Universidad de Valladolid

FACULTAD DE CIENCIAS

TRABAJO FIN DE GRADO

Grado en Física

IMPLEMENTACIÓN EXPERIMENTAL DE UN GENERADOR CUÁNTICO DE NÚMEROS ALEATORIOS BASADO EN FIBRA ÓPTICA

Autor: Pablo Galán Vázquez
Tutores: Juan Carlos García Escartín y Luis Miguel Nieto Calzada
25 julio 2022

Índice

ABSTRACT

A quantum random number generator based on the simultaneous measurement of the pair of conjugate time-frequency variables is designed and implemented. Fiber optic dispersion is used to separate in time different spectral components of an optical pulse, and a single photon detector is used to assign bit values according to detection times. Finally, a bound for the entropy with quantum origin of the generated numbers is calculated through a study of the dispersion and the Fourier limit of the pulses.

RESUMEN

Se diseña e implementa un generador cuántico de números aleatorios basado en una medida simultánea de las dos variables conjugadas tiempo-frecuencia. Se utiliza dispersión en fibra óptica para separar en el tiempo diferentes las diferentes componentes espectrales de un pulso de luz, y se utiliza un detector de fotones individuales para asignar valores de bit según los tiempos de llegada. Finalmente, se calcula una cota de la entropía de origen cuántico de los números generados a través de un estudio de la dispersión y del límite de Fourier de los pulsos.

1. Motivación y objetivos

El objetivo de este Trabajo de Fin de Grado es diseñar e implementar un generador cuántico de números aleatorios (*Quantum Random Number Generator* - QRNG) basado en el principio de incertidumbre cuántico que satisface cualquier par de variables conjugadas por la trasnformación de Fourier.

Según los principios de la mecánica cuántica es imposible determinar simultáneamente con una precisión arbitrariamente alta dos magnitudes que sean variables conjugadas, ya que la determinación de una de ellas implica la pérdida de información de la otra. Entonces, al realizar una medida simultánea de estas dos magnitudes, habrá una incertidumbre mínima en el resultado. Es imposible predecir el resultado obtenido aunque se conozca con absoluta precisión el estado del sistema.

Esto nos permite extraer entropía de origen cuántico de un sistema simplemente con realizar una medida simultánea de dos variables conjugadas, como pueden ser posición-momento o tiempo-energía.

El sistema que se utilizará será la medida de tiempos de detección de fotones en un pulso de luz coherente de envolvente gaussiana, generado por un láser, simultáneamente a la medida de la frecuencia de los mismos. La frecuencia está asociada a la energía directamente por $E = \hbar\omega$, lo que conforma el par de variables conjugadas.

La medida de la frecuencia se hace de forma indirecta aprovechando el efecto de la dispersión en fibra óptica. Diferentes componentes espectrales se propagarán a distinta velocidad a lo largo del camino recorrido por el pulso, que se ensanchará, provocando una mayor probabilidad de detección para distintas frecuencias a distintos instantes. Es decir, si se da una detección en la parte inicial, es más probable que se trate de una frecuencia mayor en el caso de dispersión normal y una frecuencia menor en el caso de dispersión anómala.

Con esta base, al asociar a cada pulso, según el instante de detección de un fotón, un valor de 0 o 1 (bits), se pueden generar cadenas de números aleatorios, con una cierta cota de origen cuántico según el peso de la incertidumbre cuántica respecto de otros factores de origen clásico. Se puede demostrar [1] que es posible certificar un origen cuántico de la entropía mediante un post-procesado de los bits generados incluso en el caso de que el efecto clásico supere las cotas cuánticas.

En la sección 2 veremos una pequeña introducción a diferentes generadores de números aleatorios, y en concreto, de generadores cuánticos de números aleatorios. Posteriormente, en la sección 3 se hará un estudio de los diferentes aspectos teóricos aprovechados en el diseño e implementación del generador que nos ocupa. Las secciones 4 y 5 describen el principio de funcionamiento del equipo utilizado y las medidas experimentales realizadas. El resultado de dichas medidas se presenta en la sección 6. Finalmente, en la sección 7 se analiza la calidad de los bits extraídos y se calcula una cota de entropía de origen cuántico de los mismos. Para concluir, en la sección 8 se sugieren posibles ampliaciones, líneas futuras y se discuten unos resultados preliminares con un láser pulsado cerca del límite de Fourier.

2. Generadores cuánticos de números aleatorios

A la hora de generar secuencias de números aleatorios, históricamente se ha recurrido a sistemas cuyo estado final es difícil de predecir, ya sea por dificultad a la hora de caracterizar el comportamiento por la complejidad del sistema, o por la dificultad de obtener las condiciones iniciales que determinan la evolución del sistema. Por ejemplo, al lanzar una moneda o un dado, es necesario conocer exactamente multitud de factores para predecir el resultado final: fuerza y velocidad con las que se lanza, características de la superficie sobre la que cae, corrientes de aire en la sala, etc.

Cuando es necesario generar de forma automática números aleatorios, principalmente para aplicaciones computacionales o criptográficas, se suele recurrir bien a generadores físicos o a algoritmos que generan cadenas de números pseudoaleatorios.

Los algoritmos que generan números pseudoaleatorios (PRNG - *Pseudo-Random Number Generators*) son útiles para producir rápidamente grandes secuencias de números, que en un principio se asemejan a una secuencia realmente aleatoria. Suele utilizarse una semilla de origen aleatorio físico, de forma que la secuencia será difícil de predecir. Debido a que los números producidos tienen características propias de los números aleatorios (equiprobables, repeticiones de secuencias escasas...), es muy común su uso para la simulación o para situaciones en las que es necesario producir una gran cantidad de números de forma rápida, pero en las que no es tan importante la impredecibilidad. No obstante, no hay que olvidar que la secuencia entera está determinada por la semilla: el algoritmo es determinista y por tanto predecible en caso de conocer la semilla. Además, las cadenas producidas tienen una longitud limitada, repitiéndose después de un cierto periodo y añadiendo sesgos importantes por ejemplo a la hora de realizar simulaciones de Monte Carlo [2] si el periodo es menor al número de números utilizados.

Por otra parte, los generadores físicos de números aleatorios aprovechan un sistema complejo o de naturaleza caótica, como puede ser ruido eléctrico en un circuito o ruido térmico. Se basan en la dificultad que supone predecir la evolución de estos sistemas para producir números aleatorios de origen físico. Son en general más lentos que los algoritmos de generación de números pseudoaleatorios, pero menos predecibles, y por tanto su uso es más común para aplicaciones criptográficas, como la creación de claves. Sin embargo, no hay ninguna ley física que impida conocer la evolución de muchos de estos sistemas en el límite clásico: en principio, sería posible para un observador externo predecir o incluso alterar los resultados.

Existe una tercera opción que consiste en utilizar un generador cuántico de números aleatorios (*Quantum Random Number Generator* - QRNG), el cual aprovecha la incertidumbre inherente a la medida de un estado cuántico para generar números aleatorios que son imposibles de predecir de antemano, y cuya naturaleza aleatoria está garantizada por las leyes físicas. Suponen por tanto un umbral de máxima seguridad, por ejemplo, para producir claves criptográficas. Actualmente hay diversas implementaciones de QRNG, utilizando diferentes sistemas y medidas para extraer la aleatoriedad de origen cuántico.

2.1. Algunos ejemplos de QRNG

Desintegración radiactiva

Los primeros QRNG se basaron en la desintegración radiactiva de elementos que produjeran radiación β. El proceso de desintegración es aleatorio y las emisiones no están correlacionadas entre sí: el momento en el que se da una desintegración no depende de emisiones anteriores. Se han utilizado diversos métodos para generar números aleatorios a partir de las detecciones de radiación en un tubo Geiger-Müller.

Un ejemplo es contar el número de desintegraciones que se dan en intervalos de tiempo fijos, que seguirán una estadística de Poisson [3]. Para cada uno de estos intervalos, se asigna 1 o 0 si el número de detecciones ha sido par o impar.

Otro método es comparar los intervalos de tiempos de llegada entre cuatro detecciones sucesivas [4]. Si el tiempo transcurrido entre las dos primeras es mayor que el tiempo entre las dos útlimas se asigna un 0, y en caso contrario se asigna un 1. En el caso de las 4 detecciones representadas en la Figura 1, puesto que t_1 es mayor que t_2, se asignaría un 0 al conjunto.

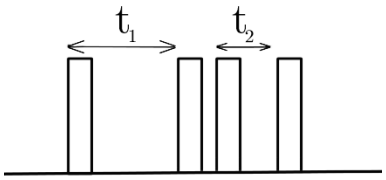


Figura 1: Esquema de asignación de un valor de 0 para cuatro detecciones sucesivas en un contador Geiger-Müller en un QRNG basado en la desintegración radiactiva.

Implementaciones ópticas

Otra opción son las implementaciones ópticas de un QRNG que utilizan la luz como sistema cuántico. Un ejemplo conocido es utilizar un divisor de haz al 50 %, que separa la luz por dos caminos diferentes. Situando fotodetectores al final de estos dos caminos, se miden las capturas de fotones individuales. Para luz coherente, las detecciones son individuales [5] y no están correlacionadas, lo que supone una fuente buena para números aleatorios, asignando 1 o 0 a la detección en cada uno de los detectores. Un esquema del funcionamiento se muestra en la Figura 2.

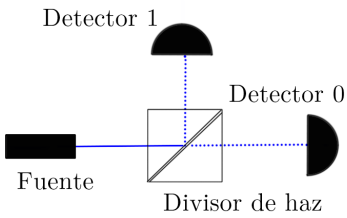


Figura 2: Esquema de funcionamiento de un QRNG basado en la detección de fotones por diferentes caminos. Un haz proveniente de un emisor de fotones individuales se divide por dos caminos. Se asigna 0 o 1 según el detector en el que se detecte un fotón.

A la hora de implementar este tipo de generador de números aleatorios experimentalmente, hay

que tener en cuenta ciertos aspectos que pueden introducir desviaciones que favorezcan la aparición de más valores de 1 o de 0. Por ejemplo, si el divisor de haz no es perfecto, se producirá una mayor redirección de la potencia óptica hacia uno de los detectores, aumentando las detecciones en el mismo. Por otro lado, es difícil asegurar que los dos detectores tengan la misma eficiencia de detección, y esto puede introducir desviaciones también. En general, la presencia de efectos que produzcan asimetría en la cantidad de 1 y 0 es inevitable en la implementación práctica de un generador, por lo que es necesario recurrir a algoritmos de post-procesado que eliminen esta asimetría.

Otro ejemplo son los generadores basados en la detección de fluctuaciones de los estados de vacío [6]. Se genera un estado de vacío de radiación $|0\rangle$, que se puede expresar en función de las cuadraturas de amplitud $|x\rangle$ de la forma

$$|0\rangle = \int_{-\infty}^{\infty} \psi(x)\,|x\rangle\,dx,$$

siendo $\psi(x)$ la función de onda del estado fundamental. Para medir los estados de cuadratura, se utiliza un haz láser auxiliar que se suma al estado de vacío, y separando el haz en dos se realiza una medida de la correlación de las fases mediante dos fotodetectores restando las corrientes que producen. En un estado de vacío las cuadraturas siguen la distribución gaussiana del estado fundamental, y asignando un cierto valor de bits a cada intervalo de amplitud, se obtienen secuencias de números aleatorios.

Una ventaja de estos últimos QRNG es que no se necesita utilizar un detector individual de fotones, y es posible realizar la medida con fotodetectores clásicos.

3. Fundamento teórico

Para caracterizar el efecto de la dispersión cromática que se utiliza en la medida indirecta de la frecuencia es necesario considerar cómo se propaga la luz guiada por una fibra óptica y los efectos de dispersión que aparecen. Esto se estudia en las secciones 3.1 y 3.2 respectivamente. En concreto, para los pulsos de envolvente gaussiana que se utilizan puede calcularse analíticamente el ensanchamiento en caso de evolución en régimen lineal (sección 3.3). Posteriormente, en la sección 3.4 se calcula la atenuación necesaria para que sea válida la hipótesis de detección de un solo fotón, y en la sección 3.5 se estudia el origen cuántico o clásico de las componentes de frecuencia del pulso. Finalmente, en la sección 3.6 se estima la cota de entropía de origen cuántico que puede extraerse de las medidas a realizar.

3.1. Propagación en fibra óptica

En un medio material, la propagación de ondas electromagnéticas viene dada por la solución a las ecuaciones de Maxwell en medios materiales con las restricciones de la geometría del medio y sus condiciones de contorno. Para una fibra óptica con simetría cilíndrica, la ecuación de onda que describe los campos de radiación tiene una solución separable en producto de función radial-angular $\vec{E}(r,\phi)$ y función del eje de simetría $\vec{E}(z)$. Debido a que las condiciones de contorno de la fibra limitan sólo en la dirección perpendicular al eje de simetría, $\vec{E}(z)$ resultará en una propagación libre en el eje z. Por otro lado, las ecuaciones de los campos en las direcciones perpendiculares al eje z vendrán determinadas por las condiciones de contorno particulares para cada perfil de índices de refracción de la fibra. De manera general, serán unos modos discretizados. El caso es completamente análogo para el campo magnético $\vec{H}$.

Para el caso simplificado de una fibra óptica con un cambio de índice de refracción abrupto entre el núcleo (*core*) de índice n_1 y radio a, y el revestimiento (*cladding*) de índice n_2 y radio lo suficientemente grande para considerarse infinito a efectos de la propagación, las soluciones exactas para $E(r,\phi)$ consisten en combinaciones lineales de las funciones de Bessel de primera (en el núcleo) y segunda especie (en el revestimiento) $J_n(ua)$ y $K_n(wa)$ con $u = {k_1}^2 - \beta^2$ y $w = \beta^2 - {k_2}^2$ siendo $k_i = 2\pi n_i/\lambda$, dondea λ es la longitud de onda de la onda que se está propagando.

Con esto, las soluciones para el caso de fibra con cambio de índice abrupto son [7]

$$\begin{aligned}
E_z(r<a) =& AJ_n(ur)e^{jn\phi}e^{j(\omega t-\beta z)},\\
H_z(r<a) =& BJ_n(ur)e^{jn\phi}e^{j(\omega t-\beta z)},\\
E_z(r>a) =& CK_n(wr)e^{jn\phi}e^{j(\omega t-\beta z)},\\
H_z(r>a) =& DK_n(wr)e^{jn\phi}e^{j(\omega t-\beta z)},
\end{aligned}$$

con la condición de que el campo en el interior de la fibra sea real, $k_2 \leq \beta \leq k_1$.

Aplicando las condiciones de contorno y de continuidad de campo tangencial (componentes E_z y E_ϕ) en la superficie, se obtiene que los valores de β están discretizados, generándose así una serie de modos de propagación del campo en el interior de la fibra. Para un campo determinado, cada uno de estos modos se caracteriza por dos números enteros que determinan el número de nodos en las soluciones radial (n) y angular (m). Según la transversalidad de los campos a la dirección de

propagación, y cuál es el campo que domina en cada caso, los modos reciben los nombres de

$$TE_{nm} : \text{Campo eléctrico transversal.}$$
$$TM_{nm} : \text{Campo magnético transversal.}$$
$$EH_{nm} \text{ o } HE_{nm} : \text{Campos eléctrico y magnético transversales.}$$

Para calcular los modos es necesario recurrir a soluciones numéricas para la ecuación de condiciones de contorno. Sin embargo, en la aproximación de guiado lento [8], en la que la diferencia entre n_1 y n_2 es pequeña, aparecen degeneraciones entre los modos $HE_{n+1,m}$ y $EH_{n-1,m}$, que se agrupan en modos propagantes linealmente polarizados, y entre los modos TE_{nm}, TM_{nm} y $HE_{n+2,m}$ que también se agrupan en modos propagantes linealmente polarizados.

Estos modos se nombran como LP_{nm}, y presentan una solución analítica [8]. Es habitual representar la propagación de los modos LP a lo largo del eje z mediante la relación entre la constante de propagación normalizada b y la frecuencia normalizada V, que en esta aproximación se definen por

$$b = \frac{(\beta/k) - n_2}{n_1 - n_2}, \qquad V = \left(\frac{2\pi a}{\lambda}\right)\left({n_1}^2 - {n_2}^2\right)^{1/2},$$

siendo $k = \frac{2\pi}{\lambda}$. La frecuencia normalizada es un número adimensional proporcional a la frecuencia del modo. El número de modos está determinado por V, y no depende de las características de la fibra.

La constante de propagación normalizada es otro número adimensional y proporcional a la constante de propagación, y por tanto inversamente proporcional a la velocidad de propagación a lo largo del eje z, normalizada de forma que la dependencia con V sea independiente de la fibra. Se anula en caso de de $\beta/k = n_2$. En esta situación, no hay modo propagante para este valor de β/k, y se dice que el modo está en corte, es decir, hay una frecuencia mínima para que se propague cada modo.

Para diferentes frecuencias, aparecen distintos modos, que tienen diferentes constantes de propagación y frecuencias de corte. Como se puede ver en la Figura 3, para todos los rangos de frecuencia, hay un modo presente: modo LP_{01}, que se conoce como modo fundamental. En la mayoría de fibras, los valores de n_1, n_2, y a son tales que a partir de la frecuencia de corte normalizada $V \geq 2{,}405$, aparece un segundo modo de propagación LP_{11}. Es habitual trabajar con fibra en régimen monomodo, es decir, por debajo de la frecuencia de corte del modo LP_{11}, de forma que el único modo que puede propagarse es el modo fundamental.

3.2. Dispersión en fibra

Al estudiar la propagación de un pulso a lo largo de la fibra, es necesario tener en cuenta mecanismos de dispersión que alteran la forma del mismo. Se pueden distinguir tres tipos de dispersión en fibra óptica según su origen.

3.2.1. Dispersión cromática

Se debe a una relación no lineal entre la frecuencia ω y la constante de propagación β. Por tener una anchura temporal finita, un pulso tendrá siempre una componente espectral que contendrá más de una frecuencia.

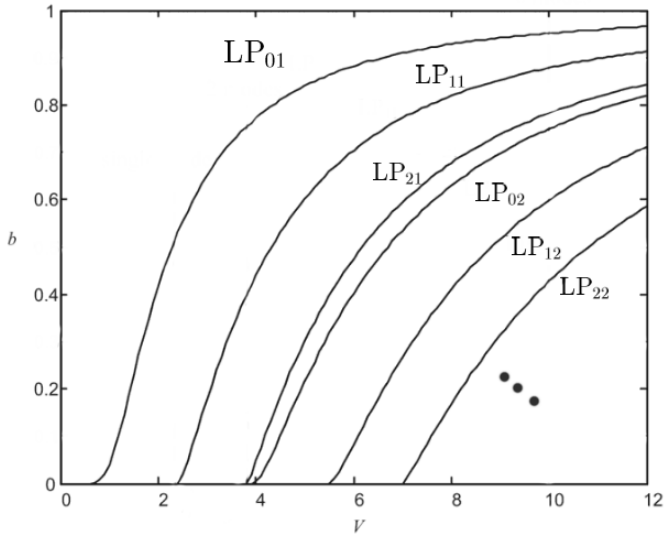


Figura 3: Constante de propagación normalizada en función de la frecuencia normalizada para los 6 primeros modos LP.

Se distinguen dos componentes de la dispersión cromática. Por un lado, el índice de refracción de un material concreto depende de la frecuencia, y no es el mismo para todas las componentes del pulso. Ésta se conoce como dispersión material. Por otro lado, la distribución del perfil de potencia en el interior de la fibra depende de la longitud de onda: distintas componentes de frecuencia tendrán diferentes porcentajes de potencia que viajan por núcleo o revestimiento, y por tanto el índice de refracción efectivo cambia con la frecuencia. Ésta es la dispersión por guiado.

Dispersión material

Consideramos un paquete de ondas centrado en ω_c y con un ancho de banda $\Delta\omega$. Si el ancho de banda es pequeño, se utiliza un desarrollo en serie hasta segundo orden alrededor de ω_c para la expresión de β

$$\beta(\omega) \approx \beta_c + \left.\frac{d\beta}{d\omega}\right|_{\omega_c} (\omega - \omega_c) + \frac{1}{2} \left.\frac{d^2\beta}{d\omega^2}\right|_{\omega_c} (\omega - \omega_c)^2 + \mathcal{O}(\omega - \omega_c)^3. \tag{1}$$

Con la definición habitual de velocidad de fase

$$v_p = \frac{\omega_c}{\beta_c},$$

la velocidad de grupo

$$v_g = \frac{d\omega}{d\beta},$$

y el parámetro de dispersión

$$D = \frac{2\pi c}{\lambda^2} \frac{d^2\omega}{d\beta^2}.$$

- El primer término en (1) del desarrollo determina la velocidad a la cual se propaga la fase en el interior.
- El segundo término en (1) determina la velocidad a la cual se propaga el paquete de ondas, centrado en ω_c.
- La dispersión aparece al considerar el tercer término de la expresión (1) (término cuadrático en ω). Para cualquier paquete de ondas que contenga varias frecuencias, éstas se propagan a diferentes velocidades a lo largo de la fibra, y por tanto se produce un ensanchamiento temporal en el pulso. Este tipo de dispersión se aprovecha durante el experimento para conseguir un ensanchamiento temporal.

Órdenes más altos en $\omega - \omega_c$ introducen dispersión de mayor orden, pero su efecto es menos notable frente a la dispersión de segundo orden y solo se observan en distancias de propagación muy largas, en casos en los que se anulen los efectos de segundo orden o en pulsos de altas potencias.

Dispersión por guiado

Aún en el caso de que un material tuviese un índice de refracción igual para todas las frecuencias, debido a la dependencia de la constante de propagación con la frecuencia, aparecería una dispersión debido a las múltiples componentes de frecuencia. En la Figura 4, vemos gráficamente como dentro de un único modo de propagación, aparecen diferentes constantes de propagación para las componentes espectrales del pulso. El efecto general es un ensanchamiento del pulso inicial. Diferentes envolventes sufrirán una deformación distinta según sus perfiles temporales y espectrales.

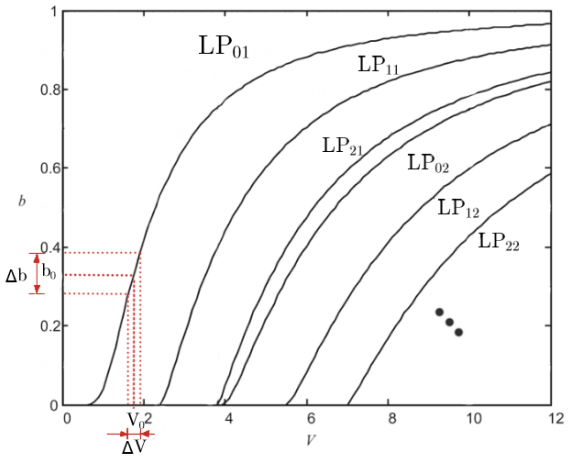


Figura 4: Dispersión por guiado.

El conjunto de los dos tipos de dispersión cromática es el que domina en el experimento diseñado. En la sección 3.3 se estudia el efecto sobre un pulso de envolvente gaussiana, que es el caso que nos ocupa para el QRNG diseñado.

3.2.2. Dispersión intermodal

Cuando en una fibra aparecen varios modos de propagación, incluso en el caso límite de tener un pulso con una sola componente en frecuencia, aparecen diferentes constantes de propagación, que corresponden a los diferentes modos. Esto queda representado en la Figura 5. El efecto es que los modos se propagan a diferentes velocidades por la fibra, y se separan a lo largo de la distancia. Al aparecer más de un modo, el pulso temporal se divide en tantos pulsos como modos propagantes. La energía tiende a repartirse por igual en ellos.

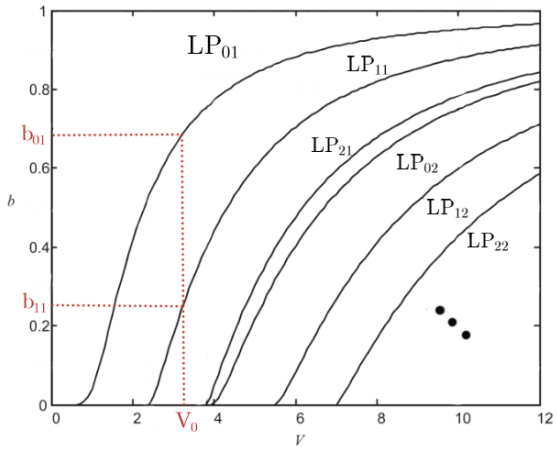


Figura 5: Dispersión modal.

En el caso real de tener más de una componente en frecuencia, aparecen ambos tipos de dispersión, cromática y modal. Si el ancho de banda es pequeño y no hay muchos modos presentes, en general será posible separar los efectos de estos dos tipos de dispersión, ya que la diferencia en β causada de dos modos discretos distintos es mucho mayor que la causada por la variación continua en frecuencias: si la distancia de propagación es suficientemente larga, ambos modos se separan espacialmente lo suficiente para detectarlos por separado.

En el experimento realizado, se trabaja en régimen monomodo, por lo que este efecto no aparecerá.

3.2.3. Dispersión por polarización

Para una simetría cilíndrica perfecta, las diferentes direcciones de polarización de los modos LP se comportan exactamente igual, ya que no hay diferencia entre las direcciones transversales al eje z. Sin embargo, en un caso real esta simetría perfecta no se da, ya que en una fibra siempre habrá dobleces, giros o pequeñas roturas. Entonces cada dirección de polarización tendrá características y constantes de propagación diferentes. El efecto es difícil de calcular y de caracterizar, aunque en la mayoría de aplicaciones su magnitud es mucho menor a otros y puede ser ignorado.

En cualquier caso, puede evitarse este problema, trabajando con fibras en las que se rompe la simetría cilíndrica de forma que permiten la propagación de un solo tipo de polarización, eliminando así la dispersión causada por otras componentes. Este tipo de fibra se denomina PM (*polarization*

maintainig).

En el experimento realizado, el efecto de la dispersión por polarización es efectivamente despreciable, como se comprueba más adelante en la sección 6.

3.3. Dispersión de un pulso de envolvente gaussiana

La ecuación de propagación escalar de la amplitud de un pulso óptico polarizado en una fibra, dentro de la aproximación de envolvente de variación lenta viene dada por la conocida como ecuación no lineal de Schrödinger [9]:

$$i\frac{\partial A}{\partial z} + i\frac{\alpha}{2}A - \frac{\beta_2}{2}\frac{\partial^2 A}{\partial T^2} + \gamma\left|A\right|^2 A = 0. \tag{2}$$

Podemos distinguir varios elementos:

- El término en α relaciona la evolución espacial de la amplitud con su valor. Se trata por tanto de un término de pérdidas: el valor de A decrece con la distancia recorrida.

- El término en β_2 relaciona la evolución espacial con la temporal: el parámetro β_2 es el segundo coeficiente en la expansión de Taylor en frecuencias de la constante de propagación, relacionado con el parámetro de dispersión D de la forma

  $$\beta_2 = \frac{2\pi c}{\lambda^2}D^{-1}.$$

  De esta forma, en la ecuación (2), este término introduce el efecto de la dispersión cromática del pulso debido a sus componentes de frecuencia.

- El término en γ relaciona la evolución con un término cúbico en A. Da cuenta de los efectos no lineales.

En el caso en el que domina la dispersión lineal frente a la no lineal, puede aproximarse $\gamma = 0$. Se incorpora el efecto de las pérdidas en la amplitud normalizada $U(z,\tau)$:

$$U(z,\tau) = \frac{1}{\sqrt{P_0}}e^{-\alpha z/2}A(z,\tau),$$

siendo P_0 la potencia máxima del pulso, y τ el tiempo normalizado a la anchura T_0, tomado centrado en el pulso en cada instante,

$$\tau = \frac{t - z/v_g}{T_0}.$$

Con estas definiciones, se reduce la ecuación (2) a

$$\frac{\partial U}{\partial z} = -i\frac{\beta_2}{2}\frac{\partial^2 U}{\partial T^2}. \tag{3}$$

Para un pulso de envolvente gaussiana de varianza ${\sigma_0}^2$, dada la condición inicial

$$U(0,T) = \exp\left(-\frac{1}{2}\frac{T^2}{{\sigma_0}^2}\right),$$

se puede calcular de forma exacta la evolución temporal utilizando su transformada de Fourier [9]

$$U(z,T) = \frac{\sigma_0}{({\sigma_0}^2 - i\beta_2 z)^{1/2}} \exp\left[-\frac{1}{2}\frac{T^2}{({\sigma_0}^2 - i\beta_2 z)}\right].$$

Puede separarse el exponente en dos términos: un término exponencial complejo, que es una modulación a la fase del pulso y no afecta a la dispersión, y un término exponencial real que mantiene una dependencia con $-T^2$:

$$U(z,T) = \frac{\sigma_0}{({\sigma_0}^2 - i\beta_2 z)^{1/2}} \exp\left[\frac{i\beta_2 T^2 z}{2\left({\sigma_0}^2 + \frac{{\beta_2}^2 z^2}{{\sigma_0}^2}\right)}\right] \exp\left[\frac{-T^2}{2\left({\sigma_0}^2 + \frac{{\beta_2}^2 z^2}{{\sigma_0}^2}\right)}\right].$$

Es decir, la envolvente mantiene la forma gaussiana, pero la anchura σ pasa a ser una función que depende en cada instante de la posición del centro del pulso z, de forma que

$$\sigma(z) = \left[\sigma_0^2 + \frac{{\beta_2}^2 z^2}{\sigma_0^2}\right]^{1/2}. \tag{4}$$

Puede reescribirse esta ecuación como

$$\frac{\sigma(z)^2}{{\sigma_0}^2} = 1 + \frac{{\beta_2}^2 z^2}{{\sigma_0}^4}, \tag{5}$$

3.4. Nivel de un solo fotón: atenuación

Por el funcionamiento de las medidas de correlación temporales del detector de fotones, sólo se registra la primera captura de un fotón dentro de la ventana de tiempo definida. Es necesario reducir ampliamente las probabilidades de que se encuentren dos fotones dentro de un mismo pulso al llegar al detector, ya que esto implicaría un aumento de detecciones en la parte inicial de la distribución, falseando las medidas al producirse una asimetría hacia esta parte. Para un pulso de luz centrado en 1548 nm, la energía de un fotón será

$$E_1 = h\nu = \frac{hc}{\lambda},$$

que toma un valor de $E_1 = 1{,}28 \cdot 10^{-19}$ J.

Al disminuir el valor medio de la energía mediante la atenuación, disminuye la probabilidad de encontrar un número alto de fotones en cada pulso. Al ser el láser una fuente de luz coherente, y no perderse esta coherencia en la interacción con los diferentes elementos del circuito, el estado de luz tras la atenuación, antes de ser detectado será un estado de luz coherente, y la distribución de fotones por pulso vendrá dada por la distribución de Poisson. Considerando cada pulso con una energía media de $\langle E\rangle$, tendremos un número medio de fotones por pulso de $\langle n\rangle = \frac{\langle E\rangle}{E_1}$.

Con esto la probabilidad de encontrar n fotones por pulso es

$$\mathcal{P}(n) = \frac{\langle n\rangle^n}{n!} \exp\left(-\langle n\rangle\right),$$

$$\mathcal{P}(n) = \frac{1}{n!}\frac{\langle E\rangle^n}{{E_1}^n} \exp\left(-\frac{\langle E\rangle}{E_1}\right).$$

Y la probabilidad de obtener 2 o más fotones por pulso será

$$\mathcal{P}(n \geq 2) = 1 - \mathcal{P}(0) - \mathcal{P}(1),$$
$$\mathcal{P}(n \geq 2) = 1 - (1 + \langle n \rangle) \exp\left(-\langle n \rangle\right).$$

Por lo tanto, la relación de detecciones que corresponden a una distribución de más de un fotón por pulso respecto a las detecciones que corresponden a un solo fotón por pulso será

$$\frac{\mathcal{P}(n \geq 2)}{\mathcal{P}(1)} = \frac{1}{\langle n \rangle} \exp\left(\langle n \rangle\right) - \frac{1}{\langle n \rangle} - 1.$$

Y en términos de la energía media

$$\frac{\mathcal{P}(n \geq 2)}{\mathcal{P}(1)} = \frac{E_1}{\langle E \rangle} \exp\left(\frac{\langle E \rangle}{E_1}\right) - \frac{E_1}{\langle E \rangle} - 1.$$

Por ejemplo, para una media de 10^{-2} fotones por pulso, se obtiene una relación del 0.5 % entre las detecciones, y para una media de 10^{-1} fotones por pulso, la relación es del 5.2 %.

3.5. Componentes de frecuencia

Cualquier pulso de luz tendrá diferentes componentes de frecuencia debido al ensanchamiento de las líneas espectrales, que puede tener diversos orígenes.

- **Ruido mecánico-térmico:** factores como variaciones en la energía aportada al sistema, vibraciones mecánicas del equipo, o cambios en el índice de refracción o el tamaño de la cavidad por fluctuaciones de temperatura.
- **Función instrumental:** debido a la construcción del interferómetro Fabry-Perot, las paredes de la cavidad tendrán unas ciertas pérdidas de energía. Esto se refleja en un ensanchamiento de las líneas espectrales, al permitir la interferencia constructiva de un rango de frecuencias alrededor de la propia de la cavidad.
- **Selección de distintos modos:** el láser utilizado puede emitir a diferentes modos. El modo predominante puede cambiar a lo largo de la emisión continua debido a cambios de temperatura.
- **Emisión espontánea:** La contribución de la emisión espontánea a la radiación produce un aumento de la anchura espectral, al no ser las emisiones a la frecuencia propia de la cavidad.
- **Límite de Fourier:** cualquier pulso de duración temporal finita tiene una componente mínima de anchura en frecuencia.

A mayores, como efectos propios de un láser de semiconductor, la anchura de su emisión depende de factores como [10]:

- El ensanchamiento de la anchura espectral de la ganancia debido a que las transiciones se dan entre bandas de valencia y conducción, en vez de entre dos niveles discretos.
- La presencia de varios modos de emisión de la cavidad en los que las ganancias superan a las pérdidas, y que por tanto pueden emitir, produciéndose emisión a varias frecuencias. En una misma región espacial, estos modos compiten entre sí y solo uno es amplificado, pero en regiones en las que este modo se anula puede darse la presencia de otro modo. Este efecto se denomina *spatial hole burning* [11].

3.5.1. Límite de Fourier

Para un pulso de duración finita, pueden definirse tanto para su distribución temporal $f(t)$ como para su distribución $F(\omega)$ (transformada de Fourier de la distribución temporal) la localización temporal t_0 y la frecuencia central ω_0 del siguiente modo [12]:

$$t_0 = \frac{1}{\|f(t)\|^2} \int f^*(t)\, t\, f(t) dt,$$
$$\omega_0 = \frac{1}{\|F(\omega)\|^2} \int F^*(\omega)\, \omega\, F(\omega)\, d\omega.$$

Asimismo, se definen la duración temporal ${\sigma_t}^2$ y el ancho espectral ${\sigma_\omega}^2$

$${\sigma_t}^2 = \frac{1}{\|f(t)\|^2} \int f^*(t)\ (t - t_0)^2\ f(t) dt,$$
$${\sigma_\omega}^2 = \frac{1}{\|F(\omega)\|^2} \int F^*(\omega)\ (\omega - \omega_0)^2\ F(\omega)\, d\omega.$$

Las definiciones así dadas son matemáticamente análogas a las definiciones del valor esperado y la varianza asociadas a los operadores en el formalismo de la mecánica cuántica. Obedecen, de la misma forma un principio de incertidumbre, según el cual el producto de las varianzas asociadas a la duración temporal y el ancho de banda tiene un valor mínimo. Si se considera la anchura de la distribución de potencia, que es la magnitud que se puede medir en el rango óptico, se tiene [12]

$${\sigma_t}^2 {\sigma_\omega}^2 \geq \frac{1}{4}, \tag{6}$$

y la igualdad se da para funciones gaussianas.

El producto mínimo tiempo-frecuencia no tiene el mismo significado que la incertidumbre cuántica asociada a dos operadores que no conmutan: los valores de tiempo y frecuencia están perfectamente definidos para una señal, se trata simplemente de una relación entre las varianzas de las distribuciones espacial-espectral.

Sin embargo, si nos limitamos a la detección de un solo fotón, podemos asociar una relación entre los operadores cuánticos:

- **Posición:** estaría relacionado con el instante de detección, puesto que, para una frecuencia fija, la velocidad de propagación es constante.
- **Momento:** estaría relacionado de manera directa con la energía y, por tanto, con la frecuencia.

Entonces, al tener una detección individual en cada suceso, el producto ${\sigma_t}^2 {\sigma_\omega}^2$ adquiere un significado de incertidumbre cuántica. En resumen, estamos asociando al fotón detectado una incertidumbre entre sus valores de posición (tiempo) y momento (frecuencia).

Puesto que la relación entre longitud de onda y frecuencia angular es

$$\omega = \frac{2\pi c}{\lambda},$$

para una función espectral estrecha, centrada en λ_0, de la relación entre las varianzas

$${\sigma_\omega}^2 = \left(\frac{\partial \omega}{\partial \lambda}\right)^2 {\sigma_\lambda}^2,$$

se sigue que

$$\sigma_\omega{}^2 = \frac{4\pi^2 c^2}{\lambda_0{}^4}\sigma_\lambda{}^2. \tag{7}$$

Además, para una función gaussiana, la anchura puede relacionarse directamente con la varianza del siguiente modo [13]:

$$\Delta\lambda = 2\sqrt{2\ln 2\,\sigma_\lambda{}^2}. \tag{8}$$

Sustituyendo las relaciones (6) y (8) en (7) se llega a que, en función de la anchura espectral en longitudes de onda, el producto mínimo para un pulso gaussiano será

$$\sigma_t{}^2\Delta_\lambda{}^2 = \frac{\lambda_0{}^4 2\ln 2}{\pi^2 c^2}\,\sigma_t{}^2\sigma_\omega{}^2 = \frac{\lambda_0{}^4\ln 2}{2\pi^2 c^2}.$$

Esto es el producto mínimo, y en el caso de un pulso de láser limitado por Fourier, la incertidumbre en frecuencias sería de origen únicamente cuántico. De esta forma, para un pulso centrado en λ_0 y con una anchura espectral $\Delta\lambda$ fija, el valor que tomaría $\sigma_{t_{(lim)}}{}^2$ sería

$$\sigma_{t_{(lim)}}{}^2 = \frac{\lambda_0{}^4\ln 2}{2\pi^2 c^2\Delta_\lambda{}^2}.$$

El láser utilizado no llega a estar en este límite. Teniendo en cuenta que la anchura espectral indicada por fabricante es de 20 nm y que el láser está centrado en 1548 nm, se tendrá que el valor de $\sigma_t{}^2$ mínimo que puede tomar el pulso es:

$$\sigma_{t_{(lim)}}{}^2\sigma_Q{}^2 \approx 5{,}601\cdot 10^{-27}\mathrm{s}^2.$$

Entonces, puesto que los pulsos generados no tienen una anchura mayor, sólo una fracción de su varianza temporal puede considerarse que tiene como origen el principio de incertidumbre de tiempo-energía. Por ejemplo, para un pulso gaussiano de anchura $\Delta t = 1\,\mathrm{ns}$, el cociente entre las varianzas de origen cuántico (σ_Q) y total del pulso (σ_0) sería de

$$\frac{\sigma_Q{}^2}{\sigma_0{}^2} \approx 3{,}106\cdot 10^{-8}.$$

3.6. Extracción de aleatoriedad de origen cuántico

Partiendo de la incertidumbre tiempo-energía nuestro objetivo es extraer números aleatorios, que tendrán un origen cuántico certificado por dicho principio de incertidumbre. La energía de cada fotón está directamente relacionada con su frecuencia de la forma $E = \hbar\omega$, por lo que la medida de la energía puede realizarse a través de una medida de frecuencia. En principio sería posible medir las frecuencias utilizando un espectrómetro, pero en este caso haremos una medida indirecta de la frecuencia a través de los tiempos de llegada. La conversión entre frecuencia y tiempo de llegada se da debido a la dispersión cromática en el guiado de los pulsos, de forma que diferentes frecuencias se propagan a distinta velocidad a través de la fibra. Este efecto de dispersión provoca un ensanchamiento en el pulso tras atravesar la fibra, que permitirá separar el efecto de la existencia de diferentes componentes espectrales en la distribución de tiempos de detección de otros efectos de ensanchamiento de origen clásico.

Para realizar las medidas, se utiliza una serie de atenuadores de forma que se disminuye la intensidad del campo hasta que solo pueda detectarse un fotón en la ventana de tiempos del detector. Para evitar correlaciones, se disminuye hasta que la probabilidad de tener 2 fotones en un pulso sea

menor que 10^{-2}.

Cada fotón detectado tendrá una frecuencia bien definida, y su instante de detección dependerá de:

1. Frecuencia: debido a la dispersión cromática, cada componente de frecuencia tiene un tiempo de llegada distinto al detector.

2. Forma temporal del pulso: aun en ausencia de dispersión, la estadística de llegada al detector seguirá la función correlación del campo. La incertidumbre de detección cuántica en el detector la agruparemos junto al resto de origen clásico, ya que viene determinada por factores como la alimentación y la temperatura del láser, o el funcionamiento del modulador.

3. Ruido instrumental: debido al *jitter*[1] de las señales de sincronización entre los diferentes equipos - generador, modulador y detector.

4. Ruido externo: fluctuaciones térmicas, calentamiento del equipo, ruido eléctrico,...

Se requiere una distribución uniforme en 0 y 1 para los bits extraídos. Aprovechando que las distribuciones de tiempos de llegadas son gaussianas, se asigna un valor de 0 a detecciones anteriores a la media, y un valor de 1 a detecciones posteriores a la media. Al seguirse una distribución simétrica, el número de ocurrencias de 1 y 0 será el mismo.

Para separar el origen cuántico y clásico de la aleatoriedad, se comparan las estadísticas de detección para el caso con y sin dispersión cromática. La diferencia de anchura entre ambas distribuciones da idea de la proporción de ensanchamiento debido a la presencia de diferentes frecuencias, y comparando esta última con la anchura mínima exigida por el límite de Fourier, se obtiene la relación de ruido cuántico y clásico (*Quantum to Classical Noise Ratio* - QCNR).

Para cada serie de medidas se realiza un estudio de la estadística de tiempos de llegada: se obtienen el centro, la forma y la anchura de la distribución. Después, a partir de cada dato de detección individual se genera una cadena de bits, asignando los valores de 0 o 1 de la forma descrita.

Con esto, es necesario un post-procesamiento de datos, en el que se corrigen posibles desviaciones asimétricas de la distribución que pueden favorecer la aparición de más 0 o 1. Estas asimetrías son sesgos inevitables y pueden aparecer por el efecto de dispersión de tercer orden, presencia de dos fotones en un pulso, variaciones a lo largo de la medida del centro de la distribución o imprecisiones a la hora de determinarlo mediante el ajuste no lineal.

3.6.1. QCNR

La anchura de la señal después de la dispersión incluye el efecto de la dispersión cromática, además de los mismos efectos que la señal medida antes de la dispersión: anchura temporal del pulso, ruido externo y de sincronización, y la posible dispersión que aparezca en el recorrido a través de las conexiones de los diferentes equipos que componen el montaje.

Como fuente de origen cuántico se tiene la incertidumbre en tiempo-energía. Se refleja en el ensanchamiento del pulso debido a la dispersión cromática. Su magnitud viene determinada por la relación entre la anchura temporal mínima dada por el principio de incertidumbre y la anchura

[1]Desviación de la periodicidad perfecta de una señal, generalmente debida a factores como ruido térmico.

temporal del pulso. La intención en el siguiente análisis es aislar la fracción de las detecciones que se corresponden a este origen.

Como fuentes de ruido clásico tendremos:

- Ruido externo. Al ser debido a ruido térmico y eléctrico, seguirá una distribución gaussiana.
- *Jitter* de sincronización. Supondremos una distribución gaussiana.
- Anchura temporal del pulso: contribuye a la varianza final de la distribución. Sigue la misma distribución gaussiana que el pulso.

Cada uno de estos efectos podría caracterizarse por separado, pero no aportaría información a la hora de procesar las medidas. Por lo tanto, se incluyen todos los efectos en conjunto en una varianza de origen clásico σ_C.

Dadas las contribuciones a la varianza de las distribución debido al ruido clásico ${\sigma_C}^2$ y de origen cuántico ${\sigma_Q}^2$, definimos la relación entre ruido clásico y cuántico ($QCNR$) como [1]

$$QCNR = 10 \log_{10} \left(\frac{{\sigma_Q}^2}{{\sigma_C}^2} \right). \tag{9}$$

Para separar las contribuciones de ambas fuentes se comparan las varianzas de las distribuciones de tiempos de llegada antes y después de la dispersión. Puesto que todos los factores que intervienen (forma temporal del pulso, ruido clásico y ensanchamiento cuántico) siguen una distribución gaussiana, entonces la forma del pulso antes y después de la dispersión seguirá siendo gaussiana, con la ventaja de que la varianza de estas distribuciones es entonces aditiva al realizar la convolución.

De esta forma, simplemente restando las varianzas de las señales antes (σ_0) y después (σ_T) de la dispersión, se extrae el valor de la fracción de la varianza de la distribución de tiempos de llegada que se debe únicamente al efecto de la dispersión cromática (${\sigma_{Ch}}^2$):

$${\sigma_{Ch}}^2 = {\sigma_T}^2 - {\sigma_0}^2.$$

Así podemos acotar el origen cuántico de la dispersión del pulso final. La fracción que se debe a la dispersión cromática será

$$\frac{{\sigma_{Ch}}^2}{{\sigma_T}^2} = \frac{{\sigma_T}^2 - {\sigma_0}^2}{{\sigma_T}^2}, \tag{10}$$

y la fracción de ésta que se debe al origen cuántico del límite de Fourier será

$$\frac{{\sigma_Q}^2}{{\sigma_0}^2}. \tag{11}$$

Entonces, se pueden certificar una fracción de los bits extraídos con un origen cuántico dado por el principio de incertidumbre. Esta será el producto de la fracción de la varianza de la distribución final que se debe a la dispersión cromática (10) por la fracción de esta última que se debe a las componentes de frecuencia cuyo origen viene dado por el límite de Fourier (11):

$$\frac{{\sigma_Q}^2}{{\sigma_C}^2} = \frac{{\sigma_{Ch}}^2}{{\sigma_T}^2} \cdot \frac{{\sigma_Q}^2}{{\sigma_0}^2},$$

y en términos de las magnitudes medidas en el laboratorio:

$$\frac{{\sigma_Q}^2}{{\sigma_C}^2} = \frac{{\sigma_T}^2 - {\sigma_0}^2}{{\sigma_T}^2} \cdot \frac{{\sigma_Q}^2}{{\sigma_0}^2}. \tag{12}$$

4. Equipo

A continuación, se describe el equipo experimental que se ha usado en el laboratorio.

(a) Láser

Se utiliza un láser de semiconductor de Fabri-Perot de Thorlabs (modelo FPL1009P-Figura 6) con montaje de mariposa de 14 pines, espectro de emisión centrado en 1548 nm y anchura a media altura de intensidad espectral de 20 nm. El espectro óptico se representa en la Figura 7. La salida del láser viene con cable de 1.5m de fibra PM conector FC/APC. El láser emite una potencia óptica continua que depende de la corriente aplicada entre los terminales de la forma representada en la Figura 8, y la temperatura: controlada mediante un termostato de enfriamiento (TEC) y medida mediante un termistor de 10 kΩ incorporado.

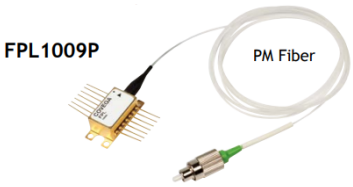


Figura 6: Láser FPL1009P.

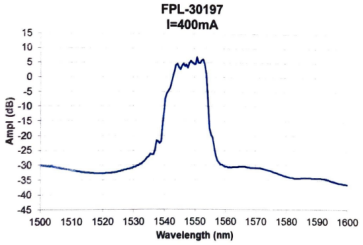


Figura 7: Espectro óptico de emisión del láser FPL1009P indicado por el fabricante.

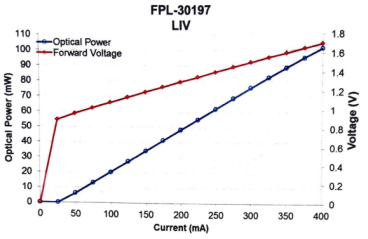


Figura 8: Relación entre corriente suministrada, voltaje y potencia óptica para el láser FPL1009P.

(b) Driver

Para el manejo del diodo láser se utiliza el Driver de Diodo Láser (cLDD) de Innolume de la Figura 9, que permite realizar las conexiones a los 14 pines del láser de forma simultánea, y controlar los valores de corriente de láser, corriente de TEC y valor de la temperatura. El driver puede conectarse y controlarse mediante software específico del fabricante, cuya interfaz puede verse en la Figura 11, a través de conexión USB a ordenador. El montaje del láser en el Driver se muestra en la figura 10.

Figura 9: cLDD

Figura 10: Láser montado en el Driver.

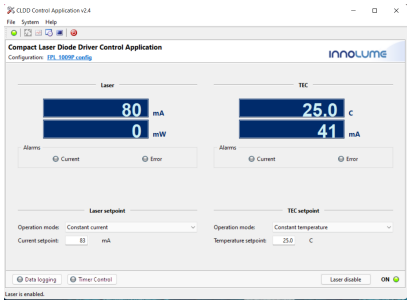


Figura 11: Interfaz de software de controlador del Driver.

(c) Fibra

Se utiliza un cable de lanzamiento OTDR de fibra óptica monomodo a 1550nm, con conexiones SC/UPC a SC/UPC de 10 km de longitud, mostrado en la Figura 12.

(d) Atenuadores

Se utilizan una serie de atenuadores que operan entre 1240 nm y 1620 nm de Thorlabs de 5 dB, 10 dB, 15 dB, 20 dBy 25 dB para disminuir la intensidad de la señal. Uno de ellos, de 10 dB, se muestra en la Figura 13.

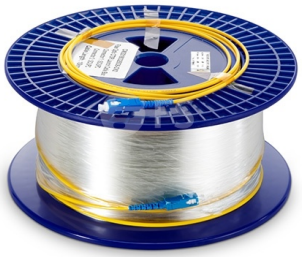


Figura 12: Cable de lanzamiento OTDR de 10 km.

Figura 13: Atenuador de 10dB.

(d) Modulador

Para modular la señal del láser y generar un pulso, se utiliza un modulador de intensidad óptico basado en $LiNbO_3$ de banda ancha (entre 1525 nm y 1605 nm) de Thorlabs, modelo LN81S-FC [14]. EL modulador reproduce en el pulso óptico la señal recibida por el *input* de RF de frecuencias hasta 15 GHz. La fibra de entrada es PM y la de salida es fibra monomodo estándar, ambas con conectores FC/UPC. El modulador se puede ver en la Figura 14, y sus conexiones en el montaje utilizado en la Figura 15.

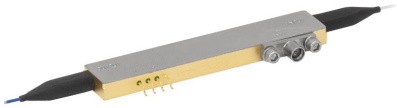


Figura 14: Modulador LN81S-FC.

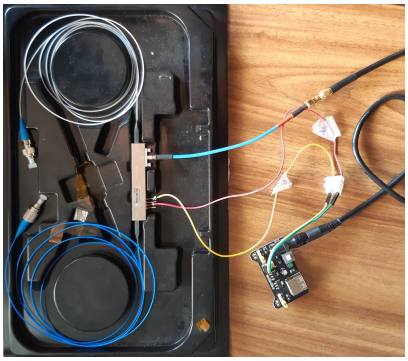


Figura 15: Montaje y conexiones del modulador de intensidad.

El principio de operación del modulador de intensidad se basa en el efecto Pockels [15], el cual es un efecto electro-óptico lineal que consiste en el cambio del índice de refracción de un medio al ser aplicado un campo eléctrico. La aplicación de un campo externo modifica la relación tensorial entre el vector desplazamiento y el vector eléctrico en el medio material, lo cual produce un cambio en el índice de refracción para el material.

La variación del índice de refracción con el campo puede expresarse en una serie de potencias de la magnitud del campo, de la forma

$$n(E) = n_0 + a_1 E + \frac{1}{2} a_2 E^2 + \cdots$$

Siempre que el grupo puntual de simetría del cristal no tenga centro de inversión que anularía el término lineal, la contribución predominante al efecto será lineal con el campo aplicado, y se tendrá

$$n(E) = n_0 - \frac{1}{2} r \, {n_0}^3 E,$$

donde n_0 es el valor del índice de refracción sin campo externo, y $r = -2\frac{a_1}{{n_0}^3}$ es el coeficiente de Pockel, que toma valores del orden de entre 10^{-12} y10^{-10} m/V [10].

El modulador funciona separando por dos caminos el haz de luz incidente. Se aplica una modulación distinta a sus fases entre estos caminos, dada por un cambio en el índice de refracción controlado por voltaje aprovechando el efecto Pockels. El campo que sigue cada uno de los caminos recorre un camino óptico diferente (misma distancia pero distinto índice), y acumularán un desfase mutuo, directamente proporcional en cada momento a la diferencia de voltaje externo aplicado al material. De esta forma, al juntarse de nuevo los dos caminos se formarán interferencias destructivas en los puntos en los cuales la diferencia de fase de ambos campos esté sea un factor de $(2n + 1)\pi$. Ajustando la señal de forma que el valor mínimo de campo eléctrico de la señal moduladora (input) se corresponda a este punto, se consigue reproducir una la señal óptica que sigue el valor de voltaje eléctrico aplicado [16]. Un esquema del funcionamiento de un modulador de amplitud se muestra en la Figura 16.

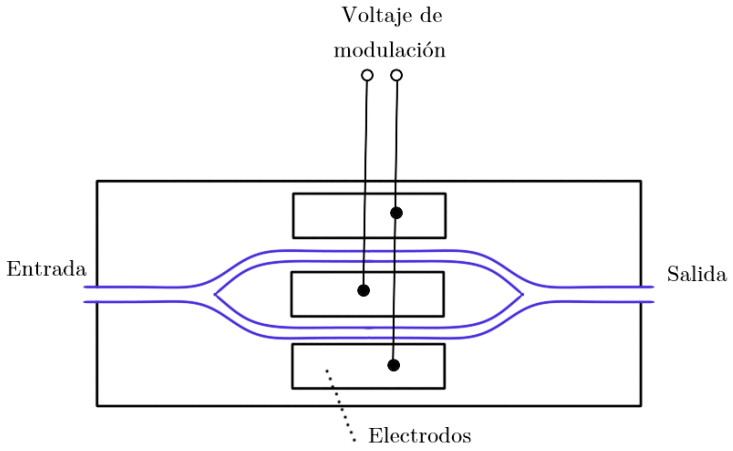


Figura 16: Esquema de funcionamiento del modulador electro-óptico de amplitud. Los dos caminos se encuentran sujetos a un índice de refracción que cambia linealmente con el voltaje aplicado, y la luz adquiere una diferencia de fase entre ambos. La señal de voltaje se aplica de forma que el campo es el mismo, pero en sentido contrario por los dos caminos, duplicando así el efecto del desfase.

Para conseguir la extinción total y una correcta modulación, es importante que los niveles de voltaje se correspondan con los característicos del medio material para el cambio de índice de refracción. Si el voltaje máximo aplicado no es suficiente para producir una diferencia de índice de refracción que produzca un desfase de π, no se producirá extinción absoluta del campo. A mayores, el modulador necesita un *offset* para establecer el punto de operación.

Para determinar los valores de voltaje necesarios, se observa en primer lugar la modulación de un pulso cuadrado de prueba en el osciloscopio mediante el detector de InGaAs, introduciendo por la entrada de voltaje de *offset* del modulador una tensión constante de 5 V y ajustando el valor de *offset* aplicando un nivel DC a la señal eléctrica hasta conseguir máxima extinción fuera del pulso. Con el mismo montaje, se determina el valor de voltaje de la señal eléctrica que mayor diferencia entre máximo y mínimo de intensidad genera.

(e) Generador de funciones

Las señales de voltaje utilizadas para modular los pulsos se generan mediante un generador de funciones de Tabor Electronics modelo WS8352 [17], que se muestra en la Figura 17. También se utiliza para la sincronización de los demás aparatos. El generador permite diseñar funciones arbitrarias con una tasa de muestras por segundo de hasta 2 G/s, y controlar independientemente dos canales de salida. Se puede manejar de forma remota a través de conexión USB mediante el software ArbConnection. La interfaz de controlador de ArbConnection se muestra en la Figura 18, y el editor de funciones se muestra en la Figura 19.

Figura 17: Generador de funciones WS8352.

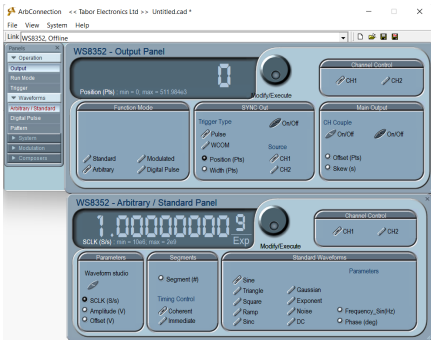


Figura 18: Interfaz de ArbConnection.

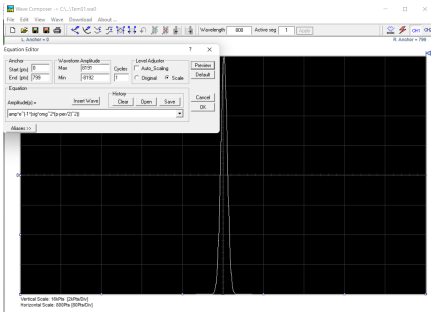


Figura 19: Interfaz de diseño de funciones para ArbConnection.

(f) Osciloscopio

Para la caracterización de las señales se visualizan en un osciloscopio de muestreo de Pico Technology modelo PicoScope 9211A (Figura 20). Permite visualizar señales en dos canales, con base de tiempos de hasta 10 ps/div y frecuencias hasta 12 GHz. El osciloscopio se controla mediante software específico del fabricante a través de conexión USB a ordenador (Figura 21).

Figura 20: Osciloscopio PicoScope 9211A.

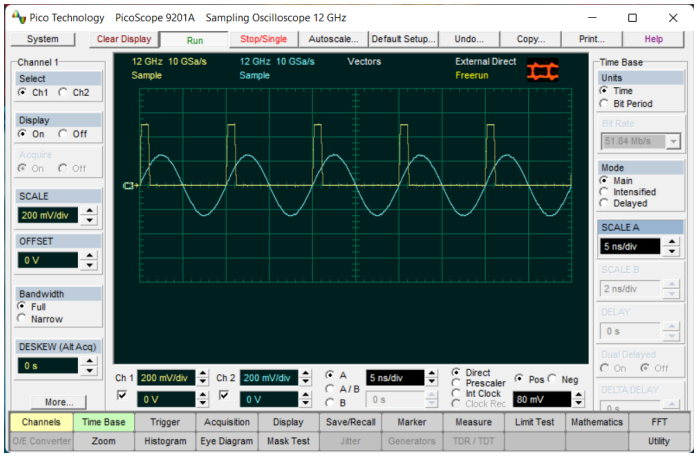


Figura 21: Interfaz de software de manejo del osciloscopio.

(g) Detector InGaAs

Para la caracterización de los pulsos se utiliza un detector rápido de InGaAs de Thorlabs modelo DET08CFC_M, mostrado en la Figura 22. El principio de operación se basa en la exposición de un semiconductor a la luz que se quiere caracteriza, con energía de GAP en el rango correspondiente. Se forma una unión P-N, y se expone la zona de carga espacial (ZCE) a la radiación. Esto provocará absorciones de fotones que excitan electrones de la banda de valencia a conducción, formándose pares electrón-hueco y produciéndose así una corriente I_{PD}, proporcional a la potencia óptica recibida (P), con una constante de proporcionalidad R (responsividad, en A/W) que depende de la longitud de onda de la señal recibida según la gráfica de la Figura 23:

$$R(\lambda) = \frac{I_{PD}}{P}.$$

Este valor de corriente que puede convertirse externamente a voltaje al pasar por una resistencia de un valor conocido, y el efecto es el de transformación de la potencia de una señal óptica a una señal de voltaje.

Para el detector utilizado, el rango espectral es de entre 800 y 1700 nm, con frecuencias de hasta 5 GHz. Consta de una entrada de fibra FC/PC y una salida SMA que se puede conectar al osciloscopio mediante un cable coaxial de 50 Ω. Se alimenta mediante una pila de 12 V. Los tiempos de respuesta son inferiores a 70 ps tanto para subida como para bajada. La respuesta típica del detector se muestra en la Figura 24.

Figura 22: Detector de infrarrojo de InGaAs DET08CFC_M.

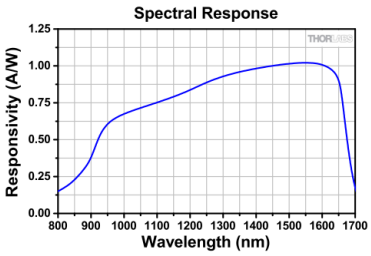


Figura 23: Sensibilidad espectral del detector DET08CFC_M.

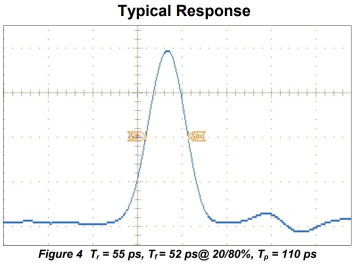


Figura 24: Respuesta típica del detector DET08CFC_M.

(h) Detector de Fotones

Se utiliza un detector de fotones individuales de Aurea modelo Lynxea_M1 [18] (Figura 25). Cuenta con un modo de correlación, que permite adquirir directamente el tiempo de detección de un fotón relativo a una señal de sincronización, situándolos en intervalos de tiempo discretos de 65 ps anchura. Se puede controlar mediante el software específico del fabricante *Aurea-Launcher* (Figura 26).

Figura 25: Detector fotones individuales Lynxea_M1.

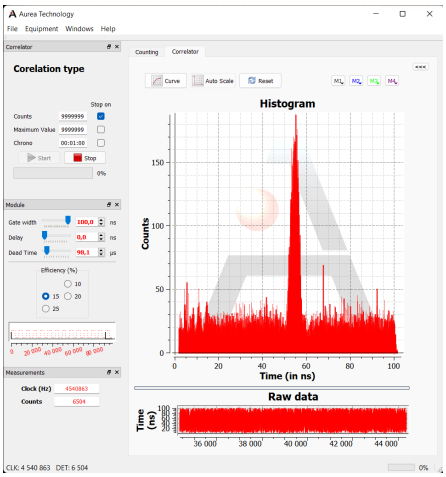


Figura 26: Interfaz de Aurea-Launcher en el modo correlación.

El detector de fotones utiliza fotodiodos de avalancha operando en régimen Geiger. Un fotodiodo de avalancha funciona de manera similar a un fotodiodo convencional, con el añadido de que opera a voltajes de inversa altos. Esto da lugar a que un electrón formado en la zona de carga espacial, al adquirir una gran energía cinética debida al campo eléctrico, pueda excitar a su vez más pares electrón-hueco, que a su vez también pueden generar más pares, produciéndose un efecto de amplificación en avalancha. Se pueden distinguir dos modos de funcionamiento [19]:

- **Régimen lineal:** para voltajes inferiores a la tensión umbral característica del diodo (V_{Th}), los pares generados no pueden acelerar lo suficiente a lo largo de la ZCE y al cabo de un número determinado de colisiones no se genera más corriente. En este caso, se consigue un efecto lineal, ya que un fotón produce una media de M electrones que contribuyen a la corriente, donde M es la ganancia del diodo, que depende de la tensión de inversa y suele tomar valores entre 10 y 100.

- **Régimen Geiger:** para voltajes superiores a V_{Th}, el efecto de avalancha no se detiene hasta que se alcanza la saturación. La saturación se da cuando la resistencia interna del diodo produce una caída de tensión que limita de nuevo el efecto. Esta caída de tensión se debe a la intensidad de corriente generada por los pares electrón-hueco del efecto de avalancha, y la saturación es entonces una situación de equilibrio. Para cada fotón se produce el mismo valor de corriente estacionaria, de ahí el origen del nombre del régimen Geiger. La velocidad a la que se da la saturación es del orden de decenas de picosegundos. Al detectarse la corriente, se deduce que se ha dado la detección de un fotón.

Para poder utilizar de forma repetida un fotodetector de avalancha en modo Geiger es necesario detener la corriente de saturación, lo cual se consigue mediante la descarga del diodo, bien de manera pasiva (a través del propio diodo) o activa (a través de un circuito externo) hasta alcanzar un voltaje inferior a V_{Th}. Esto se conoce como *quenching* y permite volver a iniciar el proceso de avalancha al absorber un fotón.

Como parámetros a considerar para este modo de detección se tienen:

- **Eficiencia:** en longitudes de onda de infrarrojo, no todas las incidencias de fotones pueden ser absorbidas por el semiconductor, y se tiene un parámetro (eficiencia) que representa cuántas absorciones se dan por cada incidencia.

- **Cuentas de oscuridad:** se da el fenómeno de cuentas de oscuridad cuando se registra una corriente que no ha sido producida por una absorción de un fotón. Se deben predominantemente a ruido térmico que produce la excitación de un par electrón-hueco en la ZCE.
- **Efectos de *Afterpulsing*:** en ocasiones la absorción de un fotón puede producir más de un pulso eléctrico, y se registran cada uno de estos como diferentes absorciones [20]. Puede deberse a efectos de cargas atrapadas en centros profundos tras la descarga del diodo.
- **Tiempo muerto de diodo:** tiempo requerido para descargar el diodo. Limita la frecuencia a la que se pueden dar detecciones y supone un límite a la tasa de generación de bits.
- **Tiempo muerto de detección:** tiempo entre detecciones que se define en el contador de fotones para permitir la descarga del diodo y además reducir los efectos de *afterpulsing*. Para los pulsos utilizados se utiliza un valor de tiempo muerto de 40 µs.

5. Descripción de los experimentos y medidas

En este capítulo se plantean y describen los montajes experimentales utilizados para la caracterización clásica (sección 5.1) y para la extracción de los bits aleatorios (sección 5.2). En la sección 5.3 se describen los pulsos de voltaje generados para modular en amplitud la señal óptica.

5.1. Caracterización Clásica

En un primer lugar se utiliza el detector de InGaAs para caracterizar la anchura de los pulsos antes y después de la dispersión. La señal de voltaje generada por el detector, que será proporcional a la potencia óptica, se visualiza en el osciloscopio y se ajustan los valores de voltaje en función del tiempo a una distribución gaussiana. El montaje utilizado para ello se representa esquemáticamente en las Figuras 27 y 28.

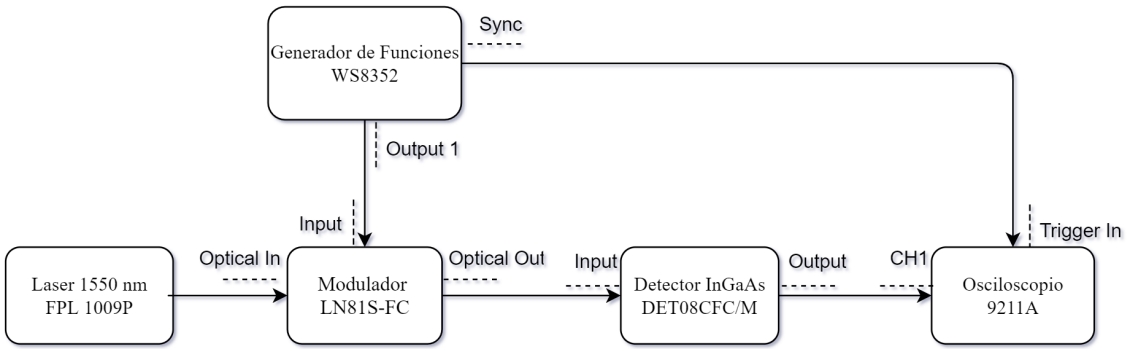


Figura 27: Diagrama del montaje para la generación y medida de tiempos de detección de fotones sin dispersión.

Para la medida sin dispersión, el valor de anchura de la distribución incluye los efectos de la anchura temporal del pulso, ruido externo y de sincronización, y la posible dispersión que aparezca en el recorrido a través de las conexiones de los diferentes equipos que componen el montaje.

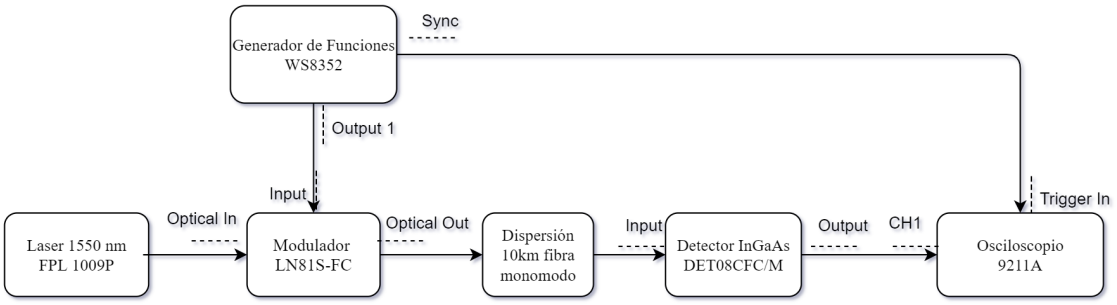


Figura 28: Diagrama del montaje para la generación y medida de tiempos de detección de fotones con dispersión.

En segundo lugar, con el mismo método se caracteriza la señal tras atravesar 10 km de fibra óptica. La anchura de esta señal ahora incluye el efecto de la dispersión cromática, además de los mismos efectos que en el caso anterior.

5.2. Caracterización Cuántica: Tiempos de detección

Siguiendo el mismo principio que en la caracterización clásica, en primer lugar se miden y caracterizan los tiempos de detección de fotones para el pulso sin dispersión cromática, y posteriormente

conectando a mayores los 10 km de fibra óptica, según los montajes de las Figuras 29 y 30

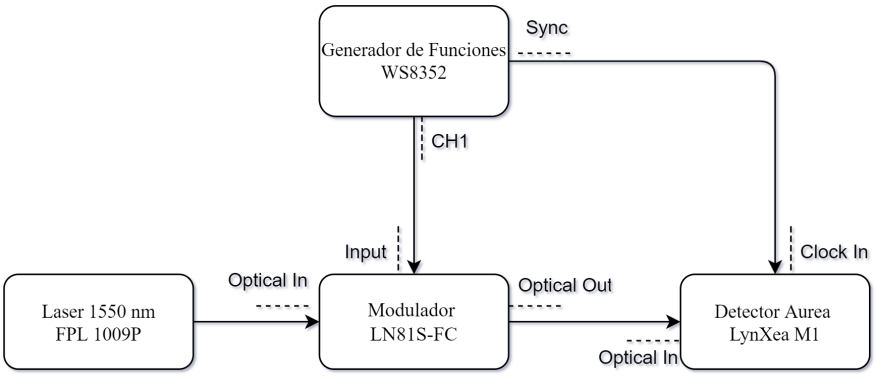


Figura 29: Diagrama del montaje para la generación y medida de tiempos de detección de fotones sin dispersión en el límite cuántico.

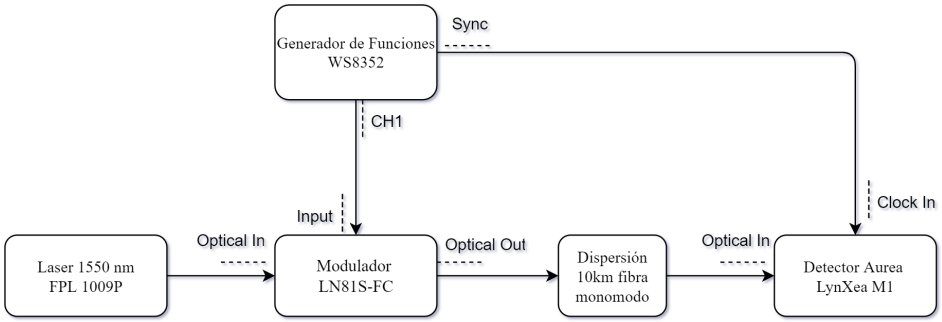


Figura 30: Diagrama del montaje para la generación y medida de tiempos de detección de fotones con dispersión en el límite cuántico.

5.3. Pulsos Utilizados

Se utilizan los siguientes pulsos ópticos, modulando en amplitud mediante el modulador según los pulsos generados en el generador de funciones. Para simplificar el tratamiento de datos se utilizan pulsos de envolvente gaussiana, y para comprobar la anchura óptima para obtener el mayor número de bits de origen cuántico, se utilizan cuatro anchuras distintas.

Se modelan con este fin dos series de pulsos. En primer lugar, para la caracterización clásica se utilizan siete pulsos con anchuras diferentes. Posteriormente, para la detección cuántica se generan los pulsos A, B, C y D.

La ecuación (en tensión eléctrica) se describe en el generador de funciones como

Figura 31: Ecuación de los pulsos en el generador de funciones WS8352.

Los parámetros del editor de ecuaciones del generador son:

- **amp**: amplitud. Valor variable en el generador.

- **p**: Punto. Para generar señales de 2.5 MHz se utilizan 800 valores de voltaje a una tasa de muestreo de $2 \cdot 10^9$ S/s
- **per**: periodo de la señal (per $= 400ns$). El pulso estará centrado en el valor $p = 200ns$.
- **omg**: frecuencia angular. Tendrá un valor fijo para todos los pulsos $omg = \dfrac{2\pi}{per} = 2\pi \cdot 2{,}5\,\text{MHz}$.

El valor de "sig" está relacionado con la varianza de la función de la forma

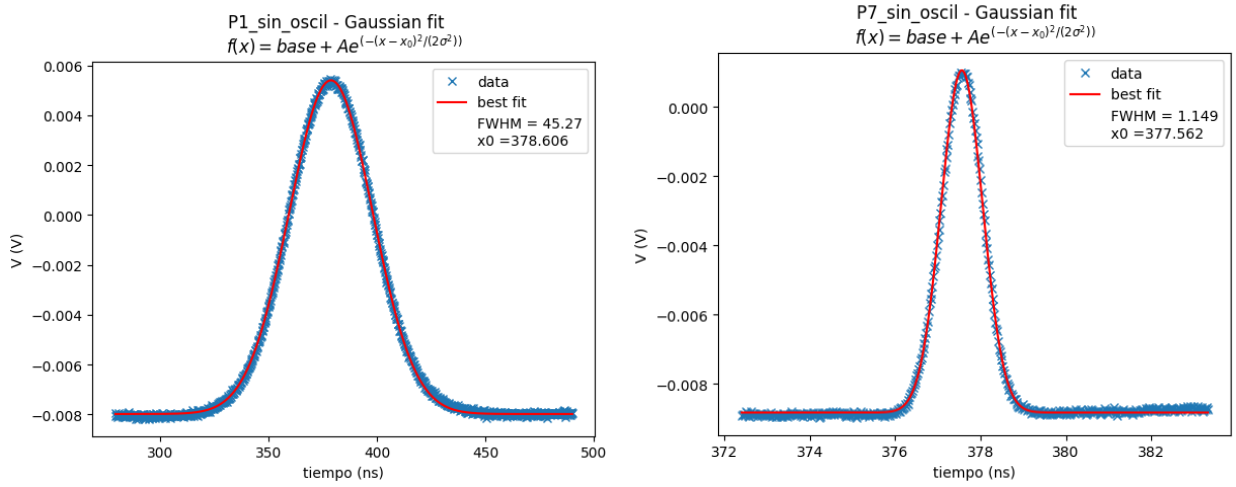
$$sig = \frac{1}{2omg^2}\frac{1}{\sigma^2}.$$

Los valores de *sig* y σ de los pulsos generados, según los valores introducidos en el generador son los indicados en la Tabla 1.

Pulso	**sig**	**σ (ns)**	**Pulso**	**sig**	**σ (ns)**
1	4	22.51	A	25	9.00
2	11	13.75	B	4476	0.67
3	25	9.00	C	9487	0.42
4	53	6.18	D	$2 \cdot 10^7$	0.01
5	200	4.46			
6	600	3.18			
7	10000	0.45			

Tabla 1: *sig* y σ según los valores del generador de funciones para los siete pulsos utilizados para la caracterización clásica (1, 2, 3, 4, 5, 6, 7) y los cuatro pulsos utilizados para las medidas cuánticas (A, B, C, D).

La visualización de los mismos en el osciloscopio mediante el detector de infrarrojo confirma que se están generando pulsos de envolvente gaussiana, y con una dependencia esperada para las anchuras, como puede apreciarse en la Figura 32, en la cual se muestran los ajustes a funciones gaussianas de los pulsos 1 y 7 a la salida del modulador.



(a) Visualización del pulso 1.

(b) Visualización del pulso 7.

Figura 32: Visualización en el osciloscopio y ajuste de los pulsos 1 y 7 a la salida del modulador de intensidad.

6. Resultados experimentales

Los resultados de las medidas en el límite clásico con el detector de infrarrojo, y el ajuste utilizado para caracterizar los pulsos se presentan en la sección 6.1. Lo mismo se presenta en la sección 6.2 para las medidas con el detector de fotones, y se describe el esquema de extracción de bits.

6.1. Medidas clásicas

Para caracterizar los pulsos en el límite clásico se realiza un ajuste a una función gaussiana utilizando los datos de voltaje en función del tiempo extraídos del osciloscopio. Se utiliza un método de optimización no lineal por mínimos cuadrados [21] a la ecuación

$$f(x) = base + amp \cdot \exp\left\{-\frac{(x-x_0)^2}{2\sigma^2}\right\},$$

con cuatro parámetros a ajustar:

- base: valor de base de voltaje, permite disminuir el efecto de una extinción no completa en el modulador y el ruido de detección.
- amp: da cuenta de la intensidad máxima generada por el pulso, es decir, es proporcional a la amplitud del pulso.
- x_0: centro de la distribución.
- σ: desviación estándar.

El ajuste se realiza tanto para las medidas previas a la dispersión como para las medidas a pulsos ya dispersados mediante el cable de lanzamiento de 10 km. Esto permite extraer, en un primer nivel clásico, el ensanchamiento debido a la dispersión cromática. Se comprueba que el efecto se debe a la dispersión cromática midiendo el efecto de la variación de ${\sigma_0}^2$ en el ensanchamiento final según la ecuación (4). Para poder realizar un ajuste lineal, se utiliza la ecuación equivalente (5).

$$\frac{{\sigma_T}^2}{{\sigma_0}^2} = 1 + \frac{{\beta_2}^2 z^2}{{\sigma_0}^4}.$$

Puesto que β_2 y $z = 10\,\text{km}$ son constantes en todas las medidas, se puede ajustar las varianzas antes y después de la dispersión según

$$\frac{{\sigma_T}^2}{{\sigma_0}^2} = b + a\frac{1}{{\sigma_0}^4}, \tag{13}$$

con $a = \beta^2 z^2$ y $b = 1$ constantes del ajuste. Los resultados de las varianzas obtenidas para los siete pulsos son los indicados en la Tabla 2.

Pulso	$\boldsymbol{\sigma_0}$**(ns)**	$\boldsymbol{\sigma_T}$**(ns)**	$\left(\boldsymbol{\sigma_T}/\boldsymbol{\sigma_0}\right)^2$	$\boldsymbol{\sigma_0}^{-4}$ **(ns^{-4})**
1	19.2244 ± 0.014	19.51 ± 0.02	1.030 ± 0.006	(7.32 ± 0.04) · 10^{-6}
2	11.703 ± 0.009	11.843 ± 0.016	1.024 ± 0.006	(5.33 ± 0.03) · 10^{-5}
3	7.897 ± 0.008	7.998 ± 0.018	1.026 ± 0.010	(2.571 ± 0.019) · 10^{-4}
4	5.537 ± 0.009	5.632 ± 0.018	1.035 ± 0.015	(1.064 ± 0.013) · 10^{-3}
5	2.897 ± 0.009	2.952 ± 0.011	1.04 ± 0.02	(1.420 ± 0.04) · 10^{-2}
6	1.630 ± 0.008	1.683 ± 0.009	1.07 ± 0.03	0.142 ± 0.005
7	0.4881 ± 0.0008	0.619 ± 0.002	1.61 ± 0.04	17.614 ± 0.2

Tabla 2: Valores de desviación estándar de los pulsos antes (σ_0) y después (σ_T) de la dispersión en 10 km de fibra óptica obtenidos a partir de las medidas con el detector de infrarrojo DET08CFC_M en el osciloscopio.

Estos datos se presentan de forma resumida en la gráfica de la Figura 33.
Los datos se ajustan a una tendencia lineal (13) y se obtienen los valores de

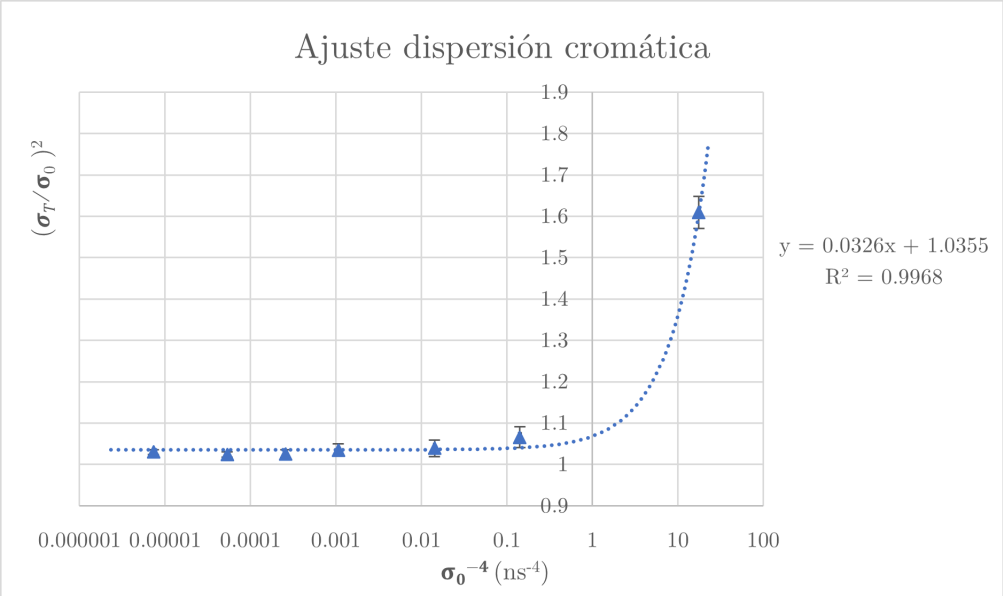


Figura 33: Gráfica del ajuste a la ecuación (13), en escala logarítmica en el eje x. Se observa el efecto esperado de ensanchamiento debido a la dispersión cromática.

$$a = 0{,}03260482 \qquad s(a) = 0{,}000828415$$
$$b = 1{,}03552979 \qquad s(b) = 0{,}005515423$$
$$R^2 = 0{,}99678262.$$

Se comprueba que se ajusta bien al ensanchamiento esperado para la dispersión cromática, lo que confirma que ésta es la dispersión dominante en el montaje utilizado. A partir del valor de a, puesto que $z = 10\,\text{km}$, se obtiene el valor de

$$\beta_2 = \sqrt{a}/z,$$
$$\beta_2 = 18{,}1 \pm 0{,}4\,\text{ps/km}.$$

Los valores obtenidos para las varianzas a la salida del modulador (σ_0) no concuerdan exactamente con los esperados según las ecuaciones de las funciones del generador, siendo los medidos notablemente menores. Para la caracterización se utilizan los valores medidos utilizando el detector de infrarrojo.

6.2. Medidas con el detector de fotones

Los datos de salida del detector de fotones consisten en una serie de instantes de detección, acompañados por un factor de corrección que corrige la no-linealidad diferencial que se da en la conversión de datos analógicos a digitales (conversión de tiempo de llegada a intervalos del histograma).

Se reconstruye una función de probabilidad de detección según el instante temporal utilizando estos datos, contando el número de detecciones que se dan en cada intervalo de tiempo. Finalmente,

se ajusta mediante un método de optimización no-lineal por mínimos cuadrados, de la misma forma que en el caso clásico, para las medidas previas a la dispersión y para los pulsos dispersados:

$$f(x) = base + amp \cdot \exp\left\{-\frac{(x-x_0)^2}{2\sigma^2}\right\}, \tag{14}$$

con cuatro parámetros a ajustar:

- base: valor de base de detecciones, permite disminuir el efecto de una extinción no completa en el modulador y las cuentas de oscuridad.
- amp: amplitud. Da cuenta del número máximo de detecciones.
- x_0: centro de la distribución.
- σ: desviación estándar.

Se toman medidas de 1 minuto para cada pulso sin dispersión, y medidas de 10 minutos de los pulsos con dispersión para extraer las cadenas de bits aleatorios.

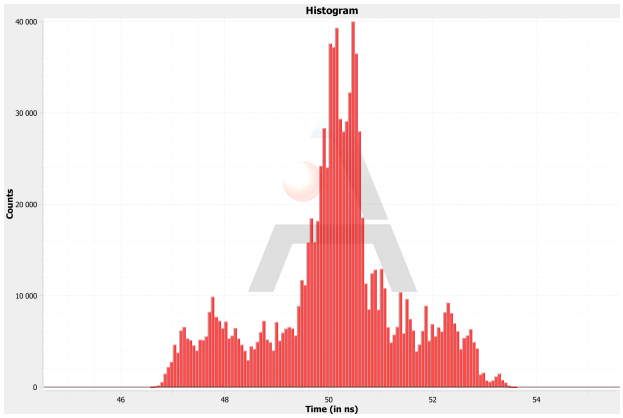
Los resultados de los ajustes se encuentran detallados en el Anexo. En la Figura 34 se muestran los histogramas de salida del detector de fotones, acompañados por el resultado del ajuste a la ecuación (14), para el pulso C. A mayores, se dividen los intervalos de tiempos de llegada correspondientes a 0 y 1.

Los resultados de los ajustes se resumen en la Tabla 3. Aparecen los valores aproximados del QCNR calculados según la ecuación (9), según los valores de anchura temporal medida antes y después de la dispersión.

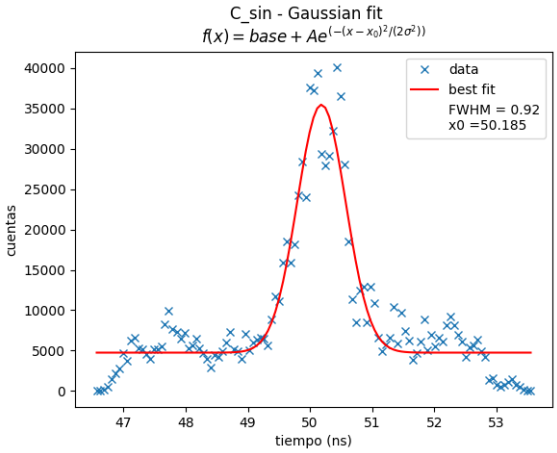
Pulso	$\boldsymbol{\sigma_0}$**(ns)**	$\boldsymbol{\sigma_0^2}$ **(ns²)**	$\boldsymbol{\sigma_T}$**(ns)**	$\boldsymbol{\sigma_T^2}$ **(ns²)**	$\boldsymbol{x_0}$ **(ns)**	**QCNR (dB)**
A	7.85 ± 0.09	62 ± 3	8.78 ± 0.19	77 ± 7	50.20 ± 0.12	-107.4 ± 1.8
B	1.01 ± 0.05	1.0 ± 0.2	1.37 ± 0.11	1.9 ± 0.6	49.89 ± 0.09	-86 ± 3
C	0.391 ± 0.018	0.153 ± 0.03	0.52 ± 0.02	0.27 ± 0.05	49.86 ± 0.02	-78 ± 2
D	0.391 ± 0.019	0.153 ± 0.03	0.45 ± 0.03	0.20 ± 0.05	49.84 ± 0.03	-80 ± 5
C2	0.391 ± 0.018	0.153 ± 0.03	0.47± 0.03	0.23± 0.06	30.56± 0.03	-79 ± 3
C3	0.391 ± 0.018	0.153 ± 0.03	0.55± 0.02	0.31± 0.05	30.65± 0.02	-77.3 ± 1.7
C4	0.391 ± 0.018	0.153 ± 0.03	0.54± 0.02	0.29± 0.05	30.60± 0.02	-77.6 ± 1.9

Tabla 3: Resultados de los ajustes de los pulsos A, B, C y D antes y después de la dispersión a la ecuación (14).

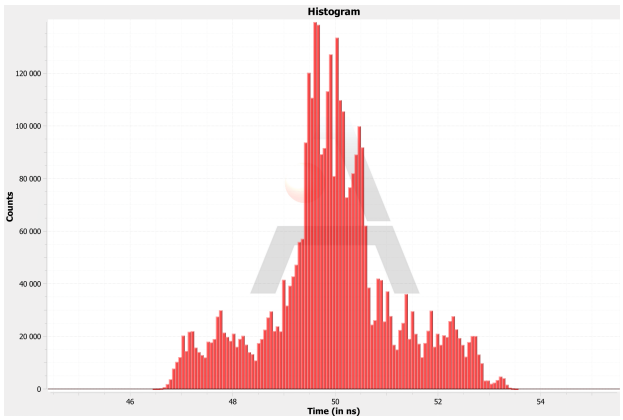
Se aprecia que para el pulso D, a pesar de tener un valor teórico de σ_0 mucho menor al pulso C, realmente se obtienen resultados similares a los del pulso C. Se debe seguramente a que el generador es incapaz de generar cambios tan rápidos en voltaje. Por lo tanto, aunque sería más conveniente utilizar un pulso lo más estrecho posible para maximizar el QCNR, se utiliza el pulso C para extraer cuatro cadenas de bits de prueba (C, C2, C3 Y C4) para comprobar diferentes resultados.



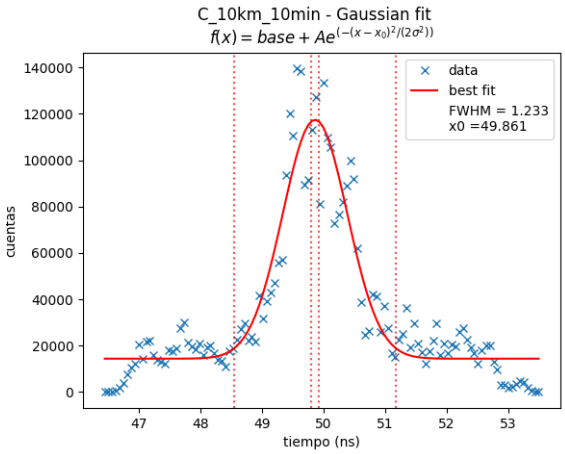
(a) Histograma de tiempos de llegada sin dispersión.



(b) Ajuste de tiempos de llegada sin dispersión.



(c) Histograma de tiempos de llegada con dispersión.



(d) Ajuste de tiempos de llegada con dispersión.

Figura 34: Comparación del pulso C antes y después de la dispersión.

Para limitar el efecto de la incertidumbre en la medida del centro de la distribución, no se consideran los tiempos de llegada que se sitúen en un intervalo $\Delta X = (x_0 - 3\sigma_{x_0}, x_0 + 3\sigma_{x_0})$ donde σ_{x_0} es el error estándar para el centro obtenido del ajuste no lineal. Asimismo, se limita la selección de detecciones dentro del pulso en un intervalo de $x_0 \pm 2{,}5\sigma_T$ para asegurar que las detecciones son mayoritariamente fotones del pulso. Un esquema de los intervalos utilizados para asignar 0 o 1 se muestra en la Figura 35.

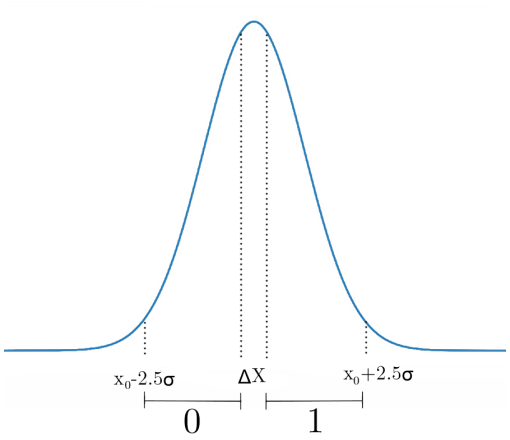


Figura 35: Intervalos utilizados para asignar 0 o 1 según los tiempos de detección.

En la medida de 10 minutos para el pulso C, se obtiene un total de 2563050 bits, lo que corresponde a una tasa de 534 kB/s.

7. Análisis de resultados

En este capítulo, se analizan los bits extraídos. En primer lugar, en la sección 7.1.1 se realiza una corrección para los sesgos y desviaciones que aparecen en el proceso de extracción. Posteriormente, en la sección 7.1.2 se calcula la entropía empírica de los bits generados. En la sección 7.1.3 se ejecutan una serie de test de aleatoriedad. Finalmente, se calcula una cota de la entropía de origen cuántico en la sección 7.2.

7.1. Calidad de los bytes extraídos

7.1.1. Corrector de Von Neumann

Los bits extraídos presentan en general sesgos que producen que haya una mayor frecuencia aparición de 1 o de 0, del orden de un 2 %.

Una corrector sencillo de implementar que corrige la desviación es el corrector de Von Neumann. Consiste en tomar series de dos bits y descartarlos, o convertirlos en 1 o 0 según la siguiente Tabla:

Entrada	Salida
00	-
01	0
10	1
11	-

Tabla 4: Conversión de bits de entrada a bits de salida en el corrector de Von Neumann.

Siempre que los bits de entrada sean independientes, este corrector elimina las desviaciones hacia un mayor número de bits de 0 o de 1 [22], pero el coste es la pérdida del 75 % de los bits en el caso de cadenas perfectamente aleatorias y sin desviación. Para cadenas que sí presenten una desviación, la pérdida de bits será mayor.

Para el caso analizado (pulso C), el número de bits iniciales es de 2463050 bits, de los cuales el 50,62 % son 1, y el 49,38 % son 0. El número de bits finales es de 637693, lo que supone una pérdida del 75,12 % de los bits.

7.1.2. Entropía binaria

Utilizamos la definición de entropía de Shannon (H) para caracterizar la entropía de los bytes generados de esta forma:

$$H = -k \sum_{i=1}^{n} p_i \log_2 p_i = \sum_{i=1}^{n} p_i \left(k \log_2 \frac{1}{p_i} \right), \tag{15}$$

donde

- k es una constante de proporcionalidad, que introduciremos de forma que la entropía máxima por byte sea de 8 bits.
- p_i es la probabilidad de que se dé el proceso i-ésimo

- n es el número total de procesos distintos posibles

Para obtener empíricamente la entropía asociada a la medida utilizada para extraer los números aleatorios, calculamos el valor de H suponiendo que las probabilidades p_i se corresponden con la frecuencia de aparición de cada combinación i.

En este caso, para un total de $8N$ bits, agrupados en bytes (8 bits/byte), entre los cuales aparece cada posible combinación (i) de bits h_i veces tendremos que

$$n = 2^8, \qquad p_i = \frac{h_i}{N}.$$

Sustituyendo estos valores en la ecuación (15) se llega a

$$H = k \sum_{i=1}^{2^8} \frac{h_i}{N} \log_2 \frac{N}{h_i}. \tag{16}$$

La entropía máxima corresponde a igualdad de probabilidad en todas las combinaciones de 8 bits. Entonces $h_i = \frac{1}{2^{-8}}$, y sustituyendo en (16) e igualando a $S_{max} = 8$, se llega a $k = 1$.

Aplicando esta definición de entropía a los bits extraídos, agrupándolos en bytes, se llega los valores de la Tabla 5.

Pulso	Entropía datos en crudo	Entropía tras corrector de Von Neumann
C	7.99839 (0.99980 por bit)	7.99764 (0.99971 por bit)
C2	7.97506 (0.99688 por bit)	7.99920 (0.99990 por bit)
C3	7.96299 (0.99537 por bit)	7.99900 (0.99988 por bit)
C4	7.99964 (0.99996 por bit)	7.99881 (0.99985 por bit)

Tabla 5: Valores de la entropía binaria calculada para los bits en crudo, y tras aplicar el corrector de Von Neumann.

7.1.3. Test de aleatoriedad

Para un generador físico de números aleatorios, la aleatoriedad realmente no es una propiedad propia de los números generados, sino que es propia del proceso utilizado para obtenerlos. En este sentido hay que confiar en que efectivamente el suceso es aleatorio. En el caso de el QRNG diseñado, esto es razonable, ya que se aprovecha una indeterminación dada por los principios de la física cuántica.

En cualquier caso, se pueden estudiar estadísticamente los números generados y compararlos con las distribuciones que serían producidas por un generador aleatorio ideal mediante diferentes test que analizan las cadenas de bits. El hecho de que los números generados pasen dichos test genera una cierta confianza hacia la aleatoriedad del proceso que los produjo. No obstante, no hay que olvidar que, a pesar de su nombre, los test de aleatoriedad comprueban estadísticas de los números, y no la aleatoriedad del suceso. Los números producidos con un generador realmente aleatorio pueden fallar algunos test, y a la inversa, un número generado de manera determinista (por ejemplo, mediante un PRNG) puede superar los test. Sin embargo, lo habitual es que una fuente aleatoria supere de forma consistente los test de aleatoriedad.

Existen diferentes test para analizar los números extraídos. Éstos analizan las cadenas de bits introducidos, realizando análisis de estadísticas como, entre otros:

- *Frequency (Monobit) Test*: frecuencia de aparición de 1 y 0.
- *Tests for the Longest-Run-of-Ones in a Block*: frecuencia de repetición ininterrumpida de un mismo bit.
- *Discrete Fourier Transform (Spectral) Test*: frecuencia de repetición de patrones de m bits.
- *The Binary Matrix Rank Test*: dependencia lineal entre subcadenas.
- *Maurer's "Universal Statistical" Test*: capacidad de compresión sin pérdida de información de la secuencia.

Comparando los resultados obtenidos de una de estas estadísticas con los esperados para una distribución ideal aleatoria y uniformemente distribuida en 1 y 0, se obtiene el denominado valor p (p-*value*) que representa la probabilidad de que un generador aleatorio ideal reproduzca resultados menos aleatorios que la muestra analizada. En el caso límite, un valor de p-*value* $= 0$ representaría la imposibilidad de que la muestra fuera aleatoria, y un valor de p-*value* $= 1$ representaría una muestra perfectamente aleatoria. Para cada test, se producen una serie de valores p.

Un generador ideal fallará una cierta cantidad de test. Para comparar las cadenas analizadas y calcular un nivel de confianza de la aleatoriedad, generalmente se establece un límite inferior α para el número de valores p que no pasen el test $\%P$, de forma que si $\%P < \alpha$ se interpreta como que la muestra ha fallado este test de aleatoriedad. Cuanto mayor sea α, más difícil será que una muestra de origen no aleatorio supere los test: disminuye los falsos positivos. Sin embargo, establecer este límite demasiado alto implica que secuencias que provienen de un proceso realmente aleatorio podrían fallar el test: aumentar α también aumenta los falsos negativos. Típicamente, se escogen valores de α entre 0,001 y 0,01.

Varios de estos test están implementados en la suite de *NIST Statistical Test Suite* [23]. Se ejecutan un total de 41 test para las secuencias extraídas. 16 de estos resultados para el pulso C, antes y después de aplicar el corrector de Von Neumann se presentan en la Tabla 6.

Para los datos sin corregir, las cadenas fallan el test de frecuencia, y por tanto fallan todos los test derivados del mismo. Una vez se aplica el corrector, las cadenas pasan todos los test de aleatoriedad consistentemente, lo que sugiere que el fallo se debía a la asimetría de 1s y 0s. Esto es así para los 4 pulsos utilizados para extraer números aleatorios. Los resultados de los test para las cuatro cadenas de bits tras aplicar el corrector de Von Neumann se pueden encontrar en el Anexo.

Test (pulso C)	Datos en crudo		Datos tras corrección	
	% P	Conclusión	% P	Conclusión
Frequency Test (Monobit)	$1.0189 \cdot 10^{-152}$	No aleatorio	0.9053	Aleatorio
Frequency Test within a Block	$1.0758 \cdot 10^{-52}$	No aleatorio	0.6907	Aleatorio
Run Test	0.0	No aleatorio	0.7137	Aleatorio
Longest Run of Ones in a Block	0.006515	No aleatorio	0.8530	Aleatorio
Binary Matrix Rank Test	0.6414	Aleatorio	0.8560	Aleatorio
Discrete Fourier Transform (Spectral) Test	0.7136	Aleatorio	0.2240	Aleatorio
Non-Overlapping Template Matching Test	$1.7280 \cdot 10^{-13}$	Aleatorio	0.3949	Aleatorio
Overlapping Template Matching Test	$4.3880 \cdot 10^{-19}$	No aleatorio	0.2156	Aleatorio
Maurer's Universal Statistical test	0.04713	Aleatorio	0.7073	Aleatorio
Linear Complexity Test	0.3671	Aleatorio	0.5032	Aleatorio
Serial test	0.0001399	No aleatorio	0.7652	Aleatorio
Approximate Entropy Test	$4.5185 \cdot 10^{-56}$	No aleatorio	0.2017	Aleatorio
Cummulative Sums (Forward) Test	$5.2463 \cdot 10^{-157}$	No aleatorio	0.4657	Aleatorio
Cummulative Sums (Reverse) Test	$4.8329 \cdot 10^{-153}$	No aleatorio	0.37947	Aleatorio
Random Excursions Test: State +1	0.3530	Aleatorio	0.2917	Aleatorio
Random Excursions Variant Test: State +1	0.6698	Aleatorio	0.9797	Aleatorio

Tabla 6: Resultados de 16 de los test aplicados para los números extraídos a partir del pulso C antes y después de aplicar el corrector de Von Neumann.

7.2. Origen cuántico

A partir del QCRN se puede estimar una cota de cuántos bits son de origen certificable cuántico según el principio de incertidumbre, según la expresión

$$B_Q = B \cdot 10^{QCNR/10},$$

donde B_Q es el número de bits de origen cuántico y B es el número de bits totales. Los resultados para los cuatro pulsos C, C2, C3 y C4 se representan en la Tabla 7.

Pulso	QCNR	Número de bits	Bits de origen cuántico
C	-78 ± 2	2563050	0.04 ± 0.02
C2	-79 ± 3	5952931	0.07 ±0.06
C3	-77.3 ± 1.7	5329672	0.10 ± 0.04
C4	-77.6 ± 1.9	5324567	0.09 ± 0.04

Tabla 7: Número de bits de origen certificable cuántico calculados para los cuatro pulsos C, C2, C3 y C4.

Los resultados son menores a la unidad, y harían falta medidas más largas para poder extraer al menos un bit de origen certificado mediante este principio de incertidumbre cuántico.

8. Posibles ampliaciones y líneas futuras

8.1. Aumento del QCNR

El mayor factor que influye en el número de bits de origen cuántico que se logran extraer es el bajo valor que toma el QCNR. El láser utilizado está bastante lejos de estar limitado por Fourier, y el cociente $\frac{{\sigma_Q}^2}{{\sigma_0}^2}$ toma valores del orden de 10^{-7}.

Una solución para esto sería trabajar con un láser pulsado limitado, o cerca del límite de Fourier, con lo que este valor aumentaría significativamente. En el caso de un pulso limitado por Fourier, se tendría $\frac{{\sigma_Q}^2}{{\sigma_0}^2} = 1$, y aunque habría que tener en cuenta los efectos inevitables de ruido instrumental y otros factores que producen un ensanchamiento, la mayor parte del valor del QCNR se deberá únicamente al cociente del ensanchamiento debido a la dispersión cromática, que para los pulsos utilizados era del orden de $\frac{{\sigma_{Ch}}^2}{{\sigma_T}^2} \approx 0{,}5$, con lo que se tendría que hasta la mitad de los bits serían de origen cuántico.

8.2. Aumento de la tasa de bits

Para aumentar la tasa de producción neta de bits, hay dos opciones:

- Aumentar la tasa de repetición del láser: se utilizan frecuencias de 2.5 MHz, mayoritariamente debido a las limitaciones del generador de señales y la sincronización con el detector. Aumentar la tasa de repetición produciría un aumento lineal del número de bits producidos.
- Aumentar el número de fotones por pulso. Esto produciría un aumento de pulsos con detección ($P(n \geq 1)$ aumenta), pero a su vez aumentaría la fracción de pulsos de dos o más fotones en las detecciones.
- Disminución del tiempo muerto del detector. El tiempo muerto supone un límite superior de la frecuencia a la cual pueden darse detecciones. Podría reducirse el tiempo muerto, y con ello aumentar el número de bits, con el uso de detectores más rápidos, siempre que no haya problemas de *afterpulsing*.

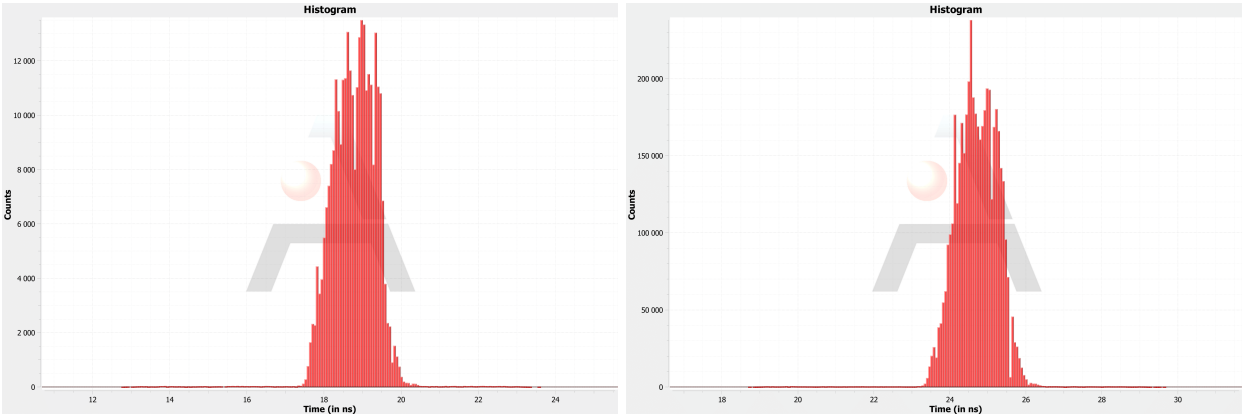
8.3. Post procesado

Existen otras opciones de post procesado de los bits para reducir las asimetrías en 1 y 0 y que eliminarían un menor porcentaje de bits, y además pueden corregir correlaciones [24].

La más común es utilizar una matriz $m \times n$ que multiplique n bits de entrada y los convierta en $m < n$ bits de salida. Esto requiere construir una matriz adecuada y de origen completamente aleatorio, e implica un estudio más detallado de la entropía y las correlaciones de los bits en crudo.

8.4. Estudio preliminar con un láser cerca del límite de Fourier

Se han intentado unas pruebas iniciales con un láser centrado en 1030 nm que emite pulsos de 1 ps de anchura a media altura temporal, muy cerca del límite de Fourier para su espectro de frecuencias. Con el equipo disponible la dificultad radica en la sincronización de los diferentes equipos debido a la alta tasa de repetición del láser y el límite de sincronización con el detector de fotones. Los resultados obtenidos indican que, a las bajas duraciones temporales a las que se está trabajando,y los efectos del *jitter* son difíciles de caracterizar y además toman valores comparables y superiores a la propia anchura del pulso. En este aspecto, no se pueden usar los mismos cálculos que para el QRNG diseñado, y es complicado establecer la cota de entropía que proviene del principio de incertidumbre debido a la dispersión. Los resultados de los histogramas de los tiempos de detección se muestran en la Figura 36.



(a) Pulso del láser cerca del límite de Fourier antes de la dispersión.

(b) Pulso del láser cerca del límite de Fourier tras ser dispersado mediante un grating de difracción.

Figura 36: Histogramas de tiempos de detección para un pulso cerca del límite de Fourier antes y después de aplicar dispersión cromática.

Una posible forma de obtener los números aleatorios sería dividir la ventana total de tiempos de llegada en 2^N intervalos equiprobables y asignar N bits al tiempo de llegada de cada fotón en según el intervalo de tiempo en el que se dé la detección. Tras una corrección con una matriz de procesado, se corrigen la mayor parte de las desviaciones y se superan la mayoría de los test, siendo los no superados distintos en cada ocasión.

9. Resumen y conclusiones

En resumen, en este Trabajo de Fin de Grado, se ha planteado y desarrollado en el laboratorio un experimento en el que extraer números aleatorios de incertidumbre de origen cuántico, para lo cual se ha:

- Estudiado y caracterizado la dispersión en fibra óptica.
- Estudiado el origen de las diferentes componentes de frecuencia de un pulso óptico de duración temporal finita.
- Diseñado un experimento que permite la extracción de bits de origen cuántico y desarrollado un código de Python que automatiza la extracción a partir de los ficheros de salida del equipo.
- Extraído cuatro cadenas de prueba de números aleatorios mediante series de medidas largas y realizado un análisis de la calidad los mismos.
- Calculado una cota para la entropía cuyo origen es el principio de incertidumbre cuántico.
- Propuesto mejoras a diferentes aspectos del QRNG.
- Planteado un experimento y realizado unas medidas iniciales con un láser cerca del límite de Fourier.

La implementación experimental del QRNG diseñado confirma los resultados esperados en cuanto a dispersión y genera números aleatorios de buena calidad, con valores altos de entropía por bit, en torno a 0.9998, y que superan consistentemente los test de aleatoriedad planteados. Las tasas de generación de bits en crudo son del orden de 500 Bytes por segundo (Bps) para el pulso C, y de 1100 Bps para los pulsos C2, C3, y C4.

Una vez aplicado el corrector de Von Neumann, las tasas caen a aproximadamente el 25 % de la tasa en crudo, es decir, unos 130 Bps para el pulso C y en torno a 280 Bps para los pulsos C2, C3 y C4. Como se ha comentado, sería posible aumentar esta tasa mediante un post procesado distinto.

Se ha podido verificar que una parte de la aleatoriedad se debe al principio de incertidumbre tiempo-energía. Este principio es una confirmación de máxima seguridad para los bits producidos, puesto que es físicamente imposible predecirlos o alterarlos, incluso aunque un atacante pudiese manipular a voluntad las condiciones del laboratorio y el equipo utilizado.

El resto de bits generados se deben también a un proceso cuántico que es el proceso de captura de un fotón. De esta forma, tienen un origen aleatorio, aunque no surjan del principio de indeterminación que buscamos para la certificación de origen cuántico impredecible. Este proceso de captura podría ser afectado por magnitudes clásicas ya que la probabilidad de detección depende de factores como la forma temporal del pulso, que podrían alterarse externamente, en caso de suponer un atacante que controlase a la perfección la emisión. No obstante, como se ha podido comprobar, la calidad de los números así generados es buena para su aplicación en distintos ámbitos, incluyendo la generación de claves criptográficas o la simulación.

A mayores, al nivel de unas primeras pruebas de concepto, se prevé que sería posible mejorar hasta casi un 50 % la tasa de bits que provienen del principio de incertidumbre, a la vez que aumentar la tasa de producción de bits en crudo, mediante un láser más rápido y de producto tiempo-frecuencia cercano al valor mínimo por Fourier.

Referencias

[1] J. Haw, S. Assad, A. Lance et al., "Maximization of Extractable Randomness in a Quantum Random-Number Generator", Phys. Rev. Applied, **Vol. 3, nº 5**, (2015).

[2] J. F. Traub, H. Woźniakowski, "The Monte Carlo Algorithm with a Pseudorandom Generator", Mathematics of Computation,**Vol. 58, nº 197**, (1992), págs. 323-339.

[3] H. Schmidt, "Quantum-Mechanical Random-Number Generator", Journal of Applied Physics, (1970), **Vol. 41, nº 2**, págs. 462-468.

[4] J. Walker. "HotBits: Genuine random numbers, generated by radioactive decay". Dirección: `https://www.fourmilab.ch/hotbits/`. Fecha de consulta: 09-07-2022.

[5] L. Mandel y E. Wolf, "Optical coherence and quantum optics", Cambridge: Cambridge University Press, (1995).

[6] C. Gabriel, C. Wittmann, D. Sych et al., "A generator for unique quantum random numbers based on vacuum states", Nature Photonics,**Vol. 4, nº 10**, (2010), págs. 711-715.

[7] G. Keiser, "Optical fiber communications", 3ª edición, MacGraw - Hill series in electrical engineering communications and signal processing. Boston: MacGraw-Hill, (2000).

[8] D. Gloge, "Weakly Guiding Fibers", Applied Optics, **Vol. 10, nº10**, (1971), págs. 2252-2258.

[9] G. P. Agrawal, "Nonlinear fiber optics", Boston: Academic Press, (2007).

[10] B. E. A. Saleh, "Fundamentals of photonics",2ª edición, Wiley series in pure and applied optics. New York: John Wiley & Sons, (2007).

[11] C. L. Tang, H. Statz y G. deMars, "Spectral Output and Spiking Behavior of Solid-State Lasers", Journal of Applied Physics,**Vol. 34, nº 8**, (1963), págs. 2289-2295.

[12] A. Papoulis, "Signal analysis", 3ª edición, Macgraw - Hill Electrical and Electronic Engineering Series. Auckland: MacGraw-Hill, (1987).

[13] E. W. Weisstein. "Gaussian Function. From MathWorld—A Wolfram Web Resource". Dirección: `https://mathworld.wolfram.com/GaussianFunction.html`. Fecha de consulta: 09-07-2022.

[14] THORLABS, "10 GHz Lithium Niobate Intensity Modulator with Internal Photodetector LN81S-FC". Dirección: `https://www.thorlabs.com/thorproduct.cfm?partnumber=LN81S-FC`. Versión de agosto 2018.

[15] J. Casas, "Óptica",7ª edición. Zaragoza: Edición del Autor, (1994).

[16] JENOPTIK Optical Systems GmbH, "Integrated-optical modulators - Technical information and instructions for use". Dirección: `https://www.jenoptik.com/products/optoelectronic-systems/light-modulation/integrated-optical-modulators-fiber-coupled`. Versión de diciembre 2019.

[17] Tabor Electronics, "Wave Standard Series: Models WS8351/2", Dirección: `https://www.taborelec.com/ws8352`. Versión A (2021).

[18] Aurea Technology, "LYNXEA_NIR - Time Resolved Single Photon Detector [900 nm - 1700 nm]. Dirección: `https://www.aureatechnology.com/en/our-tcspc-photon-counters.html`. Versión 1.2 (2018).

[19] B. F. Aull, A. H. Loomis, D. J. Young et al., "Geiger-mode avalanche photodiodes for three dimensional imaging", Lincoln Laboratory Journal, (2002), págs. 335-350.

[20] A. W. Ziarkash, S. K. Joshi, M. Stipčević et al., "Comparative study of afterpulsing behavior and models in single photon counting avalanche photo diode detectors", Scientific Reports, (2018), **Vol. 8, nº 1**, artículo 5076.

[21] M. Newville, T. Stensitzki, D. B. Allen y A. Ingargiola. "LMFIT: Non-Linear Least-Square Minimization and Curve-Fitting for Python". Dirección: `https://zenodo.org/record/11813`. Versión 1.0.3 (2021).

[22] A. A. Abbott y C. S. Calude, "Von Neumann Normalisation of a Quantum Random Number Generator", Computability,**Vol. 1, nº 1**, (2012), págs. 59-83.

[23] L. E. Bassham, A. L. Rukhin, J. Soto et al., "A statistical test suite for random and pseudo-random number generators for cryptographic application", NIST Special Publication 800-22, (2010). Versión 1a.

[24] ID Quantique, "ID Quantique Technical Paper on Randomness Extractor", ID Quantique White Paper, (2012). Versión 1.0.