



*Facultad
de
Ciencias*

**SIMULACIÓN DE UN LÁSER DE
SEMICONDUCTOR PARA LA GENERACIÓN
CUÁNTICA DE NÚMEROS ALEATORIOS**
(Simulation of a semiconductor laser for
quantum random number generation)

Trabajo de Fin de Grado
para acceder al

GRADO EN FÍSICA

Autor: Eloy Huidobro Rodríguez

Director: Ángel Alberto Valle Gutiérrez

Septiembre - 2021

A mis padres.

Agradecimientos

Quiero agradecer a mi director de Trabajo de Fin de Grado, Ángel Alberto Valle Gutiérrez, por la ayuda y el apoyo proporcionado.

Resumen

En este trabajo se ha analizado teóricamente la estadística de la fase óptica de la luz emitida por un diodo láser semiconductor sometido a una modulación periódica de la corriente de polarización aplicada. Este sistema constituye un generador de números aleatorios (QRNG) por lo que resulta de vital importancia entender la naturaleza de su aleatoriedad. Para estudiar el sistema se han empleado simulaciones numéricas de las ecuaciones de balance estocásticas (para el campo eléctrico complejo y el número de portadores) que describen el sistema. Las ecuaciones de balance contienen términos de ruido estocástico, por lo que se han resuelto utilizando métodos de integración de ecuaciones diferenciales estocásticas.

En la primera parte del trabajo se ha estudiado la dinámica de encendido del láser, observando la evolución temporal del número de fotones P , el número de electrones N y la fase óptica ϕ .

Posteriormente se ha realizado el análisis estadístico de la fase óptica y se ha demostrado que la fase no es gaussiana en los primeros pasos de la evolución del sistema. Además se ha observado que el tiempo necesario para que la fase sea gaussiana, bajo las condiciones típicas de encendido por ganancia y modulación de onda cuadrada utilizadas para la generación cuántica de números aleatorios, es del orden de los nanosegundos, lo que corresponde al tiempo que requiere el sistema para olvidar la distribución de las condiciones iniciales. Así mismo se ha estudiado el efecto de la corriente de apagado en la varianza de la fase.

Palabras clave: QRNGs, láseres de semiconductor, fase óptica, procesos estocásticos, ecuaciones de balance

Abstract

In this dissertation we have studied optical phase statistics of the light emitted by a semiconductor laser diode when subject to a periodical modulation of the applied bias voltage. This system is considered a quantum random number generator (QRNG) and as such it is of great importance to understand the nature of its randomness. Numerical simulations of the stochastic rate equations for the complex electrical field and carrier number which characterize the system have been used to study the system. Rate equations contain stochastic noise terms, making it necessary to use integration methods of stochastic differential equations to solve them.

In the first part of the work, the dynamics of the system have been analyzed, studying the temporal evolution of the number of photons P , the number of electrons N and the optical phase ϕ .

Subsequently, a statistical analysis of the optical phase has been performed. We have shown that phase diffusion (characterized by the linear dependence of the variance of the phase with time) takes place. It has also been shown that the phase is not distributed as a Gaussian during the first moments of the simulation but it does become Gaussian for times of the order of the nanosecond.

Lastly, we have studied the effect of the off current I_{off} on the variance of the phase.

Key words: QRNGs, semiconductor laser, optical phase, stochastic processes, rate equations

Índice general

1. Generadores cuánticos de números aleatorios (QRNGs)	5
1.1. Tipos de QRNGs	8
1.1.1. Single photon QRNGs	8
1.1.2. Multiphoton QRNGs	10
2. Láseres de semiconductor. Procesos estocásticos	13
2.1. Láseres de semiconductor	13
2.1.1. Principio de operación de un láser de semiconductor	15
2.1.2. Mecanismos de bombeo	16
2.1.3. Ecuaciones de balance	18
2.2. Procesos estocásticos	18
3. Modelo computacional	23
3.1. Ecuaciones de balance	23
3.2. Resolución de las ecuaciones de balance	24
4. Resultados	27
4.1. Dinámica del encendido	27
4.2. Análisis estadístico y difusión de la fase.	30
4.3. Estudio de la varianza en función de la corriente de apagado	32
5. Conclusiones	34
Referencias	36
A. Parámetros empleados en la simulación	38

Capítulo 1

Generadores cuánticos de números aleatorios (QRNGs)

La obtención de números aleatorios es de vital importancia en ciencia e ingeniería, con aplicaciones en criptografía, computación, simulaciones, cristalografía, pruebas industriales e incluso juegos de azar [1].

Históricamente se ha abordado el problema de generar números aleatorios de dos formas: algorítmica (números pseudoaleatorios) y mediante un proceso físico (no determinista) [2].

Antes de proceder a describir los generadores de números aleatorios se debe definir que se entiende por aleatoriedad. Desgraciadamente no hay una definición comúnmente aceptada de números aleatorios [3]. Sin embargo, podemos nombrar una serie de propiedades que son consideradas convenientes para las secuencias aleatorias.

El primer requisito es que la secuencia aleatoria debería ser no determinista. Lógicamente los generadores de números pseudoaleatorios que producen números aleatorios que parecen aleatorios no cumplen este requisito ya que son algoritmos que por definición son deterministas [3].

Por tanto, este requisito obliga al uso de fuentes de entropía físicas. Sin embargo no todas las fuentes de entropía física pueden ser consideradas no deterministas. Podemos distinguir entre fuentes de entropía clásicas y cuánticas. Las primeras son fuentes fundamentalmente deterministas pero que por la extrema complejidad del sistema es prácticamente imposible predecir resultados exactos. Un ejemplo de este tipo de procesos serían las fluctuaciones del valor de la presión de un gas. Estas fluctuaciones suelen ser consideradas como un proceso estocástico debido a su naturaleza colectiva. Debido a la dificultad para resolver las ecuaciones diferenciales y sustituir en la solución general las condiciones iniciales de posiciones y velocidades de todas las partículas del gas es prácticamente imposible predecir el valor exacto

de la presión del gas en un determinado instante de tiempo. No obstante, estas fluctuaciones son fundamentalmente deterministas ya que en principio es posible resolver las correspondientes ecuaciones diferenciales y hallar el valor preciso de la presión del gas en cualquier instante de tiempo [3].

Ejemplos de procesos que son puramente no deterministas son el efecto túnel electrónico a través de una barrera de potencial o la emisión espontánea de un átomo. No se puede hallar el momento de tiempo exacto en el que ocurrirá el efecto túnel a través de la barrera o en el que un átomo emite de forma espontánea un electrón. Lo único que se tiene es una probabilidad de que al medir el proceso se obtendrá un determinado resultado. A este tipo de fuentes de entropía basadas en esta clase de fenómenos se les denomina fuentes cuánticas. Solo se tratará como no deterministas a las fuentes de entropía cuánticas [3].

El segundo requisito es que la fuente de entropía no pueda ser controlada por una tercera persona. Es decir un QRNG debería ser diseñado de tal forma que un rival no podría influenciar los resultados de la medida realizada en el sistema [3].

El tercer requisito es que el proceso físico utilizado en el QRNG debería ser impredecible. Puede resultar un poco extraño e incluso redundante afirmar esto ya que los procesos cuánticos son intrínsecamente impredecibles. Ahora bien existen fenómenos en los que esto no es así. Por ejemplo, si se mide la polarización, con polarizadores alineados en el mismo eje, de dos fotones entrelazados estas medidas están 100 % correlacionadas. Es decir cada fotón puede hallarse aleatoriamente en el canal (+) o (-) del polarizador correspondiente, pero cuando el fotón 1 se encuentra polarizado positivamente el otro fotón también está polarizado positivamente. Estas correlaciones cuánticas podrían ser utilizadas por un adversario para hallar la contraseña secreta, por ello la fuente de entropía cuántica no debe tener correlaciones cuánticas que puedan ser medidas por una tercera persona. [3]

Convendría aclarar también que es lo que se entiende por el término *truly random* (verdaderamente aleatorio) presente en la literatura sobre generadores de números aleatorios. En criptografía normalmente se trabaja con secuencias de bits aleatorios distribuidos de manera uniforme, por lo que muchas veces cuando se habla de verdadera aleatoriedad se hace referencia a una distribución uniforme. No obstante, la mayoría de fuentes físicas de entropía utilizadas para generar señales aleatorias no suelen permitir la obtención directa de secuencias de bits aleatorios distribuidos de manera uniforme ya que las fluctuaciones raramente tienen una función de densidad de probabilidad (PDF) uniforme. Por tanto en el contexto de los generadores de números aleatorios físicos (RNGS) cuando se habla de verdadera aleatoriedad se hace referencia a que no se trata de un sistema pseudoaleatorio, sin importar la forma de la distribución.

Un generador de números pseudoaleatorios (PRNG) es, de forma simplificada, una fórmula matemática que produce una secuencia periódica determinista de números.

Esta secuencia viene completamente determinada por el valor inicial que es llamado *seed* (semilla). A partir de esta definición es obvio que debido al determinismo intrínseco que llevan asociados los PRNGs estos generadores no son aleatorios [2].

También existen los generadores de números aleatorios auténticos (TRNGs). Estos generadores miden un proceso físico que no se puede predecir, o al menos un proceso físico difícil de predecir y usan el resultado para crear una secuencia de números aleatorios. Los TRNGs suelen depender de valores impredecibles a los que puede accederse desde el software del ordenador o crean una secuencia en un dispositivo creado específicamente para ello, que después lo envía al sistema operativo. Al proceso de recoger datos impredecibles se le llama *entropy gathering* (recolección de entropía)[1].

Algunos autores distinguen entre aquellos generadores que usan eventos no deterministas (non physical non deterministic RNGs) y aquellos que sí están basados en efectos físicos no deterministas (physical TRNGs).

Los TRNGs se suelen clasificar en cuatro familias: Noise-based RNGs, Free-running oscillator RNGs, Chaos RNGs, Quantum RNGs (QRNGs). [2]

En este trabajo se ha centrado la atención sobre los QRNGs. ¿Ahora bien pero qué es un QRNG? Un QRNG es un generador de números aleatorios que se fundamenta en procesos cuánticos. Cabría plantearse que realmente todo proceso físico está gobernado por las leyes de la Mecánica Cuántica por lo que todo TRNG podría ser denominado un QRNG. Sin embargo, se suele reservar el nombre QRNG para aquellos generadores que utilizan procesos aleatorios intrínsecamente cuánticos medidos una y otra vez que producen bits aleatorios de tal forma que entre las medidas el sistema haya sido reseteado a las mismas condiciones iniciales. Puede parecer extraño que el mismo sistema físico, con las mismas condiciones y en el que se realiza la medición de la misma manera produzca resultados diferentes, pero esto está permitido según las reglas de la mecánica cuántica. [2]

Los generadores cuánticos de números aleatorios (QRNGs) son una familia de TRNGs en los cuales los datos producidos son resultado de un suceso cuántico. En contraste con otros sistemas físicos en los cuales la incertidumbre es resultado de una falta de conocimiento sobre el sistema, la aleatoriedad en los QRNGs es una parte esencial de la mecánica cuántica.[1]

La aleatoriedad inherente a la mecánica cuántica hace que los sistemas cuánticos sean una fuente perfecta de entropía y por tanto los QRNGs sean considerados la mejor alternativa para producir números realmente aleatorios. [1]

1.1. Tipos de QRNGs

La mayor parte de QRNGs son ópticos, es decir utilizan fotones. Esto se debe a que los fotones son fáciles de crear, manipular o ser detectados.

Entre los distintos tipos de QRNGs ópticos cabe destacar a los single photon QRNGs y a los multiphoton QRNGs. Tanto entre los single photon QRNGs como entre los multiphoton QRNGs existen diferentes modelos.

1.1.1. Single photon QRNGs

Consideremos un tipo de QRNG óptico single photon en el que un fotón circularmente polarizado llega a un *polarizing beam splitter* o PBS (divisor de haz polarizado). Este tipo de QRNGs ópticos suelen denominarse beam splitter QRNGs o QRBGs. El PBS descompone la polarización de la luz incidente y envía la componente lineal horizontal hacia una salida y la componente lineal vertical hacia otra salida (es decir una componente la transmite y la otra la refleja). En las salidas se encuentran detectores que captan el fotón. Un fotón de luz circularmente polarizada tiene la misma cantidad de polarización lineal vertical y horizontal pero como no puede dividirse en dos tiene una probabilidad del 50% de llegar a cada salida. Si se denomina a cada salida como 0 ó 1 se tendría un RNG teóricamente perfecto cuya aleatoriedad está garantizada por las leyes de la Mecánica Cuántica. El sistema que está siendo medido es todo el rato el mismo pero el resultado que arroja cada medición es completamente aleatorio. La Figura 1.1 contiene un esquema de este tipo de QRBG.

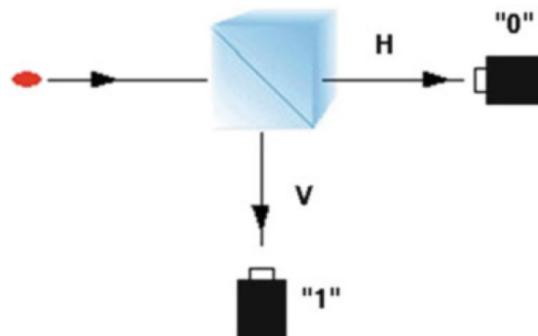


Figura 1.1: QRBG basado en un principio espacial. El fotón circularmente polarizado llega al analizador horizontal/vertical con una probabilidad del 50% de acabar en uno de los dos puertos de salida donde se encuentran los detectores. Figura extraída de la referencia [2]

Por supuesto, este tipo de detectores pueden tener imperfecciones como emisión múltiple de fotones, no tener una polarización circular perfecta, mala alineación del beam splitter, tiempo muerto del detector (tras realizar una medida hay un tiempo en el que el detector no puede realizar otra medida), efectos de memoria... Sin embargo este tipo de imperfecciones pueden ser medidas de forma separada al proceso generación de bits y por tanto su efecto en los números aleatorios puede ser estimado con precisión y tratado en el postprocesado. El mayor problema a la hora de poner en práctica un beam splitting QRNG es que requiere de dos detectores. Las diferencias iniciales entre los detectores y el alejamiento debido al paso del tiempo y/o a efectos térmicos tienen un impacto inmediato en la calidad de los números aleatorios. Si la eficiencia de los detectores no es la misma o si el beam splitter no es 50%/50% la probabilidad de unos no será igual a la probabilidad de ceros. El primer problema puede reducirse utilizando un esquema de QRBG en el que solo se utilizan un detector de fotones. Sin embargo la proporción del beam splitter debe ser ajustada mecánicamente. Por último, los problemas debidos al tiempo muerto del detector o al *afterpulsing* generan correlaciones que no pueden ser eliminadas completamente pero pueden ser reducidas en el postprocesado. [2]. En un detector single-photon ideal se genera un único pulso eléctrico por cada fotón incidente. Sin embargo, en un detector single-photon real puede ocurrir que un único fotón incidente resulta en más de un pulso eléctrico por fotón incidente. Este fenómeno recibe el nombre de *afterpulsing* [4].

Este beam splitter QRNG está basado en un sistema en el que el valor del bit aleatorio, 0 ó 1, viene dado por el lugar en el que acaba el fotón, es decir es un ejemplo de QRNG espacial. Como contraste existen los QRNGs basados en un principio temporal que utilizan información temporal de la emisión aleatoria de fotones.

Un simple método de intervalos de tiempo ha sido propuesto [2]. Los fotones de una fuente Poissoniana que emite fotones individuales llegan a un detector de fotones individuales. Tras tres detecciones de fotones se comparan los intervalos temporales t_1 y t_2 . Si $t_1 > t_2$ se genera un 0, si por el contrario $t_2 > t_1$ se genera un 1 y si $t_1 = t_2$ no se produce nada (es decir se salta). Como se utilizan fotones individuales las correlaciones se ven reducidas a niveles indetectables. El problema de este método tiene que ver con como se miden los intervalos de tiempo. Los relojes que miden los intervalos temporales t_i deben comenzar de forma sincronizada al principio de cada intervalo ya que si no se hiciese así los bits producidos estarían correlacionados aunque fuesen generados a partir de eventos perfectamente aleatorios. [2]. La Figura 1.2 contiene un esquema de este tipo de QRBG.

Otro tipo de single photon QRNG consiste en medir en un intervalo temporal determinado fotones de una fuente que emite fotones individuales. Si el número de fotones medido es par se genera un 0. Si por el contrario es impar se genera un 1.

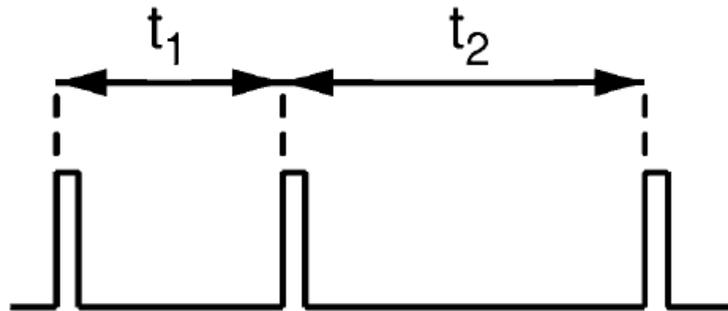


Figura 1.2: QRNG basado en un principio temporal. Los fotones de una fuente Poissoniana que emite un único fotón llegan a un detector de fotones individuales. Los intervalos temporales t_1 y t_2 obtenidos tras tres detecciones de fotones son comparados. Si $t_1 > t_2$ se genera un 0, si por el contrario $t_2 > t_1$ se genera un 1 y si $t_1 = t_2$ no se produce nada (es decir se salta). Figura extraída de la referencia [2]

1.1.2. Multiphoton QRNGs

Por otro lado, además de los single photon QRNGs existen los multiphoton QRNGs. Como ejemplo de este tipo de QRNGs está el QRNG basado en la detección interferométrica de la difusión de la fase en un diodo láser DFB (Distributed Feedback Laser) encendido por ganancia que se ha desarrollado en [5]. El encendido por ganancia a frecuencias de unos pocos GHz produce un tren de pulsos con amplitudes prácticamente iguales y fases aleatorias. Al hacer interferir los pulsos entre sí en un interferómetro Mach-Zender se generan grandes pulsos de amplitud aleatoria que son detectados y digitalizados para producir cadenas de bits aleatorios de alta velocidad. El esquema empleado puede observarse en la figura Figura 1.3.

Otra propuesta de un multiphoton QRNG similar puede encontrarse en [6], donde se ha estudiado la influencia combinada de tres efectos: chirp (el cambio de la frecuencia con el tiempo), jitter (la incertidumbre en el tiempo de encendido de los pulsos generados) y las oscilaciones de relajación. Se ha estudiado como afectan de manera conjunta a la función de densidad de probabilidad (p.d.f.) de los pulsos de interferencia de un láser semiconductor encendido por ganancia.

En este modelo, a diferencia del anterior, la medida de la interferencia de los pulsos del láser se realizaría con un interferómetro de fibra óptica de Michelson. El esquema óptico propuesto puede observarse en la Figura 1.4.

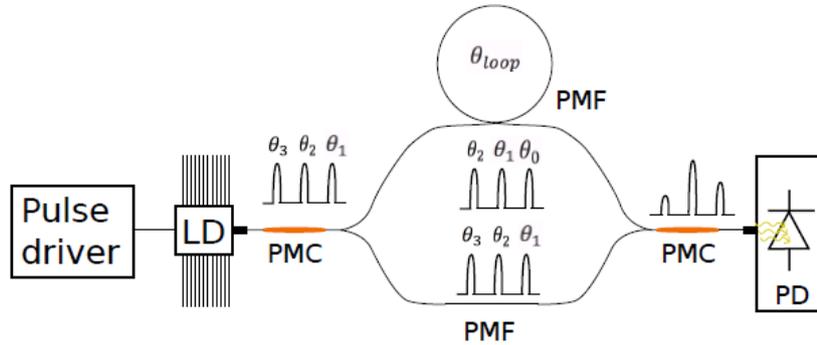


Figura 1.3: Interferómetro Mach-Zender desequilibrado (U-ZMI). Se hace que los pulsos ópticos coherentes con fase aleatoria interfieran en la salida del U-ZMI y generen intensidades aleatorias. Pulse Driver denota el generador de pulsos eléctricos que modula directamente el láser, LD es el diodo láser, PMC el acoplador que mantiene la polarización, PMF la fibra que mantiene la polarización, θ_{0-3} representa las fases ópticas de distintos pulsos consecutivos, θ_{loop} es la fase introducida por el retraso producido por el cable y PD es un fotodetector rápido. Figura extraída de la referencia [5].

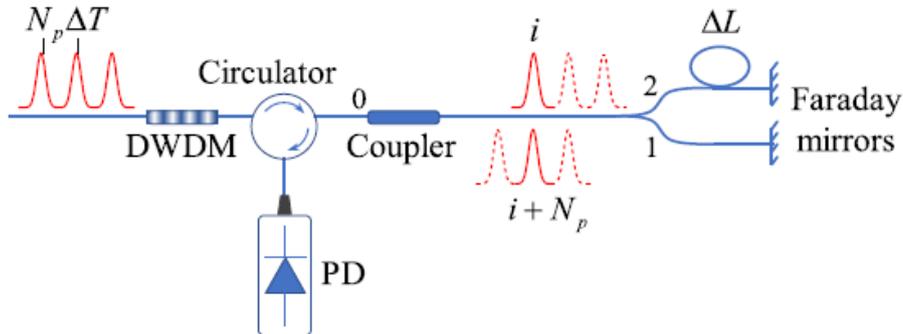


Figura 1.4: Esquema óptico utilizado para observar la interferencia de pulsos láser en [3]. El circulator se utiliza para separar las señales ópticas que viajan en sentidos opuestos y así prevenir feedback no deseado en el láser. PD designa al fotodetector, DWDM es el filtro de paso de banda multiplexado denso por división en longitudes de onda. La longitud de retraso ΔL se ha escogido de tal manera que el correspondiente tiempo de retraso sea un múltiplo del periodo de la repetición del pulso, de tal forma que en el interferómetro se encuentren el pulso i -ésimo y el pulso $i + N_p$ -ésimo, donde N_p es el número de pulsos que pasan por el brazo corto durante el tiempo necesario para que el pulso viaje por el brazo largo. Figura extraída de la referencia [6].

En estos dos ejemplos de multiphoton QRNG es esencial que la frecuencia de los

pulsos coincida con el tiempo que tardan los pulsos en recorrer el camino óptico. De esta forma la interferencia de la fase se produce de la manera deseada para la generación de números aleatorios.

Objetivo

Este trabajo se centra en el análisis estadístico de la fase óptica de un láser de semiconductor. Para ello se van a describir los conceptos teóricos necesarios. Se describirán tanto los láseres de semiconductor como los procesos estocásticos. Tras esto se explicará el modelo que describe la dinámica de este tipo de láseres. Este modelo consiste en un sistema de ecuaciones diferenciales estocásticas que describen la dinámica de los láseres de semiconductor, así como sus fluctuaciones estadísticas. Por tanto es un modelo adecuado para describir el comportamiento de sistemas multiphoton QRNG como los descritos en [5] y [6]. Se resolverán numéricamente estas ecuaciones mediante el algoritmo de Euler. Para ello se propondrá un sistema de ecuaciones de balance equivalente al sistema normalmente empleado (obtenido mediante un cambio de variables) para facilitar la integración numérica. Al obtener la solución del sistema se podrá analizar la fase óptica generada por el sistema estudiado. El objetivo principal de este trabajo es el análisis estadístico de la fase óptica de un láser de semiconductor que podría ser empleado en un multiphoton QRNG.

Capítulo 2

Láseres de semiconductor. Procesos estocásticos

Un amplificador óptico coherente es un aparato que aumenta la amplitud de un campo óptico a la vez que mantiene su fase. [7]. El principio fundamental para conseguir la amplificación coherente de la luz es la amplificación de luz por emisión estimulada de radiación, es decir, un láser.

Un láser consta de un amplificador óptico denominado medio activo (material donde se produce la inversión de población y por tanto donde se producen la mayor parte de emisiones estimuladas que generan la emisión de luz y absorciones) situado en el interior de un resonador óptico (espejos) y un mecanismo de bombeo (que proporciona la energía necesaria). La luz producida es extraída a través de un espejo que transmite de forma parcial.

2.1. Láseres de semiconductor

Se denomina semiconductor a un sólido cristalino o amorfo cuya conductividad eléctrica se encuentra típicamente entre la de un metal y la de un aislante y puede ser modificada de forma significativa cambiando la temperatura o el contenido de impurezas del material [7].

Los semiconductores tienen una serie de propiedades que son únicas en ciertos aspectos:

Un material semiconductor no puede ser visto como una colección de átomos que no interactúan, cada uno con sus niveles de energía individuales. La proximidad de los átomos en un sólido resulta en una colección de niveles de energía conjuntos.

Los niveles de energía de los semiconductores se agrupan en bandas continuas. En ausencia de excitaciones térmicas ($T = 0\text{ K}$) las bandas están completamente ocupadas o completamente vacías. La banda ocupada más alta se denomina banda de valencia y la banda vacía más baja recibe el nombre de banda de conducción. Estas dos bandas están separadas por un gap de energía. Los semiconductores cuentan con un gap de energía o separación entre la banda de valencia y la de conducción. El gap de energía $E_g = E_c - E_v$ en los láseres de semiconductor suele tener valores entre los 0.1 eV y 3 eV. Gracias a este pequeño valor del gap de energía pueden tener lugar saltos de electrones entre las bandas con la intervención de un fotón (solo puede ocurrir si $h\nu > E_g$, donde ν es la frecuencia del fotón y h la constante de Planck) [7].

Las interacciones térmicas y ópticas pueden proporcionar energía al electrón provocando que salte el gap de la banda de valencia a la de conducción, dejando tras de sí un estado vacío llamado hueco. El proceso contrario también puede ocurrir. Un electrón puede decaer de la banda de conducción a la de valencia para ocupar el estado vacío (siempre y cuando sea accesible) mediante un proceso denominado recombinación electrón hueco. Por tanto, se tienen dos tipos partículas que son portadores de carga y pueden interactuar con fotones: los electrones y los huecos [7].

Existen dos procesos fundamentales para el funcionamiento de los dispositivos optoelectrónicos de semiconductor:

La absorción de un fotón puede crear un par electrón-hueco. Los portadores de carga móviles resultantes de la absorción pueden alterar las propiedades eléctricas del material.

La recombinación de un electrón con un hueco puede producir la emisión de un fotón. El fotón emitido de forma espontánea tiene fase y dirección aleatorios. Este proceso es responsable de que comience la emisión láser [7].

Los láseres de semiconductor son una de las clases de láseres más importantes hoy en día por su gran variedad de aplicaciones directas (comunicaciones ópticas, espectroscopía, sensores, impresión) y en especial por su extendido uso como fuente de bombeo para láseres de estado sólido. [8]

El ejemplo más sencillo de un láser de semiconductor consiste en un Fabry-Pérot con una unión p-n como medio activo y dos espejos plano-paralelos con alta reflectividad como resonador óptico.

Los láseres de semiconductor requieren que el medio activo sea un material con gap directo. Esto hace que no se puedan utilizar los elementos semiconductores típicos como Si o Ge. La mayoría de láseres de semiconductor emplean combinaciones de elementos que pertenecen al tercer grupo (III) de la tabla periódica (Al, Ga, In) con elementos del quinto grupo (V) (N, P, As, Sb). Estas combinaciones pueden ser de dos elementos (binarios como el GaAs), tres elementos (ternarios como el AlGaAs)

e incluso cuatro elementos (cuaternarios). También existen láseres de semiconductor formados por combinaciones de elementos del segundo (II) y sexto grupo (VI). [8]

2.1.1. Principio de operación de un láser de semiconductor

Los semiconductores absorben y emiten fotones cuando ocurren transiciones entre diferentes niveles de energía permitidos, de acuerdo con la teoría de interacción de luz-materia. Las tres formas de interacción luz-materia son la emisión espontánea, la emisión estimulada y la absorción, como aparece en la Figura 2.1.

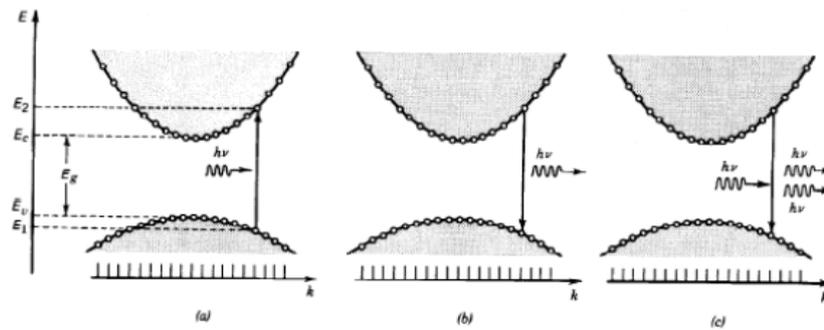


Figura 2.1: La absorción (a), emisión espontánea (b) y emisión estimulada (c) entre los niveles de energía E_2 y E_1 de un semiconductor. Figura extraída de la referencia [7].

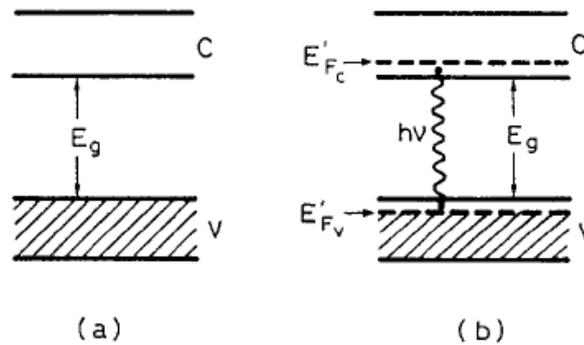


Figura 2.2: Principio de operación de un láser semiconductor. V y C son la banda de valencia y de conducción del semiconductor respectivamente y E_g es el gap de energía que las separa. Figura extraída de la referencia [8].

El esquema básico mediante el cual funciona un láser de semiconductor aparece en

la Figura 2.2. Si por simplicidad se considera que el semiconductor se encuentra a $T = 0\text{ K}$ la banda de valencia estará completamente llena de electrones mientras que la banda de conducción estará completamente vacía. Si se supone que algunos electrones son enviados a la banda de conducción mediante un mecanismo de bombeo apropiado, estos electrones en la banda de conducción tras un tiempo muy corto (del orden de 1 ps) descienden a los niveles más bajos sin ocupar de la banda de conducción. Lo mismo ocurre en la banda de valencia. Aquellos electrones en lo alto de la banda de valencia bajan a los niveles más bajos sin ocupar de esta banda, dejando tras de sí huecos en los niveles altos de la banda de valencia. En esta situación puede darse lugar la emisión de luz cuando un electrón baja de la banda de conducción y se recombina con un hueco de la banda de valencia. Este proceso de emisión de luz se denomina emisión espontánea y los fotones emitidos de esta forma tienen fase y dirección aleatorias.

Sin embargo, dadas las condiciones apropiadas puede ocurrir que esta radiación de recombinación provoque la emisión estimulada, lográndose así la acción láser. La condición para que un fotón sea amplificado en vez de ser absorbido por el semiconductor viene dada por $\nu > \frac{E_g}{h}$ [8]. La emisión estimulada es fundamental para el funcionamiento de los láseres de semiconductor.

En resumen, al incidir luz de frecuencia ν esta puede interactuar con portadores de carga de un material semiconductor mediante transiciones de banda. Los fotones incidentes pueden ser absorbidos, generando pares electrón hueco o pueden producir nuevos fotones mediante emisión estimulada producida por la recombinación de electrón y hueco. Para que la amplificación continúe, debe haber un número suficiente de electrones excitados. [7]

2.1.2. Mecanismos de bombeo

El principio básico para el funcionamiento de un láser de semiconductor es el mismo que para otros láseres: se genera una inversión de población que provoca que haya mucha más emisión estimulada que absorción.

Con el fin de conseguir la inversión de población necesaria para la acción láser se utilizan procesos de bombeo.

El bombeo se realiza típicamente de forma óptica (utilizando la luz continua o pulsada proveniente de un lámpara potente o un haz láser) o eléctrica (bien sea corriente continua, de radiofrecuencia o una corriente pulsada que se desplaza a través de un medio activo como puede ser un gas ionizado o un semiconductor) [8].

En el bombeo óptico mediante una fuente de luz incoherente, la luz de una lámpara potente es absorbida por el medio activo y de este modo los átomos son bombeados

al nivel superior del láser. Si se realiza el bombeo óptico mediante láser se requiere que la longitud de onda del láser caiga dentro de una de las bandas de absorción del medio activo. Una ventaja de la monocromaticidad del láser es que el bombeo láser puede ser empleado no solo para láseres de estado sólido o de líquido sino que puede aplicarse para láseres de gas también. [8]

El bombeo eléctrico suele lograrse mediante una descarga eléctrica lo suficientemente intensa. Este tipo de bombeo es especialmente apropiado para los láseres de gas y los láseres de semiconductor. En el caso de un láser de gas, como sus líneas de absorción son muy estrechas esto dificulta utilizar el bombeo óptico con lámparas. El caso de los láseres de semiconductor es distinto, ya que se podría utilizar el bombeo óptico de forma efectiva porque el medio semiconductor tiene una banda de absorción ancha. De hecho se ha logrado operar varios láseres de semiconductor con bombeo óptico, en particular mediante bombeo láser. Sin embargo, suele ser más útil utilizar bombeo eléctrico en los láseres de semiconductor, ya que se puede hacer fluir una densidad de corriente lo suficientemente grande a través de un semiconductor, normalmente en la forma de un diodo p-n o un diodo p-i-n. [8]

Encendido por ganancia

El encendido por ganancia (Gain-switching) es una técnica mediante la cual se puede lograr que un láser genere pulsos de luz de una duración extremadamente corta, generalmente de unas pocas décimas a unos pocos cientos de nanosegundos. Esta técnica recibe su nombre porque la ganancia láser cambia rápidamente a un valor alto. Esto se logra mediante pulsos de bombeo lo suficientemente rápidos que generan una condición de inversión de población que supera ampliamente el umbral. Con esto se consigue que la ganancia aumente muy por encima del umbral antes de que el número de fotones haya incrementado lo suficiente como para poder agotar la inversión de población. [8]

En un laser semiconductor, como se ha explicado, los pulsos de bombeo vienen típicamente dados por la corriente eléctrica. Estos pulsos permiten obtener la inversión de población y por tanto el encendido por ganancia. Al modular la corriente eléctrica mediante un voltaje de polarización (*bias voltage*) se puede controlar la forma del pulso de bombeo. Así se puede optimizar el pulso de bombeo según convenga. [8] [9].

La inversión de población en láseres semiconductores se suele alcanzar mediante inyección de corriente eléctrica en una unión p-n: el voltaje de polarización provoca que pares de portadores sean inyectados en la región de la unión, donde se recombinan mediante la emisión estimulada. [7]

En los QRNGs ópticos basados en láseres de semiconductor se suele utilizar una corriente inyectada con modulación de onda cuadrada. Esto provoca que durante

cierto tiempo la corriente supere el umbral del láser y por tanto domine la emisión estimulada. Sin embargo, durante el resto del periodo la corriente se encuentra por debajo del umbral de tal manera que domina la emisión espontánea y se tiene una evolución aleatoria de la fase óptica.

2.1.3. Ecuaciones de balance

Para modelar la dinámica de un láser semiconductor se suele utilizar un sistema de ecuaciones no lineales ordinarias, llamadas ecuaciones de balance. Estas ecuaciones diferenciales describen la evolución temporal de las poblaciones de los niveles según la influencia de transiciones (tanto aquellas inducidas de manera óptica como aquellas que no). La forma más simple de las ecuaciones de balance es la siguiente:

$$\begin{cases} \frac{dP}{dt} = a(N - N_t)P - \frac{P}{\tau_c} + \beta N \\ \frac{dN}{dt} = \frac{i}{e} - \frac{N}{\tau} - a(N - N_t)P \end{cases} \quad (2.1)$$

donde P es el número de fotones en el interior del láser, N es el número de electrones en la región activa, a es la ganancia diferencial, N_t es el número de electrones en transparencia (el sistema es denominado transparente cuando tiene lugar tanta emisión estimulada como absorción), τ_c es la vida media del fotón, β es el factor de emisión espontánea, i es la intensidad de corriente que se le proporciona al láser, e es la carga del electrón y τ es el tiempo de vida de los portadores de carga.

Las ecuaciones de balance dan cuenta de la mayor parte de la fenomenología del láser de semiconductor. No se ha encontrado solución analítica de este sistema de ecuaciones de balance debido al término no lineal NP . También cabe destacar como este sencillo modelo refleja el papel esencial que tiene la emisión espontánea. Para ello se considera el término de emisión espontánea βN . Si $\beta = 0$ se tiene una ecuación diferencial homogénea cuya solución es 0 si la condición inicial es de número de fotones nulo. Por lo tanto es fundamental que el término de emisión espontánea sea distinto de cero ($\beta \neq 0$) para poder tener un láser.

2.2. Procesos estocásticos

Los procesos estocásticos pueden ser descritos de forma sencilla como sistemas que evolucionan probabilísticamente en el tiempo. Siendo más precisos son sistemas en los que una cierta variable aleatoria dependiente del tiempo, $X(t)$ existe. Al medir

$X(t)$ para tiempos t_1, t_2, \dots se obtienen los valores x_1, x_2, \dots de $X(t)$. Se asume que existe un conjunto de densidades de probabilidad conjunta

$$p(x_1, t_1; x_2, t_2; \dots) \quad (2.2)$$

que describe el sistema de forma completa. [10]

El ejemplo más conocido de un proceso estocástico es el movimiento Browniano. El movimiento Browniano, investigado sistemáticamente por primera vez por Robert Brown, es el nombre con el que se conoce al movimiento animado e irregular al que se ven sometidos pequeños granos de polen cuando se encuentran suspendidos en agua. Albert Einstein explicó que este movimiento se debe a impactos frecuentes en los granos de polen por las moléculas del líquido que no paran de moverse incesantemente. Además, señaló que el movimiento de estas moléculas es tan complicado que su efecto en los granos de polen solo puede ser descrito probabilísticamente en función de impactos muy frecuentes y estadísticamente independientes [10].

Paul Langevin propuso un nuevo método de describir este fenómeno. La ecuación de Langevin es una ecuación diferencial estocástica (una ecuación diferencial con un término aleatorio X y cuya solución es en cierto sentido, una función aleatoria) que describe el movimiento Browniano. Cada solución de la ecuación de Langevin representa una trayectoria aleatoria diferente y utilizando propiedades de X (su fuerza de fluctuación) se pueden extraer resultados medibles.[10]. Es decir, se puede describir la evolución del sistema utilizando distintas perturbaciones aleatorias y hallando su promedio. Experimentalmente, esto sería similar a repetir el experimento el número suficiente de veces para obtener la distribución de probabilidad del proceso. Se puede demostrar [10] que una forma equivalente de resolver este proceso estocástico es la ecuación de Fokker-Planck. Considerando un movimiento unidimensional esta ecuación se ve reducida a la ecuación de difusión (2.3)

$$\frac{\partial p}{\partial t} = D \frac{\partial^2 p}{\partial x^2} \quad (2.3)$$

que expresa la probabilidad $P = P(x, t)$ de que la partícula se encuentre en una posición x en un tiempo t , donde D es el coeficiente de difusión.

Otros ejemplos de procesos estocásticos son la luz emitida por un láser o por una fuente incoherente (en el cual la aleatoriedad viene dada por la emisión espontánea), el ruido térmico en un circuito debido a la agitación térmica de los portadores de carga (ruido de Johnson-Nyquist) o el ruido en circuitos electrónicos causado por la naturaleza discreta de los portadores de carga (ruido de Shot).

Un proceso estocástico se dice estacionario si cumple que

$$P(x_1, t_1, \dots, x_n, t_n) = P(x_1, t_1 + \epsilon, \dots, x_n, t_n + \epsilon) \quad (2.4)$$

para cualquier ϵ . Es decir, cuando la distribución de probabilidad del sistema no varía para un desplazamiento en el tiempo. Así, la autocorrelación $R(t_1, t_2) = E[X(t_1)X(t_2)] = R_\tau$ depende solo de la diferencia de tiempos $\tau = t_2 - t_1$. En la ecuación (2.4) $E[X(t_1)X(t_2)]$ es el valor medio del producto de $X_1(t)$ y $X_2(t)$ obtenido para distintos resultados del experimento [10] [9].

El espectro de potencia está relacionado con la autocorrelación del proceso $R(\tau)$, mediante el Teorema de Kintchine y la Transformada de Fourier, como se muestra en las ecuaciones (2.5) y (2.6).

$$S(\omega) = \int_{-\infty}^{\infty} R(\tau)e^{-j\omega\tau} d\tau \quad (2.5)$$

$$S(\omega) = \lim_{T \rightarrow \infty} E \left[\frac{1}{2T} \left| \int_{-T}^T X(t)e^{-j\omega t} dt \right|^2 \right] \quad (2.6)$$

Existe un grupo de procesos estocásticos conocido como procesos Markovianos que cuentan con una peculiaridad que los hace especiales. En estos procesos las probabilidades condicionales están determinadas por completo por el conocimiento de las condiciones más recientes. Es decir,

$$p(x_1, t_1; x_2, t_2; \dots \mid y_1, \tau_1; y_2, \tau_2; \dots) = p((x_1, t_1; x_2, t_2; \dots \mid y_1, \tau_1). \quad (2.7)$$

Esto recibe el nombre de suposición de Markov [10].

Se puede demostrar [10] que si un proceso $x(t)$ es Markoviano

$$p(x_1, t_1, x_2, t_2, \dots, x_n, t_n) = p(x_1, t_1 \mid x_2, t_2)p(x_2, t_2 \mid x_3, t_3) \dots p(x_{n-1}, t_{n-1} \mid x_n, t_n)p(x_n, t_n) \quad (2.8)$$

Y las probabilidades condicionales $p(x_1, t_1 \mid x_2, t_2)$ satisfacen la ecuación (2.9), denominada ecuación de Chapman-Kolmogorov:

$$p(x_1, t_1 \mid x_3, t_3) = \int dx_2 p(x_1, t_1 \mid x_2, t_2)p(x_2, t_2 \mid x_3, t_3) \quad (2.9)$$

Derivando la forma diferencial de la ecuación de Chapman-Kolmogorov y asumiendo que unas cantidades en dicha ecuación son nulas la ecuación diferencial de Chapman-Kolmogorov se ve reducida a la ecuación de Fokker Planck:

$$\frac{\partial p(z, t | y, t')}{\partial t} = -\frac{\partial}{\partial z} [A(z, t)p(z, t | y, t')] + \frac{1}{2} \frac{\partial^2}{\partial z^2} [B(z, t)p(z, t | y, t')] \quad (2.10)$$

El proceso descrito por la ecuación de Fokker-Planck (2.10) se conoce matemáticamente como un proceso de difusión. Los términos $A(z, t)$ y $B(z, t)$ son el vector de arrastre y la matriz de difusión respectivamente.

Si se desarrolla la (2.10) imponiendo la condición $p(z, t | y, t) = \delta(z - y)$ y se quiere obtener $p(z, t + \Delta t | y, t) = \delta(z - y)$, se obtiene que si Δt es muy pequeño entonces $Z(t + \Delta t)$ es una gaussiana con media $y(t) + A(y, t)\delta t$ y varianza $B\delta t$, es decir, como aparece reflejado en la ecuación (2.11)

$$Z(t + \delta t) = y(t) + A(y, t)\delta t + \eta(t)\sqrt{\delta t} \quad (2.11)$$

Es decir, el sistema se mueve con un arrastre (drift) sistemático $y(t) + A(y, t)\delta t$ al que se añade una fluctuación gaussiana de varianza $B\delta t$ [10].

Algunos ejemplos de procesos Markovianos son el proceso de Wiener, el proceso de Poisson o el proceso de Ornstein-Uhlenbeck. Si se considera el proceso de Wiener con una sola variable el proceso es simplemente el movimiento Browniano. El proceso de Poisson permite describir la llegada de electrones a un ánodo. El proceso de Ornstein-Uhlenbeck se obtiene añadiendo un término de arrastre lineal al proceso de Wiener.

Las ecuaciones diferenciales estocásticas (SDE) toman la forma de la ecuación de Langevin (2.12)

$$\frac{dx}{dt} = a(x, t) + b(x, t)\xi(t) \quad (2.12)$$

donde $\xi(t)$ es el término aleatorio de fluctuación rápida y muy irregular con $\langle \xi(t) \rangle = 0$ y $\langle \xi(t)\xi(t') \rangle = \delta(t - t')$, donde la notación $\langle \rangle$ representa el promedio sobre las distintas realizaciones del ruido. El término aleatorio recibe el nombre de ruido blanco porque cumple la propiedad de que el espectro de potencia es $S(\omega) = 1$. Se puede demostrar que la ecuación (2.10) y (2.12) son equivalentes, por lo que es equivalente resolver numéricamente (2.10) que integrar numéricamente (2.12). Se obtiene que existe una conexión entre la ecuación de Fokker Planck y las ecuaciones diferenciales estocásticas que hace que sea equivalente resolver numéricamente la

ecuación en derivadas parciales (PDE) que resolver la ecuación diferencial estocástica mediante otro método numérico.

La integración numérica de la ecuación diferencial estocástica (2.12) se ha realizado utilizando el algoritmo de Euler, para lo cual se ha discretizado t , tomando $dt \approx \Delta t$. De esta manera se ha obtenido la siguiente ecuación

$$x(t + \Delta t) = x(t) + a(x, t)\Delta t + \eta(t)\sqrt{\Delta t}, \quad (2.13)$$

donde $\eta(t)$ es una gaussiana. Al ser gaussiano se obtiene que $\eta = \sqrt{V[\eta]}Z + E[\eta] = bZ$, donde los términos $E[\eta] = 0$ y $V[\eta]$ son la media y la varianza, respectivamente, de $\eta(t)$. $Z = N(0, 1)$ es una gaussiana de valor medio $\langle N(0, 1) \rangle = 0$ y desviación estándar $\sigma = 1$. Teniendo en cuenta estos valores y con el cambio de notación $x_i = x(t_i)$ se obtiene la solución mediante el siguiente algoritmo numérico [10]

$$x_{i+1} = x_i + a(x_i, t_i)\Delta t + b(x_i, t_i)Z_i\sqrt{\Delta t} \quad (2.14)$$

Capítulo 3

Modelo computacional

Muchos modelos físicos no pueden ser resueltos de forma analítica. Las simulaciones computacionales permiten obtener más información de estos modelos y los procesos físicos que representan, así como realizar predicciones. En los sistemas QRNG basados en diodos láser monomodo se suele utilizar una corriente de polarización que modula el sistema. Se ha considerado una corriente $I(t)$ de onda cuadrada que en un periodo T tiene $I(t) = I_{on}$ durante medio periodo ($T/2$) e $I(t) = I_{off}$ para el resto del periodo. La modulación se ha realizado de tal manera que $I_{off} < I_{th}$, donde I_{th} es la corriente umbral del láser. De esta manera, al mantener la corriente del láser por debajo del umbral durante un tiempo suficiente se llega a una región en la que la evolución de la fase viene dada por la emisión espontánea y por tanto la dinámica de la fase evoluciona de forma aleatoria.

3.1. Ecuaciones de balance

Se ha modelado la dinámica del láser de semiconductor encendido por ganancia mediante un sistema de ecuaciones de balance estocásticas. Las ecuaciones de balance utilizadas habitualmente incluyen cantidades como la densidad de fotones $P(t)$, la densidad de portadores $N(t)$ y la fase óptica $\phi(t)$ [11] [12] [13]. A continuación se muestra dicho sistema compuesto de las ecuaciones (3.1), (3.2) y (3.3).

$$\frac{dP}{dt} = \frac{G_N(N - N_T)}{1 + \epsilon P} P - \frac{P}{\tau_P} + \beta B N^2 + \sqrt{2\beta B P N} \xi_P \quad (3.1)$$

$$\frac{d\phi}{dt} = \frac{\alpha}{2} \left[G_N(N - N_T) - \frac{1}{\tau_P} \right] P + \sqrt{\frac{\beta B}{2P}} N \xi_\phi \quad (3.2)$$

$$\frac{dN}{dt} = \frac{I}{e} - \frac{N}{\tau_e} - \frac{G_N(N - N_T)P}{1 + \epsilon P}, \quad (3.3)$$

donde en las ecuaciones (3.1), (3.2) y (3.3) $P(t)$ es el número de fotones en el interior del láser, $\phi(t)$ es la fase óptica, $N(t)$ es el número de portadores en la región activa e $I(t)$ es la corriente inyectada. Los parámetros que aparecen en las ecuaciones son los siguientes: G_N es la ganancia diferencial, N_t el número de portadores en transparencia; es decir el número de portadores que es necesario alcanzar para que el número de absorciones sea igual al número de emisiones estimuladas, τ_p es el tiempo de vida del fotón, τ_e es el tiempo de vida de los portadores de carga (electrones), e es la carga del electrón, β la fracción de emisión espontánea acoplada al modo láser y α el factor de ensanchamiento de línea.

Los términos de Langevin ξ_P y ξ_ϕ representan fluctuaciones debidas a la emisión espontánea. Estos términos tienen la propiedad de que $\langle \xi_P \rangle = 0$ y $\langle \xi_\phi \rangle = 0$ y además cumplen la siguiente relación de correlación:

$$\langle \xi_i(t)\xi_j(t') \rangle = \delta_{ij}\delta(t - t'), \quad (3.4)$$

donde $\delta(t)$ es la delta de Dirac y δ_{ij} es la delta de Kronecker, cuyos índices i, j se refieren a las variables P y ϕ .

La intensidad de corriente que aparece en (3.3) representa la corriente de bombeo que se le aplica al láser. Si esta es lo suficientemente grande (supera la corriente umbral) se consigue la inversión de población y por tanto tiene lugar la acción láser (ya que domina la emisión estimulada).

3.2. Resolución de las ecuaciones de balance

Para resolver el sistema de ecuaciones estocásticas se ha utilizado la integración numérica, en concreto el algoritmo de Euler [14], descrito al final del Capítulo 2, (2.14). Al tratar de resolver el sistema formado por (3.1), (3.2) y (3.3) existe un problema cuando el número de fotones es muy bajo. Esto es un suceso muy común en este tipo de QRNGs, ya que como se ha explicado, durante la mitad del periodo se trabaja por debajo del umbral, lo cual implica un número de fotones bajo, de tal forma que domina la emisión espontánea. Al ser el número de fotones bajo, el ruido por emisión espontánea puede causar que P tome valores negativos en la simulación. Esto provoca inestabilidades numéricas debido a los términos en los que P está dentro de una raíz cuadrada que aparece multiplicando al término de ruido de las ecuaciones (3.1), (3.2) del modelo expuesto para describir el láser de semiconductor [11]. La propuesta [15] para resolver este problema computacional

consiste en plantear un sistema de ecuaciones de balance para el campo eléctrico $E(t)$ en vez de para $P(t)$ y $\phi(t)$ que es equivalente al sistema habitual que aparece en (3.1), (3.2) y (3.3). Este nuevo sistema que aparece a continuación en las ecuaciones (3.5) y (3.6) puede ser resuelto sin que aparezcan las inestabilidades que aquejaba el anterior sistema ya que P no aparece dentro de la raíz cuadrada que multiplica al término de ruido.

$$\frac{dE}{dt} = \frac{1}{2} \left[\left(\frac{1}{1 + \epsilon|E|^2} + i\alpha \right) G_N(N - N_T) - (1 + i\alpha) \frac{1}{\tau_p} \right] E + \sqrt{\beta B} N \xi(t) \quad (3.5)$$

$$\frac{dN}{dt} = \frac{I}{e} - \frac{N}{\tau_e} - \frac{G_N(N - N_T)|E|^2}{1 + \epsilon|E|^2} \quad (3.6)$$

El campo eléctrico complejo viene descrito por $E(t) = E_1(t) + iE_2(t)$ y el ruido causado por la emisión espontánea $\xi(t) = \xi_1(t) + i\xi_2(t)$ es un ruido blanco gaussiano que cumple que $\langle \xi \rangle = 0$ y cuya correlación viene dada por $\langle \xi(t)\xi^*(t') \rangle = \delta(t-t')$, donde δ es la función delta de Dirac. Estas nuevas ecuaciones corresponden a las del sistema anterior porque si se aplica el cambio de variable a $P = |E|^2 = E_1^2 + E_2^2$ y a $\phi = \arctan\left(\frac{E_2}{E_1}\right)$ a las ecuaciones (3.5) y (3.6) se obtienen las ecuaciones (3.1), (3.2) y (3.3). [10]

Se ha utilizado el siguiente algoritmo de Euler para resolver este nuevo sistema de ecuaciones:

$$E_1(t + \Delta t) = E_1(t) + \frac{\Delta t}{2} \left[\left(\frac{G_N(N(t) - N_T)}{1 + \epsilon|E|^2(t)} - \frac{1}{\tau_p} \right) E_1(t) - \alpha \left(G_N(N(t) - N_T) - \frac{1}{\tau_p} \right) E_2(t) \right] + \sqrt{\beta B \Delta t} N N_1(0, 1) \quad (3.7)$$

$$E_2(t + \Delta t) = E_2(t) + \frac{\Delta t}{2} \left[\left(\frac{G_N(N(t) - N_T)}{1 + \epsilon|E|^2(t)} - \frac{1}{\tau_p} \right) E_2(t) + \alpha \left(G_N(N(t) - N_T) - \frac{1}{\tau_p} \right) E_1(t) \right] + \sqrt{\beta B \Delta t} N N_2(0, 1) \quad (3.8)$$

$$N(t + \Delta t) = N(t) + \frac{I(t)}{e} \Delta t - \frac{N(t) \Delta t}{\tau_e} - \frac{G_N(N(t) - N_T)|E|^2(t)}{1 + \epsilon|E|^2(t)} \Delta t \quad (3.9)$$

donde $N_1(0, 1)$ y $N_2(0, 1)$ son distribuciones de probabilidad gaussiana de valor medio cero y estadísticamente independientes.

El algoritmo se ha empleado con pasos de integración de 0.001 ps.

En cada paso de integración del algoritmo se calcula la fase. Para ello se emplean los siguientes pasos, con la finalidad de que la fase sea una función continua (debido al uso de la función arcotangente).

Inicialmente se crea una variable denominada contador de la fase $cfase = 0$. Se considera Δt como paso de integración. El campo complejo en un instante t es $E(t) = E_1(t) + iE_2(t)$ y en un instante $t + \Delta t$ es $E(t + \Delta t) = E_1(t + \Delta t) + iE_2(t + \Delta t)$. Se definen unas variables auxiliares $X = E_1(t)E_1(t + \Delta t)$, $Y = E_2(t)E_1(t)$. Con estas variables definidas de esta manera se puede comprobar si la fase ha cambiado de cuadrante en función de lo que valgan las variables auxiliares. Si $X < 0$ ha tenido lugar un cambio de cuadrante (del 1 al 2 o del 3 al 4, y viceversa). Considerando $X < 0$ e $Y \geq 0$, en el tiempo t la fase se encontraba en los cuadrantes 1 ó 3 y por tanto se le suma π a $cfase$, $cfase = cfase + \pi$. Considerando $X < 0$ e $Y \leq 0$, en el tiempo t la fase encuentra en el cuadrante 2 ó 4 y por tanto se le resta π a $cfase$, $cfase = cfase - \pi$. Si $X \geq 0$ no ha tenido lugar ningún cambio de cuadrante y no es necesario realizar ninguna operación.

Teniendo en cuenta estas consideraciones se ha calculado la fase en cada paso de integración a través de la siguiente ecuación

$$\phi(t + \Delta t) = \arctan \left(\frac{E_2(t + \Delta t)}{E_1(t + \Delta t)} \right) + cfase \quad (3.10)$$

En la simulación se han empleado los valores numéricos de los parámetros del láser que se han obtenido para un láser semiconductor de modo discreto (DML). [15] [16]. Este es un láser semiconductor de un solo modo longitudinal que emite a una longitud de onda cercana a 1550 nm, con una intensidad de corriente umbral $I_{th} = 14.14$ mA a una temperatura de 25 °C. Los valores de los parámetros aparecen en el Apéndice A.

Cabe destacar que los resultados experimentales y los de la simulación muestran no solo un acuerdo cualitativo sino uno cuantitativo para un amplio abanico de condiciones de encendido por ganancia [11] [15] [16].

Capítulo 4

Resultados

4.1. Dinámica del encendido

Se ha analizado la evolución dinámica de las variables P (número de fotones), N (número de electrones) y ϕ (fase óptica) cuando el láser está modulado con la corriente de encendido $I_{on} = 30 \text{ mA}$, la corriente de apagado $I_{off} = 7 \text{ mA}$ con periodo $T = 1 \text{ ns}$.

Se ha representado el número de fotones P (en escala logarítmica para apreciar las fluctuaciones debidas a la emisión espontánea) y el número de portadores de carga N en función del tiempo t de 0 ns a 3 ns en la Figura 4.1. En esta figura puede observar tanto el régimen transitorio como el estacionario para P y N . Se han podido observar las oscilaciones de relajación. Al aplicar una corriente constante al láser el número de portadores aumenta. Al llegar al valor umbral para el número de portadores, N_{th} , tienen lugar emisiones estimuladas, aumentando así el número de fotones y disminuyendo el de portadores. Al seguir aplicando una corriente por encima del umbral se repite este proceso y tanto P como N presentan unas oscilaciones amortiguadas en el tiempo, denominadas oscilaciones de relajación. Estas oscilaciones de relajación son parte del comportamiento transitorio del láser. Tras un determinado tiempo estas oscilaciones se atenúan y se alcanza el equilibrio para P y N , dando paso así a un estado estacionario. Se ha estimado la frecuencia de las oscilaciones de relajación, cuya expresión teórica viene dada por [13]

$$\nu_R = \frac{1}{2\pi} \sqrt{\frac{G_N P}{\tau_p}} = \frac{1}{2\pi} \sqrt{\frac{G_N}{e}} (i - i_{th}). \quad (4.1)$$

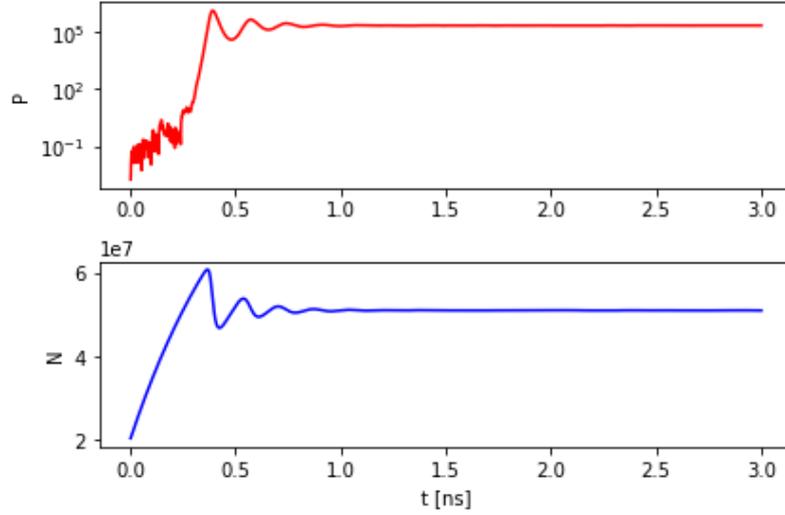


Figura 4.1: Número de fotones P (en escala logarítmica) y número de portadores de carga N en función del tiempo t de 0 ns 3 ns. La intensidad de corriente en esta figura es I_{on} de 0 ns 3 ns.

Se ha utilizado el valor de $I_{th} = 14.14$ mA para realizar la estimación, así como los valores de los parámetros que aparecen en el Apéndice, extraídos de [15] y [16].

El valor estimado de la frecuencia de las oscilaciones de relajación a partir del periodo es $\nu_R = \frac{1}{T_R} \approx \frac{1}{0.1725 \text{ ns}} \approx 5.80 \text{ GHz}$. El valor teórico es $\nu_R = \frac{1}{2\pi} \sqrt{\frac{1,48 \cdot 10^4}{1.6 \times 10^{-19} \text{ C}} (30 - 14,14) \text{ mA}} \approx 6.10 \text{ GHz}$, por lo que se observa un acuerdo bastante bueno entre el valor estimado a partir de la simulación y el valor calculado teóricamente.

Se ha observado también en la Figura 4.1 como se alcanza el estado estacionario correspondiente a I_{on} (para $t \approx 1$ ns) tras las oscilaciones de relajación.

Se ha representado la dinámica del sistema a lo largo de 3 periodos de modulación en la Figura 4.2, es decir, P , N y ϕ en función del tiempo con 3 periodos de modulación, de 1 ns a 4 ns. Se han considerado los valores de la corriente de apagado $I_{off} = 7$ mA, de la corriente de encendido $I_{on} = 30$ mA y un periodo de modulación de $T = 1$ ns.

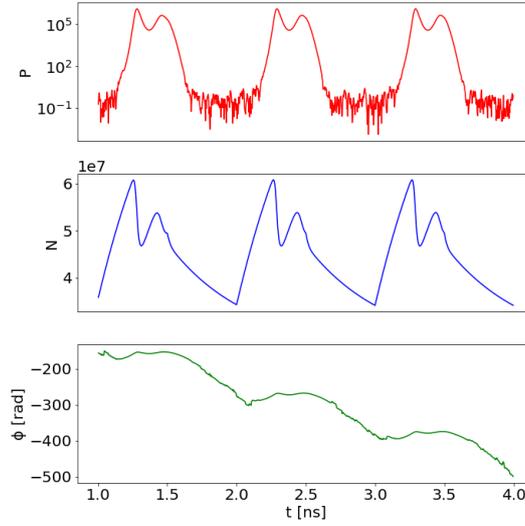


Figura 4.2: Número de fotones P , número de portadores de carga N y fase ϕ en función del tiempo t de 1 ns a 4 ns.

Se han representado tres pulsos para reflejar la dinámica del sistema a lo largo de 1 periodo de modulación en la Figura 4.3. Para representar la fase, (debido al carácter cíclico de los ángulos) se ha exigido que la fase al inicio del periodo, $\phi(0)$ sea la del periodo anterior $\phi(T)$ pero convertida al intervalo $[0, 2\pi)$. Para ello se ha utilizado la expresión $\phi(0) = \phi(T) - \text{int} \left(\frac{\phi(T)}{2\pi} \right) 2\pi$ [17].

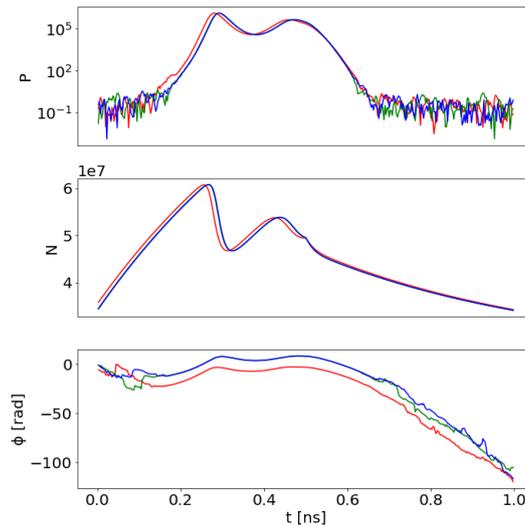


Figura 4.3: Número de fotones P , número de portadores de carga N y fase ϕ en función del tiempo t con 1 periodo de modulación.

4.2. Análisis estadístico y difusión de la fase.

Se han calculado y representado en la Figura 4.4 los momentos de la fase en función de t con el fin de obtener información sobre la difusión de la fase. Se ha representado el valor medio, la varianza, el coeficiente de asimetría y el coeficiente de kurtosis. Para una variable aleatoria x con función de distribución $f(X)$, el valor medio de una variable aleatoria es su primer momento y da una idea de la tendencia central de dicha variable aleatoria. Se define como $\mu = E[x] = \int_{-\infty}^{\infty} xf(x)dx$. La varianza es una medida de la dispersión, es decir, como de alejados están los valores de su valor medio. Se define como $V[x] = E[x^2] - E[x]^2$. El coeficiente de asimetría es el tercer momento estandarizado e indica si una variable está distribuida de forma simétrica alrededor de su valor medio. Una distribución torcida a la izquierda tendrá un valor negativo del coeficiente de asimetría. Se define como $\gamma_r = E\left[\left(\frac{X - \mu}{\sigma}\right)^3\right] = \frac{\mu_3}{\sigma^3}$, donde μ_3 representa el tercer momento, es decir, $\mu_3 = E[x^3] = \int_{-\infty}^{\infty} x^3 f(x)dx$. El coeficiente de kurtosis es el cuarto momento estandarizado y al igual que el coeficiente de asimetría da una idea de la forma de la distribución de probabilidad. En este caso este coeficiente indica el peso de la cola de la distribución comparada con la distribución normal con la misma varianza. Se define como $\kappa_r = E\left[\left(\frac{X - \mu}{\sigma}\right)^4\right] = \frac{\mu_4}{\sigma^4}$, donde μ_4 representa el cuarto momento, es decir, $\mu_4 = E[x^4] = \int_{-\infty}^{\infty} x^4 f(x)dx$. Un coeficiente de kurtosis nulo significa que la variable aleatoria es gaussiana.

Teniendo en cuenta el coeficiente de asimetría y el de kurtosis, para tener una distribución gaussiana de la fase ambos coeficientes deben hacerse cero. [17]

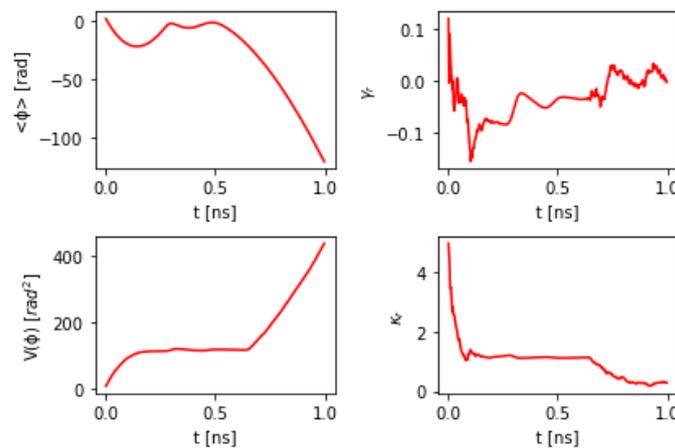


Figura 4.4: Momentos de la fase (valor medio $\langle \phi \rangle$, varianza $V(\phi)$, asimetría γ_r y kurtosis κ_r) en función del tiempo t .

En la varianza de la fase se puede apreciar dos zonas de difusión de la fase, es decir zonas en las que la varianza varía apreciablemente. Estos dos tramos son un tramo pequeño al principio del intervalo de tiempo y otro que comienza a partir de la mitad del intervalo. Estos tramos son de difusión porque la varianza crece linealmente con el tiempo. [17]

Se ha obtenido la función de distribución de probabilidad (p.d.f.) de la fase tanto al principio ($t = 0$ ns) como al final del periodo ($t = 1$ ns). Se han representado estas p.d.f en la Figura 4.5. Para obtener la p.d.f en $t = 0$ ns se ha exigido que la fase al inicio del periodo, $\phi(0)$ sea la del periodo anterior $\phi(T)$ pero convertida al intervalo $[0, 2\pi)$. Para ello se ha utilizado la expresión $\phi(0) = \phi(T) - \text{int}\left(\frac{\phi(T)}{2\pi}\right)2\pi$ [17].

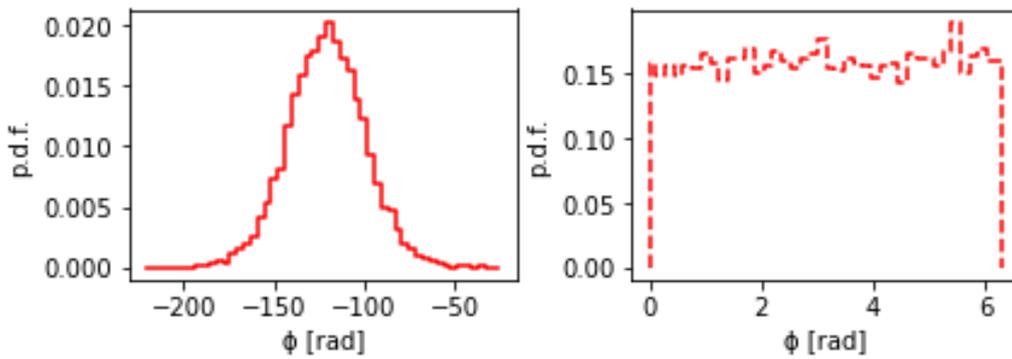


Figura 4.5: Función de densidad de probabilidad de la fase ϕ (p.d.f.) en $t = 1$ ns y en $t = 0$ ns.

Como se puede observar en la Figura 4.5 la función de densidad de probabilidad de la fase se vuelve gaussiana para tiempos grandes (de la escala de los nanosegundos) porque la influencia que podían tener la distribución de las condiciones iniciales se ha desvanecido. Además, en la Figura 4.4 se observa como el coeficiente de kurtosis κ_r tiende a cero según el tiempo aumenta. En esta figura también se puede ver como el tiempo necesario para que llegue a un valor cercano a cero es ligeramente inferior a 1 ns. Combinando la información de la p.d.f. y la del coeficiente de kurtosis se puede afirmar que el tiempo necesario para que la fase adopte una distribución gussiana es del orden del nanosegundo.

4.3. Estudio de la varianza en función de la corriente de apagado

Por último se ha estudiado como cambia la varianza de la fase $V[\phi]$ en función de la corriente de apagado. Se ha representado $V[\phi]$ para distintas corrientes de apagado I_{off} en la Figura 4.6. Se puede observar como la pendiente de $V[\phi]$ en la zona de difusión de la fase es mayor cuanto menor es I_{off} y como la pendiente de $V[\phi]$ es menos pronunciada para valores mayores de I_{off} .

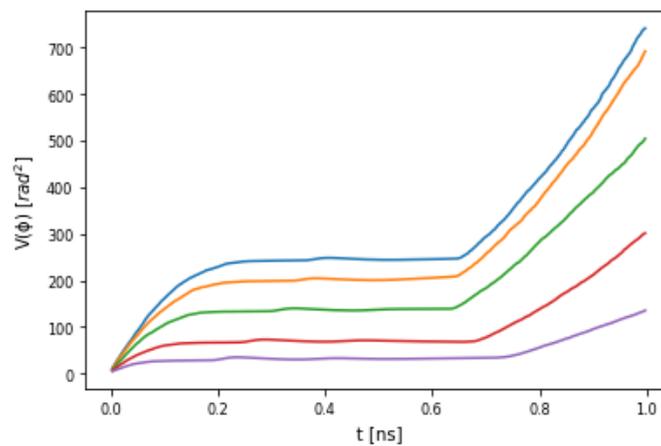


Figura 4.6: Varianza de la fase $V[\phi]$ en función del tiempo t para distintas corrientes de apagado $I_{off} = 1 \text{ mA}$ (azul), 3 mA (amarillo), 6 mA (verde), 9 mA (rojo), 12 mA (morado).

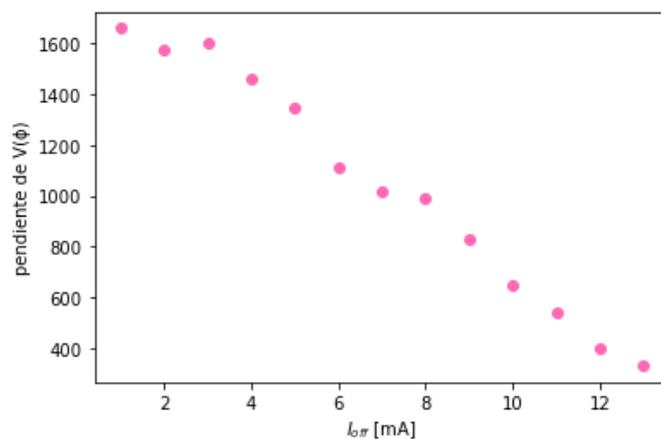


Figura 4.7: Pendientes de la varianza de la fase $V[\phi]$ en función de las corrientes de apagado I_{off} .

Se ha calculado la pendiente de las rectas en la zona de difusión de fase (cuando la varianza deja de ser constante y comienza a crecer de forma lineal con el tiempo) para distintas corrientes de apagado I_{off} y se han representado las pendientes de $V[\phi]$ en función de I_{off} en la Figura 4.7.

En la Figura 4.7 se ha observado que parece haber una relación lineal entre $I_{off} = 3 \text{ mA}$ e $I_{off} = 13 \text{ mA}$. Se ha realizado un ajuste lineal y se ha obtenido que la pendiente tiene el valor $pte = -1.25 \times 10^{14} \text{ rad}^2\text{C}^{-1}$.

Capítulo 5

Conclusiones

Se ha podido estudiar las características del encendido y la difusión de la fase de un generador de números aleatorios basado en un diodo láser semiconductor sometido a una modulación periódica de la corriente de polarización aplicada.

Cabe destacar que la simulación se ha realizado integrando numéricamente las ecuaciones diferenciales estocásticas para el campo eléctrico complejo y el número de portadores en vez de las habituales para el número de fotones, el número de portadores y la fase óptica. Esto ha permitido solventar el problema que suponía el hecho de que P pudiese tomar valores negativos por el ruido por emisión espontánea en la simulación (por estar dentro de raíces cuadradas). Esta solución al problema es más rigurosa que otros arreglos propuestos con anterioridad como tomar el valor absoluto de P , $|P|$ [9], que proporcionaba resultados adecuados en el contexto empleado ya que la corriente no se encontraba por debajo del umbral. Sin embargo este arreglo no podía ser utilizado en la simulación de generadores cuánticos de números aleatorios por lo que esta nueva solución resulta muy útil.

En resumen, se ha analizado de forma teórica la estadística de la fase en un láser semiconductor encendido por ganancia llevando a cabo simulaciones numéricas de las ecuaciones de balance estocásticas.

Como resultados importantes del análisis estadístico de la fase hay que resaltar que se ha observado la difusión de la fase (caracterizada por una variación lineal de la varianza con el tiempo), se ha obtenido la dependencia temporal de los distintos momentos de la fase y se ha demostrado que la función de densidad de probabilidad de la fase es gaussiana solo cuando la memoria de la distribución estadística de las condiciones iniciales se ha desvanecido. Así mismo se ha demostrado que el tiempo necesario para que ocurra esto en un láser semiconductor encendido por ganancia con modulación de onda cuadrada típicamente utilizada en QRNGs, es del orden de los nanosegundos. Para obtener esta información se ha estudiado la dependencia temporal del coeficiente de kurtosis, así como la función de densidad de probabilidad.

Por último hay que mencionar la relación lineal que sigue la pendiente de la varianza con la intensidad de corriente de apagado en un determinado rango de corrientes de apagado (de 3 mA a 13 mA).

Referencias

1. Herrero-Collantes, M. y Garcia-Escartin, J. C. Quantum random number generators. *Reviews of Modern Physics* **89**. ISSN: 1539-0756. <http://dx.doi.org/10.1103/RevModPhys.89.015004> (2017).
2. Stipčević, M. y Koç, Ç. K. en *Open Problems in Mathematics and Computational Science* 275-315 (Springer International Publishing, 2014).
3. Shakhovoy, R., Sych, D., Sharoglazova, V., Udaltsov, A., Fedorov, A. y Kurochkin, Y. Quantum noise extraction from the interference of laser pulses in an optical quantum random number generator. *Opt. Express* **28**, 6209-6224. <http://www.opticsexpress.org/abstract.cfm?URI=oe-28-5-6209> (2020).
4. Waris Ziarkash, A., Koduru Joshi, S., Stipčević, M. y Ursin, R. Comparative study of afterpulsing behavior and models in single photon counting avalanche photo diode detectors. *Sci Rep* **5076** (2018).
5. Abellán, C., Amaya, W., Jofre, M., Curty, M., Acín, A., Capmany, J., Pruneri, V. y Mitchell, M. W. Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode. *Opt. Express* **22**, 1645-1654. <http://www.opticsexpress.org/abstract.cfm?URI=oe-22-2-1645> (2014).
6. Shakhovoy, R., Sharoglazova, V., Udaltsov, A., Duplinskiy, A., Kurochkin, V. y Kurochkin, Y. Influence of Chirp, Jitter, and Relaxation Oscillations on Probabilistic Properties of Laser Pulse Interference. *IEEE Journal of Quantum Electronics* **57**, 1-7 (2021).
7. Saleh, B. E. A. y Teich, M. *Fundamentals of Photonics* (John Wiley & Sons Inc, 2019).
8. Svelto, O. *Principles of lasers* (Springer, 2009).
9. Díez González-Pardo, J. *Simulación de peines de frecuencia óptica generados por láseres de semiconductor* Trabajo de Fin de Grado. 2019.
10. Gardiner, C. W. *Handbook of Stochastic Methods: for Physics, Chemistry and the Natural Sciences* (Springer, 2004).
11. Quirce, A., Rosado, A., Díez, J., Valle, A., Pérez-Serrano, A., Tijero, J.-M. G., Pesquera, L. y Esquivias, I. Nonlinear Dynamics Induced by Optical Injection in Optical Frequency Combs Generated by Gain-Switching of Laser Diodes. *IEEE Photonics Journal* **12**, 1-14 (2020).

12. Schunk, N. y Petermann, K. Noise analysis of injection-locked semiconductor injection lasers. *IEEE Journal of Quantum Electronics* **22**, 642-650 (1986).
13. Larry A. Coldren Scott W. Corzine, M. L. M. *Diode Lasers and Photonic Integrated Circuits* (John Wiley & Sons, Inc., 2012).
14. Risken, H. *The Fokker-Planck Equation* (Springer, 1996).
15. Quirce, A. y Valle, A. Spontaneous emission rate in gain-switched laser diodes for quantum random number generation. *preprint* (2021).
16. Rosado, A., Pérez-Serrano, A., Tijero, J. M. G., Valle, Á., Pesquera, L. y Esquivias, I. Numerical and Experimental Analysis of Optical Frequency Comb Generation in Gain-Switched Semiconductor Lasers. *IEEE Journal of Quantum Electronics* **55**, 1-12 (2019).
17. Valle, A. Statistics of the Optical Phase of a Gain-Switched Semiconductor Laser for Fast Quantum Randomness Generation. *Photonics* **8,9,388**. ISSN: 2304-6732. <https://www.mdpi.com/2304-6732/8/9/388> (2021).

Apéndice A

Parámetros empleados en la simulación

En la simulación se han utilizado los valores que aparecen en la Tabla A.

Símbolo	Valor	Unidades
G_N	$1,48 \cdot 10^4$	s^{-1}
N_t	$1,93 \cdot 10^7$	-
ϵ	$7,73 \cdot 10^{-8}$	-
τ_P	$2,17 \cdot 10^{-12}$	s
α	3	-
β	$5,3 \cdot 10^{-6}$	-
τ_e	$0,57 \cdot 10^{-9}$	s
B	9,8	s^{-1}

Tabla A.1: Parámetros utilizados en la simulación