Nonlinear dynamics of photonic components. Chaos cryptography and multiplexing

Damien Rontani

Supélec

N° d'ordre: 2011-19-TH

THÈSE DE DOCTORAT

SPÉCIALITÉ: PHYSIQUE

École Doctorale: Énergie, Mécanique et Matériaux

présentée en vue de l'obtention du grade de
DOCTEUR de SUPÉLEC
par

Damien RONTANI

Sujet:

Dynamique Non-Linéaire de Composants Photoniques Cryptographie par Chaos et Multiplexage

Soutenue le 16 Novembre 2011 devant la commission d'examen composée de

M. Gilles MILLERIOUX	Professeur à l'Université Henri Poincaré de Nancy	Président
M. Jordi GARCIA-OJALVO	Professeur à Universitat Polytecnica de Catalunya	Rapporteur
M. Alan K. SHORE	Professeur à Bangor University	Rapporteur
M. Apostolos ARGYRIS	Chercheur à University of Athens	Examinateur
M. Alexandre LOCQUET	Chercheur à l'UMI 2958 Georgia Tech-CNRS	Examinateur
M. David CITRIN	Professeur à Georgia Tech	Co-directeur
M. Marc SCIAMANNA	Professeur à Supélec	Directeur

Damien Rontani has been financially supported by the Fondation Supélec, the Conseil Régional de Lorraine, and the National Science Foundation (NSF). He is with the department of Optoelectronic (OPTEL) at Supélec (Ecole Supérieure d'Electricité, France), the UMI 2958 Georgia Tech - CNRS (France-USA), and the School of Electrical and Computer Engineering at Georgia Tech (USA).

Acknowledgements

The present PhD research has been prepared in the framework of collaboration between the Georgia Institute of Technology (Georgia Tech, USA) and the Ecole Supérieure d'Electricité (Supélec, France), at the UMI 2958 a joint Laboratory between Georgia Tech and the Centre National de la Recherche Scientifique (CNRS, France). I would like to acknowledge the Fondation Supélec, the Conseil Régional de Lorraine, Georgia Tech, and the National Science Foundation (NSF) for their financial and technical support.

I would like to sincerely thank my "research family" starting with my two advisors who made this joint-PhD project possible; Prof. Marc Sciamanna (Supélec) and Prof. David Citrin (Georgia Tech). They both supervised my research project and provide valuable insight, input and advice, even as I was moving from a continent to the other.

Marc was still a young assistant professor when I started. He found the right words to reinsure me in the choice of pursuing academic research, a key step in my intellectual life. His unconditional support, his will to make his students successful and his passion for research were communicative and of incredible support during the difficult and stressful moments of the thesis, those which any graduate student might experience at some point. I benefited a lot from his pragmatism and great knowledge in the field of nonlinear sciences. I would like to thank him very warmly for all he has done for me.

I am also extremely thankful to David, whose experience in research help me get through the undesirable life of a graduate student. His kindness and trust were an integral part of my scientific achievements. I am mostly grateful to him for believing in my unconventional ideas. I would like also to thank him for being extremely supportive during the writing of the PhD manuscript, as he was mailing me funny "PhD Comics" cartoons to cheer me up. Finally, I would like to thank David's wife, Alka, for the kind invitations and her stunning Indian cooking.

I would like to express my thanks and gratitude to Alexandre Locquet, who co-advise me very closely during my stay in Metz. He had the difficult task to manage me and my unflagging obstinacy. His constant support, care and kindness always helped me especially in the final line of the PhD. By challenging my ideas, he definitely made me a better scientist. His main flaw would be his unconditional support to the Italian soccer team...

Georgia Tech Lorraine (GTL) was my second home. The administrative staff and professors made my research experience very agreeable. I would like to thank Yves Berthelot, president of GTL, Prof. Abdallah Ougazzaden, Director of GTL and the

UMI 2958 for letting me conduct my research in his laboratory. Amongst the various staff members, I would like to express my sincere thank to Josyane Roshitz, her help in the complex US administrative process were and still are invaluable; Jean-Jacques Michel (aka J2M) for the countless times he helped me to solve a large range of computer-related problems, John Fritch for his good advice and friendship, Sandrine Cadamuro for her help and advice to solve professional and personal issues. Finally, I would like to thank the different staff members I interact with at GTL. The warmest thanks to Florence Stoïa, Catherine Bass, and Sandra Song for their friendship, generosity, and kindness, while I was on the Atlanta campus. The members of the academic office were not in rest: Dr. Bonnie Ferri, Chris Malbrue, Tasha Torrence, and Marilou Mycko have been of incredible help and they worked tirelessly to help me in the most critical times in the organization of the PhD defense. I would like to express my sincere gratitude to them.

I would also take the opportunity to thank key people at Supélec that have contributed to the PhD success: First, Yves Tanguy former director of industrial research who introduced me to Marc in the first place. Then, Jacques Oksman, current director or research, and Joël Jacquet, delegate of research at Supélec Campus de Metz, who let me join the recently established PhD program at Supélec, and finally Patrick Turelle who has always been a great supporter. I still see most of the Supélec Campus of Metz as a big family, with whom I spent at least five years of my life. Therefore, I would like to thank all the staff members of the Metz Campus for their kindness and continuous support during my thesis.

It is often believed that research is a lonely path to walk and that most scientists are disconnected from reality. I used to share this misbelief until I met a very warm scientific community in the nonlinear sciences and photonics. Team work and collaborations have been the corner stones of this whole PhD research. Here, I would first express my sincere thanks to Silvia Ortin (Universidad de Cantabria, Spain) for her participation to the study of the security analysis of optical chaos generators and her expertise in time-series modelling and analysis. I am also extremly grateful to Atsushi Uchida (Saitama University, Japan) for his kindness, trust, and our fruitful collaboration on the generation of orthogonal codes for multiplexed chaos-based applications. Everything, started at CLEO Europe 2009 in Munich, Germany, when after a discussion, we came up to an idea which had settled a very successful and enriching collaboration. He also invited me for a truly inspirational stay in his laboratory in the region of Tokyo. There, we had the most passionate discussions on nonlinear sciences and even developed new ideas laying the foundations for future collaborative research.

I am also thankful to all the jury members, Dr. Apostolos Argyris, Prof. Jordi Garcia-Ojalvo, Prof. Gilles Millérioux and Prof. K. Alan Shore, for their availability and constructive remarks during the whole evaluation of this PhD thesis work. It was a great honor for me to present my work to you.

In the course of my time as a PhD student, I met amazing lifelong friends. They help me to enjoy Metz and Atlanta to their fullest. Chronologically, I met Frederic Pons (aka Fred) and Audric Saillard, two “Gadzards” who shared with me the secrets to survive in my residence, by sharing their Internet access! For a while, they were as brothers as I was geographically isolated (no TGV at the time) and had

to face unfavorable weather conditions... Later, new members integrated the PhD room; Zheshen Zhang, Wui-Han Go, Sarah Herbison and Mohammed Abid joined us. Sarah was greatly supportive and helped me a lot to decipher the complexity of the social interactions in the USA. Mohammed brought with him this warm and friendly spirit from the north of Tunisia. For his wedding with Hagger, he invited the whole PhD room to Sfax for an unforgettable journey. Later came Vinod Ravindran who is definitely amongst my best and closest friends. We had our desks face to face for almost two years. During that time, I tried to learn how to decipher his peculiar sense of humor and farfetched jokes, but also to assimilate some of his impressive organizational and communication skills. As I was on my way leaving GTL, new students showed up and left the lab: Konstantino Pantzas a talented greek student who speaks four languages fluently, Peter Bonano who makes me discover organics products at the "Whole Food Market" and with whom we had the craziest road trip to New-Jersey, Ning Tian my Chinese roommate for six months in Atlanta, David Swafford an american student who initiates me the Southern-American way of life and to the fundamentals of waterskiing. Later in Atlanta, I met a great friend, Hassan Kingravi with whom we had the most passionate discussions on sciences. I am also particularly grateful to Aurèle Balavoine, she was very supportive and like a little sister to me during my stay in Atlanta. My time was also shared with Supélec, where I had the opportunity to meet Ignace Gatare, Christian Dan, and Nicolas Marsal. Nicolas is one of the most talented person I have ever encountered; sciences, music, painting, magic are few of his skills. He became a great friend during my PhD training and a huge fan of some of my lame imitations (I am still wondering why). Finally, Matthieu Bloch and Laurent Capolungo, who once upon a time were PhD students and who are today successful assistant professors at Georgia Tech. Although their radically different styles, they impersonate my wildest scientific aspirations and conception of what is a modern scientist. They both give me numerous advice and I would like to thank them for that.

To conclude this long acknowledgement, I would like to express my deep thank and love to my parents and brothers, Vincent and Matthieu, who were the best support of all. They were also my toughest referees as I was choosing the career of scientist. But they always respected and supported my decision, trusting my judgements as they watched me become a true academics. I would like to dedicate my thesis to them and to my grand parents Claude and Jean Derrien, and Marie and Georges Rontani. During this period, I also get closer to some of my siblings; my cousin Anne-Laure, her Husband Madji and their four children Noémie, Yanis, Sofia, and Leïlou; my uncle Francois, his wife Hélène and their three children Charles, Juliette, and Camille. Their kindness and support were unrivaled. I would like also to thank the rest of my family (too large to be fully mentioned) for their good words and love. A final wink at my dear friends from Strasbourg; Ariel, Ania, and Jérôme, who have been there, since I have stepped in the eastern part of France for the first time many years ago.

Contents

Chapter 1

General Introduction

Abstract

This chapter details the large variety of our research topics: chaos-based communications using optoelectronic devices. Being at the crossroads of many fields (nonlinear sciences, photonics, communication theory and cryptography) not only gives the unique opportunity to understand and quantify the limitations and performances of existing chaotic cryptosystems, but also to propose new and innovative architectures. We review the concepts of physical-layer security and their applications using chaotic optoelectronic systems. We explain the principles of chaos-based communications and highlight the current limitations and challenges addressed in this thesis.

1.1 General Context of Physical Layer Security

Optoelectronic technologies have shaped the landscape of the existing optical telecommunication networks and have contributed to the information revolution of the last four decades.

These networks are made of various levels (or layers), each of them being controlled by a particular set of protocols. The typical open systems interconnection (OSI) representation of a network is composed of seven layers (Fig. 1.1), which all play a role in communicating between distant systems. Inseparable from the development of modern communications, the question of security is of prime importance. Indeed, the existence of multiple layers in the network offers many possible breaches for illegitimate users, Eve (eavesdroppers), to steal or alter sensitive information exchanged between two legitimate users commonly referred to as Alice (sender) and Bob (receiver).

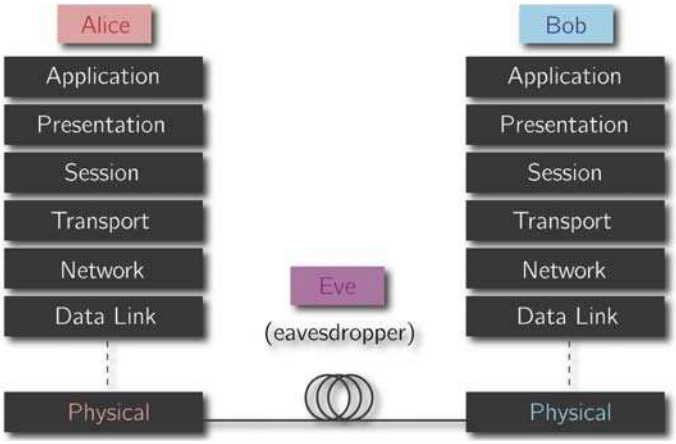

Figure 1.1: Schematic diagram of the OSI representation of a communication network.

To prevent the occurrence of such scenarios, mathematical-based cryptography was invented. It consists of two essential elements: an *algorithm* that is usually publically known by both legitimate and illegitimate users and a *key* that remains private. The security of this type of scheme depends strongly on the capacity for a given algorithm to mix the key with a plain message such that the obtained cipher will not leak information about the key, given knowledge of the algorithm. Today, there exist many cryptographic techniques that guarantee a high level of security (e.g. RSA, El-Gamal, PGP, AES, DES)[1]. These mathematical-based approaches provide a computational level of security and are adapted to the top layers of the network stack shown in Fig. 1.1.

Only recently, the physical layer has attracted attention. With our current technological level, it is now possible to harness physical principles existing in the devices transmitting and receiving the information. For optoelectronic systems, two widely discussed solutions exist to provide additional security at the physical layer:

- quantum-based communications for quantum key distribution (QKD) with the guarantee of information-theoretic security [2],

- chaos-based communications for additional computational security, similar to that of the conventional mathematical cryptographic schemes.

Current QKD systems still suffer from significant limitations in terms of bit rate (few tens of kbits/s) and of practical applicability (transmission with unconditional security only on few tens of km)[3], thus stimulating active research to improve their performances. Chaos-based communications exploit deterministic noise-like signals generated by physical nonlinear oscillators to cloak sensitive data. Optoelectronic devices are extremely popular because of their fast fluctuations, which can securely transmit data streams at high bit rates (several Gbits/s) over large distances [4].

The development of optical chaos cryptography results from three scientific milestones late in the 20th century: (i) the concept of stimulated emission (discovered by Einstein in 1917) demonstrated with semiconductor materials in 1962 [5], (ii) the development of the chaos theory to describe erratic evolutions occurring in nonlinear systems with sufficiently high dimensionality [6], and (iii) the synchronization of chaotic oscillators proved in the 1990's [7].

A generic optical chaos-based cryptographic chain consists of a legitimate user Alice, who injects with an appropriate technique the data to be transmitted in a chaotic optoelectronic device (E). The system's output, which bears the message, is then sent on a public channel wiretapped by an eavesdropper Eve. The channel couples Alice's emitter with a legitimate receiver (R) (physical copy of Alice's system) owned by Bob. Bob's system will synchronize only with the deterministic part of the signal transmitted, a property known as *chaos-pass filtering*. He duplicates Alice's chaotic carrier and uses a generalized subtraction operation to recover Alice's concealed data (Fig. 1.2). This approach was experimentally proposed by R. Roy and G.D. VanWiggeren in 1998 [8]. The instabilities in optoelectronic oscillators, traditionally considered as undesirable, were constructively used to disguise data at the physical level.

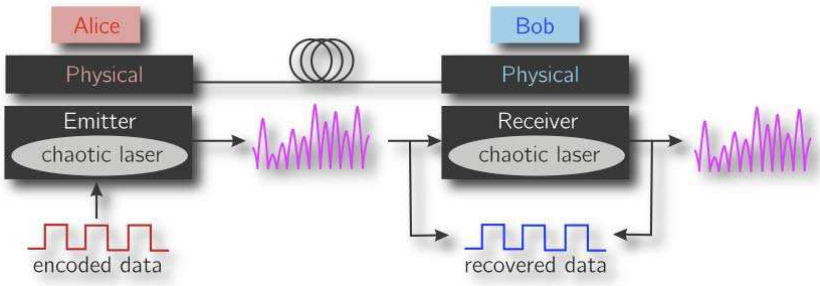

Figure 1.2: The physical layer of a communication network in the case of a chaos-based encryption and decryption using optoelectronic devices.

Optical chaos-based cryptography has great potential in terms of additional computational complexity at the physical layer and is ready for real-field applications; an experiment was conducted on a commercial fiber network in Athens (Greece) in 2005 with encrypted transmission at high bit rates (Gbit/s) [4]. The chaotic optoelectronic generators are typically based on edge-emitting semiconductor lasers

(EEL), a technology also used in diverse industrial and scientific applications, such as DVD player, bar-code readers, fiber optic networks, printers, metrology, and ultrafast measurements. Being already widely deployed in optical networks, they subsequently make good candidates for a large-scale implementation of optical chaos cryptography. Their ubiquitous presence is explained by their remarkable performance in terms of electro-optical efficiency, compactness, modulation speed, and lifetime.

1.2 Critical Issues and Challenges

1.2.1 Security of Chaos-Based Encryption

A critical issue, which has marginalized chaos cryptography and slowed down its deployment, is the analysis of security. It remains an open problem primarily due to two specific aspects of chaos-based encryption [9]:

- the use of nonlinear functions (or maps) mostly defined on continuous number sets (sometimes finite number sets) contrary to non-chaos-based encryption schemes that are exclusively defined on finite number sets.
- the analysis of security is not performed with the typical tools of mathematical cryptanalysis.

These two fundamental differences do not prevent an analogy between non-chaos-based and chaos-based encryption techniques; the chaotic system's parameters and its nonlinear function are respectively equivalent to a key and an algorithm. This justifies the existence of the various possible methods of attack on chaos-based cryptosystems described below:

- Attack on the imperfect mixing of information. This type of attack does not require any *a priori* knowledge of the parameters (key) or the nonlinear function (algorithm) and aims at a direct extraction of the message from the chaotic dynamics [10].
- Attack on the key with partial knowledge of the chaotic cryptosystem. This type of attack is analogous to those performed in conventional cryptography techniques, where the algorithm (respectively nonlinear function) is known, the eavesdropper has access to the encrypted data (respectively chaotic time series bearing the message), and only the key (resp. parameters) remains unknown.
- Attack with no *a priori* knowledge of the system. The eavesdropper only has access to the encrypted data. He must infer the nonlinear function and the parameters.

The last type of attack tests the intrinsic level of privacy that a chaos-based cryptosystem can provide. Concerning the optical-chaos generators, no studies have fully investigated the security of a large class of optoelectronic devices, namely optical delayed systems, and more specifically external-cavity semiconductor lasers (ECSL). This may prevent the use of optical chaos-based cryptography in field applications.

1.2.2 Multiplexing and Multiuser Communications

Over the past two decades, optical chaos-based communications have made tremendous progress on encryption, transmission, and decryption of a single message and have reached multi-Gbit/s secure communications [11; 12]; however, some limitations still exist; including the performance in terms of (i) bit error rate (BER) and (ii) power and spectral efficiency, which are still below those of conventional non-chaos-based encryption.

To improve the BER, the use of error control correction [13] has been proposed to improve BER performance [14]. In optoelectronic systems, the main reasons underlying BER limitations are the existence of internal or external noise sources (spontaneous emission of light or electronic noise, and channel noise, respectively) and the imperfect match between two twin physical systems (parameter mismatch). In both cases, perfect chaos synchronization is lost, subsequently leading to an increase of decryption error.

Improving spectral efficiency would consist of a better use of the available power and bandwidth by transmitting multiple messages in a same communication channel using either a single or multiple chaotic optoelectronic devices (see Fig. 1.3).

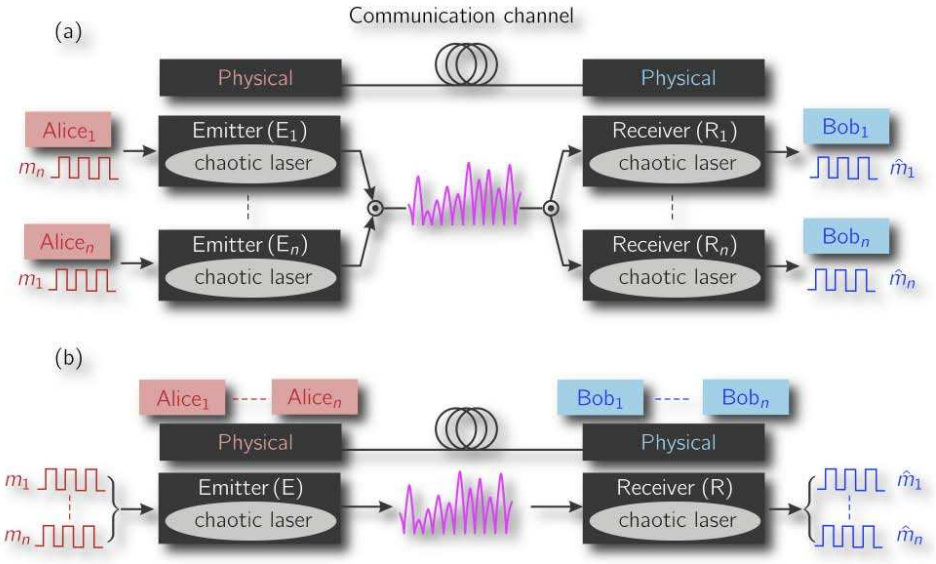

Figure 1.3: General description of the multiplexing problem using optoelectronic devices. Two possibilities exist: (a) the use of multiple oscillators (E_i) owned by Alice$_i$ to encrypt various data streams m_i and the use of multiple receiver (R_i) to decrypt each message $\hat{m}_i$; (b) the use of a single emitter shared by the Alices to encrypt their message and a single shared receiver (R) owned by the Bobs.

In conventional optical communications, various approaches to multiplex data have been developed, including time- and wavelength-division multiplexing (TDM and WDM), and more recently code-division multiple access (CDMA) [15]. In the case of chaotic systems, two approaches have been considered: type-i asynchronous methods using chaotic systems at the emission but without exploiting synchronization, and type-ii synchronous methods using chaotic systems and synchronization.

The type-i methods are well documented and understood. Their performance has been tested with various systems and architectures. A detailed review can be found in [16] and references therein. Most of the single-user optical chaos-based communications, however, rely on chaos synchronization. Consequently, any development of multiplexing techniques will naturally fall within the type-ii category. As illustrated by Fig. 1.3, there are two possibilities to encrypt/decrypt data:

- using multiple chaotic systems to encode the messages of the various Alices. Then, each output is multiplexed (combined) in a single signal that is sent trough the communication channel. At the receiver, each Bob has his own chaotic unit and will decode his corresponding message [Fig. 1.3(a)],
- using a single chaotic unit to encode the messages of the various Alices. A single multiplexed signal bearing all the messages is sent to a single receiver where the decryption is performed [Fig. 1.3(b)].

Each possibility highlights fundamental questions concerning the independent synchronization of emitter-receiver pairs injected by a single multiplexed signal (chaos multiplexing), the injection and mixing of each message, the realization of the multiplexing and demultiplexing operations, and the limitations in terms of number of users, bit rates, and computational complexity of the decryption. Most of these fundamental questions have not been deeply investigated. As a matter of fact, the first studies of chaos multiplexing were published late in the 1990's and focused on the question of multiplexed synchronization [17; 18] (no information encoded). They were followed by studies of strategies to encrypt and decrypt multiple messages using chaos synchronization and innovative encoding techniques [19; 20]. None of them, however, were exploiting optoelectronic systems with time delays.

1.3 Outline of the Thesis

This thesis focuses on the two major issues developed in the previous section, security analysis and the development of multi-user architectures with optoelectronic devices.

The present work is organized as follows.

In Chapter 2, we present the basics of chaos theory, synchronization, and cryptography. More specifically, we introduce the fundamental concepts of nonlinear systems, attractors, bifurcations, and the notions of complexity (Lyapunov exponents, dimension, and entropy). We also highlight the particular class of time-delay systems, which appears in many areas of engineering and sciences. Such systems have achieved great success in the development of secure chaos-based communications because of the large dimension of their attractor and strong entropy (apparent randomness). We conclude the chapter by detailing the most-encountered chaos-based cryptographic architectures; they are chaos masking (CMa), chaos shift keying (CSK), and chaos modulation (CMo).

In Chapter 3, we focus on the generation of optical chaos using optoelectronic devices. We review the main mechanisms and principles of operation of semiconductor lasers and detail Arrechi's classification, which justifies most of the schemes used to generate optical chaos. Finally, we describe typical chaotic optoelectronic

devices that exploit either internal or external nonlinearities, and we present their mathematical models.

Security and cryptanalysis of optical chaotic emitter with time-delay are introduced in Chapter 4. The analysis is performed on an edge-emitting laser (EEL) with an optical feedback, with no prior knowledge of the system. Similar to a situation often faced by an eavesdropper, only a scalar time series (light intensity) is available. Here, the security is considered to be the amount of information about the structure and the parameters that a system leaks in its state variables. In the case of time-delay systems, as it will be detailed later, the information on the time delay is of crucial importance to maintain a high level of confidentiality. To extract information from a time series, techniques and metrics from signal processing and information theory will be presented as well as the detection of the time-delay signature. In the case of an EEL with optical feedback, we unveil conditions on the tunable operational parameters (length of the external cavity, pumping current, and strength of the retro-injected light) that allow for strong concealment of the time-delay information. We also highlight the fundamental role of the nonlinear dynamics preceding the appearance of chaos in this system to explain the diversity of time-delay concealments previously observed, and to devise strategies to enhance them.

In Chapter 5, we propose a type-ii architecture to multiplex chaotic optical fields generated by several EELs. We go beyond the traditional approaches of the literature, consisting of an application of WDM on the top of chaotic lasers. We succeed in adapting a fundamental result from the theory of synchronization, known as the active-passive decomposition (APD) using simple optical components. Our solution consists of mutually coupling the emitters using a shared external cavity. A multiplexed optical field is subsequently generated and is injected with the proper coupling strengths into the uncoupled receivers. We derive a general semiclassical model for our global architecture and prove the possibility to achieve perfect independent synchronization of chaos for multiple pairs of lasers, yet sharing a single optical communication channel. We study the influence of the coupling parameters and number of units on the quality of synchronization, the spectral properties of the resulting scheme, and its robustness to parameter mismatch and internal sources of noise (e.g.: spontaneous-emission noise). Finally, we propose theoretical solutions to encrypt simultaneously multiple data streams using either the phase or the amplitude of the optical fields composing the multiplex signal associated with the different lasers.

One of the main issues in multiplexing techniques resides in the generation of suitable carriers to convey data while remaining separable for independent decryption of each user's data stream. Chapter 6 addresses this issue and proposes a type-ii architecture, inspired by the CDMA approach existing in conventional optical communications. Briefly described, CDMA is a spread-spectrum technique that produces and uses carriers (also known as *codes*), that are separable with respect to a statistical criterion, which is different from the time of emission or wavelength used in TDM and WDM, respectively. In this chapter, we show how to generate such codes using an optoelectronic oscillator (OEO) with multiple nonlinear delayed feedback loops. We analyze the statistics and complexity of the generated chaos as well as conditions to achieve orthogonality between each user, a fundamental property

to ensure linear complexity of the decryption with the number of users [21]. The main challenge is that optical chaotic systems generate codes that are highly time-varying, contrary to those of conventional communications designed offline and fixed during the entire transmission. We demonstrate theoretically that our architecture can transmit multiple data streams, and we propose different decoding strategies depending on the level of orthogonality between the codes.

In Chapter 7, we probe new directions to multiplex data with a high degree of confidentiality using time-delay systems. Similar to the previous chapter, we propose the use of a single oscillator with multiple delayed feedback loops, except that the data of each user is now encoded directly on each time-delay. The information sources being random, the resulting emitter is a stochastic time-delay system. The fast and random variations of the time delay offer great security with respect to known time-delay identification techniques used in Chapter 4. We focus on the conditions and various encryption strategies that will ensure maximum security, and we describe the method to retrieve the independent variations of each time delay. As a conclusion, we theoretically demonstrate the transmission at high bit rate of multiple data-streams by using the model of an optoelectronic oscillator.

Finally, in Chapter 8 we summarize the main results of the thesis and offer some perspectives and possible directions to investigate.

Chapter 2

Introduction to Chaos Theory, Synchronization, and Cryptography

Abstract

In the general introduction, we have presented the various notions necessary for the achievement of chaos cryptography. In this chapter, we detail fundamental concepts existing in nonlinear sciences, such as chaos theory and synchronization of periodic or chaotic oscillators. We also show how the appropriate combination of these two important notions can lead to innovative physical-layer encryption setups, that ensure a high level of computational security.

2.1 Chaos Theory

The theory of chaos is one of these mathematical and physical frameworks that can instantaneously seize our imagination and interest. It transcends the disciplines: philosophy, religion, mythology, or science each has its own perspectives on chaos. In this section, we give some mathematical insight and facts on the theory of chaos. We will start from a historical point of view that lays the grounds of what is known today as nonlinear science and chaos theory[1]. Then, we will present fundamental concepts such as the theory of dynamical systems, the attractors, bifurcations, route to chaos, and finally give some notions on complexity. These key concepts are illustrated on typical nonlinear systems.

2.1.1 Historical Perspective

In ancient Greek mythology, chaos was the "primeval emptiness preceding the genesis of the universe, turbulent and disordered, mixing all the elements" (adapted from [25]). From this turmoil, order eventually emerged and shaped the world. Though naive, this tale connects two key concepts of the modern theory of chaos and makes them interdependent: order and disorder. Philosopher Aristotle also articulated an important property that characterizes chaos, and will be later known as the sensitivity to initial conditions (SIC). The conclusion he drew was that "the least initial deviation from the truth is multiplied later a thousandfold" [26] (and see Stanford Encyclopedia). With this statement, Aristotle described a form of exponential divergence with time; a slightly modified (one could say disturbed) original concept or "truth" may end with a complete different and unexpected final form.

Finding its roots in social sciences and Greek myth, the idea of chaos and SIC were considered as irrelevant from a scientific point of view for centuries. Only in 1876, as James Clerk Maxwell was developing his kinetic theory, he argued that a small variation in the current state makes the prediction of future states impossible. At this time, however, he was convinced that the key factor rendering this effect visible was the complexity of the system through its large number of variables. Later in 1892, the problem of stability was addressed mathematically by Russian mathematician Aleksandr Lyapunov. For the first time, he calculated the divergence rates between the evolutions of a dynamical system with different initial conditions. At about the same time in 1898, French mathematician Jacques Hadamard remarked that a discrepancy in initial conditions of a system could lead to unpredictable long-term evolution of dynamical systems. In 1908, another French mathematician, Henri Poincaré, deepened Hadamard's idea and concluded that any prediction of future states was impossible, as a result of his famous study of the stability of the three-body problems.

Other significant milestones in the theory of dynamical systems were initiated after Henri Poincaré discoveries. We cite the work of B. Van der Pol and Aleksander Andronov in the 1920's and 1930's on the study of oscillations in relaxed and self-

[1] Excellent historical introductions to chaos theory can be found on the web site of the Stanford Encyclopedia, J. Gleick's book [22], M. Sciamanna PhD thesis [23], and M.W. Lee PhD thesis [24]. Some examples were adapted from these various references.

sustained oscillators, respectively. In the 1950's, Kolmogorov, Arnold, and Moser focused their attention on the persistence of motion of quasi-periodic oscillators and obtained the fundamental KAM Theorem.[1]

In the 1960's, the theory of chaos received unprecedented attention as Edward Lorenz, a meteorologist at the Massachusetts Institute of Technology (MIT), proposed a graphical representation of SIC in a simplified numerical model of the Earth atmosphere. Lorenz wanted to analyze data produced by his model on large sequences; however, at this time computing power was extremely limited. Therefore, to obtain large sequences, one had to run multiple sequential simulations. It is precisely what he did, except that when he initiated the next simulation with the last results from the previous run with a lower precision, he noticed that the model did not duplicate the expected evolution that a single simulation would have produced (see Fig. 2.1).

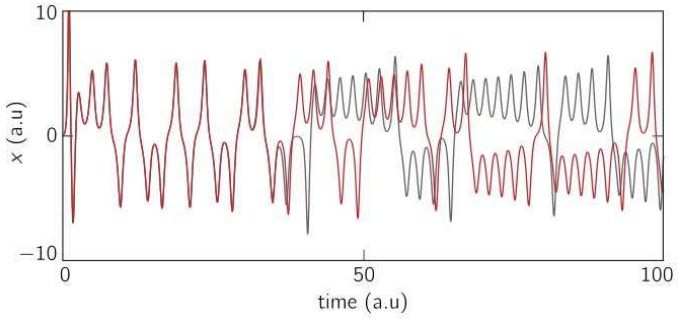

Figure 2.1: Numerical evidence of the sensitivity to initial condition in the Lorenz system, as observed historically by Lorenz. Depicted in grey is the evolution with initial condition with 5-digit precision; depicted in red the same evolution with a duplicated initial condition with a 3-digit precision.

Contrary to his expectations, the lower-precision initial conditions would not have negligible consequences on the system's dynamics. This discovery and subsequent work contribute to explain the inaccuracy of long-term weather forecasting and were summarized by E. Lorenz at the 139th meeting of American Association for the Advancement of Science (AAAS) with this now famous statement: "Does the flap of a butterfly's wings in Brazil set off a tornado in Texas?" [6]. That is how the SIC was also known as the "butterfly effect". After this major turn, research on nonlinear dynamics and chaos theory stepped up.

In 1971, David Ruelle and Floris Takens proposed an alternative mathematical explanation of the turbulence in fluid dynamics based on the existence of so-called "strange attractors" [27]. A couple of years later, Tien-Yien Li and James A. Yorke used the term chaos to describe the erratic and unpredictable behaviors arising in deterministic nonlinear maps. At the same period, Mitchell J. Feigenbaum unraveled universality of behavior occurring in a particular class of systems as they transition to chaos, and derived the Feigenbaum constant [28].

[1]The *KAM Theorem* proves the existence of invariant tori (quasi-periodic trajectories) in the phase space of an integrable hamiltonian system after perturbation.

2.1.2 Fundamentals of Nonlinear Systems Theory

2.1.2.1 Continuous Systems

A system, in which the state is changing with time, is called a dynamical system or oscillator. If the system is time-continuous, then the mathematical description of its evolution is given by an ordinary differential equation (ODE)[1] and a set of initial conditions,

$$\dot{\mathbf{x}}(t) = f(\mathbf{x}(t)), \tag{2.1}$$

$$\mathbf{x}(t_0) = \mathbf{x}_0, \tag{2.2}$$

where $\mathbf{x} \in \mathbb{R}^n$ is the state vector, f is a function $\mathbb{R}^n \to \mathbb{R}^n$, also called vector field, and $\mathbf{x}_0 \in \mathbb{R}^n$ is the initial state vector at initial time t_0. The initial conditions of the system are rarely explicitly given in the representation of a system. If the function f is nonlinear, then the system is said to be nonlinear, and linear otherwise. We define the dimension of a nonlinear system as the size of its state vector (number n of coordinates). This notion of dimension, as discussed later, is of prime importance to explain the emergence of chaotic behaviors in this type of system.

As an example, consider the nonlinear pendulum. It is comprised of a point mass m that can swing freely. It is at a distance l from its pivot and subject only to gravity g. The position of the mass is given by its angle θ, and its speed is given by $v = \dot{\theta}$. These are the two quantities necessary to describe its evolution,

$$\begin{cases} \dot{\theta} = v, \\ \dot{v} = -2\lambda\omega_0 v + \omega_0^2 \sin\theta. \end{cases} \tag{2.3}$$

The frequency of the oscillator is $2\pi\omega_0 = \sqrt{g/l}$ and the damping ratio is denoted by $\lambda > 0$. With the notation of Eq. 2.1, the state vector is given by $\mathbf{x} = (\theta, v)^T$ and the vector field by $f = (f_\theta, f_v)^T = (v, -2\lambda\omega_0 v + \omega_0^2 \sin\theta)^T$.

2.1.2.2 Discrete Systems: Maps

If a system takes its values only at regularly distributed instants, it is called time-discrete or discrete. Its mathematical representation is given by a map, which reads with the previous notations of Eqs. 2.1-2.2

$$\mathbf{x}_{k+1} = f(\mathbf{x}_k), \tag{2.4}$$

$$\mathbf{x}_{k_0} = \mathbf{x}_0, \tag{2.5}$$

with k the time index, k_0 the initial discrete time, and $\mathbf{x}_0$ an initial vector.

Concerning nonlinear maps, we cite the logistic map that models the behavior of predator-pray and was proposed by Robert May [29]. It is a discrete-time analog of the logistic equation and it reads

$$x_{n+1} = \mu x_n (1 - x_n), \tag{2.6}$$

where x_n represents the population at year n and $\mu > 0$ the rate of maximum population growth.

[1] If the system's mathematical representation does not depend explicitly on time, it is said to be *autonomous*.

2.1.2.3 Time-Delay Systems

In the two previous cases, the evolution of the state depends only on the current state (continuous time) or previous time (discrete time). Here in time-delay systems, it depends also of state in the past, a delayed state. They are mathematically described by delay differential equations (DDE),

$$\dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \mathbf{x}(t-\tau)) \text{ for } t > \tau, \tag{2.7}$$

$$\mathbf{x} = \varphi(t) \text{ for } t \in [0, \tau], \tag{2.8}$$

with $\varphi : \mathbb{R} \to \mathbb{R}^n$ a vectorial function. Contrary to systems described by ODEs, or maps, it is necessary to specify the initial conditions over a complete interval.

Time-delay or delayed systems have received considerable attention due to their peculiar properties such as infinite degrees of freedom, very large dimension of the corresponding attractor, which is often proportional to the time-delay τ.

Historically, one of the first time-delay systems ever exhibited was a Mackey-Glass system, named after the two physiologist who discovered it [30]. It models the production of blood cells in the human body and takes into account the delay existing between the genesis of cells and their maturation before injection in the blood stream. The system is described by

$$\dot{x}(t) = -ax(t) + \frac{bx(t-\tau)}{1 + x(t-\tau)^n}, \tag{2.9}$$

with $x \in \mathbb{R}$ the state variable, $a, b, n \in \mathbb{R}$ parameters of the models, and τ the time delay.

2.1.3 Notion of Stability of Nonlinear Systems

The concept of stability is ubiquitous in dynamical system theory and it underlies the notions of attractors, bifurcation theory, and synchronization. We focus on definitions for continuous systems (described by Eq. 2.1) .

A vector $\mathbf{x}_e$ is an equilibrium point if

$$f(\mathbf{x}_e) = 0. \tag{2.10}$$

It is possible to define several types of stability:

- **Lyapunov stability:** An equilibrium point is stable in the Lyapunov sense if for all $\varepsilon > 0$, there exists $\delta(t_0, \epsilon)$ such that

  $$\forall t > t_0 \quad \|x(t_0) - x_e\| < \delta(t_0, \varepsilon) \Rightarrow \|x(t) - x_e\| < \varepsilon. \tag{2.11}$$

  It guarantees that the trajectory of the system in phase space will remain in the vicinity of the equilibrium point if the initial state belongs to this vicinity. If δ does not depends on t_0, the stability is said to be *uniform*.

- **Asymptotic stability:** An equilibrium point is asymptotically stable if

  $$\|x(t_0) - x_e\| < \delta(\varepsilon) \Rightarrow \lim_{t \to \infty} \|x(t) - x_e\| = 0. \tag{2.12}$$

Asymptotic stability includes the Lyapunov stability, but imposes for all trajectories initiated in the neighborhood of the equilibrium point to converge asymptotically to it. Furthermore, a system is globally asymptotically stable if for all trajectories $x(t)$, $\lim_{t\to\infty} \|x(t) - x_e\| = 0$; in other words the system has a unique equilibrium point.

A major inconvenient with the definition of stability is that it requires the finding of the system's trajectory. Nevertheless, methods exist to determine the stability considering the system in its differential form Eq. 2.1:

- **The indirect Lyapunov method:** It consists of analyzing the eigenvalues of the linearized system at the equilibrium point $(\partial f/\partial \mathbf{x})_{\mathbf{x}=\mathbf{x}_e}$. If the linearized system is uniformly asymptotically stable then the nonlinear system described in Eq. (2.1) is locally asymptotically stable at equilibrium point $\mathbf{x}_E$.

- **The direct Lyapunov method:** It relies on the Lyapunov theorem, that provides information on the global asymptotic stability of a system by constructing an energy function $V(\mathbf{x})$ and study how its time derivative behaves. The results can be summarized in Table 2.1 (adapted from [31]).

$V(\mathbf{x})$	$-dV(\mathbf{x})/dt$	Conclusion on stability
Locally definite positive (ldp)	locally positive	stable
ldp and decrescent	locally positive	uniformally stable
ldp and decrescent	ldp	asymptotically stable
definite positive and decrescent	definite positive	globally asymptotically stable

Table 2.1: Synoptic view on the Lyapunov method and its conclusion on stability.

As an example, we apply the direct Lyapunov method to the relaxed damped nonlinear oscillator defined by $\ddot{x}(t) - 2\lambda\omega_0\dot{x}(t) + \omega_0^2 \sin(x(t)) = 0$, with $\omega_0, \lambda > 0$. Evidently, the equilibrium point is $x_e = 0$. We consider the Lyapunov function $V(x,t) = \frac{1}{2}x(t)^2 + \omega_0^2 \cos^2(x(t))$ which is positive definite. We have for the time derivative $\dot{V}(x,t) = \dot{x}\left(\ddot{x} - \omega_0^2 \sin(x)\right) = -2\lambda\omega_0\dot{x}^2(t)$, which is evidently negative definite. As a consequence, the Lyapunov theorem concludes for a damped oscillator, that its equilibrium point is globally asymptotically stable.

There exists other types of stability such as the exponential asymptotic stability with a corresponding Lyapunov theorem. For more details on the question of stability, we suggest the reference [32] to the reader.

2.1.4 Attractors and Bifurcations Theory

2.1.4.1 Notion of Phase Space

In physics, a space comprising all the accessible states of dynamical system (position and velocity, to a large sense) is called the *phase space*. For a time-continuous system with finite dimension n, the phase space is spanned by the components of its state vector, in the case of time-delay system its dimension is infinite [33].

The evolution of the dynamical system is represented by a trajectory in phase space called the orbit. An important property of a deterministic system is that its trajectory cannot self-intersect; otherwise it would contradict the uniqueness of evolution of a system for a given initial condition as stated by the Cauchy theorem.

2.1.4.2 Notions of Dissipation and Attractors

As highlighted by Ruelle and Takens [27], a complex time evolution may sometimes be advantageously represented in the phase space (S). Depending on the dissipation of a given system, the trajectories in a region of phase space may eventually converge to a subset $A \subset S$, which is typically referred to as an attractor. In the case of continuous-time system, the dissipation is defined by analyzing the evolution of a volume V of phase space,

$$\dot{V}(t) = \int_V \nabla \cdot f d\mathbf{x}, \tag{2.13}$$

with $\nabla \cdot f$ the divergence of the vector field f and defined by $\nabla \cdot f = \sum_{i=1}^{n} \partial f_i / \partial x_i$ with f_i and x_i the components of the vector field f and state vector $\mathbf{x}$, respectively.

For the example of the pendulum, the vector field is defined by $f_x = v$ and $f_v = -\gamma v - \omega_0^2 \sin x$; the divergence reads $\nabla \cdot f = \partial f_\theta / \partial \theta + \partial f_v / \partial v = -2\lambda\omega_0$. The lack of damping ($\lambda = 0$) makes the pendulum a conservative system; otherwise ($\lambda > 0$) the divergence is less than zero, and the pendulum is dissipative.

If the system is a map, the dissipation is defined after the amplitude of the determinant of the Jacobian matrix associated to the discrete vector field: $|\det(\nabla_{\mathbf{x}} f)|$. If $|\det(\nabla_{\mathbf{x}} f)| = 1$, the system is conservative, else if $|\det(\nabla_{\mathbf{x}} f)| < 1$ the system is dissipative.

An Example for discrete system is the baker's map. This transformation is defined on the unit square mapped to itself and is named after the baker, because it squeezes, cuts, and stacks iteratively the unit square, as a baker would do with the dough. Mathematically this system is modelled by

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & a \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} + \begin{pmatrix} 0 \\ \begin{cases} 0, & x_n \leqslant \frac{1}{2} \\ \frac{1}{2}, & x_n > \frac{1}{2} \end{cases} \end{pmatrix} (\text{mod } 1). \tag{2.14}$$

The nonlinearity results in the modulo operation that is responsible for the cut-and-stack. In this map, the Jacobian matrix is evidently $\nabla f = \begin{pmatrix} 2 & 0 \\ 0 & a \end{pmatrix}$ and its determinant is equal to $\det(\nabla f) = 2a$. According to the definition, if $a \in [0, \frac{1}{2}[$ the system is dissipative with a squeezing of volume that imposes the trajectories to

asymptotically converge in a bounded region of the phase space; otherwise if $a = \frac{1}{2}$ the map is conservative.

Typically, a nonlinear dissipative system can exhibit basic attractors with four different geometries: (i) an *equilibrium point* (EP or fixed point) corresponds to a stationary evolution of the system, (ii) a *limit cycle* (LC), which is a closed curve in the phase space and corresponds to a periodic evolution in the time domain with frequency f_0, (iii) a *torus* (T), which is also a closed curve in phase space embedded in a torus and corresponds to a quasi-periodic motion in the time domain, defined by the coexistence of multiple incommensurate frequencies f_{0i}, and (iv) a *strange attractor* which is a complex set with a *fractal geometry*[1] usually associated with unpredictable and erratic evolution of an oscillator in the time domain, called chaotic fluctuations.

2.1.4.3 Bifurcations Theory

The theory of bifurcations studies the topological changes of a trajectory of a dynamical system defined by

$$\dot{\mathbf{x}} = f(\mathbf{x}, \lambda),\ f : \mathbb{R}^n \to \mathbb{R}^n,\ x \in \mathbb{R}^n,\ \lambda \in \mathbb{R}^p, \tag{2.15}$$

in response to smooth variations of the system's parameter $\lambda \in \mathbb{R}^p$, commonly called the bifurcation parameter. A bifurcation is often seen as a collision or exchange of stability between two or multiple attractors (equilibrium points, limit cycles, torus), or two or multiple manifolds[2] [35; 36; 37].

When attractors collide, this induces a local topological modification of the phase space in the immediate vicinity of the collision; this is referred to as a *local bifurcation*. However, when two manifolds collide and exchange their stability the phase space structure may be globally affected; this is referred to as a *global bifurcation*. The complexity of the bifurcation is given by its *codimension*, an integer representing the number of scalar parameters amongst the vector λ that one must vary to observe a bifurcation. It represents the codimension of the parameter vector λ.

The last characteristic of a bifurcation is related to the nature of the collision between the attractors and/or manifolds. The bifurcation is said to be *supercritical* if the collision occurs with a stable structure at $\lambda > \lambda_c$, leading to a smooth transition, λ_c being the critical value of parameter for which the bifurcation occurs. On the other hand, the bifurcation is said *subcritical* if the collision occurs with an unstable structure existing for $\lambda > \lambda_c$; this results in a sudden transition.

Various bifurcations have been studied, especially those with a low codimension (one or two) as well as global bifurcations. We can cite the most common bifurcations encountered in dynamical systems:

- Local bifurcations

[1] A fractal geometry characterized a "rough or fragmented geometric shape that can be split into parts, each of which is (at least approximately) a reduced-size copy of the whole" as described by B. Mandelbrot in [34].

[2] *Manifold:* In differential geometry, a manifold is a smooth (highly differentiable) mathematical space.

- **Saddle-node bifurcation:** Before the bifurcation, two equilibrium points (EP) exist. They collide and disappear; no equilibrium points remain after the bifurcation.
- **Transcritical bifurcation:** Before the bifurcation, two equilibrium points exist with different stability. They collide and after the bifurcation their stability is exchanged.
- **Pitchfork bifurcation:** A type of bifurcation that occurs in system with symmetry. The bifurcation can be *supercritical*, when a stable equilibrium point EP_s becomes unstable and two new stable equilibrium points appears. The bifurcation can be *subcritical* when two unstable fixed points (EP_{u1}, EP_{u2}) coexist with a third stable equilibrium point EP_s that respectively disappear and becomes unstable after the bifurcation.
- **Hopf Bifurcation:** This bifurcation can be supercritical or subcritical. In the first case, an equilibrium point looses its stability while a limit cycle is appearing. In the latter case, an unstable limit cycle coexists with a stable equilibrium point before the bifurcation. After the bifurcation, the limit cycle disappears and the equilibrium point becomes unstable.
- **Period-doubling bifurcation:** An existing limit cycle with period T disappears, a newborn limit cycle appears with period $2T$.
- **Neimark-Sacker bifurcation:** A limit cycle disappears and a torus attractor emerges.

- Global bifurcations:
  - **Homoclinic bifurcation:** A limit cycle and a saddle point (unstable equilibrium point) collide together. This results in the appearance of a homoclinic orbit defined as particular trajectory of the system $x_H(t)$ that satisfies the following limits' equality,

$$\lim_{t\to-\infty} x_H(t) = \lim_{t\to\infty} x_H(t) = p, \tag{2.16}$$

    with p an equilibrium point.
  - **Heteroclinic bifurcation:** A limit cycle and two or more saddle point collide together. This results in the appearance of an heteroclinic orbit $x_{He}(t)$ that satisfies

$$\lim_{t\to-\infty} x_{He}(t) = p_1 \text{ and } \lim_{t\to\infty} x_{He}(t) = p_2, \tag{2.17}$$

    with $p_1 \neq p_2$ two equilibrium points.

2.1.5 Chaos Theory

When one is asked to define chaotic behavior, there is no single answer; for G.P. William, "Chaos is sustained and disorderly-looking long term evolution that satisfies certain special mathematical criteria and that occurs in a deterministic nonlinear system" [25]; for E. Lorenz it is also "The property that characterizes a dynamical

system in which most orbits exhibit sensitive dependence." In this subsection, we will give necessary conditions to observe chaotic behaviors in dynamical system.

In the case of a continuous system, there are three basic ingredients to ensure the emergence of chaotic behaviors: (i) a sufficient dimensionality, (ii) a nonlinearity, and (iii) a proper set of parameters that will allow the strange attractor to be the stable limit set.

The condition of dimensionality comes as a corollary of the Bendixon-Poincaré theorem, which states that given a differential equation $\dot{\mathbf{x}} = f(\mathbf{x})$ in the plane (2D) and assuming $\mathbf{x}(t)$ is a solution curve which stays in a bounded region, then either $\mathbf{x}(t)$ asymptotically converges for to an equilibrium point, or it converges to a single periodic limit cycle. It is necessary to have a system with dimension greater or equal to three (which is precisely the case of the Lorenz system studied in the next paragraph).

The nonlinearity is also necessary to couple the state variables in such a way that solutions other than the predictable solution of a linear system $\dot{\mathbf{x}}(t) = A(t)\mathbf{x}(t)$, with $A \in \mathscr{M}_{n\times n}(\mathbb{R})$, of the form $\mathbf{x}(t) = \mathbf{x}_0 \exp\left(\int_{t_0}^{t} A(u)du\right)$, appear.

2.1.5.1 Route to Chaos

Contrary to linear systems, nonlinear systems can exhibit various dynamics apart from chaotic ones (if the dimension is large enough). This diversity and the transitions (bifurcations) occurring between each of them can be probed by making varying one or several system's parameters (called bifurcation parameters). This makes it possible to observe a cascade of bifurcations to stable attractors until a strange attractor is reached. This is called a *route to chaos*. In the literature, the routes to chaos are graphically represented by a bifurcation diagram where the system's output is plotted as a function of the bifurcation parameter. There exists a large variety of routes but amongst them, three scenarios are often encountered and may be considered as universal [38]:

- **Intermittency route to chaos:** Also called Pomeau-Maneville route to chaos [39], in this scenario a single bifurcation is responsible for the alternation (or intermittence) of zones of chaotic ("turbulent") motion with zones of smooth regular ("laminar") motion. As the bifurcation parameter increases, the turbulent zones last longer and eventually, above a critical threshold, the system is always turbulent (or chaotic). The intermittency route to chaos is classified into three different types (I,II,III) depending on how the destabilization occurs.

- **Ruelle-Takens-Newhouse route to chaos:** Also called the quasi-periodic route to chaos. It consists of the following succession of three bifurcations when the bifurcation parameter is steadily increased: First, a Hopf bifurcation that leads to a stable limit-cycle of period T, second a Torus bifurcation that leads to a quasi-periodic dynamics with two incommensurate frequencies associated with a torus attractor T^2, and finally a last bifurcation turns the torus T^2 into a new attractor T^3 with three incommensurate frequencies, which rapidly destabilizes into a strange (chaotic) attractor.

- **Period-doubling route to chaos:** Also called Feigenbaum route to chaos, in this scenario, a steady state is first destabilized through a Hopf bifurcation resulting in a limit cycle of period T. Then, this limit cycle undergoes a cascade of period-doubling bifurcations until the $n-$th limit cycle of period 2^nT destabilized and the strange attractor becomes stable. This route is illustrated in Fig. 2.2.

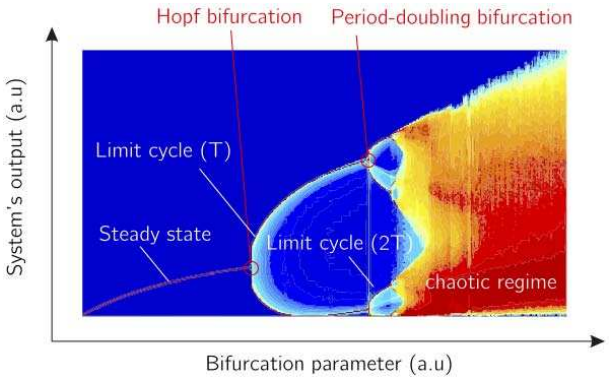

Figure 2.2: Experimental bifurcation diagram of an optoelectronic oscillator picturing a period-doubling route to chaos (courtesy of former UMR 6603 GTL-CNRS Telecom). States and bifurcation points are indicated on the figure.

2.1.5.2 Strange Attractors

In dissipative systems, the trajectory is asymptotically localized in a bounded region of the phase space called attractor. When a system exhibits chaotic behaviors, the time evolution is seemingly random. However, when the system is represented in the phase space, an ordered geometric structure becomes visible. This structure was originally called *strange attractor* by D. Ruelle and F. Takens. To illustrate it, we consider a celebrated example: the Lorenz system. It is defined as

$$\dot{x} = \sigma(y - x), \tag{2.18}$$
$$\dot{y} = \rho x - y - xz, \tag{2.19}$$
$$\dot{x} = xy - \beta z, \tag{2.20}$$

with σ the Prandtl number, ρ the Rayleigh number, and $\beta = 4/(1 + a^2)$ with a a horizontal wavenumber for the convection cells. All the parameters are positive. This is a simplified model of the convection in the atmosphere. In the phase plane defined by the coordinates (x, y, z), this system reveals a butterfly shape that later became emblematic of the chaos theory. Times series and 3D representation of the attractor are given in Fig. 2.3.

The strange attractor is said to be *fractal*, if its dimension is non-integer and has a complex geometry. Considerations on the calculation of dimension of attractor will be detailed in the following subsection.

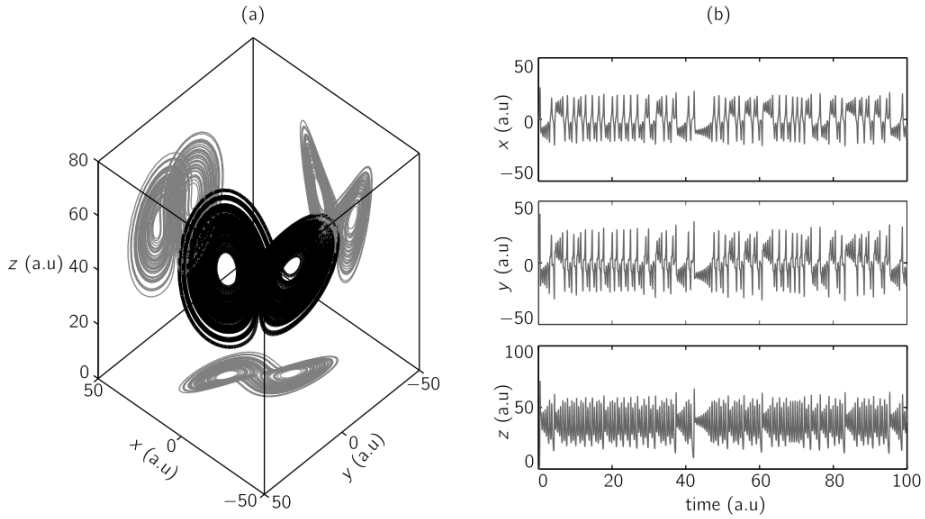

Figure 2.3: Numerical simulation of the Lorenz flow with $\sigma = 10$, $\rho = 28$ and $\beta = 8/3$. (a) The strange attractor with a butterfly shape in the 3D phase space (x, y, z). (b) Time series of each state variables (adapted from [23]).

2.1.5.3 Sensitivity to Initial Conditions (SIC) and Lyapunov Exponents

In the chaotic regime, there exists one or several directions in phase space for which an hypervolume of phase space would be stretched as time progresses. As a consequence, two neighboring trajectories arbitrary close will progressively move away from each other while remaining on the strange attractor. The system is said to be sensitive to initial conditions (SIC). Uncertainty of the initial conditions of a given system is unavoidable due to finite precision of measurement and will be amplified with time, preventing any possible forecasting. This is one of the fundamental properties of chaotic systems that E. Lorenz was the first to observe (see Fig. 2.1).

Intuitively, the unpredictability will depend on how fast two close trajectories diverge and it is consequently related to the expansion's speed of the initial hypersphere in all the directions of the phase space. The expansion rates are usually referred to as *Lyapunov exponents*. Mathematically, we consider a trajectory $\mathbf{x}(t)$ solution of the differential system Eq. 2.1 and an elementary perturbation's vector $\delta\mathbf{x}(t)$ solution of the linearized equation around the trajectory $\mathbf{x}(t)$: $\delta\dot{\mathbf{x}}(t) = \nabla f_{\mathbf{x}}\delta\mathbf{x}(t)$ and $\delta\mathbf{x}(0)$ denoting the initial perturbation. The components $\delta\mathbf{x}_i$ of the perturbation will be stretched or contracted with specific rate λ_i as illustrated in Fig. 2.4.

The rates are defined for a continuous system by

$$\lambda_i = \lim_{T\to\infty} \frac{1}{T} \log\left(\frac{\|\delta\mathbf{x}(T)\|}{\|\delta\mathbf{x}(0)\|}\right). \tag{2.21}$$

If an iterated map is considered, a small perturbation evolves as $\delta\mathbf{x}_n = \nabla f_{\mathbf{x}_{n-1}}\delta\mathbf{x}_n$. It is analogous to a geometric series except that the reason will change at every steps. By analogy to the expression in continuous time, the Lyapunov exponents are defined by $\lambda_i = \lim_{n\to\infty} 1/n \log\left(\|\delta\mathbf{x}_n\| / \|\delta\mathbf{x}(0)\|\right)$. The set of all the Lyapunov exponents is called the *Lyapunov spectrum*. For a system to be chaotic, the spectrum must have

at least one positive Lyapunov exponent to guarantee the existence of SIC.

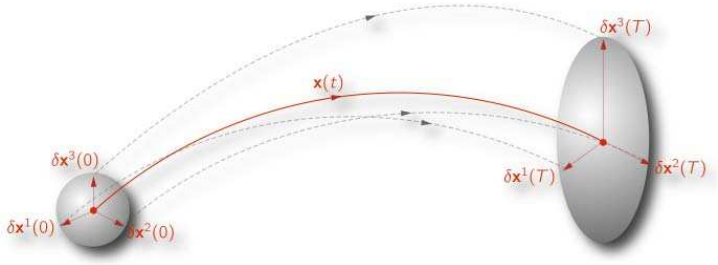

Figure 2.4: Representation of the deformation of a 3D hypersphere along the extension/contraction direction of the dynamical flow along the trajectory $\mathbf{x}(t)$.

Consider the Baker's Map to illustrate a straightforward calculation of the Lyapunov spectrum. An infinitesimal sphere is centered on a trajectory point (x_n, y_n). The perturbated coordinates along each direction are defined by $\bar{x}_n = x_n + \delta x_n$ and $\bar{y}_n = y_n + \delta y_n$. The evolution of the perturbation after n iterations of the map reads $\delta x_n = 2^n \varepsilon_{x0}$ and $\delta y_n = a^n \delta y_0$ with $\delta x_0, \delta y_0$ the initial perturbations. The Baker's map stretches the phase space in the $x-$direction, while contracting it in the $y-$direction. This gives an illustration on how it is possible to have infinitely diverging trajectories yet confined in finite phase-space volume.

2.1.6 Complexity

The complexity of chaos is characterized by two quantities: *dimension* and *entropy*. This subsection is mainly devoted to their intrinsic definitions and connections with the Lyapunov spectrum.

2.1.6.1 Dimension and Kaplan-Yorke Conjecture

To characterize the dimension of an attractor and its fractal geometry, one can use the *fractal dimension* (also known as *Kolmogorov capacity*). Self-similar structure such as fractals do not have an integer dimension such as typical mathematical objects of Euclidean geometry. To calculate this dimension, the attractor is discretized, covered with $N(\varepsilon)$ hyperboxes of size ε (see Fig. 2.5(a)). The idea behind the fractal dimension is to observe the evolution of the number of hyperboxes necessary as their size tends to zero (refinement of the discretization). The definition reads

$$d_c = \lim_{\varepsilon \to 0} \frac{\log(N(\varepsilon))}{\log(1/\varepsilon)}. \tag{2.22}$$

There is another approach to calculate the dimension of an attractor. Instead of discretizing the attractor, the whole phase space is partitioned with hyperboxes of size ε. In the phase space, the attractor intersects a finite subset of boxes (see Fig. 2.5). We introduce the probability p_i that the attractor visit the ith hyperbox and we define the *information dimension*,

$$d_I = \lim_{\varepsilon \to 0} \frac{\log(I(\varepsilon))}{\log(1/\varepsilon)}, \tag{2.23}$$

with $I(\varepsilon) = -\sum_{i=1}^{N(\varepsilon)} p_i \log(p_i)$, the information relative to the attractor geometry with a precision ε.

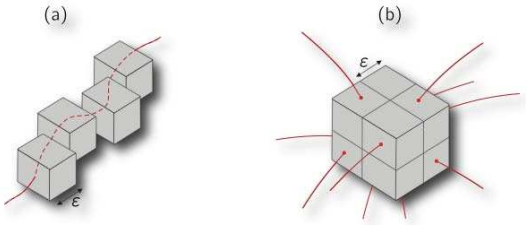

Figure 2.5: (a) Discretization of the attractor for the calculation of the fractal dimension in a 3D case. (b) Discretization of the phase space for the calculation of the information dimension. The attractor (red solid lines) intersects several boxes.

Although based on different calculation principles, these two dimensions are equal if the attractor visits with identical probability all the hyperboxes, i.e. $p_i = 1/N(\varepsilon)$. In most cases, however, this situation is not satisfied and $d_I \leq d_c$.

Numerically, the calculation of the information dimension becomes rapidly intractable as the dimension n of the phase space increases. To overcome this, D.T. Kaplan and J. Yorke came up with a conjecture linking the information dimension d_I with the Lyapunov spectrum [40],

$$d_I = d_{KY} = j + \frac{1}{|\lambda_{j+1}|} \sum_{i=1}^{j} \lambda_i, \tag{2.24}$$

with j the index that satisfy $\sum_{i=1}^{j} \lambda_i \geq 0$ and $\sum_{i=1}^{j+1} \lambda_i \leq 0$, and d_{KY} the Lyapunov or Kaplan-Yorke dimension.

2.1.6.2 Entropy and Pesin Inequality

The *Kolmogorov-Sinaï entropy* of a dynamical system characterizes how the precision of the prediction of a future state decreases with time due to the uncertainty of the initial conditions. It measures the average rate of information loss. Its definition supposes a partition of the phase state as in the case of the information dimension d_I. In practice, Kolmogorov-Sinaï entropy is defined as

$$h_{KS} = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} H\left(\mathscr{B}\right), \tag{2.25}$$

with $\mathscr{B} = \{B_i\}_{i=1,\ldots,m}$ a partition of the phase space with diameter ε that captures the attractor in the phase space during a time interval of length n (more details in footnote), $H\left(\mathscr{B}\right) = -\sum_{i=1}^{m} \mu\left(B_i\right) \log\mu\left(B_i\right)$, μ a probability measure.[1]

[1] **Notes on Kolmogorov-Sinaï entropy**: Entropy for dynamical systems is rigorously defined in the theoretical framework of measure-preserving dynamical systems. This considers a probability space $(X, \mathscr{A}, \mu, f)$ with X the state space, $\mathscr{A} = \{A_i\}_{i=1,\ldots,p}$ a partition of X, μ a probability measure on X, and f an automorphism of X. Consider the *refinement* of two partitions $\mathscr{C} \vee \mathscr{D} =$

This quantity is also linked with the Lyapunov spectrum through the Pesin inequality [42] defined as

$$h_{KS} \leq \sum_{i|\lambda_i>0} \lambda_i. \tag{2.26}$$

2.2 Synchronization

2.2.1 Historical Perspective

Synchronization comes from the greek words "*syn*" (with) and "*chronos*" (time), literally "occurring at the same time". Synchronization of oscillators is a universal and ubiquitous phenomenon in nature [43]. It was discovered by Christiaan Huygens in 1665, who observed perfect in- and out-of-phase oscillations of two pendulum clocks dynamically coupled by their common support (see Fig. 2.6) and concluded on the existence of "sympathy on two clocks" [44].

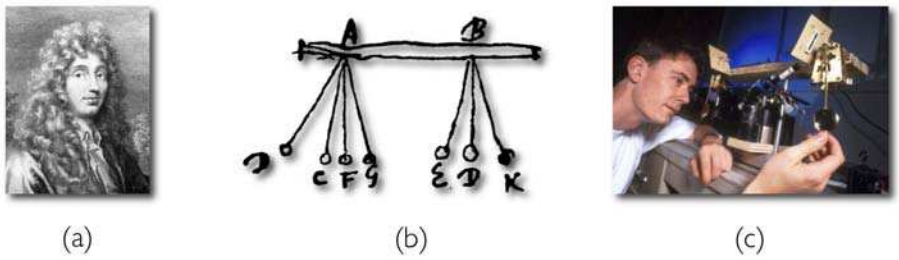

Figure 2.6: Portrait of Christiaan Huygens (a), his drawing of the synchronization experiment between two clocks located respectively in position A and B in (b), and the experiment revisited at the School of Physics at Georgia Tech [45] (c).

Approximately two centuries later in 1870, Lord Rayleigh reported for sound pipes their possibility to sound at unison and the effect of *quenching*, known as the suppression of oscillations in interacting systems [46]. In the 1920's, V. Appleton [47] and B. van der Pol [48] studied the synchronization phenomenon in triode generators under the influence of weak synchronization signals. Later in the 1940's, V. Adler described the locking phenomenon, a key concept in the synchronization of periodic oscillator [49]. Synchronization phenomena continue to be reported with spectacular examples in nature like the synchrony of flashing fireflies [50], chirping crickets [51], or more recently genetic clocks [52]. Such a phenomenon has also found an application in telecommunication and is used to synchronize electronic circuits with the phase-

$\{C_i \cap D_j | \mathscr{C} = \{C_i\}_{i=1,\dots,n}$ and $\mathscr{D} = \{D_j\}_{j=1,\dots,n}\}_{i,j}$, Kolmogorov-Sinaï entropy is defined as

$$h_{KS} = \sup_{\mathscr{A}} \lim_{n\to\infty} \frac{1}{n} H\left(\bigvee_{k=0}^{n-1} f^{-k}(\mathscr{A})\right).$$

The supremum is taken over all possible partitions $\mathscr{A}$ for the limit of the entropy H of partition $\mathscr{B} = \bigvee_{k=0}^{n-1} f^{-k}(\mathscr{A}) = \{B_i\}_{i=1,\dots m}$, that reads $H(\mathscr{B}) = -\sum_{i=1}^{m} \mu(B_i) \log \mu(B_i)$. Assuming $\mathscr{B}$ is a generating partition, the supremum over $\mathscr{A}$ corresponds to the limit to zero of diameter of partition $\mathscr{B}$. This finally leads us to Eq. 2.25. A detailed analysis can be found in [41].

locked loops (PLL). We recommend to the reader an excellent and more detailed introduction in [43].

2.2.2 Synchronization of Periodic Oscillators

Historically, the synchronization of periodic oscillators was studied with two types of interactions or couplings: unidirectional (forcing) or bidirectional (mutual). In the unidirectional configuration, a master (decoupled) drives the dynamics of a slave system. Each oscillator is characterized by its free-running frequency ω_m and ω_s, : respectively. The coupling strength is denoted η. As a result, the master (ω_m) forces the slave (ω_s) to lock on its frequency; this depends on the set of parameters (ω, η). In this parameter plane, the frequency locking region forms what is known as an *Arnold tongue* [53] (see Fig. 2.7(a2)). This triangle-shaped zone illustrates the increasing of the synchronization frequency range with the amplitude η [Fig. 2.7(a2)]. As a result, the phase of each oscillator are bounded $|\phi_m(t) - \phi_s(t)| = \text{constant}$.[1] If the frequency of master and slave are identical, their phases are also synchronized $\phi_m(t) = \phi_s(t)$. With a mutual interaction, each system influences the dynamics of its coupled partner. The frequency of each system is denoted $\omega_{1,2}$ and the coupling from System 1 to System 2 denoted η_1 (respectively η_2 for System 2 to System 1) as depicted in Fig. 2.7(b1). In the context of mutual interactions, the frequency of each oscillator changes and becomes $\Omega_{1,2}$. If $\omega_1 < \omega_2$, then the frequencies of the interacting systems typically satisfy $\omega_1 < \Omega_1, \Omega_2 < \omega_2$. When the coupling is strong enough, then there is a mutual frequency locking and $\Omega_1 = \Omega_2 = \Omega$ and $\omega_1 < \Omega < \omega_2$ [see Fig. 2.7(b2)][2]. Under these conditions, the phases of each oscillators are also locked when the oscillators have different frequencies. When the oscillators are nearly identical, then they can be synchronized in phase or anti-synchronized (as observed by C. Huygens). This paragraph has been inspired by a detailed description made in [43].

2.2.3 Synchronization of Chaotic Oscillators

The synchronization of chaotic systems with different initializations was long thought to be counterintuitive or impossible, especially because of the sensitivity to initial conditions preventing two identical chaotic systems from displaying perfectly correlated time evolutions. However, in 1983, Fujisaka and Yamada paved the way with their pioneering studies on chaos synchronization [54; 55; 56] followed by the work of L. Pecora and T. Carroll, who demonstrate theoretically and experimentally the existence of complete synchronization with an electronic version of a Lorenz system [7].

[1] In the case of unidirectional forced oscillator, the synchronization is seen as a stabilization of the phase difference between master and slave.

[2] In particular cases involving complicated interactions between the oscillators, the frequency of the synchronized system can lie outside of the frequency range $[\omega_1, \omega_2]$, an exceptional feat.

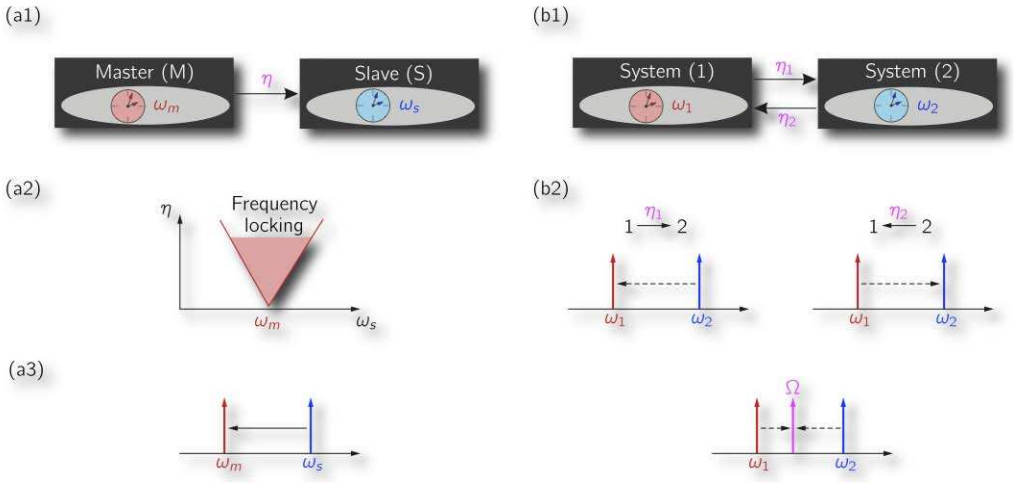

Figure 2.7: Illustration of unidirectional and mutual synchronization of two oscillators, respectively (a1) and (b1). In the unidirectional case, the master (M) pulls the slave's frequency ω_s (dotted arrow), and eventually under appropriate coupling strength locks it (a2) and $\omega_m = \omega_s$. In the mutual case, both systems interact resulting in a push-pull effect on the frequency of each system. Under appropriate coupling conditions, the two systems locks on a single frequency Ω different from their respective free running frequencies $\omega_{1,2}$.

2.2.4 Mathematical Definition and Types of Synchronization

There exist various types of synchronization. We propose in this subsection a rapid overview of their mathematical formulations:

- **Complete Synchronization:** The states of the interacting systems $\mathbf{x} \in \mathbb{R}^n$ and $\mathbf{y} \in \mathbb{R}^n$ converge asymptotically to the same evolution:

$$\lim_{t\to\infty} \|\mathbf{x}(t) - \mathbf{y}(t)\| = 0. \tag{2.27}$$

  This type of synchronization was described in [57].

- **Generalized Synchronization:** In generalized synchronization, we suppose that the states of the two interacting systems are functionally synchronized. There exists a function $\psi : \mathbb{R}^n \to \mathbb{R}^n$ such that

$$\lim_{t\to\infty} \|\mathbf{x}(t) - \psi(\mathbf{y}(t))\| = 0. \tag{2.28}$$

  This type of synchronization was proposed for the first time in [58].

- **Anticipating Synchronization:** In most cases described so far, the interaction between the systems were instantaneous. In practice and particularly in the optoelectronic systems described in Chapter 3, the interactions are delayed. This leads to the definition of the anticipating synchronization,

$$\lim_{t\to\infty} \|\mathbf{x}(t) - \mathbf{y}(t-\tau)\| = 0, \tag{2.29}$$

  with τ the time delay. This type of synchronization was proposed for the first time in [59].

- **Phase synchronization:** It is phenomenologically described for the periodic oscillators and can also be defined for chaotic systems. It relies on an extension of the notion of phase based on an analytical signal $s(t)$ derived from the state of the system $x(t)$,

$$s(t) = x(t) + i\tilde{x}(t) = a(t)e^{i\varphi(t)}, \tag{2.30}$$

  where $x(t) \in \mathbb{R}$, and $\tilde{x}(t) = \frac{1}{\pi} p.v. \int_{-\infty}^{-\infty} \frac{x(u)}{t-u} du$ analytical transform of $x(t)$ with $p.v.$ the Cauchy principal value. In this representation, $a(t)$ and $\varphi(t)$ are the analogs of an amplitude and a phase, respectively. Phase synchronization condition for chaotic systems is then identical to that of a periodic oscillator (considering $\varphi(t)$ in each system as the variable to be synchronized).

For a detailed treatment of the synchronization of nonlinear systems, we recommend to the reader Ref. [60].

The concept of synchronization is of fundamental importance for the chaos-based cryptographic setups that will be described in the next section.

2.3 Chaos-Based Communications

2.3.1 Principles

A chaos transmission chain consists of two parties, classically named Alice (sender) and Bob (receiver), who secretly exchange data on a public communication channel. Alice realizes encryption by embedding a data stream within the noise-like fluctuations generated by her chaotic emitter. Bob possesses an emitter's copy which synchronizes under appropriate coupling conditions. The deterministic nature of chaos implies that the chaotic receiver will only synchronize when the binary symbol "0" is emitted. This *chaos-pass-filtering* property [61] allows for the extraction of the original message.

There exists various methods to realize the message embedding. The most famous ones are *chaos masking* (CMa), *chaos-shift keying* (CSK) and *chaos modulation* (CMo).

2.3.2 Typical Architectures

2.3.2.1 Chaos Masking (CMa)

This approach was demonstrated for the first time in [62; 63; 64]. Alice adds her message $m(t)$ at the output $\mathbf{y}_E(t)$ of her chaotic emitter (E). Generally, the output is defined as a nonlinear function h of the state variable of the emitter $\mathbf{y}_E(t) = h(\mathbf{x}_E(t))$. If the nature of the carrier is different from that of the message, it is possible to precondition it and transform it into a physical signal $\mathbf{m}(t)$ compatible with the carrier. The signal $\mathbf{s}(t) = \mathbf{y}_E(t) + \mathbf{m}(t)$ is then transmitted into the communication channel. The chaotic fluctuations of $\mathbf{y}_E(t)$ act as a *deterministic noise* that cloak the message and prevent an eavesdropper to detect its presence easily. It is assumed that the message's amplitude remains negligible in comparison to the carrier's amplitude to ensure proper concealment and avoid the disturbance in the synchronization process.

Indeed, the signal $\mathbf{s}(t)$ is also used to chaotically synchronize the receiver (R) with (E). If the message is continuous and has a large amplitude, then the output of the receiver may significantly differ from the emitter and the recovery of the message may eventually be compromised. The legitimate receiver Bob recovers an estimate of the message performing the operation

$$\hat{m}(t) = \mathbf{s}(t) - \mathbf{y}_R. \tag{2.31}$$

If the synchronization error is small, then $\hat{m}(t) \approx m(t)$ and the message is decrypted. This is illustrated in Fig. 2.8. This method was one of the first proposed, but it lacks security because of the weak mixing of the message with the chaotic dynamics [65]. One advantage, however, is that any type of message can be transmitted: analogous or digital. This is not the case with the approach of CSK.

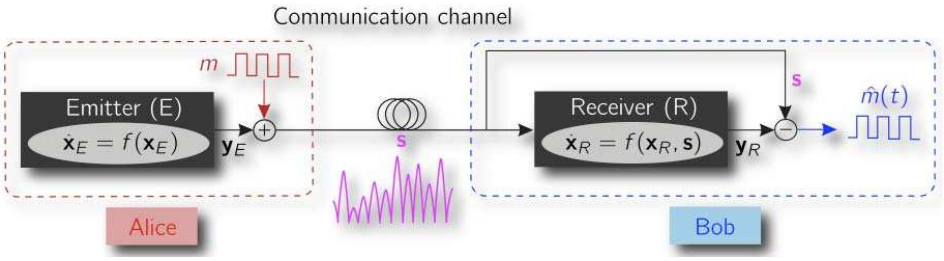

Figure 2.8: Chaos Masking (CMa) architecture.

2.3.2.2 Chaos Shift Keying (CSK)

This approach was demonstrated for the first time in [66; 67] and is tailored for digital messages with a finite set of values. Typically two binary symbols (often denoted "0" and "1") compose the message and activate a switch between two different emitters (E_1) and (E_2).They can be either structurally identical with different parameters or completely different. Alice encrypts her data-stream by switching between these two chaotic oscillators depending on the type of bit to be transmitted. For instance, each time a bit "0" is transmitted, the output of (E_1) $\mathbf{y}_{E1}(t)$ is sent in the communication channel, $\mathbf{y}_{E2}(t)$ otherwise. At the receiving end, Bob has two receivers (R_1) and (R_2), physical copies of (E_1) and (E_2), respectively. Each time that (R_1) (respectively (R_2)) will synchronize with (E_1) (respectively (E_2)), it means that $m(t) = 0$ (respectively $m(t) = 1$) was transmitted by Alice. Therefore Bob can recover the message transmitted by Alice considering the errors of synchronization at each receiver:

$$\hat{m} = 0 \text{ if } y_{R1} - s = 0 \ (m = 0 \text{ transmitted}), \tag{2.32}$$

$$\hat{m} = 0 \text{ if } y_{R2} - s = 0 \ (m = 1 \text{ transmitted}). \tag{2.33}$$

This approach is illustrated in Fig. 2.9(a). It is possible to transmit an M-ary message as well, but it would require 2^M emitters and receivers. The complexity of the decryption in a CSK approach is therefore exponential with the number of users.

It is also possible to simplify substantially the CSK approach and reduce the number of emitters involved. In the case of binary message, it is possible to consider

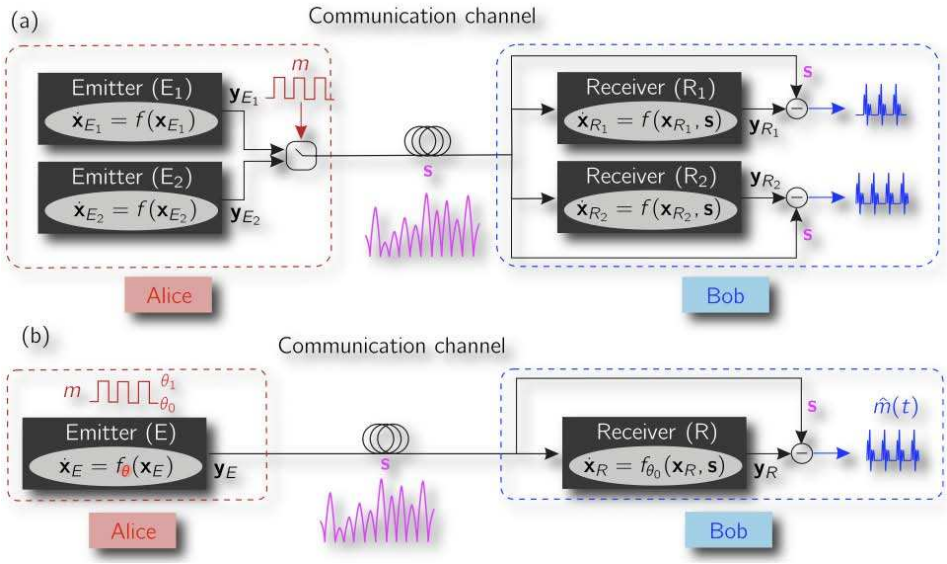

Figure 2.9: (a) Chaos Shift Keying (CSK) with two different emitters, the message m controls a switch. The decryption is performed by monitoring synchronization errors at each receiver output. (b) CSK with a single emitter, the message controls the value of a parameter of the system. The decryption is similar to (a).

a single emitter (E). Alice chooses one parameter θ amongst all of those in (E) and will modulate its value between two different levels: $\theta = \theta_0$ (respectively $\theta = \theta_1$) when $m = 0$ (respectively $m = 1$). To decrypt the message, Bob has a single receiver, with the parameter θ fixed in either of the two values. In this particular configuration, the decryption equation is similar to Eq. 2.34. A fundamental limit of the method is the synchronization time between (E_1,E_2) and (R_1,R_2) [or (E) and (R)] thus reducing the maximum bit rate compared to that of CMa. The security of this method is also considered weak, as the statistics (average or variance) of the transmitted signal may drastically change as the switch between the emitters (or parameters) is performed.

2.3.2.3 Chaos Modulation (CMo)

This approach was demonstrated for the first time in [68; 69]. It consists of the inclusion of a message $m(t)$ within a signal $s(t)$ that drives both the dynamics of the chaotic emitter and receiver. This constitutes a particular application of the so-called *active-passive decomposition* (APD) [70] where the message does not disturb the synchronization process. The encryption and decryption are illustrated in Fig. 2.10.

The legitimate receiver Bob recovers an estimate of the message performing a similar operation to that of the one used in CMa. The estimated message reads

$$\hat{m}(t) = \mathbf{s}(t) - \mathbf{y}_R. \tag{2.34}$$

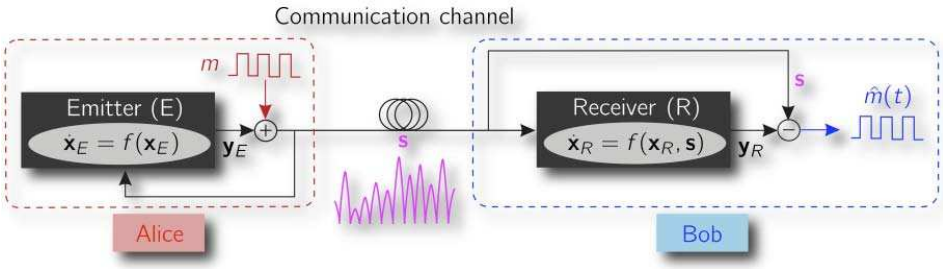

Figure 2.10: Chaos modulation (CMo) architecture. An additive CMo is illustrated.

2.4 Conclusion

In this chapter, we have reviewed the fundamental concepts of nonlinear sciences necessary to the realization of chaos-based cryptosystems. In a first section, we have introduced the theory of Chaos, starting with an historical perspective and details on fundamental notions that are associated with it; continuous and discrete systems, the stability of equilibrium points, the classes of attractors and bifurcations. We also give some insight on complexity theory used to described properties of chaotic attractors and time-series. Then in a second section, we have given insight on the theory of synchronization of periodic and chaotic oscillators. Finally in the last section, we have combined these two theories to explain the principles of chaos-based communications and some typical architectures; chaos masking (CMa), chaos-shift keying (CSK), and chaos modulation (CMo).

Chapter 3

Chaotic Optoelectronic Systems

Abstract

In this chapter, we review the fundamental concepts of the physics of semiconductor lasers and unveil the existing bridge between lasers and nonlinear science. We focus our attention on conventional edge-emitting lasers (EEL), which can be modelled semiclassically using rate equations. We explain how EELs, in certain configurations, become unstable and exhibit complex dynamics. Finally, we describe other optoelectronic systems typically encountered in the field of optical chaos-based communications such as wavelength, phase, and intensity chaos generators based on continuous wave EEL laser sources and nonlinear delayed feedback configurations. We conclude the chapter by showing various realizations of cryptographic setups with typical encryption approaches (CMa, CSK, and CMo).

3.1 Physics of Lasers

3.1.1 Principles

A laser is a physical system that generates light by amplification of stimulated emission of radiation (LASER) [71]. Its principle of operation can be phenomenologically described by a two-level atomic system in a resonant unidirectional (ring) cavity. The energy of the two-level system is increased by means of optical or electrical excitation, pumping electrons from the ground state of energy E_0 to higher-energy states thus increasing the population in level E_1. This configuration is unstable; the system releases energy by emitting a photon of frequency ω associated with the electronic transition between the two energy levels. The photon's energy satisfies $\hbar\omega = E_1 - E_0$, $\hbar$ being the Planck constant. This phenomenon known as *spontaneous emission* is a stochastic process (noise). It initially generates many photons in the resonant cavity that induce additional electronic transitions as they propagate through the excited population. This phenomenon is known as *stimulated emission*. The stimulated photons share identical physical properties (frequency and phase) with those that seeded their emission. This repeated interplay between the constantly repopulated high-energy level and the photons trapped by the resonant cavity leads to what is known as light amplification.

Below, we give the main steps leading to a comprehensive dynamical model that reflects the previous phenomenological description of a laser made in a two-level medium. More details can be found in [23; 72; 73; 74], which have inspired this section.

3.1.2 Maxwell-Bloch Equations

The dynamics of a laser is described by the dynamical interactions between three physical quantity: the electric field (E) that propagates in a ring cavity (unidirectional propagation), the macroscopic polarization (P) of the medium, and the population inversion N. The laser's equations are derived within the *semiclassical approach*. The large number of photons involved are collectively treated as a single classical continuous wave, i.e. the electric field (amplitude and phase). The medium, a collection of two-level systems, is described at the microscopic level using quantum mechanics. The evolution of the electric field is described by the *Maxwell Equations* and the properties the medium by the *Bloch Equations*. The two sets of equations are combined at the macroscopic level in the *Maxwell-Bloch Equations* after a series of simplifications detailed in the literature [73]. Ultimately, the Maxwell-Bloch equations for a homogeneously broadened two-level laser read

$$\frac{\partial E}{\partial z} + \frac{\eta}{c}\frac{\partial E}{\partial t} = i\frac{k}{2\varepsilon_0\eta^2}P - \frac{n}{2T_{ph}c}E \tag{3.1}$$

$$\frac{\partial P}{\partial t} = -i\left(\omega_A - \omega_0\right)P + i\frac{\mu^2}{\hbar^2}EN - \frac{P}{T_2} \tag{3.2}$$

$$\frac{dN}{dt} = -i\frac{1}{\hbar}\left(EP^* - E^*P\right) + \frac{N_0 - N}{T_1}, \tag{3.3}$$

with c the speed of light in vacuum, $\hbar$ the reduced Planck constant, η the refractive index of the medium, μ_0 the magnetic permeability of vacuum, ε_0 the electric permittivity of the vacuum, ω_0 the angular oscillation frequency of the electric field when described as planar wave, $k = \eta\omega_0/c$ the wave number, ω_A the angular frequency of light associated with a transition (emission or absorption) in the two-level system, T_{ph} the photon lifetime, T_2 the relaxation time of the dipole moment, T_1 the population inversion rate, N_0 is the population inversion induced by the pump at the laser threshold.

This description does not include spontaneous emission (intrinsic noise), but refined models take into account this effect [72]. In 1975, Haken highlighted a remarkable analogy between the semiclassical description of a two-level laser and the equations used by Lorenz (see Chapter 2) to describe the dynamic of the Earth atmosphere [75].

If the variations of the electric field along the propagation z-axis are neglected $|\partial E/\partial z| \ll \eta/c|\partial E/\partial t|$, the Maxwell-Bloch equations become an ordinary differential system. Furthermore, considering the proper change of variables

$$x = T_2\frac{\mu}{\hbar}E,\ y = i\frac{T_2T_{ph}\omega_0\mu}{\hbar\varepsilon_0\eta^2}P,\ z = \frac{T_2T_{ph}\omega_0\mu^2}{2\varepsilon_0\hbar\eta^2}(N_0 - N),\ \text{and}\ t = \frac{t}{T_2}, \tag{3.4}$$

and the new parameters defined by

$$\sigma = \frac{T_2}{2T_{ph}},\ \beta = \frac{T_2}{T_1},\ \rho = \frac{T_2T_{ph}\omega_0\mu^2}{2\hbar\varepsilon_0\eta^2}N_0,\ \text{and}\ \delta = (\omega_0 - \omega_A)T_2, \tag{3.5}$$

Equations 3.1-3.3 finally read

$$\frac{dx}{dt} = \sigma\,(y - x)\,, \tag{3.6}$$

$$\frac{dy}{dt} = -\,(1 - i\delta)\,y + \rho x - xz, \tag{3.7}$$

$$\frac{dz}{dt} = -\beta z + \mathrm{Re}\,(x^*y)\,. \tag{3.8}$$

These equations are equivalent to those of Lorenz and the isomorphism previously detailed between the two models is known as the *Haken-Lorenz equivalence*. It has triggered the first investigations dynamical and chaos behaviors in lasers [76].

3.1.3 A Dynamical Classification of Lasers: Arecchi's Classification

The Maxwell-Bloch equations (3.1)-(3.3) present three characteristic time scales T_1, T_2, and T_{ph} respectively affecting the dynamics of the inversion of population N, the polarization of the medium P, and the electric field E. By comparing their relative orders of magnitude, Arecchi proposed a dynamical classification of lasers [77; 78]. There are three classes:

- **Class-A lasers:** They have response times satisfying $T_1, T_2 \gg T_{ph}$, justifying the adiabatic elimination of the polarization and inversion of population. Consequently, the dynamics of a class-A laser are entirely described by the electric field equation (cf. Eq.3.1). Examples of class-A lasers are visible He-Ne lasers.

- **Class-B lasers:** They have response times satisfying $T_1, T_{ph} \gg T_2$, meaning that only the polarization may be adiabatically eliminated. The dynamics of a class-B laser are entirely described by the dynamics of its field and population inversion. Examples of class-B lasers are Nd-YAG, CO_2 and semiconductor lasers.

- **Class-C lasers:** They have response times with approximately identical order of magnitude $T_1 \approx T_2 \approx T_{ph}$. The three Maxwell-Bloch equations are necessary. Examples of class-C lasers are the NH_3 and infrared He-Ne lasers. They have sufficient degree of freedom to intrinsically exhibit chaotic behaviors [76; 79].

3.2 Physics of Semiconductor Lasers

3.2.1 Description and Principles

A semiconductor laser is typically made of a semiconductor junction coupled with an optical resonator, which in the case of an edge emitting laser (EEL) can be a Fabry-Pérot resonator. A common type of EEL is the double heterostructure laser. As shown in Fig. 3.1, the gain medium (equivalent of the two-level system in the previous section) is made of a thin semiconductor layer intercalated between two cladding layers made of different semiconductor materials. The cleaved facets in the $x - y$ planes are partially reflecting mirrors resulting in a resonant cavity.

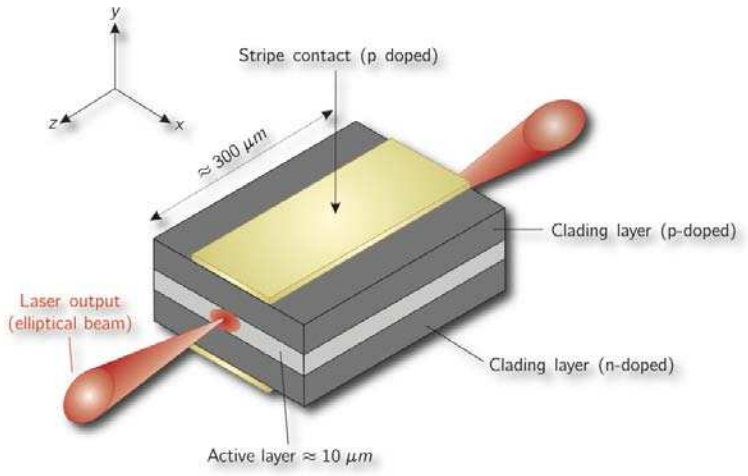

Figure 3.1: Schematic of an edge-emitting laser (EEL) based on the double heterostructure. Both facets emit coherent light. Electric pumping is provided by the strip contacts on the top and bottom of the structure.

The principles of operation of a semiconductor laser are similar to those of a two-level system described in the previous section. The mathematical model remains semiclassical with a quantum description of the medium, now a semiconductor material.

3.2.2 Physics of Semiconductor Junctions

In this subsection, a simple model for a single-mode EEL is presented. This model is known as the semiconductor rate equations. A complete and rigorous derivation of these equations is beyond the scope of this thesis; however, we provide the fundamental concepts that allow us to understand the principles of semiconductor lasers.

3.2.2.1 Basics of Semiconductors

A semiconductor material has a temperature-dependent electric conductivity, whose value lies between those of an isolator and a conductor. The band structure accounts for the energy levels of the many atoms in the material and their couplings leading to continua of energy levels, referred to as energy bands, or simply bands [80]. The bands split into two groups: the *conduction bands* and *valence bands*, where the electrons are distributed as a function of their energy E. This distribution depends on two factors: the density of states and the probability of occupancy of an electron at a given energy E. The electron occupancy is given by the Fermi-Dirac distribution,

$$f_{c,v}(E_{ec,ev}) = \frac{1}{1 + e^{\frac{E_{ec,ev} - E_{Fc,Fv}}{k_B T}}}, \tag{3.9}$$

where the indices (c, v) refer to the conduction and valence bands, k_B is the Boltzmann constant, T is the temperature, $E_{ec,ev}$ and $E_{Fc,Fv}$ are the energies of an electron and the quasi-Fermi levels of each band, respectively.[1]

The valence and conduction bands are energetically separated by a forbidden energetic zone called the band-gap with energy $E_g = E_c - E_v$, the difference of the minimum and maximum energy level of each band.

3.2.2.2 Light-Matter Interactions and Semiconductor Junctions

In a semiconductor, the stimulated emission competes with other light-matter interactions such as the spontaneous emission, photon absorption, and non-radiative recombination (see Fig. 3.2).

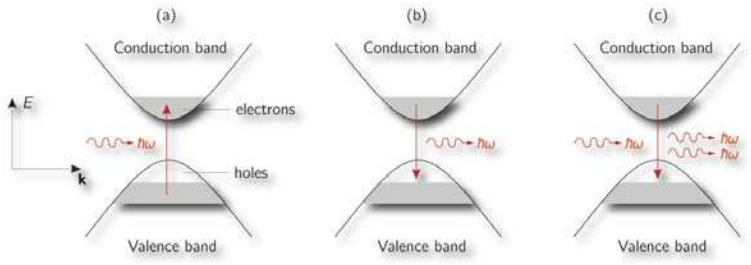

Figure 3.2: Representation of various light-matter interactions in a semiconductor material [in the plane energy-wave vector $(E, \mathbf{k})$ using a parabolic approximation for the energy band] (a) absorption of a photon of energy $\hbar\omega$, (b) spontaneous emission of a photon via electron-hole recombination, and (c) stimulated emission.

[1] The difference between the two quasi-Fermi levels gives a measure of how far the semiconductor is from equilibrium, when $E_{Fc} = E_{Fv} = E_F$ the system is at the equilibrium.

To ensure lasing, the net rate R_{st} defined as the difference between the stimulated emission and absorption process has to be positive for a photon of given energy $\hbar\omega$. One shows that $R_{st} \propto f_c(E_{ec}) - f_v(E_{ev})$ [81]; therefore, R_{st} is positive only if population inversion is achieved (the occupancy probability of an electron in the conduction band is greater than that of an electron in the valence band). This imposes a condition of separation of the quasi-Fermi levels: $E_{Fc} - E_{Fv} > \hbar\omega > E_g$. A simple structure that allows population inversion is a $p-n$ homojunction, where a $p-$type semiconductor is put in contact with a $n-$type semiconductor. To emit light by stimulated emission, an additional layer of intrinsic semiconductor is usually inserted within the $p-n$ junction and used as an active medium to enhance the stimulated emission. This forms the double heterostructure described in Fig. 3.1. The band diagram of a biased double-heterostructure laser is shown in Fig.3.3.

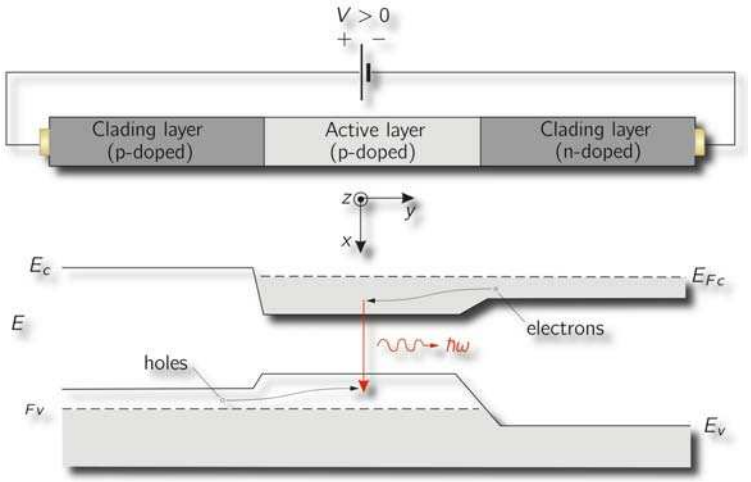

Figure 3.3: Representation of the structure and the band diagram of a double-heterostructure laser under forward bias $V > 0$. The dashed lines represent the quasi-Fermi levels $E_{Fc,Fv}$ and the solid lines represent the energy levels $E_{c,v}$ associated to each band.

The advantages of such a structure are good confinement of the carriers, which are trapped in a potential well within the active layer (no leakage of electrons in the $p-$type layer, or holes in the $n-$type layer). The active region in the heterostructure also acts as the core of a waveguide and confines the photons in the transverse direction because the bandgap being smaller, the refractive index is larger than for the heterolayers. The cleaved facets at the boundaries of the medium are partially reflecting and form a Fabry-Perot resonator. The voltage is applied to the structure to create the inversion of population and generates spontaneous emission to seed the stimulated emission. Beside sustaining the amplification, the Fabry-Perot resonator has three other consequences: (i) the selection of the longitudinal modes emitted, (ii) the selection of the polarization of the emitted light (by its geometry), and (iii) the generation of supplementary losses of photons (via the partial reflectivity of the mirrors).

3.2.3 Semiconductor-Laser Rate Equations

One of the main difficulties encountered in the modelling of a semiconductor laser using a semiclassical approach is the *inhomogeneous broadening*[1] of the optical transitions and the interactions of the electrons among themselves and with the crystal lattice of the semiconductor material. The dynamics of an semiconductor edge-emitting laser (ELL) is still performed under the framework of the semiclassical description. However, the derivation the Maxwell-Bloch equations, also called *semiconductor-laser rate equations*, become more complicated especially because of the quantum description of light-matter interaction with a semiconductor material [80]. There exists several other approaches to derive these equations, which are precisely derived in [82; 83].

After a number of assumptions, the description of the system simplifies to two ordinary differential equations:

$$\frac{dE}{dt} = \frac{1}{2}\left(g(N) - \frac{1}{T_{ph}}\right)E, \tag{3.10}$$

$$\frac{dN}{dt} = \frac{J}{e} - \frac{N}{T_1} - \frac{\varepsilon_0 n_0^2}{2\hbar\omega_0} g(N)\left|E\right|^2. \tag{3.11}$$

The quantity denoted $g(N)$ is related to the gain material and is usually approximated with a first order Taylor expansion because of its weak carrier-density dependence above the lasing threshold. The resulting expression for the gain reads

$$g(N) = g(N_{th}) + (1 + i\alpha)g_N(N - N_{th}), \tag{3.12}$$

where α is the *linewidth enhancement factor* (or Henry factor) accounting for the coupling of the phase and amplitude of the complex electric field, which is caused by a dependence of refractive index on the number of carriers in the gain medium [84]. The value of α is typically comprised in the range $3-7$ for semiconductor-bulk lasers [85], N_{th} is the population inversion at lasing threshold, $g(N_{th})$ is the threshold value of the gain that compensates exactly the losses $g(N_{th}) = 1/T_{ph}$, and g_N is the differential gain. When the laser operates above threshold, the gain eventually saturates. This saturation is phenomenologically included in the differential gain, which now depends on the photon density in the cavity via

$$g_N = \frac{G_N}{1 + \varepsilon_s \frac{\varepsilon_0 n_0^2}{2\hbar\omega_0}\left|E\right|^2}, \tag{3.13}$$

with G_N the linear gain and ε_s the saturation coefficient. Making the changes of variable $\bar{E} = \sqrt{(\varepsilon_0 n_0^2/2\hbar\omega_0)}E$, $T_{ph} = \tau_p$, and $T_1 = \tau_s$, we finally obtain the rate equations for a semiconductor laser

$$\frac{d\bar{E}}{dt} = \frac{1}{2}(1 + i\alpha)\, G_{N,\bar{E}}\bar{E} \tag{3.14}$$

$$\frac{dN}{dt} = \frac{J}{e} - \frac{N}{\tau_s} - \left(G_{N,\bar{E}} + \frac{1}{\tau_p}\right)\left|\bar{E}\right|^2 \tag{3.15}$$

[1] Carriers occupy multiple energy levels within the valence or conduction band. Consequently, the transitions will statistically generate photons with various frequencies centered with respect to $\hbar\omega_0 = E_g$. The imperfect monochromaticity of the laser optical spectrum is known as the *inhomogeneous broadening*.

with $G_{N,\bar{E}} = G_N(N - N_{th}) / \left(1 + \varepsilon_s \left|\bar{E}\right|^2\right)$. It is noteworthy mentioning a similar version of the rate equations defined for the population at the transparency N_0 and not at the lasing threshold N_{th}. In these conditions, we have $G_{N,\bar{E}} = G_N(N - N_0) / \left(1 + \varepsilon_s \left|\bar{E}\right|^2\right) - 1/\tau_p = G_{N,\bar{E}}^{(N_0)} - 1/\tau_p$. This second expression is widely encountered in the literature and will be used in the thesis.

3.2.4 Typical Dynamics of a Class-B Semiconductor Laser

The rate equations couple the complex electric field (phase $\varphi(t)$ and amplitude $\bar{E}(t)$) with the population inversion $N(t)$. The third degree of freedom of the EEL, polarization $P(t)$, being eliminated from the dynamics of the equations, the system can not exhibit cannot exhibit complex chaotic dynamics such as those of a Class-C laser.

As a matter of fact, it exists only two degrees of freedom because the phase φ is completely determined when the amplitude and the carrier density are known. As a consequence, a semiconductor laser alone cannot exhibit chaos and requires additional degrees of freedom.

As we will demonstrate it below, an EEL behaves as damped relaxed oscillator. Towards this end, we consider a small perturbation of the EEL's state vector from the steady state (E_s, φ_s, N_s):

$$\bar{E} = \bar{E}_s + \delta\bar{E}, \tag{3.16}$$

$$\varphi = \varphi_s + \delta\varphi, \tag{3.17}$$

$$N = N_s + \delta N. \tag{3.18}$$

The steady state is obtained by setting to zero the derivatives in Eqs. 3.10-3.11. It satisfies the following relations

$$\frac{G_N(N_s - N_{th})}{1 + \varepsilon E_s^2} - \frac{1}{\tau_p} = 0, \tag{3.19}$$

$$J - \frac{N_s}{\tau_s} - \frac{G_N(N_s - N_{th})}{1 + \varepsilon E_s^2} E_s^2 = 0. \tag{3.20}$$

Based on these relationships and considering the magnitude of perturbation vector to be small in comparison with that of the steady state, Eqs. - lead to a linearized system to describe the evolution of the perturbation.[1] The system reads

$$\frac{d}{dt}\begin{pmatrix} \delta\bar{E} \\ \delta\varphi \\ \delta N \end{pmatrix} = \begin{pmatrix} -\frac{1}{\tau_p}\frac{\varepsilon E_s^2}{1+\varepsilon E_s^2} & 0 & \frac{G_N E_s}{2}\frac{1}{1+\varepsilon E_s^2} \\ -\frac{\alpha\varepsilon E_s}{\tau_p}\frac{1}{1+\varepsilon E_s^2} & 0 & \frac{\alpha G_N}{2}\frac{1}{1+\varepsilon E_s^2} \\ -\frac{2E_s}{\tau_p}\frac{1}{1+\varepsilon E_s^2} & 0 & -\frac{1}{\tau_s} - G_N E_s^2 \frac{1}{1+\varepsilon E_s^2} \end{pmatrix} \begin{pmatrix} \delta\bar{E} \\ \delta\varphi \\ \delta N \end{pmatrix}. \tag{3.21}$$

The determination of the eigenvalues of the transition matrix gives insight on rates of evolution of each state variable. Their determination is possible by first calculating the determinant $\det(\lambda I - \nabla\mathbf{f}_{E=E_s,\varphi=\varphi_s,N=N_s}) = 0$. The resulting characteristic

[1] The linear transition matrix is obtained by considering the Jacobian matrix $\nabla\mathbf{f}_{E,\varphi,N}$ of the vector field of the rate equations.

polynomial reads

$$\lambda\left[\lambda^2+\left(\frac{1}{\tau_s}+\frac{G_N E_s^2+\frac{E_s^2\varepsilon}{\tau_p}}{1+\varepsilon E_s^2}\right)\lambda+\frac{1}{1+\varepsilon E_s^2}\left(\frac{G_N E_s^2}{\tau_p}\left(1+\frac{\varepsilon}{1+\varepsilon E_s^2}\right)+\frac{\varepsilon}{\tau_p\tau_s}\right)\right]=0. \tag{3.22}$$

This third-order polynomial has three roots $\lambda = 0$ and two complex conjugate roots $\lambda_\pm = \Gamma_{RO} \pm i\omega_{RO}$, with Γ_{RO} the damping ratio and $\nu_{RO} = \omega_{RO}/2\pi$ the relaxation-oscillation frequency. Their expressions read

$$\Gamma_{RO} = \frac{1}{2\tau_s}+\left(\frac{G_N}{2}+\frac{\varepsilon}{2\tau_p}\right)\frac{E_s^2}{1+\varepsilon E_s^2}, \tag{3.23}$$

$$\omega_{RO} = \left(\frac{1}{1+\varepsilon E_s^2}\left(\frac{G_N E_s^2}{\tau_p}\left(1+\frac{\varepsilon}{1+\varepsilon E_s^2}\right)+\frac{\varepsilon}{\tau_p\tau_s}\right)-\Gamma_{RO}^2\right)^{1/2}. \tag{3.24}$$

Usually, the saturation gain $\varepsilon \ll 1$ is neglected in the expression of ω_{RO}; this allows to derive a simplified expression

$$\nu_{RO}=\frac{1}{2\pi}\left(\frac{1}{\tau_p\tau_s}(\mu-1)-\frac{\mu^2}{4\tau_s^2}\right)^{1/2} \text{ with } \mu = G_N\tau_p\tau_s\left(J-\frac{N_0}{\tau_s}\right). \tag{3.25}$$

These relaxation oscillations physically correspond to an exchange of energy between the number of photons and the electronic carriers. As an illustration, we simulate the behavior of an EEL in Fig. **??**.

3.3 Generation of Optical Chaos with Laser Diodes

In this section, we review the various systems classically encountered in optical chaos-based communications. The generators are mostly based on semiconductor technology. Being in essence class-B laser, EEL can not be used to generate chaos with respect to the corollary of the Poincaré-Bendixon theorem (see Chapter 2). As a consequence, additional degrees of freedom must be added to the laser. Two strategies have been widely discussed in the literature:

- The internal nonlinearity of the semiconductor laser is exploited and additional degrees of freedom are used (optical or optoelectronic feedback, modulation, optical injection).
- The semiconductor laser is used as a continuous wavelength (CW) source that powers an external structure chaotically modulating the properties of the emitted light (amplitude, phase, wavelength, or polarization).

3.3.1 Chaos Generation with Laser's Intrinsic Nonlinearity

The addition of external degrees of freedom exploiting the internal nonlinearity of a semiconductor laser comprise essentially four different configurations: (a) the modulation of the pumping current,(b) the optical injection, and the use of (c) optoelectronic or (d) optical feedback. They are represented in Fig. 3.4.

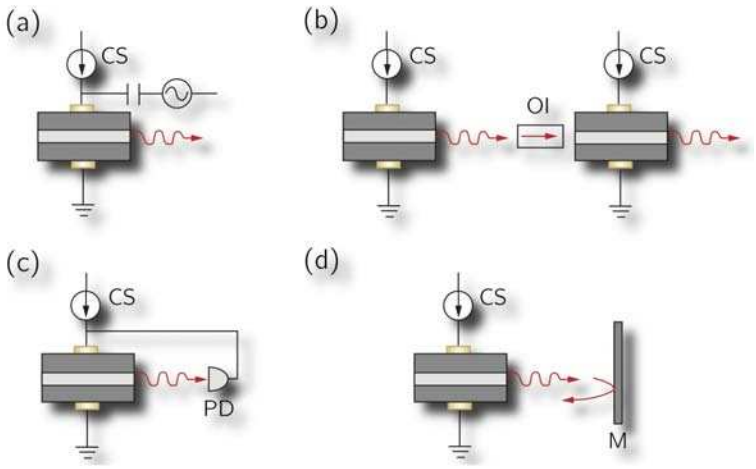

Figure 3.4: Schematics of various configurations of semiconductor lasers with additional degrees of freedom tailored for the generation of optical chaos; (a) modulation of the injection current, (b) unidirectional optical injection (c) optoelectronic feedback, and (d) delayed optical feedback also called external cavity. The abbreviations stand for SL: semiconductor laser, CS: current source, OI: optical isolator for unidirectional transmission, PD: photodiode (adapted from [23]).

The different optoelectronic systems exploiting an internal nonlinearity are described by the semiconductor rate equations with additional terms. A single set of equation can be used: [1]

$$\frac{dE}{dt} = \frac{1}{2}(1+i\alpha)\left(G_{N,E} - \frac{1}{\tau_p}\right)E + F_{ext}(t), \tag{3.26}$$

$$\frac{dN}{dt} = \frac{J(t)}{e} - \frac{N}{\tau_s} - G_{N,E}\left|E\right|^2. \tag{3.27}$$

Indeed, depending on the type of configuration, the terms $F_{ext}(t)$ and $J(t)$ will have different expressions. We detail them below:

- **(a) Modulation of the injection current:** Under standard operational conditions, the laser is electrically pumped with a DC current. The addition of an AC component with sufficient amplitude and or large frequency induces chaotically-pulsed behaviors of the emitted light [86]. In this type of architecture, however, the dimension of the chaotic pulsing is rather limited [87] due to the few additional degrees of freedom, compared to system with delayed optoelectronic feedback (Configuration (c)). In Configuration (a), we have $J(t) = J_0 + J_1 \sin \Omega t$ and $F_{ext}(t) = 0$, with Ω the angular frequency of modulation, and J_1 the amplitude of modulation.

- **(b) Optical injection:** This consists of the use of an additional laser (master) that unidirectionally injects the laser generating chaos (slave). Similarly to what is observed in the unidirectional synchronization of oscillators and depending on coupling parameters (strength and frequency), the slave laser can

[1] Usually in the literature $\bar{E}$ and $G_{N,E}^{(N_0)}$ are simply noted E and $G_{N,E}$, respectively.

lock its phase and frequency to those of the master. Furthermore, a proper coupling adjustment can induce chaotic behavior through quasi-periodic or period-doubling routes to chaos [88; 89] (A route to chaos by breaking of a torus was also reported in [90]). In this configuration, we have $J(t) = J_0$ and $F_{ext}(t) = \eta_{inj} e^{-i\Delta\omega_{inj} t} E_{inj}(t)$, with $E_{inj}(t)$ the complex optical field injected by the first semiconductor laser, η_{inj} the injection's strength, and $\Delta\omega_{inj}$ the frequency detuning between the two lasers.

- **(c) Optoelectronic feedback:** A photodiode detects the light emitted by the semiconductor, the resulting voltage proportional to the detected light is added after a certain delay to the current pumping the laser. In this configuration, we have $J(t) = J_0(1 + \eta |E(t-\tau)|^2)$ and $F_{ext}(t) = 0$ with η the optoelectronic feedback strength and τ the propagation time in the optoelectronic feedback. Depending on the sign of η, we refer to positive or negative optoelectronic feedback (POEF and NOEF, respectively). With a POEF, a period-doubling and quasiperiodic routes to chaos have been reported; they both lead to a *chaotic pulsing* (CP) regime of the light intensity [91; 92].

- **(d) Optical feedback:** A mirror is added at the output of the semiconductor laser. It forms an external cavity, where the emitted light propagates and is partially reinjected into the laser cavity. The roundtrip introduces a time delay to the laser's dynamics and adds an infinite number of degrees of freedom to the dynamical equations. The duration of the time delay τ (or length of the external cavity) with respect to the relaxation oscillation period τ_{RO} define two particular regimes: the *long-cavity regime* ($\tau > \tau_{RO}$) and *short-cavity regime* ($\tau < \tau_{RO}$) [93]. In the following, we will mainly focus our attention on the long-cavity regime. In this configuration, we have $J(t) = J_0$ and $F_{ext} = \eta e^{i\omega_0 \tau} E(t-\tau)$ and the system is called the *Lang-Kobayashi Equations* [94].

  There exist various dynamical behaviors that an ECSL can produce; for instance two different chaotic regimes, the *low-frequency fluctuations* (LFF) characterized by sudden drops of the intensity [95], and the *coherence collapse* (CC) regime [96], for which the temporal coherence of laser light suddenly drops. The chaos in CC regime has also a very large optical linewidth [97]. The origin of chaos in an ECSL are linked to the stability of its stationary solutions, called external-cavity modes (ECM). These ECMs only exist by pairs composed of stable (mode) and unstable (anti-mode) solutions. These ECMs can be deduced from solving the Lang-Kobayashi equations with the left-hand side term equal to zero. We denote $|E_s|$, $\varphi_s = \omega_s t$, and N_s the stationary solutions and inject them in the equations describing an ECSL

$$\frac{g_N (N_s - N_0)}{1 + \varepsilon |E_s|^2} - \frac{1}{\tau_p} = -2\eta \cos(\omega_s + \omega_0)\tau, \tag{3.28}$$

$$\alpha \left(\frac{g_N (N_s - N_0)}{1 + \varepsilon |E_s|^2} - \frac{1}{\tau_p} \right) = 2\omega_s + 2\eta \sin(\omega_s + \omega_0)\tau, \tag{3.29}$$

$$J - \frac{N_s}{\tau_s} - \frac{g_N (N_s - N_0)}{1 + \varepsilon |E_s|^2} |E_s|^2 = 0. \tag{3.30}$$

The solution of this system of equations start first with the determination of the stationary angular pulsation ω_s. It can be obtained by combining Eqs. 3.28 together 3.29 and reformulated as it follows

$$\Omega\tau = \omega_0\tau - \eta\tau\sqrt{1+\alpha^2}\sin\left(\Omega\tau + \text{atan}(\alpha)\right), \tag{3.31}$$

with $\Omega = \omega_s + \omega_0$. Solutions of this transcendental equation do not have an analytical expression. However, they can be found numerically and correspond to the intersection points between the sine and linear parts of Eq. 3.31 as illustrated in Fig. 3.5(a). When the feedback strength η or the time-delay τ increase, ECMs disappear and give birth to more ECMs (see Fig. 3.5(b)) through saddle-node bifurcations [98].

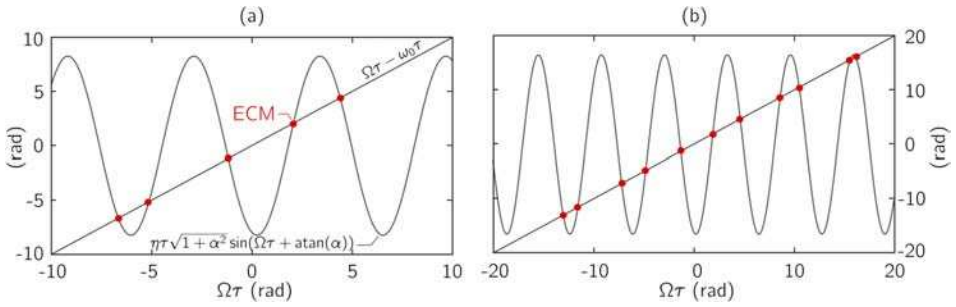

Figure 3.5: Graphical representation of the solution of the transcendental equation for the ECM. The linear and sine parts of the equation are plotted for (a) $\gamma = 1$ GHz and (b) $\gamma = 2$ GHz with $\tau = 2$ ns and $J = 1.5J_{th}$. The ECM are located (and represented by a red circle) at the intersection of the two curves. The other parameters are $\alpha = 4$, $\tau_p = 2$ ps, $\tau_s = 2$ ns, $G_N = 7.5\times10^{-13}$ m^{3}s^{-1}, $N_0 = 3\times10^{24}$ m^{-3}, $J_{th} = 1.83\times10^{33}$ m^{-3}s^{-1}, and $\varepsilon = 2.5\times10^{-23}$ m^{-3}.

The expression of ω_s can be used to find the expressions of the $|E_s|$ and N_s,

$$|E_s|^2 = \frac{1}{1+\frac{\varepsilon}{\tau_s g_N}}\left(\frac{J-\frac{N_0}{\tau_s}}{\frac{1}{\tau_p} - 2\eta\cos\left(\omega_s+\omega_0\right)\tau} - \frac{1}{\tau_s g_N}\right), \tag{3.32}$$

$$N_s = N_0 + \left(\frac{1}{\tau_p g_N} - \frac{2\eta}{g_N}\cos\left(\omega_s+\omega_0\right)\tau\right)1 + \varepsilon\left|E_s\right|^2. \tag{3.33}$$

When the feedback strength or the time-delay are further increased, the ECMs undergo a cascade of bifurcations, starting usually with a Hopf bifurcation until a stable chaotic attractor is reached by the ECSL.

We have depicted in Fig. 3.6(a) the bifurcation diagram of a route to chaos undergone by an ECSL, when the feedback strength η is taken as the bifurcation parameter. We also show a chaotic intensity time series $I(t) = |E(t)|^2$ (CC regime) and the associated RF spectrum in Fig. 3.6(b) and (c), respectively. Detailed studies on the destabilization of ECM and existence of various routes to chaos have been reported, for instance, in [99; 100].

The complexity (dimension d_{KY} and entropy h_{KS}) of the chaotic dynamics has been also characterized for the short- and long-cavity regimes in [101]. The dynamics are typically *hyperchaotic*, an expression associated with the existence of multiple

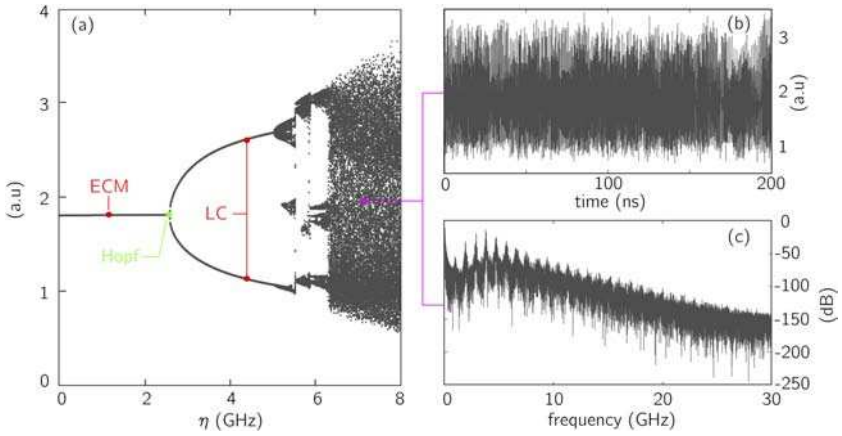

Figure 3.6: Chaos in an ECSL. (a) Diagram of bifurcation that unveils a cascade of bifurcation until a strange attractor is reached. The bifurcation parameter is the feedback strength η. An ECM is depicted by a red circle, the Hopf bifurcation that destabilizes the ECM into a limit cycle (LC) are also marked in red. In (b), a chaotic time series of the intensity $I(t) = |E(t)|^2$ is represented and in (c) its RF spectrum for $\eta = 7$ GHz. The parameters are identical to those of Fig. 3.5.

positive Lyapunov exponents. This allows the strange attractor to reach very large dimension (several tens), which is a desirable property for secure chaos-based cryptosystems.

3.3.2 Chaos Generation with External Nonlinearities

In this subsection, we present optoelectronic architectures where the semiconductor laser is a continuous wave (CW) source, whose properties are modified externally. Three architectures are presented; wavelength, intensity, and phase chaos generators.

3.3.2.1 Wavelength Chaos Generator

The architecture is described in Fig.3.7 and was presented for the first time in 1998 [102; 103]. In this paragraph, we recall the main characteristic of the system and give the important steps necessary to understand the derivation of its model. The wavelength chaos generator (WCG) is composed of a multielectrode tunable DBR[1] laser diode and a delayed feedback loop with an optical isolator, a nonlinear element, an optical delay line, a photodetector, and an RF low-pass filter.

The DBR laser diode has two sections: an active section pumped by current I_0 emits light at central wavelength Λ_0, and a passive section with a DBR [see Fig. 3.7(b)]. The DBR current $I_{DBR} = I_0 + i(t)$ controls the refractive index of the grating and allows for a smooth continuous variation of the laser's wavelength around Λ_0 (no mode hopping[2]). The emitted wavelength is $\Lambda(t) = \Lambda_0 + \lambda(t)$ with

[1]DBR stands for distributed Bragg reflectors, an interlacing of semiconductor layers with different refractive index.

[2]Mode hopping refers to as sudden jumps between different longitudinal modes in the laser cavity.

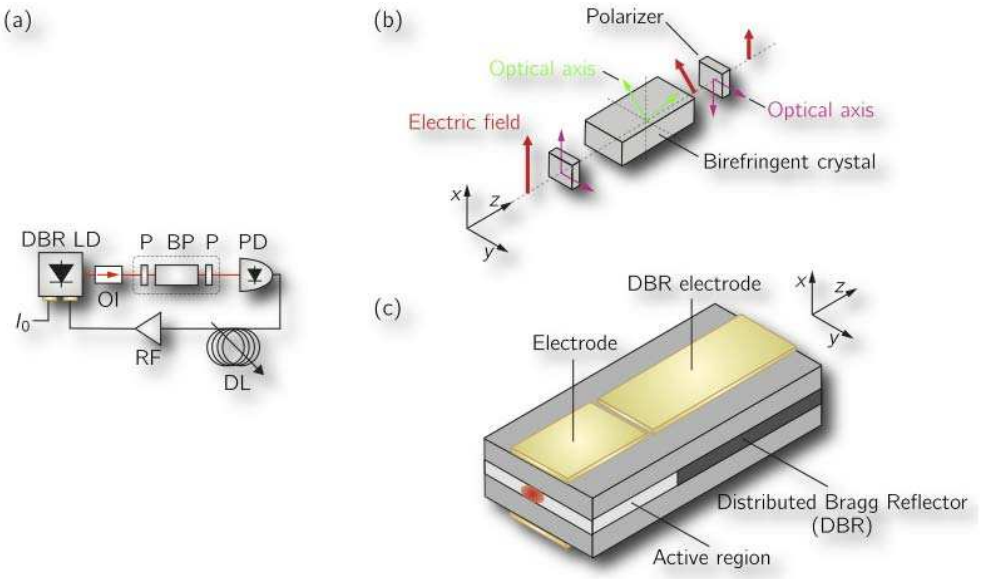

Figure 3.7: Schematic of the wavelength chaos generator based on a nonlinear fedback DBR laser diode. (a) Typical architecture with the following notations: OI: an optical isolator to prevent undesirable optical feedback, P_1 and P_2 two polarizers; BP the birefringent crystal; PD: the photodiode, DL: the delay line, RF: the RF low-pass filter. (b) Details on the nonlinear element, a birefringent crystal sandwiched into two polarizers. The directions of the optical axes of each optical components are indicated on the figure. (c) Details on the structure of a DBR laser diode and its two sections; the active section (similar to that of the EEL in Fig. 3.1) and the DBR section driven by independent electrodes.

$\lambda(t)$ directly proportional to its driving current $\lambda(t) = Si(t)$ and S the tuning rate of the laser diode.

In the delayed feedback loop, the birefringent crystal inserted between the two polarizers acts as a nonlinear filter that converts the variations of wavelength into variations of light's intensity between its input and output:

$$P_{out}(t) = P_{in}(t) \sin^2 \left(\frac{\pi D}{\Lambda(t)} \right), \tag{3.34}$$

where D is the difference of optical path in the crystal and $P_{in}(t)$ the light intensity at the output of the DBR laser diode. The excursion in wavelength being negligible compared to the central frequency $\lambda(t) \ll \Lambda_0$, a first-order Taylor expansion of Eq. 3.34 gives

$$P_{out}(t) = P_{in}(t) \sin^2 \left(\frac{\pi D}{\Lambda_0} \lambda(t) - \Phi_0 \right), \tag{3.35}$$

with $\Phi_0 = \pi D/\Lambda_0$. Such an intensity modulation is a direct consequence of the filter's structure, where the directions of the optical axes of the two polarizers are perpendicular and the axes of the first polarizer are inclined by $\pi/4$ with respect to those of the birefringent crystal (Fig.3.7 (c) and for more details see [104]).
The light is linearly converted into a current $i(t) = KP_{in}(t)$ that is delayed by τ and

finally low-pass filtered before it drives the DBR's electrode. This leads to

$$T\frac{di(t)}{dt} + i(t) = GKP_0 \sin^2\left(\frac{\pi D}{\Lambda_0}\lambda(t-\tau) - \Phi_0\right), \tag{3.36}$$

with G and T the gain and response time of the RF low-pass filter, respectively. By multiplying each side of the equation by $S\pi D/\Lambda_0$ we finally obtain an Ikeda-like equation [105] to describes the WCG

$$T\dot{x}(t) + x(t) = \beta \sin^2\left(x(t-\tau) + \varphi_0\right), \tag{3.37}$$

with $x(t) = \pi D/\Lambda_0\lambda(t)$ the dimensionless state variable, $\beta = \pi D/\Lambda_0 SKP_0$ the nonlinear gain, and $\varphi_0 = -\Phi_0$ the phase shift.

3.3.2.2 Intensity Chaos Generator

Intensity chaos generator (ICG) was first presented in 2002 [106] and is depicted in Fig.3.8. It exhibits a remarkable structural analogy with the WCG, except for the nonlinear element, the RF filter and the laser diode, which are different. It is composed of a standard monochromatic EEL laser diode, a Mach-Zehnder modulator, an optical fiber delay line, a photo-diode, and a RF band-pass filter.

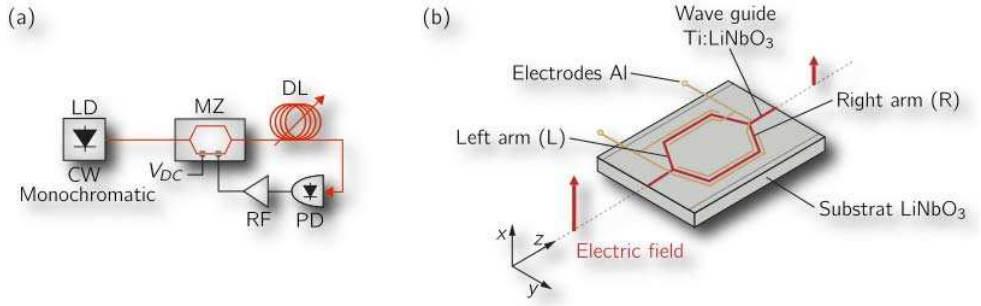

Figure 3.8: Schematic of the intensity chaos generator. (a) Overall architecture with the following acronyms: MZ: integrated Mach-Zehnder modulator, DL: delay line, PD: photodiode, RF: RF band-pass filter. (b) Zoom on the structure of an integrated Mach-Zehnder modulator with its RF and DC electrodes, and two arms (L) and (R).

The nonlinear element is the Mach-Zehnder modulator; it uses the electro-optic effect that characterizes the dependence of the refractive index $n(E)$ of a material on an electric field [104]. In each arm of the modulator, the light is phase-shifted differently before recombining at the output [see Fig. 3.8(b)]. In the left arm (L), no voltage is applied, and the field undergoes a natural phase shift $\Delta\varphi_L = \Delta\varphi_0$. In the other, a driving electrode imposes a voltage with a varying component $V(t)$ (RF voltage) and a constant DC level V_{DC}; this result in a additional phase-shift $\delta\varphi_R = \Delta\varphi_0 + \Delta\varphi_{RF} + \Delta\varphi_{DC}$. The modulation of input power reads

$$P_{out}(t) = P_{in}\cos^2\left(\frac{\pi V(t)}{2V_{\pi_{RF}}} + \frac{\pi V_{DC}}{2V_{\pi_{DC}}}\right), \tag{3.38}$$

with $V_{\pi_{RF}}$ and $V_{\pi_{DC}}$ the halfwave voltages ensuring a phase-shift equal to π and associated with the varying and constant electric fields, respectively.

The modulated light is then delayed by time τ in the delay line before being converted by the photodiode. The electrical signal is amplified and band-pass filtered. These steps lead to an integro-differential delay equation (with similar notations to those of [107])

$$\frac{1}{2\pi f_H}\dot{V}(t)+\left(1+\frac{f_L}{f_H}\right)V(t)+2\pi f_L\int_{t_0}^{t}V(u)du=gGSP_0\cos^2\left(\frac{\pi V(t-\tau)}{2V_{\pi_{RF}}}+\frac{\pi V_{DC}}{2V_{\pi_{DC}}}\right), \tag{3.39}$$

with G, f_L, and f_H the gain, low and high cut-off frequency of the RF filter, S the photodiode's sensitivity, P_0 the laser's light intensity, and g an aggregate attenuation of the feedback loop. A more condensed form of the equation can be obtained considering that usually $f_H \gg f_L$ and changing variables to give

$$T\dot{x}(t)+x(t)+\frac{1}{\theta}\int_{t_0}^{t}x(u)du=\beta\cos^2\left(x(t-\tau)+\varphi_0\right), \tag{3.40}$$

with $x(t)=\pi V(t)/(2V_{\pi_{RF}})$ the dimensional state variable, $T=1/(2\pi f_H)$ the high cut-off response time, $\theta=1/(2\pi f_L)$ the low cut-off response time, $\beta=\pi gGSP_0/(2V_{\pi_{RF}})$ the nonlinear gain, and $\varphi_0=\pi V_{DC}/(2V_{\pi_{DC}})$ the normalized bias offset.

3.3.2.3 Phase Chaos Generator

Phase chaos generators were successfully implemented in 2004 [108] and later simplified in 2009 [109]. One of the underlying motivation to develop such an architecture is mainly due to the experimental complexity associated with the mixing of message in the optical intensity chaos in the case of an ICG [110]. Its structure, shown in Fig. 3.9(a), is similar to an ICG except that interference is generated with a fiber-based interferometer before detection with a photodiode and the Mach-Zehnder modulator is replaced by a standard electro-optic phase modulator [see Fig. 3.9(b)].

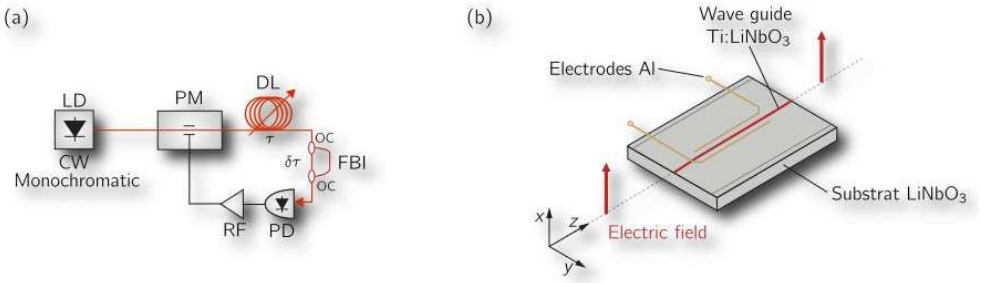

Figure 3.9: Schematic of the phase chaos generator using an optoelectronic oscillator with delayed feedback. (a) Overall architecture with the following abbreviations: PC: polarization controller, PM: integrated phase modulator, DL: delay line, OC: optical coupler, FBI: fiber-based interferometer, PD: photodiode, RF: RF band-pass filter. The delays τ and $\delta\tau$ respectively introduced by DL and FBI are indicated. (b) Details on the structure of an integrated phase modulator.

It is composed of a single arm (waveguide) where the phase is modulated through the electro-optic effect by a time-varying voltage $V(t)$, similarly to what we have in an ICG: An additional phase shift $\Delta\varphi = \pi V(t)/V_{\pi_{RF}}$ is generated. We can represent the complex electric field in a slow-varying approximation by $\mathbf{E}(t) = E_0 e^{j\varphi_0}$ and assume its amplitude being constant and phase slowly varying. After going through the phase modulator, the additional phase is added, $\mathbf{E}(t) = E_0 e^{j\varphi_0 + \Delta\varphi(t)}$. The optical field tehn propagates in the delay line for a time τ before being equally split in the two arms of a fiber-based interferometer. At its output, the electric field reads

$$\mathbf{E}(t-\tau) = \frac{E_0}{2} e^{j\varphi_0 + \Delta\varphi(t-\tau)} + \frac{E_0}{2} e^{j\varphi_0 + \Delta\varphi(t-\tau-\delta\tau)}, \tag{3.41}$$

with $\delta\tau$ the time difference introduced between the two arms of the fiber-based interferometer. Photodiode of sensitivity S detects the light intensity and converts it into a voltage:

$$V_{PD}(t) = SP_0 \cos^2\left(\frac{\pi V(t-\tau)}{2V_{\pi_{RF}}} + \frac{\pi V(t-\tau-\delta\tau)}{2V_{\pi_{RF}}} + \frac{2\pi\delta\tau}{\lambda_0}\right), \tag{3.42}$$

with $P_0 = |E_0|^2$. The electronic part of the feedback is structurally identical to that of an ICG and therefore leads to a similar adimensionnal model, which reads

$$T\dot{x}(t) + x(t) + \frac{1}{\theta}\int_{t_0}^{t} x(u)du = \beta \cos^2\left(x(t-\tau) + x(t-\tau-\delta\tau) + \varphi_0\right), \tag{3.43}$$

with $\varphi_0 = 2\pi\delta\tau/\lambda_0$ and identical notations to those used for Eq. 3.40 for all the remaining variables and parameters.

3.4 Optical Chaos Synchronization and Cryptography

In this section, we illustrate how the main techniques of chaos-based cryptography make use of optoelectronic devices. As in Chapter 2, a chaos-based communication architecture requires three essential features: (i) two identical-twin chaotic systems (E) and (R), (ii) the possibility to synchronize E and R, and (iii) a decryption operation to extract the message from the chaotic fluctuations. The introduction of the chaos synchronization concept has triggered numerous investigations using lasers. The first noteworthy results were achieved numerically for semiconductor lasers by Winful and Rahman in 1990 [111], and experimentally for CO_2 lasers by Roy and Thornburg in 1994 [112]. They paved the way to the first optical chaos transmission chains theoretically devised the same year by P. Colet and R. Roy using coupled solid state Nd:YAG lasers [113]. Later in 1996, C.R. Mirasso *et al.* proposed a numerical study of secure transmission with ECSL at the Gbit/s level [11]. But only in 1998, G.D. Van Wiggeren and R. Roy successfully implemented experimentally the first optical cryptographic setup based on chaotic erbium-doped fiber-ring lasers (EFRL) with an achievable bit rate of 126 Mbit/s [8; 114; 115]. Meanwhile, J.-P. Goedgebuer *et al.* achieved secure transmission of a sine-wave message using a wavelength chaos generator based on an optoelectronic oscillator [102; 116]. These first milestones ensured successful development of optical-chaos based communications. Shortly after

these studies, numerous optical configurations involving semiconductor lasers were proposed. Architectures using optoelectronic feedback were successful in their optical versions of CMa, CSK and CMo, ensuring Gbits/s data rates [117; 118; 119] .

3.4.1 Communications Architectures for Optoelectronic Devices with Internal Nonlinearities

In this subsection, we focus on the application of chaos masking (CMa), chaos shift keying (CSK), and chaos modulation (CMo) using optical chaos generators with internal nonlinearities. In a chaotic laser diode, there are essentially two possibilities to encrypt a message: (i) to act on the pumping current or (ii) to act on the optical output of the laser diode. For CMa and CMo the message is mixed in the optical carrier, whereas for CSK digital modulations of the current are typically used. This is has been summarized in Fig. 3.10. It is noteworthy that for CMo using laser diodes, the system requires feedback (optic or optoelectronic). At the receiver, feedback is not necessary to ensure a proper decryption; however when it is present, it usually modifies the conditions of synchronization. This results in the following classification of communication setups into *open-loop* and *closed-loop configurations*.

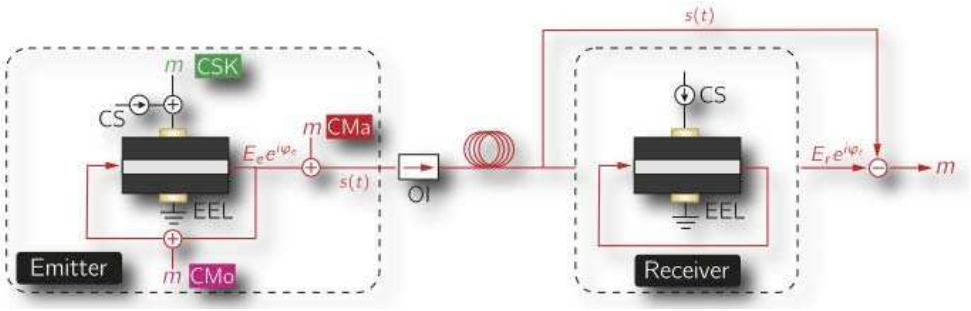

Figure 3.10: Schematic of the three typical chaos encryption techniques (CMa, CSK, and CMo) when chaotic optoelectronic devices with internal nonlinearity are used. The open- or closed-loop configuration depends on the existence of a feedback at the receiver (adapted from [120]).

3.4.1.1 Transmission Chain with an ECSL

In this subsubsection, we consider a transmission chain made with single-mode external-cavity semiconductor lasers (ECSL). Within the framework of the Lang-Kobayashi equations and neglecting the spontaneous emission noise, the cryptographic chain is modeled by

$$\frac{dE_e}{dt} = \frac{1}{2}(1+i\alpha)\left(G_{N,E_e} - \frac{1}{\tau_p}\right)E_e + F_e(t), \tag{3.44}$$

$$\frac{dE_r}{dt} = \frac{1}{2}(1+i\alpha)\left(G_{N,E_r} - \frac{1}{\tau_p}\right)E_r + F_r(t), \tag{3.45}$$

$$\frac{dN_{e,r}}{dt} = \frac{J_{e,r}}{e} - \frac{N}{\tau_s} - G_{N,E_{e,r}}\left|E_{e,r}\right|^2, \tag{3.46}$$

where the indices e, r denote variables associated with the emitter or receiver, respectively, and $F_{e,r}(t)$ is a feedback term that depends on the type of configuration and encryption used. When no message is encoded, the feedback terms read

$$F_e(t) = \eta_e e^{-i\omega_{0e}\tau_e} E_e(t-\tau_e), \tag{3.47}$$
$$F_r(t) = \eta_r e^{-i\omega_{0r}\tau_r} E_r(t-\tau_r) + \eta_c e^{-i\omega_{0e}\tau_c} E_e(t-\tau_c), \tag{3.48}$$

with $\eta_{e,r}$[1] the feedback strengths, η_c the injection strength, $\tau_{e,r}$ the roundtrip times in the external cavities, and τ_c the propagation time in the communication channel. Due to the complexity of the Lang-Kobayashi equations, only necessary conditions on the *complete synchronization* between two ECSLs can be derived. Assuming the two chaotic oscillators identical and in absence of frequency detuning $\Delta\omega_{e/r} = \omega_r - \omega_e$, it has been proven [59] that complete synchronization exists as soon as the injection and feedback strengths satisfy

$$\eta_e = \eta_r + \eta_c. \tag{3.49}$$

Under these conditions, the synchronization manifold reads

$$E_r(t) = E_e(t-(\tau_c-\tau_e)), \tag{3.50}$$
$$\phi_r(t) = \phi_e(t-(\tau_c-\tau)) - \omega_{0e}(\tau_c-\tau), \tag{3.51}$$
$$N_r(t) = N_e(t-(\tau_c-\tau)). \tag{3.52}$$

These equations highlight the crucial influence of the transmission time τ_c in the synchronization of distant ECSLs: Interestingly when $\tau_c < \tau$, the receiver can anticipate the behavior of the master[1]. This is known in the literature as *anticipating synchronization* [121]. Another type of synchronization exists with unidirectionally coupled ECSLs, the injection-locking synchronization [122], which is observed when the injection strength is far greater than the feedback strengths (at the emitter and/or receiver) $\eta_c \gg \eta_{e,r}$. This type of synchronization is more robust than CS, but remains imperfect [123; 124] though sufficient for optical-chaos transmission.

With chaos synchronization, the encryption or mixing of information in the dynamics of an ECSL is the second important issue. CMa is extremely popular and has led to successful field experiments on the Athens optical-fiber network (Greece) [4]. However, the method systematically disturbs the synchronization process which may increase the bit error rate (BER). Another popular encryption method is the CSK technique, because of its simplicity when used with ECSL [125]. Nevertheless, as any CSK method, the bit-rate will be fundamentally limited by the synchronization time of the ECSLs. Performance is usually inferior to those of a CMa [126]. When CMo is used, it generally offers the best level of performances, however, its practical implementation may become challenging especially to include the message.

Mathematically, the feedback terms have different expressions depending on the type of encryption used:

[1]When the communication chain is open-loop, the feedback strength at the receiver is zero $\eta_r = 0$ GHz.

[1]This does not violate the principle of causality. It simply states the possibility for the signal driving and synchronizing the two ECSLs to reach the receiver first.

- CMa encryption: The feedback terms at the emitter and receiver read $F_{e,CMa}(t) = F_e(t)$ and $F_{r,CMa}(t) = F_r(t) + m(t-\tau_c)$, respectively.

- CSK encryption: The feedback terms at the emitter and receiver remain identical to the case without encryption $F_{e,r,CSK}(t) = F_{e,r}(t)$. The pumping current is modulated.

- CMo encryption: The feedback terms read $F_{e,CMo}(t) = F_e(t) + m(t-\tau)$ and $F_{r,CMo}(t) = F_r(t) + m(t-\tau_c)$.

3.4.1.2 Transmission Chain with Semiconductor Lasers with Optoelectronic Feedback

Communication setups using semiconductor lasers with optoelectronic feedback share many features with those using ECSLs. The mathematical description is similar to that of an ECSL chain except for the optical feedback terms $F_e(t) = F_r(t) = 0$. The optoelectronic feedback affects the population inversion $N_{e,r}(t)$ with pumping currents depending on the delayed electrical field that read

$$J_e(t) = J_{0e}\left(1+\eta_e|E_e(t-\tau_e)|^2\right), \tag{3.53}$$
$$J_r(t) = J_{0r}\left(1+\eta_r|E_r(t-\tau_r)|^2+\eta_c|E_e(t-\tau_c)|^2\right). \tag{3.54}$$

The complete synchronization manifold has a similar structure to that of Eqs. 3.50-3.52 with the possibility of anticipation and requires analogous necessary conditions on the feedback and injection strengths $\eta_{e,r,c}$ to that of Eq. 3.49 [127; 128]. The interest in these systems is that any standard encryption technique can be easily implemented, especially CMo (the only technique that does not disturb the chaos synchronization); it now becomes as simple as CMa or CSK with ECSL. The expressions of the currents $J_e(t)$ and $J_r(t)$ for each type of encryption are given by the following:

- CMa encryption: The pumping current at the emitter and receiver respectively read $J_{e,CMa}(t) = J_e(t)$ and $J_{r,CMa}(t) = J_{0r}(1+\eta_r|E_r(t-\tau_r)|^2+\eta_c|E_e(t-\tau_c)+m(t-\tau_c)|^2)$. In CMa, the message is optically injected at the chaotic output of the emitter.

- CSK encryption: The pumping current at the emitter and receiver respectively read $J_{e,CSK}(t) = J_e(t) + m(t-\tau_e)$ and $J_{r,CSK}(t) = J_r(t)$. The message $m(t)$ is digital and usually binary.

- CMo encryption: The pumping current at the emitter and receiver respectively read $J_{e,CMo}(t) = J_{0e}\left(1+\eta_e|E_e(t-\tau_e)+m(t-\tau_e)|^2\right)$ and $J_{r,CMo}(t) = J_{0r}\left(1+\eta_r|E_r(t-\tau_r)|^2+\eta_c|E_e(t-\tau_c)+m(t-\tau_c)|^2\right)$.

Extensive work by J.-M. Liu and coworkers at the University of California at Los Angeles (UCLA) has been made with these systems. As a result, multi Gbit/s secure transmissions were successfully demonstrated [117; 118; 119].

3.4.2 Communications Architectures for Optoelectronic Devices with External Nonlinearities

In this subsection, we detail cryptographic setups involving either WCG, ICG, or PCG. Comparing with a single laser diode, the optoelectronic generators with external nonlinearities offer more possibilities of message's inclusion due to their block structure combining various components and internal transmission lines [129]. The three different chaos generators follow a generic loop structure connecting each of the following elements: a controlled or passive source, a nonlinear component, a detector, a filter, and a delay line. Subsequently, each connection between components becomes a potential input I_i to mix a message ($i \in [1, 5]$ with controlled source, $i \in [1, 4]$ with a passive source) therefore leading to many possible configurations for CMo. Each connection is also a potential output O_i that could be used in a CMa methods. Finally, some components in the loop structure may also have tunable parameters to be controlled by a user to encode a message, thus giving multiple choices to implement CSK. Some of these findings are represented in Fig. 3.11. The WCG is a typical structure with a controlled DBR laser diode; the nonlinear element is a birefringent crystal, the detector a photodiode, the filter an RF low-pass filter, and the delay line is an electronic buffer. ICG and PCG are typical architectures that make use of passive laser sources (standard CW semiconductor EEL).

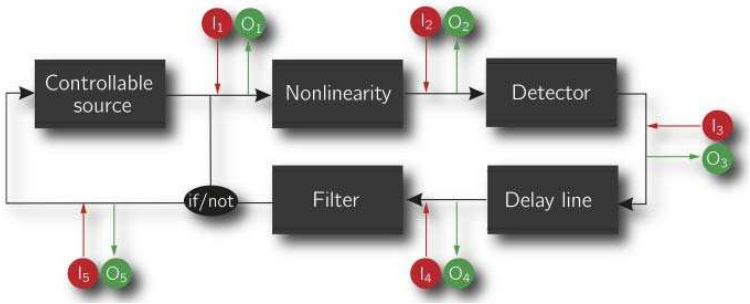

Figure 3.11: Schematics of the loop structure and the possible locations for a message's inclusion and output's selection (adapted from [129]), depending on the controllability of the source the loop ends before or just after the source. Inputs and outputs are labelled I_i and O_i, respectively. The positions of the delay line and the detector are interchangeable, thus ensuring the choice between an optical and an electrical delay line.

As in the previous case, one of the key issues is the synchronization of chaos which is necessary in optical chaos-based cryptographic schemes. Independent from the message's inclusion, the choice of the output will influence the coupling method between emitter and receiver. There are two main coupling configurations that are encountered with optoelectronic devices:

- *A diffusive-coupling configuration*, a typical closed-loop approach at the receiver [130].
- *An unidirectional-coupling configuration*, a typical open-loop approach at the receiver [7].

With the optoelectronic cryptosystems presented in this chapter, the latter coupling configuration is often preferred in the literature because of its simpler experimental implementation. As an illustration, ICG is used to implement CMa and CMo. The two different configurations can be modelled by two unidirectionally coupled integro-delay differential equations:

$$T_e\dot{x}_e + x_e + \frac{1}{\theta_e}\int_{t_0}^{t} x_e(u)du = s_{e,CMa/CMo}(t), \tag{3.55}$$

$$T_r\dot{x}_r + x_r + \frac{1}{\theta_r}\int_{t_0}^{t} x_r(u)du = s_{r,CMa/CMo}(t), \tag{3.56}$$

with $s_{e,CMa}(t) = \beta\cos^2\left(x_e(t-\tau)+\varphi_0\right)$, $s_{e,CMo}(t) = \beta\cos^2(x_e(t-\tau)+\varphi_0+m_{CMo}(t))$ at the emitter and $s_{r,CMa}(t) = \beta\cos^2(x_e(t-\tau_c)+\varphi_0)+m_{CMa}(t-\tau_c)$, $s_{r,CMo}(t) = \beta\cos^2(x_e(t-\tau_c)+\varphi_0+m_{CMo}(t-\tau_c))$ at the receiver. When no message is encrypted, the two systems are driven by an identical signal, though delayed by the transmission time τ_c. In the absence of message encryption, parameter mismatch between the emitter and receiver, and noise during transmission, the delayed synchronization error defined as $e(t) = x_r(t)-x_e(t-(\tau_c-\tau))$ follows the dynamics of a damped oscillator and converges asymptotically to zero. Consequently, the two chaotic ICGs are completely synchronized. For CMa and CMo encryption, the messages are decrypted using a simple subtraction in both cases:

$$\hat{m}_{CMa/CMo}(t-\tau_c) = s_r(t) - s_e(t). \tag{3.57}$$

Such configurations have been experimentally implemented and secure data transmissions were achieved using WCG [12], ICG [110], and more recently PCG [109].

In terms of performance, systems based on ICG and PCG have experimentally reached transmission at 3 Gbit/s with NRZ pseudo-random binary messages with a BER approximately 10^{-7} with an optical-fiber channel of a hundred of km [12]. These systems outperform architectures based on an ECSL assuming similar experimental conditions. As an example, at 2.5 Gbit/s the BER of ECSL cryptographic setups deteriorate significantly to approximately 5×10^{-2} (in the same experimental conditions to those mentioned above) [4].

3.5 Conclusions

In this chapter, we have reviewed the basics of semiconductor lasers and their application to various chaos-based cryptographic setups. First, we used a two-level medium placed in ring cavity to derive the Maxwell-Bloch equations. Then, we presented some fundamental concepts of the physics of semiconductor materials and their applications to derive the well known semiconductor-laser rate equations. After that, we discussed and modelled the most encountered optoelectronic systems used to generate optical chaos, exploiting either internal or external nonlinearities. A semiconductor laser being a crucial element in most of the architectures, our objective was for the reader to become familiar and understand the origins of simplified models that will be used extensively throughout the thesis.

Chapter 4

Security Analysis of Chaotic Optical Systems: The External-Cavity Semiconductor Laser

Abstract

A critical issue in optical chaos-based communications is the possibility for an eavesdropper to identify the parameters and the nonlinear function of a chaotic emitter and, hence, to break its security. In this chapter, we first recall various methods to break and identify a key parameter that threatens the security of time-delay chaotic systems: the time-delay. We introduce standard methods such as the autocovariance function (ACF), delayed-mutual information (DMI), local linear models (LLM), and global nonlinear models (GNM). Then, we focus our attention on a chaotic emitter that consists of a semiconductor laser with optical feedback, and the identification of its time delay corresponding to the external-cavity round-trip time, using the previously described methods applied to a chaotic time-series with no *a priori* knowledge on the ECSL. We unveil the key influence of the experimentally tunable parameters, *i.e.*, the feedback rate, the pumping current, and the time-delay value, in the identification process. Finally, we demonstrate that the time delay can be efficiently concealed and connect this result with the successive appearance of time scales in the system dynamics as it undergoes its route to chaos.

This chapter is mainly based on the two following publications:

- D. Rontani, A. Locquet, M. Sciamanna, and D.S. Citrin, "Loss of time-delay signature in the chaotic output of a semiconductor laser with optical feedback," *Opt. Lett.* **32**, 2960-2962 (2007).

- D. Rontani, A. Locquet, M. Sciamanna, D.S. Citrin, and S. Ortin, "Time-delay identification in a chaotic semiconductor laser with optical feedback: A dynamical point of view," *IEEE J. Quantum Electron.* **45**, 879-891 (2009).

4.1 Introduction

4.1.1 Security of Chaos-Based Cryptosystems

Security provided by most current software-based mathematical cryptosystems does not ensure information-theoretic security [1] except for the so-called one time pad (Vernam cipher) [131]. The computational complexity offered by these mathematical algorithms is what the chaotic oscillators aim at achieving using laws of physics. In a chaos-based cryptographic setup, the key corresponds to the set of parameters and the algorithm to the nonlinear dynamical representation of the system.

As recalled in the general introduction, two strategies exist for an eavesdropper to break a chaotic cryptosystem: (i) a direct retrieval of the embedded data stream in the chaotic carrier or (ii) a reconstruction of the chaotic dynamics with an *a posteriori* retrieval of the message. Under certain circumstances the eavesdropper can exploit her complete knowledge of the chaos-generating process (white box), partial knowledge (gray box), or total lack of knowledge (black box) to perform his attacks.

In the white-box case, the structure of the chaotic emitter is known; only the parameter set (the key) is unknown. In this case, the question of robustness of synchronization is central. On the one hand, a lack of robustness of synchronization will imply that even a legitimate receiver will not be able to synchronize and recover the encrypted message. On the other hand, if synchronization is too robust, an eavesdropper will easily synchronize even with a significantly different key.

Within this context, countless methods have been developed to break typical encryption schemes (CMa, CSK, or CMo) such as autocorrelation and spectral analysis [10], return-maps [132; 133], and parameter identification using synchronization [112]. However, in many situations the eavesdropper has only a partial or no information on the structure of the cryptosystem. He can only process a single time series wiretapped from the communication channel. The time series constitutes incomplete information on its underlying chaotic generation process. Under certain conditions known as the embedding theorem [134; 135]; however, it is possible to construct an isomorphic representation of the system's dynamics in an alternate phase space. For example, in the delay reconstruction method, the system is described by a delayed vector $[x(t), x(t-\tau_\Delta), \ldots, x(t-(m-1)\tau_\Delta)]$ with m the embedding dimension and τ_Δ a time-interval delay. This isomorphic representation is an embedding if $m > 2d_c$, where d_c is the fractal dimension of the attractor. This alternate representation of the system shares the same invariants (entropy, dimension, Lyapunov spectrum) [136] and allows for an eavesdropper to extract sensitive information from the cryptosystem. This approach has been successfully used to crack low-dimensional chaos-based cryptosystems [137; 138].

4.1.2 Security of Time-Delay Systems

The aforementioned reconstruction of the dynamics in a black-box context is tractable only for low-dimensional systems [139; 140]. Consequently, the use of high-dimensional chaotic systems should provide a higher level of computational security that renders difficult the use of embedding techniques. A simple method to design such chaotic

systems is the introduction of a time delay in the dynamics. As a matter of fact, many optical chaotic systems possess this feature, such as wavelength chaos generators (WCG) [102; 103; 116], intensity chaos generators (ICG) [12; 106], and semiconductor lasers with optical (ECSL) [94] or optoelectronic (OECSL) feedback [117] (see Chapter 3). It has been proven that high dimension and entropy occurs in these types of systems [33; 101; 141]. However, the complexity can be threatened by knowledge of the time delay. In delayed hyperchaotic systems, the security assumption is based on the computational complexity to reconstruct a high-dimensional attractor from the time series. Indeed, knowing the time delay used by a hyperchaotic generator, an eavesdropper can reconstruct the dynamics of the system in a reduced-dimensional phase space [142], thus allowing low-complex computational reconstruction methods to be efficient [143; 144]. The key behind the success of such breaking techniques relies on the knowledge of the time delay, which can be inferred from the time series using statistical signal analysis [145]. Concealing the time delay is therefore fundamental to preserve the computational security of a chaotic system. We illustrate in Fig. A.2 a security leak resulting from the knowledge of the time delay, when a WCG is analyzed.

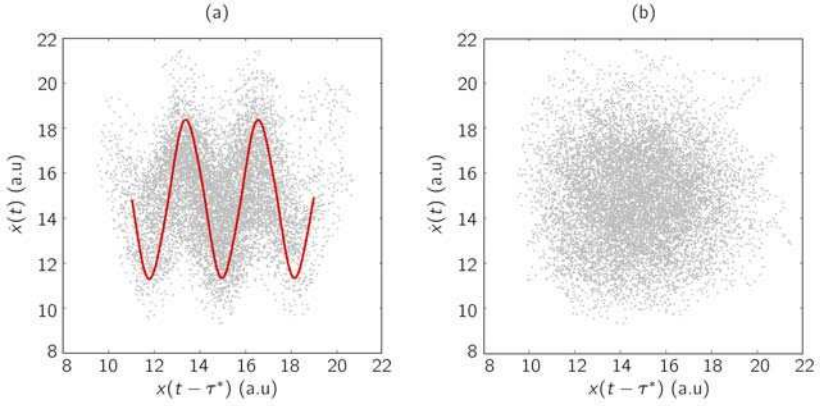

Figure 4.1: Identification of the nonlinear function of the optoelectronic WCG with knowledge of the time delay. The gray dots represent the discretized time series, in the projected plane $(\dot{x}(t), x(t-\tau^*))$. (a) $\tau^* = \tau$ (b) $\tau^* = 1.1\tau \neq \tau$. Depicted in the solid red line is the shape of the theoretical nonlinear function of the WCG. The parameters used in the simulation are $T = 10$ μs, $\beta = 30$, $\varphi_0 = \pi/4$, and $\tau = 500$ μs.

In Fig. A.2(a), the time delay is known. As a result, the time series, when projected in the plane $(\dot{x}(t), x(t-\tau^*))$, is distributed along a geometric structure with a shape depending on the system's nonlinear function. In Fig. A.2(b), however, even a 10% error in the time delay results in an apparent random distribution in the projected phase space. As a consequence, the time delay critically affects the knowledge that one can extract from the system in the reduced phase space $(\dot{x}(t), x(t-\tau^*))$. Time-delay identification should therefore be considered as an additional argument to appreciate the level of security of optical chaos-based communications, besides chaos complexity and robustness of synchronization. The security threat associated with the time delay has triggered strategies to counter its straightforward estimation; random commutations [146] and stochastic evolution of the time delay [147] are

two examples. These methods will prevent an eavesdropper to access the time-delay information using standard statistical estimation from a time series transmitted in the communication channel (described in the next section).

4.1.3 System Investigated: the ECSL

4.1.3.1 Interest in ECSL and Security Issues

Semiconductor lasers with an external cavity (ECSL) have been considered as rich sources of optical chaos, with well-known chaotic regimes such as the so-called coherence collapse [96] and low-frequency fluctuation (LFF) regimes [148]. These two regimes have received considerable attention, since they represent key elements of optical secure chaotic communications, as illustrated in the previous chapters. Their omnipresence in optical setup is explained by high modulation speed of the system, and the generation of high-dimensional and complex chaos [101], which make the ECSL a suitable chaotic optical system for secure communications.

Nevertheless, it is also essential that an ECSL's time delay should not be easily identifiable from the analysis of its time series. Until recently, ECSLs with a single optical feedback were considered as weakly secure [149; 150], such that the use of several external cavities has been suggested [150]. Interestingly, the security was systematically investigated for parameters values that ensures high chaos complexity (dimension and entropy) by analogy with situations occurring in optoelectronic systems such as WCG or ICG. In fact, in laser diodes with optical feedback, high-dimensional chaos is typically found where the optical feedback strength (η) is large, but then the time-delay value is easily retrieved from the analysis of the chaotic output using straightforward techniques. As a matter of fact, the highest level of security with respect to time-delay identification may not correspond to parameter regions where the complexity of the ECSL is maximum. This is what we propose to theoretically investigate in the next section.

4.1.3.2 Modeling & Framework of Analysis

Before investigating the theoretical estimation of the time delay, we consider a model of an chaotic ECSL owned by a legitimate user Alice. The ECSL is composed of a single-mode semiconductor laser with coherent optical feedback and is represented in Fig.4.2.

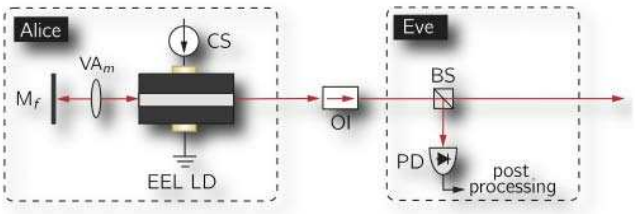

Figure 4.2: Experimental scheme of an external cavity laser (ECSL). It is composed of a laser diode (LD) electrically pumped by a current source (CS). The external cavity is composed of a variable attenuator (VA) and a mirror (M). A beam-splitter (BS) and a photodiode (PD) are used by the eavesdropper (Eve) to record the intensity time series and post-process it.

The system is modeled by the Lang-Kobayashi rate equations [94]. To reiterate, they are

$$\frac{dE(t)}{dt} = \frac{1}{2}(1+i\alpha)\left(G_{N,E} - \frac{1}{\tau_p}\right)E(t) + \eta E(t-\tau)\,e^{-i\omega_0\tau} + F(t), \quad (4.1)$$

$$\frac{dN(t)}{dt} = J - \frac{N}{\tau_s} - G_{N,E}|E|^2, \quad (4.2)$$

where $E(t) = |E|\,e^{i\varphi(t)}$ is the slowly varying complex electric field, N is the average carrier density in the active region, α is the linewidth-enhancement factor that describes the amplitude-phase coupling, $G_{N,E} = g_N(N - N_0)/(1 + \varepsilon\,|E|^2)$ is the optical gain where ε is the saturation coefficient, N_0 is the carrier density at transparency, ω_0 is the angular frequency of the solitary laser, η is the feedback rate, τ_p is the photon lifetime, τ_s is the carrier lifetime, J_{th} is the threshold current, p is the pumping factor, and τ is the delay corresponding to the round-trip time of light in the external cavity. The Langevin force $F(t)$ models the spontaneous-emission noise. Its polar decomposition in amplitude and phase is given by the two terms $F_{|E|}(t) = 2\beta N(t)/E(t) + \sqrt{2\beta N(t)}\zeta_{|E|}(t)$ and $F_\varphi(t) = 1/E(t)\sqrt{2\beta N(t)}\zeta_\varphi(t)$, where β is the spontaneous-emission rate. The variables $\zeta_{|E|}(t)$ and $\zeta_\varphi(t)$ represent uncorrelated white Gaussian noise that satisfies $\langle\zeta_{|E|}(t)\rangle = \langle\zeta_\varphi(t)\rangle = 0$, $\left\langle\zeta_{|E|}(t)\zeta^*_{|E|}(t')\right\rangle = \langle\zeta_\varphi(t)\zeta^*_\varphi(t')\rangle = \delta(t-t')$, and $\langle\zeta_{|E|}(t)\zeta^*_\varphi(t')\rangle = 0$.

The ECSL transmits its chaotic time series in an optical communication channel. We assume that an eavesdropper (Eve) can wiretap the channel and retrieve the total information on the transmitted time series. In our case, the security of the ECSL is investigated under favorable conditions where the eavesdropper wiretaps directly the optical channel, recording and analyzing the intensity time series defined as $I(t) = |E(t)|^2$.

4.2 Time-Delay Identification

In this section, we present standard techniques to recover the time-delay information: the autocovariance function (ACF), the delayed entropy and mutual information (DE and DMI), local linear models (LLM), and global nonlinear model (GNLM) such as neural networks [136]. These methods are sensitive to the presence of particular time scales in a given time series, such as a time delay. Each method will eventually detect the *signature* of a particular time-scale through a local resonance (extremum), which will later be referred to as a *peak* or *valley*. Finally, the time location of a peak or valley will be considered as a possible estimation of the time delay.

4.2.1 Autocovariance Function (ACF)

If we consider a stochastic process $X(t)$, the autocorrelation function is defined by the real function

$$R_X(t_1, t_2) = \mathbb{E}(X(t_1)X(t_2)), \quad (4.3)$$

where $\mathbb{E}(\cdot)$ is the mathematical expectation operator.[1] If we suppose that the process is wide-sense-stationary (WSS),[2] it is possible to define the autocovariance function (ACF)

$$\Gamma_X(\theta) = \mathbb{E}\left((X(t) - \mu_X)(X(t+\theta) - \mu_X)\right), \tag{4.4}$$

with $\mu_X = \mathbb{E}(X(t))$ the mean of the stochastic process. If we consider the process to be ergodic,[3] it is possible to replace the mathematical expectancy by the time average $\langle X(t)\rangle = \lim_{T\to\infty} 1/2T \int_{-T}^{T} X(t)dt$ and compute the ACF from an single time series,

$$\Gamma_X(\theta) = \langle (X(t) - \mu_X)(X(t+\theta) - \mu_X)\rangle. \tag{4.5}$$

For a given value of θ, we can geometrically interpret the ACF as a measure of the tendency of the cloud $(X(t), X(t-\theta))$ of points to be aligned along a straight line. The ACF thus measures a linear relationship between $X(t)$ and $X(t-\theta)$.

4.2.2 Delayed Entropy (DE) & Delayed Mutual Information (DMI)

The entropy and mutual information are metrics originally used in information theory [2]. Given two continuous variables X and Y with joint probability density function (pdf) $f_{X,Y}(x,y)$, and marginal pdfs $f_X(x)$ and $f_Y(y)$, the entropy and mutual information are respectively defined by

$$\mathbf{H}(X) = -\mathbb{E}\left(\ln(f_X(X)\right), \tag{4.6}$$

$$\mathbf{I}(X,Y) = \mathbb{E}\left(\ln\left(\frac{f_{X,Y}(X,Y)}{f_X(X)f_Y(Y)}\right)\right). \tag{4.7}$$

In our context, the two variables X and Y are obtained by sampling the random process $X(t)$ at two times t and $t+\theta$, and such a process is assumed to be stationary and ergodic. The probability density functions $f_{X(t),X(t+\theta)}$, $f_{X(t)}$, and $f_{X(t+\theta)}$ will be estimated by their respective histogram $\hat{f}_{X(t),X(t+\theta)}$, $\hat{f}_{X(t)}$, and $\hat{f}_{X(t+\theta)}$ computed from their time series. They lead to the approximate entropy and mutual information estimator, also called delayed entropy (DE) and delayed mutual information (DMI),

$$\hat{\mathbf{H}}(\theta) = -\mathbb{E}\left(\ln(\hat{f}_{X(t)}(X)\right), \tag{4.8}$$

$$\hat{\mathbf{I}}(\theta) = \mathbb{E}\left(\ln\left(\frac{\hat{f}_{X(t),X(t+\theta)}(X,Y)}{\hat{f}_{X(t)}(X)\hat{f}_{X(t+\theta)}(Y)}\right)\right). \tag{4.9}$$

The entropy corresponds to an average measure of disorder in a given system or random variable. The mutual information corresponds intuitively to the quantity of information that the two random variables $X(t)$ and $X(t+\theta)$ share. In time-delay

[1] If we consider a random variable X defined on the probability space $(\Omega, \mathscr{F}, P)$ with P a measure of probability, then the expectancy operator is defined by $\mathbb{E}(X) = \int_\Omega X dP$. If the variable X admits a pdf $f_X(x)$, then $\mathbb{E}(X) = \int_{\mathbb{R}} x f_X(x) dx$.

[2] **Wide-sense-stationary (WSS):** A stochastic process $X(t)$ is WSS if its mean is constant $\mathbb{E}(X(t)) = \mu_X$ and its autocorrelation depends only on $\theta = t_1 - t_2$, $R_X(t_1,t_2) = R_X(\theta) = \mathbb{E}(X(t)X(t+\theta))$.

[3] **Ergodicity:** A random process is ergodic if its averaging over a time and over its probability space are equal.

systems, the presence of a delayed feedback term induces a nonlocal time dependence in the time evolution of its state variables. The integral definition of the estimators under consideration allows for the detection of nonlocal time dependencies that are linear for the ACF and nonlinear for the DMI.

4.2.3 Local Linear Models (LLM)

The use of local linear models (LLMs) was first suggested for single time-delay scalar systems in [151; 152] and for vectorial systems in [142] and can be generalized to systems with multiple delays. A vectorial system with p time delays is considered,

$$\dot{\mathbf{x}}(t) = f(\mathbf{x}(t), \mathbf{x}(t-\tau_1), \ldots, \mathbf{x}(t-\tau_p)), \tag{4.10}$$

with $\mathbf{x} \in \mathbb{R}^n$, the state vector of the system. As a consequence, each coordinate of the reduced phase space $\Sigma = (\dot{\mathbf{x}}(t), \mathbf{x}(t), \mathbf{x}(t-\tau_1), \ldots, \mathbf{x}(t-\tau))$ is functionally related. This compels the system's attractor projection to lie within a surface $S \subset \Sigma$. In practice, the continuous space and most of the coordinates of the state vector are inaccessible; that is why we consider a discrete series of scalar measurements $\{x_k\}_{k\in\mathbb{N}}$ sampled from the system's output. A delayed phase space is then built with the coordinates

$$\begin{aligned}\Sigma_{d,\{\tau_i\}_{i=1,\ldots,N}} = (&x_{k+1}, x_k, \ldots, x_{k-(m+1)}, x_{k-\tau_1}, \ldots, \\ &x_{k-\tau_1-(m+1)}, \ldots, x_{k-\tau_p}, \ldots, x_{k-\tau_p-(m+1)}).\end{aligned} \tag{4.11}$$

The number m of additional coordinates is necessary to take into account the variables (state vector components) that are not captured by the time series and has to satisfy $m > 2n$. It is assumed that the projection of the reconstructed attractor S_d in $\Sigma_{d,\{\tau_i\}_{i=1,\ldots,N}}$ will have close geometric properties to those of the surface S associated to the true projected attractor. When the time delays are unknown and a candidate for the reconstructed phase space is considered, $\Sigma_{d,\{\theta_i\}_{i=1,\ldots,N}}$, it would correspond to the discretization of a true projected phase space $\Sigma_\theta = (\dot{\mathbf{x}}(t), \mathbf{x}(t), \mathbf{x}(t-\theta_1), \ldots, \mathbf{x}(t-\theta_N))$ where the functional relationship is not ensured and therefore the attractor is not projected on a surface S. This property is used to retrieve the information concerning the time delay. We first use a family of hyperplanes $\{L_{k,\{\tau_i\}_{i=1,\ldots,N}}\}_{k\in\mathbb{N}}$ defined in each point of the reconstructed discrete phase space $\Sigma_{d,\{\theta_i\}_{i=1,\ldots,N}}$, leading to the local linear models. The average quadratic errors are computed between this family and the projected attractor. When the set $\{\theta_i\}_{i=1,\ldots,N}$ is equal to $\{\tau_i\}_{i=1,\ldots,N}$, this error becomes minimal and this is how a single or multiple time delays can be retrieved. This method allows one to detect when the projected attractor lies on the surface S, a situation occurring only in Σ.

4.2.4 Global Nonlinear Models (GNLM)

The principles of a global nonlinear model (GNLM) are similar to those used for the LLM approach; however, instead of minimizing the quadratic error with a set of local planes, a global nonlinear function is used. A class of global discrete nonlinear functions, such a modular neural networks (MNN), has been proposed in [153] to identify a single time delay. We illustrate the MNN approach in this subsection.

The neural network aims at mimicking the structure of the equations of the nonlinear system under consideration. Toward this end, it incorporates two modules, (i) one for the non-delayed part (ND) of the system and a second one for its delayed part (D). A feedforward neural network is used for each of the modules. The first non-delayed module is fed with input data $\mathbf{x}_{ND} = (x_n, \ldots, x_{n-(m_{ND}+1)})$ whereas the second module is fed with $\mathbf{x}_D = (x_{n-\theta}, \ldots, x_{n-\theta-(m_D+1)})$, with the number of inputs m_{ND} and m_D of each module independently chosen , and θ being a candidate time delay. The output of the modular neural network is defined by

$$y_{NN} = f_{ND}(\mathbf{x}_{ND}) + f_D(\mathbf{x}_D), \tag{4.12}$$

with f_{ND} and f_D the nonlinear function associated to each module. These functions result from the particular topology of the neural network activated after being trained. Comparing to standard feedforward neural networks, the modular approach results in more flexibility for the network, with each module interacting with each other. Each module can then specialize in the reproduction of the behavior of the non-delayed and delayed vector fields of the real time-delay system. To perform the identification, the forecasting error $\sigma(\theta) = ||x_n - y_{n,NN}||$ is computed. A given value θ^* is considered to be an estimation of the true time delay τ, if the forecasting error is globally minimized.

4.3 Security Analysis of the ECSL

4.3.1 Influence of the Operational Parameters

In this subsection, we focus our attention on the capacity of an ECSL to produce consistent time-delay signatures (TDS) using ACF and DMI estimators. We illustrate the key role of (i) the feedback strength η, (ii) the pumping current J, and (iii) the time delay τ in the estimation of the time delay.

4.3.1.1 Influence of the Feedback Strength

The feedback strength η controls the optical power reinjected in the laser cavity and hence drives the contribution of the delayed intensity $I(t-\tau)$ to the time evolution of $I(t)$ wiretapped by an eavesdropper. As a matter of fact, the time-delayed feedback term $\eta E\,(t-\tau)\,e^{-i\omega_0\tau}$ is linearly introduced in the Lang-Kobayashi equations; it is thus expected that the stronger η is, the larger the information shared between $I(t-\tau)$ and $I(t)$ will be. The structure of the Lang-Kobayashi equations is such that the separation of the delayed and non-delayed part is pretty straightforward. This specificity can qualitatively explain the particular interplay of time scales, the relaxation-oscillation period τ_{RO} and the time delay τ, each associated to the respective parts of the equation. Figure 4.3 pictures a case of time-delay identification. Each line displays the recorded time series; the ACF and DMI computed for a given value of η. Large values of η lead to a strongly developed chaotic regime (Fig. 4.3(j)) for which a sharp signature of the time delay is observed. It has a large amplitude and a precise location in both the ACF and DMI (see Fig. 4.3(k)-(l)), and is a typical situation reported in the literature [149].

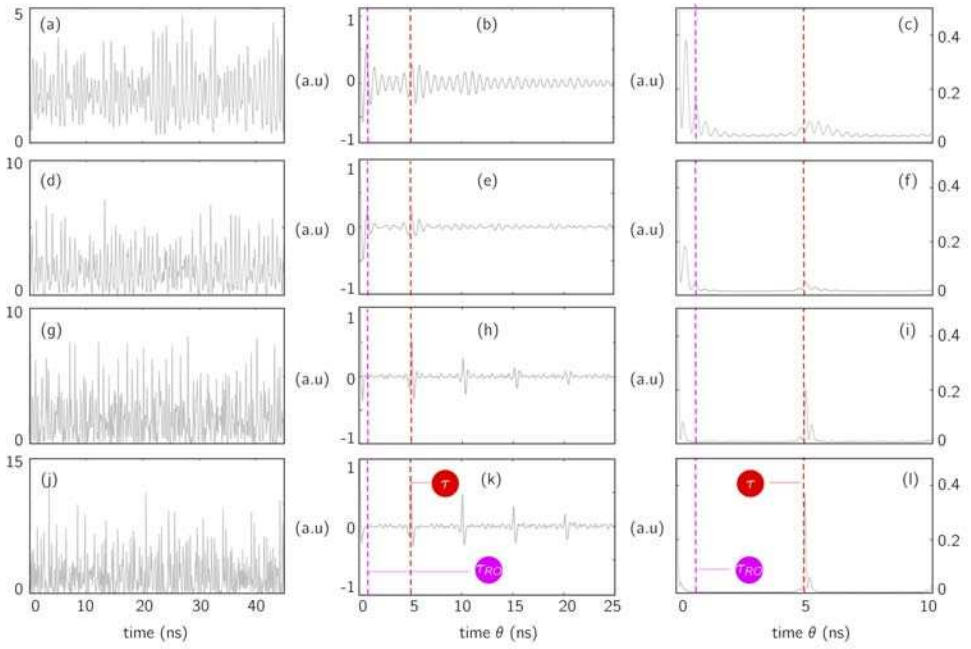

Figure 4.3: Intensity time series produced by an ECSL and recorded by the eavesdropper (1st column), autocovariance function (2nd column) and delayed mutual information (3rd column) for increasing value of the feedback rate $\eta = 2$ GHz (1st row), 5 GHz (2nd row), 10 GHz (3rd row), and 15 GHz (4th row) with a time-delay value $\tau = 5$ ns and $\tau_{RO} = 0.75$ ns. The vertical red dashed and purple dashed lines give the time location of τ_{RO} and τ, respectively.

The autocovariance also reveals the presence of signature at integer multiples of the time delay with the remarkable property that the ratio of the amplitude between consecutive signatures is approximately constant, $\Gamma_I(k\tau)/\Gamma_I((k+1)\tau) \approx \gamma < 1$ and leads to an exponential decrease of the signatures with the multiplicity order. This also reveals that the ECSL uniformly destroys the information between the intensity and its successive delayed versions. The progressive decrease in feedback strength first induces a decrease of the signature's amplitude while preserving the exponential decrease of amplitude for the signature in both estimators at the multiples of the time delay (Fig 4.3(h)-(i)), until it reaches a minimum value (Fig. 4.3(e)-(f)). Then, a qualitative change of behavior appears in the estimator for relatively weak feedback strengths; instead of a sharp peak emerging from a noisy background, the estimators present oscillations with an approximate period equal to τ_{RO}. They are locally amplified in the vicinity of integer multiple of the time delay τ (Fig. 4.3(b)-(c)). They also complicate the time-delay identification; the location and amplitude are perturbed, and the estimation of the time delay will be at the precision of $\tau_{RO}/2$. As a consequence, at weak feedback strengths a relative increase of the ECSL's security is observed, a phenomenon that was not hitherto reported. It is however still possible to retrieve a trustworthy estimation of the time delay, through the local amplification of the oscillations of the estimators. At this point, no benefit in security can be achieved by further reducing the feedback strength; if it is too weak, the ECSL is not chaotic any more.

4.3.1.2 Influence of the Pumping Current

All parameters being fixed except the time delay, the scenario of progressive loss of the clarity of time-delay signatures with decreasing feedback strength is relatively universal. In the previous subsubsection, the choice of the relaxation oscillation period $\tau_{RO} = 0.75$ ns corresponded to a level of pumping current close to the threshold (5 % above threshold current), the internal ECSL's parameters remaining identical. To investigate the influence of the pumping current J, we analyze quantitatively the location and amplitude of the time-delay signature when the feedback varies for three different pumping currents. The findings are reported in Fig. 4.4.

Figure 4.4 is obtained by considering the signature with the largest amplitude (in the ACF and DMI) in a vicinity $W(\tau)$ of the theoretical time-delay location. The curves associated with different pumping currents (triangles, circles, and squares) all present similar tendencies: V-shaped where the amplitude starts decreasing until it reaches a global minimum followed by an increasing phase as the feedback strength increases (Fig. 4.4(a)-(c)). Qualitatively, the decreasing region of the curve corresponds to a weak chaotic regime, where the laser's intrinsic nonlinearity and the delayed feedback term have equivalent driving actions. Under these conditions, the

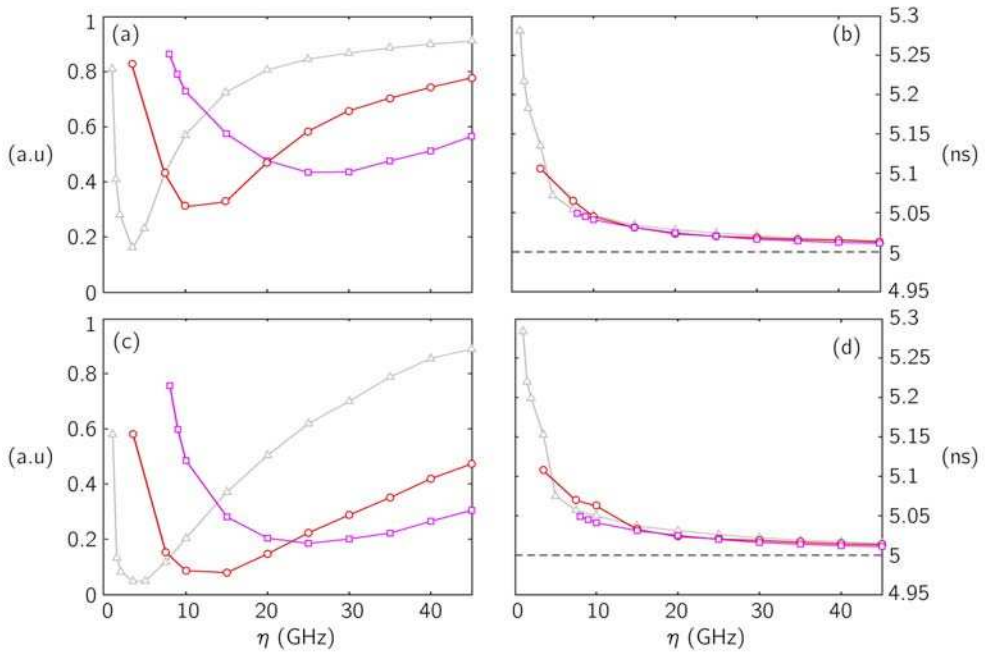

Figure 4.4: Impact of the feedback strength η and pumping current pJ_{th} on the amplitude and time location of the most significant peak in the vicinity $W(\tau) = [4.5 \text{ ns}; 5.5 \text{ ns}]$ of the time delay $\tau = 5$ ns. Sub-figures (a)-(b) give respectively the amplitude and time location of $\max_{\theta \in W(\tau)} |\Gamma_I(\theta)|$; (c)-(d) gives respectively the amplitude and time location of $\max_{\theta \in W(\tau)} |\hat{\mathbf{I}}(\theta)|$. The solid lines with gray-triangles (△), red-circles (◯), and purple-squares (□) stands for $p = 1.05$, 1.26, and 1.72, respectively. These three different values of p correspond to the relaxation oscillation periods $\tau_{RO} = 0.75$ ns, 0.33 ns, and 0.2 ns, respectively. In sub-figures (b)-(d), the dot-dashed lines give the time location of the time delay $\tau = 5$ ns.

estimators (ACF, DMI,...) may still exhibit structural relationships within the intensity time series associated with the relaxation-oscillation dynamics and the influence of the delayed injected optical field. As the feedback is increased, the influence of the relaxation oscillation becomes weaker and the signature of the relaxation oscillations tends to disappear. When the global minimum is achieved, the driving action are conforming. Then the increase of feedback strength makes the influence of the delayed optical field more significant, thus leading the amplitude of the time-delay signature to steadily increase. The increasing of the pumping current, however, shifts and opens the V-shape of the curve; the global minimum of the amplitude of time-delay signature increases and occurs for larger values of feedback strength. This implies that large pumping currents have a detrimental effect on the security of the ECSL. With the values of pumping used in Fig. 4.4, the relaxation-oscillation periods are respectively $\tau_{R0} = 0.75$ ns, 0.33 ns, and 0.2 ns. As a consequence, for weak feedback strengths, the disturbance of the oscillations in the estimators observed in Fig 4.3 will be reduced because of the precision of the time delay signature modulo $\tau_{RO}/2$. This effect is illustrated in Fig. 4.4(b)-(d). The maximum shift in the location of the estimated time delay is about $\tau_{RO}/2$, for the weakest possible feedback strengths that allow the ECSL to be chaotic. As the feedback strength increases, the locations of the signature have similar evolutions and ultimately only a small time shift persists.

In summary, this first analysis shows the key role of two operational parameters (feedback strength η and pumping current J) in the characteristics of the time-delay signature (amplitude and location). Qualitatively, it is suggested that a combination of weak feedback strength (still ensuring a chaotic regime of the ECSL) combined with a pumping current close to threshold ensures the strongest loss of information about the time delay. However, the concealment is not perfect and it is still easy for an experienced eavesdropper to recover the time-delay signature using standard techniques such as ACF or DMI. Amongst the operational parameters, there is still the time-delay that can be tuned. In the next subsection, we will address specifically the role of this parameter and show how a proper choice could lead to optimized time-delay concealment leading to a complete loss of signature.

4.3.2 Optimized Time-Delay Concealment: Influence of the Time Delay Relatively to the Relaxation-Oscillation Period

The previous section has clearly identified a form of competition at weak values of feedback strength η between two primary time scales existing in an ECSL: the relaxation-oscillation period and the time delay. This competition results in the coexistence of two signatures with dual features: a localized and impulsional shape for the time delay and a delocalized and oscillating shape for the relaxation-oscillation period. The idea behind an optimization of the concealment consists of bringing the two time scales close to each other such that it becomes difficult to identify the origin of each contribution. A new scenario of identification is considered in Fig. 4.5 with the value of the time delay $\tau = 1.2$ ns and the other parameters kept identical to those of Fig. 4.3.

Following the line of reasoning of the previous subsection, we show that the effect

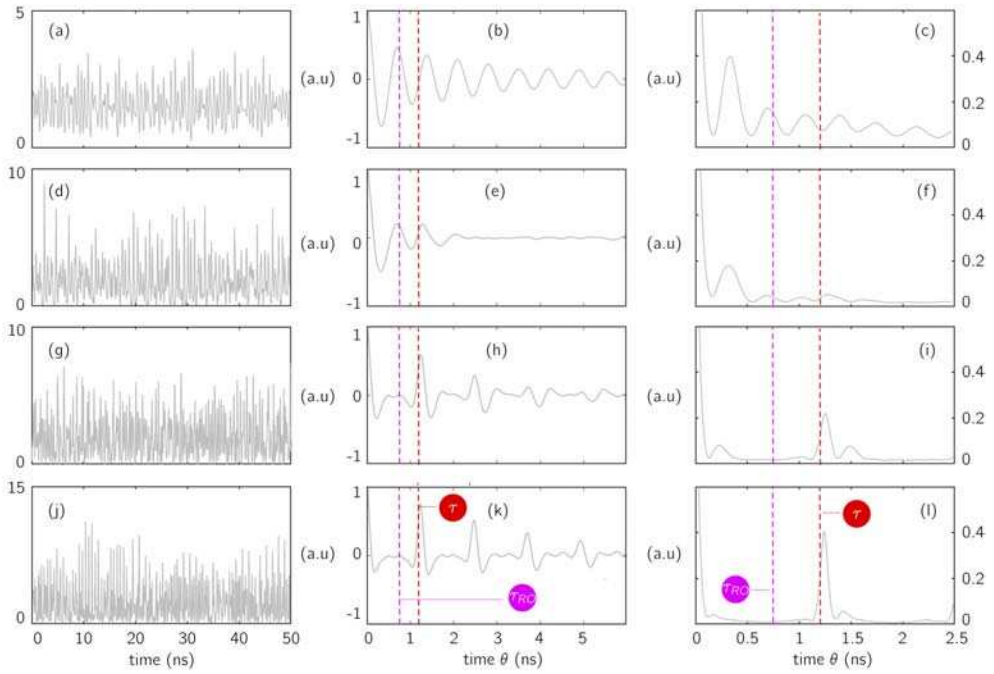

Figure 4.5: Scenario of identification with close time scales. The ECSL's intensity time series (1st column), autocovariance function (2nd column), and delayed mutual information (3rd column) are plotted for increasing value of the feedback strength $\eta = 2$ GHz (1st row), 5 GHz (2nd row), 10 GHz (3rd row), and 15 GHz (4th row) with a time delay $\tau = 1.2$ ns and $\tau_{RO} = 0.75$ ns. The vertical red dashed and purple dashed lines give the time location of τ_{RO} and τ, respectively.

of the coexistence of two time scales at weak feedback and weak pumping is stronger. When the time delay is close to the free-running relaxation-oscillation period, this may have an even stronger effect on the time-delay signature. Figure 4.5 illustrates this fact. At large feedback strength, the reduction of the time separation between τ and τ_{RO} does not produce a qualitative change of the time-delay identification; both estimators exhibit sharp time-delay signature with a precise time-location close to the theoretical time-delay (Fig. 4.5(k)-(l)). Then, a diminution of the feedback strength leads to a decrease in the signature's amplitude (Fig. 4.5(h)-(i)), as reported in Fig. 4.3. Then for a sufficiently small value of the feedback strength, the effect of the relaxation oscillation dynamics is enhanced. This leads to a time-delay signature hardly retrievable [Fig. 4.5(e)-(f)], whereas it is still possible to retrieve it when the two time scales are sufficiently disparate (Fig. 4.3(e)-(f)). We notice first that the transition between the pulse-like shape and oscillating shape of the estimator (at $\eta = 5$ GHz) corresponds to a particularly adapted situation to conceal the time-delay signature. Finally, the time-delay signature is completely lost; only oscillations are visible in the estimator and they correspond roughly to the relaxation-oscillation period [Fig. 4.5(b)-(c)]; exponentially-damped oscillations are visible in the ACF and DMI with an approximate period of τ_{RO}.

The ACF and DMI are relatively simple estimators, and the loss of time-delay signature from the analysis of intensity time series may be connected to intrinsic

limitations of the identification methods. To guarantee the robustness of the concealment, other identification methods have been tested such as the LLM and GNLM. The analysis tends to confirm that in the case of close values of τ and τ_{RO}, weak feedback strengths η and weak pumping currents J the time delay is not retrievable even with those methods. Figure 4.6 illustrates this fact by presenting the evolution of the forecasting error of a modular neural network (MNN) as a function of the candidate time delay θ.

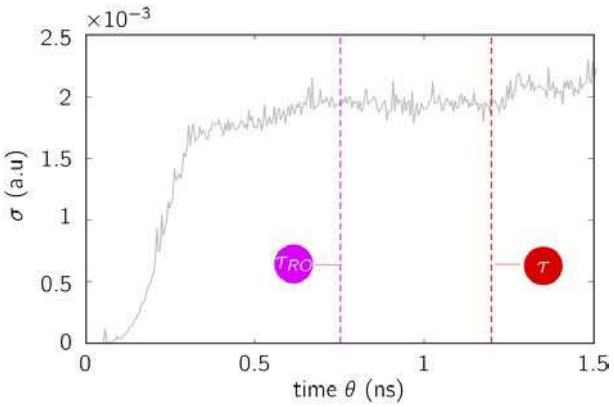

Figure 4.6: Identification with close time scales using a modular neural network (MNN) generated with the following parameters: $\tau = 1.2$ ns, $\tau = 0.75$ ns, and $\eta = 2$ GHz. The evolution of the forecasting error $\sigma(\theta)$ is plotted as a function of θ with an resolution of 5 ps. The vertical purple and red dashed lines give the time location of the delay and the relaxation oscillation period, respectively.

Figure 4.6 presents the results of a time-delay extraction based on a MNN composed of six neurons in the first layer and three neurons in the second layer for the delayed module (D) and only one neuron for the non-delayed module (ND). The plot of the forecast error reveals only a minimum for values close to $\theta = 0$ ns, that corresponds to the linear correlation time [153]. We do not observe, however, any other minimum in the vicinity of the time delay τ.

4.4 Dynamical Origin of the Time-Delay Concealment

The previous section has shown that the identification of the time delay strongly depends on the operational parameters of the ECSL: the feedback rate η, the pumping current (J), and the value of τ relatively to τ_{RO}. At high feedback strength, the estimators always possess a predictable behavior: a pulse-like shape with a clear time-delay signature. However, this regularity disappears, when the feedback rate is weak.

The detection of the relaxation-oscillation dynamics in the estimator at weak injection strength suggests a closer analysis of the time scales involved in the early stages of the ECSL dynamics. We show that the route to chaos and the frequency generated during the cascade of bifurcations shaped the estimators at weak feedback strength, when the ECSL becomes chaotic for the first time. The feedback strength η will be taken as the bifurcation parameter in the following investigations.

4.4.1 Interpretation of a Disparate Time-Scales Scenario

In this subsection, we consider the case studied in subsection 4.3.1.1 for which the time delay and the relaxation-oscillation period are disparate, $\tau = 5$ ns and $\tau_{RO} = 0.75$ ns.

The dynamics associated with this scenario are depicted in Fig. 4.7. The bifurcation diagram of the ECSL's intensity reveals a quasiperiodic (QP) route to chaos [Fig. 4.7(a)]; the stationary solution of the ECSL, an external cavity mode (ECM), is first destabilized through a Hopf bifurcation (H1) and induces time-periodic dynamics [Fig. 4.7(a1)], at frequency $f_{H1} \approx f_{RO} = 1.34$ GHz (Fig. 4.7(b1)). This periodicity is revealed by both estimators (ACF and DMI): the signature of the time scale $\tau_{H1} = 1/f_{H1}$ manifests with oscillations [Fig. 4.7(a1)-(d1)]. An increase of feedback strength destabilizes the limit cycle into a torus [Fig. 4.7(b2)] and produces new frequencies in the power spectrum [Fig. 4.7(c2)].

One strong frequency component appears separated from f_{H1} by $\Delta f = 0.19$ GHz, which is a value close to the external-cavity frequency $f_{EC} = 1/\tau = 0.2$ GHz. As a result, this new time-scale signature is superimposed on the top of the previous ones and induces a slow undamped periodic modulation of both the ACF and DMI [Fig. 4.7(d2)-(e2)]. A further increase of feedback strength is followed by the appearance of numerous new frequencies that increases the attractor complexity [Fig. 4.7(b3)-(c3)]. Nevertheless, the strong frequency components still have the identical frequency locations, thus guarantee the persistence of a global order of the time series over the long term even if on a short time the complexity (disorder) is increased. This is manifested in the estimators by a strong modulation [Fig. 4.7(d3)-(e3)]. Finally, the torus destabilizes into a chaotic attractor, whose structure in the projected space retains a vestige of the torus geometry [Fig. 4.7(b4)]. The strong aperiodicity of ECSL's chaotic regime induces the progressive loss of correlation within the intensity time series, which appears with a damp modulated shape of the estimators (Fig. 4.7(d4)-(e4)).

In conclusion, from the study of this scenario, it appears that the behavior of the estimators (ACF,DMI) is strongly conditioned by the time scales that concentrate most of the spectral energy during the cascade of bifurcations until the appearance of chaos. In this particular scenario, these are the undamped relaxation-oscillation period $\tau_{H1} = 1/f_{H1} \approx \tau_{RO}$ born from the Hopf bifurcation (H1) and a frequency at $f_{H1} - \Delta f$ with $\Delta f = 0.19$ GHz. Interestingly, the time delay is given by $\tau \approx 1/\Delta f$. The presence of two strong frequency components will induce a beating in the estimators behavior. Fast oscillations are observed at the composite frequency $f_{H1} - \Delta f/2$ with a slow modulation at frequency $\Delta f/2$ (or period 2τ), responsible for the maximum of modulation at every multiple of τ. It is noteworthy to mention the typicality of such a scenario in ECSLs, when the time scales τ_{RO} and τ are sufficiently separated. It is also representative of what could be considered as a *weakly-secure regime* for an ECSL. Indeed, the time delay appears early in the dynamics after a torus bifurcation (in Figs. 4.3-4.7), while the ECSL is still predictable. The frequencies f_{H1} and $f_{H1} - \Delta f$ persist in the early stages of the chaotic dynamics at weak feedback strengths. As a consequence, a sufficient condition to conceal the time-delay signature relies on its absence in the early stages of the ECSL's dynamics

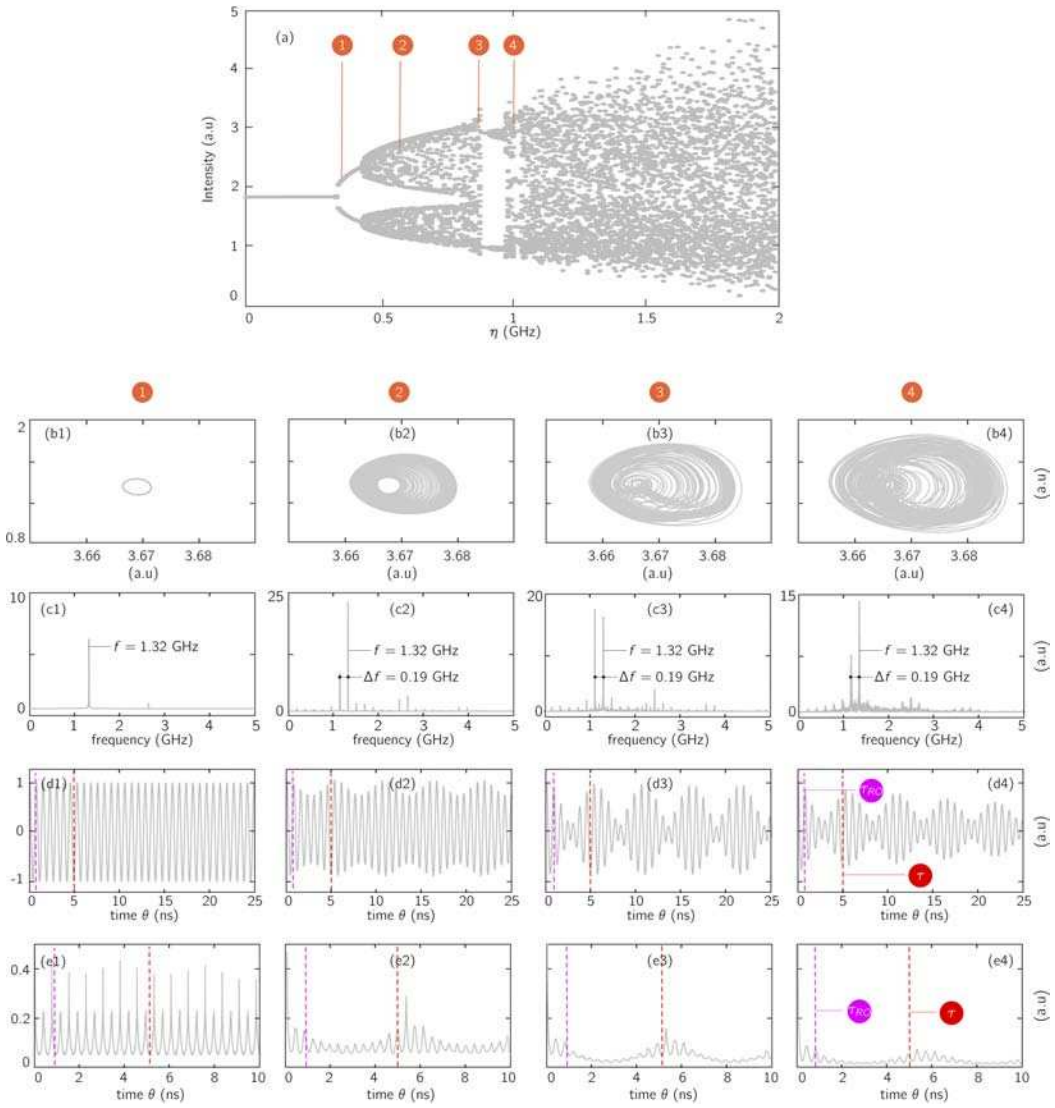

Figure 4.7: Dynamical interpretation of security in a case of disparate time scales. The time delay is $\tau = 5$ ns and $\tau_{RO} = 0.75$ ns (a) A quasiperiodic route to chaos is observed; a projection of the attractor in the $(|E|, N)$ plane (first row), power spectrum $|FT(I(t))|^2$ (second row), autocovariance (third row), and delayed mutual information (fourth row) for increasing value of the feedback rate. Each column (numbered from 1 to 4) corresponds to the feedback strengths $\eta = 0.35$ GHz, 0.55 GHz, 0.85 GHz, and 1 GHz, respectively. The vertical purple and red dashed lines give the time location of τ_{RO} and τ, respectively.

that will ensure in the weakly chaotic regime no information on the time delay. This is a situation encountered in many cases when the time scales τ_{RO} and τ are close to each other.

4.4.2 Interpretation of a Close Time-Scales Scenario

Similar to the previous section, the influence of the bifurcation cascade is investigated when the two time scales τ_{RO} and τ have close values. In this case, the analysis is performed using parameters identical to those in Fig. 4.5. The cascade of bifurcations is first analyzed in Fig. 4.8(a), and it shows a Period-Doubling route to chaos. Similar to what was observed in Fig. 4.7, we notice that the frequencies generated by the ECSL nonlinear dynamics also significantly influence the shape of the estimators. The progressive increasing in feedback strength leads to time-periodic dynamics of the ECSL [Fig. 4.8(b1)] with a frequency $f_{H1} = 1.34$ GHz [Fig. 4.8(c1)] and induces an oscillating behavior of the estimators [Fig. 4.8(d1)-(e1)]. At a larger feedback strength, a period-doubling bifurcation is observed and leads to the appearance of a new frequencies $f = f_{H1}/2$ [Fig. 4.8(c2)]. The coexistence of these two time scales modulates the shape of the estimators [Fig. 4.8(d2)-(e2)], making $2\tau_{H1} = 2/f_{H1}$ and its multiples the time-locations of the strongest contributions in the time-delay estimators. Further increase of the feedback strength η leads to the appearance of many frequencies in the ECSL's power spectrum, and has two effects on the estimators: a global amplitude's decrease, and an enhancement of the modulation [Fig. 4.8(d3)-(e3)]. Then, the appearance to many frequencies in the spectrum leads to a chaotic regime, which shows up as of exponentially damped oscillations at a frequency approximately equal to f_{H1} in both estimators [Fig. 4.8(d4)-(e4)].

In contrast to the previous case, the time delay does not appear early in the ECSL's dynamics after the occurrence of the first bifurcations nor in the power spectrum, which contains a single strong frequency component at approximately f_{H1}. This prevents a clear time-delay signature to appear in the estimators at low feedback rates. The only information given by the estimator is a measure of the undamped oscillation frequency f_{H1}, which in the case presented, is close to the relaxation-oscillation frequency $f_{RO} = 1/\tau_{RO}$.

4.4.3 Summary

In conclusion and based on the two scenarios illustrated in Figs. 4.7-4.8, the cascade of bifurcations plays a significant role in the behavior of the time-delay estimators. The first bifurcation usually leads to oscillations in the estimators at a fundamental frequency, and subsequent bifurcations shape them. The diversity of time-delay identification scenarios appearing at weak feedback strength is a direct consequence of the many existing route to chaos. Furthermore, it appears that a sufficient condition to conceal the time-delay signature is that it must not appear early in the route to chaos (as observed in Fig. 4.7(c2)). For an experienced eavesdropper, however, the information on the relaxation oscillations may still be of interest, especially if the emitter is guessed to be an ECSL. In many scenarios investigated, the oscillations in the estimator had always a period approximately equal to τ_{RO} and were related to the

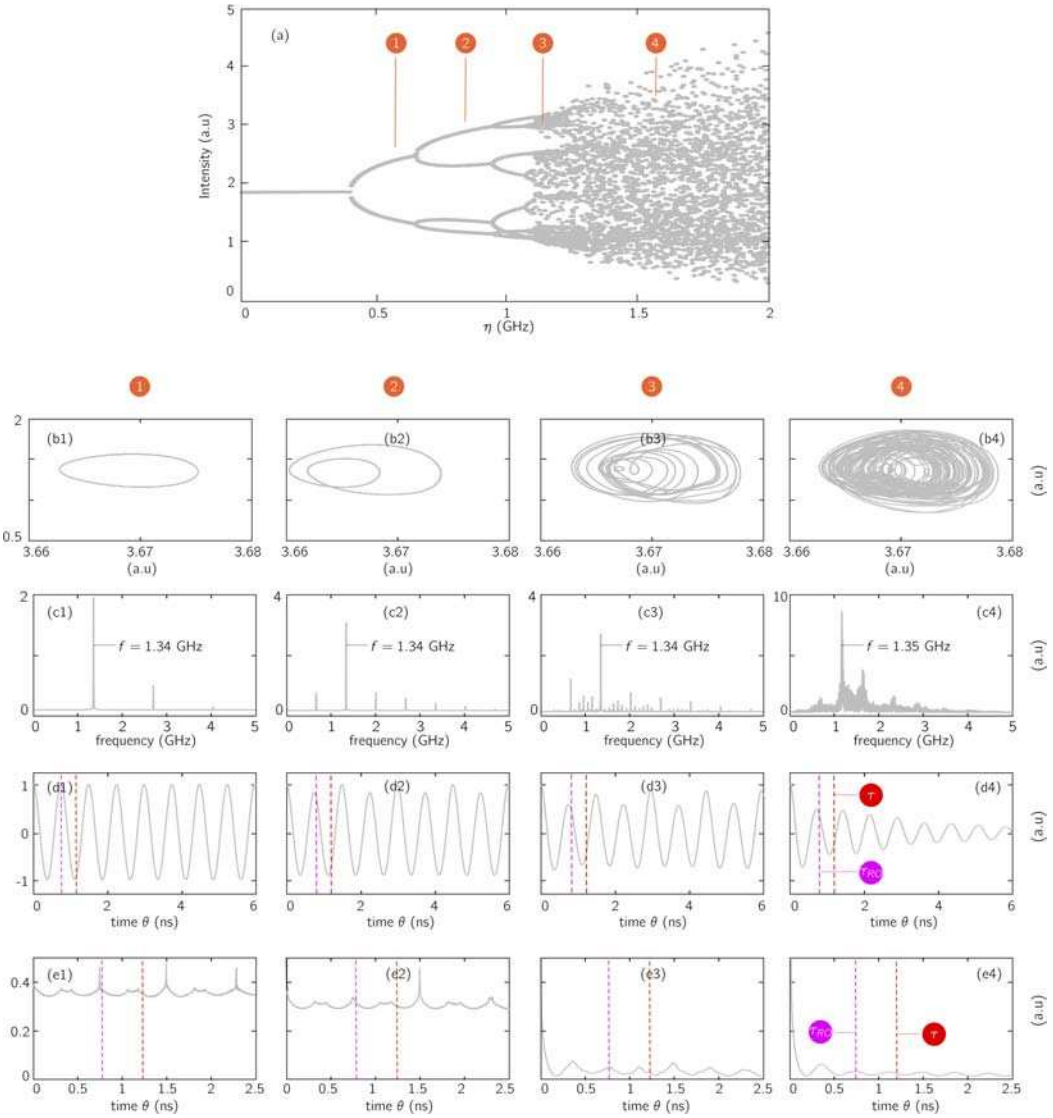

Figure 4.8: Dynamical interpretation of security in a case of close time scales. The time delay is $\tau = 1.2$ ns and $\tau_{RO} = 0.75$ ns (a) A period-doubling route to chaos is observed as well as a projection of the attractor in the $(|E|, N)$ plane (first row), power spectrum $|FT(I(t))|^2$ (second row), ACF (third row), and DMI (fourth row) for increasing value of the feedback rate. Each column (numbered from 1 to 4) corresponds to the feedback strengths $\eta = 0.6$ GHz, 0.8 GHz, 1.2 GHz, and 1.5 GHz, respectively. The vertical purple and red dashed lines give the time locations of τ_{RO} and τ, respectively.

frequencies with a strong concentration in spectral-energy density. Amongst them, the frequency emerging from the first Hopf bifurcation seems somehow preserved in the power spectrum during the entire route to chaos. This further motivates the study of its influence and role on the ECSL security.

4.4.4 Security and Frequency Concentrating a High Energy Level

In the previous illustrations, the time (or frequency) scale appearing on the first Hopf bifurcation τ_{H1} (or $f_{H1} = 1/\tau_{H1}$) remained dominant in the ECSL dynamics even when the system becomes chaotic, because it systematically concentrates a significant amount of spectral energy. Its presence seems to be responsible for the fast oscillating behavior of the time-delay estimators that persists during the entire cascade of bifurcations and can blur or even mask the time-delay signature (Figs. 4.7-4.8). The frequency f_{H1} also seems to be close to f_{RO}. However, a detailed study has shown that f_{H1} can be significantly shifted from f_{RO}. Figure 4.9 displays the evolution of f_{H1} as a function of τ (time delay) for a given value of τ_{RO}. The evolution is not monotonic; f_{H1} periodically oscillates around f_{RO} (horizontal purple dashed line). The period is close to τ_{RO}, and the oscillations' amplitudes are slowly damped. Similar conclusions have been obtained for other sets of parameters than those used in this manuscript in previous studies on ECSL dynamics [154; 155; 156]. In our context, this interesting property could be used to increase the ECSL's security. The use of frequency f_{H1} shifted from the relaxation-oscillation frequency could potentially lead to fast oscillating estimators to prevent an eavesdropper to gain insight on τ_{RO} or τ.

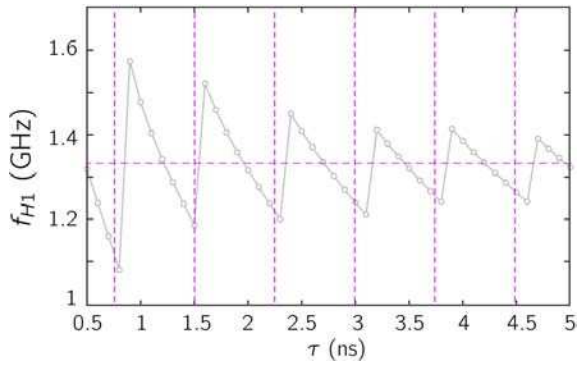

Figure 4.9: Evolution of the first Hopf frequency f_{H1} as a function of the time delay τ for $\tau_{RO} = 0.75$ ns. The horizontal and vertical dot-dashed lines represent, respectively, the relaxation oscillation frequency $f_{RO} = 1/\tau_{RO}$ and multiples of the relaxation-oscillation period τ_{RO}. The scenarios of Figs. 4.7 and 4.8 are indicated.

Our previous choice of parameters (in the disparate and close time-scales scenarios), as indicated in Fig. 4.9, coincidentally leads to situations where $f_{H1} \approx f_{RO}$. However, there are also situations, where the evolution of f_{H1} can be significantly shifted from f_{RO}, when τ and τ_{RO} are close (situation corresponding to optimized time-delay concealment). Using this particular feature, it would be possible to design an ECSL-based chaotic emitter with an ever greater security with no leakage of the time-delay and relaxation-oscillation information.

We have to be cautious in our conclusions: a strong shift of f_{H1} with respect to f_{RO} is a criterion that guarantees strong security only if f_{H1} concentrates most of the spectral energy until weakly-developed chaos is reached. This would result in estimators with oscillating signatures associated with $\tau_{H1} = 1/f_{H1}$. As a matter of fact, due to the extremely complicated behaviors of the Lang-Kobayashi equations, making such a prediction is extremely difficult. It is usually necessary to simulate the system to determine *a posteriori* the route to chaos and the corresponding level of security achieved by an ECSL-based emitter.

We illustrate this fact in Fig. 4.10. We consider for instance two close values for the time delay and the relaxation-oscillation period, respectively, taken equal to $\tau = 0.85$ ns and $\tau_{RO} = 0.75$ ns (a scenario where a strong level of security is achieved due to the proximity of the time scales). In this scenario, the route to chaos does not correspond to a standard route (QP or PD). The ECSL is destabilized through a Hopf bifurcation before it locks on a limit cycle with a frequency f_{H1b} and undergoing the cascade of bifurcations. Such a situation is illustrated in the bifurcation diagram in Fig. 4.10(a). After a first Hopf bifurcation, a limit cycle LC_1 is generated with frequency $f_{H1} = 1.64$ GHz shifted from $f_{RO} = 1.33$ GHz [Fig. 4.10(b1)-(c1)]. As the feedback strength is increased, LC_1 is replaced by two news branches associated with a new limit cycle LC_{1b} with a different frequency $f_{H1b} = 1.02$ GHz [Fig. 4.10(b2)-(c2)]. Then, LC_{1b} is destabilized with the ECSL locking on a PD limit cycle with fundamental frequency $f_{PD} = 0.88$ GHz (Fig. 4.10(b3)-(c3)). Finally, the system enters in a weakly developed chaotic regime that inherits the spectral contents of this last stable attractor (Fig. 4.10(b4)-(c4)). In this scenario, the ECSL has undergone discontinuous variations of its frequency that concentrates the largest amount of spectral energy. These variations have visible consequences on the estimators (Fig. 4.10(d1)-(d4) and (e1)-(e4)); the oscillatory shape is not related to any *a priori* known frequencies such as f_{RO}, f_{EC}, or f_{H1}. This particular route to chaos leads to nontrivial variations of the estimators such that it is virtually impossible to identify the time delay or the relaxation-oscillation period from either the ACF or DMI [Fig. 4.10(d4) and (e4)].

In conclusion, we have shown that the frequencies that appears in the cascade of bifurcations and concentrates most of the spectral energy are responsible for the oscillatory behavior observed in the weakly chaotic regimes. In numerous situations, the frequency f_{H1} of the first Hopf bifurcation controls these oscillations. It appears they can be made to be frequency shifted with respect to the relaxation-oscillation frequency f_{RO} and therefore enhance the security of an ECSL-based chaotic emitter by hiding its key information. Nevertheless, it is not systematically responsible for the fast oscillatory shape of the estimators as suggested by the last scenario investigated. Various frequencies arise from the cascade of bifurcations occurring in the ECSL, shape, and modify the oscillations in the time-delay estimators. They are in every cases responsible for blurring the time-delay signature when the feedback rate is taken relatively weak and the ECSL weakly chaotic. Finally, the diversity of routes to chaos also explains why there are so many differences in the behaviors of the estimators at weak feedback strength (where the influence of the route is still significant) by opposition to the strong feedback regime, where the estimators' behaviors are predictable.

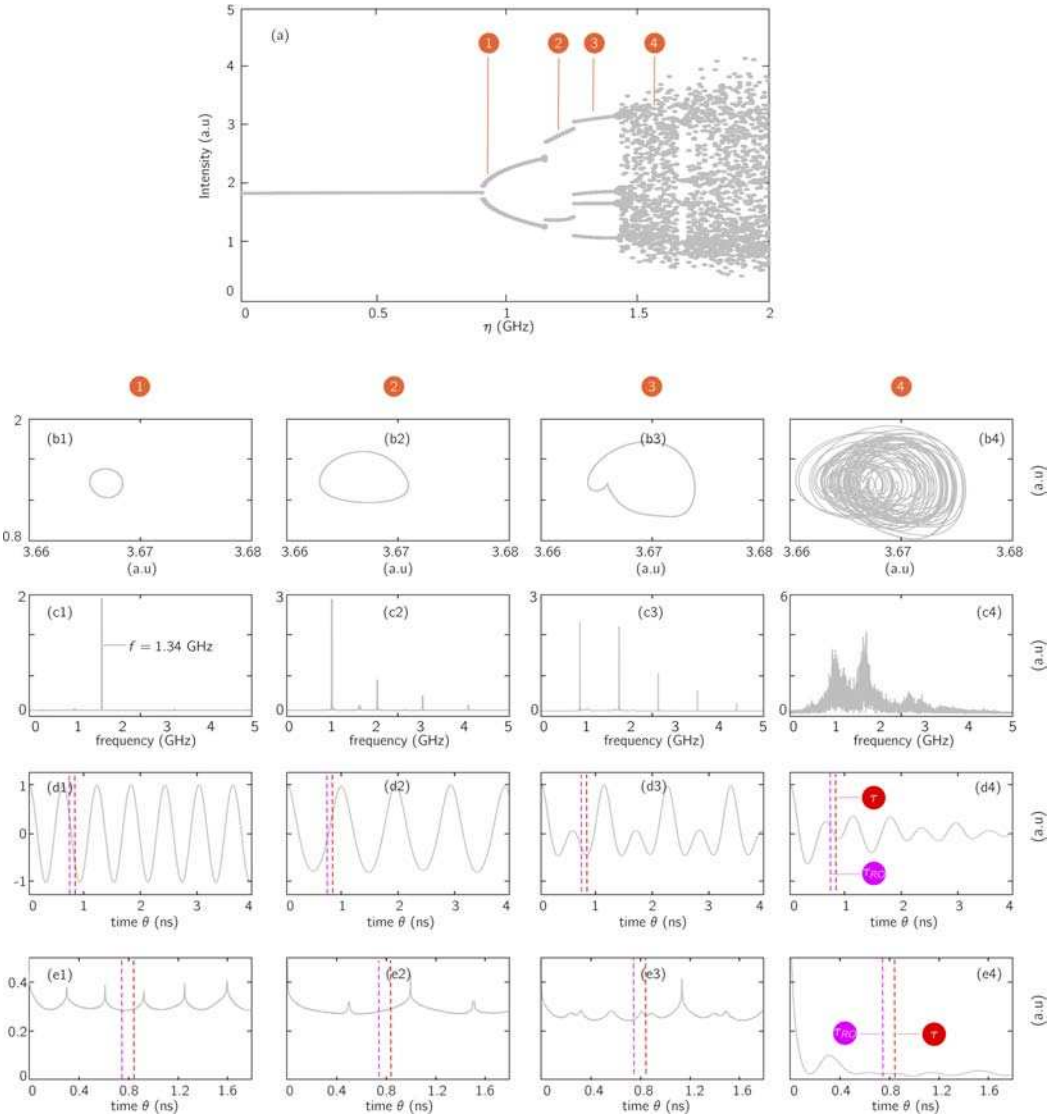

Figure 4.10: Dynamical interpretation of security in a case of close time scales, not controlled by the first Hopf bifurcation frequency f_{H1}. The time delay is $\tau = 0.85$ ns and $\tau_{RO} = 0.75$ ns (a) A nontrivial route to chaos is observed. Projection of the attractor in the $(|E|, N)$ plane (first row), power spectrum $|FT(I(t))|^2$ (second row), ACF (third row), and DMI (fourth row) for increasing value of the feedback rate. Each column (numbered from 1 to 4) corresponds to the feedback strengths $\eta = 0.6$ GHz, 0.8 GHz, 1.2 GHz, and 1.5 GHz, respectively. The vertical purple and red dashed lines give the time locations of τ_{RO} and τ, respectively.

4.5 Influence of Internal Parameters: Gain Saturation and Noise

In this section, we discuss the potential influence of two internal laser's parameters (spontaneous emission noise and gain compression coefficient), easily understood in the framework we have developed. In this context, we will analyze results on security and how some of the dynamical interpretations hold in this particular context.

4.5.1 Influence of the Spontaneous-Emission Noise

The results of the previous sections are based on a fully deterministic model of the ECSL. However, the stochastic processes modelled by the Langevin force appearing in Eqs. 4.1-4.2 may affect our results. Indeed, this additional stochastic part of the Lang-Kobayashi equations blurs the cascade of bifurcations that has already proven to be directly responsible for the concealed time-delay signatures observed in the time-delay estimators. When the feedback strength is weak, the noise acts as a major driving force for the dynamics that weakly excites the intrinsic nonlinearity of the ECSL. This stochastic excitation, however, does not influence the time-delay identification; the signature is still blurred by the time-scales related to the cascade of bifurcations. Larger feedback strength values make the noise effect negligible in comparison with the delayed-feedback term and a clear signature with an impulsional shape is observed, similar to the noiseless case. Figure 4.11 shows this result using the ACF, which is comparable to the third column of Fig. 4.3.

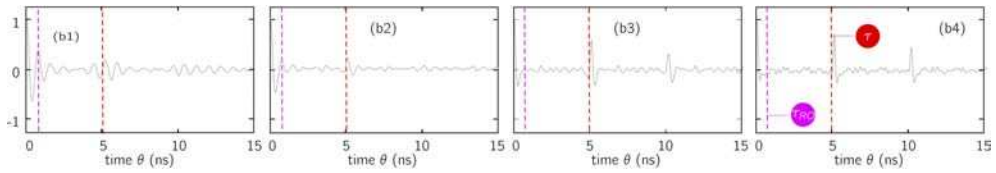

Figure 4.11: Influence of the rate of spontaneous emission β on the time-delay identification. The spontaneous emission rate is taken equal to $\beta = 10^{-3}$ s^{-1}. Each column is associated with a given feedback strength. From left to right, $\eta = 2.5$ GHz, 5 GHz, 10 GHz, and 15 GHz. The time delay and the relaxation period are equal to $\tau = 5$ ns and $\tau_{RO} = 0.75$ ns. They are represented by the purple and red dashed lines, respectively.

In conclusion, the presence of noise does not threaten or enhance significantly the security of the ECSL in terms of time-delay identification.

4.5.2 Influence of Gain Saturation

Gain saturation ε is phenomenologically introduced in the rate equations by considering an explicit intensity dependence of the gain. Since it modifies significantly the ECSL's nonlinearity, it may significantly affect security in terms of time-delay estimation.

It has already been reported that the saturation gain has a stabilizing effect on the ECSL dynamics [157]. As a consequence, reducing the value of ε will favor the driving action of $G_{N,|E|^2}E(t)$ relative to the feedback term $\eta e^{i\omega_0\tau}E(t-\tau)$. In terms

of time-delay identification, the consequences would be a persistence at larger feedback strength of the competition between the time scales generated by the cascade of bifurcations with the time delay, thus increasing the range for which an ECSL exhibits a high level of security. Figure 4.12 presents these results; two different identification scenarios based on the ACF are considered for various choices of τ_{RO} and τ for increasing values of the saturation gain ε. The first row shows simulations with close time scales ($\tau_{RO} = 0.2$ ns and $\tau = 1$ ns). For $\eta = 10$ GHz and a strong saturation gain ε, a clear time-delay signature is observed, as expected [Fig. 4.12(a4)]. A progressive disappearance of the time-delay signature at this feedback level, however, was not expected and yet it is observed, as the saturation gain is weakened (Fig. 4.12(a3)-(a2)-(a1)). These results hold also in a disparate time-scale scenario described above (second row of Fig. 4.12); the slow modulation at a period close to 2τ is also progressively weakened, thus increasing security even in a disparate time-scale scenario.

In conclusion, decreasing values of the gain saturation favor the fast time scales emerging from the laser's intrinsic nonlinearities with respect to the delay time scale. This has also proven to enhance the range of feedback rate and separation of time-scales to conceal the time delay.

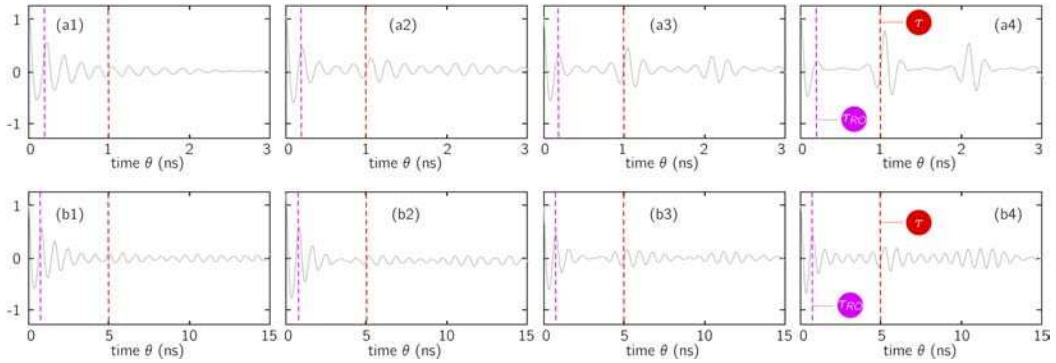

Figure 4.12: Influence of the gain saturation ε on the time delay signature for two different scenarios. The first row corresponds to a (relatively) close time-scale scenario with $\tau_{RO} = 0.2$ ns and $\tau = 1$ ns at $\eta = 10$ GHz. The second row is a disparate time-scale scenario with $\tau_{RO} = 0.75$ ns and $\tau = 1$ ns. The vertical purple and red dashed lines represent the relaxation oscillation period and the time delay, respectively. Each column corresponds to a increasing values of the saturation gain. From left to right : $\varepsilon = 0$ m^3, 0.625 m^3, 1.25 m^3, and 2.5 m^3. The purple and red vertical dashed lines gives the locations of the relaxation oscillation period and time delay, respectively.

4.6 Conclusion

In this chapter, we have analyzed the security of an ECSL in terms of time-delay identification using typical time-delay estimators (ACF and DMI). The key role of the feedback strength η, the pumping current J, as well as the choice of the time-delay τ relative to the relaxation-oscillation period τ_{RO}, has been underlined. It appears that the maximum of security, corresponding to the loss of time-delay signature, occurs

for moderate feedback strength and pumping current combined with close values of the two time-scales τ and τ_{RO}. The efficiency of the time-delay concealment finds its origin in the specific nonlinear dynamics and time scales generated in the ECSL's bifurcation cascade preceding chaos. Indeed, chaos is reminiscent of the time scales involved in the early stage of the laser dynamics, such as the undamped relaxation oscillation time and possibly PD and QP dynamics. The time-delay estimators exhibit complex modulated shapes showing these different ECSL dynamics time scales. In case the time delay τ and the relaxation oscillation period τ_{RO} are close to each other, the time-delay information is efficiently concealed thanks to a shift of the first Hopf frequency f_{H1} with respect to the relaxation oscillation frequency f_{RO}. The laser output at the Hopf frequency starts pulsing at a frequency that is neither close to $f_{RO} = 1/\tau_{RO}$ nor $f = 1/\tau$. We have also found that a suitable choice of internal parameters could lead to wider regions of operational parameter values that ensure security. It appears that the decrease in gain saturation coefficient allows to use more distant values of τ and τ_{RO} and to increase the pumping factor while maintaining time-delay concealment. The robustness of our results has been checked with other signal processing techniques such as neural networks and filling-factor methods. We expect our results to be of interest to design an optical chaotic emitter with optimal concealment of its most critical parameters, hence also improving security in optical chaos-based communications.

Chapter 5

Multiplexing Chaotic Light

Abstract

We theoretically analyze the possibility of multiplexing multiple chaotic optical fields with a strong spectral overlap. Instead of considering regular wavelength-division multiplexing (WDM) or time-division multiplexing (TDM) approaches on top of chaotic systems, we propose a radically different perspective relying on one of the fundamental concepts of the theory of synchronization, which is the active passive decomposition (APD). We numerically show that the combination of mutually coupled lasers at the emitter with a unidirectional injection into decoupled receivers can be used to multiplex and demultiplex chaotic optical fields. The separation is realized through complete chaos synchronization by each receiver, even when the various free-running lasers operate at identical frequencies. This offers new perspectives in high spectral efficiency and multiplexed transmission of information. We also demonstrate theoretically the possibility of encrypting and decrypting multiple data streams, when they are properly embedded in the phase or the amplitude of the various multiplexed optical fields.

This chapter is based on the following publication:

- D. Rontani, A. Locquet, M. Sciamanna and D.S. Citrin,"Spectrally Efficient Multiplexing of Chaotic Light", *Opt. Lett.* **35**, pp. 2016-2018 (2010)

5.1 Introduction

In this chapter, we aim at presenting an alternative view of the problem of multiplexing chaotic light fields generated by optoelectronic devices such as edge-emitting lasers (EEL). When more than two lasers are involved with a single available optical channel, it is necessary to multiplex the chaotic signals of the various users. In conventional optical communications, time- and wavelength-division multiplexing (TDM and WDM) are well-known protocols that make use of different time slots and wavelength bands, respectively, to convey each user's signal. In each case, either a given user has access to the whole channel bandwidth but only during specific time intervals (TDM) or has permanent access to a frequency slot (WDM).

Applying WDM to optical chaotic communications has already been proposed. This is commonly referred to as *chaotic WDM* in the literature and can be achieved using either multiple chaotic single-mode lasers operating at detuned wavelengths [158; 159] or multi-mode lasers [160; 161; 162]. In both cases, the lasers at the receiving end synchronize their chaotic fluctuations with those of the same-frequency emitter. Though interesting, chaotic WDM has the disadvantage of requiring a large frequency separation between channels to avoid interference between each user's wide spectrum [163], or in other words, a high degree of synchronization between the respective emitter/receiver pairs. Consequently, chaotic WDM is far less spectrally efficient than conventional WDM, thus obviating its practical deployment. Although it has not been studied in the context of optical chaos-based communications, the application of the other typical multiplexing approach, TDM, would not lead to any improvement of the spectral efficiency.

Other than the spectral inefficiency of such approaches, one of the main concerns was to find how to exploit in the best possible way the specificity of chaotic optoelectronic devices and go beyond the classical paradigms of WDM or TDM. This has led us to an analogue of the code-division multiple access (CDMA) approach, where discrimination between users' signals is made at a statistical level. As will be later illustrated, this separation is performed through the independent chaos synchronization of the various emitter/receiver pairs.

To help understand our approach, we first reinterpret the classical paradigm of unidirectional synchronization of chaotic EELs in the theoretical framework of active-passive decomposition (APD).

5.2 Optical-Chaos Synchronization Revisited

In this section, we show the close analogy that exists between APD, as established by Kocarev *et al.* in [70], and the classical problem of unidirectional synchronization of chaotic EELs [59; 121]. We first introduce the concept of APD, and then we show to what extent the result holds for a configuration involving EELs.

5.2.1 Active Passive Decomposition (APD)

Historically, APD is a generalization of the *master-slave decomposition* (MSD) introduced by Pecora and Carroll in [7]. Here, we recall this important milestone by

considering two systems: the emitter (E) and the receiver (R) with identical structures and parameters. These systems are described by their respective state variables $\mathbf{x}_E \in \mathbb{R}^n$ and $\mathbf{x}_R \in \mathbb{R}^n$; their dynamics are controlled by ODEs. Then, each system is decomposed into two interconnected subsystems, (E_m,E_s) and (R_m,R_s), as illustrated in Fig. 5.1(a); the subscripts m and s denote master and slave, respectively.

The state variables are also decomposed into $\mathbf{x}_j = (\mathbf{x}_{j_m}, \mathbf{x}_{j_s})^T$ with $j = E, R$. The dynamical representation of such system reads

$$(\mathrm{E,R}) \begin{cases} \dot{\mathbf{x}}_{j_m} = f_{j_m}(\mathbf{x}_{j_m}, \mathbf{x}_{j_s}) \\ \dot{\mathbf{x}}_{j_s} = f_{j_s}(\mathbf{x}_{j_m}, \mathbf{x}_{j_s}) \end{cases}. \tag{5.1}$$

To completely synchronize both E and R, a subsystem R_m identical to E_m is constructed [see Fig. 5.1(b)], upon which Eq. 5.1 becomes

$$(\mathrm{E}) \begin{cases} \dot{\mathbf{x}}_{E_m} = f_{E_m}(\mathbf{x}_{E_m}, \mathbf{x}_{E_s}) \\ \dot{\mathbf{x}}_{E_s} = f_{E_s}(\mathbf{x}_{E_m}, \mathbf{x}_{E_s}) \end{cases}, \text{ and } (\mathrm{R}) \begin{cases} \dot{\mathbf{x}}_{R_m} = f_{R_m}(\mathbf{x}_{E_m}, \mathbf{x}_{R_s}) \\ \dot{\mathbf{x}}_{R_s} = f_{R_s}(\mathbf{x}_{E_m}, \mathbf{x}_{R_s}) \end{cases}. \tag{5.2}$$

The subsystems E_s and R_s are synchronized, if and only if the equilibrium points of E_m and R_m are stable. In other words, the Lyapunov exponents of subsystem R_s conditioned to the trajectories of subsystem E_m have to be negative [7]. However, this method makes chaos synchronization possible only if MSD exists, where one subsystem has stable fixed points. This consequently limits the application of such a decomposition to a reduced number of chaotic systems. Furthermore, the number of possible MSD per system is limited.

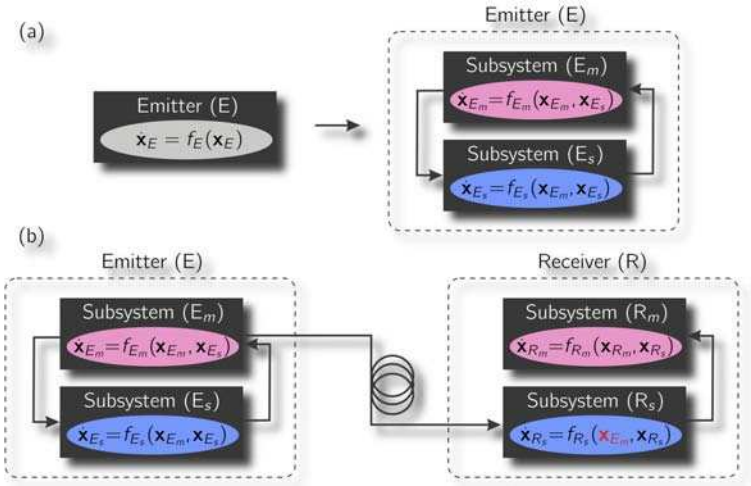

Figure 5.1: Illustration of the concept of master-slave decomposition (MSD) of (a) a single nonlinear system (E) into two interconnected subsystems (E_m,E_s) and of (b) two systems (E) and (R) potentially to ensure chaos synchronization.

As proposed by Kocarev *et al.* in [70], APD is a generalization of the MSD framework. Emitter E, which is usually in its autonomous form, is rewritten into a non-autonomous form[1] as

$$\dot{\mathbf{x}}_E = f(\mathbf{x}_E, s(t)), \tag{5.3}$$

[1]See Chapter 2 for the definitions of autonomous and non-autonomous forms.

with $s(t) = h(\mathbf{x}_E)$ (or $\dot{s}(t) = h(\mathbf{x}_E, s(t))$), $f : \mathbb{R}^n \times \mathbb{R}^p \to \mathbb{R}^n$, and $h : \mathbb{R}^n \to \mathbb{R}^p$ (or $\mathbb{R}^n \times \mathbb{R}^p \to \mathbb{R}^p$ if $s(t)$ is described by a differential equation).

If receiver R is built with an identical structure to that of emitter E and coupled with the same signal $s(t)$, its non-autonomous form reads

$$\dot{\mathbf{x}}_R = f(\mathbf{x}_R, s(t)). \tag{5.4}$$

It is possible for E and R to be synchronized; the conditional Lyapunov exponents of Eq. 5.3 have to be negative (whatever the driving signal $s(t)$ is). This also means that when E is not driven ($s(t) = 0$), it will tend to a stable equilibrium point. In other words, E is a damped or *passive* oscillator. This explains the APD appellation; the system is decomposed into its passive and *active* driving parts through the nonlinear functions f and h. A graphical representation of APD is given in Fig. 5.2.

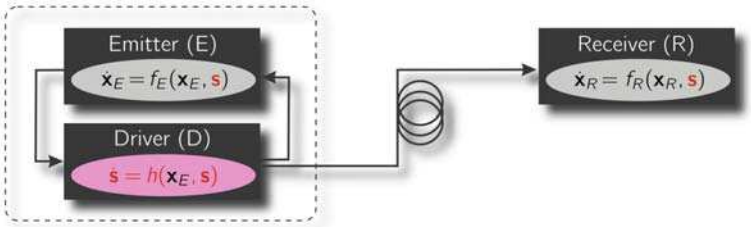

Figure 5.2: Illustration of the concept of active-passive decomposition (APD), where a Driver (D) injects emitter E and receiver R. They may under certain conditions chaotically synchronize.

5.2.2 Application to the Synchronization of Chaotic Lasers

The synchronization of chaotic EELs has been thoroughly investigated in the literature [59; 121], with details under which conditions it can be achieved. Amongst the many existing optical configurations of EELs used to exhibit chaos (see Chapter 3), the ECSL has proven to be of particular interest. It injects coherently and unidirectionally a receiver laser as depicted in Fig. 5.3. Each device can be modelled within the framework of the well known Lang-Kobayashi equations [94]. With similar notation to that used in Chapter 3, one has

$$\frac{dE_m}{dt} = \frac{1}{2}(1+i\alpha)\left(G_{N_m,E_m} - \frac{1}{\tau_p}\right)E_m + \eta_m e^{-i\omega_{0m}\tau}E_m(t-\tau), \tag{5.5}$$

$$\frac{dE_s}{dt} = \frac{1}{2}(1+i\alpha)\left(G_{N_s,E_s} - \frac{1}{\tau_p}\right)E_s + \eta_c e^{-i\omega_{0m}\tau_c}E_m(t-\tau_c), \tag{5.6}$$

$$\frac{dN_{m,s}}{dt} = J - \gamma_s N_{m,s} - G_{N_{m,s},E_{m,s}}\left|E_{m,s}\right|^2, \tag{5.7}$$

with index (m, s) referring to as master (or emitter) and slave (or receiver), respectively. The lasers used in this setup are class-B, which means that in the absence of an additional degree of freedom such as an external feedback they exhibit damped relaxed oscillations before emitting a stable constant output. An EEL is therefore *passive*, and in the proposed configuration of Fig. 5.3, the feedback term is considered

as the driving signal or the active part. By symbolically rearranging Eqs. 5.5-5.7, the model reads

$$\dot{E}_m = f_E\left(E_m, N_m, \eta_m e^{-i\omega_{0m}\tau} E_m(t-\tau)\right), \tag{5.8}$$

$$\dot{E}_s = f_E\left(E_s, N_s, \eta_c e^{-i\omega_{0m}\tau_c} E_m(t-\tau_c)\right), \tag{5.9}$$

$$\dot{N}_{m,s} = f_N\left(E_{m,s}, N_{m,s}\right). \tag{5.10}$$

Rigorously, master and slave lasers can be synchronized if they are physical twins[1] driven by identical signals. In our configuration, however, the time delays (τ and τ_c) are different in the general case. This issue can be simply solved by rewriting the equations of the master and slave lasers in shifted time frames: $t \to t - \tau_c$ and $t \to t-\tau$, respectively. The two feedback signals now read $\eta_m e^{-i\omega_{0m}\Delta\tau} E_m(t-\Delta\tau)$ and $\eta_c e^{-i\omega_{0m}\Delta\tau} E_m(t-\Delta\tau)$ with $\Delta\tau = \tau_c - \tau$. Consequently, for the two driving signals to be equal and to ensure complete synchronization, one has necessary to satisfy $\eta_c = \eta_m$, which is known as the necessary conditions of anticipating synchronization [121]. Therefore, the synchronization manifold reads[2]

$$E_s(t) = E_m(t-\Delta\tau), \tag{5.11}$$

$$\varphi_s(t) = \varphi_m(t-\Delta\tau) - \omega_{0m}\Delta\tau \bmod(2\pi), \tag{5.12}$$

$$N_s(t) = N_m(t-\Delta\tau). \tag{5.13}$$

The unidirectional coupling configuration is described in Fig. 5.3.

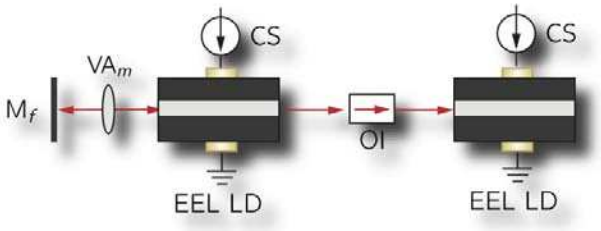

Figure 5.3: Illustration of an active-passive decomposition (APD) realized with a single pair of semiconductor laser. The master's optical field is used to drive both the master and the slave. EEL LD: Edge-emitting laser diode, CS: current source, OI: optical isolator, M$_f$: mirror, VA$_m$, VA$_c$: variable attenuator.

APD constitutes a powerful framework to investigate this classical synchronization problem. However, it only provides structural information about the nature of the driving signal, but not on the coupling values (sufficient conditions). Therefore APD, like other typical methods to determine synchronization conditions, gives necessary conditions for synchronization. Identifying synchronization of chaotic ECSLs as an APD-like problem (for the first time to the best of our knowledge) is a first important step before realizing the multiplexing of chaotic optical signals, as described in the next section.

[1] It is important to avoid parameter mismatch and noise to guarantee complete chaos synchronization.

[2] The additional term $\omega_{0m}\Delta\tau$ is a direct consequence of the time-reference shifts.

5.3 Optical Chaos Multiplexing

5.3.1 Model

In this section, we propose a new method to multiplex various chaotic optical signals produced by semiconductor lasers with identical free-running optical frequencies. Hitherto, optical-chaos multiplexing and demultiplexing techniques proposed in the literature have used lasers with different free-running frequencies [158; 163; 164], similar to the conventional WDM. In our approach, we propose to go further than this classical paradigm and make the multiplexing and demultiplexing possible using only the properties of chaos synchronization with lasers operating at identical free-running frequencies. Using simple optical components, we create a delayed optical analogy of APD. On the emitting side, a single signal $E_T(t)$ resulting from the mixing of chaotic electromagnetic fields $E_k^m(t)$ produced by multiple semiconductor lasers M_k $(k = 1, \ldots, n)$ being globally mutually coupled, is retro-injected with different feedback strengths and time-delays in each master laser M_i. Consequently, signal $E_T(t)$ is perceived by each master as a specific multiplexed signal $E_{T,k}^m(t)$. The signal $E_T(t)$ is then coherently and unidirectionally transmitted on an optical channel. On the receiving side, there are n independent semiconductor lasers S_k $(k = 1, \ldots, n)$ which operate under exactly the same conditions as the respective M_k. More specifically, they are injected with identical strength and the time-delay topologies are preserved. This implies that each slave S_k is injected by a delayed version of $E_{T,k}^m(t)$, namely $E_{T,k}^s(t)$.

Figure 5.4 shows a two-user setup composed of two mutually coupled master lasers (M_1,M_2) unidirectionally coupled with two slave lasers (S_1,S_2). Each master is subjected to delayed optical feedback from mirror Mr_f and to delayed optical injection from the other master. A linear combination of the two masters' delayed complex optical fields is thus injected into each master, but with specific strength (different variable attenuators), phase, and delay (different optical paths) for each field. The same linear combinations are then optically injected, after propagation on a shared optical channel, into the uncoupled slave semiconductor lasers S_1 and S_2.

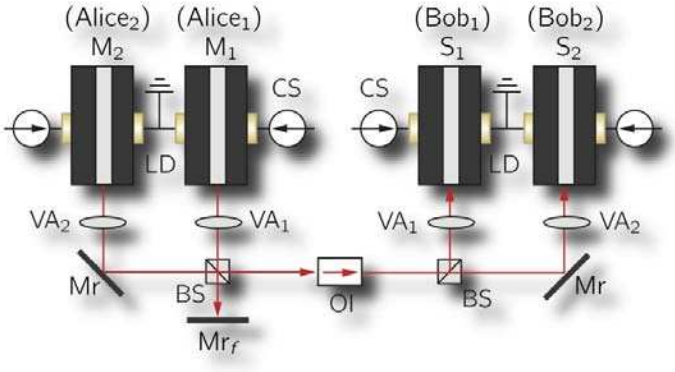

Figure 5.4: Multiplexing scheme based on semiconductor lasers optically-coupled in an APD fashion. LD: laser diode (labeled M_1, M_2 for the masters and S_1, S_2 for the slaves), CS: current source, Mr, Mr_f: mirrors, VA_1,VA_2: variable attenuators, BS: 50/50 beam splitter, OI: optical isolator.

The complete system is modeled assuming single-mode semiconductor lasers and the theoretical framework of Lang-Kobayashi [94]. The system of equations reads

$$\frac{dE_k^m}{dt} = \frac{1}{2}(1+i\alpha_k^m)\,G_k^m E_k^m + F_k^m + \sum_{j=1}^{n} \eta_{jk}^m e^{-i\omega_{0j}^m \tau_{jk}^m + i\Delta\omega_{jk}^{m/m} t} E_j^m\left(t-\tau_{jk}^m\right), \quad (5.14)$$

$$\frac{dN_k^m}{dt} = J_k^m - \gamma_{sk}^m N_k^m - (G_k^m + 1/\tau_{pk}^m)|E_k^m|^2, \quad (5.15)$$

$$\frac{dE_k^s}{dt} = \frac{1}{2}(1+i\alpha_k^s)\,G_k^s E_k^s + F_k^s + \sum_{j=1}^{n} \eta_{jk}^c e^{-i\omega_{0j}^s \tau_{jk}^c + i\Delta\omega_{jk}^{m/s} t} E_j^m\left(t-\tau_{jk}^c\right), \quad (5.16)$$

$$\frac{dN_k^s}{dt} = J_k^s - \gamma_{sk}^s N_k^s - (G_k^s + 1/\tau_{pk}^s)|E_k^s|^2, \quad (5.17)$$

where the subscript k denotes the kth lasers pair ($\mathrm{M}_k/\mathrm{S}_k$) and subscripts m, s denote master or slave variables, respectively. $E_k^{m,s} = |E_k^{m,s}|e^{i\phi_k^{m,s}}$ is the slowly-varying complex electric field and $N_k^{m,s}$ the carrier number. $G_k^{m,s} = g_k^{m,s}(N_k^{m,s} - N_{0k}^{m,s})/(1+\varepsilon_k^{m,s}|E_k^{m,s}|^2) - 1/\tau_{pk}^{m,s}$ is the nonlinear gain with $g_k^{m,s}$ the differential gain, $N_{0k}^{m,s}$ the carrier number at transparency, $\varepsilon_k^{m,s}$ the gain-saturation coefficient, and τ_{pk} the photon lifetime. $\alpha_k^{m,s}$ is the linewidth enhancement factor, $\gamma_{sk}^{m,s}$ the carrier decay rate, $J_k^{m,s}$ the pumping current density, and $\omega_{0k}^{m,s}$ the free-running laser frequency of the kth free running laser. τ_{jk}^m (τ_{jk}^c), η_{jk}^m (η_{jk}^c), and $\Delta\omega_{jk}^{m/m} = \omega_{0j}^m - \omega_{0k}^m$ ($\Delta\omega_{jk}^{m/s} = \omega_{0j}^m - \omega_{0k}^s$) are the flight time, injection strength, and detuning between the j-th and the k-th master laser (the jth master laser and the kth slave laser). Spontaneous-emission noise is modeled by Langevin sources $F_k^{m,s} = \sqrt{2\beta_k^{m,s} N_k^{m,s}}\zeta_k^{m,s}$ with β_{sp} the spontaneous-emission rate and $\zeta_k^{m,s}$ independent Gaussian white noises with unit variance.

5.3.2 Necessary Conditions for Synchronization

Assuming identical perfectly reflecting mirrors and identical optical coupling efficiencies in all laser cavities, the geometry of the system in Fig. 5.4 leads to the following relations between flight times and coupling strengths

$$\tau_{jk}^m = \tau_{kj}^m = \tau_{jj}^m + \Delta\tau_{kj}^m/2, \quad (5.18)$$

$$\eta_{kj}^m = \eta_{jk}^m = \sqrt{\eta_{kk}^m \eta_{jj}^m}, \quad (5.19)$$

with $\Delta\tau_{jk}^m = -\Delta\tau_{kj}^m = \tau_{jj}^m - \tau_{kk}^m$.

The scheme has been devised in such a way that each laser in a pair (master or slave) is subjected to n master electric fields, E_k^m ($k = 1, \ldots, n$), with the same relative time shift. Mathematically, this means that $\tau_{jj}^m - \tau_{kj}^m = \tau_{jj}^c - \tau_{kj}^c$.

Interestingly, due to the coupling strength and geometry, each laser pair (M_k,S_k) perceives its own multiplexed signal $E_{T,k}^{m,s}(t)$ derived from a unique mathematical multiplexed chaotic optical field that reads

$$E_T(t,\theta,\sigma,\mu) = \sum_{j=1}^{n} \sqrt{\eta_{jj}^m} e^{i\omega_{0j}^m(\theta+\Delta\tau_{\sigma j}^m/2) + it\Delta\omega_{j\sigma}^{\mu}} E_j^m(t-\theta-\Delta\tau_{\sigma j}^m/2), \quad (5.20)$$

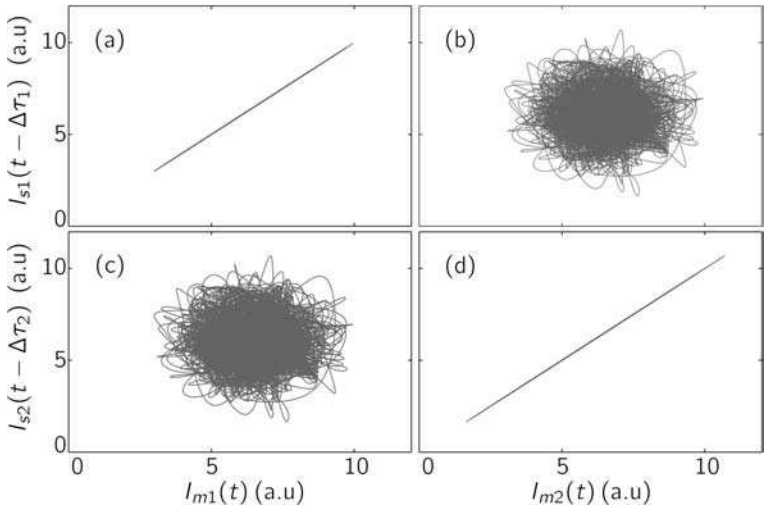

Figure 5.5: Theoretical synchronization diagrams without spontaneous-emission noise ($\beta_{sp} = 0$ s^{-1}). The synchronization diagrams present the evolutions of $(I_1^m(t), I_1^s(t-\Delta\tau_1))$ in (a), $(I_2^m(t), I_1^s(t-\Delta\tau_1))$ in (b), $(I_1^m(t), I_2^s(t-\Delta\tau_2))$ in (c), and $(I_2^m(t), I_2^s(t-\Delta\tau_2))$ in (d). The numerical values are $J_1^m = J_1^s = 2.75J_{th}$, $J_2^m = J_2^s = 2.5J_{th}$, and $\eta_{11}^m = \eta_{11}^c = 10$ GHz, $\eta_{22}^m = \eta_{22}^c = 15$ GHz, $\eta_{12}^m = \eta_{21}^m = \eta_{12}^c = \eta_{21}^c = \sqrt{\eta_1^m \eta_2^m}$, and $\tau_{11}^m = 1$ ns, $\tau_{22}^m = 4$ ns, $\tau_{11}^c = 1$ ns and $\tau_{22}^c = 4$ ns. The internal parameters are taken different for each pair : $\alpha_1^{m,s} = 5$, $\alpha_2^{m,s} = 4$, $\tau_{p1}^{m,s} = 2$ ps, $\tau_{p2}^{m,s} = 1$ ps, $\gamma_{s1}^{m,s} = 2$ ns, $\gamma_{s2}^{m,s} = 1$ ns, $\varepsilon_1^{m,s} = 5 \times 10^{-7}$, $\varepsilon_2^{m,s} = 2.5 \times 10^{-7}$, $g_1^{m,s} = 1.5 \times 10^{-4}$ s^{-1}, $g_2^{m,s} = 1 \times 10^{-4}$ s^{-1}, $N_{01}^{m,s} = 1.5 \times 10^8$, $N_{02}^{m,s} = 2 \times 10^8$.

with $\theta = \tau_{kk}^m$ or τ_{kk}^c and $\mu = m/m$ or m/s. This optical field $E_T(t)$ can be used to derive the expression of the multiplexed field injected into the kth laser pair; M_k is injected by $E_{T,k}^m(t) = \sqrt{\eta_{kk}^m} E_T(t, \tau_{kk}^m, k, m/m)$ and S_k by $E_{T,k}^s(t) = \sqrt{\eta_{kk}^c} E_T(t, \tau_{kk}^c, k, m/s)$.

Each pair (M_k,S_k) can exhibit a regime of complete synchronization in the presence of identical internal parameters, and bias current, and in the absence of noise, and frequency detuning $\Delta\omega_{kk}^{m/s} = 0$. These necessary conditions are completed by the following injection-strength constraint $\eta_{jk}^m = \eta_{jk}^c$ (equivalent to $\eta_{kk}^m = \eta_{kk}^c$ with respect to the geometry adopted in our setup) which naturally extends the single master/slave case [59; 121; 122; 123]. Moreover, non-zero flight times are responsible for specific time lags $\Delta\tau_k$ in the synchronization manifold of $\mathrm{M}_k/\mathrm{S}_k$ defined by

$$E_k^s(t) = E_k^m(t - \Delta\tau_k), \tag{5.21}$$

$$\phi_k^s(t) = \phi_k^m(t - \Delta\tau_k) - \omega_{0k}^m \Delta\tau_k (\mathrm{mod}\ 2\pi), \tag{5.22}$$

$$N_k^s = N_k^m(t - \Delta\tau_k). \tag{5.23}$$

The expression of the time lags can be simply deduced from the analysis of each electrical field injected into a given pair, namely $E_{T,k}^m(t)$ and $E_{T,k}^s(t)$ for the kth pair. The time lags are simply deduced from the necessary conditions of synchronization and read

$$\Delta\tau_k = \tau_{kk}^c - \tau_{kk}^m. \tag{5.24}$$

A simulation of two laser pairs ($n = 2$) is reported in Fig. 5.5. It shows the anticipating synchronization manifolds under ideal conditions. The time lags $\Delta\tau_k$

are here both equal to zero due to additional symmetry between the emitting and receiving ends.

An additional aspect of our architecture is its spectral efficiency, since the free-running lasers operate at identical wavelengths. However, when the chaotic regimes appear, the optical spectrum of each laser is broadened and can exhibit bandwidth of hundred of megahertz. If conventional WDM were applied on top of an optical chaos-based architecture, each chaotic optical spectrum would have to be sufficiently separated to be properly discriminated.

5.3.3 Spectral Efficiency

The proposed architecture can alleviate the spectral constraint existing in WDM by using a different method to separate multiple carriers with significant spectral overlap, *i.e.* the use of independent chaos synchronization between the different pairs M_k/S_k. Figure 5.6 shows, in the case of two pairs of lasers, the optical spectrum of each master field $\sqrt{\eta_{11}^m}E_1^m(t)$ and $\sqrt{\eta_{22}^m}E_2^m(t)$ and the formal multiplexed signal $E_T(t)$. The bandwidth is defined as the spectral width 20 dB below the maximum value of the optical spectrum. Under these conditions, the total bandwidth occupied by the multiplexed field E_T is comparable to the bandwidth of a single chaotic optical field. Taking numerical values similar to those used for Fig. 5.5, the bandwidths are $\Delta f_{E_T} \approx \Delta f_{E_1^m} \approx \Delta f_{E_2^m} \approx 25$ GHz. This means that for one data stream encoded per laser, potentially twice the amount of information per Hz could be conveyed in a single optical channel.

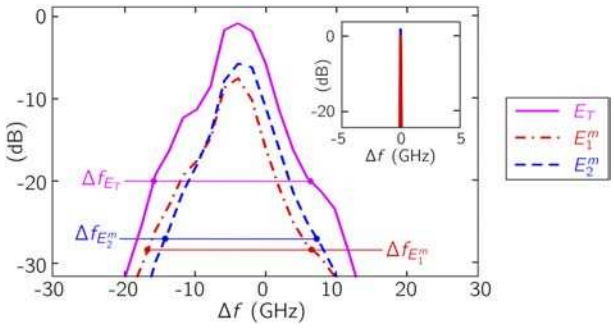

Figure 5.6: Theoretical optical spectra in the case of two pairs of lasers. The spectra of $\sqrt{\eta_{11}^m}E_1^m(t)$, $\sqrt{\eta_{22}^m}E_2^m(t)$, and $E_T(t)$ are plotted. The parameters are assumed identical to those used for Fig. 5.5. The inset shows the free-running optical spectrum of each laser (no coupling considered). The spectra are numerically computed with Welch's method.

5.3.4 Discussion on the Influence of Parameters on the Stability of Chaos Synchronization

The necessary conditions for the existence of chaos synchronization between external-cavity semiconductor lasers exhibited in the previous subsection do not guarantee the stability of the synchronization manifold. As far as ECSLs are concerned, the value of the operational and coupling parameters in this regard are of fundamental importance as detailed in [122; 123; 165]. The particular form of the semiclassical

model described by Eqs. 5.5-5.7 requires a numerical investigation of sufficient conditions for stability. Under the necessary conditions of synchronization for a single pair of ECSL, it is assumed that the master and slave are identical and driven under similar conditions. The synchronization properties depend on the pumping current J_m and the feedback strength η_m (the coupling strength is $\eta_c = \eta_m$, according to the necessary conditions). The plane (J_m, η_m) is therefore a privileged 2D parametric plane to analyze the stability and quality of complete chaos synchronization. In our context, however, it becomes much more complicated. Assuming the necessary conditions of the APD configuration are fulfilled, there is still a 4D parameter space to investigate: $(J_1^m, J_2^m, \eta_{11}^m, \eta_{22}^m)$. In this chapter, we will not give a fully detailed picture of the synchronization regions, but general tendencies on the parameter range that ensure a stable synchronization manifold. We consider a completely symmetric case in terms of the feedback strength ($\eta_{11}^m = \eta_{22}^m$) and cavity length ($\Delta\tau_{12}^m = 0$), where only the pumping currents are varying at various levels of feedback strength. The quality of synchronization is measured by the correlation coefficient

$$C_{kk}(\theta) = \frac{\langle [I_k^m(t-\theta) - \langle I_k^m(t)\rangle]\,[I_k^s(t) - \langle I_k^s(t)\rangle]\rangle}{\left\langle \left[I_k^m(t-\theta) - \left\langle I_k^m \right\rangle\right]^2 \right\rangle^{1/2} \left\langle \left[I_k^s(t-\theta) - \left\langle I_k^s \right\rangle\right]^2 \right\rangle^{1/2}}, \tag{5.25}$$

with $I_k^{m,s} = |E_k^{m,s}|^2$ the optical intensity and $\theta = \Delta\tau_k$ corresponding to the maximum correlation between $\mathrm{M}_k/\mathrm{S}_k$.

Figure 5.7 displays the evolution of cross-correlation of two pairs of lasers in the plane $(J_1^m/J_{th,1}, J_2^m/J_{th,2})$ [with $J_{th,1/2}$ the threshold currents of each laser pair] for increasing levels of feedback; each row corresponds to a pair of lasers.

Figure 5.7 reveals that the synchronization of chaos is stable for a large range of

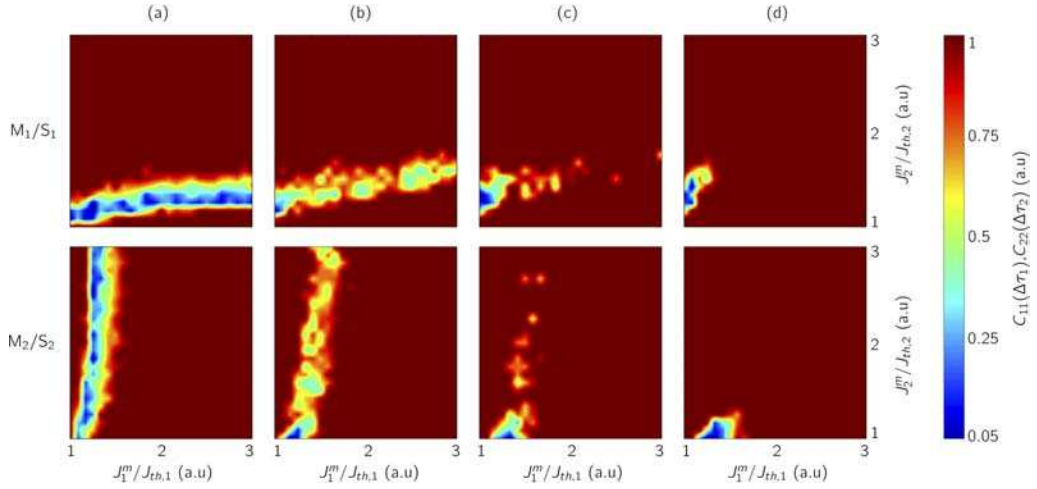

Figure 5.7: Evolution of the cross-correlation coefficients $C_{11}(\Delta\tau_1)$ (1st row) and $C_{22}(\Delta\tau_2)$ (2nd row) in the plane $(J_1^m/J_{th,1}, J_2^m/J_{th,2})$ for increasing values of the feedback strength $\eta_{11,22}^m$ (coupling strength) in a symmetric-coupling configuration: (a) $\eta_{11}^m = \eta_{22}^m = 5$ GHz, (b) $\eta_{11}^m = \eta_{22}^m = 10$ GHz, (c) $\eta_{11}^m = \eta_{22}^m = 12.5$ GHz, and (d) $\eta_{11}^m = \eta_{22}^m = 15$ GHz. The internal parameters of the EELs are identical to those used for Fig. 5.5.

operational parameters; it also highlights the existence of mixed regimes, where only one of the two pairs of lasers is synchronized whereas the other is weakly correlated. Interestingly, when the feedback is increased symmetrically for both masters (the coupling being adjusted accordingly), the zone of weak correlation shrinks dramatically for each pair. The analysis provides insight into the evolution of the general behavior of the synchronization region as the feedback strengths and pumping currents are increased. Figure 5.7 also differs from most of the plots presented in [122; 123; 165], because the necessary conditions ($\eta_{kk}^m = \eta_{kk}^c$) are always satisfied in our simulations. This is why a large region of the parameter plane exhibits a maximum level of correlation ($C_{11}(\Delta\tau_1) \approx C_{22}(\Delta\tau_2) \approx 1$). This study remains nonexhaustive, since the investigation is limited to particular 2D intersections of the 4D parametric plane. Still, it confirms that the existence of multiplexed synchronized states is not a behavioral artefact of the architecture's dynamics and that it does exist in a large region of operational parameters. As a consequence, it should be relatively easy to observe demultiplexed synchronization experimentally.

Finally, it is worth mentioning that interest in our architecture also relies on the freedom in the choice of internal parameters for the various master lasers. As long as systems within a given pair $\mathrm{M}_k/\mathrm{S}_k$ are physical twins, a complete freedom in the choice of the type of lasers is allowed. It is even possible to consider frequency detuned masters (free-running frequencies $\omega_{0i}^m \neq \omega_{0j}^m$ for $i \neq j$) although for spectral-efficiency purposes the frequencies should be close to each other.

5.3.5 Robustness of Synchronization

In this subsection, we quantify the robustness of the synchronization with respect to two major impairments: noise and parameter mismatch. Essentially, the results show that the robustness is similar to that of the complete synchronization of a single-master/single-slave configuration.

5.3.5.1 Influence of Spontaneous-Emission Noise

In the previous subsection, perfect synchronization was observed for both pairs of lasers $\mathrm{M}_k/\mathrm{S}_k$. However, the model did not take into account the existence of the intrinsic noise source due to spontaneous emission. In this subsection, we consider that the spontaneous-emission rate has the numerical value $\beta_{sp} = 1000\ \mathrm{s}^{-1}$, typically encountered in the literature [11]. Figure 5.8 represents the synchronization diagrams $(I_k^{m,s}, I_j^{m,s})$ with $k, j = \{1, 2\}$. The introduction of noise destroys the perfect synchronization observed in Fig. 5.5 since now $C_{11}(\Delta\tau_1) \approx C_{22}(\Delta\tau_2) \approx 0.97$, but the trajectories in the plane (I_k^m, I_k^s) remain relatively close to the noiseless synchronization manifolds [Figs. 5.8(a)-(b)]. These correlation levels are suitable to ensure chaos-based communications with a level of performance comparable to single-user architectures: fast transmissions with low bit-error rates (Gbit/s with BER lower than 10^{-7} [4]).

The level of decorrelation between the two different pairs remains small and is barely affected [$C_{12}(\Delta\tau_1 - \Delta\tau_2) \approx 0.07$] by the presence of spontaneous-emission noise.

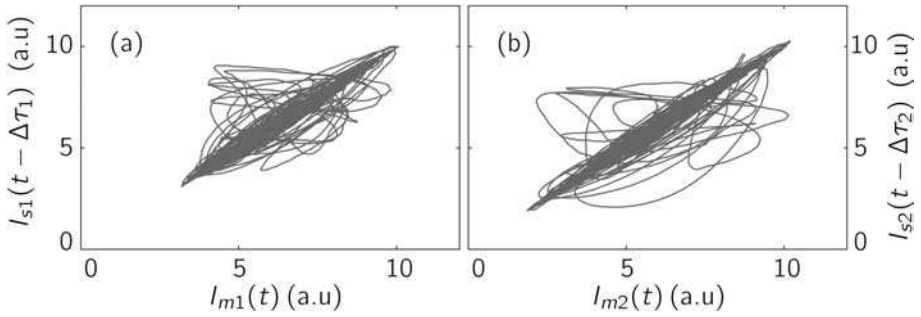

Figure 5.8: Robustness of the synchronization with respect to the presence of intrinsic noise (spontaneous emission $\beta_{sp} = 1000$ s^{-1}) in the case of two pairs of lasers. The parameters are identical to those used for Fig. 5.5.

5.3.5.2 Influence of Parameter Mismatch

We determine that perfect synchronization remains robust to parameter mismatch between lasers in a given pair M_k/S_k, if the mismatch levels are comparable to those encountered in a single-emitter/single-receiver laser configuration. This is highlighted in Fig. 5.9. Additionally, it must be noted that our APD-based coupling configuration does not limit the amount of mismatch between two different pairs (so long as they remain in chaotic regimes).

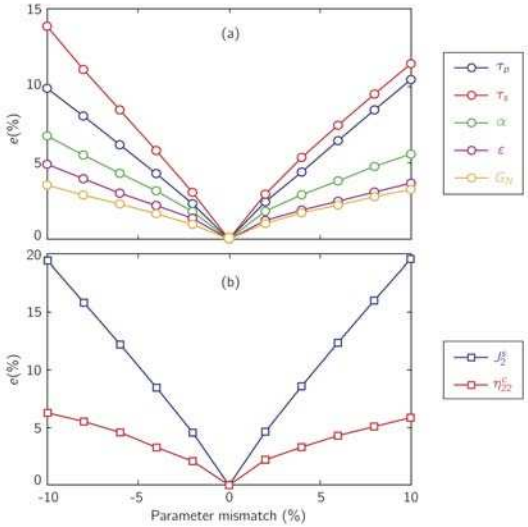

Figure 5.9: Robustness of the synchronization with respect to parameter mismatch in the case of two lasers, illustration of the pair M_2/S_2. The error of synchronization $e(\%) = |I_2^s - I_2^m|/|I_2^m|$ is function of (a) the influence of the laser's internal parameters and (b) the influence of the external parameters (pumping current and injection/coupling strengths). The parameters are identical to those used for Fig. 5.5.

5.3.6 Generalization of the Architecture

As an illustration, the case of two laser pairs has been presented, but it is possible to generalize our architecture to a larger number of lasers. As many units as desired can be introduced through the use of additional beam splitters as illustrated in Fig. 5.10.

The necessary conditions for synchronization remain unchanged when the number of users increases. Interestingly, the overall energy carried by the multiplexed optical field $E_T(t)$ increases in the shared cavity with the number of lasers; master and slave M_k/S_k in each pair will be coupled more strongly. Therefore, it is expected that the size of the parameter region that ensures synchronization will increase with the number of lasers. For instance, the pumping currents region $\{J_k^m\}_{k=1,\dots n}$ that ensures the various pairs of lasers to be synchronized would become larger at given coupling strengths. We have numerically verified this assumption by doubling the number of pairs ($n = 4$). Assuming a configuration with symmetric couplings (similar to Fig. 5.7), we find that for $\eta_{kk} = 7.5$ GHz ($j = k, \dots, 4$) smaller pumping currents ($J_k^m/J_{th,k} \in [1.1, 1.25]$) can be used to ensure the chaos synchronization of the different pairs of lasers, although such a range of values did not work when two pairs of lasers were considered. In terms of robustness, an increase in the number of units is not fundamentally limited by parameter mismatch. As illustrated in the previous subsection, parameter mismatch matters only within a given pair. The robustness to spontaneous-emission noise has also been demonstrated with four pairs of lasers. If the amount of noise in the overall architecture increases, so does the amplitude of the multiplexed field $E_T(t)$. As a consequence, we still achieve good levels of chaos synchronization between the masters and slaves of the various pairs of lasers.

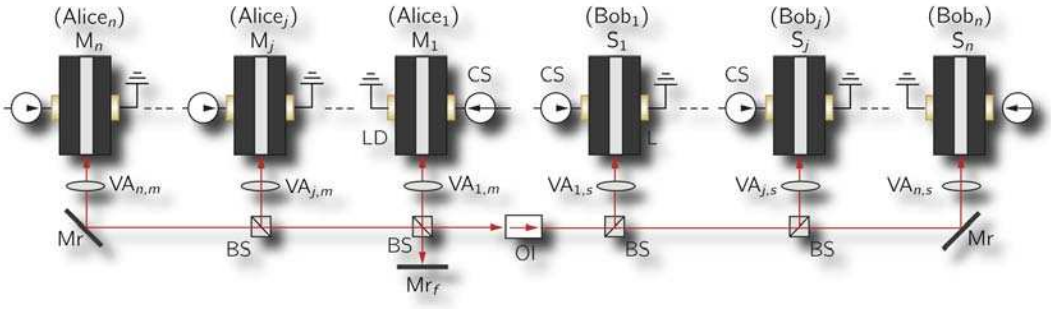

Figure 5.10: Possible generalization of our multiplexed architecture with a larger number of lasers. They share the cavity thanks to additional beam-splitters. LD: laser diode (labeled M_j and S_j for the masters and slaves, respectively), CS: current source, Mr,Mr$_f$: mirrors, VA$_{j,m/s}$: variable attenuators, BS: 50/50 beam splitter, OI: optical isolator, OC: optical coupler, Mod: amplitude/ phase modulator.

However, it requires the use of larger coupling strengths to achieve a high level of correlation compared to the case with two pairs. For instance, with $n = 4$, a symmetric coupling configuration, and a range of pumping current $J_k^m/J_{th,k} \in [1.45, 1.85]$, it requires coupling strengths of $\eta_{kk} = 20$ GHz to achieve $C_{kk}(\Delta\tau_k) \approx 0.92$ (on average) with the spontaneous-emission rate taken identical for the various

lasers $\beta_{sp} = 1000\ \mathrm{s}^{-1}$.

This quick analysis highlights the potential of our architecture for multi-user communications. Nevertheless, the synchronization properties should be thoroughly investigated to find the sets of parameters that guarantee the best level of performance. An increasing number of lasers will also make the experimental realization of our setup more difficult.

5.4 Multiplexing of Information

This study is a first inquiry into the design of a multiplexed optical chaos-based transmission chain based on the use of multiple ECSLs. In this section, we describe how information can be encrypted while exploiting our APD structure. We propose a generalization of chaos-shift keying (CSK) and chaos modulation (CMo). The messages will be either encrypted on the pumping currents for CSK, on the phase (or amplitude) of each optical field composing the multiplexed field $E_T(t)$ for CMo.

We detail the extent to which multi-user CSK and CMo encryptions are suited to our initial architecture. To reach this conclusion, we build on existing single-user methods (CMa, CSK, and CMo), analyze if their generalization to a multi-user transmission is possible, and determine their performance levels.

5.4.1 Multiplexed Optical Chaos Masking

Chaos masking (CMa) is a straightforward chaos-based encryption for single-message transmission. With optical systems, it is realized through an optical addition of uncoded binary message $m(t)$ at the output of a chaotic ECSL [166; 167]. The decryption results from the perturbation induced on the chaos synchronization at the receiving end. However, transmission of multiple messages appears to be impossible if the messages have identical properties. For instance, a two-user CMa would imply the optical addition of two uncoded messages $m_1(t)+m_2(t)$ to the multiplexed optical field at the output of the shared cavity, before its injection into the optical channel. The main issue under these conditions is that part of the information on each message is lost. For instance, if two binary messages are used by each user independently, their sum results in four different levels labelled 00, 01, 10, and 11.[1] These various values allow for the recovery of m_1 and m_2 independently, except in the case $\{01, 10\}$, for which the indeterminacy cannot be removed. Furthermore, when the number of units is increased, the number of bits that cannot be decoded increases accordingly. For instance with three binary messages, it is only possible to make the distinction between four levels out of eight: 000, 111, $\{001, 010, 100\}$, $\{011, 101, 110\}$. As a consequence, CMa cannot be transposed to a multi-user context, if uncoded data are used with our architecture.

[1] We suppose that each user is not aware of the presence of other users on the channel. If this is the case, there exist advanced coding techniques used in the framework of the *multiple-access binary erasure channel* to overcome such a limitation [2; 168]. In most of chaos-based communication schemes, however, users transmit uncoded messages. As a consequence, CMa is here inadequate compared to CSK or CMo, as illustrated below.

5.4.2 Multiplexed Optical Chaos-Shift-Keying

Chaos-shift-keying (CSK) encryption is performed through the digital modulation of the pumping current of each ECSL [169; 170; 171]. The multiplexed field carries implicit information on each message. Every time the pumping current of the kth master laser switches between one of its two levels $\{J^m_{k,0}(t), J^m_{k,1}(t)\}$, the optical field $E^m_k(t)$ is associated with a different chaotic attractor. Figure 5.11 shows a possible implementation of a CSK encryption method based on our original APD-based architecture. As a consequence, the multiplexing field summing n optical fields results

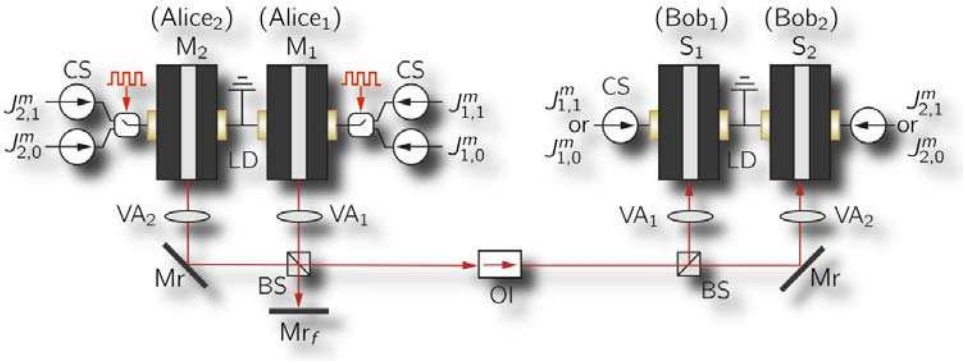

Figure 5.11: Theoretical multiplexed chaos shift-keying scheme. The two lasers are coupled in an APD fashion. Each master M_i is subjected to current $J^m_{k,0/1}$ with $k = 1, 2$. Only two receivers are used for the decryption; this corresponds to the case of a linear decryption later described in this chapter. LD: laser diode (labeled M_k and S_k for the masters and slaves, respectively), CS: current source, Mr,Mr$_f$: mirrors, VA$_1$,VA$_2$: variable attenuators, BS: 50/50 beam splitter, OI: optical isolator.

from 2^n combinations of different chaotic attractors. For the decryption, $2n$ receivers are used (the kth master is duplicated twice, each twin operating at $J^m_{k,0}$ and $J^m_{k,1}$, respectively). Their outputs are summed to generate the 2^n possible combinations. The messages bits minimize the expression

$$\{m_i\}_{i\in[\![1,n]\!]} = \min_{\{J^s_i\}_{i\in[\![1,n]\!]}} |E_T(t)|^2 - |E_D(t)|^2 \,, \tag{5.26}$$

with

$$E_D(t) = E_D(t,\theta,\sigma,\mu) = \sum_{j=1}^{n} \sqrt{\eta^m_{jj}} e^{i\omega^s_{0j}(\theta+\Delta\tau^s_{\sigma j}/2)+it\Delta\omega^\mu_{j\sigma}} E^s_j(t-\theta-\Delta\tau^s_{\sigma j}/2). \tag{5.27}$$

The squared amplitude of the field corresponds to the detection by a photodiode. The main problem with this decryption approach would be its computational complexity, which grows exponentially fast with the number n of users. Generating all the different candidate fields $E_D(t)$ will rapidly become unrealistic from an experimental point of view (because of the 2^n possibilities). Our exponentially complex decryption transposes results on a two-user CSK approach with electronic systems [172] to ECSLs. We propose another solution that consists of using a suboptimal decryption.

We consider only n receivers (instead of $2n$) set at one of the two pumping currents $\{J^m_{i,0/1}\}_{i=1\cdots,n}$ used to encode the various messages. At slave laser S_k, Bob_k monitors either of the two currents (depending on the configuration we chose),

$$I_{D,k}(t) \propto \left(|E_T(t,\tau^c_{kk},k,m/s)|^2 - \eta^m_{kk}\,|E^s_k(t-\tau^m_{kk})|^2\right), \tag{5.28}$$

$$I_{D,k}(t) \propto \left|E_T(t,\tau^c_{kk},k,m/s) - \sqrt{\eta^m_{kk}}e^{i\omega^s_{0k}\tau^m_{kk}}E^s_k(t-\tau^m_{kk})\right|^2. \tag{5.29}$$

In Eq. 5.28 two photodiodes are necessary per legitimate user Bob_k, whereas in Eq. 5.29 only one photodiode is used. This latter technique, however, requires an optical subtraction. To recover $Alice_k$'s transmitted message, Bob_k simply needs to compare the average evolution of the current $I_{D,k}(t)$. Without loss of generality, we assume that S_k is pumped with the current $J^s_k = J^m_{k,0}$ corresponding to the current used by the master M_k to encode the bit of information 0. Every time master M_k encodes a 0, its chaotic attractor coincides with that of S_k. Consequently, the contribution of optical field E^m_k will be cancelled out by E^s_k, thus inducing a decrease in the average value of the intensity $I_{D,k}$. When a bit 1 is encoded, M_k and S_k are on different chaotic attractors. The field E^s_k contributes constructively to the total intensity $I_{D,k}(t)$ at the detector and will have a higher average value compared to the previous case.

To illustrate this approach, we propose the encryption/decryption of two bit streams $m_1(t)$ and $m_2(t)$. Figure 5.12 shows how to multiplex and demultiplex two data streams at 500 Mbit/s. It appears that Eq. 5.28 achieves clearer decryption than Eq. 5.29. In this approach, in the decryption of some bits, the differences in intensity levels of $I_{D,k}$ are not sharp and may induce bit errors. Nevertheless, the complexity of the decryption remains linear with the number of users. This makes such an approach a realistic technique, when the number of lasers is increased.

The CSK method, however, has fundamental limitations. The first one is relative to the bit rate, which is limited by the resynchronization time.

Every time the pumping current is switched, it takes a certain duration (few nanosecond in ECSLs, depending on the parameters used) for the system to *jump*

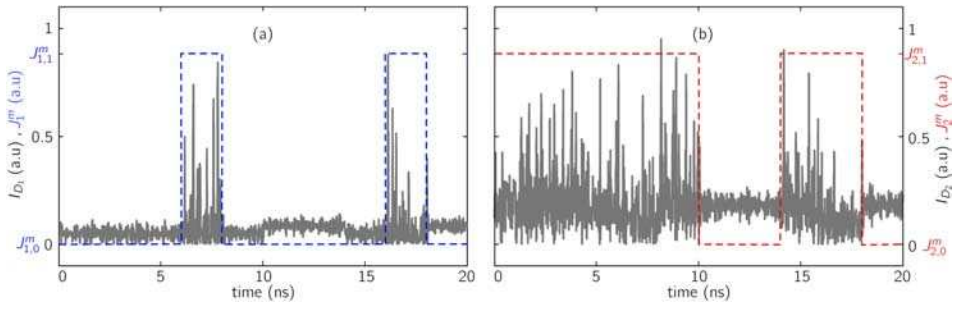

Figure 5.12: Theoretical multiplexing/demultiplexing of two binary messages m_1 and m_2 at 500 Mbit/s encoded on two pumping current levels for each laser diode $J^m_{1/2} \in \{J^m_{1/2,0}, J^m_{1/2,1}\}$. The intensity of each detector $I_{D,k}$ has been normalized with respect to its maximum value. The blue and red dashed lines represent the original messages encoded by $Alice_1$ in (a) and by $Alice_2$ in (b), on their respective laser M_1 and M_2. The numerical values are similar to those used for Fig. 5.5.

from a chaotic attractor and stabilize on another (time also associated to the relaxation oscillations of the free-running laser). The second limitation concerns the choice of the message amplitude. In a linearly complex decryption, the amplitude has to be large enough to guarantee the detectability of the encoded bits. This must be done in a way that the values of pumping current ensure sufficiently high synchronization levels in the pairs of laser M_k/S_k when the pumping currents J_k^m and J_k^s matched each other. Otherwise, the discrimination between synchronized and unsynchronized states, used in the decryption, would become inefficient. In our simulations and with our choice of parameters, the bit rate tops around 500 Mbit/s with the pumping current modulation for the encryption satisfying the following ratio $J_{1,1}^m/J_{1,0}^m \approx J_{2,1}^m/J_{2,0}^m \approx 3/2$. An increase of bit rate makes the linearly complex decryption inefficient; the discrimination between two pumping levels is not observed with the parameters under consideration, even with a large ratio $J_{k,0}^m/J_{k,1}^m$.

To a certain extent, CSK has been successfully transposed to a multi-user context with the main advantage of its structural simplicity. Nevertheless, its level of performance is limited.

5.4.3 Multiplexed Optical Chaos Modulation

In contrast to the previous approach, chaos modulation (CMo) aims at encoding the messages such that they participate in the dynamics of each emitter M_k. As a consequence, the encoding can be only performed on the amplitude or the phase of the optical fields that couple the emitters together and inject the receivers. If done properly, the encryption does not disturb the synchronization and the quality of the decryption as well as the bit-rate can be enhanced, compared to CSK. Indeed in the case of single emitter and a single receiver, CMo has already proven to be more efficient than CSK [117]. However, even if it presents theoretical advantages, CMo requires a modification of the multiplexed architecture presented in Fig. 5.4. The inclusion of phase/amplitude modulators in the emitter's shared optical cavity is not straightforward because of the following reasons:

- The modulators would contaminate the optical fields of each master, and have an averaging effect in the encoding information similar to that of the multiplexed chaos masking.
- The modulation speed will be limited to that of the cavity length, since it is necessary to wait for the multiplexed light field to make a complete round trip in the shared cavity before the modulator switches its state, thus limiting the bit rate in most situations. In the case of a single-emitter/single-receiver, a phase modulator has been placed in the cavity and the so-called on-off phase-shift keying (OOPSK) was derived [173]. It was praised for its relative security, but the modulation speed was bounded at a hundred of Mbit/s where traditional chaos-based encryption techniques reach multiple Gbit/s.

To solve this problem, we must design a structure based on the physical model described by Eqs. A.9, where the the kth data stream is encoded only onto the kth master optical field $E_k^m(t)$. A theoretical structure is proposed for two users in Fig. 5.13 (and is easily generalized to a larger number).

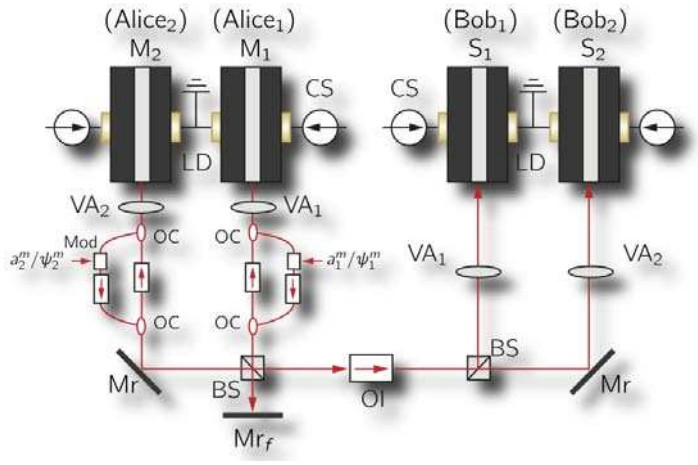

Figure 5.13: Theoretical multiplexed chaos modulation scheme. The two lasers are coupled in an APD fashion. Each modulator is included to affect only its designated field. LD: laser diode (labeled M_1, M_2 for the masters), CS: current source, Mr,Mr$_f$: mirrors, VA_1,VA_2: variable attenuators, BS: 50/50 beam splitter, OI: optical isolator, OC: optical coupler, Mod: amplitude/ phase modulator.

Although, such a setup may be difficult to realize experimentally, it still gives us a driving principle to make a multiplexed CMo with an encryption on the amplitude or the phase of the optical field. The optical circulators introduced in the various arms of the shared external cavity allow each message to be encoded only on single master field E_k^m.

The multiplexed field therefore reads

$$\begin{aligned} E_{T,CMo}(t,\theta,\sigma,\mu) = \sum_{j=1}^{n} \sqrt{\eta_{jj}^m} e^{i\omega_{0j}^m(\theta+\Delta\tau_{\sigma j}^m/2)+it\Delta\omega_{j\sigma}^{\mu}+\psi_{m,j}(t-\theta-\Delta\tau_{\sigma j}^m/2)} \\ \times(1+a_{m,j}(t-\theta-\Delta\tau_{\sigma j}^m/2))E_j^m(t-\theta-\Delta\tau_{\sigma j}^m/2), \end{aligned} \tag{5.30}$$

with $a_{m,j}(t)$ and $\psi_{m,j}(t)$ the jth message encoded either on the amplitude or the phase of the optical field E_j^m, respectively.

Under these conditions, the inclusion of the various messages does not disturb the decryption process. With a multiplexed CMo, the masters do not switch between different chaotic attractors, thus removing the limitations imposed by the resynchronization time in the CSK approach. As a consequence, higher bit rates and quality of chaos synchronization are achieved. In the case of chaotic lasers, the decryption relies mostly on intensity measurements acquired by photodiodes. However with multiplexed optical fields such as $E_T(t,\theta,\sigma,\mu)$, inevitable interferences between the master fields E_m^k will render the decryption sightly more difficult. As in the case of the multiplexed version of CSK, it is possible to design both exponentially and linearly complex decryption approaches. We illustrate each by considering an encryption on the phase.

5.4.3.1 Exponentially Complex Decryption Strategies

Without loss of generality, we consider the case of two pairs of lasers M_k/S_k coupled as described in Fig. 5.13. Assuming a binary encryption on the phase of each master field, there are four possible message combinations (also called states) labeled: 00, 01, 10, and 11. Each pair of lasers is completely synchronized, but the receiver has no knowledge of the encrypted messages. To decrypt them, different combinations of messages are formed at the receiver end to create candidate multiplexed fields $E_{D,b_1b_2\in\{00,01,10,11\}}(t,\theta,\sigma,\mu)$. These fields will be then compared to the original multiplexed signal $E_{T,CMo}(t)$. When one of the combinations at the receiver matches that of the emitter, then the difference is minimum, and it means that the state b_1b_2 with $b_j = \{0,1\}$ and $j = \{1,2\}$ (formally associated with the four possible combinations made out of the two binary phased-encoded messages ψ_1^m and ψ_2^m) was originally encoded at the emitter. The existence of such a minimum naturally leads to a decoding method via threshold detection. In our example, if we consider a detector composed of two photodiodes (to detect independently $E_{T,CMo}(t)$ and $E_{D,b_1b_2}(t)$ before being subtracted, then the output of the detector is a current intensity). The intensity at the output of this type of detector reads

$$I_{D,b_1b_2} \propto \eta_{11}^m(|E_1^m|^2 - |E_1^s|^2) + \eta_{22}^m(|E_2^m|^2 - |E_2^s(t)|^2) + 2\sqrt{\eta_{11}^m\eta_{22}^m} \times \left(|E_1^mE_2^m|\cos(\varphi_1^m + \psi_1^m - \varphi_2^m - \psi_2^m) - |E_1^sE_2^s|\cos(\varphi_1^s + \psi_{1,b_1}^m - \varphi_2^s - \psi_{2,b_2}^m)\right), \tag{5.31}$$

with $E_{1,2}^m = E_{1,2}^m(t - \Delta\tau_{1,2})$, $E_{1,2}^s = E_{1,2}^s(t)$, and $\psi_{1,2}^m \in \{\psi_{1,0/1}^m, \psi_{2,0/1}^m\}$ the binary messages.[1] Figure 5.14 reports a decryption scenario realized with identical parameters to those used for Fig. 5.5.

Each row presents the output of a different detecting circuit $I_{D,00}$, $I_{D,01}$, $I_{D,10}$, and $I_{D,11}$ (if two bits are encrypted, four detectors are necessary). When the intensity of a given detector is minimum with respect to the others, it means that the corresponding pair of bits was encoded at the emitter end. Assuming no noise in the transmission and no parameter mismatch within a given pair of lasers, the messages' retrieval is error free.

The computational complexity (2^n for a binary message and n users) of this decryption method grows exponentially fast and will rapidly limit the number of users. This has motivated the derivation of linearly complex decryption similar to what was done for the CSK in the previous subsection.

Similar results to those of Fig. 5.14 can be achieved if the encryption is performed on the optical field's amplitude.

5.4.3.2 Linearly Complex Decryption Strategies

To overcome the computational limitations in terms of users, the recovery should be performed independently on each message. We have derived decoding equations

[1] It is possible to consider another type of detection such as the *balanced homodyne detection*. Before being independently detected, each multiplexed field recombines on a 50/50 beam splitter. The decoding equations, however, are more complex.

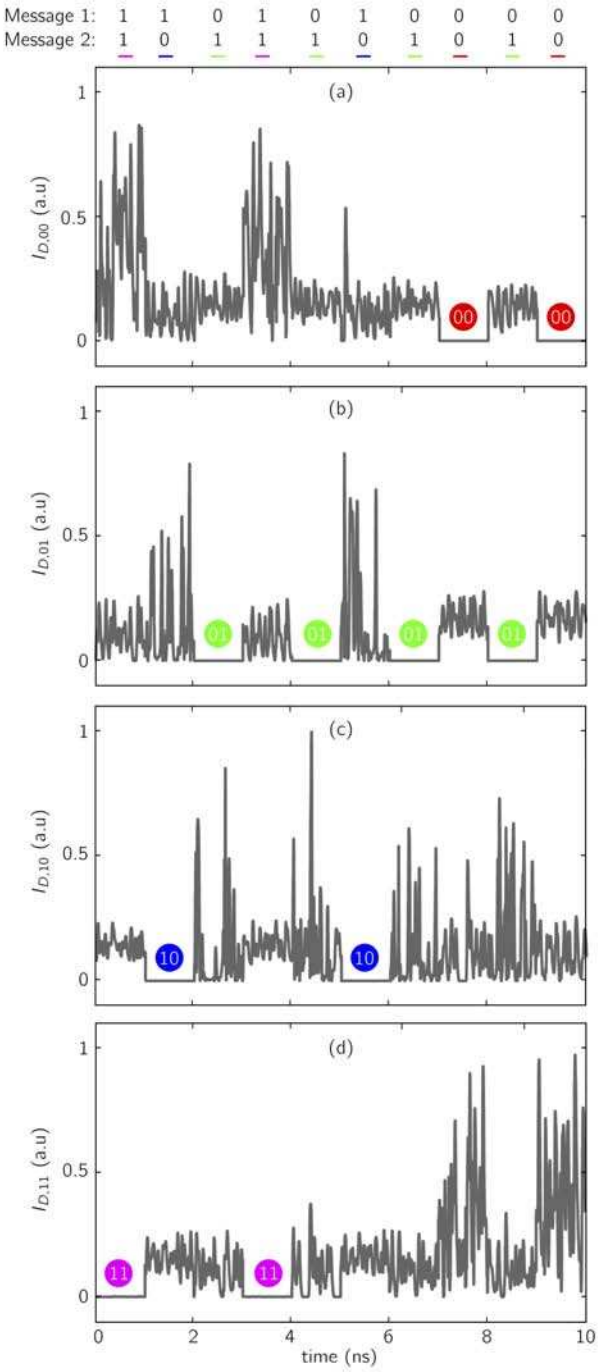

Figure 5.14: Theoretical multiplexing of two binary phased-encoded messages ψ_1^m and ψ_2^m at 1 Gbit/s. The messages are jointly decrypted by four decoding circuits. The recovery of the bits is given by $b_1 b_2 = \min\left(I_{D,00}, I_{D,01}, I_{D,10}, I_{D,11}\right)$. The normalized intensity are represented on each row. The parameters are identical to those used for Fig. 5.5.

similar to Eqs. 5.28-5.29, which can be used to recover the binary messages

$$I_{D,k}^{CMo} \propto \left| E_T(t, \tau_{kk}^c, k, m/s) - \sqrt{\eta_{kk}^m} e^{-j\omega_{0k}^s \tau_{kk}^m + \psi_{k,0/1}^m} (1 + a_{k,0/1}^m) E_k^s(t - \tau_{kk}^m) \right|^2, \quad (5.32)$$

$$I_{D,k}^{CMo} \propto |E_T(t, \tau_{kk}^c, k, m/s)|^2 - \left| \sqrt{\eta_{kk}^m} e^{-j\omega_{0k}^s \tau_{kk}^m + \psi_{k,0/1}^m} (1 + a_{k,0/1}^m) E_k^s(t - \tau_{kk}^m) \right|^2 \quad (5.33)$$

These equations correspond to two different methods of detection. Equation 5.32 corresponds to an optical subtraction of the fields E_T and E_k^s followed by a detection by a single photodiode. On the contrary, Eq. 5.33 uses two photodiodes; first each optical field (E_T and E_k^s) is detected independently, then the two electrical currents are subtracted. After numerical simulations, it appears that the first method gives better results when the encoding is performed on the phase; the other detection performs better on an amplitude encoding.

The detection is threshold-based, similar to the case of exponentially complex decryption. For each laser S_k, the legitimate user Bob_k chooses one fixed value of phase ψ_k^m (or amplitude a_k^m) among the interval $\{\psi_{k,0}^m, \psi_{k,1}^m\}$ (or $\{a_{k,0}^m, a_{k,1}^m\}$). Every time $Alice_k$ is transmitting the bit arbitrary chosen by Bob_k, the average value of the intensity at the kth detector ($I_{D,k}$) will drop out, thus allowing for a particular user to detect his data-stream. However, the detection is not as sharp as in the exponentially complex case, since only a fraction of the multiplexed signal will be cancelled out.

As a consequence, the method appears not to be sufficiently sensitive to discriminate multiple-level message (M-ary). In addition, the encoding range is intrinsically limited either by the phase or amplitude; phase information can be encoded only within the range $[-\pi, \pi]$ and amplitude information has to remain small to ensure its proper concealment in the optical chaotic carrier.

We present in Fig. 5.15 the transmission of two binary messages at 1 Gbit/s. The output of each detector is represented by a solid line, whereas the original messages, encoded on two difference phase levels $\{0, \pi\}$, are represented on the same figure in dashed lines. The decryption is realized with Eq. 5.32.

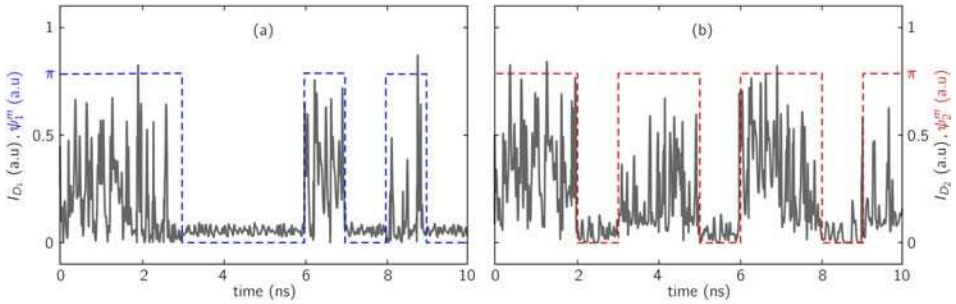

Figure 5.15: Theoretical multiplexing/demultiplexing of two binary phase-encoded messages ψ_1^m and ψ_2^m at 1 Gbit/s. The intensity of each detector $I_{D,k}$ has been normalized with respect to its maximum value. Ten decoded bits are represented. The blue and red dashed lines represent the original messages encoded by $Alice_1$ in (a) and by $Alice_2$ in (b), on their respective laser M_1 and M_2. The parameters are identical to those used for Fig. 5.5.

The decryption of each message shows the sudden dropouts of the detectors' intensity when $Alice_k$'s encoded bits $\psi_{k,0/1}^m$ match the preset value (in our simulation

$\psi_{k,0}^{m}$) used by Bob_k. The level of intensity seems close to zero, but it is mainly a scaling effect due to the normalization by the highest level of $I_{D,k}$ reached during the whole transmission. The small variations at these low levels of intensity result from the non-cancelled part that is still present in the detection.

5.5 Conclusion

In summary, we have analyzed the possibility of multiplexing multiple chaotic optical fields generated by semiconductor lasers. We have theoretically devised an architecture based on a shared external cavity, which allows for the various lasers to be globally mutually coupled. The multiplexed field obtained in the cavity results from the superposition of the fields generated by the various lasers at the emitter. This signal is then sent through a communication channel and injects slave lasers (physical copies of the masters used at the emitter end) at the receiver end; this is an optical analogue of an APD with multiple time-delay systems. We demonstrate that each pair master/slave can be chaotically synchronized when the necessary coupling conditions, which naturally extend the single-emitter/single-receiver case, are satisfied. A rapid analysis also shows a wide range of operational parameters (pumping currents and coupling strengths) ensuring the stability of the chaos synchronization manifold for each pair of lasers. The robustness of synchronization with respect to intrinsic noise and parameter mismatch is similar to that of a single pair of lasers. Therefore, the robustness is good enough to envisage the development of multiplexed optical chaos-based communications.

Concerning the transmission aspects, we proposed extending the classical encryption techniques of CMa, CSK, and CMo to a multi-user context. It appears that only CSK and CMo are adequate for the uncoded messages used. The multi-user CSK approach consists of the digital modulation of the laser pumping currents between two different levels to encrypt the messages. They are retrieved at the receiving end using either low- or high-computational complexity decryption. The latter method involves the use of multiple receivers ($2 \times n$ with n users) and the computation of all the possible combinations of signals at the receiver end that, when subtracted from the multiplexed field, lead to minima. The complexity increases exponentially fast with the number of users, thus limiting the number of messages that can be transmitted and decoded. This has motivated the development of a decryption method with a linear computational complexity; an identical number of emitters and receivers (with identical sets of parameters to those of the emitters) is used. The multiplexed field is compared individually to the various receivers' fields and each message is retrieved by a threshold-based detection. The complexity increases linearly with the number n of users, but CSK is still limited to hundreds of Mbit/s per user due to perturbations of the synchronization at the reception (intrinsically associated with the encryption). The multi-user CMo approach consists of the independent modulation of each laser field's amplitude or phase. It relies on identical decryption strategies to those developed for multi-user CSK. Nevertheless, transmissions at the Gbit/s data rates are achieved. This paves the way towards highly efficient multiplexed optical chaos-based communications.

Chapter 6

Multiplexing Chaos Using Optoelectronic Oscillators

Abstract

This chapter is dedicated to the analysis and design of an optoelectronic device to multiplex optical chaos and transmit multiple messages. The proposed architecture is derived from an existing single-loop electro-optic oscillator (EOO). We use a single chaotic optoelectronic oscillator with multiple delayed feedback loops to generate multiple orthogonal optical carriers tailored for a secure multiplexed encryption of several data streams with a decryption whose computational complexity increases linearly with the number of users. Similar to code-division multiple access (CDMA) in optical communications, chaotic signals generated by the Mach-Zehnder modulator (present in each delayed feedback loop) are used as orthogonal spreading sequences (codes) to transmit multiple messages. Chaos synchronization is then used to reproduce identical chaotic codes at the receiver's end to be later used in a correlation-based detector to recover the various messages independently. We apply numerically this method and successfully decrypt multiple digital data streams at high bit rates (multi Gbit/s).

This chapter is based on the following publication:

- D. Rontani, A. Locquet, M. Sciamanna, D.S. Citrin, and A. Uchida "Generation of Orthogonal Codes with Chaotic Optical Systems", *Opt. Lett.* **36**, pp. 2287-2289 (2011).

6.1 Introduction

Chaos-based communications are spread-spectrum techniques that provide physical-layer security but have low spectral efficiency, unless multiple data streams are encoded simultaneously. A possible solution consists of transposing the concept of code-division multiple access (CDMA) with orthogonal carriers to the context of chaos-based communications, using signals generated by chaotic optoelectronic devices with identical structures. In conventional multi-user communications, CDMA makes use of multiple fixed binary pseudo-random signals also called *codes* to spread out the spectrum of various binary data streams, as illustrated in Fig. 6.1.

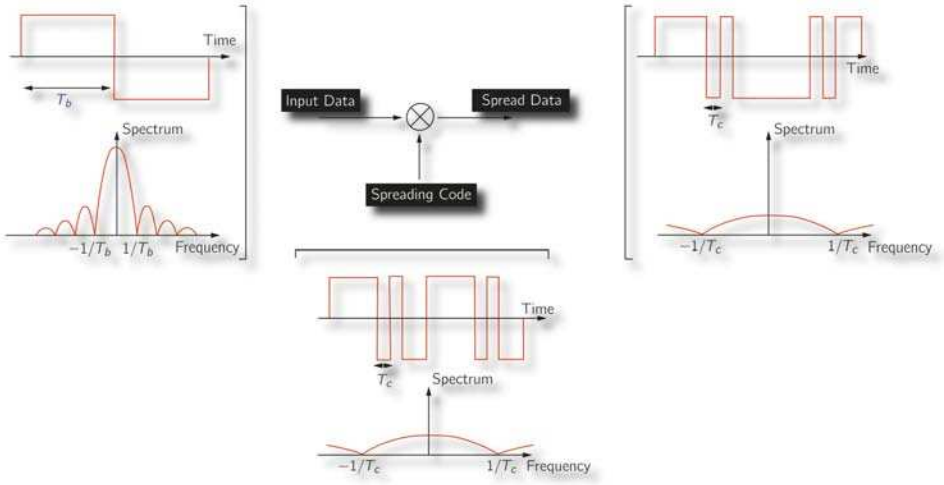

Figure 6.1: Illustration of the principles of CDMA on a binary sequence of bits of period T_b which is spectrally spread by a fixed pseudo-random sequence of period $T_s < T_b$.

Then, the spread data streams are recombined into a single signal and overlap spectrally. To recover them, a correlation-based detector [21] is used at the receiver, assuming the fixed codes to be accessible. Though orthogonality (decorrelation) between each user's code is not necessary, it is desirable as it guarantees for the decryption a linear computational complexity with the number of users (or messages).

Transposing the principles of CDMA to the context of chaos-based communications is naturally suggested by the spectral properties of the chaotic signals that can be considered as time-varying non-binary spreading sequences (time-varying codes) because of their large bandwidth compared to that of the message to be transmitted. In a single-user chaos-based cryptsystem, chaos synchronization is then used at the receiver to reproduce the chaotic signal (spreading sequence) and recover the message. Although chaos-based cryptography bares some similarities with a CDMA technique, its adaptation to the transmission of multiple messages is difficult, mostly because of the time-varying nature of the generated codes (continuously changing for every bit of transmitted messages), which requires generating processes that permanently guarantee orthogonality. This design constraint has already proven to be particularly challenging, when multiple chaotic Lorenz systems with identical structure and various set of parameters were used [19]. Indeed, the existence of general

synchronization (GS) between chaotic signals generated by each system was responsible for significant cross-correlation levels. It was also proven that orthogonality was hardly achieved as the number of chaotic Lorenz systems (or users) increases. To overcome this issue, complexifying the emitters' structure was necessary and a cascaded Lorenz structure was proposed.

In this chapter, we propose to address the generation of orthogonal *chaotic codes* by exploiting the statistical properties of chaotic signals generated by a modified version of a single delayed electro-optic generator (EOO) [102; 116], ultimately aiming at the simplest possible transposition of CDMA to the context of optical chaos-based communications. Then, we devise strategies to encrypt and decrypt the various messages.

6.2 Description and Modeling of the Optoelectronic Oscillator with Multiple Loops

In this section, we propose two different architectures based on an EOO with multiple feedback loops that are suited for multi-user communications. The first one uses multiple photodetectors and the second one uses a single photodetector, the latter being tailored for the transmission of information with an optical channel. We derive the models associated to each configuration to determine the simplest architecture that can be used to transpose CDMA.

6.2.1 Configuration (1) with Multiple Photo-Detectors

In Configuration (1), an EOO-based architecture with multiple delayed feedback loops (each of them comprises its own photodetector) is proposed for the emitter (E). Figure 6.2 depicts a realization of the modified EOO with $n = 2$ feedback loops associated with different cosine-square nonlinearities. It is composed of a monochromatic (wavelength $\lambda_0 = 2\pi/\nu_0$) CW semiconductor laser diode with optical power P_0 divided in the n separate arms, where the light is modulated by a Mach-Zehnder modulators (MZ_j) with respective constant-valued rf and dc half-wave voltages $V_{\pi_{rf_j}}$ and $V_{\pi_{dc_j}}$ and biased by voltage V_{dc_j}. The optical signals travel through different optical fibers DL_j with fixed time delays T_j. Before being recombined, they are independently detected by multiple photodetectors PD_j (of efficiency S), one per optical arm. The resulting electrical signals are combined into a single electrical multiplexed signal. It is then amplified with gain G and filtered by a band-pass filter with low and high cut-off frequencies f_L and f_H. The total attenuation of each loop is denoted $g_j < 1$ and is obtained, for instance, by using a voltage divider D_j.

These two attenuations induce different frequencies of oscillation ω_j for the cosine-square nonlinearities[1] because they reduce the electrical voltage $V(t)$ before driving

[1]The term *frequency of oscillation* ω_i of the nonlinearity is interpreted as a frequency in the following sense: with a simple delayed nonlinear feedback defined by $f(x(t-T)) = \beta\cos^2(x(t-T)+\varphi_0)$, when $x(t-T)$ varies by an amount of π/β the nonlinear function f oscillates once. Consequently, by modifying the nonlinear function with the inclusion of an additional internal gain ω_j, the nonlinear function $f(x(t-T)) = \beta_j\cos^2(\omega_j x(t-T)+\varphi_{0j})$ oscillates once if $x(t-T)$ varies by an amount of $\pi/\beta_j\omega_j$. In this framework, we can either consider that the required amount of

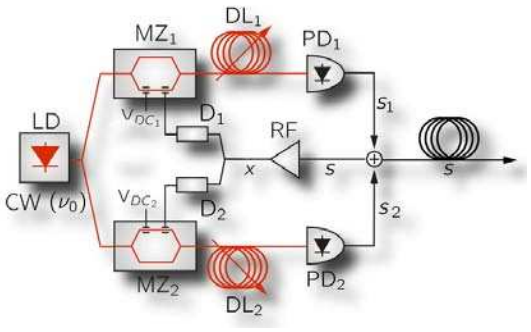

Figure 6.2: Chaotic CDMA system used as the emitter (E) in a transmission chain. As an illustration, a single optoelectronic oscillator with two feedback loops and two photodetectors is presented. LD: laser diode, $\mathrm{MZ}_{j=1,2}$: Mach-Zehnder modulator, $\mathrm{DL}_{j=1,2}$: optical delay line, $\mathrm{PD}_{j=1,2}$: photodetector, RF: band-pass amplifier, $\mathrm{D}_{j=1,2}$: voltage divider ensuring reduction factor $g_{j=1,2} < 1$, $m_{j=1,2}$: messages to be encrypted.

the respective Mach-Zehnder modulator MZ_j.

The voltage output of the RF band-pass filter $V(t)$ and its input $V_{in}(t)$ (sum of the voltage generated by the n photodetectors) are related by

$$\left(1+\frac{f_L}{f_H}\right)V(t)+\frac{1}{2\pi f_H}\frac{dV(t)}{dt}+2\pi f_L\int_{t_0}^{t}V(s)ds=GV_{in}(t)=G\sum_{j=1}^{n}V_{in,j}(t). \quad (6.1)$$

Following the filter (labeled RF in Fig. 6.2), each electric branch of the loop has a specific voltage divider D_j that attenuates the voltage $V(t)$ by the parameter $g_j < 1$. At the output of the $j-$th photodetector, the voltage $V_{in,j}(t) = SGI_{s,j}(t)$ with $I_{s,j}(t)$ the optical intensity at the output of MZ_j. Adopting similar notations to those used in [107], we derive a dimensionless dynamical model that reads

$$\tau\frac{dx}{dt}+x+\frac{1}{\theta}\int_{t_0}^{t}x\left(u\right)du=\sum_{j=1}^{n}\beta_j\cos^2\left(\omega_j x_{T_j}+\varphi_{0i}\right), \quad (6.2)$$

with $x(t)=g_1\frac{\pi V(t)}{2V_{\pi_{rf1}}}$ the dimensionless state variable, $x_{T_i}=x(t-T_i)$ the delayed variable, $\omega_j=\frac{g_jV_{\pi_{rf1}}}{g_1V_{\pi_{rfj}}}$ the frequency of oscillation of the jth nonlinearity, $\beta_j=g_1\frac{\pi GSP_j}{2V_{\pi_{rf1}}}$ the nonlinear gain of the jth loop, and $\varphi_{0j}=\frac{\pi V_{dcj}}{2V_{\pi_{dcj}}}$ the phase-shift associated to the dc bias of the MZ_j. The multiplexed signal $s(t)=\sum_{j=1}^{n}\beta_j\cos^2\left(\omega_j x_{T_j}+\varphi_{0j}\right)$ will be transmitted into an electrical communication channel. Without loss of generality, we have chosen to use $V_1(t)$, the voltage applied to the RF electrode of modulator MZ_1 and its associated reduction factor g_1, as references to derive the dimensionless model.

Interestingly, this design prevents the creation of interferences during the detection. The total feedback signal $s(t)$ is the sum of the feedback signals $s_j(t)=\beta_j\cos^2(\omega_j x_{T_j}+\varphi_{0j})$. These signals, assuming they satisfy adequate statistical properties, are natural candidates for the chaotic codes that will simultaneously carry

variation for $x(t-T)$ is smaller (clearly a gain effect) or that the nonlinear function oscillates *faster*.

the various data streams. However, the architecture is inadequate for an application in optical networks because the multiplexed signal is electrical. To circumvent this issue, the feedback signal have to be optically combined before being detected, as described below.

6.2.2 Configuration (2) with a Single Photodetector

In this subsection, we propose a solution to overcome the main drawback of the previous architecture: the electrical nature of the multiplexed signal $s(t)$ to be transmitted. The solution consists of a recombination of the optical fields from the various feedback loops before being detected by a single photodetector; the multiplexed signal is optical and couples both the emitter and receiver. The physics associated to the detection of multiple optical fields may under certain conditions lead to the creation of *interference*[1], which is not desirable for communication purposes. We propose two configurations (2a) and (2b) that use an optical multiplexed signal and are both described in Fig. 6.3.

In Configuration (2a), a single monochromatic light source is used (or multiple light sources with identical wavelength $\lambda_0 = 2\pi/\nu_0$ if additional optical power is necessary to power the architecture). As previously, each loop contains a Mach-Zehnder modulator MZ_j, an optical delay line DL_j which delay the jth optical field by T_j. A polarization controller PC_j is added to the various loops to choose polarization direction of the jth electromagnetic field $\mathbf{E}_j e^{i\phi_j - 2\pi\nu_j t}$ and possibly minimize the interference. Their complete avoidance, however, is impossible as soon as the number of loops is greater than two. Configuration (2b) uses either multiple laser diodes with different wavelengths $\lambda_j = 2\pi/\nu_j$ (with sufficiently large frequency detuning) or multiple incoherent laser diodes with identical wavelength λ_0 to prevent the appearance of interferences.

The use of a single photodetector impacts the derivation of the mathematical model for our architecture. The feedback signal will undergo significant changes with the appearance of potential interference terms (depending on the configuration (2a) or (2b) and the number of loops). First, we give an expression for the jth electric field at the output of MZ_j; it reads

$$\mathbf{E}_{j,out}(t) = \mathbf{E}_j \cos\left(\frac{\pi V_j(t-T_j)}{2V_{\pi_{RFj}}} + \frac{\pi V_{DC_j}}{2V_{\pi_{DCj}}}\right) e^{i\phi_j - 2\pi\nu_j t}, \tag{6.4}$$

with $V_j(t)$ referring to as the amplified voltage applied to the RF electrode of MZ_j. Assuming that the n optical fields interfere when detected by the single photodetec-

[1] **Recall on interference on a photodetector**. If two optical fields $\mathbf{E}_1 e^{i\phi_1 - i\omega_1 t}$ and $\mathbf{E}_2 e^{i\phi_2 - i\omega_2 t}$ are summed, their photodetection reads

$$I_D \propto |\mathbf{E}_1|^2 \langle \cos^2(\omega_1 t)\rangle_{\tau_d} + |\mathbf{E}_2|^2 \langle \cos^2(\omega_2 t)\rangle_{\tau_d} + 2\mathbf{E}_1 \cdot \mathbf{E}_2 \langle \cos(\omega_1 t - \phi_1)\cos(\omega_2 t - \phi_2)\rangle_{\tau_d}, \tag{6.3}$$

with $\langle\cdot\rangle_{\tau_d}$ the time-average operator performed on duration τ_d the integration time of the photodetector. The observation of interference requires three conditions: 1) the use of identical light sources (same optical frequency) or with different optical frequencies but with the following condition $|\nu_1 - \nu_2| \ll 1/\tau_d$, 2) a strong temporal coherence of the light sources, 3) the use of parallel polarization (optical field with orthogonal polarization do not interfere).

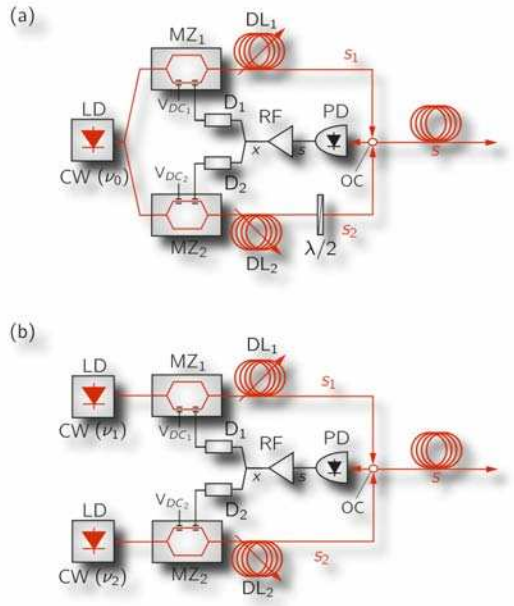

Figure 6.3: Chaotic CDMA systems used for the emitter (E). A single optoelectronic oscillator with two feedback loops and a single photodetector is used as an illustration. In configuration (a), the polarizations of the optical fields are rotated to minimize interference between the different optical arms powered by a single monochromatic source ($\lambda_0 = 2\pi/\nu_0$). In configuration (b), multiple monochromatic sources operating at different wavelength ($\lambda_j = 2\pi/\nu_j$) are used to prevent interferences on the photodetector. LD: laser diode, $\mathrm{MZ}_{j=1,2}$: Mach-Zehnder modulator, $\mathrm{DL}_{j=1,2}$: optical delay line, $PC_{j=1,2}$: polarization rotator, OC: optical coupler, PD: photodetector, RF: band-pass amplifier, $\mathrm{D}_{j=1,2}$: voltage divider ensuring reduction factor $g_{j=1,2} < 1$, $m_{j=1,2}$: messages to be encrypted.

tor, the intensity $I_s(t)$ at the output of the photodetector reads

$$\begin{aligned} I_s(t) = & \sum_{j=1}^{n} |\mathbf{E}_j|^2 \langle \cos(2\pi\nu_j t)\rangle_{\tau_d} \cos^2\left(\frac{\pi V_{j,T_j}}{2V_{\pi_{rfj}}} + \frac{\pi V_{dcj}}{2V_{\pi_{dcj}}}\right) \\ & + \sum_{j,k=1,j\neq k}^{n} \mathbf{E}_j \cdot \mathbf{E}_k \cos\left(\frac{\pi V_{j,T_j}}{2V_{\pi_{rfj}}} + \frac{\pi V_{dcj}}{2V_{\pi_{dcj}}}\right) \cos\left(\frac{\pi V_{k,\tau_k}}{2V_{\pi_{rfk}}} + \frac{\pi V_{dck}}{2V_{\pi_{dck}}}\right) \\ & \times \langle \cos(\phi_j - 2\pi\nu_j t)\cos(\phi_k - 2\pi\nu_k t)\rangle_{\tau_d}, \end{aligned} \tag{6.5}$$

with τ_d the integration time of the photodetector. During τ_d, we have

$$\langle \cos^2(2\pi\nu_j t)\rangle_{\tau_d} = 1/2, \tag{6.6}$$

$$\langle \cos(\phi_j - 2\pi\nu_j t)\cos(\phi_k - 2\pi\nu_k t)\rangle_{\tau_d} = \begin{cases} \cos(\phi_j - \phi_k) & \text{if } \nu_j = \nu_k = \nu_0, \\ 0 & \text{otherwise.} \end{cases} \tag{6.7}$$

We denote the optical power associated to the jth optical field by $P_j = |\mathbf{E}_j|^2/2$ and the factor $C_{ij} = \cos(\alpha_j - \alpha_k)\cos(\phi_j - \phi_k)$, with α_j the polarization direction of the jth linearly-polarized optical field with a reference direction. In Configuration (2a),

interference appears and the dynamical model will have an additional component in its feedback term by comparison with Configurations (1) and (2b).

Therefore, we can derive its model

$$\tau\frac{dx}{dt}+x+\frac{1}{\theta}\int_t^t x(u)du=\sum_{j=1}^{n}\beta_j\cos^2(\omega_j x\left(t-T_j\right)+\varphi_{0j}) + \sum_{j,k=1}^{n}\sqrt{\beta_j\beta_k}C_{jk}\cos\left(\omega_j x_{T_j}+\varphi_{0j}\right)\cos\left(\omega_k x_{T_k}+\varphi_{0k}\right). \tag{6.8}$$

As detailed previously, interference is inseparable from a detection by a single detector of multiple fields with similar properties (wavelength and polarization detection). Indeed, if more than two feedback loops are considered, it would require for the various polarization directions between the coherent light beams to satisfy simultaneously $\alpha_j-\alpha_k=\pi/2\ (\mathrm{mod}\pi)\ j,k\in\{1,n\}$. This would be equivalent to guarantee the linear independence of a set of n vectors in a two-dimensional space, which is impossible.

Configuration (2b) has a similar model to that of Configuration (1) because the various wavelengths prevent the existence of interference. However, if the adimensional models are identical, Configuration (2b) has the spectrum of the multiplexed signal $s(t)$ defined over multiple wavelengths. This makes Configuration (2b) similar to a WDM architecture, which is not a major drawback except for security reasons. Indeed, the multiplexing operation being only realized at the RF level, an eavesdropper could devise a spectral attack for which each optical component of $s(t)$ could be independently attacked thanks to the use of frequency filters. Nevertheless, Configuration (1) and (2b) are of great interest to determine the potential of such multiloop architectures for multiplexing purposes. Towards this end, we will start by analyzing the statistical properties of the multiplexed signal $s(t)$ and the existence of orthogonality between its components $s_j(t)$, a desired properties to ensure simple decryption strategies.

6.3 Statistical Properties

In this section, we will analyze from a theoretical and a numerical point of view the properties of an EOO with a single and multiple delayed feedback loops. The statistical and spectral properties of the multiplexed signal $s(t)$, the state variable of the system, and the existence of orthogonality between components $s_j(t)$ are detailed. Before, analyzing the case of multiple loops, we recall known properties of single-loop EOO and see how the theoretical framework of [141] may apply.

6.3.1 Case of a Single Feedback Loop

Systems described by a delay-differential equation (DDE) with a single cosine-square (or cosine) nonlinearity can generate high-dimensional chaos with Gaussian statistics [116]. We propose in this subsection to recall the origins of such statistics (a question thoroughly studied by Dorizzi *et al.* in [141]). They are linked to the fast oscillations

of the cosine-square feedback that destroy the internal correlations on short time scales. Mathematically, the solution of the DDE can be represented under an integral form. For instance with a WCG[1], it reads

$$x\left(t\right)=\int_{t_0}^{t}e^{\frac{-u}{\tau}}\frac{\beta}{\tau}\sin^2(x(t-u-T)+\varphi_0)du. \tag{6.9}$$

In this functional relation, $x(t-T)$ becomes less correlated to $x(t)$ as the feedback function oscillates and when the delay T is large. In this particular situation, the feedback is often referred to as a "random-like driving force". Indeed, the feedback function $f : x(t) \to \beta \sin^2(x(t)+\varphi_0)$ has fast variations such that its values remains correlated only during a single oscillation of f, corresponding to the time for which $x(t)$ varies from an amount $\pi\tau/\beta$. The integral solution and the concept of oscillations of function f are shown in Fig. 6.4(a). It also unveils inhomogeneities in the width of the oscillations, which are due to the irregular variations of $x(t)$. We denote $\varepsilon_k = [t_k, t_{k+1}]$ the length of the kth oscillation. For large values of the nonlinear gain β, the duration of these oscillations becomes smaller and satisfies $|\varepsilon_k| \ll 1$. This allows Eq. 6.9 to be rewritten with the approximation

$$x(t)\approx\sum_{k=0}^{\infty}e^{-\frac{t_k}{\tau}}X_k(t) \text{ with } X_k(t)=\int_{t_k}^{t_{k+1}}\frac{\beta}{\tau}\sin^2\left(x(t-u-T)+\varphi_0\right)du. \tag{6.10}$$

The processes $X_k(t)$ are considered approximately independent and identically distributed (iid). The durations ε_k are supposed to be approximately equal to an average value ε (both are reasonable assumptions when β is large). It was proven that a modified version of the Central-Limit Theorem could be used to prove that $x(t)$ has Gaussian statistics[1] [141].

To the extent of our knowledge, this theory has not been applied to an integro-delay differential system. However, systems such as the ICG also exhibit Gaussian statistics, which is a strong indication that similar mechanisms of destruction of correlation may occur. Indeed, it is possible to give an integral representation for the state variable $x(t)$ of an ICG [174]

$$x\left(t\right)=\int_{t_0}^{t}\left(\frac{1}{\tau}e^{\frac{-u}{\tau}}-\frac{1}{\theta}e^{\frac{-u}{\theta}}\right)\beta\cos^2(x(t-u-T)+\varphi_0)du, \tag{6.11}$$

assuming the characteristic times linked by the following relationship $\theta \gg \tau$ and $t \gg \tau$ to neglect the transient evolution as in [174]. The integral representation of $x(t)$, which is depicted in Fig. 6.4(b), presents remarkable similarities with that of the WCG. By adopting similar notations, we can also consider the state variable $x(t)$ to be an infinite sum of independent stochastic processes:

$$x(t)\approx\sum_{k=0}^{\infty}\left(\frac{e^{-\frac{t_k}{\tau}}}{\tau}-\frac{e^{-\frac{t_k}{\theta}}}{\theta}\right)X_k(t) \text{ with } X_k(t)=\int_{t_k}^{t_{k+1}}\beta\cos^2(x(t-u-T)+\varphi_0)du. \tag{6.12}$$

[1]The WCG is described by an Ikeda-like equation $\tau\dot{x}+x=\beta\sin^2(x(t-T)+\varphi_0)$.

[1]The state variable $x(t)$ is a deterministic value. Nevertheless, it can be considered as stochastic process for the sake of explaining its statistical properties.

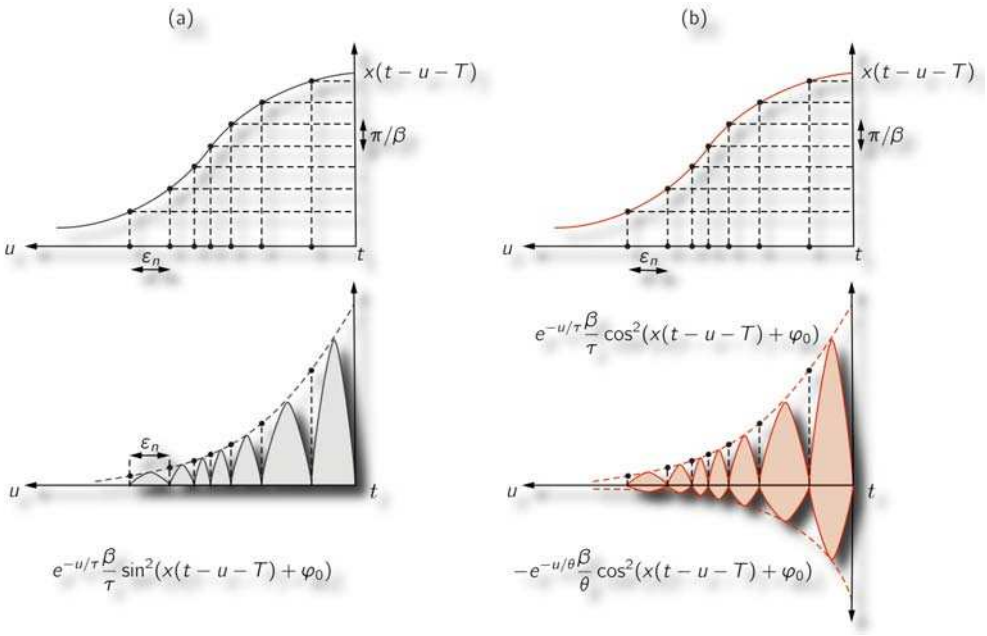

Figure 6.4: Interpretation of the integral solution of (a) a delay differential equation describing a WCG (adapted from [141]) and (b) an integro-delay differential equation of an ICG, in both case with a single feedback loop and a cosine-square nonlinearity. A variation of $x(t-T)$ of π/β achieved in the time interval ε_n is associated with an oscillation of the feedback function. The sum of the gray and red shaded regions represent x at time t for a WCG and an ICG, respectively.

The application of a modified Central-Limit Theorem under similar assumptions to those used in [141] will also lead to the generation of Gaussian statistics. This has been observed both numerically and experimentally.

6.3.2 Case of Multiple Feedback Loops

In our context, the addition of multiple loops is associated with the use of cosine-square nonlinearities with different frequencies of oscillation ω_j, phase shifts φ_{0j}, and time delays T_j ($j = 1, \ldots, n$). In this subsection, we propose to address the question of statistical properties from a qualitative point of view. In the case of configurations (1) and (2) highlighted in the previous section, the nonlinear feedback is composed of a sum of cosine-square functions with possibly cross-product of cosine functions if interference exists in the system. Contrary to the case of single-loop systems, the feedback function is not necessarily periodic[1] but it still presents fast oscillations. The destruction of the correlation is realized at multiple time scales, when the cosine square functions have different frequencies ω_j. As an illustration, we consider a feedback without interference $s(t) = \sum_{j=1}^{n} \beta_j \cos^2(\omega_j x(t-T_j) + \varphi_{0j})$ and identical time delays ($T_j = T$ for all j). Assuming the product of frequencies and nonlinear gains are ordered $\omega_1\beta_1 > \cdots > \omega_n\beta_n$, when $x(t-T)$ varies from an amount $\pi/\omega_1\beta_1$, the function $\beta\cos^2(\omega_1 x(t-T)+\varphi_{01})$ oscillates once, thus destroying the correlation existing between $x(t)$ and $x(t-T)$. Meanwhile, the other nonlinear functions oscillate

[1]The sum of two periodic function does not result in a periodic function.

$\left\lfloor \frac{\omega_j \beta_j}{\omega_1 \beta_1} \right\rfloor$ times, destroying at finer time scales the existing correlations. Consequently, if we consider time intervals $\varepsilon_k = [t_k, t_{k+1}]$ ($k \in \mathbb{N}$) for which $x(t)$ varies from $\pi/\beta\omega_1$, then the processes $X_k(t) = \int_{t_k}^{t_{k+1}} s(t-u)du$ can be considered statistically independent.

An equation similar to Eq. 6.12 can be used to theoretically guarantee the existence of Gaussian statistics for systems with multiple loops. When multiple time delays are considered, a similar approach can be used as well. The nonlinear feedback function under consideration still acts similar to a random-like driving force, when the nonlinear gains β_j are sufficiently large. Figure 6.5 shows this property with two nonlinearities. Numerical simulations confirm the first theoretical conjectures; they reveal a time series [Fig. 6.5(a)] with an approximately Gaussian probability density function (pdf) for $x(t)$ [Fig. 6.5(b)] in the case of an EOO with two feedback loops and no interference. When interference exists in the feedback, its oscillating properties qualitatively change (the modified Central-Limit theorem cannot be rigorously applied anymore), thus inducing distribution with an imperfect Gaussian shape, especially if the number of loops and the values of β_j and ω_j are not large enough. Nevertheless, it is still possible to ensure approximate Gaussian statistics, as plotted in Fig. 6.5(c)-(d), in which we have simulated Configuration (2a) with four feedback loops and interference.

Next, we investigate the internal correlations existing within $x(t)$ and $s(t)$ in the case without interference with two feedback loops ($T_1 = T_2$, and $\beta_1 = \beta_2$). We define their normalized autocovariance functions by $\rho_{xx}(u) = \Gamma_{xx}(u)/\Gamma_{xx}(0) =$

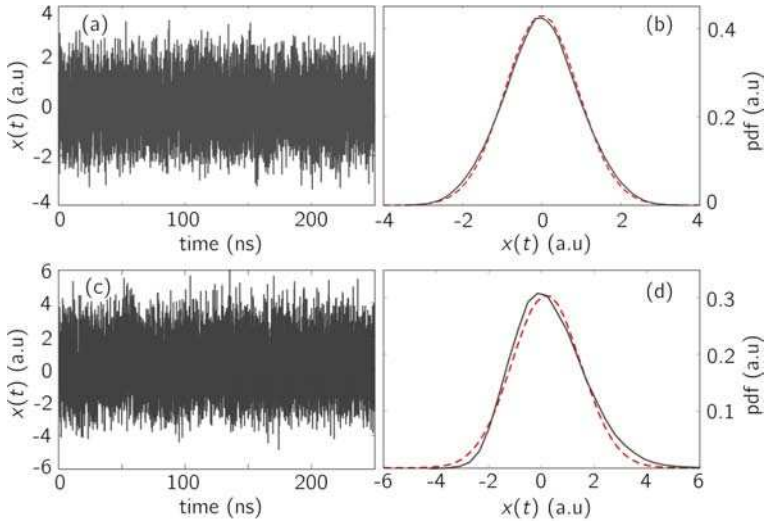

Figure 6.5: (a)-(b) Time series of $x(t)$, (c)-(d) probability density function of $x(t)$ (gray solid line) with a variance and the corresponding theoretical Gaussian distribution with identical mean and variance (red solid line), in the case of an EOO in Configuration (1) or (2b) with two feedback loops without interference (a)-(b) and with four feedback loops with interference (c)-(d). In (a)-(b), parameters are $\tau = 25$ ps, $\theta = 5$ μs, $T_1 = T_2 = 30$ ns, $\beta_{i|i=1,2} = 5$, $\varphi_{0i|i=1,2} = -\pi/4$, $\omega_2 = 2\omega_1 = 2$, and time step $\Delta t = 5$ ps. In (c)-(d), parameters are $\tau = 25$ ps, $\theta = 5$ μs, $T_j = 30 + 15(j-1)$ ns, $\beta_j = 5$, $\varphi_{0j} = -\pi/4$, $\omega_j = 1 + 2(j-1)$, $C_{ij} = \cos((i-j)\frac{\pi}{4})$ with $i \neq j = 1, \ldots, 4$.

$\langle (x(t) - \langle x \rangle)(x(t+u) - \langle x \rangle) \rangle / \langle (x(t) - \langle x \rangle)^2 \rangle$ and $\rho_{ss}(u) = \Gamma_{ss}(u)/\Gamma_{ss}(0) = \langle (s(t) - \langle s \rangle)(s(t+u) - \langle s \rangle) \rangle / \langle (s(t) - \langle s \rangle)^2 \rangle$ where $\langle \cdot \rangle$ denotes the time average. The normalized autocovariance $\rho_{xx}(u)$ decreases exponentially fast [Fig. 6.6(c)] as a consequence of $x(t)$ being a filtered version of $s(t)$. It also reveals typical correlation revivals at lags equal to multiple of the time delay T (because of the values of β we used), see Fig. 6.6(a).

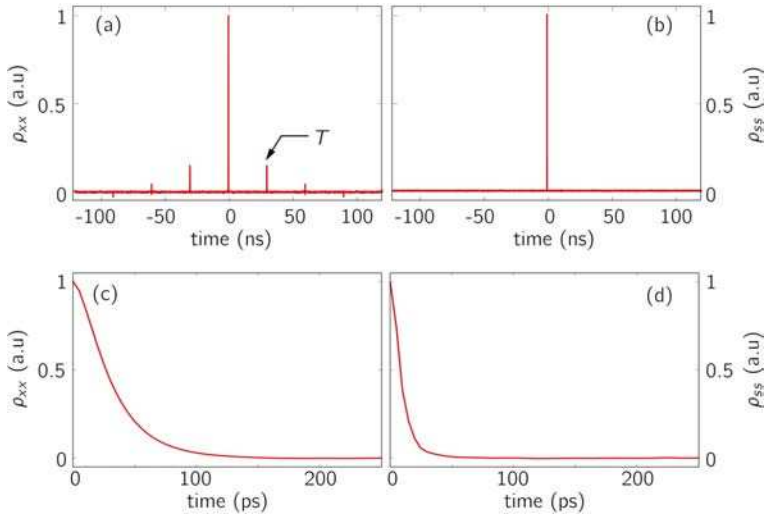

Figure 6.6: Normalized autocovariance functions ρ_{xx} and ρ_{ss} of $x(t)$ in (a) and $s(t)$ in (b), respectively. A zoom of their behavior in the vicinity of the zero lag is provided in (c) and (d), respectively. The parameters for the simulation are $\tau = 25$ ps, $\theta = 5$ μs, $T_1 = T_2 = 30$ ns, $\beta_{i|i=1,2} = 5$, $\varphi_{0i|i=1,2} = -\pi/4$, $\omega_2 = 2\omega_1 = 2$, and time step $\Delta t = 5$ ps.

The multiplexed signal $s(t)$ looses its memory faster than $x(t)$ and may be considered approximately white, $\rho_{ss}(u)$ going to zero in approximately 25 ps and remaining totally flat except for the lag $u = 0$ [see Fig. 6.6(b)] and the associated zoom [see Fig. 6.6(d)].

These results demonstrate that an EOO with multiple delayed cosine-square feedback nonlinearities with different frequencies of oscillation bares similar statistical and spectral features to those of an EOO with a single delayed feedback, especially when no interference exists in the feedback term. These properties will be later exploited for the derivation of signals to carry the digital messages associated with the various users Alice$_j$ $(j = 1, \ldots, n)$.

6.4 Orthogonality

Orthogonality is studied between the various components comprising the multiplexed signal $s(t)$, which will be used as chaotic codes for the transmission of messages. In this section, we restrict ourselves to a feedback signal without interference, such as in Configurations (1) and (2b). Each code is an optical signal that propagates in its optical loop and is defined by $s_j(t) = \beta_j \cos^2(\omega_j x_T + \varphi_{0j})$ $(j = 1, \ldots, n)$. To guarantee a reasonable level of security, we consider that all these codes have approximately the same variance, which consists of using identical nonlinear gains ($\beta_j = \beta$). Indeed,

with identical variance for the codes, we prevent a potential eavesdropper to identify the presence of multiple carriers in the multiplexed signal $s(t)$. We propose to employ these chaotic codes to transmit multiple messages. Our approach will be similar to CDMA except that the codes are time-dependent chaotic waveforms that change for every transmitted bit (or symbol) of duration T_b. Furthermore, to ensure a linear computational complexity for the decryption, the generated chaotic codes have to be *orthogonal* at all times. In this section, we provide analytical and numerical insight on this issue before devising strategies of encryption and decryption.

6.4.1 Analytical Results

We make the assumption that the state variable of the EOO with multiple feedback is a Gaussian random variable.[1] We consider that the length or duration of the code T_b is such that it is possible to assimilate the calculations over an infinite time duration with those on T_b. We consider two codes $s_i(t) = \beta\cos^2(\omega_i x(t-T_i)+\varphi_{0i})$ and $s_j(t) = \beta\cos^2(\omega_j x(t-T_j)+\varphi_{0j})$. Our objective is to calculate the crosscovariance between them. The crosscovariance is defined as

$$\begin{aligned}\Gamma_{s_i s_j} &= \left(s_i(t)-\langle s_i\rangle\right)\left(s_j(t)-\langle s_i\rangle\right), &(6.13)\\ &= \langle s_i(t)s_j(t)\rangle - \langle s_i\rangle\langle s_j\rangle, &(6.14)\end{aligned}$$

with $\Gamma_{s_i s_j} = \Gamma_{s_i s_j}(0)$. From Section 6.3, we assume that $x(t)$ is purely Gaussian at every time scale with mean $m_x = 0$ and variance σ_x^2. We define its characteristic function:

$$\psi_x(u) = e^{im_x u - 1/2\sigma_x^2 u^2}. \tag{6.15}$$

By stationarity of the process $x(t)$, the variable $x_{T_i} = x(t-T_i)$ and $x(t)$ will have the same statistical properties.

We evaluate first $\langle s_i\rangle$:

$$\begin{aligned}\langle s_i\rangle &= \left\langle \beta\cos^2\left(\omega_i x_{T_i}+\varphi_{0i}\right)\right\rangle,\\ &\overset{(a)}{=} \left\langle \frac{\beta}{2}(1+\cos\left(2\omega_i x_{T_i}+2\varphi_{0i}\right)\right\rangle,\\ &\overset{(b)}{=} \frac{\beta}{2}+\frac{\beta}{2}\mathbb{E}\left(\cos\left(2\omega_i x_{T_i}+2\varphi_{0i}\right)\right),\\ &\overset{(c)}{=} \frac{\beta}{2}+\frac{\beta}{2}\,\mathrm{Re}\left(\psi_x(2\omega_i)e^{i2\varphi_{0i}}\right),\\ \langle s_i\rangle &= \frac{\beta}{2}\left(1+\cos 2\varphi_{0i}e^{-2\sigma_x^2\omega_i^2}\right). &(6.16)\end{aligned}$$

(a) comes from the power reduction formula: $\cos^2(x) = 1/2(1+\cos(2x))$; (b) comes from the ergodicity of $x(t)$ (or $x(t-T_i)$) and the linearity of the expectancy operator $\mathbb{E}(\cdot)$; (c) comes from the characteristic function $\psi_x(u)$ of a random variable.

[1] The state variable is a deterministic quantity with respect to our physical model. However, in a first approximation it is considered as a random variable for the analytical calculations to be tractable.

We consider the least favorable case for the decorrelation of the chaotic codes, meaning $T_i = T_j = T$ for all i, j. Then, we calculate the analytical expression of $\langle s_i(t), s_j(t)\rangle$ using 1D statistics:

$$\begin{aligned}
\langle s_i(t), s_j(t)\rangle &= \mathbb{E}\left(s_i(t)s_j(t)\right), \\
&= \beta^2\mathbb{E}\left(\cos^2(\omega_i x_{T_i} + \varphi_{0i})\cos^2(\omega_j x_{T_j} + \varphi_{0j})\right), \\
\langle s_i(t), s_j(t)\rangle &= \frac{\beta^2}{8}\left(\cos(2\varphi_{0i} + 2\varphi_{0j})e^{-2(\omega_i+\omega_j)^2\sigma_x^2} + \cos(2\Delta\varphi_{0ij})e^{-2\Delta\omega_{ij}^2\sigma_x^2}\right), \\
&\quad + \frac{\beta^2}{4}\left(1 + \cos 2\varphi_{0i}e^{-2\omega_i^2\sigma_x^2} + \cos 2\varphi_{0j}e^{-2\omega_j^2\sigma_x^2}\right). \qquad (6.17)
\end{aligned}$$

The same steps to those of the derivation of $\langle s_i\rangle$ were used: ergodicity of $x(t)$, power reduction formula, trigonometric identities, and the linearity of $\mathbb{E}(\cdot)$.

It is finally possible to derive the expression of the cross-covariance between two different codes by combining the expressions of Eqs. 6.16 and 6.17. It reads:

$$\begin{aligned}
\Gamma_{s_i s_j} &= \frac{\beta^2}{8}\left(1 - e^{-4\omega_i\omega_j\sigma_x^2}\right) \times \\
&\quad \left(\cos(2\Delta\varphi_{0ij}) + \cos(2\varphi_{0i} + 2\varphi_{0j})e^{-4\omega_i\omega_j\sigma_x^2}\right)e^{-2\Delta\omega_{ij}^2\sigma_x^2}. \qquad (6.18)
\end{aligned}$$

The analytical expression of the cross-covariance shows that

$$\Gamma_{s_i s_j} \underset{\Delta\omega_{ij}\to\infty}{\sim} \frac{\beta^2}{8}\cos 2\Delta\varphi_{0ij}e^{-2\Delta\omega_{ij}^2\sigma_x^2}, \qquad (6.19)$$

if we assume that all the parameters are fixed except for $\Delta\omega_{ij}$. As a consequence, when the frequency detuning $\Delta\omega_{ij}$ increases the correlation between two given chaotic codes tends to decrease exponentially fast.

The nonlinear gain β appears explicitly as a multiplicative factor in $\Gamma_{s_i s_j}$ and implicitly in the expression the variance $\sigma_x^2 \propto \beta^2$. (A parabolic dependence is observed similar to [141]). By denoting c_β the proportionality coefficient, we end up with

$$\Gamma_{s_i s_j} \underset{\beta\to\infty}{\sim} \frac{\beta^2}{8}\cos 2\Delta\varphi_{0ij}e^{-2\Delta\omega_{ij}^2 c_\beta\beta^2}. \qquad (6.20)$$

Since the increase (or decrease) of an exponential function is faster than any polynomial function ($\lim_{\beta\to\infty}\beta^n e^{-\beta^2} = 0$), hyperchaotic regimes generate by large values of β also leads to better orthogonality between the chaotic codes at fixed detuning. Another tunable parameter that can ensure orthogonality is the relative phase shift $\Delta\varphi_{0ij} = \varphi_{0i} - \varphi_{0j}$ and respective phase of each chaotic code. They are involved in the cross-covariance expression through the multiplicative factor $\cos(2\Delta\varphi_{0ij}) + \cos(2\varphi_{0i} + 2\varphi_{0j})e^{-4\omega_i\omega_j\sigma_x^2}$. It is possible to ensure perfect orthogonality between the codes when each term in this sum is equal to zero, leading to $\Delta\varphi_{0ij} = (2p+1)\pi/4$ and $\varphi_{0i} + \varphi_{0j} = (2p+1)\pi/4$ with $p \in \mathbb{Z}$. This equalities can make only two codes to be orthogonal, but it does not ensure orthogonality of a set of codes of arbitrary large cardinality. Therefore, the phase shift $\Delta\varphi_{0ij}$ is not the most an appropriate parameter to ensure orthogonality compared to the detuning in frequencies of oscillation $\Delta\omega_{ij}$.

Finally, the duration T_b also plays a fundamental role in achieving orthogonality, defined with cross-covariance measurements. Therefore, obtaining a soundable cross-covariance estimation requires the two chaotic codes (s_i,s_j) to fluctuate sufficiently enough, in other terms T_b should be greater than several times the maximum decorrelation time of the two chaotic codes. In addition to that and because the chaotic codes are both seeded by the same $x(t)$, each code can exhibit different evolutions only if $x(t)$ also fluctuates sufficiently enough. Quantitatively, we have noticed that it is not possible to rely on cross-covariance measurements if T_b is smaller than approximately twice the decorrelation time of $x(t)$.

In conclusion, this analytical study has demonstrated the existence of a particular set of parameters that guarantees the various codes $s_j(t)$ to be orthogonal with each other, the role of the frequency detuning $\Delta\omega_{ij}$ being crucial. In the following subsection, we propose a numerical investigation to supports our theoretical findings.

6.4.2 Numerical Results

The orthogonality is studied as a function of the frequency detuning $\Delta\omega_{ij} = \omega_i - \omega_j$, the nonlinear gain β, the relative phase difference $\Delta\varphi_{0ij} = \varphi_{0i} - \varphi_{0j}$ with a short bit duration T_b. To numerically evaluate the orthogonality, we consider the normalized cross-covariance coefficient

$$\rho_{s_i s_j} = \Gamma_{s_i s_j} / (\Gamma_{s_i s_i} \Gamma_{s_j s_j})^{1/2}, \tag{6.21}$$

calculated on a finite period T_b. To ensure that orthogonality exists for all times with the time-varying codes, we repeat and average the cross-covariance measures over $5000T_b$. Figure 6.7 plots $|\rho_{s_i s_j}|$ for a bit duration $T_b = 0.4$ ns (the bit duration

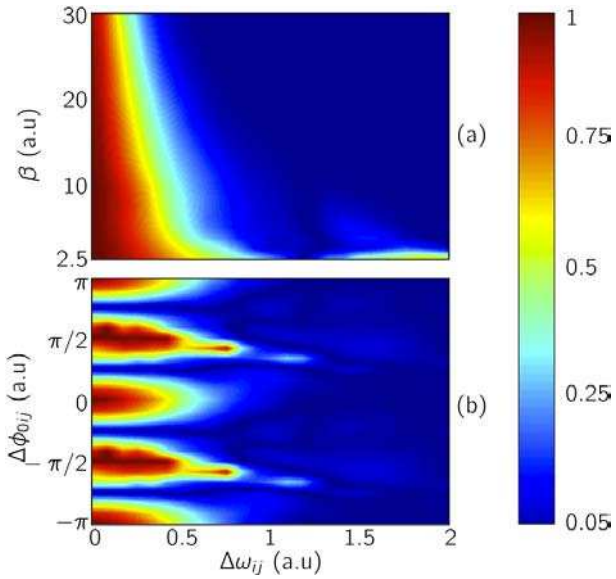

Figure 6.7: Evolution of correlation coefficient $\rho_{s_{\omega_i} s_{\omega_j}}$ in parameter space $(\Delta\omega_{ij}, \beta)$ in (a) and in $(\Delta\omega_{ij}, \Delta\varphi_{0ij})$ with $\beta = 5$, $T = 30$ ns in (b) for $T_b = 0.4$ ns. The results are averaged over $5000T_b$. The other parameters are identical to those of Fig. 6.5

in the OC-48 standard) in two different parameter planes $(\Delta\omega_{ij}, \beta)$ in Fig. 6.7(a), and $(\Delta\omega_{ij}, \Delta\varphi_{0ij})$ in Fig. 6.7(b). Figure 6.7(a) maps $|\rho_{s_i s_j}|$ with $\Delta\varphi_{0ij} = 0$ and shows the dependence of orthogonality on the nonlinear gain β. Indeed, the frequencies of oscillations of the nonlinear functions satisfy $\pi/\beta\omega_{i,j}$, which makes the code correlated enough at weak values of β even if the detuning is significant. It also shows that orthogonality becomes almost perfect when the nonlinear gain is strong enough and the detuning sufficiently large, as forecasted by the analytical results (calculated under the assumption that $T_b \to \infty$). However, when setting aside the frequency detuning $\Delta\omega_{ij}$, the relative phase shift $\Delta\varphi_{0ij}$ could also be advantageously used to generate independent codes. That is why we mapped the evolution of $|\rho_{s_i s_j}|$ in $(\Delta\omega_{ij}, \Delta\varphi_{0ij})$ with $\beta = 5$ to ensure a hyperchaotic regime. Figure 6.7(b) shows only four narrow zones of orthogonality when $\Delta\omega_{ij} = 0$. They become wider as the detuning is increased and ultimately lead to almost perfect orthogonality at any point of the parameter space $(\Delta\omega_{ij}, \Delta\varphi_{0ij})$. At zero detuning, the cross-covariance between two different codes is maximum for a phase shift $\Delta\varphi_{0ij} = k\pi/2$, $k \in \mathbb{N}$, leading to the striped zones. Their existence is related to the construction of the codes that satisfy $s_{i|\omega_i,\varphi_{0i}} = s_{i|\omega_i,\varphi_{0i}+k\pi/2}$, thus explaining the stripes at zero detuning. These two analyses confirm that one of the most interesting parameter, which easily ensures orthogonality between two arbitrary codes $s_i(t)$ and $s_j(t)$, is the frequency detuning $\Delta\omega_{ij}$.

In conclusion, the numerical findings support the theoretical results highlighted in the previous subsection. We have a guarantee that almost-perfect orthogonality is achievable with the proper set of parameters even on short durations ($T_b = 0.4$ ns). This makes the codes restricted to this time interval suitable carriers to be digitally modulated and convey independently various messages. The strategies to encrypt and decrypt information will be detailed in the next section.

6.5 Multiplexing of Information

In this section, we describe how messages can be encrypted and decrypted. A first decryption strategy makes use of orthogonality and covariance measurements, then we devise a decryption method based on covariance or least-square optimization, when orthogonality is not satisfied but linear independence is still ensured between the various codes. These methods are tailor-made for Configurations (1) and (2b) but inadequate if interference exists in the multiplexed feedback signal $s(t)$. As a consequence, we detailed how decryption could be achieved in Configuration (2a), where interference constitutes a major challenge as they couple the square-roots of the codes s_j together.

6.5.1 Architecture & Chaos Synchronization

We consider two EOOs: an emitter (E) and a receiver (R) that are subjected to an identical driving signal $s(t)$, but delayed by the transmission time T_c in the case of R.

The equations of the chaotic transmission chain read

$$\tau \dot{x}_E(t) + x_E(t) + \frac{1}{\theta}\int_{t_0}^{t} x_E(s)ds = s(t), \tag{6.22}$$

$$\tau \dot{x}_R(t) + x_R(t) + \frac{1}{\theta}\int_{t_0}^{t} x_R(s)ds = s(t - T_c). \tag{6.23}$$

This transmission chain constitutes an active-passive decomposition (APD). The left-hand sides of Eqs. A.30-A.31 are typical of second-order damped oscillators. This architecture is depicted in Fig. 6.8 for Configuration (2a) and two feedback loops.

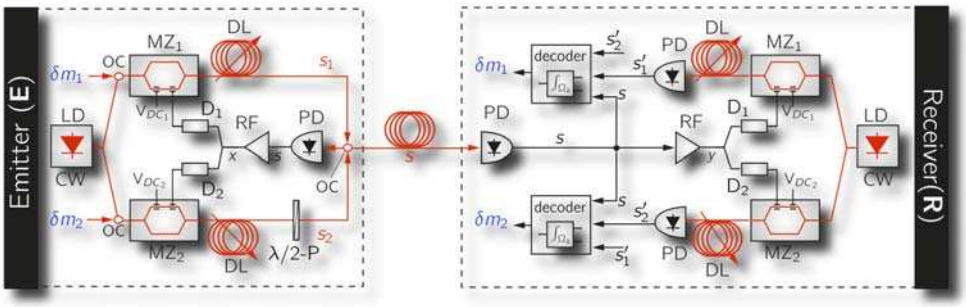

Figure 6.8: Chaotic CDMA transmission chain using for the emitter (E) and receiver (R) a single optoelectronic oscillator with two feedback loops and a single photodetector in the case of Configuration (2a). The structure of the decoding box depends on the presence of interferences or not. LD: laser diode, $\mathrm{MZ}_{j=1,2}$: Mach-Zehnder modulator, $\mathrm{DL}_{j=1,2}$: optical delay line, $\lambda/2$: halfwavelength plate, OC: optical coupler, PD: photodetector, RF: band-pass amplifier, $\mathrm{D}_{j=1,2}$: voltage divider ensuring reduction factor $g_{j=1,2} < 1$, $m_{j=1,2}$: messages to be encrypted.

By translating the time reference frame of (E) by T_c, the dynamics of the lagged-synchronization error $e_{T_c}(t) = y(t) - x(t - T_c)$ can be derived:

$$\tau \dot{e}_{T_c}(t) + e_{T_c}(t) + \frac{1}{\theta}\int_{t_0}^{t} e_{T_c}(s)ds = 0, \tag{6.24}$$

and equivalently represented by the damped oscillator

$$\ddot{e}_{T_c}(t) + 2\lambda\omega_0 \dot{e}_{T_c}(t) + \omega_0^2 e_{T_c}(t) = 0 \text{ with } \begin{cases} 2\lambda\omega_0 = \dfrac{1}{\tau}, \\ \omega_0^2 = \dfrac{1}{\theta\tau}. \end{cases} \tag{6.25}$$

This proves the asymptotic convergence to zero of the synchronization error and guarantees chaos synchronization between (E) and (R) for any set of parameters. This is of paramount importance to guarantee that the receiver can reproduce the chaotic code and ultimately decrypt the various messages.

6.5.2 Encryption

To encrypt her message, each user Alice_j ($j \in [\![1, N]\!]$) modulates digitally the non-linear gain β of its associated code $s_j(t)$ during the time T_b. Typically, in secure

chaos-based communication, the modulation depth is taken small with respect to the amplitude of the chaotic signal to prevent any direct recovery from the observation of the multiplexed signal $s(t)$. Moreover, in our there has to be an upper limit on the modulation depth to preserve orthogonality and thus message decoding. Mathematically, the digital data stream $m_j(t)$ is composed of a series of bits $m_j^{(k)} \in \{-1; 1\}$ such that

$$m_j(t) = \sum_{k=0}^{\infty} m_j^{(k)} rect(t - kT_b), \tag{6.26}$$

with $rect(t - kT_b) = H(t - kTb) - H(t - (k + 1)T_b)$ and H the Heaviside function. These messages are finally embedded in the multiplexed feedback signal $s(t)$ that becomes

$$s(t) = \sum_{j=1}^{n} \beta_j (1 + \delta m_j(t)) \cos^2 (\omega_j x_T + \varphi_{0j}), \tag{6.27}$$

with δ a multiplicative factor that satisfies $|\delta| \ll 1$. In practice, this modulation can be realized by the adjunction of an additional amplitude modulator in each optical arm, between the CW laser source and the Mach-Zehnder modulator MZ_j.

The gain modulation of the codes, which have a very large bandwidth and linear statistical independence or orthogonality (for a proper choice of parameters), is similar to digital modulation and spread-spectrum techniques encountered in CDMA [21]. Consequently, analogous strategies of decryption based on covariance measurements can be inferred in our context, as illustrated in the following subsection.

6.5.3 Decryption without Interferences

Various decryption approaches are presented in this section. They all exploit the statistical independence (partial or quasi-total) between the various chaotic codes $s_j(t)$ composing the randomly multiplexed feedback term $s(t)$. At the receiving end, each legitimate user Bob_j will generate a copy of the code employed by Alice_j to recover a targeted information. We denote this code's duplicate $s'_j(t) = \beta \cos^2(\omega_j x_R(t - T) + \varphi_{0j})$

6.5.3.1 Decryption by Covariance

This methods relies on the calculation of cross-covariance between each duplicated code s'_i and the multiplexed signal $s(t)$.

$$\begin{aligned}
\Gamma_{ss'_i} &= \left\langle \left(s(t) - \langle s \rangle\right) \left(s'_i(t) - \left\langle s'_i \right\rangle\right) \right\rangle, \\
&\overset{(a)}{=} \sum_{j=1}^{N} (1 + \delta m_j(t)) \langle \left(s_j(t) - \langle s_i \rangle\right) \left(s'_i(t) - \left\langle s'_i \right\rangle\right) \rangle, \\
\Gamma_{ss'_i}(0) &= \sum_{j=1}^{N} (1 + \delta m_j(t)) \Gamma_{s_j s'_i}.
\end{aligned}$$

Now, if we assume E and R to be chaotically synchronized, it implies the code s_i and its duplicates s'_i to be equal. Consequently, the cross-covariance becomes

$\Gamma_{ss'_i} = \sum_{j=1}^{N}(1+\delta m_j(t))\Gamma_{s'_j s'_i}$. The cross-covariance between $s(t)$ and s'_i can be expressed in terms of the cross-covariance $\Gamma_{s'_j s'_i}$ of the duplicated codes generated by the various Bobs. This expression offers to the legitimate users Bobs two possibilities: (i) decrypting their own message independently from the evolution of others or (ii) decrypting jointly all the messages at every bit period T_b.

The first approach requires that the decorrelation or orthogonality between the various codes is strong enough to neglect the contribution of other users, meaning that $|\Gamma_{s'_j s'_i}| \ll |\Gamma_{s'_i s'_i}|$. This leads to an approximate expression of $\Gamma_{ss'_i}$, where the contribution of all the messages $m_j(t)$ $(j \neq i)$ can be neglected: $\Gamma_{ss'_i} \simeq (1+\delta m_i(t))\Gamma_{s'_i s'_i} + \sum_{j=1, j\neq i}^{N}\Gamma_{s_j s'_i}$. Finally the approximate decoding equation reads:

$$\delta m_i(t) \simeq \frac{1}{\Gamma_{s'_i s'_i}}\left(\Gamma_{ss'_i} - \sum_{j=1}^{N}\Gamma_{s'_j s'_i}\right). \tag{6.28}$$

Equation 6.28 is similar to that in [19] except that we are considering autocovariance and not autocorrelation. We demonstrate numerically in Fig. 6.9 that it is possible to transmit two data streams at 2.5 Gbit/s (OC-48 standard) with Configuration (2a). In the simulations, we have chosen $\delta = 1/32$, which does not significantly disturb the multiplexed signal waveforms (good concealment) and the value of the nonlinear gain of each chaotic code (quasi-perfect orthogonality guaranteed). Furthermore, to avoid the appearance of interference, the polarization of the optical field of the two loops are set to be orthogonal (a half-wavelength plate is inserted in one optical arm).

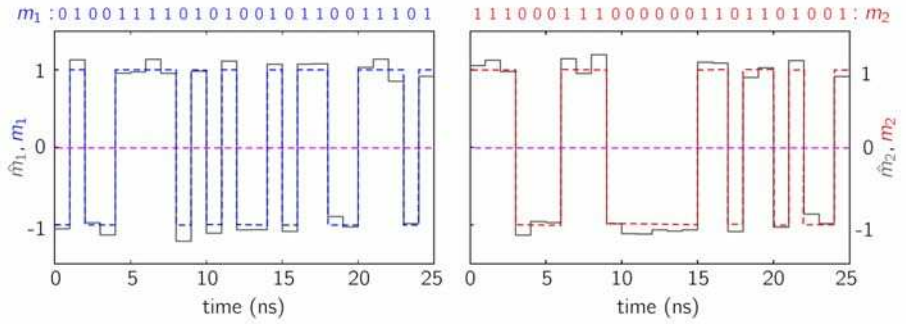

Figure 6.9: Numerical simulation of a multiplexed transmission two different messages for the simultaneous transmission of two binary messages at 2.5 Gbit/s (OC-48 standard) per user. The purple dashed line indicates the threshold used to discriminate different bit values. the dashed and solid lines represent the encrypted and decrypted messages, respectively. The simulation's parameters are $\beta_{i|i=1,2} = 5$, $\varphi_{0i|i=1,2} = -\pi/4$, $\theta = 10$ μs, $\tau = 25$ ps, $T = 30$ ns, $\Delta\omega_{12} = 2$, and $\delta = 1/32$.

It requires to neglect the messages sent by Alice$_{j\neq i}$. If they were not neglected, then the left hand of the decoding equation would be written as

$$\delta m_i(t)\,(1+\lambda_{ij}) \;\text{ with }\; \lambda_{ij} = \sum_{j=1, j\neq i}^{N}\frac{m_j(t)\Gamma_{s'_j s'_i}(0)}{m_i(t)\Gamma_{s'_j s'_i}(0)}. \tag{6.29}$$

Equation 6.29 shows the effect of other messages and their associated spreading codes (m_j and s_j, respectively). To ensure a systematic error-free decryption it is important to guarantee that the factor λ_{ij} will not affect the sign of the decrypted message. This naturally imposes the condition $|\lambda_{ij}| < 1$, which by triangular inequalities leads to a sufficient (weaker) condition

$$\sum_{i \neq j} \frac{\left|\Gamma_{s'_i s_j}\right|}{\left|\Gamma_{s'_i s_i}\right|} < 1. \tag{6.30}$$

This ensures an error-free decryption of Alice$_i$'s message and also gives an upper bound for the number of users who can transmit simultaneously decodable messages.[1]

One may see orthogonality and the decryption strategy as limiting design constraints. They can be alleviated, but they will ultimately result in an increase in computational complexity for the decryption. It is still possible to decrypt the message while keeping the contributions of the various Alices. Therefore, the various cross-covariance $\Gamma_{ss'_j}$ $(j = 1, \ldots, N)$ are now related by the linear system

$$\begin{pmatrix} \vdots \\ \Gamma_{ss'_i} \\ \vdots \end{pmatrix} = \begin{pmatrix} & \vdots & \\ \cdots & \Gamma_{s'_i s_j} & \cdots \\ & \vdots & \end{pmatrix} \begin{pmatrix} \vdots \\ 1 + \delta m_i(t) \\ \vdots \end{pmatrix}, \tag{6.31}$$

which is written in the condensed form $\mathbf{y} = \Gamma(\mathbf{1} + \delta\mathbf{m})$ with $\mathbf{m}, \mathbf{1}, \mathbf{y} \in \mathbb{R}^N$ and $\Gamma \in \mathscr{M}_{N,N}(\mathbb{R})$, the covariance matrix. In this new framework, one has to invert the covariance matrix to retrieve the various messages. This matrix is square, real valued, and symmetric; therefore it is diagonalizable in an orthonormal basis. If the N codes are orthogonal (or quasi-orthogonal), then the covariance matrix is already diagonal and invertible, the general decoding equation Eq.6.31 degenerates into Eq. 6.28. Orthogonality between codes $\{s_j\}_{j\in[1,n]}$, however, is not necessary to retrieve the various messages without error. Linear independence, a weaker constrain, is sufficient to avoid the existence of null eigenvalue that will prevent the inversion of Γ. In our context, this gives more flexibility for the choice of parameters of the chaotic codes. Finally, the generalized decoding equation reads

$$\delta\mathbf{m} = \Gamma'^{-1}(\mathbf{y}) - \mathbf{1}, \tag{6.32}$$

with Γ' the covariance matrix calculated with the duplicated codes $s'j(t)$. The computational complexity of the decryption is that of the inversion of a square matrix of size N, which is $O(N^3)$ if a Gauss-Jordan elimination is used. The complexity becomes polynomial.

6.5.3.2 Decryption by Least-Square Optimization

Another method to decrypt the various data consists of a least-square regression. This method allows for all the messages of various users to be retrieved at once. The

[1] Equations 6.29-6.30 are derived following the method described in [19]. Their mathematical expressions are similar to those of [19], except that covariance functions are used instead of correlation functions.

method is pretty similar to the previous one, except that the matrices and vectors involved are different. In this approach, we consider that we have at our disposal N_b samples every time-slots for which a bit is encoded.

$$\begin{aligned}
\mathbf{s} &= \begin{pmatrix} s^{(0)} & \cdots & s^{(N_b-1)} \end{pmatrix}^T, && (6.33)\\
&= \begin{pmatrix} \sum_{j=1}^{N}(1+\delta m_j)s_i^{(0)} & \cdots & \sum_{j=1}^{N}(1+\delta m_j)s_j^{(N_b-1)} \end{pmatrix}^T, && (6.34)\\
&= \begin{pmatrix} s_1^{(0)} & \cdots & s_N^{(0)} \\ \vdots & \ddots & \vdots \\ s_1^{(N_b-1)} & \cdots & s_N^{(N_b-1)} \end{pmatrix} (\mathbf{1}+\delta\mathbf{m}), && (6.35)\\
&= \mathbf{H}\,(\mathbf{1}+\delta\mathbf{m}), && (6.36)
\end{aligned}$$

with $\mathbf{s} \in \mathbb{R}^{N_b}$, $\mathbf{1}, \mathbf{m} \in \mathbb{R}^N$ and $\mathbf{H} \in \mathscr{M}_{N_b,N}(\mathbb{R})$. Similarly to susbection 6.5.3.1, the codes generated by the Alices are replaced in $\mathbf{H}$ by their duplicate generated by the Bobs (this is possible due to the chaos synchronization between (E) and (R)). We denotes $\mathbf{H}'$ this matrix with duplicated codes. Contrary to Eq. 6.32, Matrix $\mathbb{H}'$ is not square in general and therefore not invertible. This is the standard problem of least-square regression that can be solved by considering the pseudo inverse of $\mathbf{H}'$ (which exists if $rank(\mathbf{H}') = N$). The decoding equation finally reads

$$\delta\mathbf{m} = \left(\mathbf{H}'^T\mathbf{H}'\right)^{-1}\mathbf{H}'\mathbf{y} - \mathbf{1}. \tag{6.37}$$

This methods has similar level of complexity to that of Eq. 6.32 and is not bounded in terms of number of users, as long as linear independence is achieved for the sampled chaotic codes. With this method, we also manage to achieve transmission at 2.5 Gbit/s with a number of users comparable to that of the covariance-based decryption method.

The various decryption strategies highlighted in the previous subsection are efficient only if interference does not exist within the multiplexed signal $s(t)$ as in Configurations (1) and (2b). In the case of Configuration (2a), however, a new decoding equation must be determined, as illustrated in the following subsection.

6.5.4 Decryption with Interferences

In this subsection, we detail a possible strategy to decrypt multiple data streams, when Configuration (2a) is under consideration. This configuration is ideal for optical communications and uses a single wavelength (thus ensuring optical spectrum efficiency). However, the presence of interference makes the previous decryption strategies unusable. Therefore, we have to devised decryption techniques adapted to this specific configuration. In Configuration (2a), the message inclusion is similar to that of Fig. 6.8 (optical injection of each message in the separate arms) and the

multiplexed signal becomes

$$s(t) = \sum_{j=1}^{n} (1+\delta m_j)\beta_j \cos^2(\omega_j x_{T_j} + \varphi_{0j}) + \sum_{1\leqslant j,k\leqslant n} C_{jk}\sqrt{\beta_j\beta_k(1+\delta m_j)(1+\delta m_k)}\cos(\omega_j x_{T_j}+\varphi_{0j})\cos(\omega_k x_{T_k}+\varphi_{0k}), \tag{6.38}$$

with $|\delta| \ll 1$ and $x_{T_{j,k}} = x(t - T_{j,k})$. Similar to the case without interferences (Configurations (1) and (2b)), the multiplexed signal is used to synchronize an emitter and a receiver, and Bob_i can generate at the receiving end the duplicated codes $s'_i = \beta_i \cos^2(\omega_i y_{T_i} + \varphi_{0i})$. Interference creates a natural crosstalk between the various messages, making the decoding equation 6.28 inefficient, even when the carrier $\{s_i\}_{i\in[\![1,n]\!]}$ is a set of orthogonal signals. Here, we propose a modified decoding equation to decrypt accurately each message. We first introduce the set of root-square codes $\{r_i\}_{i\in[\![1,n]\!]}$ defined by:

$$r_i = \sqrt{\beta_i}\cos(\omega_i x_{T_i} + \varphi_{0i}). \tag{6.39}$$

At the receiving end, Bob_i will perform the crosscovariance measure between his generated waveform and the multiplexed signal s:

$$\begin{aligned}
\Gamma_{ss'_i} &= \sum_{k=1}^{n}(1+\delta m_k)\Gamma_{s_k s'_i} + \sum_{1\leqslant j,k\leqslant n} C_{jk}\sqrt{(1+\delta m_j)(1+\delta m_k)}\Gamma_{r_k r_j s'_i}, &(6.40)\\
&= (1+\delta m_i)\Gamma_{s_i s'_i} + \sum_{\substack{k=1\\k\neq i}}^{n}(1+\delta m_k)\Gamma_{s_k s'_i}\\
&\quad + \underbrace{\sum_{1\leqslant j,k\leqslant n} C_{jk}\sqrt{(1+\delta m_j)(1+\delta m_k)}\Gamma_{r_j r_k s'_i}}_{\mathbf{I}\left(\{r_j,r_k\}_{(j,k)\in[\![1,n]\!]^2}\right)}. &(6.41)
\end{aligned}$$

We rewrite the last term of the crosscovariance measurement by highlighting the message δm_i:

$$\begin{aligned}
\mathbf{I}\left(\{r_j,r_k\}_{(j,k)\in[\![1,n]\!]^2}\right) &\overset{(a)}{=} \sqrt{(1+\delta m_i)}\sum_{\substack{j=1\\j\neq i}}^{n} 2C_{ij}\sqrt{(1+\delta m_j)}\Gamma_{s'_i r_i r_j}\\
&\quad + \sum_{\substack{1\leqslant j,k\leqslant n\\ j,k\neq i}} C_{jk}\sqrt{(1+\delta m_j)\,(1+\delta m_k)}\Gamma_{s'_i r_j r_k}, &(6.42)
\end{aligned}$$

$$\mathbf{I}\left(\{r_j, r_k\}_{(j,k)\in[\![1,n]\!]^2}\right) \overset{(b)}{\approx} \left(1+\frac{\delta m_i}{2}\right)\sum_{\substack{j=1\\ j\neq i}}^{n} 2C_{ij}\left(1+\frac{\delta m_j}{2}\right)\Gamma_{s'_i r_i r_j} + \sum_{\substack{1\leqslant j,k\leqslant n\\ j,k\neq i}} C_{jk}\left(1+\frac{\delta m_j}{2}\right)\left(1+\frac{\delta m_k}{2}\right)\Gamma_{s'_i r_j r_k}, \quad (6.43)$$

$$\overset{(c)}{\approx} \delta m_i \sum_{\substack{j=1\\ j\neq i}}^{n} C_{ij}\Gamma_{s'_i r_i r_j} + \sum_{1\leqslant j,k\leqslant n} C_{jk}\Gamma_{s'_i r_j r_k}. \quad (6.44)$$

In Equality (a), we have separated the terms factorized by $\sqrt{1+\delta m_i}$ from those which are not. Then, in Approximation (b), we consider a Taylor expansion of the square function thanks to the factor $|\delta| \ll 1$. In approximation (c), we neglect all the contributions coming from δm_j with $j \neq i$ and the cross-products of messages $m_j m_k$ $(j,k \neq i)$, which are a $O(\delta^2)$. We finally obtain a linear expression in δm_i. Since the codes and square-root codes are not perfectly orthogonal, we have to keep the contributions of $\Gamma_{s'_i r_j r_k}$ to ensure a reliable decryption.

In a similar way, it is possible to simplify the second term of Eq. 6.41 by neglecting the cross-covariance factorized by δm_k $(k \neq i)$. Therefore, the second term becomes

$$\sum_{k=1,k\neq i}^{n} (1+\delta m_k)\,\Gamma_{s'_i s_k} \approx \sum_{k=1,k\neq i}^{n} \Gamma_{s'_i s_k}. \quad (6.45)$$

Finally, the approximate value of the cross-covariance $\Gamma_{ss'_i}$ becomes linear in the messages δm_i and reads

$$\Gamma_{ss'_i} \approx \delta m_i \left(\Gamma_{s'_i s_i} + \sum_{k=1,k\neq i}^{n} C_{ik}\Gamma_{s'_i r_i r_k}\right) + \sum_{k=1}^{n}\Gamma_{s'_i s_k} + \sum_{1\leqslant j,k\leqslant n} C_{jk}\Gamma_{s'_i r_j r_k}. \quad (6.46)$$

The chaos synchronization of Emitter (**E**) and Receiver (**R**) allows for each user Bob_k to replicate the code s_j. However, duplicating the square-root codes is more challenging, since it would require additional photodiodes $(n(n-1)/2)$ at the reception to generate the interference terms between all the pairs of optical fields. We assume that that $r'_j = \sqrt{\beta_j}\cos(\omega_j y_{T_j} + \varphi_{0j}) = r_j$ and $s'_j = \beta_j \cos^2(\omega_j y_{T_j} + \varphi_{0j}) = s_j$ for $j = 1, \ldots, n$. After simplifications and injection of the duplicated codes, the decoding equation Eq. 6.41 becomes

$$\delta m_i \approx \frac{1}{\Gamma_{s'_i s'_i} + \sum_{k=1,k\neq i}^{n} C_{ik}\Gamma_{s'_i r'_i r'_k}} \left(\Gamma_{ss'_i} - \sum_{k=1}^{n}\Gamma_{s'_i s'_k} - \sum_{1\leqslant j,k\leqslant n} C_{jk}\Gamma_{s'_i r'_j r'_k}\right). \quad (6.47)$$

The decryption equation (6.47) is very similar to Eq. (6.28) with no interference, except for the correcting terms at the numerator and denominators.

We have tested the modified decryption equation by simulating the encryption and decryption of four messages at 2.5 Gbits/s in an architecture with a single photodiode and four feedback loops. The results are shown in Fig. 6.10. The recovered messages present a slightly larger dispersion when compared to those recovered in non-interference architectures. Assuming the Taylor expansion of $\Gamma_{ss'_i}$ to remove the square-root functions of the messages, the left-hand side of Eq. 6.47 can be more rigorously written $\delta m_i(1+\gamma_{ik})$ with

$$\gamma_{ik} = \sum_{\substack{k=1\\k\neq i}}^{n} \frac{m_k \Gamma_{s'_i s'_k}}{m_i \Lambda_{ik}} + \sum_{\substack{k=1\\k\neq i}}^{n} \frac{m_k C_{ik}}{m_i \Lambda_{ik}} \Gamma_{s'_i r'_i r'_k} + \sum_{\substack{1\leqslant j,k\leqslant n\\ j\neq k}} \frac{C_{jk}}{2 m_i \Lambda_{ik}} (m_k + m_j + \frac{\delta m_j m_k}{2}) \Gamma_{s'_i r'_j r'_k}, \tag{6.48}$$

with $\Lambda_{ik} = \Gamma_{s'_i s'_i} + \sum_{\substack{k=1\\k\neq i}}^{n} C_{ik} \left(1 + \frac{\delta m_k}{2}\right) \Gamma_{s'_i r'_i r'_k}$. This is similar to the expression $\delta m_i(1+\lambda_{ik})$ in Eq. 6.29. It is important that the factor γ_{ik} does not induce a sign change otherwise it will induce error in the decryption in the message bit m_i. This naturally imposes the condition $|\gamma_{ik}| < 1$. A sufficient condition for the decryption can be deduced by considering a stronger constrain on γ_{ik}; by introducing the absolute values within γ_{ik} and applying the triangular inequality, we deduce the following

$$\sum_{\substack{k=1\\k\neq i}}^{n} \left|\Gamma_{s'_i s'_k}\right| + \sum_{\substack{k=1\\k\neq i}}^{n} \left|C_{ik}\Gamma_{s'_i r'_i r'_k}\right| + (2+\delta) \sum_{\substack{1\leqslant j,k\leqslant n\\ j\neq k\neq i}} \left|C_{jk}\Gamma_{s'_i r'_j r'_k}\right| < |\Lambda_{ik}|\,. \tag{6.49}$$

Moreover, we have $|\Lambda_{ik}| < \left|\Gamma_{s'_i s'_i}\right| + \sum_{\substack{k=1\\k\neq i}}^{n} \left|C_{ik}\Gamma_{s'_i r'_i r'_k}\right| \left(1+\frac{\delta}{2}\right)$. Therefore, we can deduce a sufficient condition for the decryption to be possible:

$$\sum_{\substack{k=1\\k\neq i}}^{n} \left|\Gamma_{s'_i s'_k}\right| + (2+\delta) \sum_{\substack{1\leqslant j,k\leqslant n\\ j\neq k\neq i}} \left|C_{jk}\Gamma_{s'_i r'_j r'_k}\right| < \left|\Gamma_{s'_i s'_i}\right| + \frac{\delta}{2} \sum_{\substack{k=1\\k\neq i}}^{n} \left|C_{ik}\Gamma_{s'_i r'_i r'_k}.\right| \tag{6.50}$$

The form of the sufficient condition is pretty similar to that of the case without interference (Eq. 6.30). It highlights the undesired effects of the interference cross-covariance terms that may rapidly saturate the inequality in Eq. 6.50. Therefore to ensure a satisfying level of performance with this decryption method, the codes and the square-root codes have to be quasi-orthogonal.

In summary, we have demonstrated theoretically how to decrypt messages when interference exists in the multiplexed feedback signal $s(t)$, which drives the dynamics of the emitter and the receiver. With proper adjustments, a new decoding equation was derived and it ensures a comparable level of performance to the case without interference. However, one of the main difficulty for the decryption would be the reproduction of interference patterns at the receiver end, a major challenge for an experimental realization.

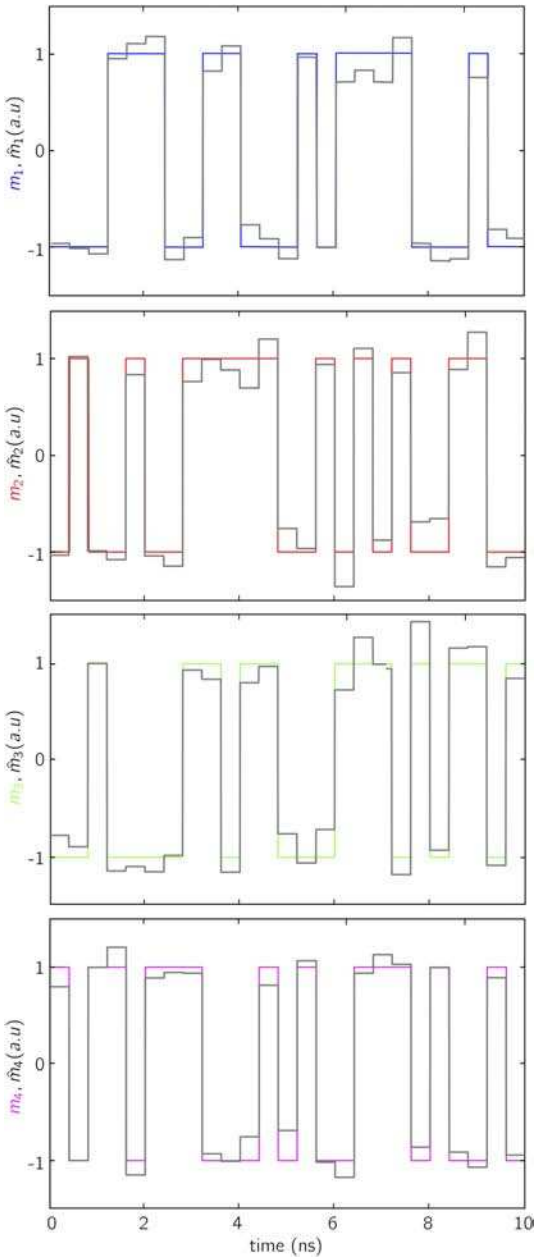

Figure 6.10: Theoretical multiplexing of four binary messages m_i at 2.5 Gbit/s (25 bits are represented for each messages). The messages are independently decrypted and requires 4 decoding circuits. In each panel, the dashed line represent the originally-encrypted messages (m_j) and the solid gray lines represent the decrypted message ($\hat{m}_j$) using decoding equation Eq. 6.47. The numerical values are $\beta_j = 5$, $C_{ij} = \cos((i-j)\frac{\pi}{4})$, $\theta = 25$ ps, $\tau = 5$ μs, $T_j = 30$ ns, $\delta = \frac{1}{32}$, and $\Delta\omega_{ij} = 2$ with $i, j = 1, \ldots, 4$ and $i \neq j$.

6.6 Conclusion

In this chapter, we have demonstrated that a single electro-optic oscillator (EOO) with multiple delayed feedback loops can be used to generate orthogonal chaotic codes. This allows to transpose efficiently code-division multiple access (CDMA) concept in the framework of optical chaos-based communications. Several configurations were illustrated to ensure and prevent optical interference during the transmission: Configuration (1) using multiple photodetectors and Configurations (2a)-(2b) using a single photodetector.

The pseudo-random sequences (codes) used to spread the data-streams result, in our context, from the output of Mach-Zehnder modulators. Each of them generates a cosine-square nonlinearity with a specific frequency of oscillation (denoted ω_j).

The statistical properties of the different chaotic codes are controlled by three different parameters: the nonlinear gain (β_j), the frequency (ω_j), and the off-set phase (φ_{0j}). We have proven that for a sufficiently large frequency detuning $\Delta\omega_{ij} = \omega_i - \omega_j$ and nonlinear gain β_j, the codes are orthogonal and can be used to transmit and recover, with a linear computational complexity, binary messages without cross-talk in configurations (1) and (2b). We numerically demonstrate encryption and decryption of several messages at high bit rate (2.5 Gbit/S, OC-48 standard). In case of imperfect orthogonality, we have also shown that it was still possible to decrypt the messages by considering a joint decryption, using either a covariance-matrix approach or least-square optimization. In both cases, however, the decryption involves the inversion of square matrices, increasing the computational complexity.

Finally, we focus our attention on Configuration (2a) that systematically exhibits interference when more than two feedback loops are considered. We have devised a decryption strategy with a linear computational complexity that guarantees an error-free decryption when the messages have sufficiently small amplitudes. However, it makes the structure of the decoder far more complex and requires to duplicate specific interference patterns at the receiver. We numerically achieve similar performance to that of configurations (1) and (2b) in terms of transmission.

As a consequence, our approach may constitute a first significant step for the application of code-division multiple access concepts to optical chaos-based communications.

Chapter 7

Multiplexing Chaos Using Stochastic Time-Delays Architectures

Abstract

This chapter investigates an efficient and fast bit-multiplexed encryption scheme exploiting hyperchaotic regimes of a single nonlinear oscillator with multiple time-delay feedback loops. This structure is of particular interest because the data stream of each user Alice$_i$ ($i = 1, \ldots n$) is encrypted through a digital modulation of the various time delays and decrypted using chaos synchronization and cross-correlation metrics. In this chapter, we will describe our particular structure, the mechanisms for encryption and decryption, and give the fundamental limitations in terms of bit rate and number of users. Our approach is numerically illustrated for a chaotic electro-optic oscillator structure based on a standard continuous-wave semiconductor laser subjected to multiple nonlinear feedback loops. We numerically demonstrate successful data transmission and recovery between multiple users at several Gbits/s on a single communication channel.

This chapter is based on the following publication:

- D. Rontani, M. Sciamanna, A. Locquet, and D.S. Citrin, "Multiplexed encryption using chaotic systems with multiple stochastic-delayed feedbacks", *Phys. Rev. E* **80**, 066209 (2009).

7.1 Introduction

The following chapter focuses on multi-user chaos-based communications using time-delay systems. Our primary objective is to make better use of the wide bandwidth provided by the chaotic oscillator, but also to increase significantly the level of security compared with the other architectures presented in this thesis.

In the two previous chapters, we have proposed architectures to multiplex optical chaotic signal and encrypt multiple messages in a CDMA fashion. Although, they allow fast and reliable Gbit/s transmissions, the level of security was not significantly enhanced compared to that of existing single-message chaos-based transmissions. When it comes to fixed time-delay systems, the computational security relies on the concealment of the time-delay information [149; 151; 152; 175] (and see Chapter 4). A natural idea to increase the security of the time-delay information is to make the delay time-varying. Following this line of reasoning, several strategies have been devised to increase the level of security:

- Periodic time-varying delays [176]: This was the first attempt to counter time-delay identification based on typical estimators (ACF, DMI, LLM, and GNM).
- Chaotic time-varying delays [177]: The optical path of an optoelectronic generator was controlled by a delayed-differential equation, thus leading to chaotic modulations of the time delay.
- Stochastic time-varying delays [147]: This was introduced as the strongest concealment of time delay thus ensuring the highest level of security. Existing time-delay identification methods fail, thus maintaining a high level of security.
- Stochastic commutating delays [146]: A nonlinear system was used with a programmable time-delayed feedback. The time-delay switches randomly between two different values.

These different configurations were first studied for the generation of highly secure chaotic carriers, but rapidly the idea that time-delay modulation could be used as a transmission vector was proposed in [178] with chaotic logistic maps. In the proposed setup, a user Alice encrypts her message $m(t)$ as an additional modulation of a state-dependent time delay $\tau(t) = g(\mathbf{x}_E(t), t) + m(t)$ with $\mathbf{x}_E \in \mathbb{R}^m$ the state variable of emitter (E) and $g : \mathbb{R}^m \to \mathbb{R}$ a continuous function. The state $\mathbf{x}_E(t-\tau(t))$ drives the dynamics of both the emitter owned by Alice and the receiver owned by a legitimate receiver Bob,

$$\text{Alice: } \dot{\mathbf{x}}_E(t) = f\left(\mathbf{x}_E(t), \mathbf{x}_E(t-\tau(t))\right), \tag{7.1}$$

$$\text{Bob: } \dot{\mathbf{x}}_R(t) = f\left(\mathbf{x}_R(t), \mathbf{x}_E(t-\tau(t))\right), \tag{7.2}$$

where $\mathbf{x}_E, \mathbf{x}_R \in \mathbb{R}^m$ is the state variable of (E) and (R) and $f : \mathbb{R}^m \to \mathbb{R}^m$ is the vector field associated with the nonlinear oscillator. To decrypt the message, Bob considers the metrics

$$M(\varepsilon) = \varepsilon - |\mathbf{x}_E(t-\tau(t)) - \mathbf{x}_R(t-\theta)|, \tag{7.3}$$

where $\theta \in [0, \tau_m]$ with $\tau_m = \max \tau(t)$. By maximizing $M(\varepsilon)$ during the duration of a bit transmitted, the authors of [178] obtain an estimation of the unknown value of $\tau(t)$. Then due to chaos synchronization at the receiver, they generate $\tau_{0,R}(t) = g(\mathbf{x}_R(t), t) = \tau_0(t)$ and recover the values of the message by simple subtraction. This method was adapted to the transmission of a single message, but either the structure or the metrics used did not allow for the transmission of multiple data-streams.

In this chapter, we will show how time-delay systems (under certain conditions) can be used favorably to overcome simultaneously these two major limitations in chaos multiplexing. We use a single chaotic oscillator with n time-delay feedback loops, each of the time delays being digitally modulated by a specific user. This approach, which is neither the overlay of TDM nor of WDM on top of a conventional chaotic system, uses a single chaotic oscillator that ensures the simultaneous encryption of n messages in a single wide-spectrum chaotic carrier. This is therefore beneficial to achieve higher spectral efficiency on the communication-channel bandwidth in comparison with WDM. Extraction of the various messages can be realized either with a high complexity (HC) or low complexity (LC) decryption strategy based on finite-time cross-correlation measurements. Additionally, the stochastic modulations of the time delays at the rate of the messages participate in the dynamical evolution of the chaotic oscillator and contribute to enhancing greatly the security of transmissions. We numerically apply our multiplexing/demultiplexing technique to an optoelectronic chaos generator based on a well-tested and reliable physical model and demonstrate theoretically multi-Gbit/s transmission per user. A discussion on the performances (spectral efficiency, bit rate) and on the limitations of the architecture will be presented as well.

7.2 Description of the Architecture

Our setup is described in Fig. 7.1. It is composed of two parts, a global emitter (E) and a global receiver (R). These two systems are unidirectionally coupled via a single communication channel and also share identical structural properties. Both use a *single* nonlinear oscillator described by their respective state variable: $\mathbf{x}_E \in \mathbb{R}^p$ and $\mathbf{x}_R \in \mathbb{R}^p$. In E, the nonlinear oscillator is fed back by n time-delayed feedback loops.

As illustrated in Fig. 7.1, at the emitter end, every legitimate user Alice$_i$ possesses a specific loop incorporating a specific nonlinearity NL_i, which processes the nonlinear oscillator's state vector $h_{Ai}(\mathbf{x}_E(t))$, with h_{A_i} a continuous nonlinear function defined on $\mathbb{R}^p \to \mathbb{R}^n$. The second element of the feedback loop is a tunable delay line DL_i that controls the variable time delay $\tau_i(t)$. This quantity is digitally modulated by Alice$_i$ to encode her data stream. Finally, the various contributions of all the users are summed in a single *multiplexed signal* $s(t)$ that reads

$$s(t) = \sum_{i=1}^{n} h_{A_i}(\mathbf{x}_E(t - \tau_i(t))). \tag{7.4}$$

The multiplexed signal $s(t)$ is generally vectorial ($s(t) \in \mathbb{R}^m$); however, the scalar case ($m = 1$) will be considered to simplify the notation and calculations.

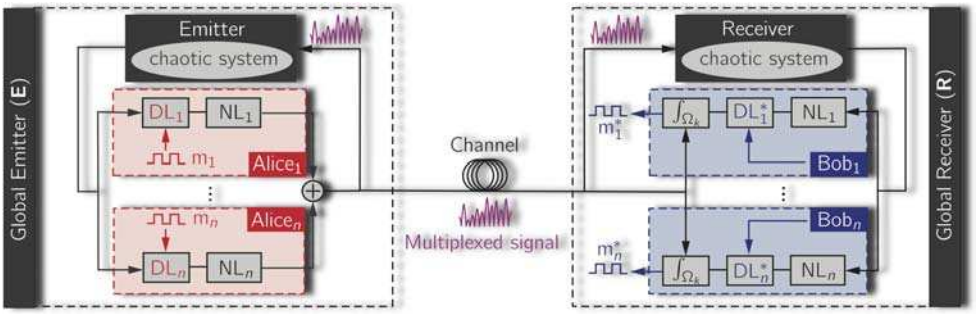

Figure 7.1: Architecture to multiplex multiple digital data streams using a single chaotic oscillator with multiple feedback loops. NL_i: the ith nonlinearity, DL_i: variable delay line modulated by Alice_i, DL_i^*: variable delay line used by Bob_i to search for a maximum of cross-correlation. m_i: message encrypted by Alice_i, m_i^*: message decrypted by Bob_i (i=1,...,n), Ω_k: time during which a symbol (or bit) of the message $\mathsf{m_i}$ is maintained constant.

For example, let us consider an optoelectronic oscillator such as those described in the previous chapter. The multiplexed signal with variable delays now reads

$$T\dot{x}(t) + x(t) + \frac{1}{\theta}\int_{t_0}^{t} x(u)du = \sum_{i=1}^{n} \beta_i \cos^2\left(x(t-\tau_i(t)+\varphi_{0i}\right), \tag{7.5}$$

assuming no use of voltage dividers before injecting the various Mach-Zehnder modulator MZ_i (see Chapter 6).

The structure initially proposed in Fig. 7.1 can be slightly modified by considering an additional nonlinear function $h : \mathbb{R}^m \to \mathbb{R}^n$ applied to the sum of the delayed feedback signals $h_{A_i}(x(t-\tau_i(t))$. This leads to a new multiplexed signal

$$s(t) = h\left(\sum_{i=1}^{n} h_{A_i}\left(x(t-\tau_i(t))\right)\right). \tag{7.6}$$

A particular example was proposed in [144] using a wavelength chaos generator with multiple electronic loops. It results in a single cosine nonlinearity applied to a sum of delayed variables,

$$T\dot{x}(t) + x(t) = \beta\cos^2\left(\sum_{i=1}^{n} x(t-\tau_i(t)) + \varphi_0\right). \tag{7.7}$$

In this example, the nonlinear functions are $h_{A_i}(y) = 1$ and $h(y) = \beta\cos^2(y+\varphi_0)$.

This signal is then sent through the communication channel and will couple the global receiver R. The nonlinear oscillator located in R is a physical twin of that of E. Consequently, the dynamics of E and R are described by the equations

$$\dot{\mathbf{x}}_E(t) = f\left(\mathbf{x}_E(t), s(t)\right), \tag{7.8}$$

$$\dot{\mathbf{x}}_R(t) = f\left(\mathbf{x}_R(t), s(t)\right), \tag{7.9}$$

where $f : (\mathbb{R}^p, \mathbb{R}^m) \to \mathbb{R}^p$ is the nonlinear function of the nonlinear oscillator.

Assuming both systems are damped oscillators when no feedback signal is injected[1], E and R are *passive* systems. Therefore, the multiplexed feedback signal $s(t)$ is, in our case, an *active* part that will drive the dynamics of E and R. Under these conditions, the APD's requirement are fully satisfied for the two systems to be completely chaotically synchronized,

$$\lim_{t\to\infty} \|\mathbf{x}_E(t) - \mathbf{x}_R(t)\| = 0. \tag{7.10}$$

The chaos synchronization is one of the key features used in the extraction of the various messages by the legitimate users Bob_i $(i = 1, \ldots, n)$. In Receiver R, each Bob has a loop sharing similar features to that of his corresponding Alice, except that his loop does not feed back the nonlinear oscillator. Bob_i's loop is also composed of the same nonlinearity NL_i described by a nonlinear function $h_{B_i} = h_{A_i} : \mathbb{R}^m \to \mathbb{R}^p$ and a tunable delay line DL_i^* generating candidate time delays $\tau_i^*(t)$ different a priori from $\tau_i(t)$. Each loop process the state variable $\mathbf{x}_R$ as it follows $h_{B_i}(\mathbf{x}_R(t - \tau_i^*(t)))$. These open loops at Receiver R are used to reproduce what the Alices are doing at Emitter E. Recovery of the information is then possible by analyzing the evolution of particular metrics (based on correlation or L^2-norm).

In the two following sections of this chapter, we will describe precisely the mechanisms used by Alices and Bobs respectively to encrypt and decrypt the multiplexed data in our architecture. One of the objectives is to guarantee a low level of computational complexity for the decryption, while maintaining a good level of computational security.

7.3 Encryption Strategies

In this section, we describe how the Alices encode their respective messages. Each user has at his disposal a random source of information composed of M_i different symbols $c_i^{(\mu_i)}$ $(\mu_i = 1, \ldots, M_i)$. These symbols' values are mapped onto a specific interval of value Δ_i $(i = 1, \ldots, n)$, later referred to as an *encryption slot* where the time delay $\tau_i(t)$ varies. In the context of digital communications, the variation of $\tau_i(t)$ must be time-discrete in their interval of definition Δ_i. We define the period of time when a symbol $c_i^{(\mu_i)}$ is maintained constant by T_s and the associated time intervals $\Omega_k = [kT_s, (k+1)T_s]$ $(k \in \mathbb{N})$, later referred to as a *time-slot*. The mathematical formulation of a digital time-delay encryption by Alice_i therefore reads

$$\tau_i(t) = \sum_{k=0}^{\infty} \tau_{i|\Omega_k} \left(H(t - kT_s) - H(t - (k+1)\,T_s)\right), \tag{7.11}$$

where $\tau_{i|\Omega_k}$ is the encoding value of the kth symbol generated by Alice_i in the time slot Ω_k, and $H(t)$ is the Heaviside function.

The method of encryption of a single user is now described. It is noteworthy to mention a simplification in our encryption compared to what is done in [178]; the time-delay modulation will be solely induced by the various information sources (no

[1]Mathematically this is equivalent to the asymptotic convergence of each state to zero.

additional state dependence is considered). Among the advantages is a simplification of the decryption process with the use of more conventional metrics such as correlation and norm 2.

Inherent to the presence of multiple users, there are several possibilities to realize the multiplexed encryption. Indeed, each loop has two degrees of freedom: the nature of the nonlinearity (NL_i) used and the encryption slots (Δ_i). As it will be detailed later, it is important to perform carefully the encryption by incorporating into it a discrimination criterion, otherwise the decryption would not be possible: the Bobs could not recover their data. Essentially, we propose two different types of encryption.

7.3.1 Encryption with Multiple Disjoint Encryption Slots

This first encryption method consists of disjoint encryption slots ($\Delta_i \cap \Delta_j = \emptyset$ for all $i \neq j$) with the freedom for the various users to choose their nonlinear function h_{A_i}.[1] Each interval is centered on a specific value: $\Delta_i = [\tau_{i_0} - \frac{\Delta\tau_i}{2}, \tau_{i_0} + \frac{\Delta\tau_i}{2}]$, where $\Delta\tau_i$ is the width of Δ_i. Figure 7.2 illustrates this approach.

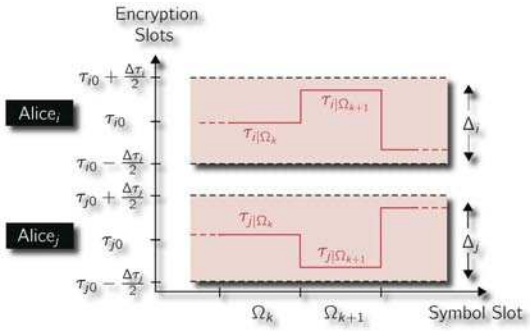

Figure 7.2: Graphical representation of the time-delay encryption realized by two different users Alice$_i$ and Alice$_j$ in their respective encryption slots Δ_i and Δ_j to be multiplexed. Two consecutive symbols are encrypted for each users $\tau_{i|\Omega_k}$ and $\tau_{j|\Omega_k}$.

7.3.2 Encryption with Multiple Overlapping Encryption Slots

This second encryption method consists of the use of encryption slots that can (partially or totally) overlap ($\Delta_i \cap \Delta_j \neq \emptyset$ for all $i \neq j$). Under these conditions, the encryption performed by each Alice necessary relies on different nonlinear functions as a discriminant criterion incorporated in the encryption. Figure 7.3 illustrates this approach with a single encryption slot shared by all the users.

[1] The use of identical nonlinearities for all the Alices is possible ($h_{A_i} = h_{A_j}$ for all (i, j)).

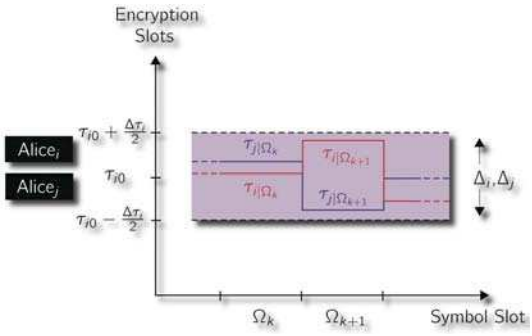

Figure 7.3: Graphical representation of the time-delay encryption realized by two different users Alice$_i$ and Alice$_j$ in their respective encryption slots Δ_i and Δ_j that completely overlap. Two consecutive symbols $\tau_{i|\Omega_k}$ and $\tau_{j|\Omega_k}$ are encrypted for each user.

7.4 Decryption Strategies and Complexity Issues

There are many degrees of freedom to encrypt multiple data streams with our architecture; however, demultiplexing at Receiver R places restriction on how these can be chosen. Decrypting the multiplexed data stream is equivalent for each Bob$_i$ to recover the time-delay modulation $\tau_{i|\Omega_k}$ for all $i = 1, \ldots, n$ and Ω_k, $k \in \mathbb{N}$. To achieve this goal, the Bobs first generate independently or jointly the candidate time delay $\tau^*_{i|\Omega_k}$ by means of their tunable delay line DL^*_i. Second, they consider an optimization problem defined with respect to appropriate metrics. Its solution will serve as a decryption for the multiplexed data streams. In the forthcoming subsections, we will detail necessary conditions for the decryption to be possible, as well as the various metrics and optimization approaches that can be used.

7.4.1 Necessary Conditions for Decryption

In the case of disjoint encryption slots, the distance between the intervals Δ_i is the *discriminating criterion*, whereas in the case of overlapping encryption slots the nonlinearity is used to identify the contributions associated to the various users. In both case, the criterion has to ensure the statistical independence between the nonlinear signals $h_{A_i}(\mathbf{x}_E(t - \tau_i(t))$ for all $i = 1, \ldots, n$ and all time. This results in additional constrains on the class of systems that can be used with our architecture, when the encryption slots Δ_i overlap. Independently of the encryption technique used, there is a set of universal conditions that are necessary for a proper decryption:

Condition (i) (Reproducibility): Emitter E and Receiver R have to be completely synchronized.

Condition (ii) (Unicity): The decryption is performed by the resolution of an optimization problem with a unique global extremum to ensure the unicity of the decrypted message for the various legitimate users, Bobs.

Condition (iii) (Metric Resolvability): Two symbols used by a given user, when encoded on time delays belonging to to the same encryption slot, have to be separable in the framework of the metrics we choose.

7.4.2 Choices of Metrics

We call a *metric* a mathematical operation that maps a vector space to the set of real numbers $\mathbb{R}$. In our case, we can use either the L^2-norm or the autocorrelation. Both are based on the definition of an inner product on a functional space.

We consider two signals (ϕ_i, ϕ_j), with finite energy (belonging to $L^2(\mathbb{R})$), and we define the *inner product* by

$$\langle \phi_i, \phi_j \rangle = \int_{\mathbb{R}} \phi_i(t)\phi_j(t)dt. \tag{7.12}$$

There is, however, a need for an inner product also defined on finite set Ω_k,

$$\langle \phi_i, \phi_j \rangle^{\Omega_k} = \int_{\Omega_k} \phi_i(t)\phi_j(t)dt. \tag{7.13}$$

If the signals depend upon time as a consequence of the definition of the inner product, it is possible to define cross-correlation measurements on infinite and finite sets, Γ and Γ^{Ω_k}. More precisely, we have $\Gamma_{\phi_i,\phi_j}(0) = \langle \phi_i, \phi_j \rangle$ and $\Gamma^{\Omega_k}_{\phi_i,\phi_j}(0) = \langle \phi_i, \phi_j \rangle^{\Omega_k}$. If the two signals are time delayed with each other then the scalar product becomes

$$\langle \phi_i(t-\tau_i), \phi_j(t-\tau_j) \rangle = \int_{\mathbb{R}} \phi_i(t-\Delta\tau_{ij})\phi_j(t)dt = \Gamma_{\phi_i,\phi_j}(\Delta\tau_{ij}), \tag{7.14}$$

with $\Delta\tau_{ij} = \tau_i - \tau_j$.

The L^2-norm is simply defined in terms of the inner product by

$$||\phi_i||_2^{\Omega_k} = \left(\langle \phi_i, \phi_i \rangle^{\Omega_k}\right)^{1/2}. \tag{7.15}$$

7.4.3 Decryption with High Computational Complexity

We consider the architecture described in Fig. 7.1 with n different users Alice$_i$ and the metrics on the finite time slot Ω_k defined above. Emitter E is fed back with $s(t) = \sum_{i=1}^{n} s_{A_i,\tau_i}$.

We assume that R is perfectly synchronized with E (Condition (i)) and that the set (T_s, s_{A_i}, Δ_i) used by each Alice is also known by their respective Bob.

Collectively for each symbol slot Ω_k, the Bobs generate a single candidate multiplexed waveform with a set of known delays $(\tau^*_{i|\Omega_k})_{i\in[\![1,n]\!]}$ that may not correspond to the delay used by the Alices,

$$s^*(t) = \sum_{i=1}^{n} h_{A_i}(x_R(t-\tau_i^*(t))) = \sum_{i=1}^{n} s_{A_i,\tau_i^*}. \tag{7.16}$$

The objective for Bob$_i$ is to recover Alice$_i$ symbols encoded onto the set of time delays $(\tau_{i|\Omega_k})_{i\in[\![1,n]\!]}$. If this condition is fulfilled, then the two signals $s(t)$ and $s^*(t)$ will be equal on every time slot Ω_k. A closer look at the signals $s(t)$ and $s^*(t)$ shows that the only difference relies on the value of the time delays. Adjusting the time delay used in $s^*(t)$ allows the decryption to be possible only if the set of time delays leading to $s(t) = s^*(t)$ is unique (Condition (ii)). The unicity originally comes from

the construction of the chaotic carriers s_{A_i,τ_i} and a proper use of encryption intervals Δ_i (disjoint with any nonlinear function or overlapping with adequate nonlinear functions). Indeed, the set of carriers $\mathscr{B} = (s_{A_i,\tau_i})_{i\in[\![1,n]\!]}$ may be viewed as a vector basis in which $s(t)$ is trivially decomposed. The signal $s^*(t)$ is also trivially decomposed into a candidate basis $\mathscr{B}^* = (s_{A_i,\tau_i^*})_{i\in[\![1,n]\!]}$ with unitary coefficients. Both bases are constructed with the same linearly independent functions except for the time delays that differ. The proper use of encryption slots Δ_i and nonlinear functions further guarantees that for all (i,j), it is not possible to find $\tau_j^* \in \Delta_j$ such that $s_{A_i,\tau_i} = s_{A_j,\tau_j^*}$. As a consequence,

$$s(t) = s^*(t) \quad \Rightarrow \quad \sum_{i=1}^{n} (s_{A_i,\tau_i} - s_{A_i,\tau_i^*}) = 0, \tag{7.17}$$

$$\Rightarrow \quad s_{A_i,\tau_i} = s_{A_i,\tau_i^*} \text{ for } [\![1,n]\!]\,. \tag{7.18}$$

Finally, based on the previous discussion and the one-to-one equality of vectors of bases $\mathscr{B}^*$ and $\mathscr{B}$, we can conclude that

$$\forall i \in [\![1,n]\!] \;\; s_{A_i,\tau_i} = s_{A_i,\tau_i^*} \text{ is equivalent to } \tau_i = \tau_i^*. \tag{7.19}$$

In a high-complexity (HC) decryption scheme, all the possible delay values are explored and tested in the product encryption space $\prod_{i=1}^{n} \Delta_i$, as illustrated in a simplified situation in Fig. 7.4.

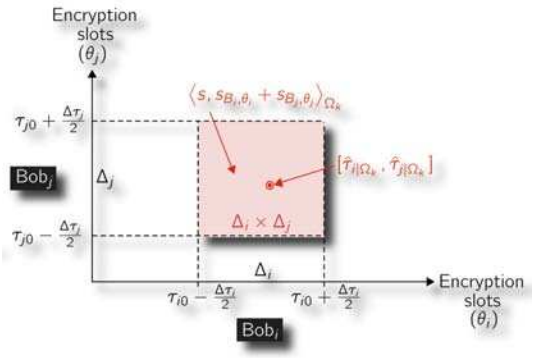

Figure 7.4: Graphical representation of a high complexity time-delay decryption realized by two different users Bob$_i$ and Bob$_j$ in the product encryption slot $\Delta_i \times \Delta_j$. The recovery of each time-delay is realized jointly and is represented by a red circular mark located at $[\theta_i, \theta_j] = [\hat{\tau}_{i|\Omega_k}, \hat{\tau}_{j|\Omega_k}]$.

The unique combination of time delays that belongs to the different encryption intervals and corresponds to a good estimation of the original message $(\tau_{i|\Omega_k})_{i\in[\![1,n]\!]}$ encrypted by the Alices is retrieved by solving either of the two following optimization problems (depending on the chosen metrics):

$$(\hat{\tau}_{i|\Omega_k})_{i\in[\![i,n]\!]} = \underset{(\tau^*_{i|\Omega_k})_{i\in[\![i,n]\!]} \in \prod_{i=1}^{n} \Delta_i}{\arg\min} \|s - s^*\|_2^{\Omega_k}\,, \tag{7.20}$$

or

$$(\hat{\tau}_{i|\Omega_k})_{i\in[\![i,n]\!]} = \underset{(\tau^*_{i|\Omega_k})_{i\in[\![i,n]\!]}\in\prod_{i=1}^{n}\Delta_i}{\arg\max} \langle s, s^*\rangle^{\Omega_k}. \tag{7.21}$$

After decryption, the estimated values are transferred to the targeted users Bob_i. The main disadvantage of this type of decryption is its exponential computational complexity. If we consider that each Alice can encrypt M different values of time delay by interval, this results in the computation of M^n operations for each time-slot Ω_k. This rapidly limits either the number of symbols used (the bit rate) or the number of users (the spectral efficiency).

To overcome this problem, we present in the next subsection a decryption method that is computationally linear with the number of users.

7.4.4 Decryption with Low Computational Complexity

We have seen that the linear independence of the different nonlinear signals $s_{A_i,\tau_{i|\Omega_k}}$ is used to ensure the recovery of a unique set of time delays $(\hat{\tau}_{i|\Omega_k})_{i\in[1,n]}$ in each encryption slot Δ_i and time slot Ω_k corresponding to the actual time-delay values $(\tau_{i|\Omega_k})_{i\in[1,n]}$. But this property, although it allows for the decryption to be possible, does not provide low complexity calculations for the decryption. Decrypting at a lower computational complexity is possible if each Bob_i can extract his own information independently while having just the multiplexing signal $s(t)$ at disposal and Alice_i's key. Furthermore, in the previous subsection we have shown that the total minimization (or maximization) of the global optimization problem result in the recovery of all the time delays at once. All the basis vectors participate in this minimization process, but it appears that the recovery of a single delay of a basis signal s_{A_i,τ_i} reduces the difference between s and s^* (*i.e.*, increase the correlation). With this phenomenon, each Bob can recover his own information independently. Mathematically, we can write both cases as

$$\left\langle s, s_{A_i,\tau_i^*}\right\rangle^{\Omega_k} = \left\langle s_{A_i,\tau_i}, s_{A_i,\tau_i^*}\right\rangle^{\Omega_k} + \sum_{j=1,j\neq i}^{n}\left\langle s_{A_j,\tau_j}, s_{A_i,\tau_i^*}\right\rangle^{\Omega_k}, \tag{7.22}$$

$$\left\|s - s_{A_i,\tau_i^*}\right\|_2^{\Omega_k} = \left\|s_{A_i,\tau_i} - s_{A_i,\tau_i^*} + \sum_{j=1,,j\neq i}^{n} s_{A_j,\tau_j}\right\|_2^{\Omega_k}. \tag{7.23}$$

On the right-hand side of both equations, there is the *resonant* (*antiresonant*) part $\left\langle s_{A_i,\tau_i}, s_{A_i,\tau_i^*}\right\rangle^{\Omega_k}$ (or $s_{A_i,\tau_i} - s_{A_i,\tau_i^*}$ if L^2-norm is considered) that will be identified and lead after optimization to the value of Alice_i's encrypted time delay in the time slot Ω_k. The other part will be referred to as the *background* and corresponds to the crosstalk and contribution of all other users. The principles of decryption using correlation metrics are illustrated in Fig. 7.5.

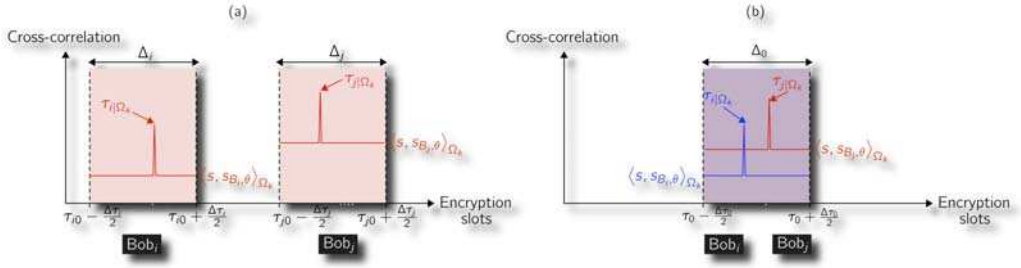

Figure 7.5: Graphical representation of the time-delay decryption realized by two users Bob$_i$ and Bob$_j$. (a) Configuration associated with multiple disjoint encryption slots Δ_i and Δ_j used by Alice$_i$ and Alice$_j$, respectively. (b) Configuration with a single encryption slot Δ_0 share by the different user at the emission and the reception. For the given time-slot Ω_k, each Bob is detecting a resonance to recover his time-delay. The cross-correlation measurements are used for the metrics.

In Fig. 7.5(a), using either the cross-correlation measurement or L^2-norm, we observe either a local maximum or minimum in each encryption interval Δ_i. Each user Bob$_i$ solves his own optimization problem by searching a maximum (or minimum) in his specific encryption slot Δ_i for each time slot Ω_k. The recovery of each symbol emitted by Alice$_i$ is described as

$$\hat{\tau}_{i|\Omega_k} = \underset{\tau^*_{i|\Omega_k} \in \Delta_i}{\arg\max} \left\langle s, s_{A_i,\tau^*_{i|\Omega_k}} \right\rangle^{\Omega_k}, \tag{7.24}$$

or

$$\hat{\tau}_{i|\Omega_k} = \underset{\tau^*_{i|\Omega_k} \in \Delta_i}{\arg\min} \left\| s - s_{A_i,\tau^*_{i|\Omega_k}} \right\|_2^{\Omega_k}. \tag{7.25}$$

The linear complexity comes from the reduction in size of the interval explored for the decryption. However, the reduction in complexity is responsible for the appearance of a correlation background (L^2-norm background) that limits the number of users, as detailed in the following sections.

7.5 Application to Optoelectronic Oscillators

7.5.1 Encryption and Decryption with Multiple Disjoint Intervals

In this section, we follow the theoretical framework presented in the previous section and numerically apply our approach to a transmission chain composed of two coupled optoelectronic oscillators subjected to four delayed feedback loops to transmit $n = 4$ independent messages. The oscillators can be built using two configurations: (i) an intensity chaos generators based on multiple Mach-Zehnder modulators in their nonlinear regimes and subjected to single time-delay feedback, or (ii) a single Mach-Zehnder fed back by multiple electronic delay loops. The total feedback signal is denoted $s(t)$; unidirectionally injects both E and R. The coupled oscillators are

modeled by the set of integro-differential delay equations similarly to the previous chapter,

$$T\dot{x}_E + x_E + \frac{1}{\theta}\int_{t_0}^{t} x_E(u)du = s(t), \tag{7.26}$$

$$T\dot{x}_R + x_R + \frac{1}{\theta}\int_{t_0}^{t} x_R(u)du = s(t), \tag{7.27}$$

where

$$s(t) = s_1(t) = \sum_{i=1}^{n} \beta_i \cos^2\left(x_{E,\tau_i} + \varphi_{0i}\right), \tag{7.28}$$

$$s(t) = s_2(t) = \beta \cos^2\left(\sum_{j=1}^{n} x_{E,\tau_j} + \varphi_0\right), \tag{7.29}$$

$x_E, x_R \in \mathbb{R}$ are the dimensionless driving voltages of E and R, respectively, T is the high cutoff response time, θ is the low cutoff response time, β_i is the normalized feedback strength of the ith Mach-Zehnder modulator, and φ_{0i} is its normalized offset phase. The set of delay integro-differential equations Eqs. 7.26-7.27 can be rewritten in ordinary differential form if the variable change $y_{E,R} = \int_{t_0}^{t} x_{E,R}(u)du$ is introduced, and thus the above theory can be applied. With the notations used in the first section, for Configuration (i) we have $h_{A_i}(x_{E,\tau_i}) = \beta_i \cos^2(x_{E,\tau_i} + \varphi_{0i})$ and $h(y) = 1$ and for Configuration (ii) $h_{A_i}(x_{E,\tau_i}) = x_{E,\tau_i}$ and $h(y) = \beta \cos^2(y + \varphi_0)$.

7.5.1.1 Simulation of a High Computational Complexity Case

We have simulated the system with the following numerical values: $T = 25$ ps, $\theta = 10$ μs, $\beta_i = 30$, $\varphi_{0i} = \frac{2i\pi}{4}$, $\Delta_i = [20i \text{ ns}, 20i + 10 \text{ ns}]$, and a symbol duration of $T_s = 1$ ns ($i = 1, \ldots, 4$). Each user Alice$_i$ has a data source $M_i = 4$ symbols (to ensure tractable computational levels) associated with corresponding time delays in the encryption slot Δ_i. We have considered the two type of signals $s_1(t)$ and $s_2(t)$; in both cases error-free decryption were achieved as long E and R were completely synchronized. The use of a multiplexed signal with the form of $s_2(t)$ allows only high-complexity decryption to work, because the function $h(y) = \beta \cos^2(y + \varphi_0)$ is not bijective on the interval of definition of $y = \sum_{j=1}^{n} x_{E,\tau_j}$ thus preventing its inversion, necessary for a low complexity decryption.

7.5.1.2 Simulation of a Low Computational Complexity Case

We have considered a system with multiple nonlinearities with numerical values for the parameters similar to the previous subsubsection with a multiplexed signal of the form $s(t) = s_1(t)$.

Figure 7.6 shows the numerical results with ideal transmission conditions: no noise and no distortion induced by the communication channel. The symbols are maintained constant during symbol time slots of duration $T_s = 1$ ns. This leads to 1 Giga symbols/s transmission per user and appears to be the lower bound of T_s when

four users send their messages. This corresponds to an equivalent 5 Gbits/s transmission per user considering that each symbol requires 5 bits to be encoded. The first and the second rows in Fig. 7.6 represent the data randomly generated by each user Alice$_i$ and the data recovered by the corresponding receiver Bob$_i$, respectively. The third row displays, for each user, the relative errors $e_i = (\tau_i - \hat{\tau}_i)/\tau_i$ in symbols recovery, which are all on average smaller than 0.5%. The decryption errors are due to uncertainties generated by the finite-time calculation of cross-correlation on the time slots Ω_k.

This intrinsically limits the resolution of the cross-correlation. However these errors can be suppressed, if the Bobs know a priori the sets of possible symbols used by the Alices, as would be expected when digital symbols are used, and if the duration of Ω_k are long enough. This proves that near-perfect decryption is achieved for four digital messages and also that these can be encoded on a large number of symbols. Correct decryption at a given symbol rate $1/T_s$ also depends on the number of users n. It affects the amplitude of the background fluctuations present in the correlation $\langle s, s_{B_i,\tau_i^*}\rangle^{\Omega_k}$, thus increasing the probability to infer an incorrect value of $\tau_{i|\Omega_k}$ from $\tau^*_{i|\Omega_k}$. This usually induces a decrease in the largest achievable bit rate when the number of users increases. As an illustration, maintaining identical parameters to those above, we achieve a maximum of six users, resulting in an equivalent aggregate bit rate of 30 Gbits/s.

7.5.2 Encryption and Decryption with Overlapping Intervals

In this subsection, we use the theoretical framework presented in the previous chapter, where an intensity chaos generator has multiple feedback loops with cosine functions with different oscillation frequencies ω_i. We still consider an architecture with

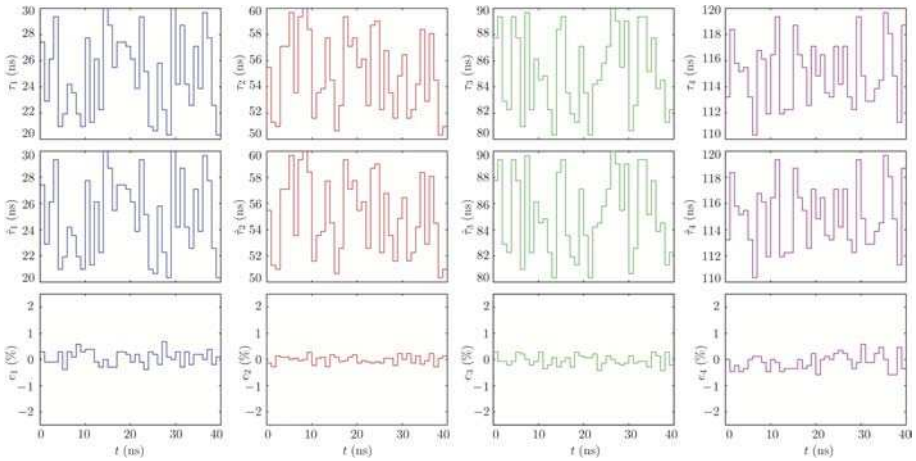

Figure 7.6: Simultaneous decryption of four messages composed of $M_i = 32$ symbols ($i = 1, \ldots, 4$) at 1 Giga symbols/s per user. The equivalent bit rate is 5 Gbits/s per user. The first line represents the input messages m_i, the second line the recovery messages $\hat{m}_i$, and the third line relative error e_i on each decrypted symbol in percentage. The equivalent aggregate bit rate is 20 Gbits/s. The metrics used are cross-correlation measurements.

four delayed feedback loops to transmit $n = 4$ independent messages. The system are modelled similar to Chapter 6 except that the time delays are time varying,

$$T\dot{x}_E + x_E + \frac{1}{\theta}\int_{t_0}^{t} x_E(u)du = \sum_{j=1}^{4} \beta_i \cos^2(\omega_i x_E(t-\tau_i(t)) + \varphi_{0i}), \quad (7.30)$$

$$T\dot{x}_R + x_R + \frac{1}{\theta}\int_{t_0}^{t} x_R(u)du = \sum_{j=1}^{4} \beta_i \cos^2(\omega_i x_E(t-\tau_i(t)) + \varphi_{0i}). \quad (7.31)$$

In this example, we consider the extreme case where the encryption slots completely overlap $\Delta_i = \Delta$. As we explain it later, this configuration appears to particularly interesting for security since the symbols used by the various users have identical values. The following numerical values are used in the simulation: $\beta_i = 30$, $\varphi_{0i} = i\frac{\pi}{4}$, $\Delta = [20\text{ ns}, 30\text{ ns}]$, and $\Delta\omega_{ij,i\neq j} = \omega_i - \omega_j = 1$ $(i = 1, \cdots, 4)$. With these values, the frequency detuning is large enough to ensure the decorrelation between the various carriers $s_{A_i}(t) = \beta\cos^2(\omega_i x_E(t-\tau_i(t)) + \varphi_{0i})$, thus leading to tractable decryption of each message independently.

Figure 7.7 shows an effective transmission at 5 Gbit/s per user with a low level of relative error when compared to those of disjoint intervals.

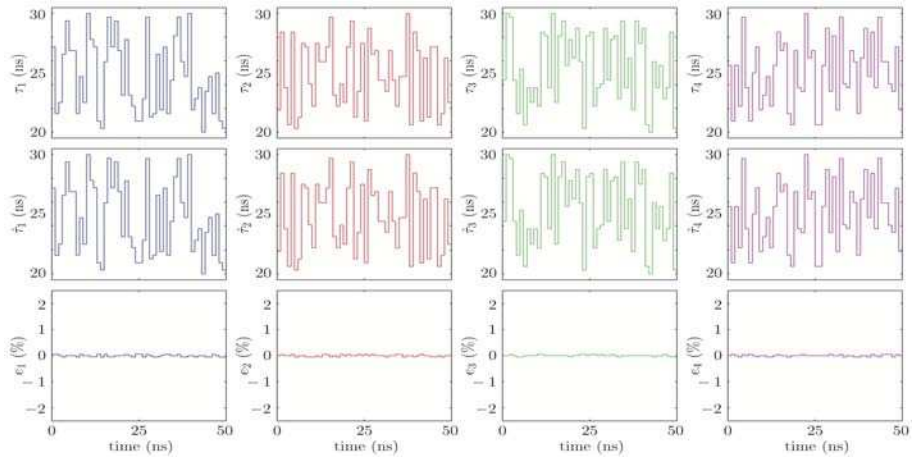

Figure 7.7: Simultaneous decryption of four messages composed with overlapping encryption slots. The structure of the figure is equivalent to that of Fig. 7.6. The equivalent aggregate bit rate is also 20 Gbits/s. The metrics used are cross-correlation measurements.

As explained above, the discrimination criterion relies here on the nonlinear functions that must produce the statistically decorrelated carriers to recover each message. With OEO-based architectures, the use of a cosine-square nonlinearity with different frequencies of oscillations gives a simple and flexible method to generate decorrelated carriers. However, in the general case producing such carriers is not easy and does not straightforwardly lead to the results observed with OEO. As an example, a numerical simulation was carried out with a Mackey-Glass system with two feedback loops to generate the signals used as carriers (similar to what was done with Eqs. 7.30-7.31). It resulted in systematic high BER if overlapping intervals

were considered due to the high correlation levels between the two carriers even when strongly mismatched parameters were used in each feedback loop.

7.6 Performance and Limitations

In this section, we analyze the performance and limitations of the proposed architecture when realized with an optoelectronic oscillator with multiple nonlinear delayed feedback loops. The performance of the system is characterized by the spectral efficiency and security in terms of time-delay identification. One of the key issues is the limitation on the number of users and on the bit rate due to the metrics used (for instance, correlation measurements). Indeed, the extraction of meaningful information is closely associated with the duration of a symbol T_s.

7.6.1 Spectral Properties and Efficiency

One of the principal objectives of multiplexed chaos-based architectures is the improvement of spectral efficiency. In the case of a single user, the proposed time-delay encryption technique can increase the intrinsic spectral efficiency of the carrier signal $s(t)$. In the case of an OEO, the increase of symbol rate $(1/T_s)$ and number of symbols M, as illustrated in Fig. 7.8, leaves the bandwidth (defined at -20 dB) unchanged. This is an extremely interesting feature of the proposed method in the case of a single message encrypted. However, when multiple users are consider, the use of several loops will affect the spectral properties of the multiplexed signal $s(t)$.

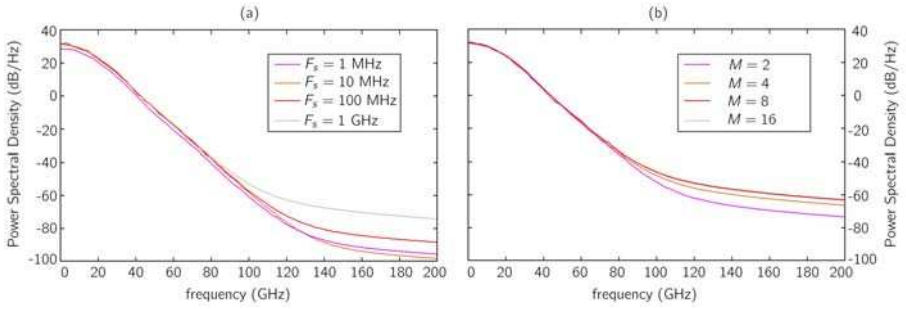

Figure 7.8: Power spectral density of the multiplexed carrier $s(t)$ in the case of a single user for an optoelectronic oscillator. (a) Influence of the symbol rate $F_s = 1/T_s$ for $M = 2$; (b) influence of the number of symbol at fixed symbol rate $F_s = 1$ GHz. The simulations have been realized with the following numerical values: $T = 25$ ps, $\theta = 5$ μs, $\beta = 5$, $\varphi_0 = \pi/4$ and $\Delta = [20\text{ ns}, 30\text{ ns}]$.

Although additional feedback loops induce an increase of bandwidth (see Fig. 7.9), there is a relative increase of spectral efficiency. In the context of optoelectronic oscillators, we monitor the evolution of the spectral properties of $s(t)$ as the number of loops increases. We notice that the bandwidth remains relatively unaffected by an increase in the number of loops, either with multiple disjoint (Fig. 7.9(a)) or overlapping encryption slots (Fig. 7.9(a)). Meanwhile, the quantity of transmitted information has been multiplied by four. If we denote W_n the bandwidth of the

architecture with n feedback loops and suppose that all the users at emitter transmit with identical bit rates $B_n = B$, then the relative increase of efficiency between a single and n users is $E = nW_1/W_n - 1$. In our cases, the bandwidths W_1 and W_4 are respectively measured as the spectral width 20 dB below the maximum value of the PSD. In each case, identical numerical values to those of Figs. 7.6 and 7.7 are used in the simulations. The bandwidths W_1 and W_4 are respectively measured 20 dB below the maximum value of the estimated PSD. When each of the four users is transmitting at 5 Gbit/s ($F_s = 1$GHz, $M_i = 32$), the percentage of relative increase of spectral efficiency is approximately 100 % when disjoint intervals are used and approximately 300 % when they completely overlap. These large values found their explanation first in the relatively small increase of bandwidth of the multiplexed signal when the number of loops in the case of disjoint encryption intervals and second in the relative decrease in bandwidth observed with overlapping encryption slots.

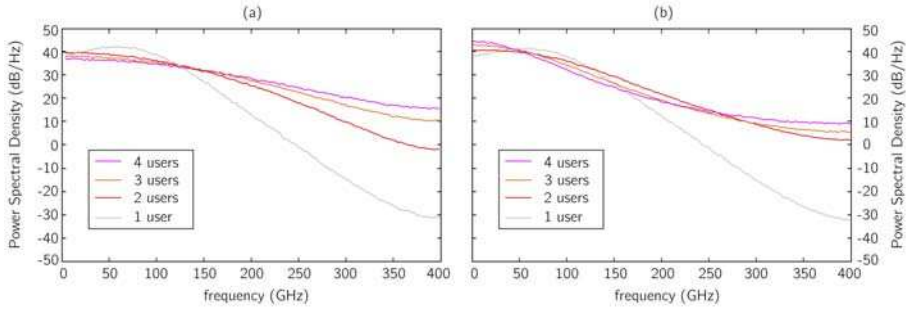

Figure 7.9: Analysis of the spectral efficiency of the architecture. The power spectral density of the multiplexed carrier $s(t)$ is represented for $n = 1, \ldots, 4$ users with identical 5 Gbit/s bit rate per user, when the encryption slots Δ_i are (a) disjoint or (b) overlapping. The numerical values used are $\beta_i = \beta = 20$, $\varphi_{0i} = i\pi/4$.

7.6.2 Bit-Rate Limitations with Low-Complexity Decryption

A possible solution to increase the bit-rate while using a low complexity decryption consists of minimizing the fluctuations of the metric's background (correlation or L^2-norm) that represents the primary source of errors when the bit rate increases, as illustrated in Fig. 7.10(a). In some cases such as the ICG, it is possible to improve the quality of the decoding by considering a modified optimization problem that will reduce the metric's fluctuations. It is assumed for the term $\langle s_{B_j,\tau_j}, s_{B_i,\tau_i^*} \rangle^{\Omega_k}$ to have approximately the same behavior for every pair $(\tau_i^*, \tau_j) \in \Delta_i \times \Delta_j$. Consequently, even without knowing which symbols are transmitted by the other users Alice$_j$, Bob$_i$ can boldly assume that τ_{j0} is always transmitted to attenuate strongly the variations of the term $\sum_{j=1, j\neq i}^{n} \left\langle s_{B_i,\tau_i^*}, s_{A_j,\tau_j} \right\rangle^{\Omega_k}$. If correlation measurements are used

as a metric, the optimization problem to solve becomes[1]

$$\hat{\tau}_i = \arg\max_{\tau_i^* \in \Delta_i} \left\{ \left\langle s, s_{B_i,\tau_i^*} \right\rangle^{\Omega_k} - \left\langle s_{B_i,\tau_i^*}, \sum_{j=1, j\neq i}^{n} s_{B_j,\tau_{j0}} \right\rangle^{\Omega_k} \right\}. \tag{7.32}$$

Figure 7.10(b) shows the elimination of the false positive detected by the optimization method (Eq. 7.24) in Fig. 7.10(a), the decrease in average of the correlation background value and minimization of its large fluctuations. However, it does not allow us to cancel all the false detection generated by a significant increase in bitrate (short values for T_s). For instance, when the transmission conditions are optimal, with $n = 4$ the BER is null when each user transmit at 1 Gsymbols/s and the standard optimization problem of Eq. 7.24 is used. If the symbol rate is doubled, then the BER is approximately 10^{-1}. Using the modified optimization problem (Eq. 7.32 and keeping the numerical values used previously, it allows one to improve on average the BER by a factor of approximately $2-3$. Figure 7.10 illustrates these results. Figure 7.10(a) depicts the evolution of $\langle s, s_{B_1,\theta}\rangle^{\Omega_k}$ for a time delay encrypted $\tau_{1|\Omega_k} = 21.5625$ ns. A sharp peak is located at $\theta = 21.6250$ ns but its amplitude is not a global extremum. In this particular case, the peak detected for the decryption correspond to $\hat{\tau}_{1|\Omega_k} = 27.6250$ ns thus leading to a decryption error. By considering the correcting quantity $\langle s - \sum_{j=2}^{4} s_{B_j,\tau_{j0}}, s_{B_1,\theta}\rangle^{\Omega_k}$, we observe a significant reduction of the oscillations of the correlation background as well as an enhancement of the peak located at $\theta = 21.6250$ ns that becomes the global extremum. As a consequence, the message encrypted by Alice_1 is properly decrypted. The improvement of the BER is illustrated in Fig. 7.10(c); the five previously corrupted bits are properly recovered, when Eq. 7.32 is used.

There exists a lower bound for the symbols' duration T_s under which systematic errors are generated with a LC decryption. This limit depends on the number of points to compute the metric (sampling rate) and on the typical time of fluctuations of signals $s_{A_i}(t)$. If one still wants to increase the bit rate at a fixed value of T_s, he has to increase the density of symbols used per encryption slot without violating the resolvability condition of the metric (necessary to ensure proper decryption). In our approach, the density of symbol in a given interval Δ_i is analog to the constellations used in conventional digital communications (e.g. quadrature amplitude modulation (QAM), phase-shift keying (PSK)). However, instead of being limited by the amount of energy attributed to each symbol, we are limited by the time separation in an encryption interval. In conventional digital communications, it is known that when the signal-to-noise ratio (SNR) is increased, the BER decreases thus leading to enhanced decryption.[2] When the channel is noisy, the symbols occupy a larger area in the energy plane (see Fig. 7.11(a)). Without channel coding, the symbols'

[1]The L^2-norm can also be used as a metric for

$$\hat{\tau}_i = \arg\min_{\tau_i^* \in \Delta_i} \left\{ \left\| s - s_{B_i,\tau_i^*} - \sum_{j=1, j\neq i}^{n} s_{B_j,\tau_{j0}} \right\|_2^{\Omega_k} \right\}.$$

[2]We do not account for the use of error control coding, that can optimize the BER at a given energy level. We simply give a general tendency of the BER as a function of the SNR.

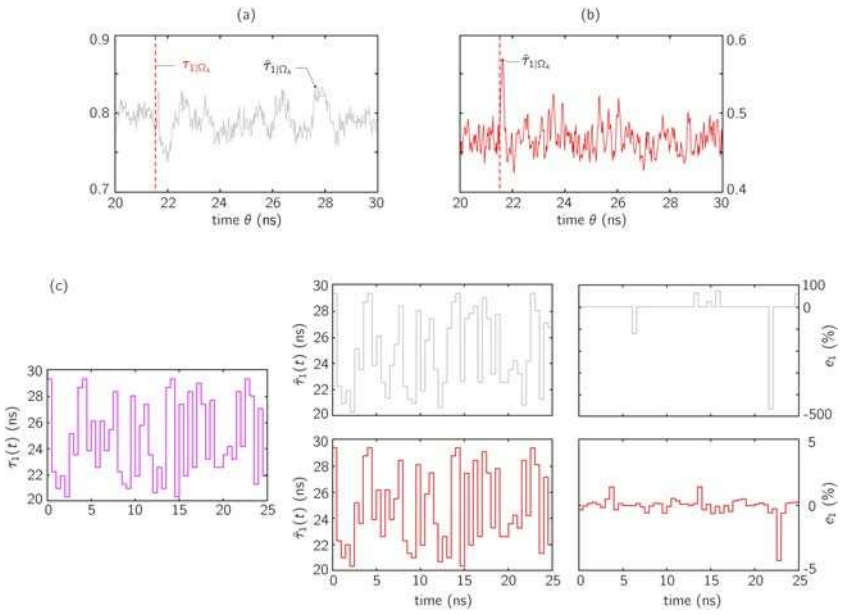

Figure 7.10: Decryption using the modified optimization problem with correlation measurements and a four-users architecture with $M_i = 32$ symbols ($i = 1, \ldots, 4$) at 2 Giga symbols/s per user. (a) Decryption of the message transmitted by Alice$_1$ using the LC optimization based on the evolution of $\langle s, s_{B_1,\theta} \rangle^{\Omega_k}$. (b) Decryption using the modified LC optimization based on the evolution of $\langle s - \sum_{j=2}^{4} s_{B_j,\tau_{j0}}, s_{B_1,\theta} \rangle^{\Omega_k}$. (c) Decrease of BER between the original (first row) and modified (second row) optimization problem on a sequence of 50 bits.

spheres must not intersect for the decryption to be error free. Therefore at a constant energy level, this limits the size of the constellation. However, with more energy per symbol (increase of SNR) it is possible to increase the size of the constellation and still maintain error-free decryption (see Fig. 7.11(b)). By analogy, the increase of energy per symbol in a constellation corresponds to enlarge the encryption slot Δ_i.

The noise induced by the communication channel scatters the position of each symbol in the quadrature plane (P, Q). In our architecture, we suppose first that the transmission is noiseless; otherwise it would disturb the chaos synchronization between E and R. In our case, the noise source comes from the computation of the metric. For instance, correlation measurements are calculated on finite time-slots Ω_k, therefore their resolution is limited. This loss of resolution can be interpreted as a noisy effect or uncertainty on the measurement. For the simulations in Fig. 7.6 the relative error of decryption is a few percent and it increases if the symbols' durations are reduced, because it becomes close to the limit in resolution of the metric. This naturally imposes a certain separation between the different symbol to ensure a proper decryption.

As an illustration, by considering an interval Δ_i with average length 1280 ns and $M = 256$ symbols, we maintain a density of 3.2 symbol/ns identical to the one used with $M = 32$ and an average length of the encryption slots of 10 ns. These values have proven to work well at 1 Gsymbol/s. Now, the binary representation of the alphabet requires 8 bits thus leading to a cumulative bit rate of 32 Gbit/s with four

users instead of the 20 Gbit/s previously reached with a 5 bits binary representation.

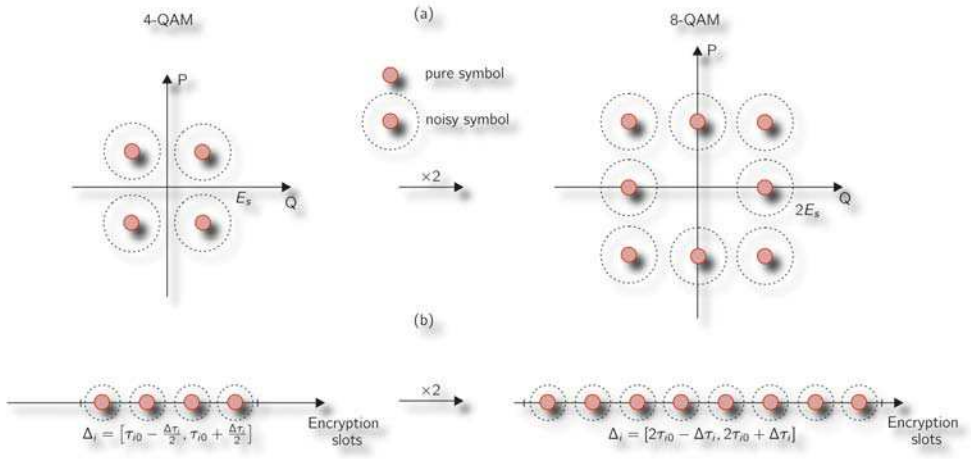

Figure 7.11: Analogy between constellation of symbols in M-ary digital coding and M-ary time-delay encoding with $M = 8$. (a) A 4-QAM is represented in the plane of the two quadrature (P, Q) with energy E_s and 8-QAM with energy $2E_s$ (b) Time-delay encoding in Δ_i with $M_i = 4$ and in $2\Delta_i$ with $M_i = 8$. The noise in the case of time-delay-based decoding is related to the limit of resolution of correlation measurements calculated on time slot Ω_k.The noisy symbols are represented by disc, whose radius correspond at the scattering at 3σ induced by a Gaussian noise $N(0, \sigma^2)$.

7.7 Security and Cryptanalysis

The security (with respect to time-delay identification) in our approach benefits from the fast stochastic and independent oscillations of each time delay on which data is encoded. It is known that fixed time-delay systems face security flaws when the values of the time delays are known. Despite their high dimensionality, an eavesdropper can attack these systems in a low-dimensional space corresponding to its actual state space dimension and where the nonlinear function of the system is identifiable at a low computational cost, thus allowing for an easy reconstruction of the emitter dynamics by analyzing the time series of the transmitted signal. Our approach corresponds to a generalization of time-delay commutations with a the single feedback case ($n = 1$, $M_1 = 2$) proposed in [146], except that in our architecture the commutations are controlled by sources of information. In a single feedback loop case with random commutation, it has been shown that a commutation time T_s smaller than the smallest symbol value could prevent an eavesdropper from sequentially cracking the cryptosystem using sections of the transmitted time series of length T_s where the delays are maintained constant.

More precisely, by considering a system with a single discrete time-varying time delay $\tau_1 \in [\tau_{10} - \Delta\tau_1/2, \tau_{10} + \Delta\tau_1/2]$ and $T_s > \min_{\Delta_1} \tau_1(t)$, an eavesdropper can theoretically perform a time-delay estimation on each time-slot $\Omega_k = [kT_s, (k + 1)T_s]$. Indeed, the detection of the a resonance associated to τ_1 is possible only if this value belongs to $\Omega_k \mod (T_s)$. Assuming now that the commutation time is

faster than the smallest value of $\tau_1(t)$, then it will be necessary for Eve to use at least $\lfloor(\max_{\Delta_1}\tau_1 - \min_{\Delta_1}\tau_1)/T_s\rfloor$ intervals to perform the detection of a resonance associated to a time delay used to encrypt a message. Meanwhile, the time delay undergoes many variations, such that an eavesdropper will detect the time-delay signatures but not their respective time of emission. This principle remains true in the multi-users case. Thus, to fulfill security requirements in our case, it is necessary for the symbol duration to satisfy the inequality

$$T_s < \min_{i,k} \tau_{i|\Omega_k}, \tag{7.33}$$

which naturally generalizes [146] and gives an upper bound to the symbol duration for the all time delays to be simultaneously concealed, when $s(t)$ is analyzed. In the most favorable scenario for the eavesdropper, a symbol's identification is possible, but the actual message remains unknown.

As an illustration, we have performed a security analysis in terms of time-delay identification using delayed mutual information (DMI, see Chapter 4). Our findings are presented in Fig. 7.12. We study an intensity chaos generator (ICG) with a single stochastic-delayed loop and analyze the impact on security of the frequency of commutation ($F_s = 1/T_s$), the number of symbols (M), and the nonlinear gain (β). Figure 7.12(a) presents a typical timedelay identification performed by an eavesdropper ignoring the exact moments of the time-delay commutations with frequency F_s satisfying the condition in Eq. A.42 and $M = 4$. Interestingly, linear combinations of the time delays are also observed (marked by red bullets). To understand the orgin of these side signatures, we consider the two-delay case (τ_{10} and τ_{11} with $M_1 = 2$). The multiplexed signal $s(t)$ is formally equivalent to a system with two loops and constant time delays activated by a function $\alpha_0(t) = \{0, 1\}$ that switches only at times $t = kT_s$ and keeps its value constant otherwise: $s(t) = \alpha_0(t)[\beta\cos^2(x_E(t-\tau_{10})+\varphi_0)] + (1-\alpha_0(t))[\beta\cos^2(x_E(t-\tau_{11})+\varphi_0)]$. In such a system with multiple loops, it is known that combinations of time delays will be observed. This is why linear combinations ($\tau_{11} \pm \tau_{10}$) of time delays are detected in our architectures when DMI is used.

At weak nonlinear gain β and a low symbol density (0.2 symbol/ns) and only two symbols ($M_1 = 2$), the frequency of commutation does not erase the time-delay signatures; it even enhances their amplitude (Fig. 7.12(b)). The number M_i of symbols used to encode Alice$_i$'s data source plays an fundamental role in the architecture's security. Indeed, if a realistic data source is employed, it may present repetitive patterns. This is particularly true in the case of binary data streams. The consecutive repetition of the same bit during many periods T_s increases the probability for an eavesdropper to access information about the system and the transmitted messages. However, if instead of encoding a binary digit of information on two time-delay values, blocks of $\log_2 M_i$ bits are used; they can capture large repetitive structures of bits and encode them as single time-delay values. Furthermore, if the density of symbols per encryption slot is increased, the individual symbol signatures become more fuzzy (Fig. 7.12(c)). Finally, as $M_i/|\Delta_i|$ is growing and if T_s is small enough, it increases the number of values to commute between and, thus, the fast digital random commutations can be considered as acting close to a

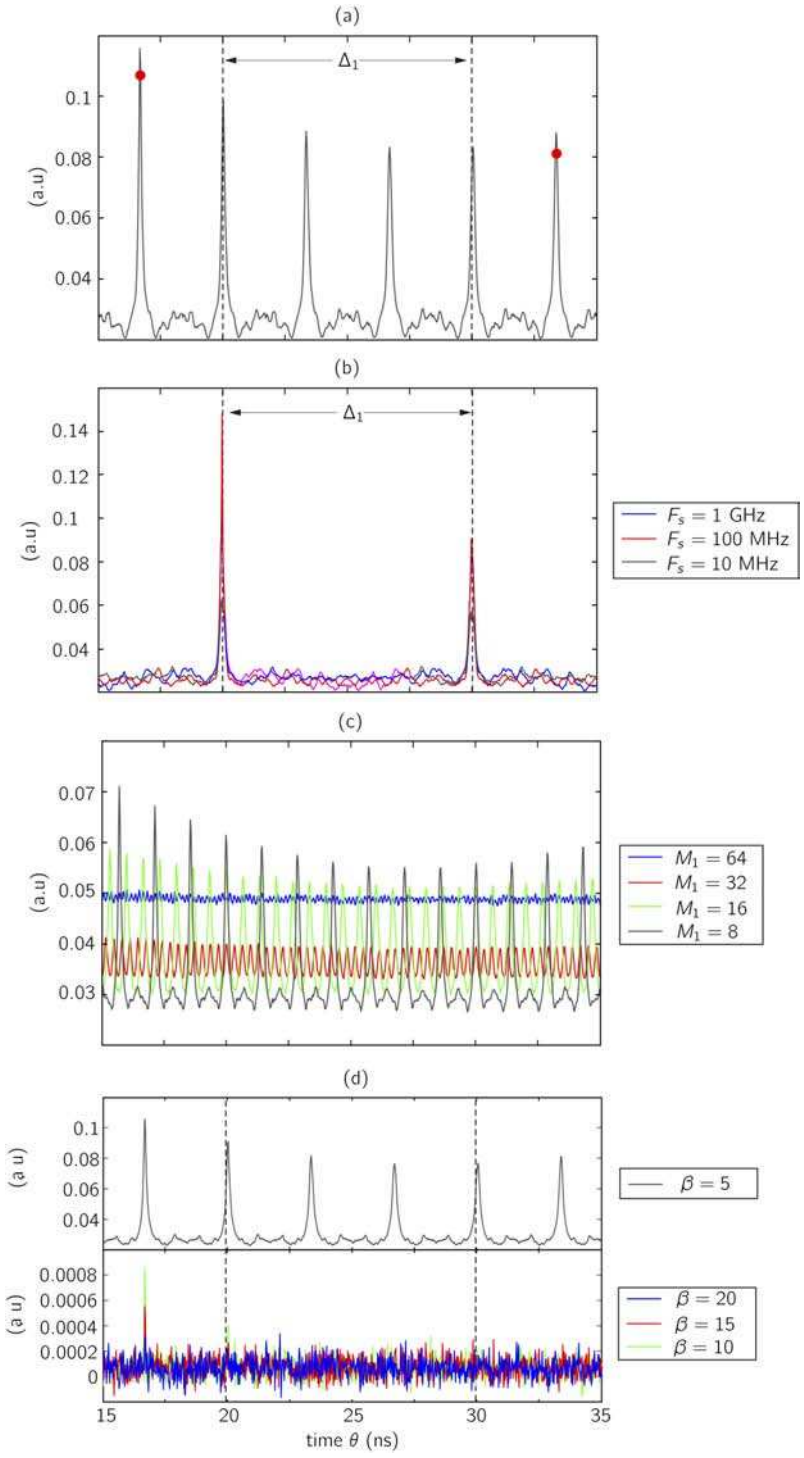

Figure 7.12: Security of our architecture based on an OEO for a single user (see Eq. 7.26). (a) Side time-delay signatures marked by red dots when $M_1 = 4$, $F_s = 1$ GHz, $\beta = 5$, and $\varphi_0 = \pi/4$. (b) Influence of the commutation frequency frequency $F_s = 1/T_s$ with $M_1 = 2$, $\beta = 5$, $\varphi_0 = \pi/4$. (c) Influence of the density of symbols $M_1/|\Delta_1|$ with $F_s = 1$ GHz, $\beta = 5$, $\varphi_0 = \pi/4$, and $|\Delta_1| = 10$ ns. (d) Influence of the nonlinear gain β with $F_s = 1$ GHz, $M_1 = 4$, and $\varphi_0 = \pi/4$.

continuous-valued continuous-time stochastic process for which security with respect to correlation-based (or DMI-based) attacks has been demonstrated [176].

Therefore, this suggests that the Alices should employ sets of symbols as large and dense as possible to tend to a stochastic evolution of the delay. Nevertheless, the decryption method intrinsically limits the density of symbols to be encoded per finite-size encryption slot beacuse of its finite resolution (see Condition (iii)), and the equivalent achievable bit rate. As far as OEO with fixed delayed feedback loop are concerned (ICG, WCG, or PCG), the increase of the feedback gain β leads to the decrease of the magnitude of the time-delay signature without its complete cancellation. With randomly commutated time delays, however, the signature totally disappears even when the density of symbol is not high (Fig. 7.12(d)). Thus, a trade-off can be found between the nonlinear strength, the commutations' rate, and the symbol density to ensure fast and secured transmission.

The analysis above has unveiled the driving principles that ensure a high level of security for a single stochastic delayed feedback system. They can be applied individually to the case of multiple users. As an illustration, in Fig. 7.13 we have numerically investigated the security of the structure described by Eq. 7.26 in the case of disjoint and overlapping intervals. The density of symbols is 3.2 symbols/ns, the nonlinear gain is strong $\beta = 20$, and the frequency of commutation is fast $F_s = 1/T_s = 1$ GHz.

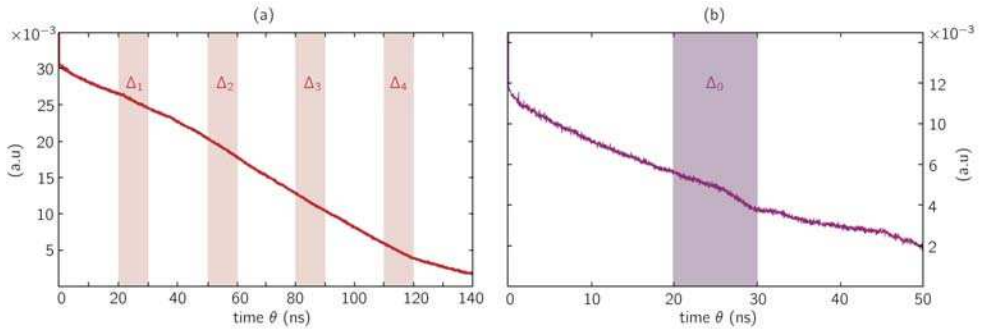

Figure 7.13: Security analysis of the architecture based on the delayed-mutual information estimator (DMI) with $n = 4$ users and (a) disjoint or (b) totally overlapping encryption slots. The nonlinear gain is identical for all nonlinear function in (a) and (b), $F_s = 1$ GHz, $\beta_i = 20$, $F_s = 1$ GHz and $M_i = 32$, thus leading to a density of 3.2 symbols/ns.

In these conditions, we see that no time-delay signatures are retrieved while using DMI regardless of the type encryption chosen. However, the case for which encryption slots Δ_i completely overlaps will provide a higher level of security. Indeed, if an eavesdropper perform a time-delay estimation based on the signal $s(t)$ and that he can (in the best-case scenario) recover the time delays used to encode the symbols, he cannot determine *a priori* how many users are using a given set of symbols, when the symbols are emitted and by whom. Consequently, this encryption is more secure than its counterpart with disjoint encryption slots for which the users can be more easily identified based on the time-delay values.

7.8 Conclusions

In this chapter, we have demonstrated the ability of a cryptosystem to encrypt n different messages using a single nonlinear oscillator subjected to n time-delayed feedback loops and to decrypt these messages using a synchronization-based technique. Our method combines the randomness of the data sources and the hyperchaotic behavior of time-delay systems in an efficient and secure way. The messages are encrypted through digital modulation of the time delays of each loop while respecting certain rules to guarantee the decryption at the receiving end. Two types of encryption have been devised to encode the message's symbol onto a time-delay: the use of (i) disjoint encryption slots Δ_i or (ii) overlapping intervals. In Configuration (i) freedom is given to the choice of the nonlinear function that carries the modulated time-delay information, whereas for Configuration (ii) the nonlinear function have to ensure proper decorrelation between the various carrier and ensure a decryption without crosstalk.

When applied to an optoelectronic oscillator, such as the intensity chaos generator, our approach has proven to theoretically achieve multi-Gbit/s transmission with multiple users while preserving a low level of computation complexity for the decryption, linearly increasing with the number of users. The increase of spectral efficiency of the architecture is significant as the number of user increases, the use of overlapping encryption intervals ensuring a higher level of performance. Furthermore, the level of security is considerably enhanced, the existing method of identification (ACF, DMI, LLM, or GNM) does not reveal any leak of information on the modulation of the time delay if the density of symbols is large and the period of switching is smaller that the minimum time-delay value used by the users to encrypt the data. Therefore, this may offer perspectives towards efficient multi-user chaos-based communications with a high level of security.

Chapter 8

Conclusion

Abstract

We recall our main results on security of optical-chaos cryptography, multiplexing, and multi-user private communications. We also propose perspectives and future directions for our research.

8.1 Summary of the Results

Optical chaos-based communications have attracted considerable attention since high-bit-rate physical-layer security has been achieved by exploiting the natural instabilities existing in optoelectronic systems. This type of communication exploits the noise-like appearance of a chaotic carrier to conceal an information-bearing message. Then, with the property of *chaos synchronization* the message is decrypted at the receiving end. The type of systems used as crypto-generators are mainly edge-emitting lasers (EEL) or vertical-cavity surface-emitting lasers (VCSEL) in various configurations (optical or optoelectronic feedback, current modulation, optical injection), optoelectronic oscillators (wavelength, intensity, or phase chaos generators), and erbium-doped fiber ring lasers (EDFRL).

Within this particular framework, a particular focus was given to fundamental properties of optical chaos synchronization, bifurcation mechanisms, and dynamical regimes of these various systems transmitting a single data stream, while using conventional chaos encryption techniques (chaos masking (CMa), chaos-shift keying (CSK), or chaos modulation (CMo)).

We have identified two open problems of fundamental importance that may prevent a large-scale deployment of optical-chaos cryptography in current optical networks: the *quantification of security* of optical cryptosystems and the possibility to *multiplex multiple chaotic optical signals* to simultaneously transmit several data streams in a single communication channel with a high level of privacy.

In this thesis, we addressed the questions of security for the class of external cavity semi-conductor lasers (ECSL) and of multiplexing using different systems (ECSL, or electro-optic chaos generators) and demonstrated theoretically the possibility of multi-user communications.

8.1.1 Security Analysis of Chaotic Optoelectronic Devices

In Chapter 4, we have analyzed the security of an ECSL in terms of time-delay identification. Indeed, the use of a time-delay system is known as a simple method to generate high-dimensional chaos, which is a desirable property to prevent the most threatening attacks (reconstruction or forecasting techniques) performed by an eavesdropper. The resulting computational security depends on the knowledge of the time delay by the eavesdropper. Therefore, it is critical to conceal this value to avoid attacks on the system in a low-dimensional phase space. With optoelectronic devices, the time-delay identification is performed on the light intensity wiretapped from the communication channel and analyzed by standard time-delay estimators such as the autocovariance function (ACF), the delayed-mutual information (DMI), or global nonlinear models (GNM). First, we have demonstrated the key role of the tunable and operational ECSL parameters on the time-delay concealment: the feedback strength (η), the pumping current (J), and the choice of the time-delay (τ, TD) value in comparison with the relaxation-oscillation period (τ_{RO}, ROP). We have also highlighted the scenarios of difficult time-delay identification (TD signature invisible or strongly perturbated in the estimators) that occur for a combination of relatively weak feedback rates, weak pumping currents, and close values of the two

time-scales TD and ROP. Second, we linked the origin of the difficult identifications with the specific nonlinear dynamics and time-scales appearing in the ECSL during its bifurcation cascade leading to chaos. At weak feedback rates, the ECSL's chaotic dynamics is reminiscent of the time scales involved in the early stages of its dynamics, such as the undamped relaxation-oscillation (UROP) time-scale and possibly time scales of Period-Doubling and Quasi-Periodic dynamics (if these routes are taken by the ECSL). In these chaotic regimes, the time-delay estimators exhibit complex modulated shapes typical of the presence of those various ECSL time scales. When TD and ROP are close to each other, the true value of the time delay is efficiently concealed in various ways: (1) significant shift of the location of the strongly-damped TD signature and (2) complete disappearance of the time-delay signature replaced by relaxed oscillations. The choice between these two generic types of concealment is made by the system as it undergoes its route to chaos. If the time delay does not appear in the early stages of the ECSL dynamics, Scenario (2) will be observed. Otherwise, it will be Scenario (1) that ensures an imperfect concealment (an experienced eavesdropper could still infer partial knowledge on the TD). The influence of some of the internal parameters of the lasers has been also investigated. We have identified that they may impact the range of the operational parameters for which a good time-delay concealment is ensured. Finally, the robustness of our results has been checked with other signal processing techniques such as neural networks, filling-factor methods, or statistics of extrema. Our results are of particular interest for designing a chaotic emitter based on an ECSL with the best concealment of its critical system parameters, hence also improving overall security in optical chaos-based communications using semiconductor-laser technologies.

8.1.2 Chaos Multiplexing and Multi-User Communications

In the second topic of the thesis, we studied various configurations and encryption methods to increase the spectral efficiency of optical chaos-based cryptosystems. We have devoted our attention to fundamental properties of chaos-synchronization of multiple chaotic lasers, and optoelectronic systems with multiple delayed nonlinear feedbacks. We have also addressed key issues on multiplexing and demultiplexing of digital information with these different architectures.

In Chapter 5, we have reported the possibility to multiplex chaotic optical fields generated by multiple edge-emitting semiconductor lasers (EELs). At the emission, the various optical fields are combined inside a shared external optical cavity into a single multiplexed signal. Each master laser (M_k, $k = 1, \ldots, n$) at the emitting side is optically injected by the other lasers with specific coupling strengths and time delays. The multiplexed signal is then unidirectionally sent through an optical channel and injects decoupled slaves lasers (S_k). The EELs are damped-relaxed or passive oscillators that require external degrees of freedom to exhibit chaotic behavior. The multiplexed electric field is considered as a driving signal for both the master and the slave of a given pair M_k/S_k. Our architecture, which is a generalization of the classical single-emitter/single-receiver synchronization problem, can be seen as an active-passive decomposition (APD) problem. Under the right necessary coupling conditions, we have demonstrated that each pair of lasers could completely syn-

chronize with specific lag times. These coupling conditions correspond to a similar injection strength of the multiplexed field to the master and to the slave of a given pair; the time lag being the time difference between the flight time in the communication channel with the optical delay associated to the corresponding arm of the shared cavity. The system being modelled in the Lang-Kobayashi framework, we unveiled several properties on the stability of the synchronization manifolds. Through a numerical analysis, we have shown that:

- The region in the $2n-$dimension operational parameters space (pumping currents of each master and injection strengths), for which complete chaos synchronization is achieved for each pair, is large. We also highlighted the existence of hybrid regimes where only specific pairs of lasers are synchronized.

- The synchronization manifold is robust with respect to intrinsic noise source (such as the spontaneous-emission noise), but the quality of synchronization degrades.

- The synchronization manifold is robust with respect to parameter mismatch (both internal and operational) between the master and the slave lasers of a given pair. Similar performance to those of the single-emitter/single-receiver case were observed. However, there are no limitations in the amount of mismatch between two different pairs.

Finally, we addressed the question of multiplexing information. We adapted conventional encryption techniques for digital messages to the multi-user case. Only CSK and CMo could be applied to our context, where uncoded messages are used. The use of CMa resulted in a partial loss of information (some combinations of bit/symbol could not be recovered). With EEL systems,

- CSK is performed by modulating the pumping current of each laser between two different levels ($J^m_{k,0}$ and $J^m_{k,1}$). Subsequently, each master M_k ($k = 1, \ldots, n$) jumps from a chaotic attractor to another one depending on the pumping current. The resulting multiplexed field can therefore be generated by 2^n different combinations of chaotic attractors (associated with each master laser) and will lead to an exponentially complex decryption, possible by the existence of chaos synchronization. However, the transition between a combination of attractors to another one is bounded by the resynchronization time, which intrinsically limits the maximum achievable bitrate (several hundreds of Mbit/s per user in our context). Different decryption strategies can be devised with either a linear or exponential computational complexity. The use of $2n$ receivers was first proposed (for each master M_k, two slaves $\mathrm{S}_{k,0}$ and $\mathrm{S}_{k,1}$ respectively pumped with the currents $J^m_{k,0}$ and $J^m_{k,1}$). Candidate combinations (2^n) are generated and subtracted from the multiplexed field before being detected by a photodiode. A minimum is observed, when a combination of n pumping currents at the receiving end matches the one used at the emitting end, and it serves as the decrypted values for the n messages at once. The complexity of this method is exponential. Another possibility consists of using n receivers and set each

of them with either one of the two pumping currents ($J_k^s = J_{k,0/1}^m$) used by their corresponding master. To recover the kth message, the kth optical field is then subtracted from the multiplexed field and the result is photodetected. The messages are recovered because of dropouts in the amplitude of the detector's output (when the pumping current of kth slave matches that of the kth master) that correspond to the cancellation of kth master field from the multiplexed field. This method is suboptimal and does not ensure a perfect discrimination threshold between the transmitted bits, but its computational complexity is linear with the number of messages.

- CMo is performed by encoding each user's message either on the amplitude or the phase of the optical field of his corresponding master. This requires the modification of the original setup by including an optical circulation. The main advantage over the CSK method is that the various messages participate to the dynamics of each emitter M_k and therefore a single chaotic attractor is used per laser. This prevents the limitations in terms of bit rate and quality of synchronization imposed by the resynchronization time in CSK. In terms of decryption, the CMo suffers from the same computational complexity issues as those of CSK and the decryption strategies are essentially identical to those exposed hereinbefore. We demonstrated numerically the possibility to encrypt two messages at 1 Gbit/s using either exponentially- or linearly-complex decryption.

Our architecture could be easily generalized to a larger number of users and handle private communications for large optical networks. It constitutes a first natural extension of the classical paradigm of private transmission of a single message using chaotic optoelectronic devices.

In Chapter 6, we have proposed to go beyond the traditional optical chaos cryptography relying essentially on CMa, CSK, or CMo. We were aiming at applying code-division multiple access (CDMA) approaches to chaotic optoelectronic devices. CDMA is a multiplexing technique widely employed in conventional communications and contrary to time- or wavelength- division multiplexing (TDM or WDM), it offers the entire channel's bandwidth at all times for every user. The discrimination is made at the statistical level and not by the time of emission (TDM) or the frequency range (WDM). In conventional multi-user communications, CDMA makes use of multiple fixed pseudo-random binary signals (known as *codes*) to spread out the spectrum of various data streams, which then are modulated and summed to overlap spectrally. At the receiver, the codes are available and used to recover the data with correlation-based detection. These codes are orthogonal (with respect to a particular inner product) and guarantee a linear complexity of decryption. These are desirable properties that we have transposed to the context of optical chaos-based communications. The main issue was the time-varying nature of the *chaotic codes* employed, changing for every bit transmitted. We proposed to use an electro-optic oscillator (EOO) with multiple delayed feedback loops, with a different cosine-square nonlinearity generated by each Mach-Zehnder modulator. Each of these nonlinearities will be used as a chaotic code to spread, modulate, and transmit a specific user's data stream. The chaotic codes have to be recombined into a single multiplexed

signal before being reinjected in the dynamics of the EOO. Two configurations have been investigated:

- Configuration (1) uses multiple photo-detectors, one per optical arm. This results in an electrical multiplexed signal comprised of a sum of cosine-square nonlinearities.

- Configuration (2) uses a single photo-detector. This results in a single optical multiplexed signal that is later electro-optically converted. Depending on the characteristic of the optical sources and optical arms used, interference may (Configuration (2a)) or not (Configuration (2b), with multiple CW laser sources emitting at different frequencies) appear, thus affecting the dynamics of the EOO architecture. In this configuration, the multiplexed signal is not necessarily a sum of cosine square functions.

For each configuration, the multiplexed signal is then transmitted to a physical copy of the EOO emitter. Chaos synchronization is ensured thanks to an APD-like structure of the overall transmission chain. In the various configurations, obtaining orthogonality (decorrelation) between the different codes is desirable to allow a large number of users to communicate and ensure a linearly-complex correlation-based decryption. The statistical properties of the code are controlled by the following parameters the external gain (β_i), the frequency of the nonlinearity (ω_i, physically an internal gain), and a phase-shift (φ_{0i}). We unveil that a combination of large values of β_i and frequency detuning ($\Delta\omega_{ij} = \omega_j - \omega_i$) ensures a quasi perfect orthogonality. We also devised several decoding strategies and demonstrated numerically private multi-user transmissions at 2.5 Gbit/s per user (bit rate of the OC-48 standard). When interference is considered in the model, performance slightly degrades but the independent recovery of multiple messages is still possible, providing an adaptation of the decoding formula.

Finally in Chapter 7, we proposed an architecture that encompasses the two aspects developed in this thesis: the security in term of time-delay concealment and the multi-user communications. We consider a nonlinear oscillator with multiple delayed nonlinear feedback loops, whose time delays are digitally modulated on M different levels (associated with $M-$ary messages) by legitimate users Alice$_i$ ($i = 1, \ldots, n$). Each time-delay varies discretely in a specific encryption slot (Δ_i, $i = 1, \ldots, n$). Two encryption strategies were devised:

- Configuration (1): disjoint encryption intervals are used, with no restriction on the choice of the nonlinear functions.

- Configuration (2): overlapping encryption intervals are used, the nonlinear functions are carefully chosen.

Each time-delay-modulated nonlinearity carries a specific user's data stream; they are all combined into a single multiplexed signal that drives the dynamics of both the emitter (E) and receiver (R). The decryption strategies for legitimate users to exchange securely information rely on the calculation of a particular metric (cross-correlation or L^2-norm) between the multiplexed signal and the various candidate

carriers, identical to those used by Alice$_i$ except for the knowledge of the time delay. The time delays can be inferred jointly (exponentially complex calculations) or independently (linearly complex calculations) by finding the maximum (or minimum) argument of the metric. The principle of our architecture has been numerically verified by simulating an electro-optic oscillator (EOO): A four-users-transmission at 5 Gbits/s per user was achieved. The security was also evaluated using standard time-delay estimators such as the delayed mutual information (DMI). We have highlighted the key roles of the density of symbols per encryption slot ($M/|\Delta_i|$) and the symbol rate on the security. When these two encryption parameters are properly chosen, the time-delay signatures (associated with M different levels) were perfectly concealed.

Our method combines the randomness of the data sources and the hyperchaoticity of time-delay systems, and offers perspectives in terms of bit rate, spectral efficiency, and privacy enhancement for future multi-user optical chaos-based communications.

8.2 Perspectives

In future research, we will complement the two axes developed in this thesis: (1) security analysis and (2) chaos multiplexing and multi-user communications. The following section presents various points that could lead to complementary results in our current research.

8.2.1 Perspectives on Security Analysis

- Our security analysis has revealed that ECSL, contrary to common knowledge, can exhibit a high level of confidentiality with respect to the time-delay identification. This result has been interpreted from a dynamical point of view; however, there are still configurations that require additional study. Configurations for which the relaxation-oscillation period τ_{RO} is greater than the time delay τ (the so-called *short-cavity* regime) have to be investigated and their level of security has to be compared to the cases studied in the thesis where τ_{RO} was smaller than τ (the so-called *long-cavity* regimes). The short-cavity configurations could be more efficient than the long-cavity ones by ensuring for instance a larger parameter range (feedback strength and pumping current) for the time-delay signature concealment. The identification of the complete structure of the ECLS and its remaining parameters based on the analysis of a single scalar intensity time series is also a possible direction.

- Our findings are based on theoretical and numerical simulations; the realization of an experimental setup to implement the optimized concealment scenarios would allow us to quantify performance in real conditions.

8.2.2 Perspectives on Chaos Multiplexing and Multi-User Communications

- **Multiplexing optical chaos using ECSL**. Our setup has highlighted for the first time a method to multiplex optical signals generated by coupled ECSLs.

The synchronization and the evolution in size of the parameter space (allowing the existence of synchronization) with an increasing number of lasers is crucial to the generalization of our multiplexing architecture. Our architecture could be also used to generate orthogonal optical signals to perform CDMA-like encryption, similar to our work with chaotic electro-optical oscillators with multiple loops. The difference would be that signals are generated by multiple chaotic oscillators. This would require a detailed analysis of the influence of internal and coupling parameters on the orthogonality.

The realization of an experimental setup starting with two pairs of lasers constitutes a major perspective of our work. This investigation could also trigger the application of our approach to other types of systems that are known to be less sensitive to external perturbations such as integrated external-cavity lasers or lasers with optoelectronic feedback. Finally, a detailed security analysis has to be performed to quantify the potential enhancement of privacy due to the use of multiple coupled systems with the various encryption setups studied: CMa, CSK, and CMo.

- **Generation of Code using Electro-optic Generators**. We have proposed various configurations for a multiplexing architecture based on electro-optic oscillators (EOO) with multiple feedback loops. The complexity of the decoding equation in the configuration with interference and the limitations in term of bit rate are two significant limitations that results mainly from our encryption strategy. Investigating alternate structures of EOO to prevent interference and new encryption strategies are important issues that deserve additional studies. Hitherto, our encryption and decryption methods have been tested only in optimal transmission conditions. Performance of the architecture must also be evaluated in more realistic condition, in the presence of noise and parameter mismatch, to probe the fundamental limits. This would pave the way toward successful implementation of an experimental setup.

Appendix A

Résumé de Thèse en Français

A.1 Introduction Générale

Les technologies optoélectroniques ont fortement contribué au développement des télécommunications optiques modernes (par exemple, sources laser, amplificateurs performants et compacts, et fibres optique). Ces réseaux possèdent une structure par couches, comme définie par la représentation OSI (*open system interconnexion*), comprenant une couche physique de bas niveau (associée au support physique du signal, optique ou électrique), et des couches haut niveaux : liaison de données, réseau, transport, session, présentation et application. Cette architecture modulaire offre cependant de nombreuses failles de sécurité menaçant l'intégrité du réseau de communication. L'essentiel des efforts de protection des systèmes de communication s'est attaché à l'utilisation et à l'amélioration constante de techniques de cryptographie mathématique. Dans cette approche, un algorithme mélange un message clair (*plain text*) avec une clé (*key*) afin que deux parties légitimes (dénomées traditionellement Alice et Bob) puissent échanger des données cryptées (*cipher text*) difficilement interprétables par un espion (dénommé Eve). Ce n'est que récemment que la couche physique a suscité l'intérêt de la communauté scientifique. Il est à présent possible d'utiliser directement les propriétés physiques du signal porteur d'information afin d'apporter un niveau de confidentialité supplémentaire. Deux solutions ont été largement étudiées :

- **Les Communications Quantiques** utilisant la nature probabiliste des photons (assurée par la mécanique quantique) afin de transmettre des informations sensibles tout en guarantissant une sécurité inconditionnelle (au sens de la théorie de l'information) [3].

- **Les Communications Chaotiques** utilisant les instabilités existant dans certaines sources optiques afin de générer des signaux pseudo-aléatoires de forte complexité dans lesquels des informations seront cachées. Cette approche garantit une sécurité algorithmique similaire à celle produite par certaines méthodes mathématiques (RSA et PGP par exemple) [9].

A l'heure actuelle, les systèmes de communication quantiques, malgré leur haut degré de confidentialité, n'offrent malheureusement que des débits limités (quelques

kbit/s) sur de courtes distances (quelques dizaines de km) et sont essentiellement utilisés pour l'échange de clés (*quantum key distribution* ou QKD). Les systèmes optiques chaotiques, au contraire, ont de larges bandes passantes, permettant l'échange de données à haut-débit (plusieurs Gbit/s) sur de larges distances [4].

Une architecture de communication par chaos optique comprend deux oscillateurs chaotiques structurellement identiques (paramètres et non-linéarité) propriétés respectives d'Alice et Bob, et situés à chacune des extrémités d'un canal de communication optique. En début de chaîne, Alice encode son message et l'incorpore au moyen d'une méthode appropriée au signal chaotique avant d'injecter le résultat de l'encryption dans le canal. En fin de chaîne, le récepteur de Bob se synchronise uniquement sur le chaos produit par Alice (la partie déterministe du signal) et une opération de soustraction est ensuite utilisée pour extraire les données encryptées. La Figure A.1 synthétise ces différentes informations.

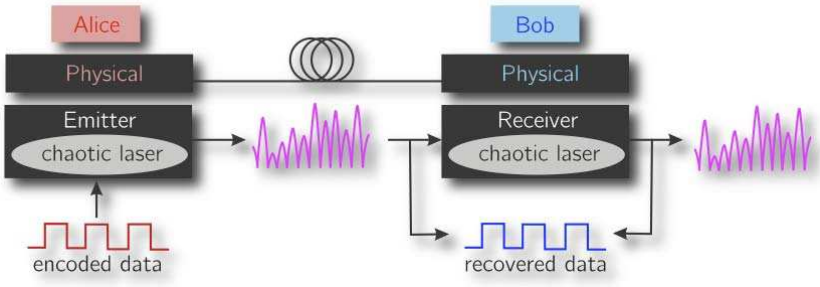

Figure A.1: Principe des communications sécurisées au niveau de la couche physique utilisant des systèmes optoélectroniques chaotiques.

Le développement des communications chaotiques optiques résulte de trois phénomènes physiques: (i) l'émission stimulée mise en évidence par Einstein (le principe physique utilisé dans les lasers), (ii) la théorie du chaos donnant un cadre mathématique aux comportements erratiques de certains systèmes non-linéaires, et enfin, (iii) la synchronisation des systèmes chaotiques. Malgré leurs performances en terme de complexité algorithmique et leurs larges bandes passantes, les communications par chaos optique demeurent marginales principalement en raison des difficultés à caractériser leur *sécurité* et à les utiliser dans un contexte multi-utilisateurs.

La recherche effectuée dans le cadre de cette thèse a contribué à l'avancement de ces deux questions ouvertes. Ce résumé vise à en rappeler les principaux résultats.

Dans la premiere section, nous nous sommes intéressés à la sécurité d'une classe particulière de générateur optique, celle des lasers à semi-conducteur à cavité externe (ECSL). Nous nous proposons de prendre la place d'Eve et d'attaquer ce système dans un contexte d'analyse difficile, celui pour lequel aucune information n'est *a priori* disponible. L'intensité optique en sortie du laser chaotique est enregistrée et analysée par le biais de techniques d'outils statistiques des séries temporelles. Dans le cadre de la thèse, la sécurité est comprise comme étant la quantité d'information pouvant être extraite de certains paramètres critiques du système (analogue d'une clé de cryptage mathématique) ou de la fonction non-linéaire du système (analogue de d'un

algorithme de cryptage). Un ECSL est un système possédant un delai, un paramètre critique pour la sécurité. Nous avons donc étudié l'influence des paramètres ajustables de l'ECSL sur l'identification de son délai: l'intensité de la rétroaction optique, la valeur du délai et le courant électrique alimentant le laser (aussi appelé courant de pompe). Dans un deuxième temps, nous avons interprété ces résultats sur la base des régimes dynamiques précédant l'apparition du chaos dans la cascade de bifurcations que l'ECSL subit avant d'entrer dans un régime chaotique.

Dans la deuxième section, nous proposons une architecture pour multiplexer des signaux chaotiques optiques produits par des ECSL. Nous démontrons la supériorité de cette approche en terme d'efficacité spectrale relativement aux méthodes de multiplexage en longueur d'onde (WDM) appliquées aux communications optiques par chaos (aussi connues sous le nom de *chaotic WDM*) [158; 161; 162]. Nous avons adapté un concept fondamental de la théorie de la synchronisation: la décomposition active-passive (*active-passive decomposition*, (APD)) [70] en utilisant des composants optiques simples. Nous démontrons la possibilité de multiplexer et démultiplexer deux signaux chaotiques optiques par synchronisation (en utilisant deux émetteurs et deux récepteurs). Les performances et la robustesse de cette structure sont analysées ainsi que la possibilité d'encrypter et de décrypter des messages.

Dans la troisième section, nous avons utilisé une classe de systèmes optoélectroniques différente de celle des deux premières sections, avec l'objectif d'utiliser un seul oscillateur chaotique pour encoder plusieurs messages au lieu d'en considérer un par message. A cette fin, nous avons modifié une structure d'un générateur de chaos électro-optique existant dans la littérature [106] en lui ajoutant plusieurs boucles de rétroaction non-linéaires utilisées pour l'encryptage des messages via, par exemple, la modulation du gain non-linéaire de boucle. Nous avons analysé différentes configurations possibles pour transmettre plusieurs messages, ainsi que les propriétés des signaux chaotiques générés au sein de chaque boucle. Nous avons expliqué dans quelle mesure l'orthogonalité (ou décorrelation) entre les différents signaux peut être utilisée avantageusement pour déterminer des équations de décryptage de faible complexité algorithmique. Enfin, nous avons analysé comment la prise en compte de phénomènes d'interférences entre signaux porteurs influait sur la récupération des messages.

Dans la quatrième et dernière section, nous avons proposé une nouvelle méthode de multiplexage des données en utilisant des systèmes à délais. Les systèmes considérés possèdent de multiples boucles de rétroactions (similaires aux systèmes étudiés précédemment) et les messages sont encodés par des modulations digitales des délais dans des intervalles de valeurs disjoints ou superposés. Les messages sont des sources d'information et, à ce titre, assurent une modulation aléatoire du délai, permettant ainsi un accroissement de la sécurité vis-à-vis de l'identification du délai. Nous avons proposé plusieurs méthodes de décryptage de complexité algorithmique exponentielle ou linéaire avec le nombre d'utilisateurs. Enfin, nous avons démontré la possibilité de communications multi-utilisateurs à très haut débits (plusieurs Gbits/s par utilisateurs).

A.2 Analyse de la Sécurité d'un Laser à Semi-Conducteur à Cavité Externe

Introduction

Il existe plusieurs possibilités pour un espion s'il désire casser les protection apportées par un système chaotique. Essentiellement, il peut soit tenter (i) une extraction directe du message à partir de la série temporelle qu'il analyse, ou (ii) reconstuire la dynamique du système chaotique et extraire le message a posteriori. De plus, sous certaines conditions, l'espion peut aussi exploiter sa connaissance complète (scénario "boîte blanche") ou partielle (scénario "boîte grise") de la nature du système chaotique, le cas le plus défavorable étant l'absence totale de connaissance (scénario "boîte noire").

Le scénario considéré est celui de la boîte noire, notre objectif étant de casser complètement le système en reconstruisant sa dynamique. Dans le cas des systèmes à délais tels qu'un laser à cavité externe (ECSL), ces méthodes sont totalement inefficaces [136] à cause des large dimensions des attracteurs chaotiques étudiés [101]. Cependant, la connaissance du délai peut menacer la complexité et la sécurité du système car l'espion peut alors reconstruire la dynamique dans un sous-espace des phases de faible dimension [142]. Nous illustrons une fuite de sécurité dans un système de type générateur de chaos en longueur d'onde [12].

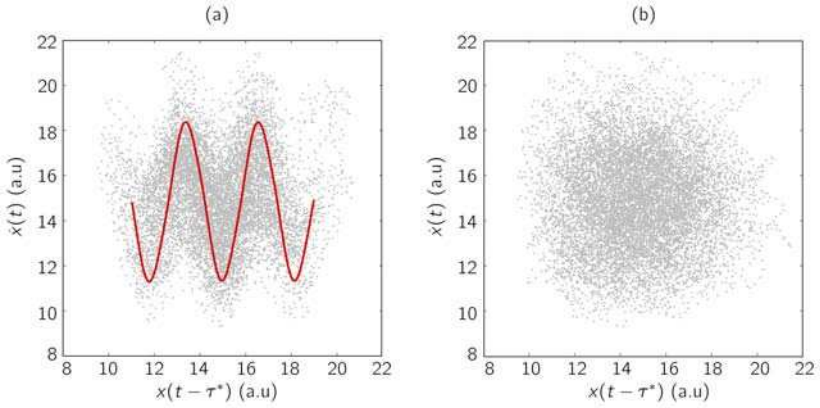

Figure A.2: Identification de la fonction non-linéaire d'un générateur de chaos en longueur d'onde décrit par une équation de type Ikeda, $T\dot{x}(t) + x(t) = \beta \sin^2(x(t-\tau) + \varphi_0)$. le nuage de points gris représente la série temporelle discrétisée et projetée dans un sous-espace des phases $(\dot{x}(t), x(t-\tau^*))$. (a) le délai est connu par l'espion $\tau^* = \tau$ (b) $\tau^* = 1.1\tau \neq \tau$ est inconnu (ou imperfectement connu). La ligne solide rouge donne la forme de la fonction mathématique existant dans le générateur de chaos en longueur d'onde. Les paramètres utilisés dans la simulations sont $T = 10$ μs, $\beta = 30$, $\varphi_0 = \pi/4$, and $\tau = 500$ μs.

La valeur du délai peut être déduite à partir de l'observation d'une série temporelle. Cela a donc conduit à l'établissement de stratégies pour contrer son identification: utilisation de commutations aléatoires [146] ou encore une évolution purement aléatoire [147] de la valeur du délai. Dans cette section, nous étudions la sécurité de l'ECSL au travers du prisme de l'identification du délai. Nous montrerons que

certains régimes peuvent assurer un haut degré de confidentialité de l'information du délai.

Contexte Théorique

Dans cette étude, nous considérons un générateur de chaos composé d'un laser à semi-conducteur soumis à une rétroaction cohérente (Alice) dont l'intensité optique est détectée et analysée par un espion (Eve). Ces informations sont brièvement résumées sur la Figure A.3

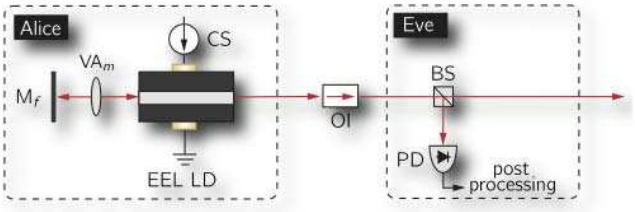

Figure A.3: Description d'un schéma expérimental de laser à cavité externe (ECSL). Le générateur de chaos d'Alice est composé d'une diode laser (LD) pompée électriquement par une source de courant stabilisée (CS). La cavité externe est composée d'un atténuateur variable (VA), et d'un miroir (M). L'espion (Eve) utilise un séparateur de faisceau (BS) et un photo-détecteur (PD).

le système est modélisé par les *Equations de Lang-Kobayashi* [94] connues pour reproduire avec fidélité les régimes dynamiques d'un ECSL observés expérimentalement. Les équations sont données ci-dessous,

$$\frac{dE(t)}{dt} = \frac{1}{2}(1+i\alpha)\left(G_{N,E} - \frac{1}{\tau_p}\right)E(t) + \eta E(t-\tau)\,e^{-i\omega_0\tau} + F(t), \quad \text{(A.1)}$$

$$\frac{dN(t)}{dt} = J - \frac{N}{\tau_s} - G_{N,E}|E|^2, \quad \text{(A.2)}$$

avec $E(t) = |E|\,e^{i\varphi(t)}$ l'enveloppe lentement variable du champs électrique ($|E|(t)$ est l'amplitude et $\varphi(t)$ la phase), N l'inversion moyenne de population dans la région active, α le facteur d'élargissement de raie ou facteur de Henry (mesurant la sensibilité de la phase à une variation d'amplitude du champs électrique), $G_{N,E} = g_N(N-N_0)/(1+\varepsilon\,|E|^2)$ est le gain optique non-linéaire avec g_N le gain linéaire, ε le coefficient de saturation, N_0 la densité de porteur à la transparence, ω_0 est la fréquence angulaire du laser sans rétroaction ($\omega_0\tau$ est la phase à l'origine), η la force de rétroaction optique, τ_p le temps de vie des photons, τ_s le temps de vie des porteurs, J_{th} le courant de seuil d'oscillation laser, p le facteur de pompe et τ le délai correspondant à un aller-retour dans la cavité externe. La force de Langevin $F(t)$ modélise le bruit d'émission spontanée. Sa décomposition en coordonnées polaires (amplitude et phase) s'écrit $F_{|E|}(t) = 2\beta N(t)/E(t) + \sqrt{2\beta N(t)}\zeta_{|E|}(t)$ et $F_\varphi(t) = 1/E(t)\sqrt{2\beta N(t)}\zeta_\varphi(t)$. Il est important de noter que ce modèle représente le comportement d'un laser monomode. En l'absence de rétroaction optique, le laser à semi-conducteur possède les propriétés dynamiques d'un oscillateur non-linéaire

amorti. En effet, avant de rejoindre son point d'équilibre, le laser présente un régime transitoire d'oscillations amorties aussi appelées dans la littérature oscillations de relaxation (*relaxation oscillations*, (RO)) et correspondant à un échange d'énergie entre les porteurs électroniques et les photons. La fréquence $\nu_{RO} = 1/\tau_{RO}$ de ces oscillations est déterminée par une analyse de stabilité linéaire du laser sans rétroaction et est fonction des différents paramètres internes. Elle s'écrit sous la forme suivante:

$$\nu_{RO} = \frac{1}{2\pi}\left(\frac{1}{\tau_p\tau_s}(\mu-1) - \frac{\mu^2}{4\tau_s^2}\right)^{1/2} \text{ avec } \mu = g_N\tau_p\tau_s\left(pJ_{th} - \frac{N_0}{\tau_s}\right). \tag{A.3}$$

La sortie de l'ECSL chaotique est injectée dans un canal de communication optique. Nous supposons que l'espion (Eve) peut sans restrictions intercepter et réaliser l'acquisition de la série temporelle générée par Alice. Typiquement, Eve essaie de reconstruire la dynamique de l'ECSL en utilisant des méthodes dites de "plongement" (*embedding techniques*) [136]. Cette approche est inefficace si la dimension de l'attracteur du système chaotique excède cinq. Les dispositifs optoélectroniques à délai, tels que les ECSL, exhibent des attracteurs de très large dimension (plusieurs dizaines) prévenant l'utilisation de plongements pour casser le cryptosystème. Cependant la connaissance du délai, comme rappelée précedemment, conditionne fortement la sécurité et retire les restrictions de reconstruction par plongement. Il est possible d'extraire la valeur du délai à partir d'une série temporelle en utilisant des méthodes telles que les fonctions d'autocovariance (ACF) et d'information mutuelle retardée (DMI). D'autres méthodes existent telles que les modèles linéaires locaux (LLM) ou non-linéaires globaux (GNM) [136]. L'ACF normalisée d'une série temporelle $X(t)$ est définie par

$$\Gamma_X = \frac{1}{\sigma_X^2}\langle (X(t)-\mu_X)(X(t+\theta-\mu_X)\rangle, \tag{A.4}$$

avec $\mu_X = \langle X(t)\rangle$, $\sigma_X^2 = \langle (X(t)-\mu_X)^2\rangle$, et $\langle\cdot\rangle$ dénotant la moyenne temporelle. La DMI est une métrique utilisée en théorie de l'information [2]. En supposant qu'une série temporelle $X(t)$ et sa version retardée $X(t-\theta)$ soient des processus aléatoires, la DMI est définie par

$$\mathbf{I}(\theta) = \mathbb{E}\left(\ln\left(\frac{\hat{f}_{X(t)X(t-\theta)}}{\hat{f}_{X(t)}\hat{f}_{X(t-\theta)}}\right)\right), \tag{A.5}$$

avec $\hat{f}_{X(t)X(t-\theta)}$, $\hat{f}_{X(t)}$, et $\hat{f}_{X(t-\theta)}$ les densités de probabilité estimées à partir de la série temporelle.

Identification du Délai dans les Equations de Lang-Kobayashi

Dans notre travail de thèse, nous avons démontré que contrairement à ce qui était communément admis, un ECSL a la capacité de masquer son information du délai (dénommée *signature*) vis à vis d'estimateurs classiques tels que l'ACF et la DMI. Nous avons identifié le rôle clé des paramètres opérationels de l'ECSL dans l'identification du délai: (i) la force de rétroaction optique η, (ii) le courant de pompe $J = pJ_{th}$ et

enfin (iii) la valeur du délai τ relative à celle de la période des oscillations de relaxation τ_{RO}. La force de rétroaction η contrôle la contribution de l'intensité retardée $I(t-\tau)$ dans l'évolution de l'intensité $I(t)$. L'introduction du champs électrique retardée $\eta e^{-i\omega_O \tau} E(t-\tau)$ dans les équations de Lang-Kobayashi A.1-A.2 étant linéaire, il est attendu qu'une augmentation de la valeur η conduise à un accroissement de l'information partagée entre $I(t)$ et $I(t-\tau)$. La Figure A.4 supporte clairement cette tendance en présentant un scénario d'identification du délai pour des valeurs croissante de η.

Pour de larges valeurs de η, les séries chaotiques analysées offrent une signature claire du délai: des "pics" de forte amplitude dans l'ACF et la DMI et dont les positions donnent une estimation de τ et de ses multiples (Fig. A.4(k)-(l)). Une diminution progressive de cette valeur entraîne dans un premier temps une décroissance de l'amplitude du "pic" (Fig. A.4(h)-(i)) jusqu'à ce qu'un minimum global pour l'amplitude du pic soit atteint (Fig. A.4(e)-(f)). Dans un deuxième temps et pour des valeurs de η plus faibles, un changement qualitatif est observé: les estimateurs présentent des oscillations rapides dont la période est approximativement égale à τ_{RO} et modulées lentement avec une période proche de la valeur τ (Fig. A.4(b)-(c)). Nous remarquons que dans ce dernier cas, la signature du délai n'est plus aussi claire, une partie de l'information a été perdue. Les oscillations dans les estimateurs, qui finissent inévatiblement par apparaître, constituent un élément clé dans la dissimulation du délai et ont leurs propriétés intimement liées aux paramètres opérationels

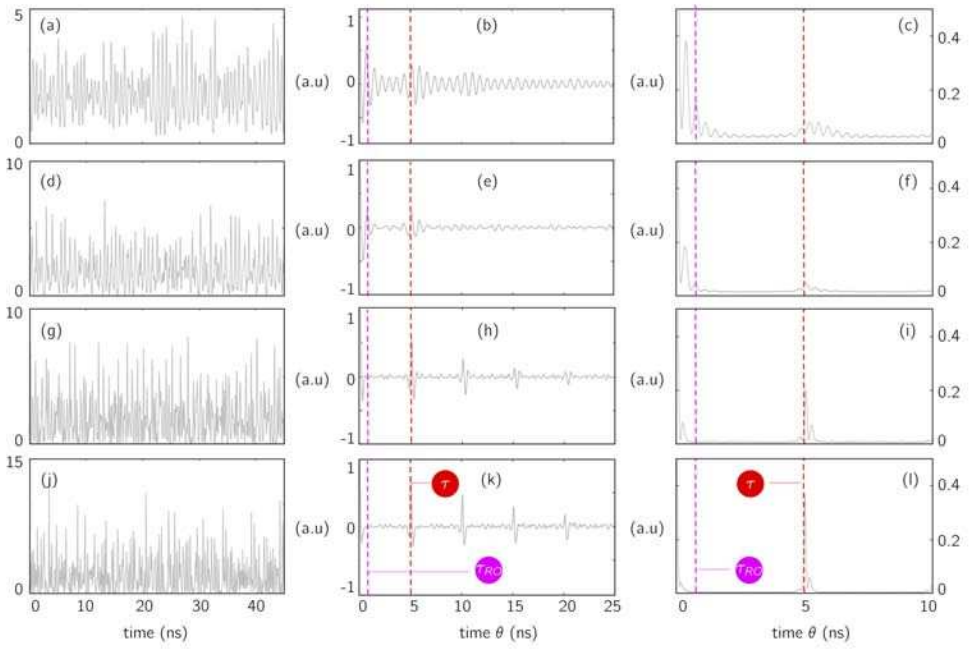

Figure A.4: Séries temporelles chaotiques de l'intensité optique générées par un ECSL et enregistrées par un espion (1ère colonne), ACF (2ème colonne), et DMI (3ème colonne) pour des valeurs croissantes de la force de rétroaction $\eta = 2$ GHz (1ère ligne), 5 GHz (2ème ligne), 10 GHz (3ème ligne), and 15 GHz (4ème ligne) avec $\tau = 5$ ns et $\tau_{RO} = 0.75$ ns. Les lignes verticales pointillées rouge et violette donnent les positions de τ_{RO} et τ, respectivement.

de l'ECSL.

L'influence du courant de pompe sur la signature du délai est étudiée dans la Figure A.5; elle illustre l'évolution de l'extremum (ou pic) le plus significatif dans un voisinage du délai $W(\tau)$ en terme d'amplitude et de position pour chacun des estimateurs ACF et DMI. Ce pic correspond à l'estimation du délai. Pour différentes valeurs du courant de pompe, la force de rétroaction η varie et révèle l'existence systématique d'un minimum global de l'amplitude de la signature (Fig. A.5(a)-(c)). Il est à noter que lorsque le courant de pompe augmente, la valeur du minimum global augmente également, l'identification du délai est donc plus aisée dans ces conditions. Pour des valeurs modérées de η, deux échelles de temps coexistent (délai et période des oscillations de relaxation) et induisent un biais dans la position du pic estimant le délai. Celui-ci conduit à une surestimation de la valeur du délai de l'ordre de $\tau_{RO}/2$ quelque soit la valeur du courant de pompe. Par la suite, elle décroît rapidement avec l'augmentation de η (Fig. A.5(a)-(c)).

L'étude de l'influence de ces deux paramètres pose les bases d'un possible masquage du délai par l'exploitation d'une forme de compétition entre deux échelles de temps

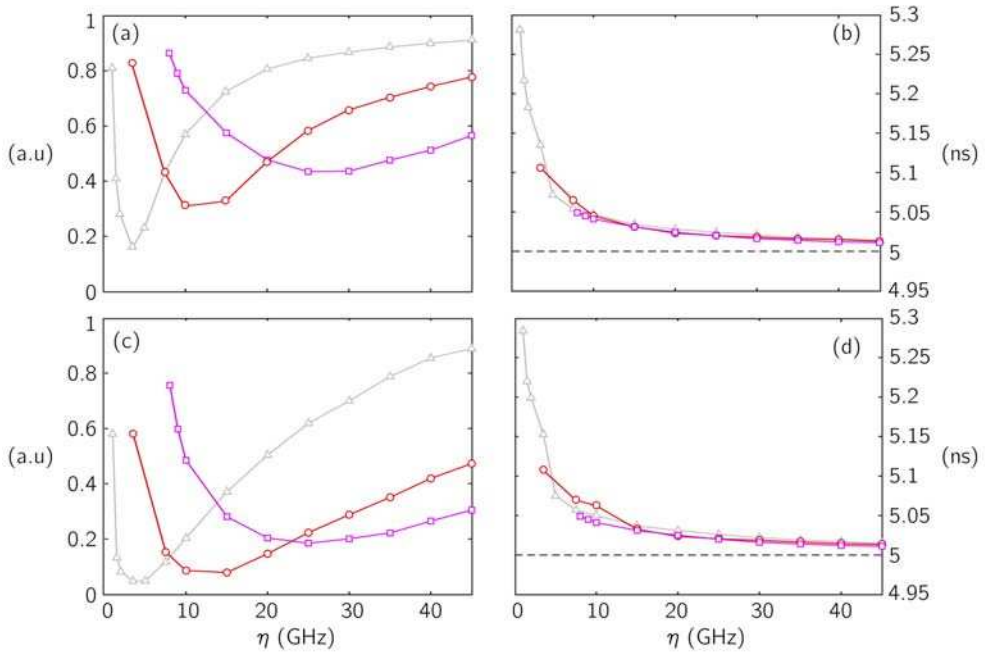

Figure A.5: Impact du courant de pompe $J = pJ_{th}$ et de la force de rétroaction η sur l'amplitude et la localisation de l'extremum le plus significatif dans un voisinage du délai avec $\tau = 5$ ns et $W(\tau) = [4.5 \text{ ns}; 5.5 \text{ ns}]$. Les figures (a)-(b) donnent l'amplitude et la localisation de $\max_{\theta \in W(\tau)} |\Gamma_I(\theta)|$, respectivement. Les figures (c)-(d) donnent les mêmes informations mais avec $\max_{\theta \in W(\tau)} |\hat{\mathbf{I}}(\theta)|$. Les lignes en trait plein avec les marqueurs triangulaires gris, (△), les marqueurs circulaires rouges (◯), et les marqueurs carrés violets (□) sont associés respectivement aux facteurs de pompe $p = 1.05$, 1.26 et 1.72. Ces trois valeurs de p correspondent à différentes valeurs de la période des oscillations de relaxation $\tau_{RO} = 0.75$ ns, 0.33 ns, et 0.2 ns, respectivement. Dans les Figures (b)-(d), les lignes pointillées donnent la localisation exacte du délai τ.

existant dans la série temporelle: une échelle dont la valeur est proche de celle des oscillations de relaxation (ET1) et le délai (ET2). Lorsque la rétroaction est faible (modérée), la signature du délai dans l'ACF ou la DMI est faible, cependant le délai reste toujours identifiable.

Optimisation de la Dissimulation du Délai & Interprétation Dynamique des Résultats

Qualitativement, la non-linéarité interne du laser et la rétroaction optique ont des influences comparables sur l'évolution de la dynamique de l'ECSL dans les régimes chaotiques faiblement développés (faibles valeurs de η). Les perturbations observées sur la signature du délai peuvent être interprétées sur la base des multiples échelles de temps existant dans l'ECSL. Ainsi, dans les régimes "faiblement" chaotiques, la période des oscillations de relaxation auto-entretenues (ET1) et le délai (ET2) sont conjointement favorisés. ET1 introduit des corrélations de courtes portées provoquant des oscillations dans l'ACF et la DMI. Ainsi, la dissimulation du délai consiste à placer l'ECSL dans un régime tel que ET1 et ET2 interagissent fortement. En terme des paramètres opérationnels, cela correspond à de faibles valeurs de η, pJ_{th} et une valeur τ proche de τ_{RO}. La Figure A.6 illustre un tel scénario.

Dans ce scénario, la séparation entre le délai et la période des oscillations de relaxation est de 0.45 ns. Comme dans la Figure A.4, l'utilisation de larges valeurs

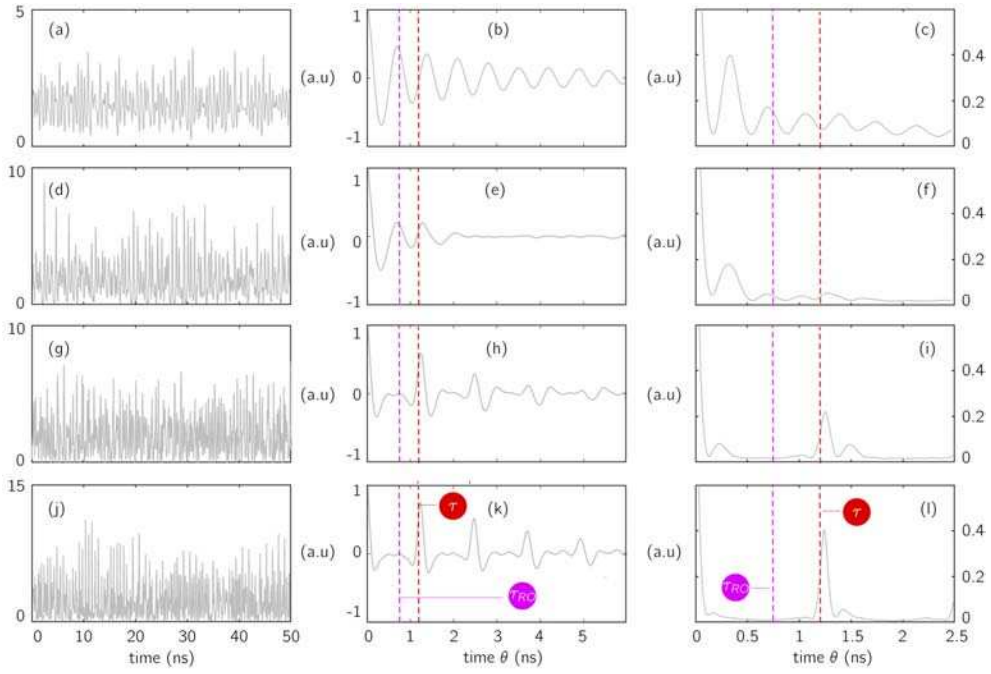

Figure A.6: Scénario d'identification du délai avec des échelles de temps ET1 et ET2 proches. l'intensité de l'ECSL, l'ACF, et la DMI sont tracées (colonnes de gauche à droite) pour des valeurs croissante de force de rétroaction $\eta = 2$ GHz, 5 GHz, 10 GHz, et 15 GHz (de la première à la dernière ligne) avec un délai $\tau = 1.2$ ns et une période des oscillations de relaxation $\tau_{RO} = 0.75$ ns. Les lignes pointillées rouge et violette donnent les positions respectives de τ_{RO} et τ.

de η conduit invariablement à une identification aisée du délai (signature impulsionnelle de grande amplitude et de position précise) (Fig. A.6(l)-(k)). La diminution progressive de η entraîne une décroissance de l'amplitude de la signature (Fig. A.6(h)-(i)). Le comportement de la signature est encore identique à celui observé dans le scénario précédent, mais diffère si η diminue. Progressivement, l'échelle de temps ET1 domine dans les estimateurs et conduit à la disparition progressive du délai (Fig. A.6(e)-(f)), puis totale (Fig. A.6(b)-(c)) au profit d'une détection de l'échelle de temps ET1 (oscillations de relaxation entretenues) differente de τ_{RO}. Il apparaît que l'utilisation de faibles valeurs de η entraîne une grande diversité de comportements des estimateurs ACF et DMI. Les régimes dynamiques sont alors faiblement chaotiques et possèdent une réminescence de la structure du dernier attracteur stable avant la transition vers le chaos. La route vers le chaos d'un ECSL varie très fortement en fonction des paramètres internes et opérationels considérés. La nature des attracteurs et leur contenu spectral peut donc fortement changer et influencer significativement le comportement des estimateurs (ACF ou DMI). Une illustration de l'influence de la route vers le chaos sur l'estimation du délai est donnée dans la Figure A.7. Elle illustre dans quelle mesure l'absence de composantes spectrales associées au délai $f_{EC} = 1/\tau$ assure sa dissimulation dans les régimes chaotiques. Elle présente une route vers le chaos par doublement de période en prenant la force de rétroaction η comme paramètre de bifurcation. Elle montre également pour différents points de la route (colonnes de gauche à droite) une projection de l'attracteur chaotique dans le plan $(|E|, N)$, le spectre RF, l'ACF et la DMI, tous trois calculés à partir de la série temporelle de l'intensité optique $I(t)$. Au cours de la route, un mode de cavité externe (solution stationnaire d'un ECSL, aussi dénomé *external cavity mode* ou ECM) est destabilisé au profit d'un cycle limite [Fig. A.7(b1)]. Sa fréquence $f_{H1} = 1.34$ GHz est identifiée par le spectre RF [Fig. A.7(c1)] et par les estimateurs ACF et DMI [Fig.A.7(d1)-(e1)]. Elle est en outre proche de la fréquence des oscillations de relaxation $f_{RO} = 1.33$ GHz. L'ECSL subit ensuite une première bifurcation *flip* conduisant à un cycle limite de période double [Fig. A.7(c2)], détectée par chacun des estimateurs [Fig. A.7(d2)-(e2)], avant de subir une cascade de bifurcations. La géométrie de l'attracteur devient plus complexe [Fig. A.7(b1)-(b4)] à mesure que le contenu fréquentiel s'enrichit. Lorsque la transition vers le chaos s'opère, une réminescence du dernier attracteur non-étrange est présente dans la géométrie du système. Fréquentiellement, cela se traduit par une persistence de la concentration en énergie spectrale des fréquences apparues au cours de la cascade de bifurcations [Fig. A.7 (c4)]. Temporellement, on observe par une décorrelation lente de l'intensité chaotique avec une forme de fonction d'ACF proche de celle associée au dernier attracteur stable [Fig. A.7]. Les régimes chaotiques obtenus, et qualifiés de faiblement développés, sont aussi ceux pour lesquels la sécurité est maximale si aucune fréquence liée au délai n'apparaît au cours de la route. La diversité des routes vers le chaos explique ainsi celle des scénarios de dissimulation observée à de faibles valeurs de force de rétroaction optique η.

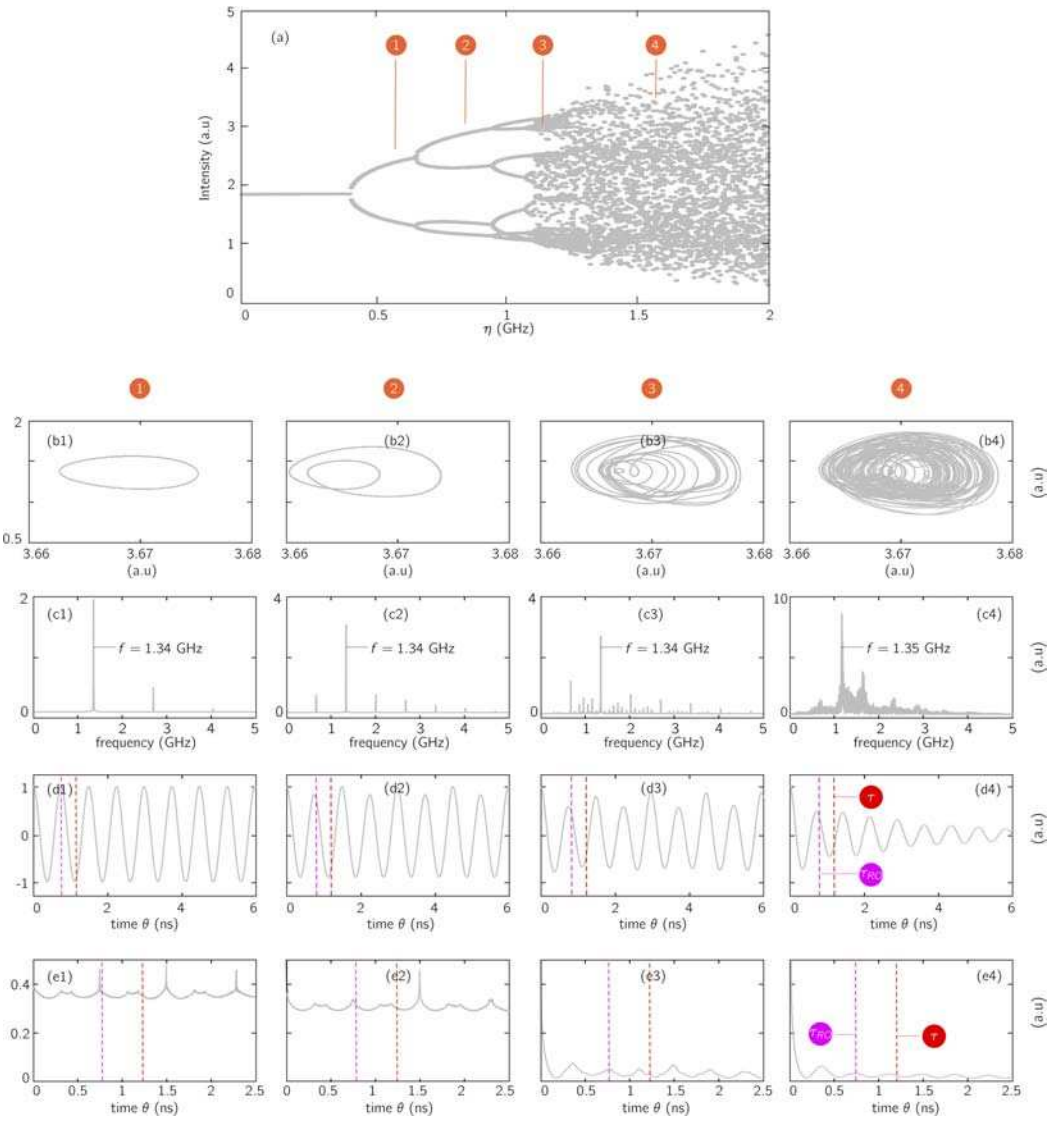

Figure A.7: Interpretation dynamique de la sécurité dans un scénario d'échelles de temps proches. Le délai vaut $\tau = 1.2$ ns et la période des oscillations de relaxation $\tau_{RO} = 0.75$ ns. Une route vers le chaos par doublement de période est observée en (a). La figure présente une projection de l'attracteur chaotique dans le plan $(|E|, N)$ (première ligne), la densité spectrale de puissance $|FT(I(t))|^2$ (deuxième ligne), l'ACF (troisième ligne) et la DMI (quatrième ligne) pour des valeurs croissantes de force de rétroaction η. Chaque colonne (numérotée de 1 à 4) correspond à une valeur de $\eta = 0.6$ GHz, 0.8 GHz, 1.2 GHz, et 1.5 GHz. Les lignes verticales pointillées de couleur violette et rouge donnent respectivement les valeurs théoriques du délai et de la période des oscillations de relaxation utilisées dans les simulations.

Conclusion

Dans cette première partie de la thèse, nous avons étudié la sécurité en terme d'identification du délai d'une classe de générateur de chaos optique : celle des lasers soumis à rétroaction optique (ECSL). En effet, le délai est un paramètre critique pour la sécurité des crypto-systèmes chaotiques retardés. Nous avons découvert le rôle clé joué par les paramètres opérationels de l'ECSL : la force de rétroaction optique η, le courant de pompe J et le délai introduit par la cavité externe du laser τ. Nous avons montré qu'une combinaison particulière de ces paramètres pouvait conduire à des comportements chaotiques assurant une dissimulation quasi-parfaite de l'information du délai (vis-à-vis des méthodes d'analyse de séries temporelles). Nous avons également interprété ces résultats sur la base des dynamiques non-linéaires présentes dans la cascade de bifurcations précédant l'apparation du chaos.

A.3 Multiplexage de Chaos Optique

Introduction

Dans cette section, nous résumons les résultats de la thèse relatifs au multiplexage de signaux chaotiques optiques et à la transmission multiplexée d'information sur base de nouvelles architectures. Les motivations ayant conduit à l'émergence des concepts de multiplexage en cryptographie par chaos sont identiques à celles des communications conventionnelles : transmission simultanée de plusieurs messages avec un seul canal de communication de disponible et l'efficacité spectrale (ou quantité d'information potentiellement transmissible par Hz). Dans les réseaux optiques, les méthodes de multiplexage temporel et fréquentiel (en anglais, *time-division multiplexing* ou TDM et *wavelength-division multiplexing* ou WDM) sont couramment utilisées [104], mais ne présentent pas d'intérêt scientifique en terme d'efficacité spectrale pour les systèmes chaotiques optiques. Cependant la technique de WDM a été utilisée avec des lasers chaotiques multimodes [160; 161; 162] ou avec plusieurs lasers monomodes décalés en fréquence [158; 159; 164]. Nous proposons dans cette partie d'aller au-delà du paradigme de TDM et WDM en exploitant un des concepts fondamentaux en synchronisation du chaos : la décomposition active-passive (en anglais, *active- passive decomposition* ou APD) formalisée dans [70]. La partie active de l'oscillateur chaotique possède au moins un exposant de Lyapunov positif, la partie passive a des exposants de Lyapunov conditionels négatifs. Deux systèmes chaotiques (émetteur et récepteur), décrits par des équations dynamiques identiques aux conditions initiales différentes, peuvent ainsi se synchroniser si leurs parties actives sont soumises à la même influence. Les EELs sont des oscillateurs non-linéaires amortis, autrement dits des systèmes passifs. Nous avons soulignée l'analogie existante entre la synchronisation retardée d'ECSLs et le cadre théorique de l'APD. Cela nous a permis de proposer une architecture de mutiplexage comprenant plusieurs ECSLs à l'émission et à la réception.

Cadre Théorique et Modélisation

Nous proposons une méthode de multiplexage de signaux optiques chaotiques générés par des lasers à semi-conducteur ayant des fréquences optiques identiques. En utilisant des composants optiques simples, nous proposons une analogie optique d'une décomposition active-passive. A l'émission, un champ optique multiplexé $E_T(t)$ (résultant de la superposition des champs chaotiques $E_k^m(t)$ de chaque laser M_k $(k = 1, \ldots, n)$) injecte toutes les diodes lasers maîtres avec des délais et forces d'injection spécifiques. Le champ optique $E_T(t)$ est ainsi perçu par M_k comme étant un champ multiplexé spécifique $E_{T,k}^m(t)$. Le signal $E_T(t)$ se propage également dans un canal de communication optique, afin d'injecter unidirectionellement n lasers esclaves découplés. Plus spécifiquement, les lasers esclaves S_k $(k = 1, \ldots, n)$ sont injectés avec des délais et couplages identiques à ceux du laser maître M_k correspondant. Cela implique que chaque laser S_k est injecté par une version retardée de $E_T(t)$ qui sera notée $E_{T,k}^s(t)$.

Figure A.8 représente une configuration à deux lasers mutuellement couplés (M_1,M_2) injectant unidirectionellement deux lasers découplés (S_1,S_2).

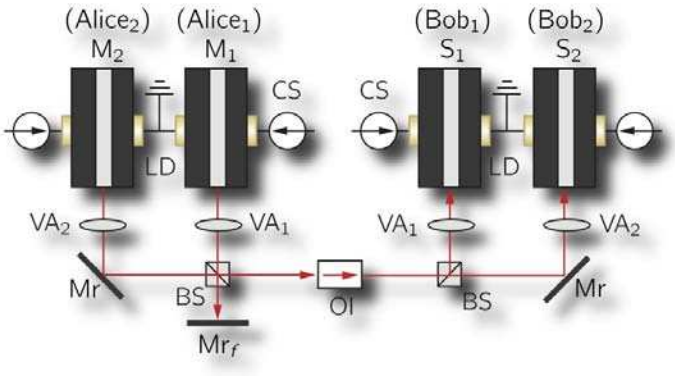

Figure A.8: Illustration de l'architecture de multiplexage de chaos optique basée sur une décomposition active-passive (APD) utilisant des lasers à semi-conducteur. Les lasers maîtres et esclaves sont respectivement labélisés $\mathrm{M}_{1,2}$ et $\mathrm{S}_{1,2}$. Les abbréviations utilisées sont CS: source de courant, Mr, Mr_f : miroir, $\mathrm{VA}_{1,2}$: atténuateur variable, BS : séparateur de faisceaux 50/50, OI : isolateur optique.

Chaque laser est soumis à l'influence de son propre champ optique retardé et réfléchi par le miroir Mr_f, ainsi qu'au champ optique issu de l'autre laser maître. La combinaison linéaire des deux champs retardés est ainsi injectée dans chaque maître, avec une force, une phase et un délai déterminés (contrôlés respectivement par des atténuateur variables et des chemins optiques différents). Le mélange optique est également transmis unidirectionellement dans le canal de communication pour injecter la paire de lasers esclaves.

L'architecture complète est modélisée en considérant des hypothèses identiques à celles issues du le formalisme des équations de Lang-Kobayashi [94]. En supposant que les lasers sont monomodes, l'architecture est décrite par le système d'équations suivant

$$\frac{dE_k^m}{dt} = \frac{1}{2}(1+i\alpha_k^m)\,G_k^m E_k^m + F_k^m + \sum_{j=1}^{n} \eta_{jk}^m e^{-i\omega_{0j}^m \tau_{jk}^m + i\Delta\omega_{jk}^{m/m} t} E_j^m\left(t-\tau_{jk}^m\right), \quad \text{(A.6)}$$

$$\frac{dN_k^m}{dt} = J_k^m - \gamma_{sk}^m N_k^m - (G_k^m + 1/\tau_{pk}^m)|E_k^m|^2, \quad \text{(A.7)}$$

$$\frac{dE_k^s}{dt} = \frac{1}{2}(1+i\alpha_k^s)\,G_k^s E_k^s + F_k^s + \sum_{j=1}^{n} \eta_{jk}^c e^{-i\omega_{0j}^s \tau_{jk}^c + i\Delta\omega_{jk}^{m/s} t} E_j^m\left(t-\tau_{jk}^c\right), \quad \text{(A.8)}$$

$$\frac{dN_k^s}{dt} = J_k^s - \gamma_{sk}^s N_k^s - (G_k^s + 1/\tau_{pk}^s)|E_k^s|^2. \quad \text{(A.9)}$$

L'indice k correspond à la $k$ième paire de lasers ($\mathrm{M}_k/\mathrm{S}_k$), les exposants m et s labelisent les variables d'état associées aux lasers maître et esclave. L'approximation lentement variable du champ optique est décrite par $E_k^{m,s} = |E_k^{m,s}|e^{i\phi_k^{m,s}}$ et l'inversion de population par $N_k^{m,s}$. Le gain non-linéaire du laser est décrit par $G_k^{m,s} = g_k^{m,s}(N_k^{m,s} - N_{0k}^{m,s})/(1+\varepsilon_k^{m,s}|E_k^{m,s}|^2) - 1/\tau_{pk}^{m,s}$, avec $g_k^{m,s}$ le gain differentiel, $N_{0k}^{m,s}$ l'inversion population à la transparence, $\varepsilon_k^{m,s}$ le coefficient de saturation de gain et τ_{pk} le temps de vie des photons. $\alpha_k^{m,s}$ est le factor de Henry, $\gamma_{sk}^{m,s}$ l'inversion de temps de vie des porteurs, $J_k^{m,s}$ la densité de courant de pompe et $\omega_{0k}^{m,s}$ la pulsation angulaire du $k$ième laser. τ_{jk}^m (respectivement τ_{jk}^c), η_{jk}^m (respectivement η_{jk}^c) et $\Delta\omega_{jk}^{m/m} = \omega_{0j}^m - \omega_{0k}^m$ (respectivement $\Delta\omega_{jk}^{m/s} = \omega_{0j}^m - \omega_{0k}^s$) sont les temps de propagation, les forces d'injection, et les décalage sen fréquence entre le $j$ième et le $k$ième laser maître (respectivement le $j$ième laser maître et le $k$ième laser esclave). Le bruit d'émission spontanée est modelisé par des forces de Langevin $F_k^{m,s} = \sqrt{2\beta_k^{m,s} N_k^{m,s}}\,\zeta_k^{m,s}$ avec β_{sp}, le taux d'émission spontané, et $\zeta_k^{m,s}$ es bruits blancs gaussiens de variance unité statistiquement independents.

La géométrie de l'architecture décrite par la Figure A.8 impose des contraintes structurelles aux délais de propagation et aux forces de couplage de l'émission :

$$\tau_{jk}^m = \tau_{kj}^m = \tau_{jj}^m + \Delta\tau_{kj}^m/2, \quad \text{(A.10)}$$

$$\eta_{kj}^m = \eta_{jk}^m = \sqrt{\eta_{kk}^m \eta_{jj}^m}, \quad \text{(A.11)}$$

avec $\Delta\tau_{jk}^m = -\Delta\tau_{kj}^m = \tau_{jj}^m - \tau_{kk}^m$.

La configuration est telle que la topologie des délais introduite à l'émission est préservée à la réception. Mathematiquement, cela se traduit par la relation

$$\tau_{kk}^m - \tau_{jk}^m = \tau_{kk}^c - \tau_{jk}^c. \quad \text{(A.12)}$$

Ces différentes contraintes permettent d'exprimer le champ optique multiplexé par une formulation mathématique compacte

$$E_T(t,\theta,\sigma,\mu) = \sum_{j=1}^{n} \sqrt{\eta_{jj}^m} e^{i\omega_{0j}^m(\theta+\Delta\tau_{\sigma j}^m/2) + it\Delta\omega_{j\sigma}^{\mu}} E_j^m(t-\theta-\Delta\tau_{\sigma j}^m/2), \quad \text{(A.13)}$$

avec $\theta = \tau_{kk}^m$ ou τ_{kk}^c, $\sigma = k$ et $\mu = m/m$ ou m/s. Le champ optique $E_T(t)$ peut ainsi être utilisé pour déterminer l'expression du champ multiplexé injecté dans la

$k$ième paire de lasers : M_k est soumis à $E^m_{T,k}(t) = \sqrt{\eta^m_{kk}} E_T(t, \tau^m_{kk}, k, m/m)$ et S_k à $E^s_{T,k}(t) = \sqrt{\eta^c_{kk}} E_T(t, \tau^c_{kk}, k, m/s)$.

Synchronisation Multiplexée et Efficacité Spectrale

Chaque paire de lasers (M_k,S_k) peut être complètement synchronisée si les paramètres internes et opérationel des lasers sont identiques. Il faut également négliger la présence du bruit et ne considérer aucun décalage en fréquence $\Delta\omega^{m/s}_{kk} = 0$. En procédant de façon analogue au cas d'une seule paire de lasers [59; 121; 123], nous avons démontré que les conditions nécessaires de synchronisation pour chaque paire impliquaient l'égalité des forces d'injection

$$\eta^c_{jk} = \eta^m_{jk} \text{ pour tous } j,k \text{ aussi équivalent à } \eta^c_{kk} = \eta^m_{kk} \text{ pour tous } k. \tag{A.14}$$

Cependant, ces conditions ne donnent pas d'information sur les valeurs des paramètres de couplage garantissant la stabilité de la synchronisation. Les temps de propogation non-nuls, inhérents à la cavité optique partagée et au canal de communication, induisent des délais $\Delta\tau_k$ dans la synchronisation de la $k$ième paire de laser. On définit alors les variétés de synchronisation associées à (M_k,S_k) par l'ensemble d'équations suivant :

$$E^s_k(t) = E^m_k(t - \Delta\tau_k), \tag{A.15}$$
$$\phi^s_k(t) = \phi^m_k(t - \Delta\tau_k) - \omega^m_{0k}\Delta\tau_k (\text{mod } 2\pi), \tag{A.16}$$
$$N^s_k = N^m_k(t - \Delta\tau_k). \tag{A.17}$$

L'expression du délai à la synchronisation peut être simplement déduit en comparant les champs optiques injectants M_k et S_k : respectivement $E^m_{T,k}(t) = \sqrt{\eta^m_{kk}} E_T(t, \tau^m_{kk}, k, m/m)$ et $E^s_{T,k}(t) = \sqrt{\eta^c_{kk}} E_T(t, \tau^c_{kk}, k, m/s)$. Il est alors aisé de déduire l'expression suivante pour les délais à la synchronisation :

$$\Delta\tau_k = \tau^c_{kk} - \tau^m_{kk}. \tag{A.18}$$

Une simulation de notre architecture est réalisée pour deux paires de lasers ($n = 2$) et apparaît en Figure A.9.

En l'absence de bruit, nous observons un diagramme de synchronisation linéaire [Fig. A.9(a1)-(a4)] correspondant à une synchronisation complète pour chaque paire. La présence de bruit d'émission spontanée détruit l'état de synchronisation parfaite, néanmoins, les deux systèmes restent partiellement synchronisés. En considérant un taux d'émission spontanée typique égal à $\beta_{sp} = 1000$ s¹, on constate que le coefficient de corrélation moyen entre les différentes variables d'état de M_k et S_k est d'environ 0.95. Ce niveau est suffisant pour guarantir des communications chaotiques avec un faible taux d'erreur binaire (BER).

L'efficacité spectrale de notre architecture est également un atout important. Si des schémas classiques de multiplexage en longueur d'onde (WDM) étaient appliqués à des architectures de communications par chaos, les spectres optiques nécessiteraient d'être suffisamment distants les uns des autres afin d'éviter toutes interférences et d'assurer leur séparation à la réception. En effet, les lasers à semi-conducteurs à

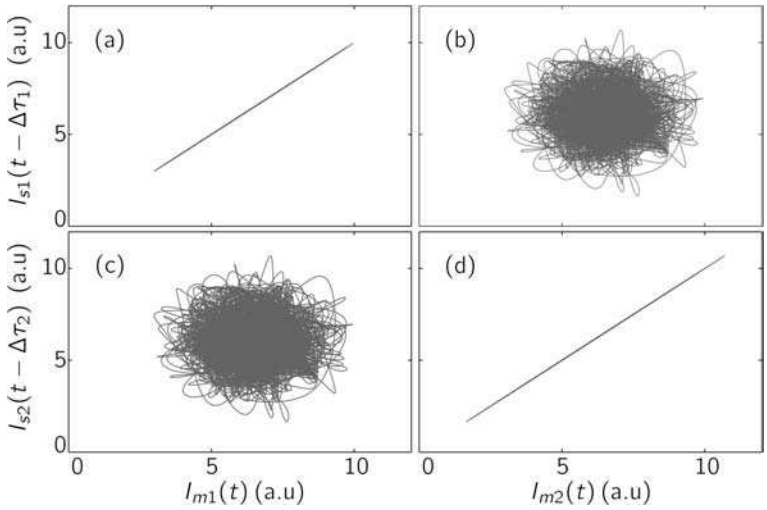

Figure A.9: Diagrammes de synchronisation théoriques sans bruit d'émission spontanée ($\beta_{sp} = 0$ s^{-1}). Les diagrammes de synchronisation présentent les évolutions de $(I_1^m(t), I_1^s(t-\Delta\tau_1))$ en (a1), $(I_2^m(t), I_1^s(t-\Delta\tau_1))$ en (a2), $(I_1^m(t), I_2^s(t-\Delta\tau_2))$ en (a3), et $(I_2^m(t), I_2^s(t-\Delta\tau_2))$ en (a4). Les valeurs numériques utilisées sont $J_1^m = J_1^s = 2.75J_{th}$, $J_2^m = J_2^s = 2.5J_{th}$, $\eta_{11}^m = \eta_{11}^c = 10$ GHz, $\eta_{22}^m = \eta_{22}^c = 15$ GHz, $\eta_{12}^m = \eta_{21}^m = \eta_{12}^c = \eta_{21}^c = \sqrt{\eta_1^m \eta_2^m}$, $\tau_{11}^m = 1$ ns, $\tau_{22}^m = 4$ ns, $\tau_{11}^c = 1$ ns et $\tau_{22}^c = 4$ ns. Les paramètres internes sont choisis différemment pour chaque paire : $\alpha_1^{m,s} = 5$, $\alpha_2^{m,s} = 4$, $\tau_{p1}^{m,s} = 2$ ps, $\tau_{p2}^{m,s} = 1$ ps, $\gamma_{s1}^{m,s} = 2$ ns, $\gamma_{s2}^{m,s} = 1$ ns, $\varepsilon_1^{m,s} = 5 \times 10^{-7}$, $\varepsilon_2^{m,s} = 2.5 \times 10^{-7}$, $g_1^{m,s} = 1.5 \times 10^{-4}$ s^{-1}, $g_2^{m,s} = 1 \times 10^{-4}$ s^{-1}, $N_{01}^{m,s} = 1.5 \times 10^8$, $N_{02}^{m,s} = 2 \times 10^8$.

cavité externe en régime chaotique ont des spectres optiques très large de l'ordre de plusieurs dizaines de GHz. Une telle approche ne résulterait pas en une amélioration de l'efficacité spectrale. Cependant, notre architecture permet de lever cette contrainte en autorisant la séparation par synchronisation de plusieurs signaux chaotiques avec de forts recouvrements spectraux. Nous avons comparé la bande passante du signal $E_T(t)$ avec $\sqrt{\eta_{kk}^m} E_k^m(t)$ dans le cas où notre architecture était composé de deux paires d'EELs. Nous avons constaté que les étalements spectraux étaient approximativement identiques, ce qui nous a permis d'envisager de transmettre deux fois plus de bit d'information par Hz.

Communications Chaotiques Multiplexées

Nous avons présenté différentes stratégies permettant le multiplexage de plusieurs messages binaires. Elles constituent une évolution des méthodes existantes pour le cas d'une seule paire émetteur/récepteur et sont connues sous les appelations de *chaos masking* (CMa), *chaos-shift keying* (CSK), et *chaos modulation* (CMo).

La technique de CMa consiste en l'addition d'un message binaire à la sortie du système chaotique optique à base d'ECSL [166]. Le message ne participant pas à la dynamique de l'ECSL et induit des perturbations à la synchronisation au niveau du récepteur. Cela permet de retrouver l'information initialement encodée. Les messages encryptés étant non codés, le CMa ne peut être utilisé avec notre architecture. En effet, l'addition de deux messages binaires m_1 et m_2, aux propriétés identiques,

induiraient une perte d'information : il devient impossible de distinguer le couple de valeurs $m_1 m_2 = \{01, 10\}$. Le nombre de combinaisons de bits indistinguables augmentant avec le nombre de paires de lasers, une version multiplexée du CMa semble inappropriée pour effectuer une transmission d'information avec notre architecture.

La technique de CSK consiste en la commutation d'un paramètre θ_E de l'émetteur entre deux états $\{\theta_0, \theta_1\}$ au rythme d'un message et à l'utilisation d'un récepteur avec une valeur de paramètre fixée $\theta_R = \theta_0$ ou θ_1. Lorsque l'émetteur et le récepteur sont synchronisés, cela signifie que les valeurs de θ_E et θ_R coincident et donc qu'un bit "0" a été transmis. Le cas contraire correspondrait à un bit "1". Cette méthode a été mise en oeuvre dans les ECSLs en modulant le courant de pompe à l'émission [169] et elle peut être appliquée à notre architecture en modulant le courant de pompe de chaque laser maître M_k ($k = 1, \ldots, n$). Cependant le décryptage doit être adapté au contexte multi-utilisateur. A cette fin, nous avons présenté deux stratégies : une première possédant une grande précision mais une complexité algorithmique exponentielle avec le nombre de messages transmis (CE) et une seconde avec une présicion réduite mais une complexité algorithmique linéaire (CL). Cette méthode d'encryptage a l'avantage d'être facilement implémentable avec une technologie à base d'ECSL, le courant de pompe étant un paramètre facilement modifiable. Cependant, le CSK est limité en terme de débit de transmission notamment à cause du temps de re-synchronisation inhérent aux commutations. En considérant des paramètres identiques à ceux employés dans la Figure A.9, nous avons ainsi pu démontrer une transmission de deux messages ($n = 2$) à 1 Gbit/s avec une stratégie de décryptage CE et à 500 Mbit/s pour une stratégie de décryption CL.

Enfin, nous avons appliqué la technique de CMo qui consiste à inclure un message dans la dynamique du système. Celui-ci participe constructivement au comportement chaotique du système et n'est donc plus considéré comme une pertubation à la synchronisation (cas du CMa et du CSK). Le décryptage dans le CMo multiplexé est identique à celui du CSK multiplexé sans être limité par le temps de re-synchronisation. La différence fondamentale s'effectue à l'encryptage : chaque message est encodé sur l'amplitude ou la phase du champ optique $E_k^m(t)$ sans affecter les champs optiques provenant des autres lasers maîtres. Le champ multiplexé $E_T(t)$ présente une nouvelle expression,

$$\begin{aligned} E_{T,CMo}(t,\theta,\sigma,\mu) = \sum_{j=1}^{n} \sqrt{\eta_{jj}^m} e^{i\omega_{0j}^m(\theta+\Delta\tau_{\sigma j}^m/2)+it\Delta\omega_{j\sigma}^{\mu}+\psi_{m,j}(t-\theta-\Delta\tau_{\sigma j}^m/2)} \\ \times (1 + a_{m,j}(t-\theta-\Delta\tau_{\sigma j}^m/2)) E_j^m(t-\theta-\Delta\tau_{\sigma j}^m/2), \end{aligned} \tag{A.19}$$

avec $a_{m,j}(t)$ (respectivement $\psi_{m,j}(t)$) le $j$ième message encodé sur l'amplitude (respectivement la phase) du champ optique E_j^m. Afin de se conformer à cette nouvelle formulation mathématique, il est nécessaire de modifier l'architecture présentée en Figure A.8. Nous introduisons chaque modulateur (de phase/amplitude) dans une circulation optique afin que seul le champ du laser maître M_k soit affecté par le $k$ième message m_k. Cette circulation est composée de deux coupleurs optiques, d'un isolateur optique et du modulateur. Une représentation schématique de l'architecture modifiée est donnée en Figure A.10 pour une transmission CMo multiplexée de deux messages.

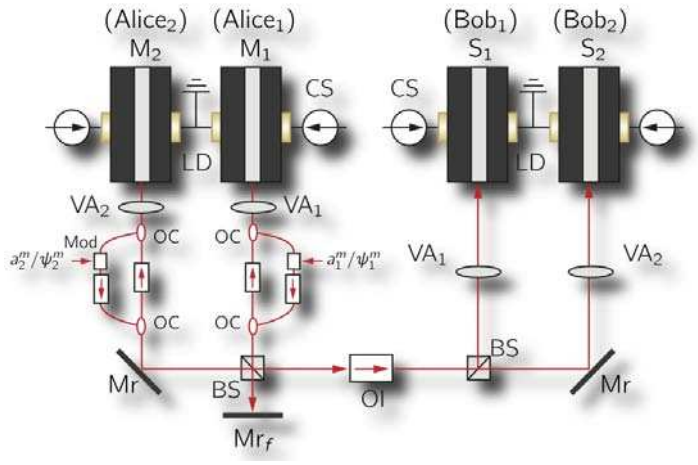

Figure A.10: Schéma théorique de multiplexage par modulation de chaos (CMo). Les deux lasers maîtres sont mutuellement couplés et les lasers esclaves découplés de telle façon que la structure soit une décomposition APD. Chaque modulateur n'affecte que le champ optique qui lui est assigné. Les abbréviations sont les suivantes LD : diode laser EEL (labelisée $M_{1,2}$ ou $S_{1,2}$ pour les masters et esclaves, respectivement), CS : source de courant, Mr,Mr_f : miroir, $VA_{1,2}$: atténuateur variable, BS : séparateur de faisceau 50/50, OI : isolateur optique, OC : coupleur optique, Mod : modulateur de phase/amplitude.

Le désavantage de ce type d'encryptage, lorsqu'il est appliqué à des ECSLs, est l'introduction d'une complexité structurelle supplémentaire. Néanmoins, les performances en terme de débit et précision de la décryption (dans les deux stratégies) est supérieure à celle du CSK. Nous avons simulé une transmission de deux messages encodés sur la phase optique de chaque laser maître M_k, chaque message ψ_k^m etant encodé sur deux valeurs de phase différentes $\{0, \pi\}$ correspondants aux deux valeurs binaires $\{0, 1\}$. Afin de récupérer chaque message, une photodiode mesure la différence de champ optique entre le champ multiplexé $E_T^s(t)$ et le champ $E_k^s(t)$ et produit une intensité électrique qui satisfait l'expression suivante :

$$I_{D,k}^{CMo} \propto \left| E_T(t, \tau_{kk}^c, k, m/s) - \sqrt{\eta_{kk}^m} e^{-j\omega_{0k}^s \tau_{kk}^m + j\psi_{k,0/1}^m} E_k^s(t - \tau_{kk}^m) \right|^2 . \tag{A.20}$$

Nous présentons dans la Figure A.11 une transmission de deux messages binaires à 1 Gbit/s avec une stratégie de décryptage à complexité linéaire. L'évolution temporelle de la sortie de chaque photodétecteur est représentée sur la figure par un trait continu gris, alors que les messages originellement encodés sur les deux états de phase $\{0, \pi\}$ sont représentés en pointillés colorés.

Le décryptage (ou détection des messages) est basée sur une détection de seuil. Pour chaque laser S_k, l'utilisateur légitime Bob_k choisit une valeur fixe de phase pour ψ_k^m dans l'intervalle $\{\psi_{k,0}^m, \psi_{k,1}^m\}$. Ainsi, chaque fois qu'$Alice_k$ transmettra un bit d'information correspondant au choix arbitraire fait par Bob_k, la valeur moyenne du courant électrique généré par le $k$ième détecteur ($I_{D,k}^{CMo}$) chutera brutalement. Cela permettra à Bob_k de détecter les différents bits de message transmis. Cependant, la détection n'est pas aussi précise que dans une stratégie de décryptage exponentiellement complexe. En effet, dans la stratégie linéaire illustrée, seule une fraction

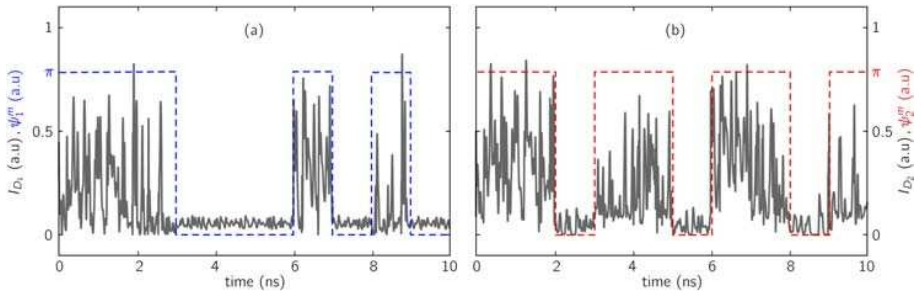

Figure A.11: Multiplexage/démultiplexage théorique de deux messages binaires encodés sur la phase optique ψ_1^m et ψ_2^m à 1 Gbit/s. Le courant généré par chaque détecteur $I_{D,k}^{CMo}$ a été normalisé par rapport à sa valeur maximale. Dix bits décodés sont représentés. Les lignes pointillées bleue et rouge correspondent aux messages encryptés par Alice$_1$ en (a) et Alice$_2$ en (b). Les paramètres de simulation sont identiques à ceux utilisés dans la Figure A.9.

du champ multiplexé $E_T(t)$ est soustrait en cas de correspondance, alors que dans le cas exponentiel la totalité du champ aurait été soustraite.

Conclusion

Nous avons exposé une nouvelle architecture de multiplexage de chaos optique basée sur l'utilisation de lasers émettant par le côté (EEL) couplés mutuellement par une cavité externe partagée. Nous avons également prouvé que la synchronisation du chaos pouvait être utilisée comme critère de séparation de différentes porteuses optiques, même si celles-ci possèdent un fort recouvrement spectral. Les conditions et la robustesse de la synchronisation du chaos pour chaque paire de lasers maître/esclave, $\mathrm{M}_k/\mathrm{S}_k$ $(k = 1, \ldots, n)$, ont été étudiées. Enfin, nous avons proposé une généralisation de méthodes d'encryptage classiques *chaos-shift keying* (CSK), et *chaos modulation* (CMo) pour une seule paire d'utilisateurs Alice/Bob, au contexte multi-utilisateurs.

A.4 Multiplexage de Chaos et Génération de Codes Optiques Orthogonaux

Introduction

Ce chapitre de thèse est dédié à l'analyse et la réalisation d'un système de multiplexage de chaos optique basé sur des dispositifs optoélectroniques afin de transmettre simultanément plusieurs messages. L'architecture proposée est issue d'un générateur de chaos en intensité [116]. Dans notre cas, nous utilisons cette même structure à base d'OEO mais en y ajoutant plusieurs boucles de rétroaction retardées. Ceci nous permettra par la suite de générer des signaux chaotiques orthogonaux et de transmettre de façon sécurisée plusieurs messages simultanément tout en garantissant un décryptage de complexité linéaire. En adoptant une philosophie identique à celle utilisée dans les méthodes de multiplexage par code (*code-division multiple access* ou CDMA) [21], les signaux chaotiques générés par des modulateurs de Mach-Zehnder (présents dans chaque boucle) sont utilisés comme séquences d'étalement

orthogonales (ou *codes*). Bien que la notion d'orthogonalité parfaite (ou décorrelation totale) entre chaque code ne soit pas nécessaire dans les approches de type CDMA, elle demeure une propriété essentielle à la simplicité algorithmique du décryptage. La transposition du CDMA en utilisant des signaux chaotiques est ambitieuse, car les codes fixes utilisés doivent être remplacés par des signaux variant dans le temps. Au niveau du récepteur, la synchronisation du chaos est utilisée pour reproduire les codes chaotiques afin de pouvoir réaliser une détection par corrélation (similaire à la méthode développée en [19]). Nous avons appliqué numériquement cette méthode et démontré la possibilité de transmettre plusieurs messages à très haut débit (multi-Gbit/s).

Architecture et Modélisation

Plusieurs architectures à base d'oscillateur électro-optique (OEO) à plusieurs boucles de rétroactions retardées sont possibles. Elles sont représentées en Figure A.12. On distingue deux classes, l'une utilisant un seul photodétecteur (Configuration 1) et l'autre en utilisant plusieurs (Configurations 2a et 2b).

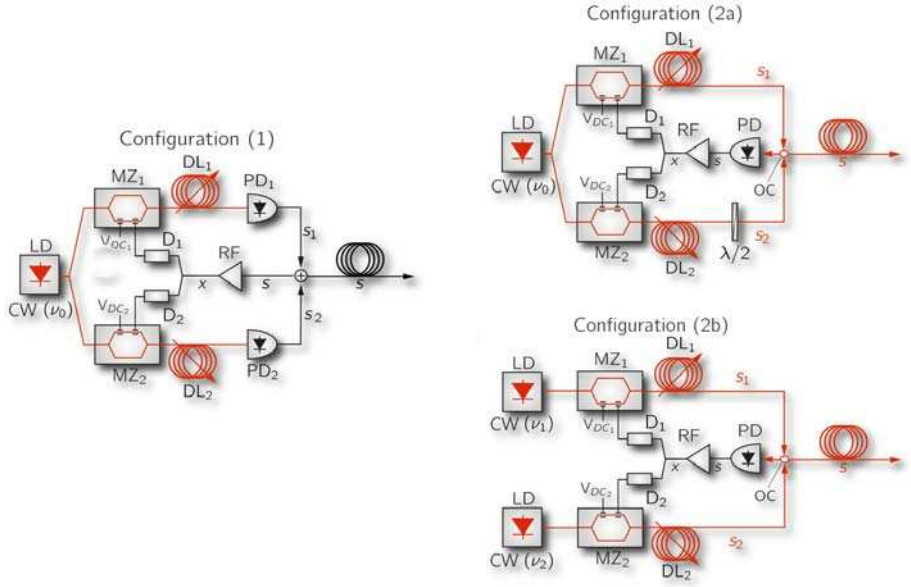

Figure A.12: Configurations des émetteurs pour la transposition du CDMA avec OEO et deux boucles de rétroaction. La Configuration (1) possède deux photodétecteurs alors que les Configurations (2a)-(2b) n'en ont qu'un. LD : diode laser, MZ$_{j=1,2}$: modulateur de Mach-Zehnder, DL$_{j=1,2}$: ligne à retard optique, PD$_{j=1,2}$: photodétecteur, RF : filtre RF passe-bande, D$_{j=1,2}$: diviseur de tension associé au facteur d'atténuation $g_{j=1,2} < 1$.

Dans la Configuration 1, l'émetteur est composé d'une source laser CW monochromatique (LD) d'une puissance optique P qui est divisée dans plusieurs bras optiques. Dans chacun d'eux, la lumière est modulée en amplitude par un modulateur de Mach-Zehnder (MZ$_i$) polarisé par la tension constante V_{dc_i} et de tensions demi-onde $V_{\pi_{rf_i}}$ (RF) et $V_{\pi_{dc_i}}$ (DC). Le champ optique linéairement polarisé se proprage dans différentes fibres optiques (DL$_i$) induisant un retard T_i pour être finalement détecté par

un photodétecteur (PD_i) d'efficacité S. Les différent signaux électriques sont ensuite recombinés en un seul signal multiplexé $s(t)$ qui est amplifié par un filtre passe-bande (RF) de gain G et de fréquences de coupures basses f_L et haute f_H. L'atténuation totale de chaque boucle est denotée $g_i < 1$ et est obtenue par des diviseurs de tension (D_i). Cela permet de modifier la fréquence d'oscillation ω_i de la non-linéarité en cosinus carré associée au modulateur MZ_i. En effet, les diviseurs D_i diminuent la tension $V(t)$ de sortie du filtre RF avant qu'elle ne soit appliquée à l'électrode de contrôle du modulateur MZ_i. En adoptant l'approche et des notations similaires à celles utilisées dans [106], il est possible de déterminer un modèle mathématique pour les Configurations (1) et (2b) :

$$\tau\dot{x}(t) + x(t) + \frac{1}{\theta}\int_{t_0}^{t} x(u)du = \sum_{i=1}^{n} \beta_i \cos^2(\omega_i x(t-T_i) + \phi_{0i}), \tag{A.21}$$

avec $x(t) = \pi g_1 V(t)/2V_{\pi_{rf_1}}$ la variable d'état du système, $x_{T_i} = x(t-T_i)$ la variable d'état retardée, $\theta = (2\pi f_L)^{-1}$, $\tau = (2\pi f_H)^{-1}$, $\beta_i = g_1 G S P_i \pi/2V_{\pi_{rf_1}}$ le gain non-linéaire, $\phi_{0i} = \pi V_{dc_i}/2V_{\pi_{dc_1}}$ un offset de phase et $\omega_i = g_i/g_1 V_{\pi_{rf_1}}/V_{\pi_{rf_i}}$ un gain interne modifiant la fréquence de la non-linearité de la $i$ème boucle de rétroaction. La présence systématique d'interférences optiques au niveau de l'unique photodétecteur utilisé dans la Configuration (2b) requiert une modification de l'équation A.21 dès que le nombre de boucles de rétroaction est supérieure à deux. Le modèle mathématique devient :

$$\begin{aligned}\tau\dot{x}(t) + x(t) + \frac{1}{\theta}\int_{t_0}^{t} x(u)du = &\sum_{i=1}^{n} \beta_i \cos^2(\omega_i x_{T_i} + \phi_{0i}) \\ &+ \sum_{j,k=1}^{n} \sqrt{\beta_j\beta_k} C_{jk} \cos(\omega_j x_{T_j} + \phi_{0j}) \cos(\omega_k x_{T_k} + \phi_{0k}),\end{aligned} \tag{A.22}$$

avec $C_{jk} = \cos(\alpha_j - \alpha_k)\cos(\varphi_j - \varphi_k)$, où α_j et φ_{0j} sont respectivement la direction de polarisation et le déphasage du champ optique dans la j-ème boucle de rétraction optoélectronique.

Propriétés Statistiques et Orthogonalité

Les systèmes chaotiques à base d'oscillateurs électro-optiques (OEO) à une seule boucle de rétroaction possèdent des statistiques approximativement gaussiennes pour leur variable d'état. L'origine d'une telle propriété réside dans les oscillations rapides de la fonction cosinus carré du terme de rétroaction : elles détruisent les corrélations internes de la variable d'état sur des échelles de temps très courtes. Il est ainsi possible d'écrire la variable d'état $x(t)$ comme la limite d'une série de variables aléatoires identiquement distribuées :

$$x(t) = \sum_{n=0}^{\infty} \left(\frac{1}{\tau} e^{-t_n/\tau} - \frac{1}{\theta} e^{-t_n/\theta} \right) X_n(t), \tag{A.23}$$

avec $X_n(t) = \int_{t_n}^{t_{n+1}} \beta \cos^2(x(t-u-T)+\phi_0)du$ et $\varepsilon_n = [t_n, t_{n+1}]$ la largeur de la n-ième oscillation de la fonction non-linéaire (résultante d'une variation de $x(t-T)$ de π/β). L'application d'une version modifiée du théorème Centrale-Limite prouve l'existence d'une statistique gaussienne (approximative) [141]. Dans le cas des Configurations (1) et (2b), l'ajout de plusieurs boucles de rétroaction (fonctions cosinus retardées de fréquences d'oscillation ω_j) ne modifie pas fondamentalement le mécanisme de destruction des corrélations aux courtes échelles de temps. En réordonnant, les produits $\omega_1\beta_1 < \cdots < \omega_n\beta_n$, lorsque la quantité $x(t-T_1)$ varie de $\pi/\omega_1\beta 1$, la fonction $s_1(t) = \beta_1 \cos^2(\omega_1 x_{T_1} + \phi_{01})$ oscillera une fois. Les autres fonctions $s_j(t) = \beta_j \cos^2(\omega_j x_{T_j} + \phi_{0j})$ oscilleront en moyenne $\left\lfloor \frac{\omega_j\beta_j}{\omega_1\beta_1} \right\rfloor$ et détruiront alors les corrélations à des échelles de temps plus fines. Par conséquent et considérant la largeur de l'oscillation de $s_1(t)$ (la plus "lente" des fonctions) $\varepsilon_{n,1} = [t_{n,1}, t_{n+1,1}]$, il est à nouveau possible de représenter la variable d'état $x(t)$ comme une somme de variables aléatoires

$$x(t) = \sum_{n=0}^{\infty} \left(\frac{1}{\tau} e^{-t_{n,1}/\tau} - \frac{1}{\theta} e^{-t_{n,1}/\theta} \right) S_n(t), \tag{A.24}$$

avec $S_n(t) = \int_{t_{n,1}}^{t_{n+1,1}} \sum_{i=1}^{n} \beta_i \cos^2(\omega_i x(t-u-T_i)+\phi_{0i})du$. Cette forte analogie avec le cas d'une unique boucle de rétroaction explique l'origine de statistiques gaussiennes pour la variable d'état des Configurations (1) et (2b). La Configuration (2a), en revanche, ne permet pas d'avoir une somme de variables indépendantes, à cause des interférences présentes : il n'est plus possible d'appliquer le théorème Centrale-Limite et celai entraîne un écart au caractère gaussien. Ces propriétés statistiques sont illustrées dans la Figure A.13 et vont permettre par la suite d'analyser les paramètres critiques garantissant l'orthogonalité entre les codes chaotiques.

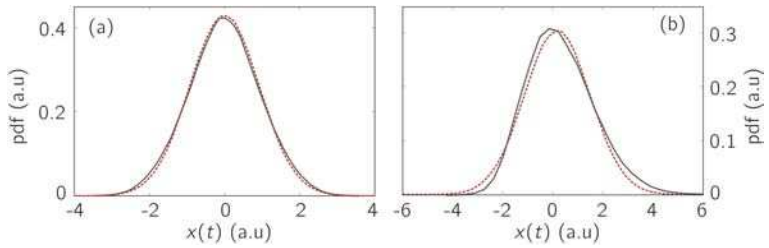

Figure A.13: Fonction de densité de probabilité de la variable d'état $x(t)$ (ligne continue grise) et la distribution gaussienne théorique associée (ligne pointillée rouge) dans le cas d'un OEO avec deux boucles de rétroaction ($n = 2$), sans interférences en (a) et avec interférences en (b). Les paramètres utilisés pour (a) sont $\tau = 25$ ps, $\theta = 5$ μs, $T_1 = T_2 = 30$ ns, $\beta_{i|i=1,2} = 5$, $\phi_{0i|i=1,2} = -\pi/4$, $\omega_2 = 2\omega_1 = 2$. Les paramètres utilisés pour (b) sont $\tau = 25$ ps, $\theta = 5$ μs, $T_j = 30 + 15(j-1)$ ns, $\beta_j = 5$, $\phi_{0j} = -\pi/4$, $\omega_j = 1 + 2(j-1)$ et $C_{ij} = \cos((i-j)\frac{\pi}{4})$ avec $i \neq j = 1, \ldots, 4$.

Notre architecture suggère un choix naturel pour les codes chaotiques : les signaux en sorties des boucles de rétroaction, soit

$$s_i(t) = \beta_i \cos^2(\omega_i x_{T_i} + \phi_{0i}). \tag{A.25}$$

En considérant $x(t)$ comme un processus stochastique stationnaire au sens large (*wide-sense stationnary* ou WSS) suivant une loi gaussienne, il est possible d'analyser les conditions d'orthogonalité entre deux codes différents $s_i(t)$ et $s_j(t)$. L'orthogonalité entre deux signaux est typiquement définie par l'annulation d'un produit scalaire également interprétable en terme d'intercovariance comme il suit :

$$\Gamma_{s_i s_j} = \left\langle s_i(t) - \mu_{s_i}, s_j(t) - \mu_{s_j} \right\rangle = \int_{-\infty}^{\infty} (s_i(t) - \mu_{s_i})(s_j(t) - \mu_{s_j}) du, \tag{A.26}$$

avec $\mu_{s_{i,j}} = \int_{-\infty}^{\infty} s_{i,j}(u) du$. En supposant que x(t) est ergodique, l'espérance mathématique $\mathbb{E}(\cdot)$ et l'opérateur de moyenne temporelle $\langle \cdot \rangle$ donneront des résultat identiques. Cela permettra ainsi de donner une expression analytique de l'intercovariance. Elle satisfait la relation suivante (considérant des délais identiques) :

$$\Gamma_{s_i s_j} = \frac{\beta_i \beta_j}{8} \left(1 - e^{-4\omega_i \omega_j \sigma_x^2}\right) \left(\cos 2\Delta\phi_{0ij} + \cos(2\phi_{0i} + 2\phi_{0j}) e^{-4\omega_i \omega_j \sigma_x^2}\right) e^{-2\Delta\omega_{ij}^2 \sigma_x^2}, \tag{A.27}$$

avec $\Delta\omega_{ij} = \omega_i - \omega_j$ le décalage en fréquence d'oscillation, $\Delta\phi_{0ij} = \phi_{0i} - \phi_{0j}$ le déphasage entre les fonctions non-linéaires et σ_x^2 la variance de $x(t)$. Généralement, les codes $s_i(t)$ sont choisis avec des gains non-linéaires identiques $\beta_i = \beta$ afin qu'ils aient tous des variances approximativement identiques (une propriété désirable pour des questions de sécurité). Sous ces conditions, il est ainsi possible d'analyser l'impact des différences de paramètres. Lorsque le décalage en fréquence $\Delta\omega_{ij}$ augmente (en considerant les autres paramètres fixes), l'intercovariance satisfait $\Gamma_{s_i s_j} \sim e^{-2\Delta\omega_{ij}^2 \sigma_x^2}$ et révèle une décroissance exponentielle de la corrélation entre deux codes. Le gain non-linéaire β apparaît quant à lui explicitement en facteur multiplicatif ainsi qu'implicitement dans la variance de la variable d'état : $\sigma_x^2 = c_\beta \beta^2$ avec $c_\beta > 0$, un coefficient de proportionalité. Une augmentation du gain non-linéaire seul conduit à l'expression suivante $\Gamma_{s_i s_j} \sim \frac{\beta^2}{8} \cos 2\Delta\phi_{0ij} e^{-2\Delta\omega_{ij}^2 c_\beta \beta^2}$, démontrant aussi la possibilité d'assurer asymptotiquement une orthogonalité quasi-parfaite. Enfin, les phases respectives $\phi_{0i,0j}$ et le déphasage relatif $\Delta\phi_{0ij}$ peuvent être ajustés aux valeurs respectives, $\phi_{0i} + \phi_{0j} = (2p+1)\pi/4$ et $\Delta\phi_{0ij} = (2p+1)\pi/4$ avec $p \in \mathbb{Z}$, afin d'assurer l'orthogonalité. Cependant, il n'existe pas de famille $\{\phi_{0i}\}_{i=1,\ldots,n}$ permettant d'assurer l'orthogonalité systématique des codes si $n > 2$. Ainsi le décalage $\Delta\omega_{ij}$ et β offrent plus de flexibilité pour la génération de codes chaotiques orthogonaux. Ces résultats ont été confirmés par des simulations numériques présentées en Figure A.14. Dans les plans de paramètres $(\Delta\omega_{ij}, \beta)$ et $(\Delta\omega_{ij}, \Delta\phi_{0ij})$, l'intercovariance normalisé $\rho_{s_i s_j} = \Gamma_{s_i s_j} / (\Gamma_{s_i s_i} \Gamma_{s_j s_j})^{1/2}$ est calculée sur une durée finie T_b, correspondant aux futures durées de modulation utilisées pour la transmission de données. Les résultats sont ensuite moyennés sur $5000 T_b$ afin de statistiquement réduire les effets de possibles *outliers*.

Il est également important de souligner l'influence de la durée T_b sur l'orthogonalité. En effet, les intercovariances sont calculables seulement pour des valeurs de T_b suffisamment longues. T_b doit être au moins deux fois plus large que le temps de décorrelation de $x(t)$, sans quoi les calculs n'auraient plus de sens.

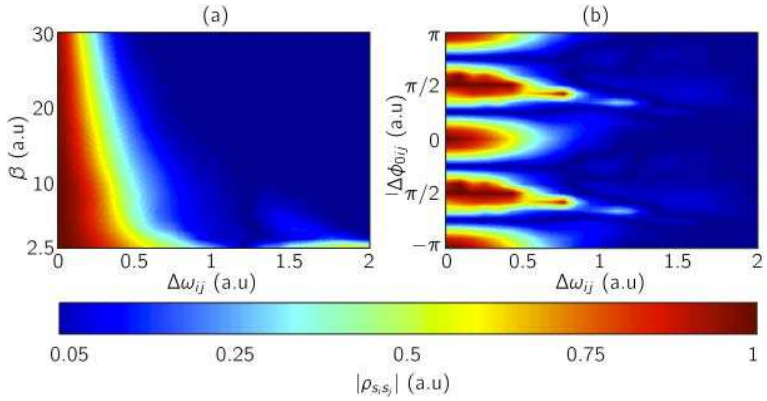

Figure A.14: Coefficient d'intercovariance normalisé $|\rho_{s_i s_j}|$ entre les codes chaotiques s_i et s_j dans les plans de paramètres $(\Delta\omega_{ij}, \beta)$ en (a) et $(\Delta\omega_{ij}, \Delta/phi_{0ij})$ en (b). Les simulations ont été réalisées sur une structure à deux boucles de rétroaction sans interférences avec des valeurs de paramètres identiques à celles de la Figure A.13(a). Les résultats sont moyennés sur $5000T_b$ avec $T_b = 0.4$ ns.

Multiplexage d'information

Les codes orthogonaux peuvent finalement être utilisés pour multiplexer et démultiplexer plusieurs messages dans l'esprit du CDMA. Pour cela, chaque gain non-linéaire β_i est modulé digitalement à la fréquence $1/T_b$ par le $i$ème message binaire m_i. Ainsi, le signal $s(t)$ peut s'écrire pour les Configurations (1)-(2b) et (2a) par les expressions suivantes :

$$s_{1,2b}(t) = \sum_{i=1}^{n} \beta_i(1+\delta m_i)\cos^2(\omega_i x_{T_i} + \phi_{0i}), \tag{A.28}$$

$$\begin{aligned} s_{2a}(t) &= \sum_{i=1}^{n} \beta_i(1+\delta m_i)\cos^2(\omega_i x_{T_i} + \phi_{0i}) \\ &\quad + \sum_{1\leqslant i,j\leqslant n} \sqrt{\beta_i\beta_j(1+\delta m_i)(1+\delta m_j)}\cos(\omega_i x_{T_i} + \phi_{0i})\cos(\omega_j x_{T_j} + \phi_{0j}), \end{aligned} \tag{A.29}$$

avec $m_i(t) = \pm 1$ et δ l'amplitude de modulation satisfaisant $|\delta| \ll 1$, permettant de préserver l'orthogonalité entre les codes et d'assurer une dissimulation efficace des messages.

Une chaîne de transmission complète pour une Configuration (2a) avec deux boucles de rétroaction est présentée en Figure A.15. Elle correspond à une structure de décomposition active-passive (APD) : les deux OEO sont ainsi soumis au même signal $s_{1,2a,2b}(t)$, au temps de transmission T_c prêt. Ainsi, les équations de la chaîne de transmission sont données par

$$\tau\dot{x}_E(t) + x_E(t) + \frac{1}{\theta}\int_{t_0}^{t} x_E(s)ds = s_{1,2a,2b}(t), \tag{A.30}$$

$$\tau\dot{x}_R(t) + x_R(t) + \frac{1}{\theta}\int_{t_0}^{t} x_R(s)ds = s_{1,2a,2b}(t - T_c). \tag{A.31}$$

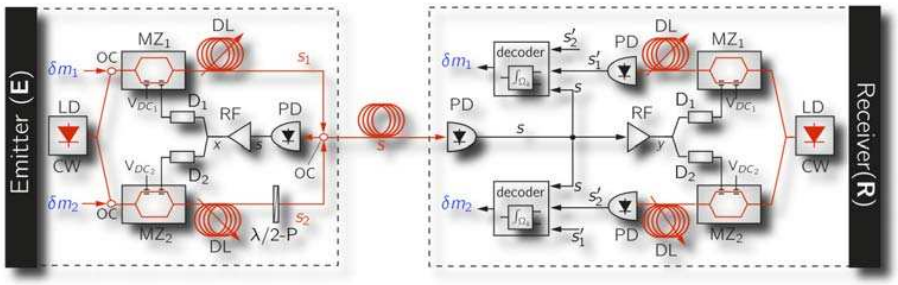

Figure A.15: Chaîne de transmission chaotique pour communications multiplexées. L'émetteur (E) et le récepteur (R) sont composés d'un OEO avec deux boucles de rétroaction et d'un seul photodétecteur [Configuration (2a)]. La structure du bloc de décodage dépend de la présence ou non d'interférences optiques. LD : diode laser, $\mathrm{MZ}_{j=1,2}$: modulateur de Mach-Zehnder, $\mathrm{DL}_{j=1,2}$: ligne à retard optique, $\lambda/2$: lame demi-onde, OC : coupleur optique, PD : photodétecteur, RF : filtre passe-bande, $\mathrm{D}_{j=1,2}$: diviseur de tension et $m_{j=1,2}$: message à encrypter.

Le décryptage des messages dépend du type de configuration et de métrique utilisée (covariance ou norme euclidienne). Il requiert la duplication des codes au récepteur, une étape clé exploitant la synchronisation du chaos existnat entre E et R. Nous présentons ici les méthodes de décryptage pour des configurations avec et sans interférences basées sur des calculs d'intercovariance.

Pour les Configurations (1) et (2b), les messages sont récupérés en considérant l'équation de décodage suivante :

$$\delta m_i(t) \approx \frac{1}{\Gamma_{s'_i s' i}} \left(\Gamma_{s s'_i} - \sum_{j=1}^{N} \Gamma_{s'_j s'_i} \right), \tag{A.32}$$

avec $s'_{i,j}(t) = \beta_{i,j} \cos^2(\omega_{i,j} x_R(t - T_{ij}) + \phi_{0i,0j})$, les réplicats respectifs des codes $s_{i,j}(t)$. L'équation A.32 est similaire à celle utilisée dans la référence [19], à l'exception des mesures d'intercovariance utilisées. Le membre de gauche de l'équation A.32 s'écrit rigoureusement

$$\delta m_i(t)(1 + \lambda_{ij}) \text{ avec } \lambda_{ij} = \sum_{j=1, j\neq i}^{N} \frac{m_j(t) \Gamma_{s'_j s'_i}}{m_i(t) \Gamma_{s'_i s'_i}}. \tag{A.33}$$

Les effets des autres messages et de leurs codes ($m_j(t)$ et $s_j(t)$, respectivement) sont ainsi mis en évidence. Afin d'assurer un décodage sans erreur du message $m_i(t)$ par Eq. A.32, il est important de garantir que le facteur λ_{ij} n'affecte pas son signe. Ainsi, la condition $|\lambda_{ij}| < 1$ doit être satisfaite ; ce qui est le cas lorsqu'il existe une orthogonalité quasi-parfaite entre les différents codes composant le signal multiplexé $s(t)$. Au regard de cette condition, le nombre d'utilisateurs pouvant communiquer simultanément est d'autant plus large que l'on s'approche de l'orthogonalité entre les différents codes. La Figure A.16 présente la transmission multiplexée de deux messages à 2.5 Gbit/s par utilisateur en utilisant une architecture à rétroaction sans interférences.

La présence d'interférences dans le signal de feedback requiert une modification de l'équation de décodage, ainsi qu'une duplication des codes "racines" définis par

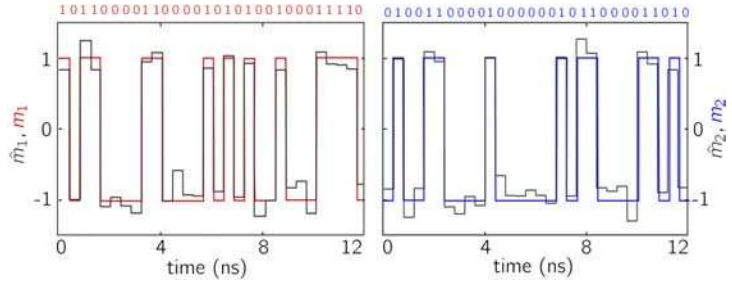

Figure A.16: Simulation numérique d'une transmission multiplexée de deux messages binaires à 2.5 Gbit/s (standard OC-48). Les lignes solides bleue et rouge désignent les messages encryptés par $\text{Alice}_{1,2}$ et les lignes solides grises ceux décryptés par les $\text{Bob}_{1,2}$. Les paramètres utilisés sont $\beta_{i|i=1,2} = 5$, $\phi_{0i|i=1,2} = -\pi/4$, $\theta = 10$ μs, $\tau = 25$ ps, $T_{i|i=1,2} = 30$ ns et $\Delta\omega_{12} = 2$.

$r_j(t) = \sqrt{\beta_j}\cos(\omega_j x_E(t - T_j) + \phi_{0j})$. Le décryptage du message m_i est réalisé par le calcul de l'intercovariance entre $s(t)$ et $s'_i(t)$ suivi d'un développement au premier ordre en δ. L'équation de décodage devient ainsi

$$\delta m_i \approx \frac{1}{\Gamma_{s'_i s'_i} + \sum\limits_{j=1, j\neq i}^{n} C_{ij}\Gamma_{s'_i r'_i r'_j}} \left(\Gamma_{s s'_i} - \sum_{j=1}^{n} \Gamma_{s'_i s'_j} - \sum_{1 \leqslant j,k \leqslant n} C_{jk}\Gamma_{s'_i r'_j r'_k} \right), \quad \text{(A.34)}$$

avec r'_j le réplicat de r_j au récepteur. Le membre de gauche de l'équation de décryptage possède également une forme rigoureuse $\delta m_i(t)(1+\gamma_{ij})$ analogue à A.33, celle-ci étant détaillée dans le manuscrit de thèse. Une simulation numérique a également prouvé que l'architecture avec interférences a la capacité de transmettre plusieurs messages à 2.5 Gbit/s avec des performances comparables à celles du cas sans interférences.

Conclusion

Dans ce chapitre, nous avons démontré qu'un OEO avec plusieurs boucles de rétroaction retardées pouvait être utilisé pour générer des codes orthogonaux chaotiques. Nous avons ainsi pu transposer une technique CDMA aux communications optiques chaotiques. Les séquences pseudo-aléatoires (codes) utilisées pour l'étalement spectral des messages sont produites par les modulateurs de Mach-Zehnder de chaque boucle. A chacun d'eux est associé une non-linéarité de type cosinus carré dont les paramètres, gain non-linéaire (β_j), fréquence d'oscillation (ω_j), offset de phase (φ_{0j}) et délai (τ_j), contrôlent les propriétés statistiques du code. S'ils sont tous générés à partir de $x(t-T)$, il apparaît qu'un décalage en fréquence $\Delta\omega_{ij} = \omega_i - \omega_j$ et un gain β_j suffisament larges en assurent l'orthogonalité. Il devient alors possible de réaliser un encryptage et un décryptage à très haut débit (numériquement 2.5 Gbit/s par utilisateur). En cas d'orthogonalité imparfaite, le décryptage des messages requiert l'utilisation de la matrice de covariance de tous les codes ou une minimisation par moindres carrés ; alors la complexité algorithmique du décryptage augmente.

A.5 Architectures à Délais Aléatoires pour Communications Chaotiques Multiplexées.

Introduction

Ce chapitre de thèse est dédié à l'utilisation d'une nouvelle classe de systèmes à délais multiples pour des applications de cryptographie multiplexée par chaos. Notre objectif premier est l'accroissement de l'efficacité spectrale et de la sécurité. Précédemment, nous avions proposé des architectures pour multiplexer plusieurs messages en utilisant des extensions de techniques d'encryptage classiques (CMa, CSK ou CMo) ou en adaptant des idées issues des approches CDMA, tout en assurant des débits de plusieurs Gbit/s par utilisateur. Néanmoins, le niveau de sécurité n'avait pas été amélioré, en particulier en ce qui concerne la dissimulation du (ou des) délai(s). Lorsque ces derniers sont fixes, l'essentiel de la sécurité algorithmique est basé sur la dissimulation de leur valeur [151; 152] (voir également Chapitre 4). Une idée naturelle pour améliorer la sécurité des systèmes à délais est de les faire varier au cours du temps. Cette ligne de raisonnement a conduit au développement de plusieurs stratégies : l'utilisation d'un délai variant périodiquement [147], aléatoirement (continûment) [178] ou par commutations aléatoires entre deux états [146]. Les deux dernières approches ont conduit à un haut degré de confidentialité de l'information du délai au regard des techniques d'estimation classiques. Parallèlement, l'idée selon laquelle une modulation du délai pouvait servir de vecteur de communication est apparue rapidement et a été démontrée avec des applications logistiques [176]. Nous avons décidé d'appliquer cette idée au contexte multi-utilisateurs, afin d'assurer des transmissions multiplexées à haut-débit et haute sécurité.

Description de l'Architecture

Notre architecture est décrite dans la Figure A.17. Elle se décompose en deux systèmes, un premier constituant l'émetteur global (E) et un second pour le récepteur global (R). Ces deux systèmes sont couplés unidirectionellement via un unique canal de communication et présentent une similarité structurelle : chacun d'eux utilise un unique oscillateur non-linéaire décrit par les variables d'état $\mathbf{x}_E \in \mathbb{R}^n$ et $\mathbf{x}_R \in \mathbb{R}^n$. A l'émetteur E, l'oscillateur est rétro-injecté par n boucles retardées et assignées spécifiquement à chaque utilisateur Alice_i. Une boucle est composée d'une non-linéarité spécifique NL_i qui agit sur la variable d'état de l'émetteur $h_{A_i}(\mathbf{x}_E(t))$ et d'une ligne à retard ajustable DL_i contrôlant le délai variable $\tau_i(t)$ modulé digitalement. Les contributions de chaque utilisateur sont ensuite additionnées pour former un unique signal multiplexé $s(t)$ satisfaisant

$$s(t) = \sum_{i=1}^{n} h_{A_i}(\mathbf{x}_E(t - \tau_i(t))). \tag{A.35}$$

Le signal $s(t)$ est généralement vectoriel ($s(t) \in \mathbb{R}^m$) mais nous nous restreindrons au cas scalaire ($m = 1$) afin de simplifier les notations et calculs.

En supposant un temps de transmission négligeable entre l'émetteur et le récepteur, le signal $s(t)$ injecte les deux systèmes de manière analogue

$$\dot{\mathbf{x}}_E = f_E(\mathbf{x}_E, s(t)) \text{ and } \dot{\mathbf{x}}_R = f_E(\mathbf{x}_R, s(t)). \tag{A.36}$$

L'hypothèse supplémentaire selon laquelle E et R se synchronisent provient de la structure APD employée.

L'encryptage de chaque message m_i est réalisé au travers de la modulation du $i$ème délai $\tau_i(t)$ au rythme de l'apparition des symboles $(c_1^{\mu_i}, \ldots, c_{M_i}^{\mu_i})$ dans un intervalle spécifié au préalable $\Delta_i = [\tau_{i_0} - \Delta\tau_i/2; \tau_{i_0} - \Delta\tau_i/2]$, appelé "intervalle d'encryptage". Les symboles sont générés séquentiellement pour chaque utilisateur dans une fenêtre temporelle denotée $\Omega_k = [kT_s, (k+1)T_s]$, où k est l'indice correspondant au $k$ième symbole et T_s sa durée. Ainsi, chaque délai est modulé digitalement comme il suit

$$\tau_i(t) = \sum_{k\in\mathbb{N}} \tau_{i|\Omega_k}(H(t - kT_s) - H(t - (k+1)T_s), \tag{A.37}$$

avec H la fonction de Heaviside et $\tau_{i|\Omega_k}$ l'encodage du $k$ième symbole généré par Alice$_i$.

Stratégies d'Encryptage et de Décryptage

L'encryptage d'une information binaire sur la valeur du délai a été proposé dans un schéma de communication à utilisateur unique [178]. Cependant, notre approche présente l'avantage de pouvoir encrypter de multiples messages M-aires. Notre encryptage s'avère plus simple que dans [178] grace à des modulations du délai induite seulement par les variations des messages. Cela a permis une simplification du décryptage via des métriques standards (corrélation, norme euclidienne). Plusieurs stratégies d'encryptage existent grace aux degrés de liberté de chaque boucle de rétroaction : le type de non-linéarité (NL$_i$) et (2) l'intervalle d'encryptage (Δ_i). Il est crucial d'inclure dans l'encryptage un critère de discrimination, sans lequel il serait impossible pour les Bobs de décrypter leur message.

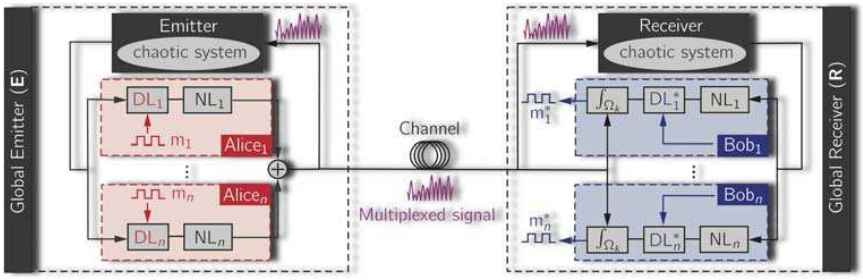

Figure A.17: Architecture utilisant un unique oscillateur chaotique avec de multiples de boucles de rétroaction afin de multiplexer des messages digitaux. NL$_i$: la $i$ème non-linéarité, DL$_i$: $i$ème ligne à retard variable modulée digitalement par Alice$_i$, DL$_i^*$: ligne à retard variable utilisée par Bob$_i$ afin de rechercher le maximum d'intercorrélation. m$_i$: message encrypté par Alice$_i$, m$_i^*$: message décrypté par Bob$_i$ ($i =, \ldots, n$), Ω_k : durée pendant laquelle un symbole (ou un bit) du message m$_i$ est maintainu constant.

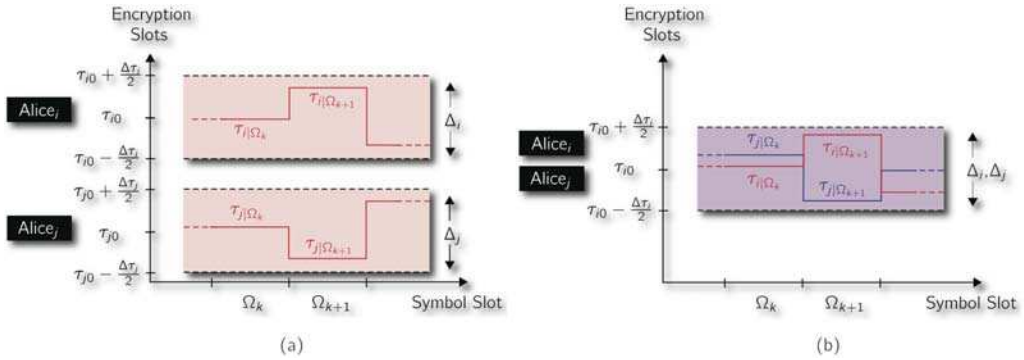

Figure A.18: Représentation graphique de l'encryptage par modulation du délai réalisé par deux utilisateurs différents Alice$_i$ et Alice$_j$ dans leurs intervalles d'encryptage respectifs Δ_i et Δ_j, disjoints en (a) et totalement superposés en (b). L'encryptage de deux symboles successifs $\tau_{i,j|\Omega_{k,k+1}}$ est illustré pour chaque utilisateur.

Nous avons proposé deux types d'encryptage différents. Le premier consiste en l'utilisation d'intervalles d'encryptage disjoints ($\Delta_i \cap \Delta_j = \emptyset$ pour tout $i \neq j$) associée à une liberté quasi-totale dans le choix de la fonction non-linéaire h_{A_i}. Cette méthode est illustrée dans la Figure A.18(a). Le second type d'encryptage consiste en l'utilisation d'intervalles d'encryptage (partiellement ou totalement) superposés ($\Delta_i \cap \Delta_j \neq \emptyset$ pour tout $i \neq j$) avec des fonctions non-linéaires spécifiques. La Figure A.18(b) illustre cette approche avec un seul intervalle d'encryptage partagé par tous les utilisateurs.

Le décryptage de chaque message revient pour Bob$_i$ à retrouver les modulations discrètes du délai $\tau_{i|\Omega_k}$ utilisées par Alice$_i$ pour tout Ω_k. Pour ce faire, les Bobs commencent par générer indépendemment ou conjointement des délais candidats τ_i^* ($i = 1, \ldots, n$) grâce à une ligne à retard réglable dénotée DL_i^*. Ensuite, ils résolvent un problème d'optimisation défini sur une "métrique" appropriée (norme euclidienne ou corrélation). Afin de garantir que la solution du problème d'optmisation corresponde bien aux valeurs du (ou des) délai(s) initialement encryptées, il est nécessaire que l'encryptage respecte la série de conditions suivante (en plus du critère de discrimination évoqué précédemment) : (i) l'émetteur E et le récepteur R doivent être complètement synchronisés, (ii) la solution au problème d'optimisation doit être unique (extremum global) et enfin (iii) deux symboles dans un intervalle d'encryptage donné doivent être séparables via la métrique considérée. La norme euclidienne et la corrélation sont toutes deux construites à partir d'un produit scalaire sur un espace fonctionnel. Pour deux signaux (φ_i, φ_j) d'énergie finie (ou appartenant à $\mathbb{L}^2(\mathbb{R})$), le produit scalaire est simplement défini par $\langle \varphi_i, \varphi_j \rangle_{\Omega_k} = \int_{\Omega_k} \varphi_i(t)\varphi_j(t)dt$; ce qui permet de déduire l'expression de la norme euclidienne, $||\varphi_i||_{\Omega_k} = \langle \varphi_i, \varphi_i \rangle_{\Omega_k}^{1/2}$. Les métriques étant définies, il est à présent possible de préciser les stratégies de décryptage en supposant que les triplets de valeurs (T_s, h_{A_i}, Δ_i) sont partagés entre les Alice$_i$ et les Bob$_i$ ($i = 1, \ldots, n$) en plus des trois conditions (i)-(iii). Les Bob$_i$ peuvent ainsi estimer indépendamment les symboles $\tau_{i|\Omega_k}$ des Alice$_i$ en détectant quelle valeur de $\tau^*_{i|\Omega_k}$ maximise l'intercorrélation $\langle s_{B_i,\tau_i^*}, s \rangle^{\Omega_k}$ avec $s_{B_i,\tau_i^*} = h_{A_i}(\mathbf{x}_R(t - \tau_i^*)) = s_{A_i,\tau_i^*}$. Les Bob$_i$ peuvent également estimer conjointement le vecteur de délais employé par

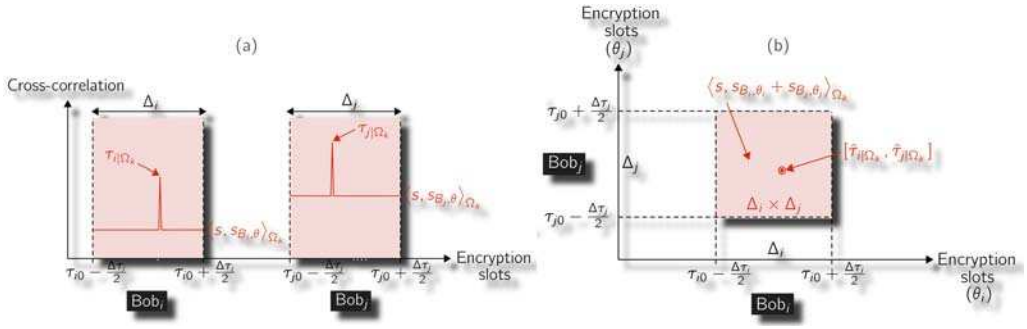

Figure A.19: Représentation graphique du décryptage des délais realisé par deux utilisateurs Bob_i et Bob_j. En (a), un décryptage avec une complexité linéaire est illustré pour une configuration avec des intervalles d'encryptages disjoints Δ_i et Δ_j. En (b), un décryptage à complexité exponentielle est présenté. Sur une période donnée Ω_k, chaque Bob détecte une résonance afin d'estimer son délai. Une mesure d'intercorrélation est utilisée comme métrique.

les Alice_i en cherchant à maximiser l'intercovariance $\langle s^*, s\rangle^{\Omega_k}$ avec $s^* = \sum_{i=1}^n s_{B_i,\tau_i^*}$. Les problèmes d'optimisation sont ainsi formulés :

$$\hat{\tau}_{i|\Omega_k} = \underset{\tau^*_{i|\Omega_k} \in \Delta_i}{\arg\max} \left\langle s, s_{B_i,\tau^*_{i|\Omega_k}} \right\rangle^{\Omega_k} \text{ décryptage indépendant,} \quad \text{(A.38)}$$

$$(\hat{\tau}_{i|\Omega_k})_{i\in[\![i,n]\!]} = \underset{(\tau^*_{i|\Omega_k})_{i\in[\![i,n]\!]} \in \prod_{i=1}^n \Delta_i}{\arg\max} \langle s^*, s\rangle^{\Omega_k} \text{ décryptage conjoint.} \quad \text{(A.39)}$$

La Figure A.19 illustre graphiquement les solutions des problèmes d'optimisation indépendant (de complexité linéaire) et conjoint (de complexité exponentielle) par détection d'une résonance dans les mesures d'intercorrélation.

Nous proposons par la suite d'exploiter ce cadre théorique et de simuler numériquement une chaîne de transmission composée de deux OEO unidirectionnellement couplés. L'émetteur est soumis à l'effet de quatre boucles de rétroaction, permettant ainsi une transmission de quatres messages simultanément. Les OEO utilisés sont analogues à ceux présentés dans le chapitre précédent : générateurs de chaos en intensité basés sur l'utilisation de plusieurs modulateurs de Mach-Zehnder. La chaîne de communication peut ainsi être modélisée par le système d'équations couplées

$$T\dot{x}_E + x_E + \frac{1}{\theta}\int_{t_0}^t x_E(u)du = s(t), \quad \text{(A.40)}$$

$$T\dot{x}_R + x_R + \frac{1}{\theta}\int_{t_0}^t x_R(u)du = s(t-\tau_c), \quad \text{(A.41)}$$

avec τ_c le délai de transmission du signal, $s(t) = \sum_{i=1}^n \beta_i \cos^2(x(t-\tau_i(t)) + \varphi_{0i})$ le signal multiplexé, $x_E, x_R \in \mathbb{R}$ les variables d'état adimensionnées, $f_H = 1/(2\pi T)$ et $f_H = 1/(2\pi\theta)$ les fréquences de coupure basse et haute, β_i le gain non-linéaire normalisé de la $i$ème boucle et φ_{0i} l'offset de phase normalisé. Il est possible de reformulé le système A.41-A.41 en un système d'équations différentielles à délai via le changement de variable $y_{E,R} = 1/T \int_{t_0}^t x_{E,R}(u)du$. Ainsi, notre stratégie d'encryptage peut

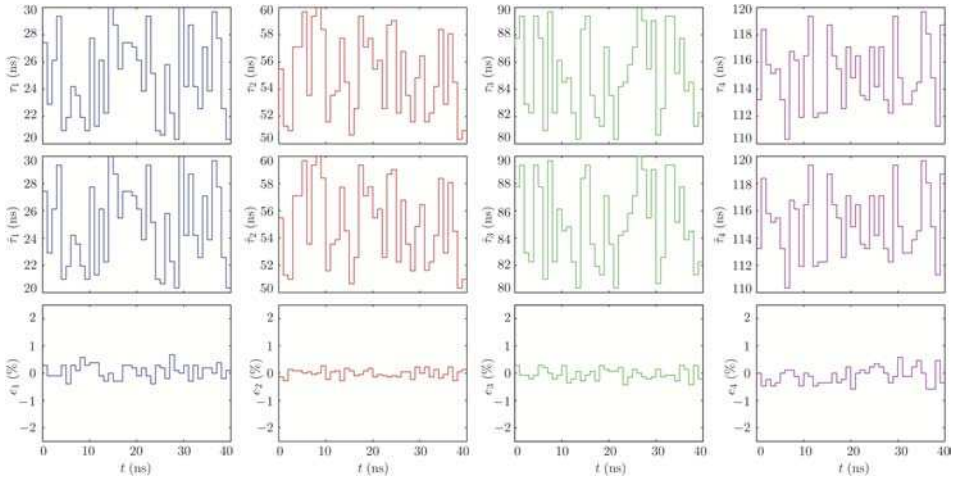

Figure A.20: Décryptage simultané de quatre messages composés chacun de $M_i = 32$ symboles ($i = 1, \ldots, 4$) à 1 Gsymboles/s par utilisateur, soit après quantification 5 Gbits/s par utilisateur, soit en cumulé 20 Gbits/s. La métrique utilisée pour le décryptage est l'intercorrélation. La première ligne de la figure représente les messages m_i encryptés par les Alice$_i$, la seconde ligne les messages $\hat{m}_i$ décryptés (ou estimés) par les Bob$_i$ et la troisième ligne les erreurs relatives e_i de décryptage de chaque symbole.

être appliquée. Nous avons simulé le système avec les intervalles d'encryptage disjoints $\Delta_i = [20i \text{ ns}, 20i + 10 \text{ ns}]$ dans lesquels $M_i = 32$ symboles sont considérés et encodés à un débit de 1 Gsymbole/s, soit $T_s = 1$ ns. Les densités dans chaque intervalle (3.2 symboles/ns) garantissent la séparabilité de chaque symbole par les mesures d'intercorrélation réalisées par les différent Bobs (condition (iii)). Les 32 symboles nécessitent une quantification sur 5 bits conduisant une transmission de 5 Gbits/s/utilisateur, soit en cumulé à 20 Gbits/s. La Figure A.20 illustre l'encryptage et le décryptage simultanés de quatre utilisateurs Alices et Bobs dans des conditions de transmissions optimales (pas de bruit, pas de distorsion dûes au canal). Les erreurs relatives de décryptage $e = (\tau_i - \hat{\tau}_i)/\tau_i$ sont également représentées et sont en moyenne inférieures à 0.5% pour ces niveaux de densité de symboles et de débit. Ces imprécisions systématiques dans le décryptage sont dues aux incertitudes associées aux calculs des intercorrélations sur des intervales de durée finie Ω_k. Cependant, elles peuvent être supprimées si Alice$_i$ communique à Bob$_i$ l'ensemble des symboles utilisés. Les performances du décryptage sont également impactées par le nombre n d'utilisateurs (ou de boucles) qui va accroître le bruit d'intercorrélation et augmenter le risque de détecter un extremum ne correspondant pas à une signature de $\tau_{i|\Omega_k}$ dans l'intervalle Δ_i.

Sécurité et Cryptanalyse

Dans notre architecture, la sécurité bénéficie des variations aléatoires et indépendantes des délais de chaque boucle de rétroaction. Comme illustré dans le Chapitre 4, les systèmes à délais fixes possèdent des défauts de sécurité dès que leurs valeurs sont connues. En effet, et malgré les larges dimensions d'attracteurs, un espion peut réussir à attaquer ce type de système dans un espace des phases de dimension réduite

correspondant à la dimension de la représentaton d'état et dans lequel la fonction non-linéaire peut être identifiable pour un faible coût algorithmique. Ainsi, il devient possible de reconstruire la dynamique du système par simple analyse de la série temporelle. Cependant, le problème de l'identification du délai devient beaucoup plus complexe si celui-ci varie de manière erratique dans le temps.

Notre approche correspond à une généralisation d'un système proposé dans [146], qui comprenait un délai unique commutant entre deux états ($n = 1, M_1 = 2$ avec les notations utilisées dans ce chapitre). Contrairement à cette première étude, notre architecture a ses commutations de délais contrôlées par des sources d'information et se font sur plus de deux états. L'analyse de sécurité d'un système à délai commutant aléatoirement a démontré qu'un temps de commutation T_s inférieur à la plus petite valeur prise par le délai permettait d'éviter qu'un espion attaque le système facilement.

Dans notre architecture, le résultat se généralise aisément et s'exprime mathématiquement sous la forme suivante :

$$T_s < \min_{i,k} \tau_{i|\Omega_k}. \tag{A.42}$$

Il devient ainsi impossible pour un espion de réaliser une estimation du délai (ou symbole) choisi par Alice$_i$ dans l'intervalle $\Omega_k = [kT_s, (k+1)T_s]$. En effet, la détection d'une résonance associée à $\tau_{i|\Omega_k}$ est possible seulement si cette valeur appartient à l'intervalle de valeur $\Omega_k \mod Ts = [0, T_s]$. Dans le cas contraire, le délai $\tau_i(t)$ serait modulé plusieurs fois. Ainsi, dans le meilleur des cas un espion détecterait les signatures des symboles sans pouvoir déterminer leur temps d'émission, et donc décoder les messages. Ce principe demeure vrai dans le contexte multi-utilisateurs, comme décrit par Eq. A.42.

A titre d'illustration, nous avons réalisé une analyse numérique de la sécurité par mesure d'information mutuelle retardée (DMI, voir Chapitre 4). Le système considéré est toujours un générateur de chaos en intensité à plusieurs délais aléatoires. Les résultats sont présentés en Figure A.21.

La densité de symbole utilisée est importante, 3.2 symboles/ns, le gain non-linéaire de chaque boucle élevé, $\beta_i = \beta = 20$ et la fréquence de commutation rapide, $F_s = 1/T_s = 1$ GHz. Dans ces conditions, nous observons qu'aucune signature des délais n'est visible lorsque l'estimateur DMI est utilisé. Des résultats similaires ont été observés lorsque les intervalles d'encryptage Δ_i sont complètement superposés. Il est également important de souligner le rôle du nombre de symboles vis-à-vis de la sécurité. En effet, si une source d'information réelle est employée, celle-ci peut générer des bits avec des *patterns* répétitifs, en particulier dans le cas de sources binaires. La répétition sur plusieurs périodes T_s d'une même valeur d'un bit accroît la probabilité qu'un espion puisse accéder à une partie du message transmis. Cependant, si l'on choisit d'encoder des blocs de $\log_2 M_i$ bits, alors il devient possible de capturer des structures binaires répétitives plus larges et de les encoder sur une unique valeur de délai. De plus, si la densité de symboles $M_i/|\Delta_i|$ par intervalle d'encryptage Δ_i est large, les signatures associées aux différents délais $\tau_{i|\Omega_k}$ ($i = 1, \ldots, n$ et $k \in \mathbb{N}$) deviennent relativement indiscernables. En effet, le nombre de symboles est suffisamment grand, il devient possible de considérer les commuta-

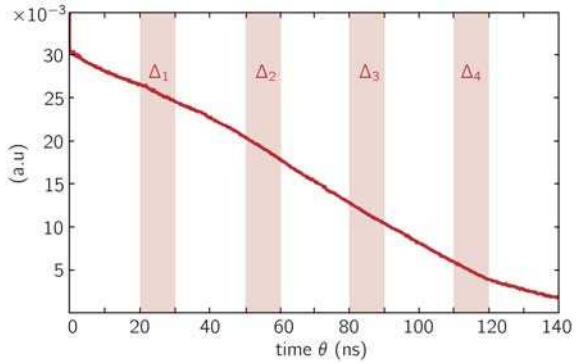

Figure A.21: Analyse de sécurité par information mutuelle retardée (DMI) d'une architecture de communication pour $n = 4$ utilisateurs avec intervalles d'encryptage disjoints $\Delta_i = [20i$ ns, $20i +$ 10 ns] avec $i = 1, \ldots, n$. Le nombre de symboles employés est $M_i = 32$ (densité de symboles 3.2 symboles/ns) avec un débit de 1 Gsymboles/s, les autres paramètres étant identiques à ceux utilisés en Figure A.20.

tions aléatoires rapides comme un processus stochastique continu, pour lequel le très haut niveau de sécurité vis-à-vis de l'estimation du délai a déjà été démontré [176].

Conclusion

Dans ce chapitre, nous avons démontré la capacité d'un crypto-système chaotique à encrypter n différents messages en utilisant un unique oscillateur non-linéaire soumis à n boucles de rétroaction retardées et à décrypter ces messages à l'aide de la synchronisation du chaos. Notre approche associe l'aléatoire de la source d'information aux comportements hyperchaotiques des systèmes à délai : les messages sont encryptés via une modulation digitale du délai de chaque boucle en respectant certaines règles garantes d'un décryptage sans erreur au récepteur. Deux types d'encryptage sont possibles afin d'associer chaque symbole du message d'un utilisateur Alice$_i$ ($i = 1, \ldots, n$) avec une valeur de délai : l'utilisation d'intervalles d'encryptage (i) disjoints ou (ii) partiellement/totalement superposés. En appliquant notre méthode à un oscillateur optoélectronique,nous avons atteint des débits théoriques de plusieurs Gbit/s par utilisateur tout en préservant un faible niveau de complexité algorithmique pour le décryptage.

A.6 Conclusion Générale

Notre travail de thèse a concentré son effort sur deux problèmes ouverts des communications chaotiques optiques : le premier concerne la quantification de la sécurité des crypto-systèmes chaotiques optiques et le second la possibilité de multiplexer et transmettre simultanément plusieurs messages avec un haut niveau de sécurité.

Analyse de Sécurité

La sécurité de l'ECSL a été évaluée en terme d'identification du délai. L'utilisation de systèmes à delais est une approche simple pour générer du chaos de haute dimension,

ce qui permet d'éviter un cassage du crypto-système par des méthodes de faible complexité. Le maintien de ce niveau de sécurité algorithmique dépend fortement de la méconnaissance du délai par l'espion. Avec des systèmes tels que les ECSLs, le délai est identifié à partir de la série temporelle de l'intensité optique en utilisant des estimateurs tels que la fonction d'autocovariance (ACF), l'information mutuelle retardée (DMI) ou encore les modèles non-linéaires globaux.

Nous avons ainsi révélé le rôle clé des paramètres opérationnels de l'ECSL sur la dissimulation de la signature du délai : la force de rétroaction (η), le courant de pompe (J) et le choix du délai (τ, TD) vis-à-vis de la période des oscillations de relaxation (τ_{RO}, ROP). Nous avons identifié que les situations conduisant à une identification difficile du délai (signature TD invisible ou fortement perturbée) apparaissent pour une combinaison de force de rétroaction et courant de pompe faibles et pour des valeurs proches des échelles de temps TD et ROP. L'impossibilité de détecter la signature du délai dans ces conditions s'est montrée robuste vis-à-vis de toutes les méthodes d'estimation connues : les statistiques d'extrema, les modèles linéaires locaux et non-linéaires globaux (réseaux de neurones). Enfin, nous avons connecté l'origine des scénarios d'identification du délai d'un ECSL aux échelles de temps apparaissant dans la cascade de bifurcations, qui précédent le régime chaotique. Nos résultats sont d'importance pour la conception d'un émetteur chaotique à base d'ECSLs de haute sécurité pour des applications de cryptographie par chaos optique.

Multiplexage de Chaos et Communications Multi-Utilisateurs

La seconde partie de notre étude s'est attachée à étudier plusieurs configurations et méthodes d'encryptage innovantes afin d'accroître l'efficacité spectrale des crypto-systèmes par chaos optique. Nous avons concentré notre attention sur les propriétés fondamentales de la synchronisation du chaos entre plusieurs lasers à semi-conducteur et sur les questions de multiplexage/démultiplexage de plusieurs messages digitaux.

Nous avons commencé par étudier la possibilité de multiplexer plusieurs champs optiques chaotiques générés par des lasers à semi-conducteur émettant par le côté (*edge-emitting semiconductor lasers* ou EEL). A l'émission, plusieurs EELs "maîtres" sont globalement mutuellement couplés via une cavité externe partagée. Les champs optiques de tous les EELs forment ainsi un unique champs optique multiplexé injectant chaque laser maître (M_k, $k = 1, \ldots, n$) avec une force de couplage et un délai spécifique. Celui-ci est ensuite injecté unidirectionnellement dans des EELs esclaves découplés (S_k). Notre architecture est une généralisation du problème de synchronisation d'une seule paire d'ECSL et peut être interprétée, dans une certaine mesure, comme une décomposition active-passive (APD). Ainsi, nous avons démontré que sous des conditions adéquates de couplage, que chaque paire de lasers pouvait présenter de la synchronisation anticipative complète avec des délais spécifiques. Nous avons également addressé la question du multiplexage d'information en adaptant les techniques d'encryptage du *chaos shift keying* (CSK), et *chaos modulation* (CMo) au contexte multi-utilisateurs. L'encryptage pour une méthode de CSK multiplexée consiste en une modulation du courant de pompe de chaque laser. Le décryptage est rendu possible par la synchronisation du chaos pour chaque paire de

lasers lorsque les courants de pompe ont des valeurs identiques. Différentes stratégies de décryptage ont été proposées avec des complexités algorithmiques respectivement exponentielles et linéaires. Les débits atteints (en simulations numériques) sont de l'ordre de plusieurs centaines de Mbits/s par utilisateur et sont limités par le temps de resynchronisation lorsque le courant de pompe est modulé.
Afin de palier à ce problème de débit, une méthode de CMo multiplexée a également été proposée. Chaque utilisateur encrypte son information sur l'amplitude ou la phase du champ optique de son laser M_k. L'emploi de cette méthode requiert cependant l'utilisation d'une circulation optique modifiant légèrement la structure initialement proposée. L'avantage majeur de cette méthode en comparaison du CSK est la participation du message à la dynamique du système, ainsi qu'à l'abscence de pertes de synchronisation entre les lasers maîtres et esclaves d'une même paire. Cela permet de lever en partie les limitations en terme de débit. En utilisant un décryptage de complexité exponentielle ou linéaire, nous avons vérifié numériquement qu'il était possible d'encrypter et décrypter deux messages à 1 Gbit/s. Nous avons par la suite proposé d'aller au-delà des méthodes d'encryptage typiques utilisées en cryptographie par chaos (CMa, CSK et CMo). Notre objectif consistait à transposer une technique de multiplexage par code (*code-division multiple access* ou CDMA) au cadre de la cryptographie par chaos en utilisant des oscillateurs électro-optiques. Le CDMA utilise des séquences pseudo-aléatoires binaires fixes (appelées *codes*) et orthogonales (vis-à-vis d'un produit scalaire), afin d'étaler spectralement les différents messages et de réaliser une superposition spectrale autorisant une séparation de chaque message à la réception par corrélation. L'utilisation de signaux chaotiques (variant pour chaque bit transmis) comme codes requiert une orthogonalité (ou décorrelation) à tout instant. Cette contrainte a été satisfaite lorsque les signaux des sorties des boucles de rétraoactions d'un oscillateur électro-optique (OEO) sont utilisés comme codes chaotiques. Chaque boucle de rétroaction contient un modulateur de Mach-Zehnder associé à une non-linéarité en cosinus carré avec une pulsation spécifique. Les différents codes modulent indépendamment chaque messages avant d'être recombinés en un unique signal multiplexé agissant sur la dynamique des OEOs à l'émission et à la réception. Cela assure une synchronisation complète du chaos. Nous avons également analysés l'influence des différents paramètres des codes sur l'orthogonalité et démontré le rôle clé du décalage en pulsation ($\Delta\omega_{ij}$) des fonctions non-linéaires et de leur gain (β_j). Nous avons proposé plusieurs stratégies de décryptage et simuler des transmission à très haut débit dans le contexte multi-utilisateurs.

Enfin et pour conclure, nous nous sommes intéressés à une architecture combinant les deux directions empruntées dans ce manuscrit de thèse. Elle consiste en un oscillateur non-linéaire avec de multiples boucles de rétroactions, dont les délais sont modulés digitalement sur M niveaux (en rapport aux messages $M-$aires) par l'utilisateur légitime Alice$_i$ ($i = 1, \ldots, n$). Chaque délai varie discrètement dans un intervalle d'encryptage Δ_i pouvant être disjoints ou superposés. Ils sont porteurs de des informations encodées par les utilisateurs et affectent les non-linéarités des boucles de rétroaction utilisées comme signaux pour la transmission d'un message. Les signaux de chaque boucle sont ensuite recombinés en un unique signal multiplexé qui gouverne les dynamiques de l'émetteur et du récepteur afin de les synchroniser

chaotiquement (dans de bonnes conditions de couplage). Les stratégies de décryptage reposent sur les calculs de métriques (intercorrélation ou norme euclidienne) entre le signal multiplexé et différents signaux candidats (même non-linéarités que celles utilisées à l'émission par les Alice$_i$ mais avec des valeurs de délais candidats). Les valeurs des différents délais utilisés à l'émission peuvent ainsi être estimées conjointement (calculs exponentiellement complexes) ou indépendamment (calculs de complexité linéaire) en détectant un extremum (maximum ou minimum) dans les métriques. Des simulations ont été réalisées avec un modèle d'OEO en démontrant la possibilité d'une transmission d'information simultanée de quatre messages à 5 Gbits/s par utilisateur. La sécurité de la méthode proposée a été évaluée vis-à-vis de l'estimation du délai par information mutuelle retardée. Un haut niveau de sécurité, signatures des délais totalement invisibles, a été observé. Cette méthode associant l'aléa des sources d'information à l'hyperchaoticité des systèmes à délais offre des perspectives inédites en terme de débit, d'efficacité spectrale et d'amélioration de la sécurité pour de futures architectures de communications multi-utilisateurs par chaos.

Bibliography

[1] D. Stinson, *Cryptography: Theory and Practice*. Chapman & Hall/CRC, third ed., 2003.

[2] T.M. Cover and J.A. Thomas, *Elements of Information Theory*. Wiley-Interscience, 2006.

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[4] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi-Lodi, P. Colet, I. Fischer, J. García-Ojalvo, C.R. Mirasso, L. Pesquera, and K.A. Shore, "Chaos-based communications at high bit rates using commercial fibre-optic links," *Nature*, vol. 438, pp. 343–346, 2005.

[5] R.N. Hall, G.E. Fenner, J.O. Kingsley, T.J. Soltys, and R.O. Carlson, "Coherent light emission from GaAs junctions," *Phys. Rev. Lett.*, vol. 9, pp. 366–369, 1962.

[6] E.N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, pp. 130–141, 1963.

[7] L.M. Pecora and T.L. Carroll, "Synchronization in chaotic systems," *Phys. Rev. Lett.*, vol. 64, pp. 821–824, 1990.

[8] G.D. Van Wiggeren and R. Roy, "Communication with chaotic lasers," *Science*, vol. 279, pp. 1198–1200, 1998.

[9] L.E. Larson, J.-M. Liu, and L.S. Tsimring, *Digital Communications Using Chaos and Nonlinear Dynamics*. Springer, 2006.

[10] T. Yang, L.B. Yang, and C.M. Yang, "Breaking chaotic secure communications using a spectrogram," *Phys. Lett. A*, vol. 247, pp. 105–111, 1998.

[11] C.R. Mirasso, P. Colet, and P. Garcia-Fernandez, "Synchronization of chaotic semiconductor lasers: Application to encoded communications," *IEEE Photonic Technol. Lett.*, vol. 8, pp. 299–301, 1996.

[12] J.-P. Goedgebuer, L. Larger, and H. Porte, "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," *Phys. Rev. Lett.*, vol. 80, pp. 2249–2252, 1998.

[13] S. Li and D.J. Costello Jr., *Error Control Coding*. Prentice Hall, 2nd ed., 2004.

[14] A. Argyris, E. Grivas, M. Hamacher, A. Bogris, and D. Syvridis, "Chaos on-a-chip secures data transmission in optical fiber links," *Opt. Exp.*, vol. 18, pp. 5188–5198, 2010.

[15] G. Agrawal, *Fiber-Optic Communication Systems*. John Wiley and Sons, 2002.

[16] W.M. Tam, F.C.M. Lau, and C.K. Tse, *Communications with Chaos: Multiple Access Techniques and Performance*. Elsevier, 2006.

[17] L.S. Tsimring and M.M. Sushchik, "Multiplexing chaotic signals using synchronization," *Phys. Lett. A*, vol. 213, pp. 155–166, 1996.

[18] Y. Liu and P. Davis, "Dual synchronization of chaos," *Phys. Rev. E*, vol. 61, pp. R2176–R2179, 2000.

[19] K. Yoshimura, "Multichannel digital communications by the synchronization of globally coupled chaotic systems," *Phys. Rev. E*, vol. 60, pp. 1648–1657, 1999.

[20] S. Sundar and A.A. Minai, "Synchronization of randomly multiplexed chaotic systems with application to communication," *Phys. Rev. Lett.*, vol. 85, pp. 5456–5459, 2000.

[21] J.G. Proakis, *Digital Communications*. McGraw Hill, 2000.

[22] J. Gleick, *Chaos: Making a New Science*. Heinemann, 1987.

[23] M. Sciamanna, *Nonlinear dynamics and polarization properties of externally driven semiconductor lasers*. PhD in Applied Physics, Faculté Polytechnique de Mons, 2004.

[24] M.W. Lee, *Etudes de Comportements Chaotiques en Modulation de Cohérence et Application à la cryptographie*. PhD in Engineering Sciences, Université de Franche-Comté, 2002.

[25] G.P. William, *Chaos Theory Tammed*. Taylor & Francis, 1997.

[26] Aristotle, "On the heavens," in *The Complete Works of Aristotle: The Revised Oxford Translation* (J. Barnes, ed.), vol. 1, Princeton University Press, 1985.

[27] D. Ruelle and F. Takens, "On the nature of turbulence," *Commun. Math. Phys.*, vol. 20, pp. 167–192, 1971.

[28] M. Feigenbaum, "Quantitative universality for a class of nonlinear transformation," *J. Stat. Phys.*, vol. 19, pp. 25–52, 1978.

[29] R. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, pp. 459–467, 1976.

[30] M.C. Mackey and L. Glass, "Oscillations and chaos in physiological control systems," *Science*, vol. 197, pp. 287–289, 1977.

[31] R.M. Murray, Z. Li, and S. Shankar Sastry, *A mathematical introduction to Robotic Manipulation*. CRC Press, 1994.

[32] S. Shankar Sastry, *Nonlinear systems: Analysis, Stability, and Control*. Springer, 1999.

[33] J.D. Farmer, "Chaotic attractors of an infinite-dimensional dynamical system," *Physica D*, vol. 4, pp. 366–393, 1982.

[34] B.B. Mandelbrot, *The Fractal Geometry of Nature*. W.H. Freeman and Company, 1982.

[35] J.D. Crawford, "Introduction to bifurcation theory," *Rev. Mod. Phys.*, vol. 63, pp. 991–1037, 1991.

[36] S. Wiggins, *Introduction to Applied Nonlinear Dynamical Systems and Chaos.* Springer, 1990.

[37] J. Guckenheimer and P. Holmes, *Nonlinear Oscillations, Dynamical Systems and Bifurcations of Vector Fields*. Springer, 2002.

[38] J.-P. Eckmann, "Roads to turbulence in dissipative dynamical systems," *Rev. Mod. Phys.*, vol. 53, pp. 643–654, 1981.

[39] C. Jeffries and J. Perez, "Observation of a pomeau-manneville intermittent route to chaos in a nonlinear oscillator," *Phys. Rev. A*, vol. 26, pp. 2117–2122, 1982.

[40] D.T. Kaplan and J. Yorke, *In functional differential equations and approximation of fixed points*. Springer, 1979.

[41] J.-P. Eckmann and D. Ruelle, "Ergodic theory of chaos and strange attractors," *Rev. Mod. Phys.*, vol. 57, pp. 617–656, 1985.

[42] J. Pesin, "Characteristic lyapunov exponents and smooth ergodic theory," *Russ. Math Surveys*, vol. 32, pp. 55–114, 1977.

[43] A. Pikovsky, M. Rosenblum, and J. Kurths, *Synhronization: a Universal Concept of Nonlinear Sciences*. Cambridge University Press, 2003.

[44] C. Huyghens, "Horologium oscillatorium," 1673.

[45] M. Bennett, M.F. Schatz, H. Rockwood, and K. Wiesenfeld, "Huygens' clocks," *Proc. Roy. Soc. London A*, vol. 458, pp. 563–579, 2002.

[46] J. Rayleigh, *The Theory of Sound*. Dover, 1945.

[47] E. V. Appleton, "The automatic synchronization of triode oscillator," *Proc. Cambridge Phil. Soc. (Math. and Phys. Sci.)*, vol. 21, pp. 231–248, 1922.

[48] B. van der Pol, "A theory of the amplitude of free and forced triode," *Vibration. Radio Rev.*, vol. 1, pp. 701–710, 754–762, 1920.

[49] R. Adler, "A study of locking phenomena in oscillators," *Proc. IRE*, vol. 34, pp. 351–357, 1946.

[50] J. Buck and E. Buck, "Mechanism of rythmic synchronous flashing of fireflies," *Science*, vol. 159, p. 1319, 1968.

[51] T.J. Walker, "Accoustic synchrony: Two mechanisms in the snowy tree cricket," *Science*, vol. 166, p. 891, 1969.

[52] T. Danino, O. Mondragoó-Palomino, L.S. Tsimring, and J. Hasty, "A synchronized quorum of genetic clocks," *Nature*, vol. 463, pp. 326–330, 2010.

[53] V. Arnold, "Cardiac arrhythmias and circle mappings," *Chaos*, vol. 1, pp. 20–24, 1991.

[54] H. Fujisaka and T. Yamada, "Stability theory of synchronized motion in coupled-oscillator systems," *Prog. Theor. Phys*, vol. 69, pp. 32–47, 1983.

[55] H. Fujisaka and T. Yamada, "Stability theory of synchronized motion in coupled-oscillator systems 2. the mapping approach," *Prog. Theor. Phys*, vol. 70, pp. 1240–1248, 1983.

[56] H. Fujisaka and T. Yamada, "Stability theory of synchronized motion in coupled-oscillator systems 3. mapping model for continuous systems," *Prog. Theor. Phys*, vol. 72, pp. 885–894, 1984.

[57] S. Boccaletti, L. M. Pecora, and A. Pelaez, "Unifying framework for synchronization of coupled dynamical systems," *Phys. Rev. E*, vol. 63, p. 066219, 2001.

[58] N.F. Rulkov, M.M. Sushchik, L.S. Tsimring, and H.D.I. Abarbanel, "Generalized synchronization of chaos in directionally coupled chaotic systems," *Phys. Rev. E*, vol. 51, pp. 980–994, 1995.

[59] H.U. Voss, "Anticipating chaotic synchronization," *Phys. Rev. E*, vol. 61, pp. 5115–5119, 2000.

[60] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares, and C.S. Zhou, "The synchronization of chaotic systems," *Phys. Rep.*, vol. 366, pp. 1–101, 2002.

[61] I. Fischer, Y. Liu, and P. Davis, "Synchronization of chaotic semiconductor laser dynamics on subnanosecond time scales and its potential for chaos communication," *Phys. Rev. A*, vol. 62, p. R011801, 2000.

[62] K.M. Cuomo and A.V. Oppenheim, "Circuit implementation of synchronized chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, pp. 65–68, 1993.

[63] K.M. Cuomo, A.V. Oppenheim, and S.H. Strogatz, "Synchronization of lorenz-based chaotic circuits with applications to communications," *IEEE T. Circuits Syst.*, vol. 40, pp. 626–633, 1993.

[64] O. Morgül and M. Feki, "A chaotic masking scheme by using synchronized chaotic systems," *Phys. Lett. A*, vol. 251, pp. 169–176, 1999.

[65] A. Jacobo, M.C. Soriano, I. Fischer, C.R. Mirasso, and P. Colet, "Chaos-based optical communications: Encryption Vs. nonlinear filtering," *IEEE J. Quantum Electron.*, vol. 46, pp. 499–505, 2010.

[66] H. Dedieu, M.P. Kennedy, and M. Hasler, "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE T. Circuits Syst.*, vol. 40, pp. 634–642, 1993.

[67] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurcat. Chaos*, vol. 2, pp. 973–977, 1993.

[68] C.W. Wu and L.O. Chua, "A simple way to synchronize chaotic systems with applications to secure communication systems," *Int. J. Bifurcat. Chaos*, vol. 3, pp. 1619–1627, 1993.

[69] K.S. Halle, C.W. Wu, M. Itoh, and L.O. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurcat. Chaos*, vol. 3, pp. 469–477, 1993.

[70] L. Kocarev and U. Parlitz, "General approach for chaotic synchronization with applications to communication," *Phys. Rev. Lett.*, vol. 74, pp. 5028–5031, 1995.

[71] A. Einstein, "Zur quantentheorie der strahlung," *Physicalische Zeitschrift*, vol. 18, pp. 121–128, 1917.

[72] G.P. Agrawal and N.K. Dutta, *Semiconductor Lasers, 2nd Ed.* Kluwer Academic, 1993.

[73] J. Ohtsubo, *Semiconductor Lasers: Stability, Instability and Chaos, 2nd Ed.* Springer, Series in Optical Sciences, 2007.

[74] I. Gatare, *Polarization Switching, Locking and Synchronization in VCSELs with Optical Injection.* PhD in physics, Université Paul Verlaine Metz (UPV-M) and Vrje Universiteit Brussel, 2008.

[75] H. Haken, "Analogy between higher instabilities in fluids and lasers," *Phys. Lett. A*, vol. 53, pp. 77–78, 1975.

[76] C.O. Weiss, A. Godone, and A. Olafsson, "Routes to chaotic emission in a cw he-ne laser," *Phys. Rev. A*, vol. 28, pp. 892–895, 1983.

[77] F.T. Arecchi, G.L. Lippi, G.P. Puccioni, and J.R. Tredicce, "Deterministic chaos in lasers with injected signal," *Opt. Comm.*, vol. 51, pp. 308–314, 1984.

[78] J.R. Tredicce, F.T. Arecchi, G.L. Lippi, and G.P. Puccioni, "Instabilities in lasers with an injected signal," *J. Opt. Soc. Am. B*, vol. 2, pp. 173–183, 1985.

[79] C.O. Weiss, W. Klische, P.S. Ering, and M. Cooper, "Instabilities and chaos of a single mode nh3 ring laser," *Opt. Commun.*, vol. 44, pp. 405–408, 1985.

[80] W.W. Chow and S.W. Koch, *Semiconductor-Laser Fundamentals: Physics of the Gain Materials*. Springer, 1999.

[81] J.-M. Liu, *Photonic Devices*. Cambridge University Press, 2005.

[82] J. Yao, G.P. Agrawal, P. Gallion, and C.M. Bowden, "Semiconductor laser dynamics beyond the rate-equation approximation," *Opt. Commun*, vol. 119, p. 246, 1995.

[83] G.H.M. van Tartwijk and G.P. Agrawal, "Laser instabilities: a modern perspective," *Prog. Quant. Electron.*, vol. 22, pp. 43–122, 1998.

[84] C.H. Henry, "Theory of the linewidth of semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 18, pp. 259–264, 1982.

[85] M. Osinski and J. Buss, "Linewidth broadening factor in semiconductor lasers - an overview," *IEEE J. Quantum Electron.*, vol. 23, pp. 9–29, 1987.

[86] C.H. Lee, T.H. Yoon, and S.Y. Shin, "Period doubling and chaos in a directly modulated laser diode," *Appl. Phys. Lett.*, vol. 46, pp. 95–97, 1985.

[87] Y.C. Chen, H.G. Winful, and J.-M. Liu, "Subharmonic bifurcations and irregular pulsing behavior of modulated semiconductor lasers," *Appl. Phys. Lett.*, vol. 47, pp. 208–210, 1985.

[88] T.B. Simpson, J.-M. Liu, A. Gravielides, V. Kovanis, and P.M. Alsing, "Period-doubling route to chaos in a semiconductor laser subject to optical injection," *Appl. Phys. Lett.*, vol. 64, pp. 3539–3541, 1994.

[89] T.B. Simpson, J.-M. Liu, A. Gravielides, V. Kovanis, and P.M. Alsing, "Period-doubling cascade and chaos in a semiconductor laser with optical injection," *Phys. Rev. A*, vol. 51, pp. 4181–4187, 1995.

[90] B. Krauskopf, S. Wieczorek, and D. Lenstra, "Different types of chaos in an optically injected semiconductor laser," *Appl. Phys. Lett.*, vol. 77, pp. 1611–1613, 2000.

[91] F.Y. Lin and J.-M. Liu, "Nonlinear dynamical characteristics of an optically injected semiconductor laser subject to optoelectronic feedback," *Opt. Commun.*, vol. 221, pp. 173–180, 2003.

[92] S. Tang and J.-M. Liu, "Chaotic pulsing and quasi-periodic route to chaos in a semiconductor laser with delayed opto-electronic feedback," *IEEE J. Quantum Electron.*, vol. 37, pp. 329–336, 2001.

[93] T. Heil, I. Fischer, W. Elsässer, and A. Gavrielides, "Dynamics of semiconductor lasers subject to delayed optical feedback: The short cavity regime," *Phys. Rev. Lett.*, vol. 87, p. 243901, 2001.

[94] R. Lang and K. Kobayashi, "External optical feedback effects on a semiconductor injection laser properties," *IEEE J. Quantum Electron.*, vol. 16, pp. 347–355, 1980.

[95] I. Fischer, G.H.M van Tartwijk, A.M. Levine, W. Elsässer, E.O. Gobel, and D. Lenstra, "Fast pulsing and chaotic itinerancy with a drift in the coherence collapse of semiconductor lasers," *Phys. Rev. Lett.*, vol. 76, pp. 220–223, 1996.

[96] D. Lenstra, B.H. Verbeek, and J. den Boef, "Coherence collapse in single-mode semiconductor lasers due to optical feedback," *IEEE J. Quantum Electron.*, vol. 21, pp. 674–679, 1985.

[97] R.W. Tkach and A.R. Chraplyvy, "Regimes of feedback effects in 1.5 μm distributed feedback lasers," *J. Lightwave Technol.*, vol. 4, pp. 1655–1661, 1986.

[98] D.M. Kane and K.A. Shore, *Unlocking Dynamical Diversity.* John Wiley *&* Sons, 2005.

[99] J. Mørk, B. Tromborg, and J. Mark, "Chaos in semiconductor lasers with optical feedback: Theory and experiment," *IEEE J. Quantum Electron.*, vol. 28, pp. 93–108, 1992.

[100] A. Hohl and A. Gavrielides, "Bifurcation cascade in a semiconductor laser subject to optical feedback," *Phys. Rev. Lett.*, vol. 82, pp. 1148–1151, 1999.

[101] R. Vicente, J. Dauden, P. Colet, and R. Toral, "Analysis and characterization of the hyperchaos generated by a semiconductor laser subject to a delayed feedback loop," *IEEE J. Quantum Electron.*, vol. 41, pp. 541–548, 2005.

[102] J.-P. Goedgebuer, L. Larger, H. Porte, and F. Delorme, "Chaos in wavelength with a feedback tunable laser diode," *Phys. Rev. E*, vol. 57, pp. 2795–2798, 1998.

[103] L. Larger, J.-P. Goedgebuer, and J.-M. Merolla, "Chaotic oscillator in wavelength: a new setup for investigating differential difference equations describing nonlinear dynamics," *IEEE J. Quantum Electron.*, vol. 34, pp. 594–601, 1998.

[104] R. Boyd, *Nonlinear Optics.* John Wiley and Sons, 3rd ed., 2002.

[105] K. Ikeda and K. Matsumoto, "High-dimensional chaotic behavior in systems with time-delayed feedback," *Physica D*, vol. 29, pp. 223–235, 1987.

[106] J.-P. Goedgebuer, P. Levy, L. Larger, C.C. Chen, and W.T. Rhodes, "Optical communication with synchronized hyperchaos generated electro-optically," *IEEE J. Quantum Electron.*, vol. 38, pp. 1178–1183, 2002.

[107] Y. Chembo Kouomou, P. Colet, L. Larger, and N. Gastaud, "Chaotic breathers in delayed electro-optical systems," *Phys. Rev. Lett.*, vol. 95, p. 203903, 2005.

[108] E. Genin, L. Larger, J.-P. Goedgebuer, M.W. Lee, R. Ferriere, and X. Bavard, "Chaotic oscillations of the optical phase for multigigahertz-bandwidth secure communications," *IEEE J. Quantum Electron.*, vol. 40, pp. 294–298, 2004.

[109] R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. Udaltsov, and J. Dudley, "Electro-optic delay oscillator with nonlocal nonlinearity: Optical phase dynamics, chaos, and synchronization," *Phys. Rev. E*, vol. 80, p. 026207, 2009.

[110] N. Gastaud, S. Poinsot, L. Larger, J.-M. Merolla, M. Hanna, J.-P. Goedgebuer, and E. Malassenet, "Electro-optical chaos for multi-10 gbit/s optical transmissions," *Electron. Lett.*, vol. 40, pp. 898–899, 2004.

[111] H.G. Winful and L. Rahman, "Synchronized chaos and spationtemporal chaos in arrays of coupled lasers," *Phys. Rev. Lett.*, vol. 65, pp. 1575–1578, 1990.

[112] R. Roy and K.S. Thornburg, "Experimental synchronization of chaotic lasers," *Phys. Rev. Lett.*, vol. 72, pp. 2009–2012, 1994.

[113] P. Colet and R. Roy, "Digital communications with synchronized chaotic lasers," *Opt. Lett.*, vol. 19, pp. 2056–2058, 1994.

[114] G.D. Van Wiggeren and R. Roy, "Optical communication with chaotic waveforms," *Phys. Rev. Lett.*, vol. 81, pp. 3547–3550, 1998.

[115] G.D. Van Wiggeren and R. Roy, "Chaotic communication using time-delayed optical systems," *Int. J. Bif. Chaos*, vol. 9, pp. 2129–2156, 1999.

[116] L. Larger, J.-P. Goedgebuer, and F. Delorme, "Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator," *Phys. Rev. E*, vol. 57, pp. 6618–6624, 1998.

[117] J.-M. Liu, H.F. Chen, and S. Tang, "Synchronized chaotic optical communications at high bit rates," *IEEE J. Quantum Electron.*, vol. 38, pp. 1184–1196, 2002.

[118] S. Tang, H.F. Chen, S.K. Hwang, and J.-M. Liu, "Message encoding and decoding through chaos modulation in chaotic optical communications," *IEEE T. Circuits-I*, vol. 49, pp. 163–169, 2002.

[119] S. Tang and J.-M. Liu, "Message encoding-decoding at 2.5 Gbits/s through synchronization of chaotic pulsing semiconductor lasers," *Opt. Lett*, vol. 26, pp. 1843–1845, 2001.

[120] A. Locquet, "Chaos-based secure optical communications using semiconductor lasers," in *Handbook of Information and Communication Security* (M. Stamp and P. Stavroulakis, eds.), ch. 10, pp. 451–478, Springer, 2010.

[121] C. Masoller, "Anticipation in the synchronization of chaotic semiconductor lasers with optical feedback," *Phys. Rev. Lett.*, vol. 86, pp. 2782–2785, 2001.

[122] A. Locquet, F. Rogister, M. Sciamanna, P. Megret, and M. Blondel, "Two types of synchronization in unidirectionally coupled chaotic external-cavity semiconductor lasers," *Phys. Rev. E*, vol. 64, p. 045203(R), 2001.

[123] A. Locquet, C. Masoller, and C.R. Mirasso, "Synchronization regimes of optical-feedback-induced chaos in unidirectionally coupled semiconductor lasers," *Phys. Rev. E*, vol. 65, p. 056205, 2002.

[124] M. Murakami and J. Ohtsubo, "Synchronization of feedback-iunduced chaos in semiconductor lasers by optical injection," *Phys. Rev. A*, vol. 65, p. 033826, 2002.

[125] C.R. Mirasso, J. Mulet, and C. Masoller, "Chaos shift-keying encryption in chaotic external-cavity semiconductor lasers using a single-receiver scheme," *IEEE Photonic Technol. Lett.*, vol. 14, pp. 456–458, 2002.

[126] J.-M. Liu, H.F. Chen, and S. Tang, "Optical-communication systems based on chaos in semiconductor lasers," *IEEE T. Circuits-I*, vol. 48, pp. 1475–1483, 2001.

[127] S. Tang and J.-M. Liu, "Chaos synchronization in semiconductor lasers with optoelectronic feedback," *IEEE J. Quantum Electron.*, vol. 39, pp. 708–715, 2003.

[128] S. Tang and J.-M. Liu, "Experimental verification of anticipated and retarded synchronization in chaotic semiconductor lasers," *Phys. Rev. Lett.*, vol. 90, p. 194101, 2003.

[129] V.S. Udaltsov, J.-P. Goedgebuer, L. Larger, and W. T. Rhodes, "Communicating with optical hyperchaos: Information encryption and decryption in delayed nonlinear feedback systems," *Phys. Rev. Lett.*, vol. 86, pp. 1892–1895, 2001.

[130] K. Pyragas, "Synchronization of coupled time-delay systems: Analytical estimations," *Phys. Rev. E*, vol. 58, pp. 3067–3071, 1998.

[131] G.S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," *Journal of the IEEE*, vol. 55, pp. 109–115, 1926.

[132] T. Yang, L.B. Yang, and C.M. Yang, "Cryptanalyzing chaotic secure communications using return maps," *Phys. Lett. A*, vol. 245, pp. 495–510, 1998.

[133] G. Pérez and H.A. Cerdeira, "Extracting messages masked by chaos," *Phys. Rev. Lett.*, vol. 74, pp. 1970–1973, 1995.

[134] F. Takens, *Detecting Strange Attractors in Turbulence*, vol. 898 of *Lecture Notes in Mathematics*. Springer, 1981.

[135] F. Takens and M.M. Sushchik, "Detecting nonlinearities in stationary time series," *Int. J. Bifurcation Chaos*, vol. 3, pp. 241–256, 1993.

[136] H. Kantz and T. Schreiber, *Nonlinear Time-Series Analysis*. Cambridge University Press, 1997.

[137] K.M. Short, "Unmasking a modulated chaotic communications scheme," *Int. J. Bifurc. Chaos*, vol. 6, pp. 367–375, 1996.

[138] K.M. Short and A.T. Parker, "Unmasking a hyperchaotic communication scheme," *Phys. Rev. E*, vol. 58, pp. 1159–1162, 1998.

[139] H.S. Greenside, A. Wolf, J. Swift, and T. Pignataro, "Impracticality of a box-counting algorithm for calculating the dimensionality of strange attractors," *Phys. Rev. A*, vol. 25, pp. 3453–3456, 1982.

[140] H. Kantz, A. Wolf, J. Swift, and T. Pignataro, "Scalar observations from a class of high-dimensional chaotic systems: Limitations of the time delay embedding," *Chaos*, vol. 7, pp. 423–429, 1997.

[141] B. Dorizzi, B. Grammaticos, M. Le Berre, Y. Pomeau, E. Ressayre, and A. Tallet, "Statistics and dimension of chaos in differential delay systems," *Phys. Rev. A*, vol. 35, pp. 328–339, 1987.

[142] R. Hegger, M.J. Bünner, H. Kantz, and A. Giaquinta, "Identifying and modeling delay feedback systems," *Phys. Rev. Lett.*, vol. 81, pp. 558–561, 1998.

[143] V.S. Udaltsov, J.-P. Goedgebuer, L. Larger, J.-B. Cuenot, P. Levy, and W. T. Rhodes, "Cracking chaos-based encryption systems ruled by nonlinear delay-differential equations," *Phys. Lett. A*, vol. 308, pp. 54–60, 2003.

[144] V.S. Udaltsov, L. Larger, J.-P. Goedgebuer, A. Locquet, and D.S. Citrin, "Time-delay identification in chaos-based cryptosystems ruled by delay-differential equation," *J. Opt. Technol.*, vol. 72, pp. 373–377, 2005.

[145] M.D. Prokhorov, V.I. Ponomarenko, A.S. Karavaev, and B.P. Bezruchko, "Reconstruction of time-delayed feedback systems from time series," *Physica D*, vol. 203, pp. 209–223, 2005.

[146] C. Robilliard, E. H. Huntington, and J. G. Webb, "Enhancing the security of delayed differential chaotic systems with programmable feedback," *IEEE T. Circuits-II*, vol. 53, pp. 722–725, 2006.

[147] W.-H. Kye, M. Choi, S. Rim, M.S. Kurdoglyan, C.-M. Kim, and Y.-J. Park, "Characteristics of a delayed system with time-dependent delay time," *Phys. Rev. E*, vol. 69, p. 055202(R), 2004.

[148] C. Risch and V. Voumard, "Self pulsation in the output intensity and spectrum of GaAs-AlGaAs cw diode lasers coupled to a frequency selective external optical feedback," *J. Appl. Phys.*, vol. 48, pp. 2083–2085, 1977.

[149] M.J Bünner, A. Kittel, J. Parisi, I. Fischer, and W. Elsässer, "Estimation of delay times from a delayed optical feedback laser experiment," *Europhys. Lett.*, vol. 42, pp. 353–358, 1998.

[150] M.W. Lee, P. Rees, K.A. Shore, S. Ortin, L. Pesquera, and A. Valle, "Dynamical characterisation of laser diode subject to double optical feedback for chaotic optical communications," *IEE Proc. Optoelectron.*, vol. 152, pp. 97–102, 2005.

[151] M.J Bünner, M. Popp, T. Meyer, A. Kittel, and J. Parisi, "Recovery of scalar time-delay systems from time series," *Phys. Lett. A*, vol. 211, pp. 345–349, 1996.

[152] M.J Bünner, T. Meyer, A. Kittel, and J. Parisi, "Recovery of time-evolution equation of time-delay systems from time-series," *Phys. Rev. E*, vol. 56, pp. 5083–5089, 1997.

[153] S. Ortin, J.M. Gutierrez, L. Pesquera, and H. Vasquez, "Nonlinear dynamics extraction for time-delay systems using modular neural networks synchronization and prediction," *Physica A*, vol. 351, pp. 133–141, 2005.

[154] C. Masoller, "Effect of the external cavity length in the dynamics of a semiconductor laser with optical feedback," *Opt. Commun.*, vol. 128, pp. 363–376, 1996.

[155] A. Murakami and J. Ohtsubo, "Stability analysis of semiconductor laser with phase-conjugate feedback," *IEEE J. Quantum Electron.*, vol. 33, pp. 1825–1831, 1997.

[156] A. Murakami and J. Ohtsubo, "Dynamics and linear stability analysis in semiconductor lasers with phase-conjugate feedback," *IEEE J. Quantum Electron.*, vol. 34, pp. 1979–1986, 1998.

[157] C. Masoller, "Comparison of the effects of nonlinear gain and weak optical feedback on the dynamics of semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 33, pp. 804–814, 1997.

[158] A. Uchida, S. Kinugawa, T. Matsuura, and S. Yoshimori, "Chaotic wavelength division multiplexing for optical communication," *Opt. Lett.*, vol. 29, pp. 2731–2733, 2004.

[159] M.W. Lee and K.A. Shore, "Two-mode chaos synchronisation using a multimode external-cavity laser diode and two single-mode laser diodes," *IEEE J. Lightwave Technol.*, vol. 23, pp. 1608–1673, 2005.

[160] J.K. White and J.V. Moloney, "Multichannel communication using an infinite dimensional spatiotemporal chaotic system," *Phys. Rev. A*, vol. 59, pp. 2422–2426, 1999.

[161] J.M. Buldú, J. García-Ojalvo, and M.C. Torrent, "Multimode synchronization and communication using unidirectionally coupled semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 40, pp. 640–650, 2004.

[162] J.M. Buldú, J. García-Ojalvo, and M.C. Torrent, "Demultiplexing chaos from multimode semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 41, pp. 164–170, 2005.

[163] J.-Z. Zhang, A.-B. Wang, J.-F. Wang, and Y.-C. Wang, "Wavelength division multiplexing of chaotic secure and fiber-optic communications," *Opt. Express*, vol. 17, pp. 6357–6367, 2009.

[164] A. Uchida, S. Kinugawa, T. Matsuura, and S. Yoshimori, "Dual synchronization of chaos in microchip lasers," *Opt. Lett.*, vol. 28, pp. 19–21, 2003.

[165] A. Locquet, C. Masoller, P. Megret, and M. Blondel, "Comparison of two types of synchronization of external-cavity semiconductor lasers," *Opt. Lett.*, vol. 27, pp. 31–33, 2002.

[166] A. Sánchez-Díaz, C.R. Mirasso, P. Colet, and P. García-Fernandez, "Encoded Gbit/s digital communications with synchronized chaotic semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 35, pp. 292–297, 1999.

[167] J. Ohtsubo, "Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback," *IEEE J. Quantum Electron.*, vol. 38, pp. 1141–1154, 2002.

[168] T. Kasami and S. Lin, "Coding for a multiple-access channel," *IEEE T. Inform. Theory*, vol. 22, pp. 129–137, 1976.

[169] V. Annovazzi-Lodi, S. Donati, and A. Sciré, "Synchronization of chaotic lasers by optical feedback for cryptographic applications," *IEEE J Quantum Electron.*, vol. 33, pp. 1449–1454, 1997.

[170] S. Sivaprakasam and K.A. Shore, "Message encoding and decoding using chaotic external-cavity diode lasers," *IEEE J. Quantum Electron.*, vol. 36, pp. 35–39, 2000.

[171] R. Vicente, P. Perez, and C.R. Mirasso, "Open- versus closed-loop performance of synchronized chaotic external-cavity semiconductor lasers.," *IEEE J. Quantum Electron.*, vol. 38, pp. 1197–1204, 2002.

[172] P. Arena, A. Buscarino, L. Fortuna, and M. Frasca, "Separation and synchronization of piecewise linear chaotic systems," *Phys. Rev. E*, vol. 74, p. 026212, 2006.

[173] T. Heil, J. Mulet, I. Fischer, C.R. Mirasso, M. Peil, P. Colet, and W. Elsässer, "On/Off phase shift keying for chaos-encrypted communication using external-cavity semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 38, pp. 1162–1170, 2002.

[174] Y. Chembo Kouomou, P. Colet, N. Gastaud, and L. Larger, "Effect of parameter mismatch on the synchronization of chaotic semiconductor lasers with electro-optical feedback," *Phys. Rev. E*, vol. 69, p. 056226, 2004.

[175] V.I. Ponomarenko and B.P. Bezruchko, "Extracting information masked by the chaotic signal of a time-delay system," *Phys. Rev. E*, vol. 66, p. 026215, 2002.

[176] W.-H. Kye, M. Choi, M.-W. Kim, S.-Y. Lee, S. Rim, C.-M. Kim, and Y.-J. Park, "Synchronization of delayed systems in the presence of delay time modulation," *Phys. Lett. A*, vol. 322, p. 045202(R), 2004.

[177] M.W. Lee, L. Larger, and J.-P. Goedgebuer, "Transmission system using chaotic delays between lightwaves," *IEEE J. Quantum Electron.*, vol. 39, pp. 931–935, 2003.

[178] W.-H. Kye, M. Choi, C.-M. Kim, and Y.-J. Park, "Encryption with synchronized time-delayed systems," *Phys. Rev. E*, vol. 71, p. 045202(R), 2005.

List of Publications

Journal Publications

- D. Rontani, A. Locquet, M. Sciamanna, D.S. Citrin, and A. Uchida. "Generation of Orthogonal Codes Using Chaotic Optical Systems", *Opt. Lett.* **36**, 2287-2289 (2011).

- D. Rontani, A. Locquet, M. Sciamanna, and D.S. Citrin. "Spectrally Efficient Multiplexing of Chaotic Light", *Opt. Lett.* **35**, 2016-2018 (2010).

- D. Rontani, M. Sciamanna, A. Locquet, and D.S. Citrin "Multiplexed Encryption Using Chaotic Systems with Multiple Stochastic-delayed Feedbacks", *Phys. Rev. E* **80**, 066209 (2009).

- D. Rontani, A. Locquet, M. Sciamanna, D.S. Citrin, and S. Ortin, "Time Delay Identification in the Chaotic Output of a Semiconductor Laser with Optical Feedback: a Dynamical Point of View", *IEEE J. Quantum Electron.* **45**, 879-891 (2009).

- D. Rontani, A. Locquet, M. Sciamanna, D.S. Citrin "Loss of Time-Delay Signature in the Chaotic Output of a Semiconductor Laser with Optical Feedback", *Opt. Lett.* **32**, 2960-2962 (2007).

Conference Publications

- D. Rontani, A. Locquet, M. Sciamanna, D.S. Citrin and A. Uchida, "Multiplexed Communications with Chaotic Optoelectronic Devices". To appear in *Technical Digest of NOLTA'11*, Kobe (Japan), 2011.

- D. Rontani, A. Locquet, M. Sciamanna, D.S. Citrin and A. Uchida, "Multiple-Access Optical Chaos-Based Communications Using Optoelectronic Systems". To appear in *Technical Digest of CLEO/QELS'10*, San-Jose (USA), 2010.

- D. Rontani, D.S. Citrin, A. Locquet and M. Sciamanna, "Multiplexed Chaos-Based Communications with Semicondutor Lasers". To appear in: *Dynamics Days South-America*, São-José des Campos (Brazil), 2010.

- D. Rontani, A. Locquet, M. Sciamanna and D.S. Citrin, "Multiplexed Synchronization of Optical Chaos using Coupled External Semiconductor Lasers". To

appear in: *Proceedings of SPIE: Semiconductor Lasers and Laser Dynamics III*, Brussels (Belgium), 2010.

- D. Rontani, A. Locquet, M. Sciamanna, D.S. Citrin and A. Uchida, "Multiplexed Chaos-based Communications Using Stochastic Time-delays", *Dynamics Days US 2010*, Evanston (USA), 2010.

- D. Rontani, A. Locquet, M. Sciamanna, and D.S. Citrin, "Multiplexing Information Using Chaotic Oscillators with Multiple Feedback Loops", *Proceedings of CHAOS'09*, Chania (Greece), 2009.

- D. Rontani, A. Locquet, M. Sciamanna, and D.S. Citrin, "Multiplexing Digital Information Using HyperChaotic Optoelectronic Oscillators with Nonlinear Time-delayed Feedback Loops", *Technical Digest of CLEO'09*, Munich (Germany), 2009.

- D. Rontani, A. Locquet, M. Sciamanna, and D.S. Citrin, "Security Analysis of Chaotic Semiconductor Laser with Optical Feedback", *A Future in Light*, Metz (France), 2009.

- D. Rontani, A. Locquet, M. Sciamanna, and D.S. Citrin, "Masking the Time-delay from the Chaotic Output of a, External-Cavity Semiconductor Laser", *Proceedings of SPIE: Semiconductor Lasers and Laser Dynamics III*, Strasbourg (France), 2008.

- D. Rontani, A. Locquet, M. Sciamanna, and D.S. Citrin, "Identification de la Valeur du Retard d'un Laser à Cavité Externe Chaotique", *Comptes-rendus de la 11ème Rencontres du Non-linéaire*, Paris (France), 2008.

- D. Rontani and H. Siguerdidjane, "Robust Flatness Based Control and Motion Planning of a micro-UAV", *Proceedings of the 17th IFAC Symposium onf Automatic Control in Aerospace*, Toulouse (France), 2007.

Curriculum Vitae

Damien RONTANI was born in Clamart, France, on July 28, 1980. In 2005, he received the M.Sc. degree in electrical and computer engineering both from the Ecole Supérieure d'Electricité (Supélec), Metz, France, and the Georgia Institute of Technology (Georgia Tech), Atlanta, USA. Since Fall 2006, he is working towards the Ph.D. degree jointly at Supélec and Georgia Tech in the framework of the international collaboration: the Unité Mixte Internationale UMI 2958 Georgia Tech - CNRS, located in France.

His research interests include the study of nonlinear dynamics of semiconductor lasers and their application for fast and secure transmissions, nonlinear time-series analysis, time-delay systems, chaos synchronization, communication theory and cryptography, physical layer security, random number generation with physical entropy sources, and the physics of dynamical networks. Damien Rontani is referee for Optics Letters, Optics Express, IEEE Journal of Quantum Electronics, IEEE Photonics Technology Letters, and Optics Communications.

Contact Information

- *Supélec : Ecole Supérieure d'Electricité*
  Department of Optoelectronic and Telecommunication (OPTEL)
  2, Rue Edouard Belin
  57070 Metz, France
  ✉ *e-mail:*damien.rontani@supelec.fr

- *Georgia Tech : Georgia Institute of Technology*
  School of Electrical and Computer Engineering
  777 Atlantic Drive NW Atlanta, GA 30332-0250 USA
  ✉ *e-mail:*damien.rontani@gatech.edu

- *Unité Mixte Internationale UMI 2958 Georgia Tech - CNRS*
  Georgia Tech Lorraine
  2-3 Rue Marconi
  57070 Metz, France
  ✉ *e-mail:*damien.rontani@georgiatech-metz.fr

Education

- **Since 2006:** PhD graduate fellow jointly at Georgia Tech Atlanta, USA, and Supélec Metz, France, in electrical and computer engineering and applied physics.
- **2006:** M.Sc. in information, energy, and systems from Supélec, Gif-sur-Yvette, France.
- **2005:** M.Sc. in electrical and computer engineering from Georgia Tech, Atlanta, USA and Supélec, Gif-sur-Yvette and Metz, France.

Academic and Professional Experience

- **2009-2011: Graduate Research Assistant at Georgia Tech (Atlanta, USA)** Researcher in the School of Electrical and Computer Engineering on secure data multiplexing with chaotic optoelectronics systems. The position included teaching duties at the undergraduate level.
- **2006-2009: Research Fellow at Supélec (Metz, France)** Reasearcher in the Department of Optoelectronic and Telecommunication (OPTEL) on the nonlinear dynamics of photonic components. The position also included teaching duties and laboratory instruction at the undergraduate level.
- **Summer 2006: Research Internship at Supélec (Gif-sur-Yvette, France)** A 4 months internship working on the development of control laws for a nonlinear unmanned aerial vehicle (UAV).
- **Summer and Fall 2004: Industrial Research Internship at SAGEM (Paris, France)** A 6 months internship working on the automatic calibration of infrared (IR) detector using image processing techniques.
- **Spring 2004: Industrial Research Contract with MBDA (Paris, France) and Supélec (Metz, France)** A 4 months contract on the automatic extraction of road from SAR images using quadratic active contours.
- **Summer 2003: Technical Internship at Thales Avionics (London, UK)** A 3 months internship on the design of electronic equipment testing.

Academic and Professional Services

- Secretary of the OSA (Optical Society of America) student chapter of the European campus of Georgia Tech, France from 2009 to 2010.
- Reviewer in international journals: Optics Letters, Optics Express, IEEE Journal of Quantum Electronics, IEEE Photonics Technology Letters, and Optics Communications.