Universidad Autónoma de Baja California

Facultad de Ingeniería, Arquitectura y Diseño

Maestría y Doctorado en Ciencias e Ingenierîa

Sincronización de Láseres

TESIS

que para cubrir parcialmente los requisitos necesarios para obtener el grado de

MAESTRO EN INGENIERIA

Presenta

ALEJANDRO AGUILAR YAÑEZ

Ensenada, Baja California, Junio del 2014.

UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE INGENIERÍA, ARQUITECTURA Y DISEÑO

Sincronización de láseres

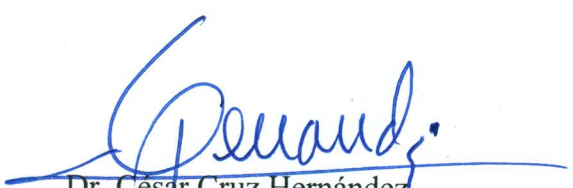
TESIS

Que para obtener el grado de maestría en ingeniería presenta:

Alejandro Aguilar Yáñez

Aprobada por:

Dra. Rosa Martha López Gutiérrez
Director de tesis



Dr. César Cruz Hernández
Miembro del comité

Dra. Liliana Cardoza Avendaño
Miembro del comité

Ensenada Baja California, México. Junio 2014

Resumen de la tesis de Alejandro Aguilar Yáñez, presentada como requisito parcial para la obtención del grado de MAESTRO EN INGENIERÍA. Ensenada Baja California México, Junio del 2014.

SINCRONIZACIÓN DE LÁSERES

Director de Tesis: Dra. Rosa Martha López Gutiérrez

El presente trabajo de investigación versa sobre la sincronización de láseres en régimen caótico. Se incluyen ejemplos de sistemas caóticos representados por ecuaciones diferenciales, los cuales son resueltos mediante el método del diseño de un observador mediante formas hamiltonianas. Esta metodología nos permite sincronizar los láseres utilizando solo una variable, esto se debe a que en los láseres experimentalmente solo tenemos acceso a la intensidad del campo eléctrico.

se definen los láseres y el amplificador EDFA, se da una introducción sobre su historia y su relación con la tecnología. Se definen los diferentes tipos de láseres que existen y se estudia la relación entre los láseres y el caos.
Principalmente se consideran dos sistemas de láser: El láser semiconductor y el láser EDFRL (Erbium Doped Fiber Ring Laser). Se analizan los modelos, se desglosa cada elemento de las ecuaciones diferenciales y se estudia su dinámica dentro del sistema.

Finalmente se presenta el desarrollo de la sincronización de un láser semiconductor y un láser EDFRL. Se proporcionan los resultados obtenidos mediante gráficas y la solución de los sistemas caóticos que modelan su comportamiento.

Palabras clave: Láser, semiconductor, EDFRL, sistemas caóticos, sincronización, formas hamiltonianas, caos.

Agradecimientos

A la Dra. Rosa Martha López Gutiérrez y al Dr Cesar Cruz Hernández, que gracias a su apoyo paciencia y comprensión me fue posible el desarrollo esta tesis. No solo me compartieron su conocimiento, también me brindaron su amistad.

A mis padres Jose Manuel Aguilar Camacho y Maria Elena Yáñez Espino, que gracias a su apoyo incondicional nunca me falto nada en la vida.

A mi Hermano Jose Manuel Aguilar Yáñez, que sin su ejemplo no sería la persona que ahora soy.

A mi novia Karla Gallegos Quintero, por todo mi tiempo que le robé durante la realización de esta tesis.

Índice general

Índice de figuras

Capítulo 1

Introducción

1.1. Motivación

Las comunicaciones seguras han sido necesarias desde los inicios de la humanidad, el transmitir información de manera segura y confidencial se ha convertido más allá de un lujo en una necesidad. Hace miles de años atrás, con los inicios de la criptografía se dieron los primeros intentos de comunicaciones seguras, las cuales han ido evolucionando desde el simple uso del papel y el lápiz, hasta algoritmos complejos por medio de computadoras y software.

Debido al inmenso crecimiento tecnológico, la velocidad de cálculo de las computadoras modernas es cada vez mas rápida y precisa, por lo que se pone en riesgo la seguridad de los sistemas actuales de encriptado. Por esta razón, se han ido buscando algoritmos alternos que puedan soportar los ataques de las computadoras mas avanzadas y una de las grandes propuestas como solución a este problema son los algoritmos caóticos, que a raíz de la sincronización de este tipo de sistemas [Pecora y Carrol 1990] se desprendió una amplia gama de posibilidades para el uso de los sistemas caóticos dentro de las comunicaciones seguras.

Con el crecimiento de la población, la exigencia en las tasas de transmisión y el ancho de banda ha ido aumentando de manera prácticamente exponencial, hoy en día casi todos los sistemas de comunicaciones son por medio de comunicaciones ópticas y es aquí en donde entran los láseres. Con estos sistemas podemos alcanzar velocidades de hasta 10 GBit/s y una gran flexibilidad de transmisión y modulación. Por los motivos mencionados anteriormente es que esta tesis se centra en la sincronización de láseres caóticos, dando el enfoque aplicado a las comunicaciones seguras, proporcionando así una aportación mas dentro de esta área de investigación.

1.2. Planteamiento del problema de estudio

En la actualidad es de lo más normal el uso de las comunicaciones en nuestras vidas cotidianas, las utilizamos en nuestro entretenimiento, en los negocios, en las relaciones sociales y personales, e inclusive para fines militares. El tener información significa tener poder, y es por ello que el dar una mayor seguridad a nuestra información se convierte en un tema de suma importancia y de interés.

Actualmente el algoritmo de cifrado AES es el que domina las aplicaciones en cuestión a seguridad, sin embargo tiene un tiempo determinado de vida útil. Se estima que en no más de 10 años la seguridad del algoritmo AES sea fuertemente vulnerable y a pesar de que aún no se han detectado ataques que rompan totalmente el algoritmo, si se han presentado avances y ataques que cuestionan la seguridad del mismo. Un ejemplo muy reciente de esto es el artículo Biclique Cryptanalysis of the Full AES presentado en la Crypto 2011 cryptology conference el 16 de agosto del 2011 en Santa Barbara California, donde se muestra una técnica que permite obtener las claves secretas del algoritmo AES hasta 5

veces más rápido que con un ataque de fuerza bruta. A pesar de estos ataques no se cuestiona totalmente la seguridad del algoritmo AES, sin embargo es solo cuestión de tiempo el desarrollo de las técnicas y la ruptura del algoritmo en un futuro. Ante esta situación, se está trabajando en distintas propuestas para sustituir al cifrado AES y una de las alternativas para un nuevo algoritmo de cifrado es la teoría del caos, es por ello que sin dejar a un lado las tecnologías actuales, se pretende reforzar la seguridad en las comunicaciones utilizando los sistemas caóticos. Como la tendencia de esta área es trabajar en dominios ópticos empleamos el uso de láseres como semiconductor o EDFA para lograr comunicaciones seguras.

Se considera la siguiente situación: Alicia (transmisor) desea mandar un mensaje a Bob (receptor) a través de un canal público, el cual es observado por Eva (intruso). Si Alicia no quiere que su mensaje sea leído por ninguna otra persona que no sea Bob (como por ejemplo Eva) tendrá que enviar su mensaje encriptado utilizando una clave, la cual solo la deberá de conocer Bob, de esta manera Bob sera la única persona habilitada para desencriptar la información (Fig 1.1) [Lomonaco samuel 2001].

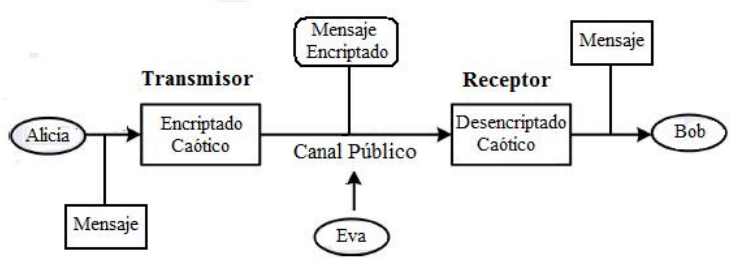


Figura 1.1: Proceso de transmisión de un mensaje encriptado mediante un canal inseguro.

En el diseño de un sistema criptográfico, los algoritmos de encriptación deben tener la propiedad de que los datos originales deben ser recuperados a partir de los datos encriptados o criptogramas, esto si el valor de la clave utilizada es conocido. La clave se debe mantener en secreto a pesar de dar a conocer el texto cifrado como información pública. La fortaleza de un criptosistema es medida por la dificultad para determinar dicha clave.

Los sistemas caóticos han sido desarrollados con gran interés en las comunicaciones a través de la teoría del caos, la cual por medio de un sistema dinámico no lineal y a partir de ciertas condiciones iniciales puede tener resultados prácticamente impredecibles. Debido a las características de las señales caóticas se despertó un fuerte interés en la aplicación de la dinámica caótica dentro de las comunicaciones seguras. En los sistemas caóticos se cumplen ciertas propiedades interesantes que ayudan a generar características de confusión y difusión requeridas para sistemas criptográficos. La no linealidad, su aparente comportamiento aleatorio, su espectro de banda ancha, su ergodicidad y sensibilidad a condiciones iniciales son unas de las principales características que colocan de manera ideal a los sistemas caóticos como solución a la transmisión segura de información.

El uso de los láseres con dinámicas caóticas dentro de las comunicaciones seguras tiene grandes ventajas, que como ya se ah mencionado podemos alcanzar velocidades de hasta 10 GBit/s y una gran flexibilidad de transmisión y modulación. En un láser podemos lograr que la intensidad de la luz emitida comience a variar de forma irregular, caótica, casi errática, por lo que el láser emitirá luz compleja. Aunque nosotros no lo notemos a simple vista, porque estos cambios de intensidad ocurren a escalas de mil-millonésimas de segundo, los efectos pueden ser devastadores en ciertas aplicaciones, como por ejemplo, en los sistemas de comunicaciones ópticas. En la presente tesis se plantea el sincronizar

dos láseres EDFA mediante el uso de hamiltonianos y diseño de un observador, metodología propuesta en [Sira-Ramírez y Cruz-Hernández 2000:2001].

1.3. Antecedentes

A raíz de los trabajos de Pecora y Carrol [1990] donde se demostró teórica y experimentalmente la sincronización de sistemas caóticos, se empezaron a desenvolver distintos métodos y alternativas sobre la sincronía de estos sistemas. Se han reportado diferentes técnicas y desarrollos que han dejado abierta la posibilidad de usar esta sincronización en la construcción de sistemas de encriptado. Los trabajos mas conocidos son: Encriptamiento por adición, ver por ejemplo cuomo et. al. [1993], encriptamiento por modulación paramétrica, ver por ejemplo Yang y Chua [1990] y encriptamiento por conmutación entre dos atractores caóticos, ver por ejemplo Parlitz et. al. [1992].

En el área de los láseres también se han ido desarrollando varias técnicas de sincronización y comunicaciones caóticas. Algunas de las publicaciones recientes y relacionadas a esta tesis se presentan a continuación:

- Se profundiza en el análisis teórico del amplificador EDFA, propone diferentes modelos con diferentes resultados para demostrar como la cantidad de parámetros usados afectan los resultados experimentalmente a comparación de los modelos que están en muchas ocasiones alejados de los resultados exactos. Da un enfoque hacia el funcionamiento básico del láser y su amplificación para poder comprender este fenómeno físico [Belloui 2011].

- Se Publica una investigación sobre la sincronización de caos y transmisión de mensajes entre dos láseres de semiconductor con acoplamiento mutuo, conducidos mediante un tercer láser de semiconductor de cavidad externa. Presentan resultados por medio de simulaciones [Ning Jiang 2010]

- Se propone un sistema de comunicaciones ópticas basadas en los principios de sincronización de oscilaciones caóticas. El transmisor y receptor están compuestos por dos láseres de semiconductor de cavidad externa caótica, configurados como maestro y esclavo [Pisarchik 2010].

- Se genera una doble longitud de onda caótica en un solo láser EDFL, utilizan un filtro óptico para fluctuar entre las dos señales. La generación de caos es obtenida por dos métodos: por la modulación de la fuente del diodo láser, cerca de la frecuencia de las oscilaciones de relajación y mediante una modulación a través de un modulador opto-electrónico dentro de cada longitud de onda generada [Fan Zhang 2005].

- Desarrollan un modelo en Simulink implementado por Novak y Gieske (2002), donde agregan el ruido de la emisión espontanea amplificada y la longitud de onda óptima. El modelo es originalmente utilizado para explicar la dinámica de los sistemas de longitud de onda con multiplexado [Stephen Pinter 2004].

- Se publica un artículo donde describen las características de una señal caótica generada en un láser semiconductor. Explican y demuestran por medio de un modelo numérico como se pueden generar efectos de caos usando las propiedades de filtrado de un láser con respecto a señales ópticas inyectadas en un sistema [Atsushi Uchida 2003].

- Presenta un modelo para la caracterización y extracción de parámetros de un EDFA. El método propuesto para el modelo puede ser usado para simular el comportamiento de la ganancia y el ruido de amplificadores para DWDM (Dense wavelength division Multiplexing o bien, multiplexación por división en longitudes de onda densas) o puede ser usado para reemplazar los costosos dispositivos de medición de hasta 80 o más longitudes de onda, seleccionando fuentes de láser sintonizables o fijas [Schmidtke 2001].

- Presenta un modelo dinámico de la ganancia del láser EDFA por medio de ecuaciones diferenciales ordinarias. El modelo provee una manera rápida de calcular la ganancia dinámica del láser EDFA. Muestra además, explícitamente como la frecuencia de oscilación de relajación del láser y la constante de amortiguación son afectadas por los parámetros designados en las expresiones analíticas [Qian Yu 1999].

- Demuestra por medio de simulaciones numéricas que dos sistemas caóticos generados por dos láseres de semiconductor acoplados, pueden ser sincronizados usando retroalimentación óptica directa [Annovazzi 1996].

Una de las publicaciones de mayor interés para esta tesis es la sincronización de sistemas caóticos por formas hamiltonianas y diseño de un observador no lineal de estado, reportada en [Sira-Ramírez y Cruz-Hernández 2000; 2001], debido a que es la metodología adoptada para la sincronización de los láseres efectuada en esta tesis.

1.4. Objetivos

Con la realización de la presente tesis de maestría, se pretende alcanzar el siguiente objetivo general y objetivos particulares.

1.4.1. Objetivo General

- Sincronización de láseres como generadores de caos y sus aplicaciones a las comunicaciones

1.4.2. Objetivos Específicos

- Generar caos utilizando el láser EDFA y medir su nivel caótico, simulación.
- Sincronizar dos láser EDFA empleando formas hamiltonianas y diseño de un observador no lineal de estado, simulación.
- Transmitir información privada de manera segura, mediante la sincronización de láseres.

1.5. Metodología Adoptada

Para alcanzar los objetivos planteados se utilizara el modelo del láser EDFA y la metodología de sincronización por formas hamiltonianas y diseño de un observador no lineal de estado, reportado en [Sira-Ramírez y Cruz-Hernández 2000; 2001]. Esta metodología nos permite sincronizar los láseres utilizando solo una variable, esto se debe a que en los láseres experimentalmente solo tenemos acceso a la intensidad del campo eléctrico. Una vez alcanzada la sincronización se utilizan los esquemas de comunicaciones seguras. La metodología resumida es la siguiente:

- Se analizan los modelos de diferentes tipos de láseres, se desglosa cada elemento de las ecuaciones diferenciales y se estudia su dinámica dentro del sistema.

- Generar caos en el láser mediante programación en Matlab y aplicar métodos de análisis para verificar su comportamiento caótico.

- Sincronizar dos láseres empleando formas hamiltonianas y diseño de un observador no lineal de estado, simular los resultados mediante programación en Matlab haciendo uso de las herramientas de programación del software. Probar distintas condiciones con variaciones en los parámetros y comparar resultados.

- Utilizar la sincronización de los láseres para su aplicación a las comunicaciones seguras.

Resumiendo, se pretende simular un sistema de encriptado transmitiendo información de manera segura. Se utiliza el modelo del láser EDFRL (Erbium Doped Fiber Ring Laser) reportado en [L. G. Luo and P. L. Chu 1998], como encriptador en la configuración maestro esclavo usando la metodología de sincronización por formas hamiltonianas y diseño de un observador no lineal de estado.

1.6. Organización de esta tesis

En el capitulo 1 se da una breve introducción del contenido de esta tesis, se plantea el problema de estudio, los antecedentes, los objetivos y la motivación para la realización de la misma. Así como también se define la metodología de estudio adoptada para la realización del presente trabajo de tesis.

En el capitulo 2 se da una breve introducción acerca de la criptografía. Contiene una reseña acerca su historia y se definen los tipos de criptografía

existentes, se mencionan algunos ejemplos y se detallan los conceptos relacionados. También se mencionan las técnicas de criptografía utilizadas desde la antigüedad hasta la fecha y se habla sobre el futuro de la misma.

El capitulo 3 trata acerca de la teoría del caos y la sincronización de sistemas caóticos. Se inicia con una breve introducción de la teoría del caos, su historia y su relación con la criptografía. Se mencionan las aplicaciones y características del caos. Se definen los conceptos de sincronización caótica y los tipos de estados sincronizados. Ademas, se define el método de sincronización mediante formas hamiltonianas y diseño de un observador no lineal de estado, el cual es utilizado para la sincronización de láseres en esta tesis.

En el capitulo 4 se definen los láseres y el amplificador EDFA, se da una introducción sobre su historia y su relación con la tecnología. Se definen los diferentes tipos de láseres que existen y se estudia la relación entre los láseres y el caos. Ademas, se explica y estudia el funcionamiento de los diferentes láseres incluyendo al láser semiconductor y se presentan ejemplos e ilustraciones que describen los comportamientos de los distintos sistemas de láseres.

El capitulo 5 trata sobre la sincronización caótica de láseres. Se inicia con una breve introducción sobre los sistemas de láseres acoplados y el comportamiento de los estados dinámicos que los componen. Se explica la comprensión de la dinámica de láseres y el método de sincronización mediante formas hamiltonianas y diseño de un observador. También se definen los modelos dinámicos de un láser semiconductor y un láser EDFRL, los cuales son sincronizados mediante el método anteriormente mencionado. Se presenta el desarrollo paso a paso de la sincronización y los resultados numéricos obtenidos.

Capítulo 2

La criptografía y los sistemas de encriptado

2.1. Introducción

Desde los orígenes de la humanidad el hombre siempre ha tenido la necesidad de comunicarse, el transmitir información se ha convertido en una de las principales necesidades dentro de cualquier sociedad. Las comunicaciones son utilizadas desde fines personales hasta fines militares.

Desde que las sociedades comprendieron el valor de la información como elemento de poder, surgió la criptografía; disciplina que ha cambiado sin lugar a duda, el curso de la historia. Anteriormente con los inicios de la criptografía se dieron los primeros intentos de comunicaciones seguras, los cuales datan desde hace mas de 4500 millones de años en el Antiguo Egipto, hasta los algoritmos cuánticos mas sofisticados de las sociedades modernas.

Personajes importantes dentro de la historia hicieron uso de la criptografía para lograr formar sus grandes imperios, tal es el caso de Julio Cesar, el cual

empleaba una sencilla técnica de encriptado para hacer llegar sus mensajes de manera segura, esta técnica es uno de los primeros métodos de encriptado documentados. No solo personajes de talla militar usaron esta disciplina, si no que también artistas como es el caso de Leonardo Davinci, el cual escribía mensajes "ocultos" dentro de sus trabajos.

A raíz de la segunda guerra mundial se desprendieron importantes acontecimientos dentro de la criptografía, como por ejemplo; la transición de la criptografía clásica a la criptografía moderna, la ruptura de sistemas criptográficos y un gran paso para los inicios de una nueva era dentro de las comunicaciones seguras.

En este capitulo, se presenta un resumen de los datos mas importantes dentro de la historia de la criptografía clásica, la criptografía moderna y el futuro de esta disciplina dentro de los próximos años. Se abordan los diferentes tipos de criptografía y los distintos sistemas de encriptado desarrollados con el paso del tiempo.

2.2. Historia de la criptografía

La palabra criptografía proviene del griego krypto, que significa oculto, y graphos, que significa escribir, lo que literalmente traducido significa escritura oculta. Tradicionalmente se ha definido como la parte de la criptología que se ocupa de las técnicas, bien sea aplicadas al arte o la ciencia, que alteran las representaciones lingüísticas de mensajes, mediante técnicas de cifrado y/o codificado, para hacerlos ininteligibles a intrusos (lectores no autorizados) que intercepten esos mensajes

La historia de la criptografía viene de miles de años atrás, desde el simple uso del papel y el lápiz hasta algoritmos complejos por medio de computadoras y software. A principios del siglo XX, la invención de máquinas mecánicas y elec-

tromecánicas complejas, como la máquina de rotores Enigma, proporcionaron métodos de cifrado más sofisticados y eficientes y la posterior introducción de la electrónica y la computación ha permitido sistemas mas elaborados que siguen teniendo gran complejidad. Hasta los años 70, la criptografía segura era dominio casi exclusivo de los gobiernos. Desde entonces, dos sucesos la han colocado de lleno en el dominio público: la creación de un estándar de cifrado público (DES); y la invención de la criptografía asimétrica.

El uso más antiguo conocido de la criptografía se halla en jeroglíficos no estándares tallados en monumentos del Antiguo Egipto (hace más de 4500 años). Sin embargo, no se piensa que sean intentos serios de comunicación secreta, sino intentos de conseguir misterio, intriga o incluso diversión para el espectador. Más tarde, eruditos hebreos hicieron uso de sencillos cifrados por sustitución monoalfabéticos (como el cifrado Atbash), quizás desde el 500 al 600 A.C.

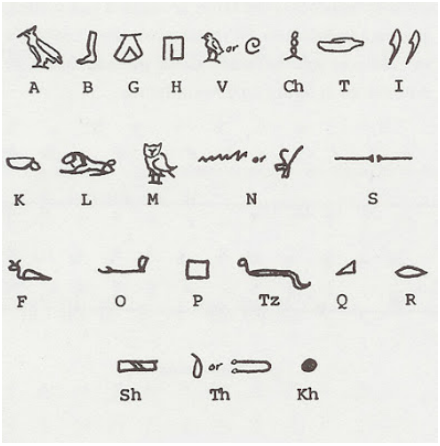


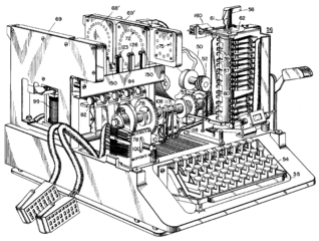
Figura 2.1: Alfabeto Egipcio de Jeroglíficos

La criptografía tiene una larga tradición en las escrituras religiosas que podrían ofender a la cultura dominante o a las autoridades políticas. Quizás el caso más famoso es el 'número de la bestia', del libro del Apocalipsis en el Nuevo Testamento cristiano. El '666' puede ser una forma criptográfica (es decir,

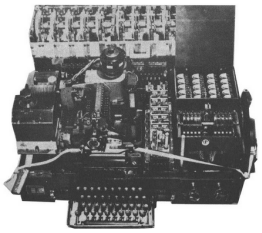
cifrada) de ocultar una referencia peligrosa; muchos expertos creen que es una referencia oculta al Imperio Romano, o más probablemente al propio emperador Nerón (y así a las políticas persecutorias romanas), que sería entendida por los iniciados (los que 'tenían la clave del entendimiento'), y sin embargo sería segura o al menos negable si atraía la atención de las autoridades. Al menos para las escrituras ortodoxas cristianas, casi toda esta necesidad de ocultación desapareció con la conversión y adopción del cristianismo como religión oficial del Imperio por parte del emperador Constantino.

Mas tarde aparece la técnica del análisis de frecuencias para romper los cifrados por sustitución monoalfabéticos, en algún momento alrededor del año 1000. Fue el avance criptoanalítico más importante hasta la Segunda Guerra Mundial. La criptografía fue teniendo mas importancia y relevancia al pasar de los años ocasionando sucesos de suma importancia en los que hasta la muerte estaba involucrada. Fuera del Medio Oriente y Europa, la criptografía permaneció comparativamente subdesarrollada. En Japón no se utilizó la criptografía hasta 1510, y las técnicas avanzadas no se conocieron hasta la apertura del país hacia occidente en los años 1860.

En la Segunda Guerra Mundial, las máquinas de cifrado mecánicas y electromecánicas se utilizaban extensamente, los alemanes hicieron gran uso de diversas variantes de una máquina de rotores electromecánica llamada Enigma (Ver figura 2.2) . El matemático Marian Rejewski, de la Oficina de Cifrado polaca, reconstruyó en diciembre de 1932 la máquina Enigma del ejército alemán, utilizando la matemática y la limitada documentación proporcionada por el capitán Gustave Bertrand, de la inteligencia militar francesa. Ademas de la máquina Enigma, se utilizaron las máquinas Typex britanica y la Sigaba (figura 2.2.1), ambas eran diseños de rotores eletromecánicos similares en espíritu a la Enigma, aunque con mejoras importantes.



2.2.1: Máquina Estaunidense Sigaba



2.2.2: Máquina Enigma

Figura 2.2: Máquinas de Encriptado usadas durante la segunda guerra mundial

Este fue el mayor avance del criptoanálisis en más de mil años. Rejewsky y sus colegas de la Oficina de Cifrado, Jerzy Rózycki y Henryk Zygalski, continuaron desentrañando la Enigma y siguiendo el ritmo de la evolución de los componentes de la máquina y los procedimientos de cifrado. Al irse deteriorando los recursos financieros de Polonia por los cambios introducidos por los alemanes, y al irse avecinando la guerra, la Oficina de Cifrado, bajo órdenes del estado mayor polaco, presentaron a representantes de la inteligencia francesa y británica los secretos del descifrado de la máquina Enigma, el 25 de julio de 1939, en Varsovia [Steven Levy 2002].

2.3. Criptografía Clásica

Los métodos clásicos son aquellos en los que, además de las máquinas dedicadas para cifrar, se usan por separado técnicas de sustitución y transposición aplicadas a los caracteres del mensaje en claro. Las técnicas criptográficas utilizadas en este caso son en su totalidad orientadas a sistemas de clave secreta, generalmente manteniendo también en secreto el algoritmo, incluso en el caso en que el cifrador cuente con una clave secreta. El cifrado se realiza sobre caracteres alfanuméricos, por lo general alfabéticos, y en ese mismo formato se transmiten o almacenan [Domínguez Esp inoza 2007].

En criptografía, el cifrado clásico (figura 2.2) es un tipo de cifrado que fue usado históricamente pero que ahora ha caído, mayormente, en desuso. En general, los cifrados clásicos operan en un alfabeto de letras (como "A-Z"), a las cuales se les aplican métodos a mano o con aparatos mecánicos muy simples. Son tipos muy básicos de cifrado, lo que no los hace muy fiables, especialmente después del desarrollo de nueva tecnología. Métodos más modernos usan ordenadores u otra tecnología digital, que opera con bits y bytes. Muchos cifrados clásicos fueron usados por gente muy conocida como Julio César y Napoleón, quienes crearon sus propios cifrados que después han sido usados popularmente. Muchos cifrados tienen un origen militar y fueron usados para trasportar mensajes secretos entre personas del mismo bando. Los sistemas clásicos son bastante susceptibles de un ataque con solo texto cifrado, algunas veces incluso sin el conocimiento del sistema en sí mismo, usando herramientas como el análisis de frecuencias. Algunas veces se agrupan junto con los cifrados clásicos otras máquinas mecánicas o electro mecánicas, como la Enigma.

La oficina de asuntos exteriores japonesa utilizo un sistema eléctrico lógico basado en uniselectores, también utilizo varias máquinas similares para los agregados de algunas embajadas japonesas. una de estas recibió el nombre de "Máquina M" por EU y otra fue apodada "Red". Todas fueron rotas en mayor o menor grado por los aliados.

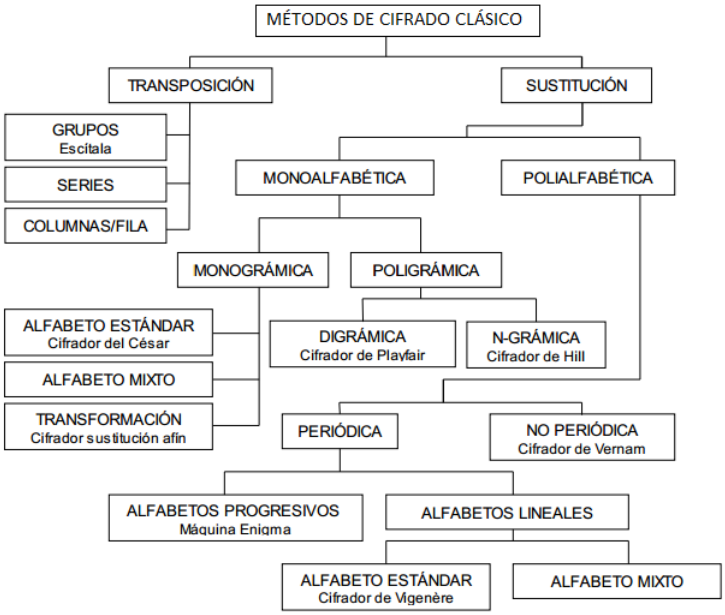


Figura 2.3: Clasificación de los métodos clásicos de cifrado y algunos ejemplos.

El primer caso claro de uso de métodos criptográficos se dió durante la guerra entre Atenas y Esparta, el instrumento usado fue nombrado escitala espartana. El historiador griego Plutarco, describe la escitala de la siguiente manera: “La escitala (figura 2.4) era un palo o bastón en el cual se enrollaba en espiral una tira de cuero. Sobre esa tira se escribía el mensaje en columnas paralelas al eje del palo. La tira desenrollada mostraba un texto sin relación aparente con el texto inicial, pero que podía leerse volviendo a enrollar la tira sobre un palo del mismo diámetro que el primero”. Con este sistema los gobernantes de Espartana transmitieron, con eficacia, sus instrucciones secretas a los generales de su ejército, durante las campañas militares. Lógicamente, este procedimiento suponía que tanto el emisor como el receptor del mensaje dispusieran de un palo o bastón con las mismas características físicas: grosor y longitud.

Durante siglos la criptografía caminó por la senda de la sustitución y la

transposición. En los escritos medievales sorprenden términos como Oobice o Thfpflxctxs. Para esconder sus nombres, los copistas empleaban el alfabeto zodiacal, formaban anagramas alterando el orden de las letras (es el caso de oobice, anagrama de Boecio) o recurrían a un método denominado fuga de vocales, en el que éstas se sustituían por puntos o por consonantes arbitrarias (Thfpflxctxs por Theoflactus). Esta simplicidad hizo que la sustitución fuera el procedimiento dominante a lo largo del primer milenio de nuestra era. Por esa época, muchos estudiosos consideraban a la cifra de sustitución como indescifrable.

Figura 2.4: La escitala, primer caso claro de uso de métodos criptográficos

Sin embargo, en la ciudad de Bagdad fueron los primeros en descifrar. El artífice fue el sabio árabe conocido como Al-Kindi (801-873), él fue un importante filósofo árabe y un estudioso de las Ciencias. Autor de unos 300 libros sobre: medicina, matemáticas, lingüística y música. Uno de sus tratados más importantes, redescubierto en el año 1987, se encuentra en el archivo Sulaimaniyyah de Estambul, titulado: "Sobre el desciframiento de mensajes criptográficos". El sistema para resolver los enigmas criptográficos está descrito claramente en dos breves párrafos, dice Al Kindi : "Una manera de resolver un mensaje cifrado, si sabemos en qué lengua está escrito, es encontrar un texto llano escrito en la misma lengua, suficientemente largo, y luego contar cuantas veces aparece cada letra. A letra que aparece con más frecuencia la llamamos "primera", a la siguiente en frecuencia la llamaremos"segunda".... y así hasta que hayamos cubierto todas las letras que aparecen en nuestro texto. Luego observamos el texto

cifrado que queremos resolver y clasificamos sus símbolos de la misma manera. Encontramos el símbolo que aparece con mayor frecuencia y lo sustituimos por la "primera" de nuestro texto, hacemos lo mismo con la "segunda" y así sucesivamente, hasta que hayamos cubierto todos los símbolos del criptograma que queremos resolver". Para facilitar el desciframiento siguiendo este procedimiento nos puede ayudar el saber cuales son las frecuencias relativas de las letras y de algunas palabras más frecuentes [Santiago Fernández 2004].

En el famoso relato el escarabajo de oro, escrito por el americano Edgar Allan Poe y publicado el año 1843, se describe como el héroe del relato a William Legrand, quien consigue descubrir el lugar en el que se encuentra un fabuloso tesoro, descifrando un mensaje criptográfico escrito sobre un pergamino. El procedimiento utilizado por W. Legrand para desentrañar el cifrario del pergamino es un método estadístico, basado en la frecuencia de las letras que componen un texto inglés. En definitiva, el método coincide exactamente con el propuesto por el sabio árabe Al-Kindi. Hemos de reconocer que Allan Poe era un excelente criptoanalista aficionado. También el escritor francés Julio Verne (1828-1905) utilizó la criptografía en varias de sus novelas, una de ellas Viaje al centro de la Tierra.

En general, existen dos grandes grupos de cifrados: los algoritmos que utilizan una única clave tanto en el proceso de cifrado como en el de descifrado, y los que utilizan una clave para cifrar mensajes y una clave distinta para descifrarlos. Los primeros se denominan cifras simétricas, de clave simétrica o de clave privada y son la base de los algoritmos de cifrado clásico. Los segundos se denominan cifras asimétricas, de clave asimétrica o de clave pública y forman el núcleo de las técnicas de cifrado modernas. [Jiménez Hidalgo 2008]

2.3.1. Criptografía Simétrica

La criptografía simétrica, también conocida como criptografía de clave secreta o criptografía de una clave, es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

Existe una clasificación de este tipo de criptografía en tres familias:

- Criptografía simétrica de bloques.
- Criptografía simétrica de lluvia.
- Criptografía simétrica de resumen.

Aunque con ligeras modificaciones un sistema de criptografía simétrica de bloques puede modificarse para convertirse en alguna de las otras dos formas, sin embargo es importante verlas por separado dado que se usan en diferentes aplicaciones. La criptografía simétrica ha sido la más usada en toda la historia, ésta a podido ser implementada en diferente dispositivos, manuales, mecánicos, eléctricos, hasta los algoritmos actuales que son programables en cualquier computadora.

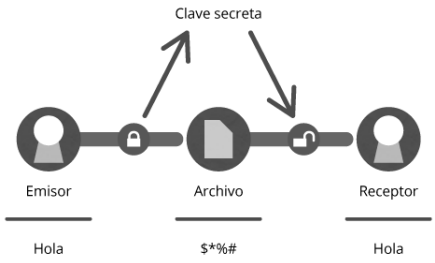


Figura 2.5: Esquema de cifrado simétrico

La idea general es aplicar diferentes funciones al mensaje que se quiere cifrar de tal modo que solo conociendo una clave pueda aplicarse de forma inversa para poder así descifrar. Aunque no existe un tipo de diseño estándar, quizá el más popular es el de Fiestel, que consiste esencialmente en aplicar un número finito de interacciones de cierta forma, que finalmente da como resultado el mensaje cifrado. Este es el caso del sistema criptográfico simétrico más conocido, DES.

Como ejemplo de sistema simétrico está la máquina Enigma. Como bien se ha mencionado éste fue un sistema empleado por Alemania durante la Segunda Guerra Mundial, en el que las claves se distribuían a diario en forma de libros de códigos. Cada día, un operador de radio, receptor o transmisor, consultaba su copia del libro de códigos para encontrar la clave del día. Todo el tráfico enviado por ondas de radio durante aquel día era cifrado y descifrado usando las claves del día. Algunos ejemplos de algoritmos simétricos son DES, 3DES, RC5, AES, Blowfish e IDEA [www.wikipedia.com].

2.4. Criptografía Moderna

La era de la criptografía moderna comienza realmente con Claude Shannon, que podría decirse que es el padre de la criptografía matemática. En 1949 publicó el artículo Communication Theory of Secrecy Systems en la Bell System Technical Journal, y poco después el libro Mathematical Theory of Communication, con Warren Weaver. Estos trabajos, junto con los otros que publicó sobre la teoría de la información y la comunicación, establecieron una sólida base teórica para la criptografía y el criptoanálisis. Y, a la vez, la criptografía desapareció de la escena para quedarse dentro de las organizaciones gubernamentales secretas como la NSA. Muy pocos trabajos se hicieron públicos hasta mediados de los 70, cuando todo cambió.

A mediados de los 70 se vivieron dos importantes avances públicos (es decir, no secretos). El primero fue la publicación del borrador del Data Encryption Standard en el Registro Federal estadounidense el 17 de marzo de 1975. La propuesta fue enviada por IBM, por invitación de la Oficina Nacional de Estándares (ahora NIST), en un esfuerzo por desarrollar sistemas de comunicación electrónica segura para las empresas como los bancos y otras organizaciones financieras grandes.

El segundo desarrollo, en 1976, fue quizás más importante todavía, ya que cambió de manera fundamental la forma en la que los criptosistemas pueden funcionar. Fue la publicación del artículo New Directions in Cryptography, de Whitfield Diffie y Martin Hellman. Introdujo un método radicalmente nuevo para distribuir las claves criptográficas, dando gran un paso adelante para resolver uno de los problemas fundamentales de la criptografía, la distribución de claves, y ha terminado llamándose intercambio de claves Diffie-Hellman. El artículo también estimuló el desarrollo público casi inmediato de un nuevo tipo de algoritmo de cifrado, los algoritmos de cifrado asimétrico.

Antes de eso, todos los algoritmos de cifrado útiles eran algoritmos de cifrado simétrico, en los que tanto el remitente como el destinatario utilizan la misma clave criptográfica, que ambos deben mantener en secreto. Todas las máquinas electromecánicas utilizadas en la Segunda Guerra Mundial eran de esta clase lógica, al igual que los cifrados César y Atbash y en esencia todos los cifrados y sistemas de códigos de la historia.

En cambio, el cifrado de clave asimétrica utiliza un par de claves relacionadas matemáticamente, en el que una de ellas descifra el cifrado que se realiza con la otra. Algunos (pero no todos) de estos algoritmos poseen la propiedad adicional de que una de las claves del par no se puede deducir de la otra por ningún método conocido que no sea el ensayo y error. Con un algoritmo de este tipo,

cada usuario sólo necesita un par de claves. Designando una de las claves del par como privada (siempre secreta) y la otra como pública (a menudo visible), no se necesita ningún canal seguro para el intercambio de claves. Mientras la clave privada permanezca en secreto, la clave pública puede ser conocida públicamente durante mucho tiempo sin comprometer la seguridad, haciendo que sea seguro reutilizar el mismo par de claves de forma indefinida.

La efectividad de los algoritmos asimétricos depende de una clase de problemas matemáticos conocidos como funciones de un solo sentido, que requieren relativamente poca potencia de cálculo para ejecutarse, pero muchísima potencia para calcular la inversa. Un ejemplo clásico de función de un sentido es la multiplicación de números primos grandes. Es bastante rápido multiplicar dos primos grandes, pero muy difícil factorizar el producto de dos primos grandes. Debido a las propiedades matemáticas de las funciones de un sentido, la mayor parte de las claves posibles tienen poca calidad para su uso criptográfico; solo una pequeña parte de las claves posibles de una cierta longitud son candidatas ideales, y por tanto los algoritmos asimétricos requieren claves muy largas para alcanzar el mismo nivel de seguridad proporcionado por las claves simétricas, relativamente más cortas. Las exigencias de generar el par de claves y realizar el cifrado/descifrado hacen que los algoritmos asimétricos sean costosos computacionalmente.

Aunque los cifrados modernos como el AES están considerados de alta seguridad, todavía siguen adoptándose malos diseños, y en las décadas recientes ha habido varias rupturas criptoanalíticas notables. Ejemplos famosos de diseños criptográficos que se han roto incluyen al DES, el primer esquema de cifrado Wi-Fi, WEP, el sistema Content Scramble System utilizado para cifrar y controlar el uso de los DVD, y los cifrados A5/1 y A5/2 utilizados en los teléfonos móviles GSM. Además, no se ha demostrado que alguna de las ideas matemáticas que

subyacen a la criptografía de clave pública sean no vulnerables, y por tanto es posible que algún descubrimiento futuro haga inseguros todos los sitemas que dependen de ella. Aunque poca gente prevé un descubrimiento así, el tamaño de clave recomendado sigue aumentando, al aumentar y hacerse más barata la potencia de cálculo para romper códigos [www.wikipedia.com].

El futuro de la criptografía moderna va dirigido a la criptografía cuántica, dentro de 25 años, muchos de los secretos que guarda el mundo moderno bajo potentes algoritmos criptográficos, como los datos médicos o la información clasificada de los gobiernos, correrán un peligro real de saltar por los aires. La criptografía cuántica se encargará de que su descifrado sea un juego de niños, susceptible de caer en manos de terroristas o criminales. Quien realizó tal profecía fueron respetables investigadores como Martin Hellman, coinventor de la criptografía de clave pública, y el criptólogo argentino Hugo Scolnik, durante sus intervenciones en el Día Internacional de la Seguridad de la Información en la Universidad Politécnica de Madrid.

Hellman y Scolnik sostienen que la criptografía cuántica está aún en un estado inicial y hasta dentro de 25 años no se verán sus primeras aplicaciones prácticas, que romperán con facilidad los actuales sistemas de cifrado. Mientras tanto, ha empezado una carrera paralela para proteger la información que debería seguir siendo secreta cuando irrumpa la criptografía cuántica. En general observar un sistema cuántico perturba al mismo, e impide que el observador conozca su estado exacto antes de la observación. Por lo tanto, si un sistema cuántico es utilizado para transferir información, alguien que quiera espiar la comunicación, o incluso el receptor previsto, podría verse impedido de obtener toda la información enviada por el emisor. Este rasgo negativo de la mecánica cuántica, conocido como principio de incertidumbre de Heisenberg, ha encontrado un uso positivo en las comunicaciones seguras [Merce Molist 2008].

A diferencia de los métodos convencionales que basan su seguridad en principios matemáticos, la criptografía cuántica se basa en principios físicos. Ya que por las leyes de la física cuántica es imposible medir un estado cuántico de un sistema sin alterarlo y según los físicos nunca va a ser posible. Se cree que la criptografía cuántica es un criptosistema indestructible. Incluso existen al menos dos estudios independientes que afirman haber probado su seguridad definitiva, es decir una prueba de que los protocolos criptográficos cuánticos son inmunes a todas las estrategias de escucha.

2.4.1. Criptografía asimétrica

La criptografía asimétrica, también llamada criptografía de clave pública o criptografía de dos claves, es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente el mismo par de claves.

Los sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

Algunos ejemplos de algoritmos asimétricos son el RSA, usado como estándar de facto para la firma digital, el algoritmo DSS, usado solo en la firma digital y el ECC, el cual es mas complicado que el RSA pero necesita menos procesamiento.

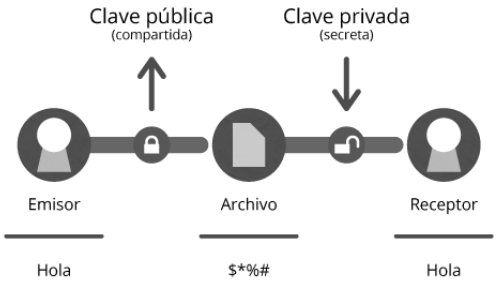


Figura 2.6: Esquema de cifrado asimétrico

Las dos principales ramas de la criptografía asimétrica son:

- Cifrado de clave pública: un mensaje cifrado con la clave pública de un destinatario no puede ser descifrado por nadie (incluyendo al que lo cifró), excepto por un poseedor de la clave privada correspondiente, este será el propietario de esa clave y la persona asociada con la clave pública utilizada. Se utiliza para confidencialidad.

- Firmas digitales: un mensaje firmado con la clave privada del remitente puede ser verificado por cualquier persona que tenga acceso a la clave pública del remitente, lo que demuestra que el remitente tenía acceso a la clave privada (y por lo tanto, es probable que sea la persona asociada con la clave pública utilizada) y la parte del mensaje que no se ha manipulado. Se utiliza para cuestiones de autenticidad [www.wikipedia.com].

2.5. Criptografía híbrida

Este sistema es la unión de las ventajas de los dos anteriores, debemos de partir que el problema de ambos sistemas criptográficos es que el simétrico es inseguro y el asimétrico es lento. En estos sistemas se usa la llave pública del receptor para encriptar una clave simétrica que se usara en el proceso de comunicación encriptada [Pedro Gutiérrez 2013].

El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo):

- Generar una clave pública y otra privada (en el receptor).
- Cifrar un archivo de forma síncrona.
- El receptor nos envía su clave pública.
- Ciframos la clave que hemos usado para encriptar el archivo con la clave pública del receptor.
- Enviamos el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).

2.6. Conclusiones

Con paso del tiempo la criptografía ha sido de gran utilidad dentro de las sociedades, el transmitir información de manera confidencial es una tarea cada vez mas complicada debido al rápido avance de las matemáticas y las tecnologías actuales. El uso de la criptografía viene dándose desde la época de los egipcios (1900 A.C) hasta la actualidad, con la implementación del algoritmo de cifrado AES. A pesar de las grandes tecnologías de nuestra época, este algoritmo debe

de ser sustituido por otro de mayor seguridad y es por esto que aun se continua trabajando en la búsqueda de algoritmos mas eficientes.

El contenido de este capítulo fue tomado de las siguientes fuentes: [Domínguez Espínoza 2007], [Jiménez Hidalgo 2008], [Lomonaco, Samuel J. Jr. A Talk on Quantum Cryptography or How Alice Outwits Eve. 2001], [Pedro Gutiérrez 2013], [Santiago Fernández 2004], [Stallings, William. Cryptography and Network Security: Principles and Practice. Prentice Hall, 1998.], [Steven Levy 2002], [www.wikipedia.com].

Capítulo 3

Caos y Sincronización

3.1. Introducción

Actualmente, en los estudios relacionados con las comunicaciones seguras es muy común encontrarnos con la teoría del caos, esta teoría es una de las grandes propuestas de los últimos años para usarse como nuevo algoritmo de cifrado. El conocido efecto mariposa, termino acuñado por el matemático y meteorólogo estadounidense Edward Norton Lorenz, nos explica como el simple aleteo de una mariposa puede provocar un Tsunami al otro lado del mundo. El efecto mariposa es un concepto que hace referencia en la noción del tiempo a las condiciones iniciales dentro del marco de la teoría del caos.

La idea es que dadas unas condiciones iniciales de un determinado sistema caótico, la más mínima variación en ellas puede provocar que el sistema evolucione en ciertas formas completamente diferentes. De manera que una pequeña perturbación inicial, mediante un proceso de amplificación, podrá generar un efecto considerablemente grande a mediano o corto plazo de tiempo. Lorenz construyó un modelo matemático muy simplificado, que intentaba capturar el

comportamiento de la convección en la atmósfera. El matemático estudió las soluciones de su modelo y se dio cuenta que alteraciones mínimas en los valores de las variables iniciales resultaban en soluciones ampliamente divergentes. Su investigación dió origen a un renovado interés en la teoría del caos, como por ejemplo, su uso en las comunicaciones seguras.

La idea general para transmitir información a través de sistemas caóticos es que la señal de información esté inmersa en el sistema transmisor, el cual produce una señal caótica, esta señal es recobrada cuando el transmisor y el receptor son idénticos. Desde la observación de Pecora y Carroll acerca de la posibilidad de sincronizar dos sistemas caóticos, se han desarrollado bastantes esquemas de sincronización. La sincronización se puede clasificar en sincronización mutua (o acoplamiento bidireccional) y sincronización maestro-esclavo (o acoplamiento unidireccional).

En este capítulo, se definen los conceptos de caos y sincronización, se presentan las distintas formas de sincronía para los sistemas caóticos y se explica la teoría del caos y su aplicación a las comunicaciones seguras.

3.2. La teoría del caos

La teoría del caos es una rama de las matemáticas, la física y otras ciencias que trata ciertos tipos de sistemas dinámicos muy sensibles a las variaciones en las condiciones iniciales. Pequeñas variaciones en dichas condiciones iniciales pueden implicar grandes diferencias en el comportamiento futuro; complicando la predicción a largo plazo. Esto sucede aunque estos sistemas son en rigor determinísticos, es decir; su comportamiento puede ser completamente determinado conociendo sus condiciones iniciales. El nombre de ”teoría del caos” viene del hecho de que los sistemas que la teoría describe están aparentemente desordenados,

pero la teoría del caos es realmente acerca de encontrar el orden subyacente en los datos aparentemente aleatorios [http://www.imho.com/grae/chaos/chaos.html].

Los sistemas dinámicos se pueden clasificar básicamente en:

- Estables
- Inestables
- Caóticos

Un sistema estable tiende a lo largo del tiempo a un punto u órbita según su dimensión (como por ejemplo los atractores). Un sistema inestable se escapa de los atractores, mientras que un sistema caótico manifiesta los dos comportamientos. Por un lado, existe un atractor por el que el sistema se ve atraído, pero a la vez, hay "fuerzas" que lo alejan de éste. De esa manera, el sistema permanece confinado en una zona de su espacio de estados, pero sin tender a un atractor fijo.

Una de las mayores características de un sistema inestable es que tiene una gran dependencia de las condiciones iniciales. De un sistema del que se conocen sus ecuaciones características, y con unas condiciones iniciales fijas, se puede conocer exactamente su evolución en el tiempo. En el caso de los sistemas caóticos, una mínima diferencia en esas condiciones hace que el sistema evolucione de manera totalmente distinta. Ejemplos de tales sistemas incluyen el sistema solar, las placas tectónicas, los fluidos en régimen turbulento y los crecimientos de población.

En la mayoría de sistemas dinámicos se encuentran elementos que permiten un tipo de movimiento repetitivo y a veces, geométricamente establecido. Los atractores son los encargados de que las variables que inician en un punto de partida mantengan una trayectoria establecida, y lo que no se puede establecer

de una manera precisa son las oscilaciones que las variables puedan tener al recorrer las órbitas que lleguen a establecer los atractores.

Gran parte de los tipos de movimientos mencionados en la teoría del caos suceden alrededor de atractores muy simples, tales como puntos y curvas circulares llamadas ciclos límite. En cambio, el movimiento caótico está ligado a lo que se conoce como atractores extraños, que pueden llegar a tener una enorme complejidad como, por ejemplo, el modelo tridimensional del sistema climático de Lorenz, que lleva al famoso atractor de Lorenz (Fig. 3.1). Los atractores extraños son curvas del espacio de fases que describen la trayectoria elíptica de un sistema en movimiento caótico. Un sistema con estas características es impredecible, conocer su configuración en un momento dado no permite predecirla con certeza en un momento posterior [www.wikipedia.com].

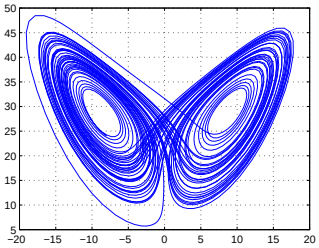


Figura 3.1: Atractor Caótico de Lorenz

El atractor de Lorenz es, quizá, uno de los diagramas de sistemas caóticos más conocidos, no sólo porque fué uno de los primeros, sino también porque es uno de los más complejos y peculiares, pues desenvuelve una forma muy peculiar más bien parecida a las alas de una mariposa.

3.3. Características del caos

Un sistema visto desde el punto de vista del caos, es un sistema flexible y no lineal, en donde el azar y lo no predecible juegan un papel fundamental. Un ejemplo de sistema caótico podría ser un río, en donde cada partícula de agua sigue una trayectoria aleatoria e impredecible, sin embargo no rompe con la dinámica establecida en el mismo río. En la geometría moderna surgen figuras caóticamente raras y bellas como resultado de modelos recursivos que generan comportamientos impredecibles, sin embargo estos conservan un cierto orden [Leandro Rodríguez].

Para conocer si un sistema es caótico, se suelen buscar las siguientes características:

- Sensibilidad a las condiciones iniciales. Esta característica implica que cada punto en un sistema es arbitrariamente aproximado por otros puntos con trayectorias futuras significativamente diferentes. Entonces, una pequeña perturbación en la trayectoria actual puede llevar a un diferente comportamiento más adelante.

- Topológicamente transitivo. Esto significa que el sistema evolucionara con el tiempo, así que una región o conjunto abierto de su espacio eventualmente se sobrepondrá con otra región dada.

- Densidad de órbitas periódicas. La densidad de órbitas periódicas significa que cada punto del espacio es aproximado arbitrariamente de manera cercana por órbitas periódicas. Sistemas topológicamente transitivos que fallen esta condición, probablemente tampoco tengan sensibilidad a las condiciones iniciales, y por lo tanto pueden no ser caóticos.

Estas características son las principales al momento de detectar sistemas caóticos, sin embargo existen otras características mas, como por ejemplo: los siste-

mas caóticos suelen tener un espectro de frecuencias con componentes planas, como le ocurre a un ruido aleatorio y además presentan exponentes de Lyapunov positivos.

3.4. Aplicaciones del caos

La Teoría del Caos y la matemática caótica resultaron ser una herramienta con aplicaciones a muchos campos de la ciencia y la tecnología. Gracias a estas aplicaciones el nombre se torna paradójico, dado que muchas de las prácticas que se realizan con la matemática caótica tienen resultados concretos porque los sistemas que se estudian están basados estrictamente con leyes deterministas aplicadas a sistemas dinámicos.

Las aplicaciones de la teoría del caos van desde las áreas de la meteorología o la física cuántica hasta la arquitectura a través de los fractales, también podemos encontrar su aplicación en el estudio de la medicina para el entendimiento de enfermedades graves, como por ejemplo la epilepsia. Otro campo de aplicación es la economía, debido a que un sistema dinámico puede referirse a la bolsa de valores para un economista [Leandro Rodríguez].

En la música también encontramos aplicación en la teoría del caos, muchos de los músicos modernos utilizan fractales para realizar sus composiciones musicales, no importa el género de música, en la mayoría de los casos, este método es aplicable para cualquier genero musical. Por último, cabe mencionar que otra de las aplicaciones del caos es en la transmisión segura de información, la cual sera el tema de estudio dentro de esta tesis.

3.5. Sincronización Caótica

El término sincronía significa literalmente "coincidencia en el tiempo" u "ocurriendo al mismo tiempo", y se refiere a la coincidencia de fenómenos y eventos en las ciencias naturales, ingeniería y en humanidades. El concepto de sincronización está usualmente ligado al movimiento periódico. Dos señales periódicas están sincronizadas si sus periodos son idénticos. Esta definición resulta ser inadecuada en el contexto de las señales caóticas. En este caso se requiere que las señales sean idénticas, al menos asintóticamente cuando el tiempo t $\rightarrow\infty$.

Uno de los rasgos mas sobresalientes de los sistemas caóticos es su dependencia con las condiciones iniciales del sistema, que hace que la mas mínima diferencia en la descripción del estado del sistema provoquen cambios que hacen distintos a sistemas complejos que originalmente, eran tan parecidos como se les quiera suponer [Angel Rodriguez 2009].

La idea que subyace bajo el fenómeno de sincronización es que dos sistemas caóticos, que inicialmente evolucionan sobre atractores diferentes, al acoplarse de algún modo, finalmente siguen una trayectoria común. La sincronización entre dos sistemas se consigue cuando uno de los dos sistemas cambia su trayectoria a la seguida por el otro sistema o bien a una nueva trayectoria común a ambos sistemas. Cabe mencionar que hay una gran diferencia en los procesos a la consecución de estados sincronizados, dependiendo del tipo de acoplamiento que estos presenten.

3.5.1. Definición

Podemos definir la sincronización caótica como sigue: [Cruz-Hernández y Mortynyuk 2009]: *Considere un sistema caótico modelado por la ecuación de estado*

$$\dot{x} = f(x) \tag{3.1}$$

y otro por

$$\dot{\hat{x}} = f(x) \tag{3.2}$$

con f, un campo vectorial con estados $x(t)$ y $\hat{x}(t)$ definidos en $\mathbb{R}^n$. Se dice que ambos sistemas sincronizaran completamente si para cualquier valor de las condiciones iniciales $x(0)$ y $\hat{x}(0)$, se cumple que

$$lim_{t\to\infty}\|x(t) - \hat{x}(t)\| \equiv 0.$$

Se define la siguiente diferencia como el error de sincroniza entre los osciladores (3.1) y (3.2)

$$e(t) = x(t) - \hat{x}(t) \tag{3.3}$$

3.5.2. Acoplamiento unidireccional

Es también conocida como sincronización maestro-esclavo, el sistema global está formado por dos subsistemas acoplados según una configuración de tipo maestro-esclavo. Eso implica que el comportamiento del sistema esclavo depende del comportamiento del sistema maestro mientras que este último no se ve influenciado por el comportamiento del sistema esclavo. Como resultado, el sistema esclavo se encuentra forzado a seguir la dinámica (o una función propia de la dinámica) del maestro [Cisneros Tamayo 2010].

3.5.3. Acoplamiento bidireccional

Es también conocida como sincronización mutua y es muy diferente del acoplamiento unidireccional. Aquí los dos sistemas están acoplados uno con el otro y el factor de acoplamiento produce la regulación o el ajuste de los ritmos en una variedad de sincronización común, induciendo un comportamiento de sincronización mutua. Esta situación ocurre en fisiología, entre el sistema cardíaco y el respiratorio, o entre neuronas interactuando, o en la óptica no lineal (como en láseres con retroalimentacion). Dentro de esta clasificación , la aparición y la robustez de los estados de sincronización ha sido establecida mediante diferentes esquemas de acoplamiento, tales como el método de Pecora y Carroll [He & Vaidya 1992; Pecora & Carroll 1990, 1991], la realimentación negativa [Kapitaniak 1994] , acoplamiento esporádico [Amritkar & Gupte 1993], descomposición activa-pasiva [Kocarev & Parlitz 1995; Parlitz et al. 1996b].

3.6. Tipos de estados sincronizados

A continuación se describen algunos tipos de sincronización existentes, ya que podemos encontrar muchos más y éstos incluso se pueden generalizar a sistemas discretos [Gerard Vidal 2010].

- Sincronización completa

  La sincronización completa fue el primer tipo descubierto. Consiste en una perfecta unión de las trayectorias caóticas de dos sistemas conseguidos por medio de una señal de acoplamiento. Con este mecanismo se demuestra que dos sistemas caóticos son acoplados unidireccionalmente sólo si todos los exponentes de Lyapunov del subsistema a sincronizar son negativos.

- Sincronización generalizada

  En la sincronización generalizada se usan sistemas completamente diferentes y se asocia la salida de uno de ellos como una función dada de la entrada del otro.

- Sincronización de fase

  La sincronización de fase se utiliza para sistemas de osciladores no idénticos o sistemas rotatorios, que pueden alcanzar un régimen intermedio donde se produce una unión de las fases, mientras la correlación entre las amplitudes permanece débil (amplitudes descorrelacionadas, caóticas).

- Sincronización con retardo

  La sincronización de retardo es un paso entre la sincronización de fase y la completa. La cuestión radica en que existe un limite asintótico entre el tiempo τ_{lag} , de salida de un sistema, y la salida del otro τ_{lag}. Esto hace que las fases y las amplitudes vayan unidas, pero con la presencia de un tiempo de retardo.

- Sincronización de retardo intermitente

  En este escenario, la mayor parte del tiempo los sistemas verifican la sincronización de fase, pero existen estallidos intermitentes de comportamientos no sincronizados, debido a que la trayectoria pasa por una región del atractor donde el exponente local de Lyapunov se acorta en alguna dirección y se vuelve positivo.

- Sincronización casi completa

  La "casi" sincronización es debida a la existencia del limite asintótico entre un subconjunto de variables de un sistema y el correspondiente subconjunto de variables del otro sistema [César Moreno Sierra 2005].

3.7. Sincronización mediante formas hamiltonianas y diseño de un observador no lineal de estado.

La gran mayoría de los sistemas caóticos se pueden representar en su forma canónica hamiltoniana. Mediante esta representación es posible la reconstructibilidad de un vector de estado de una señal de salida, la cual se evalúa a partir de la observabilidad o, en su defecto, de la detección de un par de matrices constantes. Se define este método a partir de [Sira-Ramirez y Cruz-Hernández 2000; 2001].

Consideremos una función de energía suave, dada en su forma generalizada hamiltoniana

$$\dot{x} = \mathcal{J}(x)\frac{\partial H}{\partial x} + S(x)\frac{\partial H}{\partial x}, x \in R^n$$

donde $H(x)$ es la función de energía, la cual es globalmente definida positiva en R^n. El vector columna $\frac{\partial H}{\partial x}$ representa el gradiente de la función de energía. Frecuentemente se usa la función de energía de la forma cuadrática:

$$H(x) = \frac{1}{2}x^T M x$$

con M siendo una matriz constante, simétrica y definida positiva. En tal caso $\frac{\partial H}{\partial x} = Mx$.

Las matrices cuadradas $\mathcal{J}(x)$ y $S(x)$, satisfacen para toda $x \in R^n$ y cumplen con las siguientes propiedades: $\mathcal{J}(x) + \mathcal{J}(x)^T = 0$ y $S(x) = S^T(x)$, lo que representa a una matriz antisimetrica y una matriz simétrica respectivamente.

El vector de campo $\mathcal{J}(x)\frac{\partial H}{\partial x}$, exhibe la parte conservativa del sistema, $s(x)\frac{\partial H}{\partial x}$ representa la parte no conservativa del sistema. Para ciertos sistemas, la matriz simétrica $S(x)$ es definida negativa o semidefinida negativa.

Algunas veces, en el contexto de diseño de observadores, podemos escribir un sistema de ecuaciones no lineales en la forma especial:

$$\dot{x} = \mathcal{J}(y)\frac{\partial H}{\partial x} + (I + S)\frac{\partial H}{\partial x} + \mathcal{F}(y) \qquad x \in R^n$$

$$y = C\frac{\partial H}{\partial x}, \quad y \in R^m$$

donde $F(y)$ representa al vector de campo desestabilizante, S representa a una matriz simétrica, no necesariamente de signo definido.

El contenido de este capítulo fue tomado de las siguientes fuentes: [A. d'Anjou, C. Sarasola y F.J. Torrealdea. Caos Determinista. En SIGMA Revista Matemática (en linea), mayo 2005, vol 26.], [Angel Rodriguez 2009], [César Moreno Sierra "Métodos de sincronización de sistemas caóticos], [Cisneros Tamayo "sistemas caóticos aplicados en telecomunicaciones" Tesis de maestría. Instituto Politécnico Nacional, 2010], [Gerard Vidal Cassanya "Sincronización y control de sistemas dinámicos en régimen de caos espacio-temporal" Tesis doctoral. Universidad de Navarra, Facultad de ciencias, 2010], [Julien Clinton Sprott, Elegant chaos. Algebraically simple chaotic flows, World Scientific, 2010.], [www.imho.com/grae/chaos/chaos.html], [www.wikipedia.com].

3.8. Conclusiones

La teoría del caos, la cual se origino desde hace varios años atrás, seguirá siendo un amplio y fuerte tema de estudio dentro de los próximos años. Podemos encontrarnos con este fenómeno en muchas de las situaciones que enfrentamos todos los días. En la naturaleza, encontramos distintos ejemplos de comportamientos caóticos así como también de sincronización; tal es el ejemplo de las luciérnagas, que al encender su luz en manadas durante la noche, estas alcanzan una sincronía y encienden y pagan su luz en un mismo tiempo. Además se explicó el origen de la teoría del caos, sus características y aplicaciones así como también la sincronización de sistemas caóticos, la cual, es de suma importancia para poder aplicar a las comunicaciones seguras la teoría del caos. Se definió el método de sincronización mediante formas hamiltonianas, el cual sera ejemplificado mas adelante con láseres EDFRL.

Capítulo 4

Láseres y el amplificador EDFA

4.1. Introducción

En poco más de medio siglo el láser ha transformado nuestra sociedad, actualmente es muy común encontrarnos con soportes como el CD, el DVD o el Blu-ray; lectores de códigos de barras, de impresoras láser o bien, con fibra óptica. Esta ultima es de suma importancia en nuestra sociedad puesto que las comunicaciones actuales dependen de la fibra óptica debido a su gran capacidad de transmisión de datos, ya que el creciente incremento de la población exige una mayor velocidad de transmisión.

Los láseres de semiconductores o diodos láser mueven y almacenan gran parte de la información que maneja la sociedad, y para usos a distancias largas emplean amplificadores ópticos como el amplificador EDFA (erbium doped fiber amplifier). Los láseres son esencialmente sistemas caóticos descritos por ecuaciones diferenciales no lineales con tres variables y muestran una amplia va-

riedad de dinámicas caóticas. La irregularidad inducida por la dinámica caótica es esencialmente diferente de la fluctuación al azar basada en procesos estocásticos, ya que el sistema puede ser descrito caótico por un conjunto de ecuaciones rigurosas, es decir, ecuaciones deterministas.

La dinámica caótica producida en sistemas ópticos tiene considerable atención por sus aplicaciones potenciales en las telecomunicaciones en especial en codificación de comunicaciones ya que el caos óptico puede ser usado para enmascarar los mensajes transmitidos entre un emisor-receptor. El estudio de los fenómenos caóticos es una amplia parte de de la teoría de sistemas no lineales, que con ella nacen ramas importantes dentro de esta área como la óptica no lineal [Senior 2008].

En este capitulo se definen los láseres semiconductor y EDFRL, (erbium doped fiber ring láser) así como también los amplificadores EDFA. Se dan algunos ejemplos de modelos de láseres y se discute su relación con el caos.

4.2. Láseres

La palabra láser proviene de sus siglas en ingles “Light Amplification by the Stimulated Emission of Radiation”, es un dispositivo que utiliza un efecto de la mecánica cuántica, la emisión inducida o estimulada para generar un haz de luz coherente de un medio adecuado y con el tamaño, la forma y la pureza controlados.

Los láseres producen el mejor tipo de luz para la comunicación óptica. La luz láser ideal es la de una sola longitud de onda, esto se relaciona con las características moleculares del material utilizado en el láser y se forma en haces paralelos y es en una sola fase. Es decir, es “coherente”. Los láseres pueden ser modulados (controlados) con mucha precisión, existen récords de pulsos de hasta 0.5 femto segundos. Ademas, pueden producir una potencia relativamente alta, como es el caso de algunos tipos de láseres que producen hasta kilowatts de potencia. En aplicaciones de comunicaciones, están disponibles láseres de semiconductor de potencia aproximada a 20 miliwatts, esto es mucha mas potencia de lo que los LEDS pueden generar [Keiser 2003].

El principio de operación de un láser es la emisión estimulada, ésta ocurre cuando algún estimulante externo (como un fotón incidente) causa que un electrón excitado salte a un nuevo nivel de energía. El fotón emitido en este proceso tiene la misma energía que el fotón incidente y esta en fase con el. Para que se de la emisión estimulada es necesario que ocurran primero una serie de procesos a nivel atómico.

La figura 4.1 muestra el proceso completo.

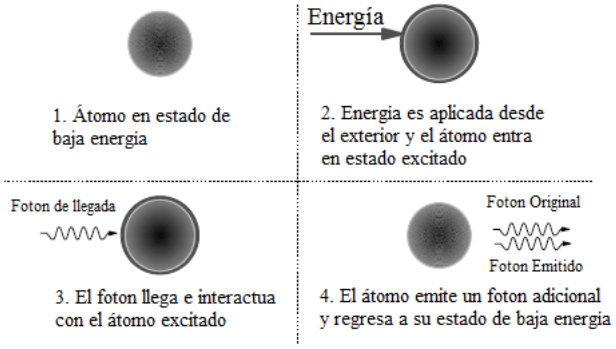


Figura 4.1: Proceso de generación de luz láser

1. Un electrón dentro de un átomo (o una molécula o un ion) comienza en un estado estable de bajo consumo de energía comúnmente llamado el estado ”tierra”.

2. La energía se suministra desde el exterior y es absorbida por la estructura atómica después de lo cual el electrón entra en un estado excitado (mayor energía).

3. Un fotón llega con una energía cercana a la misma cantidad de energía que el electrón necesita para alcanzar el estado estable. (Esto es sólo otra manera de decir que la longitud de onda de los fotones que llegan es muy cercana a la longitud de onda en la cual el electrón excitado emite su propio fotón)

4. El fotón de llegada desencadena una resonancia con el átomo excitado. Como resultado, el electrón excitado sale de éste estado y cambia a un estado más estable renunciando a la diferencia de energía en la forma de un fotón.

Existen diferentes tipos de láseres pero los 4 tipos principales son: el láser FP (Fabry-Perot), el DFB (distributed-feedback), el láser sintonizable y el láser VCSEL (vertical cavity surface-emitting láser).

4.2.1. Láser Fabry-Perot

En el láser Fabry-Perot (FP), la cavidad de acción láser se define por las dos caras de los extremos de la cavidad. Estos se denominan facetas y actúan como espejos que reflejan la luz. Esta estructura se denomina cavidad de Fabry-Perot. Dado que esta cavidad es bastante larga, el láser oscilara simultáneamente en varios modos de frecuencias.

El láser de Fabry-Perot es conceptualmente sólo un LED con un par de espejos finales. Los espejos son necesarios para crear las condiciones adecuadas para que se produzca la acción láser. En la práctica, por supuesto, es algo más complejo que esto, pero no por mucho. El láser de Fabry-Perot recibe su nombre (y su principio de funcionamiento) del hecho de que su cavidad actúa como un resonador Fabry-Perot. Para entender el funcionamiento del láser de Fabry-Perot es necesario primero entender el funcionamiento del filtro de Fabry-Perot (figura 4.2).

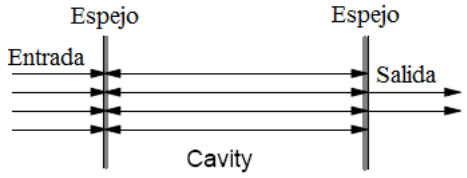


Figura 4.2: Filtro Fabry-Perot

Al colocar dos espejos uno enfrente del otro, forman una cavidad resonante. La luz rebota entre los dos espejos. Cuando la distancia entre los espejos es un

múltiplo entero de medias longitudes de onda, la luz se refuerza en sí. Las longitudes de onda que no son de resonancia se someten a la interferencia destructiva con ellos mismos y se reflejan de distancia. Este principio también se aplica en el láser FP aunque la luz es emitida dentro de la cavidad en sí en lugar de llegar desde el exterior [Dutton 1998].

4.2.2. Láser DFB (distributed-feedback)

En un láser de retroalimentación distribuida (DFB ó distributed feedback) una serie de reflectores estrechamente espaciados proporcionan retroalimentación de luz en una manera distribuida por toda la cavidad. A través de un diseño adecuado de estos reflectores, que normalmente son algún tipo de rejilla, el dispositivo puede ser hecho para oscilar en un sólo único modo con una anchura de línea muy estrecha. Esto significa que emite a una longitud de onda bastante bien definida. La longitud de onda de funcionamiento particular, se puede seleccionar en el momento de la fabricación del dispositivo mediante una elección apropiada de la separación del reflector. Los láseres DFB-monomodo se utilizan ampliamente en sistemas de transmisión de alta velocidad.

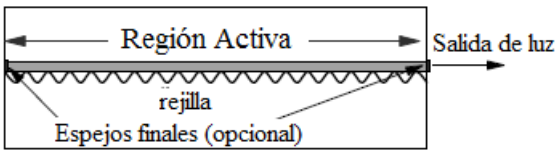


Figura 4.3: Esquemático de un láser DFB

4.2.3. Láser sintonizable

En muchas redes existe la necesidad de sintonizar la longitud de onda de un transmisor láser. Esto es especialmente importante en una red de múltiples longitudes de onda que utiliza muchos transmisores láser que operan en una cuadrícula de longitudes de onda estrechamente espaciadas sobre la misma fibra. Dado que cada láser debe emitir a una longitud de onda precisa (dentro de una fracción de un nanómetro), la capacidad de sintonizar con precisión el láser es esencial. Un número de diferentes tecnologías se han considerado para la toma de láseres sintonizables, teniendo cada uno sus ventajas y limitaciones con respecto al rango de afinación , velocidad de sintonía, potencia y complejidad de control . El láser DFB ha existido por mucho tiempo y es muy fiable, pero su tiempo de optimización es lento [Keiser 2003].

4.2.4. Láser VCSEL (vertical cavity surface emitting láser)

El láser de emisión superficial con cavidad vertical , es un diodo semiconductor que emite luz en un haz cilíndrico vertical de la superficie de una oblea, y ofrece ventajas significativas cuando se compara con láser de emisión lateral comúnmente usados en la mayoría de comunicaciones por fibra óptica. Los láseres VCSEL pueden ser construidos con materiales como GaAs e InGaAs.

Un láser VCSEL consta de pilas de hasta 30 capas delgadas para crear reflejos colocadas en ambos lados de una oblea de semiconductor para formar una cavidad de láser, pueden tener una buena calidad de haz sólo para áreas bastante pequeñas (diámetros de unos pocos microns) y por lo tanto están limitados en términos de potencia de salida.

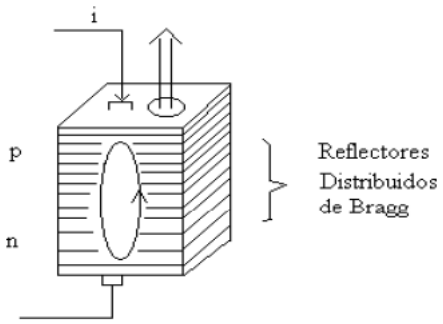


Figura 4.4: Estructura de un láser VCSEL

Para el funcionamiento del láser VCSEL se requiere de una región activa de emisión de luz encerrada en un resonador que consta de dos espejos. En este caso, los espejos son parte de las películas epitaxiales, por lo que estas películas se sobreponen formando una pila. Estos espejos son conocidos como reflectores distribuidos de Bragg [Aguilar Soto 2008].

4.3. Láseres y caos

Fue en 1963 que Lorenz investigó el comportamiento de los fluidos como un modelo atmosférico y demostró que los sistemas no lineales descritos por tres variables podrían exhibir dinámica caótica. Muchos investigadores eran conscientes de la existencia de dinámicas complejas en sistemas bien definidos desde 1900. Poincaré (1913), un destacado matemático francés, fue el primero que destacó la "sensibilidad a las condiciones iniciales" en los sistemas dinámicos. Sin embargo, la investigación moderna de caos se inició a partir del estudio de las dinámicas irregulares y complejas de sistemas no lineales desarrolladas por Lorenz. El caos es no sólo una descripción de un punto de vista diferente de los fenómenos no lineales, sino también en sí mismo una nueva física.

El caos siempre está acompañado por la no linealidad. La no linealidad en un sistema significa simplemente que los valores medidos de las propiedades en el sistema dependen de una manera complicada de las condiciones del estado anterior. La no linealidad en un sistema no siempre garantiza la existencia de caos, pero de alguna forma se requiere de ésta para la realización de la dinámica caótica.

Los sistemas no lineales pueden ser también encontrados en la óptica. Muchos de los materiales y dispositivos ópticos muestran una respuesta no lineal y por lo tanto, son candidatos como elementos no lineales en los sistemas caóticos. Uno de estos dispositivos es el láser. Dado que los láseres son propios sistemas no lineales y se caracterizan típicamente por tres variables; campo, la polarización de la materia, y la inversión de población, también son candidatos para los sistemas caóticos.

A mediados de la década de 1970 se demostró por Haken que los láseres son sistemas no lineales similares al modelo de Lorenz y que muestran una dinámica caótica en sus potencias de salida. Se asumió un modelo de láser de anillo y se consideraron átomos de dos niveles en el láser. Aunque los láseres no siempre se describen por su modelo, la aproximaciones son razonables para la mayoría de los láseres. A partir de entonces, las ecuaciones de velocidad de láser que son descritas por las ecuaciones no lineales con tres variables, se llaman ecuaciones de Lorenz-Haken después de su contribución [Ohtsubo 2007].

Arecchi et al. (1984) investigaron los sistemas de láser desde el punto de vista de los tiempos de relajación característicos de las tres variables y categorizaron a los láseres en 3 clases. De acuerdo con sus clasificaciones, uno o dos de los tiempos de relajación son en general muy rápidos en comparación con las otras escalas de tiempo y la mayoría de los láseres son descritos por ecuaciones de velocidad con una o dos variables. Por lo tanto, estos son sistemas estables que se clasifican en

láseres clase A y B. Sólo los láseres de clase C tienen la descripción completa de las ecuaciones de velocidad con tres variables y pueden mostrar una dinámica caótica. Sin embargo, los láseres clase A y B pueden mostrar dinámicas caóticas cuando uno o más grados de libertad son introducidos en el sistema del láser. En esta tesis se describe y se sincroniza un láser de clase C.

4.4. Amplificador EDFA

Los amplificadores de fibra son amplificadores ópticos que usan fibra dopada. Estos amplificadores necesitan de un bombeo externo con un láser de onda continua a una frecuencia óptica ligeramente superior a la que amplifican. Típicamente, las longitudes de onda de bombeo son 980 nm o 1480 nm y para obtener los mejores resultados en cuanto a ruido se refiere, debe realizarse en la misma dirección que la señal. La figura 4.5 muestra el esquema de funcionamiento de un amplificador básico [P. Martin *et. al.* 2010].

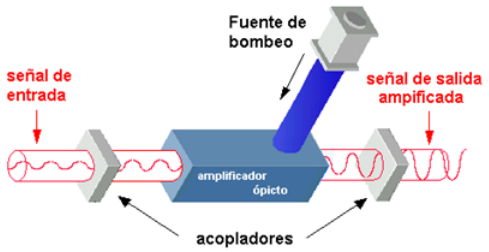


Figura 4.5: Esquema de funcionamiento de un amplificador óptico básico

El láser EDFA es un amplificador óptico, el cual sin necesidad de convertir las señales ópticas a eléctricas las amplifica directamente, el fundamento de un amplificador óptico es el proceso de emisión estimulada al igual que en un láser. Su estructura es similar a la de un láser salvo que no posee una realimentación para evitar que el dispositivo oscile, de forma que puede elevar el nivel de po-

tencia de la señal pero no generar una señal óptica coherente. Los EDFA son los amplificadores de fibra más empleados en la actualidad no solo en el contexto de comunicaciones de largo alcance de fibra óptica, sino que de manera eficiente pueden amplificar la luz en la región de longitud de onda de 1550-nm, donde las fibras de telecomunicaciones tienen el mínimo de pérdidas.

Una configuración típica de un amplificador EDFA se muestra en la figura 4.5. Su núcleo es la fibra óptica dopada con erbio, que suele ser una fibra monomodo. En este caso, la fibra activa es "bombeada" con la luz de dos diodos láser (bombeo bidireccional), aunque el bombeo unidireccional hacia adelante o hacia atrás es también muy común.

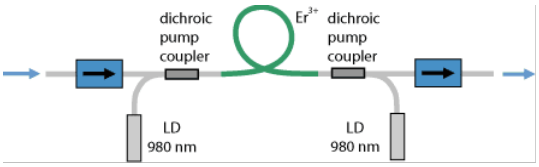


Figura 4.6: Configuración típica de un amplificador EDFA

Los amplificadores EDFA cumplen con varias funciones dentro de los sistemas de comunicaciones de fibra óptica, las aplicaciones más importantes son las siguientes:

- La potencia de un transmisor de datos puede ser impulsada con un EDFA de alta potencia antes de entrar en un largo tramo de fibra u otro dispositivo que tenga grandes pérdidas, como por ejemplo un divisor de fibra óptica. Al amplificar la señal aseguramos que las pérdidas no sean tan notables.

- El amplificador también puede ser utilizado frente a un receptor de datos si la señal que llega es débil. A pesar de que el amplificador produce ruido, esto puede mejorar la relación señal-ruido y la tasa de transmisión de datos posible, ya que el ruido del amplificador puede ser más débil que el ruido de entrada del receptor. Es más común, sin embargo, utilizar fotodiodos de avalancha, que amplificación de señal incorporados.

- Los amplificadores se pueden conectar en una especie de conexión en serie con la señal óptica para utilizarlos entre largos períodos de transmisión. La utilización de amplificadores múltiples en un enlace largo de fibra óptica tienen la ventaja de que pueden compensar las grandes pérdidas de transmisión sin dejar que la caída de la potencia óptica llegue a niveles muy bajos, lo que echaría a perder la relación señal-ruido, evita además la transmisión de exceso de potencias ópticas en otros lugares [www.rp-photonics.com].

Los elementos básicos para implementar un EDFA son:

- El medio activo donde se produce la inversión de población. Formado por un tramo de fibra óptica de SiO_2 con el núcleo dopado con iones de erbio.

- La fuente de bombeo óptico a 1480 o 980nm, formada por un láser semiconductor.

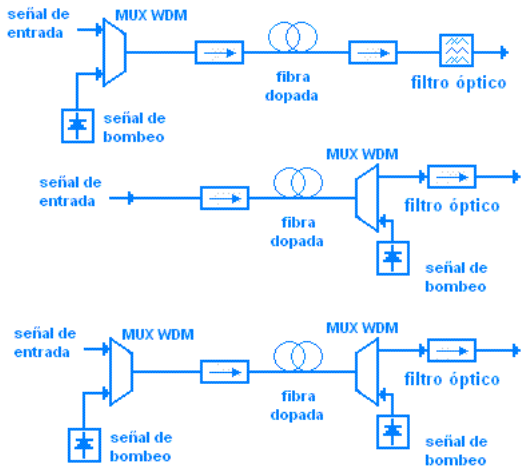


Figura 4.7: Configuraciones de un amplificador EDFA

En la figura 4.7 se muestran las configuraciones posibles del EDFA. La primer configuración es la más empleada generalmente. La señal que hay que amplificar y la señal de bombeo se inyectan al EDFA combinadas por medio de un acoplador. El primer aislador se emplea para impedir la propagación hacia fuera del EDFA de emisión espontánea (ruido ASE) que se genera y se propaga en sentido contrario al de la transmisión. El bombeo y la amplificación se realizan en el mismo sentido que la propagación. A la salida se coloca otro aislador que evita la entrada al EDFA y por tanto su amplificación de cualquier señal reflejada. Finalmente se emplea un filtro óptico para filtrar el ruido ASE, generado en el amplificador, que se encuentre fuera de la banda de la señal útil.

La siguiente configuración se diferencia de la anterior en que la señal de bombeo se inyecta al EDFA en sentido contrario a la propagación. El aislador de la entrada además de cumplir las funciones anteriores, tiene la misión de evitar la propagación de la señal de bombeo fuera del amplificador. La ventaja de esta configuración es que permite ganancias más altas, pero sus características de ruido son peores.

La tercera configuración es una combinación de las dos anteriores. Consiste en un doble bombeo, por lo que se denomina bombeo dual o bidireccional. La ganancia por tanto puede llegar a duplicarse. Este esquema es muy empleado en la implementación de amplificadores repetidores [Aguilar Sánchez 2010].

4.4.1. Amplificador de semiconductor

Los amplificadores ópticos de semiconductor ("SOA" por sus siglas en ingles "semiconductor optical amplifier") se basan en la misma tecnología que los diodos láser. Un SOA es esencialmente un láser de semiconductor que está funcionando por debajo de su punto de umbral. El atractivo de esto es que los SOA pueden operar en todas las bandas de fibra de longitud de onda.

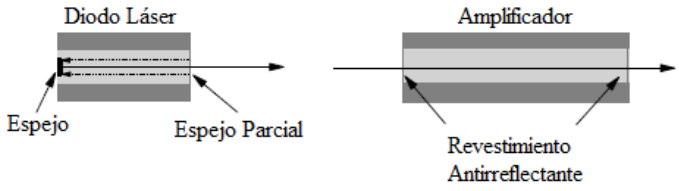


Figura 4.8: Relación de un amplificador óptico de semiconductor con un láser

Por otra parte, ya que se basan en la tecnología de semiconductores estándar, que pueden ser integrados fácilmente en el mismo sustrato que otros dispositivos y circuitos (por ejemplo, acopladores, aisladores ópticos, y los circuitos del receptor) ópticos. En comparación con un DFA (doped fiber amplifier, como por ejemplo un EDFA), el amplificador SOA consume menos energía, se construye con un menor número de componentes, y puede ser alojado de forma compacta en un paquete estándar de mariposa de 14 pines. Los amplificadores SOA tienen una respuesta de ganancia más rápida (del orden de 1 a 100 ps), lo que son utilizados para la conmutación y procesamiento de señales [Keiser 2003].

4.4.2. Amplificadores de efecto Raman

Los amplificadores que utilizan el principio de dispersión estimulada Raman fueron ampliamente investigados a fines de 1980, pero el interés se desvaneció después de la invención del amplificador EDFA. Los amplificadores Raman son muy eficaces, pero tenían un problema importante ya que los láseres de bajo costo de longitud de onda apropiada no estaban disponibles. En 1997 hay un renacimiento del interés en ellos (al menos en parte), debido a las innovaciones en el diseño de fibra de rejilla de Bragg.

A diferencia de los EDFA y de los SOA, los amplificadores Raman se basan en un una interacción no lineal entre la señal óptica y la señal de bombeo de alta potencia. De esta forma, la fibra convencional ya instalada puede ser usada como medio con ganancia para la amplificación Raman. Sin embargo, es mejor emplear fibras especialmente diseñadas (fibra altamente no lineal) en las que se introducen dopantes y se reduce el núcleo de la fibra para incrementar su no linealidad [P. Martin et. al. 2010].

4.5. Conclusiones

En este capitulo se definieron los conceptos de láseres y su relación con el caos. Actualmente con el desarrollo de las tecnologías modernas, cada ves es mas fácil encontrar dispositivos como los láseres, lo que los convierte en un tema de estudio de bastante interés. La combinación de caos y láseres se dio a raíz de la exigencia de las comunicaciones modernas, así como también del aprovechamiento de este fenómeno físico dentro de los mismos. Con el desarrollo de los amplificadores ópticos se fortalece aun mas esta relación, ya que cumplen un papel importante al evitar el cambio de óptico a eléctrico amplificando la luz láser directamente.

Los emisores de luz láser caótica ofrecen una infraestructura tecnológica novedosa que puede resolver importantes problemas en los sistemas de comunicación y en la tecnología de la información, incluyendo la privacidad, la eficiencia computacional y el consumo de energía.

Capítulo 5

Sincronización de láseres

5.1. Introducción

Los sistemas de láseres acoplados exhiben una gran variedad de estados dinámicos, incluyendo sincronización de oscilaciones caóticas y periódicas. Estos comportamientos se encuentran en diferentes sistemas de la naturaleza y la ciencia tales como: reacciones químicas, dinámica de población, neuronas acopladas y dinámica de fluidos entre otros. La comprensión de la dinámica de láseres acoplados es esencial tanto para la ciencia fundamental como para varias aplicaciones en cuanto a comunicaciones caóticas se refiere [Almanza 2009].

Para sincronizar las formas de onda caóticas, los sistemas de láser deben ser acoplados entre sí. En los esquemas de acoplamiento es muy importante considerar la sincronización de caos y estas se pueden clasificar principalmente en dos tipos: unidireccional y bidireccional. Uno de los esquemas más simples de acoplamiento para la sincronización de caos es la inyección unidireccional de un láser (conocido como láser maestro o drive) a otro láser (conocido como láser esclavo o response).

Estos esquemas de acoplamiento pueden ser extendidos a un láser con señal de auto-retroalimentación. Esta señal en el láser maestro no solo es usada para general caos, también es usada para mantener la simetría de el sistema entre los láseres maestro y esclavo. Otra clasificación de los esquemas de acoplamiento puede ser introducida por acoplamiento coherente e incoherente. En el acoplamiento coherente, el campo eléctrico de la salida de un láser maestro es directamente inyectado en la cavidad del láser esclavo. Por otra parte, el acoplamiento incoherente indica que solo la intensidad de salida del láser maestro interactúa con la intensidad del láser o la inversión de población del láser esclavo [uchida 2012].

5.2. Sincronización Caótica en Láseres

La idea de sincronización del caos fue rápidamente aplicada a circuitos electrónicos reales después de la propuesta de Pecora y Carrol. Sin embargo, el método no es aplicable en forma directa a los sistemas de láser ya que no es posible dividir en subsistemas las dinámicas de las variables del láser.

Las estrategias desarrolladas de sincronización del caos para la mayoría de los sistemas no lineales, tales como circuitos no lineales, no se pueden aplicar directamente en láseres debido a un número de diferencias significativas entre los láseres y otros sistemas dinámicos no lineales. Dichas diferencias son las siguientes:

- Un láser es una entidad integrada que no puede ser fácilmente descompuesto en subsistemas.

- Para un láser dado, no es posible ajustar arbitrariamente sus parámetros dinámicos intrínsecos y pueden ser sólo variados por su dependencia lineal con la potencia del láser.

- Una de sus variables dinámicas, la densidad de portadores, no es directamente accesible externamente, por lo que no se puede utilizar para acoplar el transmisor y el receptor para la sincronización de láseres.

- Cuando la intensidad de campo es transmitida y acoplada al receptor, la magnitud y fase son transmitidas y acopladas por igual. No es posible transmitir solo la magnitud y no la fase, o bien, la fase y no la magnitud [Ohtsubo 2007].

De forma contraria, las condiciones para obtener una sincronización idéntica a través de sistemas de láseres acoplados son principalmente las siguientes:

- Todos los sistemas de láser deben constar de dispositivos idénticos con los ajustes de parámetros idénticos.

- Todos los sistemas de láser deben estar sujetos a la señal del láser maestro o de realimentación. La "simetría" de los sistemas de láseres acoplados resulta en una solución síncrona de los sistemas dentro del contexto matemático, por lo que una sincronización idéntica puede ser alcanzada.

- La solución síncrona debe de ser estable [Uchida 2012].

5.3. Sincronización Caótica Generalizada y Completa

Existen dos orígenes diferentes de sincronización de caos en sistemas diferenciales de retardo no lineales, tales como sistemas de láser de semiconductor con realimentación óptica y retroalimentación optoelectrónica. El primero consta de sincronización de las señales caóticas con base en los fenómenos ópticos de inyección. El segundo es la sincronización completa del caos en el que dos sistemas pueden ser descritos por un conjunto de ecuaciones diferenciales idénticas dentro del contexto matemático. En el sentido ordinario, sabemos que la sincronización caótica ocurre cuando el receptor recibe una señal caótica del transmisor y dicha señal es recuperada exitosamente por el receptor.

El fenómeno de inyección óptica viene dado cuando la salida del receptor es por lo general una señal amplificada de la señal transmitida. Por lo tanto, una excelente señal sincronizada es obtenida en el sistema receptor siempre y cuando se logre una clara amplificación. Sin embargo, existen distorsiones que se introducen a las formas de onda obtenidas por inyección óptica. A este esquema se le conoce como sincronización generalizada.

La diferencia entre sincronización generalizada y sincronización completa esta bien definida. El esquema de sincronización de caos de un sistema en particular puede ser distinguido fácilmente calculando el tiempo de retardo entre el transmisor y receptor.

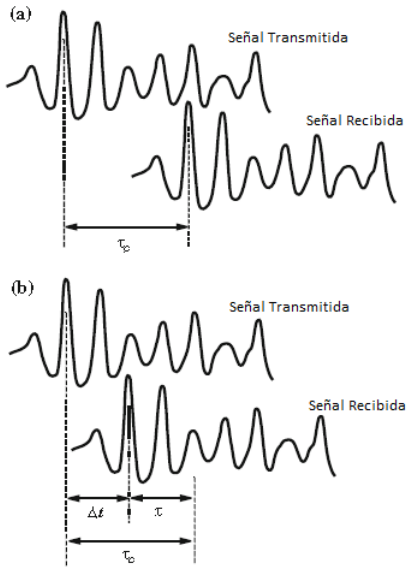


Figura 5.1: Tiempo de retardo entre el transmisor y receptor en una sincronización caótica. La figura a) corresponde a una sincronización caótica generalizada y la figura b) corresponde a una sincronización caótica completa. τ_c representa el tiempo de transmisión del transmisor al receptor y τ representa el tiempo de retroalimentación óptica en el transmisor y receptor.

5.4. Sincronización de láseres de semiconductor mediante formas hamiltonianas

Los láseres semiconductores directamente modulados han sido recientemente utilizados para exhibir caos en ciertos rangos de frecuencia y corrientes de modulación. Se basan en un sistema simple de dos ecuaciones de velocidad que rigen la dinámica de poblaciones de electrones y fotones dentro de la cavidad del láser. La modulación de la corriente proporciona el tercer grado de libertad necesario para el caos, haciendo que el sistema no lineal sea no autónomo.

La respuesta dinámica de un láser semiconductor se ve fuertemente afectada por la ganancia no lineal que debe ser incluida en las ecuaciones de velocidad para un modelado realista del láser .

El siguiente modelo de láser semiconductor exhibe oscilaciones caóticas y periódicas a medida que varia la amplitud y la frecuencia de modulación. El sistema es sincronizado mediante formas hamiltonianas.

Modelo

$$\frac{dN}{dt} = \frac{1}{\tau_\epsilon} = \left[\frac{I_b + I_m sin(\phi)}{I_{th}} - N - \frac{N-\delta}{1-\delta} P \right]$$

$$\frac{dP}{dt} = \frac{1}{\tau_P} \left(\frac{N-\delta}{1-\delta} (1 - \epsilon P) P - P + \beta N \right)$$

$$\frac{d\phi}{dt} = 2\pi f_m$$

Parámetros del modelo:

Tiempo de Vida del Electrón	$\tau_\epsilon = 3 \times 10^{-9}$
Corriente de Umbral	$I_{th} = 26 \times 10^{-3}$
Corriente de Polarización	$I_b = 1.5 \times I_{th}$
Amplitud de Modulación	$I = 0.55 \times I_{th}$
Constante Adimensional	$\delta = 692 \times 10^{-3}$
Tiempo de vida del foton	$\tau_p = 6 \times 10^{-12}$
Reducción de ganancia no lineal	$\epsilon = 1 \times 10^{-4}$
Factor de emisión espontanea	$\beta = 5 \times 10^{-5}$
Frecuencia de modulación	$f_m = 0.8 \times 10^{9}$

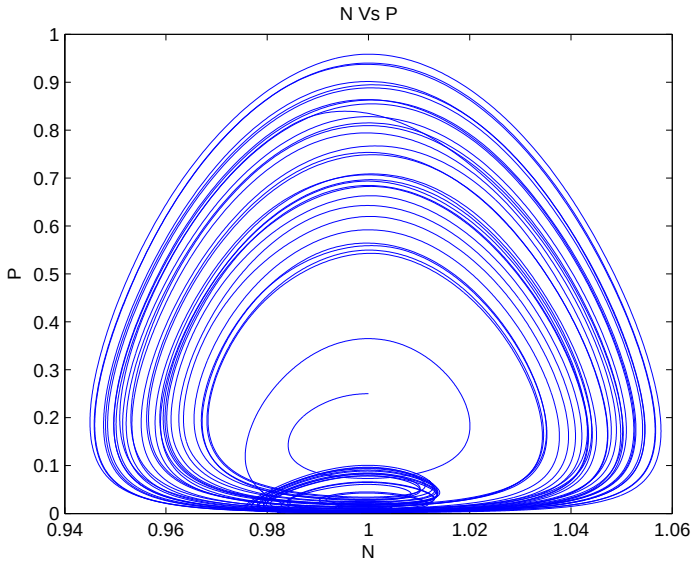


Figura 5.2: Gráfica de fase del modelo del láser semiconductor

Los estados N y P representan la densidad normalizada de portadores y fotones respectivamente. Teóricamente tenemos acceso a estos parámetros, pero en la practica no es posible. El procedimiento para sincronizar el modelo mediante formas hamiltonianas es el siguiente:

Simplificamos el modelo mediante los siguientes cambios de variable

$A = \frac{1}{3\times10^{-9}}$ $\qquad$ $D = \frac{\delta}{1-\delta}A$

$V = A\,\frac{I_m}{I_{th}}$ $\qquad$ $E = \frac{1}{6\times10^{-12}}$

$C = \frac{1}{1-\delta}A$ $\qquad$ $F = \frac{1}{1-\delta}E$

$$
\begin{aligned}
\dot{N} &= 500 \times 10^6 + V sin\phi - AN - CNP - DP \\
\dot{p} &= FNP - FN\epsilon P^2 - F\delta P + F\delta\epsilon P^2 - EP + E\beta N \\
\dot{\phi} &= 2\pi f_m
\end{aligned}
$$

Por comodidad sustituimos los estados del sistema por $\dot{x}$

$$
\begin{aligned}
\dot{x_1} &= 500 \times 10^6 + V sin(x_3) - Ax_1 - Cx_1x_2 - Dx_2 \\
\dot{x_2} &= Fx_1x_2 - F\epsilon x_1x_2^2 - F\delta x_2 + F\delta\epsilon x_2^2 - Ex_2 + E\beta x_1 \\
\dot{x_3} &= 2\pi f_m
\end{aligned}
$$

Llevamos el modelo a su forma hamiltoniana utilizando la siguiente función de energía

Función de Energía

$$H(x) = \frac{1}{2}(x_1^2,\, x_2^2,\, x_3^2)$$

$$\frac{\partial H}{\partial x} = [x_1,\, x_2,\, x_3]$$

Expresamos el modelo en su forma hamiltoniana:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & -\frac{E\beta+D}{2} & 0 \\ \frac{E\beta+D}{2} & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} -A & -D+\frac{E\beta+D}{2} & 0 \\ -D+\frac{E\beta+D}{2} & -F\delta-E & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$+ \begin{bmatrix} 500\times 10^6 + Vsin(x_3) - Cx_1x_2 \\ Fx_1x_2 - F\epsilon x_1x_2^2 + F\delta\epsilon x_2^2 \\ 2\pi f_m \end{bmatrix}$$

Simplificando la ecuación:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2}(-E\beta-D) & 0 \\ -\frac{1}{2}(-E\beta-D) & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} -A & \frac{1}{2}(E\beta-D) & 0 \\ \frac{1}{2}(E\beta-D) & -F\delta-E & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

$$+ \begin{bmatrix} 500\times 10^6 + Vsin(x_3) - Cx_1x_2 \\ Fx_1x_2 - F\epsilon x_1x_2^2 + F\delta\epsilon x_2^2 \\ 2\pi f_m \end{bmatrix} \qquad (5.1)$$

La señal a transmitir en el observador sería x_2 por lo que tomamos el vector $c = [010]$, y procedemos a formar una matriz K tal que podamos comprobar que la matriz simétrica $\left[S - (KC + C^T K^T)\right]$ es definida negativa o semidefinida, para ello tomamos una matriz $K = [k_1\, k_2\, k_3]^T$.

$$KC + C^T K^T = \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \begin{bmatrix} k_1 & k_2 & k_3 \end{bmatrix}$$

$$KC + C^T K^T = \begin{bmatrix} 0 & k_1 & 0 \\ 0 & k_2 & 0 \\ 0 & k_3 & 0 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ k_1 & k_2 & k_3 \\ 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & k_1 & 0 \\ k_1 & 2k_2 & k_3 \\ 0 & k_3 & 0 \end{bmatrix}$$

$$\left[S - (KC + C^T K^T)\right] = \begin{bmatrix} -A & \frac{1}{2}(E\beta - D) & 0 \\ \frac{1}{2}(E\beta - D) & -F\delta - E & 0 \\ 0 & 0 & 0 \end{bmatrix} - \begin{bmatrix} 0 & k_1 & 0 \\ k_1 & 2k_2 & k_3 \\ 0 & k_3 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} -A & \frac{1}{2}(E\beta - D) - k_1 & 0 \\ \frac{1}{2}(E\beta - D) - k_1 & -F\delta - E - k_2 & -k_3 \\ 0 & -k_3 & 0 \end{bmatrix} \tag{5.2}$$

El observador queda como

$$\begin{bmatrix} \dot{\epsilon}_1 \\ \dot{\epsilon}_2 \\ \dot{\epsilon}_2 \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2}(-E\beta - D) & 0 \\ -\frac{1}{2}(-E\beta - D) & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \epsilon_1 \\ \epsilon_2 \\ \epsilon_3 \end{bmatrix} + \begin{bmatrix} -A & \frac{1}{2}(E\beta - D) & 0 \\ \frac{1}{2}(E\beta - D) & -F\delta - E & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} \epsilon_1 \\ \epsilon_2 \\ \epsilon_3 \end{bmatrix}$$

$$+ \begin{bmatrix} 500 \times 10^6 + Vsin(x_3) - Cx_1x_2 \\ Fx_1x_2 - F\epsilon x_1 x_2^2 + F\delta\epsilon x_2^2 \\ 2\pi f_m \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \\ k_3 \end{bmatrix} e_y$$

La dinámica del error de sincronización esta dada por

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \end{bmatrix} = \begin{bmatrix} 0 & \frac{1}{2}(-E\beta - D - k_1) & 0 \\ -\frac{1}{2}(-E\beta - D - k_1) & 0 & \frac{1}{2}k_3 \\ 0 & -\frac{1}{2}k_3 & 0 \end{bmatrix} \frac{\partial H}{\partial e}$$

$$+\begin{bmatrix} -A & \frac{1}{2}(E\beta - D - k_1) & 0 \\ \frac{1}{2}(E\beta - D - k_1) & -F\delta - E - k_2 & -\frac{1}{2}k_3 \\ 0 & -\frac{1}{2}k_3 & 0 \end{bmatrix} \frac{\partial H}{\partial e}$$

Simplificando y haciendo las operaciones correspondientes, los errores quedan como

$$\begin{aligned} \dot{e}_1 &= -e_2 D - k_1 e_2 - A e_1 \\ \dot{e}_2 &= -e_1 E\beta + e_2(-F\delta - E - k_2) \\ \dot{e}_3 &= -k_3 e_2 \end{aligned} \tag{5.3}$$

Aplicando el teorema establecido en [Sira-Ramirez y Cruz-Hernández 2000; 2001] encontramos la matriz de las constantes K

$$2[S - \frac{1}{2}(KC + C^T K^T)] = \begin{bmatrix} -2A & E\beta - D - k_1 & 0 \\ E\beta - D - k_1 & 2(F\delta - E - k_2) & -k_3 \\ 0 & -k_3 & 0 \end{bmatrix}$$

Aplicando el criterio de silvester y haciendo que la matriz sea <0 para obtener los valores de k_1, k_2 y k_3 tenemos lo siguiente:

Calculamos los menores principales de la matriz :

$$\begin{bmatrix} -2A & E\beta - D - k_1 & 0 \\ E\beta - D - k_1 & 2(F\delta - E - k_2) & -k_3 \\ 0 & -k_3 & 0 \end{bmatrix} < 0$$

$$\triangle_1 = -2A$$

$$\triangle_2 = det \begin{bmatrix} -2A & E\beta - D - k_1 \\ E\beta - D - k_1 & 2(F\delta - E - k_2) \end{bmatrix} < 0$$

Simplificando y resolviendo tenemos que:

$$k_2 < \frac{k_1^2 - 2mk_1 + m^2 - R}{4A},\ m = E\beta - D, \quad R = 4A(F\delta + E)$$

$$\triangle_3 = det \begin{bmatrix} -2A & E\beta - D - k_1 & 0 \\ E\beta - D - k_1 & 2(F\delta - E - k_2) & -k_3 \\ 0 & -k_3 & 0 \end{bmatrix} < 0$$

$$k_3 > 0 \tag{5.4}$$

Si hacemos $k_1 = 0$

$$k_2 < \frac{(E\beta - D)^2}{4A} - F\delta + E$$

Graficando los errores del sistema (5.3) con los valores obtenidos de $k_1,\ k_2\, y\, k_3$ obtenemos que los errores $\dot{e}_1$ y $\dot{e}_2$ tienen una convergencia a cero, mientras que el error $\dot{e}_3$ tiende a un valor distinto. De acuerdo la definición de sincronización caótica dada en la capitulo 3 [Cruz-Hernández y Mortynyuk 2009], buscamos que los errores de sincronía tiendan a cero.

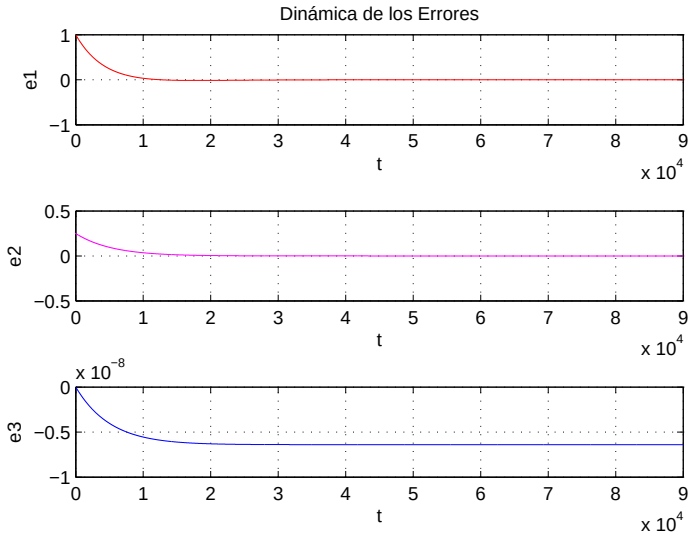


Figure 5.3: Errores de sincronía $\dot{e}_1$, $\dot{e}_2$ y $\dot{e}_3$

Como se puede apreciar en la figura 5.3, el error de sincronía $\dot{e}_3$ no converge a cero, esto es debido a que en el sistema mismo el estado $\dot{x}_3$ es una constante, lo cual es imposible de llevar a cero puesto que nuestra condición esta dada por $k_3 > 0$.

5.5. Sincronización de láseres EDFRL mediante formas hamiltonianas

Los láseres de fibra dopada con erbio han sido objeto de estudio debido a sus potenciales aplicaciones en diversos campos, tales como las comunicaciones, la detección, la espectroscopia y la medicina. Desde un punto de vista fundamental de la dinámica del láser, los láseres de fibra son tambien de gran interes ya que se caracterizan por tiempos de relajacion lenta. El estudio del caos en este tipo de láseres se inicio con los láseres de fibra dopados con Nd [Liguo Luo 1998].

El siguiente modelo de láser EDFRL es un sistema acoplado de segundo

orden no homogeneo, no lineal, invariante en el tiempo y no autonomo. Es un láser de tres niveles con tres estados, considerado clase B y se rige por dos ecuaciones de velocidad, una para el campo E_{LA} y otra para la inversion de poblacion D_A.

Modelo del Láser (EDFRL)

$$\begin{aligned} \dot{E}_{LA} &= -k_a(E_{LA} - c_a S_m) + g_a E_{LA} D_A + \xi_{LA} \\ \dot{D_A} &= -\frac{1}{\tau}\left[(1 + I_{PA} + E_{LA}^2)\right] D_A - I_{PA} + 1 \end{aligned}$$

$$\begin{aligned} k_a &= k_{a0}\left(1 + m_a sin(\omega_a t)\right) \\ S_{in} &= S_0(1 - sin(\omega_s t)) \end{aligned}$$

donde E_{LA} es el campo eléctrico y D_A es la densidad de la inversión de población.

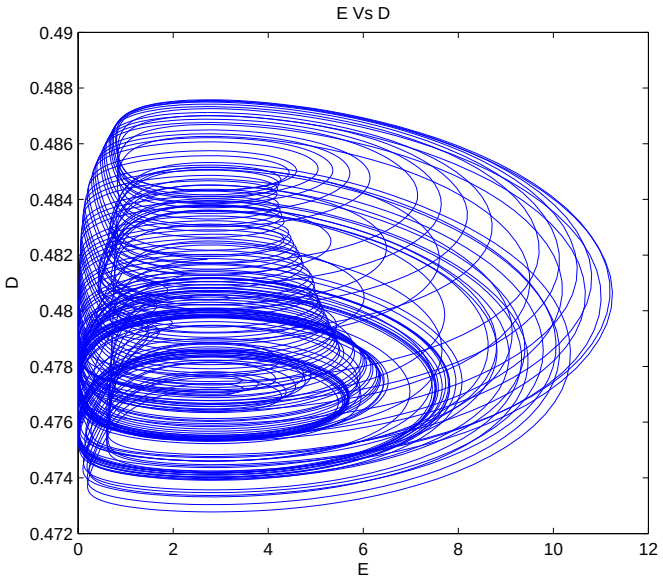


Figura 5.4: Gráfica de Fase del modelo del láser EDFRL

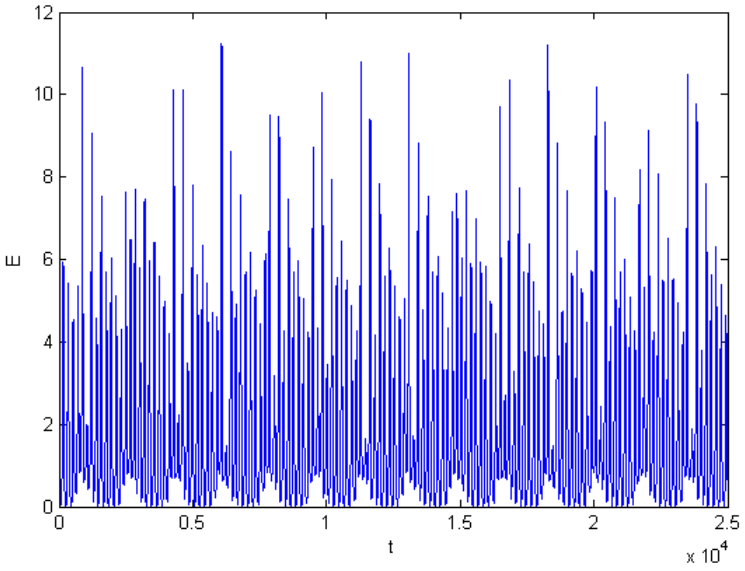


Figura 5.5: Intensidad de campo E_{LA}

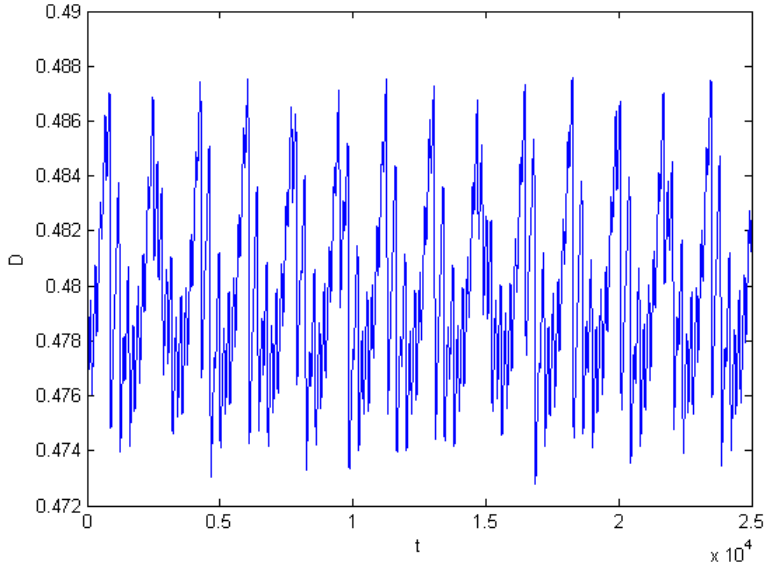


Figura 5.6: Densidad de la inversión de población D_A

Para representar el modelo en su forma hamiltoniana es necesario simplificarlo y por cuestiones prácticas hacer los cambios de variable $\dot{E}_{LA}$ y $\dot{D}_A$ por $\dot{x}_1$ y $\dot{x}_2$

$$\dot{x}_1 = -k_a x_1 + c_a s_{in} k_a + g_a x_1 x_2 + \xi_{LA}$$

$$\dot{x_2} = ABx_2 - Ax_1^2 x_2 + AI_{PA} - A \tag{5.5}$$

Donde $A = \frac{1}{\tau}$, $B = (-1 - I_{PA})$

Representando la ecuación 5.5 en su forma canonica hamiltoniana y usando $\frac{\partial H}{\partial x} = [x_2,\, x_1 x_2]$ tenemos:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} 0 & \frac{g_a - AB}{2} \\ -\left(\frac{g_a - AB}{2}\right) & 0 \end{bmatrix} \begin{bmatrix} x_2 \\ x_1 x_2 \end{bmatrix} + \begin{bmatrix} 0 & \frac{g_a + AB}{2} \\ \frac{g_a + AB}{2} & 0 \end{bmatrix} \begin{bmatrix} x_2 \\ x_1 x_2 \end{bmatrix}$$

$$+ \begin{bmatrix} -k_a x_1 + c_a s_{in} k_a + \xi_{LA} \\ -A x_1^2 x_2 + A I_{PA} - A \end{bmatrix}$$

El obervador (esclavo) quedaria como:

$$\begin{bmatrix} \dot{\epsilon}_1 \\ \dot{\epsilon}_2 \end{bmatrix} = \begin{bmatrix} 0 & \frac{g_a - AB}{2} \\ -\left(\frac{g_a - AB}{2}\right) & 0 \end{bmatrix} \frac{\partial H}{\partial \epsilon} + \begin{bmatrix} 0 & \frac{g_a + AB}{2} \\ \frac{g_a + AB}{2} & 0 \end{bmatrix} \frac{\partial H}{\partial \epsilon}$$

$$+ \begin{bmatrix} -k_a x_1 + c_a s_{in} k_a + \xi_{LA} \\ -A x_1^2 x_2 + A I_{PA} - A \end{bmatrix} + \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} (x_1 - \epsilon_1)$$

Como la señal a transmitir es x_1, el vector $C = \begin{bmatrix} 1 & 0 \end{bmatrix}$ por lo que los errores de sincronia estan dados por

$$\dot{e} = \jmath(x) \frac{\partial H(e)}{\partial e} + (I + S) \frac{\partial H(e)}{\partial e} - k e_y$$

$$e_y = C \frac{\partial H}{\partial e},\; e_y \,\epsilon\, R^m$$

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \end{bmatrix} = \begin{bmatrix} 0 & \frac{g_a - AB}{2} \\ -\left(\frac{g_a - AB}{2}\right) & 0 \end{bmatrix} \frac{\partial H}{\partial e} + \begin{bmatrix} 0 & \frac{g_a + AB}{2} \\ \frac{g_a + AB}{2} & 0 \end{bmatrix} \frac{\partial H}{\partial e}$$

$$- \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} (e_y)$$

$$e_y = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} e_2 \\ e_1 e_2 \end{bmatrix} = e_2$$

Realizando las operaciones matriciales podemos representar el error en su forma convencional

$$\begin{aligned} \dot{e}_1 &= e_1 e_2 g_a - k_1 e_2 \\ \dot{e}_2 &= e_2(AB - k_2) \end{aligned} \tag{5.6}$$

Determinamos los rangos de las ganancias del observador mediante

$$2\left[s - \frac{1}{2}\left[KC + C^T K^T\right]\right] < 0$$

$$2\left[\begin{bmatrix} 0 & \frac{g_a + AB}{2} \\ \frac{g_a + AB}{2} & 0 \end{bmatrix} - \frac{1}{2}\left[\begin{bmatrix} k_1 \\ k_2 \end{bmatrix}\begin{bmatrix} 1 & 0 \end{bmatrix} + \begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} k_1 & k_2 \end{bmatrix}\right]\right] < 0$$

$$\left[\begin{bmatrix} 0 & g_a + AB \\ g_a + AB & 0 \end{bmatrix} - \left[\begin{bmatrix} k_1 & 0 \\ k_2 & 0 \end{bmatrix} + \begin{bmatrix} k_1 & k_2 \\ 0 & 0 \end{bmatrix}\right]\right] < 0$$

$$\begin{bmatrix} 0 & g_a + AB \\ g_a + AB & 0 \end{bmatrix} - \begin{bmatrix} 2k_1 & k_2 \\ k_2 & 0 \end{bmatrix} < 0$$

$$\begin{bmatrix} -2k_1 & g_a + AB - k_2 \\ g_a + AB - k_2 & 0 \end{bmatrix} < 0 \tag{5.7}$$

Aplicando el teorema de silvester para obtener los valores de las ganancias k_1 y k_2, tomamos los menores principales de la matriz (5.7), el primer menor es $-2k_1$

$$\triangle_1 = -2k_1 < 0 \qquad \therefore\ k_1 > 0$$

Para el segundo menor calculamos el determinante de la matriz

$$\triangle_2 = (-2k_1)(0) - (g_a + AB - k_2)(g_a + AB - k_2)$$

$$\triangle_2 = -(g_a + AB - k_2)^2$$

Donde

$$B = (-1 - I_{PA}) \quad I_{PA} = 10 \quad B = -11 \quad \tau = 10^{-3}$$

$$g_a = 2k_{a0} \quad k_{a0} = 3.3 \times 10^7 \quad g_a = 6.6 \times 10^7$$

$$AB = \left(\frac{1}{10^{-3}}\right)(-11) = -1,100$$

Sustituimos por conveniencia $g_a + AB$ por C

$$C = g_a + AB$$

$$C = 6.6 \times 10^7 - 1,100 \rightarrow C = 65\,998.9 \times 10^3$$

$$\triangle_2 = -(C - k_2)^2$$

$$\triangle_2 = -(C^2 - 2Ck_2 + k_2^2)$$

$$-(C^2 - 2Ck_2 + k_2^2) < 0$$

Resolviendo la ecuación cuadratica y posteriormente la desigualdad tenemos que $k_2 < C$ debido a que en $k_2 = C$, $k_2 = 0$

Una ves obtenidos los valores de las ganacias K_1, K_2 y K_3 es posible obtener las graficas de los errores de sincronía, graficas de fase y los estados sincronizados del modelo.

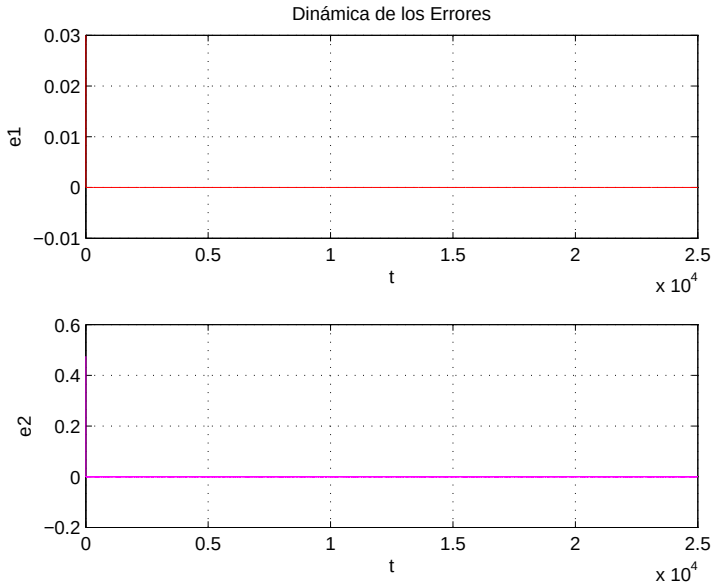


Figura 5.7: Gráfica de los errores de sincronía $\dot{e}_1$ y $\dot{e}_2$.

Gráficas de Estados

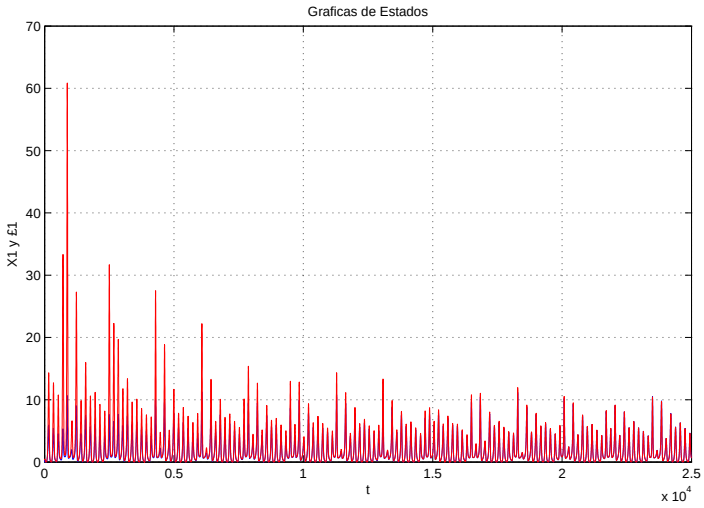


Figura 5.8: Sincronización de maestro (azul) $\dot{x}_1$ y esclavo (rojo) ε_1

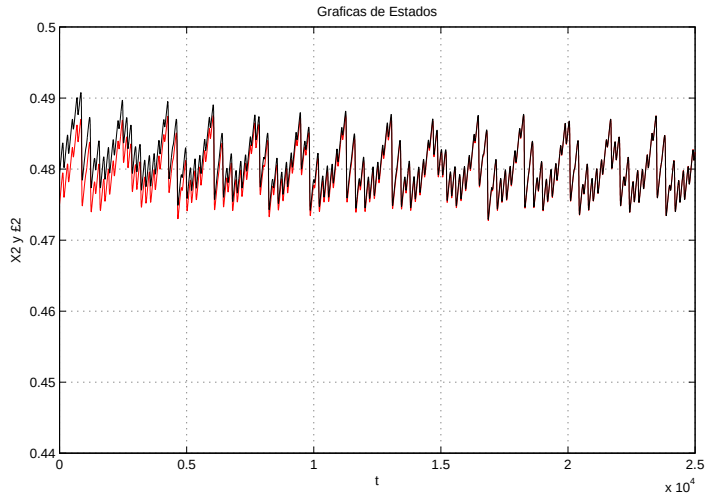


Figura 5.9: Sincronización del maestro (rojo) $\dot{x}_2$ y el esclavo (negro) ε_2

Gráficas de Fase

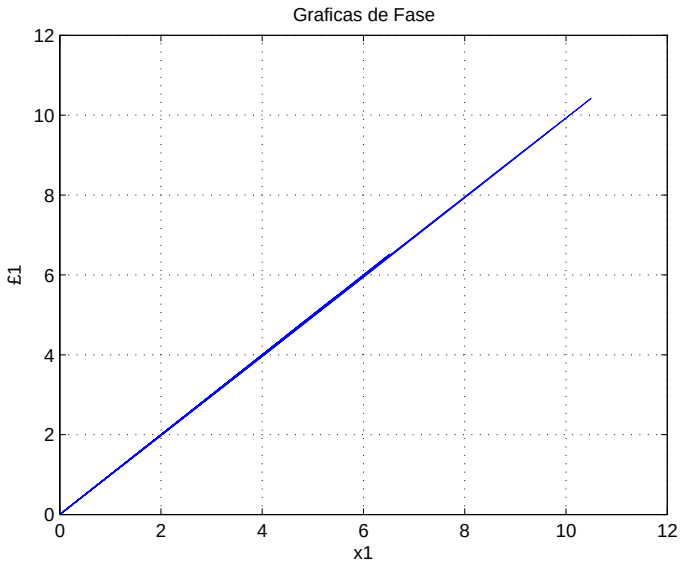


Figura 5.10: Gráfica de fase $\dot{x}_1$vs ε_1

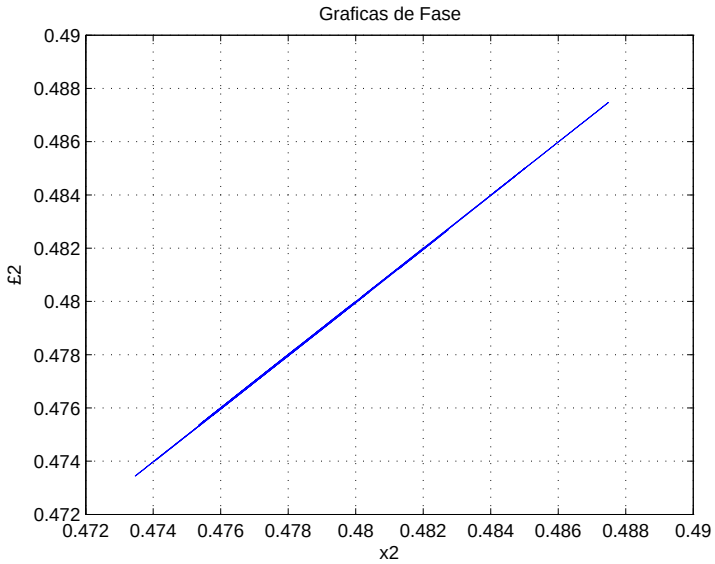


Figura 5.11: Gráfica de fase $\dot{x}_2$vs ε_2

5.6. Conclusiones Generales y Trabajo a Futuro

Se hizo un análisis sobre la sincronización de láseres empleando el método de diseño de un observador no lineal mediante formas hamiltonianas. Se estudiaron los láseres de semiconductor y EDFRL. En el láser de semiconductor, el caos es generado mediante retroalimentación óptica mientras que en el láser EDFRL el caos es generado mediante un modulador óptico. El objetivo de la generación del caos en estos láseres es proporcionar una forma de onda de enmascaramiento óptico que pueda ocultar un mensaje análogo o digital.

Para poder lograr una comunicación encriptada caoticamente es necesario una sincronización. El método de sincronización caótica mediante formas hamiltonianas es un método muy preciso y que garantiza la sincronización de cualquier sistema caótico. Sin embargo, en este capitulo se estudiaron dos casos de sincronización muy particulares en donde en uno de los modelos no alcanzo en su totalidad la sincronización de los estados.

Dada la dinámica del modelo del láser semiconductor, es necesario plantear una nueva función de energía y llevar al modelo a una forma de onda hamiltoniana diferente a la planteada en el capitulo. Ademas, es necesario resaltar que el método de sincronización mediante formas hamiltonianas tiene un desarrollo mas profundo para casos especiales, el cual no fue estudiado en el desarrollo de esta tesis.

La sincronización del modelo del láser EDFRL resulto exitosa debido a la dinámica de las ecuaciones diferenciales que conforman el modelo del láser. La creación del observador y los respectivos cálculos de las ganancias K_1, K_2 y K_3 fueron suficientes para llevar a cero los errores de sincronía y obtener la gráfica de fase con un angulo de 45 grados.

El modelo del láser EDFRL, puede ser fácilmente modificado al igual que su comportamiento caótico con tan solo variar alguno de sus parámetros. La

dependencia de la dinámica caótica del láser EDFRL esta dada por 5 parámetros claves. La potencia de bombeo, el indice de modulación, coeficiente de ganancia de la cavidad, la perdida de la cavidad y la frecuencia de modulación angular.

Como trabajo a futuro se proponen las siguientes actividades:

- Transmisión de una señal analógica mediante dos láser EDFRL empleando los modelos sincronizados en esta tesis.
- Transmisión de una señal digital mediante dos láser EDFRL empleando los modelos sincronizados en esta tesis.
- Estudiar el comportamiento del modelo del láser EDFRL mediante las variaciones de sus parámetros.
- Estudiar el comportamiento del modelo del láser Semiconductor mediante las variaciones de sus parámetros.
- Realizar la comunicación entre una red de maestros y esclavos.
- Reproducir los resultados numéricos de forma experimental.
- Análisis de la comunicación mediante la presencia de ruido en la señal de transmisión.

Bibliografía

[1] A. Anjou C.; Sarasola y F.J. Torrealdea. Caos determinista. *En SIGMA Revista Matemática (en linea), mayo 2005, vol 26.*

[2] Annovazzi-Lodi V. ; Donati S. y Scire A. Synchronization of chaotic injected-laser systems and its application to optical cryptography. *IEEE Journal of Quantum Electronics*, 32(6):953–959, 1996.

[3] Bouzid B. Theoretical analysis of erbium doped fiber amplifier. *Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International*, 2011.

[4] César Moreno Sierra. Métodos de sincronización de sistemas caóticos. 2005.

[5] Cisneros Tamayo. sistemas caoticos aplicados en telecomunicaciones. *Tesis de maestría, Instituto Politécnico Nacional*, 2010.

[6] Emmanuel Desurvire. *Erbium-Doped Fiber Amplifiers: Principles and Applications*. Wiley-Interscience, 1994.

[7] Fan Zhang ; Chu P.L. ; Lai R. y Chen G.R. Dual-wavelength chaos generation and synchronization in erbium-doped fiber lasers. *IEEE Photonics Technology Letters*, 17(3):549–551, 2005.

[8] Galende Díaz J.C. *Criptografía. Historia de la escritura cifrada.* Ed. Complutense., Madrid, 1995.

[9] Gerard Vidal Cassanya. Sincronización y control de sistemas dinámicos en régimen de caos espacio-temporal. *Tesis doctoral, Universidad de Navarra, Facultad de ciencias.*, 2010.

[10] Gerd Keiser. *Optical Communications Essentials.* McGraw-Hill Professional, 2003.

[11] Harry Dutton. *Understanding Optical Communications.* Prentice Hall, 1998.

[12] Julien Clinton Sprott. *Elegant Chaos: Algebraically Simple Chaotic Flows.* World Scientific Publishing Co Pte Ltd, 2010.

[13] Junji Ohtsubo. *Semiconductor Lasers: Stability, Instability and Chaos.* Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2007.

[14] John Senior. *Optical Fiber Communications: Principles and Practice.* Prentice Hall, 2008.

[15] Keang-Po Ho. *Phase-Modulated Optical Communication Systems.* Springer-Verlag New York Inc., 2005.

[16] Liguo Luo. ; T.J. Tee. y P. L. Chu. Chaotic behavior in erbium-doped fiber-ring lasers. *J. Opt. Soc. Am. B*, 15:972–978, 1998.

[17] Lucena López J.M. *Criptografía y Seguridad en Computadores.* Tercera Edición, 2003.

[18] Moon Francis. *Chaotic and Fractal Dynamics.* Springer-Verlag New York, LLC., 1990.

[19] Ning Jiang. Chaos synchronization and communication in mutually coupled semiconductor lasers driven by a third laser. *IEEE/OSA Journal of Lightwave Technology*, 28(13):1978–1986, 2010.

[20] Philippe C. Becker. *Erbium-Doped Fiber Amplifiers: Fundamentals and Technology.* Academic Press, 1999.

[21] Pinter S. ; Jean Jiang y Fernando X. A dynamic multi-wavelength simulink model for edfa. *Electrical and Computer Engineering, 2004. Canadian Conference on*, 2004.

[22] Pisarchik A.N.; Ruiz-Oliveras F.R. Optical secure communication system based on chaos synchronization. *Optical Communication Systems (OPTICS), Proceedings of the 2010 International Conference on*, 2010.

[23] P. Martín-Ramos ; J. Martín-Gil y P. Chamorro-Posada. *Amplificadores de fibra óptica dopada con Erbio e Iterbio (EDFAs y YEDFAs).* Dpto. de Teoría de la Señal e Ingeniería Telemática, Universidad de Valladolid, 2010.

[24] Qian Yu ; Chongcheng Fan. Simple dynamic model of all-optical gain-clamped erbium-doped fiber amplifiers. *IEEE/OSA Journal of Lightwave Technology*, 17(7):1166–1171, 1999.

[25] Schmidtke H.J. ; Heckel W. ; Heppner B.H. ; Peller U. ; Horwath J. y Leitgeb E. Edfa models for network simulation purposes. *Electron Devices for Microwave and Optoelectronic Applications, 2001 International Symposium on*, 2001.

[26] Sira-Ramírez H y Cruz-Hernández C. Synchronization of chaotic systems: A generalized hamiltonian systems approach. *International Journal of Bifurcation and Chaos*, 11:1381–1395, 2001.

[27] Uchida A. ; Liu Yun ; Davis P. Characteristics of chaotic masking in synchronized semiconductor lasers. *IEEE Journal of Quantum Electronics*, 39(8):963–970, 2003.

[28] Verónica Aguilar Sánchez. Estudio de la factibilidad para la implementación de la tecnología fso en una cadena de supermercados en la ciudad de quito y su posible diseño. *Tesis de licenciatura, Escuela Politecnica Nacional*, 2010.

[29] Weiss C. O. ; Brock J. Evidence for lorenz-type chaos in a laser. *Phys. Rev. Lett.*, 57:2804–2806, 1986.

[30] William Stallings. *Cryptography and Network Security: Principles and Practice*. 2010.