Universitat de les Illes Balears
CSIC
IFISC
Instituto de Física Interdisciplinar y Sistemas Complejos

UIB
Universitat de les Illes Balears

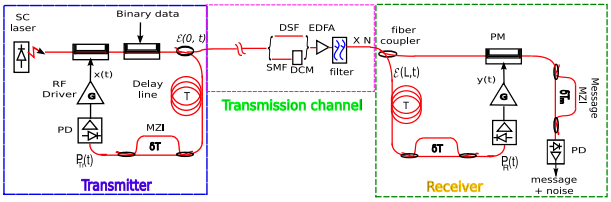
PhD Thesis

Chaos and Synchronization in Opto-electronic Devices with Delayed Feedback

Thesis Presented by **Romain Modeste NGUIMDO** for the PhD in Physics of the Universitat de les Illes Balears.

Pere
COLET RAFECAS
Supervisor

Romain Modeste
NGUIMDO
Author



Palma de Mallorca, 2011

Acknowledgments:

This work is the Thesis for the PhD in Physics of the Universitat de les Illes Balears, Spain, and it has been done thanks to the program "Formación de personal de investigación (FPI)".

I would therefore like to express my deepest gratitude to:

- The Spanish Government, as well as the University of Balearic Islands who have both given me the opportunity to complete my higher education in Spain.
- Prof. Pere Colet for his insightful guidance, constant encouragement, the supervision of this work and his dedicated attention to me. I will never forget his entire disponibility and implication for this work. I have learnt to pursue perfection from his serious attitude towards everything. Without his patient instruction, this thesis would not have been completed. Thanks to him I have never felt far of my family and my country. I will never thank him enough as he put me in contact with Prof. Laurent Larger to whom I learnt a lot.
- Prof. Laurent Larger for his invaluable help. Thanks to him, I have been always motivated to persue this work. His serious attitude towards research really fascinated me and he helped me to believe on me. His advices and guidance have tremendous influence on my professional and personal growth. I will never forget about the "Green" Franche Comté and ST-Institut, Optics laboratory. Thanks to him Besançon has become my second home after Palma. Really I am in short of words to express my special gratitude towards him.
- The staff of IFISC for their help and the nice working environment that they create. Special thanks to Prof. Maxi San Miguel for always fighting for us.
- Profs. Claudio Mirasso, Raúl Toral, Emilio Hernández-García and Víctor M. Eguíluz for their teachings and advices for my integration in Palma and IFISC. I also specially thanks Prof. Ingo Fischer who helped me in some of my trips, trips that allowed me to learn new things. Also thanks to Prof. Manuel Matías for his fruitful advices.
- Prof. Paul Woafo for his always invaluable teachings and for his fruitful advices.
- Dr. Yanne Kouomou Chembo for trusting in my capabilities. His encouragement and advices always provided me with new prospectives in the field of my research.
- Prof. Luís Pesquera who gave me the opportunity to visit him at the unviversity of Cantabria. Thanks to him, I learnt about the neural networks from Dr. Silvia

Ortín to whom I also send my deep regards. I really appreciated the discussions and their entire disponibilty.

- My wife Jenette Mbawou for all her support and for being so patient. Thanks to your invaluable encouragements, I have always found energy to keep going in this work. We use to say that one hand can never tie the bundle. It is a great luck for me sharing my life with you.
- Adrian Jacobo for sharing with me so many good moments, and for his help with my research.
- My gratitude also goes to Dr. Vasile Tronciu for helping us with the DDE-BIFTOOL program.
- Drs. Roberta Zambrini, Miguel C. Soriano for their hospitality and for their valuable help and also for directing my first steps in Mallorca.
- I would like to mention all those with whom I shared some moments at IFISC: Alejandro Herrada, Juan Carlos, Xavi Castelló, Maria, Ismael, Jade Martínez, Toni Peréz Serrano, Toni Pérez, Luis Lafuerza, Przemek Grabowicz, Murat Tugrul, Jose María Aparicio (Pepe), Diana Alejandra Arroyo Almanza, Joao Bettencourt, Miguel A. Escalona-Morán, Juan Fernández Gracia, Pablo Fleurquin, Konstantin Hicke, Leonardo Lyra Gollo, Gonzalo Manzano, Ricardo Martínez, Neus Oliver, Xavier Porte Parera.
- I also think of Roman Lavrov, Romain Martinenghi, Sergei Rybalko and Maxime Jacquot, all from FEMTO-ST for their hospitality.
- To Inma Carbonell, Marta Ozonas, Rosa María Rodríguez, Rubén Tolosa, Eduardo Herraiz, M. Antònia Tugores Pons, Josep Canyelles Pericás, you are all the best. I also express my deepest gratitude to Gaspar (son Lledo) who has always helped me to renew my residence permit.
- I am sincerely grateful to M. Rigobert Dumont and his wife Ameline for their invaluable support. I would like also to thank my other countrymen with whom I shared some nice moments.
- I would like to dedicate this thesis to my parents, who have given all their love to me, encouraged and supported me unconditionally all the time.
- Last but not the least, financial support from MICINN, Spain, and Feder under Projects TEC2006-10009 (PhoDeCC), FIS2007-60327 (FISICOS) and TEC2009-14101 (DeCoDicA) and by EC Project PHOCUS (FP7-ICT-2009-C-240763) is acknowledged, as well as the fellowship BES-2007-14627 under the FPI program of MICINN.

- Finally, thanks to everybody from who I have learned something in this life.

⟨⟨ En Afrique, on n'oublie jamais la source qui a donné l'eau en saison sèche, quand arrive la saison de pluie.⟩⟩

⟨⟨ In Africa, we never forget the river that has given the water in the dry season when the raining season comes.⟩⟩

Contents

Resumen

Esta tesis tiene por objetivo general el estudio de la dinámica no lineal en distintos sistemas electro-ópticos. Por un lado se estudia la utilización de estos sistemas para generar caos de alta complejidad con vistas a comunicaciones ópticas encriptadas y por otro como generadores de microondas de alta pureza espectral.

En los últimos años se han diseñado diversos sistemas optoelectrónicos basados en láseres de semiconductor y sujetos a retroalimentación óptica o electro-óptica para generar portadoras caóticas que permitan encriptar mensajes. Estos sistemas han sido estudiados tanto desde un punto de vista teórico como experimental y, más allá del laboratorio, en algunos casos se han utilizado en pruebas de campo en redes de fibra comercial instalada. La utilización de los láseres de semiconductor como fuentes viene motivada por su facilidad integración en redes ópticas, por su fiabilidad y por su bajo coste. Dada la rápida dinámica de estos láseres, el tiempo de realimentación es superior a las escalas de tiempo internas, por lo desde un punto de vista matemático estos son sistemas con retraso, los cuales pueden desarrollar caos de alta dimensionalidad. Por otro lado la rapidez de la dinámica permite alcanzar velocidades de transmisión de varios Gb/s.

Aunque se han obtenido resultados muy interesantes en el lado de las prestaciones, las cuestiones relacionadas con la seguridad han estado mucho menos consideradas. En este tipo de encriptación basada en hardware el mantener ocultos los parámetros de operación es un elemento esencial para preservar la seguridad. Se ha visto que en algunos casos los parámetros de operación pueden identificarse en la portadora caótica transmitida. En particular si bien el tiempo de retraso es un elemento clave en la generación de caos, también es uno de los parámetros más vulnerables a identificación. A pesar de que la identificación del tiempo de retraso no implica necesariamente que se pueda decodificar el mensaje, sí que abre las puertas a ataques posteriores.

En este contexto, y después del capítulo 1 introductorio y del 2 de descripción de los sistemas considerados, investigamos en el capítulo 3 la seguridad en las configuraciones existentes más comunes: láseres de semiconductor con retroalimentación óptica y sistemas electro-ópticos con retroalimentación diseñados para generar caos en la intensidad o en la fase. Los resultados de este estudio demuestran que el retraso se puede sacar en todos estos sistemas usando diversos métodos de análisis de series temporales, tales como la autocorrelación y la entropía mutua retrasada. En particular, en láseres de semiconductor con realimentación óptica en los que se había propuesto la ocultación del tiempo de retraso eligiendo éste de manera que fuese similar a la escala de tiempo interna de oscilación de relajación, demostramos que si bien este tipo de camuflaje funciona en la serie temporal de la intensidad del

campo eléctrico, falla de forma evidente analizando la fase o cualquier cuadratura del campo (como la parte real o imaginaria).

Llegados a este punto nos centramos en el desarrollo de sistemas que presenten un grado más elevado de seguridad. Como primera propuesta (capítulo 4) investigamos la dinámica en dos sistemas con realimentación electro-óptica en los que implementamos una retroalimentación adicional en el láser de semiconductor utilizado como fuente de luz en el sistema. Con este método, aumentamos tanto el número de parámetros del sistema como la complejidad de su dinámica. Estudiamos la sincronización de emisor y receptor y mostramos que el receptor autorizado puede decodificar el mensaje en forma apropiada.

Una segunda propuesta (capítulo 5) consiste en la introducción de un novedoso sistema que integra una clave digital en el sistema caótico, lo cual constituye un primer puente entre la criptografía algorítmica y la basada en caos. El esquema propuesto, basado en los sistemas electro-ópticos para generación de caos en fase, incorpora dos bucles conectados en serie. Uno permite generar la portadora transmitida mientras que el otro genera una variable interna en la cual se implementa la clave digital. Por un lado, la clave digital aumenta en forma significativa el tamaño de la clave global del sistema. Por otro, los resultados indican que la clave digital permite camuflar el tiempo de retraso, de manera que este no puede ser identificado analizando la serie temporal con las técnicas usuales. Simultáneamente el caos generado por el doble bucle de retraso camufla la clave digital.

En el capítulo 6, consideramos una configuración que incorpora dos bucles electro-ópticos para generación de caos en fase acoplados en paralelo. Encontramos que dicho sistema permite ocultar los tiempos de retraso relacionados con el bucle interno, incluso sin llave digital. Esta configuración permite también la inclusión de una clave digital la cual aumenta el tamaño de la clave global del sistema. En este caso la clave digital dificulta la identificación de los tiempos de retraso asociados al bucle externo, pero no llega a camuflarlos completamente.

Después del análisis de la seguridad en los sistemas actuales y de la propuesta de nuevos sistemas, en el capítulo 7 estudiamos los efectos del canal de transmisión. En particular analizamos los efectos de la dispersión en la fibra óptica. Los resultados indican que el mensaje no se puede recuperar después algunos kilómetros de propagación en fibra monomodo usual. Pero, el mensaje se recupera correctamente si compensamos la dispersión de forma adecuada o si usamos fibra con dispersión desplazada.

Finalmente para mostrar los múltiples usos de los sistemas electro-ópticos, investigamos en el capítulo 8 un sistema electro-óptico con doble bucle para generar microondas de alta pureza espectral. Encontramos que este sistema puede generar microondas de mucha mayor amplitud que su equivalente con un sólo bucle. Además,

demostramos que este sistema permite reducir el ruido de fase hasta 20 dB permitiendo obtener unas prestaciones mejores que los sistemas anteriores (-50 dB a 10 Hz y -150 dB a 1 MHz).

Chapter 1

General Introduction

1.1 Electro-optic Devices

Electro-optic systems involve components or devices which operate by modifying the optical properties of a material through an electric field. The change can take place in the optical absorption, e.g., change of the absorption constants or creation of an absorption band at some wavelengths which gives rise to a change in color. The change can also be in the reflective index, e.g., pockels effect (or linear electro-optic effect), Kerr effect (or quadratic electro-optic effect, QEO effect) or electro-gyration (rotation of the beam polarization plane due to the electric field).

Electro-optic modulators are excellent examples of optical devices whose the reflective index linearly change with the electric field (pockels effect) when an electrical modulation is applied. Figure 1.1 shows an electro-optical modulator designed for intensity modulation (a) and its schematic representation (b). Electro-optical modulators can also be designed for phase, frequency, amplitude, or polarization modulation.

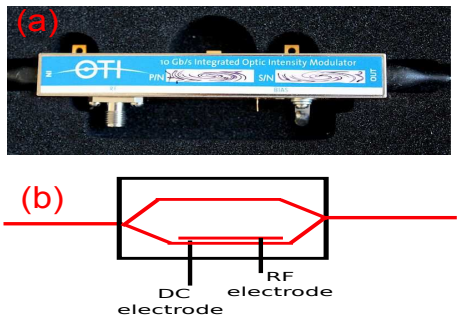


Figure 1.1: An optical intensity modulator for optical telecommunications (Figure taken from [1]).

Electro-optic systems are found useful for a variety of applications. They can be used to produce images of an object through illumination, amplification, or thermal imaging. They can be also used to generate ultra-pure microwaves and complex carriers for telecommunications applications. In the frame of this thesis, we study electro-optic devices for telecommunications applications. In the context of chaos communications, they are useful for generating broadband carriers within which multi-gigabit information can be securely encoded and successfully decoded. As for the microwave generation, electro-optics systems can be used for time-frequency metrology and radar applications. The following sections provide an introductory background to secure communications and microwave generation.

1.2 Secure Communications

Protecting sensitive information from undesired interception has always drawn attention in communication networks. Traditionally, the confidentiality and the authentication of information are achieved through mathematical algorithms. More recently, other encryption techniques has been introduced such as quantum key distribution and chaos-based communications.

1.2.1 Algorithmic cryptography

The operating principle consists in digitalizing analogic signals to be transmitted, such as voice, video, text,etc.. and then convoluting them with a given binary pattern (key). Subsequently, the resulting binary string is sent through a public communication channel [2]. There are basically two types of algorithms: those that make use of a symmetric (private) key and those that use an asymmetric (public) key. In the first one, the recipient decodes the message using the same key-string code as used for encryption.

As shown in Fig. 1.2, it is required that the two parties agree upon a key using another secure channel (for example, a face-to-face meeting or an exchange via a trusted courier). Security relies on the fact that for a given key of length N (with N large as possible), an eavesdropper has 2^N possible keys to explore and it is very difficult to know which is the appropriate one. An example of this type of encryption is the Vernam cipher [3]. In the Vernam cipher, the message (plain-text) is encrypted by applying a XOR logical operation, bit-by-bit, with the secret key, which is randomly generated. The key must be as long as the message. The result of the XOR operation generates the text to be transmitted (cipher-text). The authorized receiver decodes the message by performing a XOR operation between the cipher-text and the key. The Vernam algorithm has been mathematically proved to be fully secure if (and only if) the key is fully random, the key is as long as the message and the key is used only once.

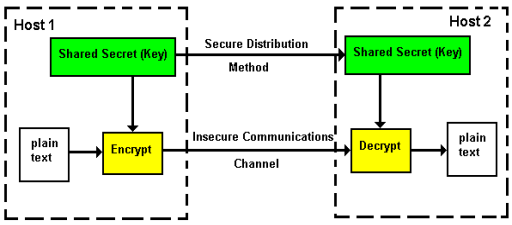


Figure 1.2: Symmetric Cryptography (Figure taken from [4]).

Other examples of common symmetric key algorithms are data encryption standard (DES), advanced encryption standard (AES), international data encryption standard (IDEA), and RC4 (Ron's Code), and typical key sizes are 64, 128, or 192, 256,.., bits. The main drawback of symmetric key cryptography is that it is

not suitable for secure communications between two persons who do not know each other (for instance, it is not suitable for business operations and digital signature).

To circumvent the drawbacks of the symmetric-key cryptography, other software cryptosystems relying on asymmetric-key algorithms (public-key cryptography) have been developed [5]. In these systems, the message encrypted with one key can only be decrypted with the paired key. Given one key, it is computationally not feasible to derive the paired key.

Figure. 1.3 illustrates the use of asymmetric cryptography for classic confidential communications. It works by making one key, called the public key, widely available, while maintaining the other key secret, called the private key. The receiver sends the public key to the emitter who uses it to code the message. The message can only be decoded using the private key kept by the receiver. This scheme is used for example in digital signatures. However, it should be noticed that asymmetric algorithms use significant computational resources in comparison with their symmetric counterparts and therefore are generally not used to encrypt bulk data streams. The most popular asymmetric public-key encryption systems are the so-called Rivest, Shamir and Adleman (RSA) algorithms proposed by Ron Rivest, Adi Shamir and Len Adelman in 1978 [5].

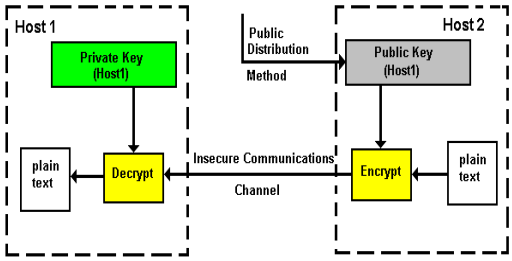


Figure 1.3: Asymmetric Cryptography (Figure taken from [4]).

Because of the limitations of the asymmetric key algorithms such as the limited speed and non-absolute security, symmetric-key algorithms are still actively pursued in the algorithmic community, including new stream cyphers [6] and cryptographic hash functions [7]. Besides, hybrid algorithms such as Pretty Good Privacy (PGP) algorithm combine public key encryption to define a private key used for fast symmetric encryption [8].

Despite the efforts made for providing appropriate algorithms the growing computation capabilities increasingly threatens current algorithmic cryptography. For example, the American scientist Peter Shor implemented in 1994 an algorithm capable of cracking any convoluted message (cipher-text) encrypted with a public key algorithm, such as RSA algorithm [5] and its variants, and schemes based on elliptic functions [9, 10], by factoring and computing discrete logarithms on quantum computers [11, 12]. Nonetheless, the capability of breaking the Shor's algorithm depends on the available computer power. Without waiting for quantum computer construction, a public-key RSA operating with a string code of 512-bit, still consid-

ered secure in late 1990 has been broken in 1999 using 300 computers, so that it is now required to use at least 1024-bit or 2048-bit key string codes in any software cryptosystem [13]. These last findings in software cryptography underlies a latent threat to modern cryptography. Arguably the construction of quantum computers would definitively devastate the foundations of modern cryptography.

1.2.2 Quantum cryptography

In order to strengthen the process of securely exchanging the secret key other approaches have been proposed. Out of those, the quantum cryptography relies on the peculiar properties of quantum mechanics, which allow two remote parties to communicate a private, secret key, protected from eavesdropping by the laws of physics. This key can then be used in a conventional cryptographic algorithm. Quantum key distribution (QKD) was proposed by Bennett and Brassard in 1984 [14]. It establishes a shared key between the sender of the message and the recipient, while preventing for eavesdropping [15]. The prevention to the eavesdropper's presence is made possible through Heisenberg uncertainty principles, which guarantee that measuring quantum data disturbs it, and that disturbance alerts authorized users.

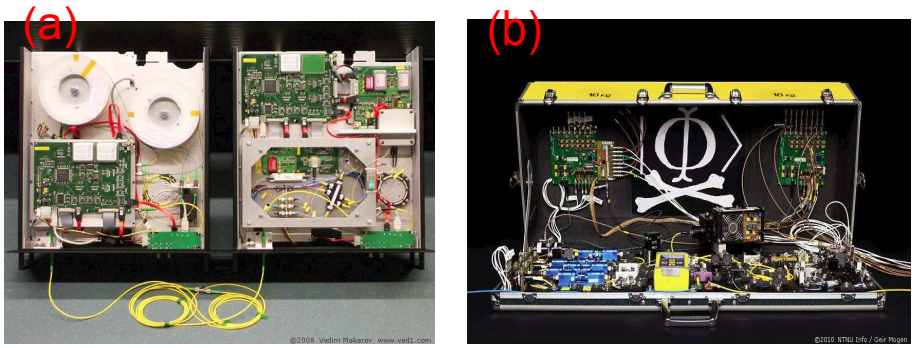


Figure 1.4: (a) Commercial quantum key distribution system manufactured by ID Quantique. Box covers removed. Alice at left, Bob at right; (b) Quantum hacker experimental setup (Figures taken from [17]).

Today, some commercial QKDs are already available to strengthen security when operating with software cryptosystems, evidencing thereby the maturity of QKD technology and its practical interests [see Fig. 1.4 (a)]. However, recent investigations show that, since practical implementations do not operate at the quantum limits (single photon), it is possible for an eavesdropper to fully remote-control the detectors that notify for his presence so as to tracelessly acquire the full secret key [16, 17]. Figure 1.4 (b) shows the device developed to demonstrate this attack [17]. Unfortunately, this loophole can be likely applied to most QKD systems. In addi-

tion, quantum cryptography has some severe limitations. Among others, its inability of encrypting information in real time and the fact that key generation rate is still only of several tens of KHz because of noise and attenuation in the quantum channel.

1.2.3 Key-distribution based on giant fiber lasers

In the framework of the key exchange, another way to proceed relies on mutually coupled optical systems [18, 19]. Figure 1.5 shows an example of secure key distribution using a giant fiber laser system. The system is made up of three mirrors at each end and the choice of the same mirror or not by the two parties, determines the lasing characteristics of the laser, allowing each one to deduce which mirror was selected at the other end and, thus, to exchange a bit.

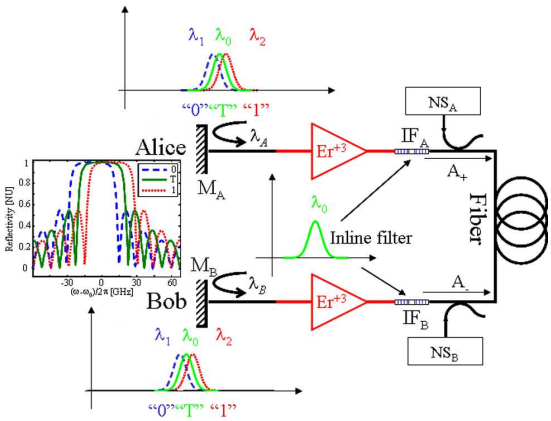


Figure 1.5: Concept for secure key distribution based on establishing laser oscillations between the sender and receiver: Giant Fiber Lasers system for secure key distribution.M_A, M_B: Alices and Bobs end mirrors; IF_A, IF_B: inline filters; NS_A, NS_B: broadband noise sources. Inset: Frequency response of the three mirrors at the three different states (Figure taken from [18]).

As the authors explained "*The system consists of a long erbium doped fiber laser with Alice at one end and Bob on the other. Bob and Alice can each choose independently a mirror from a set of three mirrors (one set at each end), labeled* T, 1, *and* 0 *(see the inset in Fig. 1.5), and use it as the laser reflector at their end. Each of the three mirrors in a set has its peak at a different frequency. The* T *mirror is centered on* ω_0, *mirror* 1 *is centered on* $\omega_0 + \delta\omega$, *and mirror* 0 *is centered on* $\omega_0 - \delta\omega$. *The erbium-doped amplifiers (EDFA) provide the optical gain for the laser, and the inline filters* IF_A *and* IF_B *are narrow-band filters centered at* $\omega 0$. *Each communication cycle (e.g., the generation of a bit for the key) starts with Alice and Bob placing their mirror at* ω_0 *(*T*). This phase resets the symmetry of the system and establishes synchronization. Next, they each randomly select a bit (e.g.,* 0 *or* 1*) and switch on the appropriate mirror. The laser gain is maintained at a level such that if they pick different bits, there is sufficient gain for the laser to lase at* ω_0 *but at a lower amplitude compared to the* T *state. If they both choose* 1, *the lasing wavelength shifts to* $\omega_0 + \delta\omega$, *and if they choose* 0, *the lasing wavelength shifts to* $\omega_0 - \delta\omega$. *The choice of mirrors determines the lasing characteristics of the laser, allowing each of the two parties to deduce which mirror was selected at the other end*

and, thus, to exchange a bit. To achieve security, the determination of the mirrors choice should be simple for legitimate users but very difficult (ideally impossible) for an eavesdropper (Eve)" [18]. This scheme could, in principle, operate faster than the current QDK systems but it will not be sufficiently fast for the real time data transmission.

1.3 Chaos-based Communications

A hardware cryptosystem that can complement the future software cryptography in real high speed data transmission is chaos-based communications. An efficient cryptography could therefore proceed either by first encrypting the data in software and latter transmit it using a hardware system operating in a chaotic regime or by using hybrid systems which mix a digital key with chaotic carriers. The foundations of chaotic cryptosystems on one hand relies on the unpredictability of the chaotic behavior and its sensitivity to initial conditions, and on the other hand, on the deterministic properties of the chaos allowing for synchronization, necessary for message decoding at the receiver. Within the frame of this thesis, we will particularly focus on this type of encryption systems.

1.3.1 Emergence of chaos in systems

Chaos is a paradigmatic concept used to describe deterministic dynamical systems whose behavior is complex, unpredictable and extremely sensitive to initial conditions [20, 21, 22, 23, 24]. This happens even though these systems are deterministic, meaning that their future behavior is fully determined by their initial conditions, with no random elements involved. It is essentially characterized by its sensitivity to initial conditions (popularly referred to as the butterfly effect). Indeed, small differences in initial conditions, such as those due to rounding errors in numerical computation, yield widely diverging outcomes for chaotic systems, rendering long-term prediction impossible in general. Quantitatively, the divergence between two trajectories in phase space starting with a small initial separation $\delta\mathbf{Z}_0$ can be approximated by

$$|\delta\mathbf{Z}(t)| \approx e^{\lambda_e t}|\delta\mathbf{Z}_0| \tag{1.1}$$

where λ_e is the Lyapunov exponent. The calculation of Lyapunov exponents is an efficient way to characterize the dynamics. In chaotic systems, at least one of the Lyapunov exponents is positive. Chaos was first explicitly evidenced by Edward Lorenz in a pioneering paper entitled "Deterministic non periodic flow" [25]. In

lasers, chaos goes back to the pioneering works of Haken in 1975 [26]. It has subsequently proven that when a system presents both nonlinearity and complex enough phase space, it can lead to chaotic behavior. Chaotic behavior has been encountered in many lasers (solid-state [27], gas ring [28], semiconductor [29], etc..) operating under appropriate conditions. Typically, chaos can emerge in any continuous system described by differential equations with both nonlinearity and phase space dimension larger than two (the Poincaré-Bendixon theorem precludes the existence of chaos in two dimensions). However, in discrete systems only the nonlinearity is necessary to induce chaotic regimes. The maps are typical examples illustrating this latter case. In systems such as ordinary differential equations and maps, the phase space is finite-dimension while the dimension is infinite for delay differential equations or partial differential equations. In dissipative systems showing chaotic behaviors, the system typically evolves to a chaotic attractor whose dimension is smaller than the one of the phase space. The dimensionality of the chaotic attractor depends on the parameters of the system and it is usually finite even in infinite dimensional systems.

1.3.2 From chaos to chaos-based communications

Before chaos cryptography, chaos was basically an useful tool for the understanding of some phenomena in biology, chemistry, physics, etc.. The usefulness of chaos for applications changed significantly thanks to the pioneering work of Pecora and Caroll who, in 1990 succeeded in synchronizing two chaotic systems linking them with common signals [30]. Three years latter, in 1993, Cuomo *et al.* demonstrated the first chaos based on communications implemented with the electronic circuits [31]. This demonstration definitively paved the road for chaos-based communications. Since then, many types of synchronization have been identified in chaotic systems, leading therefore to the possibility of encoding the message within any accessible physical variable (power, phase, wavelength, etc..). Among others [32],

- Phase synchronization: The concept of chaotic phase synchronization reflects systems for which the phase $\phi(t)$ chaotically fluctuates while the amplitude of the signal evolve freely and remain unrelated [33, 34]. Phase synchronization arises when the difference between instantaneous phases $\phi_1(t)$ and $\phi_2(t)$ of chaotic signals is limited in time:

$$|\phi_1(t) - \phi_2(t)| < const. \tag{1.2}$$

- Complete synchronization: It implies exact correspondence between state vectors of interacting (unidirectionally or reciprocally coupled) systems: $x(t) \equiv u(t)$. This regime occurs only in coupled systems with identical elements, e.g., each component having the same dynamics and parameter set [35, 36, 37].

- Lag synchronization: It occurs when the interacting systems undergo almost identical oscillations but shifted over a certain time interval τ, e.g., $x(t) \approx u(t+\tau)$ [33, 38, 39, 40]. This type of synchronization is used in chaotic communications where the shift time interval τ arises from the travel time between the emitter and the receiver.

- Generalized synchronization: it is characterized by the existence of a functional relationship between the state of the coupling systems, e.g., the response system is a function of the driving system, $x(t) = F(u(t))$ [35, 36].

The majority of chaos-based optical communications schemes are based on complete synchronization (or lag synchronization when the travel time between emitter and receiver is taken into account) or on generalized synchronization (in the case of the use of semiconductor lasers with optical feedback for which the receiver system is typically not identical to the emitter since it has an injected signal from the emitter).

1.3.3 Message insertion

Different approaches for the transmission of information signals using chaotic dynamics have been proposed. The most used approaches to encode the message are:

♣ Chaos masking (CMS): The message is mixed with the chaotic carrier after it leaves the loop of the transmitter. Thus, the message does not contribute to the carrier generation in the transmitter. The masking can be done in several ways including addition of the message to the chaotic carrier or modulation of the amplitude of the chaotic carrier [1] [41, 42]. In these schemes, the amplitude of the message must be small enough to allow high-quality synchronization and to conceal it.

♣ Intra-loop chaos modulation: The message is embedded within the transmitter loop, and therefore affects the dynamics of the transmitter [43]. The message can enter in the loop either additively (additive chaos modulation, ACM) or multiplicatively (multiplicative chaos modulation, MCM). The widespread one is the ACM scheme. In both cases, the message can have a large amplitude without compromising the synchronization. However, one should make sure that the amplitude of the carrier is larger than that of the message in order to avoid direct detection of the message.

♣ Chaos shift key (CSK): In this type of the scheme, the digital message directly modulates a control parameter in the transmitter. Thus, such control parameter switches between two distinct levels depending on whether a "0" or "1"

[1] modulation of the amplitude has been referred by some authors as "chaos modulation"

bit is transmitted. Meanwhile, the receiver system is biased at a fixed parameter value which is, for example, the level at which "0"bit is transmitted [44, 45]. The message is recovered by measuring the synchronization error between the transmitter and receiver (very low error or no error for "0" bit and large error for "1"). A drawback of this scheme is that the bit rate has to be slow enough for the receiver to resynchronize.

1.3.4 Security in chaos communications

The encryption efficiency of chaos-based communication systems relies on two necessary key points: the unpredictability of the carrier signal and the sensitivity of the synchronization to parameter mismatch. However, the security in hardware cryptosystems is most probably the main Achilles' heel because it implies many factors and the deficiency of only one can definitively collapse the viability of the system. Among the strong requirements that any chaotic cryptosystem should fulfill, one finds the efficient masking of the message within the chaotic carrier [46]. This condition is in general fulfilled when a small amplitude message is hidden within much faster chaotic fluctuations with large amplitude. Second, the system should be able to conceal itself the parameters which meanwhile serve as the physical keys for decryption. Third, the chaotic carrier should be complex enough to prevent its reconstruction using simple techniques such as return maps. For example, some communication schemes using low-dimensional chaotic signals can be unmasked because of their narrow spectra. Their dynamics can be reconstructed from time series [47, 48, 49, 50] or suitable return maps [51, 52, 53]. Fourth, the parameter space dimension should be large enough to avoid breaking by brute-force-attack or similar techniques. Further interesting recommendations to achieve a reasonable degree of security has been suggested [54], as well as some methods to quantify the cryptanalysis of chaotic encryption schemes [55].

1.3.5 Optical chaos communications

The first scheme for optical chaos communications was proposed in 1994 based on a loss-modulated solid-state laser [56]. However, as the previous electronic systems proposed, this system has a low-dimensional chaotic attractor and therefore it can be attacked by an eventual eavesdropper. Besides solid state lasers are of little use in optical communication networks. Therefore the next step was to consider semiconductor lasers [41]. Those can become chaotic with some external feedback which can be modeled with a delay differential equations. From mathematical point of view, the appearance of a delayed term in a differential system drastically changes the analysis: the solution is no more uniquely defined by a single initial condition,

but requires a continuous interval of values $x(t)$ over the time interval $[t_0 - T, t_0]$. Thus the phase space becomes infinite dimensional allowing attractors with arbitrary high dimension. Given this advantage and its applicability to optical networks, delayed systems based on semiconductor lasers are considered as a prototype of systems in which very high complexity can be encountered.

Semiconductor lasers have also the advantages of being small in size, cheap to produce, electrically pumped, and easy to modulate. In general, the dynamics of a single-mode homogeneously broadband semiconductor laser can be described by three basic variables: the slowly varying complex amplitude of the electric field $E(t)$, the material population inversion density $\mathcal{N}(t)$ and the complex amplitude of the material polarization $\mathcal{P}(t)$. The variables $E(t)$, $\mathcal{N}(t)$ and $\mathcal{P}(t)$ are, respectively, governed by three important time constants: the cavity decay time $1/\gamma$, the population relaxation time τ_{R0}, and the material polarization relaxation time τ_q. For semiconductor lasers, $\tau_q \ll 1/\gamma, \tau_{R0}$ so that the behavior of $\mathcal{P}(t)$ adiabatically follows that of $E(t)$ and $\mathcal{N}(t)$. Despite this system is described by three real variables (amplitude, phse and inversion population, for example), in practice solitary semiconductor lasers do not exhibit complicated dynamics without external perturbation. Deviations from steady-state continuous-wave (CW) emission can only be damped through relaxation oscillations, responsible of the energy exchange between electron and photon [57]. However, it has been demonstrated that semiconductor lasers subject to feedback can exhibit much more complex dynamics, suitable for chaos communications. Besides the delay, this approach is rendered possible capitalizing on either the nonlinear nature of the laser or adding an external nonlinearity.

The four sub-classes of nonlinear dynamics most used in chaos-based communications are shown in Figure 1.6. In Fig. 1.6 (a), a linear feedback is obtained via an external mirror placed so that a fraction of the light is reflected back to the cavity (all-optical feedback system) [59]. The nonlinearity is given by the coupling between the optical field amplitude and the inversion population density inside the semiconductor laser. The dynamics of such systems can be described using the Lang and Kobayashi model [60]. This scheme has been widely used [41, 42, 62]. In Fig. 1.6 (b), a part of the laser output is fed to a delay fiber and then detected by photodiode which converts the optical signal into the electrical variations used to modulate the pump current of the laser. In this case, the feedback is nonlinear [63, 64, 65]. In Fig. 1.6 (c), the output of a continuous-wave (CW) laser semiconductor laser goes through an electro-optical modulator. The electro-optical modulator is driven by an electro-optical delay loop similar to the previous case. This type of electro-optical systems with nonlinear feedback was first proposed by Ikeda [66] and has been implemented later using semiconductor lasers [43, 67]. Finally, Fig. 1.6 (d) illustrates a solid state laser with modulated pump as in [56]. Other systems that

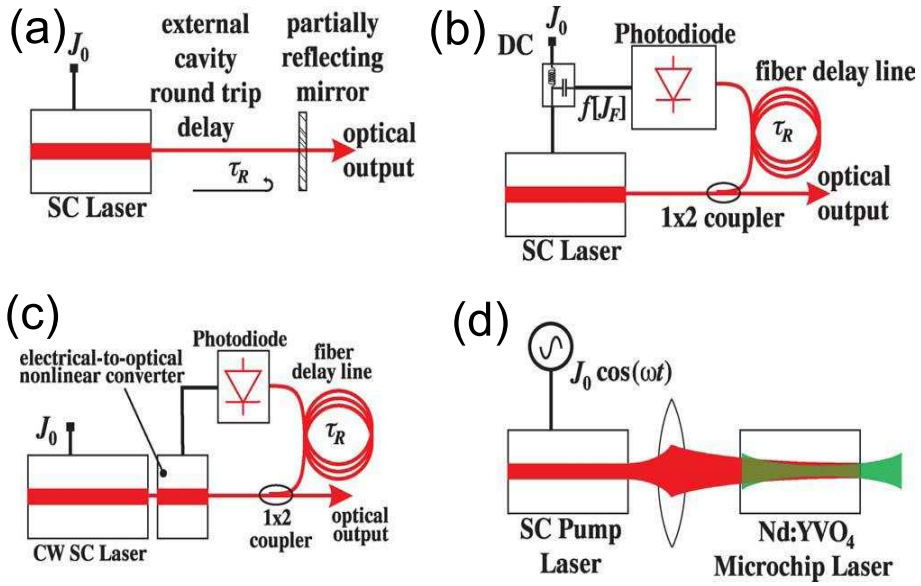


Figure 1.6: Four sub-class of nonlinear dynamics in Optics mostly involved in optical chaos generation for encryption (Figure taken from ref.[58]).

have been suggested for optical chaos cryptography include fiber ring lasers [68, 69] and microchip lasers [70].

The first laboratory experiments demonstrating the potential of optical chaos communications came at late 90' using fiber lasers [71] and optoelectronic feedback devices [43, 67]. Several experimental demonstrations followed which triggered specific research projects. A US research consortium MURI[2] demonstrated the possibility of 2.5 Gb/s pseudo random message transmission using a laser subjected to optoelectronic feedback (with achieved bit error rate (BER) of the order of 10^{-4} in a back-to-back transmission [72]). The OCCULT[3] European project demonstrated an electro-optical setup with improved performance (low BER $\sim 10^{-8}$-10^{-9} at 3 Gb/s [73]).

These last years, dramatic progress in chaos-based communications have been made with experiments in realistic field networks. In particular, two main successful demonstrations implying multi-gigabit information transmission in real installed optical networks over several tens of kilometers [74, 75]. Figure 1.7 (a) shows the field experiment of fibre transmission in the optical communication network of Athens, Greece [74]. During the transmission, the messages were hidden within a strong chaos generated from semiconductor lasers with all-optical feedback [Fig. 1.7 (b)] or by electro-optical feedback systems [Fig. 1.7 (c)]. Current performances of all-optical

[2]Multidisciplinary University Research Initiative
[3]Optical Chaos Communication Using Laser-diode Transmitters, http://ifisc.uib-csic.es/project/occult/

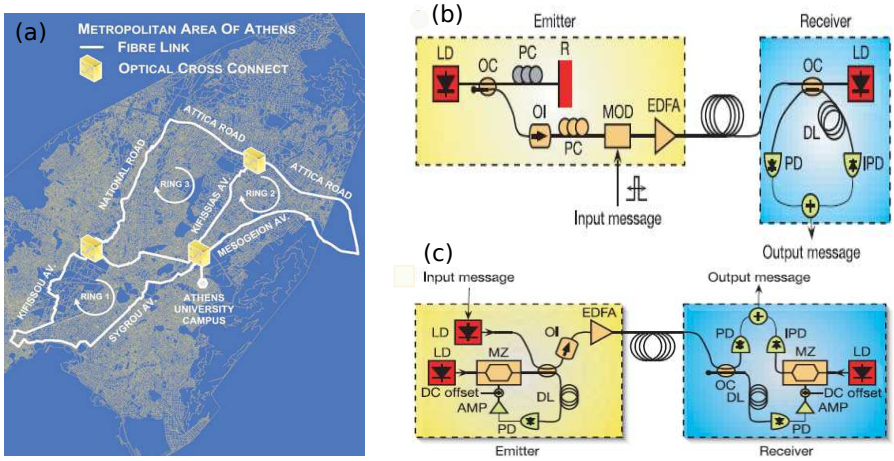


Figure 1.7: (a) Field experiment of fibre transmission in the optical communication network of Athens, Greece. (b) Experimental setup for all-optical feedback system. (c) Experimental setup for electro-optical feedback system which makes use of an integrated Mach-Zehnder interferometer (MZ) (Figure taken from [74]).

systems for secure transmission are limited to 2.5 Gb/s because of their signal bandwidth while electro-optical systems are capable of developing strong chaos with a bandwidth which can span over several tens of GHz. In such electro-optical system the chaos was induced in intensity. Encouraged by this success, another electro-optic system which, induces chaos in phase has been proposed [76], and successfully tested in the installed optical network infrastructure of Frères Lumières in Besançon, France [75], allowing the remarkable rate of 10 Gb/s message transmission. The details in these systems are given in the next chapter.

As a final remark, electro-optic systems are very flexible and, in fact, they are also actively investigated for other applications which require very low noise. Thus they are suitable as ultra-pure microwave generators as described in the next section.

1.4 Photonics Microwave Generation

A microwave is an electromagnetic wave whose frequency in vacuum is between 300 MHz and 300 GHz, thus corresponding to a wavelength between 1 mm and 1 m. Microwaves are useful for a wide variety of technological applications such as radio and television broadcasting, radars, microwave ovens and mobile telecommunications networks. Depending on the application, a certain purity is needed. In mobile telecommunications, for example, in which microwaves are used as carriers to be modulated by information-bearing signals, fairly purity is acceptable. On the

contrary, exceptional pure microwaves are required in radar, time frequency metrology or in lightwave technology where the purity is directly connected to the system performance.

Traditionally, microwave signals are generated using complicated electronic circuits. As microwave signals are distributed over metallic waveguides such as coaxial cables, the attenuation reduces the transmission power significantly, requiring multiple amplifications in the communication network. In order to overcome such problems, the idea of delivering microwave signals over optical fibers offers an excellent solution due to the low attenuation of optical fibers. Basically, such microwaves can be generated through optical heterodyne technique, where the outputs of two lasers with different wavelengths are coupled and sent to a photodetector for beat frequency generation [77]. When the two frequencies are coupled, heterodyning creates two new frequencies (called heterodynes), one is the sum of the two frequencies mixed while the other is their difference. Subsequently the desired one is used while the other is filtered out at the mixer output. However, in such systems, the linewidth of the microwave signal is rather broad due to the lack of phase correlation of two separated laser sources, and hence its overall performance is degraded.

One of the most used optical systems for microwave generation was proposed by X. S. Yao *et al.* [78]. It converts continuous light energy into stable and spectrally pure microwave signals. In such system, the purity of microwave signal is achieved thanks to a delay line inserted into the loop. The role of the delay is to store the energy providing an equivalent to a quality factor given by $Q = 2\pi f_m T$ where f_m is the microwave frequency and T the delay induced by the delay line. The main advantage of the OEO is its capability of generating ultra-stable, spectrally pure microwave with frequency which can be as large as 75 GHz and with a phase noise lower than -140 dBc/Hz at 10 kHz [79, 80]. Late on, these studies were complemented by Y.K. Chembo *et* al. who provided a dynamics approach to investigate analytically the stability properties of OEOs [81] and also to predict eventual instabilities [82]. Next we provide better understanding of the phase noise, which is an Achilles' heel in most of these systems.

1.4.1 Effects of phase noise on microwave oscillators

Self-sustained oscillators are characterized by their radial component (amplitude) which is stable and their polar component (phase) rather neutrally stable. The trajectory for its steady-state evolves along a close curve called a limit cycle as the consequence of the system periodicity [32, 83]. The state is therefore ultimately attracted to the limit cycle for any starting point, out to it as shown in Fig. 1.8. This peculiar property of physical systems directly affects their fluctuation behavior.

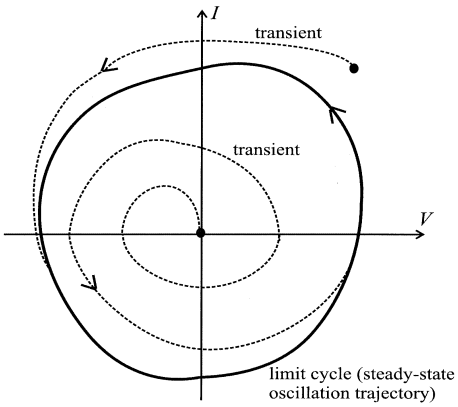


Figure 1.8: Limit cycle in the Voltage-Intensity state space (Figure taken from [84]).

Effectively, as the amplitude is stable, after any perturbations in that direction, due to noise, the state tends to return to the limit cycle and consequently the effects of noise would remain small. However, as the phase is rather neutrally stable, fluctuations induced by noise in the direction along the limit cycle do not experience any restoring force to return the phase to its original value. Consequently, in the presence of noise, the state point walks randomly along the limit cycle, or in other words, the phase undergoes a diffusion process.

Given the necessity to get around the phase noise (at least to lower it at acceptable level), some earlier pioneering works were devoted to oscillator phase noise to elucidate its fundamental mechanism [85, 86] and recent works such as those in [84] pointed out that phase noise can induce a damping of the amplitude. To clearly understand the effects of phase noise, let us perform a thought experiment by considering an ensemble composed of sufficiently large number of identical oscillators starting with the same initial phase conditions (for instance zero at $t = 0$). In voltage-intensity phase space as shown in Fig. 1.9 (a) (right), the state points of the ensemble of all the oscillators are all in top of one to another. Thus, the signals from the ensemble are all also on top of one to another since the oscillators are at the same initial state [Fig. 1.9 (b) (right)] and as consequence the time-dependent probability

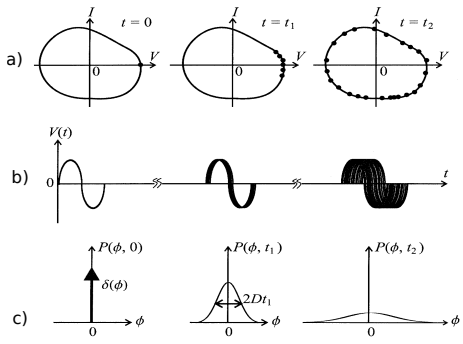


Figure 1.9: Phase diffusion in the state-space (a) and the time-domain (b), and time evolution of $P(\phi(t), t)$ (c); all cases assuming $t_1 < t_2$ (Figure taken from [84]).

distribution of the phase[4] $p(\phi(t), t)$ is a delta function [Fig. 1.9 (c) (right)].

However, as the time elapses, the rotating oscillation points diffuse along the limit cycle [see Fig. 1.9 (a) (center)], leading to incoherent oscillator signals [see Fig. 1.9 (b) (center)] and the probability distribution spreads out [see Fig. 1.9 (c) (center)]. This spreading out is typically measured in term of the diffusion parameter which indicates how fast the phase diffusion occurs. For sufficiently long time, the rotating oscillation points eventually spreading over the entire limit cycle [see Fig. 1.9 (a) (right)], the oscillator signals are completely incoherent [see Fig. 1.9 (b) (right)] and the probability distribution looks similar to a Lorentzian with shorter shape and fatter [see Fig. 1.9 (c) (right)]. This implies that the oscillator will completely lose its initial phase information after a sufficiently long time. Therefore, the performance of any system running as oscillator is critically determined by the phase noise.

1.4.2 Reduction of phase noise in oscillators

To reduce the phase noise in oscillators, the first requirement consists in optimizing the components used. Then the noise can be further reduced using alternative techniques. Out of those, the noise filtering technique [87], the noise-to carrier ratio minimization [88], the exploitation of time variance [89], the use of devices such as coupled oscillators [90] and the use of resonators having good quality factor [91] have been explored. In the optical case, microwave generations based on external modulation [92] and those using a dual-wavelength lasers [93] are examples of devices operating with low phase noise. Recent theoretical study of opto-electronic oscillators phase noise confirmed that the use of a long delay line plays a main role in lowering the phase noise [94]. Within the frame of this thesis, we will also provide more details to such systems.

1.5 Dissertation Organization

After the proofs of principles, the main goals of research in the field of chaos-based communications are related to performance and to security issues. This thesis intends to identify and to propose solutions to some of the drawbacks encountered in chaos-based communications. This challenge at some point requires the re-evaluation and adaptation of existing schemes, and often require the development of new setups. In the context of microwave generations, we also study the possibility of further reducing the phase noise in current electro-optic devices. The dissertation is organized as follows

[4] $P(\phi(t), t)d\phi$ represents the probability for the phase to be in $(\phi, d\phi)$ for a given time, t.

- Chapter 2 gives an overview on the basic systems involved in practical experiments. We also describe in detail how the receivers are built.
- Chapter 3 points out the loopholes in the systems studied in chapter 2 and justifies the need to strengthen their security. Particular attention is paid to delay time identification which is an ingredient necessary for chaotic system reconstructions.
- In chapter 4, we study the dynamics of an electro-optic delay system when besides the usual feedback, an additional feedback is applied to the light source. We describe the system in detail, and investigate effects of this extra feedback on the dynamics and on the performance for chaos communications.
- Chapter 5 is devoted to the study of a system with two phase-chaos electro-optic loops connected in serial. We use this scheme to implement a digital key which besides being an ingredient necessary for successful decoding, also provides concealment of the delay time.
- Chapter 6 studies electro-optic phase chaos systems with two chains connected in parallel and with a receiver that operates in semi-closed loop. In particular we also investigate the conditions of high quality synchronization.
- Chapter 7 deals with the effects of fiber propagation on broadband chaos. Theoretical and experimental approaches are used to explore different ways to overcome the dispersion effects.
- In Chapter 8, we study an opto-electronic system with a double loop for ultra-pure microwave generations. The problem of phase noise reduction is investigated.
- Chapter 9 summarizes the main results of the thesis and proposes some perspectives for future investigations.

Chapter 2

Broadband Chaos Generators Using Semiconductor Lasers

In this chapter, we focus on the properties of nonlinear opto-electronic systems for broadband chaos-based communications. In particular we review the three most used configurations: semiconductor lasers with all-optical feedback, intensity chaos electro-optic delay systems, and phase chaos electro-optic delay systems. All these three configurations have been implemented in field experiments carried out using installed optical fiber in different cities [74, 75].

The chapter is organized as follows: In Sec. 2.1, we briefly describe the case of SL subject to all-optical feedback. Secs. 2.2 and 2.3 are devoted to electro-optic systems generating chaos in intensity and in phase, respectively. Finally a brief conclusion is given at the end of the chapter.

2.1 Semiconductor Lasers with All-optical Feedback

One of the most fundamental configurations used to generate a high-dimensional chaotic optical output is a single-mode semiconductor lasers with optical feedback. The feedback is induced from a fraction of the output radiation reflected back to the active region of the laser via an external mirror [see Fig. 2.1]. The dynamics of such system can be described by the Lang and Kobayashi equations in terms of complex electric field $E(t)$ and carrier number $\mathcal{N}(t)$ inside the active layer [60]. For the emitter, such equations

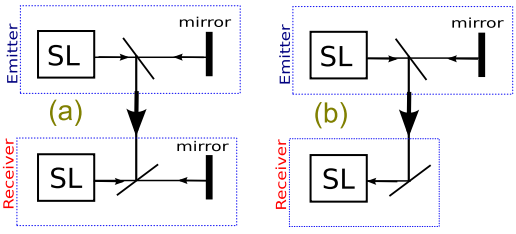


Figure 2.1: Scheme for chaos synchronization of semiconductor lasers (SLs) with optical feedback. (a) Configuration using a closed-loop receiver. (b) Configuration using an open-loop receiver.

are

$$\frac{dE(t)}{dt} = \frac{1+ia}{2}\left(g_m \frac{\mathcal{N}-\mathcal{N}_0}{1+\varrho|E(t)|^2} - \gamma\right) E(t) + \kappa E(t-T)e^{-i\omega_0 T},$$
$$\frac{d\mathcal{N}(t)}{dt} = J_0 - \gamma_e \mathcal{N}(t) - g_m \frac{\mathcal{N}-\mathcal{N}_0}{1+\varrho|E(t)|^2}|E(t)|^2, \tag{2.1}$$

where $i^2 = -1$, the carrier lifetime $1/\gamma_e$ is defined as the average time it takes an excess of carriers to recombine, the photons lifetime $1/\gamma$ is a time constant that describes the decay of energy in a cavity, g_m is the gain parameter, $\mathcal{N}_0$ is the carrier number at transparency, ω_0 is the free running frequency of the solitary laser, a is the linewidth enhancement factor (also known as α-factor)[1], T is the external cavity round-trip after one reflection, κ is the feedback strength, J_0 the injected current and ϱ is the nonlinear saturation factor. The gain saturation factor given by $(1+\varrho I)$ is included in [61] to summarize a set of physical effects that eventually bound the material gain as the number of intracavity photons increases. The threshold current which corresponds to the minimum value beyond which all the losses (absorption, etc..) are compensated is given by

$$J_{th} = \gamma_e(\frac{\gamma}{g_m} + \mathcal{N}_0). \tag{2.2}$$

The behavior of the laser mostly depends on the system parameters. The easily experimentally accessible ones are the injection current J_0, the feedback strength κ and the round trip delay time T. For numerical simulations, we consider the following parameters: $\gamma = 5\times10^{11}$ s^{-1}, $\gamma_e = 5\times10^{8}$ s^{-1}, $a = 5$, $g_m = 1.5\times10^{-8}$ ps^{-1}, $\mathcal{N}_0 = 1.2\times10^{8}$, $\varrho = 2\times10^{-7}$ [41, 95]. For these parameters the solitary laser threshold current is $J_{th} = 7.1 \times 10^{16}$s^{-1} which corresponding to a threshold current intensity of 11.8 mA. Through this thesis we will consider delay times larger than 0.85 ns. These delay times are in to the so-called long cavity regime. In this regime, the dynamics has similar characteristics for any feedback phase [96]. Therefore,we will take the feedback phase $\omega_0 T$ (modulo 2π) to be zero.

Under moderate feedback rates, Eqs. (2.1) can develop chaotic behavior with very high complexity due to the nonlinear nature of the lasers [96]. Fig. 2.2 shows various route to chaos depending on the experimentally tunable parameter T when considering κ as the bifurcation parameter. Figure 2.3 displays the power (a) and the optical (b) spectra of the system for moderate feedback. It turns out that this scheme can allow for the generation of chaotic carriers which span over several Gigahertz.

[1]To avoid confusion with the α used as the fiber attenuation factor in chapter 7, here we use a instead of the standard notation, α.

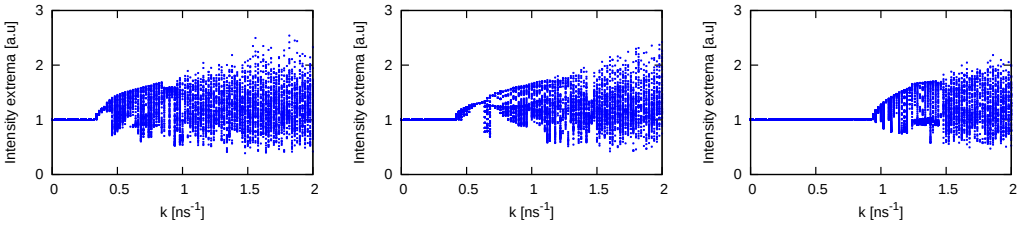


Figure 2.2: Bifurcation diagrams with the feedback rate κ taken as the bifurcation parameter. It shows the route to chaos for (left) $T = 5$ ns, (center) $T = 1.2$ ns, (right) $T = 0.85$ ns.

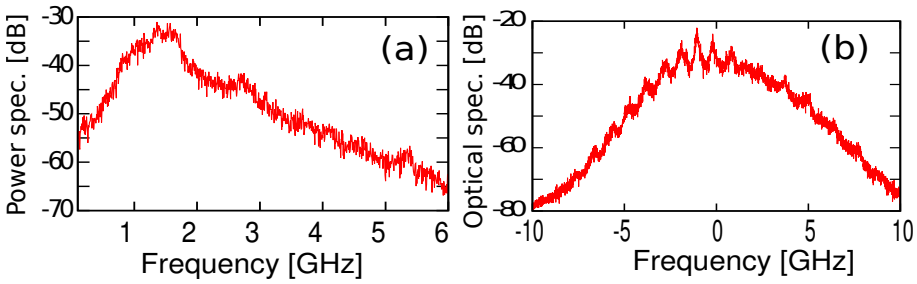


Figure 2.3: Power (a) and optical (b) spectra for $\kappa = 2.5$ ns^{-1} and $T = 1$ ns.

Successful chaos-based communication using this scheme is based on synchronization of an emitter master laser and a receiver slave laser which is achieved by injecting part of the light emitted by the former into the latter. The associated receiver can be subject to its own feedback loop (closed loop configuration) [see Fig. 2.1 (a)] or not (open loop configuration) [see Fig. 2.1 (b)]. The receiver dynamics can be described by

$$\begin{aligned}
\frac{dE'(t)}{dt} &= \frac{1+ia'}{2}\left(g'_m\frac{\mathcal{N}'-\mathcal{N}'_0}{1+\varrho'|E'(t)|^2}-\gamma'\right)E'(t)+\kappa'E'(t-T')e^{-i\omega'_0T'}+\kappa_rE(t),\\
\frac{d\mathcal{N}'(t)}{dt} &= J'_0-\gamma'_e\mathcal{N}'(t)-g'_m\frac{\mathcal{N}'-\mathcal{N}'_0}{1+\varrho'|E'(t)|^2}|E'(t)|^2,
\end{aligned} \tag{2.3}$$

where the prime denotes the receiver parameters and variables. For open loop receivers, $\kappa' = 0$ while for closed loop receivers $\kappa' \neq 0$. The term $\kappa_r E(t)$ accounts for the injection of the transmitter laser field into the receiver one. Ideally an open loop receiver with identical parameters as the transmitter and choosing $\kappa_r = \kappa$, can synchronize perfectly with the master since $E'(t) = E(t-T)$ is a solution of Eqs. (2.1) and (2.3) [97, 98].

However, this identical synchronization turns out to be quite difficult to achieve since it immediately disappears as soon as there is some parameter mismatch [97]. Another possible synchronization in this system is the generalized synchronization in which the power of the receiver $P'(t) \simeq \alpha' P(t)$ [99]. While this synchronization

does not correspond to a mathematical exact solution, it is usually good enough to allow for message codification and decodification [41, 97].

The message can be encoded in several ways. As an example, it can be encoded by modulating the transmitter chaotic intensity output so that the transmitted signal is given by

$$P_T(t) = (1 + \alpha_m m(t))P(t), \tag{2.4}$$

where $P_T(t)$ is the intensity of the transmitted signal including the message while $P(t) \propto |E(t)|^2$ is the intensity of the carrier only, α_m is the amplitude of the message. In this case, the message can be recovered at the receiver side through the operation $m'(t) = (1 - P(t)/P'(t))/\alpha_m$ where $P'(t) \propto |E'(t)|^2$. Thus when $P'(t)$ synchronizes with $P(t)$, the message can be recovered. The quality of the recovered message will therefore depend on the synchronization quality. At this point, the performance depends on the receiver configuration [95]. It was claimed that an open loop receiver configuration is mechanically more stable, easier to implement and very robust against frequency detuning and small parameters mismatch [42, 100], and has a shorter resynchronization time in case the connection is suddenly interrupted [65, 97]. However, a proper decoding of the message demands a larger amplitude of the message than the closed loop receiver configuration. This is a serious drawback as a large amplitude of the encoded message compromises the performance and security of the system. Therefore it is more suitable to use closed loop receivers for which despite being sensitive to parameter mismatch, a relatively large region of synchronization can be found [95, 97, 101].

2.2 Electro-optic Systems with Delay Generating Intensity Chaos

One of the systems belonging to the suitable class of chaotic systems able to develop high complexity was proposed by Goedgebuer et *al.* in 2002 [102]. This system uses a nonlinear delay feedback loop illuminated by a CW semiconductor laser (see Fig. 2.4). The nonlinearity is implemented through a lithium niobate $(LiNbO)_3$ Mach-Zehnder modulator, which is a customized integrated optics telecom device. This architecture has many advantages for optical communications. Through having good stability and controllability in real conditions, it also has great

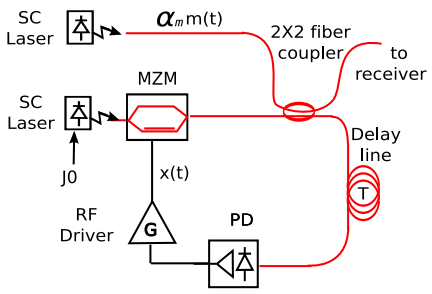


Figure 2.4: Emitter setup of basic electro-optic intensity chaos generator, adapted from [103].

architectural flexibility so that some components can be replaced to change different parameters (bandwidth, noise, efficiency etc..) or even to modify the architecture (additional delays, transformations etc..). Furthermore, it can be easily designed in matched pair. The system is composed of:

- A CW semiconductor laser (SL) delivering a constant power $P_0 = h\nu I$ (where h stands for the Planck constant, ν is the photon emission frequency and $I \propto |E(t)|^2$ the photon number).
- A Mach-Zehnder modulator (MZM): The light coming from the SL is evenly split into the two arms of the MZM and interferes at its output. The refractive index of one arm is modulated by the output voltage of an electronic driver. The applied voltage has two components: a constant or DC component V_B that allows to select the operating point of the modulator; and a radio-frequency (RF) component $V(t)$ which is used to generate the chaos. The complex envelope of the electric field at the MZM output can be written as

$$E(t) = \frac{1}{2}E_0 \left\{ 1 + e^{i\left[\frac{\pi V(t)}{V_{\pi RF}} + \frac{\pi V_B}{V_{\pi DC}}\right]} \right\},$$

  where $V_{\pi RF}$ and $V_{\pi Dc}$ stand for the RF half-wave and the bias electrode half-wave, respectively and E_0 is the amplitude of the SL output. The optical output power is given by

$$P(t) = P_0 \cos^2 \left[\frac{\pi V(t)}{2V_{\pi RF}} + \frac{\pi V_B}{2V_{\pi DC}} \right],$$

  where $P_0 = |E_0|^2/(\mu_0 c)$, μ_0 being the vacuum permeability and c the speed of the light.
- A fiber delay line used to delay the optical signal in time. The fiber is assumed not to be dispersive (independent to the frequency of delayed signal) so that the delay time T is given by as $T = L/V_g$, where L is the fiber length while V_g is the group velocity.
- An amplified photodiode with sensitivity S to detect the optical signal (intensity) and convert it into an electrical signal,
- A RF driver whose output modulates the MZM and closes the delay loop. The RF driver is naturally a filter which can be low-pass, high-pass or band-pass of any order. Table 2.1 overviews the main fundamental 1^{st} order filters.

Here, we assume that the RF driver behaves as a first-order bandpass linear filter with gain G_0. Thus the system can be described by the RF output voltage as

$$\left(1 + \frac{\tau}{\theta}\right) V(t) + \tau \frac{dV}{dt}(t) + \frac{1}{\theta} \int_{t_0}^{t} V(t')dt' = G_0 S_0 P(t - T), \tag{2.5}$$

Filter kind	Representation in time domain	Bandwidth
Low-pass 1^{st} order	$x(t) + \tau \frac{dx(t)}{dt}$	$[0, f_H = 1/(2\pi\tau)]$
high-pass 1^{st} order	$x(t) + \frac{1}{\theta}\int_{t_0}^{t} x(t')dt'$	$[f_B = 1/(2\pi\theta), \infty]$
band-pass 1^{st} order	$\left(1 + \frac{\tau}{\theta}\right) x(t) + \tau \frac{dx(t)}{dt} + \frac{1}{\theta}\int_{t_0}^{t} x(t')dt'$	$[f_B, f_H]$

Table 2.1: Filters and their corresponding equations.

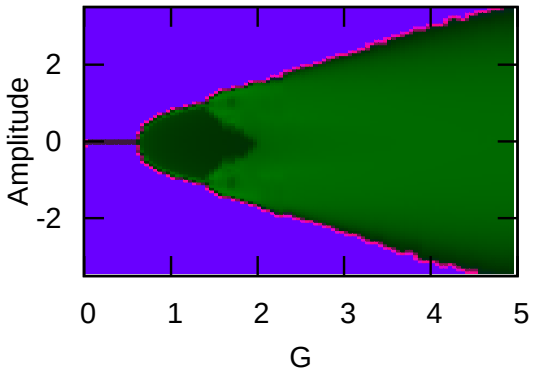


Figure 2.5: Bifurcation diagram showing signal amplitude distribution in dependence on feedback gain G for parameters $\tau = 20$ ps, $\theta = 1.6$ μs, $G = 5$, $T = 30$ ns and $\phi = \pi/4$.

where η_0 accounts for overall losses. Since we are going to consider systems for which $\tau \ll \theta$, the term τ/θ can be neglected as compared to 1.

The message $m(t)$ is added within the chaotic carrier as shown in Fig. 2.4. In practice, this is achieved through another SL having the same wavelength but with orthogonal polarization in order to prevent for the interference between light beams of the chaotic optical intensity carrier and the optical intensity binary data. For security issues, fast polarization scrambling is required to prevent from a simple polarization splitting attack on the transmission line. For the modeling purposes, we introduce $x(t) = \pi V(t)/(2V_{\pi RF})$, $u = \int_{t_0}^{t} x(t')dt'$ so that the system can be described by

$$x + \tau\frac{dx}{dt} + \frac{1}{\theta}u = G\{\alpha_m m(t-T) + \cos^2[x(t-T) + \phi]\}, \quad (2.6)$$

$$\frac{du}{dt} = x, \quad (2.7)$$

where the parameters are the fast cutoff time scale τ, the slow cutoff response time θ, the offset phase $\phi = \pi V_B/(2V_{\pi_{DC}})$ and the normalized electro-optical loop gain $G = \pi S G_0 P_0 \eta_0/2V_{\pi RF}$ while α_m is the ratio between the message and the carrier light beam. For high values of the bifurcation parameter G, the interplay between

nonlinearity and delay generates a chaotic output. Typical parameters used to induce strong chaotic behavior in this system are $\tau = 20$ ps, $\theta = 1.6$ μs, $G = 5$, $T = 30$ ns and $\phi = \pi/4$. Figure 2.5 displays the bifurcation diagram of such system as a function of the feedback gain G. It can be seen that for large value of G, the system is highly chaotic. Its Lyapunov dimension has been found to be greater than 1000 for $T = 30$ ns and $G = 5$ [104]. With such large dimension, one may expect that it will be computationally very complex to reconstruct the high-dimensional attractor from the time series.

To decrypt the encoded message a receiver is built similarly to the emitter using an open loop configuration as shown in Fig. 2.6. The signal coming from the emitter is split in two parts. One part is used to drive the nonlinear processing branch that, in suitable conditions, regenerates the chaotic carrier without message $x'(t)$. The receiver can be described by

$$x' + \tau' \frac{dx'}{dt} + \frac{1}{\theta'} u' = G' \left\{ \alpha_m m(t-T) + \cos^2 \left[x(t-T') + \phi' \right] \right\}, \tag{2.8}$$

$$\frac{du'}{dt} = x'. \tag{2.9}$$

In a back-to-back configuration, $x'(t)$ synchronizes with $x(t)$ for identical parameters. As shown in Fig. 2.6 the output of the receiver MZM is then detected by the photodiode PD_- and combined with the second part of the transmitted signal detected by PD_+. Therefore, the message is obtained by canceling the chaos in the combiner. The output of the combiner reads

$$m'(t) \propto G \left\{ \alpha_m m(t) + \cos^2 \left[x(t) + \phi \right] \right\} + G' \cos^2 \left[x(t) + \phi' \right]. \tag{2.10}$$

The cancellation of the message is easily achieved experimentally operating the MZM with a $\pi-$shifted static phase in the receiver (e.g. $\phi' = \phi + \pi/2$). Alternatively this could have been done using balanced photodiodes and exchanging their inputs or using an inverted amplifier at the receiver. Note that for small mismatch, acceptable synchronization quality is still achieved [105]. Moreover, practical demonstrations have shown that even when the emitter and the receiver are located far one from another, good synchronization quality (with BER of the order 10^{-7} for a message at 3 Gb/s) is obtained after compensating for the fiber losses and its dispersion effects [74].

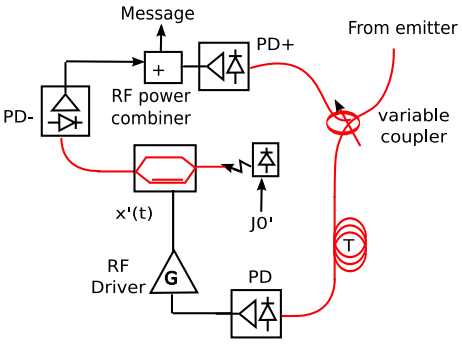


Figure 2.6: Receiver setup of basic electro-optic intensity chaos generator, adapted from [103] .

2.3 Electro-optic Systems with Delay Generating Phase Chaos

Encouraged by the performances obtained from the previous system, a promising optic phase chaos system has been recently proposed [76, 75]. This setup has led to the most efficient and the fastest experimental demonstration of chaos communication. The schematic representation of such system is shown in Fig. 2.7. In this system, the intensity modulator MZM in Fig 2.4 is replaced by two other devices, namely a fast phase modulator (PM) and an imbalanced passive Mach-Zehnder interferometer (MZI), with time imbalance longer than the characteristic time of the phase modulation.

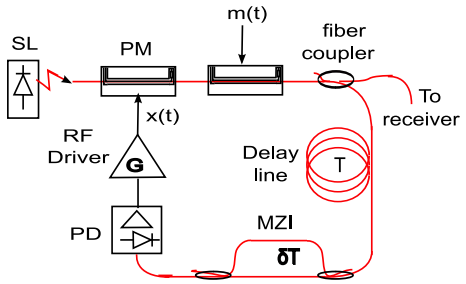


Figure 2.7: Phase chaos emitter setup. MZI: Mach-Zehnder interferometer; PD: photodiode; PM: phase modulator; SL: semiconductor laser.

The transmitter thus consists of a CW distributed feedback semiconductor laser feeding a $LiNbO_3$ phase modulator with the wavelength $\lambda = 2\pi c/\omega_0 = 1.55\ \mu$m. This phase modulator having a halfwave voltage of V_π, receives the electrical chaotic input from a broadband RF driver, and translates this electrical signal modulation into the optical phase while keeping the intensity unchanged. The optical phase therefore changes proportionally to the voltage applied to the modulator, and the time dependent phase shift introduced by the modulation is

$$\varphi(t) = \pi \frac{V(t)}{V_\pi}\,. \tag{2.11}$$

The message is mixed with the chaos through a second cascaded phase modulator, which is assumed for simplicity to have the same V_π. The message phase modulation is performed by driving the modulator with a V_π peak-to-peak voltage in order to add a π phase shift, following the standard differential phase shift keying (DPSK) modulation scheme. Hence, the encoded message introduces in practice an additional phase shift, so that the total optical phase at the output of the message phase modulator reads:

$$\psi(t) = \pi \frac{V(t)}{V_\pi} + \pi \frac{\mu_m(t)}{V_\pi}\,, \tag{2.12}$$

where $\mu_m(t) = \pm V_\pi$ is the message amplitude. The electric field has only one polarization in our system, so that we can restrict ourselves to a scalar description of the optical field. The modulator output is split in two parts, one is transmitted through the channel while the other enters in the delay line. From Eq. (2.12), the

complex electric field envelope with the message can be written as

$$E(t) = E_0 e^{i\psi(t)}\,, \tag{2.13}$$

where E_0 is the constant field amplitude at the output of the SL. This envelope is then optically delayed in time T while traveling through the optical feedback path in the transmitter so that the total electric field at the MZI input can be written as

$$\mathcal{E}(t) = E_0 e^{i[\omega_0(t-T)+\psi(t-T)]}, \tag{2.14}$$

where ω_0 stands for the central frequency of the laser. The optical signal subsequently crosses an imbalanced passive MZI that performs a nonlinear phase-to-intensity conversion as follows

$$\begin{aligned} \mathcal{E}'(t) &= \frac{E_0}{2}\left\{e^{[i\omega_0(t-T)+i\psi(t-T)]} + e^{[i\omega_0(t-T-\delta T)+i\psi(t-T-\delta T)]}\right\} \\ &= \frac{E_0}{2}e^{[i\omega_0(t-T)]}\left\{e^{[i\psi(t-T)]} + e^{[-i\omega_0\delta T+i\psi(t-T-\delta T)]}\right\}. \end{aligned} \tag{2.15}$$

This therefore evidences that this conversion is led by the mean of a *nonlocal nonlinearity in time*, since it is ruled by an *intrinsic differential delay* which should be significantly greater than the typical phase variations timescale. The MZI imbalance is also responsible for an extra constant phase $\omega_0\delta T$ of the interference condition, which corresponds to the static operating point of the nonlinear conversion. The optical intensity at the MZI output is thus a nonlinear nonlocal transformation of the phase modulation:

$$P_{\mathrm{Tr}}(t) = P_0 \cos^2\left\{\frac{1}{2}\left[\omega_0\delta T + \psi(t-T) - \psi(t-T-\delta T)\right]\right\}, \tag{2.16}$$

where $P_0 = |E_0|^2/(\mu_0 c)$. This optical intensity is then converted to the electrical domain by a photodiode. The obtained electrical signal is then band-pass filtered by the electronics of the feedback loop, whose RF frequency filtering process can be modeled in the time domain by an integro-differential operator characterized by a high- and a low-frequency cut-off. For sake of simplicity we assume that the filter is linear and of second order, so that the dynamics of the input RF voltage at the input of the chaos phase modulator obeys

$$V(t) + \tau\frac{dV}{dt}(t) + \frac{1}{\theta}\int_{t_0}^{t} V(t')dt' = \eta_0 G_0 S P_{\mathrm{Tr}}(t)\,, \tag{2.17}$$

where θ and τ are the characteristic response times attached to the low and high cut-off frequencies of the filter respectively, G_0 stands for the amplifier gain, η_0

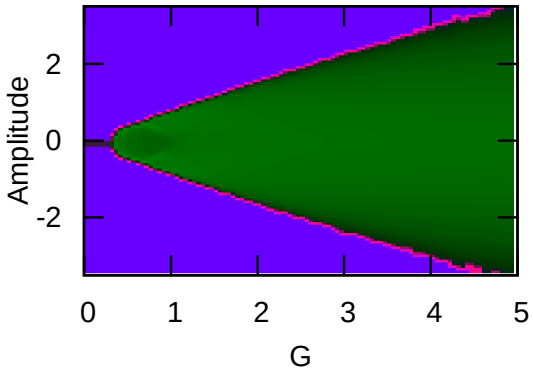


Figure 2.8: Bifurcation diagram showing signal amplitude distribution in dependence on feedback gain G for parameters $\tau = 20$ ps, $\theta = 1.6$ μs, $G = 5$, $T = 30$ ns and $\phi = \pi/4$.

accounts for overall optical losses, and S is the photodetection efficiency. Note that the condition $\tau \ll \theta$ has been taken into account in the above equation (easily fulfilled assumption, since the feedback filtering is broadband for telecom devices). For mathematical convenience we introduce the dimensionless variables $x(t)$ and $m(t)$ as follows:

$$x(t) = \pi \frac{V(t)}{2V_\pi} \equiv \frac{\varphi(t)}{2}, \tag{2.18}$$

$$m(t) = \pi \frac{\mu_m(t)}{2V_\pi}, \tag{2.19}$$

so that Eq. (2.17) can be rewritten in the dimensionless form as

$$x(t) + \tau \frac{dx}{dt}(t) + \frac{1}{\theta} u = G \cos^2 \left\{ \Delta(x)_T + \Delta(m)_T + \Phi_0 \right\}, \tag{2.20}$$

$$\frac{du}{dt} = x, \tag{2.21}$$

where and $\Delta(F)_T = F(t-T) - F(t-T-\delta T)$, $G = \pi \eta_0 G_0 S P_0/(2V_\pi)$ is the overall feedback loop gain, and $\Phi_0 = \omega_0 \delta T/2$ is a constant offset phase. This equation rules the dynamics of the input RF voltage at the first phase modulator. The delay term therefore involves the difference $x(t-T) - x(t-T-\delta T)$ instead of $x(t-T)$ as in the intensity chaos system. For the same parameters as used for the intensity chaos system, the dynamical properties of the system are intrinsically different [76]. Figure. 2.8 displays the bifurcation diagram for this system as G increases for parameters $\tau = 20$ ps, $\theta = 1.6$ μs, $T = 30$ ns, $\phi = \pi/4$, and $\delta T = 400$ ps. An interesting remark is that the threshold beyond which the system starts

oscillating is reduced by factor 2 compared to the intensity chaos system, due to the fact that, $x(t-T)-x(t-T-\delta T)$ have variations whose amplitude can be twice higher than that of $x(t-T)$. Besides, the message is embedded within the phase while it was integrated in amplitude in the previous case.

The receiver is built in the symmetric way to the transmitter. In practice the offset phase Φ_0 is strongly sensitive to environmental fluctuations, and it needs to be actively controlled through a fine tuning of δT (e.g. thermal control between the imbalanced arms of the interferometer): the chaotic masking thus remains deterministic and controllable, which is a required condition for proper chaos replication at the receiver side.

The modeling of chaos cancellation can be described following a similar approach as previously done for the emitter. The receiver equations can be written as

$$x'(t)+\tau'\frac{dx'}{dt}(t)+\frac{1}{\theta'}u' = G'\cos^2\left\{\Delta(x)_T+\Delta(m)_{T'}+\Phi'_0\right\}, \tag{2.22}$$

$$\frac{du'}{dt} = x. \tag{2.23}$$

In order to remove the chaotic masking, the replicated chaos needs to have the opposite sign with respect to the emitter one. As already stated, this is easily achieved experimentally operating the MZI with a $\pi-$shifted static phase. When the receiver applies an additional phase modulation onto the received light beam, proportionally to the signal $x'(t)$, this leads to a total optical phase modulation proportional to $(x+x')$ at the chaos cancellation output. A DPSK message modulation is then applied at the transmitter to retrieve $m(t)$ as stated before, due to the anti-phase chaos replica expected for $x'(t)$. The resulting light beam can then be processed through a standard DPSK demodulator matched with the message bit rate (imbalanced MZI with δT_m in Fig.2.9). The photodiode detects

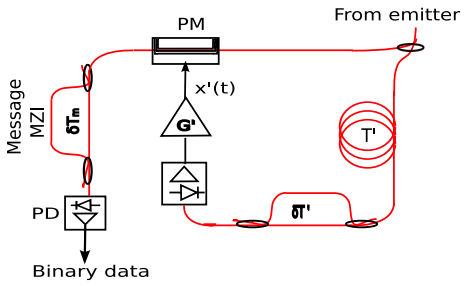


Figure 2.9: Phase chaos receiver setup. MZI: Mach-Zehnder interferometer; PD: photodiode; PM: phase modulator.

$$m'(t)\propto\left|e^{2i[x(t)+x'(t)]}+e^{2i[x(t-\delta T_m)+x'(t-\delta T_m)]}\right|^2. \tag{2.24}$$

This scheme has led to a recovered message at 10 Gb/s with a BER of 10^{-7} over more than 100 km [75]. More details in fiber dispersion effects regarding this scheme will be provided in chapter 7. In order to improve the security in such systems, it is worth to first identify the loopholes. The next chapter is devoted to this issue.

2.4 Conclusions

In this chapter, we have overviewed the three main configurations widely investigated for optical communication applications and which have been successfully tested in the installed optical networks. For each system, we have provided details in the emitter and receiver modeling, as well as the way to encode and decode the message.

Chapter 3

Loopholes in Opto-electronic Delay Devices

Since the security of the chaotic hardware cryptography schemes strongly depends on the concealment of the system parameters, it is worth to carefully investigate different ways which can lead to the extraction of the parameters. An eventual eavesdropper can have access to the transmission channel and may be able to record all the necessary data, at least in principle. The eavesdropper can then apply time series analysis techniques to these data in order to identify the system parameters. Thus, each variable that can be intercepted or reconstructed from the intercepted signal, should be carefully analyzed in order to estimate the security level of the system. Once the critical parameters are identified, the eavesdropper can try to reconstruct the receiver or to decode the message using an alternative technique such as neural networks [106]. One of the most critical parameters in the systems described in chapter 2 is the delay time.

The outline of the chapter is as follows. Sec. 3.1 describes the different delay time identification techniques used in this thesis. In Sec. 3.2 we investigate the delay time identification in semiconductor lasers with optical feedback from the intensity and phase time-series as well as from field quadratures. In Sec. 3.3 and Sec. 3.4 we apply the delay identification techniques to the intensity and phase chaos electro-optical systems. In Sec. 3.5 the same techniques are applied for delay time identification from the transmitted signals while in Sec. 3.6 we attempt the identification of other system parameters. Sec. 3.7 gives some concluding remarks.

3.1 Delay Time Identification Techniques

The delay time is, to our knowledge, the necessary ingredient in all approaches to replicate the underlying dynamics in chaotic delay systems. For example, even in hyper-chaotic systems the knowledge of the delay time allows for the projection of the high-dimensional attractor onto a reduced dimensional phase space, which

makes the system more vulnerable [107]. Several techniques can be used to identify the delay time. Among them, we find

- Autocorrelation (AC) function: It measures the linear relation between the variable $x(t)$ and its time-shifted version $x(t+s)$. For continuous systems, it is defined as

$$C(s) = \int_{-\infty}^{+\infty} x(t)x(t+s)dt, \tag{3.1}$$

  When scanning over s, the delay time is extracted as the first pronounced peak or valley given by the AC after the peak at $s = 0$. Other peaks can be also observed at multiples of the delay time period, but with smaller amplitude.

- Delayed mutual information (DMI): It measures the amount of the information that can be obtained about one variable by observing another. The DMI between $x(t)$ and $x(t+s)$ is a positive quantity defined as

$$DMI(s) = \sum_{x(t),\, x(t+s)} p(x(t), x(t+s)) \ln \frac{p(x(t), x(t+s))}{p(x(t))p(x(t+s)))}, \tag{3.2}$$

  $p(x(t))$ is the probability distribution function of $x(t)$ while $p(x(t), x(t+s))$ stands for the joint probability distribution function between $x(t)$ and $x(t+s)$ [108, 109]. The calculation of the DMI also gives a peak at the delay time and at its multiples.

- Time distribution extrema (TDE): TDE relies on a statistical analysis of the time intervals between extrema in the time series. One first determines extrema in the time series and then analyzes the time intervals between them [110, 111]. For different values of lag-time s, we count the number of pairs of extrema separated in time by s, normalized to the total number of extrema. In other words, it gives an estimation of the probability to find a pair of extrema in $x(t)$ separated by s, given a sufficiently number of extrema.

- Filling factor (FF): For a given equation $\dot{x}(t) = F\left[x(t-s), x(t)\right]$, we project the trajectory $\vec{x}(t)$=($x(t-s)$, $x(t)$, $\dot{x}(t)$) from the infinite dimensional phase space into a three-dimensional space which is spanned by the coordinates ($x(t-s)$, $x(t)$, $\dot{x}(t)$)[112, 113]. When $s = T$, the trajectory ($x(t-s)$, $x(t)$, $\dot{x}(t)$) is confined to a surface, leading therefore to a minimum fractal dimension (between 1 and 2). A potential way to compute the FF consists in covering the ($x(t-s)$, $x(t)$, $\dot{x}(t)$) by cubes and count the number of cubes which has been visited at least one time, normalized to the total number of cubes. This method can be quite simplified by working only with the extrema of $x(t)$, e.g. $\dot{x}(t) = 0$. In this

case, the trajectory is reduced to $(x_{ext}(t-s),\, x_{ext}(t))$ where $x_{ext}(t)$ stands for extrema of $x(t)$ and therefore the cubes are replaced by squares. Also, it is convenient to have a long time series.

It is known that the AC and the DMI overestimate the delay time by an amount related to the fastest time scale of the system intrinsic dynamics, while the TDE and the FF show minimum at the exact value of delay time. Next we use these estimators to identify the delay time in the systems described in chapter 2. We also investigate its robustness of each estimator to noise.

3.2 Delay Time Identification in Chaotic Semiconductor Lasers with All-optical Feedback

In SL with all-optical feedback two important time scales coexist, namely the relaxation oscillation period τ_{Ro} and the external cavity round-trip time T [114]. It should be noted that for the solitary laser the relaxation-oscillation period τ_{R0} is given by

$$\tau_{R0} = \frac{2\pi}{\sqrt{\gamma_e \gamma (b-1) - \gamma_e b^2/4}}, \tag{3.3}$$

where $b = g_m \left(J_0 - \gamma_e \mathcal{N}_0\right) / \left(\gamma \gamma_e\right)$. Thus with the parameters given in chapter 2, $\tau_{R0} = 0.75$ ns. It has been suggested that the delay time can be hidden when parameters are such that delay time is close to the relaxation period of the laser operating with moderate feedback [115, 116]. In that case the interplay between the intrinsic SL dynamics and the delayed feedback leads to a concealment of the delay time. These results have been experimentally verified recently [117]. Both theoretical and experimental results were obtained by computing statistical quantifiers from intensity time series. However, these results can depend on the observable [118]. Since the phase of the electrical field is also a part of the signal transmitted through the public channel, it can be also used by an eventual eavesdropper for data analysis. In this section we discuss the role of the phase in the delay time identification [119]. In particular we show that for SL with optical feedback even if the delay time is hidden in the intensity time series it can be readily identified from the phase or from quadrature time series.

Figure 3.1 displays the results for the autocorrelation (left column) and delayed mutual information (right column) as computed from intensity time series. Here we only consider the cases for which the system is chaotic. For moderate values of the feedback rate, such as $\kappa = 2.5$ ns^{-1} [Fig. 3.1 (a) and (d)] and $\kappa = 5$ ns^{-1} [Fig. 3.1 (b) and (e)], the delay time (vertical dashed line) cannot be easily identified. As shown

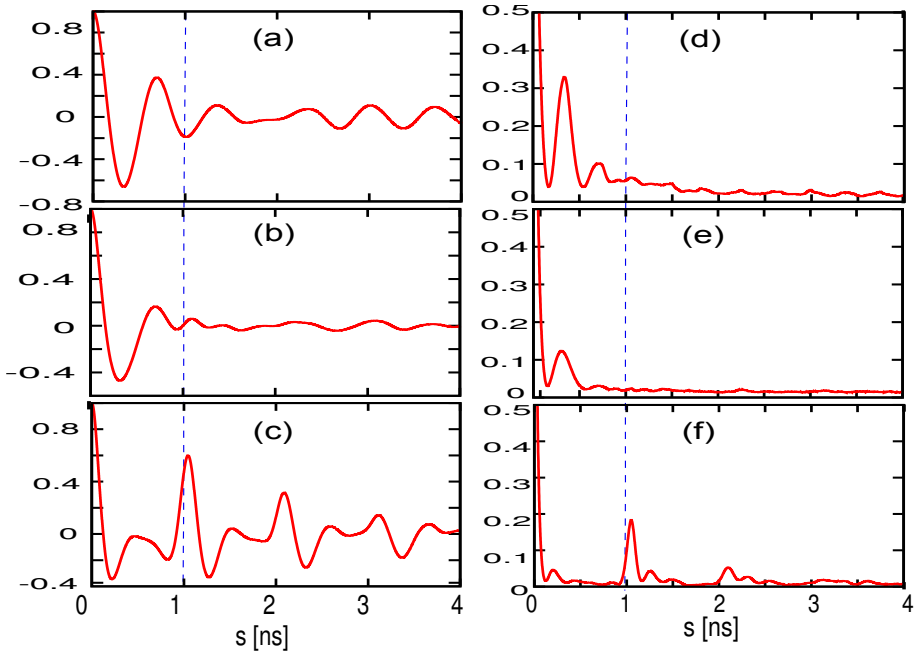


Figure 3.1: Autocorrelation (left) and DMI (right) for $\kappa = 2.5$ ns^{-1} (a, d), $\kappa = 5$ ns^{-1} (b, e) and $\kappa = 10$ ns^{-1} (c, f) obtained from the intensity time series, $|E(t)|^2$. The vertical dashed line indicates the delay time $T = 1$ ns. For the parameters chosen $\tau_{R0} = 0.75$ ns.

in [115] the more pronounced maxima of the DMI and minima of $C(s)$ are located around $\tau_{R0}/2$ while there is no significant trace of the delay time. This is an effect of the interplay between the feedback and the intrinsic SL dynamics. It is worth noting that the value of T is within the interval $[\tau_{R0} + 0.15$ ns, $\tau_{R0} + 0.35$ ns$]$ which was found as leading to well delay time concealment for moderate feedback rate when computing the quantifiers from the intensity time series [115]. For larger feedback rate, the contribution of the delay term in Eq. (2.1) becomes more important, so that the delay time is no longer concealed. For example for $\kappa = 10$ ns^{-1} a clear peak is observed around the delay time both in autocorrelation [Fig. 3.1 (c)] and DMI [Fig. 3.1 (f)] functions as also shown in [115, 116] for the same parameters.

While the intensity can be measured by an eventual eavesdropper through a simple detection (using a photodiode) of the transmitted signal, the phase $\varphi(t) \equiv Arg[E(t)]$ of the transmitted signal can also be detected although it requires the use of more sophisticated devices such as an optical 90^o hybrid coupler [120, 121], and it is more difficult to measure experimentally. The knowledge of these two components allows the reconstruction of the real and the imaginary parts of the complex field.

Figure 3.2 displays $C(s)$ (left column) and DMI (right column) computed from the phase $\varphi(t)$ (solid line) recovered within the interval $[-\pi, \pi]$, and from the real part $\mathcal{R}e\,[E(t)]$ (dashed line) of the electric field. As shown, the delay time can be

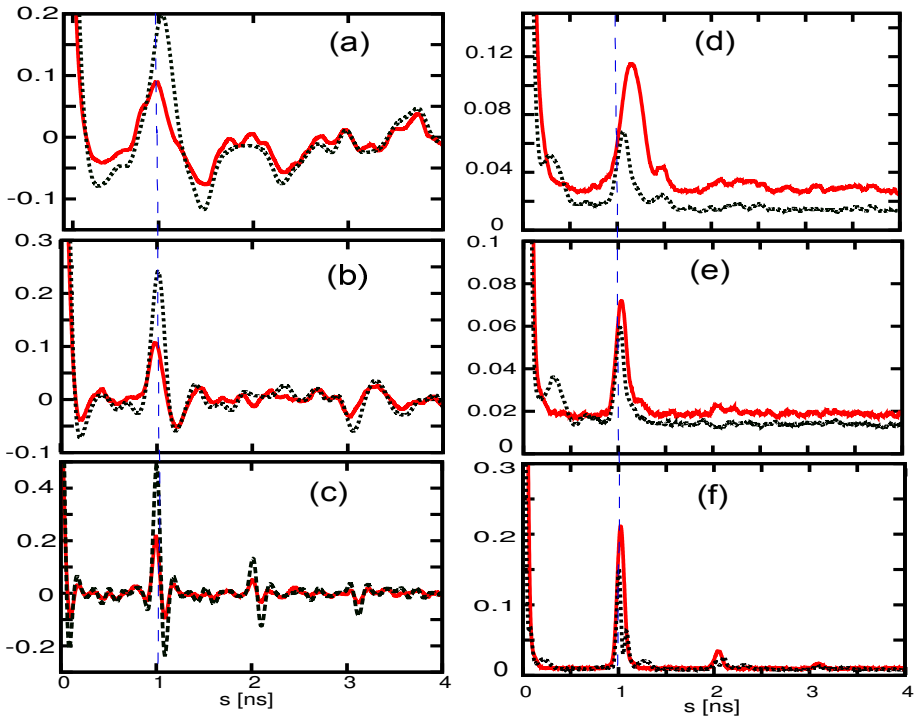


Figure 3.2: Autocorrelation (left) and DMI (right) as in Fig. 3.1 computed from $\varphi(t)$ (solid line) and $\mathcal{R}e[E(t)]$ (dotted line).

identified even for $\kappa = 2.5$ ns^{-1} in both the autocorrelation and the DMI, although the DMI peak is narrower and thus more distinguishable. The peak for the DMI appears at a slightly larger value as compared to the actual value of the delay time while the peak for the autocorrelation is located very close to the actual delay time. As the feedback rate increases, both the autocorrelation and DMI peaks become narrower and more distinguishable while the location of the DMI peak gets closer to the actual delay time. Finally, for $\kappa = 10$ ns^{-1}, for which the delay signature was already found from intensity series, the peaks in $C(s)$ and in DMI computed from $\varphi(t)$ or $\mathcal{R}e\,[E(t)]$ are sharper and more precisely located than those obtained from the intensity time series. We have found that the delay time is identified from $\varphi(t)$ or $\mathcal{R}e\,[E(t)]$ even when $T = \tau_{R0}$. For the imaginary part of the field or for other quadratures one obtains similar results to those obtained for the real part.

Globally, the peak for the phase in the DMI is larger than that obtained from the real part of the field, while the opposite occurs for the autocorrelation. This indicates that phase indeed carries a nonlinear relationship between its state and its lagged-version. Linear relationships, such as the ones measured by the correlation, turns out to be stronger for the quadratures. The different results for intensity and phase can be explained from the dynamics. From Eqs. (2.1), the phase equation

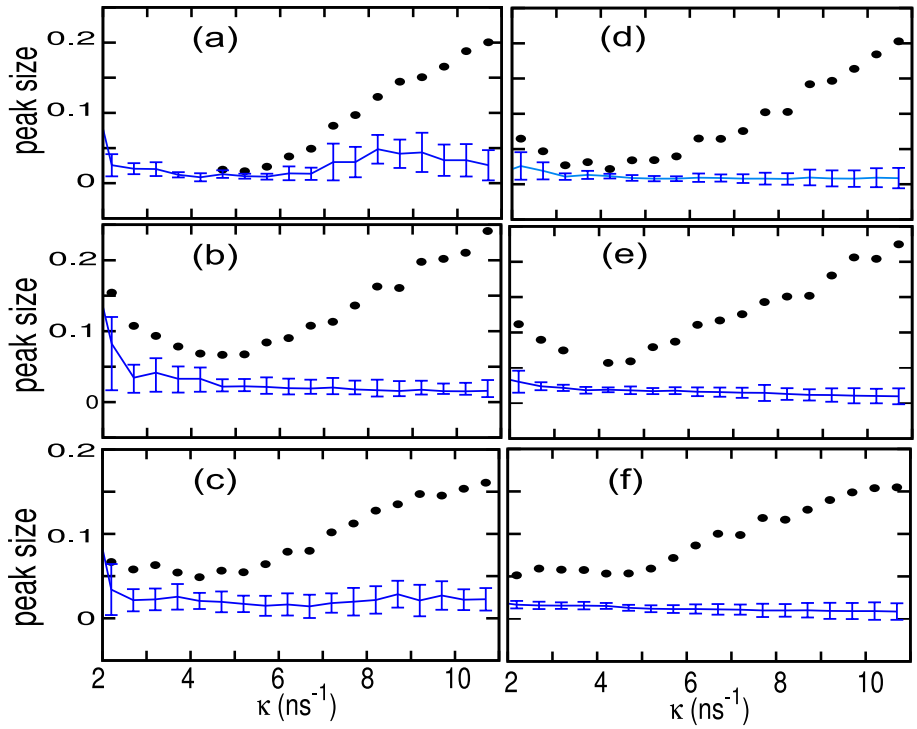


Figure 3.3: Size of the DMI peak signaling the delay time computed from $|E(t)|^2$ (a, d), $Arg(E(t))$ (b, e) and $\mathcal{R}e(E(t))$ (c, f). For the left column $T = 1$ ns while the right one $T = 5$ ns. Solid lines and bars correspond to the background mean value and standard deviation.

can be written as

$$\frac{d\varphi}{dt} = \frac{a}{2}\left(g_m \frac{\mathcal{N} - \mathcal{N}_0}{1 + \varrho|E(t)|^2} - \gamma\right) + \kappa \frac{|E(t-T)|}{|E(t)|} \sin\left[\varphi(t-T) - \varphi(t) - \omega_0 T\right]. \quad (3.4)$$

The last term tends to keep constant the difference $\varphi(t-T) - \varphi(t)$, so that the dynamics of $\varphi(t-T)$ is strongly linked to that of $\varphi(t)$. On the contrary, the equation for the intensity does not have a term depending on $|E(t)|^2 - |E(t-T)|^2$ which could push $|E(t)|^2$ close to $|E(t-T)|^2$.

Figure 3.3 (left column) shows the size of the peak found in the DMI computed from the intensity (upper row), from the phase (middle row) and from $\mathcal{R}e\,[E(t)]$ (bottom row) as function of the feedback strength for $T = 1$ ns. As an indication of the background level we also show the average and standard deviation (vertical bars) of the DMI on the interval from 2 to 4 ns. Two main regions can be identified: For $\kappa \gtrsim 6$ ns^{-1} it is possible to distinguish a peak around the delay time from the background level independently to the variable used. Furthermore, in this region the size of the peaks increases linearly with the feedback strength. For smaller values of κ the size of the peak depends strongly on the variable chosen to compute the DMI. While the peak obtained from the intensity time series merges with the background,

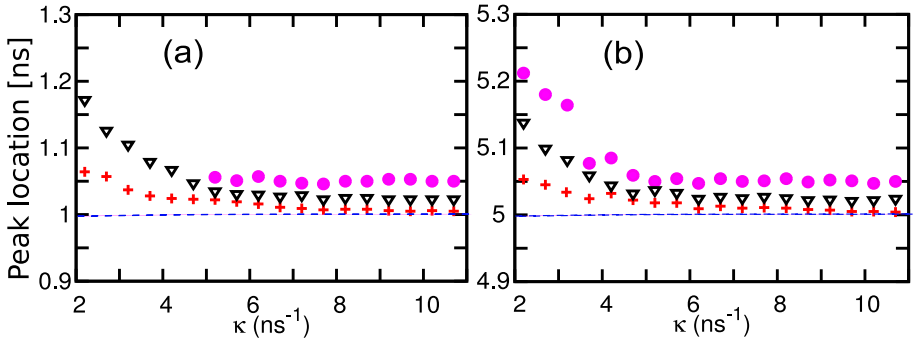


Figure 3.4: Location of the DMI peak for $T = 1$ ns (a) and $T = 5$ ns (b) when computing the DMI from $|E(t)|^2$ (•), $Arg(E(t))$ (▼) and $\mathcal{R}e(E(t))$ (+). The horizontal dashed line indicates the delay time location $T = 1$ ns (a) and $T = 5$ ns (b).

the one from the phase or the real part remains always distinguishable.

For $T = 5$ ns [Fig. 3.3 (right column)] the delay time can be identified using DMI even from the intensity time trace [115]. Still, as shown in the figure, the peak can be better identified from the background level (here calculated in the interval from 5.5 to 7.5 ns) when the DMI is computed from the phase or a quadrature.

Fig. 3.4 compares the location of the peaks in DMI computed from different variables. It turns out that the real part $\mathcal{R}e\,[E(t)]$ appears as the variable from which the delay time signature can be retrieved with more accuracy even when the delay time is close to the relaxation period. The peak for the intensity time series is not only the less visible, as discussed before, it is also the one located farther away from the actual delay time.

In summary, our results show that in SL with external feedback the delay time can be identified from the phase or quadrature time series by the means of autocorrelation or DMI even when it is concealed in the intensity time series. Besides providing more visible peaks, phase and quadratures also lead to a more precise location of the peak. The difference in the information carried out by intensity and phase can be further illustrated by looking at the power and optical spectra. While the power spectrum computed from the intensity does not reveal the presence of a delay time [Fig. 3.5 (a) and (b)] corresponding to $\kappa = 2.5$ ns^{-1} and $\kappa = 5$ ns^{-1} respectively, the optical spectrum, which depends on both the intensity and the phase of the laser, hints the presence of a delay time, Fig. 3.5 (d) and (e). The delay time defines the spacing between the modes present around the maximum of the optical spectrum. For $\kappa = 10$ ns^{-1} for which the delay time can be identified from both intensity and phase time series, it is also seen that both the power and the optical spectra reveal that signature [Fig. 3.5 (c) and (f)]. In SL the α-factor a determines the strength of the coupling between amplitude and phase dynamics. Increasing a as shown in Fig. 3.6 the coupling becomes stronger and thus the size

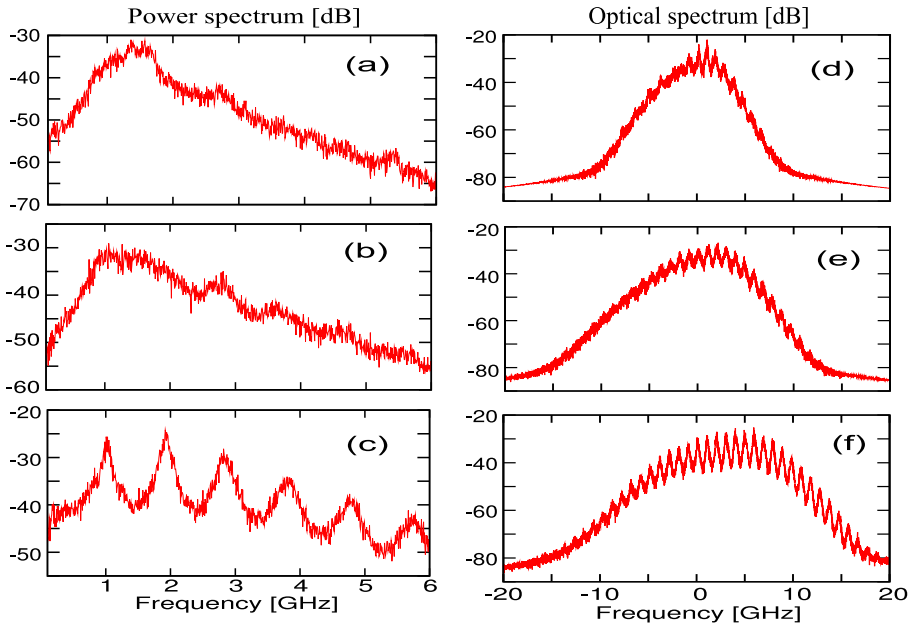


Figure 3.5: Power (left) and optical (right) spectra for $\kappa = 2.5$ ns^{-1} (top row), $\kappa = 5$ ns^{-1} (center row) and $\kappa = 10$ ns^{-1} (bottom row) considering $T = 1$ ns.

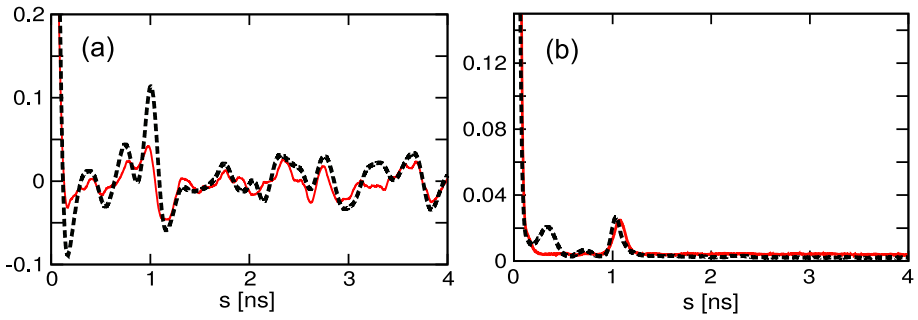


Figure 3.6: Autocorrelation (a) and DMI (b) for $\kappa = 2.5$ ns^{-1}, $T = 1$ ns and $a = 10$ computed from $\varphi(t)$ (solid line) and $\mathcal{R}e[E(t)]$ (dotted line).

of the DMI or autocorrelation peaks computed from the phase decrease. We have checked that for the practical values of the α-factor a, the peak is always visible around the delay time, at least in DMI.

While the results presented in this section do not take into account the noise, we note that the autocorrelation and the DMI are robust to noise so that the results obtained with noisy time series are similar. The spontaneous emission noise of SL can be modeled by adding a stochastic term to the Lang-Kobayashi equations as

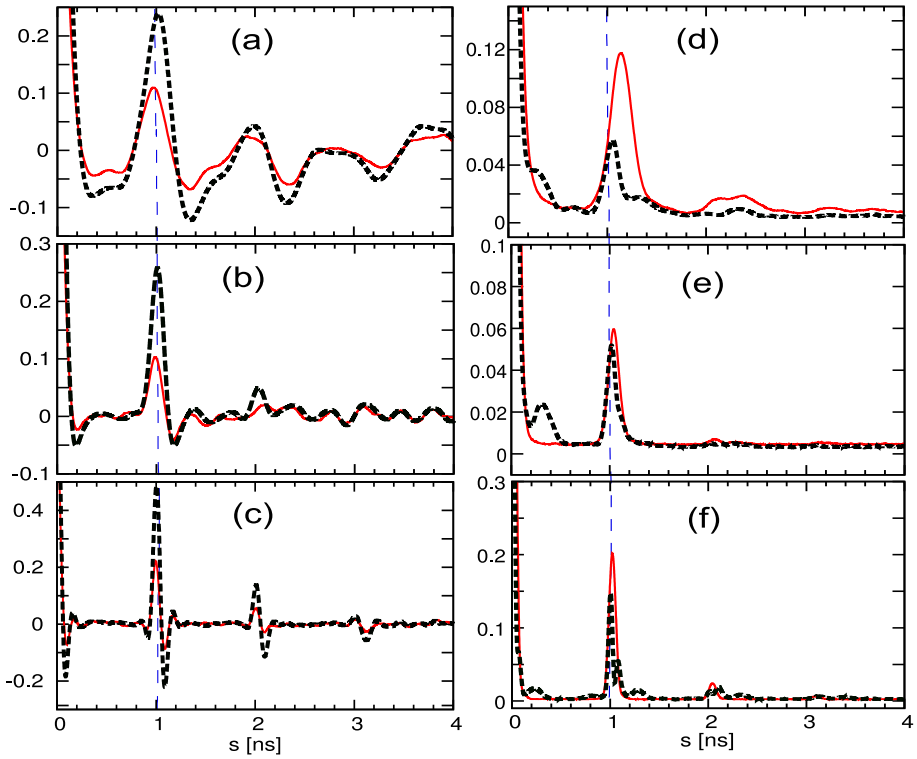


Figure 3.7: Autocorrelation (left) and DMI (right) as in Fig. 3.2 but considering $D_m = 10^3$ s^{-1} computed from $\varphi(t)$ (solid line) and $\mathcal{R}e[E(t)]$ (dotted line).

follows

$$\frac{dE(t)}{dt} = \frac{1+ia}{2}\left(g_m \frac{\mathcal{N}-\mathcal{N}_0}{1+\varrho|E(t)|^2} - \gamma\right) E(t) + \kappa E_T e^{-i\omega_0 T} + \sqrt{2D_m \mathcal{N}(t)}\chi(t),$$
$$\frac{d\mathcal{N}(t)}{dt} = J_0 - \gamma_e \mathcal{N}(t) - g_m \frac{\mathcal{N}-\mathcal{N}_0}{1+\varrho|E(t)|^2}|E(t)|^2, \tag{3.5}$$

where D_m is the spontaneous emission rate, $E_T \equiv E(t-T)$ and $\chi(t)$ is a Gaussian white noise of zero mean and correlation $< \chi(t)\chi^*(t') >= 2\delta(t-t')$ [122]. As shown in Fig. 3.7, the results obtained with noise are similar to that obtained without it, both in the autocorrelation and in the DMI.

3.3 Delay Time Identification in Intensity Chaos Opto-electronic Systems

Here we focus on delay time identification in the intensity chaos system considering $G = 5$ which leads to hyper-chaotic dynamics. Figure 3.8 (two top rows) shows the results using the techniques described before applied to the time series $x(t)$. As it can

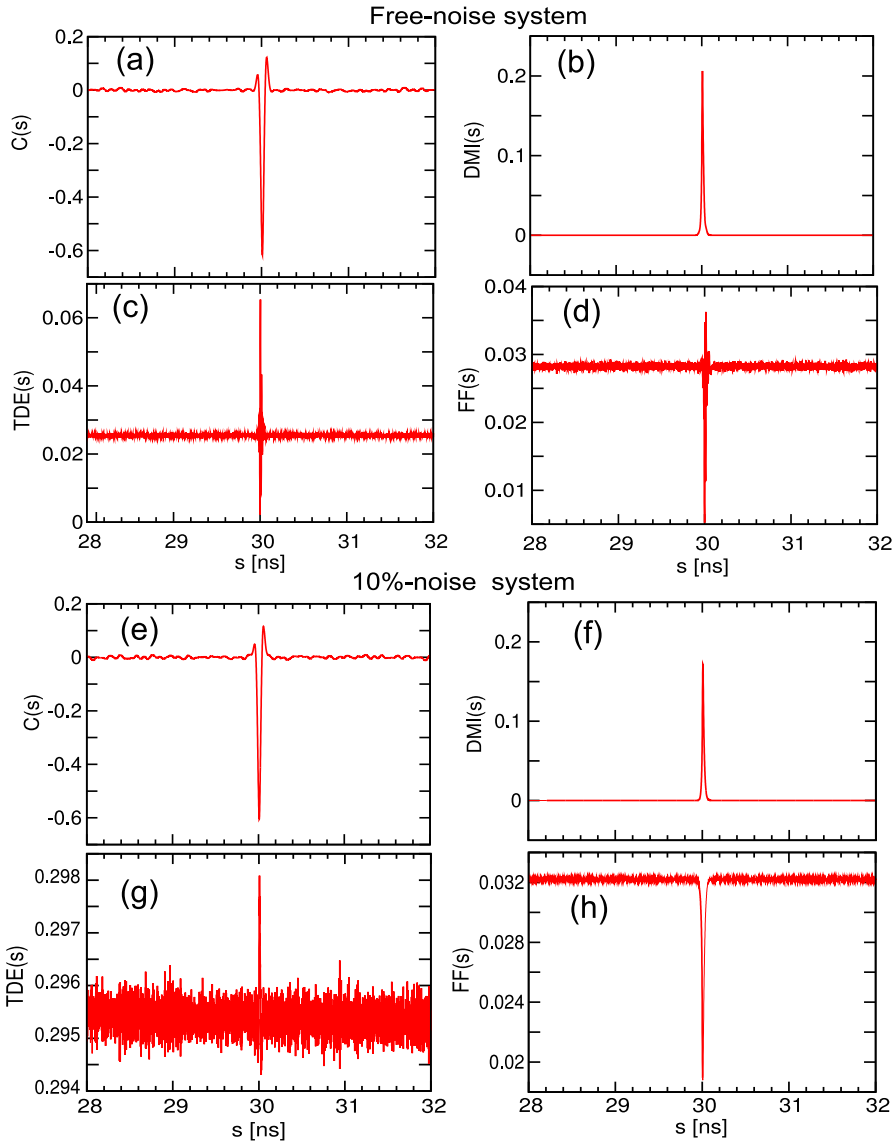


Figure 3.8: (a), (e) AC, (b), (f) DMI, (c), (g) TDE and (d), (h) FF functions as a function of an embedding delay s computed from 10^7 data points corresponding to a 10 μs time series generated from Eqs. (2.6) and (2.7). (a)-(d) correspond to the case without noise. (e)-(f) correspond to a time series obtained by adding a Gaussian white noise of amplitude 10% of the carrier amplitude. All the estimator results are normalized to 1.

be seen, a very pronounced valley or peak is found around 30 ns, which corresponds to the delay time. The results were obtained using 10^7 data points corresponding to a time series of 10 μs recorded after the transient time of 30 μs. The peak appears in AC and DMI at a position which overestimates the delay time by $\tau/2$ (the lowest scale of the model). In order to point out the robustness of different estimators, we

deliberately add a Gaussian white noise of amplitude 10% of the carrier amplitude to the time series generated from free-noise system. Figure 3.8 (two bottom rows) displays the results when applying the delay time identification techniques to the noisy time series. It turns out that, despite the noise, all the techniques reveal the delay time signature. However, while the peak/valley size in AC (e) and DMI (f) is almost the same compared to that found for the free-noise system, e.g (a) and (b) respectively, the visibility of the peak/valley obtained in TDE (g) and FF (h) is significantly reduced as compared to (c) and (d). These results indicate that TDE and FF are sensitive to noise and therefore for a further increase of the noise amplitude, they can become inefficient to identify the delay time.

3.4 Delay Time Identification in Phase Chaos Opto-electronic Systems

As the intrinsic properties of this system are different, this could also affect the delay time identification. Assuming that the time series $x(t)$ from Eqs. (2.20) and (2.21) can be intercepted, a similar approach can be followed for delay-time retrieving. Figures 3.9 (two top rows) show the results for delay time identification considering a free-noise system. One can properly identify peaks or valleys at 30 ns and 30.4 ns corresponding to delay times T and $T + \delta T$, respectively. However, it is seen that the peak sizes are much smaller compared to those found from the intensity setup described by Eqs. (2.6) and (2.7). Note that for the autocorrelation, for example, the peak is 10 times smaller while the DMI peak is about 70 times smaller. This can be explained by the interplay between the two delays. On the other hand, the analysis of Fig. 3.9 (e) and (f) confirm the robustness of AC and DMI to noise, while the TDE (g) and FF (h) do not allow to discriminate the peak at the delay time to the background noise when analyzing a 10%-noise system. In a practical situation, these two last techniques can be inefficient for delay time identification since real systems are always noisy.

The results in the delay time identification were found out in the previous sections by analyzing the ideal signal $x(t)$ which in some cases is not precisely the one transmitted. Besides, the message can also influences the dynamics and have an effect on delay time identification. This is discussed in the next section.

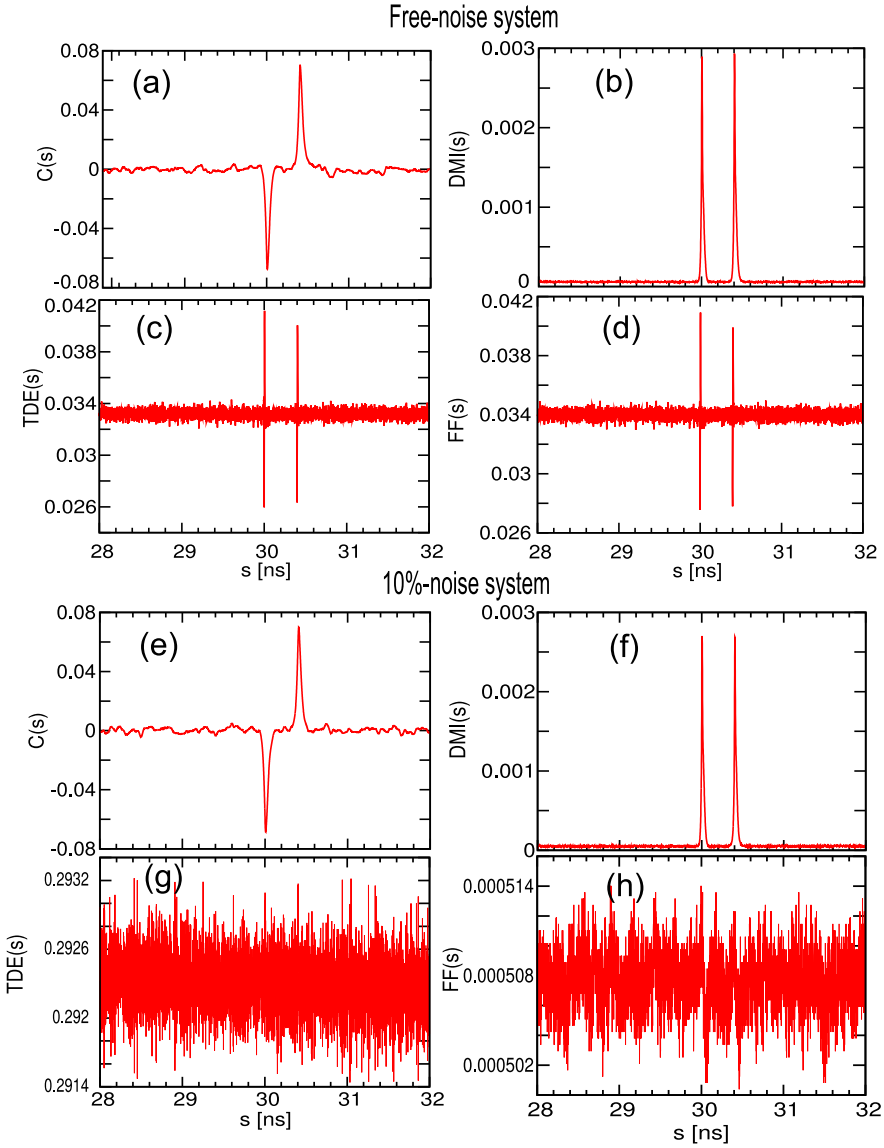


Figure 3.9: (a), (e) AC, (b), (f) DMI, (c), (g) TDE and (d), (h) FF functions as a function of an embedding delay s computed from 10^7 data points corresponding to a 10 μs time series generated from Eqs. (2.20) and (2.21). (e)-(d) correspond to the case without noise. (e)-(f) correspond to a time series obtained by adding a Gaussian white noise of amplitude 10% of the carrier amplitude. All the estimator results are normalized to 1.

3.5 Delay Time Identification from Detected Signal with Message

The first stage in eavesdropping information consists in its interception using appropriate devices. The main objective of this section is to analyze the signal which can

be effectively detected through the transmission channel. The question is addressed considering the intensity and phase chaos electro-optical generators discussed previously. Note that for the all-optical feedback system, the real detected output is proportional to $|E(t)|^2$, already analyzed in the previous section. Through this scheme, the message is embedded with the chaos using chaos masking procedure. Since the message is added outside of the carrier generator, its amplitude should be very small to prevent for direct detection of an intruder and thus cannot really modify the carrier properties so as to blur the delay time.

3.5.1 Intensity chaos model

For the intensity chaos scheme, the overall power that an eavesdropper can detect using photodiode placed in the optical transmission line can be written as

$$\pounds(t) = G'\big\{\alpha_m m(t) + \cos^2[x(t-T)+\phi]\big\}, \tag{3.6}$$

where $G' = PS$ is the amplitude of transmitted signal with P being the amplitude of the power launched into the fiber while S is the sensitivity of the photodiode used for detection. Figure 3.10 displays the size of the peaks at delay time T when the quantifiers are computed from $\pounds(t)$ as the bit rate is varied both in AC (a) and DMI (b) considering different message amplitudes. It turns out that, despite the message, a clear peak emerges closer to the delay time as it was already the case when analyzing $x(t)$ for a system without message. For high message amplitude or high bit rate, the peaks on the estimators decrease but they are always visible at least in the DMI. These results definitively show that in intensity chaos scheme, the delay time can be extracted even when the message is embedded. Not even $\alpha_m = 1$, which means that the amplitude of the message is equal to that of the carrier, can conceal the delay time. Note that $\alpha_m = 1$ is too large for secure transmission since the message can be partially directly detected in $\pounds(t)$.

3.5.2 Phase chaos model

When the data are encoded within a phase, it becomes necessary to use, before photodetectors, devices which can enable to capture the phase variations. Among others, it is possible to use a Fabry-Perot or a Mach-Zehnder interferometer to first convert the phase variations into intensity variations, or optical hybrid couplers to directly estimate the phase. If we assume the message as a non-return to zero sequence having an amplitude matching the cascaded PM halfwave voltage, $m(t)$ then takes logical 0 when no bit is transmitted and $\pi/2$ when a bit 1 is transmitted. When the message is encoded through this topology, the optical signal which leaves

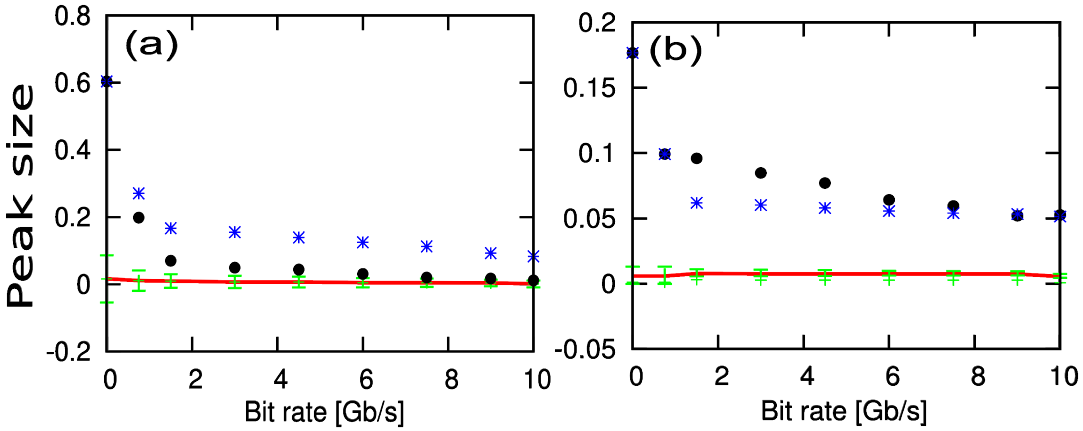


Figure 3.10: Recorded peak size at T for a message amplitude $\alpha_m G$ with $\alpha_m = 1$ ($\bullet$ symbol) and $\alpha_m = 0.4$ ($*$ symbol) versus the bit rate, (a) from AC function, (b) from DMI. The red line corresponds to the mean value of the maxima given by AC or DMI while the bars (green in color) stand for the deviation around this mean value.

the emitter to the receiver is given by

$$E(t) = E_0 e^{2i[x(t)+m(t)]}, \tag{3.7}$$

where E_0 is the constant amplitude of the electric field at the SL output. Here, we use a MZI with imbalanced delay δT_m to convert the chaotic phase variations carrying the message into the intensity ones. The total power which can be detected after transforming the phase into the intensity variations is

$$\pounds(t) = G' \cos^2 \left[(x(t) - x(t - \delta T_m) + m(t) - m(t - \delta T_m) \right], \tag{3.8}$$

We assume for our numerical calculations $SP = 5$ and $\delta T_m = 0.5$ ns. Figure 3.11 displays the peaks given at delay times T ($\bullet$ symbol) and $T+\delta T$ ($*$ symbol) obtained both in AC (a) and DMI (b) considering a time series given by Eq. (3.8). In (a), the peaks in the AC are identifiable only when no message is present or with a message with bit rate less than $1/\delta T$. The peaks approach the noise background as the bit rate is larger than the inverse of the delay time difference $1/\delta T$, e.g. 2.5 Gb/s. Surprisingly, no distinguishable peak is found in the DMI [see Fig. 3.11 b)], even in the absence of the message. The inset plot in Fig. 3.11 illustrates the case without message (blue color), with a 1 Gb/s message (black color) and with a message at 10 Gb/s (red color).

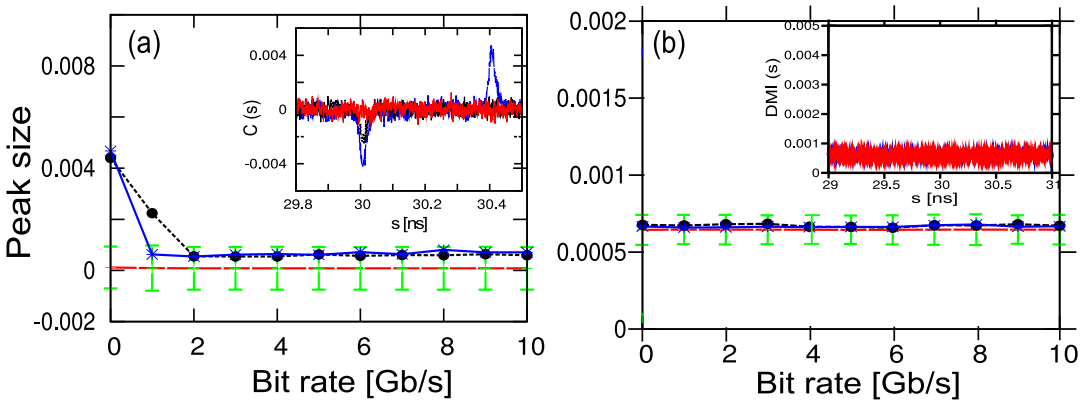


Figure 3.11: Recorded peak size at T ($\bullet$ symbol) and $T+\delta T$ ($*$ symbol) versus the bit rate, a) from autocorrelation function, b) from mutual information. The dashed (red in color) line corresponds to the mean value of the background noise considering the highest 2000 spurious peaks while the bars (green in color) stand for the deviation around this mean value. The inset plot illustrates the case without message (blue color), with a 1 Gb/s message (black color) and with a 10 Gb/s message (red color).

3.6 Identification of Other Parameters

In chaos communication schemes, the extraction of delay time is not enough for unmasking the underlying dynamics. Nonetheless it can contribute to recover other system parameters. In this section we show that once the delay time is identified, systems described by scalar equation can be fully reconstructed. The full reconstruction of a nonlinear system with multiples variables is much more difficult than that of a scalar system.

3.6.1 Intensity chaos opto-electronic system

For intensity chaos schemes as described by Eqs. (2.6) and (2.7), besides the delay time other parameters of the system are the high (low) cutoff response times τ (θ), and the overall loop gain G. They are presumed to be unknown by an intruder. However, real keys are only those which cannot be revealed even using identification methods for chaotic series. On a wavelength chaotic generator which is modeled by a scalar delay system similar to the one for intensity chaos but without a low cutoff filter, Udaltsov *et al.* have shown that it is possible to recover the parameters, once the delay time is identified [108]. They used the spline interpolation to identify the nonlinear function form as a $\sin^2(.)$-function from time series $\lambda(t)$, then they assumed the nonlinear function to be $A\sin^2[B\lambda(t)+C]$ where the parameters A, B and C were subsequently identified as that for which the minimum synchronization

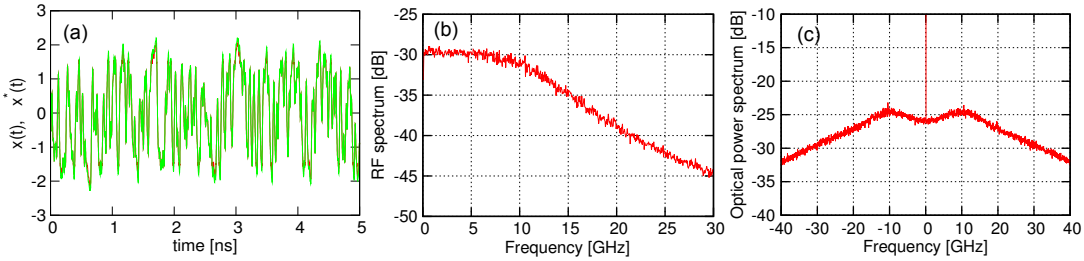


Figure 3.12: (a) A part of the original (red color) and the reconstructed (green color) time series generated from Eqs. (2.6) and (2.7). (b) Corresponding radio-frequency spectrum and (c) Optical power spectrum at the output of MZM.

error in (A,B,C)-plane is obtained. Along the same line, another method based on time extrema statistics has been used to recover the parameters for a Mackey-Glass system [110]. In both cases, the authors made use of the dynamical variable which can be directly intercepted.

Here we attempt the reconstruction of an intensity chaos system for which the dynamical variable is not directly intercepted. We assume that the intruder has knowledge of the topology and can intercept the time series. According to the scheme presented in Sec. 2.2, the transmitted signal can be written as

$$\pounds(t) = G'\{\cos^2[x(t)+\phi]\}. \tag{3.9}$$

The dynamical variable, $x(t)$ can be reconstructed from the intercepted signal, $\pounds(t)$, as follows

$$x^*(t) + \phi = \frac{1}{2}\arccos\left[\frac{2\pounds(t) - G'}{G'}\right], \tag{3.10}$$

where $x^*(t)$ is the reconstructed state of $x(t)$. By applying the average over time in each side of Eq. (3.10), one obtains

$$\langle x^*(t)\rangle + \phi = \frac{1}{2}\left\langle \arccos\left[\frac{2\pounds(t) - G'}{G'}\right]\right\rangle. \tag{3.11}$$

The presence of the low cutoff integral term $u(t)$ in Eq. (2.6) imposes the mean value $\langle x^*(t)\rangle$ to be zero in order to ensure the convergence of the solution even at infinite time. The offset phase, ϕ, is then given by

$$\phi = \frac{1}{2}\left\langle \arccos\left[\frac{2\pounds(t) - G'}{G'}\right]\right\rangle. \tag{3.12}$$

Therefore the reconstructed states, $x^*(t)$, can be deduced as

$$x^*(t) = \frac{1}{2}\arccos\left[\frac{2\pounds(t) - G'}{G}\right] - \frac{1}{2}\left\langle \arccos\left[\frac{2\pounds(t) - G'}{G'}\right]\right\rangle, \tag{3.13}$$

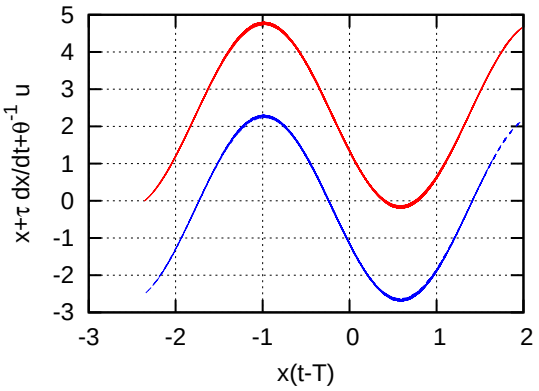


Figure 3.13: Left hand side of Eq. (2.6) as a function of $x(t-T)$ constructed from an intercepted time series without the message. (Red color) $\theta = 1.6\ \mu s$, (blue color) $\theta \to \infty$.

However, because of the periodicity of *cosine*-functions, $x^*(t)$ always evolves within the range $-\pi$ and π. The π jumps artificially created by the arccos-function have to be corrected (by adding $\pm\pi$) so that the time trace for $x(t)$ is continuous. Deriving Eq. (3.13) with respect to time, one obtains

$$\frac{dx^*(t)}{dt} = \frac{-d\pounds(t)/dt}{\sqrt{G'^2 + [2\pounds(t) - G']^2}}. \tag{3.14}$$

Discretizing Eq. (3.14) for the points in the data series, one obtains

$$x_{k+1} = x_k - \frac{\pounds_{k+1} - \pounds_k}{\sqrt{G'^2 + [2\pounds_k - G']^2}}. \tag{3.15}$$

This discretized version is used to correct the artificial π jumps. Figure 3.12 shows the reconstructed time traces (green color) in comparison with the original one (red color). It turns out that both traces are match very well [see Figure 3.12 (a)].

By plotting the spectrum both in electrical (b) and optical (c) domains, it appears that signal bandwidth may span over more than 30 GHz around the nominal frequency of the laser beam. By inspecting the RF power spectrum displayed in Fig. 3.12 (b), the value of the high cutoff frequency, τ can be estimated around 9 GHz which corresponds to $\tau^* = 17.7$ ps while the real cutoff response time is $\tau = 20$ ps. The difference between the estimated and the real value is 11.5% which for τ-mismatch is a good result for an eavesdropper since for this parameter, good synchronization is still obtained even with a mismatch larger as 15% [105]. Alternatively, this parameter can be determined used time extrema statistics if the delay time is known [110].

Given the values of τ and T, an estimation of the nonlinear function can be done by plotting the left hand side of Eq. (2.6) as a function of delayed variable, $x(t-T)$. Since the value of θ is a priori unknown, its role in synchronization can be pointed out by separately studying the cases with and without the low cutoff response time θ. Figure 3.13 displays the nonlinear function of the model neglecting the integral term (blue color) and when taking into account the integral with the correct value of θ (red color). Inspecting this figure, it appears that the integral term just shifts the nonlinear function of $G/2$ corresponding to the continuous component of $\cos^2(.)$ which is removed by the integral (high-pass filter). By measuring the peak-to-peak amplitude of the nonlinear function, one notices that it exactly coincides with the overall loop gain G. Finally, the last parameter θ can be deduced by averaging over time each side of Eq. (2.6), e.g.

$$\theta = \frac{-\tau \left\langle \frac{dx}{dt} \right\rangle + G \left\langle \left\{ \cos^2 \left[x(t-T) + \phi \right] \right\} \right\rangle}{\left\langle \int_{t_0}^{t} x(t')dt' \right\rangle}. \tag{3.16}$$

One can also notice that the value of the nonlinear function for $x(t-T) = 0$ coincides with that of $G\cos^2\phi$. Thus, knowing G, one can deduce the value of ϕ. Also it is worth noting that the accurate estimation of the integral requires a long time trace.

When the message is encoded through this scheme, the intercepted signal becomes

$$\pounds(t) = G' \left\{ \alpha_m m(t) + \cos^2 \left[x(t) + \phi \right] \right\}, \tag{3.17}$$

and thus the value of ϕ given by

$$\phi = \frac{1}{2} \left\langle \arccos \left[\frac{2\pounds(t) - 2G'\alpha_m m(t) - G'}{G'} \right] \right\rangle, \tag{3.18}$$

becomes difficult to estimate since $\alpha_m m(t)$ is not known.

3.6.2 Phase chaos opto-electronic system

Besides the parameters mentioned above the phase chaos system has an additional imbalanced delay time δT. Furthermore, the eavesdropping of the message can be more complicated as it is encoded in the phase rather than in the intensity which is easier to detect. Note that the recovery of the phase requires more sophisticated equipment whose the accuracy may also play an important role.

Assuming that the phase can be intercepted, a similar approach can be followed for its reconstruction. We plot the RF power spectrum (Fig. 3.14) and extract its -3 dB frequency, which, in principle, corresponds to the high cutoff frequency of the filter. We obtain a -3 dB frequency of about 8 GHz corresponding to the cutoff

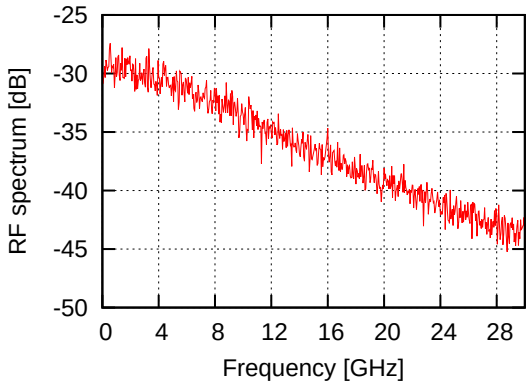


Figure 3.14: RF spectrum of $x(t)$.

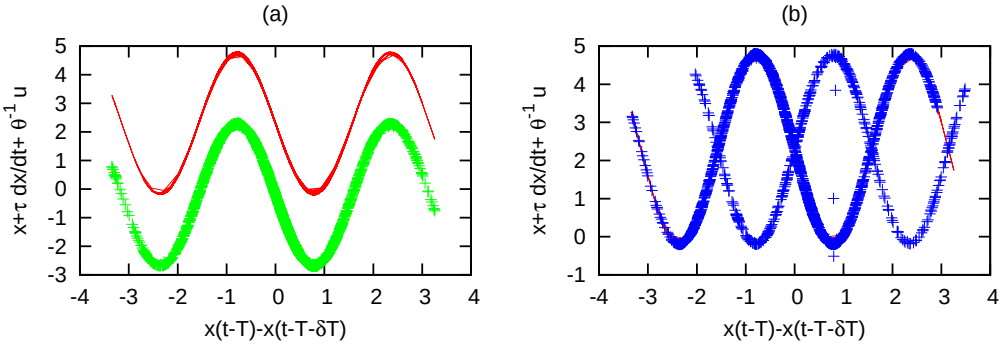


Figure 3.15: $x + dx/dt + u/\theta$ as a function of $x(t-T) - x(t-T-\delta T)$ for (a) $\theta = 1.6$ μs (solid line) and $\theta \to 0$ (symbol line) without message, (b) for $\theta = 1.6$ μs considering a 1 Gb/s message (symbol line) and no message (solid line). The plots were obtained with parameters $\tau = 12.2$ ps, $\theta = 1.6$ μs, $T = 30$ ns, $\delta T = 400$ ps and $\phi = \pi/4$.

response time $\tau^* = 19.9$ ps while the real value is $\tau = 20$ ps. Given the value of τ, T and δT, we plot $x + dx/dt$ as a function of $x(t-T) - x(T+\delta T)$ as shown in Fig. 3.15. The effect of the integral, as before, is to shift the nonlinear function. From the curve amplitude, one extracts G. The value of ϕ is extracted at $x(t-T) - x(T+\delta T) = 0$.

Figure. 3.15 (b) displays the nonlinear function when the message is encoded. It shows two curves whose one, corresponding to the bit 0 ($m(t) = 0$) coincides with the curves without the message. The second curve related to the bit 1 ($m(t) = \pi/2$), is $\pi/2$-dephased to the first one. However, it should be noticed that the estimation of the parameters can be compromised in real systems because of the noise.

3.7 Conclusions

Our efforts to identify the drawbacks in opto-electronic systems for chaos communications has led to the conclusion that the delay time is the most vulnerable parameter which can be retrieved using delay time identification techniques. These results therefore confirm those already reported in the literature [107, 114, 123, 124]. In fact we have found that, although their high complexity, the delay time can be identified in such systems using standard methods and when even computing from noisy series gained from systems with multiple delays as already reported in [110]. Still worse, we have found that some scalar systems can be fully reconstructed once the delay time is known. However, full reconstruction seems difficult for multiple variable systems, although the extraction of the delay time is possible.

Chapter 4

Dynamics of Electro-optic Delay Systems with Feedback in the Laser Source

The previous chapter has shown the limits of scalar systems once the topology is known. Besides, optical chaos encrypted communications require a wide spectrum of the chaotic carrier to efficiently mask the message from eventual eavesdroppers. This goal can be achieved in optoelectronic devices by increasing the gain loop parameter [96, 125]. However, the loop gain, and consequently the complexity of the system, is experimentally limited due to the saturation of some device components. Therefore, it becomes necessary to investigate alternative ways to produce a stronger chaos complexity. Moreover, the increase in the number of the system parameters can also be fruitful for providing more security since an eavesdropper has to face up the parameter mismatches to succeed in building an adequate receiver necessary for the decryption of the message. A way to reach all these purposes can consist in involving an extra feedback loop feeding the laser. It is worth noting that the feedback in the controlled source has been previously considered in opto-electronic systems by Udaltsov *et al.* as a possible way to get around delay time cracking [109].

In this chapter, we explore the impact of such combination as a fruitful alternative for improving security in electro-optic delay systems [126]. The chapter is organized as follows: In Sec. 4.1 we introduce two new configurations differing in the way the laser feedback is performed. Sec. 4.2 is devoted to the theoretical and numerical results of each configuration while Sec. 4.3 deals with the synchronization and the effects of parameter mismatch. In Sec. 4.4, the viability of the models is numerically tested by encoding and decoding the message. Finally Sec. 4.5 provides some concluding remarks and outlooks.

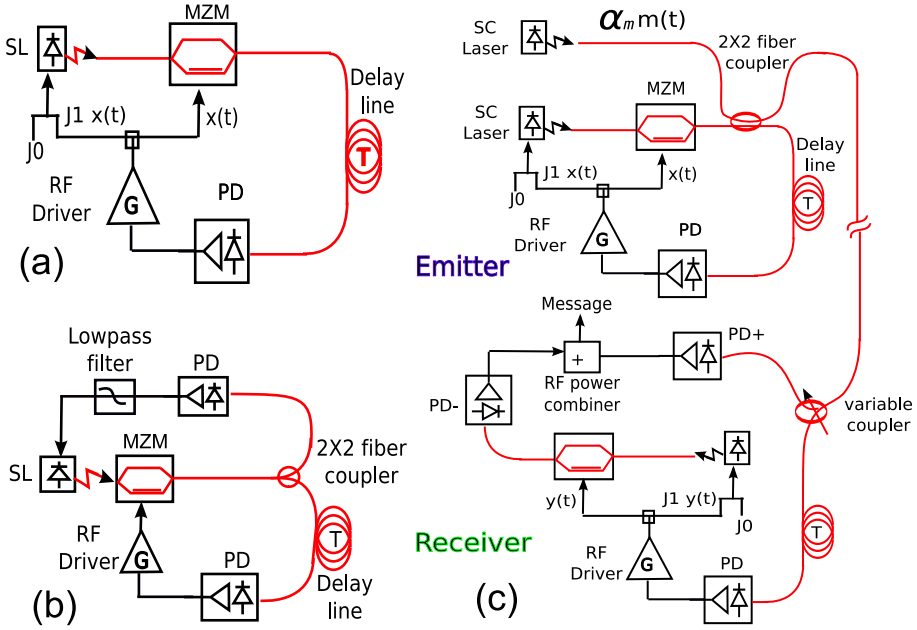


Figure 4.1: Schematic setup: (a) Emitter for System I; (b) Emitter for System II; (c) Full emitter-receiver setup for system I.

4.1 The System

We consider a modification of the basic architecture presented in Sec. 2.2 in which a part of the signal from the filter loop is used to modulate the pump current of semiconductor laser. Therefore, now the laser output power depends on the RF voltage $x(t)$, meaning that the overall loop gain G in Eq. (2.6) which is proportional to the laser output power is also time dependent $G(t) = G_1 I(t)$, where G_1 is the normalized electro-optical gain coefficient while $I = |E(t)|^2$ is the photon number. Therefore Eqs. (2.6) and (2.7) become

$$x + \tau\frac{dx}{dt} + \frac{1}{\theta}u = G_1 I(t-T)\cos^2\left[x(t-T)+\phi\right], \tag{4.1}$$

$$\frac{du}{dt} = x. \tag{4.2}$$

The photon number I is obtained from the semiconductor laser rate equations [122]:

$$\frac{dI}{dt} = (\mathcal{G}-\gamma)I, \tag{4.3}$$

$$\frac{d\mathcal{N}}{dt} = J_0 - \gamma_e\mathcal{N} - \mathcal{G}I + F(x), \tag{4.4}$$

$$\mathcal{G} = g_m(\mathcal{N}-\mathcal{N}_0)/(1+\varrho I), \tag{4.5}$$

where the parameters are as defined in Eq. (2.1). It is clearly seen that additionally to the DC current component J_0, we have a feedback contribution $F(x)$ which is a function of the RF voltage, $x(t)$. The explicit expression of $F(x)$, and consequently the behavior of the system depends on the setup. Here we consider two different schematic setups as shown in Figs. 4.1.

4.1.1 System I

A fraction of the RF output voltage is converted to current J_1 using a voltage-to-current converter, and injected back to the laser [Fig. 4.1 (a)] so that

$$F(x) = J_1 x(t). \tag{4.6}$$

Since $x(t)$ is a dimensionless variable, J_1 has the same unit as J_0. It is worth to note that the modeling holds for a laser whose bandwidth is larger than that of the photodiode or RF driver meaning that the laser does not filter the signal.

4.1.2 System II

A fraction of the optical light is detected at the output of MZM using a 2×2 fiber coupler and an additional photodetector, then it is converted into an electrical signal and finally into a current to modulate the pump [Fig. 4.1 (b)]. In this process those frequencies larger than the photodetector bandwidth f_c are filtered out. We model this as a low-pass filter having input signal $J_1 G_1 I \cos^2[x(t) + \phi]$ which comes from converting the optical signal into an electric one. The feedback contribution in laser in this case is then given by

$$\frac{dF}{dt} = -2\pi f_c \big\{ F - J_1 G_1 I \cos^2[x(t) + \phi] \big\}. \tag{4.7}$$

It is worth noting that in System I, the signal is divided in the electrical domain using the RF divider while in System II, it is done in optical domain through an optical fiber splitter. As $u(t)$ is an integral, $\langle x(t) \rangle$ should be zero in order to ensure the convergence of the solution even at infinite time. This is true for the case of no feedback in the laser as well as for the two new systems introduced here. For system I the feedback dependent current injected in the laser F has a zero average, so that the average of the output intensity $\langle I \rangle$ is the same as the constant laser power without the feedback, and $G_1 \langle I \rangle = G$. That is not the case for system II.

4.2 Theoretical and Numerical Study

For the numerical study, we take the following parameter values $g_m = 1.5 \times 10^{-8}$ ps^{-1}, $\varrho = 2 \times 10^{-7}$, $N_0 = 1.2 \times 10^8$, $\gamma = 3.3 \times 10^{11}$ s^{-1}, $\gamma_e = 5 \times 10^8$ s^{-1} [127]. With these

parameters, the threshold current is $J_{th} = 7.1 \times 10^{16}$ s^{-1}. For the electro-optical loop, we consider $\tau = 20$ ps, $\theta = 1.6$ μs, $G_1 = 2.89 \times 10^{-5}$, $T = 30$ ns. Others parameters will be stated in the figure captions.

4.2.1 System I

To find the fixed points, all the derivatives are set to zero, $dx/dt = dw/dt = 0$. There is a single fixed point solution $(x_{st}, w_{st}, I_{st}, \mathcal{N}_{st})$ given by

$$\begin{aligned} x_{st} &= 0, \\ w_{st} &= \theta G_1 I_{st} \cos^2\phi, \\ I_{st} &= \frac{J_0 g_m - \gamma_e g_m \mathcal{N}_0 - \gamma_e \gamma}{\gamma(g_m + \varrho\gamma_e)}, \\ \mathcal{N}_{st} &= \frac{g_m \mathcal{N}_0 + \gamma + \varrho J_0}{g_m + \varrho\gamma_e}. \end{aligned} \tag{4.8}$$

Assuming $x = x_{st} + \delta x$, $w = w_{st} + \delta w$, $I = I_{st} + \delta I$ and $\mathcal{N} = \mathcal{N}_{st} + \delta\mathcal{N}$, and linearizing Eqs. (4.1), (4.3)-(4.5) around the fixed point, the stability of this fixed point is determined by the following 4×4 matrix

$$\mathcal{M} = \begin{pmatrix} \tilde{a}_{11} + a_{11}e^{-\lambda T} & a_{12} & a_{13}e^{-\lambda T} & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & a_{33} & a_{34} \\ J_1 & 0 & a_{43} & a_{44} \end{pmatrix}$$

where the coefficients are

$$\begin{aligned} &a_{11} = -\frac{G_1 I_{st}}{\tau}\sin 2\phi, \tilde{a}_{11} = -\frac{1}{\tau}, a_{12} = -\frac{1}{\tau\theta}, \\ &a_{13} = \frac{G_1 \cos^2\phi}{\tau}, a_{33} = -\frac{\varrho\gamma I_{st}}{1+\varrho I_{st}}, a_{34} = \frac{g_m I_{st}}{1+\varrho I_{st}}, \\ &a_{41} = J_1, a_{43} = \frac{-\gamma}{1+\varrho I_{st}}, a_{44} = -\gamma_e - \frac{g_m I_{st}}{1+\varrho I_{st}}. \end{aligned} \tag{4.9}$$

The steady state is stable if the real part of all the eigenvalues λ are negative. The spectral analysis of delayed systems is more involved than that of ordinary systems since the term $e^{-\lambda T}$ in the matrix $\mathcal{M}$ leads to a characteristic equation which can have an infinite number of eigenvalues. Out of all those eigenvalues, typically one computes a finite set of the eigenvalues with largest real part. One of the packages that can be used for this purpose involves the DDE-BIFTOOL algorithm in MATLAB [128]. In this method characteristic roots are computed through successive approximations. We henceforth use this method to investigate the stability of the steady state given above. The presence of $\sin 2\phi$ and $\cos^2\phi$

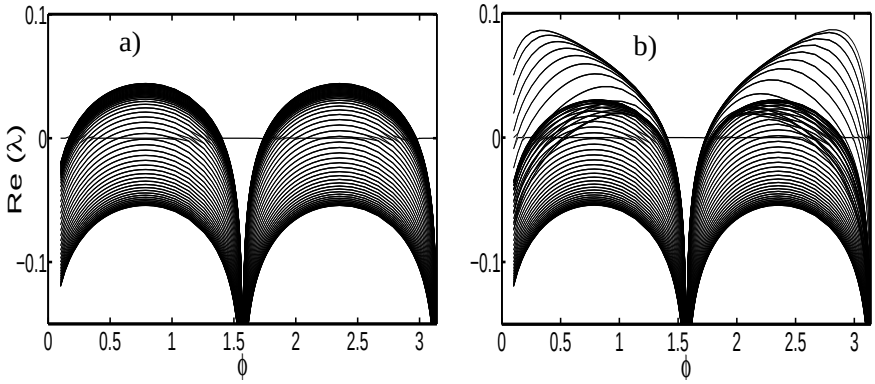


Figure 4.2: Real part of the top eigenvalues versus offset phase for (a) $J_1 = 0.0$ and (b) $J_1 = 0.08J_0$. We have chosen $J_0 = 1.5J_{th}$ which corresponds to $\langle G \rangle = G_1 \langle I \rangle = 3.08$.

in the matrix coefficients shows that the function is π-periodic. Therefore we can perform the stability analysis only over the interval $[0, \pi]$ without loosing generality. Figure 4.2 shows the real part of the top eigenvalues of $\mathcal{M}$. When the feedback is only applied to the MZM ($J_1 = 0$) [Fig. 4.2 (a)], there are three stable regions (around zero, $\pi/2$ and π) corresponding to the offset phases which lead to the predominance of destructive interference. Adding the feedback to the SL the stationary state for $\phi = 0$ or π is destabilized while the stationary state corresponding to $\phi = \pi/2$ remains stable [see Fig. 4.2 (b) for $J_1 = 0.08J_0$].

Figure 4.3 (left) shows the bifurcation diagram for $J_1 = 0$ displaying all the maxima and minima of a long time trace obtained for each value of the offset phase ϕ. All the results are obtained after integrating over a time of 40 μs which is 25 times longer than the slowest time scale θ of the model. The time step used for the numerical integration is 1 ps. The single value for the amplitude maxima found for phases close to zero, $\pi/2$ and π corresponds to the stable steady state described in the previous paragraph. Multiple values for the amplitude maxima or minima correspond to multi-periodic or chaotic behaviors. Figure 4.3 (right) shows the corresponding bifurcation diagram for $J_1 = 0.08J_0$. As predicted by the linear stability analysis, the steady state solutions for offset phase $\phi = 0$ and $\phi = \pi$ are now unstable and the system displays a chaotic behavior. Furthermore inspecting the values of the offset phases for which the system is already unstable, we see that typically the spread of bifurcation diagram looks larger and denser indicating that the system has become more chaotic by applying feedback in the laser.

Quantitatively speaking, one could characterize the complexity using the dimensionality of the attractor. However, in delay systems the dimensionality grows linearly with the delay time while the complexity of the system does not change so much. Therefore it is more convenient to characterize the complexity by the means

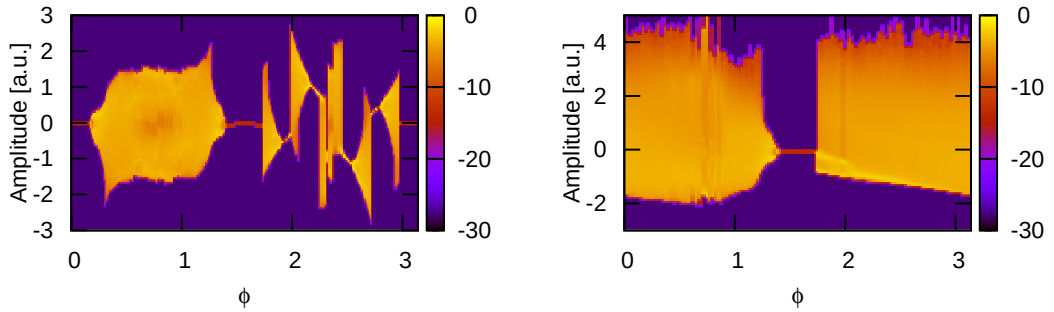


Figure 4.3: Bifurcation diagram versus offset phase ϕ for $J_0 = 1.5J_{th}$: (left) $J_1 = 0.0$ and (right) $J_1 = 0.08J_0$.

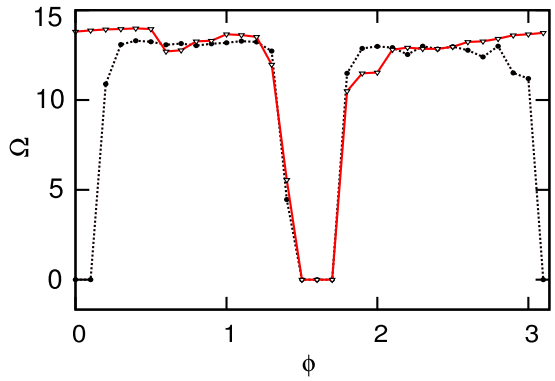


Figure 4.4: Entropy Ω of $x(t)$ versus offset phase ϕ for $J_1 = 0$ ($\bullet$ symbol) and $J_1 = 0.08J_0$ (∇ symbol). We use a data series with 4×10^7 points sampled in 4×10^6 histogram bins.

of the statistical entropy which is an indicator showing how the system is organized or disorganized. Gain of the entropy indicates the increase of disorder and eventually the increase of the system complexity. The entropy of a system described by a variable $x(t)$ is defined as

$$\Omega = -\sum_{x(i)} p(x(i)) \ln \left[p(x(i))\right], \tag{4.10}$$

where $p(x)$ is the density probability function of $x(t)$. Figure 4.4 shows the entropy of the system for $J_1 = 0$ ($\bullet$ symbol) and $J_1 = 0.08J_0$ (∇ symbol) obtained for different values of the offset phase ϕ. It can be seen that the system becomes more chaotic (higher entropy) by applying the feedback in the laser. This is noticeably true for the values of ϕ for which steady states were observed without the feedback in the laser. Also, there are some values of ϕ for which the system is in fact less chaotic. Note that the steady state solutions are here indicated by zero-entropy.

On the other hand, different dynamical regimes can be observed by simply

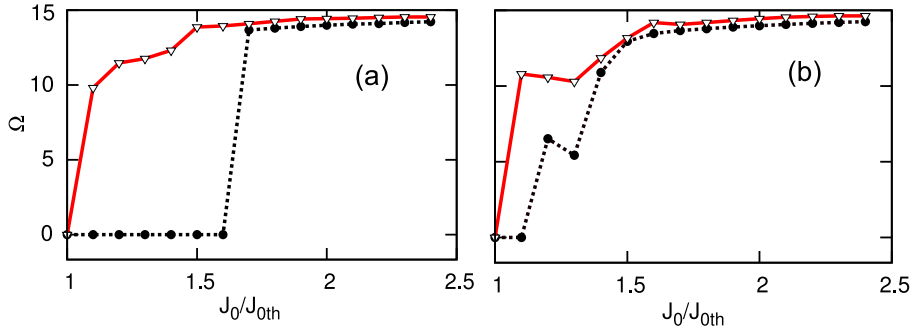


Figure 4.5: Entropy versus the injection current J_0 for offset phases $\phi = 0.1$ (a) and $\phi = \pi/4$ (b). We have taken $J_1 = 0.0$ ($\bullet$ symbol) and $J_1 = 0.08J_0$ (∇ symbol) . We use a data series with 4×10^7 points sampled in 4×10^6 histogram bins.

changing the pump current J_0. Figures 4.5 show the entropy displayed by varying the pump current, J_0, either when there is no feedback in the laser ($\bullet$ symbol) or considering feedback in the laser (∇ symbol) for two values of the offset phase as indicated in the figure caption. For $\phi = 0.1$ when there is no feedback in the laser, the system does not go into a chaotic regime until $J_0 \simeq 1.6J_{th}$. By adding the feedback in the laser, the system becomes chaotic much earlier ($J_0 \simeq 1.1J_{th}$) [see Fig. 4.5 (a)]. For $\phi = \pi/4$ the system goes smoothly into a chaotic regime for $J_0 \simeq 1.1J_{th}$ when no feedback is present in the laser. Adding the feedback in the laser, the fixed point is destabilized just after the threshold ($J_0 \simeq 1.01J_{th}$) [see Fig. 4.5 (b)].

4.2.2 System II

The fixed point of this model is given by $(x_{st}, w_{st}, I_{st}, N_{st}, F_{st})$ where

$$
\begin{aligned}
x_{st} &= 0, \\
w_{st} &= \theta G_1 I_{st} \cos^2\phi, \\
I_{st} &= \frac{(J_0 + F_{st})g_m - \gamma_e g_m \mathcal{N}_0 - \gamma_e\gamma}{\gamma(g_m + \varrho\gamma_e)}, \\
\mathcal{N}_{st} &= \frac{g_m\mathcal{N}_0 + \gamma + \varrho(J_0 + F_{st})}{g_m + \varrho\gamma_e}, \\
F_{st} &= J_1 G_1 I_{st} \cos^2\phi.
\end{aligned}
\tag{4.11}
$$

We should note that for this system the photon number at the steady state is larger and depends on the offset phase. The stability of this fixed point can be investigated following an approach similar to that of subsection 4.2.1. Since now we

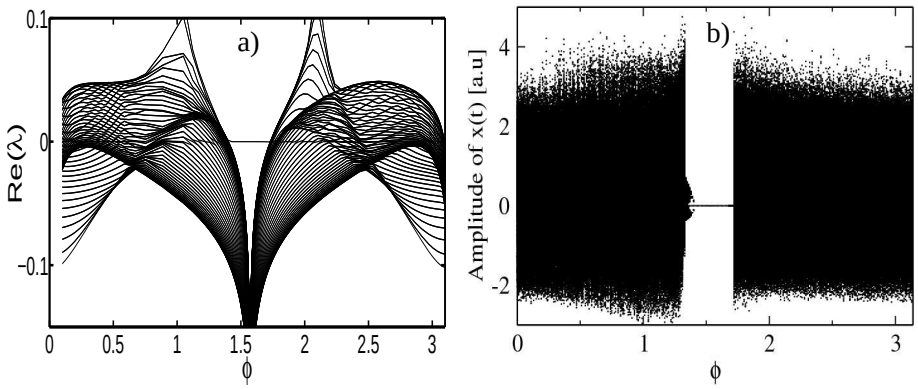


Figure 4.6: a) Real part of the top eigenvalues of matrix $\mathcal{M}$ and b) bifurcation diagram versus offset phase for $J_0 = 1.5J_{th}$ and $J_1 = 0.08J_0$.

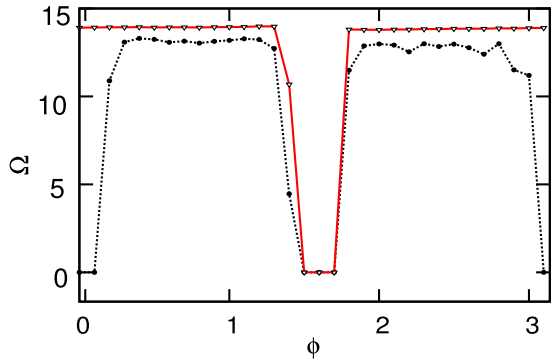


Figure 4.7: Entropy Ω of $x(t)$ versus offset phase ϕ for $J_1 = 0$ ($\bullet$ symbol) and $J_1 = 0.08J_0$ (Δ symbol). We use a data series with 4×10^7 points sampled in 4×10^6 histogram bins.

have an extra equation [Eq. (4.7)] we have to deal with the 5×5 matrix

$$\mathcal{M} = \begin{pmatrix} \tilde{a}_{11} + a_{11}e^{-\lambda T} & a_{12} & a_{13}e^{-\lambda T} & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & a_{33} & a_{34} & 0 \\ 0 & 0 & a_{43} & a_{44} & 0 \\ \eta_e I_{st} \sin(2\phi) & 0 & -\eta_e \cos^2\phi & 0 & -2\pi f_c \end{pmatrix}$$

where $\eta_e = 2\pi f_c J_1 G_1$ and the coefficients a_{ij} are given by Eq. (4.9) with I_{st} given by Eq. (4.11). The real part of the top eigenvalues of this matrix are plotted in Fig. 4.6 (a). As happens for system I the feedback in the laser destabilizes the steady state around the offset phases 0 and π while a narrow region of stability for the stationary state remains for an offset phase around $\phi = \pi/2$. Figure 4.6 (b) shows the bifurcation diagram as a function of the offset phase. Comparing this figure with Fig. 4.3 (left), it can be seen that the system develops more chaotic regions than system with no feedback in the laser. Furthermore, Fig. 4.7 clearly

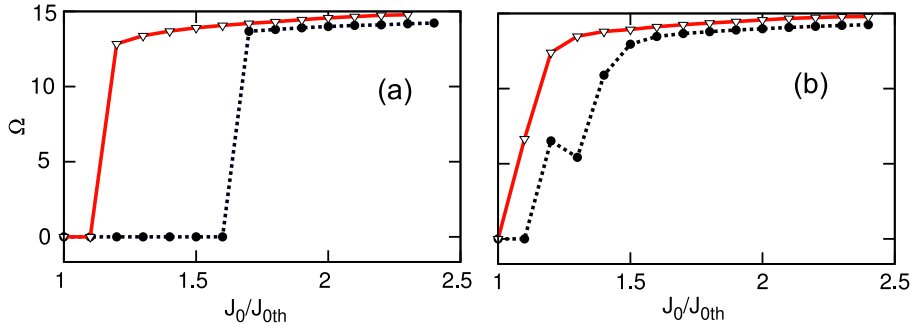


Figure 4.8: Entropy versus the injection current J_0 for offset phases $\phi = 0.1$ (a) and $\phi = \pi/4$ (b). We have taken $J_1 = 0.0$ ($\bullet$ symbol) and $J_1 = 0.08J_0$ (Δ symbol). We use a data series with 4×10^7 points sampled in 4×10^6 histogram bins.

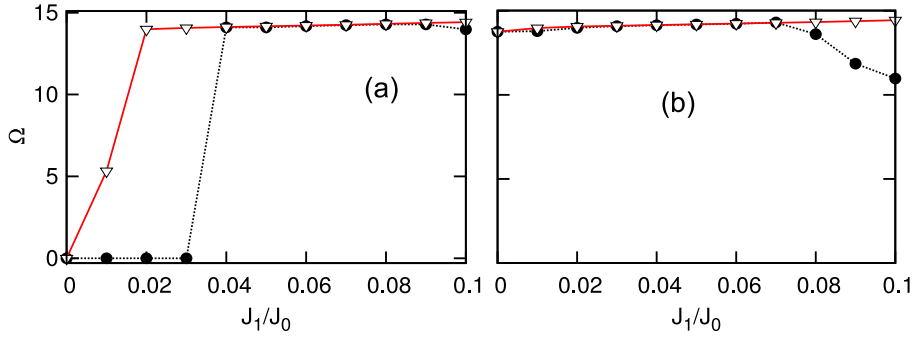


Figure 4.9: Entropy versus J_1 for (a) $\phi = 0.1$ and (b) $\phi = \pi/4$ considering system I ($\bullet$ symbol) and system II (Δ symbol). We use a data series with 4×10^7 points sampled in 4×10^6 histogram bins. We consider a pump current $J_0 = 1.5J_{th}$.

evidences that system II is more chaotic for the whole range of offset phases than the system without feedback in the laser and than system I with the same J_1. In Fig. 4.8 we plot the entropy as function of the injected current J_0 for $J_1 = 0.08J_0$ and two values for the offset phase. When comparing with the case without the feedback in laser, it is seen that for both values of the offset phase chaos starts being developed for a lower value of the pump current J_0.

4.2.3 Other results

To sum up this section, we plot the entropy of each proposed system as function of the laser feedback strength parameter J_1 considering $J_0 = 1.5J_{th}$. It can be seen from Fig. 4.9 (a) that the feedback in the laser induces chaos for the offset phase $\phi = 0.1$ for which the system is stable without J_1. This happens faster for system II than for system I. An increase in J_1, for a fixed value of offset phase $\phi = 0.1$ leads to a more chaotic behavior for both systems. When considering $\phi = \pi/4$ as

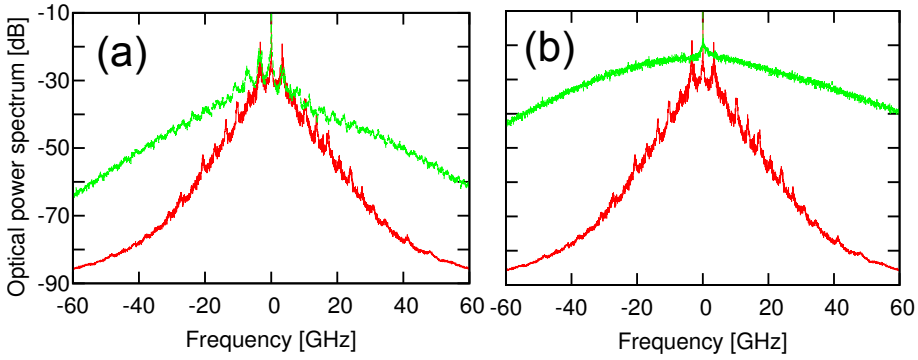


Figure 4.10: Optical power spectrum at the output of MZM considering $J_0 = 1.5J_{th}$ and $\phi = 0.3$: $J_1 = 0$ (red line), $J_1 = 0.08J_0$ (green line) for (a) system I and (b) system II.

shown in Fig. 4.9 (b), the entropy for system II keeps increasing with J_1 in the range of parameters we have explored. On the contrary, the entropy of system I starts decreasing after some threshold around $0.08J_0$ meaning that the effect of the feedback in the laser becomes negative.

On the other hand it is also possible to evidence the increase in chaos complexity by plotting the power spectrum of the optical signal transmitted from the emitter to the receiver. The optical output intensity of the MZM is given by $G_1 I(t) \cos^2 [x(t) + \phi]$. Figures 4.10 show, in green color, the optical power spectrum for system I (a) and system II (b) in comparison with the system without feedback in the laser (red color). The peak at frequency zero corresponds to the DC component of the optical power output. What matters for chaos codification is the rest of the spectrum beyond the DC peak. For $J_1 = 0$, when no feedback is applied to the laser (red line) the power spectrum spans over 55 dB in the range of 60 GHz and present peaks around the DC frequency spacing by the inverse of delay time. For $J_1 = 0.08J_0$ (green line), the spectrum broadens significantly. For system I the spectrum spreads only over 40 dB in the range of 60 GHz. The spectrum of system II is even broader, spreading 20 dB over the same frequency range. We can also notice that the peaks around the central frequency have disappeared for system II, meaning that full chaos has been developed.

4.3 Receiver System and Effects of Parameter Mismatch

4.3.1 Receiver system

For each model, the receiver is built similarly to the emitter. The only difference is that the receiver is fed back by the light only coming from the master instead of itself light. The full emitter-receiver scheme of System I is represented in Fig. 4.1

(c). The feedback in the receiver laser comes from the RF driver output. System II is built similarly but feedback in the receiver laser comes from its MZM output. Introducing $y(t) = \pi V'(t)/(2V_\pi)$ and $u' = \int_{t_0}^{t} y(t')dt'$, the receiver dynamics is given by

$$\frac{dI'}{dt} = (\mathcal{G}' - \gamma')I', \tag{4.12}$$

$$\frac{d\mathcal{N}'}{dt} = J_0' - \gamma_e'\mathcal{N}' - \mathcal{G}'I' + F(y), \tag{4.13}$$

$$y + \tau'\frac{dy}{dt} + \frac{1}{\theta'}u' = G_1' I(t - T') \cos^2\left[x(t - T') + \phi\right], \tag{4.14}$$

where the prime "′" denotes the receiver. It is important to remark that Eq. (4.14) is independent of the receiver laser parameters. However, the receiver laser is necessary for decoding. That is why it is more convenient to measure the synchronization quality between the emitter and the receiver at the output of the MZMs rather than their RF inputs as it is usually the case. For this purpose, we define $\pounds(t)$ and $\pounds'(t)$ as the detected power by PD_+ and PD_-, respectively, assuming the same sensitivity of photodiodes S. They can be therefore written as

$$\pounds(t) = SG_1 I(t) \cos^2\left[x(t) + \phi\right], \tag{4.15}$$

$$\pounds'(t) = SG_1' I'(t) \cos^2\left[y(t) + \phi'\right]. \tag{4.16}$$

The quality of that synchronization depends on several factors, including the parameter mismatch between the master and the receiver, the presence of noise fluctuations and the degradation due to fiber propagation effects. The latter has been considered in [129] for the chaos generated by an all-optical feedback system where the authors showed that compensating the losses by in-lining EDFAs every 50 km and using dispersion shifted fiber, one can minimize the fiber effects to the very acceptable level. Also, in ref. [130] similar results were found out using standard transmission fibers and then compensating the dispersion using dispersion compensation modules. Here we neglect the effect of noise fluctuations and therefore we focus on the effect of parameter mismatch. We first consider that all the receiver parameters are identical to the master except for the delay time.

Figures 4.11 show the time trace of $\pounds(t)$ and $\pounds'(t)$ when the two delay times are different. It can be seen that system II induces faster fluctuations than system I (notice the different scale in the time axis of the figure). In both cases the receiver synchronizes with the master shifted in time $\Delta T = T' - T$. Thus mismatches in the delay time produce a trivial effect. The flying time, delays induced by the electrical connections, and the response time of the system (which play exactly the

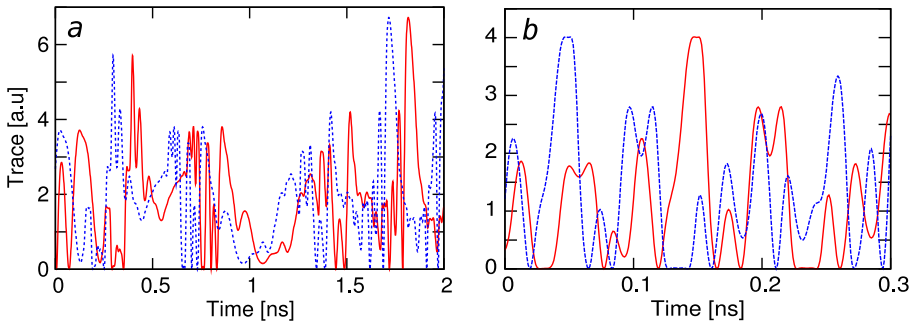


Figure 4.11: Emitter (solid red line) and receiver (dashed blue line) time traces at the MZM output for $\Delta T = -0.1$ ns considering (a) system I and (b) system II. $J_0 = 1.5J_{th}$,$J_1 = 0.08J_0$ and $\phi = 0.3$.

same role as the receiver delay time) just shift the time traces [105]. However, a slight difference on other parameters between the emitter and receiver due to manufacturing mismatches, which are unavoidable, can degrade the synchronization as addressed in the next subsection.

4.3.2 Effects of parameter mismatch

The quality of the synchronization between master and receiver can be characterized by the synchronization error and the cross-correlation. The average synchronization error is given by

$$\sigma = \sqrt{\frac{\langle \varepsilon_{\Delta p}^2 \rangle}{\langle \pounds_p^2(t) \rangle}}, \tag{4.17}$$

where $\varepsilon_{\Delta p}(t) = \pounds'_{p'}(t) - \pounds_p(t)$. This is an indicator of the minimum modulation amplitude below which the encoded message cannot be recovered. The sub-indexes p and p' in the master and slave time traces reflect the fact that the master and slave systems may operate with different parameter values. The cross-correlation

$$\Gamma_{\pounds\pounds'}(s) = \frac{\left\langle \left[\pounds_p(t) - \left\langle \pounds_p(t) \right\rangle\right]\left[\pounds'_{p'}(t+s) - \left\langle \pounds'_{p'}(t) \right\rangle\right] \right\rangle}{\sqrt{\left\langle \left|\pounds_p(t) - \langle \pounds_p(t) \rangle\right|^2 \right\rangle \left\langle \left|\pounds'_{p'}(t) - \langle \pounds'_{p'}(t) \rangle\right|^2 \right\rangle}}, \tag{4.18}$$

is a qualitative indicator of the topological distortion of slave trajectory. Notice that for $\pounds = \pounds'$, Eq. (4.18) defines the autocorrelation function. In the following, we analyze the influence of mismatch in each parameter individually, considering $\Delta T = 0$. For such detuning value, the correlation is maximum for $s = 0$.

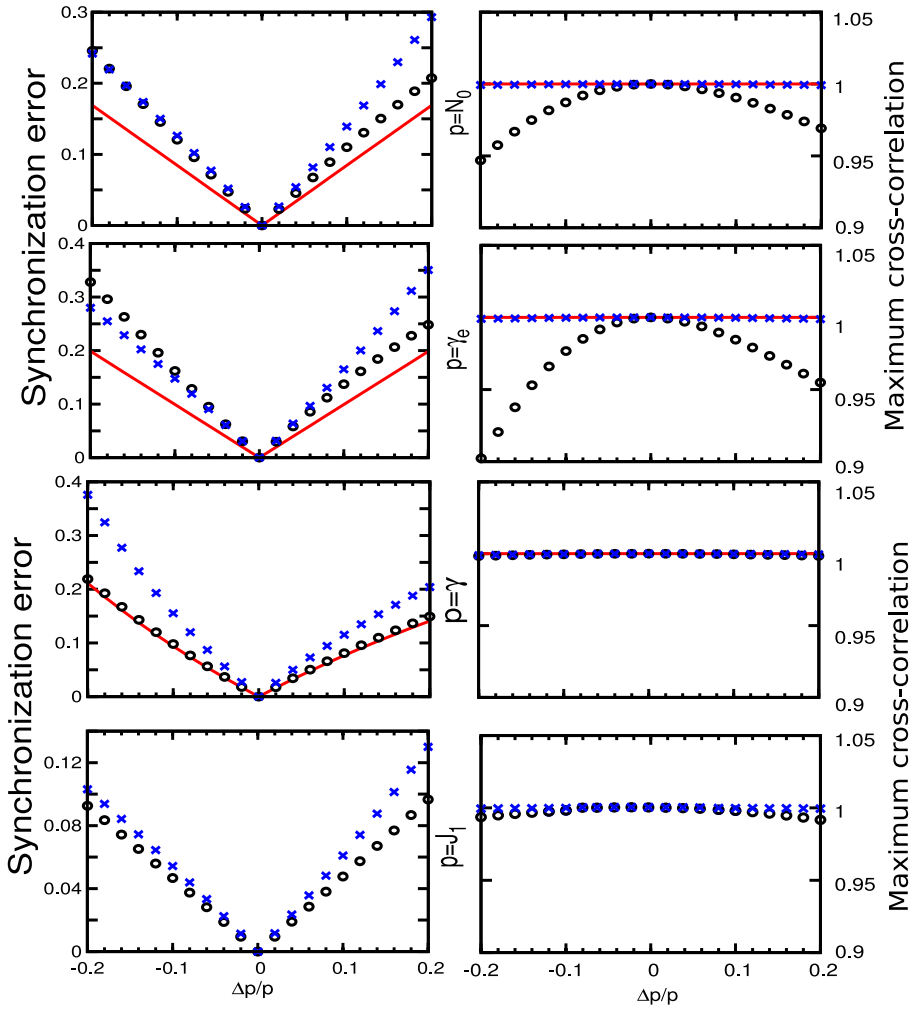


Figure 4.12: Average synchronization error, σ (left panels) and maximum cross-correlation, $\Gamma_{xy}(0)$ (right panels) given by Eqs. 4.17 and 4.18, respectively, as function of the laser parameter mismatch ($\Delta p = p' - p$) in $\mathcal{N}_0$, γ_e, γ and J_1 (from top to bottom). The solid line corresponds to $J_1 = 0$ (no feedback in the laser), ($\circ$) to system I with $J_1 = 0.08J_0$ and ($\times$) to system II also with $J_1 = 0.08J_0$.

Figure 4.12 shows the synchronization error (left panels) and the cross-correlation (right panels) for different mismatches in the laser parameters. For a mismatch in $\mathcal{N}_0$ and γ_e, the synchronization error grows basically linearly with the mismatch. The degradation of the synchronization with the mismatch is stronger for system I ($\circ$) and system II ($\times$) as compared with the system without laser feedback (solid line). For $\mathcal{N}_0$ and γ_e, negative mismatch has stronger effect than positive one for system I whereas the opposite happens for system II.

The mismatch in γ is the one that has stronger effects in system II while its

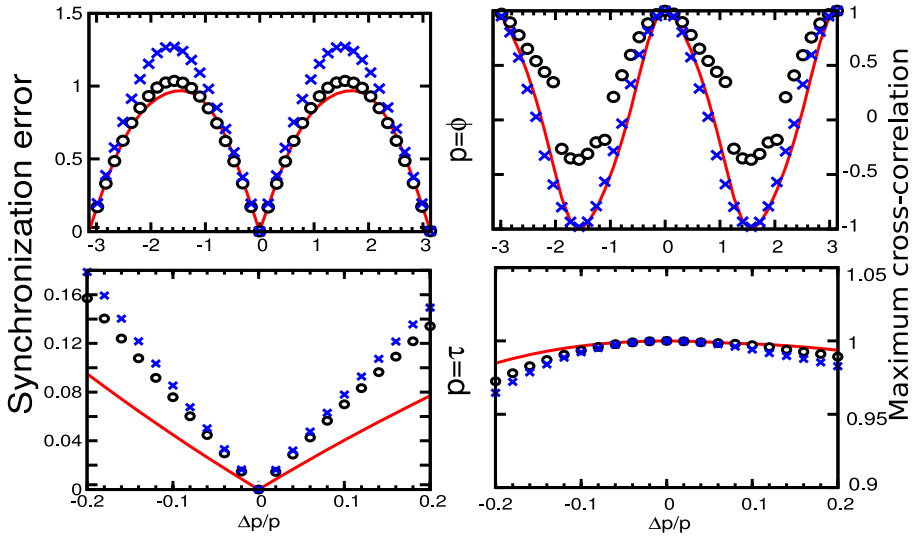


Figure 4.13: Average synchronization error, σ (left panels) and maximum cross-correlation, $\Gamma_{\mathcal{L}\mathcal{L}'}(0)$ (right panels) given by Eqs. 4.17 and 4.18, respectively, as function of the filter loop parameter mismatch in ϕ (top row) and τ (bottom row). The solid line corresponds to $J_1 = 0$ (no feedback in the laser), ($\circ$) to System I with $J_1 = 0.08J_0$ and ($\times$) to System II also with $J_1 = 0.08J_0$.

effects in system I are the same as in the original system without a feedback in the laser. Besides for system II, the effect of this mismatch is very asymmetric being more pronounced for negative ($\gamma' > \gamma$) than for positive mismatch. This asymmetry is already present when the laser operates in CW (solid line) and is magnified by the feedback in the laser. The mismatch in J_1 induces a synchronization error that grows symmetrically (asymmetrically) for system I (system II). For positive mismatch in system II, ($J_1' < J_1$) the degradation grows faster than for negative mismatch.

The results for the cross-correlation are quite different for systems I and II. For system I the cross-correlation function shows a parabolic shape for mismatches in $\mathcal{N}_0$ and γ_e while the cross-correlation for the other mismatches is always close to 1. System II shows for all the mismatches a cross-correlation which is practically 1. This means that the synchronization error obtained in Fig. 4.13 (left) comes from difference in the amplitude. In fact in the system without feedback, the effect of the mismatch in the overall gain G is to change the amplitude of the variable which affects more the synchronization than the cross-correlation.

As for the other parameters, the effect of mismatch in the slow cutoff time θ is typically negligible in this kind of systems [105], so we focus on the mismatch in the offset phase ϕ and the fast cutoff time τ. Results are plotted in Fig. 4.13. The synchronization quality is very sensitive to the offset phase mismatch. When the laser operates in CW (solid line) by changing the offset phase the system goes from

perfect synchronization (for zero or π mismatch) to perfect anti-synchronization (for $\pm\pi/2$ mismatch) in which $\pounds'(t) = \pounds(t)$ ($\sigma = 1$ and $\Gamma_{\pounds\pounds'} = -1$). For chaos communication the chaotic masking can be removed through the anti-synchronization by operating the MZM π-shifted offset phase, e.g. $\phi' = \phi + \pi$. When the feedback is added to the laser, perfect synchronization is still present for zero and π mismatch but the perfect anti-synchronization is degraded mainly for system II. As for the fast cutoff time τ mismatch, it plays the same role in system I and II. Nevertheless the effect of τ-mismatch is always less important than the other mismatches discussed before. The cross-correlation function shows a parabolic shape for system I while it looks constant for system II.

4.4 Encoded/Decoded Message

As mentioned before, in chaos-based optical communication systems, the amplitude of the message to be encrypted should be small compared to the amplitude of chaotic carrier to ensure the secrecy and to avoid large distortions of the transmitted signal which could prevent the receiver to synchronize with the emitter. When the message is encoded, the system performance can be affected in different ways (dynamics, synchronization and communication performance) depending on the encoding scheme [131]. Numerical simulations have shown that the additive chaos modulation (ACM) scheme can increase the complexity of the chaotic waveforms maintaining at the same time the synchronization quality before and after a message is encoded [132].

In the scheme as shown in Fig. 4.1 (c), we encode the message using the ACM technique as described in sec. 2.2. We assume the message to be encoded in the chaotic system as a sequence of a non-return-to-zero (NRZ) pseudorandom bit sequence of 1 Gb/s bit rate. The output of the laser diode containing message can be written as $p_1 m(t)$ where $m(t)$ is 1 when an optical power P_1 is transmitted and 0 when no optical power is transmitted. The mixing is performed through an all-optical 2×2 fiber coupler which is also used to send the output to the receiver. When the message is embedded within the chaos, Eq. (4.1) becomes

$$x + \tau\frac{dx}{dt} + \frac{1}{\theta}u \;=\; G_1 I(t-T)\cos^2\left[x(t-T)+\phi\right] + \alpha_m m(t-T), \qquad (4.19)$$

where $\alpha_m = \pi P_1/2V_\pi$ is the amplitude of the message. Here we use $\alpha_m = 0.3$ which is much smaller than the average gain $\langle G_1 I\rangle \approx 3.08$. Figures 4.14 (a) and (b) display the eye diagrams of the signal transmitted to the receiver for systems I and II, respectively. In both cases, it can be seen that the eye diagrams are completely close so that one cannot distinguish the chaotic fluctuations from the message. The

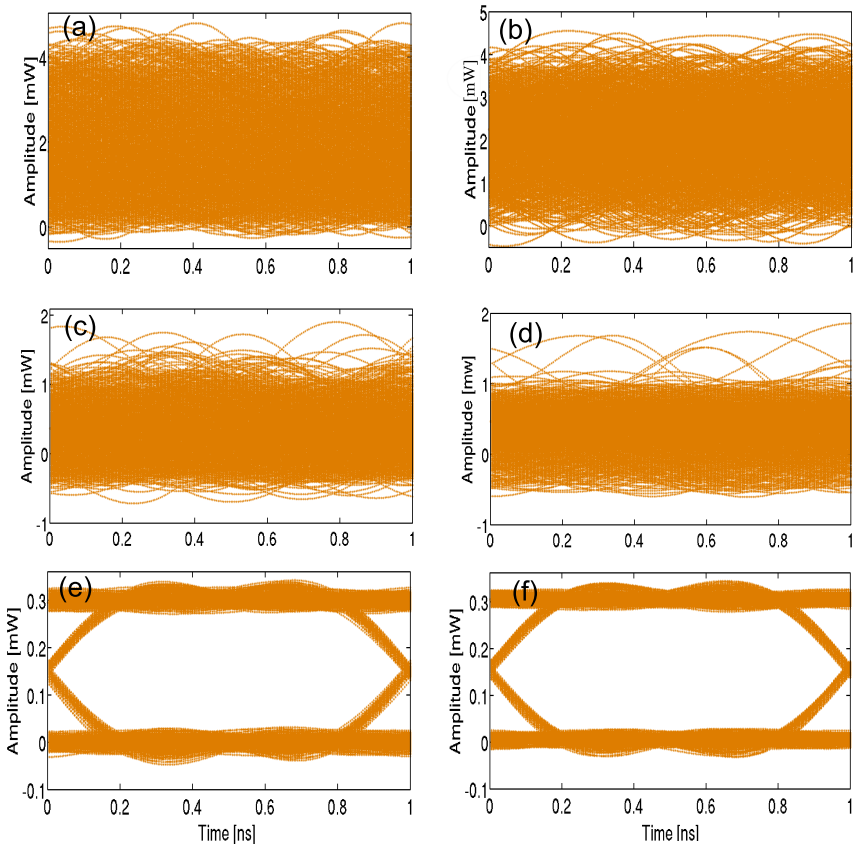


Figure 4.14: Eye diagrams for the transmitted signal (top row) and recovered message obtained considering on one hand -20% and 20% (center row) and on the other hand -1% and 0.1% (bottom row) mismatch in τ and γ respectively, when the message is encoded through either system I (a, c, e) or system II (b, d, f). Other parameters considered are $J_0 = 1.5J_{th}$, $J_1 = 0.08J_0$ and $\phi = 0.3$.

hidden message can only be discriminated from the chaotic fluctuations when using an authorized receiver and its quality depends on how capable the receiver is to remove the chaos.

The recovery process at the receiver is as follows: At the input of the receiver, the transmitted signal is split into two parts, one part is used to drive the slave system which ideally should have parameters identical to the emitter, while the other part is directly detected by the photodiode PD_+. Taking into account the message, the slave system dynamics is ruled by

$$y + \tau\frac{dy}{dt} + \frac{1}{\theta}u' \;=\; G_1' I(t-T)\cos^2\left[x(t-T)+\phi\right] + \alpha_m m(t-T). \qquad (4.20)$$

The output of the slave system is detected using balanced photodiode PD_- and the message is finally retrieved in the RF power combiner which typically subtracts

PD_- from PD_+ signals after carefully matching all the parameters. In fact, the signal at the RF power combiner [see Fig. 4.1 c)] can be written as

$$\pounds_m(t) \;=\; S'\left\{G_1 I\cos^2\left[x(t)+\phi\right]+\alpha_m m(t)\right\}-SG_1' I'\cos^2\left[y(t)+\phi'\right], \quad (4.21)$$

where S and S' are factors accounting for the PD_- and PD_+ sensitivities and fiber couplers, respectively. If the receiver and emitter synchronize perfectly, $x(t)=y(t)$, $I'(t)=I(t)$, and taking $G_1'=G_1$, $S'=S$, $\phi'=\phi$, we have from Eq. (4.21)

$$\pounds_m(t)=S\alpha_m m(t) \quad (4.22)$$

which is the recovery message in perfect conditions. However, it is worth to note that this perfect recovery of the message is difficult in real situations because of noise and various mismatches. For an unauthorized receiver, the mismatch is large and consequently it fails to correctly discriminate the chaos from the message. For $S=1$ and $\alpha_m=0.3$, Fig. 4.14 (c) [(d)] show the eye diagram for system I [system II] obtained considering -20% and 20% mismatch in τ and γ respectively. In both cases, the eye diagrams are completely close meaning that even with just 20% of mismatch in two parameters, the message cannot be retrieved. When the same mismatches are decreased to -1% and 1% respectively, the eye diagrams both from system I and system II are completely open as shown in Fig. 4.14 (e) and (f). Thus, an authorized receiver can successfully recover the message while an unauthorized one fails to retrieve it.

4.5 Conclusions and Final Remarks

In this chapter, we have studied two electro-optical delay feedback systems pumped by a semiconductor laser subject to feedback. In particular we have introduced two new different schemes in which it can be implemented. The additional feedback in the laser makes the semiconductor laser to operate in a chaotic regime instead of CW. As a consequence the overall system becomes more chaotic as shown by the increase of statistical entropy. Furthermore the additional feedback induces chaos for parameter values in which the system was not chaotic. These effects are already clearly observed when the amplitude of the feedback in the semiconductor lasers is only 16% of the DC pump current. Therefore this is a useful mechanism to generate broader bandwidth chaos.

Despite the systems are more chaotic, high-quality synchronization is still possible when the mismatch in parameters is small allowing for message decoding. The additional parameters to be turned, in order to achieve synchronization, increase the difficulties of an eventual eavesdropper to decode the message without the adequate receiver system.

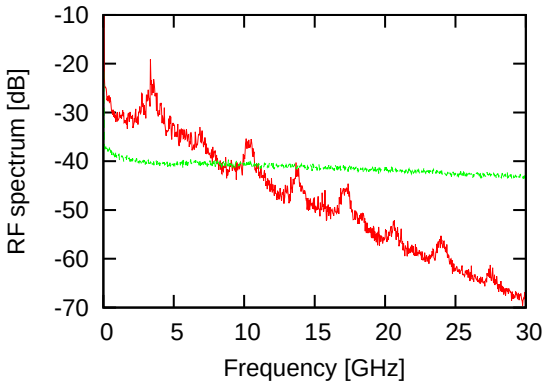


Figure 4.15: RF spectrum of $\pounds(t)$ for system I (red line) and for system II (green line) considering $J_0 = 1.5J_{th}$, $J_1 = 0.08J_0$ and $\phi = 0.3$.

One of the main advantages of the models studied in this chapter concerns the data interception. In fact, the reconstruction of the underlying dynamics strongly depends on the observable (variable) which is analyzed [118] as discussed in chapter 3. In our case, the direct detection of the transmitted signal leads to

$$\pounds(t) \sim \left|E(t)\left\{1 + e^{2i[x(t)+\phi]}\right\}\right|^2 = I(t)\cos^2[x(t)+\phi], \tag{4.23}$$

which is more difficult to analyze than $x(t)$ or $I(t)$. Even using an optical 90^o hybrid coupler, the reconstruction of $x(t)$ is now indeed difficult since the intensity $I(t)$ is also time-dependent. An eventual eavesdropper therefore has to attempt the identification of the parameters from $\pounds(t)$. Figure 4.15 shows the RF spectrum of $\pounds(t)$ for system I and II. As it can be seen, it does not reveal the cutoff frequency of the filter as it is the case for RF spectrum of $x(t)$ [see Fig. 3.12 (b)]. Notice that the RF spectrum of $\pounds(t)$ for system II is particularly flat.

Chapter 5

Electro-optic Phase Chaos Systems With Digital Key Performing Time Delay Concealment

In chaos encryption there is no rigorous counterpart to the digital key of algorithmic cryptography. Confidentiality relies essentially on the hardware parameters that should be kept secret. As discussed in chapter 3, the delay time in itself can be identified from the transmitted signal using several methods. Still worse, under the assumption of noise-free or even of small amplitude noise, the underlying chaotic dynamics of some systems can be reconstructed once the delay time is identified, using appropriate techniques such as artificial neural networks [106]. Furthermore, hardware cryptosystems also suffer from a relatively low parameter space dimension (a sort of equivalent to the digital key size in algorithmic encryption). This problem arises from the fact that apart from the delay time, other parameters have quite limited range of values for which strong chaos is obtained. This exposes the system to brute-force attacks. Given current computer speed, it is generally agreed that a key space of size less than 2^{100} is not sufficiently secure [54]. This goal seems difficult in practice when dealing only with hardware cryptosystems. The situation becomes critical with the identification of the delay time.

To circumvent these drawbacks, we propose in this chapter to implement a currently suggested principle in algorithmic cryptography, which consists in mixing different algebra when constructing the encryption algorithm [133]. We combine a pseudo-random binary sequence (PRBS) used in symmetric-key encryption, with a high-dimensional chaotic time series generated by an analog physical system, to make a symmetric-key encryption system with enhanced cryptographic security by reciprocal concealment [134]. At this point we notice that while public-key encryption schemes have won popularity, they have drawbacks such as limited speed and non-absolute security. Thus symmetric-key algorithms are still actively pursued,

including new stream cyphers[1] and cryptographic hash functions[2]. Besides, hybrid algorithms such as PGP (Pretty Good Privacy) combine public key encryption to define a private key used for fast symmetric encryption [8].

In general chaotic communications mix the digital message and the chaotic carrier, however this mixing is quite weak and the statistical properties of the message cannot be controlled beforehand, thus the masking of the chaotic carrier statistical properties is quite limited. Through the introduction of an amplitude-balanced entropy mixing between a PRBS and a chaotic generation process, we perform an efficient entropy amplification for the resulting carrier even in absence of any message. As a consequence, this approach proposes a solution both for the problem of the introduction of an efficient digital key in chaos communications, as well as for the problem of delay time concealment. There have been indeed recently a few attempts to address separately these issues. In semiconductor lasers with optical feedback, the optical feedback phase plays an important role in the synchronization [135] thus a digital key implemented by modulating that phase was suggested [136]. In the same context, it has been also suggested [116] that delay time can be masked if chosen to be close to the laser relaxation time, however the phase still carries information revealing the delay time signature (see Sec. 3.2, [134]). Systems with delay time modulation [137, 138, 139] proposed as alternatives to get around the delay time extraction, are however very difficult to implement practically.

The configuration studied here is based on a double electro-optic delayed feedback dynamics. The scheme allows on one hand to integrate a digital key required for successful decryption which can be implemented as a long PRBS generated by an appropriate algorithm or as a relatively short sequence generated from a natural random process used repetitively. On the other hand, the involved digital random sequence performs a concealment of the delay time, under conditions described later, so that the delay time cannot be anymore identified from the time series using known methods. The digital key is in principle intended to generate a long PRBS, as it is classically used in some algorithmic encryption scheme. Besides the scheme, our proposal is based physically on high speed phase chaos [76] which has been recently successfully tested in a chaos communication field experiment up to 10 Gb/s [75].

The chapter is outlined as follows. In Sec. 5.1 we introduce the system and in Sec. 5.2 we characterize its dynamics. In Sec. 5.3 we show the effect of the digital key in the identification of the delay time from a time series. In Sec. 5.4 we discuss the sensitivity of the synchronization on the digital key. Finally in Sec. 5.5 we give some concluding remarks.

[1]European project eSTREAM (http://www.ecrypt.eu.org/stream).
[2]NIST call for the future SHA-3 (http://csrc.nist.gov/groups/ST/hash/sha-3/)

5.1 The System

The system under study is based on the phase chaos communication scheme presented in [76], however with structural architecture modifications, in order to ensure the efficient achievement of our initial goal: security enhancement of chaos communication through the use of digital key. It is illustrated in Fig. 5.1. Both emitter and receiver consist of two similar nonlinear delayed differential processing chains, serially connected. The sub-indexes $k = 1, 2$ refer to elements of the same chain. In each chain, one has an electro-optic phase modulator (PM) having a half-wave voltage V_π, and seeded by a continuous-wave (CW) telecom semiconductor laser (SL), which is phase modulated by an external signal (whether the PRBS R, or the message m to be securely transmitted). The electrical input of the PM of a chain is driven by the electrical output of the other chain. The PM optical output of one chain thus consists of two superimposed phase modulations, the PRBS or the message, and the nonlinear delayed differential processing performed by the other chain. The phase modulated light beam is then processed according to the delayed nonlinear dynamics of its chain. The delay time T_k is performed by a length of fiber. The nonlinear transformation is performed non locally in time, between the input phase and the output intensity of an imbalanced interferometer (e.g. a passive Mach-Zehnder interferometer MZI), which imbalancing delay times δT_k is required to be longer than the typical time scale of the phase modulation as earlier described in 2.3. The intensity fluctuations resulting from this nonlinear conversion of the phase modulation, are then detected by an amplified broadband telecom photodiode. The output electrical signal is further amplified by an RF driver, which gives the output of the processing chain serving as the electrical input for the other chain. The transmitted phase modulated light beam is the output of PM_2, which contains the linearly superimposed phase modulation of the message in standard DPSK (differential phase shift keying) format. It is worth noting that the message m is linearly added within the chaotic phase of the optical light beam to be transmitted while the PRBS R is similarly added in the chaotic phase of another light beam. The PRBS generator can be, for example, a linear feedback shift-register (LFSR) with primitive feedback polynomial, which can be efficiently implemented in hardware [140]. In this case, the common secret between the emitter's PRBS and the receiver one is the initial state of the LFSR. However, it should be adjusted taking into account the shift in time between the emitter and the receiver.

The dynamical modeling of the encoding can be described as follows. The electronic bandwidth of the feedback loop is assumed to result from two cascaded linear first-order low-pass and high-pass filters. Considering the filter output voltages $V_1(t)$ and $V_2(t)$ in chains 1 and 2 respectively and performing a derivation

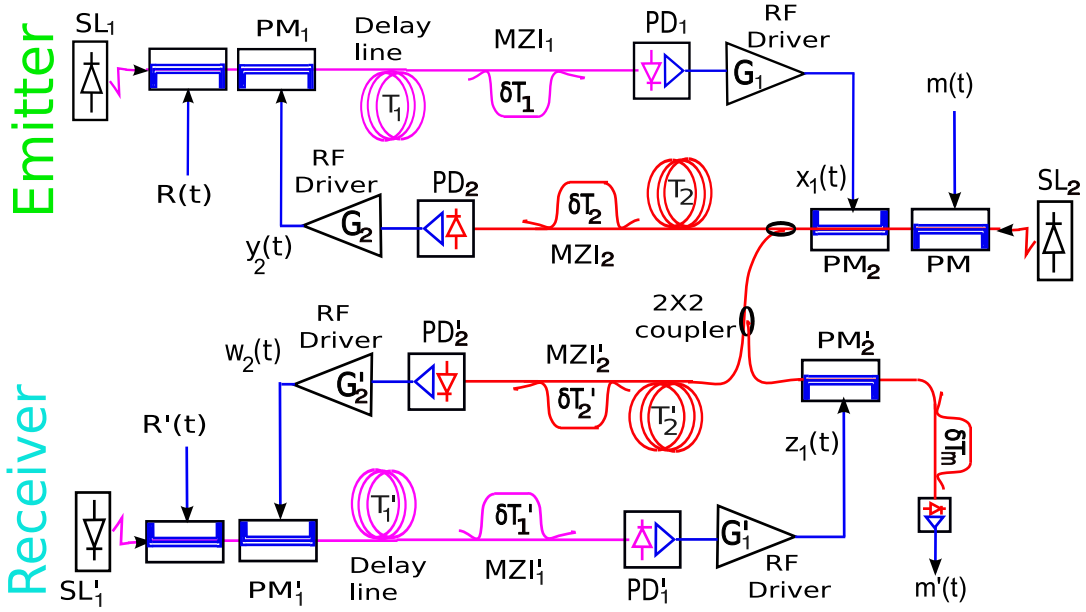


Figure 5.1: Transmitter and receiver setup: SL: semiconductor laser, PM: phase modulator, MZI: imbalanced Mach-Zehnder interferometer, PD: photodiode, $x_1(t)$ and $y_1(t)$ are dimensionless output voltage of RF driver for external and internal loop while $R(t)$ and $m(t)$ are pseudo-random bit sequence and message, respectively. Sub-indexes 1 and 2 refer to the internal and to the transmitted light beam parameters, respectively.

similar to the one given in Sec. 2.3, it turns out that the emitter dynamics can be described by the dimensionless output filter variables $x_1(t) = \pi V_1(t)/(2V_{\pi,1})$ and $y_2(t) = \pi V_2(t)/(2V_{\pi,2})$:

$$x_1 + \tau_1 \frac{dx_1}{dt} + \frac{1}{\theta_1} u_1 = G_1 \cos^2\left[\Delta(y_2)_{T_1} + \Delta(R)_{T_1} + \phi_1\right], \tag{5.1}$$

$$y_2 + \tau_2 \frac{dy_2}{dt} + \frac{1}{\theta_2} u_2 = G_2 \cos^2\left[\Delta(x_1)_{T_2} + \Delta(m)_{T_2} + \phi_2\right], \tag{5.2}$$

$$\frac{du_1}{dt} = x_1, \tag{5.3}$$

$$\frac{du_2}{dt} = y_2, \tag{5.4}$$

where $\Delta(F)_{t_0} = F(t-t_0) - F(t-t_0-\delta t_0)$. The parameters are the feedback strengths G_1, G_2, the delay times T_1, T_2, the fast (slow) filter characteristic response times τ_1, τ_2 (θ_1, θ_2), the MZI imbalanced delays δT_1 and δT_2, and the MZI static phases ϕ_1 and ϕ_2.

At the receiver side, the decoding is performed as follows. The input phase modulated light beam is split into two paths. The long path replicates the two serial processing chains used for the encoding at the emitter, in which of course a

synchronized PRBS is involved, thanks to the knowledge of the digital secret key. The analog secret key consists in the hardware parameters determining the devices of the two serial processing chains, and their exact operating conditions. The output of the two processing chains, after being inverted, serves as the electrical input of PM'_2, which is intended to cancel the pseudo-random phase modulation superimposed to the message. The dynamics at the receiver is given by:

$$z_1 + \tau'_1 \frac{dz_1}{dt} + \frac{1}{G'_1} v_1 = G'_1 \cos^2\left[\Delta(w_2 + R')_{T'_1} + \phi'_1\right], \tag{5.5}$$

$$w_2 + \tau'_2 \frac{dw_2}{dt} + \frac{1}{\theta'_2} v_2 = G'_2 \cos^2\left[\Delta(x_1 + m)_{T'_2} + \phi'_2\right], \tag{5.6}$$

$$\frac{dv_1}{dt} = z_1, \tag{5.7}$$

$$\frac{dv_2}{dt} = w_2, \tag{5.8}$$

where primes refer to the receiver parameters. The output of PM'_2 is then expected to be the phase modulation issued by the message only. It can be demodulated using a standard DPSK demodulator, consisting in an MZI with an imbalanced delay time δT_m and a photodetector as discussed in Sec. 5.4.

5.2 Characterization of the Dynamics

To show the effect of including a digital key, we first characterize the chaotic dynamics generated by the transmitter when no message is encoded. Convenient bifurcation parameters for the system are the feedback strengths G_1 and G_2. Since the message is embedded within the transmitted light beam described by dynamical variable $x_1(t)$, we can henceforth focus on this variable to analyze different behaviors of the system. We measure the complexity by means of the statistical entropy in (G_1, G_2)-plane considering two cases: without digital key and with digital key in order to point out the PRBS role in the statistical properties of the carrier $x_1(t)$. Numerical simulations are performed considering the key physical parameters arbitrary chosen, within the range of experimentally accessible values [76], as follows: $T_1 = 15$ ns and $T_2 = 17$ ns, $\tau_1 = 20$ ps, $\tau_2 = 12.2$ ps, $\theta_1 = 1.6$ μs, $\theta_2 = 1.6$ μs, $\delta T_1 = 510$ ps, $\delta T_2 = 400$ ps, $\phi_1 = \pi/8$, $\phi_2 = \pi/4$. Other parameters are stated in the figure captions when necessary. Figure 5.2 shows the entropy of $x_1(t)$ in (G_1, G_2)-plane without PRBS (a) and with a PRBS key of amplitude $\pi/2$ at 3 Gb/s (b). It turns out that without PRBS ($R = 0$), the entropy of the system is smaller than 6 for $G_1 G_2 < \sqrt{2}$. It grows as G_1 and/or G_2 increases and for $G_1 = G_2 = 5$,

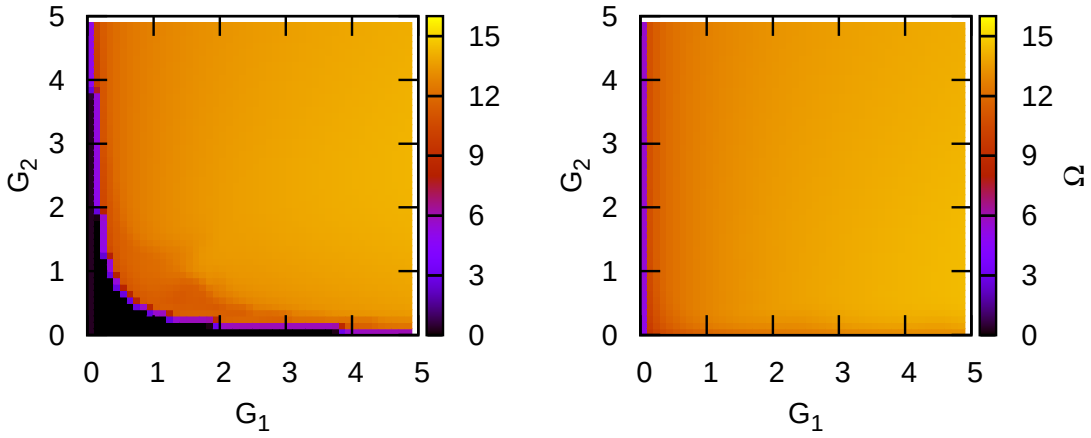


Figure 5.2: Statistical entropy Ω of $x_1(t)$ in (G_1, G_2) plane without PRBS (left panel) and with a PRBS key of amplitude $\pi/2$ at 3 Gb/s. The entropy was calculated using a data series with 4×10^7 points recorded after the transient time and sampled into 4×10^6 histogram bins.

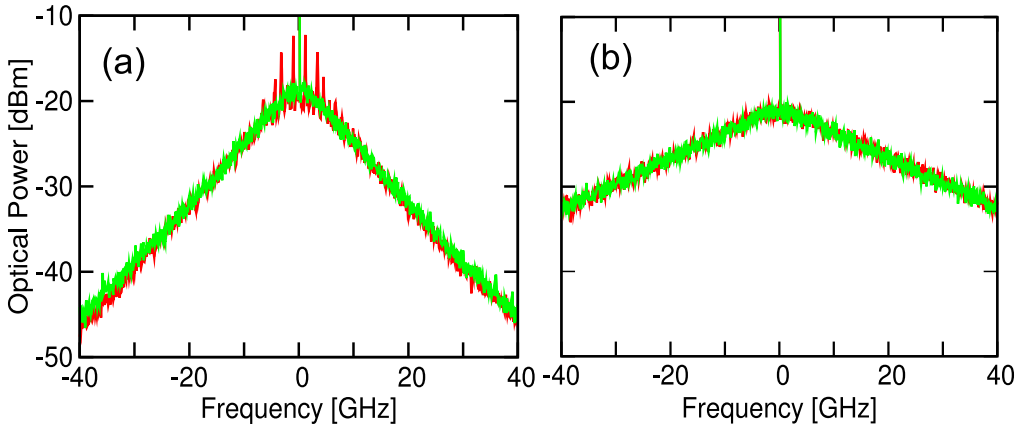


Figure 5.3: Optical power spectrum at the output of PM without the message and when no PRBS is involved (red line) or considering a PRBS key of amplitude $\pi/2$ at 3 Gb/s (green line). a) $G_1 = G_2 = 2$ and b) $G_1 = G_2 = 4$.

it reaches a value around 14.4, which corresponds to a completely chaotic system. Notice that a completely random process would lead to a maximum entropy given by the natural logarithm of the number of bins, which in our case is ≈ 15.2. Comparing the entropy without and with PRBS, it is clear that the PRBS increases significantly the entropy for small feedback strengths. For large feedback strength the effect is smaller. These results can be also evidenced by plotting the optical spectrum as shown in Fig. 5.3. For $G_1 = G_2 = 2$ (a), the spectrum shows peaks

around the central frequency when no PRBS is integrated (red line). These peaks emerge at the frequency corresponding to the inverse of δT_1, which is smallest delay time involved in the chaotic transmitted phase generation $x_1(t)$ [see Eq. (5.1)]. The peaks disappear when PRBS is added (green line). For $G_1 = G_2 = 4$, both spectra obtained with and without PRBS are similar evidencing therefore the smaller effect of the digital key for this case.

5.3 Effect of the PRBS on Delay Time Identification

This section is intended to investigate in which conditions the delay time can be concealed. Before investigating delay time concealment, let us clarify what are the relevant times for successful decoding, that is, whether synchronization depends on the individual delays T_1 and T_2 , or only on the total delay $T = T1 + T2$. Assuming $R' = R$ and identical parameters for emitter and receiver except for the delay times T_1 and T_2, by Fourier transforming Eqs. (5.2), (5.4), (5.6), and (5.8) and subsequently dividing Eqs. (5.2) by (5.6), one obtains

$$\frac{Y_2(\omega)}{W_2(\omega)} = e^{-i\omega(T_2 - T_2')}, \tag{5.9}$$

where $F(\omega)$ stands for the Fourier transform of $f(t)$. The relationship between $Y_2(\omega)$ and $W_2(\omega)$ given by Eq. (5.9) indicates that

$$w_2(t) = y_2(t + (T_2 - T_2')). \tag{5.10}$$

Thus, by replacing Eq. (5.10) into the right hand side of Eq. (5.5) and subsequently Fourier transforming Eqs. (5.1), (5.3), (5.5), and (5.7), it turns out that

$$\frac{X_1(\omega)}{Z_1(\omega)} = e^{-i\omega(T_1 + T_2 - T_1' - T_2')}, \tag{5.11}$$

As the total delay time is $T = T_1 + T_2$ for the emitter and $T' = T_1' + T_2'$ for the receiver, it turns out that

$$X_1(\omega) = Z_1(\omega) \tag{5.12}$$

for $T = T'$ even when the individual delay times are different. Therefore, for identical parameters between the emitter and the receiver and for $R' = R$, $x_1(t)$ will synchronize with $z_1(t)$ provided $T = T'$. We have also numerically checked that the synchronization still takes place at the receiver as long as the overall delay time T is the same for emitter and receiver, even if individual delays T_1 and T_2 are different.

Since real systems are always noisy, another interesting point would be to investigate the robustness of the quantifiers to noise. Appropriate ones for unmasking

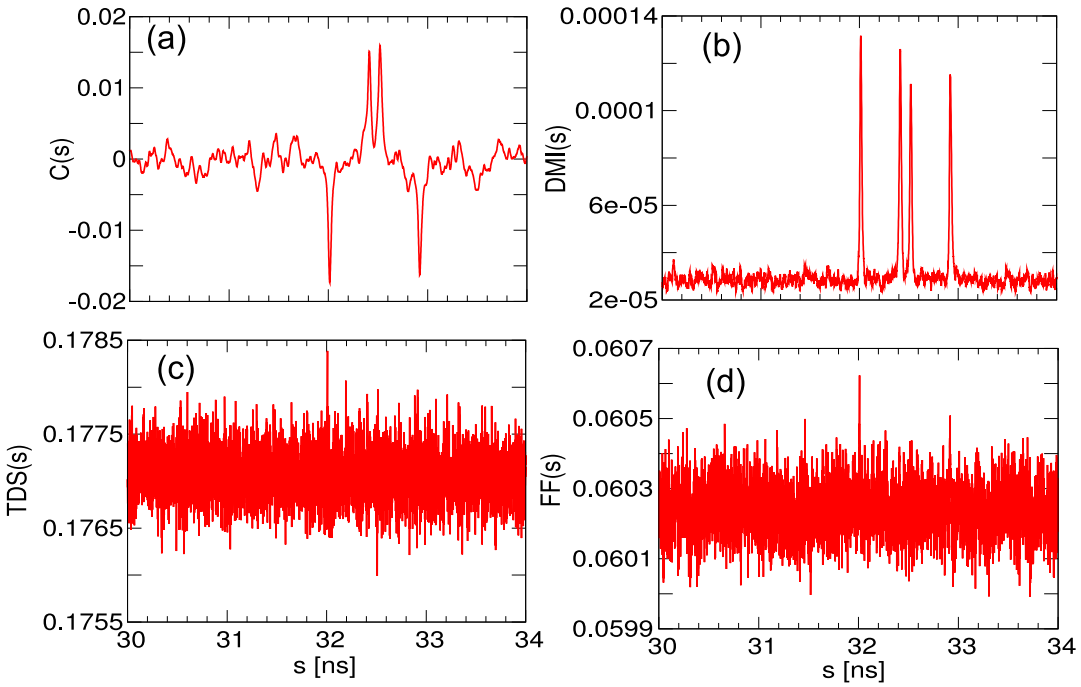


Figure 5.4: (a) AC, (b) DMI, (c) TDE and (d) FF functions as a function of an embedding delay s computed from 10^7 data points corresponding to a 10 μs time series after adding a Gaussian white noise of amplitude 3.5% of the carrier amplitude. The time series were generated from a system without PRBS ($R(t) = 0$). All the results are normalized to 1.

the delay time signatures are those robust to noise. To figure out this issue, let us first consider a noisy series by adding to the carrier generated without PRBS a Gaussian white noise of amplitude 3.5% of the carrier amplitude. Figure 5.4 shows the delay time identification computed using the methods described in chapter 3. As it can be seen, despite the presence of noise in the time series, clear peaks are found at $T = T_1 + T_2$, $T + \delta T_1$, $T + \delta T_2$ and $T + \delta T_1 + \delta T_2$ both in the autocorrelation (a) and in the delayed mutual information (b), evidencing therefore that even with noise, the delay times can still properly be identified. On the contrary, no clear peaks are distinguishable at the different delay times when computing the time distribution statistics (c) or the filling factor (d) from the same noisy series. Thus taking into account the fact that experimental time series are always noisy, we henceforth focus only upon AC and DMI methods since TDE and FF methods are so sensitive to noise that even just a small noise added to the carrier prevent them to work properly. Once the quantifiers are chosen, we can henceforth consider again a free-noise time series in our analysis since it is the ideal case for an eavesdropper to attempt the delay time identification.

As in the previous section, we consider that no message is transmitted ($m(t) =$

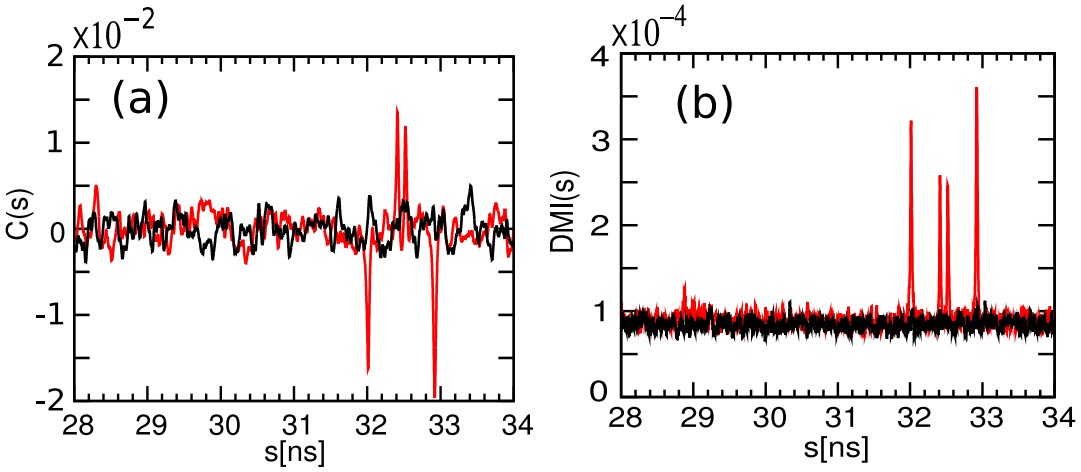


Figure 5.5: Autocorrelation function $C(s)$ (a) and delayed mutual information DMI(s) (b) of $x_1(t)$ without PRBS (red line), and with a PRBS of amplitude of $\pi/2$ at 3 Gb/s (black line). A time series of length 10 μs with 10^7 data points was used.

0) to show the role of the PRBS in the delay time identification. The graphs in Fig. 5.5 display the autocorrelation (a) and the DMI (b) computed from the transmitted phase proportional to $x_1(t)$, when no PRBS is used (red line) and with a PRBS at 3 b/s with an amplitude of $\pi/2$ (black line). In the first case both functions show peaks at $T = T_1 + T_2$, $T + \delta T_1$, $T + \delta T_2$ and $T + \delta T_1 + \delta T_2$, so that all relevant delay times can be readily identified. The delay time signature vanishes completely when the PRBS is included.

Figs. 5.6 (a) and (b) show the size of peaks found in $C(s)$ and in the DMI at the relevant delay times as a function of the PRBS bit rate considering an amplitude of $\pi/2$. The peaks are clearly distinguishable for zero bit rate (no PRBS). When increasing the bit rate, the peak size decreases and approaches the background value of these functions (green line). The background mean and standard deviation are calculated in Fig. 5.6 using the highest 2000 spurious local maxima (e.g. excluding the peaks corresponding to real delay times). For low bit rates $R(t)$ and $R(t - \delta T_1)$ take the same value most of the time, so $\Delta(R)$ vanishes most of the time and therefore its effect is small (see the concept of temporal non locality as introduced in [76] and as discussed in Sec. 2.3). Therefore the peaks both in the DMI and in $C(s)$ can still be distinguished from the background standard deviation, shown with bars in the figure. When the bit rate reaches a value corresponding to the inverse of δT_1 (~ 1.97 Gb/s), $\Delta(R)_{T_1}$ is typically non zero, and the PRBS plays a key role in the dynamics, concealing the delay time peaks.

The size of the peaks as function of the PRBS modulation amplitude is shown in Figs. 5.6 (c) and (d). An important remark is that the PRBS modulation am-

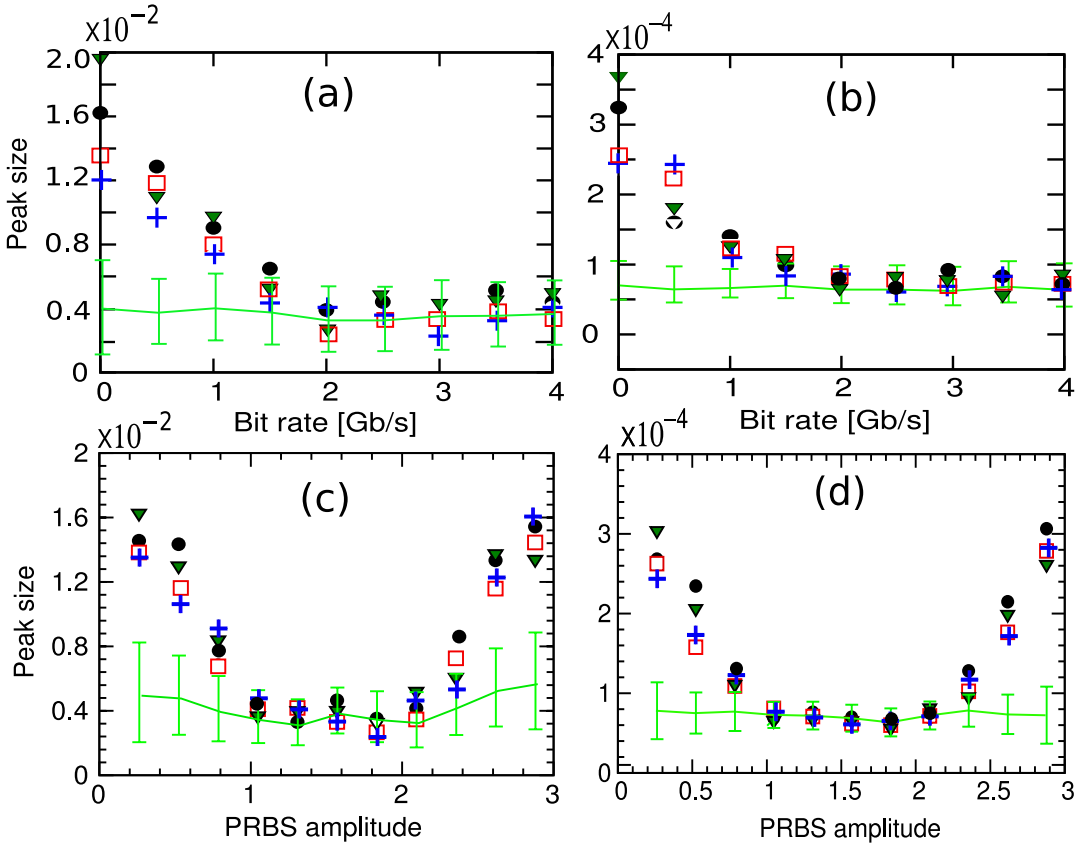


Figure 5.6: Absolute value of the peaks in $C(s)$ (a,c), and DMI (b,d), at T (•), $T+\delta T_2$ (□), $T+\delta T_1$ (+) and $T+\delta T_1+\delta T_2$ (▼) vs. the PRBS bit rate (upper row) and PRBS amplitude (bottom row). In (a) and (b) the PRBS amplitude is $\pi/2$ while in (c) and (d) the PRBS bit rate is 3Gb/s. Solid line and bars correspond to the background mean value and standard deviation. A series of length 267 times T was used.

plitude is a π-periodic function associated to the periodicity of $\cos^2$ in Eq. (5.1). Thus, a PRBS of amplitude π has no effect since $\Delta(R)_{T_1}$ only takes values 0 or π and both are equivalent in the $\cos^2$ term. Efficient concealment occurs for amplitudes between $\pi/3$ and $2\pi/3$ approximately. We have found that this range increases when increasing G_1 and/or G_2.

Remarkably enough, while the PRBS conceals the delay time in the chaotic carrier $x_1(t)$, the cross-correlation between $x_1(t)$ and $R(t)$ is of the order of 10^{-3}, meaning that the digital key itself is also concealed in the chaotic carrier. This is explained by the fact that the interplay between balanced amplitudes of the chaos and a PRBS is optimizing the mutual nonlinear mixing, resulting in an efficient mutual masking of each signal by the other.

On the other hand, it should be noticed that for $\delta T_1 = \delta T_2$, the interplay

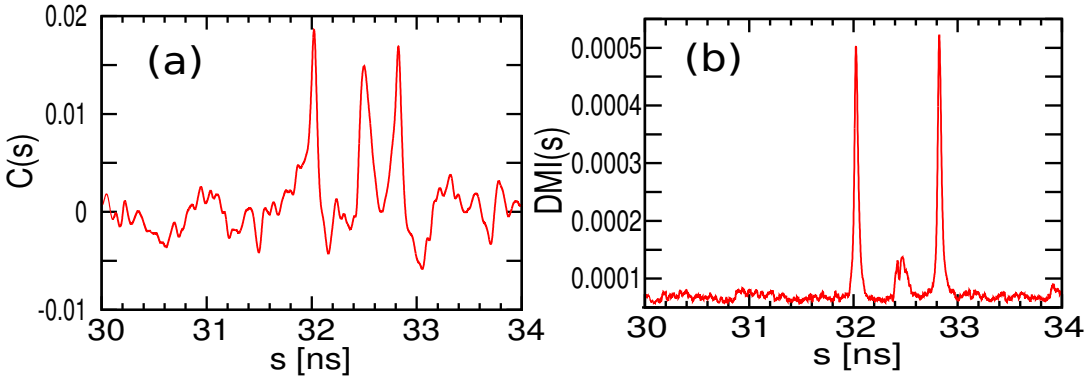


Figure 5.7: Autocorrelation function $C(s)$ (a) and delayed mutual information DMI(s) (b) of $x_1(t)$ considering $\Delta T_1 = \Delta T_2 = 400$ ps. A time series of length 10 μs with 10^7 data points was used. All the results are normalized to 1.

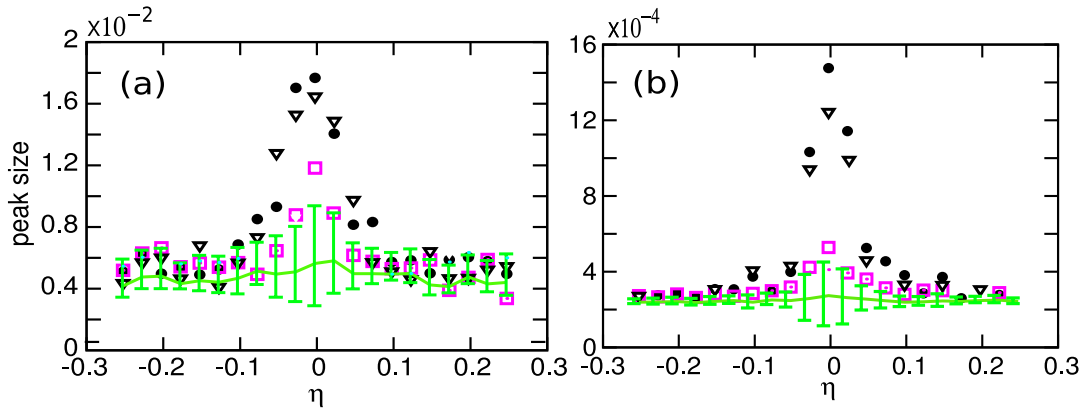


Figure 5.8: Absolute value of the peaks in $C(s)$ (a), and DMI (b), at T (•), $T + 2\delta T_1 + \tau_1 + \tau_2$ (□), $T + 2\delta T_1$ (▽) as a function of mismatch $\eta = (\delta T_2 - \delta T_1)/\delta T_1$ considering $\delta T_1 = 400$ ps. Solid line and bars correspond to the background mean value and standard deviation. A series of length 267 times T was used.

between δT_1 and δT_2 leads to a resonance and consequently, pronounced peaks are observed at T, $T + \delta T_1$, $T + 2\delta T_1$. Figures 5.7 (a) and (b) illustrate this issue. For the autocorrelation the middle peak is indeed located at $T + \delta T_1$. For the DMI the middle peak is composed of two peaks one at $T+\delta T_1$ and the other at $T+\delta T_1+\tau_1+\tau_2$. This splitting may explain the small size of the intermediate peak in the DMI.

While typically the delay time signature is reduced when increasing the overall loop gain, we have found that when $\delta T_1 = \delta T_2$ the delay time can always be identified even for $G_1 = G_2 = 15$, way beyond experimental limits. Therefore for efficient delay time concealment, one needs to take $\delta T_1 \neq \delta T_2$.

The dependence of the concealment on the mismatch between the two shorter

delay times $\eta = (\delta T_2 - \delta T_1)/\delta T_1$ is investigated in Fig. 5.8. It turns out that as such mismatch increases, the peak sizes both in C(s) and DMI(s) decrease so that it becomes very difficult to identify the delay time for a mismatch greater than about 20%. In particular, we note that the delay time signature is lost in the autocorrelation already at a 10% mismatch while the DMI allows the identification of the delay time up to 20% mismatch.

5.4 Synchronization and Sensitivity to Digital-Key Mismatch

In order to decode the message, the receiver electro-optic phase modulator PM_2 applies an additional phase modulation onto the received light beam, proportionally to the signal $z_1(t)$. This leads to a total optical phase modulation proportional to (x_1+z_1) at the PM_2' output. The resulting light beam can then be processed through a standard DPSK demodulator matched with the message bit rate (imbalanced MZI with δT_m in Fig.5.1). The photodiode detects

$$P_m(t) \propto \cos^2\left[\bar{\Delta}(x_1 + m + z_1)_{\Delta T_m}\right]. \tag{5.13}$$

where $\bar{\Delta}(F)_{\delta T_m} = F(t) - F(t - \delta T_m)$. The decoded message $m'(t)$ is obtained from $P_m(t)$. For perfect anti-synchronization, $z_1(t)$ is equal to $-x_1(t)$, and $m'(t)$ reproduces $m(t)$. For a receiver system with identical parameters but with a π-shift in the receiver MZM (that is $\phi_1' = \phi_1 \pm \pi/2$), $z_1(t) = -x_1(t)$, the anti-synchronization between $z_1(t)$ and $x_1(t)$, is obtained if $R' = R$. While hardware mismatch is unavoidable in practice, several field experiments of chaos communications [74, 75] have demonstrated that the resulting synchronization error is still acceptable. Moreover, the electro-optic phase dynamics we consider as our experimental basis, has led to the best experimental chaos synchronization quality reported so far over more than 10 GHz bandwidth. The correct decoding however depends strongly on the simultaneous matching of all the parameters in the emitter and receiver, in the same way as it was already investigated in the literature [105]. The sensitivity of the decoding with respect to the physical parameter mismatch is thus not revisited here. In order to check that the precise knowledge of the pseudo-random digital sequence indeed brings significant additional security we consider in the following that the receiver parameters are identical to the transmitter. The differences $\delta_1(t) = z_1(t) - x_1(t)$

and $\delta_2(t) = w_2(t) - y_2(t)$ follow

$$\delta_1 + \tau_1 \frac{d\delta_1}{dt} + \frac{1}{\theta_1}\varepsilon_1 = -G_1 \sin\left[\Delta(\delta_2)_{T_1} + \Delta(R' - R)_{T_1}\right] \times \sin\left[2\Delta(y_2)_{T_1} + \Delta(\delta_2)_{T_1} + \Delta(R + R')_{T_1} + 2\phi_1\right], \tag{5.14}$$

$$\delta_2 + \tau_2 \frac{d\delta_2}{dt} + \frac{1}{\theta_2}\varepsilon_2 = 0, \tag{5.15}$$

$$\frac{d\varepsilon_1}{dt} = \delta_1, \tag{5.16}$$

$$\frac{d\varepsilon_2}{dt} = \delta_2. \tag{5.17}$$

From Eq. (5.15), we find two roots of the characteristic polynomial corresponding to the homogeneous solutions as

$$r_\pm = \frac{-1 \pm \sqrt{1 - 4\tau_2/\theta_2}}{2\tau_2}. \tag{5.18}$$

Because of the very large bandwidth of the filter, $\tau_1/\theta_1 \approx 10^{-5}$, the roots can be approximated by

$$r_+ \approx -1/\theta_2, \qquad r_- \approx -1/\tau_2. \tag{5.19}$$

Thus since both solutions are negative, it turns out that δ_2 decays to zero after the longer characteristic time, e.g. θ_2. For $R' = R$, after δ_2 has decayed to zero, the right hand side of Eq. (5.14) vanishes so that δ_1 also decays to zero after the longer characteristic time θ_1. Therefore the receiver synchronizes perfectly to the emitter after a transient time of order $\theta_1 + \theta_2$. However, if there is a mismatch in the PRBS then the right hand side of Eq. (5.14) does not vanish and therefore δ_1 is finite, resulting in a degraded synchronization. Actually, for identical parameters, δ_2 always decays to zero independently of any eventual PRBS mismatch, indicating that the internal variable does synchronize. Synchronization degradation takes place on the transmitted variable. Figure 5.9 (a) displays the root-mean square synchronization error

$$\sigma = \sqrt{\frac{\langle \delta_1(t)^2 \rangle}{\langle x_1(t)^2 \rangle}} \tag{5.20}$$

as a function of the percentage of wrong bits η in the receiver PRBS, where $\langle\rangle$ stands for time average. Synchronization error grows fast from zero when the PRBSs differ. Even for a 1% difference in the PRBS key the synchronization error is close to 25% indicating a very poor synchronization. When synchronization is degraded, $z_1(t)$ does not replicate $x_1(t)$, and the quality of the recovered message decreases. The most relevant way to characterize this is by measuring the BER of the recovered message. Figure 5.9 (b) shows the bit error rate (BER) in the case of identical

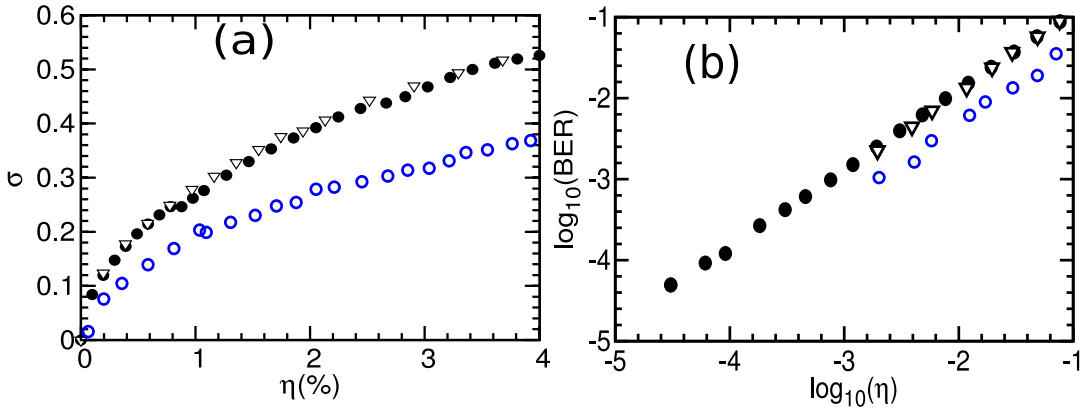


Figure 5.9: Influence of the PRBS-mismatch on (a) synchronization error σ and (b) on bit error rate (BER) for $m(t)$ transmitted at 10 Gb/s; vs. rate of wrong bit η in receiver PRBS key. We consider PRBSs of amplitude $\pi/2$ and length 2^{15} ($\bullet$) and 2^9 (Δ) bits generated at 3 Gb/s. The ($\circ$) symbol (blue color) is obtained for a PRBS of length of 2^9 bits generated at 1 Gb/s.

parameters as a function of the PRBS mismatch for a pseudorandom message transmitted at 10 Gb/s. The BER increases linearly with η. For a pseudorandom message of amplitude $\pi/2$ (which corresponds to 30% of the carrier amplitude) transmitted at 10 Gb/s a 1% mismatch in the PRBS leads to a BER of 0.01.

It should be noticed that the digital key can be implemented as a long sequence of bits generated by an appropriate algorithm or alternatively as a finite length sequence used repetitively. We find similar results in both cases provided the length of the sequence long enough as illustrated in Fig. 5.9 (b) for keys which are 2^{15} and 2^9 bit long. Besides the PRBS mismatch influence depends on the PRBS bit rate. Thus, as already mentioned, its effect is much smaller for bit rate smaller than $1/\delta T_1$ as evidenced with open circle symbols in Fig. 5.9 corresponding to PRBS with bit rate 1 Gb/s.

5.5 Conclusions

In conclusion we have shown that a digital key can be integrated with a chaos-based communication system in a way that it conceals the delay time and it is necessary ingredient for decoding. Besides bridging the gap between symmetric-key algorithmic cryptography and chaos-based encoding, the concealment of the delay time is particularly relevant to prevent from eventual eavesdropper attacks. In our phase-chaos electro-optical delay system the chaotic dynamics does not reveal the digital key so it is possible to use it in a repetitive way while concealing it. The interference generated by the two similar delay times present in our system plays a

critical role in the mutual concealment. We have found that in the electro-optical set-up for intensity chaos generation with a single delay time no concealment takes place. In our system, the effective key-space of the encryption can be defined as the product of the analog key size and the digital one. From another viewpoint, the mixing of a digital source of entropy, and an analogue one, can be viewed as an entropy amplification procedure, which is strongly relevant in terms of cryptographic security. Furthermore, the setup can be easily modified or reconfigured, both from the digital or analogue source of entropy.

On a broad perspective, as for PGP, chaotic symmetric encryption schemes as proposed here may be typically dedicated to high speed secure data transmission. Asymmetric encryption (based on algorithmic cryptography, mutually coupled optical chaos [18] or quantum key distribution [15]) could bring the complementary solution for efficient and secure (perhaps slower) secret key exchange.

Chapter 6

Electro-optic Phase Chaos Systems in Parallel Configuration

The electro-optical chaos generators considered in the previous chapters have a very large degree of flexibility. An interesting structural modification can consist in organizing the system studied in the previous chapter in a parallel configuration keeping the fundamental ideas which are the implementation of both an internal variable and a digital key. Such configuration re-organization will therefore require to regenerate the non-transmitted light beam at the receiver. This makes the receiver to operate in semi-closed loop, which is known to be very sensitive to synchronization.

The chapter is organized as follows. Sec. 6.1 provides a description of the model. Sec. 6.2 is devoted to the analysis of the delay time concealment. Sec. 6.3 deals with the synchronization between the emitter and the receiver for identical parameters. Sec. 6.4 addresses the effects of a digital key on the decoding process of the message. Finally, Sec. 6.5 provides some concluding remarks.

6.1 System

Figure 6.1 shows the parallel configuration setup. This configuration typically allows the use a single light source for the whole emitter-receiver system instead of three independent light sources as it was the case for the serial configuration. Also, while in the serial configuration the optical signal undergoes two phase modulations (chaotic modulation + either pseudorandom or message modulation) before the MZI_1, in this case four phase modulations (two chaotic proportional to $x_1(t)$ and $y_2(t)$ + pseudorandom + message) are successively applied to the optical signal, which is subsequently split in two parts. Each part is delayed in a fiber loop before the phase-to-intensity conversion by the MZI_1 or MZI_2 followed by the detection at the photodiode. The dynamics of this system can be described in terms of the dimensionless variables $x_1(t)$ and $y_1(t)$ as

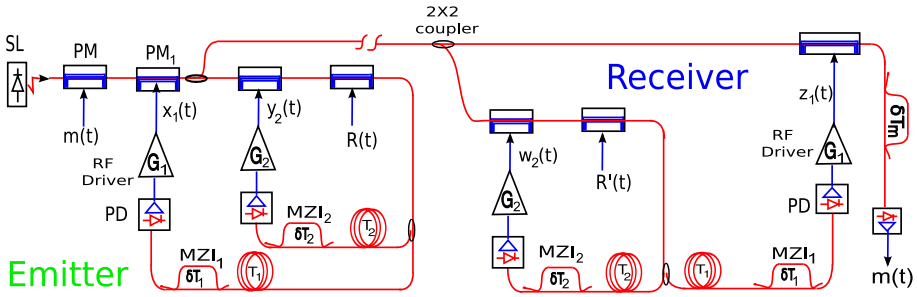


Figure 6.1: Transmitter and receiver setup in the parallel configuration: SL: semiconductor laser, PM: phase modulator, MZI: imbalanced Mach-Zehnder interferometer, PD: photodiode, $x_1(t)$ and $y_2(t)$ are the dimensionless output voltages of the RF drivers for the external and the internal loops while $R(t)$ and $m(t)$ are the pseudo-random bit sequence and message, respectively. Sub-indexes 1 and 2 refer to the internal and to the transmitted light beam parameters, respectively.

$$x_1 + \tau_1 \frac{dx_1}{dt} + \frac{1}{\theta_1} u_1 = G_1 \cos^2 \left[\Delta(x_1 + y_2)_{T_1} + \Delta(R + m)_{T_1} + \phi_1 \right], \quad (6.1)$$

$$y_2 + \tau_2 \frac{dy_2}{dt} + \frac{1}{\theta_2} u_2 = G_2 \cos^2 \left[\Delta(x_1 + y_2)_{T_2} + \Delta(R + m)_{T_2} + \phi_2 \right], \quad (6.2)$$

$$\frac{du_1}{dt} = x_1, \quad (6.3)$$

$$\frac{du_2}{dt} = y_2, \quad (6.4)$$

where again $\Delta(F)_{t_0} = F(t - t_0) - F(t - t_0 - \delta t_0)$. For numerical simulations, we use the parameters $T_1 = 15$ ns and $T_2 = 17$ ns, $\tau_1 = 20$ ps, $\tau_2 = 12.2$ ps, $\theta_1 = 1.6$ μs, $\theta_2 = 1.6$ μs, $\delta T_1 = 510$ ps, $\delta T_2 = 400$ ps, $\phi_1 = \pi/4$, $\phi_2 = \pi/8$, $G_1 = 5$ and $G_2 = 3$. With those parameters, the complexity of the system is similar to that obtained for serial configuration.

6.2 Delay Time Concealment

In the parallel configuration, the delay time can be extracted using the same techniques as before. Different from the serial configuration, here T_1 and T_2 are both relevant and not just their sum. However, the total number of relevant delay times is still four, e.g. T_1, $T_1 + \delta T_1$, T_2 and $T_2 + \delta T_2$. Figure 6.2 displays the autocorrelation (a) and the DMI (b) without (red line) and with a PRBS of amplitude $\pi/2$ at 3 Gb/s (black), computed from a long series for $x_1(t)$. We do not take into account the message in this section ($m = 0$). Without PRBS, relevant peaks are found both in the autocorrelation and in the DMI at delay times T_1 and $T_1 + \delta T_1$. However,

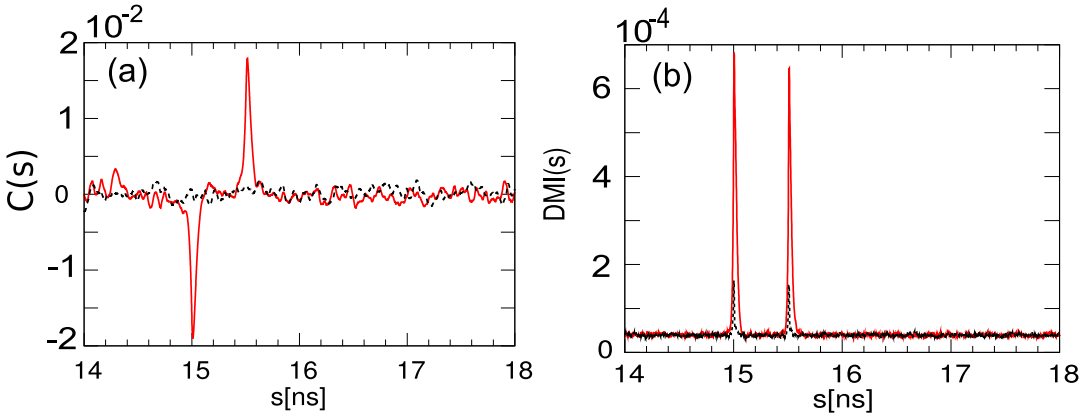


Figure 6.2: Autocorrelation function $C(s)$ (a) and delayed mutual information DMI(s) (b) of $x_1(t)$ without PRBS (red line), and with a PRBS of amplitude $\pi/2$ at 3 Gb/s (black). We consider $\delta T_1 = 510$ ps and $\delta T_2 = 400$ ps. A time series of length 10 μs with 10^7 data points was used.

no relevant peak is found around other delay time positions, e.g T_2 and $T_2 + \delta T_2$. We have found that even using the time distribution extrema and the filling factor methods for the free-noise system, the delay time signatures remain concealed at T_2 and $T_2 + \delta T_2$. Note that the concealed delay times correspond to those involved in the equation for the non-transmitted variable $y_2(t)$ [see Eq. (6.2)].

When adding the PRBS, it turns out that autocorrelation is not efficient to identify the delay times anymore while the size of the peak given by the DMI considerably decreases. The persistence of the peaks even when considering the PRBS can be understood as follows. Without PRBS the size of the peaks obtained around the delay time is stronger than in the case of the serial configuration for the same parameters (compare the red line of Fig. 6.2 with that of Fig. 5.5). This therefore indicates that the relationship between $x_1(t)$ and its delayed values for the parallel configuration is stronger than for the serial one. Effectively, the amplitude of the chaos driving the nonlinear term in Eqs. (6.1) and (6.2) for the parallel configuration is twice than that for the serial configuration, e.g. $x_1(t) + y_2(t)$ instead of $y_2(t)$ for serial configuration, and therefore the mixing of the PRBS and the chaos is less balanced so that the PRBS cannot conceal the delay time. However, the cross-correlation between $x_1(t)$ and $R(t)$ is of the order of 10^{-3}. Thus the PRBS remains efficiently masked by the chaos as for the serial configuration. One can also remark that in any case the effect of the PRBS is to reduce the peak size even if it is not capable of a full concealment.

Another relevant point consists in investigating the conditions for which the system guarantees the concealment of T_2 and $T_2 + \delta T_2$. In other words, any linear relationship between $x_1(t)$ and $y_2(t)$ will consequently lead to appearance of peaks

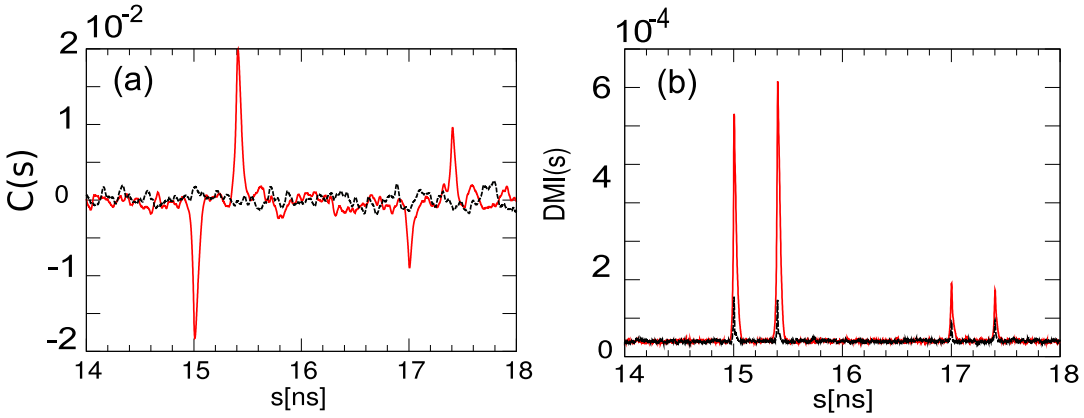


Figure 6.3: Autocorrelation function $C(s)$ (a) and delayed mutual information DMI(s) (b) of $x_1(t)$ without PRBS (red line), and with a PRBS of amplitude of $\pi/2$ at 3 Gb/s (black). We consider $\delta T_1 = \delta T_2 = 400$ ps. A time series of length 10 μs with 10^7 data points was used.

even at T_2 and $T_2+\delta T_2$. The investigation of such a linear relationship between $x_1(t)$ and $y_2(t)$ is possible in Fourier domain. Thus, by Fourier transforming Eqs. (6.1) and (6.2), one obtains

$$X_1(\omega)\left(1+i\omega\tau_1+\frac{1}{i\omega\theta_1}\right) = G_1 e^{-i\omega T_1}\mathbf{FT}\Big\{\cos^2\left[\bar{\Delta}(x_1+y_2)_{\delta T_1}+\bar{\Delta}(R)_{\delta T_1}+\phi_1\right]\Big\},$$
$$Y_2(\omega)\left(1+i\omega\tau_2+\frac{1}{i\omega\theta_2}\right) = G_2 e^{-i\omega T_2}\mathbf{FT}\Big\{\cos^2\left[\bar{\Delta}(x_1+y_2)_{\delta T_2}+\bar{\Delta}(R)_{\delta T_2}+\phi_2\right]\Big\},$$

where $\bar{\Delta}(F)_{\delta t_0} = F - F(t-\delta t_0)$ and $\mathbf{FT}\{x\}$ stands for the Fourier transform of x. For $\delta T_1 = \delta T_2$ and $\phi_1 = \phi_2$, it turns out that

$$\frac{X_1(\omega)}{Y_2(\omega)} = \frac{G_1\left(1+i\omega\tau_2+\frac{1}{i\omega\theta_2}\right)}{G_2\left(1+i\omega\tau_1+\frac{1}{i\omega\theta_1}\right)}\exp\left[-i\omega(T_1-T_2)\right]. \tag{6.5}$$

Equation (6.5) shows linear relationship between $x_1(t)$ and $y_2(t)$ and consequently clear peaks also emerge at T_2 and $T_2+\delta T_2$ when $\delta T_1 = \delta T_2$. Figure 6.3 shows the appearance of peaks at T_2 and $T_2+\delta T_2$ both from autocorrelation and DMI, even when the offset phases are different. For this specific case, we have found that clear peaks also appear at $T_2 - T_1$ (which are out of the range of the figure) as a consequence of the linear relationship which also exists between $x(t)$ and $x(t-(T_2-T_1))$ [114]. This result therefore shows that only imbalanced delays can lead to delay concealment by breaking the relationship between $x_1(t)$ and $y_2(t)$.

6.3 Synchronization

The part of the signal sent to the receiver is taken at the output of the PM_1 and consequently, the non-transmitted variable $y_2(t)$ has to be generated at the receiver, through an internal closed loop. We investigate here the conditions for possible synchronization when assuming identical parameters for emitter and receiver. Considering the receiver setup shown in Fig. 6.1, its dynamics can be described by

$$z_1 + \tau_1 \frac{dz_1}{dt} + \frac{1}{\theta_1} v_1 = G_1 \cos^2 \left[\Delta(x_1 + w_2)_{T_1} + \Delta(R' + m)_{T_1} + \phi_1 \right], \quad (6.6)$$

$$w_2 + \tau_2 \frac{dw_2}{dt} + \frac{1}{\theta_2} v_2 = G_2 \cos^2 \left[\Delta(x_1 + w_2)_{T_2} + \Delta(R' + m)_{T_2} + \phi_2 \right], \quad (6.7)$$

$$\frac{dv_1}{dt} = z_1, \quad (6.8)$$

$$\frac{dv_2}{dt} = w_2. \quad (6.9)$$

For $G_2 = 0$, $w(t)$ decays to zero after the characteristic time θ_2. The system therefore operates in open loop and consequently the synchronization is always guaranteed for identical parameters as shown in [76]. Thus starting from $G_2 = 0$ and keeping receiver parameters identical to the emitter ones, we gradually increase G_2 in order to investigate the range of G_2 for which synchronization is possible. An efficient way to do that consists in investigating the stability of the complete synchronization between $z_1(t)$ and $x_1(t)$ (characterized by the coincidence of states between $x_1(t)$ and $z_1(t)$, e.g., $x_1(t) = z_1(t)$) either through the root-mean square synchronization error or by estimating the largest conditional Lyapunov exponent (LCLE).

As in the previous case, Eq. (5.20) can be used for estimating the synchronization error between $x_1(t)$ and $z_1(t)$. Regarding the LCLE, it can be defined following the pioneering work of Pyragas in [141] which states that the stability of the synchronization in a delayed system can be determined by looking at the growth of state vector $\delta \in \mathbb{L}$ (where $\mathbb{L}$ is a suitable space function) constructed in the interval $\left[t - T, t\right]$. Since the system has four different delay times, T_1, $T_1 + \delta T_1$, T_2, $T_2 + \delta T_2$, we should consider the largest delay involved in the system. In our case the system largest delay time is $T_D = T_2 + \delta T_2$. Defining $\delta_1 = z_1(t) - x_1(t)$ and $\delta_2 = w_2(t) - y_2(t)$ as in the previous chapter the LCLE defined in [141] can be actually modified for this system as

$$\lambda_L = \lim_{t \to \infty} \frac{1}{t} \ln \left\{ \frac{\left[\int_{-T_D}^{0} \delta_1^2(t + t') dt' \right]^{1/2}}{\left[\int_{-T_D}^{0} \delta_1^2(t') dt' \right]^{1/2}} \right\}. \quad (6.10)$$

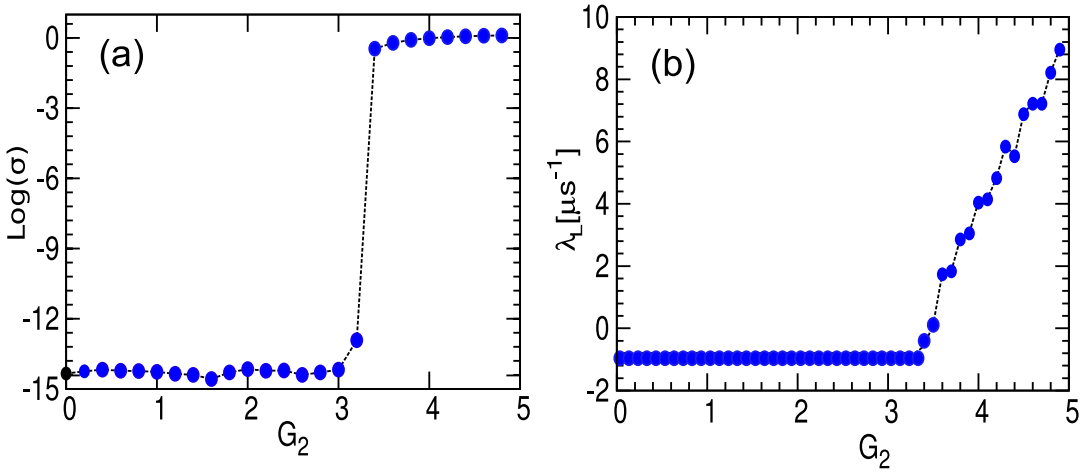


Figure 6.4: (a) Synchronization Error σ in logarithmic scale, (b) Largest conditional Lyapunov exponent (LCLE) versus G_2 considering $G_1 = 5$.

Stable synchronization occurs for $\lambda_L < 0$. By subtracting Eq. (6.1) from (6.6) and Eq. (6.2) from (6.7) and linearizing for δ_1 and δ_2, one obtains

$$\delta_1 + \tau_1 \frac{\delta_1}{dt} + \frac{1}{\theta_1}\varepsilon_1 = -G_1 \Delta(\delta_2)_{T_1} \sin\left[2\Delta(x_1 + y_2)_{T_1} + 2\Delta(R)_{T_1} + 2\phi_1\right], \quad (6.11)$$

$$\delta_2 + \tau_2 \frac{\delta_2}{dt} + \frac{1}{\theta_2}\varepsilon_2 = -G_2 \Delta(\delta_2)_{T_2} \sin\left[2\Delta(x_1 + y_2)_{T_2} + 2\Delta(R)_{T_2} + 2\phi_2\right], \quad (6.12)$$

Thus $\delta_1(t)$ to be used in Eq. (6.10) can be obtained by numerical resolution of Eqs. (6.1), (6.2), (6.11) and (6.12). Note that λ_L depends implicitly on the feedback strengths G_1 and G_2.

Figure 6.4 (a) shows the synchronization error σ in logarithmic scale as function of G_2 for $G_1 = 5$ which corresponds to a relatively high loop gain. It turns out that up to $G_2 = G_2^{\text{th}} \approx 3.2$, perfect synchronization indicated by a very small synchronization error ($\sigma < 10^{-13}$ corresponding to the numerical accuracy) is observed. Beyond this threshold value for G_2, desynchronization rapidly appears as indicated by a synchronization error which is of order 1. Similar results are found in Fig. 6.4 (b) which displays the LCLE as a function of G_2. Furthermore, it can be seen that for all the values of G_2 for which $x_1(t)$ and $z_1(t)$ synchronize, e.g. $G_2 < G_2^{\text{th}}$, the LCLE takes always the same value θ_1^{-1} which corresponds to the slowest characteristic time of the system. Beyond G_2^{th}, any small perturbation $\delta_1(t)$ or $\delta_2(t)$ grows in time and therefore λ_L becomes positive indicating desynchronization between the emitter and receiver. We have found that even setting $R = 0$, the range of values for G_2 for which synchronization takes place remains the same. Similar values for the synchronization threshold G_2^{th} are obtained for other values of the external

loop gain G_1 provided $G_1 > 3$. Therefore in what follows we will consider only $G_2 < G_2^{\text{th}} \approx 3.2$.

6.4 Effect of the PRBS on Synchronization

Although in the parallel configuration the PRBS does not completely conceals the delay times T_1 and $T_1+\delta T_1$, it can still play a key role in parameter space dimension. For $R' \neq R$ the dynamics of $\delta_1(t)$ and $\delta_2(t)$ is given by

$$\begin{aligned}
&\delta_1 + \tau_1 \frac{d\delta_1}{dt} + \frac{1}{\theta_1}\varepsilon_1 = -G_1 \sin\left[\Delta(\delta_2)_{T_1} + \Delta(R'-R)_{T_1}\right] \\
&\quad \times \sin\left[2\Delta(x_1+y_2)_{T_1} + \Delta(\delta_2)_{T_1} + \Delta(R+R'+2m)_{T_1} + 2\phi_1\right], \qquad (6.13)\\
&\delta_2 + \tau_2 \frac{d\delta_2}{dt} + \frac{1}{\theta_2}\varepsilon_2 = -G_2 \sin\left[\Delta(\delta_2)_{T_2} + \Delta(R'-R)_{T_2}\right] \\
&\quad \times \sin\left[2\Delta(x_1+y_2)_{T_2} + \Delta(\delta_2)_{T_2} + \Delta(R+R'+2m)_{T_2} + 2\phi_2\right], \qquad (6.14)\\
&\frac{d\varepsilon_1}{dt} = \delta_1, \qquad (6.15)\\
&\frac{d\varepsilon_2}{dt} = \delta_2. \qquad (6.16)
\end{aligned}$$

These equations indicate that, contrary to the serial configuration, δ_2 does not always decays to zero independently of any eventual PRBS mismatch. Synchronization degradation therefore takes place both on internal and the transmitted variables. Furthermore, it is noteworthy that no synchronization is possible between $x_1(t)$ and $z_1(t)$ when the internal variables do not synchronize, e.g. $\delta_2(t) = 0$.

Figure 6.5 shows both the mean square synchronization error (a) and the BER (b) as a function of PRBS mismatch for different values of the internal loop gain G_2. For $G_2 = 0$, there is no internal variable and therefore synchronization degradation relies on the transmitted variable as found for the serial configuration. The synchronization error grows faster with the mismatch and just a 1% PRBS mismatch leads to a synchronization error of about 25% similar to that found in the serial configuration. Regarding the BER obtained for $G_2 = 0$, it grows linearly with the PRBS mismatch and in fact the results are similar to those obtained in the serial configuration for $G_1 = G_2 = 5$. When increasing G_2, the degradation becomes stronger both in synchronization error and BER. As an illustration, for $G_2 = 3$ the degradation for 0.4% PRBS mismatch is similar to that obtained for 2% of PRBS mismatch when considering $G_2 = 0$. Also, as for the serial configuration, we have found that for bit rates lower than $1/\delta T_1$, the effect of the PRBS is largely reduced.

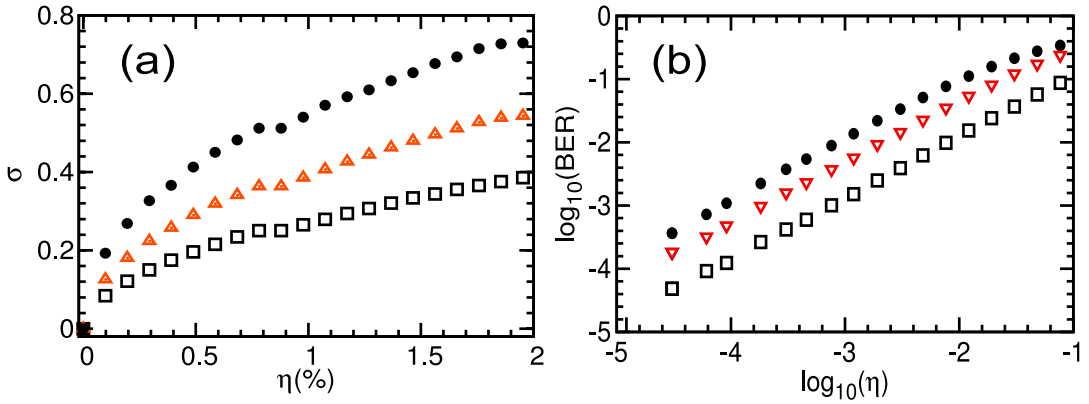


Figure 6.5: Influence of the PRBS-mismatch η on (a) Synchronization evaluated through the root-mean square synchronization error σ without the message, and (b) on the BER for a 10Gb/s message. We have considered a PRBS $R(t)$ of length 1024 bits generated at 3 Gb/s, $G_1 = 5$ and $G_2 = 0$ ($\square$), $G_2 = 2$ ($\triangle$), $G_2 = 3$ ($\bullet$).

6.5 Conclusions

We have studied in this chapter a configuration based on two parallel electro-optic phase-chaos loops. This allows for the generation of two phase-chaos variables, one of which is transmitted to the receiver while the other remains internal. The system also allows for an efficient implementation of a digital key. A suitable receiver is organized in a semi-closed loop configuration since it contains both an open loop for the transmitted variable and a closed one for the internal variable. Starting from single loop system ($G_2 = 0$), we have investigated the conditions for high synchronization quality. Thus, it was found that synchronization takes place even for moderate values of the internal loop gain up to $G_2 \approx 3.2$. For the values range of G_2 for which the system synchronizes, we have found that the system conceals all the internal loop delay times even without any digital key. On the other hand, we have found that the digital key decreases the signature corresponding to the two delay times of the external loop although it does not completely suppress them. Interestingly, the effect of digital key on synchronization degradation is stronger than for the serial configuration so that its integration efficiently increases the parameter space dimension in chaos-based communications.

Chapter 7

Effect of Fiber Dispersion on Broadband Chaos Implemented by Electro-Optic Phase Chaos Systems

7.1 Introduction

Real communication networks will require the use of transmitters and receivers operating in synchronized chaotic regime, even if located far one from another [31]. In general, the signals are transmitted to receiver via either the electrical or the optical channels. The latter is the most used in the current communications because of their very large bandwidth and their low losses. However, besides the problem of signal-to-noise ratio caused by the noise and various mismatches in parameters between the emitter and the receiver, which are general for any communication system, one should additionally overcome the fiber effects. In fact, during its travel through the fiber, the carrier is subjected to attenuation, Kerr nonlinearity and chromatic dispersion. The latter effect is the most damaging in broadband chaos communication because the encrypted signal bandwidth may span over several tens GHz around the nominal frequency of the laser beam. Hence, dispersion shuffles this broadband spectrum and, as a consequence, synchronization noise arises because of imperfect chaos replication at the receiver. This residual cancellation noise is naturally expected to increase with the spectral bandwidth of the signal, with the length of the fiber link, and with the absolute value of the chromatic dispersion.

For optical chaos communication networks, the chaotic carriers used for encryption can be generated using a wide variety of architectures ranging from the amplitude/ intensity [67, 74, 142] to phase modulation schemes [75, 76]. In our case, the carriers launched into the fiber are generated from the electro-optic nonlinear delay phase chaos generator presented in Sec. 2.3 and the results reported

in this chapter indicate a better synchronization performance [143] when compared with previous measurements in electro-optical intensity chaos [144]. To the best of our knowledge, very few investigations have been devoted to the topic of fiber propagation effects on the performance of chaos cryptography [42, 129, 130, 145], and they were exclusively based on numerical simulations. Fiber transmission has been considered, nonetheless, in some experimental works [74, 146], but no detailed analysis on the fiber dispersion effects has been reported.

Our aim in this chapter is to address this issue with a joint theoretical and experimental analysis, and with a particular emphasis on the exploration of various dispersion management schemes able to minimize the detrimental effects of chromatic dispersion. The chapter is organized as follows. In Sec. 7.2 we briefly overview the optical fiber effects. In Sec. 7.3 we present the system under study. The Sec. 7.4 is devoted to the study of cancellation (or synchronization) noise, while Sec. 7.5 is dedicated to the corresponding spectra. The last section summarizes our results and concludes the chapter.

7.2 Overview on Optical Fiber Effects

In its simplest form, an optical fiber consists of a central glass core surrounded by a cladding layer. It can be designed using several types of materials chosen to minimize the loss and the distortion of the signal during its transmission through the fiber.

7.2.1 Origin of fiber impairments

Losses, nonlinearity and dispersion are the major unwanted properties of optical fibers in lightwave communication.

• Fiber losses: The losses in optical fibers dominantly result from the material absorption and Rayleigh scattering. The first arises from impurities in the fiber materials while the second comes from density fluctuations frozen into the fused silica during manufacture. As one may therefore expect, fiber losses depend on the wavelength of light. It has been found that losses are considerably higher at shorter wavelengths, reaching a minimum level of about 0.2 dB/km at 1.55 μm which is the wavelength used for current communications. In general, a transmitted signal undergoes an exponential attenuation $e^{-\alpha L}$ when traveling over the fiber, where α is the attenuation factor and L the fiber length. To get around the attenuation problem, current optical fiber communications inline erbium-doped fiber amplifiers (EDFA) to compensate for losses which have been accumulated during the propagation.

• Fiber nonlinearities: On a fundamental level, the origin of nonlinear response is related to anharmonic motion of bound electrons under the influence of an applied field. The material polarization which depends on higher-order susceptibility is responsible for nonlinear effects such as higher-harmonic generation and sum-frequency generation [147]. Besides defects or color centers inside the fiber core can also contribute to second-harmonic generation under certain conditions. Single mode fibers are therefore preferred than multi-mode fibers for optical fiber communications. Special efforts have been done to annihilate some sources of nonlinearities so that most of the nonlinear effects in optical fibers are currently originated only from nonlinear refraction and the Kerr effect.

• Dispersion: Dispersion is composed of polarization dispersion and chromatic dispersion. In our case, only the chromatic dispersion captures our attention since efforts have been ever made to limit the polarization dispersion at very acceptable level in current commercial optical fiber communications. Furthermore, the effects of polarization mode-dispersion in chaos encryption, have been already investigated in [148]. Regarding the chromatic dispersion it is mainly caused by the interaction between the light pulse and the material used to manufacture the optical fiber. Besides that, a light pulse is affected by the waveguide dispersion so that the total chromatic dispersion is the balance between the material and the waveguide dispersions. Mathematically, the effects of fiber dispersion are accounted for by expanding the mode-propagation constant β in a Taylor series around the central frequency ω_0 as follows

$$\beta(\omega) = \beta_0 + \beta_1(\omega - \omega_0) + \frac{1}{2}\beta_2(\omega - \omega_0)^2 + ..., \tag{7.1}$$

where the parameter $\beta_1 = (d\beta/d\omega)$ stands for the inverse of group velocity V_g, e.g. $\beta_1 = 1/V_g$, while $\beta_2 = (d^2\beta/d\omega^2)$ is the group velocity dispersion coefficient [149]. The latter determines how much an optical pulse would broaden on propagation inside the fiber. In the straightforward form,

$$\beta_2 = -\frac{\lambda^2}{2\pi c}D, \tag{7.2}$$

where D is the fiber dispersion coefficient, λ is the optical carriers wavelength, and c is the speed of light in vacuum. In some cases such as dispersion shifted fibers for which the 2^{nd} order dispersion is small, the third order dispersion is taken into account and consequently, Eq. (7.1) should be expanded up to 3^{rd} order.

7.2.2 Operating principle of dispersion in communications

For a single mode fiber, Eq. (7.1) underlies that a specific spectral component at the frequency ω would arrive at the output end of the fiber after a delay time

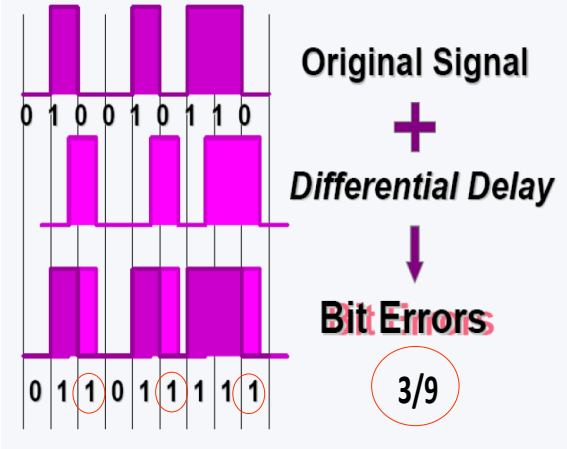


Figure 7.1: How the dispersion reacts to induce bit errors.

$T = L/V_g$. However in real communication networks all light sources emit not only at a single wavelength λ, but in the band of the spectral width, $\Delta\lambda$, distributed around. Different wavelengths in the band $\Delta\lambda$ travel at slightly different speeds and if the distance over which they travel is significant, they arrive at different time, leading therefore to spreading or broadening of the original signal. For an optical source emitting in the range of wavelength $\Delta\lambda$, the frequency spread can be determined. In fact, if $\Delta\omega$ is the spectral width of the pulse, the extent of pulse broadening for a fiber of length L is governed by [150]

$$\Delta T = \frac{dT}{d\omega}\Delta\omega = \frac{d}{d\omega}\left(\frac{L}{v_g}\right)\Delta\omega = L\frac{d^2\beta}{d\omega^2}\Delta\omega = L\beta_2\Delta\omega. \tag{7.3}$$

The lag time at arrival ΔT is called differential delay. Since $\omega = 2\pi c/\lambda$, $\Delta\omega = (-2\pi c/\lambda^2)\Delta\lambda$, Eq. (7.3) can be also written

$$\Delta T = LD\Delta\lambda, \tag{7.4}$$

with D expressed in units of ps/(km-nm). Figure 7.1 illustrates the potential action of the dispersion on the real transmitted data. When a sequence of logical bits (0, 1) are transmitted though the fiber, they disperse during propagation and do not arrive simultaneously at the fiber output after a long distance traveling. The bit error numerically obtained by confronting the recovery data to the original shows how some bits have been distorted. Of course, this number is expected to increase with the transmission distance. It is worth noting that the effect of dispersion on the bit rate $\mathcal{B}$ can be estimated by using the criterion $\mathcal{B}\Delta T < 1$, e.g. $\mathcal{B}L|D|\Delta\lambda < 1$.

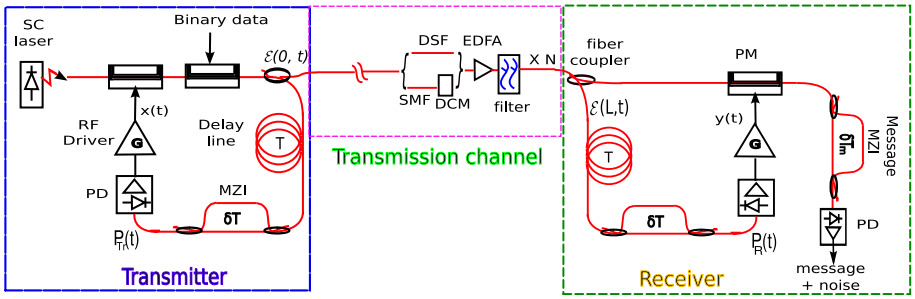


Figure 7.2: Experimental setup. EDFA: erbium-doped fiber amplifier; MZI: Mach-Zehnder interferometer; PD: photodiode; PM: phase modulator; SL: semiconductor laser; SMF: Single Mode Fiber, DCM: Dispersion Compensation Module DSF: Dispersion Shifted Fiber.

This condition allows to estimate the order of magnitude of the bit rate that can be transmitted depending on the fiber characteristics and the spectral of the emitted source. It should be also stressed that although the information carried by some pulses is distorted, it is not lost. Thus, it can be recovered if the distorted pulses are restored [151] using dispersion management.

7.3 Optical Channel and Receiver

7.3.1 Emitter and optical channel

The full experimental setup of emitter-receiver including the fiber transmission channel is shown in Fig. 7.2. As earlier derived in Sec. 2.3 the emitter dynamics including the message can be described by

$$x + \tau\frac{dx}{dt} + \frac{1}{\theta}u = G\cos^2\left\{\Delta x_T + \Delta m_T + \Phi_0\right\}, \tag{7.5}$$

$$\frac{du}{dt} = x. \tag{7.6}$$

According to the experimental setup, the light beam launched into the fiber communication channel corresponds to the optical signal at the second phase modulator output. The system configuration as shown in Fig. 7.2 allows to derive the electric field envelope of the transmitted light

$$\mathcal{E}(0,t) = E_0 \exp\left\{2i[x(t) + m(t)]\right\}. \tag{7.7}$$

The above equation is taken as the initial condition to simulate the propagation of the chaotic carrier along the fiber, which is modeled by the following nonlinear

equation [147]:

$$\frac{\partial \mathcal{E}}{\partial z}(z,t) = -\frac{\alpha}{2}\mathcal{E}(z,t) - \beta_1 \frac{\partial \mathcal{E}}{\partial t}(z,t) \quad - \quad i\frac{\beta_2}{2}\frac{\partial^2 \mathcal{E}}{\partial t^2}(z,t) + \frac{\beta_3}{6}\frac{\partial^3 \mathcal{E}}{\partial t^3}(z,t) + i\gamma \left|\mathcal{E}(z,t)\right|^2 \mathcal{E}(z,t), \tag{7.8}$$

where β_k (k=1, 2, 3) is the k^{th} order dispersion, γ is the nonlinear Kerr factor and α is the linear attenuation. In the reference frame moving with the group velocity ($t \to t - \beta_1 z$), Eq. (7.8) becomes

$$\frac{\partial \mathcal{E}}{\partial z}(z,t) = -\frac{\alpha}{2}\mathcal{E}(z,t) - i\frac{\beta_2}{2}\frac{\partial^2 \mathcal{E}}{\partial t^2}(z,t) + \frac{\beta_3}{6}\frac{\partial^3 \mathcal{E}}{\partial t^3}(z,t) + i\gamma \left|\mathcal{E}(z,t)\right|^2 \mathcal{E}(z,t). \tag{7.9}$$

It is worth recalling that if the third order dispersion is neglected, Eq. (7.9) is the dispersive nonlinear Schr´odinger equation. The time of flight after propagation over a fiber length L is $T_D = L/\beta_1$. As discussed later, two scenarios are to be considered for transmission channel in this chapter. One including single mode fiber plus dispersion compensation and another considering a dispersion shifted fiber. In both cases, after propagating $\mathcal{E}(0,t)$ over a distance $L \leq 50$ Km (and eventually going through dispersion compensation) the output is amplified to compensate for the losses. Experimentally amplification is realized by an EDFA followed by an optical channel filter that removes most of the spontaneous emission noise introduced by the EDFA. Therefore in the numerical simulation we consider a noiseless amplifier.

7.3.2 Receiver

Similarly to the previous chapters, the receiver stage does simultaneously undertake two distinct actions: chaos cancellation, and DPSK message demodulation. The receiver input light is split into two parts using a variable coupler: one part is sent to a nonlinear delay processing branch, while the second part is fed into the local electro-optic phase modulator which role is to remove electro-optically the chaotic phase encryption mask. The amplifier and the variable coupler are set in such a way that the field going into the delay branch, $\mathcal{E}(L,t)$, has the same mean power P_0 as in the transmitter. In the case of an ideal chaos cancellation, the receiver phase modulation output therefore corresponds to a standard DPSK-modulated light beam (the one imposed by the message phase modulator in the transmitter). The optical field arriving at the receiver MZI is $\mathcal{E}(L,t)$, so the MZI intensity output is

$$P_{\mathrm{R}}(t) = \frac{1}{\mu_0 c}\frac{1}{4}\left|\mathcal{E}(L, t-T')e^{i(2\Phi_0'+\pi)} + \mathcal{E}(L, t-T'-\delta T')\right|^2, \tag{7.10}$$

where the prime ($'$) indicates the receiver parameters. As already stated, the replicated chaos with the opposite sign is obtained by operating the MZI with a $\pi-$shifted

static phase as indicated in Eq. (7.10). Alternatively this could have been done using balanced photodiodes and exchanging their inputs or using an inverted amplifier at the receiver.

Under such conditions the normalized signal $y(t)$ driving the receiver phase modulator with an anti-replica of the chaotic masking, is ruled by the following "open loop" dynamics:

$$y(t) + \tau' \frac{dy(t)}{dt} + \frac{1}{\theta'} \int_{t_0}^{t} y(s)ds = G' \frac{P_R(t)}{P_0}, \tag{7.11}$$

where $G' = \pi \eta'_0 G'_0 S' / (2V'_{\pi RF})$.

The receiver PM applies the phase modulation given by $y(t)$ to the received light beam in order to remove the chaotic carrier. The resulting light beam can then be processed through a standard DPSK demodulator matched with the message bit rate (imbalanced MZI with δT_m in Fig. 7.2). The photodiode detects

$$\mu_R(t) = \frac{1}{4} S \left| \mathcal{E}(L,t) e^{2iy(t)} + \mathcal{E}(L, t - \delta T_m) e^{2iy(t-\delta T_m)} \right|^2 . \tag{7.12}$$

In the absence of a binary DPSK message, the sum $\varepsilon = (x + y)$ is used to evaluate the accuracy of the phase chaos cancellation. Similarly to the usual signal-to-noise ratio, a cancellation-to-chaos ratio can be defined in order to analyze the accuracy of the chaos cancellation in a normalized way.

7.4 Numerical Results: Cancellation Noise

In this section, we theoretically investigate the time-domain variations of the cancellation noise when the fiber and the chaotic carrier parameters are varied. This analysis relies on the coupled Eqs. (7.5), (7.6), (7.9) and (7.11) with the parameters $\tau = 20$ ps, $\theta = 1.6$ μs, $\delta T = 0.4$ ns, $\Phi_0 = \pi/4$ and $T = 70$ ns. The power P_0 is 5 mW, and we consider a single mode fiber (SMF) for the transmission channel, with parameters $\beta_2 = 20$ ps^2 km^{-1}, $\beta_3 = 0.1$ ps^2 km^{-1}, $\gamma = 1.1$ W^{-1}km^{-1}, $\alpha = 0.2$ dB km^{-1} (0.046 km^{-1}). The propagation of the optical signal in the optical fiber channel is simulated using the split-step Fourier algorithm, while the calculation of the emitter receiver dynamics is performed using the predictor-corrector algorithm. The influence of parameter mismatch has already been explored elsewhere [105] for a similar electro-optic chaos communication system, so that we can here concentrate on the effects of the fiber channel only. In this section all the receiver parameters will thus be assumed to be perfectly matched. This hypothesis enables an easier understanding of the cancellation noise that is exclusively due to fiber propagation effects. Without any message inserted, we characterize the system performance using the

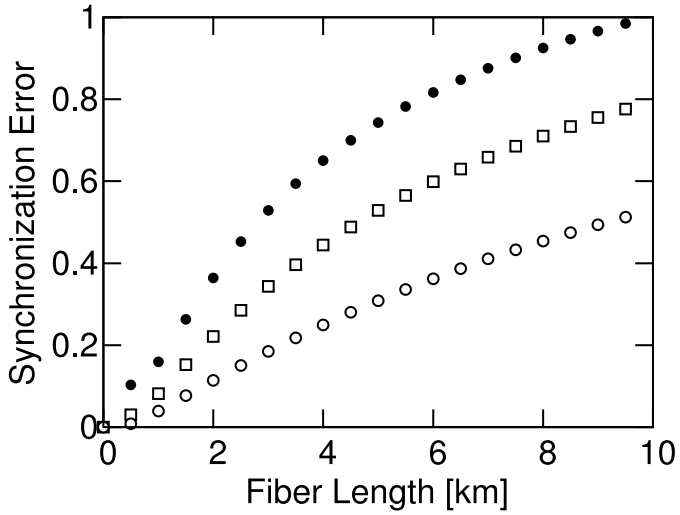


Figure 7.3: Numerical simulation of the synchronization error between the emitter and receiver as a function of fiber length in a standard SMF with $\beta_2 = 20$ ps^{2}km^{-1} and $\beta_3 = 0$. The various values of the feedback gains are $G = 2.5$ ($\circ$), $G = 3.5$ ($\square$), and $G = 5.0$ ($\bullet$).

normalized cancellation-to-chaos ratio defined as

$$\sigma = \sqrt{\frac{\langle \varepsilon^2(t) \rangle}{\langle x^2(t) \rangle}}\,. \tag{7.13}$$

We remark that perfect cancellation of the chaos is expected when $y(t)$ perfectly anti-synchronizes with $x(t)$. Figure 7.3 illustrates clearly the dramatic influence of the fiber channel on the chaos cancellation at the receiver, when SMF only is involved in the optical link. The situation worsens as expected for higher feedback strength ($G = 5.0$), as this corresponds to an even broader chaotic spectrum to be conveyed through the dispersive channel (thereby it increases the linear frequency mixing effect of dispersion). For each situation reported in Fig. 7.3, we clearly see that a strong signal distortion occurs already for propagation over 10 km of SMF. In this case, the message could not be successfully retrieved because the synchronization error is too large. Typically, one would expect this error to be below 10%, which is of the order of the best experimental cancellation-to-chaos ratio due to residual parameter mismatch in a back-to-back configuration [76].

Since the nonlinear effects are relatively weak in our context, the large distortion mainly originates from chromatic dispersion. This first result on a standard non compensated fiber channel shows that phase chaos communication is requiring necessarily a proper management of the dispersion effects.

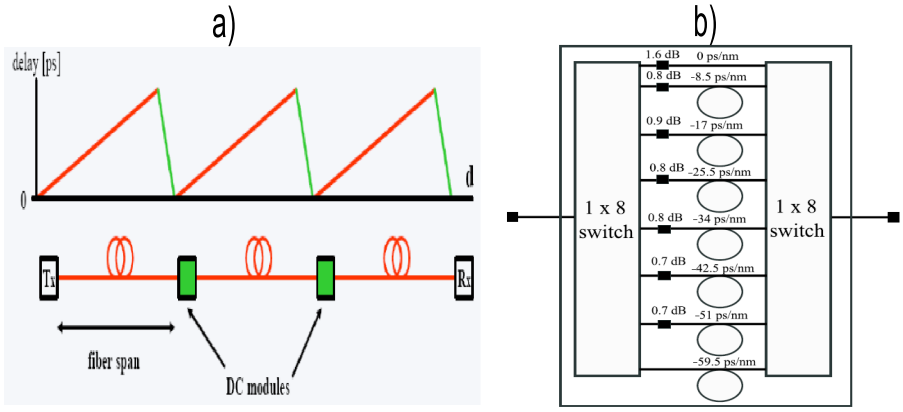


Figure 7.4: (a) Operating principle of transmission including dispersion compensation in chaos communications, (b) Prototype of tunable DCM able to compensate for a dispersion between 0 and 59.5 ps/nm in steps of 8.5 ps/nm.

7.4.1 Using dispersion-compensation

Dispersion can be compensated either using a dispersion compensation module (DCM) or a dispersion compensating fiber (DCF). In both cases the principle consists in propagating a signal through the SMF which generates a differential delay. Then this differential delay is reduced using a component (DCF or DCM) which has a strong dispersion with the opposite sign. The process is repeated at regular intervals throughout the fiber as it is shown in Fig. 7.4 (a). In Fig. 7.4 (b) we show an example of DCM designed to operate between 0 and 59.5 ps/nm by switching between several subcomponents that allow to compensate for different dispersions in steps of 8.5 ps/nm. For ideal chromatic dispersion compensation, the SMF and DCF lengths are chosen to satisfy the condition

$$\sum_k \beta_2^k L_1^k + \beta_{2DCF}^k L_2^k = 0, \tag{7.14}$$

where k indicates the parameters attached to the k^{th} portion. In this chapter we consider only one of the portions. Generally, a DCF has nominal values which are typically ten times higher than those of the fiber to be compensated for, and attenuation in DCFs is usually higher as well. Therefore, in order to adequately compensate for the dispersion induced in the SMF, we consider the parameters $\beta_{2DCF} = -10\beta_2$, $\alpha_{DCF} = 3\alpha$ and $\gamma_{\mathrm{DCF}} = 6\ \mathrm{W}^{-1}\mathrm{km}^{-1}$. Hence, after the propagation over a SMF with length L_1, the signal is launched into a DCF with length $L_2 \ll L_1$, and which satisfies the condition

$$\beta_2 L_1 + \beta_{2DCF} L_2 = 0\,. \tag{7.15}$$

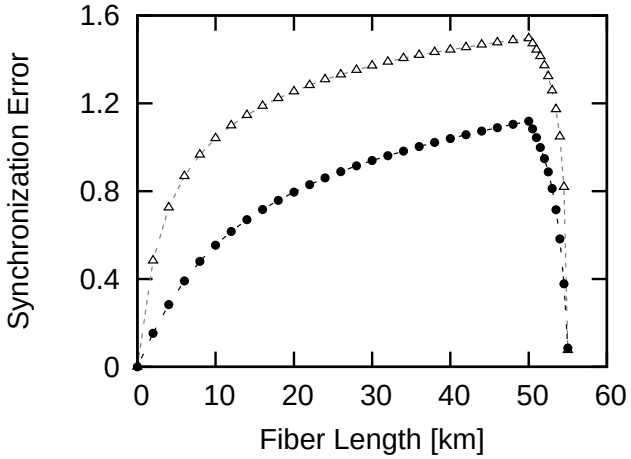


Figure 7.5: Numerical simulation of the dispersion compensation using DCFs with $\beta_{2\mathrm{DCF}} = -200$ ps^2/km, $\beta_{3\mathrm{DCF}} = 0.1$ ps^3/km, $\alpha_{\mathrm{DCF}} = 0.6$ dB, $\gamma_{\mathrm{DCF}} = 6$ W^{-1}km^{-1}. The values used for the feedback gains are $G = 2.5$ (•) and $G = 5.0$ (△). When the chaotic carrier is launched at $z = 0$, the synchronization error increases steadily but at $z = 50$ km, a 5 km-long DCF is used and drastically reduces the cancellation noise.

In Fig. 7.5, the chaotic carrier undergoes distortion after traveling over $L_1 = 50$ km of SMF, and then is launched into a DCF in which it goes back closer to its initial state. In the figure we plot what would be the synchronization error if a receiver was placed at a given point in the fiber. Synchronization error grows with the propagation distance until the DCF is reached, and then it decreases owing to the compensation. Finally for a 5 km compensation with DCF, one can obtain a synchronization error as small as 7.5% when considering a transmitter with $G = 5$. The situation is almost the same for smaller gain values ($G = 2.5$), where the synchronization error is also estimated to 7.5%. Hence, for DCFs, the compensation is almost independent of G. It is interesting to note that this residual synchronization error is exclusively due to the effect of the fiber nonlinearity, and the third order dispersion which remain uncompensated. Simulation results without the nonlinear term in Eq. (7.9) indeed yields a quasi-null synchronization error (below 0.5%), even if the 3rd order dispersion is not matched.

7.4.2 Using a dispersion-shifted fiber (DSF)

Another alternative way for the reduction of dispersion effects over a fiber channel is to use a DSF in which the second order dispersion is set close to zero, without modifying the other properties of the fiber. This small value of the dispersion is due to the fact that this type of fiber is built adding some doped components so

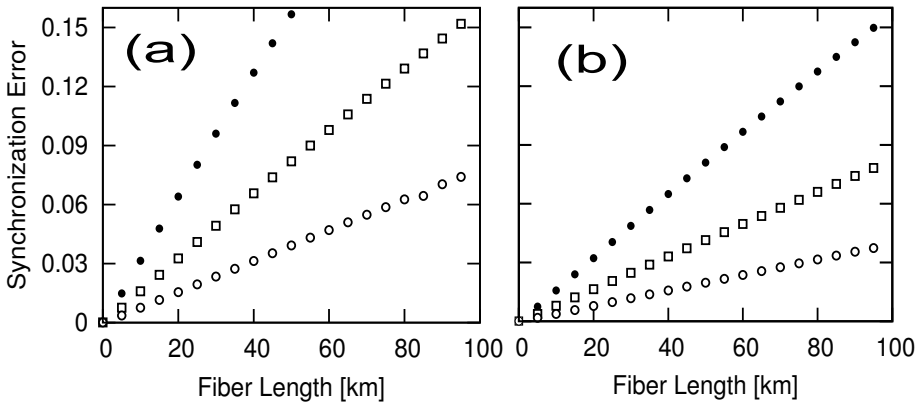


Figure 7.6: Numerical simulation using DSFs. The values used for the gains are $G = 2.5$ (∘), $G = 3.5$ (□), and $G = 5.0$ (•). (*a*) Synchronization error with the parameters $\beta_2 = 0.2$ ps^{2}km^{-1} and $\beta_3 = 0$. (*b*) Synchronization error with the parameters $\beta_2 = 0.1$ ps^{2}km^{-1} and β_3=0.1 ps^{3}km^{-1}.

that the zero-dispersion is shifted to or closer to the emitted wavelength, 1.55 μm, instead of being at 1.3 μm as it is the case for the standard fiber. The ideal case would be to have the zero-dispersion exactly at the emitted wavelength. But in practice this condition is rarely fulfilled and some small dispersion is still found out. The results obtained with this method are displayed in Fig. 7.6, showing the evolution of the synchronization error when a carrier is transmitted through a DSF. In Fig. 7.6 (a), the broadest chaotic spectrum ($G = 5.0$) is still distorted, so that the synchronization error reaches 15% after a propagation over $L \sim 50$ km, with $\beta_2 = 0.2$ ps^{2}km^{-1}. Operating in weak chaotic regime ($G = 2.5$), the signal is much less distorted since the synchronization error calculated after the propagation over 100 km is less than 9%. If one manages to reduce the value of β_2 (e.g. down to 0.1 ps^{2}km^{-1}), better synchronization is achieved as shown in Fig. 7.6(b), even when third order dispersion is considered (about 10% after 50 km, with the highest gain G). It can be noted that globally, the DSF compensation scheme is more efficient for lower gain values in Figs. 7.6 (a) and 7.6 (b); the optimum has therefore to be found between increased security (requiring strong hyperchaos and a broad spectrum through a high gain) and increased signal-to-noise ratio (requiring a minimization of the cancellation noise).

7.5 Experimental Results: Cancellation Noise Spectra

We have performed experimental measurements in order to evaluate the chaos cancellation level after propagation in optical fiber spools available in the laboratory. Chaos cancellation spectra measurements were chosen as indicators of the chaos

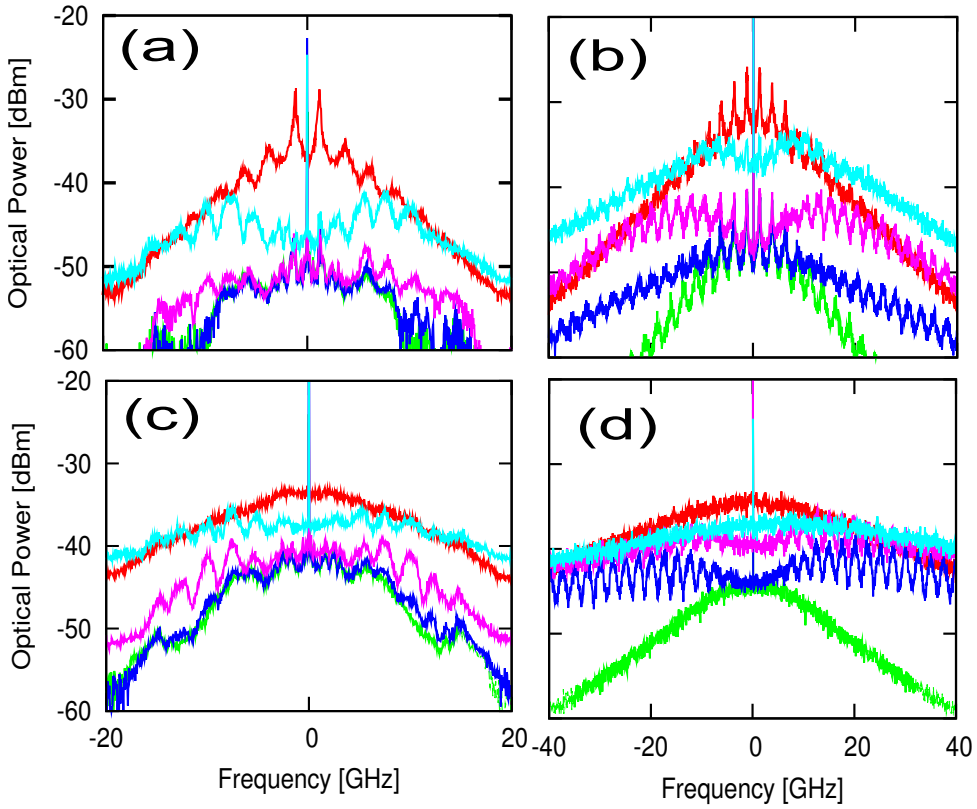


Figure 7.7: Experimental (a, c) and numerical (b, d) chaos cancellation spectra for transmission over standard SMF spools, with (a, b) $G = 2.5$ and (c, d) $G = 5.0$. Red: chaotic carrier; Green: back-to-back transmission; Blue: $L = 1$ km; Magenta: $L = 3$ km; Cyan: $L = 21$ km. The numerical results have been obtained considering a mismatch of 5% in τ and 10% in G.

communication link performance, in order to have a relevant comparison between experiment and theory. To improve the synchronization quality, additional 7.73 GHz low-pass filters (corresponding in the modeling to a slightly slower response time τ) have been added right after the photodiodes, as it is usually the case for 10 Gb/s data detection in optical communication networks. We expect thus that the width of the chaotic carrier is better matched to that of 10 Gb/s DPSK message spectrum (higher frequency chaotic spectral components would anyway not be useful for message masking at that bit rate). Our cancellation spectra are obtained with an optical spectrum analyzer (OSA) with 10 MHz resolution. For each chaos cancellation spectrum, we also recorded the corresponding chaotic spectrum without cancellation, so that the difference between the two situations can lead easily to the cancellation-to-chaos ratio in the spectral domain. It should be noted that the chaotic spectrum is obtained from the output of the cascaded PM while the cancellation spectra result from the receiver PM.

Figures 7.7 (a), (c) display several experimental cancellation spectra after propagation in standard SMFs. It is intended to evidence the degradation of chaos cancellation when dispersion effects grow with increase of the fiber length. As in Fig. 7.3, the parameters varied were the feedback loop gains and the fiber lengths. The numerical power spectral density of the optical field is shown in panels (b), (d). It is worth noting that experimental spectra decay faster than numerical ones because the experimental filter is of higher order. Figures 7.7 (a), (b) display the low gain case. A few peaks are easily recognizable in the carrier spectrum, thereby indicating that the full hyperchaotic regime (strong, flat, and broadband) has not been reached completely with such a gain. When the propagation length is low (0 and 1 km), the cancellation noise is globally higher than 20 dB (this figure can straightforwardly be considered as a kind of chaos-to-cancellation ratio). A degradation is observable when L is increased up to 3 km, and for a 21 km link, the chaotic carrier is not canceled at all beyond 7 GHz. For the highest achievable feedback gain $G = 5.0$ [Figure 7.7 (c)], the spectrum of the carrier is much smoother, as the full hyperchaotic regime is obtained. In this case, the cancellation performance is between 15 and 20 dB in the back-to-back configuration. However, the same degradation is witnessed as the fiber lengths increase. Hence, at this stage of the experimental study, it is clear that multi-Gb/s chaos cryptosystems cannot be operated in standard optical networks with SMFs beyond few kilometers without dispersion compensation, as the cancellation performance becomes severely degraded.

7.5.1 Using dispersion compensation modules (DCMs)

At the experimental level, we compensate the fiber dispersion through the utilization of DCMs. The principle of compensating with DCMs consists in propagating the carrier over a fiber length L_1, then launching it into the DCM which is adjusted so that the cancellation is the best possible. Even though DCMs are not exactly equivalent to the DCFs used in the numerical analysis in Sec. 7.4.1, the underlying physical mechanism is very similar, at least for the second order dispersion phenomena.

In Figs. 7.8 (a), (c), a tunable dispersion compensation module with a wide bandwidth and a large control tuning range is used (TDCM from Teraxion). Very good cancellation spectra is obtained by tuning DCM either to -360 ps/nm to compensate for a dispersion over 20 km of SMF or to -880 ps/nm for 50 km of SMF, independently of the feedback strength G. Typically, the use of DCMs is seen here as an excellent alternative at up to 50 km, as it enables to cancel almost completely the detrimental effects of fiber dispersion, with a weak penalty of the order of 1 dB (experimentally, the synchronization error, or equivalently the chaos can-

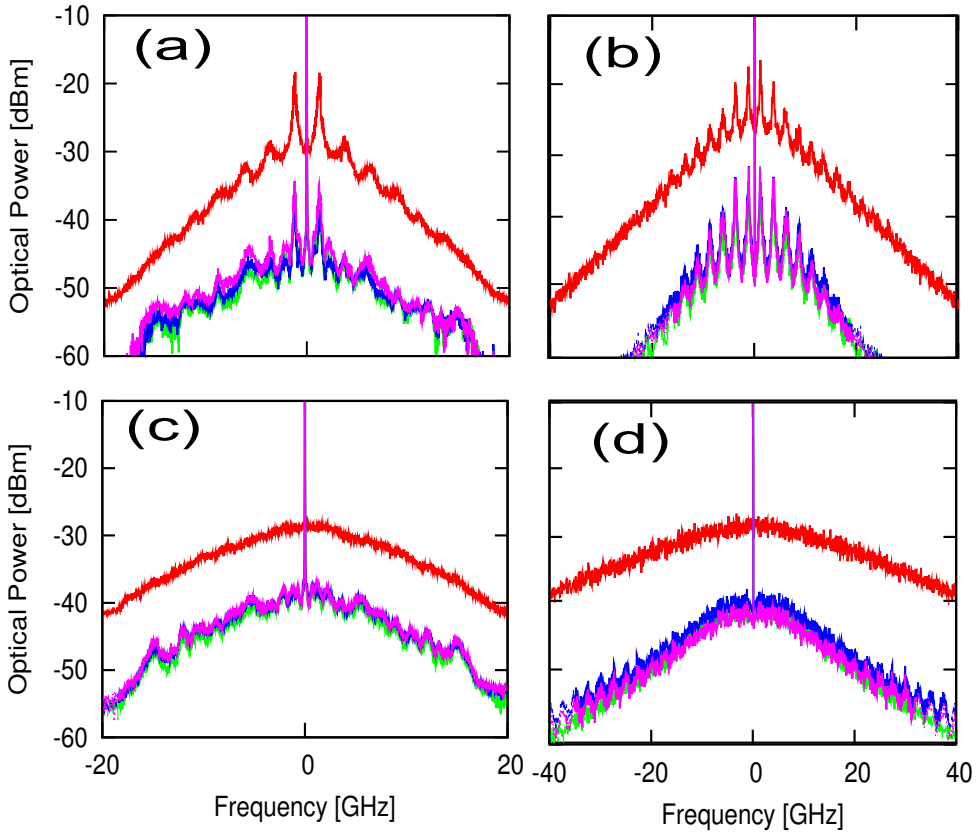


Figure 7.8: Experimental (a, c) and numerical (b, d) chaos cancellation spectra for transmission over SMF spools and using dispersion compensation. (a, b) $G = 2.5$ and (c, d) $G = 5.0$. Red: chaotic carrier; Green: back-to-back transmission, blue: $L = 20$ km of SMF; Magenta: $L = 50$ km of SMF. Numerical results has been obtained considering DCF as in Fig. 7.5 and a mismatch of 5% in τ and 10% in G.

cellation level, is mainly dominated by unavoidable residual parameter mismatch). For comparison the numerical spectra using a DCF with parameters as in Fig. 7.5 and considering a mismatch of 5% in τ and 10% in G is shown in Figs. 7.8 (b), (d). It should be noticed here that we can highlight an interesting issue of the dispersion sensitivity of phase chaos communication schemes. The use of DCM could indeed not only be efficient for channel dispersion compensation. Such modules could also be involved inside the phase chaos generation feedback loop, for introducing additional system complexity and security. The dispersion value set at the transmitter would thus represent an additional secret key as a physical parameter, which would be required at the receiver with the right value, in order to achieve the actual phase chaos cancellation and the decoding of the chaotic masking.

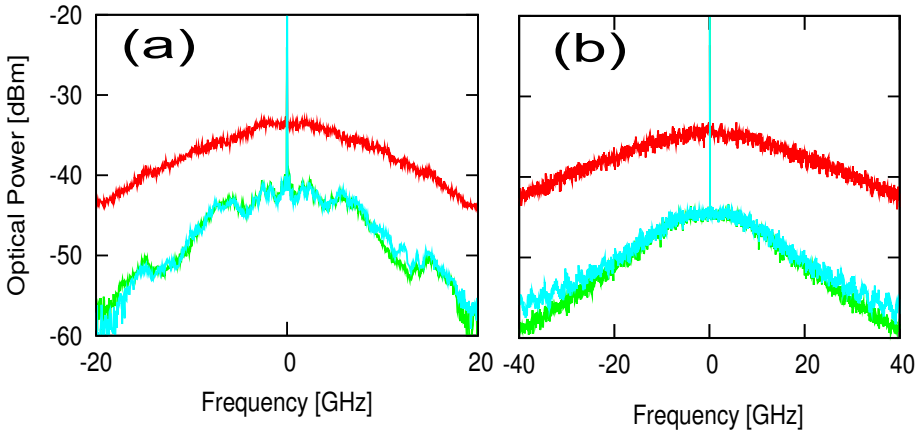


Figure 7.9: Experimental (a) and numerical (b) chaos cancellation spectrum for transmission over a 22 km-long DSF spool, with $G = 5.0$. Red: chaotic carrier; Green: back-to-back transmission; Cyan: $L = 22$ km. The numerical results has been obtained considering $\beta_2 = 0.1$ ps^{2}km^{-1}, β_3=0.1 ps^{3}km^{-1} and a mismatch of 5% in τ and 10% in G.

7.5.2 Using dispersion-shifted fibers (DSFs)

Another solution that can be experimentally implemented is to use DSFs, exactly as in the numerical analysis of Sec. 7.4.2. In Fig. 7.9, the measurement of DSF influence on transmission is reported. Though the operating wavelength (1562.0 nm) was slightly different from the zero-dispersion wavelength of the DSF fiber (1550.8 nm), dispersion was low enough so that after transmission over 22 km of fiber only small differences from the back-to-back case are seen in the cancellation spectrum. If compared with transmission over SMF without dispersion compensation [Fig. 7.7 (b)], equally small distortion of the cancellation spectrum is observed only for the 1 km SMF case, while the effects of longer fibers are significantly more pronounced.

7.6 Summary and Conclusions

We have led a joint theoretical and experimental study to investigate the detrimental effects of fiber propagation on the synchronization of an optical phase-chaos emitter-receiver system separated by several tens of km, and potentially operating up to 10 Gb/s. We have shown that when propagating in standard SMFs, the broadband chaotic carriers are drastically affected by chromatic dispersion, and message recovery is impossible beyond few kilometers. We have explored two classical methods of dispersion management, namely dispersion compensation fibers/modules and dispersion-shifted fibers, in order to evaluate their suitability for optical chaos cryptosystems. Both numerical and experimental results have shown that the can-

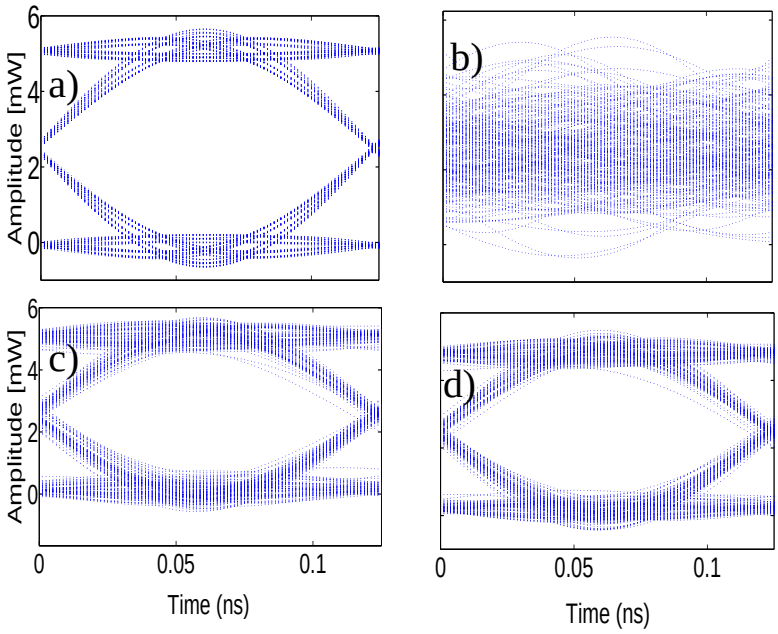


Figure 7.10: Numerical eye diagrams for (a) the original message and the recovered one $\mu_r(t)$ after propagation over (b) 21 km of SMF (as in Fig. 7.7), (c) 50 km of SMF and 5 km of DCF (as in Fig. 7.8) and (d) 55 km of DSF (as in Fig. 7.9).

cellation noise can be reduced down to the level of the back-to-back configuration. In particular, our experimental tests led with 20 km DSF, and 50 km of SMF+DCM have successfully reduced/compensated the fiber contribution and enabled a cancellation noise figure ranging from 10 to 20 dB. We have also found numerically that fiber channel nonlinear effects contributes up to a negligible percentage to the cancellation-to-chaos ratio, when proper dispersion compensation is achieved. This numerically found contribution is compatible with the actually obtained minimum experimental value of the cancellation-to-chaos ratio.

Finally, Fig. 7.10 shows the results of numerical simulations for the eye diagram of a 8 Gbs/s message decoded after propagation by a receiver with a mismatch of 5% in τ and 10% in G. The decoded message μ_R given by Eq. (7.12) is to be compared with the input message going through an equivalent detection scheme involving a MZI with delay δT_m. When fiber dispersion effects are compensated or a DSF is used the message can be clearly recovered. These results thereby indicate that our phase chaos cryptosystem can be integrated in standard optical fiber networks where such dispersion management schemes are actually implemented. Moreover dispersion sensitivity can be beneficial to enhance chaos communication security, through a secretly set DCM inside the chaos generation process.

Chapter 8

Opto-electronic Microwave Oscillator with Double Loop

8.1 Introduction

As stated in Sec. 1.4, OEOs are promising devices to generate stable and spectrally pure microwave signals. Despite its apparent advantage of being simple to construct, the original scheme presented by X. S.Yao and L. Maleki [79] has a major flaw: the long storage delay, responsible for the excellent spectral purity, defines closely spaced modes which are difficult to filter and hence degrade the overall performance. Several corrective routes have been proposed, the most widely known of which are an extremely narrow band intra-cavity microwave filter and a dual optoelectronic loop configuration and which considerably reduced the spurious peak sizes [152].

In this chapter we study an opto-electronic delay system with double loop for ultra-pure microwave generation [153]. As discussed herein the results show better performance regarding the microwave amplitude generation and the phase noise reduction than those already reported in the literature. The outline is as follows: In Sec. 8.2, we overview the main results obtained in OEO system with single loop. Sec. 8.3 we describe the system in detail. In Sec. 8.4 we derive the amplitude equation for double loop OEO. In Sec. 8.5 we perform the simulations to check the predicted steady states. Sec. 8.6 is dedicated to phase noise performance of both systems in comparison to the single loop OEO. Sec. 8.7 concludes the chapter.

8.2 Opto-electronic Microwave Oscillator with a Single Loop

To better appreciate the usefulness of opto-electronic microwave oscillator with double loop, we first study in this section the equivalent of such system with a single loop. It is schematically presented in Fig. 8.1 (a) [81], which is similar to the intensity chaos generator presented in Sec. 3.1 without the message and with an additional component (narrow passband filter) serving to select the microwave frequency while filtering out all other frequencies [compare Fig. 8.1 (a) to Fig. 2.4].

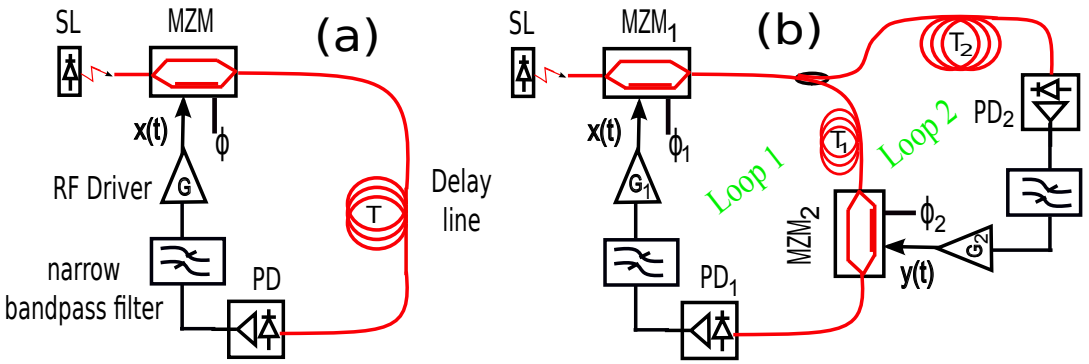


Figure 8.1: Setup: SL: semiconductor laser, MZM: Mach-Zehnder modulator, PD: photodiode, (a) OEO with single loop, (b) OEO with double loop.

The characteristics of the narrow band filter are its central frequency $\Omega_0/2\pi$ and its -3 dB bandwidth $\Delta\Omega/2\pi$. Proceeding as in Sec. 2.2 the dynamics of the microwave oscillation can be described in term of the usual dimensionless variable $x(t)$ as

$$x + \tau\frac{dx}{dt} + \frac{1}{\theta}u = G\cos^2\left[x(t-T)+\phi\right], \tag{8.1}$$

$$\frac{du}{dt} = x, \tag{8.2}$$

where $G = \pi S G_0 P_0 \eta_0/2V_{\pi RF}$ is the normalized feedback gain, $\phi = \pi V_B/2V_{\pi DC}$ is the Mach-Zehnder offset phase and $\tau = 1/\Delta\Omega$ and $\theta = \Delta\Omega/\Omega_0^2$ are the characteristic timescale parameters of the bandpass filter. Usually in these systems a long fiber delay is required to store the energy (typically one uses 4 km of fiber length corresponding to $T = 20$ μs). Since the ratio between the fastest and slowest dynamical timescales τ/θ is in the order of 10^7 and because of the large delay time, one needs a lot of memory to compute Eqs. (8.1) and (8.2). One option to get around was introduced by Y. K. Chembo *et al.* [81]. It consists in deriving the microwave amplitude equation from Eqs. (8.1) and (8.2) taking advantage of some features of the system. In fact, as the filter is narrowly resonant around the central frequency $\Omega_0/2\pi$, the filter output can be written in term of slowly varying amplitude $\mathcal{A}(t) = Ae^{i\psi(t)}$ as

$$x(t) = \frac{1}{2}\mathcal{A}(t)e^{i\Omega_0 t} + cc \equiv A(t)\cos\left[\Omega_0 t + \psi(t)\right], \tag{8.3}$$

where 'cc' stands for the complex conjugate, $A(t)$ is the modulus of the slowly varying amplitude $\mathcal{A}(t)$ while $\psi(t)$ stands for its slow varying phase. As was done in [81], the expression of $x(t)$ given by Eq. (8.3) can be used to simplify the nonlinear term $\cos^2\left[x(t-T)+\phi\right]$. Thus, one can Fourier-expand it in harmonics of Ω_0 using

the Jacobi-Anger expansion

$$e^{iz\cos\alpha} = \sum_{q=-\infty}^{\infty} i^q \mathcal{J}_q(z) e^{iq\alpha}, \tag{8.4}$$

where $\mathcal{J}_q$ are the qth-order Bessel functions of the first kind being q an integer. Then

$$\cos^2\left[x(t-T)+\phi\right] = \frac{1}{2} + \frac{1}{2}\mathcal{J}_0\left(2A_T\right)\cos 2\phi + \frac{1}{2}\sum_{q=1}^{\infty} i^q \mathcal{J}_q\left(2A_T\right)\cos(q\Omega_0 t - q\Omega_0 T + q\psi_T)\left[e^{2i\phi} + (-1)^q e^{-2i\phi}\right]. \tag{8.5}$$

Although an infinite number of frequencies besides the fundamental ($q = 1$) can be generated during the modulation at the output of MZM$_1$, they are all discarded by the filter. Thus disregarding all the spectral components except the fundamental harmonic in Eq. (8.5), Eq. (8.1) can be rewritten as

$$x + \tau\frac{dx}{dt} + \frac{1}{\theta}u = -\frac{1}{2}G\sin 2\phi\,\mathcal{J}_1\left(2A_T\right)e^{i(\Omega_0 t - \Omega_0 T + \psi_T)} + cc. \tag{8.6}$$

For further simplifications it is mathematically convenient to write the integral as

$$u(t) = \frac{1}{2}\mathcal{U}(t)e^{i\Omega_0 t} + cc, \tag{8.7}$$

where $\mathcal{U}(t)$ is a slowly varying amplitude and neglecting $\ddot{\mathcal{U}}$ as compared to $\Omega_0\dot{\mathcal{U}}$. Here the dot here stands for the derivative. Thus by making use of Eq. (8.2), the left hand side of Eq. (8.1) can be written as

$$\frac{du}{dt} + \frac{1}{\Delta\Omega}\frac{d^2u}{dt^2} + \frac{\Omega_0^2}{\Delta\Omega}u \approx \frac{1}{2}\left[\left(1 + 2i\frac{\Omega_0}{\Delta\Omega}\right)\dot{\mathcal{U}}(t) + i\Omega_0\mathcal{U}(t)\right]e^{i\Omega_0 t} + cc. \tag{8.8}$$

By deriving Eq. (8.7), it turns out that $\mathcal{A} = \dot{\mathcal{U}} + i\Omega_0\mathcal{U} \simeq i\Omega_0\mathcal{U}$. Therefore the left hand side of Eq. (8.1) can be written as

$$\frac{1}{2}\left[\left(\frac{2}{\Delta\Omega_1} - \frac{i}{\Omega_0}\right)\dot{\mathcal{A}}(t) + \mathcal{A}(t)\right]e^{i\Omega_0 t} + cc. \tag{8.9}$$

Thus Eq. (8.6) becomes

$$\dot{\mathcal{A}} + \mu e^{iv}\mathcal{A} = -G\sin 2\phi e^{iv}e^{-i\Omega_0 T}\mathcal{J}_{C1}\left(2A_T\right)\mathcal{A}_T, \tag{8.10}$$

where $\mathcal{J}_{C1}(x)$ is the Bessel Cardinal function defined as $\mathcal{J}_{C1}(x) = \mathcal{J}_1(x)/x$. Other introduced parameters are

$$Q = \frac{\Omega_0}{\Delta\Omega}; \qquad \mu = \frac{\Delta\Omega/2}{\sqrt{1 + \left[1/(2Q)\right]^2}}; \qquad v = \arctan\left[\frac{1}{2Q}\right], \tag{8.11}$$

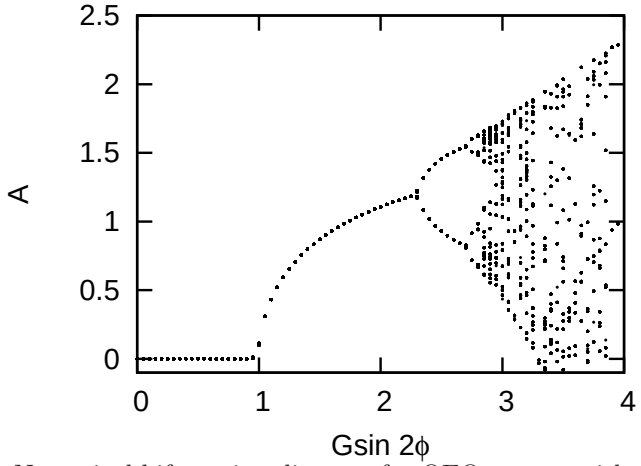


Figure 8.2: Numerical bifurcation diagram for OEO system with a single loop.

where Q is the quality factor of the selective RF filter and μ and v act as the parameters of the effective filter. For high quality factor (typically $Q \sim 200$), $\mu \simeq \Delta\Omega/2$. Thus the effective bandwidth is $\mu \simeq \Delta\Omega/4\pi$. The quantity $\Omega_0 T$ is the round-trip phase shift accumulated along the oscillation loop. Typically the system operates in the phase matching condition $e^{-i\Omega_0 T} = \pm 1$. Here we choose $e^{-i\Omega_0 T} = -1$ so that microwave generation takes place for $\sin 2\phi > 0$. When considering $e^{-i\Omega_0 T} = +1$ the microwave generation takes place for $\sin 2\phi < 0$.

8.2.1 Steady state solutions

Pure microwaves of constant amplitude correspond to stable fixed points of Eq. (8.10). Thus, for $\dot{A} = 0$, $A^{st} = 0$ is a trivial fixed point while

$$A^{st} = \mathcal{J}_{C1}^{-1}\left[\frac{1}{2G\sin 2\phi}\right], \tag{8.12}$$

is the non-trivial fixed point which exists only for $G\sin 2\phi > 1$. In [81], the authors demonstrated that the trivial fixed point is stable for $G\sin 2\phi < 1$ while the non-trivial steady state solution is stable for $1 < G\sin 2\phi < 2.31$. Figure 8.2 shows the bifurcation diagram obtained by displaying the maxima and the minima extracted by simulating Eq. (8.10). This bifurcation diagram shown in Fig. 8.2 is in full agreement with that of [81]. Furthermore, one can notice that stable microwaves can be generated with amplitudes in the range [0, 1.2] corresponding to the feedback strength $1 < G\sin 2\phi < 2.31$. For $G\sin 2\phi > 2.31$, the amplitude undergoes an oscillatory instability [81].

8.2.2 Stochastic phase equation

The noise can be taken into account in the amplitude equation through making use of Langevin formalism, that is, in adding noise sources to a core deterministic model for the microwave dynamics [94]. Two main noise contributions are to be considered,

- additive noise which results from noisy nature of different components such as photodiode, amplifier, etc.. For each loop, it is considered to be spectrally white. Around the central frequency Ω_0, it can be written as

$$\xi(t) = \frac{1}{2}\xi_a(t)e^{i\Omega_0 t} + \frac{1}{2}\xi_a^*(t)e^{-i\Omega_0 t}, \tag{8.13}$$

  where $\xi_a(t)$ is the complex Gaussian white noise with correlation $\langle \xi_a(t)\xi_a^*(t')\rangle = 4D_a\delta(t-t')$ corresponding to the power density $|\xi(\omega)|^2 = 2D_a$.

- multiplicative noise: It results from the overall gain fluctuations. It has in general a non trivial structure since it is composed from very different noise contributions. It can be assumed as flicker near the carrier and white above a certain knee-value as it has been observed in experiments [94]. The multiplicative noise can be taken into account in the loops by adding a small perturbation term to the overall loop gain, e.g. $G + \delta G$. Thus if we consider dimensionless multiplicative noise $\eta_m(t) = \delta G/G$, its empirical noise power density can be considered as

$$|\eta_m(\omega)|^2 = 2D_m\left[1 + \frac{\Omega_H}{\omega + \Omega_L}\right], \tag{8.14}$$

  where Ω_L and Ω_H are the low and the high corner frequency, respectively.

Thus taking into account the noise terms, the stochastic equation for the slowly varying amplitude can be written from Eq. (8.10) as

$$\dot{\mathcal{A}} + \mu e^{iv}\mathcal{A} = -G\sin 2\phi e^{iv}e^{-\Omega_0 T}\left[1+\eta(t)\right]\mathcal{J}_{C1}\left(2A_T\right)\mathcal{A}_T + \mu e^{iv}\xi_a. \tag{8.15}$$

Since $\mathcal{A} = Ae^{i\psi}$, Eq. (8.15) can be rewritten as

$$\begin{aligned}\dot{A} + i\dot{\psi}A &= -\mu e^{iv}A + 2\mu G\sin 2\phi J_{C1}\left(2A^{st}\right) \\ &\quad \times\left[1+\eta_m(t)\right]A_T e^{i(\psi_T-\psi+v)} + \mu e^{iv}\xi_a'(t),\end{aligned} \tag{8.16}$$

where $\xi_a'(t) = e^{-i\psi}\xi_a$ is a complex Gaussian white noise with the mean zero and the same variance as ξ_a, e.g. $\langle \xi_a'(t)\xi_a'^*(t')\rangle = 4D_a\delta(t-t')$. From Eq. (8.16), the stochastic phase equation can be written as

$$\dot{\psi} = -\mu\sin v + 2\mu G\sin 2\phi J_{C1}\left(2A^{st}\right)\left[1+\eta_m(t)\right]\frac{A_T}{A}\sin(\psi_T - \psi + v) + \mu\frac{\zeta_\psi(t)}{A^{st}}, \tag{8.17}$$

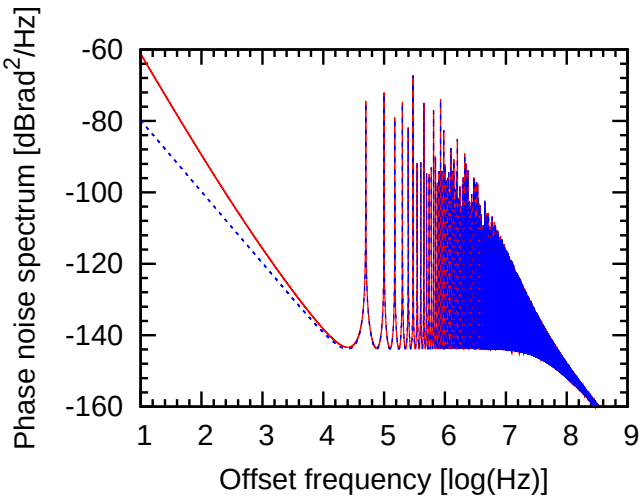


Figure 8.3: Theoretical phase noise spectrum of the opto-electronic microwave oscillator with single loop considering the multiplicative noise as flicker (solid line) or white (dashed line) for $A = 0.41$.

where $\zeta_\psi(t) = \xi'_{a,Re}(t)\sin v + \xi'_{a,Im}(t)\cos v$ is a real Gaussian white noise with zero mean and variance as that of $\xi(t)$ e.g. $\langle \zeta_\psi(t)\zeta^*_\psi(t')\rangle = 2D_a\delta(t-t')$. The sub-indexes Re and Im refer to the real and imaginary parts of $\xi'_\psi(t)$, respectively. As discussed in Sec. 1.4, we assume the fluctuations on the amplitude are of the second order meaning that we can assume $A(t) \backsimeq A(t-T) \backsimeq A^{st}$. Thus by further considering that the phase fluctuations evolves so that $\sin(a-b) \approx a-b$, which is typically the case for the OEOs studied here, Eq. (8.17) becomes

$$\dot{\psi} = \mu\left(\psi_T - \psi\right) + \frac{\mu}{2Q}\eta_m(t) + \mu\frac{\zeta_\psi}{A^{st}}. \tag{8.18}$$

Since Eqs (8.49) is linear, the phase noise spectrum in the whole frequency range can be obtained from the squared modulus of its Fourier transform. Thus considering that all noise sources are uncorrelated, the Fourier transforms $\Psi(\omega)$ of the phase $\psi(t)$ can be written as

$$|\Psi(\omega)|^2 = \frac{\dfrac{\mu^2}{4Q^2}|\eta_m(\omega)|^2 + \dfrac{2\mu^2}{|A^{st}|^2}D_a}{|i\omega + \mu(1-e^{-i\omega T})|^2}. \tag{8.19}$$

As already stated, Eq. (8.19) shows that the phase noise spectrum depends on the delay time T, on the quality factor Q and also on the bandwidth μ. Figure 8.3 displays such spectrum considering two cases: the case for which the multiplicative noise is taken as a white noise (dashed line) and the one for which it is considered as a flicker noise (solid case). We have taken the following parameter values $D_m = 5.0\times10^{-11}$ rad^2/Hz, $D_a = D_{a2} = 9.0\times10^{-16}$ rad^2/Hz, $\Omega_H = 100$ MHz, $\Omega_L = 1$ Hz,

$\mu = 50\pi$ MHz, $Q = 200$ and $A^{st} = 0.41$. The results show that the phase noise is around -60 dBrad^2/Hz at 10 Hz when considering the multiplicative noise as a flicker while it is around -80 dBrad^2/Hz at 10 Hz considering the multiplicative noise as a white noise. In both cases the phase noise is around -150 dBrad^2/Hz at 50 KHz. Beyond this frequency, the first spurious peak appears followed by other spurious peaks at the integer multiples of the round-trip frequency 50 kHz. The first spurious peak located around $1/T$ has a height of about 60 dB. We should note that the results obtained with a flicker noise agree better with experimental results [94] than those obtained with a white noise.

8.3 Opto-electronic Microwave Oscillator with Double Loop

The system under study is organized in a double delay feedback loop as shown in Fig. 8.1 (b). The first loop, which is reminiscent from the initial loop structure, consists in a semiconductor laser (SL) injecting light into a Mach-Zehnder modulator (MZM_1) which receives electrical signals $V(t)$ and V_B in its radio-frequency (RF) and DC voltage electrodes, respectively. The output of MZM_1 can be written as

$$E_1(t) = \frac{E_0}{2}\Big\{1 + e^{2i[x(t)+\phi_1]}\Big\}, \tag{8.20}$$

where E_0 is the SL output amplitude, $x(t) = \pi V_1(t)/(2V_{\pi RF})$ is the dimensionless voltage, $\phi_1 = \pi V_{B,1}/(2V_{\pi_{DC}})$ is the offset phase and $V_{\pi RF}$ and $V_{\pi Dc}$ stand for the RF half-wave and the bias electrode half-wave, respectively. Subsequently, $E_1(t)$ is split into two parts. One part is delayed by a time T_2 and then converted into an electrical signal via the photodiode PD_2. The output of PD_2, $|E_1(t-T_2)|^2$, is fed to a narrow band filter with a central -3 dB frequency $\Omega_0'/2\pi$ having bandwidth $\Delta\Omega_2/2\pi$, and after amplification is applied as voltage $V_2(t)$ to MZM_2 RF electrode. The narrow filter eliminates all the harmonics except the fundamental one. The second part of $E_1(t)$ is launched into an optical delay line and then fed to MZM_2 whose output

$$E_2(t) = \frac{E_1(t-T_1)}{2}\Big\{1 + e^{2i[y(t)+\phi_2]}\Big\}, \tag{8.21}$$

is detected by PD_1. Here $y(t) = \pi V_2(t)/(2V_{\pi RF})$ and $\phi_2 = \pi V_{B,2}/(2V_{\pi_{DC}})$. The electrical signal $|E_2(t)|^2$ is fed to another narrow band microwave RF filter of central frequency $\Omega_0/2\pi$ with -3 dB bandwidth $\Delta\Omega_1/2\pi$ and then is fed to MZI_1 RF electrode after amplification. In this scheme the MZM_1 optical output plays a double role. On one hand it becomes, after the delay time T_1, the optical input of MZM_2 and on the other hand, after a delay T_2 it is used to drive RF electrode of MZM_2.

Proceeding as in Sec. 2.2 , it can be demonstrated that the system shown in Fig. 8.1 (b) can be described by the dimensionless amplifier outputs $x(t)$ and $y(t)$ as follows

$$x + \frac{1}{\Delta\Omega_1}\frac{dx}{dt} + \frac{\Omega_0^2}{\Delta\Omega_1}u_1 = \frac{|E_2(t)|^2}{|E_0|^2}G_1 \tag{8.22}$$
$$= \frac{G_1}{4}\Big[F(x_{T_1},\phi_1) + F(y,\phi_2) + F(x_{T_1},\phi_1)F(y,\phi_2) + 1\Big],$$
$$y + \frac{1}{\Delta\Omega_2}\frac{dy}{dt} + \frac{\Omega_0'^2}{\Delta\Omega_2}u_2 = \frac{|E_1(t-T_2)|^2}{|E_0|^2}G_2 = \frac{G_2}{2}[F(x_{T_2},\phi_1) + 1], \tag{8.23}$$
$$\frac{du_1}{dt} = x, \tag{8.24}$$
$$\frac{du_2}{dt} = y, \tag{8.25}$$

where $x_{t_0} = x(t-t_0)$, $F(x,\phi) = \cos[2x(t) + 2\phi]$ and G_1 and G_2 are the overall loop gains. The integral variables u_j $(j = 1, 2)$ impose the mean value of $x(t)$ and $y(t)$ to be zero in the stationary regimes.

8.4 Amplitude Equation for a Double Loop Opto-electronic Oscillator

We assume identical filters, narrowly resonant around the central frequency $\Omega_0'/2\pi = \Omega_0/2\pi$ so that any harmonic different to the fundamental one is filtered out. Thus the output of each amplifier oscillates at the central frequency Ω_0. Therefore $x(t)$ and $y(t)$ can be written in terms of slowly varying amplitudes $\mathcal{A}(t) = Ae^{i\psi(t)}$ and $\mathcal{B}(t) = Be^{i\varphi(t)}$ as

$$x(t) = \frac{1}{2}\mathcal{A}(t)e^{i\Omega_0 t} + cc \equiv A(t)\cos[\Omega_0 t + \psi(t)], \tag{8.26}$$
$$y(t) = \frac{1}{2}\mathcal{B}(t)e^{i\Omega_0 t} + cc \equiv B(t)\cos[\Omega_0 t + \varphi(t)]. \tag{8.27}$$

Through these expressions of $x(t)$ and $y(t)$, the functions F in the right hand side of Eqs. (8.22) and (8.23) can be, as before, approximated using the Jacobi-Anger expansion. Then by discarding all the spectral components of the signal except the fundamental harmonic, we have

$$F(x_{T_2},\phi_1) = -\sin 2\phi_1 \mathcal{J}_1(2A_{T_1})\, e^{i\left(\Omega_0 t - \Omega_0 T_1 + \psi_{T_1}\right)} + cc. \tag{8.28}$$

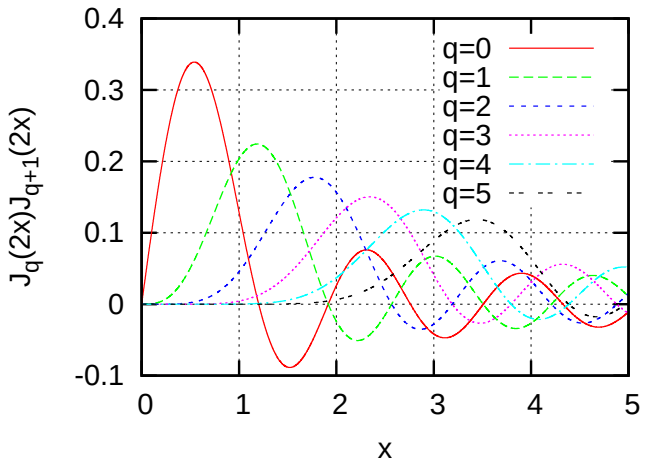


Figure 8.4: Product of Bessel functions $J_q(2x)J_{q+1}(2x)$ versus argument x for different values of q.

and

$$F(x_{T_1},\phi_1)F(y,\phi_2) = -\frac{1}{2}\sum_{q=-\infty}^{\infty} \mathcal{J}_q\left(2A_{T_1}\right)\mathcal{J}_{-q+1}\left(2B\right)e^{i\left[\Omega_0 t - q\Omega_0 T_1 + q\psi_{T_1} + (-q+1)\varphi\right]}$$
$$- \mathcal{J}_q\left(2A_{T_1}\right)\mathcal{J}_{-q-1}\left(2B\right)e^{-i\left[\Omega_0 t + q\Omega_0 T_1 - q\psi_{T_1} + (q+1)\varphi\right]}$$
$$\times\Big\{\sin(2\phi_1+2\phi_2) - (-1)^q\sin(2\phi_1-2\phi_2)\Big\}. \tag{8.29}$$

Equation (8.4) can be truncated since the Bessel functions decrease faster to zero as the order q increases. Figure 8.4 shows the product $\mathcal{J}_q(2x)\mathcal{J}_{q+1}(2x)$ (where $q = 1,..,5$) as a function of x. It turns out that, for any argument smaller than 4 (corresponding to microwave amplitude smaller than 2) the Bessel functions of order 6 or greater can be neglected.

To derive the equations for the complex amplitudes $\mathcal{A}$ and $\mathcal{B}$ we have to consider the spectral components in $e^{i\Omega_0 t}$ in the left hand side of Eqs. (8.22) and (8.23). To do that, as in Sec. 8.2 for a single loop, we consider

$$u_k(t) = \frac{1}{2}\mathcal{U}_k(t)e^{i\Omega_0 t} + cc, \tag{8.30}$$

where $\mathcal{U}_k(t)$ is a slowly varying amplitude and neglecting $\ddot{\mathcal{U}}_k$ as compared to $\Omega_0\dot{\mathcal{U}}_k$ where the dot here stands for the derivative, the left hand side of Eqs. (8.22) and (8.23) can be written as

$$\frac{du_k}{dt} + \frac{1}{\Delta\Omega_k}\frac{d^2u_k}{dt^2} + \frac{\Omega_0^2}{\Delta\Omega_k}u_k \approx \frac{1}{2}\left[\left(1+2i\frac{\Omega_0}{\Delta\Omega_k}\right)\dot{\mathcal{U}}_k(t) + i\Omega_0\mathcal{U}_k(t)\right]e^{i\Omega_0 t} + cc. \tag{8.31}$$

By deriving Eq. (8.30), it turns out that $\mathcal{A} = \dot{\mathcal{U}}_1 + i\Omega_0\mathcal{U}_1 \simeq i\Omega_0\mathcal{U}_1$. Therefore the LHS of Eq. (8.22) can be written as

$$\frac{1}{2}\left[\left(\frac{2}{\Delta\Omega_1} - \frac{i}{\Omega_0}\right)\dot{\mathcal{A}}(t) + \mathcal{A}(t)\right] e^{i\Omega_0 t} + cc, \tag{8.32}$$

and similarly for the left hand side of Eq. (8.23) in terms of $\mathcal{B}$.

Finally, collecting all fundamental harmonic terms, the equations for slowly varying envelopes $\mathcal{A}(t)$ and $\mathcal{B}(t)$ can be written as

$$\dot{\mathcal{A}} + \mu_1 e^{iv_1}\mathcal{A} = -\frac{1}{2}\mu_1 e^{iv_1} G_1 \Big\{ \sin 2\phi_2 \mathcal{J}_1(2B) e^{i\varphi} + \sin 2\phi_1 \mathcal{J}_1(2A_{T_1}) e^{i\psi_{T_1}} e^{-i\Omega_0 T_1} + \cos 2\phi_1 \sin 2\phi_2 \sum_{p=-2}^{2} \mathcal{C}_{2p} + \sin 2\phi_1 \cos 2\phi_2 \sum_{p=-2}^{2} \mathcal{C}_{1-2p} \Big\}, \tag{8.33}$$

$$\dot{\mathcal{B}} + \mu_2 e^{iv_2}\mathcal{B} = -\mu_2 e^{iv_2} G_2 \sin 2\phi_1 \mathcal{J}_1(2A_{T_2}) e^{i(\psi_{T_2} - \Omega_0 T_2)}, \tag{8.34}$$

where we have introduced

$$\mathcal{C}_q = \mathcal{J}_q(2A_{T_1})\mathcal{J}_{1-q}(2B) e^{i\left[-q\Omega_0 T_1 + q\psi_{T_1} + (1-q)\varphi\right]}, \tag{8.35}$$

and the parameters

$$Q_k = \frac{\Omega_0}{\Delta\Omega_k};\ \mu_k = \frac{\Delta\Omega_k}{\sqrt{4 + Q_k^{-2}}};\ v_k = \arctan\left[\frac{1}{2Q_k}\right]. \tag{8.36}$$

For oscillations to be sustained the phase matching conditions should be fulfilled, $e^{-i\Omega_0 T_k} = \pm 1$. The matching condition $e^{-i\Omega_0 T_1} = +1$ is equivalent to $e^{-i\Omega_0 T_1} = -1$ by changing ϕ_1 by $-\phi_1$ and $\varphi(t)$ by $\varphi(t) + \pi$. Similarly $e^{-i\Omega_0 T_2} = \pm 1$ are equivalent changing ϕ_2 by $-\phi_2$ and $\psi(t)$ by $\psi(t) + \pi$. Therefore without loss of generality we will consider $e^{-i\Omega_0 T_1} = -1$ and $e^{-i\Omega_0 T_2} = +1$.

Fix points are given by $\dot{\mathcal{A}} = \dot{\mathcal{B}} = \dot{\psi} = \dot{\varphi} = 0$. From Eq. (8.34), we have

$$B^{st} = -G_2 \sin 2\phi_1 \mathcal{J}_1(2A^{st}) e^{i(\psi^{st} - \varphi^{st})}. \tag{8.37}$$

Since B^{st} is a real positive quantity, the imaginary exponent has to be either 0 or π depending on the sign of $\sin 2\phi_1$ and $\mathcal{J}_1(2A^{st})$. There are two options: $\psi^{st} = \varphi^{st}$ (*Case I*) corresponding to in-phase microwave emission and $\psi^{st} = \varphi^{st} + \pi$ (*Case II*), out-of-phase microwave emission. Since the amplitude of the microwave emission is small enough so that $\mathcal{J}_1(2A^{st})$ remains positive, to have a positive B^{st} for Case I $\phi_1 \in [-\pi/2, 0]$ while for Case II $\phi_1 \in [0, \pi/2]$.

From Eq. (8.33) we have

$$A^{st} = \frac{G_1}{2}\mathbf{H}_{\pm}(\phi_1, \phi_2), \tag{8.38}$$

where

$$\begin{aligned}\mathbf{H}_{\pm}(\phi_1,\phi_2) =& \sin 2\phi_1 \mathcal{J}_1(2A^{st}) \mp \sin 2\phi_2 \mathcal{J}_1\left(2B^{st}\right) \\ & \mp \cos 2\phi_1 \sin 2\phi_2 \sum_{p=-2}^{2} \mathcal{J}_{2p}(2A^{st})\mathcal{J}_{1-2p}(2B^{st}) \\ & + \sin 2\phi_1 \cos 2\phi_2 \sum_{p=-2}^{2} \mathcal{J}_{1-2p}(2A^{st})\mathcal{J}_{2p}(2B^{st}). \end{aligned} \tag{8.39}$$

$\mathbf{H}_+$ corresponds to *Case I* while $\mathbf{H}_-$ to *Case II*. Since $H_-(\phi_1,\phi_2) = H_+(\phi_1,-\phi_2)$ the mathematical fixed points that satisfy $\psi^{st} = \varphi^{st}$ (Case I) are exactly the same as the ones obtained for Case II with the opposite ϕ_2. However, for Case I only the solutions with $\phi_1 \in [-\pi/2, 0]$ are physical while for Case II the physical solutions correspond to $\phi_1 \in [0, \pi/2]$. Notice that since off-set phases appear in Eqs. (8.37) and (8.38) as $2\phi_1$ and $2\phi_2$ it is enough to explore the interval $[-\pi, \pi]$ for both phases.

The trivial solution $A^{st} = B^{st} = 0$ is always present. As for nontrivial solutions we first notice that for $G_2 = 0$, $B^{st} = 0$ and, since $\mathcal{J}_q(0) = 0$ for $q \neq 0$, the system is equivalent to a single loop OEO with gain $G_1(1 + \cos 2\phi_2)/2$. In this case the non-trivial solution exists only for $G_1 > G_1^{th} = 2/\sin 2\phi_1(1 + \cos 2\phi_2)$ [82].

We can in fact obtain an analytical approximation close to threshold for microwave emission since A^{st} and B^{st} are small and Eqs. (8.37) and (8.38) can be expanded in series. For Case II one gets

$$A^{st} = \frac{G_1}{2}\left[g_1 A^{st} - \frac{g_2}{2} A^{st3}\right], \tag{8.40}$$

where

$$g_1 = \sin 2\phi_1[1 + \cos 2\phi_2 + G_2 \sin 2\phi_2(1 + \cos 2\phi_1)] \tag{8.41}$$

$$\begin{aligned} g_2 =& \sin 2\phi_1[1 + \cos 2\phi_2 + G_2 \sin 2\phi_2(1 + 4\cos 2\phi_1)], \\ & + \sin^3 2\phi_1[3G_2^2 \cos 2\phi_2 + G_2^3 \sin 2\phi_2(1 + \cos 2\phi_1)]. \end{aligned} \tag{8.42}$$

The non trivial solution is

$$A^{st} = \sqrt{\frac{2}{g_2}\left(g_1 - \frac{2}{G_1}\right)}. \tag{8.43}$$

The threshold for out-of-phase microwave emission is given by $G_1 g_1 = 2$. The threshold for in-phase microwave emission is the same since g_1 depends only on $\cos 2\phi_2$. For $\phi_1 \in [-\pi/2, 0]$ the physical solution is the in-phase one while for $\phi_1 \in [0, -\pi/2]$.

For arbitrary values of the gains G_1 and G_2 Eqs. (8.37) and (8.38) are solved numerically to determine the stationary amplitudes. Figure 8.5 displays the region

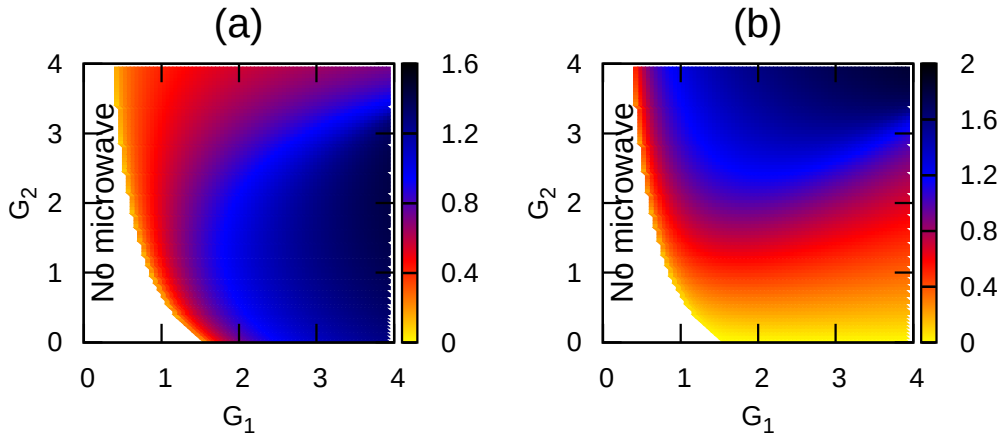


Figure 8.5: Non-zero stationary solution given by Eqs. (8.37) and (8.38) with H_{-}. (a) A^{st} and (b) B^{st} displayed in (G_1, G_2)-plane considering $\phi_1 = 0.5$ and $\phi_2 = 0.5$

of existence and the amplitude of out-of-phase microwave emission obtained from Eqs. (8.37) and (8.38) with H_{-} in (G_1, G_2)-plane considering $\phi_1 = 0.5$ and $\phi_2 = 0.5$. For small values of G_1 the non-trivial stationary solution does not exist. The range of values of G_1 for which the non-trivial solution exists widens as G_2 increases. Besides the values of A^{st} and B^{st} can be high as 1.2 and 2.0 respectively.

We now address the dependence of microwave emission as function of the offset phases ϕ_1 and ϕ_2. Figure 8.6 displays the out (in)-of-phase microwave emission amplitude obtained from Eqs. (8.37) and (8.38) with H_{-} in the (ϕ_1, ϕ_2) parameter space considering $G_1 = 2.5$ and $G_2 = 2.5$. The contour of the region of microwave emission can be determined by the threshold condition $G_1 g_1 = 2$. For $\phi_1 \in [-\pi/2, 0]$ the physical solution is the in-phase one while it is in the in-of-phase for $\phi_1 \in [0, \pi/2]$. The offset phases ϕ_1 and ϕ_2 play a very relevant role in determining the existence and amplitude of the microwave emission. Depending on ϕ_1 and ϕ_2 the non-trivial steady state may have a large amplitude signaling a strong microwave emission or may even not exist (no microwave emission). The large amplitudes are associated to an effective constructive interference of the two delay loops while the parameter regions where no microwave emission takes place are associated to destructive interference.

The results of this section has been obtained with the phase matching $e^{-i\Omega_0 T_1} = -1$ and $e^{-i\Omega_0 T_2} = 1$. For $e^{-i\Omega_0 T_1} = -1$ and $e^{-i\Omega_0 T_2} = -1$ the results are the same since the in-phase solution for a given ϕ_2 corresponds in our phase matching to the out-of-phase solution for $-\phi_2$, which is the in-phase solution for ϕ_2. For $e^{-i\Omega_0 T_1} = 1$ and $e^{-i\Omega_0 T_2} = \pm 1$ the regions of in-phase and out-of-phase microwave emission in parameter space would be the same as here but changing ϕ_1 by $-\phi_1$ and ϕ_2 by $-\phi_2$.

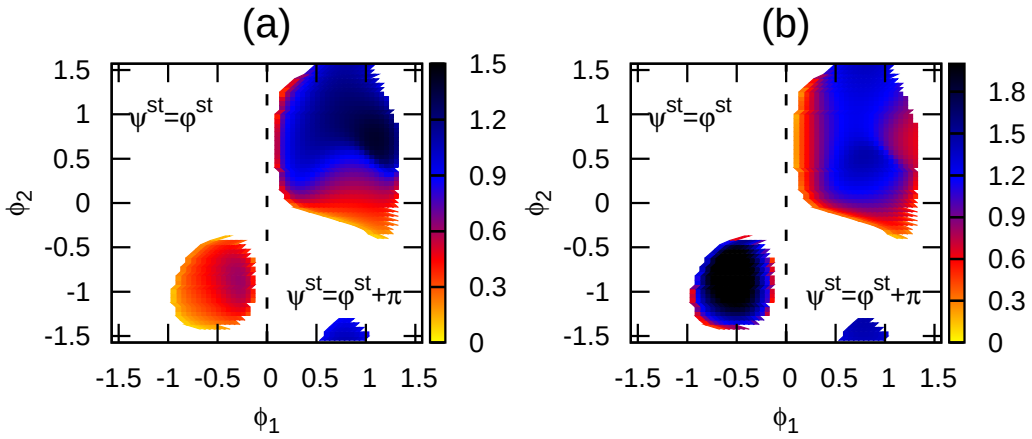


Figure 8.6: Non-zero stationary solution given by Eqs. (8.37) and (8.38) with H_{-}. (a) A^{st} and (b) B^{st} displayed in (ϕ_1, ϕ_2)-plane considering $G_1 = 2.5$ and $G_2 = 2.5$.

8.5 Numerical Simulations

In order to check our analytical results and also to investigate the stability of the fixed points shown in Figs 8.5 and 8.6, Eqs. (8.33) and (8.34) are numerically integrated using a predictor-corrector method. For numerical simulations, we also consider the parameters $\Omega_H = 100$ MHz, $\Omega_L = 1$ Hz, $\mu_1 = \mu_2 = 50\pi$ MHz, $Q_1 = Q_2 = 200$ and $G_1 = 2.5$. The initial conditions are chosen so that, after the transient, the system evolves to the physical solutions, e.g. $A \geq 0$ and $B \geq 0$.

Taking the loop gain G_2 as the bifurcation parameter and considering $\phi_1 = 0.5$ and $\phi_2 = 0.5$, Fig. 8.7 displays bifurcation diagrams of the amplitude for various loop gain G_1, obtained by extracting different maxima and minima in the time series after the transient. In this scenario, the bifurcation diagrams show that, depending on G_1, the system can be in a non-trivial steady state for the amplitude (corresponding to a pure microwave generation) or in a more complex dynamics when the stationary solution is destabilized through a Hopf bifurcation which induces modulated amplitudes [see Fig. 8.7 (b) and (c)]. For higher values of G_2, it is seen that the system induces chaotic amplitudes even for relatively low G_1. On the other hand, while the steady state amplitudes of the first filter output follow a parabolic evolution with respect to G_2, those of the second filter output are basically linear with G_2 [see Fig. 8.7 (d) and (e)].

The first results in Fig. 8.7 suggest a closer analysis of the stability of the stationary solution in the (G_1, G_2)-plane. To do that and to compare with the analytical results we display in the (G_1, G_2)-plane only the steady states amplitudes [e.g. periodic behavior in $x(t)$]. Numerically we consider that the amplitude is

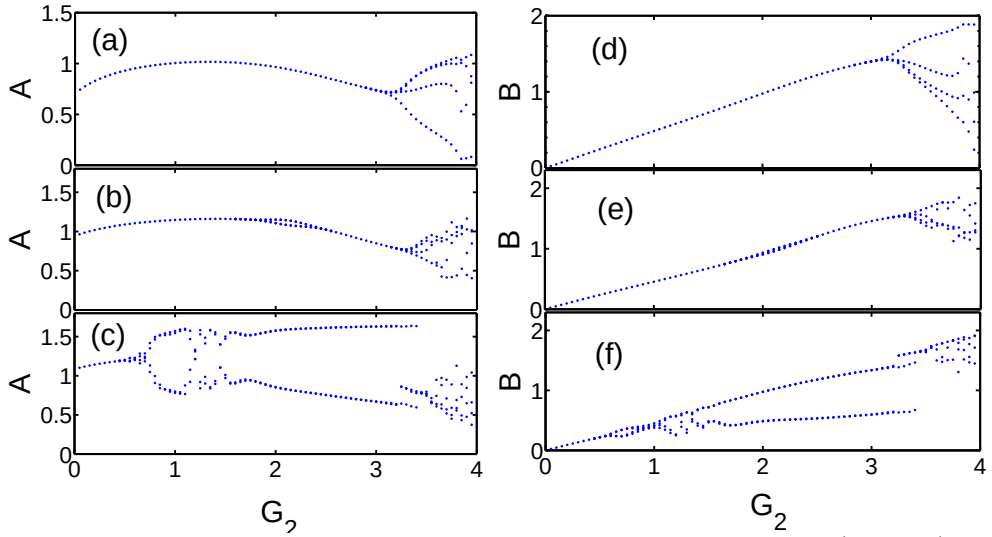


Figure 8.7: Numerical bifurcation diagrams with respect to G_2 for $G_1 = 2$ (top row), $G_1 = 2.5$ (middle row) and $G_1 = 3.0$ (bottom row); considering $T_1 = 20$ μs and $T_2 = 10\ T_1$ and the initial conditions $A(0) = B(0) = 0.2$ and $\psi(0) = \varphi(0) = 0.5$. Other parameters are $\mu_1 = \mu_2 = 50\pi$ MHz, $Q_1 = Q_2 = 200$, $\phi_1 = 0.5$ and $\phi_2 = 0.5$.

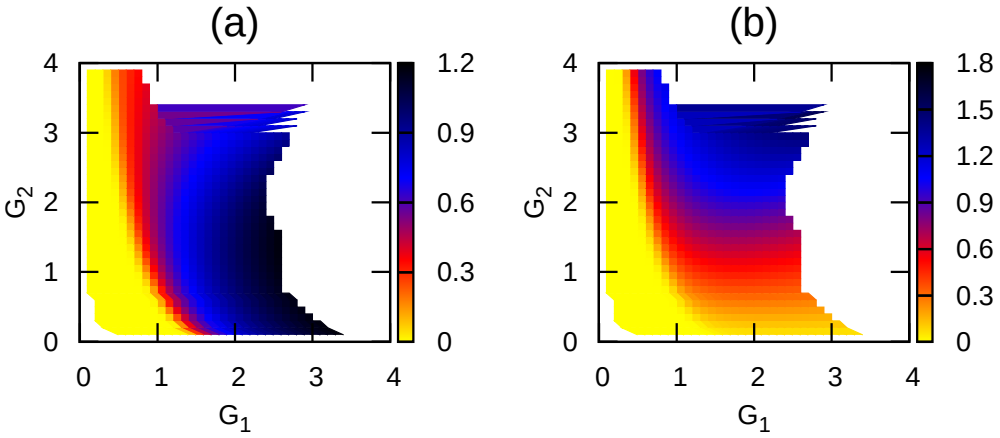


Figure 8.8: Numerical results giving the microwave amplitudes in (G_1, G_2)-plane obtained from Eqs. (8.33) and (8.34) (a) A and (b) B considering $\phi_1 = \pi/4$ and $\phi_2 = 0$. The initial conditions and the parameters were set as in Fig. 8.7.

stationary if after the transient time, it changes in less than 10^{-4} (allowing for the integration errors). Figure. 8.8 shows the results. The empty regions correspond to the values of G_1 and G_2 for which no steady state is found. While the microwave amplitudes in the first loop can be high as 1.2 in amplitude [Fig. 8.8 (a)], that in the second loop can be close to 1.8 [Fig. 8.8 (b)]. It therefore constitutes a potential way

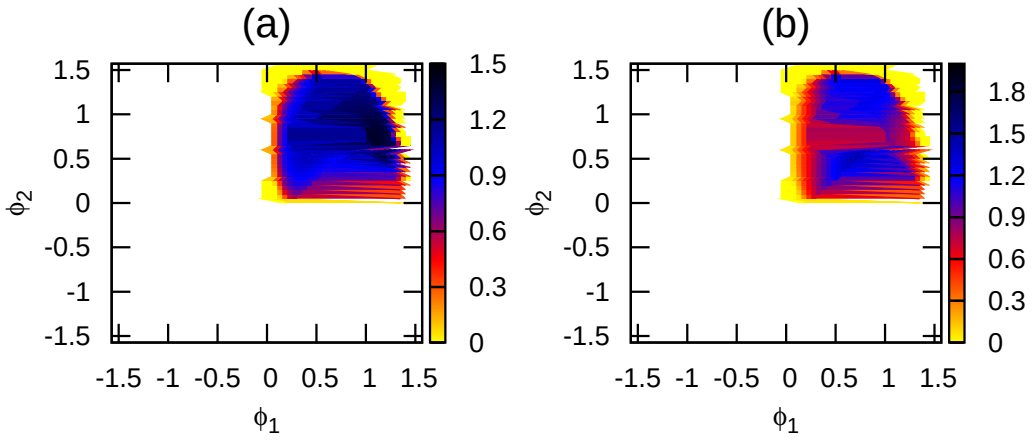


Figure 8.9: Numerical results giving the microwave amplitudes in (ϕ_1, ϕ_2)-plane obtained from Eqs. (8.33) and (8.34) (a) A and (b) B considering $G_1 = 2.5$ and $G_2 = 2.5$. The initial conditions and the parameters were set as in Fig. 8.7. The empty regions correspond to the modulated amplitudes.

to generate microwaves with higher amplitudes than the single loop which indeed generates the maximum microwave amplitude of 1.2 as found in ref.[82]. Also note that these results are in excellent agreement with those predicted previously (see Fig. 8.5). Note that the white regions of Fig. 8.5 which correspond to the region where only the trivial zero solution exists correspond in the numerical simulation to zero amplitude and therefore are plotted in yellow in color in Fig. 8.8.

Figure 8.9 displays the numerical results obtained from Eqs. (8.33) and (8.34) in (ϕ_1, ϕ_2)-plane for $G_1 = 2.5$ and $G_2 = 2.5$ considering as already stated $e^{-i\Omega_0 T_1} = -1$ and $e^{-i\Omega_0 T_2} = +1$. It turns out that almost all the predicted steady state amplitudes displayed in Fig. 8.6 for $\phi_1 \in [0, \pi/2]$ (out-of-phase microwaves) are stable when $\phi_1 > 0$ while those predicted for $\phi_1 \in [-\pi/2, 0]$ are all unstable (in-of-phase microwaves). Curiously enough even Fig. 8.6 shows that, for some offset phases, even the trivial steady state solution are unstable.

8.6 Comparison of Phase Noise Between OEOs with Single and Double Loop

For comparison, we first derive the corresponding phase noise equation for the OEO with double loop.

8.6.1 Stochastic phase equation for OEO with double loop

Considering the phase matching $e^{-i\Omega_0 T_1} = -1$ and $e^{-i\Omega_0 T_2} = 1$ the stochastic equations for slowly varying envelope $\mathcal{A}(t)$ and $\mathcal{B}(t)$ can be written as

$$\dot{\mathcal{A}}+\mu_1 e^{iv_1}\mathcal{A} = -\frac{1}{2}\mu_1 e^{iv_1} G_1(1+\eta_{m1})\Big\{ \sin 2\phi_2 \mathcal{J}_1(2B)e^{i\varphi} - \sin 2\phi_1 \mathcal{J}_1(2A_{T_1})e^{i\psi_{T_1}} + \cos 2\phi_1 \sin 2\phi_2 \sum_{p=-2}^{2} \bar{\mathcal{C}}_{2p} - \sin 2\phi_1 \cos 2\phi_2 \sum_{p=-2}^{2} \bar{\mathcal{C}}_{1-2p} \Big\} + \mu_1 e^{iv_1}\xi_{a1} \tag{8.44}$$

$$\dot{\mathcal{B}}+\mu_2 e^{iv_2}\mathcal{B} = -\mu_2 e^{iv_2} G_2(1+\eta_{m2}) \sin 2\phi_1 \mathcal{J}_1(2A_{T_2})e^{i\psi_{T_2}} + \mu_2 e^{iv_2}\xi_{a2}, \tag{8.45}$$

where

$$\bar{\mathcal{C}}_q = \mathcal{J}_q(2A_{T_1})\mathcal{J}_{1-q}(2B)e^{i\left[q\psi_{T_1}+(1-q)\varphi\right]} \equiv \bar{\mathcal{R}}_q + i\bar{\mathcal{I}}_q. \tag{8.46}$$

Since $\mathcal{A} = Ae^{i\psi}$ and $\mathcal{B} = Be^{i\varphi}$, the stochastic phase noise equations from Eqs. (8.44) and (8.45) can be written as

$$\begin{aligned}\dot{\psi} + \mu_1 \sin v_1 =& \frac{\zeta_\psi}{A} - \frac{\mu_1 G_1}{2A}\Big[1+\eta_{m1}(t)\Big]\Big\{ \sin 2\phi_2 \mathcal{J}_1\left[2B\right] \\ &\times \sin(v_1+\varphi-\psi) - \sin 2\phi_1 \mathcal{J}_1\left[2A_{T_1}\right]\sin(v_1+\psi_{T_1}-\psi) \\ &+ \sum_{p=-2}^{2} \sin 2\phi_1 \cos 2\phi_2 \bar{\mathcal{I}}_{2p} - \sum_{p=-2}^{2} \cos 2\phi_1 \sin 2\phi_2 \bar{\mathcal{I}}_{1-2p}\Big\},\end{aligned} \tag{8.47}$$

$$\dot{\varphi} + \mu_2 \sin v_2 = \frac{\zeta_\varphi}{B} - \frac{\mu_2 G_2}{B} \sin 2\phi_1 \left[1+\eta_{m2}(t)\right] \mathcal{J}_1\left[2|A_{T_2}|\right] \sin(v_2+\psi_{T_2}-\varphi), \tag{8.48}$$

where $\zeta_\psi = \xi_{a1,Re}(t)\sin(v_1-\psi) + \xi_{a1,Im}(t)\cos(v_1-\psi)$ and $\zeta_\varphi = \xi_{a2,Re}(t)\sin(v_2-\varphi) + \xi_{a2,Im}(t)\cos(v_2-\varphi)$ are independent Gaussian white noises with variances $\langle\zeta_\psi(t)\zeta_\psi^*(t')\rangle = 2D_{a1}\delta(t-t')$ and $\langle\zeta_\varphi(t)\zeta_\varphi^*(t')\rangle = 2D_{a2}\delta(t-t')$. The sub-indexes Re and Im refer to the real and imaginary parts.

Assuming $A(t) \backsimeq A(t-T) \backsimeq A^{st}$, we can consider that the phase fluctuations evolves so that $\sin(a-b) \approx a-b$, which is typically the case for the OEOs studied here. Thus, Eqs. (8.47) and (8.48) become

$$\dot{\psi} = \mu_1 \left[\alpha_\pm \psi_{T_1} + \beta_\pm \varphi - \psi + \frac{1}{2Q_1}\eta_{m1}(t) + \frac{\zeta_\psi}{A^{st}}\right], \tag{8.49}$$

$$\dot{\varphi} = \mu_2 \left[(\psi_{T_2}-\varphi) + \frac{1}{2Q_2}\eta_{m2}(t) + \frac{\zeta_\varphi}{B^{st}}\right], \tag{8.50}$$

where the coefficients are

$$\alpha_{\pm} = \frac{1}{\mathbf{H}_{\pm}}\Big\{ -\sin 2\phi_1 \mathcal{J}_1(2A) - 5\mathcal{J}_5(2A)\,\mathcal{J}_4(2B)$$
$$-\cos 2\phi_1 \sin 2\phi_2 \sum_{p=0}^{1}(2p+1)\mathcal{J}_{2p+1}(2A)\left[\mathcal{J}_{2p}(2B) + \mathcal{J}_{2(p+1)(2B)}\right]$$
$$\mp \sin 2\phi_1 \cos 2\phi_2 \sum_{p=1}^{2} 2p\mathcal{J}_{2p}(2A)\left[\mathcal{J}_{2p-1}(2B) + \mathcal{J}_{2p+1}(2B)\right]\Big\}, \tag{8.51}$$

$$\beta_{\pm} = \frac{1}{\mathbf{H}_{\pm}}\Big\{ \pm \sin 2\phi_2 \mathcal{J}_1(2B) \pm 5\mathcal{J}_4(2A)\,\mathcal{J}_5(2B)$$
$$\pm \sin 2\phi_1 \cos 2\phi_2 \sum_{p=0}^{1}(2p+1)\mathcal{J}_{2p+1}(2B)\left[\mathcal{J}_{2p}(2A) + \mathcal{J}_{2(p+1)(2A)}\right]$$
$$+\cos 2\phi_1 \sin 2\phi_2 \sum_{p=1}^{2} 2p\mathcal{J}_{2p}(2B)\left[\mathcal{J}_{2p-1}(2A) + \mathcal{J}_{2p+1}(2A)\right]\Big\}. \tag{8.52}$$

Here again the signs (+) and (−) refer to the *Case I* and *Case II*, respectively. In both cases, it is important to note that $\alpha_{\pm} + \beta_{\pm} = 1$. This relationship shows that the system keeps the neutral stability of the phase since 0 is still an eigenvalue. Also, it is worth noting that for $B = 0$ (single OEO loop), $\alpha_{\pm} = 1$ and $\beta_{\pm} = 0$ and therefore Eq. (8.49) degenerates to that obtained with single loop OEO. In the following, we investigate the performance of the system to phase noise when comparing with a single loop optoelectronic microwave oscillator. A way to do that consists in comparing the phase noise spectrum of the two systems.

8.6.2 Phase noise spectrum for OEO with double loop

Considering that all noise sources are uncorrelated, the Fourier transforms $\Psi(\omega)$ and $\Phi(\omega)$ of the phases $\psi(t)$ and $\varphi(t)$, respectively can be written from Eqs (8.49) and (8.50) as

$$\left|\Psi(\omega)\right|^2 = \frac{\left(\omega^2+\mu_2^2\right)\left(\frac{\mu_1^2}{4Q_1^2}\left|\eta_{m1}(\omega)\right|^2 + \frac{2\mu_1^2}{|A_1^{st}|^2}D_{a1}\right) + \mu_1^2\alpha_2^2\left(\frac{\mu_2^2}{4Q_2^2}\left|\eta_{m2}(\omega)\right|^2 + \frac{2\mu_2^2}{|A_2^{st}|^2}D_{a2}\right)}{\left|\left(i\omega+\mu_1\left(1-\alpha_1 e^{-i\omega T_1}\right)\right)\left(i\omega+\mu_2\right) - \mu_1\mu_2\alpha_2 e^{-i\omega(T_1+T_2)}\right|^2}, \tag{8.53}$$

$$\left|\Phi(\omega)\right|^2 = \frac{\mu_2^2\mu_1^2\left(\frac{1}{4Q_1^2}\left|\eta_{m1}(\omega)\right|^2 + \frac{2}{|A_1^{st}|^2}D_{a1}\right) + \left|i\omega+\mu_1\left(1-\alpha_1 e^{-i\omega T_1}\right)\right|^2\left(\frac{\mu_2^2}{4Q_2^2}\left|\eta_{m2}(\omega)\right|^2 + \frac{2\mu_2^2}{|A_2^{st}|^2}D_{a2}\right)}{\left|\left(i\omega+\mu_1\left(1-\alpha_1 e^{-i\omega T_1}\right)\right)\left(i\omega+\mu_2\right) - \mu_1\mu_2\alpha_2 e^{-i\omega(T_1+T_2)}\right|^2}. \tag{8.54}$$

At this stage, we note that for $\alpha_2 = 0$ (single loop OEO) one recovers the phase noise spectrum formula given by Eq. (8.19).

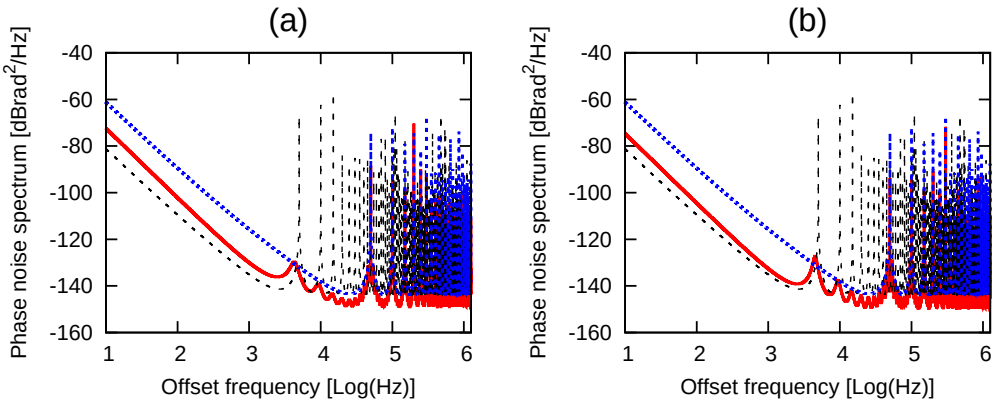


Figure 8.10: Comparison of the theoretical phase noise spectrum of an opto-electronic microwave oscillators with single loop given by Eq. (8.19) (dotted line) for $A = 0.41$ and $T = 20$ μs and (dashed line) for $A = 0.41$ and $T = 200$ μs with the results for a double loop given by Eq. (8.53) (solid line), both above threshold in a 500 MHz. The parameters for the double loop are as follows $\phi_1 = 0.5$ and $\phi_2 = 0.5$, (a) $T_1 = 20$ μs, $T_2 = 10T_1$ and $G_2 = 0.5$, (b) $T_1 = 20$ μs, $T_2 = 10T_1$ and $G_2 = 2.5$. In both the cases, $G_1 = 2.0$ leading to (a) $A = 0.93$ and $B = 0.24$, (b) $A = 0.86$ and $B = 1.22$.

8.6.3 Comparison phase noise spectra between OEOs with single and double loop

In addition to the parameters used in the previous sections, we also consider the parameters related to noise as $D_{m1} = D_{m2} = 5.0 \times 10^{-11}$ rad^2/Hz, $D_{a1} = D_{a2} = 9.0 \times 10^{-16}$ rad^2/Hz, $\phi_1 = 0.5$ and $\phi_2 = 0.5$. For comparison, Fig. 8.10 displays the phase noise spectrum for the single loop OEO, given by Eq. (8.19) considering $T = 20$ μs (blue line) and $T = 200$ μs (black line), and for double loop described by Eq. (8.53) for various values of G_2, T_1 and T_2 (solid line) considering $\phi_1 = 0.5$ and $\phi_2 = 0.5$. First we compare a double loop OEO with delays $T_1 = 20$ μs (4 km of fiber length), $T_2 = 10T_1$ and $G_1 = 2.0$ with the single loop OEO with delay $T = 20$ μs and the microwave amplitude $A = 0.41$. For $G_2 = 0.5$, the microwave amplitudes in the first and second loops are $A = 0.93$ and $B = 0.24$. It turns out that the phase noise is reduced of about 14 dB in the frequency area below $1/T_2$ [see Fig. 8.10 (a)]. In fact, as the quality factor is proportional to the fiber length, the increase of fiber length leads to its improvement. Therefore the effect of the multiplicative noise [see Eq. (8.53)] is reduced leading to the phase noise reduction observed in the region below $1/T_2$ for which the phase noise is dominated by multiplicative noise. Curiously enough the spurious peaks which would have appeared between $1/T_2$ and $1/T_1$ are damped due to interferences between the two combined signals in MZM$_2$. Note that in all the cases, a small spurious peak still appears at $1/T_1$ meaning that a small

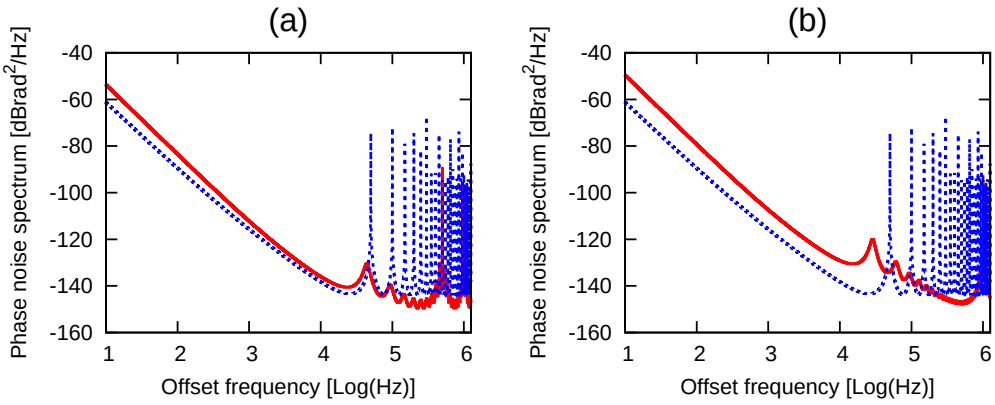


Figure 8.11: Comparison of the theoretical phase noise spectrum of an opto-electronic microwave oscillators with single loop given by Eq. (8.19) (dotted line) for $A = 0.41$ and $T = 20$ μs and (dashed line) for $A = 0.41$ and $T = 200$ μs with the results for a double loop given by Eq. (8.53) (dashed blue line), both above threshold in a 500 MHz. The parameters for the double loop are as follows $\phi_1 = .5$ and $\phi_2 = 0.5$,(a) $T_1 = 2$ μs, $T_2 = 10T_1$ and $G_2 = 0.7$, (b) $T_1 = 1$ μs, $T_2 = 30T_1$ and $G_2 = 0.2$. In both cases, $G_1 = 2.0$ leading to (a) $A = 0.97$ and $B = 0.34$ and (b) $A = 0.82$ and $B = 0.1$.

constructive interference still exists for this mode. Besides, it should be noted that the effect of the additive noise depends on A. Since for the parameters considered, A for the double loop OEO is larger than that obtained for the single loop OEO and therefore the effect of the additive noise is also reduced here. For frequencies above $1/T_1$, strong spurious peaks appear as in the single loop case. If the same delay line ($T = 200$ μs) was used in single loop, the performance of the system would have compromised due to appearance of the spurious peaks between $1/T_2$ and $1/T_1$ [Fig. 8.10 (black)]. When increasing $G_2 = 2.5$ (which leads to microwave amplitude $A = 0.85$ and $B = 1.22$), the phase noise is further reduced to about 18 dB for $\leq 1/T_2$ [see Fig. 8.10 (b)]. We have found that as G_2 increases, the spurious peak amplitudes in the damping frequency region increase as well. Also, one can notice that, in this case, the phase noise in the frequency region below $1/T_2$ get closer to that obtained considering $T = 200$ μs in a single loop OEO. The reduction of the spurious peak amplitude in OEO using several fiber loops has been reported in [154]. However the overall performance was significantly worse than the one reported in this work.

In second place, we reduce the delay of both loops in the double loop OEO by a factor 10, so that $T_1 = 2$ μs and $T_2 = 10T_1$ while G_1 is kept unchanged ($G_1 = 2.0$), and we compare the results with those obtained for the single loop OEO as before (e.g. considering a single loop with delay $T_1 = 20$ μs) [Fig. 8.11 (a)]. As in the previous case, the spurious peaks between $1/T_2$ and $1/T_1$ are suppressed. The

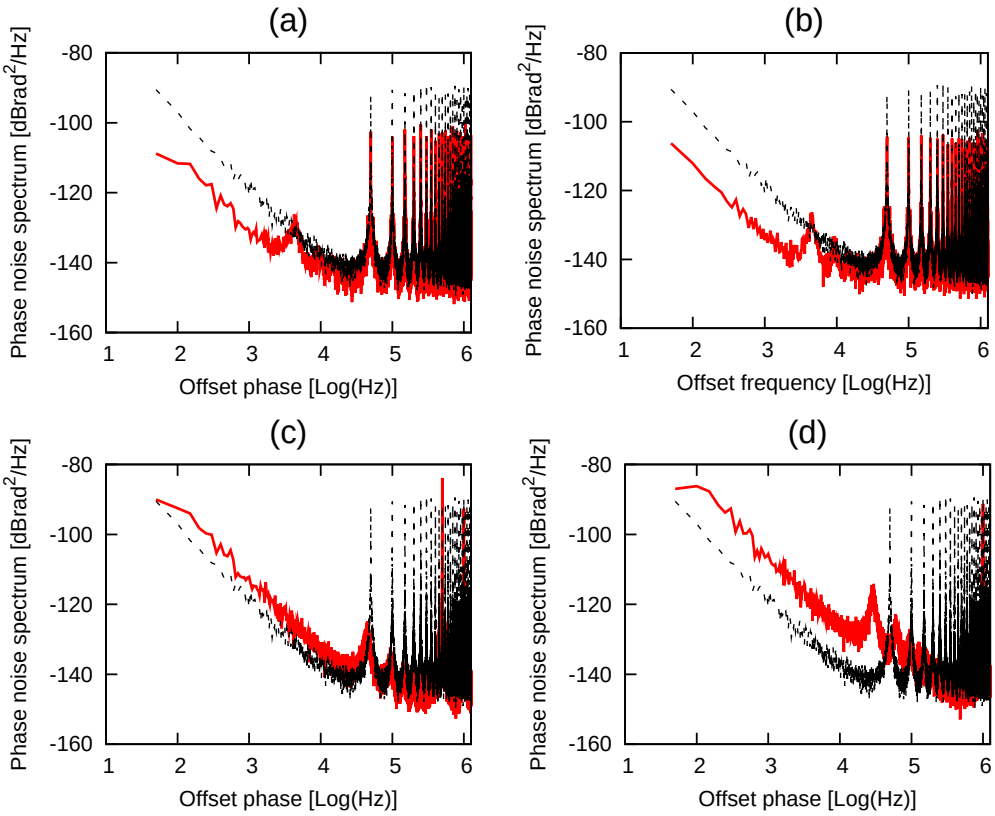


Figure 8.12: Comparison of the numerical phase noise spectrum of an opto-electronic microwave oscillators with single loop [82] (dotted line) for $A = 0.41$ and $T = 20$ μs with the results for a double loop given by Eqs. (8.33) and (8.34) (solid line), both above threshold in a 500 MHz. The parameters for the double loop are as follows $\phi_1 = 0.5$ and $\phi_2 = 0.5$, (a) $T_1 = 20$ μs, $T_2 = 10T_1$ and $G_2 = 0.5$, (b) $T_1 = 20$ μs, $T_2 = 10T_1$ and $G_2 = 2.5$, (c) $T_1 = 2$ μs, $T_2 = 10T_1$ and $G_2 = 0.7$, (d) $T_1 = 1$ μs, $T_2 = 30T_1$ and $G_2 = 0.2$. We consider the multiplicative noise as a Gaussian white noise with power density $|\eta_{1,2}(\omega)|^2 = 2D_{m1,2})$. The spectrum is obtained by computing a time series of 0.08 s sampled into 10 equal parts.

first strong spurious peak appears around $1/T_1$ =500 kHz. Therefore, the phase noise performance of the system is improved enough since the same phase noise performance is obtained for single OEO loop but at 50 kHz. Better results can be achieved tuning the values of T_1, T_2 and G_2. For example Fig. 8.11 (b) shows the results for $T_1 = 1$ μs, $T_2 = 30T_1$ and $G_2 = 0.2$ corresponding to $A = 0.82$ and $B = 0.1$, again compared with the same single loop OEO with $T_1 = 20$ μs and $A = 0.41$. In that case, the phase noise floor is around -150 dBrad^2/Hz at 1 MHz and around -50 dBrad^2/Hz at 10 Hz. While Figs. 8.10 and 8.11 plot only the phase noise for the first loop, we have found that the results for the phase noise in the second loop are very similar. In the region dominated by the multiplicative noise

(frequencies below $1/T_2$) they coincide. In the region dominated by the additive noise (frequencies above $1/T_1$) the phase noise for the second loop is slightly larger than $\Psi(\omega)$ since for our parameters $A > B$ [Fig. 8.10 (a) and Figs 8.11 (a) and (b)].

In order to confirm these results, Eqs. (8.33) and (8.34) are directly simulated using the second order Runge-Kutta method for stochastic equations. These equations include noise both in phase and amplitude. For the sake of simplicity, the multiplicative noises are considered in simulations as Gaussian white instead of flicker ones, e.g. with spectral density $|\eta_{m1,2}(\omega)|^2 = 2D_{m1,2}$. Figure 8.12 displays the numerical phase noise spectrum results for the same cases as in Figures 8.10 and 8.11 considering $T_1 = 20$ μs for single loop OEO. In Fig. 8.12 (a) and (b), the phase noise is considerably reduced in the OEO system with double loop as already found in analytics. For example one can see that the spurious peaks between $1/T_2$ and $1/T_1$ are damped while the strong spurious peaks above $1/T_1$ emerge at the exact positions predicted from the analytical results [see Fig. 8.10 (a) and (b)]. Although the multiplicative noises considered in the simulations are white, it can be seen that, qualitatively speaking, the same conclusions as those predicted from analytics arise for all the cases. This therefore evidences that the improvements found in the double loop configuration do not depend on the nature of the noise.

On the other hand, the results in Fig. 8.12 (c) and (d) also evidence the possibility of extending the region of low phase noise up to 1 MHz through the use of OEO system with double loop. Also, it is worth noting that the difference in the low frequency regime between the simulations and the analytics is due to the fact that the multiplicative noise has been considered flicker in analytical results (as it was discussed in Figs. 8.10 and 8.11) and white in simulations.

8.7 Conclusions

This chapter has presented a theoretical and numerically study of OEO with double loop designed for microwave generation with phase noise improvement. Our approach has consisted in comparing the phase noise spectra of the OEO with double loop with that of a system with a single loop. We have found that the double loop configuration can suppress the spurious peaks in frequency range comprised between to the inverse of the two delay times, (e.g. between T_2^{-1} and T_1^{-1}) so that it is possible to have phase noise of about -150 dBrad^2/Hz at 1 MHz or to improve the phase of up to 18 dB closer to the carrier. An interesting remark is that while the maximum amplitude of A^{st} is around 1.2 in single OEO, a maximum amplitude of B^{st} can be high as 1.8. As a consequence microwaves with high amplitudes and low phase noise can be obtained by adjusting G_2.

Chapter 9

General Conclusions and Future Work

9.1 General Conclusions

The potential of electro-optic systems for chaos communication applications has already demonstrated in realistic installed networks. The aim of this dissertation was to develop new electro-optic delayed systems capable of providing better performances than the existing systems, both in security and message decoding points of view. A review of the existing models indicated a need for a fresh look at structural architecture modifications, in order to take steps towards the design of more efficient systems. Using time series analysis techniques, such as autocorrelation and delayed mutual entropy, we have shown that the delay time is a vulnerable parameter for such systems. In particular, we have found that despite it has been reported that in all-optical feedback systems the delay time can be concealed in the intensity time series if it is chosen to be close to the relaxation time [115, 116], the delay time can still be identified from the phase of the transmitted electric field or from its quadratures. This result also evidences that the phase carries more information than the intensity or that it is easier to retrieve that information from the phase than from the intensity.

As for electro-optic systems, our results have confirmed that the delay time can be identified using the same techniques, even in the systems with multiple delay times. The results obtained when analyzing the dynamical variable of the model has shown that scalar systems can be fully reconstructed and consequently cannot be as secure as expected. In a practical chaos encryption system, one would probably prefer a more complex and dedicated nonlinear devices such as a multiple arms imbalanced interferometer instead of a standard MZI. The physical parameters defining the dynamic and static conditions of each interferometer arm, in this case, would represent an additional customized secret key of the hardware encryption.

To overcome the problem of scalar variable systems and also some experimental constraints, the idea of using an additional feedback to the laser source was presented

in this dissertation. That leads to a system displaying more complex behavior and with a larger number of parameters that an eavesdropper has to face up. The results showed that depending on how the laser feedback is performed, the chaos characteristics are quite different (see Fig. 4.11). We also showed that the message can be efficiently encoded and recovered using an authorized receiver.

Inspired by our results in delay time identification, which showed smaller peak sizes at the relevant delay times for electro-optic phase chaos systems, we implemented a digital key in this type of systems. To do that we made important structural architecture modifications in the system, so that the system now includes two delay loops in serial configuration. This allows to combine a pseudo-random binary sequence used in symmetric-key encryption, with a high-dimensional chaotic time series generated by an analog physical system, to make a symmetric-key encryption system with enhanced cryptographic security by reciprocal concealment. Besides bridging the gap between symmetric-key algorithmic cryptography and chaos-based encoding, the concealment of the delay time is particularly relevant to prevent from eventual eavesdropper attacks. Furthermore the digital key increases drastically the parameter space dimension. The experimental basis (electro-optic phase chaos) we have used to simulate the performance of our new concept, is currently the state of the art in terms of synchronization quality and bandwidth for practical chaos communication schemes (10Gb/s field experiment demonstration in our Ref.[75]). This new proposal is in line with the concept of algebra mixing algorithm, currently suggested to bridge the gap between software and hardware cryptography. The flexibility of the system allows for its easy reconfiguration to communicate between different people.

The flexibility in the design of this electro-optical delay systems has been proven through the parallel reconfiguration of the loops. The parallel loop configuration allows for the concealment of the internal loop delay times even without a digital key. Still the digital key can be introduced as an additional security element to increase the parameter space dimension. However, in this case, the digital key is not capable of fully concealing the external loop delay times.

We have also studied the detrimental effects of fiber propagation on the synchronization when using a phase chaos system. Theoretical and experimental results have shown that the proper retrieving of the message after few kilometers of propagation is impossible when using standard optical fibers. However, by using dispersion shifted fibers or by compensating for the dispersion accumulated during the propagation, we have found that the message can be properly recovered after propagation over more than 50 km, even when the third order dispersion and the nonlinear effects are not compensated.

Finally as a proof of electro-optic system versatility, we have numerically and

analytically studied an OEO with double loop for microwave generation. The results indicated that higher microwave amplitudes can be obtained with an OEO with double loop than with a single loop. One of the main improvements by the double loop system refers to the purity of the generated microwaves. In particular, the second loop can allow either to damp the spurious peaks so that the performance of the system is extended up to 1 MHz or to decrease in about 20 dB the phase noise close to the carrier.

9.2 Future Work

Very good performances have been found in the different systems presented in this dissertation. However, the experimental confirmation has been provided only partially. Thus, it will be of great interest to verify experimentally the theoretical results obtained here for the electro-optic delay systems with double loop both for chaos-based communications and for ultra-pure microwave generation.

We note also that very few investigations have been dedicated to the implementation of the schemes which could enable the implementation of asymmetric-key cryptography through a chaotic dynamics. Thus, it will be quite interesting to study possible configurations of electro-optical phase chaos systems suited for bidirectional communications on top of which asymmetric key cryptography could eventually be implemented.

Regarding the microwave generation, although good results have been obtained using a long delay line, future microwave generation may require more compact devices. An option has recently proposed by K. Volyanskiy *et al.* [155]. It consists in replacing the narrow filter and the delay line by a resonator. However, the phase noise in such system is higher. In addition, the theoretical derivation of a dynamical model for this system is still lacking. Future work could therefore focus on this aspect which will allow a better understanding of the system, necessary to improve its performance such as the reduction of the phase noise.

CURRICULUM VITAE

Civil Status

Name: NGUIMDO Romain Modeste

Born on: March 15^{th}, 1981 at Fongo-Tongo (Cameroon)

Sex: Male

Marital status: Married without child

Nationality: Cameroonian

Mailing address: Romain Modeste Nguimdo

IFISC (CSIC-UIB), Edifici Instituts Universitaris de Recerca Campus Universitat de les Illes Balears E-07122 Palma de Mallorca, Spain.

E-mail address: modeste1981@yahoo.fr & modeste@ifisc.uib.es

Academic Background

September 2008: Master Degree (with thesis) in physics

Starting date: October 2007

Title: Optical Communications Using Chaotic Carriers Generated by Electro-optical Feedback Devices.

Supervisor: Prof. Pere Colet.

Place: Institute for Cross-Disciplinary Physics and Complex Systems (IFISC) University of Balearic Islands, Palma de Mallorca, Spain.

December 2006: Master Degree (with thesis) in physics, Option: Mechanics

Starting date: September 2005

Title: Waves Amplification in Discrete Nonlinear Electrical Lines: Direct Numerical Simulation.

Supervisor: Prof. Paul Woafo.

Place: University of Yaoundé I, Yaoundé, Cameroon

November 2004: Post-Master's Certificate of Advanced Studies in Physics

Place: University of Yaoundé I, Yaoundé, Cameroon

September 2003: Bachelor's Degree of Physics

Place: University of Dschang, Dschang, Cameroon.

Actual Postition

Since October 2007: PhD student at IFISC, University of Balearic Islands, Palma de Mallorca, Spain.

Research Interests

Modeling and analysis of nonlinear dynamical systems

Optoelectronics, photonics, and laser physics

Optical telecommunication networks, light wave and microwave technologies

Optical fiber

Numerical simulations and series analysis

Publications

- R. M. Nguimdo, P Colet, C. Mirasso, "Electro-Optic Delay Devices With Double Feedback", J. of Quantum Electron. 46, 1436 (2010).
- R. M. Nguimdo, R. Lavrov, P. Colet, M. Jacquot, Y. K. Chembo, and L. Larger, "Effect of Fiber Dispersion on Broadband Chaos Communications Implemented by Electro-Optic Nonlinear Delay Phase Dynamics" J. of Lightwave Technology 28, 2688 (2010).
- R. M. Nguimdo, P Colet, L. Larger and Lus Pesquera, "Digital Key for Chaos Communication Performing Time Delay Concealment", Phys. Rev. Lett. 107, 034103 (2011).
- R. M. Nguimdo, M. C. Soriano, P. Colet, "Role of the Phase on Time Delay Identification in Semiconductor Laser with Optical Feedback" *Opt. Lett.* **36** 4332 (2011).
- R. M. Nguimdo, Y. K. Chembo, P. Colet and L. Larger, "Opto-electronic Microwave Oscillator with Double Loop: Phase noise performence" (Submitted for publication).
- M. Nguimdo, S. Noubissié and P. Woafo, "Waves Amplification in Discrete Nonlinear Electrical Lines : Direct Numerical Simulation", J. Phys. Soc. Jpn. 77, 124006 (2008).

Oral Presentation

1- Institut Femto-St April 28^{th}, 2009, Franche-Comté, France, "Chaos-Based Optical Communications Using Opto-electronic Devices with Two Wavelength Multiplexing".

2-Institute for Cross-Disciplinary Physics and Complex Systems (IFISC) July 28^{th}, 2010, Palma de Mallorca, Spain, "Effect of Fiber Dispersion on Broadband Chaos Communications Implemented by Electro-Optic Nonlinear Delay Phase Dynamics".

3-Instituto de Fsica de Cantabria (IFCA) October 7^{th}, 2010, Santander, Spain, "Chaos Encryption Potential Using Electro-optic Phase Generator".

Poster and Presentation to Conference

- R. M. Nguimdo, P. Colet and L. Larger, "Chaos-based Optical Communications Using Opto-electronic Devices with Two Wavelength Multiplixing", FisEs2009, Spain.
- R. M. Nguimdo, P. Colet and C. R Mirasso, "Electro-Optic Delay Devices With Double Feedback", FisEs2009, Spain.
- R. M. Nguimdo, R. Lavrov, P. Colet, M. Jacquot, Y. K. Chembo, and L. Larger, "Effect of Fiber Dispersion on Broadband Chaos Communications Implemented by Electro-Optic Nonlinear Delay Phase Dynamics", JNOG 2010, France.
- R. M. Nguimdo, P Colet, L. Larger and L. Pesquera, "Digital Key for Chaos Communication Performing Time Delay Concealment", Cleo/Europe 2011, Germany.
- R. M. Nguimdo, P Colet, L. Larger and L. Pesquera, "Digital Key for Chaos Communication Performing Time Delay Concealment", FisEs2011, Spain.
- M. Jacquot, R. Lavrov, J. Oden, Y. Chembo, R. M. Nguimdo, P. Colet, and L. Larger, " Field experiment optical chaos communication @ 10Gb/s demonstrating electro-optic phase chaos principles", Cleo/Europe 2011, Spain.

Long Stays

1- FEMTO-ST Institute, University of Franche-Comté
From February 1^{st} to May 1^{st}, 2010 (3 months), Besançon, France

Topic: Security issues in electro-optic phase chaos generator.

2- FEMTO-ST Institute, University of Franche-Comté
From February 1^{st} to May 1^{st}, 2011 (3 months), Besançon, France
Topic: Modeling optoelectronic microwaves using Whispering-gallery modes.

Language Skills

French (native),
English (very good),
Spanish (good).

Programming Language Skills

Fortran,
Matlab,
Mathematica.

Bibliography

[1] http://en.wikipedia.org/wiki/Electro-optic_modulator.

[2] B. Schneier, "Applied Cryptography", 2^{nd} Edition, Wiley (1995).

[3] Gilbert S. Vernam, "Secret signaling system", U.S. Patent 1310719, (1919).

[4] http://www.zytrax.com/tech/survival/encryption.html#terminology

[5] R. Rivest, A. Shamir, and L. Adelman, *Communications of the ACM* **21**, 120 (1978).

[6] See for example the web page of the European project eSTREAM (http://www.ecrypt.eu.org/stream).

[7] See for example the NIST call for the future SHA-3 (http://csrc.nist.gov/groups/ST/hash/sha-3/).

[8] P. R. Zimmermann, "PGP: Source code and internals", Cambridge, Mass: MIT Press (1995).

[9] V. Miller, "Use of elliptic curves in cryptography", *in CRYPTO 85 Proceedings, Lect. Notes in Computer Science* **218**, p. 417 (1985). DOI: 10.1007/3-540-39799-X_31.

[10] N. Koblitz, *Mathematics of Computation* **48**, 203 (1987).

[11] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", 35^{th} Annual Symposium on Foundations of Computer Science (FOCS 1994), p. 124, IEEE Computer Society Press (1994). DOI: 10.1109/SFCS.1994.365700

[12] I. L. Chuang, R. Laflamme, P. W. Shor, and W. H. Zurek, *Science* **8**, 1633 (1995).

[13] M. Bloch, PhD thesis, "Algorithme de réconciliation et méthodes de distribution quantique de clés adaptées au domaine fréquentiel", University of Franche-Comté (2006).

[14] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing", in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, (IEEE, New York)* p. 175 (1984).

[15] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[16] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar1, and V. Makarov, *Nature Photonics* **4**, 686 (2010).

[17] http://www.iet.ntnu.no/groups/optics/qcr/.

[18] J. Scheuer and A. Yariv, *Phys. Rev. Lett.* **97**, 140502 (2006).

[19] M. Peil, L. Larger, and I. Fischer, *Phys. Rev. E* **76**, 045201 (2007).

[20] H. Bai-Lin, "Chaos", World Scientic, Singapore Vol. I (1984) and Vol. II (1989).

[21] J. Gleick, "Chaos: Making a New Science", Penguin (2008).

[22] L. Glass and M. C. Mackey, "From clocks to chaos: The rythms of life", Princeton University Press, Princeton (1988).

[23] S. H. Strogatz, "Nonlinear dynamics and chaos: With applications to physics, biology, chemistry, and engineering", Addison-Wesley, Reading (1994).

[24] R. C. Hilborn, "Chaos and Nonlinear Dynamics: An introduction for scientists and engineers", Oxford University Press 2^{nd} Edition, New-York (2000).

[25] E. N. Lorenz, *J. Atmos. Sci.* **20**, 130 (1963).

[26] H. Haken, *Phys. Lett. A* **53**, 77 (1975).

[27] C. Bracikowski and R. Roy, *Chaos* **1**, 49 (1991).

[28] M. V. Danileiko, A. L Kravchuk, V. N. Nechiporenko, A. M. Tselinko, and L. P. Yatsenko, *Kvantovaya Elektron. (Moscow)* **13**, 2147 (1986).

[29] Y. Cho and T. Umeda, *Optics Commun.* **59**, 131 (1986).

[30] L. M. Pecora and T. L. Carroll, *Phys. Rev. Lett.* **64**, 821, (1990).

[31] K. M. Cuomo and A. V. Oppenheim, *Phys. Rev. Lett.* **71**, 65 (1993).

[32] A. Pikovsky, M. Rosenblum and J. Kurths, "Synchronization: A universal concept in nonlinear sciences", Cambridge Nonlinear Science Series, Cambridge University Press, Cambridge (2003).

[33] M. G. Rosenblum, A. S. Pikovsky and J. Kurths, *Phys. Rev. Lett.* **76**, 1804 (1996).

[34] G. V. Osipov, A. S. Pikovsky, M. G. Rosenblum, and J. Kurths, *Phys. Rev. E* **55**, 2353 (1997).

[35] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. I. Abarbanel, *Phys. Rev. E* **51**, 980 (1995).

[36] L. M. Pecora, T. L. Carroll, and J. F. Heagy, *Phys. Rev. E* **52**, 3420 (1995).

[37] L. Kocarev and U. Parlitz, *Phys. Rev. Lett.* **76**, 1816 (1996).

[38] S. Rim, I. Kim, P. Kang, Y.-J. Park, and C-M. Kim, *Phys. Rev.E* **66**, 015205 (2002).

[39] D. Pazo, M. A. Zaks, and J. Kurths, *Chaos* **13**, 309 (2003).

[40] M. Zhan, G. W. Wei, and C.-H. Lai, *Phys. Rev. E* **65**, 036202 (2002).

[41] C. R. Mirasso, P. Colet, and P. García-Fernández, *Phot. Tech. Lett.* **8**, 299 (1996).

[42] A. Sanchez-Diaz, C. R. Mirasso, P. Colet, and P. García-Fernández, *IEEE J. Quantum Electron.* **35**, 292 (1999).

[43] J. P. Goedgebuer, L. Larger, and H. Porte, *Phys. Rev. Lett.* **80**, 2249 (1998).

[44] C. Mirasso, J. Mulet, and C. Masoller. *IEE Phot. Tech. Lett.* **14**, 456 (2002).

[45] T. Heil, J. Mulet, I. Fischer, C. Mirasso, M. Peil, P. Colet, and W. Elsässer, *IEEE J. Quantum Electron.* **38**, 1162 (2002).

[46] A. Jacobo, M. C. Soriano, C. R. Mirasso, and P. Colet, *IEEE J. Quantum Electron.* **46**, 499 (2010).

[47] K. M. Short, *Int. J. Bifurcation Chaos* **4**, 959 (1994).

[48] K. M. Short, *Int. J. Bifurcation Chaos* **6**, 367 (1996).

[49] K. M. Short, *Int. J. Bifurcation Chaos* **7**, 1579 (1997).

[50] D. R. Kulkarni and R. E. Amritkar, *Int. J. Bifurcation Chaos* **11**, 3133 (2001).

[51] G. Pérez and H. A. Cerdeira, *Phys. Rev. Lett.* **74**, 1970 (1995).

[52] C.-S. Zhou and T.-L. Chen, *Phys. Lett. A* **234**, 429 (1997).

[53] T. Yang, L.-B. Yang, and C.-M. Yang, *Phys. Lett. A* **245**, 495 (1998).

[54] G. Alvarez and S. J. Li, *Int. J. Bifurcation Chaos* **16**, 2129 (2006).

[55] R. Tenny and L. Tsimring, *Int. J. Bifurcation Chaos* **14** 3949 (2004).

[56] P. Colet and R. Roy, *Opt. Lett.* **19** (1994).

[57] "Fundamental issues of nonlinear laser dynamics". B. Krauskopf and D. Lenstra eds., AIP Conference Proceedings **548**, Springer-Verlag (2000).

[58] L. Larger, J. P. Goedgebuer, *Comptes Rendus Physique*, **5**, 609 (2004).

[59] J. Mörk, B. Tromborg, and J. Mark, *IEEE J. Quantum Electron.* **28**, 93 (1992).

[60] R. Lang and K. Kobayashi, *IEEE J. Quantum Electron.* **16**, 347 (1980).

[61] G. P. Agrawal, *J. Appl. Phys.*, **63**, 1232 (1988).

[62] P. Spencer and C. R. Mirasso, *IEEE J. Quantum Electron.* **35**, 803, (1999).

[63] H. F. Chen and J. M. Liu, *IEEE J. Quantum Electron.* **36**, 27 (2000).

[64] I. Fischer, Y. Liu, and P. Davis. *Physical Review A* **62**, 011801 (2000).

[65] M. Peil, T. Heil, I. Fischer, and W. Elsässer, *Phys. Rev. Lett.* **88**, 174101 (2002).

[66] K. Ikeda, *Opt. Commun.* **30**, 257 (1979).

[67] L. Larger, J. P. Goedgebuer, and F. Delorme, *Phys. Rev. E* **57**, 6618 (1998).

[68] G. D. Van Wiggeren and R. Roy, *Science* **279**, 1198 (1998).

[69] G. D. Van Wiggeren and R. Roy, *Int. J. Bifurcation Chaos* **9**, 2129 (1999).

[70] A. Uchida, M. Shinozuka, T. Ogawa, and F. Kannari, *Opt. Lett.* **24**, 890, (1999).

[71] G. D. Van Wiggeren and R. Roy, *Phys. Rev. Lett.* **81**, 3547 (1998).

[72] J. Liu, H. Chen, and S. Tang, *IEEE J. Quantum Electron.* **38**, 1184 (2002).

[73] L. Larger, J. Goedgebuer, and V. Udaltsov, *Comptes Rendus Physique* **5**, 669 (2004).

[74] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C.R. Mirasso, L. Pesquera, and K.A. Shore, *Nature* **438**, 343 (2005).

[75] R. Lavrov, M. Jacquot, and L. Larger, *IEEE J. Quantum Electron.* **46**, 1430 (2010).

[76] R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. Udaltsov, and J. Dudley, *Phys. Rev. E* **80**, 026207 (2009).

[77] U. Gliese, T. N. Nielsen, M. Bruun, E. L. Christensen, K. E. Stubkjaer, S. Lindgren, and B. Broberg, *IEEE Photon. Technol. Lett.* **4**, 936 (1992).

[78] X. S. Yao and L. Maleki, *Electronics Letters*, **30** (18), 1525 (1994).

[79] X. S. Yao and L. Maleki, *J. Opt. Soc. Amer. B* **13**, 1725, (1996).

[80] X. S. Yao and L. Maleki, *IEEE J. Quantum Electron.* **32**, 1141 (1996).

[81] Y. K. Chembo, L. Larger, H. Tavernier, R. Bendoula, E. Rubiola, and P. Colet, *Opt. Lett.*, **32**, 2571 (2007).

[82] Y. K. Chembo, L. Larger, and P. Colet, *IEEE J. Quantum Electron.* **44**, 858 (2008).

[83] A. A. Andronov, A. A. Vitt, and S. E. Khaikin, "Theory of oscillators", Dover Publications (1987).

[84] D. Ham and A. Hajimiri, *IEEE Journal of Solid-State Circuits* **38**, 407 (2003).

[85] M. Lax, *Phys. Rev.* **160**, 290 (1967).

[86] D. B. Leeson, *Proc. IEEE,* **54**, 329, (1966). DOI: 10.1109/PROC.1966.4682.

[87] E. Hegazi, H. Sjoland, and A. A. Abidi, *IEEE Journal of Solid-State Circuits* **36**, 1921 (2001).

[88] D. Ham and A. Hajimiri, *IEEE Journal of Solid-State Circuits* **36**, 896 (2001).

[89] A. Hajimiri and T. H. Lee, *IEEE Solid-State Circuits* **33**, 179 (1998).

[90] J. J. Kim and B. Kim, "A low-phase-noise CMOS LC oscillator with a ring structure" in *IEEE International Solid-State Circuits Conference, 2000. ISSCC Digest of Technical Papers*, p. 430 (2000). DOI: 10.1109/ISSCC.2000.839846.

[91] W. Andress and D. Ham, "Standing wave oscillators utilizing wave-adaptive tapered transmission lines" in *Symposium on VLSI Circuits, 2004. Digest of Technical Papers*, p. 50 (2004). DOI: 10.1109/VLSIC.2004.1346499.

[92] G. Qi, J. P. Yao, J. Seregelyi, S. Paquet, and C. Belisle, *IEEE Trans. Microwave Theory Tech.* **53**, 3090 (2005).

[93] X. Chen, J. P. Yao, and Z. Deng, *Opt. Lett.* **30**, 2068 (2005).

[94] Y. K. Chembo, K. Volyanskiy, L. Larger, E. Rubiola, and P. Colet, *IEEE J. Quantum Electron.*, **45**, 178 (2009).

[95] M. C. Soriano, P. Colet, and C. R. Mirasso, *IEEE Photon. Technol. Lett.* **21**, 426 (2009).

[96] R. Vicente, J. Daudén, P. Colet, and R. Toral, *IEEE J. Quantum Electron.* **41**, 541 (2005).

[97] R. Vicente, T. Pérez, and C. R Mirasso, *IEEE J. Quantum Electron.* **38**, 1197 (2002).

[98] C. Masoller, *Phys. Rev. Lett.* **86**, 2782 (2001).

[99] J. Revuelta, C. R. Mirasso, P. Colet, and L. Pesquera, *IEEE Photon. Technol. Lett.* **14** 140, (2002).

[100] X. Li, W. Pan, B. Luo, and D. Ma, *IEEE J. of Quantum Electron.* **42**, 953 (2006).

[101] M. W. Lee, J. Paul, S. Sivaprakasam, and K. A. Shore, *Optics Lett.* **28**, 2168 (2003).

[102] J.-P. Goedgebuer, P. Levy, L. Larger, C.-C. Chen, and W. T. Rhodes, *IEEE J. Quantum Electron.* **38**, 1178 (2002).

[103] Y. Chembo Kouomou, P. Colet, L. Larger, and N. Gastaud, *IEEE J. Quantum Electron.* **41**, 156 (2005).

[104] R. Lavrov, "Electro-optic chaos via differential phase modulation: application to physical layer protection of 10 Gbps optical communications", PhD thesis, University of Franche-Comté (2010).

[105] Y. C. Kouomou, P. Colet, N. Gastaud, and L. Larger, *Phys. Rev. E* **69**, 056226 (2004).

[106] S. Ortín, J. Gutiérrez, L. Pesquera, and H. Vasquez, *Physica A* **351**, 133 (2005).

[107] R. Hegger, M. J. Bünner, H. Kantz, and A. Giaquinta, *Phys. Rev. Lett.* **81**, 558 (1998).

[108] V. S. Udaltsov, J. P. Goedgebuer, L. Larger, J. B. Cuenot, P. Levy, and W. T. Rhodes, *Phys. Lett. A* **308**, 54 (2003).

[109] V. S. Udaltsov, L. Larger, J. P. Goedgebuer, A. Locquet, and D. S. Citrin, *J. Opt. Technol.* **72**, 373 (2005).

[110] M. D. Prokhorov, V. I. Ponomarenko, A. S. Karavaev, and B. P. Bezruchko, *Physica D* **203**, 209 (2005).

[111] B. P. Bezruchko, A. S. Karavaev, V. I. Ponomarenko, and M. D. Prokhorov, *Phys. Rev. E* **64**, 056216 (2001).

[112] M. J. Bünner, M. Popp, T. Meyer, A. Kittel, and J. Parisi, *Phys. Rev. E* **54**, 3082 (1996a).

[113] M. J. Bünner, M. Popp, T. Meyer, A. Kittel, and J. Parisi, *Physics Letters A* **211**, 345 (1996b).

[114] S. Ortín, "Nonlinear dynamics reconstruction by neural networks of delay time chaotic systems" PhD thesis, Universidad de Cantabria (2010).

[115] D. Rontani, A. Locquet, M. Sciamanna, and D. S. Citrin, *Opt. Lett.* **32**, 2960 (2007).

[116] D. Rontani, A. Locquet, M. Sciamanna, D. S. Citrin, and S. Ortin, *IEEE J. Quantum Electron.* **45**, 879 (2009).

[117] J. G. Wu, G. Q. Xia, X. Tang, X. D. Lin, T. Deng, L. Fan, and Z. M. Wu, *Optics Express* **18**, 6661 (2010).

[118] C. Letellier, L.A. Aguirre, and J. Maquet, *Phys. Rev. E* **71**, 066213 (2005).

[119] R. M. Nguimdo, M. C. Soriano, and P. Colet, *Opt. Lett.* **36** 4332 (2011).

[120] H. C. Wang, K. P. Ho, H. K. Chen, and H. C. Lu, *J. Lightwave Technol.* **24**, 5075 (2006).

[121] L. Zimmermann, K. Voigt, G. Winzer, K. Petermann, and C. M. Weinert, *IEEE Photon. Technol. Lett.* **21**, 143 (2009).

[122] G. P. Agrawal and N. K. Dutta, "Semiconductor Lasers", 2^{nd} ed. Van Nostrand Reinhold (New York) (1993).

[123] M. J. Bünner, M. Ciofini, A. Giaquinta, R. Hegger, H. Kantz, R. Meucci, and A. Politi, *The European Physical Journal D* **10**, 165 (2000a). DOI: 10.1007/s100530050538.

[124] M. J. Bünner, M. Ciofini, A. Giaquinta, R. Hegger, H. Kantz, R. Meucci, and A. Politi, *The European Physical Journal D* **10**, 177 (2000b). DOI: 10.1007/s100530050539.

[125] J. Goedgebuer, L. Larger, and H. Porte, *Phys. Rev. E* **57**, 2795 (1998).

[126] R. M. Nguimdo, P. Colet, and C. R. Mirasso, *IEEE J. Quantum Electron.* **46**, 1436 (2010).

[127] V. Z. Tronciu, C. R. Mirasso, and P. Colet, *J. Phys. B: At. Mol. Opt. Phys.* **41**, 155401 (2008).

[128] K. Engelborghs, T. Luzyanina, and G. Samacy, *Report* TW 330, 2001; web: http://www.cs.kuleuven.ac.be/cwis/research/twr/research/software/delay /ddebiftool.shtml.

[129] A. Bogris, D. Kanakidis, A. Argyris, and D. Syvridis, *IEEE J. Quantum Electron.* **40**, 1326 (2004).

[130] D. Kanakidis, A. Bogris, A. Argyris, and D. Syvridis, *IEEE J. Lightwave Technol.* **22**, 2256 (2004).

[131] S. Tang and J. M. Liu, *IEEE J. Quantum Electron.* **39**, 1468 (2003).

[132] S. Tang, H. F. Chen, S. K. Hwang, and J. M. Liu, *IEEE Trans. Circuits Syst. I* **49**, 163 (2002).

[133] A. Klimov and A. Shamir, "New Cryptographic Primitives Based on Multiword T-Functions", in Fast Software Encryption, ed. by B. Roy and W. Meier, Lect. Notes in Computer Sciences 3017, p. 1, Springer, Berlin (2004). DOI: 10.1007/978-3-540-25937-4_1.

[134] R. M. Nguimdo, P. Colet, L. Larger, and L. Pesquera, *Phys. Rev. Lett.* **107**, 034103 (2011).

[135] M. Peil, T. Heil, I. Fischer, and W. Elsässer, *Phys. Rev. Lett.*, **88**, 174101 (2002).

[136] A. Bogris, P. Rizomiliotis, K. E. Chlouverakis, A. Argyris, and D. Syvridis, *IEEE J. Quantum Electron.* **44**, 119 (2008).

[137] W. H. Kye, M. Choi, and C.-M. Kim, *Phys. Rev. E* **71**, 045202(R) (2005).

[138] C. Robilliard, E. H. Huntington, and J. G. Webb, *IEEE Trans. Circuits Syst.* **53**, 722 (2006).

[139] D. Rontani, M. Sciamanna, A. Locquet, and D. S. Citrin, *Phys. Rev. E* **80**, 066209 (2009).

[140] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, "Handbook of Applied Cryptography", CRC Press Boca Raton, FL (1996).

[141] K. Pyragas, *Phys. Rev. E* **58**, 3067 (1998).

[142] S. Donati and C. R. Mirasso, Guest Editors, Feature Section on Optical Chaos and Applications to Cryptography, *IEEE J. Quantum Electron.*, **38**, #9 (2002).

[143] R. M. Nguimdo, R. Lavrov, P. Colet, M. Jacquot, Y. K. Chembo, and L. Larger, *J. Lightwave Technol.* **28**, 2688 (2010).

[144] N. Gastaud, S. Poinsot, L. Larger, J.-M. Merolla, M. Hanna, J.-P. Goedgebuer, and F. Malassenet, *Electron. Lett.* **40**, 898 (2004).

[145] S. F. Yu, P. Shum, and N. Q. Ngo, *Opt. Commun.*, **200**, 143 (2001).

[146] A. Argyris, E. Grivas, M. Hamacher, A. Bogris, and D. Syvridis, *Optics Express*, **18**, 5188 (2010).

[147] G. P. Agrawal, "Nonlinear fiber optics", 4$^{\text{th}}$ ed., Academic Press, (2007).

[148] C. Antonelli, A. Mecozzi, M. Santagiustina, and L. Ursini, *IEEE Photon. Technol. Lett.* **21**, 1387 (2009).

[149] M. Born and E. Wolf, "Principles of optics", 7$^{\text{th}}$ ed., Cambridge University Press, New York (1999).

[150] G. P. Agrawal, "Fiber-Optic Communication Systems", 2$^{\text{nd}}$ ed., Wiley, New York (1997).

[151] M. Guy, and Y. Painchaud, "Fiber Bragg Gratings: A versatile approach to dispersion compensation", Photonics Spectra, p. 96 (August 2004).

[152] X. S. Yao and L. Maleki, *IEEE J. Quantum Electron.* **36**, 79 (2000).

[153] R. M. Nguimdo, Y. K. Chembo, P. Colet, and L. Larger, "Electro-optic microwave oscillator with double loop: Phase noise performance" (submitted).

[154] D. Eliyahu and L. Maleki "Low phase noise and spurious level in multi-loop opto-electronic oscillators" in *Proc. 2003 IEEE International Frequency Control Symposium and 17 European Frequency and Time Forum*, p. 405 (2003). DOI 10.1109/FREQ.2003.1275126.

[155] K. Volyanskiy, P. Salzenstein, H. Tavernier, M. Pogurmirskiy, Y. K. Chembo, and L. Larger, *Optics Express* **18**, (2010).