnología cuántica desde un satélite espacial, rompiendo el récord de la distancia más larga en una comunicación cuántica [5].

En este estudio emulamos la transmisión de información cifrada por medio de un protocolo de criptografía cuántica, a través de fibra óptica, utilizando un sistema de comunicaciones clásico y uno cuántico, tomando en cuenta el efecto del ruido térmico y la atenuación propia de la fibra óptica, con el fin de comparar las prestaciones de ambos sistemas en diversas condiciones.

2. Materiales y métodos

2.1 Sistemas de Telecomunicaciones

De forma general podemos describir un sistema de telecomunicaciones utilizando un diagrama de bloques como el de la Figura 1. La fuente de información emite un mensaje, que puede ser voz, imagen, texto o cualquier otro. El transmisor convierte el mensaje en un estado o en una señal, como una onda electromagnética o radiación óptica emitida por un láser. Esta señal es transmitida a través de un canal físico, donde se ve afectada por el ruido y la atenuación propia del canal. En el extremo receptor, se obtiene una versión distorsionada de la señal transmitida. Finalmente, el receptor extrae, de esta señal, una réplica aproximada del mensaje original.

Figura 1. Diagrama de bloques de las partes esenciales de un sistema de telecomunicaciones; adaptada de [6].

Para explicar y comparar los sistemas de comunicaciones clásico y cuántico, damos como ejemplo uno de los métodos utilizados en este estudio para la transmisión de información entre dos puntos.

La modulación 2-PSK clásica consiste en modular en fase una señal portadora, como por ejemplo una sinusoide, para transmitir símbolos dentro de un alfabeto finito. En este caso el alfabeto es binario, donde los símbolos {1, -1} representan los bits {0, 1}, respectivamente. El símbolo '1' se transmite como $v_T(t) = V_0 \cos(2\pi v t)$, y el '-1' como la misma señal, pero desfasada noventa grados, $v_T(t) = V_0 \cos(2\pi v t + \pi)$. La amplitud V_0 es calculada a partir del periodo de símbolo (T) el cual está limitado por el ancho de banda, la frecuencia (v) y la constante de Planck (h) según la siguiente fórmula [6]:

$$V_0 = \sqrt{\frac{N_s\, h\, v}{T}}$$

La amplitud V_0 también depende del número promedio de fotones de señal (N_s), que es el número de fotones que en media se generan en un haz del láser por segundo. Nos referimos a estos en media ya que no son generados de manera equiespaciada en el tiempo. A mayor potencia del láser, mayor intensidad de fotones se estarán generando.

En la modulación 2-PSK cuántica el transmisor prepara dos estados cuánticos, uno para representar cada símbolo. En este caso los estados, denominados estados coherentes, se modelan a partir de la radiación coherente de un láser, como se muestra en la siguiente fórmula [6]:

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

Donde α en un estado coherente genérico puede ser un número complejo cualquiera, sin embargo, en una 2-PSK, α será $+1$ ó -1 y su módulo al cuadrado representa el número promedio de fotones en dicho estado, siendo igual a N_s. Por su parte, $|n\rangle$ representa un estado que contiene exactamente *n* fotones. En ambos casos la información modulada es enviada a través del canal, en nuestro caso una fibra óptica, donde sufre los efectos del ruido térmico y de la atenuación característica de la fibra.

La atenuación introducida por la fibra, que viene determinada por un parámetro β expresado en dB/Km y por la longitud de la misma, crece exponencialmente cuando dicha distancia aumenta. Si bien en ambos casos esta atenuación supone una reducción de la potencia, en el caso clásico modelaremos este fenómeno como un decremento en la amplitud (V_0) de la señal modulada, mientras que en el caso cuántico lo haremos como un decremento en el número promedio de fotones transmitidos.

El segundo efecto que tenemos en cuenta es el ruido térmico. El ruido térmico lo cuantificamos como el número promedio de fotones térmicos radiados a una cierta frecuencia (*v)* y a una temperatura (T_0*)*, de acuerdo con la siguiente ecuación [6]:

$$N = \frac{1}{e^{\left(\frac{hv}{kT_0}\right)} - 1}$$

donde *h* es la constante de Planck y *k* es la constante de Boltzmann.

Sin embargo, no solo afectarán a nuestro sistema aquellos fotones que se encuentren dentro del ancho de banda de nuestra señal, sino también todos los que se radien dentro del ancho de banda de nuestro soporte físico, que es la fibra, ya que es la parte de nuestro sistema que se calienta. Por ello, obtendremos el número de fotones como la integral de la expresión anterior para todo el ancho de banda del canal que utilizamos en la fibra.

2.2 Distribución de claves cuánticas

Muchas comunicaciones actualmente son cifradas utilizando algoritmos como RSA, Diffie Hellman, entre otros. En estos algoritmos la seguridad radica en la alta dificultad de resolver complejos problemas matemáticos, como la factorización de números enteros o el cálculo de logaritmos discretos en un cuerpo finito. Estos métodos han probado ser seguros frente a las capacidades de cómputo de los ordenadores actuales, pero esta seguridad se ve amenazada por el rápido avance de los ordenadores cuánticos.

En este estudio utilizamos un protocolo de cifrado basado en los principios de la mecánica cuántica, llamado BB84, para encriptar los datos a transmitir. Este protocolo se fundamenta principalmente en dos teoremas: la no-clonación y la verdadera aleatoriedad.

En primer lugar, el teorema de no-clonación sostiene que información cuántica arbitraria no puede ser copiada [6]. Esto se debe a que, de manera general, cuando nosotros medimos un sistema cuántico desconocido obtenemos una medida aleatoria y además alteramos la información del sistema.

La aleatoriedad en los bits utilizados en las claves de cifrado es sumamente importante para mantener la seguridad de la información, sin embargo, los ordenadores actuales solo son capaces de generar secuencias pseudoaleatorias [7]. Esto puede suponer un gran problema puesto que estas secuencias pseudoaleatorias suelen generarse a partir de una *seed*, que en caso de ser conocida por nuestro adversario podría comprometer seriamente la seguridad del sistema. Los principios de la física cuántica nos ofrecen formas de obtener una secuencia verdaderamente aleatoria como se menciona en el teorema anterior.

El protocolo BB84 utiliza cuatro estados cuánticos ortogonales dos a dos y pertenecientes a dos bases distintas. La base $B^+ = \{|\gamma_0^+\rangle, |\gamma_1^+\rangle\}$ representa los bits '0' y '1' en base "+" y la base $B^x = \{|\gamma_0^x\rangle, |\gamma_1^x\rangle\}$ representa los bits '0' y '1' en base "x", respectivamente[3]. El transmisor elige una secuencia de bits como clave y en qué base transmitirá cada uno de forma aleatoria. El receptor elige también aleatoriamente qué bases usará para medir cada estado recibido. Cuando la base utilizada por ambos extremos coincide, significa que el estado es medido en el receptor usando el operador de la base correspondiente, lo que dará la medida correcta el 100% de las veces, en caso contrario se obtendrá aleatoriamente '0' o '1'. Por último, emisor y receptor intercambian, a través de un canal público, las bases que utilizaron para transmitir y medir, respectivamente. Descartan todos los bits obtenidos con bases distintas y la clave será la secuencia de bits restante [7]. Esta clave es utilizada para cifrar la información antes de ser transmitida y para descifrarla una vez recibida, en ambos casos se utiliza una operación XOR.

3. Resultados y discusión

En nuestro programa, realizado sobre MATLAB [8], emulamos la transmisión de información cifrada tanto sobre un sistema de comunicaciones clásico como sobre un sistema de comunicaciones cuántico, permitiendo así la comparación de ambos. Además, el usuario podrá elegir una serie de parámetros de tal forma que podrá ver como se comportaría cada uno de estos sistemas bajo las condiciones elegidas. Estos parámetros son:

- Número de fotones de señal promedio (N_s): ya explicado anteriormente.
- Temperatura a la que funciona nuestro sistema (T_{emp}): la temperatura determinará la intensidad de fotones ($\mathcal{N}$) que la fibra óptica radia, los cuales distorsionarán la señal en mayor o menor medida (ruido térmico).
- Orden de la modulación utilizada (M): orden de la modulación PSK, orden dos en los ejemplos.
- Longitud del enlace de la fibra óptica (L): determinará la atenuación de la fibra.

En cuanto a la información a transmitir, nuestro código es capaz de digitalizar tanto audios como imágenes, por lo que a parte de los parámetros deterministas del sistema como la BER (*bit error rate*, el número de bits transmitidos de forma errónea sobre los totales) o la $P_{e,símbolo}$, podremos tomar una fotografía o nota de voz y comparar sus respectivas versiones, una obtenida a través del sistema clásico y otra a través del sistema cuántico, pudiendo tener una noción visual o sonora de la distorsión introducida.

Para mostrar el efecto de esa distorsión en este informe, emplearemos una imagen como información a transmitir. Comenzaremos analizando el caso sin ruido térmico e iremos aumentando la temperatura para ver cómo afecta este incremento a cada uno de los sistemas. Por último, para el caso sin ruido, tendremos en cuenta la atenuación de la fibra y analizaremos como cambian las prestaciones al transmitir sobre un enlace de 4km. Compararemos las BER prácticas con las teóricas obtenidas con las siguientes fórmulas [6]:

$$BER_{clásica,teo} = Q\left(\sqrt{\frac{4N_s}{1+2\mathcal{N}}}\right),\ BER_{cuántica,teo} = \frac{1}{2}\sum_i Tr[b_{ii}^* b_{ii}]$$

3.1 *Comparación en función de la temperatura*

3.1.1 *Temperatura* -200℃

En primer lugar, analizaremos el caso en el que apenas exista ruido térmico. Para ello, introducimos una temperatura muy baja de tal manera que los fotones que genera la fibra a causa del calor son prácticamente despreciables. En esta primera transmisión las imágenes obtenidas son las mostradas en la Figura 2.

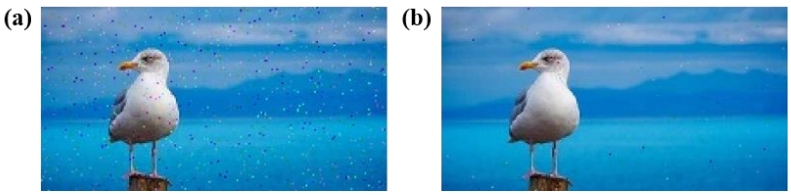


Figura 2. **(a)**Transmisión con sistema clásico. **(b)** Transmisión con sistema cuántico. $T = -200$℃.

Podemos ver que la distorsión (patente en los pixeles de colores discordantes) en la imagen transmitida clásicamente es mucho mayor que en la imagen transmitida a través del sistema cuántico. En cuanto a los parámetros deterministas, se encuentran en la Tabla 1.

Sistema empleado	N_s	Temperatura ($°C$)	Longitud del enlace (m)	BER	$BER_{teórica}$
Clásico	1.5	-200	0	0.0072265	0.0071529
Cuántico	1.5	-200	0	0.00059273	0.00062007

Tabla 1. Comparación de BER para una $T = -200$℃.

3.1.2 *Temperatura* 0℃

En esta transmisión, mantenemos los parámetros anteriores excepto la temperatura, que pasará de los $-200°C$ a los $0°C$. Vemos las dos versiones de la ilustración en la Figura 3.

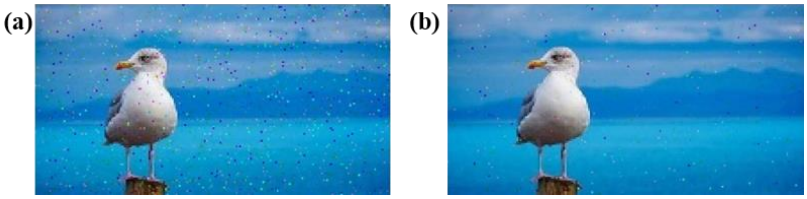


Figura 3. **(a)**Transmisión con sistema clásico. **(b)** Transmisión con sistema cuántico. $T = 0$℃.

En la Tabla 2 se muestran los parámetros de esta la transmisión.

Sistema empleado	N_s	Temperatura ($°C$)	Longitud del enlace (m)	BER	$BER_{teórica}$
Clásico	1.5	0	0	0.0089711	0.0089004
Cuántico	1.5	0	0	0.0021156	0.0021935

Tabla 2. Comparación de BER para una $T = 0℃$.

Podemos apreciar claramente en las imágenes, que el sistema cuántico sigue siendo superior, de hecho, hay cuatro veces menos errores en la transmisión cuántica que en la clásica. Podríamos pensar, por tanto, que el sistema cuántico sigue suponiendo una gran mejora sobre el clásico, sin embargo, al hablar en términos de probabilidad de error una mejora considerable es expresada en décadas, por lo que la mejora que supone el sistema cuántico sobre el clásico no es tan grande como a simple vista pueda parecer. Asimismo, si comparamos estos resultados con la transmisión para $-200℃$, podemos apreciar como el rendimiento del sistema clásico apenas cambia (la BER pasa de 0.0072 *a* 0.0089) mientras que para el sistema cuántico la probabilidad de error se sitúa ya en el mismo orden de magnitud que el sistema clásico (de 0.00059 a 0.00211). Es decir, mientras que el sistema clásico se ha mantenido prácticamente invariante frente al ruido, el sistema cuántico ha sufrido un deterioro notable en sus prestaciones.

3.1.3 *Temperatura* $20℃$

En esta tercera comparación, volvemos a modificar únicamente la temperatura, situándola ahora en $20°C$. El resultado de esta transmisión se muestra en la Figura 4.

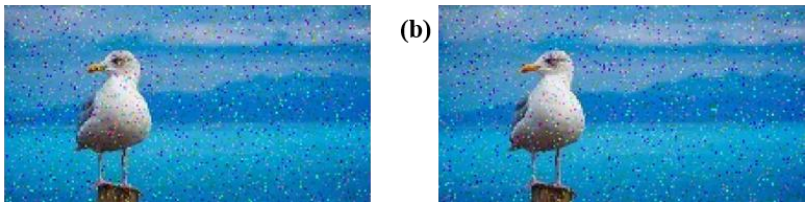


Figura 4. **(a)**Transmisión con sistema clásico. **(b)** Transmisión con sistema cuántico. $T = 20℃$.

Una vez más, al aumentar la temperatura, aumenta la distorsión en ambas imágenes, sin embargo, el hecho más significativo es que ya no apreciamos una mejora del sistema cuántico respecto del clásico, es decir, conforme aumenta la temperatura, la superioridad del sistema cuántico respecto al clásico decae. Los parámetros de esta transmisión quedan reflejados en la Tabla 3.

Sistema empleado	N_s	Temperatura ($°C$)	Longitud del enlace (m)	BER	$BER_{teórica}$
Clásico	1.5	20	0	0.028248	0.028123
Cuántico	1.5	20	0	0.027262	0.027679

Tabla 3. Comparación de BER para una $T = 20℃$.

Como podemos observar, las BER para ambos sistemas son prácticamente idénticas. Comparando con la anterior transmisión, mientras que la probabilidad de error del sistema clásico aumenta en un factor de 3, la BER del sistema cuántico en esta transmisión es casi 13

veces mayor que en la anterior. El sistema clásico ha alcanzado el rendimiento del sistema cuántico en lo que a probabilidad de error se refiere.

3.1.4 *Temperatura* 50℃

Para terminar el análisis de las prestaciones en función de la temperatura, saturaremos ambos sistemas de ruido térmico. Las fotografías en este caso se muestran en la Figura 5.

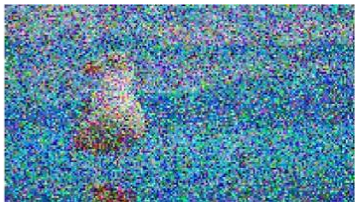
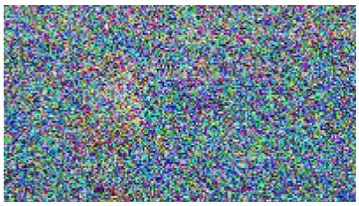
(a)  **(b)** 

Figura 5. **(a)**Transmisión con sistema clásico. **(b)** Transmisión con sistema cuántico. $T = 50℃$.

Cuando saturamos con ruido térmico podemos apreciar que el sistema que mejor funciona, en términos de probabilidad de error, es el clásico.

Sistema empleado	N_s	Temperatura ($°C$)	Longitud del enlace (m)	BER	$BER_{teórica}$
Clásico	1.5	50	0	0.24107	0.24105
Cuántico	1.5	50	0	0.37845	0.44644

Tabla 4. Comparación de BER para una $T = 50℃$.

3.2 *Transmisión en función de la distancia*

Por último, haremos una demostración del efecto que tiene la atenuación que introduce la propia fibra sobre la comunicación, para lo cual volveremos al caso sin ruido, pero en este caso introduciremos una longitud de enlace de 4km.

(a)  **(b)** 

Figura 6. **(a)**Transmisión con sistema clásico. **(b)** Transmisión con sistema cuántico. $T = -200℃$ y L = 4km

Sistema empleado	N_s	Temperatura ($°C$)	Longitud del enlace (m)	BER	$BER_{teórica}$
Clásico	1.5	-200	0	0.0072265	0.0071529
Clásico	1.5	-200	4000	0.012913	0.012743
Cuántico	1.5	-200	0	0.00059273	0.00062007
Cuántico	1.5	-200	4000	0.0017316	0.0017033

Tabla 4. Comparación de BER para una $T = -200℃$ y L = 4km.

En este contexto, podemos apreciar que para el sistema clásico las prestaciones en términos de BER empeoran casi al doble, mientras que en el cuántico lo hacen casi en un factor de tres, por lo que no hay un efecto notablemente mayor en uno respecto al otro.

4. Conclusiones

Como hemos visto en la sección tres, la superioridad del sistema de comunicación cuántico sobre el clásico es evidente. A pesar de esto, debemos matizar esta afirmación. El sistema cuántico será superior al clásico siempre y cuando los niveles de ruido térmico (la temperatura de trabajo) se mantengan bajos ya que, como hemos visto a través de la secuencia de imágenes, conforme crece la temperatura las prestaciones de ambos sistemas tienden a igualarse, llegando el sistema cuántico a ser superado por el clásico cuando la temperatura alcanza niveles muy altos. Es aquí donde comienzan las dificultades para emplear de manera práctica sistemas cuánticos ya que, aunque teóricamente es posible estabilizar fotones a temperaturas tan bajas, la complejidad es enorme y aún más si tenemos en cuenta que debemos mantener esas temperaturas criogénicas a lo largo de decenas de kilómetros. En cuanto al futuro de este emulador, su desarrollo aún no ha terminado ya que tenemos una serie de funciones pendientes de introducir para futuras versiones. Entre ellas se encuentran:

- Introducción de una interfaz gráfica para facilitar la interacción con el usuario.
- Emular la presencia de un espía, Eve, que trate de robar la clave secreta que generamos para cifrar la información.
- Introducir amplificadores en el enlace, de tal manera que podamos emular la transmisión a lo largo de grandes distancias.

Agradecimientos

A ISDEFE por el soporte económico a los estudiantes para la realización de este trabajo.

Referencias

[1] Möller, M., Vuik, C. On the impact of quantum computing technology on future developments in high-performance scientific computing. Ethics Inf Technol 19, 253–269 (2017). Disponible: https://doi.org/10.1007/s10676-017-9438-0

[2] Valdemolillos, C. (2020, Agosto 21). IBM dobla la potencia de su red de computación cuántica. [Online] Disponible: https://www.muycomputerpro.com/2020/08/21/ibm-dobla-rendimiento-computacion-cuantica

[3] Varona, B. (2020, septiembre 25) La carrera por la supremacía cuántica: Google vs. IBM. [Online] Disponible: https://innovadores.larazon.es/es/la-carrera-por-la-supremacia-cuantica-google-ibm/

[4] Universidad Politécnica de Madrid.(2018, junio 15) La UPM, Telefónica y Huawei realizan una experiencia piloto sobre criptografía cuántica. [Online] Disponible: https://www.upm.es/UPM/SalaPrensa/Noticias_de_investigacion?prefmt=articulo&fmt=detail&id=f38a0ad337204610VgnVCM10000009c7648a____

[5] Domínguez, N. (2020, junio 16). China crea un sistema de comunicación cuántica desde el espacio imposible de espiar. [Online] Disponible: https://elpais.com/ciencia/2020-06-15/china-crea-un-sistema-de-comunicacion-cuantica-desde-el-espacio-imposible-de-espiar.html

[6] Cariolaro, G. Quantum Communications. Suiza: Springer, 2015.

[7] THORLABS Discovery. (2017) EDU-QCRY. EDU-QCRY/M. Quantum Cryptography Demonstration Kit. [Online] Disponible: https://www.thorlabs.com/drawings/da2025f890d466ab-BEDB677B-A5A4-4E99-279E155781474117/EDU-QCRY1_M-EnglishManual.pdf

[8] MATLAB. MathWorks, 2019.