Universidad de Cantabria

Facultad de Ciencias

GENERACIÓN CUÁNTICA DE NÚMEROS ALEATORIOS BASADA EN LÁSERES DE SEMICONDUCTOR DE CAVIDAD VERTICAL

(Quantum generation of random numbers based on vertical-cavity surface-emitting lasers)

Trabajo de Fin de Grado
para acceder al

GRADO EN FÍSICA

Autor: Alfonso Lázaro del Pozo

Director: Ángel Alberto Valle Gutiérrez

Co-Director: Ana Quirce Teja

Junio - 2023

Resumen

En este trabajo se presenta un estudio experimental de la excitación aleatoria de los dos modos linealmente polarizados de un VCSEL cuya corriente aplicada es cambiada de forma periódica en el tiempo. Se demuestra que la probabilidad de excitación de un modo linealmente polarizado cambia significativamente con el valor de la amplitud de voltaje, la temperatura y el tiempo de muestreo. A partir de la elección adecuada de estos parámetros se identifican situaciones en las que las distribuciones de las señales polarizadas linealmente son aproximadamente uniformes. Se han considerado métodos de postprocesamiento con códigos BCH y de Von Neumann para reducir el sesgo de las secuencias de bits obtenidas y tratar de analizar gráficamente la aleatoriedad de los resultados, con el objetivo de determinar si este sistema es un buen candidato como generador cuántico de números aleatorios.

Palabras clave: Generador de números aleatorios, VCSEL, emisión espontánea, conmutación de polarización.

Abstract

This work presents an experimental study of the random excitation of the two linearly polarized modes of a VCSEL whose applied current is changed periodically in time. It is shown that the probability of excitation of a linearly polarized mode changes significantly with the value of voltage amplitude, temperature and sampling time. From the appropriate choice of these parameters, situations are identified in which the distributions of linearly polarized signals are approximately uniform. Post-processing methods with BCH and Von Neumann codes have been considered to reduce the bias of the obtained bit sequences and to try to analyze graphically the randomness of the results, with the aim of determining if this system is a good candidate as a quantum random number generator.

Key Words: Random number generator, VCSEL, spontaneous emission, polarization switching.

Agradecimientos

Quiero expresar mi más sincero agradecimiento a todas las personas que me han apoyado en la realización de este trabajo. A mis amigos, familiares, profesores y mi codirectora, Ana. En especial deseo agradecer a mi director, Ángel, por su orientación y dedicación a lo largo de todo el proceso, y a mi madre, Claudia, por ser la persona que más me apoya y ayuda en todos los aspectos de mi vida.

Índice

Capítulo 1
Motivación, objetivos y estructura del trabajo

En este capítulo introductorio se presenta una visión general del trabajo y se establecen los objetivos y la estructura del mismo. Además, se brinda una breve introducción a los conceptos clave que se abordarán en los capítulos siguientes.

La criptografía es un campo fascinante que ha desempeñado un papel crucial en la seguridad de la información a lo largo de la historia y continúa siendo muy relevante en la era digital actual. La criptografía es fundamental para garantizar la confidencialidad, integridad y autenticidad de la información. Comprender cómo funcionan los algoritmos criptográficos permite apreciar su importancia y entender cómo se aplican en la protección de datos en diversas áreas, como las comunicaciones, las transacciones financieras o la protección de la privacidad. La criptografía es una disciplina en constante evolución para poder hacer frente a los nuevos desafíos tecnológicos y las amenazas emergentes. Explorar las técnicas criptográficas modernas aporta una visión sobre cómo se abordan los problemas de seguridad en la actualidad. El desarrollo criptográfico, que puede sonar muy complejo y emplearse en situaciones muy específicas, está presente en muchos aspectos de nuestra vida cotidiana, mismamente en las contraseñas de redes sociales. Trabajar en un proyecto de esta índole es una oportunidad para adquirir ciertas nociones de programación, análisis de algoritmos y teoría de la información.

En criptografía, el concepto de aleatoriedad es fundamental, especialmente en la generación de claves criptográficas y en la resistencia a ataques de fuerza bruta. La aleatoriedad explora conceptos como distribuciones de probabilidad o procesos estocásticos, y este trabajo ayuda a lograr una cierta comprensión sobre cómo se aplican estos conceptos en el análisis de datos. En concreto, la generación de números aleatorios es un tema importante en la informática y simulación de sistemas. Leer y estudiar sobre los métodos y algoritmos para generar números aleatorios ayuda a entender cómo se construyen secuencias aparentemente aleatorias y cómo se pueden evaluar su calidad y propiedades estadísticas.

De los múltiples generadores de números aleatorios, este trabajo aborda la utilización de láseres de semiconductor. Estos dispositivos están siendo muy desarrollados en la actualidad y tienen una amplia gama de aplicaciones en diversos campos. En este caso, nos centramos en las comunicaciones ópticas. Al estudiar estos dispositivos, se comprende cómo funcionan en la transmisión de datos a alta velocidad a través de fibras ópticas, su papel en las redes de comunicación y su integración en sistemas de procesamiento de información.

En este trabajo se pretende evaluar la importancia de los números verdaderamente aleatorios en la criptografía, explorando también los principales algoritmos de encriptación, como la encriptación de almohadilla de un solo uso o la generación de los números pseudoaleatorios.

Por otra parte, se busca conocer la estructura general de un láser y comprender los procesos físicos principales en los que se basa el funcionamiento de los láseres de semiconductor, como la recombinación electrón-hueco y la unión p-n en materiales semiconductores. En concreto, se exploran la características y aplicaciones de un láser de emisión vertical (VCSEL). Una vez caracterizado el VCSEL, el experimento consiste en la adquisición de datos físicos y su conversión a bits, para analizar la aleatoriedad de los resultados obtenidos.

La estructura de la memoria es la siguiente: los capítulos 2 y 3 consisten en una breve introducción sobre criptografía y láseres de semiconductor, respectivamente. En el capítulo 2 se comenta la importancia de la criptografía, tanto históricamente como en la actualidad, y se mencionan los principales algoritmos de encriptación. El capítulo 3 presenta la estructura general de un láser y los principales fenómenos físicos básicos para el funcionamiento de los láseres de semiconductor.

En el capítulo 4 se explica la configuración experimental con la que se ha trabajado y una pequeña descripción de los instrumentos involucrados. El capítulo 5 incluye la caracterización del láser empleado.

En el capítulo 6 se analizan los resultados experimentales obtenidos en crudo, buscando la mejor elección de parámetros de amplitud de señal V_{on}, temperatura y tiempo de muestreo t_s, para obtener una secuencia binaria lo más aleatoria posible. Por su parte, en el capítulo 7 se han plasmado de diferentes maneras secuencias de bits postprocesados para intentar analizar visualmente su aleatoriedad.

Finalmente, en el capítulo 8 se discuten e intentan sacar conclusiones sobre los resultados mostrados en los capítulos 6 y 7.

Capítulo 2
Introducción a la criptografía

El origen de la criptografía se remonta a miles de años, desde que el ser humano comenzó a comunicarse a través de mensajes escritos. Desde entonces, se han utilizado diferentes técnicas y algoritmos para proteger la privacidad y el contenido de la información [1].

Uno de los primeros ejemplos de criptografía se puede encontrar en la Antigua Grecia, donde Heródoto relata en su obra *Historias* (libro V) que el general Histieo tatuó la cabeza de un esclavo para enviar a los griegos un mensaje que solo podía leerse al rapar al esclavo. Otro ejemplo temprano empleado desde el Imperio Romano es el Cifrado César, que consistía en desplazar cada letra del alfabeto un número determinado de posiciones. En el caso de la posición 3, la letra A se convertiría en una D, la B en una E, y así sucesivamente.

A lo largo de la historia, se han desarrollado múltiples técnicas y algoritmos criptográficos, desde el cifrado de sustitución simple hasta los complejos algoritmos asimétricos utilizados en la actualidad. Durante la Segunda Guerra Mundial, la criptografía desempeñó un papel crucial en la victoria de los aliados, gracias al trabajo de matemáticos, entre los que destacan Alan Turing y Joan Clarke, que lograron descifrar los códigos diseñados por las fuerzas del Eje.

Actualmente, la criptografía se usa en muchos ámbitos diferentes, desde la banca y las finanzas hasta la comunicación por Internet y el almacenamiento de datos. La evolución de esta disciplina ha sido impulsada por el avance de la tecnología y la necesidad de proteger la información en un mundo cada vez más digitalizado.

2.1. Principales algoritmos de encriptación

Fundamentalmente, la criptografía persigue la confidencialidad, integridad y autenticidad del mensaje. Para ello, se puede codificar y descodificar un mensaje mediante una clave privada, empleando la denominada criptografía simétrica. Este método es rápido y eficiente, pero requiere que el emisor y el receptor compartan la misma clave.

Un algoritmo de cifrado simétrico, ampliamente usado hoy en día para la protección de información sensible, desde médica hasta gubernamental, es el AES (Advanced Encryption Standard), desarrollado por los criptógrafos belgas Joan Daemen y Vincent Rijmen en 1998. El tamaño de la clave puede variar entre 128, 192 y 256 bits, lo que la hace muy segura y difícil de descifrar mediante ataques de fuerza bruta. Este algoritmo opera sobre bloques de datos de 128 bits y, a través de un proceso de sustitución-permutación iterativo, genera la salida cifrada [1].

Es posible usar dos claves diferentes, una pública para cifrar la información y que puede ser compartida sin comprometer la seguridad de los datos, y otra privada para descifrar

el contenido y que solo la posee el receptor. Este método de clave asimétrica es más seguro, pero también más lento.

Un ejemplo de algoritmo de cifrado asimétrico es el RSA, creado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman. Este algoritmo se fundamenta en dos conceptos matemáticos: en la idea de que es fácil multiplicar dos números primos enormes pero muy difícil factorizar el producto resultante en sus factores primos originales y en la función aritmética mod, cuyo resultado es el resto obtenido al realizar una división, obviando el cociente [2].

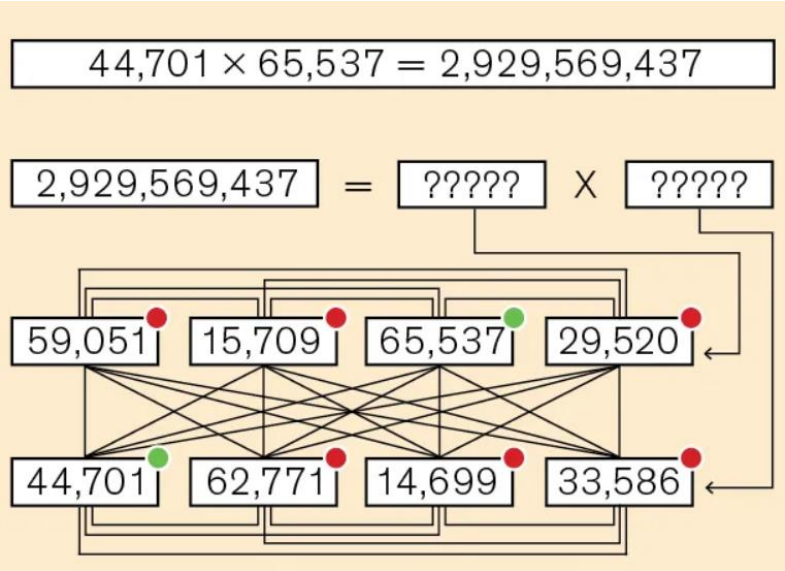

Figura 2.1: Cualquier ordenador puede multiplicar dos números primos grandes rápidamente, pero el proceso inverso de tomar el resultado y probar todas las opciones posibles hasta hallar los factores iniciales es muy lento [3].

Para generar las claves, se seleccionan dos números primos grandes, P y Q, y se calcula su producto $\mathrm{K} = \mathrm{PQ}$. A continuación, se escoge un número primo pequeño, E, que no sea divisor de $(\mathrm{P}-1)(\mathrm{Q}-1)$, y se calcula su inverso modular D [2]. A la hora de cifrar un mensaje, el remitente lo convierte en un número entero M y aplica la función de cifrado $\mathrm{C} = \mathrm{M}^{\mathrm{E}}\mathrm{mod}\mathrm{K}$, utilizando la clave pública (K, E). El destinatario recibe el mensaje cifrado y lo decodifica empleando la función $\mathrm{M} = \mathrm{C}^{\mathrm{D}}\mathrm{mod}\mathrm{K}$, mediante su clave privada (D). Para escoger cada número P y Q, se necesita generar un número aletaorio de un determinado tamaño que, en caso de no ser primo, se le sumará una cierta cantidad para que pase las pruebas de primalidad.

Cuanto mayor sea la longitud de la clave, mayor será la seguridad del algoritmo, aunque también aumentará el tiempo necesario para realizar las operaciones criptográficas. RSA es muy habitual en la protección de transacciones financieras y en la protección de la privacidad de las comunicaciones.

Aunque en la presente era digital que vivimos la criptografía es una herramienta esencial para garantizar la seguridad de la información, todavía presenta limitaciones que hacen vulnerable su protección. Hay que tener en cuenta que la criptografía avanzada es una disciplina muy compleja que requiere de un conocimiento especializado para su implementación y que resulta muy costoso desarrollarla correctamente. Además, se trata de un proceso computacionalmente intensivo en el que puede que se aumente el

tamaño de los datos cifrados, afectando a sistemas con limitaciones de almacenamiento o ancho de banda.

Por desgracia, los ataques informáticos son muy comunes y, pese a que los algoritmos criptográficos son matemáticamente seguros, las claves utilizadas para cifrar y descifrar la información pueden ser vulneradas mediante técnicas de fuerza bruta, ataques de diccionario o ataques de phishing.

2.2. Encriptación de almohadilla de un solo uso y números pseudoaleatorios

Factores como la longitud, el período de uso y la aleatoriedad de una clave influyen considerablemente en el grado de seguridad de esta. A mayor número de caracteres que compongan una clave, crecerá exponencialmente el número de combinaciones posibles que habría que probar para descifrar la información mediante un ataque de fuerza bruta. Así mismo, las claves se vuelven más inseguras con el tiempo y es importante renovarlas regularmente. Por último, la aleatoriedad se refiere a la complejidad de la clave en sí misma, de manera que esté constituida por todo tipo de caracteres, ya sean letras, números, símbolos ortográficos… y evitar así que sea forzada por ataques de diccionario.

En 1882, Frank Miller, un banquero de Sacramento, desarrolló un método de cifrado absolutamente indescifrable, la encriptación de almohadilla de un solo uso, que proponía desplazar cada letra del mensaje un número aleatorio de veces y, sin dicha secuencia, no se podría leer el contenido. Por ejemplo, para codificar el mensaje GATO, la letra G podría moverse tres posiciones, de manera que se convertiría en una J, la A pasaría a ser una B al variar una posición, la T sería una V si se desplaza dos lugares y la O se transformaría en una S al llevarla cuatro posiciones hacia adelante. De esta forma, el mensaje encriptado sería JBVS y la cadena de números aleatorios 3-1-2-4 sería la clave necesaria para desencriptar dicho mensaje. Para ser realmente efectiva, la clave codificaría un único mensaje y se eliminaría [3].

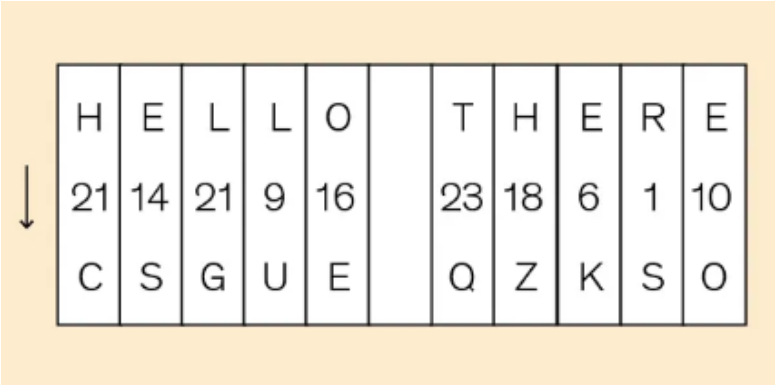

Figura 2.2: Encriptación de almohadilla de un solo uso [3].

Este método, aunque es empleado para el intercambio de información crucial, como puede ser entre gobiernos, presenta el problema de que la longitud de la clave es igual a la del mensaje, lo que lo hace poco operativo. Además, la producción de números aleatorios resulta muy complicada y, por ello, es muy habitual en criptografía el desarrollo de algoritmos deterministas para generar números pseudoaleatorios. Aunque estos números se comportan de manera similar a los aleatorios y resultan muy útiles

para la codificación de información, hay que tener en cuenta que no cumplen verdaderamente la propiedad de aleatoriedad y que pueden llegar a ser predecibles si se conoce el algoritmo subyacente.

Estos algoritmos toman una semilla como valor inicial, que determina completamente la serie de números generada. Por tanto, si se parte de una misma semilla, la secuencia de números será la misma. Normalmente, los generadores de números pseudoaleatorios se basan en la teoría de números. Por ejemplo, Lehmer implementó un algoritmo que, mediante una fórmula recursiva, genera una secuencia de números que parecen aleatorios:

$$X_{n+1} = (aX_n + b) \ \ mod m; \quad n \geq 0$$

Donde X_0 es la semilla, X_n es el número generado en el paso n y a $(0 \leq a < m)$, b $(0 \leq b < m)$ y m $(m > 0)$ son el factor multiplicativo, aditivo y módulo, respectivamente. Los números de salida son muy sensibles a estos parámetros, que deben elegirse apropiadamente, y son periódicos, aunque el período es tan grande que pueden ser una buena aproximación a números aleatorios [4].

2.3. Números verdaderamente aleatorios

Una manera de generar números verdaderamente aleatorios es midiendo procesos físicos, como el número de veces que sale cara al tirar una moneda. Al no basarse en un algoritmo, estos números no pueden predecirse o reproducirse, lo que los hace más seguros que los números pseudoaleatorios.

A grandes rasgos, los generadores de números verdaderamente aleatorios se pueden clasificar en los siguientes grupos [5]:

1. Basados en ruido: generan números aleatorios midiendo una fuente de ruido físico. Un ejemplo es el ruido atmosférico, que tiene lugar debido a interferencias electromagnéticas, y que se puede capturar mediante un receptor de radio ajustado a una frecuencia que no transmite ninguna señal, eliminando cualquier otra fuente de ruido. También se pueden usar generadores de ruido térmico, que se basan en las fluctuaciones de velocidad y dirección de los electrones al moverse en un conductor. Se suele emplear un diodo como elemento activo, debido a su alta resistencia eléctrica y su sensibilidad a las fluctuaciones de temperatura. Estos generadores suelen ser poco eficientes, ya que es necesario capturar y procesar una gran cantidad de datos.

2. Basados en caos: se aprovechan del comportamiento impredecible de sistemas caóticos, muy susceptibles a pequeños cambios en las condiciones iniciales. Un enfoque frecuente para construir números aleatorios es utilizar un mapa caótico, que se trata de una función matemática que genera una secuencia de números a partir de la dinámica caótica del sistema. Con este método se puede producir una gran cantidad de números rápidamente, pero pueden predecirse si se conocen las condiciones de partida.

3. Oscilador de funcionamiento libre: se trata de un circuito electrónico que genera una oscilación continua de alta frecuencia sin ninguna entrada ni control externo. Para generar números aleatorios, la salida del oscilador se muestra a intervalos regulares y se mide la fluctuación de tiempo; es decir, pequeñas variaciones en el período del oscilador. Estos tipos de generadores son relativamente sencillos de implementar y solo requieren unos pocos componentes. Sin embargo, son muy sensibles a factores ambientales como la temperatura, las interferencias electromagnéticas y el ruido de la fuente de alimentación, que degradan la calidad de los números aleatorios.

4. Cuánticos: se basan en una amplia gama de fenómenos cuánticos, como la emisión de fotones por un láser, la transmisión de fotones a través de fibras ópticas o la detección de fotones individuales mediante fotodetectores. Las partículas subatómicas se comportan imprevisiblemente y, aunque no cualquier resultado es posible, no se puede predecir cuál de los plausibles va a ocurrir. Estos procesos cuánticos generan fluctuaciones aleatorias en la señal, que se pueden medir y convertir en una secuencia de números aleatorios. De esta manera, los números producidos no son predecibles, incluso si se conoce todo el proceso de generación de estos. Pero también tienen sus desventajas, pues todo el desarrollo que conllevan es muy lento y costoso, debido a la complejidad de los dispositivos cuánticos necesarios.

A pesar de sus limitaciones y complejo desarrollo, los números aleatorios son necesarios en todos los métodos criptográficos para garantizar la seguridad de la información. El generador que analizamos en este trabajo está basado en la aleatoriedad de los fotones de emisión espontánea que inducen la generación de pulsos ópticos en un láser de semiconductor cuya corriente es modulada periódicamente en el tiempo. La explicación del fenómeno de la emisión espontánea de un fotón durante el decaimiento de un átomo excitado requiere de la cuantización del campo electromagnético. Los sucesos de emisión espontánea están estimulados por las fluctuaciones del campo eléctrico del vacío cuántico. La emisión espontánea puede entenderse como fluctuaciones del vacío amplificadas y, por tanto, se puede considerar ruido cuántico.

Capítulo 3
Introducción a los láseres de semiconductor

3.1. Estructura general de un láser

Un láser (Light Amplification by Stimulated Emission of Radiation) es un dispositivo que produce luz coherente y de alta intensidad. En general, cualquier láser consiste en un medio activo, material responsable de la emisión estimulada de radiación, y un resonador óptico, que encierra al medio activo mediante dos espejos paralelos, uno totalmente reflectante y otro parcialmente reflectante, y amplifica la luz emitida por este. A través del espejo parcialmente reflectante se forma el haz de salida del láser [6].

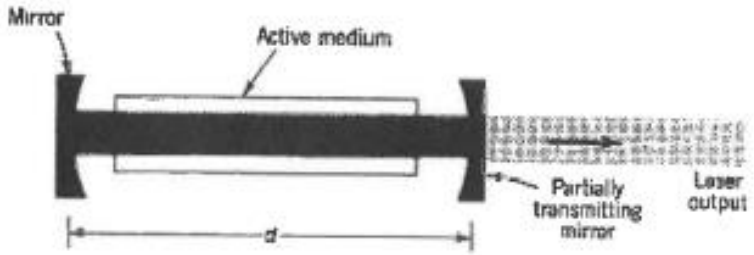

Figura 3.1: Estructura general de un láser.

Para que el medio activo pueda emitir fotones y generar luz láser necesita una fuente externa de energía que excite sus átomos, elevando su energía a un nivel superior. Cuando estos átomos regresan a su estado original, emiten fotones que, a su vez, estimulan a otros átomos a emitir más fotones, lo que produce una cascada de emisiones de luz. El mecanismo de bombeo que suministra la energía depende del tipo de medio activo. Por ejemplo, en los láseres de diodo, la fuente de energía es una corriente eléctrica que pasa a través de un material semiconductor, mientras que, en los láseres de gas el bombeo de energía puede ser una descarga eléctrica que ioniza el gas y lo excita [7].

El resonador permite crear una retroalimentación óptica que amplifica y mantiene la emisión de luz coherente y monocromática. Cuando los fotones son emitidos por el medio activo, algunos de ellos se reflejan en los espejos y regresan. Estos fotones estimulan la emisión de fotones adicionales, aumentando la intensidad de la luz del láser en cada ciclo. La distancia entre los espejos determina la longitud del resonador y, por tanto, la longitud de onda del haz láser [7].

Los láseres tienen una amplia gama de aplicaciones como la cirugía ocular, tratamientos dermatológicos, soldadura de materiales, comunicaciones por fibra óptica para transmitir la información de manera más rápida… [8]

3.2. Recombinación electrón-hueco en semiconductores

En general, los materiales semiconductores tienen enlaces muy covalentes, con gran solapamiento entre orbitales, lo que hace que el gap entre la banda de valencia y la de conducción sea pequeño ($\sim 0.1 - 3$ eV) al ser estas muy anchas. A $\mathrm{T} = 0$ K la banda de valencia está llena y la de conducción vacía, por lo que se comportan como aislantes. Al aumentar la temperatura presentan conductividad que crece exponencialmente con T, debido a los saltos de electrones desde la banda de valencia a la de conducción, dejando huecos en la primera, de manera que ambos tipos de portadores de carga (electrones y huecos) suman sus efectos a la conductividad [9].

Al excitar electrones desde la banda de valencia a la banda de conducción por aumento de temperatura o por absorción de un fotón, se forman pares electrón-hueco. La recombinación de un electrón con un hueco es el principal mecanismo de desexcitación de electrones desde la banda de conducción a la de valencia.

Esta recombinación puede ser no radiativa (sin emitir fotón). Es el mecanismo más probable, donde los electrones de la banda de conducción son atrapados por impurezas cargadas positivamente. El electrón atrapado va bajando su energía liberando energía térmica al entorno, hasta llegar a la banda de valencia [9].

Cuando el material se somete a un campo eléctrico o es iluminado y los electrones se excitan, la recombinación radiativa se produce al desexcitarse el electrón emitiendo un fotón. Este tipo de recombinación puede ocurrir en los procesos de emisión espontánea o emisión estimulada. En la primera, el electrón y el hueco se combinan sin la ayuda de otro fotón y es el proceso según el que operan los LED, mientras que la emisión estimulada se sirve de un fotón externo para la emisión de un segundo fotón idéntico. Ambos fotones pueden interaccionar nuevamente con otros electrones excitados, llevando a cabo una amplificación de la radiación inicial [9].

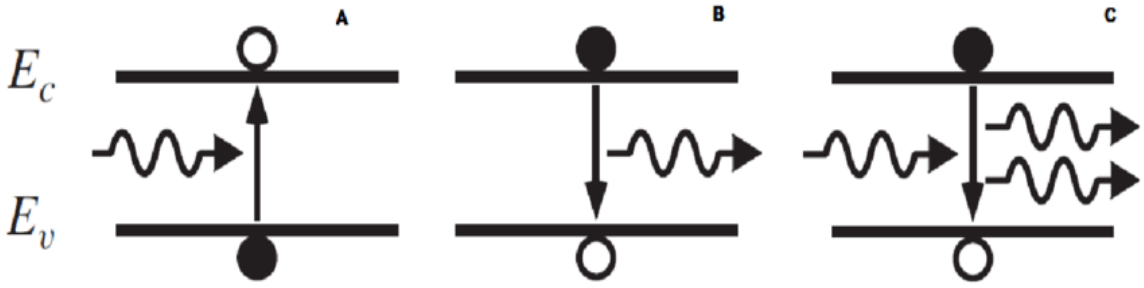

Figura 3.2: Absorción de un fotón para generar el par electrón-hueco (A). Recombinación del par electrón-hueco por emisión espontánea de un fotón (B). Recombinación del par electrón-hueco estimulada por un fotón, que induce la emisión de otro fotón idéntico (C).

3.3. Unión p-n en láseres de semiconductor

La recombinación electrón-hueco por emisión estimulada es la base del funcionamiento de los láseres de semiconductor, en los que una corriente eléctrica o un haz de fotones excita una estructura de semiconductor, produciendo una emisión de luz coherente y monocromática.

En los láseres de semiconductor, el medio activo es un material semiconductor dopado con impurezas para crear una unión p-n (unión entre una región con exceso de

electrones y otra con deficiencia de ellos). La mayoría de estos láseres se basan en el arseniuro de galio (GaAs) dopado con impurezas de aluminio o de indio [7].

Consideremos un semiconductor con una parte p dopada con una concentración N_a de impurezas aceptoras, que son aquellas que tienen valencia menor que los átomos a los que sustituyen en el cristal, y la otra parte n dopada con una concentración N_d de impurezas dadoras, que son aquellas que tienen valencia mayor que los átomos del cristal a los que reemplazan. En la región de trabajo todas las impurezas están ionizadas, de manera que tenemos concentraciones de aceptores ionizados negativamente N_a^- en la parte p y de dadores ionizados positivamente N_d^+ en la parte n [9].

Consideremos primero que las dos partes no están en contacto. En la zona p hay mayoría de huecos en la banda de valencia e impurezas aceptoras fijas cargadas negativamente, mientras que en la parte n hay mayoría de electrones en la banda de conducción e impurezas dadoras fijas cargadas positivamente.

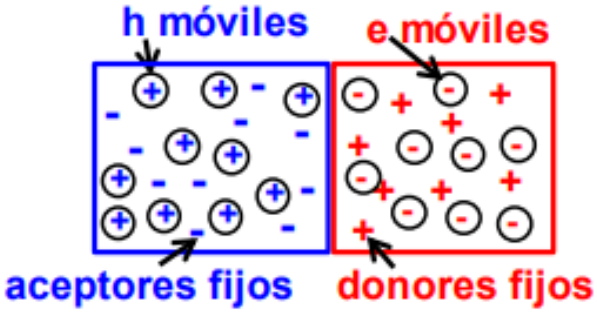

Figura 3.3: Zonas p (recuadro azul) y n (recuadro rojo) sin entrar en contacto [9].

Estudiamos ahora el preciso instante en que unimos las partes p y n. Aunque cada zona es eléctricamente neutra, el continuo movimiento de los portadores móviles provoca que en la parte p de la zona de unión abrupta haya un pequeño predominio de carga negativa fija, mientras que en el lado n haya un pequeño predominio de la carga positiva fija. Estas cargas fijas dan lugar a una estrecha región de transición con un minúsculo campo eléctrico de derecha a izquierda, que desplaza los electrones de esa zona hacia la derecha y a los huecos hacia la izquierda, lo que incrementa el tamaño de la región de transición y de su campo eléctrico hasta llegar a una situación de equilibrio, donde el campo de transición vale típicamente $E \sim 10^5\ V/cm$ [9].

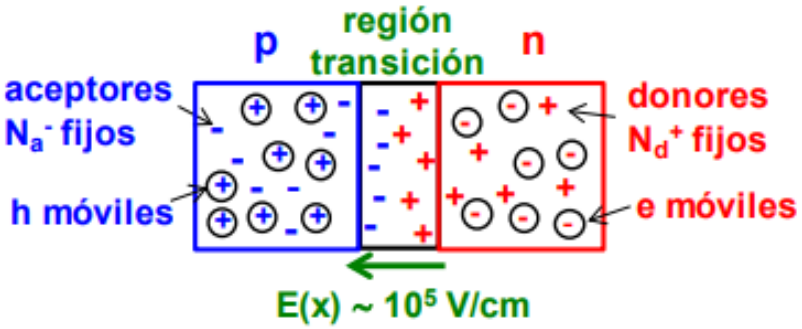

Figura 3.4: Formación de la región de transición y el campo de transición al unir las partes p y n [9].

Al aplicar un potencial externo $V > 0$ se tiene una polarización directa, que reduce la barrera en la región de transición debido a que el campo E se ve reducido ligeramente por el pequeño campo eléctrico de la batería. Esta reducción de la barrera hace que la difusión de electrones y huecos aumente exponencialmente, favoreciendo su recombinación por medio de la emisión estimulada [7].

Los láseres de semiconductor están formados por capas de materiales de semiconductor. Entre esas capas se puede formar una o varias uniones p-n. Esta configuración se conoce como heteroestructura, utilizada para crear una región activa en la que se produce la emisión de luz. Esta región se compone de una capa delgada con un gap estrecho que se encuentra entre dos capas con un gap más ancho. Esta heteroestructura confina los portadores de carga en la región activa. Además, cuanto menor es el ancho del gap, mayor es el índice de refracción del material, de manera que la luz también se confina en dicha región por reflexión interna total.

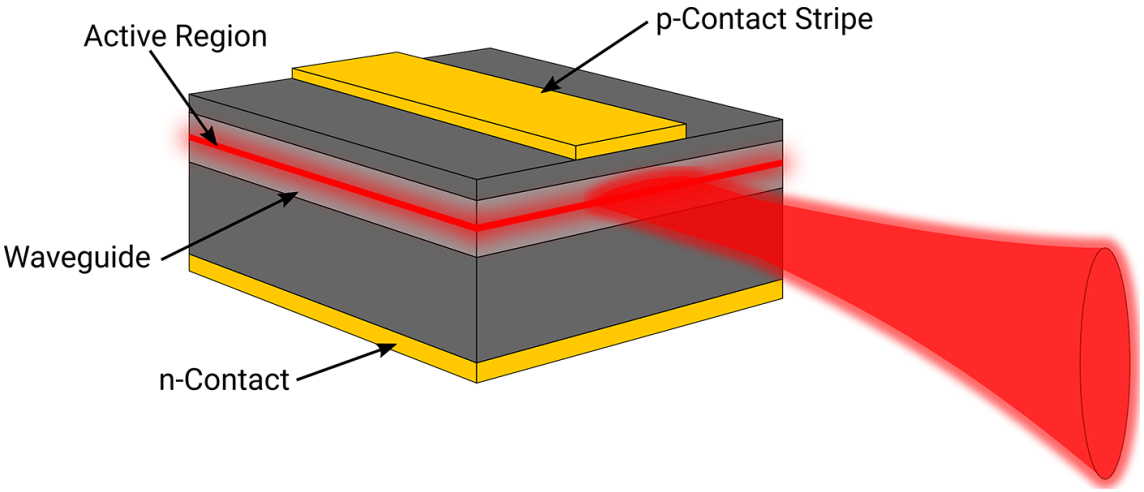

Figura 3.5: Esquema general de un láser de emisión lateral.

Dependiendo de la dirección del haz de luz respecto a la región activa, se pueden distinguir dos tipos principales de láseres de semiconductor: láseres de emisión lateral, en los que la dirección del rayo es paralela al plano de la región activa, y de emisión vertical, en los que la dirección es perpendicular. Este último tipo ha sido con el que se ha desarrollado este trabajo.

3.4. Láseres de emisión vertical (VCSEL)

Los láseres de semiconductor de cavidad vertical se caracterizan porque la dirección del haz de luz es perpendicular al plano de la región activa. Estos dispositivos suelen emitir luz polarizada linealmente a lo largo de una de las direcciones del cristal en el plano del medio activo. En algunos de estos láseres la polarización puede cambiar $90°$ al cambiar la corriente aplicada al dispositivo. La siguiente figura muestra la estructura típica de un VCSEL.

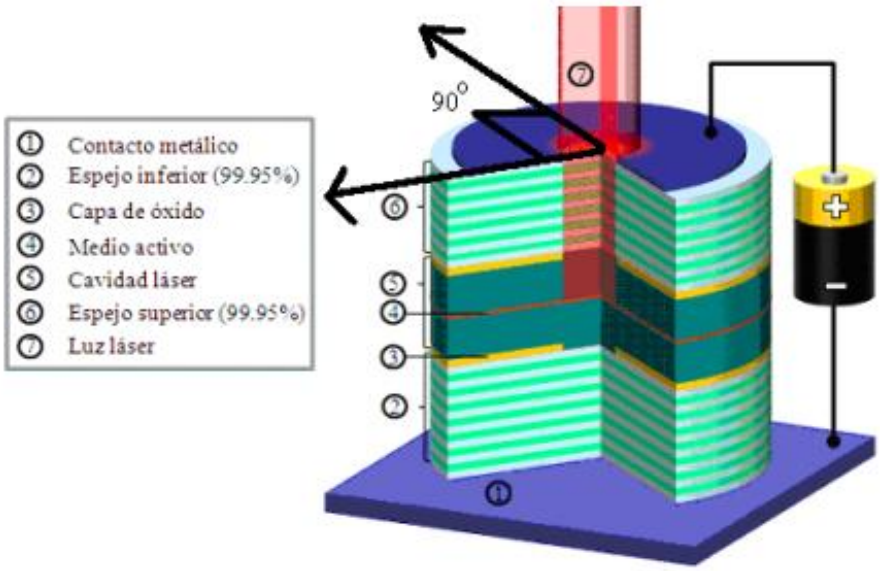

Figura 3.6: Esquema general de un VCSEL.

En un VCSEL, la longitud de la cavidad óptica es muy pequeña (del orden de unas pocas longitudes de onda) para que el láser opere en un único modo longitudinal. La cavidad óptica está delimitada por dos espejos de alta reflectividad, conocidos como reflectores de Bragg distribuidos (DBR). La reflectividad de estos espejos es superior al 99%, lo que reduce notablemente las pérdidas dentro del medio activo permitiendo una emisión láser muy eficiente [10].

Los VCSEL tienen varias ventajas sobre los láseres convencionales de emisión lateral, incluyendo una emisión de luz más eficiente, una mayor estabilidad y uniformidad de emisión, y un menor costo de fabricación. Además, los VCSEL son ideales para su uso en aplicaciones de comunicaciones ópticas, ya que su emisión de luz vertical permite un acoplamiento óptico en fibra óptica más fácil y tienen una alta densidad de empaquetado, requieren una corriente de operación umbral baja y consumen una cantidad de energía relativamente pequeña [11].

Comúnmente, la luz emitida por un VCSEL se polariza linealmente a lo largo de una de dos componentes ortogonales, y la conmutación o “switching” de polarización (PS) entre los dos modos polarizados linealmente se observa a menudo cuando se cambian la corriente o la temperatura. Por ejemplo, aumentando la corriente a una temperatura constante se produce este fenómeno de “switching” entre las dos componentes linealmente polarizadas, que se trata de un giro de $90°$ en la dirección de de la polarización del haz [12].

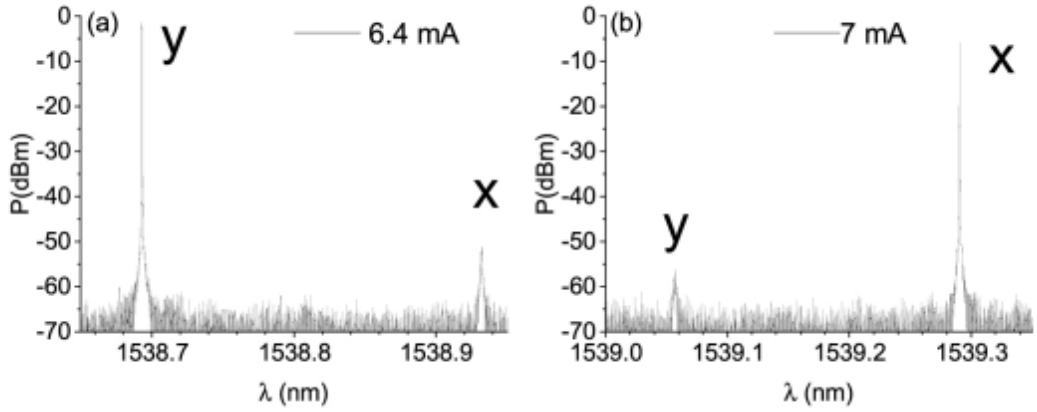

Figura 3.7: Espectro óptico antes y después del switching para temperatura constante de $25℃$. Corriente de 6.4 mA (a) y 7 mA (b) [13].

Este fenómeno de conmutación de la polarización ocurre al incrementar la corriente en un VCSEL, lo que produce un aumento de la temperatura en el interior del dispositivo debido al efecto Joule, causado por la corriente que fluye a través de los espejos, que tienen una resistencia eléctrica apreciable. Este aumento de temperatura provoca un cambio en el espectro de ganancia del material de semiconductor hacia longitudes de onda más largas. La longitud de onda de la luz emitida en un VCSEL está determinada por la cavidad de resonancia del láser y no por el espectro de ganancia. Como resultado, el espectro de ganancia se va desplazando de manera que, mientras la corriente es pequeña, el modo de polarización con menor longitud de onda (Y en la Figura 3.7) tiene una ganancia mayor que el modo polarización con longitud de onda más larga (X en la Figura 3.7). Para corrientes más altas, el predominio de la ganancia se invierte [6].

El cambio de la curva de ganancia con la corriente está ilustrado en la Figura 3.8, donde λ_S y λ_L son las longitudes de onda correspondientes a las polarizaciones Y y X, respectivamente. La longitud de onda de ambas polarizaciones aumenta también a medida que aumenta la corriente (ver Figura 3.7). Este incremento es mucho menor que el corrimiento de la curva de ganancia. La longitud de onda crece porque al aumentar la corriente, y debido a la resistencia eléctrica de los espejos por el efecto Joule, incrementa la temperatura en el interior del láser, lo cual lleva a un aumento en el índice de refracción, situación típica en los semiconductores. La longitud de onda crece según la condición de resonancia $\lambda = \frac{2nL}{q}$, donde L es la separación entre espejos, q es un número natural y n es el índice de refracción. Las longitudes de onda λ_S y λ_L son distintas debido a que el material del VCSEL es birrefringente; es decir, que tiene distinto índice de refracción para las dos polarizaciones ($n_s \neq n_L$).

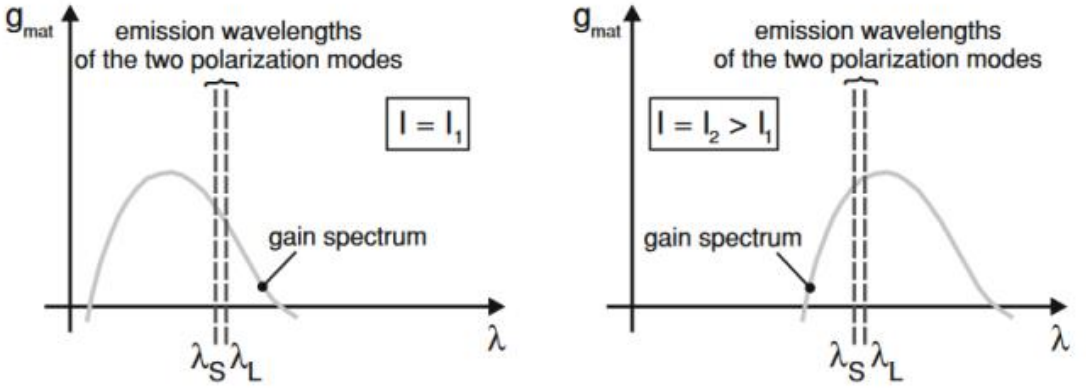

Figura 3.8: Para una corriente I_1, el modo de polarización con longitud de onda más corta (λ_S) tiene una ganancia mayor que el modo con longitud más larga (λ_L). Para una corriente $I_2 > I_1$, el espectro de ganancia se ha corrido de manera que ahora predomina el modo con mayor longitud de onda [14].

Capítulo 4
Montaje experimental y descripción del equipo

En la Figura 4.1 se muestra el montaje experimental dispuesto para la generación de números aleatorios, basada en pulsos ópticos generados mediante la conmutación de ganancia de un VCSEL. Este láser está conectado a un controlador de temperatura, que permite regular la temperatura del entorno. La corriente aplicada al láser está dada por la superposición de dos señales eléctricas: una corriente de polarización (I_{off}), suministrada por una fuente de corriente, y una señal cuadrada, proporcionada por un generador de patrones de pulsos. Para minimizar los efectos de retroalimentación en el VCSEL, se acopla un aislante óptico. Asimismo, se emplea un controlador de polarización y un divisor de haz polarizado para separar los dos modos de polarización lineal del VCSEL. Las señales ópticas correspondientes a cada uno de estos dos modos de polarización son transformadas al dominio eléctrico a través de dos fotodetectores. Una vez convertidas, dichas señales se registraron en tiempo real en un osciloscopio para obtener los perfiles temporales de los pulsos ópticos correspondientes a cada una de las polarizaciones lineales. Además, se caracterizó el espectro óptico mediante un analizador de espectros ópticos de alta resolución y se obtuvo la potencia óptica de cada polarización usando medidores de potencia óptica [13].

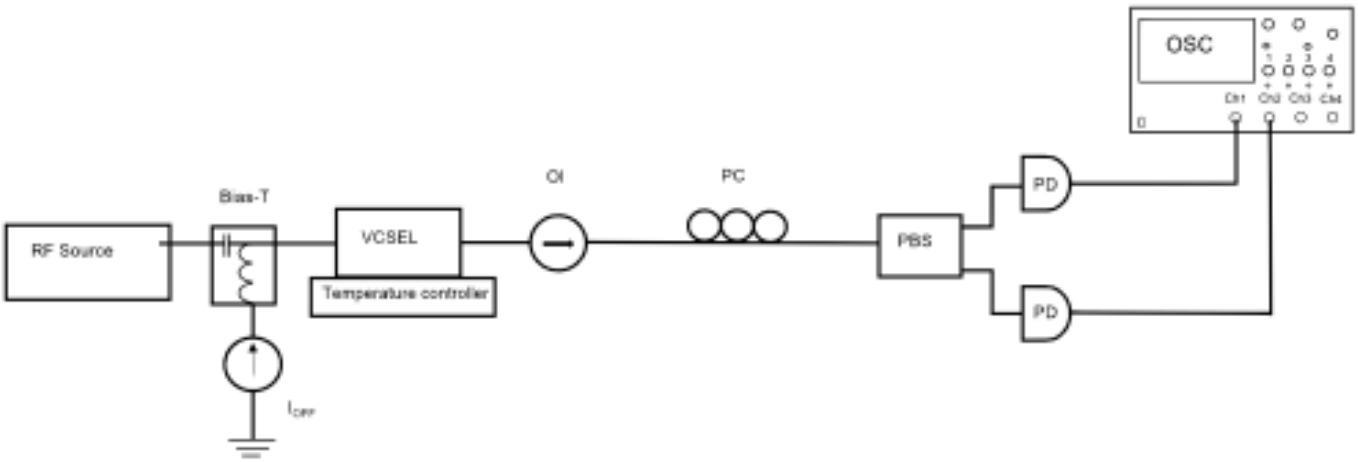

Figura 4.1: Configuración experimental. OI: aislante óptico, PC: controlador de polarización, PBS: divisor de haz polarizado, PD: fotodetectores, OSC: osciloscopio. Todos los elementos ópticos están conectados mediante fibras ópticas.

Seguidamente, se ofrece una breve explicación sobre cada instrumento que conforma el montaje de la Figura 4.1:

- **VCSEL:** A lo largo del experimento, se ha empleado un láser comercial de RayCan monomodo diseñado para comunicaciones de alta velocidad, basado en una región activa de InAlGaAs y que emite a una longitud de onda de aproximadamente $\lambda = 1550$ nm. Este dispositivo ofrece velocidades de datos de

hasta 4 Gbps y es apropiado para redes de acceso de corta distancia (< 2 km) y redes de área metropolitana, así como Gigabit Ethernet. El VCSEL está colocado en una montura láser Thorlabs LDM56M que incluye una bias-T capaz de modular la radiofrecuencia de la corriente láser hasta un máximo de 600 MHz.

- **Controlador de temperatura:** Se trata de un controlador de temperatura termoeléctrico Thorlabs TED200C, muy adecuado para diodos láser y detectores. La resolución del aparato es de 0.01 ℃ y tiene una estabilidad de temperatura ≤ 0.002 ℃.

- **Fuente de corriente:** La corriente de polarización es suministrada por una fuente Thorlabs LDC200C, que funciona con todas las polaridades de diodo láser y fotodiodo. Esta fuente tiene un rango de 0 a 20 mA, con una resolución de 1 μA.

- **Generador de patrones:** La señal cuadrada es producida por un generador de patrones de pulsos Anritsu MU181020A, que puede funcionar hasta una velocidad de datos de 12.5 Gbps.

- **Conectores de fibra:** Los diferentes instrumentos se han acoplado mediante conectores de fibra óptica FC/APC, que tienen un diámetro de 2.5 mm.

- **Aislante óptico:** Es un dispositivo que permite que la luz pase en una sola dirección mientras que bloquea el paso en la dirección opuesta. Un aislante óptico típicamente consta de un polarizador, un material que cambia la polarización de la luz, y otro polarizador. La luz que llega al primer polarizador está polarizada en una dirección particular, y luego pasa a través del material de cambio de polarización. Si la luz ha cambiado su polarización en la dirección adecuada, puede pasar a través del segundo polarizador, que bloqueará el paso de la luz polarizada en la dirección opuesta.

- **Controlador de polarización:** Se ha empleado un controlador Thorlabs FBR05, que consta de tres láminas retardadoras: una $\lambda/2$ entre dos $\lambda/4$. Estas placas se pueden girar de tal forma que siempre es posible encontrar una posición que transforme culaquier estado de polarización de entrada en cualquier estado de polarización de salida.

- **Divisor de haz polarizado:** Se ha utilizado un combinador/divisor Newport F-PBC-15-SM-FA, capaz tanto de combinar la luz de dos fibras de entrada en una única fibra de salida, como de separar las componentes de polarización ortogonales de una señal de entrada entre dos fibras de salida. Este dispositivo opera a una longitud de onda central de 1550 nm y tiene una pérdida máxima por inserción de 0.6 dB.

- **Fotodiodos:** Para convertir la señal óptica en eléctrica, se han usado dos fotodetectores rápidos Thorlabs PDA8GS con 9 GHz de ancho de banda. Estos fotodiodos operan en un rango de longitud de onda de $750 - 1650$ nm con una respuesta de pico de 0.95 A/W a los 1550 nm.

- **Osciloscopio:** Las trazas temporales de las señales provenientes de los fotodetectores se registraron en tiempo real en un osciloscopio con un ancho de banda de $13\ \mathrm{GHz}$ y una frecuencia de muestreo de $20\ \mathrm{GSa/s}$.

- **Analizador de espectro óptico de alta resolución:** Se ha empleado el Aragon Photonics BOSA 210, con una resolución óptica de $10\ \mathrm{MHz}$ y una precisión de longitud de onda de $\pm 0.5\ \mathrm{pm}$.

Capítulo 5
Caracterización del VCSEL

Como ya se ha mencionado, el VCSEL empleado opera en un único modo longitudinal y transversal en todo el rango de corriente. Para caracterizar el dispositivo, se ha fijado el controlador de temperatura a 22 ℃ y se ha medido la potencia en función de la intensidad de corriente. Los resultados se muestran en la Figura 5.1. Usando estos datos se puede determinar la corriente umbral, a partir de la cual la emisión estimulada empieza a dominar a la espontánea.

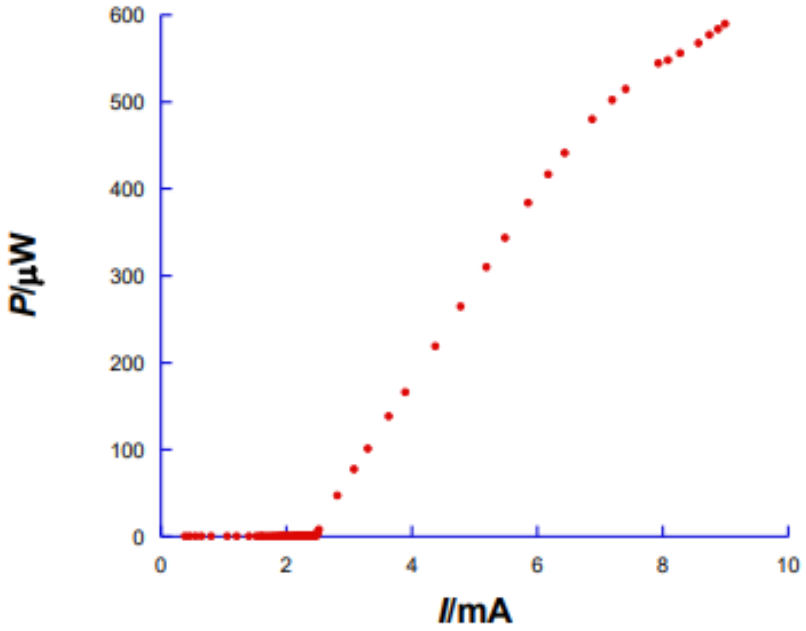

Figura 5.1: Curva luz-corriente a 22 ℃.

Por ello, se han tomado los puntos con potencia apreciable que mejor se ajustan a una recta. En la ecuación de la recta obtenida en la Figura 5.2, la corriente umbral se obtiene cuando la potencia es nula.

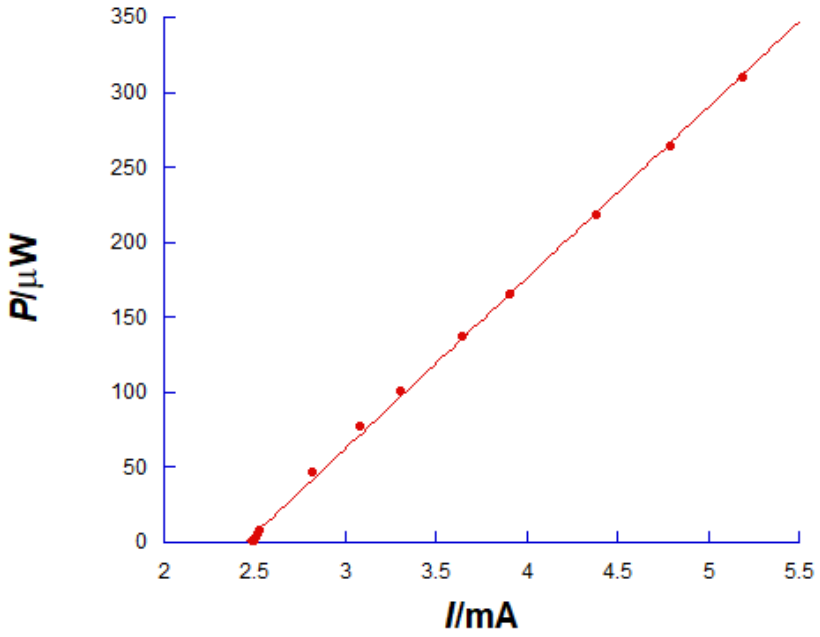

Figura 5.2: Puntos experimentales de la Figura 4.1 que mejor se ajustan a una recta. La ecuación obtenida es: $P = (113.8 \pm 0.9) \cdot I - (279 \pm 3)$.

A partir de esta ecuación, la corriente umbral obtenida es $I_{th} = 2.45 \pm 0.05$ mA. Para todas las medidas posteriores, es conveniente que la corriente de polarización I_{off} (la dada por el controlador de corriente) se encuentre ligeramente por debajo de la umbral, de manera que se ha escogido $I_{off} = 0.92 I_{th} = 2.25 \pm 0.05$ mA.

La potencia del láser y la corriente umbral se relacionan con la eficiencia cuántica diferencial (η) mediante la siguiente expresión: $P = \eta \frac{hc}{e\lambda}(I - I_{th})$, donde h es la constante de Planck, c es la velocidad de la luz y e es la carga del electrón. La eficiencia obtenida a partir del mejor ajuste lineal por mínimos cuadrados es $\eta = (14.19 \pm 0.11)\%$.

La curva luz-corriente resuelta en polarización se muestra en la Figura 5.3 para la misma temperatura que la curva de la Figura 5.1. En ella se muestra la potencia medida en ambos puertos de salida del divisor de haz polarizado en función de la corriente.

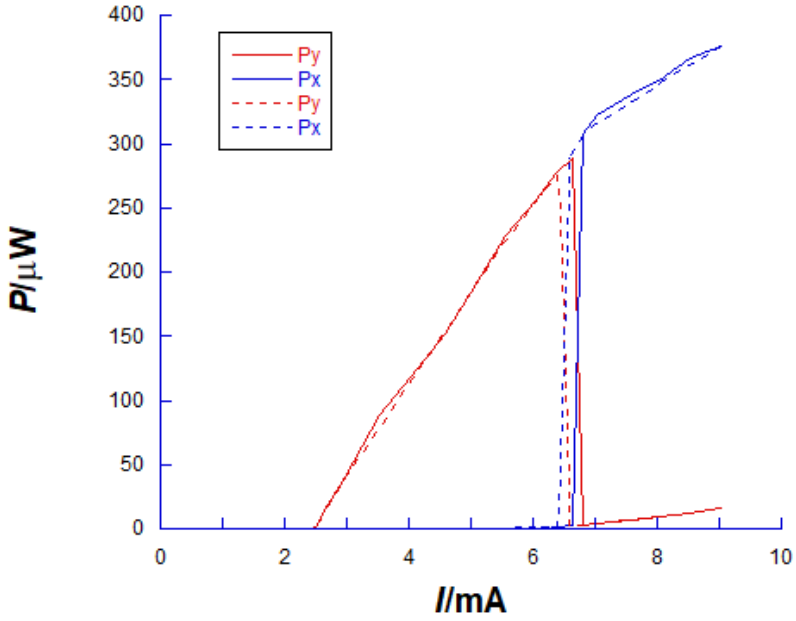

Figura 5.3: Potencia medida en las dos polarizaciones lineales en función de la corriente cuando esta aumenta (líneas continuas) y disminuye (líneas discontinuas). Las líneas rojas corresponden a la polarización Y, y las azules a la X.

En la Figura 5.3 se puede observar el mencionado fenómeno de switching de polarización (PS) desde la longitud de onda corta (Y) al modo de polarización de longitud de onda larga (X). Al incrementar la corriente el PS se produce en torno a $6.8\ \mathrm{mA}$, mientras que al disminuirla tiene lugar cerca de los $6.4\ \mathrm{mA}$. La formación de este ciclo de histéresis indica la existencia de una región biestable de polarización de aproximadamente $0.4\ \mathrm{mA}$ de ancho. La Figura 5.4 ilustra este comportamiento biestable, pues se observa que el espectro óptico cuando la corriente es de $6.6\ \mathrm{mA}$ es diferente dependiendo de si se ha obtenido aumentando o disminuyendo la corriente.

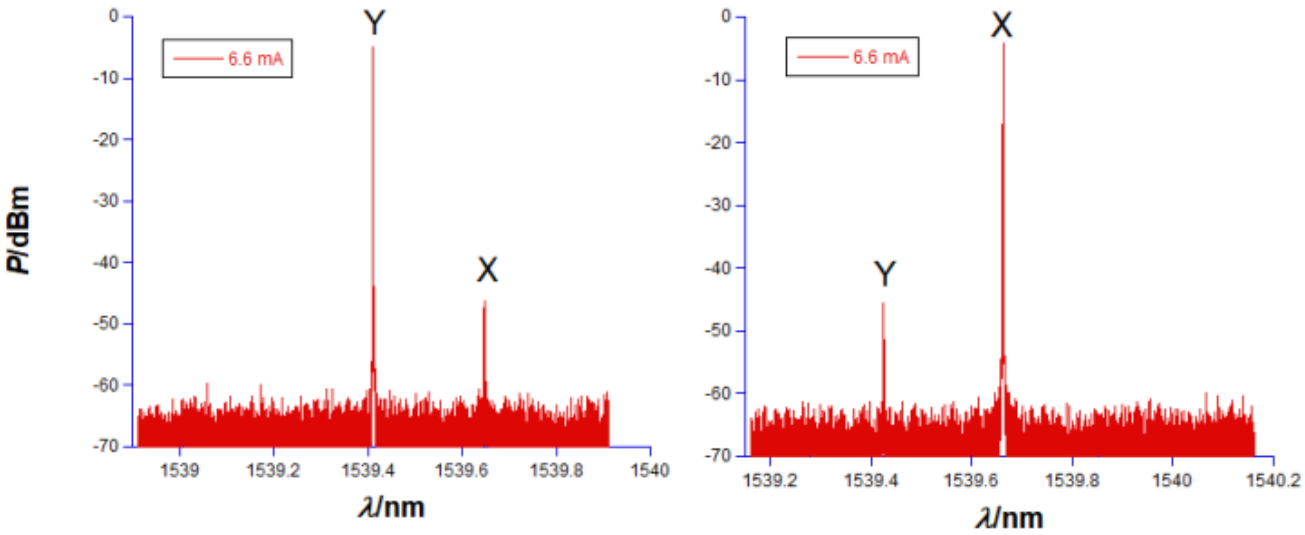

Figura 5.4: Espectro óptico en la región biestable ($I = 6.6\ \mathrm{mA}$) aumentando y disminuyendo la corriente, respectivamente.

En la Figura 5.5 se muestra el espectro óptico antes y después del switching para una temperatura de $22\ ℃$. Se puede apreciar una separación de longitudes de onda de $0.238\ \mathrm{nm}$ entre las polarizaciones Y y X, que corresponde de aproximadamente a una separación en frecuencias ópticas de $\Delta\upsilon = 30.1\ \mathrm{GHz}$.

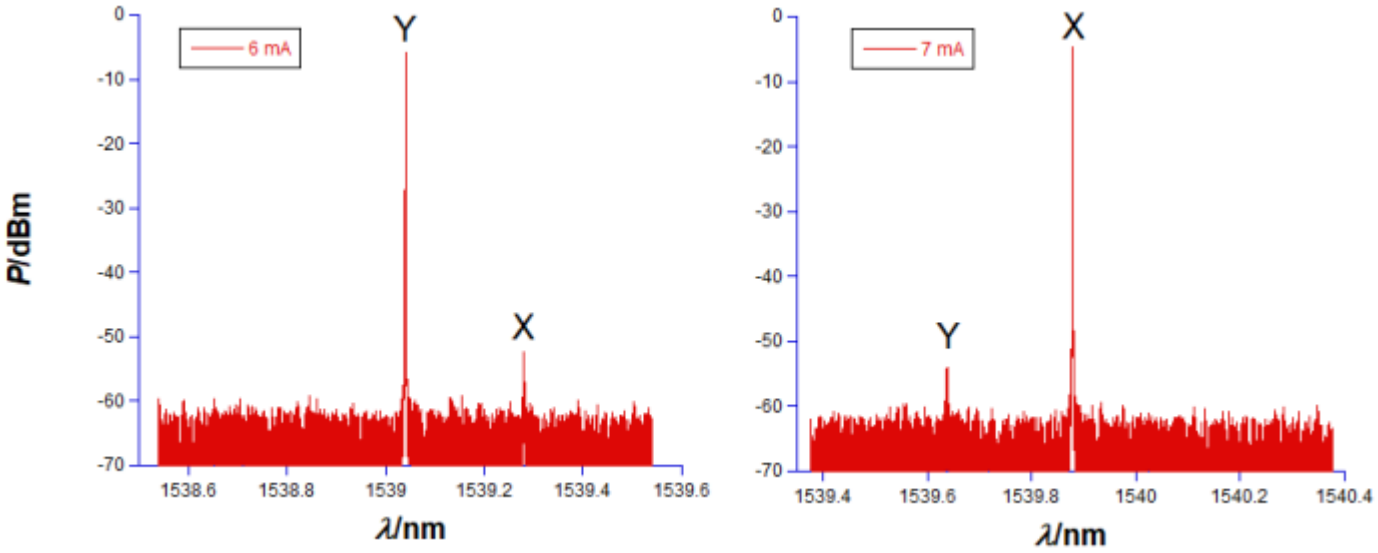

Figura 5.5: Espectro óptico para una corriente de $6\ \mathrm{mA}$ y $7\ \mathrm{mA}$, respectivamente.

La Figura 5.6 muestra cómo, para una temperatura exterior del VCSEL fija, el espectro óptico se va desplazando hacia longitudes de onda mayores a medida que se aumenta la corriente, fenómeno explicado en el capítulo 3.

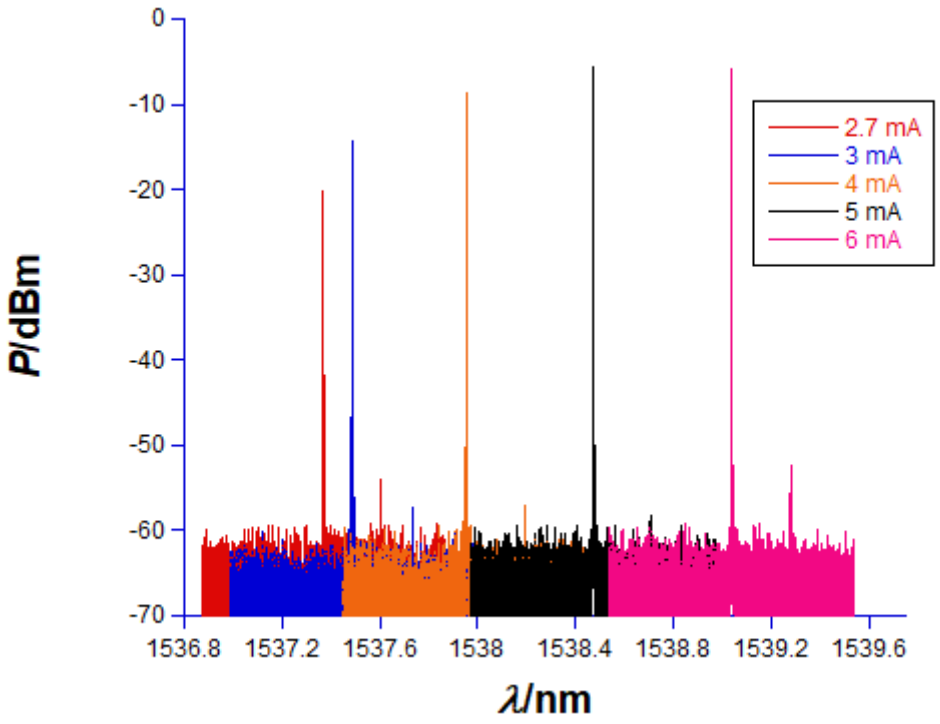

Figura 5.6: Espectros ópticos para intensidades de corriente crecientes a una temperatura fija de $22\ ℃$.

Por último, se ha medido el valor de la longitud de onda correspondiente al pico de mayor intensidad para cada espectro y se han representado estos valores en función de la corriente.

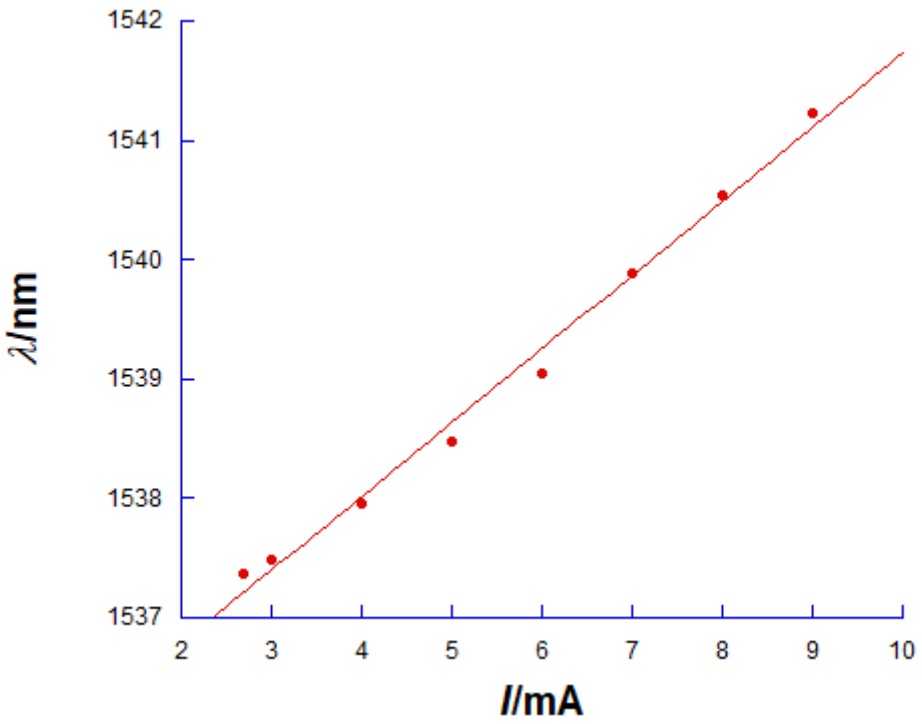

Figura 5.7: Valor de la longitud de onda en el pico de emisión frente a la corriente para $T = 22$ ℃.

Se puede apreciar en la Figura 5.7 una relación lineal entre la intensidad de corriente y la longitud de onda de los picos de emisión. Tras realizar un ajuste por mínimos cuadrados, la ecuación obtenida es $\lambda = (0.62 \pm 0.02) \cdot I + (1535.50 \pm 0.14)$. De esta manera, conociendo la corriente del láser aplicada, se puede estimar la longitud de onda a la que se encuentra el pico de emisión.

Capítulo 6
Resultados y análisis de datos en crudo

A lo largo del experimento, se ha trabajado con una frecuencia de modulación del VCSEL $f = 200\ \mathrm{MHz}$, de manera que el período del pulso de tensión aplicado por el generador de tramas es $\mathrm{T} = 1/f = 5\ \mathrm{ns}$. Este pulso tiene una amplitud constante V_{on} durante la primera mitad del período y es nulo durante la segunda mitad. El VCSEL está sometido a una corriente de polarización $I_{off} = 0.92 I_{th} = 2.25\ \mathrm{mA}$. Las medidas se han tomado para amplitudes de la señal V_{on} entre $0.3\ \mathrm{V}$ y $2.0\ \mathrm{V}$ en intervalos de $0.1\ \mathrm{V}$ y para temperaturas del controlador entre $19\ ^{\circ}\mathrm{C}$ y $25\ ^{\circ}\mathrm{C}$.

La generación de números aleatorios puede obtenerse muestreando regularmente las señales X e Y obtenidas en el osciloscopio, $V_X(t)$ y $V_Y(t)$, respectivamente. La comparación entre las amplitudes de las señales X e Y para un tiempo de muestreo t_s, que se trata de un tiempo medido con respecto al tiempo en que se empieza a aplicar el pulso de voltaje, determina el bit aleatorio obtenido. En nuestro caso, consideramos que si $V_X(t_s) > V_Y(t_s)$ se tiene un bit '0', y en caso contrario un bit '1'.

La Figura 6.1 ilustra las amplitudes de las señales temporales V_X y V_Y, registradas en el osciloscopio para una temperatura externa $T = 22\ ^{\circ}\mathrm{C}$, una señal $V_{on} = 1.3\ \mathrm{V}$ y un tiempo de muestreo $t_s = 2.2\ \mathrm{ns}$.

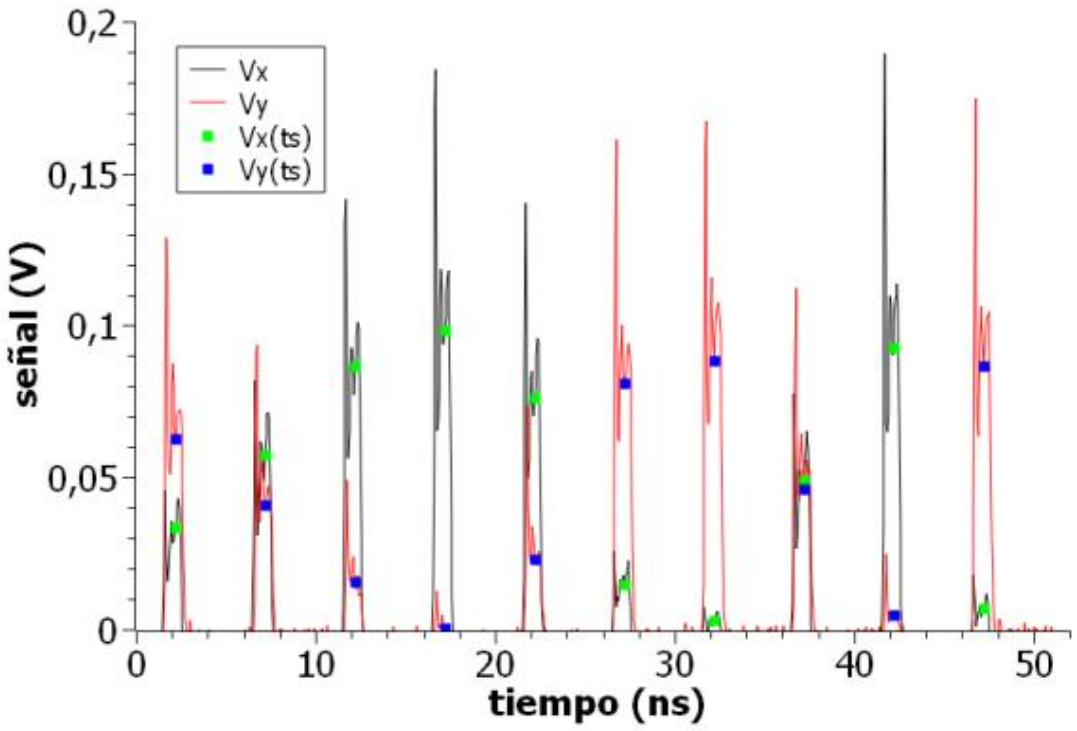

Figura 6.1: Trazas temporales experimentales de las señales correspondientes a la polarización X (línea negra) y la polarización Y (línea roja) para $T = 22\ ^{\circ}\mathrm{C}$, $V_{on} = 1.3\ \mathrm{V}$ y $t_s = 2.2\ \mathrm{ns}$. El valor de la señal X y la señal Y para un determinado tiempo de muestreo lo indican los puntos verdes y azules, respectivamente.

Se puede observar que ambas polarizaciones se excitan aleatoriamente al aplicar V_{on} $(t = 0\ \mathrm{ns})$ y cómo la señal decae al cabo de medio período aproximadamente. En algunas ocasiones una de las polarizaciones predomina durante todo el pulso, mientras que otras veces las polarizaciones alternan el dominio a lo largo del pulso. Siempre que se da este segundo caso, la polarización X se acaba recuperando (pulsos 2 y 8 de la Figura 6.1) [13].

Se puede observar también en la Figura 6.1 que la polarización X es la que se excita al final del pulso en la mayoría de los casos. Sin embargo, en algunos pulsos, como el primero, domina la polarización Y. Esto sucede porque el sistema aún no ha alcanzado el estado estacionario. Durante el primer pulso la polarización X apenas se excita porque V_{on} debe aplicarse durante un tiempo mucho mayor que $5\ \mathrm{ns}$ para permitir que la señal V_X se recupere y llegue al estado estacionario. Este comportamiento refleja que la corriente aplicada al láser es mayor que la corriente a la que se produce el fenómeno de switching de polarización, explicado en el capítulo 3. De este modo, la polarización X es estable y la polarización Y es inestable [13].

Se ha comprobado que para un período suficientemente grande la polarización X domina siempre la emisión, por lo que hay que considerar valores del período lo suficientemente pequeños como para que el VCSEL esté siempre en régimen transitorio, sin dejar que el dispositivo alcance su estado estacionario [13]. Esta situación se ve reflejada en la Figura 6.1. De este modo, no es necesario operar en la región biestable, que como se puede ver en la Figura 5.3 es bastante estrecha, para lograr un QRNG (Quantum Random Number Generator) utilizando la polarización del VCSEL.

En la Figura 6.2 se muestran los histogramas de las señales X e Y para las mismas condiciones de la Figura 6.1. Ambas señales tienen formas similares y presentan máximos locales cercanos a los valores mínimo y máximo de las señales. Esta situación se ha evaluado para el tiempo de muestreo específico de $t_s = 2.2\ \mathrm{ns}$ y cambiará significativamente si se toma otro tiempo de muestreo diferente. Este y similares histogramas se han realizado con 10^4 datos.

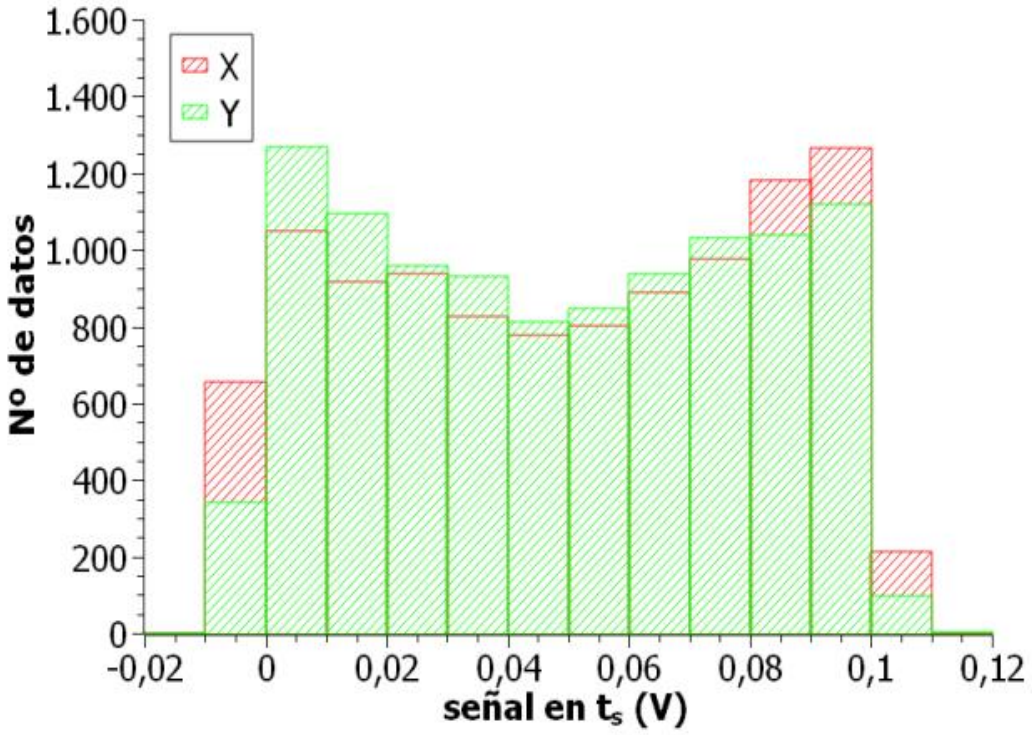

Figura 6.2: Histograma de las señales X e Y para $T = 22$ °C, $V_{on} = 1.3$ V y $t_s = 2.2$ ns.

Para analizar el efecto de la temperatura en nuestro sistema consideramos la probabilidad de excitación de la polarización X, $P(X > Y)$, como la probabilidad de obtener $V_X(t_s) > V_Y(t_s)$; es decir, la probabilidad de obtener un bit '0'. Por ejemplo, en el caso analizado en la Figura 6.1 se tiene $P(X > Y) = 0.511$.

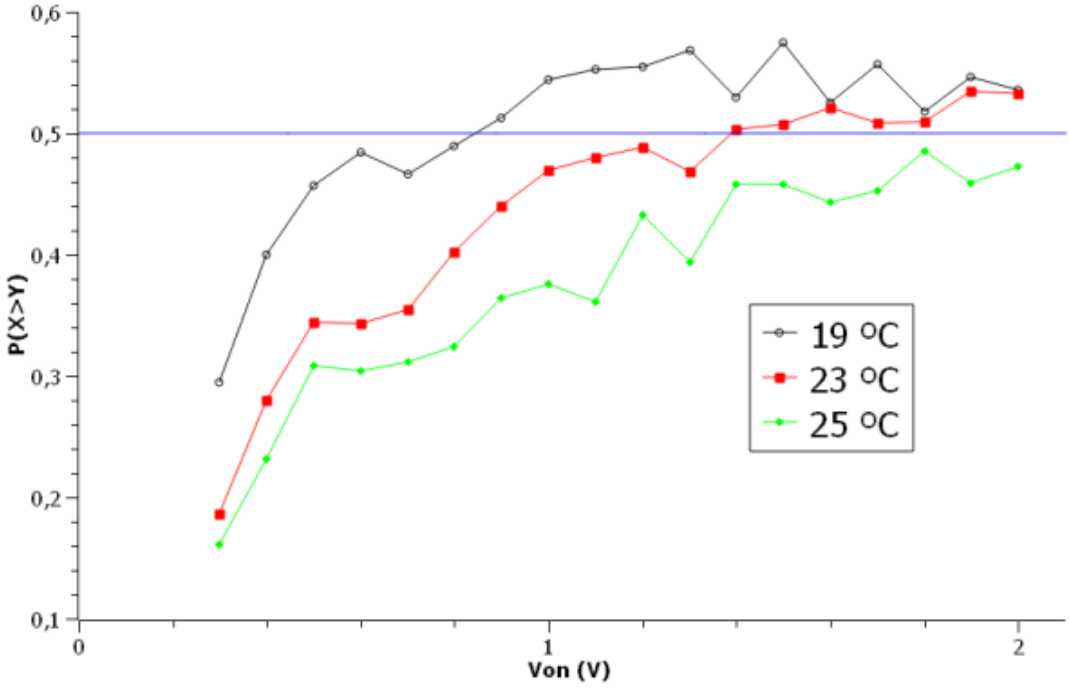

Figura 6.3: Probabilidad de excitación de la polarización X en función de V_{on} para diferentes valores de la temperatura y $t_s = 2.2$ ns.

En la Figura 6.3 encontramos que $P(X > Y)$ disminuye para temperaturas crecientes. Además, tras un incremento inicial de $P(X > Y)$ cuando V_{on} es pequeño, se obtiene una saturación de los valores de la probabilidad para un rango amplio de valores de la señal V_{on}. También se puede observar que el cambio de $P(X > Y)$ cuando la temperatura varía en 6 ℃ puede ser relativamente grande. Por ejemplo, para $V_{on} = 1.1$ V, $P(X > Y)$ disminuye de 0.552 a 0.361 cuando T pasa de 19 ℃ a 25 ℃.

El comportamiento de saturación anterior también se observa al modificar el tiempo de muestreo, como se demuestra en la Figura 6.4. La dependencia de $P(X > Y)$ del valor de t_s muestra que el rango de variación de esta probabilidad aumenta a medida que lo hace el tiempo de muestreo. La probabilidad de excitar la polarización X aumenta con V_{on} porque es precisamente dicha polarización la que se excita para valores altos de la corriente aplicada como puede verse en la Figura 5.3.

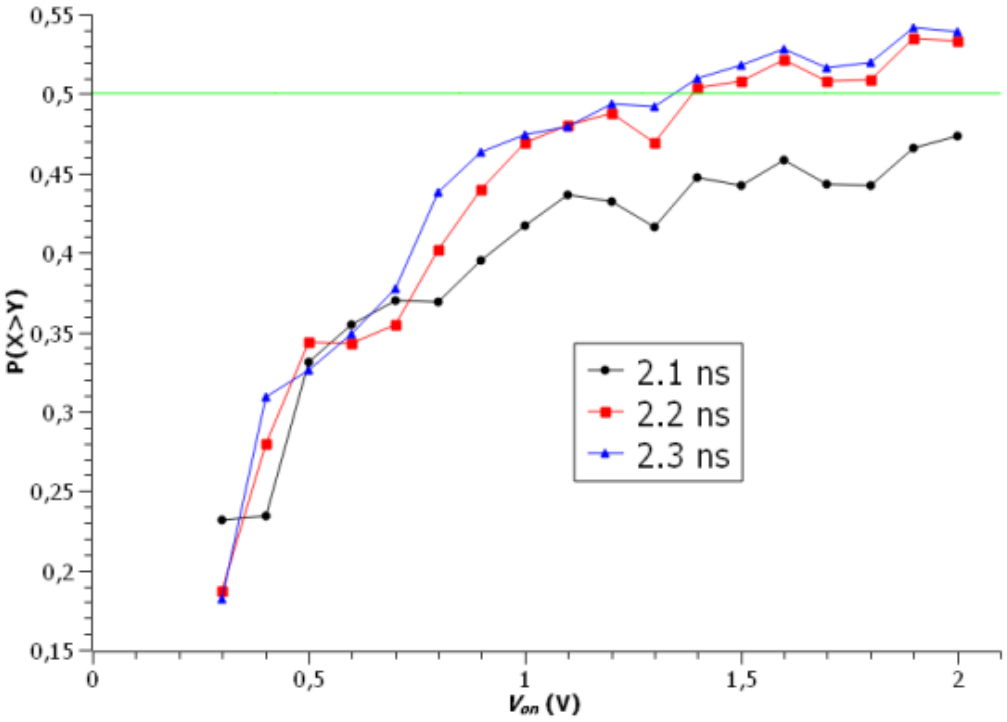

Figura 6.4: Probabilidad de excitación de la polarización X en función de V_{on} para diferentes tiempos de muestreo y $T = 23$ ℃.

En la Figura 6.5, donde se representan las trazas temporales correspondientes a ambas polarizaciones para dos valores distintos de V_{on}, también puede apreciarse que cuando V_{on} es pequeño y el tiempo de muestreo elegido ($t_s = 2.2$ ns) se encuentra a mitad del pulso, se excitan preferiblemente los pulsos polarizados en Y, con una probabilidad $P(X > Y) = 0.187$. En caso contrario, cuando se tiene una señal V_{on} grande, los pulsos polarizados en X se excitan con una probabilidad mayor, pues $P(X > Y) = 0.533$, acorde a los resultados de la Figura 6.4.

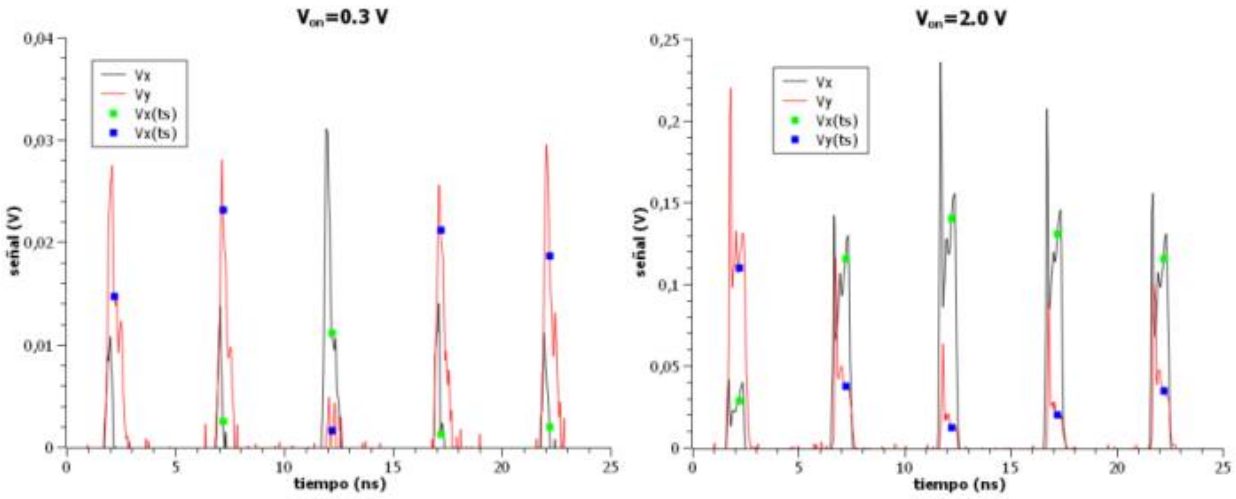

Figura 6.5: Trazas temporales experimentales de las señales correspondientes a la polarización X (línea negra) y la polarización Y (línea roja) para $T = 23$ °C, $V_{on} = 0.3$ V (izquierda) y $V_{on} = 2.0$ V (derecha), y $t_s = 2.2$ ns. El valor de la señal X y la señal Y para un determinado tiempo de muestreo lo indican los puntos verdes y azules, respectivamente.

A diferencia de lo que ocurre en la Figura 6.1, donde la polarización excitada al final del pulso casi siempre era la X, en la Figura 6.5 para $V_{on} = 0.3$ V es la señal Y la que se excita casi siempre al final del pulso [13]. Este resultado indica que se está aplicando una corriente menor a la de switching mientras V_{on} es aplicado, lo que concuerda con la Figura 5.3, donde para corrientes pequeñas domina la polarización Y. En cambio, para $V_{on} = 2.0$ V la situación es muy similar a la de la Figura 6.1, pues en ambos casos la corriente aplicada supera a la de switching.

En la Figura 6.6 se han representado los histogramas de las señales X e Y para dos valores diferentes de t_s, para ayudar a comprender mejor la evolución de la probabilidad de excitación con la variación del tiempo de muestreo. Las condiciones de temperatura y amplitud de señal son las mismas que en la Figura 6.1 ($T = 22$ °C; $V_{on} = 1.3$ V).

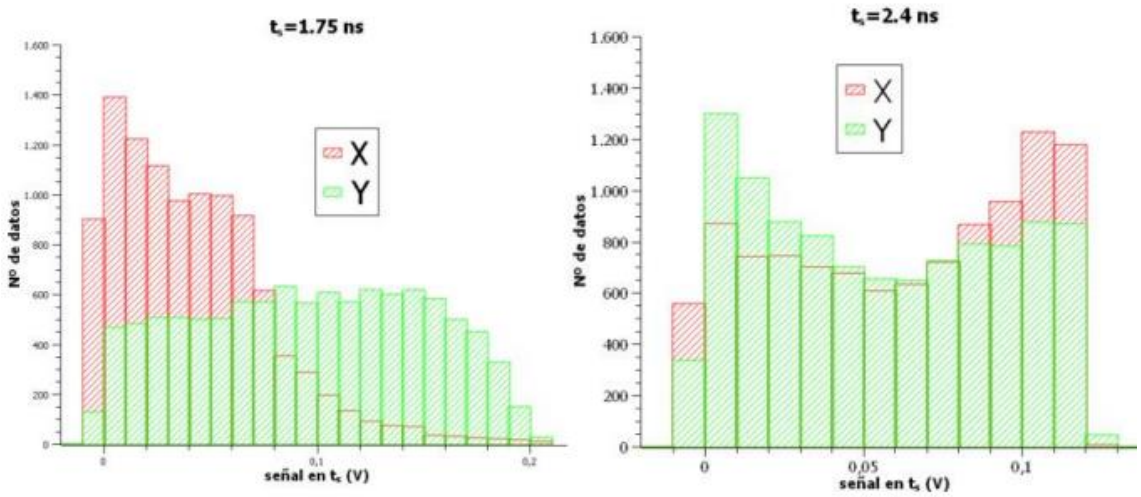

Figura 6.6: Histogramas de las señales X e Y para $T = 22$ ºC, $V_{on} = 1.3$ V, y $t_s = 1.75$ ns (izquierda) y $t_s = 2.4$ ns (derecha).

Como puede verse en la Figura 6.6, para un tiempo de muestreo pequeño ($t_s = 1.75$ ns) la polarización Y se excita preferentemente. El rango de variación entre V_X y V_Y es amplio dado que las señales se están muestreando en un instante cercano a la excitación del primer pico de los pulsos en la Figura 6.1. Al aumentar el tiempo de muestreo a un momento próximo a la caída de la señal ($t_s = 2.4$ ns) es la polarización X la que predomina, pues como ya se ha discutido, esta polarización se recupera al final del pulso al ser la estable. Para tiempos de muestreo intermedios, como en la Figura 6.2, ambas distribuciones presentan formas semejantes.

En el resto de este capítulo elegiremos los parámetros de temperatura, modulación y tiempo de muestreo para obtener un histograma de $V_X(t_s)$ y $V_Y(t_s)$ con una forma lo más semejante posible a una distribución uniforme. Esto contrasta con las formas obtenidas en la Figura 6.2, en la que ambas funciones tenían claros máximos locales próximos a los valores mínimos y máximos de las señales, de tal forma que la probabilidad de obtener valores en la parte central de los histogramas era baja.

En la Figura 6.7 se ilustra el histograma de la señal Y con unos parámetros para los que se ha encontrado la forma más próxima a la de una distribución uniforme. Esta Figura 6.7 se ha obtenido para una temperatura $T = 24$ ºC, una amplitud de señal $V_{on} = 1.4$ V y un tiempo de muestreo $t_s = 1.75$ ns.

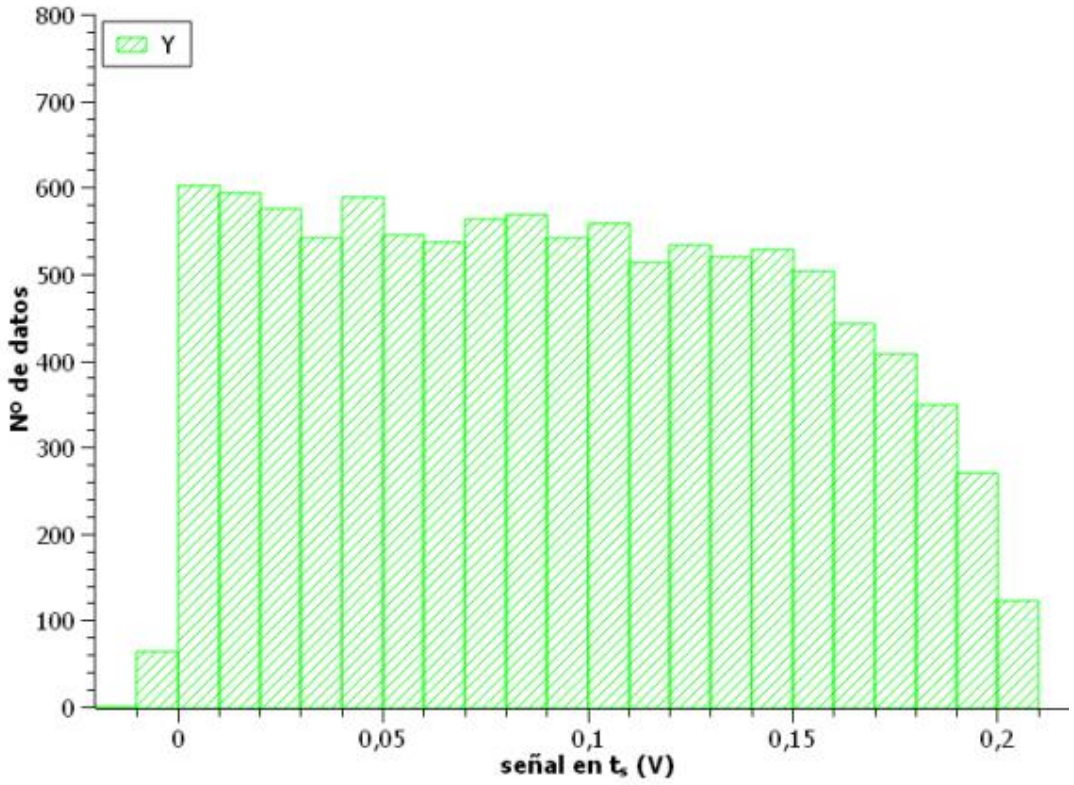

Figura 6.7: Histograma de la señal Y para $T = 24$ ℃, $V_{on} = 1.4$ V y $t_s = 1.75$ ns.

La Figura 6.8 muestra las amplitudes de las señales temporales V_X y V_Y, registradas en el osciloscopio para las mismas condiciones que las de la Figura 6.7.

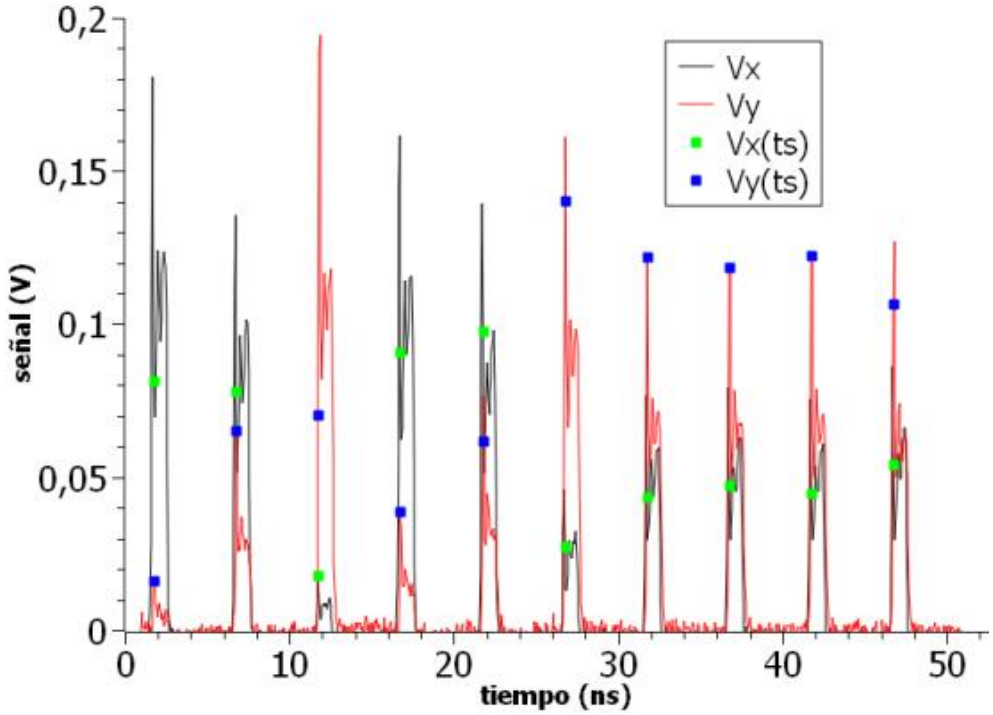

Figura 6.8: Trazas temporales experimentales de las señales correspondientes a la polarización X (línea negra) y la polarización Y (línea roja) para $T = 24$ ℃, $V_{on} = 1.4$ V y $t_s = 1.75$ ns. El valor de la señal X y la señal Y para un determinado tiempo de muestreo lo indican los puntos verdes y azules, respectivamente.

El hecho de encontrar el histograma más parecido a una distribución uniforme para estas condiciones concuerda con los resultados explicados. Al aplicar una amplitud de señal $V_{on} = 1.4\ \mathrm{V}$, la corriente aplicada supera a la del switching, con lo que cabría esperar un predominio de la polarización X, al igual que en la Figura 6.1, pero se ha aumentado la temperatura y se ha seleccionado un tiempo de muestreo bajo, en un instante próximo a la excitación del primer pico de los pulsos, que favorece el predominio de la señal Y.

Capítulo 7
Resultados y análisis de datos postprocesados

Como ya se ha comentado en el capítulo 2, la generación de números aleatorios desempeña un papel fundamental en la criptografía. Sin embargo, los generadores de números aleatorios no son perfectos y pueden exhibir patrones no deseados o sesgos, lo que puede afectar la validez y confiabilidad de los resultados obtenidos. Por ello, en ocasiones es necesario aplicar técnicas de postprocesado para abordar estas limitaciones y mejorar la aleatoriedad y uniformidad de los datos.

Los tests de NIST (National Institute of Standards and Technology) son un conjunto de pruebas estadísticas diseñadas para evaluar la calidad y aleatoriedad de las secuencias de números binarios producidas por generadores de números aleatorios. El conjunto de pruebas de NIST consta de 15 tests diferentes que evalúan diversas propiedades estadísticas de las secuencias de números, incluyendo la frecuencia de unos y ceros, la presencia de patrones repetitivos, la autocorrelación y la entropía. Estas pruebas buscan detectar cualquier desviación significativa de la verdadera aleatoriedad [15]. Sin embargo, es importante destacar que los tests de NIST no garantizan una aleatoriedad perfecta, pero proporcionan un análisis estadístico útil de la calidad de una secuencia de números generados. Si una secuencia no pasa los tests de NIST, se sugiere que se realicen mejoras en el generador de números aleatorios para tener una mayor confiabilidad en su uso.

La cantidad de datos necesaria para pasar los tests de NIST puede variar dependiendo del generador de números aleatorios y de los requisitos específicos de la aplicación. En general, se recomienda un tamaño de muestra lo suficientemente grande para obtener resultados estadísticamente significativos. En este capítulo se ha trabajado con ficheros de datos, obtenidos con el sistema experimental descrito en los capítulos anteriores, que han sido postprocesados (resultando en archivos con una cantidad almacenada de bits entre 10^5 y 10^9) siguiendo dos métodos diferentes: postprocesamiento no lineal de Von Neumann y postprocesamiento con códigos BCH. El objetivo de este capítulo es visualizar gráficamente la aleatoriedad de los números generados tras postprocesar los bits obtenidos en el experimento. La verificación de si estos bits pasan los tests de NIST va más allá de los objetivos de este trabajo. La demostración de que estos bits postprocesados con Von Neumann y con una gran variedad de códigos BCH han superado las baterías de NIST se puede ver en [16].

7.1. Postprocesado Von Neumann

Antes de introducir la técnica de postprocesamiento empleada, es necesario definir el concepto de sesgo o bias: $e = p(0) - 1/2$; es decir, la probabilidad de obtener un bit '0' menos un medio. En esta sección consideramos el algoritmo de postprocesamiento no

lineal de Von Neumann. El proceso de postprocesamiento se realiza en los pares de bits consecutivos en la secuencia binaria generada. Se siguen los siguientes pasos [17]:

1. Tomar cada par de bits consecutivos en la secuencia producida.
2. Descartar aquellos pares de bits que sean iguales (‘00’ o ‘11’).
3. Si el par de bits es diferente (‘01’ o ‘10’), se toma el primer bit del par como el bit de salida.

Suponemos que para un bias e, la probabilidad de tener un bit ‘0’ es $p(0) = e + 1/2$ (por tanto, la probabilidad de obtener un bit ‘1’ es $p(1) = 1/2 - e$). Tras aplicar los pasos previamente explicados, la probabilidad de obtener ahora un bit ‘0’ es $p(0) = \frac{p(01)}{p(01)+p(10)} = 1/2$, eliminando el bias por completo [17].

Empleando este método, la tasa de obtención de un par útil (‘01’ o ’10’) es $2(1/4 - e^2)$. En realidad, por cada par de salida se considera un único bit, por lo que la tasa es $1/4 - e^2$, lo que supondría un descarte del 75% de los bits en el mejor de los casos. De esta manera, el post procesamiento Von Neumann es muy eficiente para reducir el sesgo a cambio de un rendimiento discreto.

Para plasmar la aleatoriedad de los datos postprocesados con este método de Von Neumann se han elaborado una serie de estructuras mediante diversos códigos escritos en Python. Por ejemplo, en la Figura 7.1 se ilustran matrices de diferentes dimensiones dependiendo del tamaño del archivo de datos. En estas matrices cada elemento corresponderá a un bit de la secuencia. El primer programa (Apéndice A) lee el fichero de datos y si el bit es ‘0’, se asignará el color negro, mientras que, si el bit es ‘1’, se asignará el color blanco.

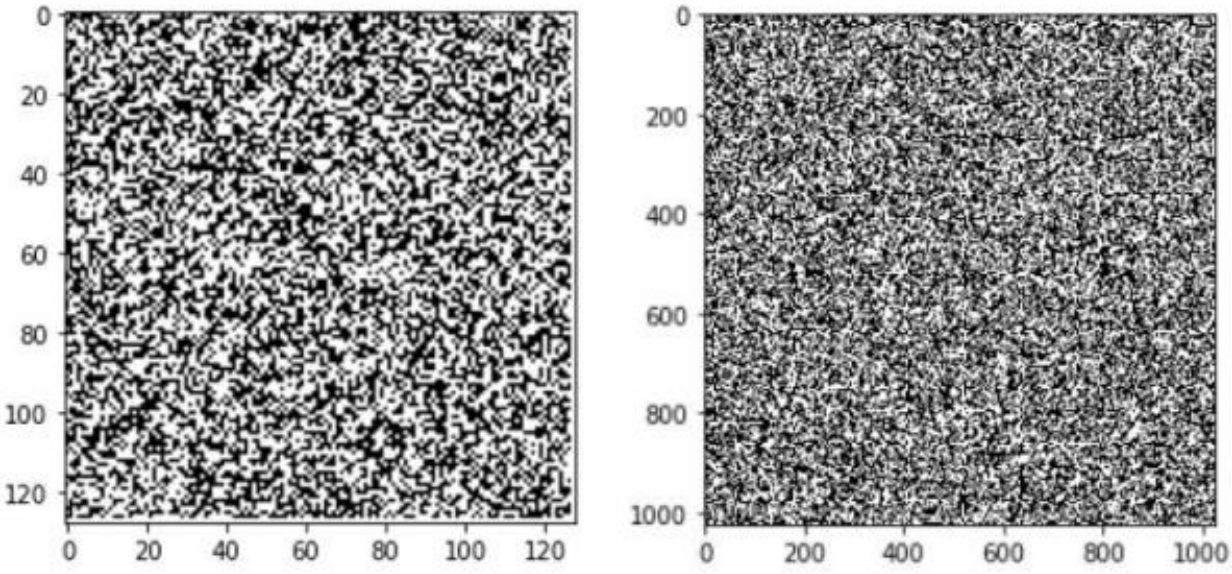

Figura 7.1: Matrices de 128×128 para 10^5 bits (imagen de la izquierda) y de 1024×1024 para 10^7 bits (imagen de la derecha). Los elementos negros corresponden a bits ‘0’ y los blancos a bits ‘1’.

Este tipo de representación puede resultar útil para visualizar estructuras en la secuencia de bits, especialmente cuando se trata de secuencias binarias. Al asignar colores distintos a los diferentes valores de los bits, se puede plasmar claramente la distribución

de unos y ceros en la secuencia. En la Figura 7.1, no se pueden apreciar a simple vista patrones o formas que comprometan la propiedad de aleatoriedad.

En la Figura 7.2 se representa el número racional obtenido a partir de 16 bits frente al número racional obtenido a partir de los 16 bits anteriores, para un conjunto de datos de 10^5 bits. Esto se ha llevado a cabo con un segundo programa (Apéndice B) que lee el archivo, agrupa los bits en grupos de 16 y los divide entre 2^{16} para transformarlos en números racionales comprendidos entre el cero y el uno. Finalmente, se dibuja cada número racional obtenido $i + 1$ frente al anterior i.

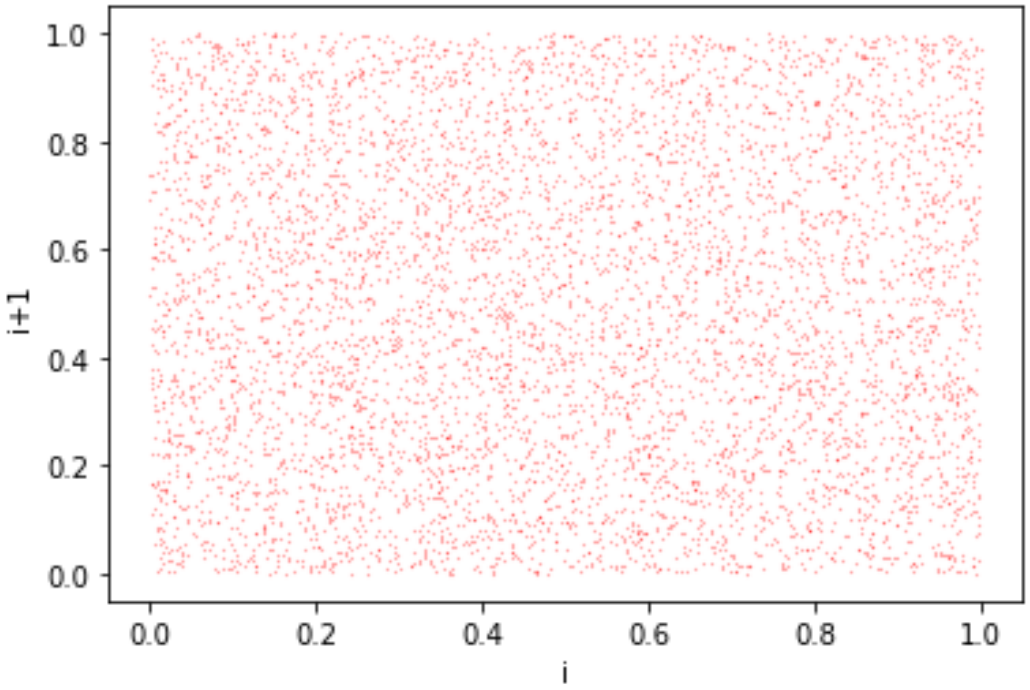

Figura 7.2: Representación de un número $i + 1$ frente al anterior i para un archivo de 10^5 bits.

Al tomar los bits en grupos de 16 y convertirlos en números racionales entre cero y uno, se puede reducir y comprimir la cantidad de datos necesarios para representar la secuencia binaria. Este proceso ayuda a visualizar los datos binarios de manera más eficiente y facilita el análisis de patrones o detección de anomalías en la distribución de los puntos. En la Figura 7.2, no se observa ninguna correlación entre un número racional obtenido y su anterior.

Mediante un tercer programa (Apéndice C) se ha confeccionado una FDP (función de densidad de probabilidad) en la Figura 7.3 para un fichero de 10^7 bits. De nuevo, el software recibe el fichero de datos, agrupa los bits en grupos de 16 y los convierte en números racionales comprendidos entre el cero y el uno. Una vez transformados, el programa elabora una FDP para los números racionales i.

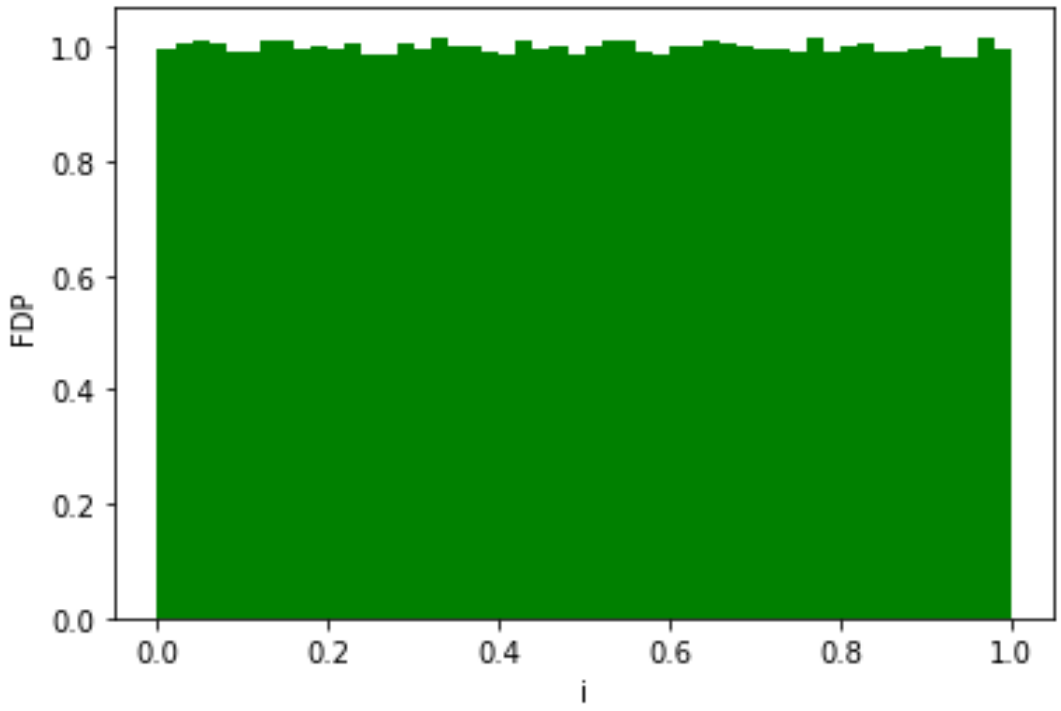

Figura 7.3: Función de densidad de probabilidad de los números racionales i entre cero y uno, para un archivo de 10^7 bits.

Al agrupar los bits en tandas de 16 y calcular la función de densidad de probabilidad de una secuencia binaria, se puede aprovechar la redundancia o la estructura de los datos binarios para llevar a cabo un análisis más eficiente de su distribución y sus características estadísticas. Esto puede ser útil para identificar patrones, detectar anomalías o realizar comparaciones con otras distribuciones conocidas. En la Figura 7.3, se ha obtenido una función de densidad de probabilidad que se aproxima bastante a una distribución uniforme, lo cual es un buen indicativo de la aleatoriedad de los bits postprocesados por el método de Von Neumann.

7.2. Postprocesado con códigos BCH

En esta sección consideramos las técnicas de postprocesado de códigos correctores lineales $[n,\ k, d]$-BCH (Bose-Chaudhuri-Hocquenghem), que se basan en el siguiente teorema [18]: *Sea G un corrector lineal que mapea n bits a k bits. Entonces, el sesgo de cualquier combinación lineal no nula de los bits de salida es menor o igual que $2^{d-1}e^d$, donde e es el sesgo de la secuencia de bits en crudo y d es la mínima distancia del código lineal construido por la matriz generadora G.*

Se utilizan los códigos $[n,\ k, d]$-BCH definidos sobre el campo finito $GF(2)$ y donde $n + 1$ es potencia de 2. Para los bits en bruto de entrada $(x_{n-1}, \dots, x_0)$, la salida $(y_{k-1}, \dots, y_0)$ se obtiene como:

$$\begin{pmatrix} g_{n-k} & \cdots\cdots\cdots & g_0 & 0\ldots\ldots 0 \\ 0 & g_{n-k} & \cdots\cdots\cdots g_0 & 0\ldots\ldots 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0\ldots\ldots & 0 & g_{n-k} & \ldots\ldots g_0 \end{pmatrix} \begin{pmatrix} x_{n-1} \\ x_{n-2} \\ \vdots \\ x_0 \end{pmatrix} = \begin{pmatrix} y_{k-1} \\ y_{k-2} \\ \vdots \\ y_0 \end{pmatrix}$$

y $g(x) = g_{n-k}x^k + \cdots + g_1 x + g_0$ es el polinomio generador cíclico del código $[n,\ k, d]$-BCH [16].

El rendimiento, k/n, puede ser mucho mayor que el obtenido con el método de Von Neumann (que como ya se ha explicado en la sección 7.2 es del 25% en un caso ideal), manteniendo al mismo tiempo una reducción de sesgo $2^{d-1}e^d$ muy eficiente. Esto significa que eligiendo un valor k ligeramente inferior a n se puede alcanzar un rendimiento elevado [16].

En la Figura 7.4 se muestran las matrices elaboradas por el programa del Apéndice A, para ficheros de 10^5 y 10^7 bits, respectivamente. Estos ficheros se han obtenido haciendo un postprocesado con $n = 1023$, $k = 1003$ y $d = 5$. El rendimiento es por tanto muy cercano a uno $(k/n = 0.98)$. Al igual que en la Figura 7.1 obtenida para bits postprocesados por el método de Von Neumann, en la Figura 7.4 no se pueden apreciar a simple vista patrones en la distribución de los ceros y unos de la secuencia binaria de bits postprocesados con códigos BCH.

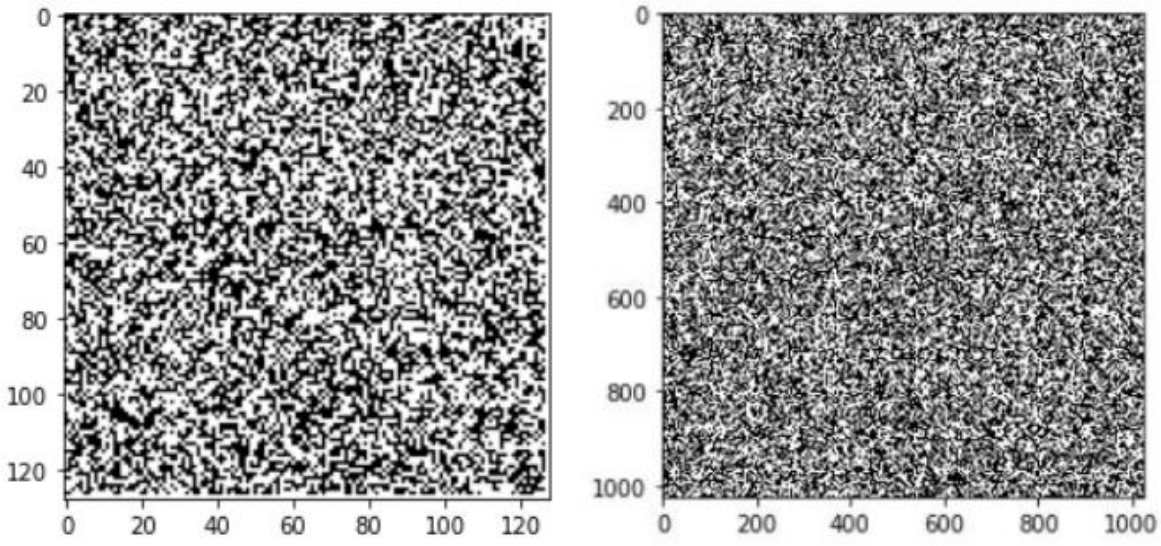

Figura 7.4: Matrices de 128×128 para 10^5 bits (imagen de la izquierda) y de 1024×1024 para 10^7 bits (imagen de la derecha). Los elemenos negros corresponde a bits '0' y los blancos a bits '1'.

Se ha empleado el programa del Apéndice B para transformar una secuencia de 10^5 bits en números racionales entre cero y uno. En la Figura 7.5 se representa cada número $i + 1$ frente al anterior i. Como ocurría en la Figura 7.2, en la Figura 7.5 tampoco se puede discernir a simple vista una correlación entre un número $i + 1$ y su anterior i.

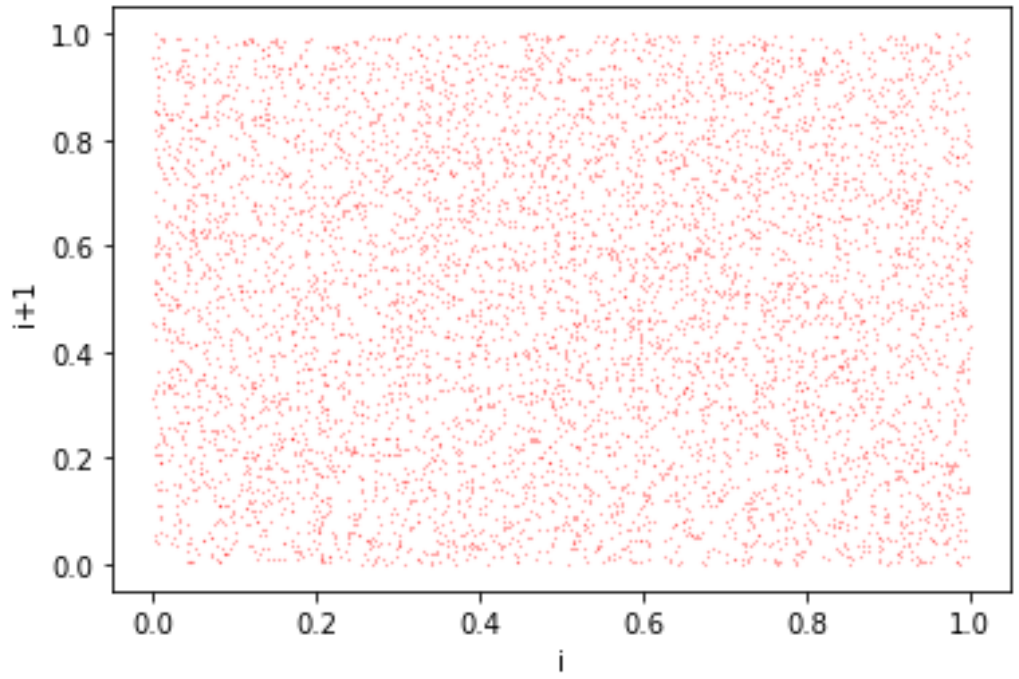

Figura 7.5: Representación de un número $i + 1$ frente al anterior i para un archivo de 10^5 bits.

Por último, haciendo uso del programa del Apéndice C, se muestra una FDP de los números racionales i entre cero y uno para un archivo de 10^7 bits en la Figura 7.6. Se puede observar cómo se obtiene una distribución muy semejante a la uniforme, al igual que en la Figura 7.3 para el postprocesado de Von Neumann. Esto indica que ambos tipos de postprocesamiento son prometedores para lograr la aleatoriedad de los resultados.

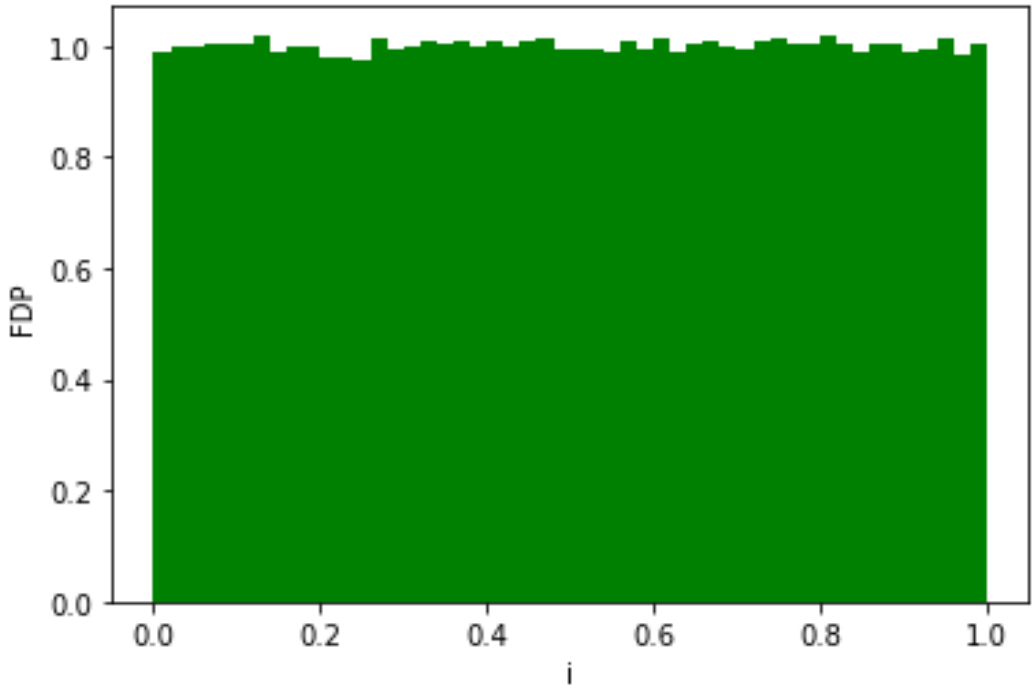

Figura 7.6: Función de densidad de probabilidad de los números racionales i entre cero y uno, para un archivo de 10^7 bits.

Capítulo 8
Discusiones y conclusiones

8.1. Discusión de los resultados en crudo

Como se ha podido observar a lo largo del capítulo 6, los resultados obtenidos dependen en gran medida de la amplitud de la señal V_{on}, del tiempo de muestreo elegido y de la temperatura. Ya se ha comentado que la probabilidad de excitación del modo polarizado X aumenta con el valor del pulso V_{on} debido a que se alcanza y supera la corriente a la que se produce el fenómeno de switching de polarización. Esto se refleja en la Figura 5.3, donde se ve que el modo X predomina para corrientes altas.

En cuanto a la dependencia con la temperatura, en la Figura 8.1 se observa claramente que la probabilidad de excitación de la señal X decrece con la temperatura. Esta relación puede explicarse considerando cómo depende el dicroísmo del VCSEL de la temperatura. El dicroísmo representa la diferencia de pérdidas entre ambas polarizaciones lineales del VCSEL. Se ha observado que en VCSELs similares al usado en este experimento el aumento de temperatura induce un dicroísmo que favorece a la polarización de menor longitud de onda [12], la Y en nuestro caso.

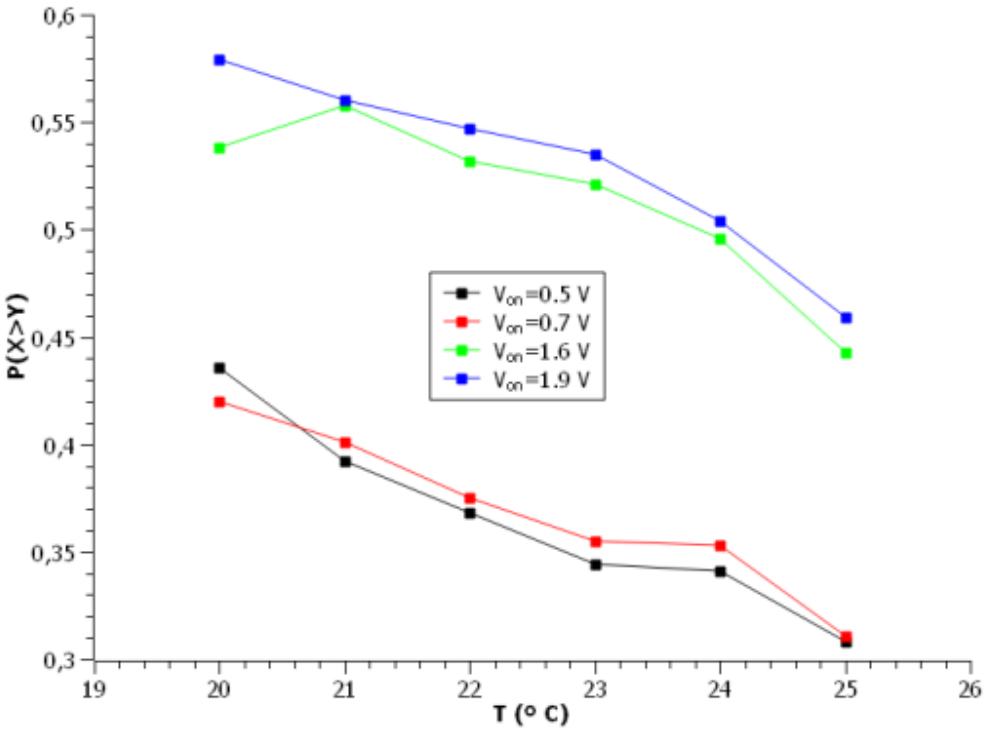

Figura 8.1: Probabilidad de excitación de la polarización X en función de la temperatura para diferentes valores de V_{on} y $t_s = 2.2$ ns.

También se ha observado que $P(X > Y)$ aumenta a medida que lo hace el tiempo de muestreo t_s. Esto sucede porque para períodos de tiempo suficientemente grandes el VCSEL opera en el estado estacionario, donde la polarización X domina siempre la emisión. Considerando valores del tiempo pequeños para que el dispositivo opere siempre en régimen transitorio, sin dejar que el VCSEL alcance el estado estacionario, se suaviza el dominio de la señal X y, además, se evita la necesidad de trabajar en la región biestable.

En conclusión, para lograr un QRNG utilizando la polarización del VCSEL hemos procedido de tal manera que se pueda obtener $P(X > Y) \sim 0.5$. Para ello hemos elegido los parámetros de V_{on}, T y t_s más adecuados para obtener un histograma con la forma lo más parecida posible a la distribución uniforme, visto en la Figura 6.7. Los mejores resultados se han encontrado para valores V_{on} donde la corriente supera a la de switching y, por tanto, domina la polarización X. Esto se compensa trabajando a temperaturas más elevadas y en tiempos de muestreo cercanos al primer pico de excitación, para favorecer el predominio de la señal Y y lograr que las probabilidades de ambas polarizaciones se equilibren lo máximo posible.

8.2. Discusión de los datos postprocesados

El postprocesamiento es necesario en los generadores de números aleatorios porque las salidas en bruto de los generadores físicos muestran desviaciones del ideal matemático de bits estadísticamente independientes y uniformemente distribuidos [5]. En el capítulo 7 de este trabajo se han considerado dos técnicas de postprocesamiento: códigos no lineales de Von Neumann y familia de códigos lineales BCH.

Los ficheros de datos postprocesados con los que se ha trabajado habían superado previamente los tests de NIST [16]. Se ha intentado plasmar gráficamente la aleatoriedad de estos resultados mediante distintas figuras para los dos tipos de postprocesamiento empleados. En ningún caso se puede apreciar patrones en las matrices de ceros (negro) y unos (blanco) de las Figuras 7.1 y 7.4 o correlaciones entre puntos que representan un número racional frente al anterior en las Figuras 7.2 y 7.5. Además, las funciones de densidad de probabilidad obtenidas en las Figuras 7.3 y 7.6 se asemejan a la forma de una distribución uniforme, lo cual es un buen indicativo en cuanto a la aleatoriedad de los bits postprocesados.

Comparando ambos tipos de postprocesado, se obtienen resultados similares para archivos del mismo tamaño. El postprocesado Von Neumann sacrifica el rendimiento en pos de eliminar el bias completamente, pues en el mejor de los casos, aprovecha el 25% de los bits. Por su parte, el postprocesado con códigos BCH logra reducir significativamente el bias manteniendo un rendimiento muy cercano al 100% (98% en este caso).

Resumiendo, postprocesando con dos métodos diferentes los bits obtenidos a partir de la configuración experimental desarrollada en el capítulo 6, los ficheros de bits resultantes han superado las pruebas de NIST y se ha mostrado visualmente la

aleatoriedad resultante. El hecho de no apreciar patrones o estructuras que indiquen una correlación entre los datos no implica necesariamente su aleatoriedad, pero estos resultados preliminares indican que el sistema empleado puede ser un buen candidato para la generación de números aleatorios.

Bibliografía

[1] Stinson, D. R., & Paterson, M. *Cryptography: Theory and Practice*. CRC Press. (2018).

[2] Poskitt, K. *The Secret Life of Codes*. Scholastic. (2009).

[3] Abellán, C. *The Future of Cybersecurity Is the Quantum Random Number Generator.* IEEE Spectrum. (2021, 29 julio). https://spectrum.ieee.org/the-future-of-cybersecurity-is-the-quantum-random-number-generator

[4] Mannalath, V., Mishra, S. K., & Pathak, A. *A Comprehensive Review of Quantum Random Number Generators: Concepts, Classification and the Origin of Randomness*. arXiv (Cornell University). (2022). https://doi.org/10.48550/arxiv.2203.00261

[5] M. Stipčević and Ç. K. Koç, "True random number generators," in Open Problems in Mathematics and Computational Science, (Springer, 2014). https://doi.org/10.1007/978-3-319-10683-0

[6] Rivero, I., & Valle, A. *Estudio experimental de un generador cuántico de números aleatorios basado en láseres de semiconductor*. Trabajo de Fin de Grado, Universidad de Cantabria. (2022, junio).

[7] Saleh, B. E. A., & Teich, M. C. Fundamentals of Photonics. Wiley Series in Pure and Applied Optics. (1991). https://doi.org/10.1002/0471213748

[8] Olmo R. & Nave.R. *Aplicaciones del Láser.* Hyperphysics. http://hyperphysics.phy-astr.gsu.edu/hbasees/optmod/lasapp.html

[9] Prof. Antonio Aramburu-Zabala. *Tema 8. Semiconductores. Apuntes de la asignatura de Física Cuántica III*. Universidad de Cantabria.

[10] Chow, W., Choquette, K. D., Crawford, M. A., Lear, K. L., & Hadley, G. R. *Design, fabrication, and performance of infrared and visible vertical-cavity surface-emitting lasers*. IEEE Journal of Quantum Electronics, 33(10), 1810-1824. (1997). https://doi.org/10.1109/3.631287

[11] Jewell, J. L., Harbison, J. P., Scherer, A., Lee, Y., & Florez, L. T. *Vertical-cavity surface-emitting lasers: Design, growth, fabrication, characterization*. IEEE Journal of Quantum Electronics, 27(6), 1332-1346. (1991). https://doi.org/10.1109/3.89950

[12] Quirce, A., Valle, A., Pesquera, L., Thienpont, H., & Panajotov, K. *Measurement of Temperature-Dependent Polarization Parameters in Long-Wavelength VCSELs*. IEEE Journal of Selected Topics in Quantum Electronics, 21(6), 636-642. (2015). https://doi.org/10.1109/jstqe.2015.2410260

[13] Quirce, A. & Valle, A. *Random polarization switching in gain-switched VCSELs for quantum random number generation.* Optics Express 30(7) 10513. (2022). http://doi.org/10.1364/oe.446838

[14] Ostermann, J. & Michalzik, R. *Polarization Control of VCSELs.* Springer series in optical science, 147-179. (2013). https://doi.org/10.1007/978-3-642-24986-0_5

[15] *Random Bit Generation.* CSRC. (2022) https://csrc.nist.gov/Projects/Random-Bit-Generation/Documentation-and-Software

[16] Valle-Miñón, M., Quirce, A., Valle, A., & Gutiérrez, J. G. *Quantum random number generator based on polarization switching in gain-switched VCSELs*. Optics continuum, 1(10), 2156. (2022). https://doi.org/10.1364/optcon.464530

[17] S.-H. Kwok, Y.-L. Ee, G. Chew, K. Zheng, K. Khoo, and C.-H. Tan. "A comparison of post-processing techniques for biased random number generators," in IFIP International Workshop on Information Security Theory and Practices, (Springer, 2011).

[18] P. Lacharme. "Post-processing functions for a biased physical random number generator," in International Workshop on Fast Software Encryption, (Springer, 2008).

Apéndice A

Este código, escrito en Python, confecciona una matriz a partir de una secuencia binaria. En primer lugar, el programa recibe el fichero de bits con la función 'open'. Una vez leído, escribe la secuencia como un vector y crea una matriz cuadrada vacía, cuya dimensión (a) depende de la cantidad de bits almacenada en el archivo empleado. Mediante un bucle 'for', se va llenando la matriz con los bits y, finalmente, se usa un comando específico que asigna el color negro a los elementos '0' y el blanco a los '1'.

```
6   import numpy as np
7   import matplotlib.pyplot as plt
8
9   with open("fichero.txt", "r") as datos: #Función para leer el fichero de bits
10      valores = []
11      for linea in datos:
12          valores.append([int(x) for x in linea.strip().split(",")])
13
14  valores = np.asarray(valores) #Hace un vector con la secuencia de bits
15  M = np.zeros((a,a)) #Construye una matriz cuadrada vacía de dimensiones axa
16
17  for i in range (0,a-1): #Se va llenando la matriz con los bits
18      for j in range(0,a-1):
19          M[i,j]=np.int(valores[i+a*j])
20
21  fig1=plt.figure(1)
22  ax1=fig1.add_subplot(111)
23  plt.imshow(M, cmap='Greys') #Asigna el negro al '0' y el blanco al '1'
24  plt.scatter(i, j, s=0.1)
25  plt.show() #Dibuja la matriz
```

Apéndice B

Al igual que el programa del Apéndice A, el siguiente código recibe el fichero de bits y escribe la secuencia binaria en forma de vector. A continuación, agrupa los bits de 16 en 16 y crea una matriz vacía cuya dimensión es el número de bits de la secuencia original del archivo dividido por 16. Con un bucle 'for' se pasa cada grupo de 16 bits de sistema binario a decimal, y dividiendo cada número por 2^{16}, se obtienen números racionales entre cero y uno. Con otro bucle 'for' se almacenan los números racionales i en una variable x, y los números $i+1$ en una variable y. Haciendo uso de la función 'plot', se representa y en función de x; es decir, cada número racional $i+1$ frente a su anterior i.

```
import numpy as np
import matplotlib.pyplot as plt

with open("fichero.txt", "r") as datos: #Función para leer el fichero de bits
    valores = []
    for linea in datos:
        valores.append([int(x) for x in linea.strip().split(",")])

valores = np.asarray(valores) #Hace un vector con la secuencia de bits
final_vector=int(np.floor(np.size(valores)/16)) #Agrupa los bits de 16 en 16
Valores_binarios = np.zeros(final_vector) #Crea una matriz vacía de dimensión
#numero de bits del fichero entre 16

number=0
for i in range(0,final_vector): #Transforma cada grupo de 16 bits en un número
    for j in range(0,15):
        number = number+valores[16*i+j]*2.**(j+1)
    Valores_binarios[i]=number/2**16 #Se divide por 2^16 para obtener números
    #racionales entre 0 y 1
    number=0

x=[]
y=[]
for i in range(0, len(Valores_binarios)-1):
    x.append(Valores_binarios[i]) #Número racional i
    y.append(Valores_binarios[i+1]) #Siguiente número racional i+1

plt.plot(x, y, 'bo', marker = ".", markersize=0.2, color="red")
plt.xlabel('i')
plt.ylabel('i+1')
plt.show() #Dibuja cada número real i+1 frente al número anterior i
```

Apéndice C

Este tercer código sigue los mismos pasos que el programa del Apéndice B para obtener números racionales entre cero y uno. Con estos números i y el comando 'plt.hist', el programa elabora una función de densidad de probabilidad.

```
import numpy as np
import matplotlib.pyplot as plt

with open("fichero.txt", "r") as datos: #Función para leer el fichero de bits
    valores = []
    for linea in datos:
        valores.append([int(x) for x in linea.strip().split(",")])

valores = np.asarray(valores) #Hace un vector con la secuencia de bits
final_vector=int(np.floor(np.size(valores)/16)) #Agrupa los bits de 16 en 16
Valores_binarios = np.zeros(final_vector) #Crea una matriz vacía de dimensión
#numero de bits del fichero entre 16

number=0
for i in range(0,final_vector): #Transforma cada grupo de 16 bits en un número
    for j in range(0,15):
        number = number+valores[16*i+j]*2.**(j+1)
    Valores_binarios[i]=number/2**16 #Se divide por 2^16 para obtener números
    #racionales entre 0 y 1
    number=0

plt.hist(Valores_binarios, bins=50, density = True, rwidth=1, color = "green")
plt.xlabel('i')
plt.ylabel('FDP')
plt.show() #Dibuja la FDP de los números racionales i obtenidos
```