**Université de Franche-Comté**

**École Doctorale SPIM**

# Thèse de Doctorat

Spécialité Optique et Photonique

présentée par :

**Mourad NOURINE**

## Étude des communications optiques sécurisées par chaos intégrant une clé physique via un composant électro-optique dédié

**Thèse dirigée par L. Larger, Professeur, Université de Franche–Comté**

soutenue le 22 septembre 2010.

**Jury :**

| | | |
|---|---|---|
| Président : | H. Maillotte | Directeur de recherche CNRS, Directeur du Département d'Optique, Institut FEMTO-ST, UFC |
| Rapporteurs : | S. El-Assad | HDR, Maître de Conférences, Université de Nantes |
| | M. Sciamanna | Professeur, École Supérieure d'Électricité, Metz |
| Examinateurs : | G. Millérioux | Professeur,CRAN-ESSTIN, Université Henri Poincaré Nancy 1 |
| | J. Hauden | Directeur R & D, Photline Technologies, Besançon |
| | L. Larger | Professeur, Institut FEMTO-ST, Département d'Optique, UFC |
| | Y.K. Chembo | Chargé de recherche CNRS, Institut FEMTO-ST, UFC |

*À ma mère et à la mémoire de mon père*

*À toute ma famille sans exception*

*À mon grand frère : Dhada H'mida*

*À mon adorable femme qui a toujours été là pour moi*

*À mes deux filles (nées pendant ces travaux de thèse) : Maeva et Lynda*

Mourad.

# Remerciements

Cette thèse a été réalisée au sein de l'équipe optoélectronique du Département d'Optique de l'Institut FEMTO-ST de Besançon, unité de recherche associée au CNRS n° 6174, de l'Université de Franche-Comté.

Ces quelques années passées sur ce sujet très intéressant ont été pour moi une expérience très enrichissante, aussi bien scientifiquement qu'humainement. Je remercie tout d'abord le Directeur du laboratoire, Monsieur **Hervé Maillotte**, Directeur de recherche CNRS pour avoir accepté d'être le Président de mon jury.

Je tiens à exprimer toute ma gratitude à mon directeur de thèse Monsieur le Professeur **Laurent LARGER**, de m'avoir fait confiance pour l'étude de ce sujet passionnant, pour l'accueil qu'il m'a réservé dès le début, pour le suivi de ces travaux, pour ses encouragements et pour ses conseils avisés. Un grand MERCI Laurent.

Je suis très sensible à l'intérêt pour ces travaux dont ont témoigné les autres membres de mon jury. J'adresse toute ma profonde gratitude à **Safwan El-Assed**, HDR et Maître de conférences à l'Université de Nantes, et à **Marc Sciamanna**, Professeur à SUPELEC de Metz, d'avoir acceptés d'être rapporteurs de cette thèse. J'exprime mes plus vifs remerciements à **Jérôme Hauden**, Directeur R & D de Photline Technologies à Besançon, et à **Gilles Millérioux**, Professeur au CRAN-ESSTIN de l'Université Henri Poincaré Nancy 1, d'avoir acceptés d'être membres de mon jury.

Je tiens tout particulièrement à remercier **Yanne Kouomou Chembo**, Chargé de recherche CNRS à Institut FEMTO-ST, avec qui j'ai pris grand plaisir à travailler. Je le remercie d'avoir participé au jury, mais surtout pour son aide et sa collaboration à mes travaux de recherches. Je lui adresse toute ma reconnaissance pour ses conseils pertinents et les nombreuses discussions que nous avons eues sur l'entropie, le chaos et bien d'autres sujets.

J'aimerais aussi remercier quelques personnes du labo d'Optique pour l'aide occasionnelle qu'elles m'ont apportée : Fadi Baida, pour l'utilisation de son calculateur numérique, Nadège Courjal, pour ses corrections d'un chapitre, Valérie Fauvez et Joelle Daumet, pour leurs gentillesse administrative, Sarah Djaouti et Belinda Lafon, pour leurs aide en recherche d'articles bibliographiques, ainsi que Pierre-Ambroise Lacourt et Maxime Jacquot. Je tiens tout particulièrement à remercier Jean-Marc Merolla, HDR et Chargé de recherche CNRS, pour les fructueuses discussions que j'ai eues avec lui sur le modulateur QPSK, mais surtout pour son aide à me trouver un job dans la région parisienne.

Je voudrais maintenant exprimer toute ma reconnaissance à tous les (ex)thésards et (ex)post-doctorants qui ont participé à la bonne ambiance du laboratoire et qui m'ont

permis de travailler ou de ne pas travailler, mais toujours dans d'excellentes conditions : Stéphane Poinsot (première personne à me montrer le fonctionnement d'un modulateur MZ expérimentalement), Matthieu Roussey (marci pour le LateX), Abderrahmane Belkhir (initiation aux simulations numériques sous matlab), Yannick Poujet, Ryad Bendoula, Michael Peil, Kirill Volyanskiy (merci pour la résolution des problèmes dûs aux virus informatiques), Hervé Tavernier, Romain Lavrov, Johann Cussey, Jassem Safiou, Nasser Nour, Mathieu Mivelle, Olivier Gaiffe, Idriss Abdoulkader Ibrahim (en bref : Abdoul) et tous les autres.

Je remercie également mes collègues du bureau -113b, les présents et les absents lors de ma soutenance, pour lesquels ce travail de thèse n'aurait pas été mené dans une bonne ambiance : Manoj Bhuyan, Vincent Pureur, Benjamin Wetzel, et le tonton qui a tiré les oreilles de ma fille Maeva : Abdel-Hamid Hmima.

Enfin, j'adresse un grand **merci** à ma famille, mes parents et mes sœurs pour leur confiance et leur soutien sans faille. A tous mes amis (khali Ahmed, Zoubir, Ali, Bouboul, Said, Mustapha, Belka,....), et à toutes les personnes qui se sont données la peine de me soutenir durant cette thèse.

M. comme Mourad.

# Résumé

Ce travail de thèse étudie la démonstration numérique et expérimentale de la génération de signaux chaotiques à partir d'une nouvelle architecture optoélectronique, appartenant à la catégorie des systèmes d'Ikeda, et destinée aux communications de données optiques sécurisées par chaos à haut débits. Le principe s'appuie sur une dynamique électro-optique non linéaire à multiples retards, dont la non linéarité est construite grâce à un interféromètre à 4 ondes réalisé en optique intégrée ($LiNbO_3$), et disposant de 2 électrodes de modulation indépendantes, autrement dit : **une non linéarité bidimensionnelle (2D)**. Cet interféromètre est un modulateur QPSK (Quadrature Phase Shift Keying), qui fait partie de la famille des modulateurs Mach-Zehnder à 4 bras ; il permet pratiquement de relier 2 boucles de rétroaction optoélectroniques, pour produire un chaos sur la variable dynamique intensité optique.

La dynamique particulière obtenue peut se résumer à un modèle théorique de deux équations intégro−différentielles, excitées par un terme non linéaire retardé qui est fonction de deux variables dynamiques couplées. Au travers d'une étude numérique et expérimentale, nous avons cherché à analyser certains des nombreux comportements dynamiques que peut présenter cet oscillateur, en fonction de divers paramètres physiques du montage : régimes de point fixe stable, périodiques, et chaotiques.

La mise en œuvre du montage expérimental a permis de valider le modèle théorique adopté pour les simulations. Ainsi, cet oscillateur permet de disposer d'une part, d'une dynamique ultra-rapide jusqu'à des fréquences de plusieurs GHz (environ 13 GHz), et d'autre part, de générer un chaos de grande dimension destiné au cryptage physique de données optiques. Enfin, le potentiel de décryptage du système cryptographique complet, composé d'un émetteur et d'un récepteur, a été mis en évidence numériquement en modulant chaotiquement une information binaire à plus de 3 Gbit/s.

# Abstract

This work develops a numerical and experimental demonstration for the generation of chaotic signals using a new optoelectronic architecture belonging to the class of Ikeda systems. The principle relies on an electro-optic non-linear delay dynamics, which non linearity is performed by a 4 waves integrated optics interferometer including 2 independent electro-optic modulation inputs : **the nonlinearity is therefore two-dimensional (2D)**. This interferometer is a Quadrature Phase Shift Keying (QPSK) modulator, which is a type of the integrated lithium niobate ($LiNbO_3$) Mach-Zehnder modulators with 4 arms. This component allows to link two electro-optic loops to produce a chaotic optical intensity.

The dynamics of the microwave oscillation can be described by two integro-differential nonlinear delayed equations, with a nonlinear delayed term which is a function of two coupled variables. We have built a mathematical model of the system and analysed a number of its possible solutions : stable steady states, periodic and chaotic regimes.

The experimental observations allowed to validate the dynamical model, through good qualitative agreements with the numerical simulations. This oscillator allows both to have ultra-fast dynamics up to several GHz frequencies, and potentially high dimensional chaos intended for encryption of optical data at the physical layer. Finally, the potential of decryption rate of the complete cryptographic system, consisting of a transmitter and a receiver, is numerically demonstrated using chaotic modulation of digital information at the rate higher than 3 Gbit/s.

# Table des matières

# Table des figures

# Liste des tableaux

# Introduction

L'essence même de la cryptographie est de permettre à deux entités de communiquer *via* un réseau public de sorte qu'un tiers à l'écoute soit dans l'impossibilité de comprendre le contenu des messages échangés. Par réseau public on entend un médium de communication qui ne comporte aucune restriction ni contrôle d'accès. Cela peut être le réseau téléphonique ou Internet par exemple. L'utilisation de moyens cryptographiques doit rendre inexploitables les informations illégitimement recueillies sur le canal public.

L'usage de la cryptographie est fondamental lorsque la confidentialité des communications ne doit souffrir d'aucune faille. C'est le cas par exemple de certains messages à caractère militaire ou, bien entendu, de transactions bancaires dans le cadre d'une activité de commerce électronique. Actuellement, des algorithmes informatiques[1] pour crypter les données existent (cryptographie à clé secrète, cryptographie à clé publique...), et ils sont par ailleurs largement répandus à cause de leur haut degré de sécurité. Ces algorithmes sont utilisés en général au niveau des différentes couches du modèle OSI simplifié, à l'exception de la couche physique. Cependant, leur coût élevé en terme de temps de calcul, surtout lorsque la quantité des données à chiffrer/déchiffrer est grande, reste un frein qui entraîne par exemple une diminution du débit des communications sécurisées.

En réponse à cette problématique, à partir des années 1980, deux nouveaux types de cryptographies adaptées aux transmissions par fibres optiques sont apparus. Le premier est la cryptographie quantique [1], dont le principe est celui d'Heisenberg, selon lequel la mesure d'un système quantique perturbe ce système. Il est alors possible de transmettre une clé en étant sûr qu'elle n'a pas été " écoutée ", et de l'utiliser ensuite pour le déchiffrement. Le second type est la cryptographie par chaos [2], dont le cryptage et le décryptage de l'information s'effectue directement sur la couche physique en temps réel, en noyant le message informatif dans un signal chaotique. Elle utilise les propriétés des dynamiques chaotiques, en l'occurrence une évolution temporelle d'apparence erratique, un spectre large et un déterminisme local.

De nombreuses communautés scientifiques ont consacré un effort de recherche théorique et expérimentale considérable, pour développer ces nouveaux types de cryptage. Ce manuscrit de thèse se situe dans le contexte des « communications chaotiques » sécurisées, il appartient de ce fait à la famille de la cryptographie par chaos. En effet, depuis que les

[1] Exemples d'algorithmes historiquement pertinents : le DES (Data Encryption Standard) ; IDEA (International Data Encryption Algorithm) ; RSA (Rivest, Shamir et Adleman) ; AES (Advanced Encryption Standard) ; ...

travaux de Pecora et Carroll [2] ont démontré la possibilité de synchronisation du chaos déterministe, les travaux sur la cryptographie par chaos n'ont jamais cessé de croître : améliorations des systèmes mais surtout diversifications de générateurs des signaux chaotiques.

Nous nous sommes intéressés plus particulièrement aux systèmes non linéaires à retard(s), car ils peuvent produire des dynamiques chaotiques d'une grande complexité, condition pour laquelle un bon masquage d'une information utile semble nécessaire. De plus, le système à délais que nous proposons est un système optoélectronique, d'une génération nouvelle en termes d'architecture et de configuration, avec lequel nous visons à terme une application en communications de données optiques sécurisées par chaos en temps réel à haut débits.

Ce manuscrit s'articule en quatre chapitres :

Le premier est une introduction générale aux systèmes dynamiques non linéaires chaotiques, ainsi qu'à un certain nombre d'outils mathématiques utilisés pour les étudier. Les différents aspects de la génération de signaux chaotiques seront présentés, et un état de l'art sur les différents systèmes cryptographiques par chaos sera exposé. Une description globale du générateur de chaos proposé, avec la mise en avant de ses originalités, sera donnée en fin de chapitre.

Dans le deuxième chapitre, nous présenterons le cœur de cet oscillateur chaotique, à savoir l'élément réalisant sa fonction non linéaire au travers de sa description générale et de sa modélisation. Afin de le simuler numériquement et d'obtenir ses diverses évolutions dynamiques possibles, la mise en équations de cet oscillateur sera aussi développée.

Le troisième chapitre est consacré à l'étude de ce générateur de chaos, et au système de cryptographie complet, composé d'un émetteur et d'un récepteur. Les diverses architectures de ce système seront développées, et l'analyse de la multitude des régimes dynamiques produits sera aussi présentée.

Le quatrième et dernier chapitre présentera la partie expérimentale du travail. Ils s'agira de la caractérisation des composants, des résultats de comportements dynamiques générés par l'oscillateur chaotique dans deux configurations différentes par leur architecture. Ces résultats seront comparés à ceux obtenus numériquement aux chapitres 2 et 3. Enfin, nous conclurons en insistant sur les principaux résultats qui ont été obtenus, et nous discuterons des perspectives découlant de ces travaux.

# Chapitre 1

# Le chaos et architecture de l'émetteur

Le but de ce premier chapitre est de présenter d'une part quelques rappels indispensables à la compréhension de ce manuscrit, et d'autres part de donner l'ensemble des notions nécessaires à la description, à l'analyse et à la compréhension du comportement temporel des systèmes dynamiques. Il commencera par un bref rappel de quelques définitions liées au chaos et aux dynamiques non linéaires. En général ces définitions sont relatives à tous les systèmes dynamiques, mais nous privilégierons souvent ceux à comportements chaotiques. Ensuite, nous évoquerons un certain nombre d'outils mathématiques qui permettent de caractériser les divers comportements dynamiques engendrés par ces systèmes. Ces outils seront pour la plupart utilisés lorsque nous étudierons notre système de cryptographie.

La deuxième partie sera dédiée à la présentation du principe de fonctionnement d'un oscillateur non linéaire à retard, ainsi qu'à son modèle associé. Cette classe particulière d'oscillateurs est directement concernée par ce travail de thèse. Puis dans une troisième partie, nous exposerons les différentes méthodes d'intégration numérique des modèles mathématiques proposés.

Dans une quatrième partie, nous allons matérialiser le problème par une brève présentation de quelques exemples physiques déjà étudiés dans la littérature. Et afin de situer la nouveauté et l'originalité de notre système de cryptage, une description rapide des différents systèmes à retard développés dans notre laboratoire sera donnée. Les différentes méthodes de codage/décodage seront aussi décrites brièvement.

Enfin, la dernière partie de ce chapitre sera consacrée entièrement à notre générateur de chaos, en présentant ses originalités et ses principaux avantages. Puis avant de conclure, nous donnerons une description globale, largement développée, de l'architecture de l'émetteur du système cryptographique proposé.

## 1.1 Le chaos et les systèmes dynamiques

### 1.1.1 Généralités sur le chaos

Pendant plusieurs siècles, l'homme pensait qu'une connaissance complète des paramètres d'un phénomène, à un instant donné, lui permettait d'en prédire l'évolution passée ou à venir, cela sans aucune autre limite que l'imperfection des méthodes expérimentales. Cette idée a été formulée par Pierre-Simon de Laplace en 1776 dans son Essai sur les probabilités. Pourtant, au début du XX$^{e}$ siècle, Henri Poincaré montrait à travers l'étude de la stabilité du système solaire par le problème à trois corps, que même si les lois naturelles n'auraient plus de secret pour nous, nous ne pourrions connaître la situation initiale qu'approximativement, et selon lequel « d'infimes incertitudes sur l'état initial d'un système pourraient en engendrer de très grandes sur l'état final » [3]. L'étude de Poincaré est considérée comme la première manifestation de la théorie du chaos.

Loin de prétendre donner ici un historique détaillé sur la théorie du chaos, qui est devenue une discipline à part entière vers 1975, nous cherchons plutôt à présenter certaines définitions (systèmes dynamiques, déterminisme, conditions initiales ...) utiles à la compréhension du mot chaos tel que le scientifique le comprend, c'est-à-dire que le sens de celui-ci ne signifie pas *absence de l'ordre*, mais il se rattache à une notion d'imprévisibilité, d'impossibilité de le prévoir à long terme [4].

#### 1.1.1.a Les systèmes dynamiques non linéaires

La notion de système dynamique est relative à tous les systèmes dont l'évolution dépend du temps ou de l'espace. Cette notion est donc générique et peut se retrouver dans divers domaines comme la physique, la chimie, la biologie, ... etc. En général, pour comprendre ou prévoir des phénomènes réels générés par ces systèmes, la démarche à suivre consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Si cette relation est une opération de proportionnalité, le phénomène est dit " linéaire ". Mathématiquement, cela revient à dire si une cause $x_1$ entraîne un effet $y_1$ et une cause $x_2$ produit un effet $y_2$, alors une cause totale $x_1 + x_2$ entraîne un effet $y_1 + y_2$ (l'effet de la somme est la somme des effets).

Dans le cas d'un phénomène non linéaire, l'effet n'est pas proportionnel à la cause. Afin de mieux comprendre ce phénomène, nous décrirons dans le paragraphe suivant un exemple en mécanique, qui illustre bien ce principe : le mouvement du pendule libre non amorti [5].

Considérons un pendule, schématisé sur la figure 1.1, constitué d'une masse $m$ ponctuelle soumise à un champ de pesanteur vertical, d'accélération $g$, et isolée de toute perturbation extérieure. Celle-ci est attachée à un point $A$ par un lien rigide de longueur $l$, de sorte qu'il n'y ait aucun frottement susceptible d'amortir le mouvement de la masse qui se déplace dans le plan vertical passant par $A$. On définit $\theta(t)$ comme l'angle entre le fil et l'axe vertical.

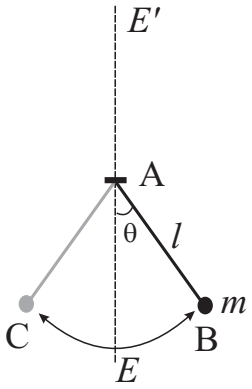



Figure 1.1 – *Pendule libre non amorti.*

En appliquant le principe fondamental de la dynamique, on aboutit à un modèle qui se traduit par l'équation ci-dessous.

$$\frac{d^2\theta(t)}{dt^2} = -\frac{g}{l}\sin\theta(t) \tag{1.1}$$

Cette équation contient un terme non linéaire $\sin\theta(t)$ qui peut être simplifié par une approximation linéaire $\sin\theta(t) \approx \theta(t)$, valable seulement pour de petits déplacements angulaires. Lorsqu'on fait cette approximation linéaire, le modèle simple qui en résulte décrit seulement une petite partie des comportements possibles du pendule : un mouvement d'oscillation périodique autour de la position d'équilibre $E$.

Par contre, le modèle non simplifié correspondant à l'équation (1.1) permet lui de décrire certains comportements du pendule, qui ne peuvent pas l'être par le modèle linéaire. Il s'agit par exemple de la position d'équilibre instable $E'$ où la masse est exactement au-dessus du point d'attache $A$. Si l'énergie du pendule est encore supérieure à celle requise pour atteindre cette position, le pendule n'oscille plus autour du point d'équilibre stable $E$, mais acquiert un mouvement de rotation plus au moins régulier autour du point d'attache. Dans ces conditions, la trajectoire de la masse, représentée par la variable dynamique $\theta(t)$, peut avoir divers allures que seul le modèle non linéaire peut décrire.

On comprend à travers cet exemple, que la dynamique non linéaire a fait apparaître une très grande richesse de comportements dynamiques. L'étude des phénomènes chaotiques s'inscrit dans le cadre de la théorie de ces systèmes non linéaires.

#### 1.1.1.b Chaos déterministe

L'ensemble des modèles mathématiques décrivant les systèmes dynamiques non linéaires peut être classé en deux catégories, selon qu'ils sont probabilistes ou déterministes, bien que dans certains cas, comme en physique quantique, la séparation ne soit pas si nette [6]. Dans un modèle probabiliste, un ensemble de conditions initiales connues entraîne des probabilités d'évolution du système. Celui-ci possède globalement plusieurs

états finaux qui peuvent exister, chacun avec une certaine probabilité. Au contraire, dans le cas des modèles déterministes, des conditions initiales connues conduisent à une évolution parfaitement déterminée, et les mêmes causes produisent toujours les mêmes effets.

Une propriété importante liée aux systèmes déterministes est la prévisibilité. En effet, en connaissant le modèle et les conditions initiales à l'instant $t_0$, l'état du système est prévisible à tout instant $t > t_0$. Cependant, depuis la découverte des phénomènes chaotiques, la prévisibilité n'est plus systématiquement liée au déterminisme. De ce fait, il convient alors de distinguer les phénomènes aléatoires du chaos déterministe qui nous intéresse ici.

Dans les phénomènes aléatoires, il est absolument impossible de prévoir la trajectoire d'une quelconque particule. C'est le cas typique du mouvement brownien découvert par Robert Brown en 1827, qui désigne le mouvement aléatoire d'une particule : il est incessant, isotrope et c'est de plus un processus de Markov du premier ordre, c'est-à-dire que le mouvement à venir est indépendant du mouvement passé. Pour l'observer, il suffit d'examiner au microscope une suspension de grains de pollen : ces particules effectuent des mouvements incessants et aléatoires, mouvements résultant d'impulsions transmises par les molécules du milieu soumises à l'agitation thermique [7].

À l'opposé, la dynamique chaotique se produit par une loi dynamique. On l'appelle donc *chaos déterministe*. Les systèmes dynamiques chaotiques sont caractérisés par certaines équations rendant compte du phénomène, mais dont les solutions (approximatives, faute de pouvoir les solutionner exactement) sont sensibles aux conditions initiales. La notion de déterminisme est ainsi intrinsèquement liée à tous les systèmes dont l'évolution est définie par un ensemble d'équations différentielles.

#### 1.1.1.c Sensibilité aux conditions initiales

Une autre propriété des phénomène chaotiques est qu'ils sont très sensibles aux perturbations (conditions initiales). L'un des premiers chercheurs à s'en être aperçu fut Edward Lorenz qui, au début des années 1960, travaillait sur le problème de la modélisation de la dynamique atmosphérique [8]. Fonctionnaire comme météorologue au MIT[1], il disposait pour ce faire d'un ordinateur et d'un modèle mathématique assez simple : un système différentiel à trois variables dynamiques indépendantes, autrement dit, 3 *degrés de liberté*.

En refaisant les calculs pour une séquence particulière de mesures, et pour économiser du temps de calcul, Lorenz commença au milieu de la séquence au lieu du début. Il prit alors comme conditions initiales les nombres qu'il avait déjà imprimés, et quand il regarda le résultat obtenu une heure plus tard, la séquence obtenue évolua de manière différente par rapport à la première séquence calculée. Il chercha alors à expliquer ce qui s'était produit. Il remarqua que l'ordinateur stockait des nombres possédant 6 chiffres après la virgule alors que l'imprimante n'en considérait que 3. Ce détail à priori insignifiant a permis de mettre en évidence la sensibilité de tels systèmes par rapport aux conditions initiales.

[1] Massachusetts Institute of Technology

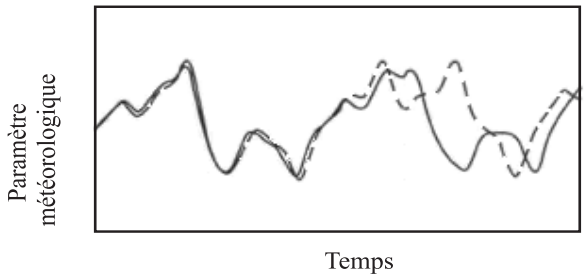



Figure 1.2 – *Évolution temporelle pour deux conditions initiales très proches.*

E. Lorenz venait de découvrir que dans les systèmes dynamiques non linéaires, d'infimes différences dans les conditions initiales engendreraient des trajectoires totalement différentes (figure 1.2). De ce fait, il comprit qu'il serait impossible de prédire avec précision la météo à long terme. Il utilisa les mots suivants, souvent résumés par « Effet papillon » : « Le battement d'aile d'un papillon, aujourd'hui à Pekin, engendre dans l'air des remous qui peuvent se transformer en tempête le mois prochain à New York. » [4].

À partir de cet exemple, nous voyons donc qu'une très légère modification des conditions initiales entraîne des changements importants pour l'évolution future du système. Expérimentalement, cette faible modification peut par exemple être due au bruit ou à un manque de précision dans la définition pratique des conditions initiales. Les dynamiques chaotiques présentent donc une grande sensibilité aux conditions initiales ; c'est une de leurs caractéristiques principales.

#### 1.1.1.d Espace des phases

Un système dynamique est caractérisé par un certain nombre de variables d'état, qui ont la propriété de définir complètement l'état du système à un instant donné. Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ces variables d'état au cours du temps. Pour représenter l'état de ce système, on utilise couramment en physique un espace de dimension égal au nombre de variables d'état. Cet espace est appelé « espace des phases » où chaque point définit un état différent du système. Lorsque ce système évolue dans le temps, ses variables d'état évoluent et le point associé à cet état décrit une trajectoire, appelée également une orbite.

Pour un système dynamique déterministe, une trajectoire dans l'espace des phases a la propriété essentielle de ne posséder aucune intersection avec elle-même ou avec d'autres. En effet, imaginons qu'une ou plusieurs trajectoires de l'espace des phases se recoupent en un point. Si on considère maintenant ce point comme l'état initial, le système peut donc évoluer selon plusieurs de ces trajectoires possibles et par conséquent, son évolution n'est plus déterminée par son état initial. L'intersection de trajectoires dans l'espace des phases est incompatible avec le caractère déterministe du système.

Reprenons l'exemple du pendule libre donné sur la figure 1.1. Ce système possède deux variables d'état qui le caractérisent complètement, $\theta$ l'angle à la verticale et $\dot{\theta}$ sa dérivée

par rapport au temps, qui représente la vitesse angulaire de la masse. L'espace des phases possède donc deux dimensions [5].

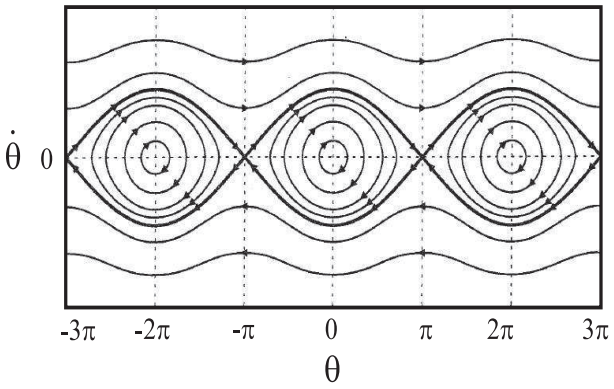



Figure 1.3 – *Trajectoires d'un pendule libre non amorti dans l'espace des phases.*

Dans cet espace des phases, représenté sur la figure 1.3, chaque point correspond à un état du pendule, défini par sa position angulaire $\theta$ en abscisse et sa vitesse angulaire $\dot{\theta}$ en ordonnée. Chaque ligne représente une trajectoire du pendule pour une énergie donnée. Les trajectoires circulaires correspondent aux petites oscillations du pendule autour de sa position d'équilibre stable $E$ (figure 1.1), et lorsque l'énergie du pendule est supérieure à un certain seuil[2], la trajectoire n'est plus fermée, et le pendule possède donc un mouvement de rotation autour de l'axe.

L'ensemble des trajectoires représentées dans cet espace des phases montrent une propriété de ce système parfaitement déterministe : il n'existe aucune intersection entre les trajectoires. Les points $(2n\pi, 0)$ ne sont pas des intersections mais des *points singuliers*, auxquels nous nous intéresserons dans la suite.

L'espace des phases de la figure 1.3 permet de visualiser simplement l'ensemble des comportements dynamiques du pendule. Cependant, tous les systèmes dynamiques ne peuvent pas être décrits par deux variables d'états, et particulièrement ceux à comportements chaotiques. En effet, une trajectoire chaotique se situe sur un *attracteur étrange*, dans un espace des phases de dimension supérieure ou égale à 3.

#### 1.1.1.e Stabilité, attracteur et caractère pseudo-aléatoire

Par définition, la stabilité est le caractère de ce qui tend à demeurer dans le même état malgré de petites perturbations. Rapportée aux systèmes dynamiques, il s'agit de la solution du modèle mathématique du système. Pour illustrer cette notion de stabilité, revenons à l'exemple du pendule libre non amorti dont l'espace des phases est décrit sur la figure 1.3. Il existe deux points singuliers qui correspondent à des positions d'équilibre du pendule :

[2]Il s'agit de l'énergie particulière $(g/l)^{1/2}$. La trajectoire dans l'espace des phases — figure 1.3— passe par un des points $((2n+1)\pi, 0)$, qui correspond à la position d'équilibre instable $E'$ (voir figure 1.1).

- Le premier correspond à la position basse, représentée par le point $E$ sur la figure 1.1 et située aux points $(2n\pi, 0)$ sur la figure 1.3. Il s'agit d'une position d'équilibre du pendule, c'est-à-dire si le pendule se trouve initialement à cette position, il va y rester : c'est la notion de position d'équilibre ou de *point fixe*. Si maintenant le pendule est placé initialement dans une position différente mais proches de la verticale, le système va rester, tout en oscillant, dans le voisinage de la position d'équilibre : c'est la notion de *stabilité du point fixe*.

- Le deuxième point singulier du système correspond à la position haute du pendule, représentée par $E'$ sur la figure 1.1 et situé aux points $((2n+1)\pi, 0)$ sur la figure 1.3. C'est une position d'équilibre *instable* : lorsque le pendule est placé initialement dans cette position, il y reste, mais s'il est placé initialement à proximité, il s'en éloigne inéluctablement.

La notion de *stabilité* est définie ici au sens de Lyapunov [9] : un point d'équilibre est stable si le système reste au voisinage de ce point lorsqu'il est initialement placé dans ce voisinage. De plus, si le système se rapproche de ce point d'équilibre, alors cet état d'équilibre est dit asymptotiquement stable. Cette position d'équilibre, ou point fixe, est un *attracteur* : le système évolue vers cet état, pour un ensemble de conditions initiales données. Cependant, la notion de stabilité peut s'appliquer aussi à des régimes dynamiques oscillatoires. Dans ce cas, le comportement final du système est une oscillation périodique. L'attracteur associé est appelé « *cycle limite* ».

Le chaos est toujours la conséquence d'instabilité [10], et l'exemple du pendule seul ne peut devenir chaotique : il n'est décrit que par deux variables dynamiques, sa position et sa vitesse, mais il suffit de lui adjoindre une variable supplémentaire pour qu'il puisse le devenir [11]. Une façon très simple est de stimuler périodiquement le pendule avec une force extérieure : la variable supplémentaire est alors la phase de cette stimulation. Mais dans un esprit de compréhension plus générale des systèmes dynamiques non linéaires, nous avons choisi de prendre un autre exemple de système considéré comme le prototype des systèmes dits « *chaotiques* ». Ce système nous l'avons déjà introduit précédemment et possède trois variables dynamiques : le *système de Lorenz*.

En effet, le modèle dynamique de Lorenz est constitué par un système de trois équations différentielles non linéaires de la forme :

$$\begin{cases} \dot{x} &= P_r \cdot (y - x) \\ \dot{y} &= r \cdot x - x \cdot z - y \\ \dot{z} &= x \cdot y - b \cdot z \end{cases} \tag{1.2}$$

où $x(t)$, $y(t)$ et $z(t)$ sont des variables dynamiques qui définissent des trajectoires dans un espace des phases. $P_r$, $r$ et $b$ sont des paramètres sans dimension qui jouent un rôle de changement de l'allure de la trajectoire.

L'ensemble de la trajectoire solution de l'équation (1.2), pour des paramètres fixés, constitue le célèbre *attracteur de Lorenz* (voir figure 1.4a). En général, un attracteur attire asymptotiquement des *conditions initiales* vers une même trajectoire solution, et l'ensemble des conditions initiales aboutissant à un même attracteur est un *bassin d'attraction* associé à cet attracteur.

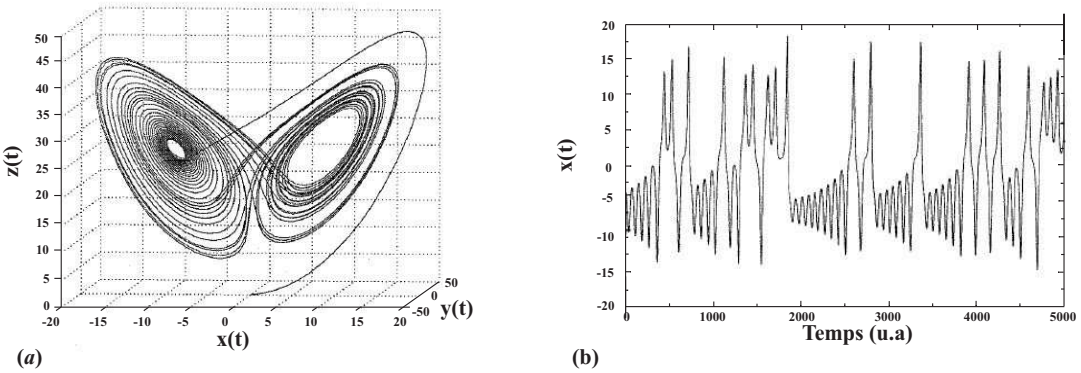



Figure 1.4 – (*a*) *Attracteur étrange de Lorenz.* (*b*) *Série temporelle chaotique.* *Paramètres numériques :* $P_r = 10$ *;* $r = 28$ *;* $b = 8/3$

L'attracteur étrange possède une structure dense et complexe qui est à l'origine de la propriété de *sensibilité aux conditions initiales* [12]. Les trajectoires ne sont ni périodiques, ni quasi périodiques, mais plutôt apériodiques. Sur la figure 1.4a, ces dernières sont chaotiques, elles sont denses mais ne se croisent jamais entre elles, bien qu'elles parcourent deux ailles bien localisées et bornées dans l'espace. Le processus à la base de ce mélange dense de trajectoires est appelé *étirement-repliement.*

L'idée d'étirement est à la base de la propriété de *sensibilité aux conditions initiales* : si l'on étire 2 trajectoires infiniment proches, leur écart initial va nécessairement augmenter au fur et à mesure de l'opération d'étirement. La dynamique évoluant dans un espace borné, les trajectoires infiniment proches ont besoin, pour s'écarter, d'un étirement infiniment long. Pour conserver une évolution dynamique dans un espace borné, un deuxième processus est nécessaire, le repliement. Si le repliement est suffisamment présent tout au long de la trajectoire, le domaine où évolue le chaos est stable, c'est un attracteur. L'étirement-repliement est à l'origine de la structure en *feuillets* que l'on trouve dans de nombreuses dynamiques chaotiques [11].

La figure 1.4b présente l'évolution temporelle chaotique (ou pseudo-aléatoire) de la variable dynamique $x(t)$. Cette dernière oscille tantôt autour d'une valeur positive, tantôt autour d'une valeur négative, et ce, d'une manière tout à fait imprédictible.

#### 1.1.1.f Section de Poincaré

Pour observer les trajectoires d'un attracteur, il est parfois très utile de réduire la dimension $d$ de l'espace des phases. Proposée par H. Poincaré, la méthode consiste à faire une coupe de la trajectoire par un plan dans l'espace des phases et à relever, dans ce

plan, tous les points d'intersection de la trajectoire perçant ce dernier dans un sens donné (figure 1.5). L'ensemble des points obtenus s'appelle une *section de Poincaré*. En plus de la diminution de l'espace des phase $d$ en $d-1$, cette méthode permet de réduire le nombre de données à manipuler en ne conservant que les points d'intersection des trajectoires avec le plan. Le reste des points de la trajectoire étant ignorés, la dynamique est ainsi plus facile à étudier.

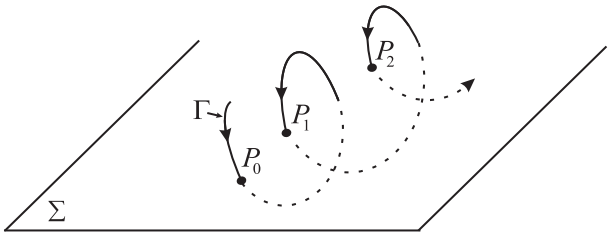



Figure 1.5 – *Section de Poincaré : la trajectoire* $\Gamma$ *coupe le plan* $\Sigma$ *en des points* $P_n$. *Ces points appartiennent à la section de Poincaré* [5].

La coupe de Poincaré est un outil d'étude visuel des propriétés dynamiques dans l'espace des phases. Elle permet aussi le passage d'une loi dynamique continue à une loi discrète. Ainsi, la structure en feuillet des attracteurs étranges apparait dans la section sous forme de lignes imbriquées. Une trajectoire dense sur un ruban (modèle de Lorenz) devient un ensemble de portions de courbes, discontinues mais denses. Cependant, le choix de la section n'est pas quelconque, car des problèmes peuvent se poser. Si, par exemple, une trajectoire forme une boucle juste avant la section choisie, cette boucle ne sera pas « vue » au travers de la section de Poincaré. On essaie en général de prendre une section que la trajectoire traverse toujours, ou presque, de manière orthogonale.

En résumé, les caractéristiques essentielles d'un système chaotique présentées dans les paragraphes précédents peuvent être récapitulées de la manière suivante : il s'agit d'un système déterministe signifiant que la dynamique en cause obéit bien à des lois mais, que l'évolution des phénomènes concernés est imprévisible du fait de leur sensibilité à toute perturbation. Ces lois, dans les cas qui nous intéressent, sont sous la forme d'équations différentielles et le comportement chaotique est le résultat de phénomènes principalement non linéaires. Ce comportement est caractérisé par son instabilité qui se traduit par une sensibilité importante aux conditions initiales. Le phénomène chaotique a une allure pseudo-aléatoire semblable à celle d'un bruit blanc, dont la trajectoire se situe sur un attracteur étrange dans un espace des phases de dimension supérieure ou égale à 3.

Cependant, apportons une précision sur le terme chaotique. Un système est dit chaotique lorsque dans certaines conditions il se comporte d'une manière chaotique. Mais il se peut que, dans d'autres conditions, ce même système peut avoir un autre comportement non chaotique, par exemple oscillatoire. Il est donc utile de chercher des moyens de caractériser *a priori* un régime dynamique et *a posteriori*, s'il s'agit d'un régime chaotique, de savoir dans quelle mesure il est chaotique.

### 1.1.2 Caractérisation d'un signal chaotique

L'identifications des propriétés vues précédemment d'un comportement chaotique requiert un certain nombre d'outils à même de les mesurer, à partir de l'observation du comportement du système non linéaire. Ce sont ces outils que nous allons tenter de décrire maintenant. Certains sont déjà bien connus en traitement de signal (analyse statistique, analyse fréquentielle), et d'autres seront plus spécifiquement issus du domaine des dynamiques non linéaires (diagrammes de bifurcation, diagramme entropique).

#### 1.1.2.a Outils statistiques

L'une des premières étapes dans la caractérisation d'un signal est son analyse statistique. Les signaux chaotiques que nous cherchons à obtenir devront préférentiellement présenter une signature statistique aussi proche que possible de celle d'un vrai bruit, c'est-à-dire d'un signal aléatoire. Cette recherche est motivée, d'un point de vue probabiliste, par le fait que le bruit blanc se caractérise par un profil de distribution statistique Gaussien. Bien qu'il est très répandu en théorie et en pratique, ce profil est intéressant pour les communications chaotiques sécurisées : l'analyse de la distribution statistique du chaos par un espion ne pourra lui donner d'information pertinente sur l'origine déterministe de ce chaos.

**Distribution de probabilité**

Pour une meilleure compréhension, nous définissons au préalable ici quelques variables du système dynamique :

- soit $x(t)$ le signal temporel caractérisant la dynamique non linéaire ;
- soit $P(x)$ la distribution de probabilité du signal $x(t)$.

La distribution de probabilité $P(x)$ traduit la répartition en amplitude du signal $x(t)$, avec bien sûr la somme $\int P(x)\,\mathrm{d}x$ égale à 1 comme tout ensemble de probabilités. Théoriquement, cette distribution est continue en fonction de $x$, et dans le cas du modèle Gaussien, elle se présente sous la forme :

$$P(x) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left\{-\frac{(x-\mu)^2}{2\,\sigma^2}\right\} \tag{1.3}$$

où $\sigma^2$ est la variance et $\mu$ la valeur moyenne. En pratique, les valeurs de la variable statistique sont considérées comme appartenant à des intervalles en nombre fini, et non à une distribution continue comme dans (1.3). La représentation graphique dans ce cas

pratique est un *histogramme*, dont le principe de construction est simple : il suffit de définir une plage d'amplitude délimitée par deux valeurs[3] $a_{min}$ et $a_{max}$, partagée en $N_H$ segments. Ensuite, on dénombre les points de chaque segment pour avoir sa densité de probabilité, ce qui se traduit mathématiquement par : on établit un lien entre la valeur $x_i$ et l'indice $l_i$ du segment dans lequel elle est comprise. Ce lien est donné par la relation (1.4).

$$l_i = \text{ceil}\left[\frac{(N_H - 1)\,(x_i - a_{min})}{a_{max} - a_{min}}\right] \tag{1.4}$$

On calcule ensuite $N_H$ valeurs $H_k$, où $H_k$ est le nombre d'occurrences de $k$ dans l'ensemble des valeurs $l_i$, ce qui se traduit par la relation (1.5)[4].

$$H_k = \sum_{i\,=\,0}^{N_H-1} \delta_{kl_i} \tag{1.5}$$

Enfin, il suffit de normaliser les valeurs $H_k$. Le résultat de ce calcul, donné par la relation (1.6), aboutit à un ensemble de $N_H$ valeurs $P_k$ dont la somme est 1.

$$P_k = \frac{H_k}{\sum_{m\,=\,0}^{N_H-1} H_m} \quad ; \quad k = 0, \ldots, N_H - 1 \tag{1.6}$$

Cette distribution de probabilité approchée est d'autant plus proche de celle théorique que le nombre $N_H$ de segments est important, et que la durée du signal $x(t)$ est longue.

### Entropie

Dans le cadre de la théorie de l'information, l'entropie est une mesure de la création naturelle d'information par le système dynamique [13]. L'entropie utilisée dans ce contexte — relation (1.7) — est statistique [14], et elle mesure la quantité d'information contenue dans un signal en fonction de la distribution de probabilité associée.

$$E = -\sum_{k=0}^{N_H-1} P_k \log_2 P_k \tag{1.7}$$

Un signal de type constant dans le temps a une entropie nulle, car sa densité de probabilité est égale à 1 pour cette constante et nulle pour toutes les autres. Ce type de

[3] La valeur $a_{min}$ est légèrement plus petite que l'amplitudes minimale du signal $x(t)$. La valeur $a_{max}$ est légèrement plus grande que l'amplitudes maximale de $x(t)$.

[4] $\delta_{mn}$ est le symbole de Kronecker. Il prend la valeur 1 si $m = n$ ou la valeur 0 si $m \neq n$.

signal ne contient aucune information non prévisible. Un signal dont la distribution de probabilité est uniformément répartie sur $n$ valeurs (c'est-à-dire : $P_k = 1/n$ pour chacune des valeurs), l'entropie résultante est $E = \log_2 n$. L'exemple du signal en créneau ($n = 2$ niveaux), a une entropie $E = \log_2 2 = 1$ bit (signification : le signal en créneau a 1 bit d'information).

Il a été démontré [15, 16] que l'entropie statistique $E$ vérifie la relation suivante :

$$0 \leq E \leq \log_2 N_H \tag{1.8}$$

où $N_H$ représente le nombre de segments utilisés pour le calcul de la distribution de probabilité, exposée précédemment. Comme il a été déjà expliqué, la valeur de l'entropie nulle — relation (1.8) — correspond à un signal ne contenant pas d'information (constant), et la limite supérieure $\log_2 N_H$ correspond à un signal contenant un maximum d'information, dont la distribution est répartie uniformément sur toute la plage d'amplitude.

Dans le cas d'un système potentiellement chaotique, l'intérêt de l'entropie est de pouvoir déterminer globalement à partir d'une seule valeur $E$ si le système fonctionne en régime périodique ou en régime chaotique. Cependant, cet intérêt est relatif dans la mesure où l'entropie est du même ordre de grandeur qu'il s'agisse d'un signal chaotique ou d'un signal périodique occupant un grand nombre de niveaux. Cet outil est donc utilisé en première approche pour caractériser grossièrement le type de régime dynamique.

#### 1.1.2.b Outils propres aux systèmes linéaires

Nous allons décrire deux autres outils de caractérisation très classique en traitement de signal, et qui seraient inévitablement utilisés par un espion pour l'analyse du signal chaotique porteur de l'information. Ces outils — le spectre et l'autocorrélation — sont toutefois utilisables pour caractériser tout type de signaux qu'ils soient d'origine linéaire ou non linéaire, de type périodique, quasi-périodique, pseudo-aléatoire ou encore complètement aléatoire (bruit blanc par exemple).

##### Spectre

Un signal temporel $x(t)$ peut être représenté, dans le domaine fréquentiel, par le calcul de son spectre. L'outil utilisé pour ce calcul est la transformée de Fourier dont le principe général est de décomposer un signal quelconque en une somme de sinusoïdes de fréquences, amplitudes et phases différentes. La formulation mathématique est décrite par la relation (1.9), où $t$ et $f$ sont les deux variables réciproques temps, fréquence. $\tilde{X}(f)$ représente le spectre complexe du signal $x(t)$.

$$\tilde{X}(f) = \int_{-\infty}^{+\infty} x(t) \cdot e^{-i2\pi ft} dt \tag{1.9}$$

Le spectre complexe étant assez difficile à représenter, c'est la raison pour laquelle on le décompose en général en deux parties : le spectre d'amplitude $|\tilde{X}(f)|$ et le spectre de phase $\angle\tilde{X}(f)$. On utilise aussi le spectre de puissance $|\tilde{X}(f)|^2$, appelé couramment densité spectrale de puissance. Dans la suite, nous n'utiliserons pas le spectre d'amplitude, mais seulement celui de puissance. Celui-ci correspond généralement aux mesures expérimentales fournies par un analyseur de spectre.

Dans les cas pratiques, on se limite souvent à une version discrétisée de cette transformée de Fourier dans l'espace des fréquences (soit $N_E$ le nombre total échantillons). On parle de transformée de Fourier discrète (1.10), que l'on obtient à partir d'une version échantillonnée $x_n$ avec un pas $T_e$, du signal d'origine en temps continu $x(t)$. Tous les appareils d'acquisition numériques des signaux fournissent, en général, ce spectre discrétisé, par l'intermédiaire d'un algorithme de calcul dit FFT (Fast Fourier Transform).

$$\tilde{X}_k = \sum_{n=0}^{N_E-1} x_n \cdot \exp\left(-i2\pi\frac{k\cdot n}{N_E}\right) \quad ; \quad k = 0,\ldots,N_E-1 \tag{1.10}$$

L'allure générale du spectre de puissance dépend, à l'évidence, de la manière dont le signal $x(t)$ évolue au cours du temps. Pour un signal périodique, une sinusoïde par exemple, le spectre va faire apparaître un pic unique au niveau de la fréquence de la sinusoïde. Un signal carré est un autre exemple de signaux périodiques, son spectre se caractérise par plusieurs raies dont la première correspond à la fréquence du signal (appelée fréquence fondamentale), et dont les suivantes sont les harmoniques (ayant des fréquences multiples de la fréquence fondamentale).

Pour un signal apériodique, il n'y a plus de raies caractéristiques sur le spectre, mais plutôt un ensemble continu de fréquences. Cependant, il faut noter que dans un contexte de dynamiques chaotiques, certaines propriétés du spectre permettent de distinguer un signal chaotique d'un signal purement aléatoire. Ces propriétés sont liées au système lui-même telle que la fréquence de coupure à laquelle la dynamique chaotique est contrainte, ou encore le type et l'ordre du filtre utilisé. La fréquence de coupure du système générateur du chaos se manifeste par un spectre limité en fréquences : c'est l'une des principales différences entre un spectre de signal chaotique et celui d'un signal de type bruit blanc. Le type de processus dynamique à l'origine du comportement chaotique (la fonction de filtrage d'un passe-bas, passe-haut, passe-bande) est une information que peut donner aussi le spectre, par sa ressemblance à la fonction de transfert de ces filtres. L'ordre du filtre utilisé peut être obtenu en calculant la pente de décroissance du spectre en décibel par décade (une pente faible correspond à un ordre petit et une pente raide à un ordre élevé).

En résumé, la représentation spectrale d'un signal met en évidence le type de régime dynamique. Le spectre d'un signal périodique présente un certain nombre de pics régulièrement espacés et bien visibles, alors que celui d'un signal chaotique se rapproche d'un spectre de type bruit coloré, contenant un ensemble continu mais limité de fréquences. Des exemples de tels signaux seront présentés un peu plus loin au chapitre 3.

**Autocorrelation**

La fonction de corrélation entre deux signaux $x(t)$ et $y(t)$ est un outil mathématique permettant d'analyser le degré de ressemblance entre ces deux signaux, à une translation près. La formule analytique de cette fonction est donnée par :

$$C_{XY}(\tau) = \int_{-\infty}^{+\infty} x(t) \cdot y(t-\tau)\, dt \tag{1.11}$$

Lorsque l'expression (1.11) est appliquée à deux signaux identiques, il s'agit de la fonction d'autocorrélation, notée $C_{XX}(\tau)$. Celle-ci permet de mettre en évidence l'autosimilarité d'un signal, comme par exemple, une certaine périodicité à l'intérieur du signal.

Dans le cas de l'analyse d'un signal réel (par exemple échantillonné), la durée d'observation est nécessairement limitée et correspond à la plus grande possible (fonction de la mémoire disponible), de façon à prendre le plus de variations possibles du signal. Dans ces conditions, la formule analytique (1.11) est remplacée par son équivalent discret (1.12). Sa résolution temporelle $\Delta t$ est identique à celle du signal $x(t)$.

$$C_{XX}(\tau_k) = \frac{1}{N_E - |k|} \sum_{i=0}^{N_E-1-|k|} x(t_i) \cdot y(t_i - \tau_k) \tag{1.12}$$

$$\text{avec :} \qquad k = -N_E + 1, \ldots, N_E - 1 \quad ; \quad \tau_k = k \cdot \Delta t$$

Cet outil d'analyse — l'autocorrélation — possède quelques propriétés importantes qui permettent d'avoir certaines informations sur le signal temporel $x(t)$. Parmi ces propriétés, elle admet un maximum global à l'origine $C_{XX}(0)$. Ce maximum correspond à l'énergie du signal $x(t)$. Un autre intérêt est donné par sa transformée de Fourier qui, d'après le théorème de Wiener-Khintchine, correspond à la densité spectrale de puissance de $x(t)$.

### 1.1.2.c Outils propres aux systèmes non linéaires chaotiques

Les outils d'analyse que nous avons vus jusqu'à présent sont utilisés pour caractériser tout type de signal. Intéressons-nous maintenant au cas particulier d'un signal issu d'un système chaotique, c'est-à-dire un système qui peut engendrer une multitude de régimes dynamiques différents. Les outils que nous allons présenter — les diagrammes de bifurcation et entropique — permettent de caractériser le système dynamique dans son ensemble. En d'autres termes, il est possible grâce à ces outils, d'avoir une vue globale d'un ensemble de comportements dynamiques différents. Il s'agit en réalité plus de méthode de représentation que d'outils d'analyse.

### Diagramme de bifurcation

Un système dynamique chaotique possède en général un certain nombre de paramètres qui influencent son comportement. Prenons comme exemple l'application logistique donnée par la relation (1.13), qui est un système dynamique à temps discret [17].

$$x_{n+1} = a \cdot x_n \left(1 - x_n\right) \quad ; \quad n = 0, 1, 2, \cdots \tag{1.13}$$

Le paramètre $a$ représente plus précisément le poids de la transformation non linéaire. En fonction de ce paramètre, l'application logistique va présenter différents régimes dynamiques (nous reviendrons sur ces régimes un peu plus loin). Il est donc intéressant de disposer d'une technique de représentation permettant d'appréhender le changement de comportement de l'application en fonction de ce paramètre. Cette technique est le diagramme de bifurcation comme illustré sur la figure 1.6.

Le tracé de ce diagramme consiste à porter sur l'axe des abscisses le paramètre $a$, dit paramètre de bifurcation, et sur l'axe des ordonnées l'ensemble des amplitudes de la variable dynamique $x$. Une troisième échelle en niveau de gris ou en couleur permet de coder la fonction de densité de probabilité de l'amplitude des ordonnées. Pratiquement, la méthode consiste à calculer les $N_H$ valeurs de la densité de probabilité approchée $P_k$ donnée par la formule (1.6), pour chacune des valeurs croissantes (ou décroissantes) du paramètre de bifurcation $a$.

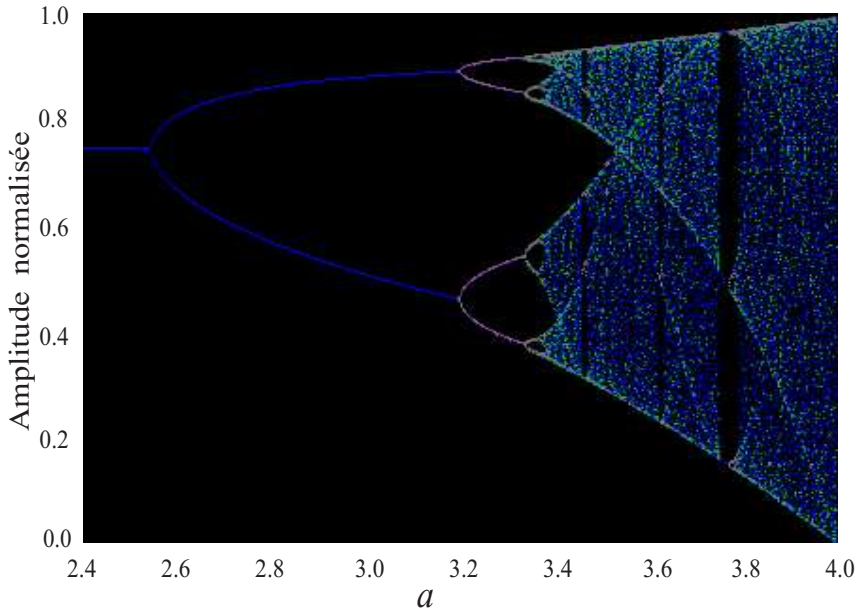



Figure 1.6 – *Diagramme de bifurcation de l'application logistique.*

Parmi les informations que l'on peut déduire d'un diagramme de bifurcation, on peut citer au moins deux exemples. Le premier est le type de comportement dynamique du système, pour une valeur donnée du paramètre de bifurcation. D'après le diagramme de la figure 1.6, le type point fixe stable, pour lequel le système n'évolue pas au cours du temps,

s'observe sur l'intervalle $[2,4\,;2,5]$ par exemple. À la valeur $a = 3,3$ le régime dynamique est périodique ($x_n$ oscille entre qutre valeurs). Pour $a = 4$, le système ne présente aucune périodicité apparente, la dynamique est du type chaotique.

Le deuxième exemple d'informations est le type d'enchaînement des régimes dynamiques lorsque le paramètre de bifurcation est augmenté. Ces enchaînements sont parfois appelés « *route vers le chaos* ». Dans le cas de l'application logistique décrite par l'équation (1.13), cette route est la cascade de dédoublements de période[5], comme on peut le déduire facilement de son diagramme de bifurcation.

### Diagramme entropique

Le diagramme de bifurcation, que nous venons de voir, est un outil bien adapté pour l'étude d'un système dynamique en fonction d'un seul paramètre. Mais lorsqu'il y a plus d'un paramètre de bifurcation, son exploitation devient difficile et peu pratique. Cependant, il est possible de représenter un ensemble de régimes dynamiques en fonction cette fois de deux paramètres, en utilisant l'entropie $E$ — relation (1.7) — à la place de la distribution de probabilité $P(x)$. Ce type de représentation est appelé le diagramme entropique, et il consiste à traduire le type de comportement dynamique par un niveau de gris ou de couleur relatif à la valeur de son entropie statistique.

Par exemple, un régime périodique se traduit par une faible entropie, et donc il sera un point gris clair sur un diagramme entropique. De la même façon, un régime chaotique, d'entropie élevée, est représenté par un gris foncé. Le diagramme entropique est une sorte de carte de comportements du système en question, dont on se sert pour associer un régime dynamique à un couple de paramètres.

Nous venons de décrire quelques outils que nous utiliserons plus loin pour l'analyse de notre système chaotique. Il existe bien sûr d'autres outils que nous n'avons pas décrits (comme l'information mutuelle moyenne, les exposants de Lyapunov, l'approximation linéaire locale, ...), outils intéressants, mais nous nous sommes contentés de décrire uniquement ceux qui ont été utilisés durant ces travaux. Cependant, avant d'utiliser ces outils, il faut d'abord pouvoir générer le signal chaotique à analyser. Nous allons donc, dans la section suivante, tenter d'exposer l'un des principes de génération d'un signal chaotique que nous mettrons en œuvre expérimentalement.

## 1.2 Génération de signal chaotique

Sans vouloir entrer dans beaucoup de détails théoriques, nous présentons dans cette section un principe général de génération d'un signal chaotique, puis la mise en équation du système qui le génère. Le système étudié ici est basé sur une structure générale très simple, qui est celle d'un oscillateur non linéaire à retard.

[5] D'autres routes typiques vers le chaos sont : l'intermittence, la quasi-périodicité $\cdots$ [5].

### 1.2.1 Principes

Les générateurs de chaos en temps continu peuvent être classés en trois catégories. Tout d'abord les oscillateurs non autonomes, qui sont excités par un signal externe, en général sinusoïdal. La sortie du circuit est le résultat d'une transformation dynamique non linéaire, c'est le signal chaotique. Un circuit RLC avec une diode pour remplir le rôle de l'élément non linéaire est un exemple classique de ce premier type d'oscillateur [18]. Le second type d'oscillateur est basé sur une dynamique non linéaire autonome à 3 variables [19], modélisé par une équation différentielle ordinaire (EDO). Ces oscillateurs sont fréquemment utilisés dans la littérature pour la réalisation de systèmes de codage par chaos [20]. La dimension de leur attracteur est assez faible (inférieur à 3) mais suffisante pour générer un signal chaotique. Les systèmes de Lorenz et de Rössler sont des exemples typiques de cette catégorie.

Enfin, le troisième type de dynamique chaotique est généré par des systèmes différentiels non linéaires à retard. C'est cette classe particulière d'oscillateurs qui nous intéresse, car le système de cryptographie qui fait l'objet du présent travail de thèse est basé sur un générateur de chaos appartenant à cette catégorie. Nous l'introduisons donc par une brève description de son schéma bloc schématisé sur la figure 1.7.

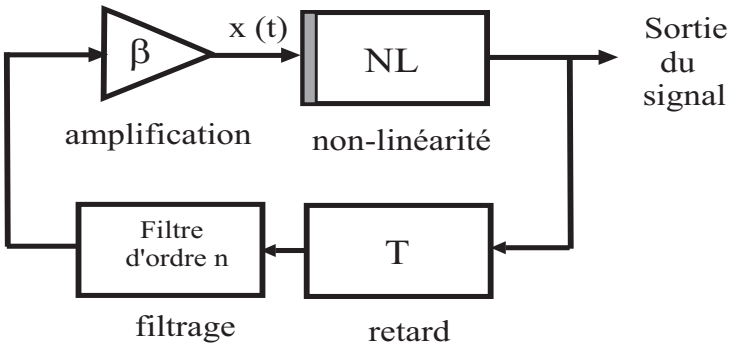



Figure 1.7 – *Schéma de principe d'un oscillateur non linéaire à retard.*

Ce schéma bloc d'un générateur de chaos auto-entretenu est composé de 4 éléments, dont chacun possède dans la boucle un rôle bien particulier. D'un point de vue générique, on peut décrire la fonction de chacun de ces éléments par :

1. La non linéarité représente le seul élément non linéaire dans la boucle de contre-réaction. Elle sera présentée plus en détails par la suite.

2. Le retard temporel pur $T$ est caractéristique de ce type de système. Les différentes réalisations pratiques de cette fonction dépendent du contexte expérimental. Pour ne citer qu'un exemple dans le domaine optique, des longueurs de fibres optiques sont couramment utilisées.

3. La boucle de contre-réaction comprend un élément amplificateur dont le gain global normalisé est appelé $\beta$. Ce gain souvent utilisé comme paramètre de bifurcation,

permet de modifier le comportement dynamique du système, et en général un régime chaotique correspond à un gain élevé.

4. Un filtre limitant la dynamique non linéaire à retard du système. Le choix du type de filtre déterminera la bande passante du système, ainsi que l'ordre de l'équation différentielle permettant la modélisation du fonctionnement du générateur de chaos.

Nous venons de décrire un schéma bloc d'un oscillateur non linéaire à retard, d'apparence simple, mais capable de générer des comportements dynamiques très complexes. Ce synoptique met en évidence les paramètres qu'il est nécessaire de connaître pour pouvoir analyser correctement la multitude de comportements dynamiques engendrés. Nous allons maintenant procéder à sa mise en équation afin de l'étudier théoriquement et de le simuler numériquement.

### 1.2.2 Modélisation

Comme dans tout système physique, le temps de réaction du système générateur de chaos n'est pas infiniment court. C'est le filtre linéaire utilisé dans la boucle de contre réaction qui définit la dynamique du système.

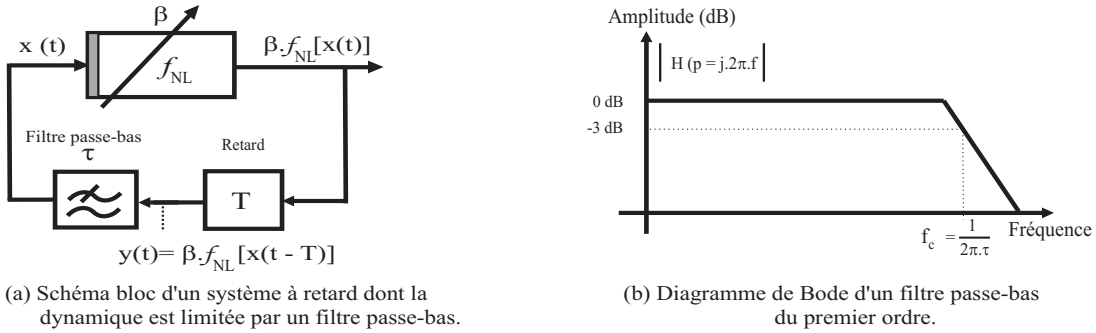
En effet, si on suppose que ce temps de réaction est nul, cela signifie que la transition entre l'entrée et la sortie est infiniment rapide. Dans ce cas, le système se réduit à une itération non linéaire du type *application discrète* $x_{n+1} = f[x_n]$, où $x_{n+1}$ représente l'état futur du système à l'instant discret $n+1$. Un tel modèle a été étudié par R. May pour l'observation de l'évolution d'une population animale dans un contexte proie-prédateur, dans le cas d'une fonction $f[x]$ parabolique [17]. Cependant, dans une configuration réaliste, aucun système physique basé sur une boucle de contre réaction ne possède un temps de réponse nul.

En tenant compte du temps de réaction du système, ceci revient à faire intervenir dans la boucle de contre réaction un filtre, dont la constante de temps correspond au temps de réponse. Suivant le type de filtrage effectué, l'évolution chaotique aura des caractéristiques différentes. Nous allons donc établir le modèle du système pour deux types de filtres différents : un filtre passe-bas et un filtre passe-bande.

#### a. Filtre passe-bas

Un filtre passe-bas dont le diagramme de Bode est représenté sur la figure 1.8b ne laisse passer que les basses fréquences, et atténue les hautes fréquences associées à des oscillations très rapides du signal généré dans la boucle. Ce type de filtre est caractérisé par une constante de temps rapide $\tau$ qui indique, dans la boucle de contre réaction, une durée minimum nécessaire au système pour effectuer une transition. Le paramètre $\tau$ est remplacé lors d'une analyse harmonique par la *fréquence de coupure* ($f_c = 1/2\pi.\tau$)

pour caractériser la limitation dynamique. Tant que la fréquence du signal d'entrée est petite devant $f_c$, le filtre est utilisé à l'intérieur de sa bande passante et la sortie recopie l'entrée, sinon les amplitudes de la sortie sont atténuées d'autant plus qu'on s'éloigne de la *fréquence de coupure*.




(a) Schéma bloc d'un système à retard dont la dynamique est limitée par un filtre passe-bas.

(b) Diagramme de Bode d'un filtre passe-bas du premier ordre.

FIGURE 1.8 – *Dynamique non linéaire limitée par un filtre passe-bas.*

Selon le schéma bloc de la figure 1.8a, où on a séparé les effets non linéaires et les effets dynamiques pour des besoins de modélisation, la loi d'évolution temporelle de la variable $x(t)$ est une dynamique du premier ordre exprimée dans le domaine de Laplace. En effet, la fonction de transfert de Laplace $H(p)$ d'un filtre passe-bas est donnée par :

$$H(p) = \frac{X(p)}{Y(p)} = \frac{1}{1 + \tau \cdot p} \tag{1.14}$$

La dynamique se met alors en équation par passage du domaine de Laplace au domaine temporel, ce qui donne l'*équation différentielle du premier ordre* suivante :

$$x(t) + \tau \cdot \frac{dx}{dt}(t) = y(t) \tag{1.15}$$

Cependant, à travers la boucle du système, la sortie du filtre passe-bas est rebouclée sur son entrée en subissant une transformation non linéaire, une amplification et un retard dans le temps, ce qui se traduit par l'égalité $y(t) = \beta.f_{NL}\,[x(t-T)]$. En remplaçant cette expression de $y(t)$ dans l'équation (1.15), on obtient une « ***équation différentielle du premier ordre à retard*** » (EDR du premier ordre) suivante :

$$x(t) + \tau.\frac{dx}{dt}(t) = \beta.f_{NL}\,[x(t-T)] \tag{1.16}$$

La dénomination mathématique exacte de l'équation (1.16) est : *équation différentielle non linéaire à différence*[6]. Cette équation n'a aucune solution analytique à notre

[6]En anglais : *non linear difference differential equation.*

connaissance, car certaines de ces solutions sont chaotiques et par essence ne peuvent être exprimées analytiquement.

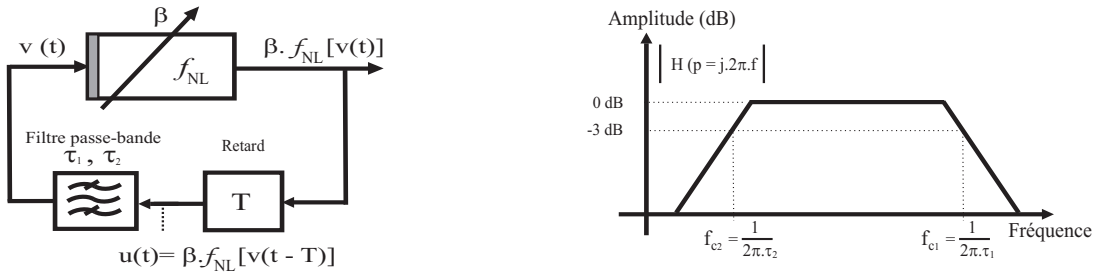
La loi d'évolution temporelle de la variable $x(t)$ est une dynamique du premier ordre avec un terme à retard. Le premier ordre signifie que seule la dérivée première du temps intervient ; il correspond physiquement à un terme de dissipation d'énergie (frottement, effet Joule, ou système non conservatif). Le terme à retard est d'une importance capitale, il permet de distinguer en premier lieu un système générateur de chaos d'un simple système bistable, et la présence du retard temporel dans la boucle de contre-réaction modifie complètement le comportement dynamique de l'ensemble.

En effet, alors que le bistable du premier ordre ne peut présenter que des solutions du type point fixe attractif ou répulsif, la présence du retard, s'il est suffisamment important par rapport à la constante de temps ($T \gg \tau$), permet d'augmenter considérablement le nombre de degrés de liberté du système, et par là le nombre de comportements dynamiques possibles. Signalons au passage, que la condition ($T \gg \tau$) n'est pas obligatoire pour que le système génère une dynamique chaotique ; il peut atteindre ces régimes même lorsque ($\tau \geq T$) à condition que le gain de la boucle soit suffisamment important [21,22].

Cependant, on peut comprendre que l'évolution du signal $x(t)$ généré dépend — en plus de l'état initial de ce système — de chacun des paramètres : $f_{NL}$, $T$, $\beta$ et $\tau$. Nous reviendrons sur ce point un peu plus loin dans le cadre de la modélisation d'un générateur de chaos dont la dynamique est limitée par un filtre passe-bande.

### b. Filtre passe-bande

Un schéma de principe d'un diagramme de Bode d'un filtre passe-bande est illustré sur la figure 1.9b. C'est un filtre ne laissant passer qu'un intervalle de fréquences compris entre la *fréquence de coupure haute* $f_{c1}$ et la *fréquence de coupure basse* $f_{c2}$. Sa bande passante est l'intervalle de fréquences $[f_{c1}, f_{c2}]$ qui correspond aux fréquences telles que le le module de la fonction de transfert soit supérieur à 3 dB en dessous du maximum (dans le cas de la figure 1.9b, le maximum est 0 dB).




(a) Schéma bloc d'un système à retard dont la dynamique est limitée par un filtre passe-bande.

(b) Diagramme de Bode d'un filtre passe-bande du second ordre.

Figure 1.9 – *Dynamique non linéaire limitée par un filtre passe-bande.*

A noter qu'un filtre passe-bande peut être vu comme la cascade de deux filtres : un passe-bas et un passe-haut. La fréquence $f_{c1}$ caractérise le filtre passe-bas, et la fréquence $f_{c2}$ caractérise le filtre passe-haut. Cette remarque nous sera utile par la suite lorsque nous aborderons la mise en équations du système, mais d'abord intéressons nous à la modélisation d'un filtre passe-bande tel qu'il est schématisé sur la figure 1.9b.

Chaque filtre passe-bande est caractérisé par deux constantes de temps $\tau_1$ et $\tau_2$ qui représentent les temps de réponse finis du filtre. Elles sont reliées directement aux *fréquences de coupures* $f_{c1}$ et $f_{c2}$ du filtre, leur expression est donnée par :

$$\tau_{1,2} = \frac{1}{2\pi.f_{c1,2}} \tag{1.17}$$

C'est à partir de la fonction de transfert du filtre passe-bande que nous arrivons à modéliser un système à retard utilisant un tel filtre pour limiter sa dynamique. Le principe déjà étudié précédemment pour déterminer la loi d'évolution dynamique d'un oscillateur utilisant un filtre passe-bas reste donc le même. En effet, la fonction de transfert $H(p)$ d'un filtre passe-bande dans le domaine de Laplace est donnée par l'équation suivante :

$$H(p) = \frac{V(p)}{U(p)} = \frac{\tau_2 \cdot p}{(1+\tau_2 \cdot p)(1+\tau_1 \cdot p)} \tag{1.18}$$

avec $V(p)$ la tension de sortie et $U(p)$ la tension d'entrée aux bornes du filtre. La mise en équation du système se fait tout simplement par le retour au domaine temporel de l'équation (1.18) *via* une *transformée de Laplace inverse* $\{L^{-1}\}$. L'équation obtenue est une *équation différentielle du second ordre*, dont l'expression est donnée par :

$$v(t) + [\tau_1 + \tau_2]\frac{dv}{dt}(t) + \tau_1 \cdot \tau_2 \frac{d^2v}{dt^2}(t) = \tau_2 \cdot \frac{du}{dt}(t) \tag{1.19}$$

D'après le schéma-bloc de la figure 1.9a, la sortie du filtre est rebouclée à son entrée. Ce qui se traduit analytiquement dans ce cas par l'égalité : $u(t) = \beta.f_{NL}\left[v(t-T)\right]$. À partir de cette égalité, on peut déduire la dérivée première $(du/dt)$ du second terme de l'équation différentielle (1.19). Son expression est donnée par l'équation suivante :

$$\frac{du}{dt}(t) = \beta.\frac{d}{dt}\Big[f_{NL}\left[v(t-T)\right]\Big] \tag{1.20}$$

Ainsi, la modélisation du système à retard dont la dynamique est limitée par un filtre passe-bande est obtenue en remplaçant l'expression du terme $(du/dt)$, donnée par (1.20), dans l'équation (1.19). Celle-ci est décrite alors par :

$$v(t) + [\tau_1 + \tau_2]\frac{dv}{dt}(t) + \tau_1 \cdot \tau_2 \cdot \frac{d^2v}{dt^2}(t) = \beta \cdot \tau_2 \cdot \frac{d}{dt}\Big[f_{NL}\left[v(t-T)\right]\Big] \tag{1.21}$$

La présence du terme de la dérivée seconde de la variable dynamique par rapport au temps nous a permis de classer l'EDR (1.21) du second ordre. Toutefois, un changement de variables approprié permet toujours de passer d'une équation différentielle d'ordre $n$ à un système de $n$ équations différentielles du premier ordre, et vice-versa. Ainsi, par soucis de simplicité, nous allons réécrire l'équation (1.21) sous forme d'un système de deux EDR du premier ordre. Cette approche sera utilisée lorsque nous aborderons la résolution numérique des équations régissants la dynamique de notre système.

### c. Passage d'une EDR du second ordre à un système de deux EDR du premier ordre

La démarche à suivre est simple. En effet, nous avons déjà signalé précédemment qu'un filtre passe-bande, qui définit la dynamique du système, peut être réalisé par la mise en cascade de deux filtres : un passe-bas et un passe-haut. Le principe de réalisation est illustré sur la figure 1.10 en supposant que la dynamique pour chacun d'eux est du premier ordre. Un simple arrangement de la fonction de transfert du filtre passe-bande, donnée par l'équation (1.18), nous permet d'exprimer celle-ci, dans le domaine de Laplace, par le produit des deux fonctions de transfert de chacun des deux filtres passe-bas et passe-haut.

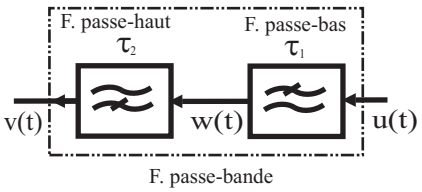



Figure 1.10 – *Filtre passe-bande.*

Pour exprimer ce que cela signifie mathématiquement, nous introduisons ici une nouvelle variable $W(p)$, dans le domaine de Laplace, qui représente simultanément la sortie du filtre passe-bas et l'entrée du filtre passe-haut (figure 1.10). On obtient alors une nouvelle réécriture de l'équation (1.18) sous la forme :

$$V(p) = \underbrace{\left(\frac{\tau_2 p}{1+\tau_2 p}\right)}_{p.\,haut} . \underbrace{\left(\frac{1}{1+\tau_1 p}\right)}_{p.\,bas} \cdot U(p) = \left(\frac{\tau_2 p}{1+\tau_2 p}\right) \cdot W(p) \tag{1.22}$$

À partir de (1.22), le système à deux équations (1.23) est déduit aisément.

$$\begin{cases} V(p) = \dfrac{\tau_2 p}{1+\tau_2 p} \cdot W(p) \\ W(p) = \dfrac{1}{1+\tau_1 p} \cdot U(p) \end{cases} \tag{1.23}$$

Par le moyen de la $\{L^{-1}\}$, on fait passer le système d'équations (1.23) dans le domaine temporel. On obtient alors — système (1.24) — deux équations différentielles du premier ordre, en fonction de 3 variables $v$, $w$ et $u$.

$$\begin{cases} v(t) + \tau_2 \cdot \dfrac{dv}{dt}(t) \ = \tau_2 \dfrac{dw}{dt}(t) \\ w(t) + \tau_1 \cdot \dfrac{dw}{dt}(t) = u(t) \end{cases} \tag{1.24}$$

Maintenant, en remplaçant la variable $u(t)$ par son expression $u(t) = \beta \cdot f_{NL}\left[v(t-T)\right]$ ; le système d'équations (1.24) est ramené au système (1.25). Ce dernier est finalement un *système de deux EDR du premier ordre.*

$$\begin{cases} v(t) + \tau_2 \cdot \dfrac{dv}{dt}(t) \ = \dfrac{\tau_2}{\tau_1} \cdot \Big[\beta \cdot f_{NL}\left[v(t-T)\right] - w(t)\Big] \\ w(t) + \tau_1 \cdot \dfrac{dw}{dt}(t) = \beta \cdot f_{NL}\left[v(t-T)\right] \end{cases} \tag{1.25}$$

Le système d'équations (1.25) nous servira ultérieurement comme base de modélisation. Il a l'avantage d'être maniable par rapport à sa résolution numérique. De façon concrète, il est plus facile de manipuler numériquement des équations différentielles du premier ordre que celles du second ordre, avec en plus les spécificités particulières de leurs termes à retard.

La description qui vient d'être faite sera appliquée lorsque nous aborderons notre générateur de chaos expérimental, et plus particulièrement sa mise en équations, où on a utilisé uniquement des filtres passe-bande pour limiter les dynamiques chaotiques.

Après avoir décrit ces systèmes à retard en terme de modélisations, nous allons présenter dans la section suivante quelques méthodes d'intégration numérique, couramment utilisées, qui permettent de simuler ces systèmes. Nous justifions ensuite le choix de la méthode d'intégration retenue pour résoudre les EDRs décrivant le générateur de chaos proposé.

## 1.3 Méthodes de résolutions numériques

Les méthodes d'intégration numérique des équations différentielles peuvent être classées en deux types : les méthodes explicites et les méthodes implicites [23]. Une méthode est dite « *explicite* » si la valeur $x_{i+1}$ peut être calculée directement à l'aide des valeurs précédentes $x_i$ (ou d'une partie d'entre elles). Une méthode est dite « *implicite* » si la valeur $x_{i+1}$ n'est définie que par une relation implicite fonction de $x_i$.

Généralement, la connaissance des conditions initiales est nécessaire pour rechercher la solution d'une EDO, c'est ce qu'on appelle communément le problème de Cauchy, ou encore tout simplement problème aux valeurs initiales. Il suffit de connaître $x(0)$ et $\dot{x}(0)$ pour trouver les solutions d'une EDO du second ordre par exemple.

Cependant, la présence du terme retardé d'une durée égale au retard temporel $T$ dans les EDRs, implique qu'une condition initiale particulière appartient à l'ensemble des valeurs définies sur l'intervalle de temps $[0\,,\,T]$ [24]. La taille de chacune de ces conditions initiales dans ce cas est infinie. En d'autres termes, la détermination de la solution exacte d'une EDR est liée à la connaissance d'un nombre infini de valeurs ; c'est ce qui est intéressant pour nous car certaines de ces solutions sont chaotiques, et elles ne peuvent être retrouvées par simple connaissance du modèle décrivant le système de cryptographie proposé. Nous allons donc présenter dans les paragraphes suivants deux méthodes d'intégrations explicites — Euler et Runge-Kutta — et une méthode implicite, celle du prédicteur-correcteur.

### 1.3.1 Méthode d'Euler

C'est la plus simple et traditionnellement la méthode la plus utilisée pour trouver une solution approchée d'une équation différentielle. Mais d'abord considérons la forme générale (1.26) de cette équation, qui sera également utilisée pour expliquer les autres méthodes de résolutions numériques.

$$\frac{dx}{dt}(t) = F(x,t) \tag{1.26}$$

L'approximation numérique s'effectue par un développement de Taylor à l'ordre 1 du terme dérivée première de l'équation (1.26) :

$$\frac{dx}{dt}(t) = \lim_{h \longrightarrow 0} \frac{x(t+h) - x(t)}{h} = F(x,t)$$

où $h$ est le pas d'échantillonnage de la méthode. En discrétisant la variable temporelle ($t = h.i$ ; $i = 0,\ 1,\ 2,\ \ldots$ entier), on obtient donc la relation de récurrence suivante :

$$x_{i+1} = x_i + h\ .\ F(x_i, t_i) + O(h^2) \tag{1.27}$$

Les termes d'ordre 2 sont négligés, et donc la formule est d'ordre 1. À titre indicatif, le calcul de $N$ premiers échantillons s'effectue de la manière suivante :

$$\begin{aligned} x_1 &= x_0 + h\ .\ F(x_0, t_0) \\ x_2 &= x_1 + h\ .\ F(x_1, t_1) \\ \ldots &= \ldots\ldots\ldots\ldots \\ x_N &= x_{N-1} + h\ .\ F(x_{N-1}, t_{N-1}) \end{aligned}$$

Cette méthode utilise un pas d'intégration constant, et converge très mal [25]. L'erreur de rapprochement de la solution exacte est due principalement, en plus des erreurs de troncature inhérente à tous les calculs informatiques, à l'erreur d'intégration. Celle-ci est de l'ordre du pas d'échantillonnage au carré, et par conséquent $h$ devra être pris suffisamment petit afin de la réduire. L'avantage majeur de cette méthode est sa rapidité d'exécution, car elle demande relativement peu d'opérations de calculs.

### 1.3.2 Méthode de Runge-Kutta d'ordre 4

L'algorithme de Runge-Kutta utilise plusieurs points intermédiaires pour calculer la valeur de $x_{i+1}$ à partir de la valeur de $x_i$. Cette méthode est dite d'ordre 4 car elle est basée sur un développement de Taylor à l'ordre 4, suivie d'une moyenne pondérée sur toutes les estimations de $x_{i+1}$ ainsi réalisées. L'expression liant $x_{i+1}$ et $x_i$ est donnée par l'équation suivante :

$$x_{i+1} = x_i + \frac{h}{6} \cdot (k_1 + 2 \cdot k_2 + 2 \cdot k_3 + k_4) + O(h^5) \tag{1.28}$$

avec :

$$k_1 = F(x_i, t_i) \tag{1.29}$$

$$k_2 = F(x_i + \frac{h}{2} \cdot k_1,\ t_i + \frac{h}{2}) \tag{1.30}$$

$$k_3 = F(x_i + \frac{h}{2} \cdot k_2,\ t_i + \frac{h}{2}) \tag{1.31}$$

$$k_4 = F(x_i + h \cdot k_3,\ t_i + h) \tag{1.32}$$

Cette méthode est à pas constant, très utilisée pour réaliser les intégrations numériques. Elle a le principal avantage d'avoir une précision en $h^4$, et converge rapidement. Néanmoins, elle reste assez coûteuse en temps de calcul car, elle nécessite d'évaluer de manière itérative 4 fois la fonction $F$. On note aussi un autre inconvénient de cette méthode, c'est son inefficacité pour certains types d'équations différentielles comme les systèmes d'équations « *raides*[7] ».

La raideur signifie qu'une des variables évolue incomparablement plus vite qu'une autre [26]. Ce problème se pose principalement lorsque le phénomène physique est décrit par *un système d'équations différentielles*, où plusieurs constantes de temps caractéristiques sont très différentes. Un exemple physique de ce type de problème raide est le système d'équations (1.25) modélisant un système à retard, lorsque la bande passante du filtre passe-bande est très large. Les constantes de temps $\tau_1$ et $\tau_2$ sont dans ce cas très différentes, et elles vont faire décroître plus ou moins rapidement les différentes composantes du système. Prenons un exemple simple pour illustrer ce problème d'équations raides. Il est tiré de la référence [27] que l'on peut présenter de la façon suivante :

Soit un système physique dont le comportement est décrit par le système d'équations différentielles suivant :

$$\begin{cases} \dfrac{dx}{dt}(t) = -x(t) + 95\ y(t) \\ \dfrac{dy}{dt}(t) = -x(t) - 97\ y(t) \end{cases} \tag{1.33}$$

avec les conditions initiales $x_0 = 1$ et $y_0 = 1$, les solutions exactes de ce système d'équations sont les suivantes :

[7] dites *stiff* en anglais.

$$\begin{cases} x(t) = \dfrac{1}{47}\Big[95\ \exp(-2\,t) - 48\ \exp(-96\,t)\Big] \\ y(t) = \dfrac{1}{47}\Big[-\ \exp(-2\,t) + 48\ \exp(-96\,t)\Big] \end{cases} \tag{1.34}$$

On peut remarquer – solutions exactes (1.34) – qu'il existe un facteur $48 = 96/2$ entre les deux constantes de temps des solutions $x(t)$ ou de $y(t)$. Autrement dit, il y a deux échelles de temps données par les exponentielles dans chaque solution.

Une intégration numérique du système (1.33) par la méthode explicite de Runge-Kutta, va nécessiter d'utiliser un pas d'échantillonnage très petit devant la constante de temps rapide du système ($h \ll 1/96$), pour que la méthode soit stable. La figure 1.11 représente les courbes des solutions obtenues après intégration numérique. On constate que, dans le même intervalle de temps d'intégration $[0, 2]$, la solution $y(t)$ décroit d'une façon extrêmement rapide par rapport à la solution $x(t)$.

L'influence de la raideur peut être illustrée par exemple sur la figure 1.11a de la manière suivante : au début de l'axe des abscisses (échelle temporelle), la " pente " est grande, ceci étant lié au fait que le facteur multiplicatif du terme $\{\exp(-96\,t)\}$ est grand, autrement dit la variable $x(t)$ varie vite, puis, quand le temps devient grand, la variable varie plus lentement. Là est la variété des échelles de temps (les dynamiques représentées par ce systèmes sont à la fois très lentes et très rapides).

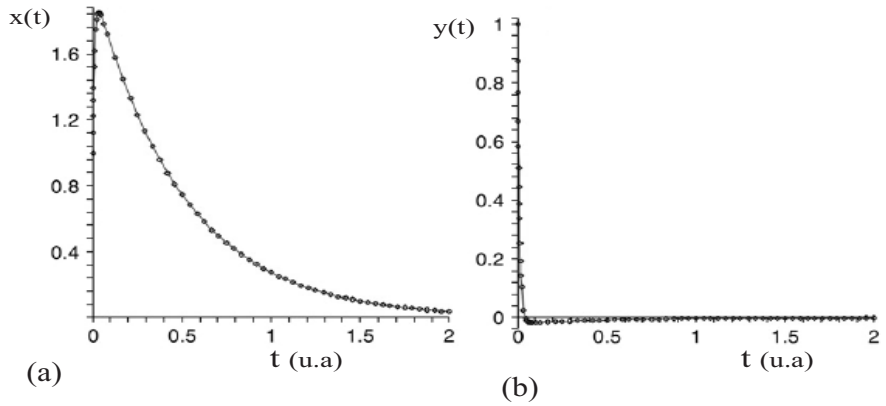



Figure 1.11 – *Exemple de solution d'une équation différentielle raide* [27].

Néanmoins, ces équations raides peuvent être résolues de manière précise par les méthodes d'intégration implicites. Ce sont des méthodes à pas multiples comme la méthode d'Adams-Moulton (*backward Adams method*) ou la méthode du prédicteur-correcteur. En effet, pour calculer une approximation de l'échantillon $x_{i+1}$, la méthode de Runge-Kutta n'utilise pas les échantillons obtenus antérieurs à $x_i$. Les méthodes multi-pas, au contraire, vont systématiquement utiliser ces échantillons. Dans le paragraphe suivant, nous présentons seulement la méthode du prédicteur-correcteur, car elle sera l'unique méthode implicite utilisée par la suite.

### 1.3.3 Méthode de prédicteur-correcteur

Cette méthode est appelée aussi méthode à multiples valeurs, c'est-à-dire la valeur de $x_{i+1}$ est donnée en fonction de $x_{i-1}, x_{i-2}, \ldots, x_{i-p}$, ou $p$ est un entier. L'ordre de la méthode est déterminé par le nombre de valeurs antérieures utilisées ($n = p + 1$). L'algorithme de la méthode est basé sur le principe d'une valeur prédite $x_{i+1}^{(p)}$, qui est estimée proche de la valeur finale $x_{i+1}$, et évaluée par un schéma de prédicteur d'ordre $n$, puis corrigée par l'algorithme du correcteur du même ordre $n$.

Le fait de prédire une valeur puis de l'introduire dans l'algorithme juste pour la corriger, permet de réduire le temps de calcul de la valeur approchée, et par conséquent de réduire considérablement l'erreur de troncature due aux calculs informatiques. Cette méthode procure une meilleure précision pour un coût en temps de calcul réduit, particulièrement lorsqu'une bonne donnée initiale $x_{i+1}^{(0)}$ est fournie.

**Prédicteur :** Les termes d'ordre 5 sont négligés, donc à l'ordre 4, le *prédicteur* est obtenu grâce au schéma d'intégration d'Adams-Bashforth, appelé aussi méthode d'Adams ouverte suivant :

$$x_{i+1}^{(p)} = x_i + \frac{h}{24}\Big[55F(x_i,t_i) - 59F(x_{i-1},t_{i-1}) + 37F(x_{i-2},t_{i-2}) - 9F(x_{i-3},t_{i-3})\Big] \quad (1.35)$$

**Correcteur :** Le *correcteur* est obtenu à partir de la formule d'Adams-Moulton, appelé aussi méthode d'Adams fermée au 4ème ordre, donné par :

$$x_{i+1}^{(p+1)} = x_i + \frac{h}{24}\Big[9F(x_{i+1}^{(p)},t_{i+1}) + 19F(x_i,t_i) - 5F(x_{i-1},t_{i-1}) + F(x_{i-2},t_{i-2})\Big] \quad (1.36)$$

On note que le calcul de la première valeur approchée par cette méthode va nécessiter la connaissance de trois valeurs antérieures à celle-ci (en plus de la CI : $x_0$), donc un procédé d'initialisation du calcul doit être effectué pour amorcer l'algorithme du prédicteur-correcteur. Ces trois premières valeurs $x_1$, $x_2$ et $x_3$ sont calculées, dans notre cas, par la méthode de Runge-Kutta d'ordre 4.

Par rapport aux travaux de la présente thèse, de part la précision et son adaptation aux équations raides, la méthode du prédicteur-correcteur sera l'unique méthode employée pour trouver les solutions des EDR, décrivant les dynamiques chaotiques de notre système cryptographique. Comme signalé aussi précédemment, la méthode de Runge-Kutta d'ordre 4 sera seulement utilisée pour initialiser le procédé de calcul du prédicteur-correcteur. Les résultats obtenus seront exploités au moyen de plusieurs types de représentation comme les séries temporelles, les diagrammes de bifurcations ou encore les diagrammes entropiques.

Après avoir décrit ces systèmes à retard en terme de modélisations, puis présenté les méthodes numériques permettant de les simuler, nous allons maintenant illustrer ces dynamiques par des exemples physiques déjà étudiés dans la littérature.

## 1.4 Exemples de système d'Ikeda

Les systèmes différentiels non linéaires à retard ont commencé à être étudiés au début des années 80. C'est exactement en 1979, que le premier modèle dynamique en optique, contenant un retard temporel et une constante de temps, a été proposé par Kensuke Ikeda [28]. Son modèle est aujourd'hui appelé *système d'Ikeda*. Ce système repose sur une EDR du premier ordre, comme celle qui est donnée dans le cas général, par l'équation (1.16) d'une dynamique non linéaire limitée par un filtre passe-bas.

La figure 1.12 montre le dispositif expérimental utilisé par Ikeda. IL est constitué de 4 miroirs permettant le piégeage de la lumière dans une cavité en anneau. Le temps de parcours de cette cavité par la lumière définit le retard $t_D$ du système dynamique. Deux des 4 miroirs possèdent une réflectivité totale (100 %), et les deux autres ont des coefficients de réflexion inférieurs pour permettre, d'un côté d'exciter la cavité par un faisceau laser d'intensité constante, et de l'autre l'extraction d'une partie du faisceau fluctuant en intensité dans la cavité. À l'intérieur de la cavité se trouve un milieu optique non linéaire (une cellule absorbante à deux niveaux atomiques), qui transforme le champs électrique entrant en un champs sortant atténué et déphasé ; cette transformation est en fonction du niveau de l'intensité en entrée.

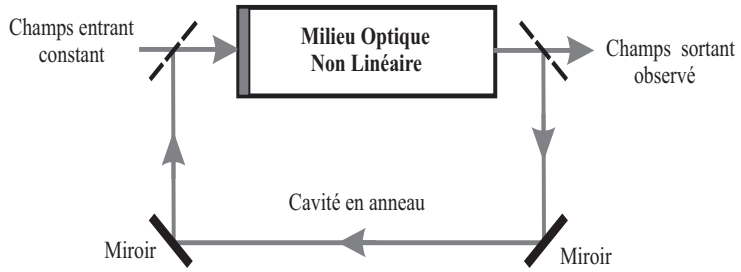



Figure 1.12 – *Schéma expérimental du modèle d'Ikeda.*

La modélisation est obtenue à partir de l'intégration des équations Maxwell-Bloch dans le milieu absorbant. Le résultat aboutit à une EDR du premier ordre, dite « *équation d'Ikeda* », dont l'expression réduite est la suivante [29] :

$$\tau \cdot \frac{d\phi}{dt}(t) = -\phi + A^2\Big[1 + 2B\cos\left[\phi(t - t_D) - \phi_0\right]\Big] \tag{1.37}$$

où $A$ est un paramètre proportionnel à la lumière incidente, $B$ caractérise la dissipation du champ électrique dans la cavité, $\phi(t)$ la variable dynamique correspondant à la phase optique, et $\phi_0$ un offset de phase.

La constante de temps du système correspond à la durée de vie des niveaux. Elle doit être suffisamment inférieure au retard temporel pour obtenir *l'instabilité d'Ikeda*. Cette condition ($\tau \ll t_D$) permet de réduire l'équation (1.37), dans le cadre d'une approximation dite « *adiabatique* », à un modèle discret itératif. Cependant, la validité de cette approximation, qui signifie que le terme différentiel de l'équation (1.37) est négligé, est limitée aux régimes dynamiques de faible complexité.

En tenant compte de la constante de temps, divers comportements de stabilité, multistabilité et instabilité de l'intensité en sortie ont été étudiés. Théoriquement, Ikeda a démontré certains comportements dynamiques dont le chaos. Expérimentalement, ses collègues H. Nakatsuka *et al.* ont utilisé une cavité en anneau, excitée par des impulsions optiques, pour engendrer un déphasage par effet non linéaire [30].

Sur la base du modèle d'équation d'Ikeda, d'autres montages expérimentaux ont été réalisés par d'autres chercheurs. Sans donner ni trop de détails ni une liste exhaustive, on peut citer quelques publications et références choisies par l'ordre chronologiques suivant :

- Avril 1982, un montage optique a été présenté par F. Hopf *et al.* [21] pour le chaos en intensité. Le montage est basé sur un schéma bistable hybride opto-électronique à retard. En effet, la boucle d'oscillation chaotique est composée d'un modulateur électro-optique massif, constitué par un cristal KDP[8] entre deux polariseurs croisés, qui sert d'élément non linéaire, et d'un système électronique. Le retard temporel est réalisée par une ligne à retard numérique (une mémoire FIFO[9]). Les auteurs ont particulièrement étudié les bifurcations successives par dédoublement et les conditions d'apparition d'harmoniques impairs [31].

- Décembre 1982, un autre montage est présenté par A. Neyer et E. Voges. C'est le premier système expérimental utilisant un composant optique intégré. Leur système se base sur l'utilisation *d'un modulateur électro-optique intégré de Mach-Zehnder* (nous reviendrons sur les caractéristiques de ce composant par la suite). Un câble coaxial de longueur 200 $m$ est utilisé pour avoir un retard temporel de 1 $\mu s$. A cause de l'utilisation de composants rapides, l'hypothèse adiabatique a été utilisée dans l'analyse théorique de ce montage [32].

- Avril 1985, un système acousto-optique est réalisé par R. Vallée et C. Delisle. La fonction retard temporel a été réalisée par l'introduction d'une fibre optique dans la boucle du système (10 $\mu s$ pour 2 $km$ de fibre). La démonstration expérimentale de l'importance du retard, par rapport à la dynamique générée, a été étudiée pour plusieurs valeurs du retard temporel [33].

- Août 1995, P. Celka a réalisé un montage électro-optique dont la structure se ressemble à celle réaliser par F. Hopf *et al.* Mais au lieu d'utiliser un cristal KDP, Celka a utilisé *un interféromètre Mach-Zehnder intégré sur niobate de lithium.* Un ordinateur contrôle un générateur de tension et génère un retard temporel. Pour plus de détails, nous invitons le lecteur à consulter la référence de son auteur [34].

- Avril 1998, le premier générateur de *chaos en longueur d'onde* basé sur l'équation d'Ikeda est réalisé par L. Larger (le dispositif expérimental complet de ce générateur sera décrit ultérieurement ; il a concrètement inspiré le sujet traité par la présente thèse). L'utilisation d'un laser DBR[10] accordable à l'intérieur de la boucle d'oscillation a permis de générer une dynamique chaotique de la longueur d'onde [35].

[8] Potassium Dihydrogène Phosphate.
[9] First In First Out.
[10] En anglais, Distributed Bragg Reflector.

En un tour d'horizon rapide loin d'être complet, on peut citer encore d'autres expériences qui existent dans la littérature, et qui portent sur l'étude des dynamiques non linéaires à retard. Par exemple les dynamiques basées sur un interféromètre de Fabry-Pérot [36, 37], sur les lasers semi-conducteurs [38–44], sur *le chaos en état de polarisation* d'un laser [45–48], ou encore tout récemment par des composants photoniques intégrés [49, 50].

Dans la majorité des systèmes dynamiques à retard que nous venons de citer, c'est l'intensité du laser qui joue le rôle de variable dynamique, excepté pour *le chaos sur l'état de polarisation* ou *en longueur d'onde*. Particulièrement, le dispositif expérimental utilisant cette dernière variable dynamique — *longueur d'onde* — a été étudié et réalisé pour la première fois au Laboratoire d'Optique Pierre-Michel Duffieux (LOPMD) de Besançon, le laboratoire[11] dans lequel les travaux de la présente thèse se sont déroulés. Depuis que ce générateur a fait ses preuves dans le cadre de la sécurisation de l'information [51], d'autres variables dynamiques ont été explorées, toujours dans le même objectif, à des fins de cryptographie par chaos. Ces variables sont : l'intensité optique [52, 53], le retard optique [54–56], la fréquence [57, 58] et la phase optique [59–62]. De tous ces systèmes à retard, nous avons choisi de présenter dans la partie suivante deux exemples, chacun utilisant une variable dynamique différente (longueur d'onde et intensité optique), et un filtrage différent (passe-bas et passe-bande).

### a. Chaos en longueur d'onde

L'étude des systèmes dynamiques générant du chaos en longueur d'onde ont commencé au laboratoire LOPMD à la fin des années 80 [63, 64]. À la suite de ces travaux, un montage amélioré utilisant un laser à réseau de Bragg distribué (DBR) accordable a été réalisé [35,65]. Le montage expérimental du générateur de chaos en longueur d'onde a été

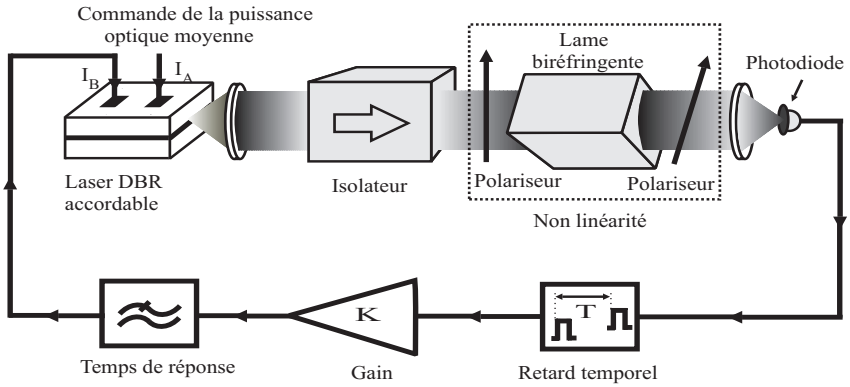



Figure 1.13 – *Générateur de chaos en longueur d'onde.*

[11] Il s'appelle actuellement : Département d'Optique de l'institut FEMTO-ST (Franche-Comté Electronique Mécanique Thermique et Optique - Sciences et Technologies).

réalisé dans sa version originale par Laurent Larger dans le cadre de sa thèse [13]. Par la suite, des études complémentaires ont été effectuées par Jean-Baptiste Cuenot [6] et Xavier Bavard [7], également dans le cadre de leurs travaux de thèse en doctorat, portant sur l'étude, l'analyse et l'amélioration de la transmission.

La figure 1.13 représente les principaux éléments constituant la boucle à retard du générateur de chaos en longueur d'onde. C'est un système opto-électronique (oscillateurs basés sur des composants optiques et électroniques). La partie optique est constituée de la diode laser DBR, d'un cristal biréfringent (élément non linéaire) placé entre deux polariseurs croisés et d'un photodétecteur. La partie électrique est composée de plusieurs composants que l'on peut regrouper en trois catégories : la ligne à retard, l'amplification et le filtrage.

C'est grâce à la diode laser DBR que des fluctuations chaotiques de la longueur d'onde sont générées. Cette diode est du type multi-électrodes et accordable mono-fréquences. Elle émet quasiment monochromatiquement dans le domaine infrarouge (la longueur d'onde moyenne émise est $\lambda_0 = 1.55$ $\mu$m). La puissance optique et la longueur d'onde sont réglables par des courants appliqués sur ces électrodes. En effet, la diode DBR est composée d'une cavité en deux parties. La première est une zone active amplificatrice large bande. Le gain de cette zone est contrôlé par un courant $I_A$ extérieur à la boucle (figure 1.13) ; ce courant permet de maîtriser la puissance optique à la sortie de la diode. La deuxième partie est un réseau de Bragg modulé par un courant $I_B$ permettant la sélection d'une seule longueur d'onde parmi celles générées dans la zone active. Ce courant $I_B$ contrôle l'indice de réfraction du réseau et permet d'ajuster la longueur d'onde $\lambda$ émise par la diode. La dynamique chaotique du système est décrite par une EDR du premier ordre, elle régit entièrement l'évolution temporelle de la variation de la longueur d'onde $\delta\lambda(t)$, autour de la longeur d'onde moyenne $\lambda_0$ :

$$\delta\lambda(t) + \tau.\frac{d\delta\lambda}{dt}(t) = \beta_\lambda \,.\sin^2\left[\frac{\pi.\,\Delta_0}{\lambda_0^2}\,.\,\delta\lambda(t-T) + \frac{\pi.\,\Delta_0}{\lambda_0}\right] \tag{1.38}$$

où $\Delta_0$ est une différence de chemin optique, et $\beta_\lambda$ représente le gain de la boucle de contre-réaction exprimé en unités de longueur d'onde. Le filtre biréfringent est utilisé pour convertir les fluctuations de la longueur d'onde en variations d'intensité, sa fonction non linéaire est du type sinusoïdal.

### b. Chaos en modulation d'intensité

Un second oscillateur électro-optique non linéaire à retard a été étudié par Pascal Levy [52] et Nicolas Gastaud [53], dans le cadre de leur thèse. Cet oscillateur permet de générer une modulation chaotique de l'intensité lumineuse. Ce système est basé sur des composants standards des télécommunications hauts débits où expérimentalement, un taux d'erreur binaire (BER[12]) de $7.10^{-9}$ est obtenu pour un débit de transmission de 3 Gbit/s [66]. La

[12]En anglais : Bit Error Rate

non linéarité du montage expérimental est réalisée, comme dans les montages de Neyer & Voges, et Celka, par *un interféromètre de Mach-Zehnder en optique intégrée*, avec son contrôleur de polarisation et son alimentation continue permettant de régler son point de fonctionnement (figure 1.14).

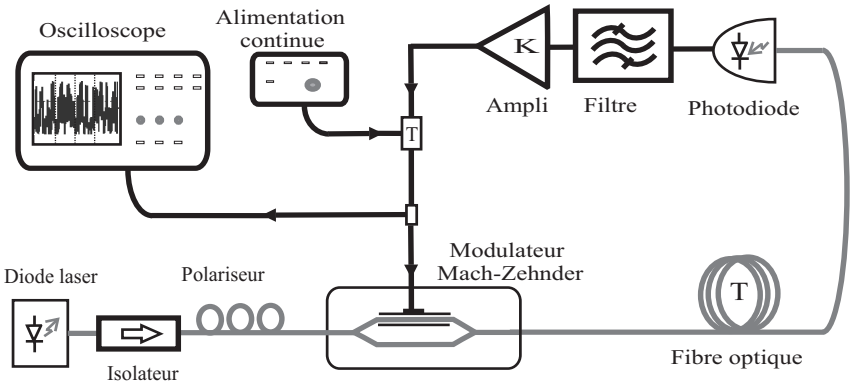



Figure 1.14 – *Générateur de chaos en modulation d'intensité.*

La dynamique chaotique du système est exprimée par une EDR du second ordre, sa forme intégro-différentielle à retard est donnée par :

$$x(t) + \tau.\frac{dx}{dt}(t) + \frac{1}{\theta} \cdot \int_{-\infty}^{t} x(\theta)d\theta = \beta \cdot F_{NL}\Big[x(t-T)\Big] \tag{1.39}$$

où $x(t)$ est une variable sans dimension relative à la tension de modulation du MZ. $\tau$ et $\theta$ sont des constantes de temps du filtre passe-bande, et $F_{NL}[.]$ est une fonction non linéaire en $\cos^2$. Pour plus de détails, nous invitons le lecteur à consulter les références [67, 68].

Ce type de systèmes est très intéressant pour les communications optiques sécurisées, dans la mesure où on dispose d'une large bande pour insérer un message utile. Le sujet traité dans ce rapport de thèse sera basé en partie sur au moins un des aspects caractérisant ce type de systèmes.

## 1.5 Cryptage de signaux par chaos

La présentation qui vient d'être faite a mis en avant divers systèmes à retard produisant des dynamique chaotiques. Une fois que ces signaux sont générés, ils peuvent servir, dans le contexte des communications par chaos, à transmettre un message informatif sécurisé. En effet, le but ultime de tous ces générateurs de chaos a été d'effectuer une transmission sécurisée de message, autrement dit : *un cryptage de signaux par chaos.* L'aspect pseudo aléatoire d'un signal chaotique lui procure l'apparence d'un bruit. Cette

apparence est exploitée pour noyer un message qui devient masqué par le chaos, supposé difficile à identifier. La technique d'insertion du message est appelée *« le codage »*, et la récupération de l'information au niveau du récepteur s'appelle *« le décodage »*. Le succès de l'opération codage/décodage réside dans le pouvoir et la capacité du récepteur à distinguer un signal chaotique d'un bruit quelconque, en reproduisant, en répliquant, ou encore en se synchronisant avec le chaos utilisé lors du masquage par l'émetteur.

En effet, nous avons vu précédemment que la dynamique chaotique possède en apparence une évolution aléatoire. Son spectre de fréquence est bruité, il est composé d'un ensemble continu de fréquences avec un niveau d'amplitude quasi constant. Une information utile présente également un spectre continu à plusieurs fréquences, d'amplitude variable. Lorsque l'opération de codage est effectuée, la qualité de la transmission se mesure par le rapport signal sur bruit en décibels ( $[S/B]_{dB}$). Si ce rapport est positif cela signifie que le signal informatif est prédominant ; s'il est négatif, le message ne peut être récupéré correctement, car c'est le bruit qui prédomine. C'est ce dernier cas qui nous intéresse en sécurisation par chaos.

Effectivement, l'objectif étant de transmettre un message sans qu'il soit détecté, puis décodé par un éventuel espion. En sachant que le signal généré par un oscillateur à comportement chaotique ressemble à un bruit, si son amplitude est supérieure à celle du signal informatif, le résultat de l'addition est une information dont $[S/B]_{dB}$ est négatif. De ce fait, un récepteur classique ne sera pas capable de traduire l'information cachée dans le signal.

Le décodage au niveau du récepteur suppose que celui-ci est capable de distinguer un signal chaotique d'un message informatif. À cause du déterminisme du chaos généré, cette opération est devenue possible lorsque le récepteur crée un signal chaotique quasi-identique à celui émis par l'émetteur. On parle alors de *synchronisation des systèmes émetteur et récepteur* sur laquelle nous reviendrons par la suite. Dans la section suivante, nous supposerons que la synchronisation de l'émetteur et du récepteur est réalisée, et nous allons présenter brièvement, trois des principales techniques de modulation en communication chaotique sécurisée : la modulation chaotique, le masquage chaotique, le chaos shift keying, et leurs versions étendues.

### 1.5.1 Modulation chaotique

La figure 1.15 illustre le principe général de codage par modulation chaotique, où le signal informatif participe directement à la dynamique de l'émetteur. Autrement dit, le message utile est inséré dans la boucle de contre réaction qui génère le signal chaotique. Cette opération s'effectue à l'aide d'une des variables physiques du système : l'intensité optique, la phase, le retard optique, la fréquence... etc. Il est à noter que dans la totalité des schémas de communications chaotiques développés dans notre laboratoire, la modulation chaotique est le type de technique de cryptage utilisée. La transmission d'un message utile a été démontrée expérimentalement sur de nombreux systèmes différents [51, 66, 69, 70].

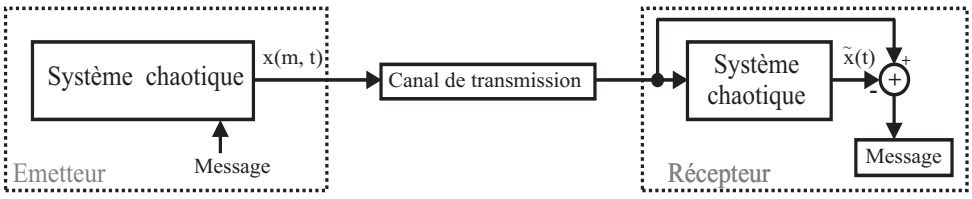



Figure 1.15 – *Principe de communication par modulation chaotique.*

Le fait d'introduire le message dans la boucle a pour conséquence une influence directe sur la dynamique chaotique, ceci permet d'augmenter la complexité du chaos généré [71], et donc de la sécurité de la transmission en réalisant un masquage réciproque entre chaos et message. De plus, pour un récepteur en boucle ouverte, on montre que l'amplitude du signal informatif n'a en principe aucune influence sur la synchronisation avec le récepteur, contrairement au cas du masquage chaotique, où le bruit de transmission et l'erreur d'accordabilité des paramètres de l'émetteur seront les deux sources d'erreur de décodage [51].

Cependant, le point d'insertion du message a une influence notable sur l'architecture du récepteur permettant le décodage [72]. Si ce point se situe à l'extérieur de la boucle d'oscillation, juste à la sortie du signal chaotique créé par l'émetteur, on ne parle plus de modulation chaotique mais de *masquage chaotique*.

### 1.5.2 Masquage chaotique

La méthode de masquage chaotique consiste à mélanger l'information au chaos à l'extérieur de la boucle d'oscillation. La figure 1.16 représente le cas particulier où le mélange des signaux utile $m(t)$ et chaotique $x(t)$ est réalisé par l'intermédiaire d'une addition. C'est la somme de ces deux signaux $m(t) + x(t)$ qui est transmise de l'émetteur vers le récepteur.

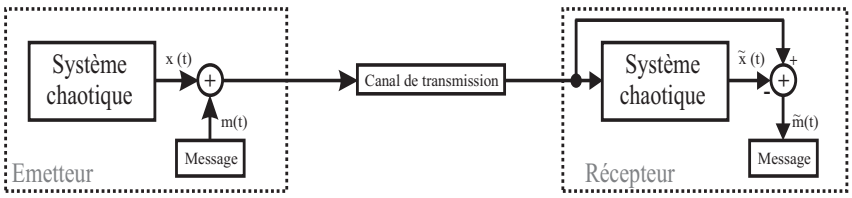



Figure 1.16 – *Principe de communication par masquage chaotique.*

En l'absence du message $m(t)$ à transmettre, $\widetilde{m}(t)$ est vue comme une erreur de synchronisation due à la non reproductibilité parfaite du chaos des deux dispositifs émetteur et récepteur. Dans ce cas, $\widetilde{m}(t)$ s'appelle « *erreur de décodage résiduelle* », on la note alors $\epsilon(t)$ afin de la différencier du message utile. Cette erreur de décodage résiduelle dépend essentiellement de la différence des paramètres entre l'émetteur et le récepteur. Cependant,

lorsque le signal $m(t)$ est inséré, sa reconstitution dépend de la robustesse de la synchronisation, c'est-à-dire, la tendance naturelle du récepteur à se synchroniser sur le signal chaotique reçu, même en présence du signal utile. Dans ces conditions, le signal $m(t)$ joue le rôle d'une perturbation de faible amplitude, et le message $\widetilde{m}(t)$ est alors obtenu par simple soustraction du signal sortant au signal entrant du récepteur :

$$\widetilde{m}(t) = x(t) - \widetilde{x}(t) \tag{1.40}$$

En général, la communication par chaos peut être rendue sécurisée si l'on exploite correctement les propriétés du signal chaotique, en particulier son apparence bruité et son spectre large. En effet, pour avoir une information noyée dans l'apparence bruité du chaos généré, l'amplitude $A_{\text{info}}$ du signal informatif $m(t)$ doit être relativement faible par rapport à l'amplitude $A_{\text{chaos}}$ du signal chaotique $x(t)$. En plus de cette condition, et afin qu'une éventuelle extraction par analyse spectrale et filtrage puisse retrouver les fréquences dominantes du message utile, le spectre de $m(t)$ doit être compris dans la gamme des fréquences du spectre chaotique, c'est-à-dire, la fréquence centrale du signal utile $m(t)$ ne doit en aucun cas être supérieure à la plus haute fréquence du signal chaotique.

Toutefois, dans un environnement particulièrement bruité, l'amplitude $A_{\text{info}}$ doit être suffisante pour que le récepteur puisse distinguer le message $m(t)$ du bruit résiduel $\epsilon(t)$. Ce choix d'amplitude du message, pas trop forte devant le signal chaotique, puis pas trop faible devant le bruit de synchronisation, est contraint par un rapport entre l'amplitude du signal d'information et l'amplitude du signal chaotique $R_{(\text{info/chaos})}$. Ce rapport limite quantitativement la qualité du masquage de l'information. Plus $R_{(\text{info/chaos})}$ est petit, plus la qualité du masquage peut être choisie élevée, et la sécurité de l'information s'en trouve améliorée. Une valeur expérimentale de $-10\ dB$ de ce rapport est considérée comme suffisamment petite pour que l'information ne soit pas détectée dans le signal chaotique transmis.

Un autre rapport important à prendre en compte dans le cryptage par masquage, est le rapport signal sur bruit $[S/B]_{dB}$ à la sortie du récepteur. Ce rapport introduit à la section 1.5 page 34, est calculé entre l'amplitude du signal décrypté $A_{\widetilde{m}(t)}$ et l'amplitude de l'erreur de décodage résiduelle $A_{\epsilon(t)}$. Le rapport $[S/B]_{dB}$ caractérise dans ce cas la qualité du décodage. Plus ce rapport est élevé, ce qui se traduit par une amplitude du signal informatif restitué grande, meilleure est la qualité du décodage. Enfin, pour plus d'informations et de détails sur le cryptage par masquage, nous renvoyons le lecteur aux références [73–76].

### 1.5.3 Chaos shift keying

Un autre procédé de transmission chaotique de données est la communication chaotique CSK (Chaos Shift Keying) [77–79], qui s'applique lorsque le message est binaire. Elle s'inspire de la méthode numérique de codage en transmission de signaux électriques, la modulation à saut de fréquence FSK (Frequency Shift Keying).

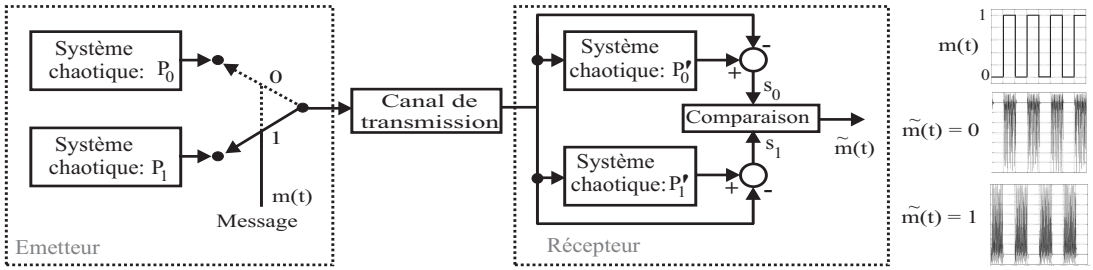



Figure 1.17 – *Schéma de principe de communication par CSK.*

Le cryptage par commutation de clé, dont le principe est illustré sur la figure 1.17, repose sur la valeur de l'amplitude du signal binaire à transmettre. Une opération de commutation est employée selon la valeur du message binaire : si sa valeur est 0, le système chaotique $P_0$ est choisi et le signal de sortie est transmis, sinon la sortie du système chaotique $P_1$ est transmise. Dans ce sens, le message binaire commute l'émetteur entre deux attracteurs étranges correspondant à deux systèmes chaotiques. Le récepteur est composé de deux systèmes chaotiques $P_0^{'}$ et $P_1^{'}$ qui correspondent respectivement à $P_0$ et $P_1$. Supposons que le canal de transmission est parfait, et que le signal transmis est 0, alors le système $P_0^{'}$ se synchronise avec le système chaotique $P_0$, mais le système $P_1^{'}$ ne pourra pas être synchronisé. Le message est restitué selon l'erreur de synchronisation de ($P_0^{'}$,$P_0$) et ($P_1^{'}$,$P_0$), suivi d'un traitement de signal approprié.

Pour que la sécurité de la transmission soit assurée en utilisant cette technique de cryptage, il faut que les trajectoires chaotiques suivies dans le cas où $m(t) = 0$ et $m(t) = 1$ soient suffisamment proches, pour qu'on ne puisse pas les distinguer par un simple examen temporel du signal transmis ou par analyse spectrale. Néanmoins, ce qui va limiter le débit du signal informatif est le fait que à chaque fois que l'on transmet par exemple un 0 après un 1, il faut laisser le temps au récepteur de se synchroniser pour que l'on puisse déterminer que c'est un 0 qui est transmis. La durée d'un bit doit donc être supérieure au temps de synchronisation. Ceci fixe la limite supérieure de la fréquence du signal utile.

Enfin, il existe dans la littérature d'autres variantes de la méthode CSK, qui se basent principalement sur l'énergie du bit des deux systèmes chaotiques $P_0^{'}$ et $P_1^{'}$. Parfois, uniquement un seul système chaotique est employé pour générer deux énergies de bit différentes, par exemple par amplificateur, par retard, ou par phase. La méthode s'appelle alors dans ces cas, respectivement le DCSK (Differentiel CSK) [80, 81], le FM-DCSK (Frequency Modulated DCSK) [82], et PSK (Phase Shift Keying) [38]. Une autre variante de la modulation CSK est d'utiliser le signal binaire à l'intérieur de la boucle d'oscillation. Dans ce cas, le CSK sera considéré comme un cas particulier de la modulation chaotique pour les signaux numériques.

C'est pratiquement cette dernière variante de cryptage que nous allons utiliser pour transmettre un message utile. Mais avant de décrire cette variante de cryptage, nous commençons d'abord par présenter la dynamique chaotique que nous avons spécifiquement étudiée dans le cadre de cette thèse.

## 1.6 Le générateur de chaos à modulateur QPSK

Dans les différents systèmes à retard qui ont été décrits, la clé de cryptage est constituée par l'ensemble des paramètres physiques du générateur de chaos. Les paramètres du système sont : la non linéarité, le retard temporel, le gain et le filtre limitant la dynamique chaotique. Nous verrons plus en détails ces paramètres ultérieurement lors de la description générale de notre système. Nous allons aborder ici plus directement le cœur du travail effectué, en commençant d'abord par présenter le contexte et les objectifs de nos travaux de recherche.

### 1.6.1 Contexte et objectifs

Les systèmes de cryptographie proposés jusqu'à présent peuvent être regroupés en deux classes, ceux qui utilisent les non linéarités intrinsèques et ceux pour lesquels une non linéarité est produite par des composants externes [54]. La première classe correspond par exemple au cas du laser à fibre ou encore du laser semi-conducteur à cavité externe [38]. Ces systèmes génèrent une dynamique chaotique extrêmement rapide. La deuxième classe regroupe entre autre les systèmes basés sur des circuits électroniques et les systèmes opto-électroniques, elle a l'avantage d'être plus souple et plus précise au niveau du réglage des paramètres.

Le système de cryptage par chaos que nous proposons fait partie de la deuxième classe. C'est un système cryptographique électro-optique basé sur une nouvelle architecture de systèmes à retard générateurs de dynamiques chaotiques. La sécurité des systèmes de cryptage au niveau physique en général repose, comme dans les approches algorithmiques, sur la taille de sa clé cryptographique. Plus la taille de la clé est grande, meilleure est la sécurité du système. C'est dans cet esprit d'augmenter la taille de la clé cryptographique que le thème de cette thèse a été élaboré. Nous nous sommes fixés comme objectif l'étude d'un nouveau système générateur de chaos à des fins cryptographique, original par son architecture, et robuste par le nombre de paramètres physiques de sa clé cryptographique.

Nous allons aborder dans le paragraphe suivant ce générateur de chaos expérimental, que nous avons mis en œuvre et étudié. Nous commençons d'abord par le présenter, puis nous décrirons son principe de fonctionnement en soulignant ses originalités.

### 1.6.2 Présentation et description générale du système

Le dispositif expérimental de l'oscillateur chaotique est illustré sur la figure 1.18. C'est un générateur électro-optique dont la partie électronique est repérable en noire, et la partie optique en gris.

#### a. Principe de fonctionnement

Ce générateur de chaos est formé par 2 boucles de contre-réaction reliées à un modulateur QPSK (Quadrature Phase Shift Keying). Ce modulateur électro-optique est parti-

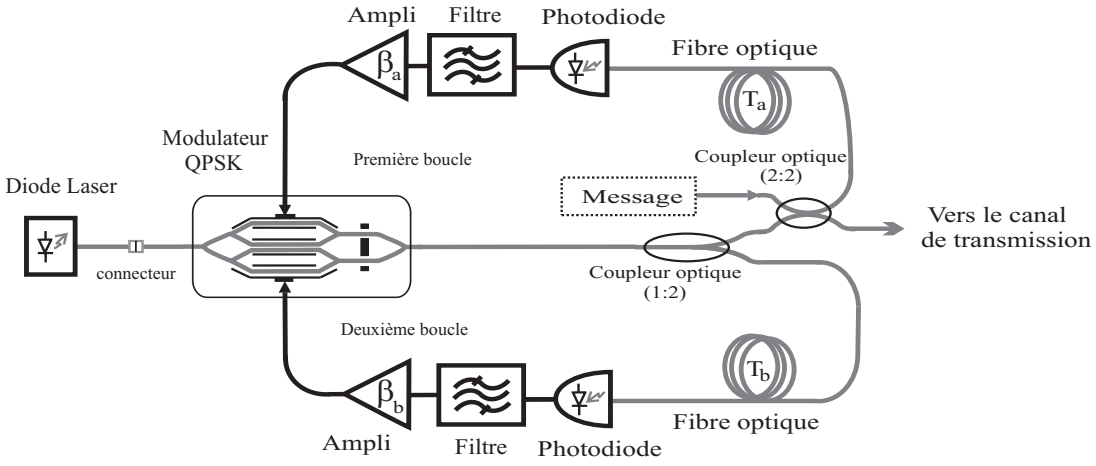



Figure 1.18 – *Architecture du générateur de chaos à modulateur QPSK.*

culier par son architecture ; il appartient à la famille des modulateurs Mach-Zehnder à 4 bras, et il est intégré sur le Niobate de Lithium. Cet élément clé est un composant commercial récent, originellement destiné à des nouveaux formats de modulation numérique pour les télécommunications optiques [83]. Il permet pratiquement dans notre cas la réalisation d'une fonction non linéaire bidimensionnelle. Le reste du générateur de chaos est plus classique. Il est constitué (de gauche à droite) par les composants suivants :

- une diode laser monomode reliée à une fibre optique à maintien de polarisation ; sa longueur d'onde d'émission est celle habituellement utilisée dans les télécommunications optiques ($\lambda_0 = 1,55\ \mu$m).
- le modulateur électro-optique QPSK est déjà évoqué. Il a la particularité d'avoir 2 entrées RF indépendantes et 3 tensions de polarisation indépendantes. Ce composant représente le cœur du système, sa fonction de transfert de modulation réalise la fonction non linéaire du générateur de chaos.
- le système présente aussi l'originalité d'avoir 2 boucles de contre-réactions électro-optiques non linéaires, impliquant chacune un élément retardant, une photodiode de conversion optique / électrique, un filtre électronique large bande et un élément amplificateur.

  **1. La première boucle** est réalisée par la mise en série des éléments suivants :
  - un coupleur optique (2 entrées / 2 sorties) permettant d'insérer le message utile par l'une de ses entrées, et d'envoyer le mélange (chaos + message) d'une part vers la première contre-réaction, et d'autre part vers le canal de transmission.
  - une fibre optique réalisant un retard temporel pur, et constituant un paramètre physique « clé » de la première boucle de contre-réaction (la valeur très précise de ce retard est nécessaire pour l'opération de synchronisation / décodage).

- une photodiode permettant de convertir la puissance optique en un signal électrique.
- un filtre passe-bande limitant la bande passante du signal chaotique électrique.
- un amplificateur électronique réglable pour ajuster le gain de boucle de la contre-réaction.

2. **La deuxième boucle** de rétroaction est réalisée par des éléments semblables à ceux utilisés dans la première boucle, à l'exception du coupleur optique à (2 entrées / 2 sorties) qui ne fait plus partie de cette seconde boucle de contre-réaction.

Le processus dynamique réalisé par cet oscillateur en double boucle fermée peut être décrit de la manière suivante : une diode laser fibrée alimente optiquement le modulateur QPSK. Le faisceau lumineux traversant le modulateur QPSK subit à la sortie une variation d'intensité non linéaire par rapport à chacune des deux tensions appliquées aux électrodes de commandes RF1 et RF2 du modulateur. Le coupleur (1 entrée / 2 sorties) divise ensuite cette intensité optique en deux quantités égales. Les signaux issus des sorties de ce coupleur sont ensuite retardés différemment dans chaque boucle par une certaine longueur de fibre optique (quelques centimètre à quelques mètres), puis ils sont détectés par des photodiodes. Les signaux électriques obtenus sont filtrés, puis amplifiés pour y être réinjectés sur les électrodes de modulation RF du QPSK. La présence du coupleur optique (2 entrées / 2 sorties) dans la première boucle ne sert qu'à mélanger le message avec la modulation chaotique de l'intensité.

À partir de la description globale qui vient d'être donnée, les avantages de ce système sont nombreux. Nous en citons quelques uns dans le paragraphe suivant.

### b. Originalités et principaux avantages

Le générateur de chaos proposé est composé de deux boucles de rétroaction, dont chacune est constituée d'éléments différents d'une boucle à une autre. La clé de cryptage physique de ce système, qui représente l'ensemble des paramètres du dispositif, est donc augmentée par rapport aux systèmes cryptographiques déjà étudiés (voir la section 1.4). Nous donnerons l'ensembles des paramètres physiques constituant cette clé un peu plus loin dans ce manuscrit.

Le point d'insertion [72] du message n'a pas été plus particulièrement abordé dans le cadre de cette thèse. Il est choisi dans la partie optique de la chaîne d'oscillation, comme dans la référence [53]. Ceci présente pratiquement les avantages suivants : l'utilisation d'un coupleur optique à large bande permet de travailler à des débits très élevés, qu'il soit numérique ou analogique. Dans un contexte expérimental similaire [66], dont nous souhaitons tirer parti, une architecture de décodeur performant a déjà fait ses preuves. Enfin, ce générateur de chaos utilise un modulateur électro-optique d'intensité de type

Mach-Zehnder à 4 bras intégré, qui permet de relier deux rétroactions retardées *via* ses entrées de modulations indépendantes. La grandeur qui est rebouclée sur ses électrodes est la puissance optique de sortie du modulateur, détectées et amplifiées par des photodiodes et des amplificateurs télécom. Il faut noter que tous ces composants électro-optiques et optoélectroniques sont fréquemment employés, avec diverses architectures, en télécom optiques ultra-rapides. Ceci représente un avantage en terme de compatibilité technologique de ce type de composants dédiés.

## 1.7 Conclusion

Ce chapitre était dédié à l'introduction des systèmes électro-optiques de cryptographie par chaos. Ainsi, le principe de génération d'un signal à caractère pseudo-aléatoire et les modélisations des différents systèmes à retard sous forme d'EDR ont été présentés. Ceci nous a permis de choisir et de justifier les méthodes de simulation numérique de ces dynamiques. Des exemples concrêts d'oscillateurs de ces approches chaotiques ont été donnés, et ont permis de décrire une partie de l'état de l'art du domaine. L'approche proposée dans ce manuscrit a pu être ainsi située. La présentation de quelques méthodes d'insertion de message dans les systèmes à retard, nous a permis de préciser le type de cryptage par chaos que nous allons utiliser : la modulation chaotique. Finalement, une première description globale du générateur de chaos étudié a été donnée en fin de chapitre.

Dans le chapitre suivant, nous allons étudier en détail les comportements possibles du générateur de chaos proposé. Nous commencerons par donner des éléments de théorie propre au modulateur QPSK, puis nous étudierons le dispositif complet permettant de générer la dynamique chaotique.

# Chapitre 2

# Description et modélisation du générateur de chaos

Nous venons de donner au chapitre 1 une description globale de notre générateur de chaos. Celui-ci va nous permettre de réaliser des communications sécurisées par cryptage chaotique, qui se fera sur la variable intensité optique. Dans ce chapitre, constitué de 4 parties, nous allons étudier ce générateur en commençant par sa fonction non linéaire, représentée dans le dispositif expérimental par la fonction de transfert du modulateur QPSK. Pour appréhender la modélisation et l'analyse de ce modulateur, nous avons jugé utile de donner, dans une première partie, quelques principes de base sur les modulateurs électro-optiques intégrés sur le $LiNbO_3$ en général. Cette introduction va nous permettre par la suite de mieux saisir le fonctionnement du QPSK, et de donner ainsi la fonction non linéaire analytique.

Nous consacrerons ensuite une partie entière à l'étude de l'influence des paramètres de contrôle de ce modulateur. Cette étude va nous aider à comprendre la répercution d'une action d'un paramètre de commande par rapport à la fonction non linéaire du système. Puis, nous donnerons une description rapide de la chaîne optoélectronique de détection, de filtrage et d'amplification du générateur de chaos proposé.

Dans une troisième partie, nous procèderons à la mise en équations de l'oscillateur chaotique, afin de le simuler numériquement par la suite. À travers cette modélisation, nous essayerons d'obtenir numériquement ses diverses évolutions dynamiques, et de prévoir ainsi son fonctionnement expérimental. Enfin, nous terminerons ce chapitre en donnant quelques tests numériques qui ont permis de valider le programme de calcul de l'algorithme de la méthode de résolution numérique adoptée.

## 2.1 Quelques rappels de base

La fonction non linéaire du générateur de chaos proposé est basée sur la fonction de transfert d'un modulateur de type électro-optique. Les matériaux susceptibles d'assu-

rer un effet électro-optique se divisent en général en trois catégories : les polymères, les semi-conducteurs III-V et les cristaux électro-optiques dont le Niobate de Lithium fait partie [84–87]. Nous nous intéressons uniquement à cette dernière catégorie, puisque dans notre cas, le modulateur QPSK est intégré sur ce cristal. La maturité technologique, les faibles dépendances en longueur d'onde, et les faibles pertes optiques sont autant d'atouts qui justifient le succès technologique en optique intégrée de ce cristal.

Le principe physique de fonctionnement de tout ces modulateurs est basé sur l'effet Pockels. En effet, les matériaux électro-optiques ont un indice optique $n$ qui dépend au premier ordre d'un champ électrique statique extérieur $\overrightarrow{E_e}$. La variation d'indice $\Delta n$ induite dépend des directions du champ électrique $\overrightarrow{E_e}$ et du champ optique $\overrightarrow{E_{opt}}$. Pour évaluer cette variation d'indice[1], on utilise le tenseur électro-optique $[\mathbf{r}]$ de dimensions $6 \times 3$. La direction des champs optique et électrique est choisie de façon à bénéficier d'une efficacité électro-optique maximale, c'est-à-dire, avec le plus grand coefficient du tenseur.

Pour le $LiNbO_3$, le coefficient de tenseur électro-optique le plus grand est le $r_{33}$, sa valeur vaut 30.8 pm/V. Et afin d'exploiter efficacement ce tenseur, les champs optique et électrique doivent être polarisés suivant l'axe extraordinaire du cristal (axe $z$). La variation d'indice due à l'application du champs électrique $\overrightarrow{E_e}$ est alors donnée par la relation suivante :

$$\Delta n = -\frac{1}{2} \,.\, n_e^3 \,.\, r_{33} \,.\, < E_{e(Z)} > \tag{2.1}$$

où $< E_{e(Z)} >$ est la moyenne algébrique de la composante suivant $z$ du champ $\overrightarrow{E_e}$ sur l'ensemble du guide optique, et $n_e$ l'indice extraordinaire du cristal.

L'effet électro-optique trouve un grand domaine d'applications : la modulation de phase ou d'amplitude de la lumière, le Q-switching ou le mode-locking des lasers,...etc. Dans notre laboratoire, des modulateurs intégrés sur le $LiNbO_3$ ont été déjà employés dans des dispositifs expérimentaux pour générer des dynamiques chaotiques.

En effet, nous avons cité au premier chapitre deux types de ces composants : le modulateur de phase et le modulateur d'intensité de type Mach-Zehnder. Nous allons consacrer les deux paragraphes suivants à la description de ces deux composants ; cette description est une introduction préliminaire à l'étude du modulateur QPSK.

### a. Modulateur de phase

Nous avons vu à travers l'effet Pockels que l'application d'un champ électrique sur un cristal se traduit par des variations d'indice de réfraction. Cette variation peut être exploitée de manière linéaire par exemple dans un modulateur de phase. En effet, ce modu-

[1]Si la variation d'indice de réfraction est proportionnelle au champ électrique appliqué, on parle d'effet électro-optique linéaire ou d'effet Pockels. Si elle est proportionnelle **au carré** du champ, il s'agit alors de l'effet électro-optique quadratique ou effet Kerr. Cet effet est normalement négligé quand l'effet linéaire est présent.

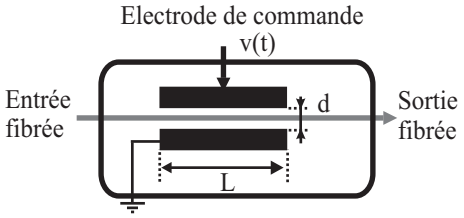



FIGURE 2.1 – *Schéma de principe d'un modulateur de phase.*

lateur est composé d'un cristal $LiNbO_3$ dans lequel un guide d'onde est intégré. Sur ce cristal deux électrodes sont déposées – figure 2.1 – auxquelles une tension variable $v(t)$ est appliquée. Cette tension constitue un champ transverse à la propagation, qui induit une modification de l'indice de réfraction selon la relation (2.2).

$$\Delta n = -\frac{1}{2} \cdot n_e^3 \cdot r_{33} \cdot \frac{V}{d} \tag{2.2}$$

avec $V$ l'amplitude de la tension appliquée, et $d$ la distance entre les deux électrodes. Le déphasage de l'onde optique apporté par le guide d'onde est proportionnel à l'indice de réfraction. Par conséquent, ce déphasage est proportionnel à la tension appliquée aux bornes des électrodes. L'application d'un champ électrique entraîne donc un déphasage $\phi$ entre les deux ondes optiques d'entrée et de sortie du modulateur. Ce déphasage peut être résumé par la relation :

$$\phi = \frac{2\pi}{\lambda} \cdot \Delta n \cdot L \tag{2.3}$$

où $L$ est la longueur d'interaction entre le champ électrique et le champ optique, et $\lambda$ la longueur d'onde du signal optique. L'expression de la variation de la phase en fonction de la tension appliquée à l'électrode de commande du modulateur, est obtenue par simple arrangement des relations (2.3) et (2.2). Elle est donnée par :

$$\phi(t) = \pi \cdot \frac{v(t)}{V_\pi} \tag{2.4}$$

avec :

$$V_\pi = \frac{\lambda \cdot d}{n_e^3 \cdot r_{33} \cdot L}$$

où $V_\pi$ est la tension demi-onde qui permet de réaliser un déphasage électro-optique de $\pi$.

Nous avons introduit ici les notions de déphasage $\phi(t)$ et de tension demi-onde $V_\pi$. Celles-ci seront utilisées dans la modélisation du modulateur Mach-Zehnder, que nous allons décrire maintenant, puis dans le modulateur QPSK.

### b. Modulateur Mach-Zehnder

L'effet Pockels est exploité aussi dans un modulateur d'intensité d'une structure de type Mach-Zehnder (figure 2.2a). Le guide optique se divise en deux branches par une jonction Y, puis à l'aide d'une deuxième jonction Y, ces deux branches se rejoignent. La figure 2.2b illustre un exemple où un des bras optiques est recouvert par l'électrode chaude, porteuse du signal électrique, tandis que le deuxième bras est recouvert par la masse. Le champs électrique régnant sur le bras n° 2 (représenté en traits pointillés) a un sens opposé au champ électrique appliqué au bras n° 1. L'indice effectif optique $n$ diminue sur l'un des bras, alors qu'il augmente sur l'autre. Ceci entraine une différence de phase — relation (2.5) — entre les signaux optiques issus de chacune des branches.

$$\Delta\phi \simeq \frac{2\pi}{\lambda}\left(\Delta n_1 - \Delta n_2\right) \cdot L \tag{2.5}$$

avec $L$ est la longueur d'interaction. $\Delta n_1$ et $\Delta n_2$ sont les variations d'indices dues respectivement aux champs électriques moyens régnant sur les guides optiques des bras 1 et 2.

- Pour une certaine tension de référence $V_0$ pilotant l'électrode chaude, le signal optique issu du bras n° 1 est en phase avec le signal issu du bras n° 2, l'interférence entre ces deux signaux est constructive, et l'intensité optique en sortie de l'interféromètre est maximale.

- Si la tension appliquée est augmentée ou diminuée telle que les signaux optiques sont en opposition de phase à la sortie de la deuxième jonction Y ($\Delta\phi = \pi$), l'interférence est destructive, et l'intensité de sortie est minimale. La variation de tension qui permet de réaliser cette opposition de phase est celle que nous avons déjà évoquée, la tension demi-onde $V_\pi$.

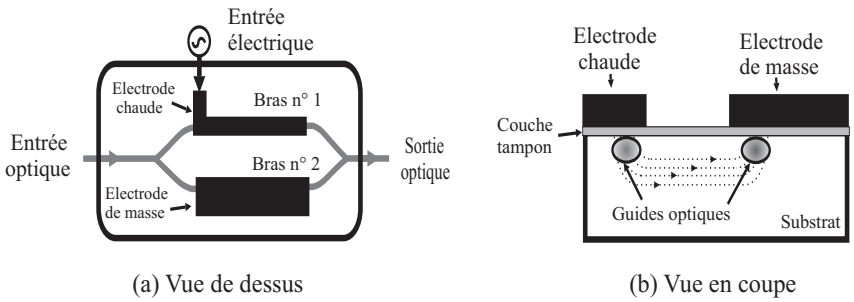



Figure 2.2 – *Principe de fonctionnement d'un modulateur MZ électro-optique. Les traits pointillés sur la vue en coupe représentent les lignes de champ électrique. La zone grisée entre électrodes et substrat est une couche tampon pour éviter les pertes optiques dans le métal.*

En général, chaque modulateur MZ dispose d'une électrode DC et d'une électrode RF. La première permet de fixer le point de fonctionnement du modulateur à l'aide d'une tension continue, et la seconde permet d'acheminer le signal électrique de modulation. Mais la structure de ces électrodes joue un rôle important sur la variation de l'intensité optique en sortie [86]. En effet, selon que le guide optique est en dessous des électrodes, ou entre les électrodes, le cristal $LiNbO_3$ réagit différemment. C'est la raison pour laquelle les modulateurs MZ sont classés en deux catégories : les modulateurs en coupe X [88], et les modulateurs en coupe Z [89], qui diffèrent par la direction des axes du cristal relativement au plan du modulateur.

1. **Modulateurs MZ en coupe $X$ :**

   Le plan du modulateur est perpendiculaire à l'axe $X$ du cristal (figure 2.3a). Pour bénéficier du coefficient du tenseur le plus élevé $r_{33}$, il faut que les champs électriques et optiques soient polarisés suivant l'axe $Z$ du cristal. Ceci implique que le champ électrique, comme le champ optique, soit parallèle au plan du modulateur et perpendiculaire à la direction de propagation, qui est suivant $Y$. Ces conditions de polarisation sont obtenues en plaçant les guides optiques entre les électrodes. La polarisation dans cette configuration est dite TE (Transverse Electrique).

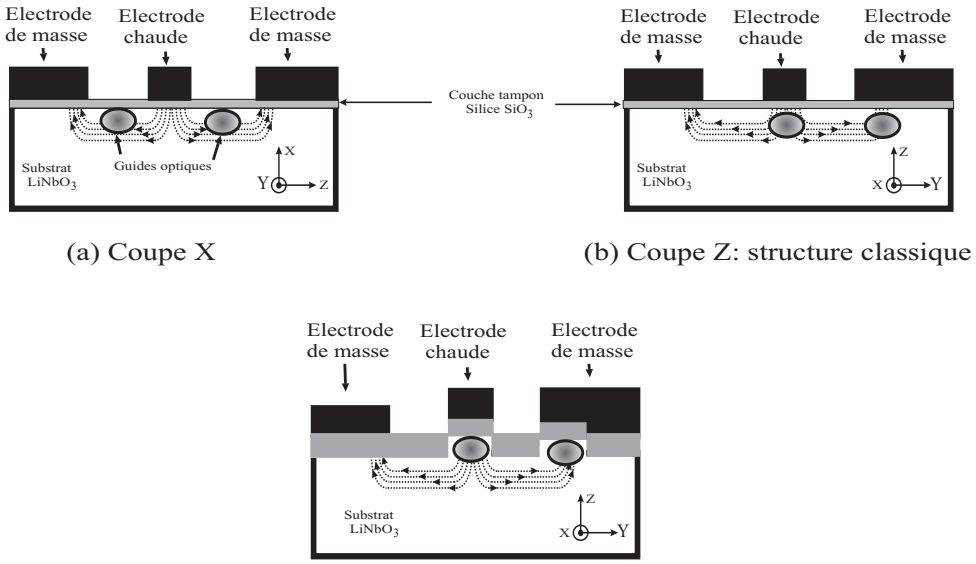
   Comme illustré sur la figure 2.3a, un modulateur $LiNbO_3$ en coupe $X$ est symétrique. La configuration des électrodes est dite en *push-pull*. Cette dénomination signifie que lorsqu'une tension sur l'électrode chaude est appliquée, les électrodes et les guides en regard sont disposés de telle sorte que, le champ électrique soit en sens inverse dans chacun des deux bras du MZ. Un des avantages de cette structure est que le champ optique sortant du MZ subit une modulation de fréquence parasite[2] fortement réduite. De ce fait, le paramètre de chirp des modulateurs MZ en coupe $X$ est très faible. Cette propriété est très appréciée pour les télécommunications à très haut-débit. À titre d'exemple, des transmissions à 40 Gbit/s sont déjà réalisées en utilisant cette coupe [91].

   L'inconvénient des modulateurs en coupe $X$ est leur tension de commande relativement élevée, conséquence de la présence d'une couche tampon pour préserver la bande passante du modulateur. En effet, les modulateurs $LiNbO_3$ ont besoin d'une couche en silice ($SiO_2$) épaisse entre le guide et les électrodes pour bénéficier d'une large bande passante. En revanche, le champ électrique vu par le guide optique est affaibli par cette couche diélectrique, d'où une tension de commande conséquente. Cet inconvénient est réduit considérablement dans le cas d'une coupe $Z$.

2. **Modulateurs MZ en coupe $Z$ :**

   Le plan du modulateur est perpendiculaire à l'axe extraordinaire $Z$ du cristal (figure 2.3b). Afin d'utiliser le coefficient du tenseur $r_{33}$, les électrodes sont placées au-dessus des guides optiques. Ainsi, le champ électrique est parallèle à l'axe $Z$ du cristal sur la section du guide, et le champ magnétique est parallèle au plan du modu-

[2] En anglais : *chirp*. C'est une variation de fréquence parasite qui accompagne une modulation en amplitude. Il se déduit de la variation temporelle de la phase [90] : $\delta f = \frac{1}{2\pi} \cdot \frac{d\phi}{dt}(t)$.




(a) Coupe X

(b) Coupe Z: structure classique

(c) Coupe Z: structure en ridge

Figure 2.3 – *Vues transversales de différentes coupes d'un modulateur MZ à un seul driver.*

lateur. Le champ électrique sous l'électrode centrale est plus intense s'il y a deux masses au lieu d'une seule. C'est ce qui permet un gain global d'efficacité, malgré une réduction de l'interaction électro-optique pour le guide optique placé sous l'électrode de masse. Le mode de polarisation est dit TM (Transverse Magnétique).

Un modulateur en coupe $Z$ est asymétrique. L'asymétrie des champs électriques appliqués, fait que les ondes se propageant sur les deux bras sont soumises a un déphasage différent. Les recouvrements sous l'électrode centrale et sous les plans de masse entre les champs électriques et optiques sont aussi différents. Cette asymétrie entre les deux bras optiques entraine une modulation de phase résiduelle du champ optique en sortie du modulateur. Le paramètre chirp donc n'est pas nul et représente ainsi un inconvénient. C'est ce qui fait que les modulateurs en coupe $Z$ en structure classique – figure 2.3b – ne conviennent pas aux télécommunications à haut-débit.

En revanche, comparablement aux modulateurs en coupe $X$, les modulateurs en coupe $Z$ ont des tensions demi-onde plus faibles. La coupe offre encore plus de liberté comme nous pouvons le constater sur la figure 2.3c. Cette structure est dite en « *ridge* », car les guides optiques se trouvent placés sur des crêtes creusées sur le substrat. L'intérêt de cette configuration est de pouvoir disposer d'un paramètre supplémentaire, la profondeur de la gravure entre les électrodes. Cette profondeur permet en général de réaliser l'accord entre les indices optique et électrique, sans nuire à l'efficacité électro-optique. Lorsque une couche de silice est ajoutée, elle permet aussi de diminuer les tensions de commandes. À titre d'exemple, des modulateurs à bande passante de 100 GHz sont déjà réalisés avec une structure en ridge [92].

Nous venons de décrire des modulateurs d'intensité de type MZ pilotés par un seul driver. De même il existe des modulateurs qui sont commandés par deux drivers [93–95], cette configuration consiste à utiliser deux électrodes centrales comme le montre par exemple la figure 2.4.

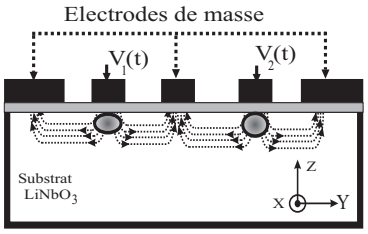



FIGURE 2.4 – *Vue transversale d'un modulateur MZ en coupe Z à double driver.*

L'utilisation de ces modulateurs MZ pour la génération de comportements chaotiques nécessite une tension de commande supérieure à leur tension demi-onde $V_\pi$, leur fonction de transfert devient ainsi fortement non linéaire. C'est en exploitant cette propriété que leur fonction de transfert est devenue intéressante dans les schémas classiques d'oscillateurs chaotiques à retard (un exemple est donné à la section 1.4).

**- Fonction de transfert d'un modulateur MZ simple**

La figure 2.5 illustre un schéma de principe de modélisation d'un modulateur MZ intégré. Lorsqu'un faisceau lumineux d'intensité constante est injecté à son entrée, un déphasage $\varphi(t)$ est alors appliqué à l'onde optique parcourant la branche soumise à l'électrode chaude. La non linéarité est la fonction qui relie la puissance optique de sortie et la tension de commande. Il s'agit bien d'une relation sinusoïdale, comme dans le modèle classique des dynamiques d'Ikeda. Physiquement, on peut déduire cette non linéarité de la manière suivante :

Considérons un champs électrique à l'entrée du modulateur : $E_{in}(t) = \sqrt{P_0}\exp(j\omega_0 t)$, avec $P_0$ la puissance optique à l'entrée du MZ, et $\omega_0$ la fréquence angulaire de la source laser.

L'une des branches du MZ est soumise simultanément à une tension continue et à une tension variable. La tension continue $V_{DC}$ est appliquée sur l'électrode DC, tandis que la tension variable $v(t)$ est appliquée à l'électrode RF. Ces deux tensions induisent sur l'onde

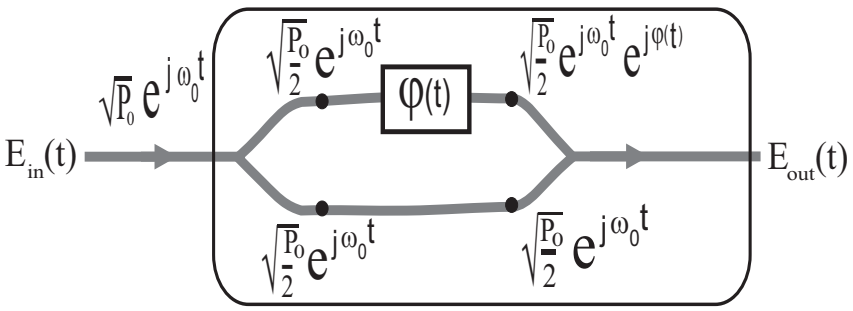



Figure 2.5 – *Principe de modélisation d'un modulateur MZ simple.*

se propageant le long de cette branche un déphasage $\varphi(t)$ donné par la relation suivante :

$$\begin{aligned} \varphi(t) &= \pi.\frac{v(t)}{V_{\pi RF}} + \pi.\frac{V_{DC}}{V_{\pi DC}} \\ &= \pi.\frac{v(t)}{V_{\pi RF}} + \phi \end{aligned} \tag{2.6}$$

où $V_{\pi RF}$ et $V_{\pi DC}$ sont des tensions demi-ondes, respectivement en régime dynamique et en régime statique. Et $\phi$ est un déphasage statique lié à l'application de la tension continue $V_{DC}$. Au point de recombinaison des 2 branches, à l'aide de seconde jonction en Y, les ondes interfèrent : le champ électrique en sortie $E_{out}(t)$ est égal à la somme des deux champs électriques de chaque branche. Son expression est donnée par :

$$E_{out}(t) = \frac{\sqrt{P_0}}{2}\Big[1 + \exp(j\varphi(t))\Big]\exp(j\omega_0 t) \tag{2.7}$$

L'expression de la puissance optique $P_{out}(t)$ à la sortie du modulateur est obtenue par le calcul de la moyenne — relation (2.8) — du module au carré du champ électrique résultant $E_{out}(t)$.

$$P_{out}(t) = \langle |\vec{E_{out}}|^2 \rangle = \vec{E_{out}} \cdot \vec{E_{out}}^{\,*} \tag{2.8}$$

Ainsi, $P_{out}(t)$ est donnée par :

$$P_{out}(t) = P_0 \cos^2\Big[\frac{\varphi(t)}{2}\Big] \tag{2.9}$$

Finalement, nous obtenons l'expression de la fonction non linéaire — relation (2.10) — du modulateur MZ en remplaçant, tout simplement, l'expression de $\varphi(t)$ donnée par la relation (2.6) dans (2.9).

$$f_{NL}[v(t)] = P_{out}(t) = P_0 \cos^2\left[\pi\frac{v(t)}{2V_{\pi RF}} + \frac{\phi}{2}\right] \tag{2.10}$$

Enfin, il existe plusieurs études et publications de systèmes d'Ikeda [28,32,69], utilisant la non linéarité $f_{NL}[v(t)]$ pour produire des comportements chaotiques. Dans la suite, nous appliquerons le même raisonnement pour déterminer la fonction de transfert du modulateur QPSK.

À présent, nous allons commencer l'étude de l'oscillateur par sa fonction non linéaire, avec comme introduction, un bref historique et quelques références dans la littérature de systèmes ayant utilisés un modulateur QPSK.

## 2.2 Étude du générateur de chaos

### 2.2.1 La fonction non linéaire

Le nouvel oscillateur chaotique sur la variable intensité optique est basé sur un modulateur QPSK relativement récent. C'est un produit que l'on trouve commercialement, en particulier auprès de la societé Photline Technologies[3]. Cette société a été crée dans le cadre du transfert des technologies en septembre 2000, par des chercheurs du laboratoire LOPMD.

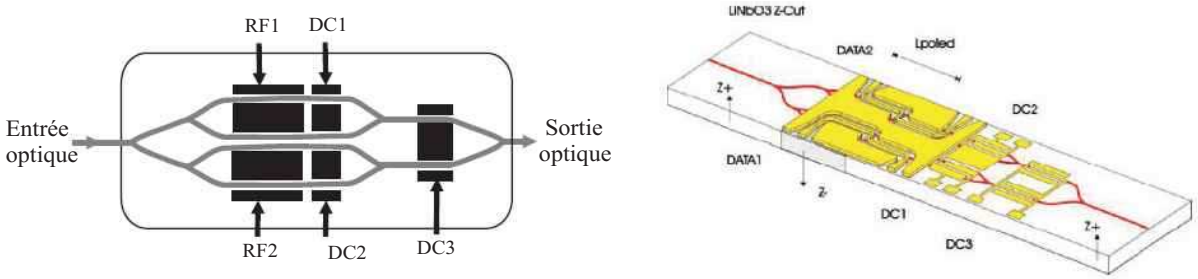
En 2006, le premier modulateur QPSK intégré sur le $LiNbO_3$ coupe $Z$ a été réalisé par cette société. C'était dans le cadre d'un projet européen « synQPSK[4] » destiné à des nouveaux formats de modulation numérique pour les télécommunications optiques [83]. Son principe de fonctionnement est basé sur une modulation optique synchrone par déplacement de phase en quadrature (à 4 états) en utilisant des lasers standards. Ainsi, une transmission numérique est réalisée avec succès à 1.6 Gbit/s [96].
Par la suite (2007–2008), la transmission en optique cohérente a permis d'une part d'améliorer le même système [97], et d'autre part, d'atteindre de très haut-débits [98] de l'ordre de 40 Gbit/s. Une combinaison de deux modulateurs QPSK en parallèle est aussi utilisée dans ce même projet [99, 100].

Récemment, la combinaison de 2 modulateurs QPSK a été employée pour mesurer les performances du multiplexage en longueur d'onde (WDM : Wavelength Division Multiplexing), qui est une technique très utilisée en communications optiques. L'objectif était de réaliser une DP-QPSK[5] à un débit de 40 Gbit/s. Cette combinaison de 2 modulateurs a permis la mesure de la dispersion de mode de polarisation (PMD : Polarization Mode Dispersion) [101].

Dans la totalité des applications qui viennent d'être citées, le modulateur QPSK employé — figure 2.6b — est intégré sur $LiNbO_3$ de coupe $Z$ [83]. Les amplitudes des tensions de modulation utilisées, celles qui sont appliquées aux électrodes RF, restent au plus égales aux tensions demi-onde du modulateur. Dans notre application, qui requiert un fonctionnement fortement non linéaire pour la génération de signaux chaotiques, nous

[3] http ://www.photline.fr
[4] Key Components for Synchronous Optical Quadrature Phase Shift Keying Transmission
[5] Dual-Polarization-QPSK

avons utilisé un modulateur intégré de coupe $X$ (figure 2.6a). Certains avantages et inconvénients d'une telle coupe ont été exposés en page 47, et dans le paragraphe suivant, nous allons donner la description générale de ce composant.




(a) Coupe X (b) Coupe Z

Figure 2.6 – *Les différents types de modulateur QPSK.*

### 2.2.1.a Description du modulateur QPSK

La figure 2.6a schématise la configuration du modulateur QPSK utilisé pour réaliser la fonction non-linéaire. À première vue, nous pouvons l'assimiler à la mise en parallèle de deux modulateurs MZ classiques. Mais cette approche n'est pas toute à fait exacte, car l'ensemble des deux modulateurs sont intégrés avec la particularité d'une électrode DC supplémentaire. En effet, le modulateur possède au total 3 électrodes DC et 2 électrodes RF. Le rôle de chacune de ces électrodes peut être décrit, comme dans un modulateur MZ simple, de la manière suivante :

- Les tensions continues appliquées aux deux premières électrodes $DC_1$ et $DC_2$ permettent indépendamment de régler les points de fonctionnement de chacun des interféromètres $MZ_1$ et $MZ_2$ en parallèle. Une troisième tension continue $DC_3$ permet de contrôler la phase relative des deux sorties des $MZ_1$ et $MZ_2$, qui génèrent alors en sortie du composant une interférence à 4 ondes.
- Aux deux électrodes RF1 et RF2 sont appliquées deux tensions de modulation indépendantes. Ces électrodes permettent donc d'acheminer les signaux électriques variables, qui interagissent avec la lumière se propageant dans les guides optiques. La disponibilité de 2 entrées RF pour la construction d'une non linéarité bidimensionnelle est une autre particularité du modulateur QPSK.

### 2.2.1.b Modélisation du modulateur QPSK

Pour modéliser le modulateur QPSK, nous nous sommes inspirés directement de celui du modulateur MZ simple, donné en page 50. La figure 2.7 montre le schéma de principe

correspondant au QPSK utilisé pour la réalisation de la fonction non linéaire bidimensionnelle, notée par $f_{NL}[v_a, v_b]$.

L'expression de l'intensité optique, qui représente la variable de sortie du modulateur, est fonction des tensions appliquées sur ces électrodes RF ($v_a$ sur RF1 et $v_b$ sur RF2) ainsi que de trois tensions continues, appelées aussi tensions de bias ($V_{DC1}$, $V_{DC2}$ et $V_{DC3}$) qui permettent d'ajuster les points de repos de la condition d'interférence à 4 ondes.

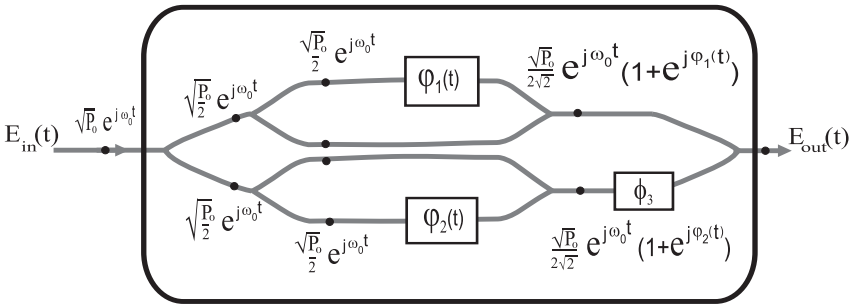



FIGURE 2.7 – *Principe de modélisation du modulateur QPSK.*

L'expression analytique de la fonction de transfert du modulateur QPSK peut s'établir de la manière suivante :

- Sur l'électrode $\mathrm{DC}_m$ ($m = 1, 2, 3$) est appliquée une tension continue $V_{DC_m}$. Un déphasage $\phi_m$ est introduit sur l'onde optique qui se propage le long de la branche soumise à la tension $V_{DC_m}$ (comme illustré sur la figure 2.7). L'expression de ce déphasage est donnée par :

$$\phi_m = \pi \cdot \frac{V_{DC_m}}{V_{\pi DC_m}} \tag{2.11}$$

  où $V_{\pi DC_m}$ est la tension demi-onde, qui permet de réaliser un déphasage de $\pi$ avec l'électrode $\mathrm{DC}_m$.

- Sur les électrodes $\mathrm{RF}_{1,2}$ sont appliquées respectivement 2 tensions variables $v_{a,b}(t)$. Ces dernières sont des tensions de modulation, et elles introduisent des déphasages variables $\varphi_{1,2}(t)$. Les expressions de ces déphasages sont données par :

$$\varphi_{1,2}(t) = \pi \cdot \frac{v_{a,b}(t)}{V_{\pi RF_{1,2}}} + \phi_{1,2} \tag{2.12}$$

  où $V_{\pi RF_{1,2}}$ sont des tensions demi-ondes, qui permettent de réaliser en régime dynamique un déphasage de $\pi$ respectivement dans les interféromètres $\mathrm{MZ}_1$ et $\mathrm{MZ}_2$.

L'expression de la puissance optique $P_{out}(t)$ à la sortie du modulateur QPSK est obtenue par le calcul de la moyenne — relation (2.8) — du module au carré du champ électrique résultant $E_{out}(t)$. Nous rappelons ici volontairement cette relation :

$$P_{out}(t) = \langle |E_{out}(t)|^2 \rangle = f_{NL}[v_a, v_b](t) \tag{2.13}$$

En imposant un champ en entrée du modulateur sous la forme $E_{in}(t) = \sqrt{P_0}.\exp(j\omega_0 t)$ ($P_0$ est la puissance optique à l'entrée du QPSK, $\omega_0 = 2\pi.c/\lambda_0$ est la fréquence angulaire de la source laser, et $c$ est la vitesse de la lumière), le champ électrique $E_{out}(t)$ en sortie du modulateur QPSK est donné par :

$$E_{out}(t) = \frac{\sqrt{P_0}}{4}\left[1 + \exp\left(j\varphi_1(t)\right) + \left[1 + \exp\left(j\varphi_2(t)\right)\right]\exp\left(j\phi_3\right)\right]\exp\left(jw_0 t\right) \tag{2.14}$$

Il vient finalement pour la fonction de modulation non linéaire bidimensionnelle (une annexe en fin du manuscrit est disponible pour plus de détails) :

$$f_{NL}[v_a, v_b](t) = \frac{P_0}{4}\left\{\cos(\psi_3)\Big[\cos(\psi_3) + 2\cos\big(\psi_1 + \psi_2\big)\cos\big(\psi_2 + \psi_3 - \psi_1\big)\Big] + \cos^2\big(\psi_2 + \psi_3 - \psi_1\big)\right\} \tag{2.15}$$

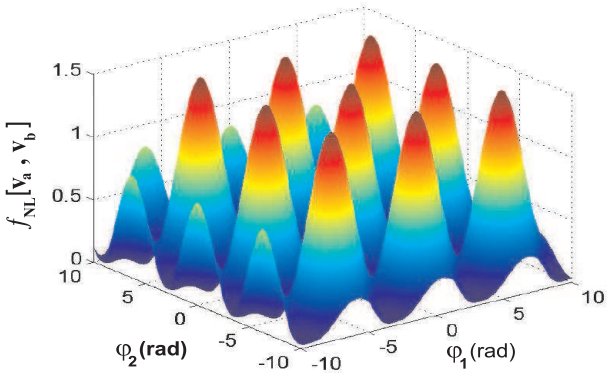
avec :

$$\psi_1 = \frac{\varphi_1(t)}{2}; \qquad \psi_2 = \frac{\varphi_2(t)}{2}; \qquad \psi_3 = \frac{\phi_3}{2};$$

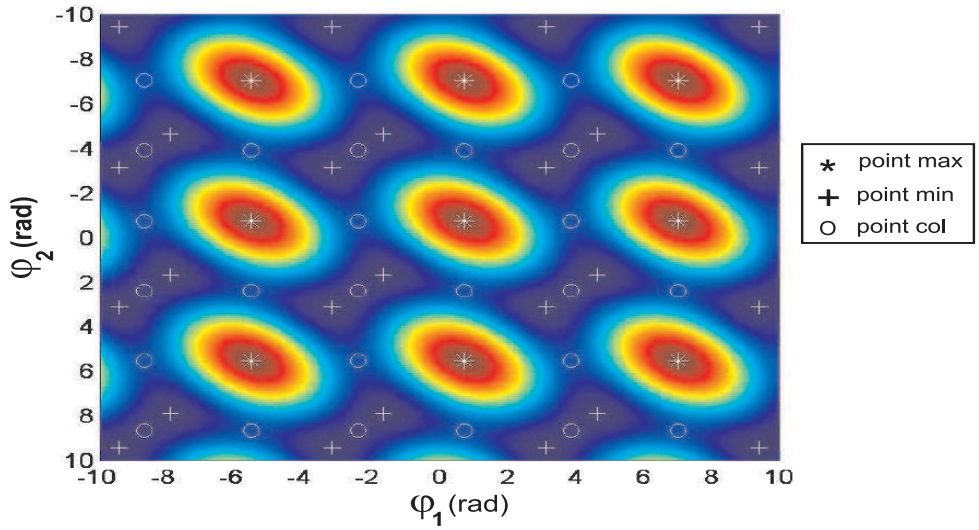
Une condition nécessaire sur la non linéarité pour obtenir une dynamique chaotique est de présenter un extrémum dans l'intervalle de variation des variables d'entrées. Cette condition est suffisamment vérifiée par $f_{NL}[v_a, v_b]$, donnée par la relation (2.15), comme le montre un exemple de son allure sur la figure 2.8a.

On constate que la forme globale de $f_{NL}[v_a, v_b]$ ressemble à « *un emballage d'œufs* », où plusieurs extrema sont présents. Physiquement, ces extrema traduisent des maxima et des minima de la puissance optique, leurs positions et leurs périodicités — figure 2.8b — sont mieux représentées lorsque $f_{NL}[v_a, v_b]$ est ramenée à un plan (nous reviendrons sur ces points particuliers dans la partie expérimentale).

Par ailleurs, une fois le modulateur QPSK inséré dans le montage générateur de chaos, nous n'avons accès aux réglages de ses paramètres (afin d'ajuster son point de fonctionnement) que par les tensions des bias appliquées à ses électrodes DC. Dans la section suivante, nous allons donc étudier l'effet de ces tensions sur l'allure globale de la fonction non linéaire $f_{NL}[v_a, v_b]$.




(*a*) *Vue en 3D*




(*b*) *Vue de dessus*

FIGURE 2.8 – *Fonction non linéaire bidimensionnelle du modulateur QPSK. Paramètres de simulation* : $\phi_1 = 0,9$ rad ; $\phi_2 = -0,7$ rad ; $\phi_3 = 1,5$ rad ; $P_0 = 2$ ;

### 2.2.1.c Influence des tensions de bias sur la non linéarité

Pour l'étude de l'influence des tensions de bias sur la non linéarité, la démarche suivie repose sur le principe de fixer à la fois tous les paramètres du modulateur QPSK, puis de faire varier un seul d'entre eux ($\phi_1$, $\phi_2$ ou $\phi_3$). Nous avons utilisé à cette fin les paramètres donnés au tableau 4.10 et fixé les tensions DC arbitrairement.

Les résultats obtenus peuvent être commentés de la manière suivante : une variation de $\phi_1$ induit une *translation horizontale* de la cannelure de la fonction non linéaire (figures 2.9), alors que $\phi_2$ induit une *translation verticale* de celle-ci (figures 2.10). Contrairement à l'action sur $\phi_1$ et $\phi_2$, le déphasage statique $\phi_3$ agit directement sur le contraste

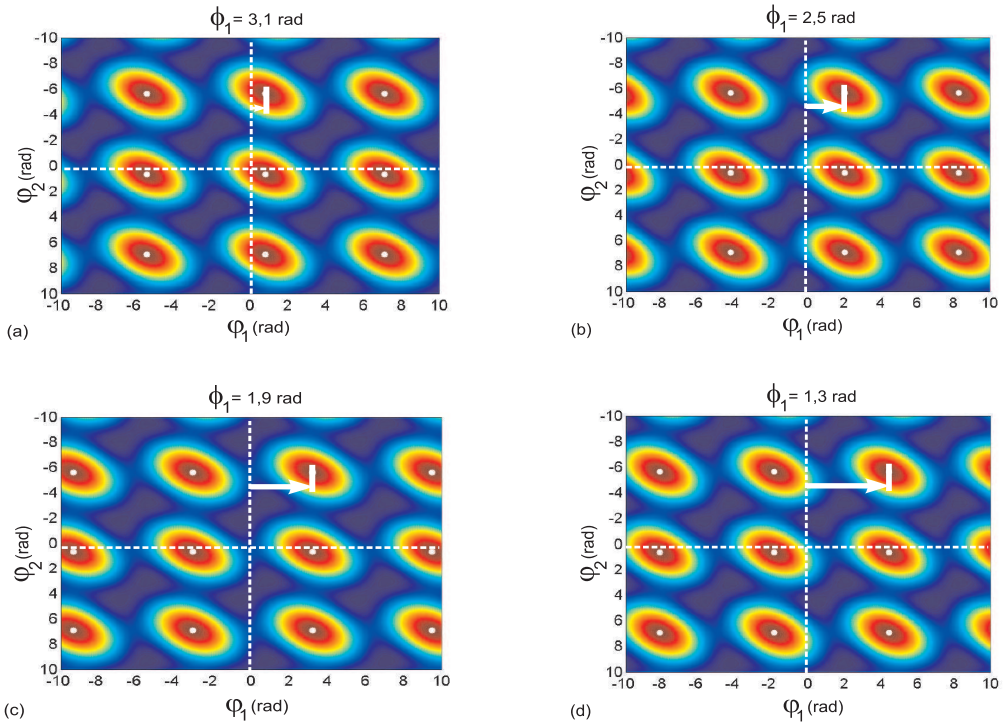



FIGURE 2.9 – *Influence de la tension $V_{DC1}$ : translation horizontale de la cannelure.*

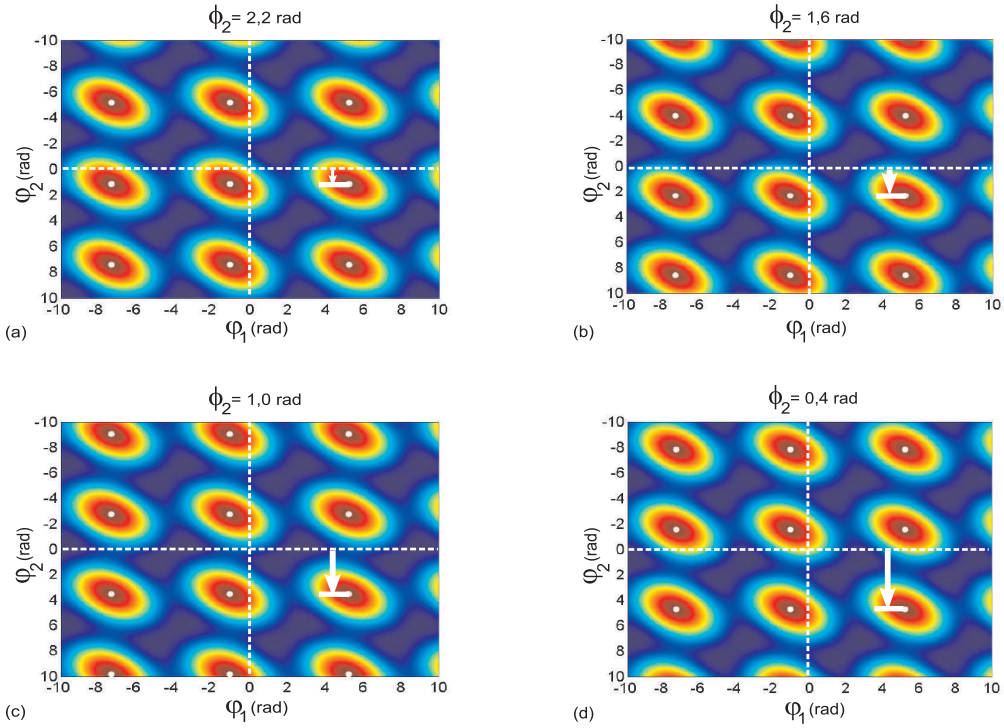
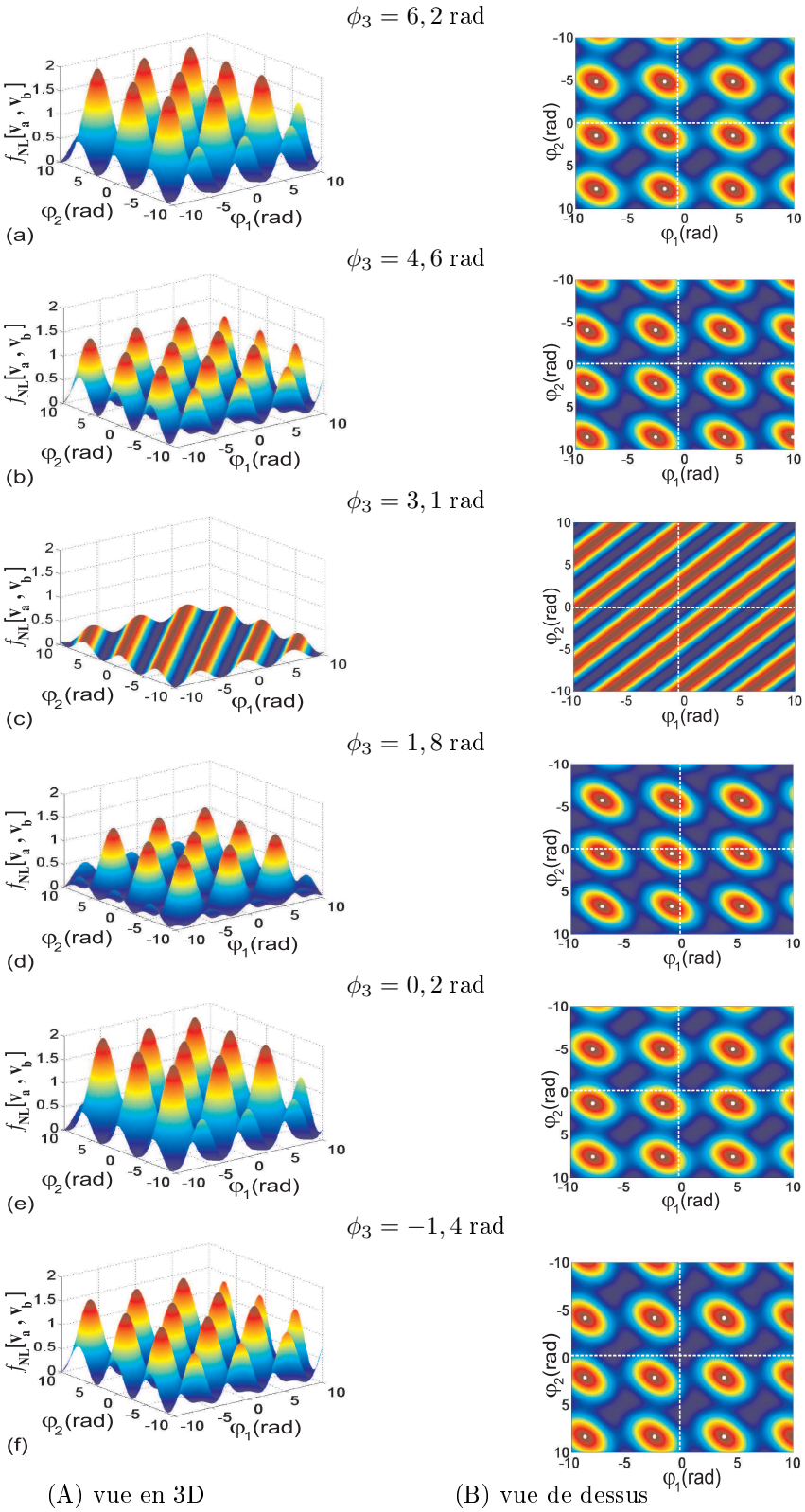



FIGURE 2.10 – *Influence de la tension $V_{DC2}$ : translation verticale de la cannelure.*




(A) vue en 3D (B) vue de dessus

Figure 2.11 – *Influence de la tension de bias $V_{DC3}$.*

de la figure d'interférence. En effet, les résultats obtenus – figures 2.11 – montrent comment l'amplitude de la non linéarité subit soit un étirement ou une affinité selon l'axe $f_{NL}[v_a, v_b]$.

Ainsi, nous venons de voir que les tensions de commandes ($V_{DC1}$, $V_{DC2}$ et $V_{DC3}$) permettent de contrôler, et donc d'avoir la possibilité de faire un choix adéquat de la condition d'interférence au point de repos du modulateur QPSK. À titre d'exemple, l'extinction de l'un des interféromètres $MZ_{1,2}$ (interférences destructives) correspond à $\phi_{1,2} = \pm\,\pi$ mod $[2\pi]$, ce qui réduit $f_{NL}[v_a, v_b]$ dans ce cas à la non linéarité[6] d'un MZ simple.

À présent, nous allons aborder dans la partie qui suit les autres composants du générateur de chaos. Ces composants qui constituent chaque boucle de rétroaction sont : la source lumineuse, le retard temporel et la chaîne optoélectronique de détection, de filtrage et d'amplification. La caractéristique commune de tous ces éléments est la linéarité de leur fonction de transfert.

### 2.2.2 Les éléments linéaires du générateur de chaos

À l'exception du modulateur QPSK, les différents éléments restants de l'oscillateur chaotique sont classiques et linéaires. Pratiquement, nous avons une grande variété de choix de ces composants, ce qui constitue un très grand nombre de clés de codage. Les deux boucles de rétroaction sont constituées de mêmes éléments, mais de caractéristiques choisies différentes, car nous rappelons que l'objectif est d'augmenter le nombre de paramètres de la clé cryptographique.

#### a. La source laser

Comme nous l'avons signalé précédemment dans la description globale du système (section 1.6.2), la source lumineuse de notre générateur de chaos est une diode laser monomode, dont la longueur d'onde d'émission est $\lambda_0 \simeq 1,55\ \mu m$ (valeur quelconque *à priori*). Il est important de noter qu'il n'y a aucune dynamique propre au laser lui-même ; il sert seulement de source d'énergie optique continue, qui alimente l'entrée optique du modulateur QPSK, mais il n'intervient nullement dans le processus dynamique (contrairement aux lasers à cavité externe).

#### b. Retard temporel

Chacune des deux boucles de l'oscillateur chaotique contient un retard temporel. Un signal $s(t)$ à l'entrée de la boucle (A) est simplement transformé en $s(t-T_a)$ à la sortie de la boucle. Le même signal est transformé en $s(t-T_b)$ à la sortie de la seconde boucle (B).

[6] Les calculs détaillés sont disponibles en fin du manuscrit.

Pour réaliser expérimentalement cette fonction de retard, nous avons choisi la solution la plus simple et la plus efficace. Celle-ci consiste à insérer dans les boucles de l'oscillateur des longueurs de fibres optiques différentes. Le retard temporel ainsi introduit est donné par la relation suivante :

$$T = \frac{n}{c} \cdot L \tag{2.16}$$

où $c = 3.10^8\ m.s^{-1}$ est la vitesse de la lumière, $L$ est la longueur de la fibre optique et $n \simeq 1,5$ est l'indice de réfraction de la fibre à la longueur d'onde du faisceau laser. À titre d'exemple, une longueur de 20 $m$ de fibre optique correspond à un retard temporel de $0,1\ \mu s$. Ce retard est très grand par rapport aux temps de réponse des composants télécom ultra-rapides, et donc il garantit la génération d'un hyperchaos (la dimension étant de l'ordre du rapport retard sur temps de réponse).

**c. La chaîne optoélectronique d'amplification et de filtrage**

Chaque boucle de rétroaction du générateur de chaos est constituée d'un élément de détection, de filtrage et d'amplification. L'élément de détection est une photodiode qui convertit la puissance optique en signal électrique. L'élément de filtrage est un filtre passe-bande, dont le rôle est de limiter la dynamique chaotique du système. Enfin, un amplificateur variable permet d'ajuster le gain de boucle avant d'attaquer l'entrée électrique du modulateur QPSK par l'électrode RF.

Notons enfin que la chaîne optoélectronique comporte aussi 2 coupleurs optiques comme illustré sur la figure 2.12. Le premier coupleur permet de répartir la puissance optique issue du modulateur QPSK entre les deux boucles de rétroaction. Le second coupleur permet d'insérer le message utile et de transmettre le signal chaotique généré.

## 2.3 Mise en équations de l'émetteur

Le processus différentiel se modélise à partir de la fonction de transfert du filtre passe-bande de la branche électronique de l'oscillateur. Comme l'oscillateur est formé par 2 boucles de contre-réactions contenant 2 filtres passe-bande différents, nous adoptons pour désigner les paramètres de chaque boucle les notations suivantes (voir la figure 2.12) : tous les paramètres de la boucle (A) seront indexés par la lettre « a », et tous les paramètres de la boucle (B) seront indexés par la lettre « b ».

Ainsi, la dynamique globale est modélisée par 2 équations différentielles du second ordre à retard (système d'EDR) suivantes :

$$x_i(t) + [\tau_{1i} + \tau_{2i}]\frac{dx_i}{dt}(t) + \tau_{1i} \cdot \tau_{2i}\frac{d^2x_i}{dt^2}(t) = \beta_i \cdot \tau_{2i} \cdot \frac{d}{dt}\Big[f_{NL}[x_a, x_b](t - T_i)\Big] \tag{2.17}$$

où $(i = a, b)$ selon la boucle concernée, et les autres paramètres sont définis un peu plus

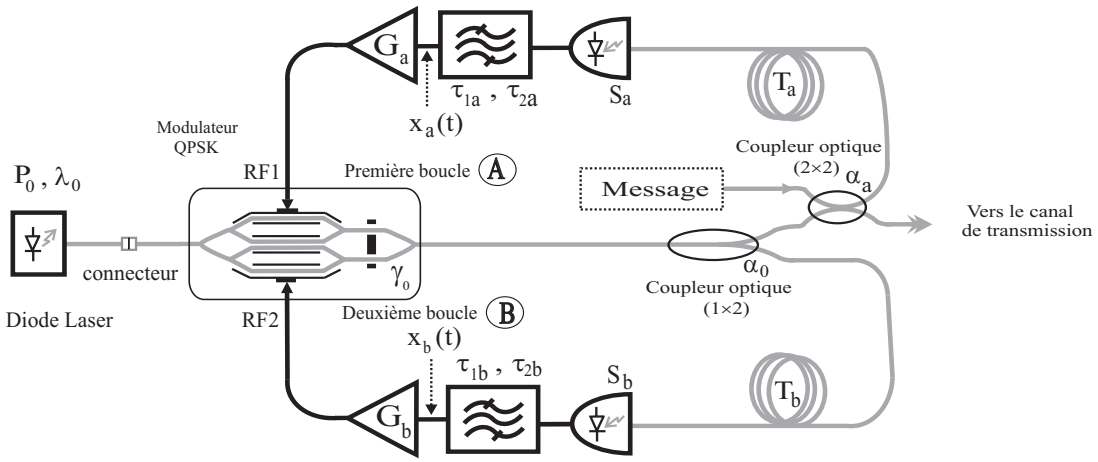



Figure 2.12 – *Schéma bloc du système émetteur.*

loin. Le système d'EDR (2.17) est obtenu selon les étapes détaillées à la section 1.2.2, et il peut se réécrire encore sous la forme d'un système d'EDR du premier ordre suivant :

$$\begin{cases} x_i(t) + \tau_{2i} \,.\, \dfrac{dx_i}{dt}(t) = \dfrac{\tau_{2i}}{\tau_{1i}} \,.\, \Big[\beta_i \,.\, f_{NL}\left[x_a, x_b\right](t - T_i) - y_i(t)\Big] \\ y_i(t) + \tau_{1i} \,.\, \dfrac{dy_i}{dt}(t) = \beta_i \,.\, f_{NL}\left[x_a, x_b\right](t - T_i) \end{cases} \tag{2.18}$$

avec :

$x_i(t) = \pi.\frac{v_i(t)}{2.V_{\pi RF1,2}}$ et $y_i(t) = \pi.\frac{w_i(t)}{2.V_{\pi RF1,2}}$ : des variables normalisées de la boucle $i$ ;

$\tau_{1i} = \frac{1}{2.\pi.f_{c1i}}$ : constante de temps haute du filtre passe-bande de la boucle $i$ ;

$\tau_{2i} = \frac{1}{2.\pi.f_{c2i}}$ : constante de temps basse du filtre passe-bande de la boucle $i$ ;

$\beta_i = \frac{K_i \,.\, P_0 \,.\, \gamma_0}{2.V_{\pi RF1,2}} = \pi.\frac{P_0 \,.\, \gamma_0 \,.\, G_i \,.\, S_i \,.\, \alpha_0 \,.\, \alpha_a}{2.V_{\pi RF1,2}}$ : gain normalisé de la boucle $i$ avec :

$P_0$ : puissance optique de la diode laser ;
$\gamma_0$ : coefficient des pertes optiques du modulateur QPSK ;
$G_i$ : gain de l'amplificateur de la boucle $i$ ;
$S_i$ : sensibilité du photodétecteur de la boucle $i$ ;
$\alpha_0$ : coefficient de couplage du coupleur optique (1×2) ;
$\alpha_a$ : coefficient de couplage du coupleur optique (2×2). Ce coefficient n'apparaît pas pour la boucle (B) ;

$V_{\pi RF1,2}$ : tension demi-onde des interféromètres simples $MZ_{1,2}$ ;

$f_{NL}[x_a, x_b](t - T_i)$ : la fonction non linéaire vue par la boucle $i$, son expression est donnée par l'équation (2.15).

Maintenant que le générateur de chaos à modulateur QPSK est mis en équations, nous allons pouvoir le simuler numériquement. Dans un premier temps, nous avons implémenté sous le logiciel Matlab l'algorithme de la méthode prédicteur-correcteur résolvant le système d'EDR (2.18). Nous avons constaté malheureusement, à cause du nombre assez élevé d'opérations de calcul à effectuer, que le temps de calcul du langage Matlab est très long et coûteux en terme de mémoire. Nous avons donc opté pour l'implémentation de cette méthode en langage C, qui a l'avantage d'être beaucoup plus rapide.

## 2.4 Tests de validation

Dans le but de valider le programme de calcul de l'algorithme de la méthode de résolution numérique, nous avons effectué plusieurs tests de validation (réponses à un échelon, à une impulsion, à une sinusoïde). Par ailleurs, ces tests permettent aussi de déterminer les durées des régimes transitoires à supprimer, car les termes retardés $x_i(t - T_i)$ du système d'EDR (2.18) sont pris en compte seulement après un calcul jugé suffisant. Ce calcul sera donné au fur et à mesure qu'on présente certains tests.

L'approche adoptée consiste à observer la divergence naturelle d'une évolution dynamique obtenue par le programme implémenté, comparée à celle donnée par un modèle théorique exact. Le principe de celle-ci est de remplacer l'expression de $f_{NL}[x_a, x_b]$ dans le système d'EDR (2.18) par la fonction test, puis de comparer les résultats obtenus. Un exemple de calcul analytique est donné ci-dessous pour la réponse du système à un échelon.

L'ensemble des paramètres de simulation est donné au tableau 2.1. Ces paramètres sont choisis de manière à correspondre à la réalité expérimentale. On note que le pas d'intégration $h$ est choisi suffisamment petit, de telle sorte qu'il soit bien inférieur à la plus petite constante de temps du système, respectant ainsi la condition de précision de l'algorithme utilisé. On note aussi que les deux équations de (2.17) sont chacune du même type, et sont simulées bien sûr avec le même algorithme.

**- Exemple de test : réponse à un échelon**

En remplaçant $f_{NL}[x_a, x_b]$ par une constante qui vaut 1 (échelon unitaire), les équations du système (2.17) deviennent indépendantes. La solution analytique de la première équation par exemple est donnée par :

$$x_a(t) = \frac{\tau_{2a}}{\tau_{1a} - \tau_{2a}} \cdot R(t) \cdot \Big[ \exp(-t/\tau_{1a}) - \exp(-t/\tau_{2a}) \Big] \tag{2.19}$$

où $R(t)$ est la fonction de Heaviside (où fonction échelon).

| **Boucle (A)** | | **Boucle (B)** | |
|---|---|---|---|
| $T_a$ | 10 ns | $T_b$ | 7,2 ns |
| $f_{c1a}$ | 13 GHz | $f_{c1b}$ | 13 GHz |
| $f_{c2a}$ | 300 kHz | $f_{c2b}$ | 300 kHz |
| $\tau_{1a} = \frac{1}{2.\pi.f_{c1a}}$ | 12,2 ps | $\tau_{1b} = \frac{1}{2.\pi.f_{c1b}}$ | 12,2 ps |
| $\tau_{2a} = \frac{1}{2.\pi.f_{c2a}}$ | 0,53 $\mu$s | $\tau_{2b} = \frac{1}{2.\pi.f_{c2b}}$ | 0,53 $\mu$s |
| $\beta_a$ | 10,0 | $\beta_b$ | 10,0 |
| **Autres paramètres** | | | |
| Pas d'intégration $h$ | | 1 ps | |
| Intervalle d'intégration | | 600×$T_a$= 6 $\mu$s | |

TABLE 2.1 – *Paramètres de simulation utilisés pour les tests de validation.*

Avant d'analyser les résultats obtenus de ce test, une remarque s'impose ici à propos des constantes de temps de la solution (2.19) : le rapport ($\tau_{2a}/\tau_{1a} = 4,3.10^4$) est très grand, et par conséquent, les équations du systèmes EDR (2.17) sont des équations raides. Ce qui nous réconforte une fois de plus dans le choix de la méthode prédicteur-correcteur, qui est adaptée à ce type d'équation.

Les solutions analytique — équation (2.19) — et numérique du test sont tracées sur la figure 2.13a. D'après cette figure, la solution analytique coïncide avec celle calculée par la méthode d'intégration. Nous remarquons aussi que les deux courbes ne se superposent pas parfaitement, comme le confirme le calcul de l'écart entre les deux solutions (courbe de l'erreur). Cet écart est dû aux erreurs de troncature inhérentes à tous les calculs informatiques. Lorsqu'on observe l'évolution de la dynamique loin de l'origine, ce qui constitue un régime transitoire, on constate que les deux solutions convergent — figure 2.13b — et l'écart tend vers zéro.

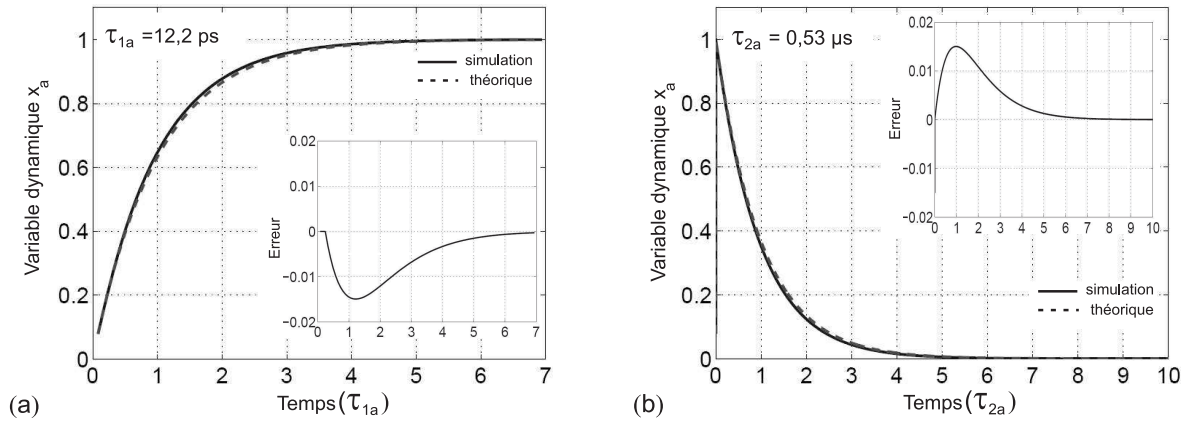



FIGURE 2.13 – *Réponse du système à un échelon unitaire.*

La durée du régime transitoire est calculée par analogie à la décharge d'un condensateur, qui est considérée complète à partir de $5\,\tau'$ (où $\tau'$ est la constante de temps de charge). Ce qui correspond dans le cas de la figure 2.13.b à un régime permanent considéré établi à partir de $5\,\tau_{2a}$.

Dans tous nos calculs de portion de trajectoire chaotique exempte de phénomènes transitoires, nous avons considéré que la durée minimale du transitoire est de $6\,\tau_{2a}$, ce qui correspond à environ à 3 million d'échantillons à supprimer, avec un pas $h$ de 1 ps.

Parmi les différents tests de validation, la figure 2.14a représente la courbe obtenue de la réponse impulsionnelle du système. L'impulsion d'entrée est retardée dans le temps de $5\,\tau_{2a}$, et l'algorithme de calcul réagit de la même façon. Le dernier test effectué est de remplacer la fonction d'excitation $f_{NL}[x_a, x_b]$ par une sinusoïde. Ce test nous renseigne particulièrement sur la valeur moyenne de la réponse du système en régime permanent. Théoriquement, celle-ci doit être nulle au delà du régime transitoire, et comme on peut le constater sur la figure 2.14b, cette propriété est vérifiée.

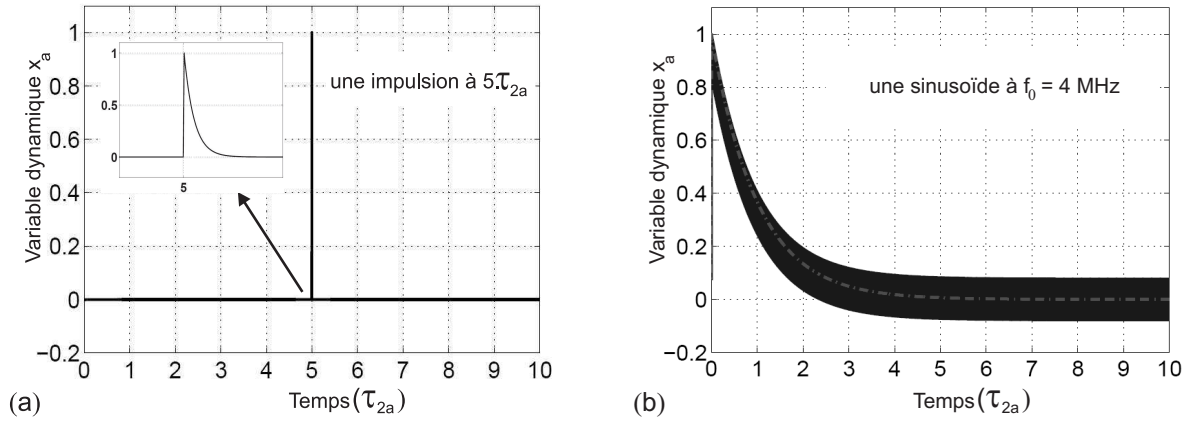



FIGURE 2.14 – *Réponse numérique du système du second ordre passe-bande. (a) à une impulsion. (b) à une sinusoïde.*

## 2.5 Conclusion

Ce chapitre a été consacré à la description et à la modélisation du générateur de chaos proposé. Nous avons commencé par donner quelques rappels de base sur les interféromètres électro-optiques intégrés sur le $LiNbO_3$, jugés nécessaires pour appréhender l'architecture et le fonctionnement complexe du modulateur QPSK. Nous avons ensuite déterminé la fonction de transfert de ce modulateur qui représente la fonction non linéaire bidimensionnelle du système.

Par la suite, nous avons décrit avec plus de détails les principales fonctions de ce générateur, en commençant par sa fonction non linéaire. Puis, nous avons décrit les chaînes optoélectroniques et l'ensemble des éléments linéaires. Enfin, nous avons mis le système

sous forme d'un système d'EDR du second ordre. Le modèle théorique ainsi obtenu est implémenté, puis validé en opérant quelques tests de validation.

Dans le chapitre suivant, cette modélisation va nous permettre de simuler numériquement l'oscillateur à modulateur QPSK, en explorant en particulier sa capacité à produire des dynamiques chaotiques complexes.

# Chapitre 3

# Étude numérique et analyse du système cryptographique

À travers la modélisation du générateur de chaos à modulateur QPSK qui vient d'être faite, nous allons pouvoir le simuler numériquement et analyser les solutions calculées. L'ensemble des outils — diagramme de bifurcation, diagramme entropique, section de Poincaré, ... etc — qui seront utilisés pour l'étude des évolutions dynamiques générées est présenté au chapitre 1. Le présent chapitre expose les résultats obtenus en utilisant ces outils, et il est constitué de 3 parties.

La première est consacrée à une discussion approfondie sur l'émetteur par des analyses temporelles, spectrales et statistiques, suivie d'une autre analyse dans l'espace des phases et par la fonction d'autocorrélation. Ces deux analyses vont nous permettre d'explorer les dynamiques générées par une première architecture de l'oscillateur formée par une seule boucle, puis dans une seconde architecture formée par deux boucles.

La deuxième partie sera dédiée à l'étude de l'influence de certains paramètres — le point de fonctionnement du QPSK, les retards temporels, les bandes passantes — constituant la clé de cryptage sur la dynamique chaotique générée. Cette étude nous permettra d'identifier les paramètres du système à choisir, dans la perspective d'assurer une confidentialité optimale des transmissions. Le choix de ces paramètres est basé essentiellement sur la complexité et la stationnarité du chaos engendré.

La troisième et dernière partie sera consacrée au système cryptographique complet émetteur-récepteur. Et comme la plupart des approches de la transmission chaotique sont basées sur la synchronisation du chaos, nous rappellerons quelques unes des techniques les plus utilisées. Puis nous donnerons une vue d'ensemble des principaux schémas de transmission chaotique envisageables dans le cadre de ce système de transmission. Nous consacrerons en fin de chapitre une section à l'étude de la sensibilité de la synchronisation, après avoir fixé les conditions de couplage permettant un décodage de bonne qualité.

| **Boucle (A)** | | **Boucle (B)** | |
|---|---|---|---|
| $T_a$ | 61 ns | $T_b$ | 60 ns |
| $f_{c1a}$ | 13 GHz | $f_{c1b}$ | 13 GHz |
| $f_{c2a}$ | 50 kHz | $f_{c2b}$ | 30 kHz |
| **Paramètres de la non linéarité** | | | |
| $V_{\pi DC1}$ | 7,40 V | | |
| $V_{\pi DC2}$ | 7,14 V | | |
| $V_{\pi DC3}$ | 14,24 V | | |
| $V_{\pi RF1}$ | 5,84 V | | |
| $V_{\pi RF2}$ | 6,08 V | | |
| **Autres paramètres** | | | |
| Pas d'intégration $h$ | 1 ps | | |
| Intervalle d'intégration | $700 \times T_a = 42{,}7$ $\mu$s | | |
| Intervalle de l'histogramme $N_H$ | 250 | | |

TABLE 3.1 – *Paramètres utilisés pour les simulations numériques.*

L'ensemble des paramètres de simulation qui sont utilisés dans nos investigations numériques est donné au tableau 3.1. Ce sont typiquement les paramètres de fonctionnement du générateur de chaos expérimental.

## 3.1 Système à une seule boucle de rétroaction

On entend par le système à une seule boucle le cas où, expérimentalement, l'une des boucles de rétroaction est laissée ouverte. Cela revient à considérer numériquement un gain global de celle-ci nul ($\beta_a = 0$ ou $\beta_b = 0$). Nous avons choisi la boucle (A) afin d'étudier le système dynamique à une seule rétroaction.

### Condition d'interférence au point de repos du QPSK

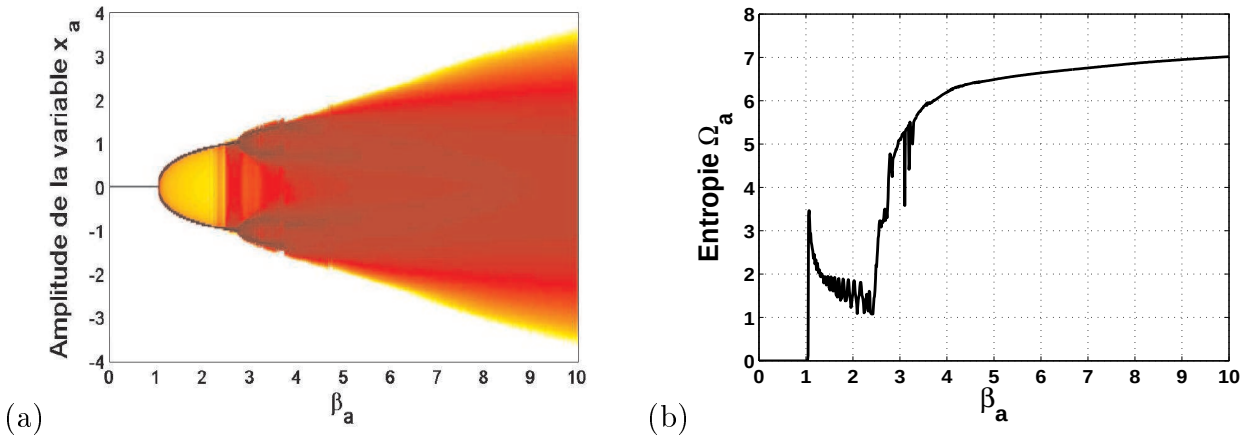
Dans l'étude qui suit, le point de fonctionnement du QPSK est fixé de manière à ramener sa fonction de transfert à celle d'un MZ simple. Ainsi, l'expression de la non linéarité (2.15) se réduit à (3.1), et la condition d'interférence ($\phi_1 = \phi_2 = 1,2$ rad ; $\phi_3 = 0$ rad) est choisie de façon à positionner ce point sur la partie linéaire de la cannelure du seul $MZ_1$ actif dans cette configuration.

$$f_{NL}[v_a, v_b] = P_0 \cos^2(\psi_1) \tag{3.1}$$

### 3.1.1 Diagramme de bifurcation et diagramme entropique

Les bifurcations sont des changements qualitatifs des propriétés d'une solution dynamique. Elles interviennent lors de l'évolution d'un paramètre du système, qui dans notre cas correspond principalement au gain de boucle. Un diagramme de bifurcation permet de mettre en évidence le type d'évolution temporelle sous la forme d'une densité de probabilité en fonction de ce paramètre.

Mais cet outil de représentation visuelle a ses limites, comme par exemple la non distinction parmi les régimes chaotiques des régimes qualifiés de breathers chaotiques [102]. Ces derniers sont des oscillations chaotiques sur une échelle de temps courte, mais quasi-périodique sur l'échelle de temps lente. Leurs comportements ne permettent pas un codage d'une information à flux continu dans le temps (codage de l'information en "clair" dans les intervalles de temps où les bouffées chaotiques sont absentes).




(a) (b)

Figure 3.1 – *Système à une seule boucle de rétroaction.* $\beta_b = 0$. (*a*) *diagramme de bifurcation.* (*b*) *diagramme entropique.*

La figure 3.1 illustre les diagrammes de bifurcation et entropique du générateur de chaos lorsque la boucle (B) est ouverte ($\beta_b = 0$). Ces diagrammes sont tracés en fonction du gain global normalisé $\beta_a$, avec tous les autres paramètres constants (tableau 3.1). À travers ces deux diagrammes, la description de l'évolution du comportement dynamique du système à une seule boucle peut se faire de la façon suivante :

- Pour de faibles valeurs du paramètre de bifurcation ($\beta_a < 1$), le système n'oscille pas car le gain de boucle est inférieur aux pertes. Les régimes dynamiques sont donc des points fixes stables et l'entropie, qui mesure le degré de désordre de l'évolution temporelle, est nulle. Soumis à une perturbation, le système revient systématiquement au point fixe initial. On constate autour de $\beta_a = 1$, une évolution du point fixe stable vers une solution périodique. La première bifurcation (bifurcation de Hopf) se produit alors, et elle fait apparaître un premier saut sur le diagramme entropique.

- En augmentant le gain ($\beta_a > 1$), la route vers le chaos est entamée par des régimes périodiques. Le système commence à osciller entre 2 niveaux, puis il subit une succession de bifurcations au fur et à mesure que le gain augmente jusqu'à environ $\beta_a \approx 3,8$. Nous distinguons à première vue dans cet intervalle sur le diagramme de bifurcation les régimes périodiques d'ordre 2, puis d'ordre 4.

  Nous remarquons aussi dans la plage de variation ($2 < \beta_a < 3$) qu'il y a un changement brusque de couleur de la densité de probabilité, ce qui indique que d'autres régimes périodiques supplémentaires (ou pseudo-périodiques) coexistent dans cet intervalle. Cette hypothèse se traduira par un élargissement de spectre lors d'une analyse spectrale où encore l'apparition de plusieurs niveaux sur la densité de probabilité (nous reviendrons un peu plus loin sur cette remarque). La courbe de l'entropie confirme en partie cette hypothèse et enregistre à chaque bifurcation un pic croissant ou décroissant (un artéfacts de calcul). Ces pics traduisent un signal de moins en moins ordonné, et de plus en plus instable jusqu'à environ $\beta_a = 2,8$. Ensuite, l'entropie augmente continûment jusqu'à saturation, signature d'un déterminisme sous-jacent (pour un phénomène strictement aléatoire[1] au sens mathématique, l'entropie prend une valeur infinie) [103].

- Pour $\beta_a \approx 3$ ; des régimes chaotiques complexes commencent à apparaître, ce qui constitue une limite représentant l'analogue du point d'accumulation, bien connu dans le cas des dynamiques discrètes. Au delà de ce point les régimes dynamiques sont entièrement chaotiques, ce qui se confirme encore par leur entropie élevée, caractéristique d'un signal désordonné.

Les diagrammes que nous venons de décrire correspondent à un point de fonctionnement bien précis du modulateur QPSK ($\phi_1 = \phi_2 = 1,2$ et $\phi_3 = 0$ rad). Mais lorsque celui-ci est différent de ce point, nous allons voir qu'il est nécessaire de faire un choix adéquat de la condition d'interférence afin d'obtenir une dynamique chaotique.

**Choix des paramètres : $\phi_1$, $\phi_2$ et $\phi_3$**

Pour une investigation plus globale de la dynamique du système en fonction de la condition d'interférence, nous considérons dans ce qui suit les déphasages statiques du QPSK comme paramètres de bifurcation, possibilité tout à fait réalisable expérimentalement, en ajustant les tensions des bias. Le gain de la boucle (A) est fixé à une valeur élevée ($\beta_a = 10$), permettant ainsi d'assurer au système, d'après le diagramme de la figure 3.1a, un régime dynamique de nature chaotique.

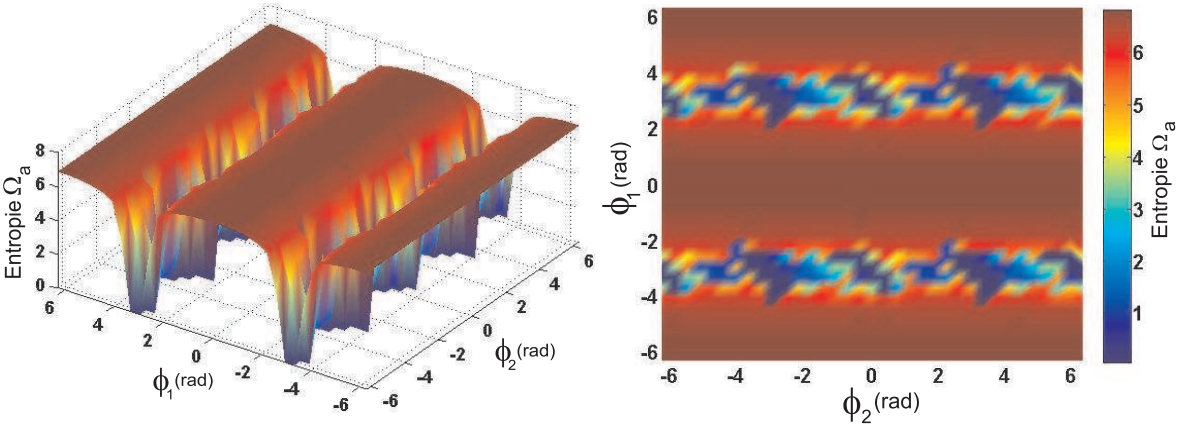
La figure 3.2 montre le diagramme entropique obtenu lorsque les déphasages $\phi_1$ et $\phi_2$ sont variés et $\phi_3$ fixe. À certaines valeurs (aux alentours de $\phi_1 = 0 \bmod[2\pi]$, et $\forall\ \phi_2$), on constate que l'entropie sature à une valeur autour de 6 – 8. Celle-ci se trouve justifiée

[1] L'entropie d'une variable aléatoire continue est infinie. Ce résultat est intuitif, car une variable aléatoire continue peut prendre une infinité de valeurs sur $\mathbb{R}$, et cela implique que la probabilité sur une valeur tend vers 0 et donc, à cause du logarithme, l'entropie tend vers l'$\infty$.

— relation (1.8) — par le nombre de segments utilisés ($N_H = 250$), pour le calcul de la distribution de probabilité.

$$\log_2(N_H) = \log_2(250) \simeq 7,9 \tag{3.2}$$

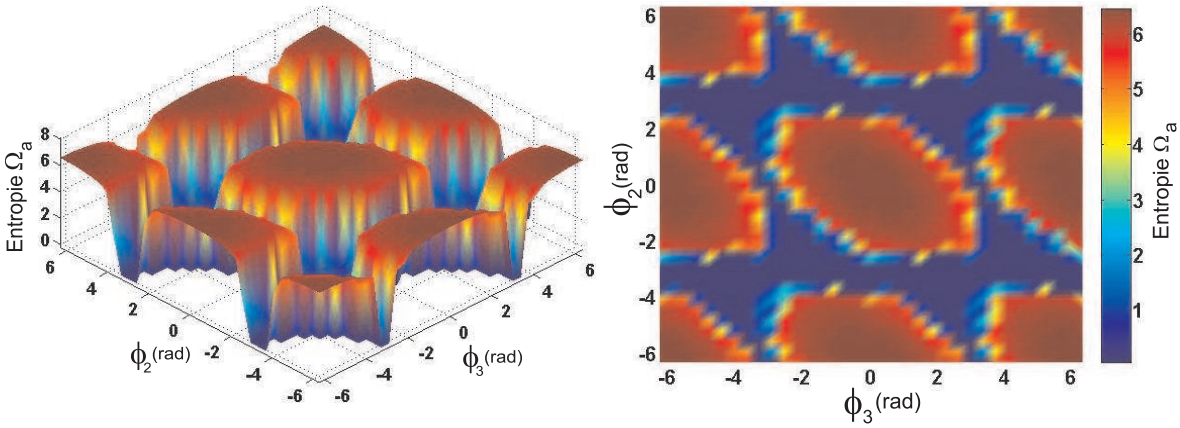
On constate aussi qu'aux environs de ($\phi_1 = \pi \bmod[2\pi]$, et $\forall\ \phi_2$), l'entropie est minimale voire nulle. Ce constat est trivial, car l'interféromètre de la boucle de rétroaction $MZ_1$ est dans ce cas en extinction, et de plus, aucune modulation RF n'est appliquée sur le $MZ_2$ (système à une seule boucle).




(a) Vue en 3D (b) Vue de dessus

Figure 3.2 – *Diagramme entropique en fonction de $\phi_1$ et de $\phi_2$ du système à une seule boucle. Paramètres de simulation : $\beta_a = 10$ ; $\beta_b = 0$ ; $\phi_3 = 0$ rad.*

En résumé, on déduit du diagramme de la figure 3.2, qu'à la condition $\phi_3 = 0$ rad, le système en architecture à une seule boucle peut générer des régimes chaotiques complexes (entropies maximales) en choisissant $\phi_1$ autours de 0 mod[$2\pi$] rad, et que le paramètre $\phi_2$




(a) Vue en 3D (b) Vue de dessus

Figure 3.3 – *Diagramme entropique en fonction de $\phi_2$ et de $\phi_3$ du système à une seule boucle. Paramètres de simulation : $\beta_a = 10$ ; $\beta_b = 0$ ; $\phi_1 = 1,5$ rad.*

n'a pas (ou peu) d'influence dans ces conditions. Mais à cause de son impact direct sur l'amplitude de la non linéarité, lorsque le paramètre $\phi_3$ est différent de la valeur indiquée précédemment, il devient nécessaire de bien choisir le domaine de variation de $\phi_2$ afin d'obtenir une dynamique chaotique. Ce choix peut s'effectuer par exemple à partir du diagramme entropique représenté sur la figure 3.3. D'après ce diagramme, on constate qu'aux alentours de certaines valeurs ($\phi_2 = \pi \mod[2\pi]$ : extinction du $MZ_2$, et $\phi_3 = \pi \mod[2\pi]$), l'entropie reste faible malgré le gain élevé de la boucle de rétroaction ($\beta_a = 10$). Par contre, aux voisinages de $\phi_2 = \phi_3 = 0 \mod[2\pi]$, ce qui correspond physiquement à une condition d'interférence autour du maximum de transmission de la puissance optique du modulateur QPSK (i.e : $|f_{NL}[.]| \approx 1$), l'entropie est nettement plus élevée. Ainsi, on peut choisir sans grande difficulté les paramètres $\phi_2$ et $\phi_3$ autours de ce maximum de transmission.

Nous venons de donner un moyen graphique, permettant de choisir la condition d'interférence du QPSK, en se basant sur le critère de l'entropie maximale finie, caractéristique d'un signal chaotique complexe. Nous venons aussi de décrire les diagrammes de bifurcation et entropique du système à une seule boucle. Ces diagrammes représentent une vue de l'ensemble des comportements dynamiques — points fixes, périodiques et chaotiques — que peut générer le système. Nous allons à présent approfondir l'analyse de ces divers comportements, et explorer ce qui se passe à l'intérieur de ces dynamiques.

### 3.1.2 Analyse temporelle, statistique et spectrale

Avec une boucle du système ouverte et suivant les valeurs du gain de la boucle fermée, nous pouvons obtenir des traces temporelles de différents types. Afin de les analyser, nous avons choisi 4 régimes sur le diagramme de bifurcation de la figure 3.1a. Ces régimes sont révélateurs et correspondent à des valeurs de $\beta_a$ illustrant 2 régimes périodiques et 2 régimes chaotiques.

#### Régimes périodiques

La figure 3.4 illustre un régime périodique d'ordre 2, correspondant à feedback considéré faible $\beta_a = 1,5$. Cette évolution périodique est nettement visible sur la densité de probabilité, ainsi que sur la trace temporelle. On observe sur cette dernière — figure 3.4a — une période de l'ordre de $2\,T_a$ et un signal dont les plateaux sont légèrement inclinés, à cause de la fréquence de coupure basse qui filtre les composantes continues (les plateaux sont constants dans le cas d'une dynamique passe-bas) [104]. On retrouve aisément sur le spectre[2] — figure 3.4c — l'inverse de la période observée : $(2T_a)^{-1} = 8,19$ MHz.

[2]La résolution de la FFT calculée est de : $1/(h\,.\,2^{23}) = 119.2$ kHz ; avec $h = 1$ ps est le pas d'échantillonnage, et $2^{23}$ est le nombre d'échantillons de la trace temporelle.

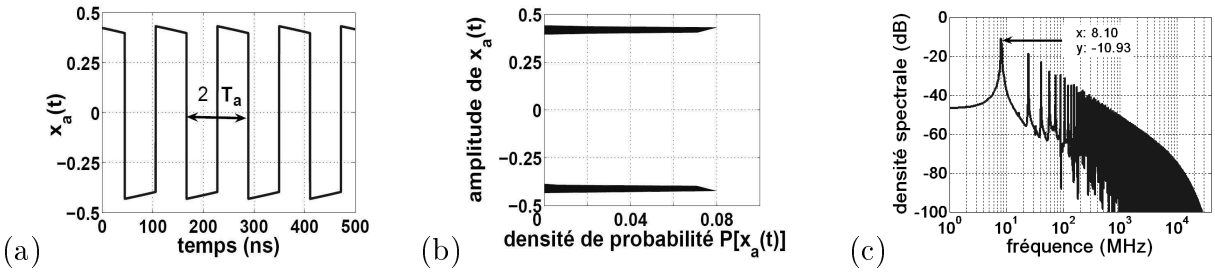



FIGURE 3.4 – *Système à une seule boucle de rétroaction.* $\beta_a = 1,5$ ; $\beta_b = 0$
*Régime périodique d'ordre* 2.

En augmentant le paramètre de bifurcation ($\beta_a = 3,5$), un régime pseudo−périodique est observé, comme le montre la figure 3.5. La répartition de la densité de probabilité montre l'existence de 4 pics dominants, avec toutefois une forte densité au pied de chaque pic. Cette dernière explique en partie les changements brusques de couleurs, que nous avons évoqué précédemment dans le diagramme de bifurcation (figure 3.1a). Le système possède donc un motif pseudo-périodique, de période $4T_a$, comme l'indique le pic spectral de la figure 3.5c : $(4T_a)^{-1} = 4,09$ MHz.

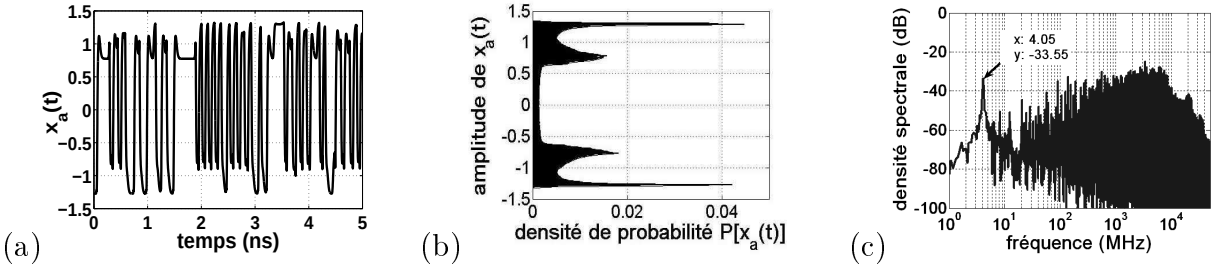



FIGURE 3.5 – *Système à une seule boucle de rétroaction.* $\beta_a = 3,5$ ; $\beta_b = 0$
*Régime pseudo-périodique.*

### Régimes chaotiques

Le diagramme de bifurcation — figure 3.1a — nous indique qu'au delà de $\beta_a \approx 4$, les régimes obtenus sont chaotiques. Pour vérifier cette indication et explorer donc la dynamique générée, nous avons choisi deux valeurs du gain $\beta_a$ supérieures à cette valeur.

La figure 3.6 illustre un régime chaotique obtenu pour la première valeur $\beta_a = 5,5$. Ce régime dynamique est caractérisé par une trace temporelle d'apparence bruitée et un spectre quasi-plat (aucune fréquence n'est privilégiée). Cependant, comme on peut le remarquer sur la figure 3.6b, la distribution de la densité de probabilité n'est pas gaussienne,

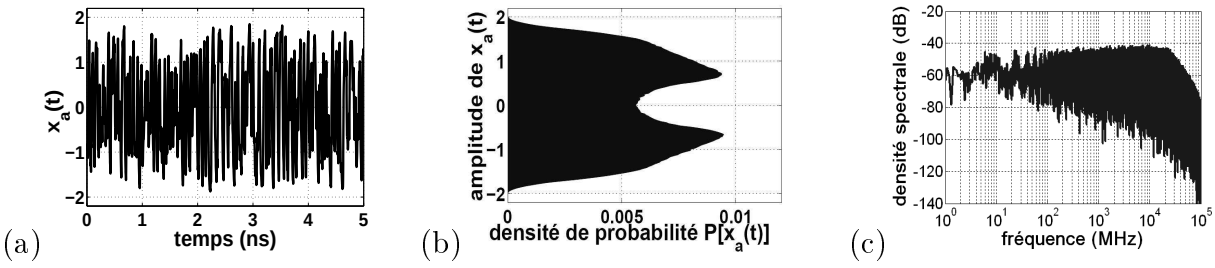



FIGURE 3.6 – *Système en une seule boucle de rétroaction.* $\beta_a = 5,5$ ; $\beta_b = 0$
*Régime chaotique non gaussien.*

contrairement au profil associé à la deuxième valeur élevée ($\beta_a = 9,5$) du paramètre de bifurcation représenté sur la figure 3.7b. Le régime dynamique observé en cette dernière valeur de $\beta_a$ est entièrement chaotique, et son spectre est plat.

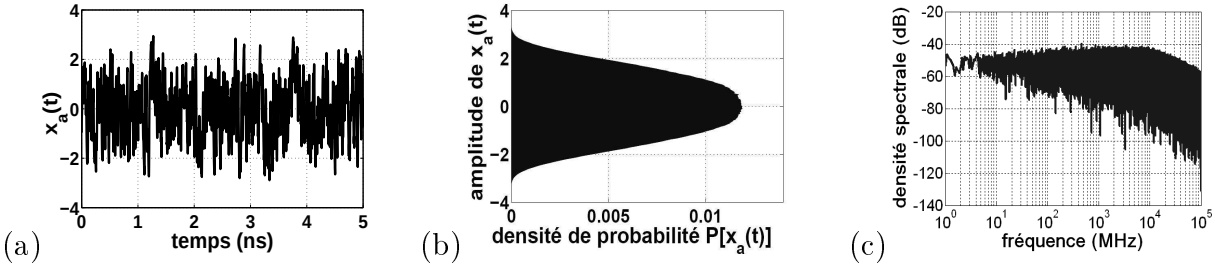



FIGURE 3.7 – *Système à une seule boucle de rétroaction.* $\beta_a = 9,5$ ; $\beta_b = 0$
*Régime chaotique gaussien.*

Les différents types de signaux que nous venons de présenter sont représentatifs de la multitude de régimes dynamiques, que peut produire ce générateur de chaos. Nous allons investir encore ces dynamiques par d'autres moyens, qui vont nous permettre par la suite de bien les cerner et de mieux comprendre les diverses routes possibles vers le chaos.

### 3.1.3 Autocorrelation et carte de premier retour

Une représentation graphique du régime dynamique dans un espace des phases n'est pas évidente. Car en général, les méthodes couramment utilisées pour définir les coordonnées de cet espace sont d'utiliser les variables $x(t)$ et $\dot{x}(t)$ pour un espace des phases à 2 dimensions. Une autre méthode plus adaptée à partir d'une dynamique disponible par sa série temporelle $x(t)$, consiste à choisir des valeurs instantanées de $x(t)$. Par conséquent, des coordonnées en 2D sont obtenus en formant un point par $(x(t),\ x(t-\tau_i))$, où $\tau_i$ est un intervalle de temps [105].

Dans notre cas, la seconde méthode est adaptée[3] à notre système à une seule boucle. En effet, il est possible de donner une représentation qualitative simplifiée de l'attracteur à partir de $x_a(t)$ dans un espace des phases en prenant le délai $T_a$ pour intervalle $\tau_i$. Dans ce cas, nous obtenons des coordonnées de $x_a(t)$ et de $x_a(t - T_a)$. Ce choix est justifié par la simple raison que ce délai se révèle par la fonction d'autocorrélation.

En effet, cette fonction contient la " mémoire " du signal, et permet donc d'accéder à la mesure de sa persistance [103]. Dans le cas d'un signal périodique, la mémoire persiste uniformément — il y a corrélation forte d'un instant à l'autre — tandis que dans le cas du bruit blanc — la corrélation est strictement nulle — il n'y a aucune mémoire à cause de l'absence totale d'une organisation temporelle.

Dans les paragraphes suivants (valable aussi pour la section 3.2.3), les quatre représentations sont toutes disposées sur 2 lignes et 2 colonnes. Sur la première ligne, la courbe (a) représente le diagramme dans l'espace à 2 dimensions, et la courbe (b) celui à 3 dimensions. Ces deux diagrammes sont tracés pour une durée de 5 fois $T_a$ (pour le système en double boucle ; voir le dernier paragraphe de cette section). Sur la deuxième ligne, la courbe (c) représente la section de Poincaré réalisée à partir du diagramme des phases en 3 dimensions à $x_a(t - 2\,T_a) = 0$. La courbe (d) représente la fonction d'autocorrélation calculée à partir de la trace temporelle $x_a(t)$ sur une durée de 915 ns, équivalente à 15 fois le délai $T_a$.

### Régimes périodiques

La figure 3.8a illustre un attracteur reconstruit dans un espace des phases à 2 dimensions pour $\beta_a = 2,2$. La trajectoire de cet attracteur est un cycle limite stable où deux régions dans l'espace des phases sont fréquemment visitées. La coupe de Poincaré — figure 3.8c — permet facilement de retrouver ces deux régions. La courbe de la fonction d'autocorrélation est périodique, de période 122,1 ns. Cette dernière correspond à une valeur légèrement surestimée [106] de $2\,T_a$. L'origine de la surestimation est due principalement à la constante de temps rapide du système.

Lorsque le paramètre de bifurcation est un peu plus élevé ($\beta_a = 3,1$), un attracteur quasi-périodique apparaît (figure 3.9a). On observe sur ce diagramme un nuage de points particulièrement dense dans quelques régions, et moins dense autour de la trajectoire. L'aspect dense du nuage de points signifie que cette région de l'attracteur est fréquemment visitée par la variable dynamique.

Par rapport à la reconstruction dans l'espace des phases en 2 D, la topologie de l'attracteur en 3 D — figure 3.9b — illustre encore mieux le tracé de la trajectoire de cet attracteur pseudo-périodique. Dans la coupe de Poincaré (figure 3.9c), on retrouve 4 groupes de points qui représentent les 4 régions les plus visitées de l'attracteur. Les pics de la fonction d'autocorrélation — figure 3.9d — ont une amplitude assez importante aux multiples du délai $T_a$ ; ce qui se traduira lors d'une éventuelle cryptanalyse par une identification facile du retard temporel du système.

[3]Le système est de dimension infinie, donc son "vrai" espace des phases est aussi infini. Il est donc impossible à représenter, et la simplification consiste à projeter cet espace dans un autre à 2 dimensions (mais qui n'est pas l'espace des phases). Cet espace à 2D est parfois appelé carte de premier retour quand on prend, comme dans notre cas, $[x_a(t), x_a(t - T_a)]$ comme coordonnées de cet espace.

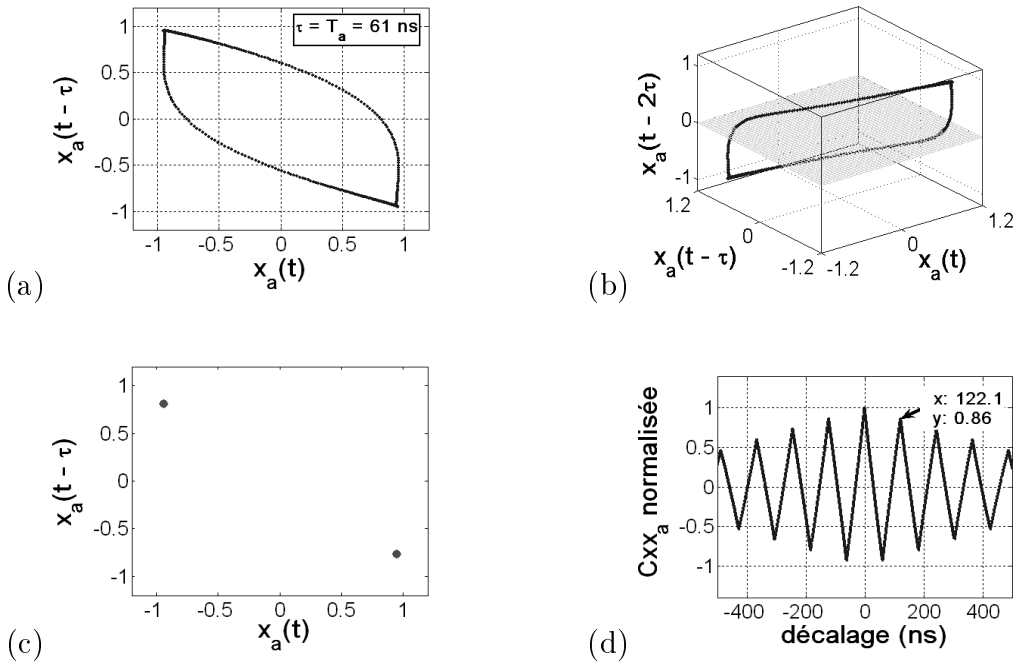



FIGURE 3.8 – *Système à une seule boucle de rétroaction.* $\beta_a = 2,2$ ; $\beta_b = 0$ *Régime périodique d'ordre* 2.

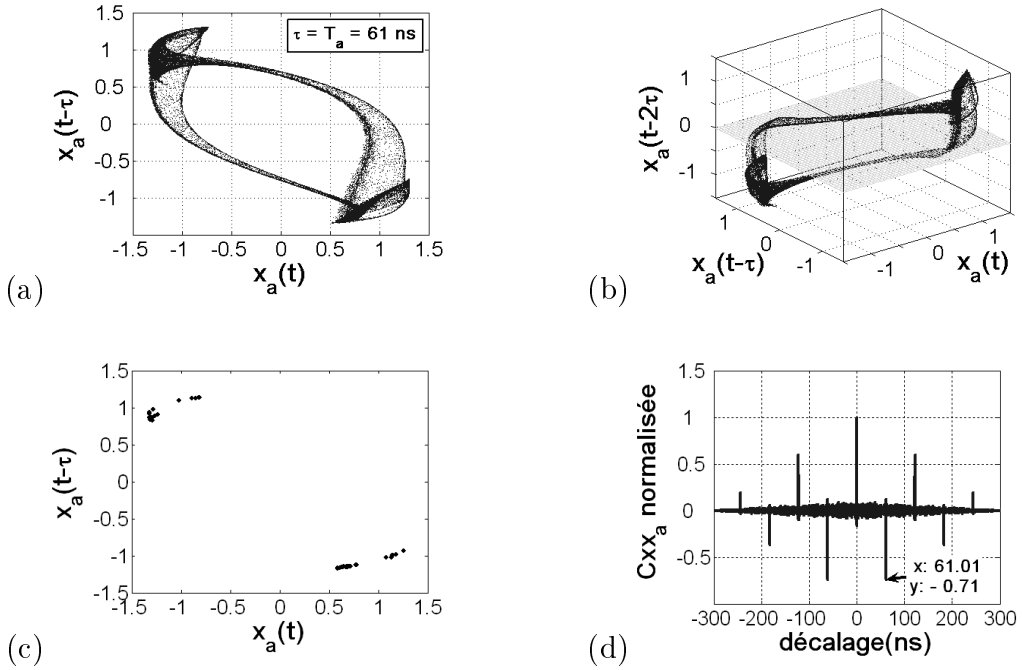



FIGURE 3.9 – *Système à une seule boucle de rétroaction.* $\beta_a = 3,1$ ; $\beta_b = 0$ *Régime pseudo-périodique.*

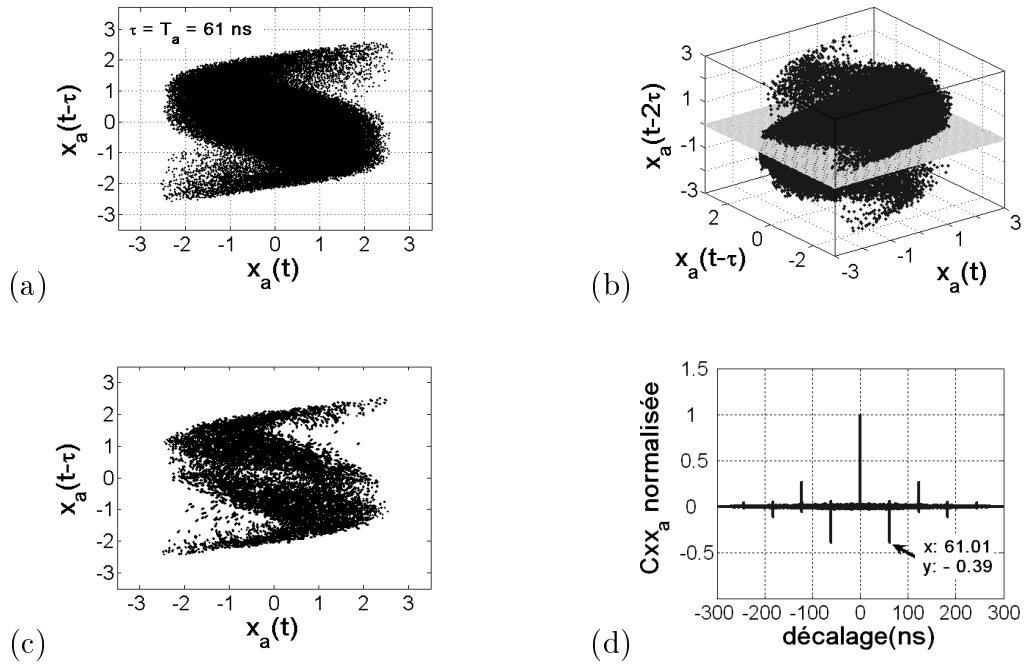



FIGURE 3.10 – *Système en une seule boucle de rétroaction.* $\beta_a = 6,5$ ; $\beta_b = 0$ *Régime chaotique.*

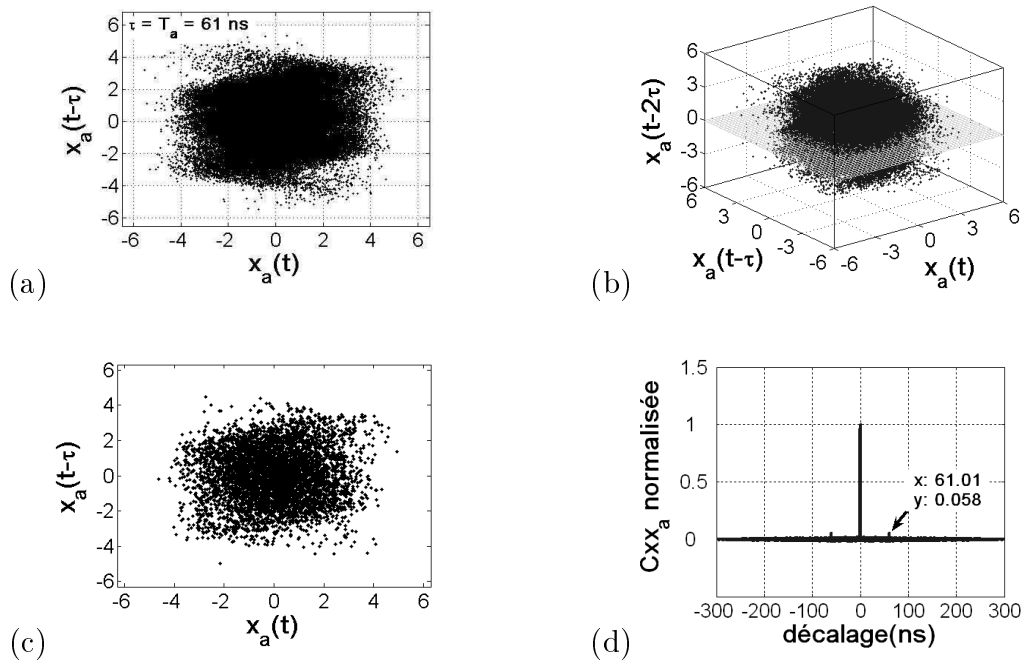



FIGURE 3.11 – *Système en une seule boucle de rétroaction.* $\beta_a = 9,8$ ; $\beta_b = 0$ *Régime chaotique très complexe.*

**Régimes chaotiques**

Les figures 3.10 et 3.11 montrent les résultats obtenus pour 2 valeurs du paramètre de bifurcation $\beta_a$ supérieures au gain du point d'accumulation. Nous observons pour un $\beta_a = 6,5$ que le diagramme des phases — figure 3.10a — forme un nuage de points réparti selon une figure aux contours bien déterminés. Cette forme est révélatrice de la fonction non linéaire. On distingue alors une répartition des amplitudes du signal chaotique sur un peu plus d'une période de la fonction non linéaire. Les points appartenant à la section de Poincaré — figure 3.10c — sont aussi ordonnés en une structure bien définie. La signature déterministe de la dynamique apparaît assez nettement dans ce type de représentation.

Lorsque le paramètre de bifurcation est encore augmenté ($\beta_a = 9,8$), on distingue grossièrement — figure 3.11a — la région de la fonction non linéaire occupée par le signal chaotique. Le diagramme dans l'espace des phases à 3 dimensions ressemble à une boule où la distinction des trajectoires est très difficile, voire impossible. La section de Poincaré — figure 3.11c — montre une région de l'espace des phases bornée recouverte de manière dense. Cette caractéristique est la signature d'un régime dynamique complexe, et de dimension plus grande que celle choisie pour la reconstruction.

La différence notable entre ces deux régimes chaotiques ($\beta_a = 6,5$ et $\beta_a = 9,8$) peut s'observer sur la fonction d'autocorrélation. En effet, les pics de cette fonction sont nettement plus visibles pour la première valeur du gain — figure 3.10d — que la seconde (voir la figure 3.11d). Dans le cas de ce dernier, l'amplitude des pics est très faible devant l'amplitude du pic central. Expérimentalement, ces faibles amplitudes seront facilement confondues avec les amplitudes du bruit du système, dont nous n'avons pas tenu compte en simulations.

En résumé, nous venons de voir que le système à une seule boucle de rétroaction génère une multitude de régimes périodiques et chaotiques, selon la valeur croissante du feedback $\beta_a$. Nous avons remarqué aussi que, la fonction d'autocorrélation révèle le délai $T_a$ pour toutes les valeurs du paramètre de bifurcation $\beta_a$ étudiées.

Pour la suite de l'étude, nous allons utiliser de façon naturelle cette propriété de la fonction d'autocorrélation pour représenter l'état du système. Autrement dit, la représentation du diagramme dans l'espace des phases, dans le cas du système en double boucle, sera donnée en fonction de $\tau^*$, où $\tau^*$ est la valeur du délai du premier pic mesuré par la fonction d'autocorrélation. On note que cette valeur de $\tau^*$ dépend simultanément des 2 délais ($T_a$ et $T_b$), et non d'un seul.

## 3.2 Système en double boucle de rétroaction

Lorsque la seconde boucle de rétroaction est fermée, nous disposons de 3 variables dynamiques, de deux types différents (électrique et optique), pour l'étude du générateur de chaos. Les deux premières sont électriques : $x_a(t)$ représentant l'évolution dynamique de la boucle (A), et $x_b(t)$ représentant celle de la boucle (B). La dernière est une variable optique : l'intensité optique, représentée par $f_{NL}[x_a, x_b](t)$.

Pratiquement, c'est cette dernière variable dynamique que nous avons utilisée, comme le montre le dispositif expérimental schématisé sur la figure 3.12. En effet, la variable mesurée est la puissance optique en sortie du générateur de chaos ; elle est obtenue après détection, pré-amplification et filtrage — dynamique passe-bande — par une photodiode ultra-rapide. Cette puissance est destinée initialement à être envoyée vers le récepteur, variable à laquelle *a priori* un éventuel espion peut accéder par simple intrusion sur le canal de transmission.

Les processus différentiels de $x_a(t)$ et de $x_b(t)$ sont donnés à la section 2.3. Celui donnant accès à $f_{NL}[x_a, x_b](t)$ est du même type, comme nous allons le rappeler brièvement ci-dessous. L'indice « $_{NL}$ » dénote tous les paramètres du dispositif de mesure de cette variable dynamique.

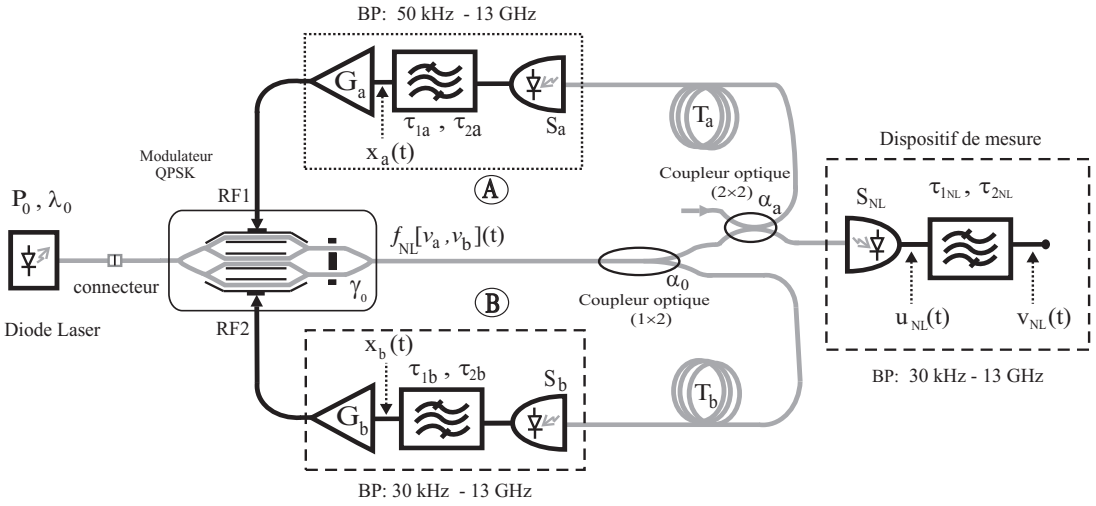



Figure 3.12 – *Système générateur de chaos à double boucle de rétroaction.*

– La fonction de transfert $H_{NL}(p)$ du filtre du dispositif de mesure, dans le domaine de Laplace, est donnée par :

$$H_{NL}(p) = \frac{V_{NL}(p)}{U_{NL}(p)} = \frac{\tau_{2NL} \cdot p}{(1 + \tau_{2NL} \cdot p)(1 + \tau_{1NL} \cdot p)} \tag{3.3}$$

où $\tau_{1NL}$ et $\tau_{2NL}$ sont les constantes de temps associées aux fréquences de coupure haute et basse du filtre à $-3$ dB, correspondant au système de détection.

– Passage de (3.3) dans le domaine temporel :

$$v_{NL}(t) + [\tau_{1NL} + \tau_{2NL}]\frac{dv_{NL}}{dt}(t) + \tau_{1NL} \cdot \tau_{2NL}\frac{d^2 v_{NL}}{dt^2}(t) = \tau_{2NL} \cdot \frac{d}{dt}\Big\{u_{NL}(t)\Big\} \tag{3.4}$$

– La puissance optique $P(t)$ à l'entrée de la photodiode peut s'écrire :

$$P(t) = \gamma \cdot P_0 \cdot f_{NL}[v_a, v_b](t) \tag{3.5}$$

où $\gamma$ est le facteur de perte de la boucle (A). Il vaut ($\gamma = \gamma_0 \cdot \alpha_0 \cdot \alpha_a$) ; l'ensemble de ces paramètres est défini page 60.

– Après la conversion optique/électrique (conversion linéaire) :

$$u_{NL}(t) = S_{NL} \cdot P(t) = S_{NL} \cdot \gamma \cdot P_0 \cdot f_{NL}[v_a, v_b](t) \tag{3.6}$$

où $S_{NL}$ est la sensibilité du photodétecteur.

– En remplaçant (3.6) dans (3.4), on obtient :

$$v_{NL}(t) + [\tau_{1NL} + \tau_{2NL}]\frac{dv_{NL}}{dt}(t) + \tau_{1NL} \cdot \tau_{2NL}\frac{d^2 v_{NL}}{dt^2}(t) = \tau_{2NL} \cdot K_{NL} \cdot \frac{d}{dt}\Big\{ f_{NL}[v_a, v_b](t) \Big\} \tag{3.7}$$

avec :

$$K_{NL} = S_{NL} \cdot \gamma_0 \cdot \alpha_0 \cdot \alpha_a \cdot P_0$$

– **Normalisation :** le filtre passe-bande du dispositif de mesure présente les mêmes caractéristiques que celui de la boucle (B). De plus, les photodétecteurs utilisés sont aussi du même type, ce qui permet de déduire que :

$$\tau_{1NL} = \tau_{1b} \quad ; \quad \tau_{2NL} = \tau_{2b} \quad ; \quad S_{NL} = S_b \tag{3.8}$$

C'est la raison pour laquelle nous avons opté pour une normalisation de la tension électrique $v_{NL}(t)$ par rapport à la tension demi-onde $V_{\pi RF2}$ :

$$x_{NL}(t) = \pi \cdot \frac{v_{NL}(t)}{2V_{\pi RF2}} \tag{3.9}$$

Après cette normalisation, l'équation (3.7) devient :

$$x_{NL}(t) + [\tau_{1NL} + \tau_{2NL}]\frac{dx_{NL}}{dt}(t) + \tau_{1NL} \cdot \tau_{2NL}\frac{d^2 x_{NL}}{dt^2}(t) = \tau_{2NL} \cdot \beta_{NL} \cdot \frac{d}{dt}\Big\{ f_{NL}[x_a, x_b](t) \Big\} \tag{3.10}$$

avec :

$$\beta_{NL} = \pi\frac{K_{NL}}{2V_{\pi RF2}} = \pi\frac{P_0 \cdot \gamma_0 \cdot \alpha_0 \cdot \alpha_a \cdot S_{NL}}{2V_{\pi RF2}} \tag{3.11}$$

Ainsi, l'équation (3.10) régit la dynamique de la mesure de $f_{NL}[x_a, x_b](t)$. Et comme les paramètres de filtrage de cette mesure sont les mêmes que ceux de la boucle (B), on peut déduire aisément la relation (3.12), et on pourrait écrire aussi une relation similaire avec $x_a(t)$.

$$x_b(t) = \frac{\beta_b}{\beta_{NL}} \cdot x_{NL}(t - T_b) \tag{3.12}$$

avec $\beta_b/\beta_{NL} = G_b/\alpha_a$ ; un facteur de proportionnalité, que l'on peut déduire de (3.11).

### 3.2.1 Diagrammes de bifurcation et entropiques

Pour tracer les diagrammes de bifurcation du système à double boucle, nous avons fixé les valeurs du gain $\beta_b$ de la seconde boucle d'une manière totalement arbitraire. Ce choix est exigé par ce type de représentation graphique, car on ne peut représenter qu'un seul paramètre variable à la fois (le gain $\beta_a$ dans notre cas). Pour la suite, nous considérons ces valeurs de $\beta_b$ (deux à deux) respectivement : faible, moyen et élevé.

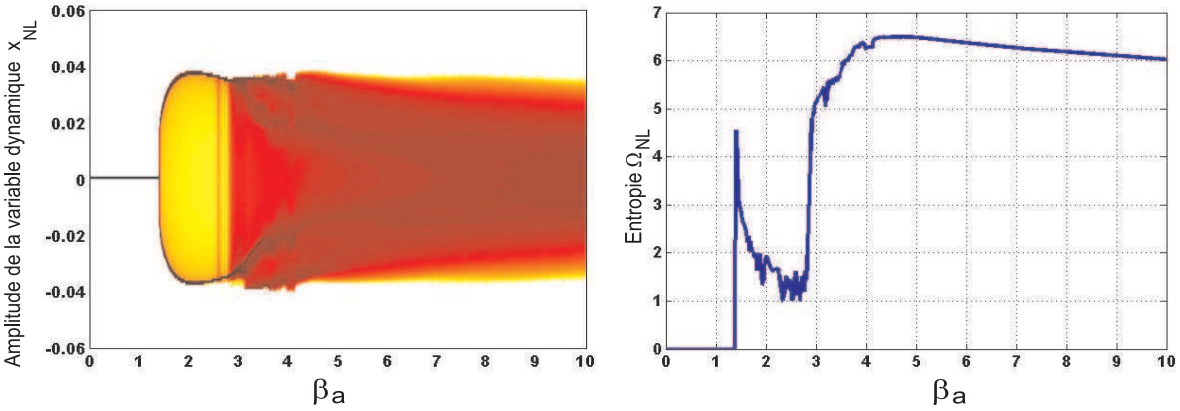
Nous rappelons aussi qu'au tableau 3.1 est donné l'ensemble des paramètres du générateur de chaos à double boucle. La condition d'interférence au point de repos du QPSK est fixée de la manière suivante : $\phi_1 = 1,1$ rad (partie quasi-linéaire de la cannelure du $MZ_1$), $\phi_2 = -0,1$ rad et $\phi_3 = -0,5$ rad. Ainsi, les résultats obtenus sont représentés sur les figures 3.13 :

1. À partir des diagrammes de bifurcation 3.13a et 3.13b (à gauche), nous pouvons identifier divers régimes : stationnaire (un point fixe stable), périodique (un nombre fini d'états : un cycle attracteur) ou encore chaotique (un grand nombre de solutions). La bifurcation de Hopf et les cycles de période T2 et T4 sont clairement repérables sur les deux diagrammes, mais les cycles en $2^n$ au delà de $n = 2$ sont difficiles à observer sur ce type de représentation graphique. Ainsi, on peut seulement deviner que lorsque le gain de la boucle (B) est faible, l'évolution de la dynamique suit alors la route traditionnelle vers le chaos par une cascade par dédoublement de période.

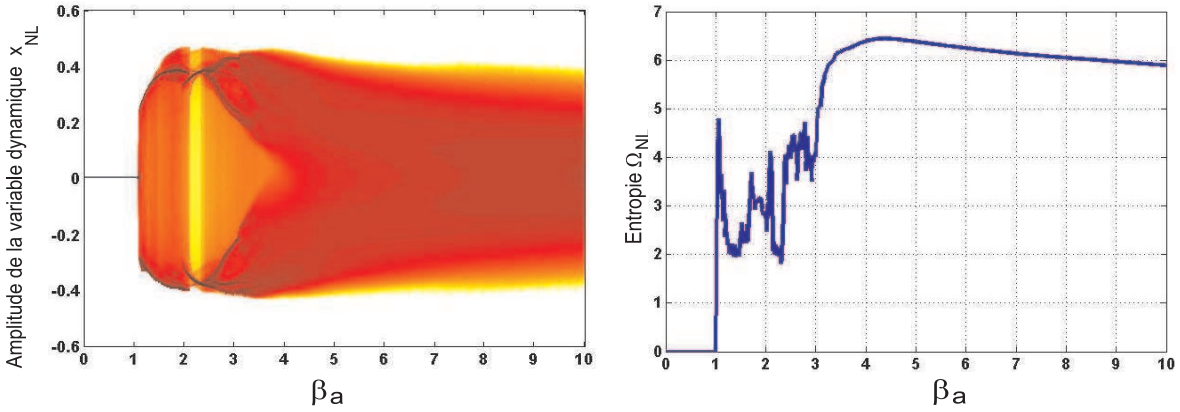
2. Lorsque le gain de la boucle (B) est augmenté ($\beta_b = 2,6$ : considéré moyen), nous constatons que la transition du régime stationnaire vers les régimes chaotiques devient brutale — figure 3.13c — dans le sens que les régimes qualifiés de périodiques ne sont pas observés. Lorsque ce gain est encore augmenté ($\beta_b = 3,5$), un autre scénario de transition — figure 3.13d — est obtenu mais cette fois-ci de périodiques vers les régimes chaotiques. Ainsi, l'influence du feedback $\beta_b$ sur la dynamique globale générée par l'oscillateur est ici mise en évidence, confirmant ainsi la dépendance des dynamiques des deux boucles de rétroaction du système.

3. Contrairement aux deux cas précédents (feedback $\beta_b$ faible et moyen), les diagrammes de bifurcation et entropiques 3.13e et 3.13f montrent que la dynamique du système est chaotique dès le début des enregistrements. Il nous semble que ce résultat est trivial, car le système se trouve initialement déjà en oscillations chaotiques, à cause de la valeur élevée (respectivement $\beta_b = 6,5$ et $\beta_b = 9,5$) du gain de la seconde boucle .

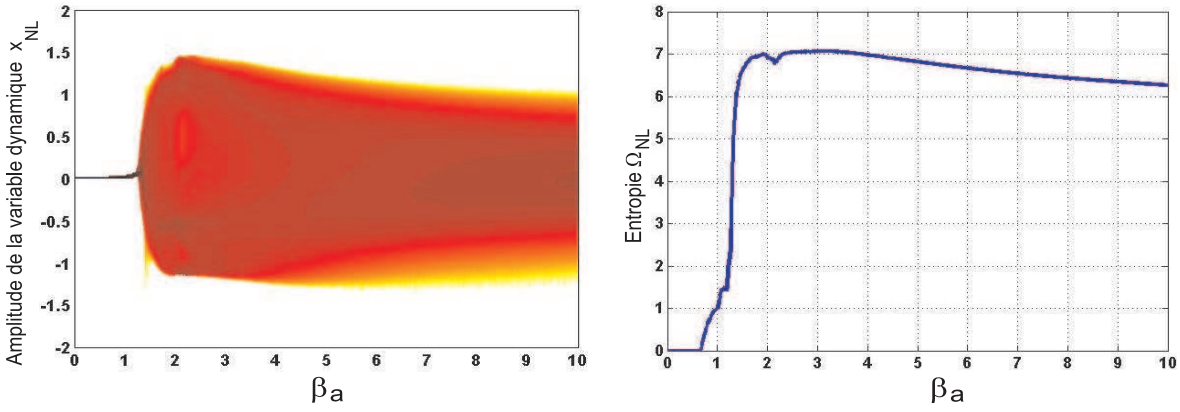
Les différents exemples de diagrammes de bifurcation et entropiques, que nous venons de voir, montrent que la dynamique générée dépend simultanément des deux feedback du système. Certes la route vers le chaos est observée pour 6 valeurs du gain $\beta_b$, mais en terme d'exploration globale de la dynamique de l'oscillateur, il serait plus significatif de considérer ce gain comme un deuxième paramètre de bifurcation. L'outil d'analyse alors le plus approprié est, par exemple, un diagramme entropique en 3 dimensions.



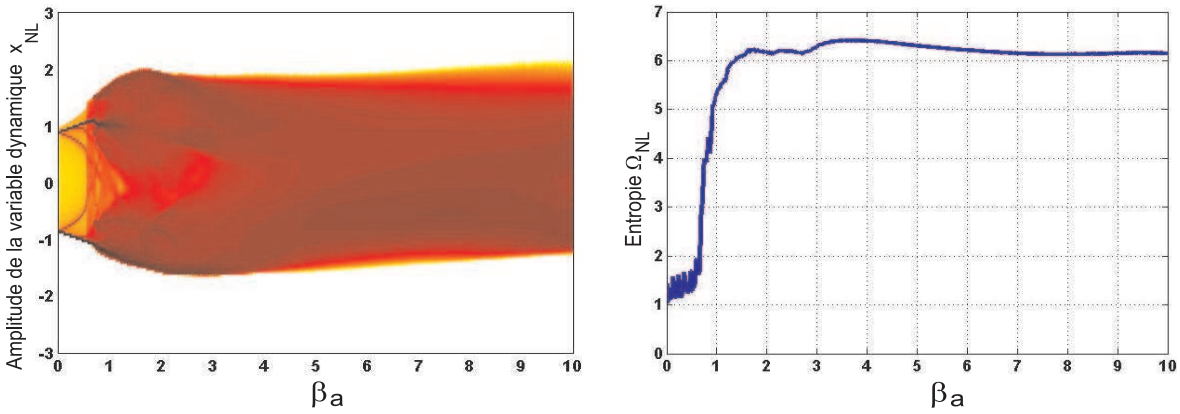

(a) feedback faible: $\beta_b = 0{,}1$ ;



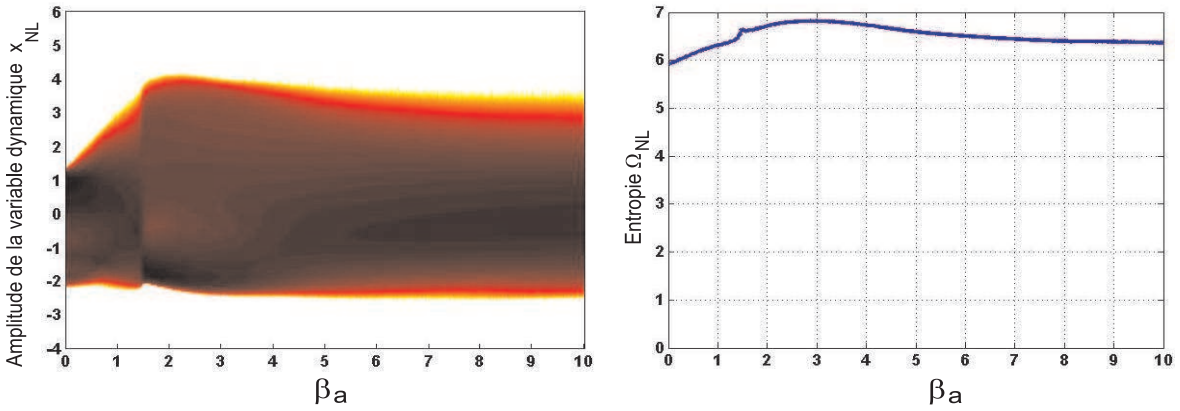

(b) feedback faible: $\beta_b = 1{,}1$ ;



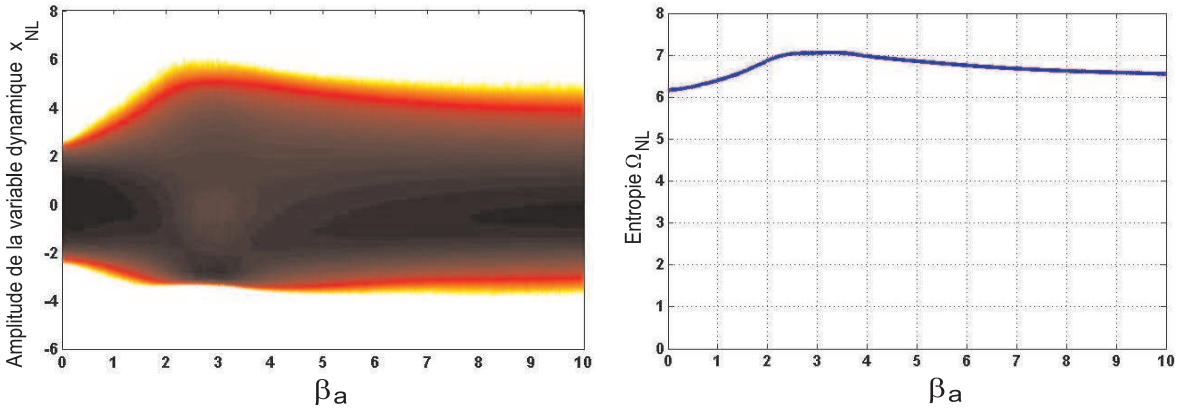

(c) feedback moyen: $\beta_b = 2{,}6$ ;




(d) feedback moyen: $\beta_b = 3{,}5$ ;




(e) feedback élevé: $\beta_b = 6{,}5$ ;

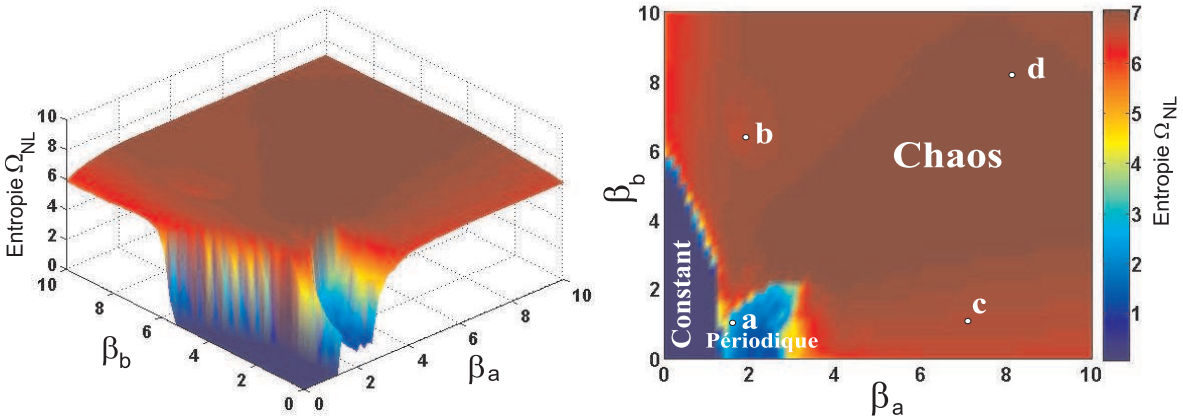



(f) feedback elevé: $\beta_b = 9{,}5$ ;

Figure 3.13 – *Diagrammes de bifurcation et entropiques du système à double boucle en fonction de $\beta_a$ pour plusieurs valeurs de $\beta_b$. Les autres paramètres sont fixés à :* $T_a = 61$ ns ; $T_b = 60$ ns ; $\phi_1 = 1{,}1$ rad ; $\phi_2 = -0{,}1$ rad ; $\phi_3 = -0{,}5$ rad.

La figure 3.14a illustre ce diagramme entropique en fonction des gains $\beta_a$ et $\beta_b$. Il s'agit en réalité d'un résumé de l'ensemble des diagrammes entropiques que nous avons vu précédemment dans le cas du système à double boucle. On remarque une fois de plus que l'entropie d'information sature, ce qui est caractéristique d'une structure cachée déterministe (différentiation d'un système purement aléatoire).

La figure 3.14b représente la variation de l'entropie dans le plan ($\beta_a$, $\beta_b$), et comme on peut le remarquer, elle n'est pas symétrique par rapport aux deux axes du plan. Ceci est dû principalement à la condition d'interférence au point de repos du QPSK. Autrement dit, pour chaque point de fonctionnement du modulateur, la carte de la figure 3.14b est modifiée. Cependant, cette carte nous permet toujours de repérer les zones importantes de régime chaotique, à partir desquelles on choisira le domaine de fonctionnement en ($\beta_a$, $\beta_b$) pour une application de communication par chaos.




(a) Vue en 3D (b) Vue de dessus

Figure 3.14 – *Variation de l'entropie en fonction des gains de rétroaction $\beta_a$ et $\beta_b$. (mêmes autres paramètres qu'à la* Fig 3.13).

Il nous paraît évident qu'un système destiné au cryptage de l'information doit être analysé en profondeur ; c'est la raison pour laquelle nous ne nous contentons pas uniquement des résultats obtenus à partir des diagrammes de bifurcation et entropiques. Nous allons donc, dans une première partie, explorer ce système par une analyse temporelle, statistique et spectrale. Puis dans une seconde partie, nous l'examinerons dans un pseudo-espace des phases et par la fonction d'autocorrélation.

### 3.2.2 Analyse temporelle, statistique et spectrale

Pour les analyser, nous avons choisi sur le diagramme entropique de la figure 3.14b quatre points différents (a, b, c et d), correspondant à des couleurs différentes de l'entropie. Ces points sont représentatifs, d'après cette carte, de régimes dynamiques différents.

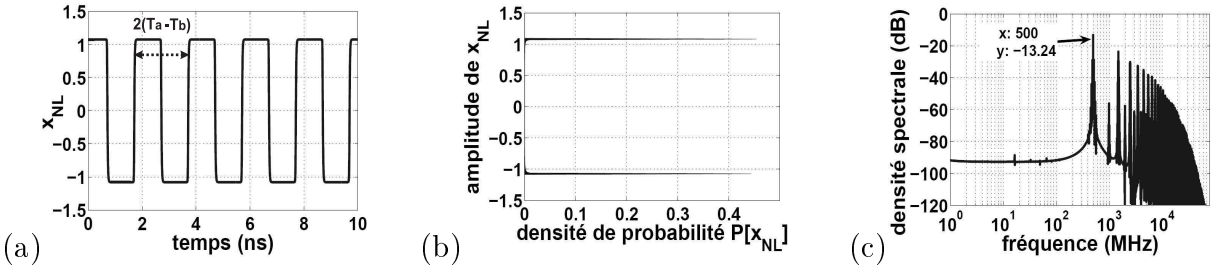



Figure 3.15 – *Système à double boucle de rétroaction.* $\beta_a = 1,4$ ; $\beta_b = 1,4$ *Régime périodique d'ordre* 2 (point " a " de la figure 3.14).

La figure 3.15 illustre les résultats obtenus pour le **point " a"**. Les paramètres $\beta_a$ et $\beta_b$ de ce point sont relativement faibles et le système est en régime périodique. Comme le montre la trace temporelle 3.15a, la période de ce régime correspond au double de la différence des 2 délais du système : $2(T_a - T_b) = 2$ ns. Le spectre associé 3.15c montre un pic très net correspondant à l'inverse de cette période, autrement dit à la fréquence d'oscillation : $[2(T_a - T_b)]^{-1} = 500$ MHz.

En faisant varier un seul délai du système avec le maintien de l'autre constant (dans les mêmes conditions de paramètres qu'au point " a"), les courbes des figures 3.16a et 3.16b confirment que la période observée correspond bien au double de la différence des 2 délais du système (une annexe en fin du manuscrit est disponible pour plus de détails).

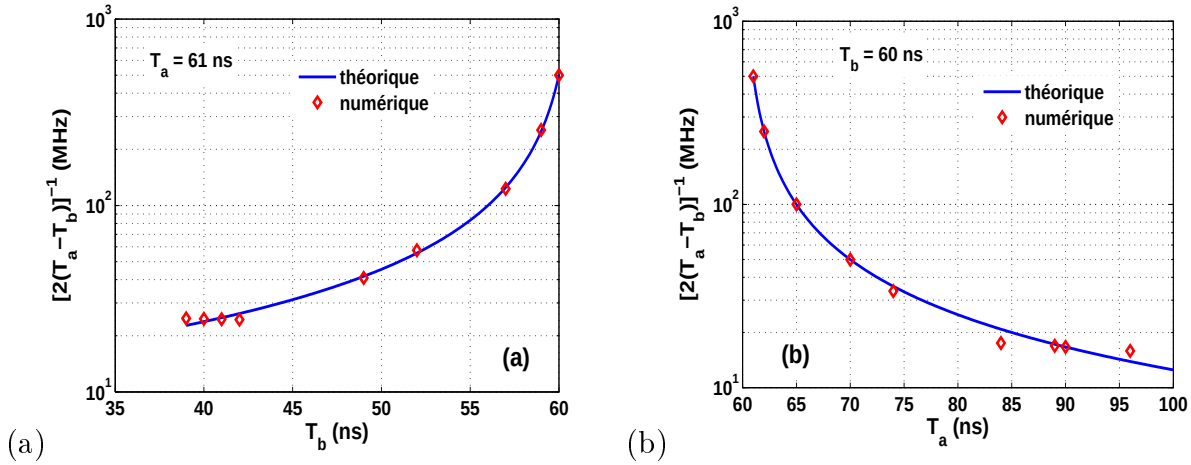



Figure 3.16 – *Variation de la fréquence d'oscillation* (*a*) *en fonction du délai* $T_b$ *;* (*b*) *en fonction du délai* $T_a$*. La courbe théorique correspond au traçage de* $[2(T_a - T_b)]^{-1}$ *en fonction d'un délai, et celle du numérique correspond au pic révélé par la FFT de l'algorithme implémenté. Les paramètres sont les mêmes que ceux du point " a " de la Figure.* 3.14.

Au **point " b"**, le gain de rétroaction d'une boucle est faible et le gain de l'autre est élevé. La figure 3.17 montre que ce point est en régime chaotique, avec cependant une forte composante périodique. L'harmonique de cette dernière est clairement visible sur le spectre 3.17c, et elle correspond à la même fréquence observée précédemment au point " a".

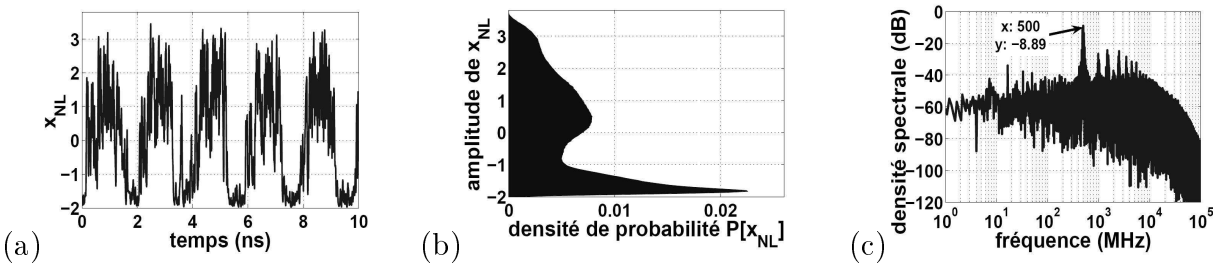



FIGURE 3.17 – *Système à double boucles de rétroaction.* $\beta_a = 1,6$ ; $\beta_b = 6,2$ *Régime chaotique* (point " b" de la figure 3.14).

Comme nous l'avons constaté expérimentalement puis numériquement, il faut noter que dans un type de régime tel que celui du point " b" , où le gain d'une boucle est élevé et l'autre faible, un réglage minutieux de la condition d'interférences du QPSK permet facilement de faire basculer la dynamique du système dans un régime chaotique plus complexe.

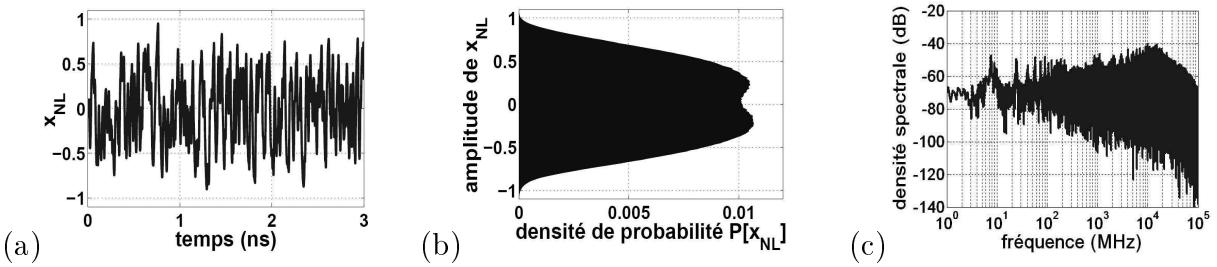



FIGURE 3.18 – *Système à double boucle de rétroaction.* $\beta_a = 7,2$ ; $\beta_b = 1,4$ *Régime chaotique* (point " c" de la figure 3.14).

Le **point " c"** se présente typiquement dans la situation que nous venons d'évoquer. En effet, malgré le gain faible d'une boucle ($\beta_b = 1,4$), avec cependant un gain élevé de l'autre ($\beta_a = 7,2$), le système a un comportement chaotique développé (figure 3.18). On constate qu'aucune harmonique n'est privilégiée dans le spectre, contrairement aux cas précédents des points " a" et " b". L'allure bruitée de la trace temporelle et son spectre assez plat sont les caractéristiques de ce régime chaotique.

La figure 3.19 illustre les résultats obtenus pour le régime dynamique du **point " d"**. Les gains $\beta_a$ et $\beta_b$ sont relativement élevés et le système oscille chaotiquement. On peut

remarquer que la distribution d'amplitude — figure 3.19b — est proche d'une gaussienne, et que la trace temporelle est presque indiscernable d'un bruit blanc (certes spectralement délimité par la bande passante de la boucle de rétroaction).

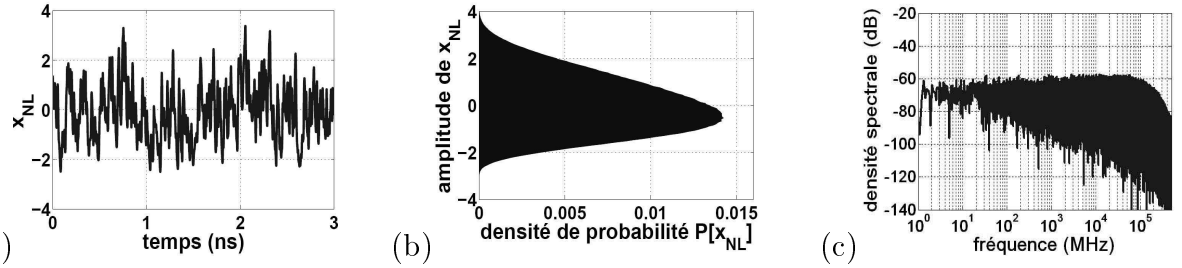



Figure 3.19 – *Système à double boucle de rétroaction.* $\beta_a = 8,2$ ; $\beta_b = 8,1$ *Régime chaotique* (point " d" de la figure 3.14).

### 3.2.3 Autocorrelation et carte de premier retour

Nous présentons dans cette partie les résultats obtenus, par l'analyse dans un pseudo-espace des phases, des régimes dynamiques des 4 points choisis précédemment. Nous signalons par avance que ces résultats sont seulement qualitatifs pour au moins deux raisons : absence d'une méthode précise adaptée à un système contenant 2 retards temporels différents, et complexité des dynamiques observées. Ces raisons peuvent donc introduire une éventuelle erreur d'appréciation, plus particulièrement sur le décalage $\tau^*$ évalué par la fonction d'autocorrélation.

La figure 3.20 montre les résultats de représentation du régime dynamique relatifs au **point " a "**. Le décalage $\tau^*$ correspond au premier pic enregistré par la fonction d'autocorrélation. On constate que l'harmonique révélée précédemment par l'analyse spectrale (figure 3.15c), et qui correspond à $2(T_a - T_b) = 2$ ns, est aussi décelée par la fonction d'autocorrélation. Le régime dynamique obtenu est périodique, ce qui est confirmé par l'attracteur en 2 D, ou encore par la coupe de Poincaré. La reconstitution de l'attracteur dans un espace des phases à 3 dimensions montre que la trajectoire évolue vers un cycle limite stable (figure 3.20b), caractéristique d'un régime périodique d'ordre 2.

Le **point " b "** correspond à l'état du système lorsqu'un gain d'une boucle est faible et l'autre est élevé ($\beta_a = 1,6$ et $\beta_b = 6,2$ ; figure 3.21). D'après la figure 3.21a, on observe un nuage de points s'alignant sous une certaine forme qui confirme le déterministe du chaos généré. Ce nuage de points est dense dans une région de l'attracteur, ce qui est confirmée auparavant par un pic très net — figure 3.17b — de la répartition de la densité de probabilité. Le caractère dense du nuage met en évidence le passage d'un très grand nombre de trajectoires, mais ce pseudo-espace des phases n'est pas suffisant pour décrire de manière unique l'état dynamique du système par un point dans l'espace. La reconstruction

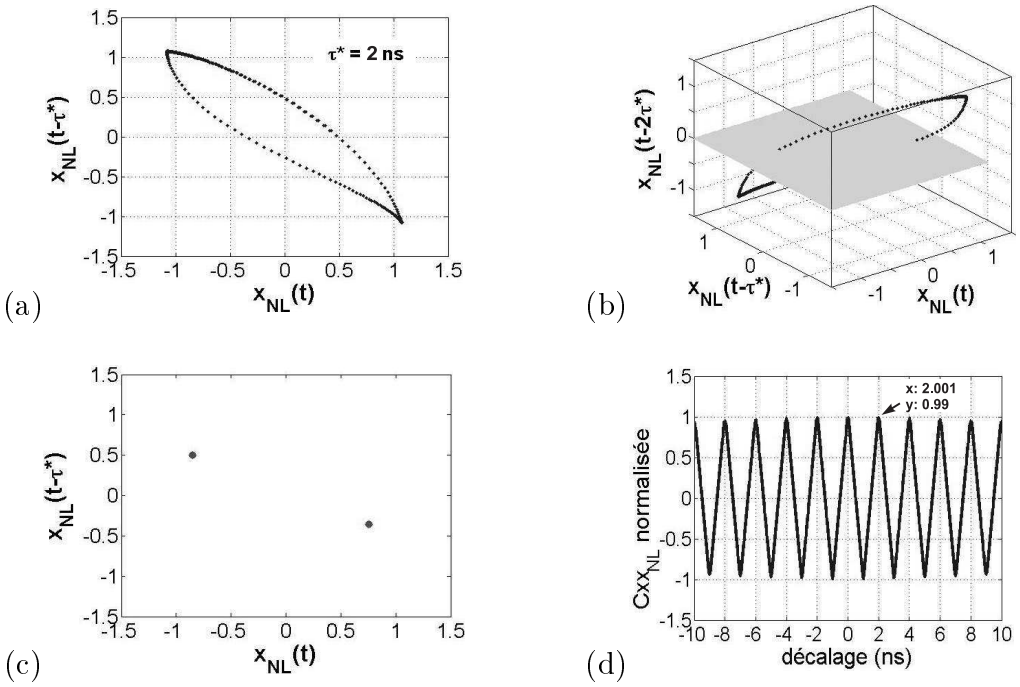



FIGURE 3.20 – *Système à double boucle de rétroaction.* $\beta_a = 1,4$ ; $\beta_b = 1,4$ *Régime périodique d'ordre* 2 (point " a " de la figure 3.14).

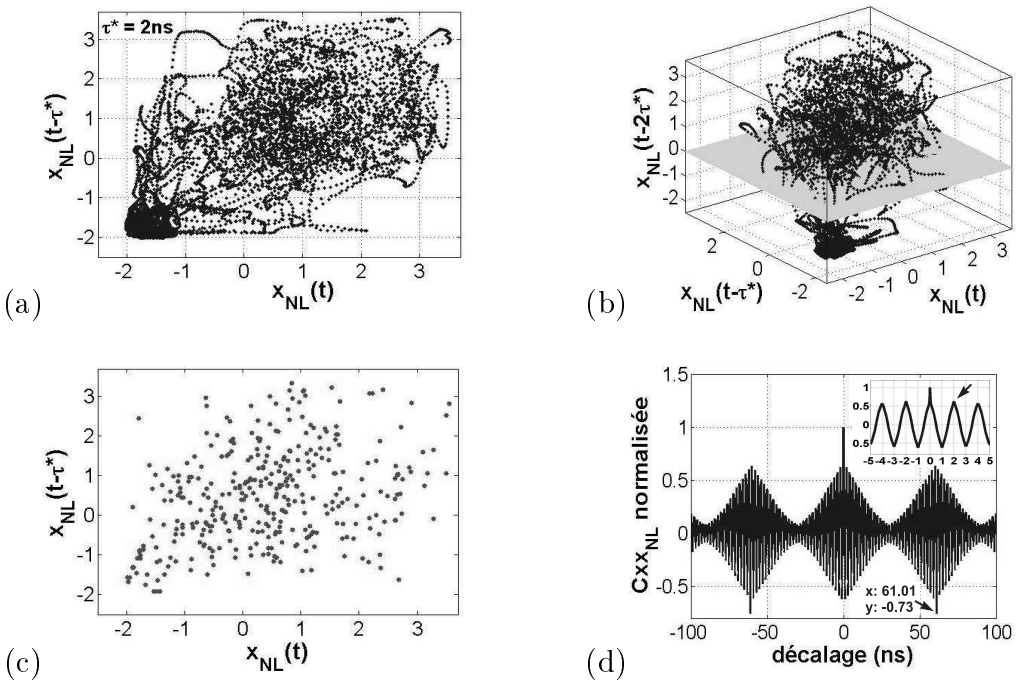



FIGURE 3.21 – *Système à double boucle de rétroaction.* $\beta_a = 1,6$ ; $\beta_b = 6,2$ *Régime chaotique* (point " b " de la figure 3.14).

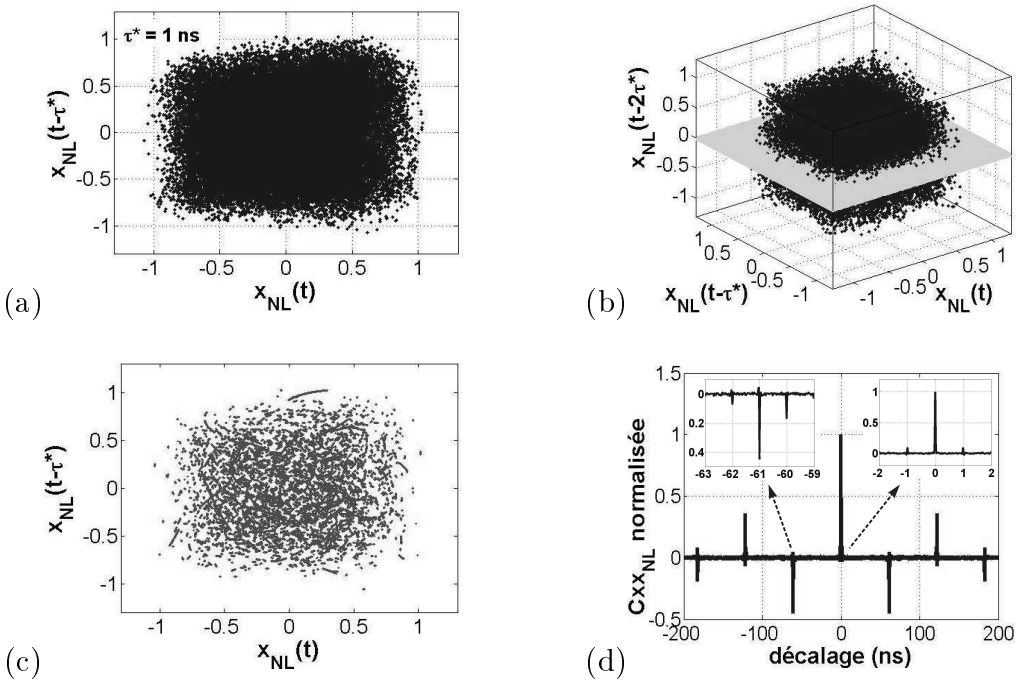



FIGURE 3.22 – *Système à double boucle de rétroaction.* $\beta_a = 7,2$ ; $\beta_b = 1,4$ *Régime chaotique* (point " c " de la figure 3.14).

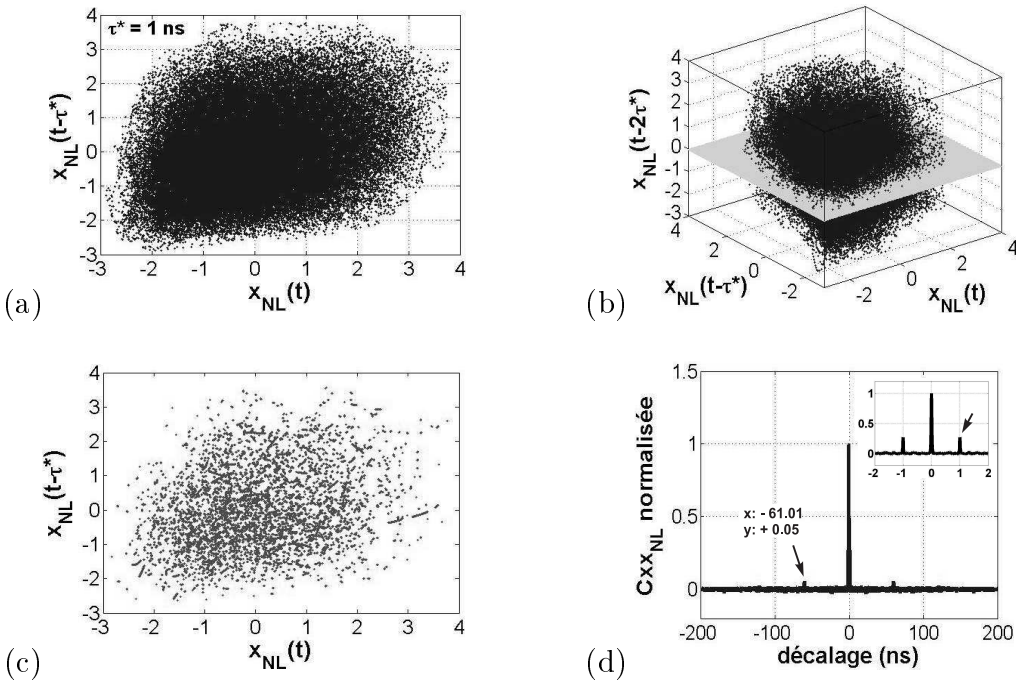



FIGURE 3.23 – *Système à double boucle de rétroaction.* $\beta_a = 8,2$ ; $\beta_b = 8,1$ *Régime chaotique* (point " d " de la figure 3.14).

de l'attracteur dans un espace des phases à 3 D s'est révélée aussi peu efficace et d'allure complexe (figure 3.21b). Cette complexité est due probablement au choix du décalage $\tau^*$ évalué par la fonction d'autocorrélation. La figure 3.21d montre la courbe de cette fonction, où on peut remarquer non seulement qu'elle possède une pseudo-période égale au double de la différence des deux délais du système $2(T_a - T_b) = 2$ ns, mais aussi qu'elle est modulée par une enveloppe pseudo-périodique égale à $61,01$ ns. Cette dernière correspond *a priori* à la valeur surestimée du plus grand délai du système $T_a$.

La figure 3.22 montre les résultats obtenus de l'analyse du **point " c "**. On constate que la fonction d'autocorrélation enregistre des pics réguliers espacés d'une durée de $61,01$ ns. Cette durée correspond à la valeur surestimée du retard temporel $T_a$. Un zoom autour du pic central de cette fonction (voir le zoom à droite de la figure 3.22d) révèle un pic à 1 ns, ce qui correspond *a priori* à la différence des deux délais du système ($T_a - T_b = 1$ ns). On constate également qu'une valeur surestimée du délais $T_b$, qui vaut $60,01$ ns, est aussi repérée (voir le zoom à gauche de la figure 3.22d).

En résumé, la fonction d'autocorrélation au point " c " a permis d'identifier les 2 délais du système, ainsi que leur différence, ce qui constitue un inconvénient majeur lors d'une éventuelle cryptanalyse du système.

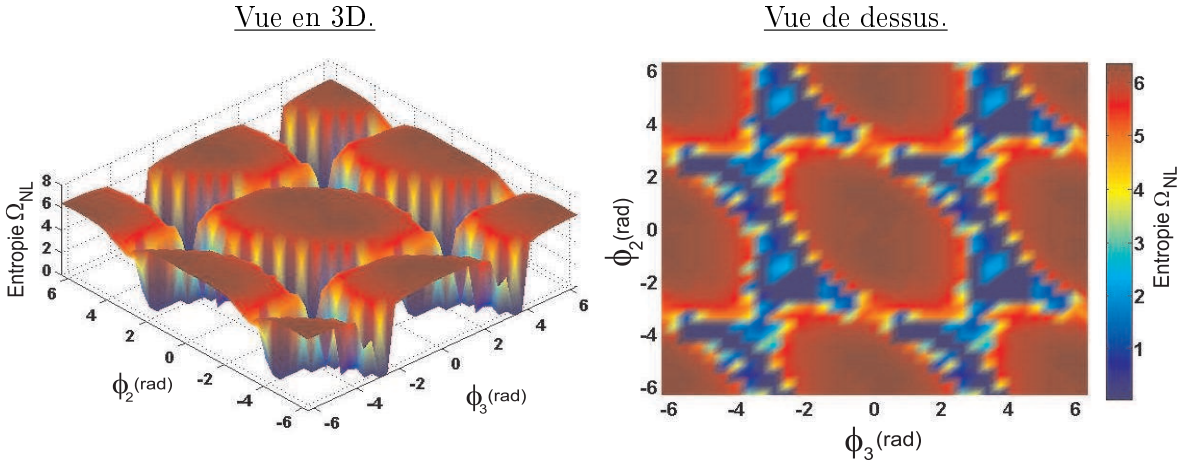
Le **point " d "** correspond, nous le rappelons, à l'état du système lorsque les 2 paramètres de bifurcation sont relativement élevés ($\beta_a = 8,2$ et $\beta_b = 8,1$). La figure 3.23a représente la carte du premier retour, qui montre que les trajectoires occupent une zone aux abords bien limités. Ce fait est une illustration de l'ordre prédéterminé qui régit le tracé des trajectoires successives de l'attracteur. La courbe de la fonction d'autocorrélation — figure 3.23d — enregistre des pics d'amplitude très faible (environ -26 dB), voire quasiment nulle au delà des limites du pic central (le bruit du système n'est pas pris en compte dans les simulations).

Nous venons de passer en revue quelques régimes dynamiques possibles que peut produire le système à double boucle. Les cas évoqués ne font apparaître qu'une partie de la richesse de l'ensemble de ces régimes, car nous avons vu jusqu'à présent seulement l'évolution des dynamiques du système en fonction de 2 paramètres ($\beta_a$ et $\beta_b$) ; il suffit qu'un seul soit élevé pour que la dynamique soit chaotique. Nous allons poursuivre cette étude dans ce qui suit, pour avoir une vision plus globale de l'influence des autres paramètres. Nous explorons particulièrement ceux qui sont accessibles expérimentalement, c'est-à-dire les bias du modulateur, les retards temporels et les bandes passantes des filtres.

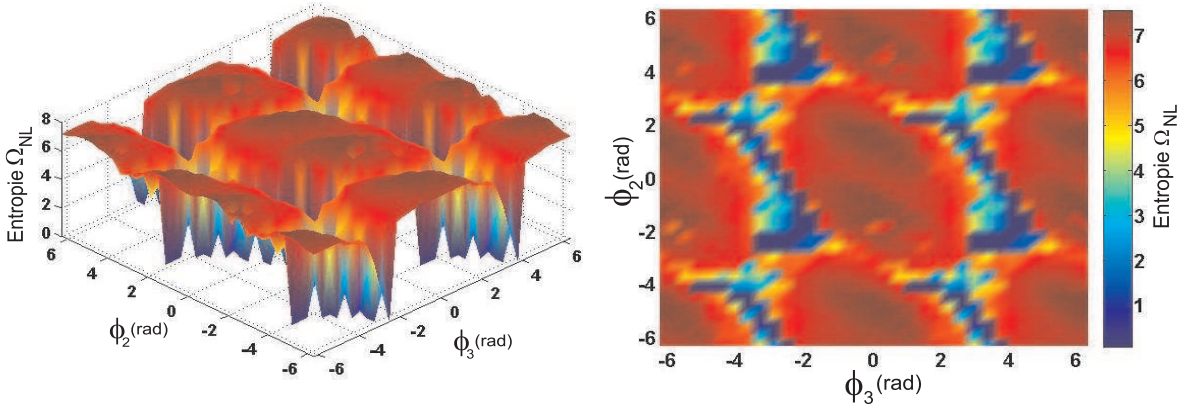
## 3.3 Influence des autres paramètres de l'émetteur

### 3.3.1 Influence des paramètres du modulateur QPSK

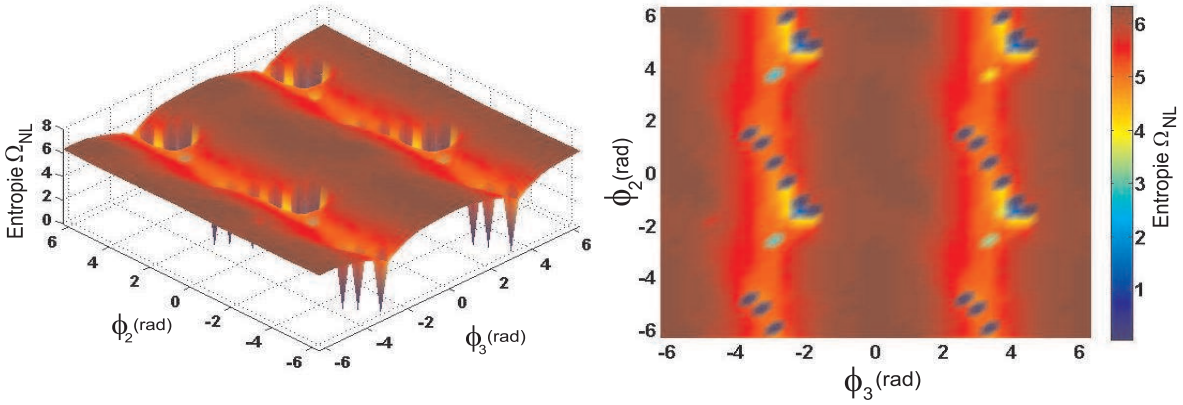
Nous entendons par les paramètres du modulateur QPSK seulement les phases statiques $\phi_1$, $\phi_2$ et $\phi_3$. Expérimentalement, ces paramètres peuvent être réglés facilement en agissant, comme nous l'avons vu au chapitre 2 à la partie modélisation du modulateur, sur




(a) feedback faible: $\beta_b$=1;

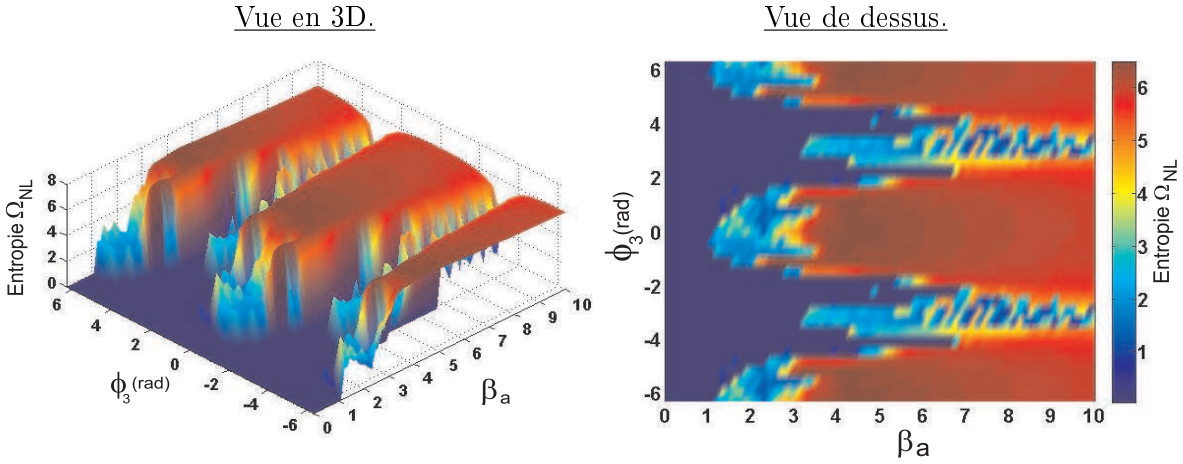



(b) feedback moyen: $\beta_b$=3;

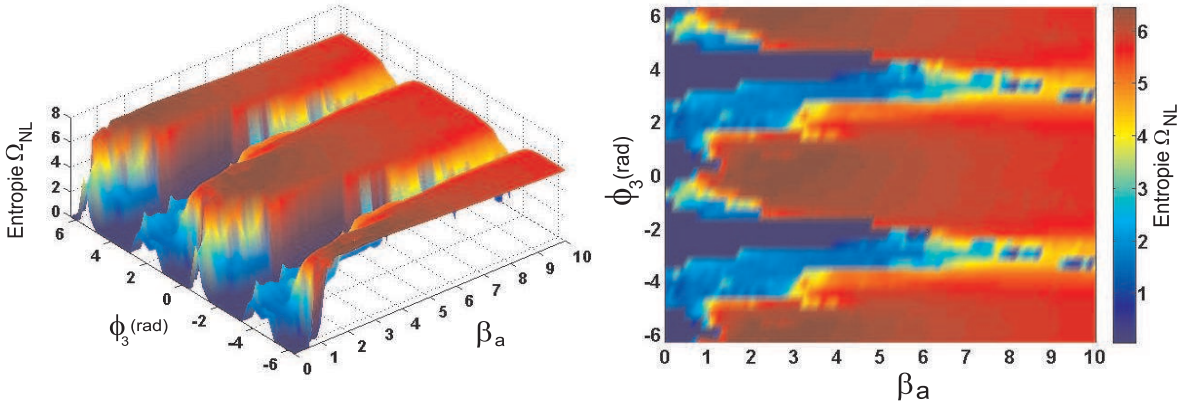



(c) feedback élevé: $\beta_b$=8;

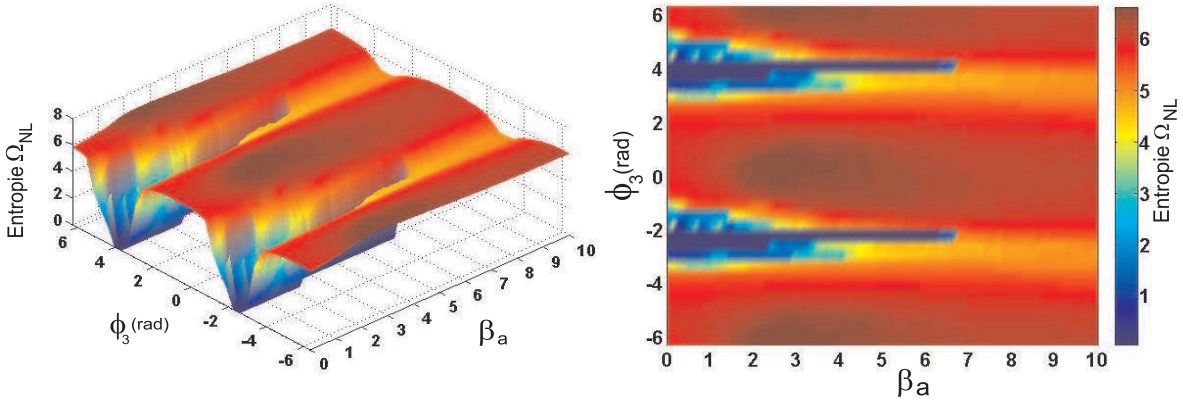
Figure 3.24 – *Diagrammes entropiques en fonction des déphasages $\phi_2$ et de $\phi_3$ du système à double boucle. Paramètres de simulation : $\beta_a = 10$ ; $\phi_1 = 1,1$ rad.*




(a) feedback faible: $\beta_b$=1;




(b) feedback moyen: $\beta_b$= 3;




(c) feedback élevé: $\beta_b$= 8;

FIGURE 3.25 – *Diagrammes entropiques en fonction de $\phi_3$ et de $\beta_a$ du système à double boucle. Paramètres de simulation* : $\phi_1 = 1,1$ rad ; $\phi_2 = 0,5$ rad.

les tensions de bias appliquées aux trois électrodes DC. Il est donc intéressant de voir dans quelles mesures ces paramètres sont susceptibles de modifier les régimes dynamiques accessibles au cours de la variation des gains de boucle ($\beta_a$ et $\beta_b$). Ces derniers jouent aussi un rôle déterminant pour le tracer des diagrammes, mais pour des raisons de clarté, nous avons choisi le gain global de la boucle (A) élevé ($\beta_a = 10$), permettant ainsi de lui assurer des oscillations chaotiques, et l'autre gain variable en sorte que sa valeur soit faible ($\beta_b = 1$), puis moyen ($\beta_b = 3$), et enfin élevé ($\beta_b = 8$).

La figure 3.24 montre les résultats obtenus lorsque $\phi_2$ et $\phi_3$ sont variés, avec $\phi_1$ fixé sur la partie linéaire de la cannelure. On constate encore une fois — relation 3.2 — que l'entropie sature pour toutes la valeurs de $\beta_b$ choisies. Lorsque ce dernier est faible (voir la figure 3.24a), le diagramme ressemble grossièrement à celui qu'on a déjà vu dans le cas du fonctionnement du système à une seule boucle (figure 3.3). Les zones d'entropie élevée restent localisées aux alentours de $\phi_2 = \phi_3 = 0 \bmod[2\pi]$, et celles à entropie faible (ou nulle) aux environs de $\phi_2 = \phi_3 = \pi \bmod[2\pi]$. À noter qu'il est de même pour le paramètre $\phi_1$ ; les résultats obtenus en faisant varier ce paramètre ressemblent globalement à ceux de la figure 3.24, raison pour laquelle nous avons jugé inutile de les présenter.

De ces résultats une autre information peut être déduite, plus précisément d'après les diagrammes 3.24b et 3.24c : les zones à faible entropie tendent à se réduire lorsque le feedback $\beta_b$ est augmenté ; cela se traduit physiquement par des régimes dynamiques de plus en plus désordonnés. Par ailleurs, à cause de l'influence du déphasage $\phi_3$ sur l'amplitude de la non linéarité, la figure 3.24c met aussi en évidence la dépendance forte de la dynamique générée en fonction de $\phi_3$. Ce fait permet de considérer l'effet de variation de ce paramètre comme semblable à celui d'un gain de rétroaction.

En effet, les résultats obtenus — figure 3.25 — montrent que, pour certains valeurs de ce paramètre ($\phi_3 = \pi \bmod[2\pi]$), les régimes chaotiques ne sont pas atteints même pour des gains de boucle relativement élevés (figure 3.25c). Cet état du système s'explique par l'absence d'un extrémum dans l'intervalle de balayage de la fonction non linéaire, dont l'allure ressemblerait à celle représentée sur la figure 2.11c en page 57.

À partir de l'analyse que nous venons de voir, il résulte que le choix du point de fonctionnement du QPSK est très important ; le chaos engendré par le système est lié fortement à ce point. La complexité des régimes chaotiques observés dépend en général des 3 phases, mais plus particulièrement elle est très sensible à la phase $\phi_3$. Cette complexité est maximale en terme d'entropie aux alentours de : $0 \bmod[2\pi]$ rad ; ce qui correspond physiquement au maximum de transmission du modulateur QPSK (i.e : $|f_{NL}[.]| = 1$).

Enfin, on note ici que la condition d'interférence choisie à la section 3.2.1, afin de tracer les diagrammes de bifurcation du système à double boucle, est basée en partie sur les critères de cette conclusion. Cette condition d'interférence restera la même pour la suite de l'étude.

### 3.3.2 Influence des retards temporels

Afin de déterminer l'influence des délais du système sur la dynamique chaotique générée, nous allons utiliser deux outils : le spectre et la fonction d'autocorrélation. L'approche adoptée est très simple, dans la mesure où on fixe tous les paramètres[4], et on fait varier uniquement l'un des retards temporels du système : le délai $T_b$.

Parmi le large choix des 2 gains de rétroaction pour lesquels le chaos est observé, nous nous limiterons à la situation suivante : un feedback élevé et l'autre faible. Cette configuration a l'avantage de permettre la synchronisation, comme nous le verrons plus tard. Ainsi, les résultats obtenus dans 2 cas différents, en fonction de la valeur du gain $\beta_b$, sont donnés par :

1. Le premier cas est la variation du délai $T_b$ avec un feedback faible ($\beta_b = 1,8$). Les résultats obtenus dans ces conditions de fonctionnement sont illustrés sur la figure 3.26. On constate que globalement les dynamiques chaotiques observées sont de plus en plus développées, dans le sens où les composantes périodiques repérées sont de moins en moins visibles sur les spectres de Fourier. Les amplitudes de ces composantes sont de plus en plus faibles sur les graphes de la fonction d'autocorrélation, au fur et à mesure que le délai $T_b$ augmente.

   Nous pouvons conclure, comme on pouvait s'y attendre, que plus le délai est grand, plus la dynamique chaotique générée est complexe.

2. Le deuxième cas étudié ici est toujours la variation de $T_b$, mais cette fois-ci avec un feedback élevé ($\beta_b = 10$). Les figures 3.27 montrent les résultats graphiques ainsi observés. On constate que contrairement au cas précédent, des composantes périodiques fortes sont toujours observables quelque soit le régime dynamique généré.

D'après ces résultats, nous pouvons déduire que l'obtention de régimes chaotiques complexes, loin des régimes périodiques pour pouvoir masquer correctement l'information, les délais du système doivent être choisis suffisamment grands, et plus particulièrement, le plus grand des délais du système doit être inséré dans la boucle de rétroaction où le feedback est élevé.

### 3.3.3 Influence des bandes passantes des filtres

Nous avons déjà évoqué au chapitre 2 que les constantes de temps, qui sont caractéristiques des filtres passe-bandes, constituent une partie de la clé cryptographique. En changeant les bandes passantes des filtres, nous obtenons de nouvelles clés cryptographiques du système. Cet avantage de l'oscillateur chaotique lui procure donc la qualité d'un système reconfigurable, d'où l'intérêt de voir l'influence de ces bandes passantes sur la dynamique chaotique générée. À titre d'exemples, nous allons présenter sans entrer dans

[4] L'ensemble des paramètres utilisés est donné au tableau 3.1.

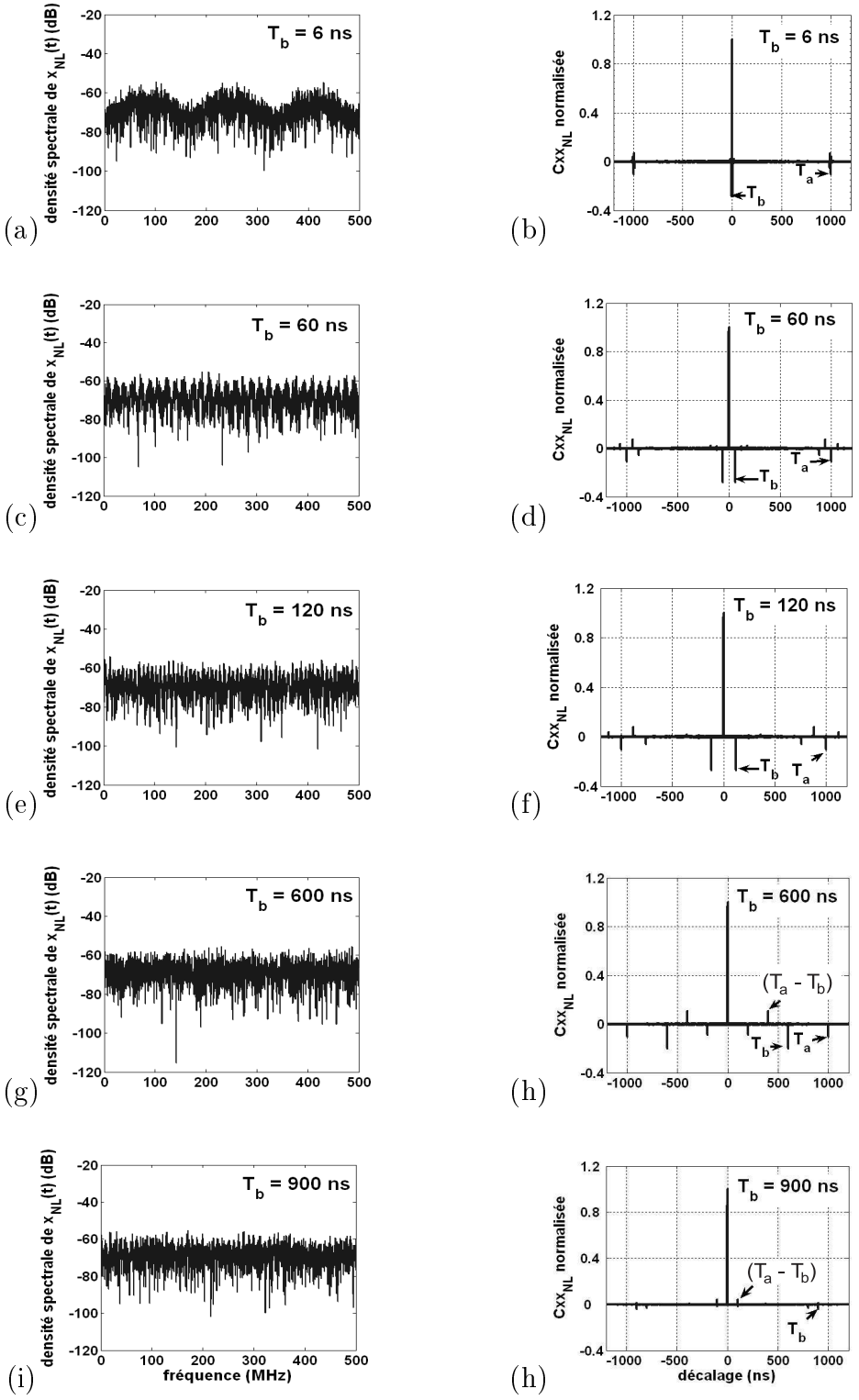



Figure 3.26 – *Influence du délai de la boucle* $(B)$ *à gain faible.* $T_a = 1\,\mu s$ ; $\beta_a = 10$ ; $\beta_b = 1,8$

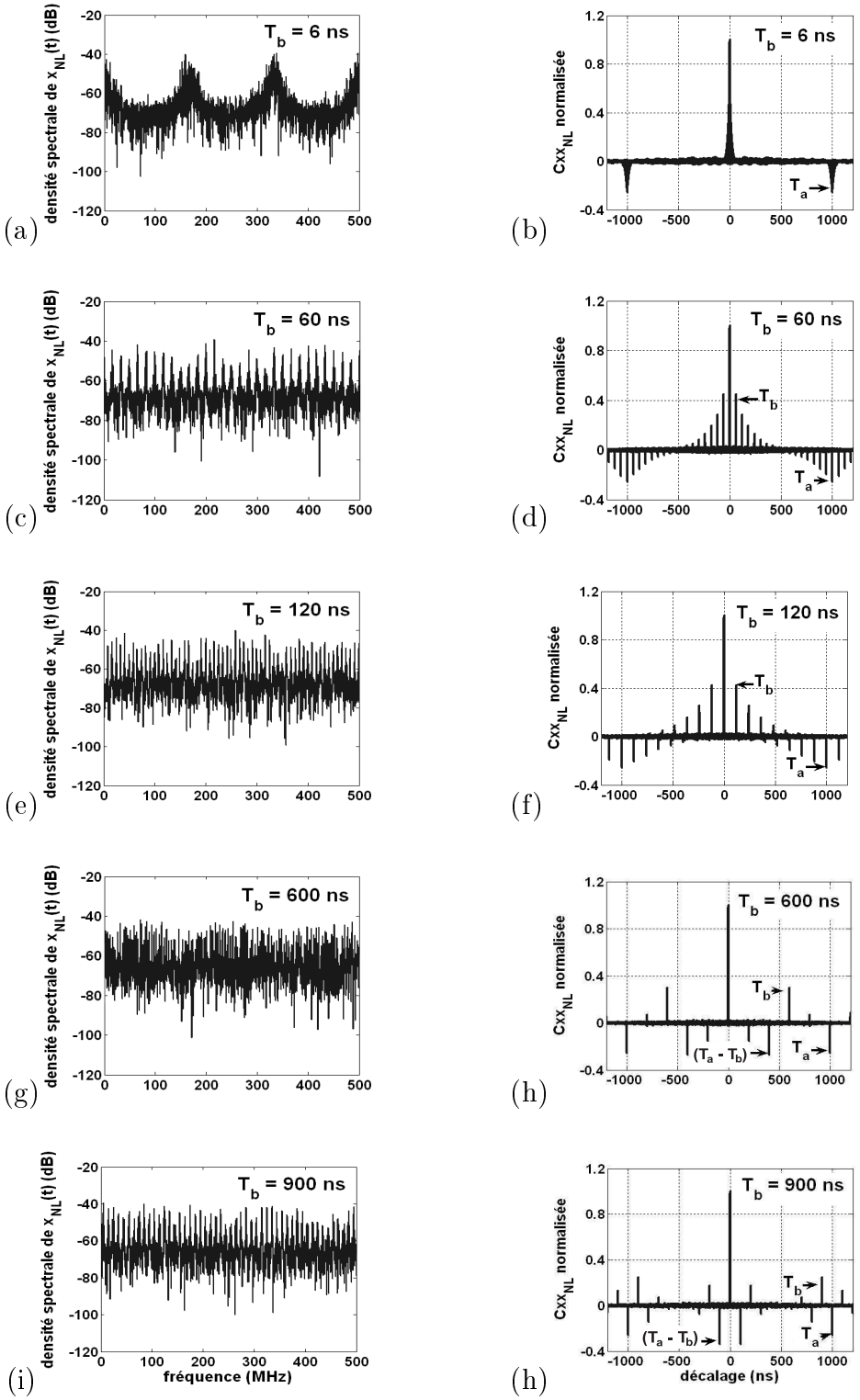



FIGURE 3.27 – *Influence du délai de la boucle* $(B)$ *à gain élevé.* $T_a = 1\,\mu s$ ; $\beta_a = 1,8$ ; $\beta_b = 10$

les détails trois configurations possibles du système, où seul les bandes passantes des filtres sont différentes. Ces configurations sont choisies suivant ces bandes de la manière suivante : la première est lorsque la bande-passante d'un filtre est comprise dans la bande passante de l'autre, la deuxième est lorsque seule une partie de la bande passante est commune entre les deux filtres, et enfin la dernière configuration, lorsqu'elles n'ont pas d'intervalle de fréquences en commun.

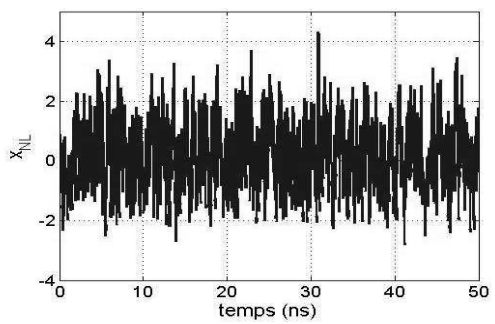
La figure 3.28 montre les traces temporelles chaotiques obtenues et les spectres associées aux trois configurations choisies. Nous constatons qu'en général la bande passante du système est réduite, et particulièrement lorsqu'il n'y a pas d'intervalle de fréquence en commun ($3^{\text{ième}}$ cas sur la figure ; le régime chaotique n'est ni entièrement développé, ni stationnaire).

Réduire les bandes passantes du système *a priori* n'est pas souhaitable, car elle implique la réduction du débit de transmission d'informations. Par contre, ces résultats ouvrent des perspectives nouvelles et prometteuses, pour augmenter le degré de la sécurité des transmissions par chaos. À titre d'exemple, nous avons vu à travers la fonction d'autocorrélation que les délais du système sont décelables dans certaines configurations du générateur. Une suggestion de solution pour remédier à cet inconvénient, et qui reste par ailleurs une piste à explorer, est de procéder à un filtrage des fréquences correspondantes à ces délais à travers les bandes passantes du système.

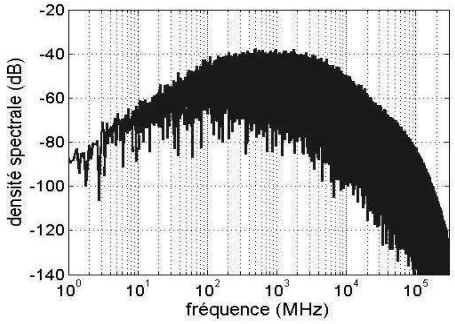
## 3.4 Synchronisation émetteur/récepteur

Dans cette section nous allons aborder le système de cryptographie chaotique complet, composé d'un émetteur et d'un récepteur. La restitution du message utile, introduit par modulation chaotique, dépend en premier lieu de la capacité du récepteur à reproduire le plus fidèlement possible les oscillations de l'émetteur [107]. Ce processus de reproduction est appelé communément « la synchronisation ».

Dans la littérature plusieurs concepts de synchronisation ont été proposés dans le but de dupliquer le signal chaotique employé à l'émetteur. Parmi ces concepts, on trouve la méthode de la synchronisation chaotique identique [2], développée sur la base de circuits chaotiques couplés, avec l'un maître et l'autre esclave. Une autre approche plus récente est la méthode de synchronisation généralisée [108–110]. Cette méthode est basée aussi sur une paire de systèmes configurés en maître-esclave, mais cette fois la synchronisation n'est pas limitée à l'identité (rapport de proportionnalité constant). Un dernier exemple de ces méthodes est celle de la synchronisations de phase entre deux circuits chaotiques couplés, dont le principe est basée sur la réalisation d'une cohérence de phase entre les variables d'états des systèmes considérés [111, 112]. Nous orientons le lecteur pour plus de détails sur ces méthodes, en plus des références que nous venons de citer, à la référence [113] qui décrit aussi bien ces méthodes ainsi que d'autres configurations de synchronisation.

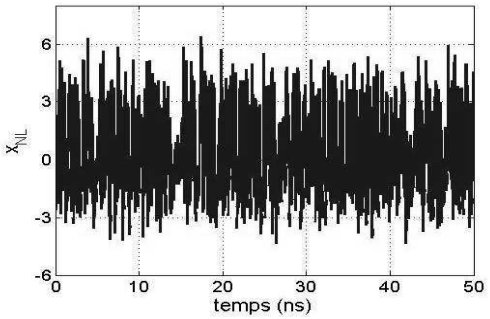



(a)

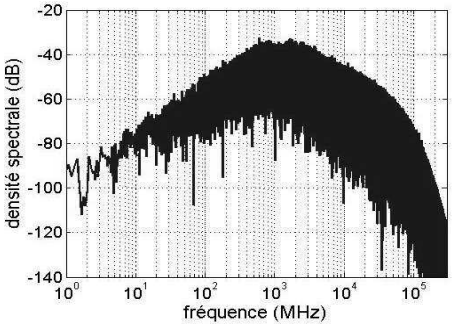



(b)

**1er cas :** filtre (A) : 30 kHz $\longrightarrow$ 13 GHz, filtre (B) : 100 MHz $\longrightarrow$ 3 GHz

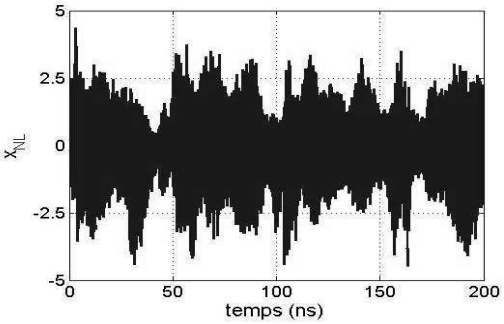



(c)

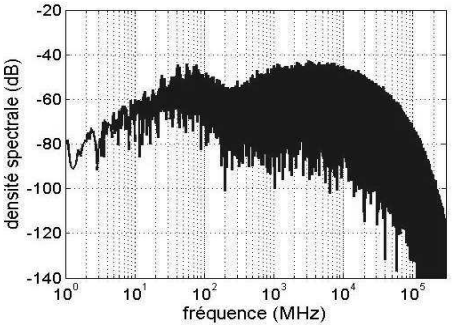



(d)

**2ième cas :** filtre (A) : 30 kHz $\longrightarrow$ 800 MHz, filtre (B) : 500 MHz $\longrightarrow$ 13 GHz




(e)




(f)

**3ième cas :** filtre (A) : 30 kHz $\longrightarrow$ 13 MHz, filtre (B) : 1 GHz $\longrightarrow$ 13 GHz

Figure 3.28 – *Exemples d'influence des bandes passantes des filtres sur la dynamique du système.* $\beta_a = \beta_b = 10$.

Néanmoins, pour illustrer la méthode de synchronisation par couplage entre deux systèmes chaotiques, nous avons choisi de présenter brièvement la synchronisation identique proposée par Pecora et Carroll [2]. Celle-ci a l'avantage de représenter une solution simple et performante, dont l'objectif est que l'esclave reproduise l'état du maître après un régime transitoire. En effet, Pecora et Carroll ont considéré l'émetteur comme étant un système dynamique *autonome* (maître), et le récepteur comme un sous-système *non-autonome* (esclave). Ce dernier est constitué d'une partie dupliquée du maître. Une formulation analytique plus simple de leur concept de synchronisation peut se faire de la façon suivante : considérons un système dynamique maître initial, de dimension $n$, représenté par la relation suivante :

$$\dot{u} = f(u) \tag{3.13}$$

où $u = [u_1, \ldots, u_n]^T$ est un vecteur d'état de l'oscillateur. Ce vecteur est divisé arbitrairement en 2 vecteurs appartenant à 2 sous espaces de l'espace des phases ($v = [v_1, \ldots, v_m]^T$ et $w = [w_{m+1}, \ldots, w_n]^T$). Chacun de ces 2 vecteurs répond à une loi dynamique dérivée conformément aux relations suivantes :

$$\begin{cases} \dot{v} = g\big[v, w\big] = \big[f_1(u), \ldots, f_m(u)\big] \\ \dot{w} = h\big[v, w\big] = \big[f_{m+1}(u), \ldots, f_n(u)\big] \end{cases} \tag{3.14}$$

Le sous-système esclave (le récepteur) est construit sur le modèle du vecteur $w$, soit $w'$. Pour qu'il puisse reproduire la même dynamique du maître, il est nécessaire de lui transmettre le vecteur $v$, comme illustré sur la figure 3.29.

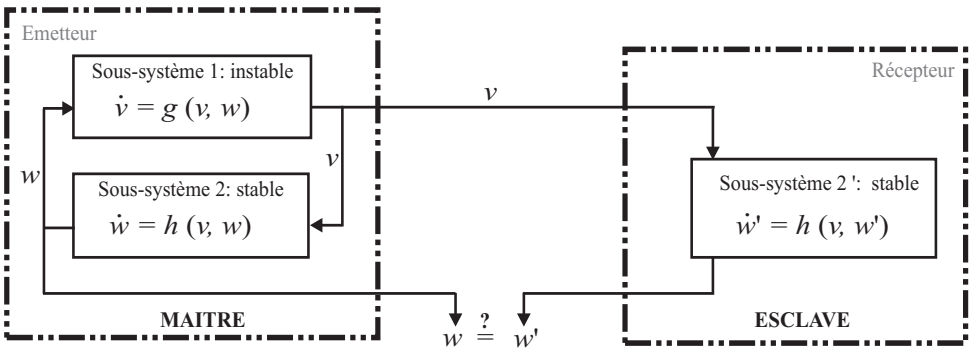



FIGURE 3.29 – *Schéma du principe de synchronisation identique.*

La dynamique du système esclave est donc décrite par :

$$\dot{w'} = h(v, w') \tag{3.15}$$

Par définition, les variables $w$ et $w'$ se synchronisent si la différence $\Delta w = w' - w$ converge vers 0 dans le temps ($t \longrightarrow \infty$). Plus concrètement, Pecora et Carroll ont démontré que $\Delta w$ évolue selon une loi dynamique du type :

$$\dot{w} = D_w h(v, w) \cdot \Delta w \tag{3.16}$$

où $D_w h$ est le Jacobien du système $w$. Il faut noter qu'à partir de l'équation (3.16), les exposants de Lyapunov peuvent être obtenus. Si les exposants sont tous négatifs, le sous-système est stable, et le vecteur $w'$ du système esclave va suivre le comportement $w$ du maître. Une synchronisation parfaite peut alors être obtenue. Ces exposants sont connus sous le nom d'*exposants de Lyapunov conditionnels* (CLE[5]).

Cette méthode de synchronisation identique a été appliquée numériquement par ces auteurs à des systèmes dynamiques connus (Lorenz et Rössler [114]), et ils ont démontré que la synchronisation est relativement robuste même avec de petits écarts de paramètres allant de 10 à 20 %. Cependant, cette méthode est conditionnée par la possibilité de décomposer le système maître en sous-sytèmes, dont l'un au moins est stable (c'est-à-dire tous ses exposants de Lyapunov sont négatifs), ce qui n'est physiquement pas toujours possible.

L'exemple de synchronisation que nous venons de décrire ne sera pas appliqué intégralement pour la synchronisation de notre système, mais le principe sera le même. En effet, vu que le critère de stabilité du sous-système du maître est basé sur les exposants de Lyapunov, ceux-ci n'ont pas été calculés dans le cadre de cette thèse. Nous avons donc adopté une méthode de cryptage-décryptage plus souple, qui a fait ses preuves dans le cadre des autres démonstrateurs de cryptage par chaos [13,35]. Cette méthode est basée sur le principe de la boucle ouverte du récepteur. Elle consiste à faire passer le signal chaotique transmis, au niveau du récepteur, par une boucle ouverte contenant les mêmes éléments que ceux présents à l'émetteur.

À présent, nous allons présenter les architectures envisageables du système cryptographique complet, puis nous les explorerons à travers une étude numérique. Cette étude va nous permettre de comprendre, d'une part, comment choisir les paramètres de fonctionnement du système complet, et d'autre part, quelle est la configuration du système récepteur privilégiée afin de restituer le message utile avec une bonne qualité de décodage.

### 3.4.1 Architecture du système cryptographique complet

Un schéma du principe de l'ensemble du système (émetteur + récepteur) est illustré sur la figure 3.30. L'architecture du récepteur est déterminée par l'architecture de l'émetteur, avec toutefois quelques différences entre les deux. Avant de détailler ces différences, nous adoptons à partir de cette section pour indiquer qu'il s'agit des paramètres du récepteur, la notation par le symbole *tilda* «˜» de tous ses paramètres.

[5]En anglais : Conditional Lyapunov Exponents

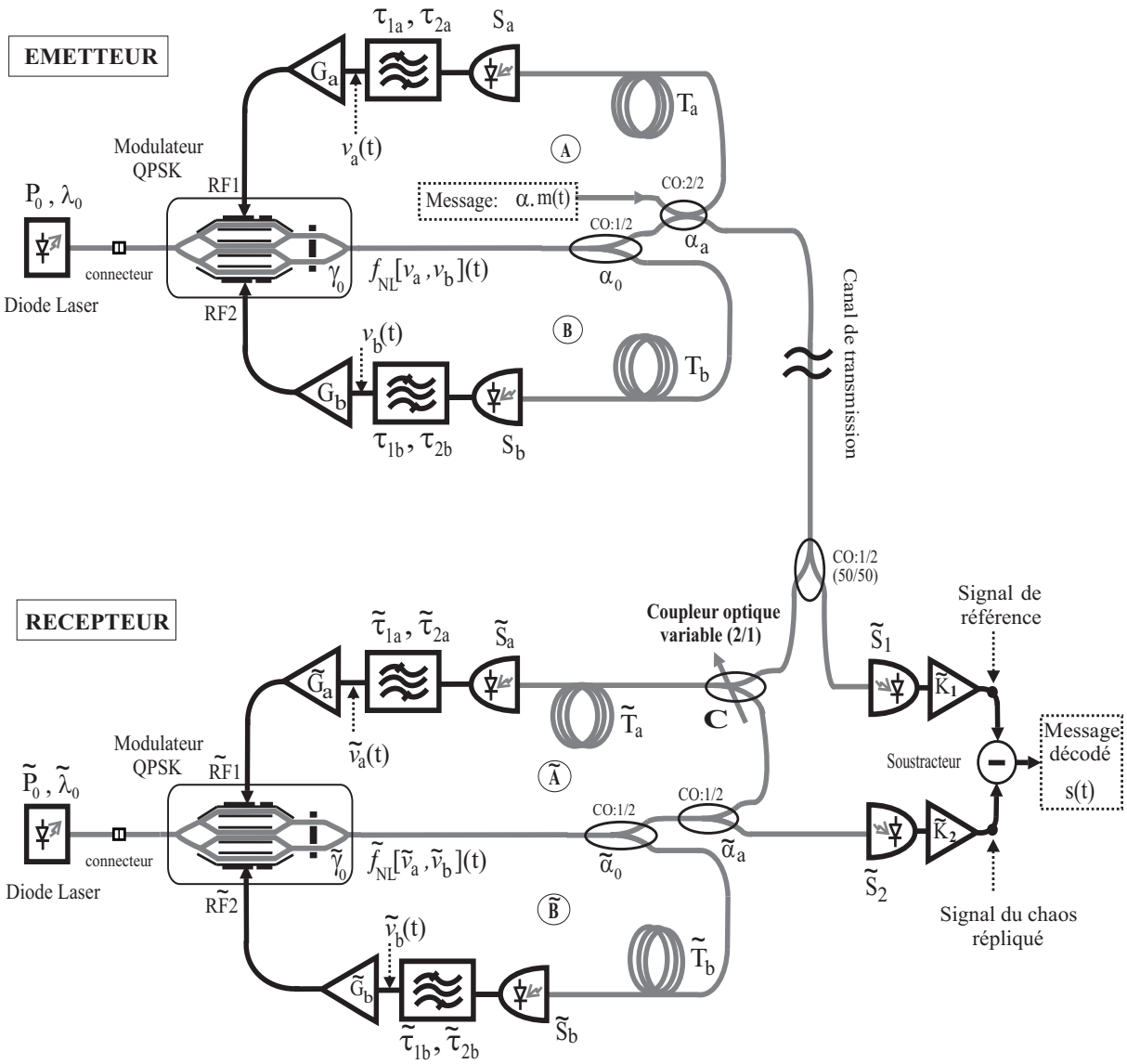



FIGURE 3.30 – *Schéma de principe du système cryptographique complet. Le récepteur est couplé en boucle fermée.*

Même si l'architecture du récepteur est très proche de celle de l'émetteur par certains aspects (mêmes blocs fonctionnels, mêmes composants), il n'en reste pas moins différent : le signal chaotique masquant le message est traité par deux voies différentes. En effet, grâce à un coupleur optique (1 entrée /2 sorties), le signal chaotique reçu est divisé en 2 signaux optiques. Le premier est directement détecté et converti en électrique par une photodiode rapide, puis amplifié pour fournir à la fin : **le signal de référence**.

Le second signal optique est combiné avec la contre-réaction de la boucle $(\tilde{A})$ à l'aide d'un coupleur optique variable (2 entrées/1 sortie), qui se caractérise par *un taux de couplage variable* $C$. Le signal optique ainsi combiné parcourt les mêmes éléments que le signal de contre-réaction de la boucle (A) de l'émetteur. La récupération du signal à la sortie du récepteur s'effectue à l'aide d'un autre coupleur optique (1 entrée /2 sorties) *via*

la boucle $(\tilde{A})$. Ainsi, après une conversion optique / électrique et une amplification RF, ce signal représente : **le signal du chaos répliqué**.

L'extraction du message s'effectue en additionnant le signal du chaos répliqué avec celui de référence *via* un diviseur de puissance monté en combineur de puissance (2 signaux d'entrée, 1 signal de sortie). L'addition se fait de telle manière à annuler la composante chaotique du signal de référence. Cette opération se réalise lorsque le signal du chaos répliqué devient l'opposé du signal de référence par un réglage adéquat des phases du modulateur QPSK du récepteur. Dans ce cas, l'addition qu'effectue le diviseur de puissance devient une soustraction dont résulte le message décodé.

Pour avoir toutes les chances de récupérer un message de bonne qualité, les oscillations du signal chaotique répliqué doivent correspondre aux oscillations que l'émetteur génère juste avant l'insertion optique du message. Cependant, pour restituer un message au niveau du récepteur, il faut d'abord l'introduire au niveau de l'émetteur. Nous allons donc, dans ce qui suit, voir comment l'insertion du message se fait au niveau du modèle régissant la dynamique de l'émetteur, puis nous étudierons le récepteur, après sa mise en équations, pour déterminer les conditions de couplage favorables permettant de restituer ce message.

### 3.4.2 Mise en équation du récepteur

Nous nous limitons dans cette étude à un message $m(t)$ de nature binaire. L'expression de $m(t)$ n'apparaît pas dans le système d'EDR (2.17) qui régit le comportement dynamique de l'émetteur. Ce message est injecté par modulation chaotique — section 1.5.1 — au niveau de la boucle (A) de l'émetteur. Ce qui se traduit par les équations suivantes :

**- Système d'EDR du second ordre avec message [Émetteur] :**

$$\begin{cases} x_a(t) + [\tau_{1a} + \tau_{2a}] \cdot \dfrac{dx_a}{dt}(t) + \tau_{1a} \cdot \tau_{2a} . \dfrac{d^2x_a}{dt^2}(t) = \beta_a \cdot \tau_{2a} \cdot \dfrac{d}{dt}\Big\{ \underbrace{f_{NL}[x_a, x_b](t - T_a) + \alpha \cdot m(t)}_{z_a(t)} \Big\} \\ x_b(t) + [\tau_{1b} + \tau_{2b}] \cdot \dfrac{dx_b}{dt}(t) + \tau_{1b} \cdot \tau_{2b} \cdot \dfrac{d^2x_b}{dt^2}(t) \ = \beta_b \cdot \tau_{2b} . \dfrac{d}{dt}\Big\{ f_{NL}[x_a, x_b](t - T_b) \Big\} \end{cases} \tag{3.17}$$

où $\alpha$ est un taux de masquage, défini comme étant le rapport entre l'amplitude du message et l'amplitude du signal chaotique. Ce taux de masquage joue un rôle déterminant par rapport à la qualité de masquage de l'information (nous reviendrons un peu plus loin sur ce point).

**- Système d'EDR du premier ordre avec message [Émetteur] :**
(utilisé pour l'algorithme numérique)

$$\begin{cases} x_a(t) + \tau_{2a} \cdot \dfrac{dx_a}{dt}(t) = \dfrac{\tau_{2a}}{\tau_{1a}} \cdot \left\{ \beta_a \cdot \Big[ \underbrace{f_{NL}\left[x_a, x_b\right](t - T_a) + \alpha \cdot m(t)}_{z_a(t)} \Big] - y_a(t) \right\} \\ y_a(t) + \tau_{1a} \cdot \dfrac{dy_a}{dt}(t) = \beta_a \cdot \Big[ \underbrace{f_{NL}\left[x_a, x_b\right](t - T_a) + \alpha \cdot m(t)}_{z_a(t)} \Big] \end{cases} \tag{3.18}$$

$$\begin{cases} x_b(t) + \tau_{2b} \cdot \dfrac{dx_b}{dt}(t) = \dfrac{\tau_{2b}}{\tau_{1b}} \cdot \Big[ \beta_b \cdot f_{NL}\left[x_a, x_b\right](t - T_b) - y_b(t) \Big] \\ y_b(t) + \tau_{1b} \cdot \dfrac{dy_b}{dt}(t) = \beta_b \cdot f_{NL}\left[x_a, x_b\right](t - T_b) \end{cases} \tag{3.19}$$

Par souci de simplification d'écriture, posons (comme représenté sur le système (3.17)) :

$$z_a(t) = f_{NL}\left[x_a, x_b\right](t - T_a) + \alpha \cdot m(t) \tag{3.20}$$

L'indice de $z_a(t)$ nous rappelle que le signal est de la provenance de la boucle (A) de l'émetteur. En raisons de contraintes technologiques, le signal optique transmis de l'émetteur vers le canal de transmission est aussi prélevé de cette boucle. Nous appelons ce signal $x_{\text{émett}}$, dont l'expression est donnée par la relation suivante :

$$x_{\text{émett}}(t) = \beta_a \cdot z_a(t) \tag{3.21}$$

Dans l'hypothèse que le canal de transmission n'introduit aucune modification sur le signal transmis $x_{\text{émett}}(t)$, celui-ci est divisé en 2 signaux égaux à l'entrée du récepteur par un coupleur optique ($50 \times 50$). L'un de ces signaux est injecté dans la boucle ($\tilde{A}$) du récepteur, et l'autre après sa détection et son amplification[6] est celui que nous avons appelé le signal de référence. L'expression de celui-ci est donnée par :

$$x_{\text{réf}}(t) = \frac{1}{2} \cdot \widetilde{K}_1 \cdot \widetilde{S}_1 \cdot x_{\text{émett}}(t) = \widetilde{k}_1 \cdot \Big[ f_{NL}\left[x_a, x_b\right](t - T_a) + \alpha \cdot m(t) \Big] \tag{3.22}$$

avec $\widetilde{k}_1 = (\beta_a \cdot \widetilde{K}_1 \cdot \widetilde{S}_1)/2$ ; représentant le taux de couplage optique et de la sensibilité du photodétecteur du signal de référence.

[6] **Remarque importante** : pour des raisons de simplification, nous considérons que la dynamique de détection et d'amplification est linéaire, et ne fait subir aucun filtrage supplémentaire au signal reçu. Ces conditions sont tout à fait réalisables lorsque la bande passante de cette dynamique est très large par rapport à celle de l'émetteur. Dans le cas contraire, sa mise en équation sera semblable à celles effectuées au chapitre 1, dans le cas d'un filtre passe bande par exemple.

L'autre signal optique — celui injecté dans la boucle ($\tilde{A}$) du récepteur — parcourt la même chaîne d'éléments appairés avec ceux de la boucle (A) de l'émetteur. Et comme l'architecture du système récepteur est quasi identique à celle de l'émetteur, le comportement dynamique du récepteur est régit lui aussi par un système d'EDR, donné par (3.23).

**- Système d'EDR du second ordre avec message [Récepteur] :**

$$\begin{cases} \widetilde{x}_a(t) + [\widetilde{\tau}_{1a} + \widetilde{\tau}_{2a}] \cdot \dfrac{d\widetilde{x}_a}{dt}(t) + \widetilde{\tau}_{1a} \cdot \widetilde{\tau}_{2a} . \dfrac{d^2\widetilde{x}_a}{dt^2}(t) = \widetilde{\beta}_a \cdot \widetilde{\tau}_{2a} \cdot \dfrac{d}{dt}\Big\{\widetilde{yy}_a(t)\Big\} \\ \widetilde{x}_b(t) + [\widetilde{\tau}_{1b} + \widetilde{\tau}_{2b}] \cdot \dfrac{d\widetilde{x}_b}{dt}(t) + \widetilde{\tau}_{1b} \cdot \widetilde{\tau}_{2b} \cdot \dfrac{d^2\widetilde{x}_b}{dt^2}(t) \ = \widetilde{\beta}_b \cdot \widetilde{\tau}_{2b} . \dfrac{d}{dt}\Big\{\widetilde{f}_{NL}[\widetilde{x}_a, \widetilde{x}_b](t - \widetilde{T}_b)\Big\} \end{cases} \tag{3.23}$$

**-Système d'EDR du premier ordre avec message [Récepteur] :**
(utilisé pour l'algorithme numérique)

$$\begin{cases} \widetilde{\tau}_{2a} \cdot \dfrac{d\widetilde{x}_a}{dt}(t) = \dfrac{\widetilde{\tau}_{2a}}{\widetilde{\tau}_{1a}} \cdot \Big[\widetilde{\beta}_a \cdot \widetilde{yy}_a(t) - \widetilde{y}_a(t)\Big] - \widetilde{x}_a(t) \\ \widetilde{\tau}_{1a} \cdot \dfrac{d\widetilde{y}_a}{dt}(t) = \widetilde{\beta}_a \cdot \widetilde{yy}_a(t) - \widetilde{y}_a(t) \end{cases} \tag{3.24}$$

$$\begin{cases} \widetilde{\tau}_{2b} \cdot \dfrac{d\widetilde{x}_b}{dt}(t) = \dfrac{\widetilde{\tau}_{2b}}{\widetilde{\tau}_{1b}} \cdot \Big[\widetilde{\beta}_b \cdot \widetilde{f}_{NL}\left[\widetilde{x}_a, \widetilde{x}_b\right](t - \widetilde{T}_b) - \widetilde{y}_b(t)\Big] - \widetilde{x}_b(t) \\ \widetilde{\tau}_{1b} \cdot \dfrac{d\widetilde{y}_b}{dt}(t) = \widetilde{\beta}_b \cdot \widetilde{f}_{NL}\left[\widetilde{x}_a, \widetilde{x}_b\right](t - \widetilde{T}_b) - \widetilde{y}_b(t) \end{cases} \tag{3.25}$$

avec :

$$\widetilde{yy}_a(t) = \widetilde{f}_{NL}\left[\widetilde{x}_a, \widetilde{x}_b\right](t - \widetilde{T}_a) + C\Big[f_{NL}\left[x_a, x_b\right](t - T_a) + \alpha\, m(t) - \widetilde{f}_{NL}\left[\widetilde{x}_a, \widetilde{x}_b\right](t - \widetilde{T}_a)\Big] \tag{3.26}$$

À noter que le signe « − » devant le terme $\widetilde{f}_{NL}[...]$ de la relation (3.26) est dû à l'opposition du chaos répliqué au récepteur par rapport au chaos de référence de l'émetteur. Le signal optique chaotique répliqué est prélevé de la boucle ($\tilde{A}$) du récepteur *via* un coupleur optique 1 entré/2 sorties (voir la figure 3.30, son coefficient de couplage est $\widetilde{\alpha}_a$). Son expression juste à la sortie du coupleur est donnée par :

$$x_{\text{récept}}(t) = \widetilde{\beta}_a \cdot \widetilde{f}_{NL}\left[\widetilde{x}_a, \widetilde{x}_b\right](t - \widetilde{T}_a) \tag{3.27}$$

Ce signal optique $x_{\text{récept}}(t)$ est ensuite détecté, puis converti en un signal électrique par une photodiode, de sensibilité $\widetilde{S}_2$, puis amplifié par un facteur $\widetilde{K}_2$, pour enfin donner naissance au signal chaotique répliqué. L'expression de ce dernier est donnée par :

$$x_{\text{rép}}(t) = \widetilde{K}_2 \cdot \widetilde{S}_2 \cdot x_{\text{récept}}(t) = \widetilde{k}_2 \cdot \widetilde{f}_{NL}\left[\widetilde{x}_a, \widetilde{x}_b\right](t - \widetilde{T}_a) \tag{3.28}$$

Enfin, le décodage s'effectue par l'opération : $x_{\text{réf}}(t) + x_{\text{rép}}(t)$, comme expliqué précédemment. Le signal décodé $s(t)$ ainsi obtenu est donné par :

$$s(t) = \widetilde{k}_1 \cdot \Big[f_{NL}\left[x_a, x_b\right](t - T_a) + \alpha \cdot m(t)\Big] + \widetilde{k}_2 \cdot \widetilde{f}_{NL}\left[\widetilde{x}_a, \widetilde{x}_b\right](t - \widetilde{T}_a) \tag{3.29}$$

Lorsque le récepteur est parfaitement réglé (synchronisation parfaite), le signal décodé $s(t)$ est proportionnel au message $m(t)$. Cette synchronisation est idéale, loin des conditions réelles de fonctionnement du système physique. En effet, comme le montre la relation (3.29), $s(t)$ dépend principalement de la similarité des 2 fonctions non linéaires réalisées respectivement par l'émetteur et le récepteur. L'architecture en boucle fermée du récepteur influe directement sur cette similarité des fonctions non linéaires. En fait, la configuration du récepteur dans ce cas lui procure un aspect de générateur de chaos autonome, capable de générer ses propres oscillations indépendamment de l'émetteur. La solution — récepteur synchronisé sur l'émetteur — est induite grâce au taux de couplage imposé entre ces deux systèmes. Ce taux de couplage est représenté par le coefficient $C$ dans l'équation (3.26), et réalisé par exemple par un coupleur optique variable (voir la figure 3.30).

Nous allons donc, dans la section suivante, étudier numériquement l'état de synchronisation en fonction de $C$, et chercher dans quelles conditions le récepteur en boucle fermée est capable de répliquer les oscillations chaotiques de l'émetteur. La précision de cette réplication en fonction des différents paramètres du récepteur constitue la clé de décodage.

### 3.4.3 Condition de couplage

L'approche suivie consiste à considérer tous les paramètres du récepteur identiques à ceux de l'émetteur, et à faire varier le coefficient de couplage $C$. Dans ces conditions, l'erreur de décodage générée est une erreur de synchronisation, notée « $\varepsilon(C)$ » . Nous définissons alors une erreur instantanée de synchronisation par la relation suivante :

$$\sigma(t) = x_{\text{rép}}(t) - x_{\text{réf}}(t) \tag{3.30}$$

L'erreur $\varepsilon(C)$ est estimée à partir de sa valeur quadratique moyenne normalisée. Sa normalisation est effectuée par rapport à l'amplitude efficace de l'oscillation chaotique de l'émetteur. Son expression est donnée par la relation suivante :

$$\varepsilon(C) = 100 \cdot \frac{< \sigma^2 >}{< x^2_{\text{réf}} >} \qquad (\%) \tag{3.31}$$

Nous avons cherché à estimer cette erreur dans deux configurations différentes : la première est sans insertion de message et la seconde avec message. Dans le cas sans message, l'erreur $\varepsilon(C)$ est toujours nulle pour toute valeur du coefficient de couplage $C$ allant de 0 à 1 (0 : aucun couplage, 1 : couplage total). Ce résultat est trivial compte tenu des conditions idéales considérées. Par contre, lorsqu'un message est inséré, nous avons constaté que la situation est complètement différente.

En effet, lorsque le système est considéré totalement synchronisé (le temps nécessaire à la synchronisation correspond grossièrement à la durée des régimes transitoires estimée à $6\tau_{2b} = 31,8\,\mu$s), nous avons introduit un message binaire codé NRZ[7]. Ce message est une séquence numérique générée aléatoirement (figure 3.32a), dont le temps d'un bit est de 300 ps (débit binaire $\approx$ 3,3 Gbit/s), et un taux de masquage très faible ($\alpha \approx 1\%$).

Les résultats obtenus — figure 3.31 — montrent que l'erreur de synchronisation dépend simultanément du coefficient de couplage $C$ et de la valeur du gain global de l'une des boucles du système ($\beta_b$ dans le cas de cette figure). Nous constatons que l'erreur diminue globalement lorsque le coefficient $C$ tend vers 1. Ceci se traduit par la tendance du système à se synchroniser pour un couplage total. Nous constatons aussi qu'à partir d'un certain seuil de couplage ($C \approx 0,5$), cette erreur tend à s'annuler pour des gains $\beta_b$ faibles. Cette tendance paraît tout à fait logique, car plus $\beta_b$ est élevé, plus le fonctionnement autonome du récepteur est favorisé par rapport au couplage venant de l'émetteur [115].

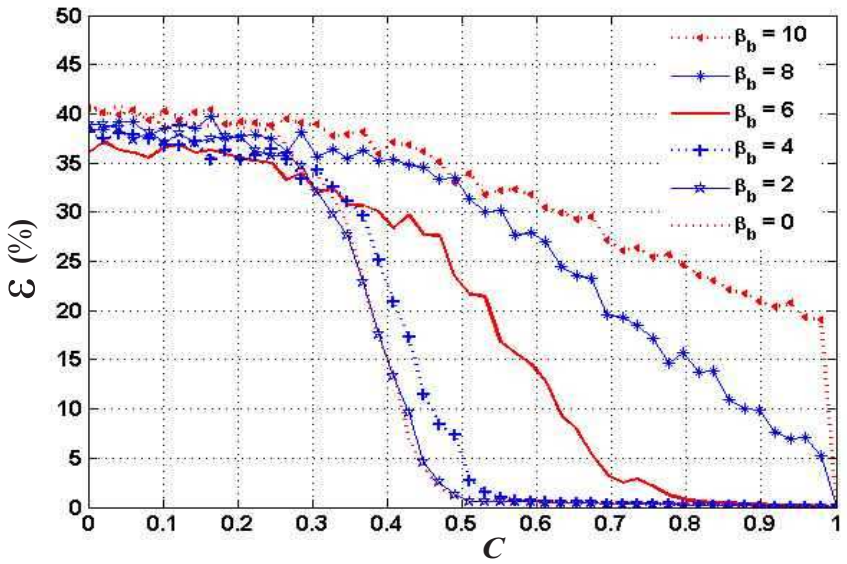



FIGURE 3.31 – *Évolution de l'erreur de synchronisation.* $\beta_a = 10$.

[7] En anglais : Non Return to Zero

Cependant, même si les solutions adéquates sont imposées au système ($\beta_b$ faible, $C$ proche de 1, $\alpha$ faible), la synchronisation du récepteur en boucle fermée reste difficile à réaliser. Ces propos sont justifiés par les résultats obtenus lors de nos tentatives de décodage, dans les conditions les plus probables de fonctionnement du système physique, à savoir des conditions initiales (CI) différentes entre l'émetteur et le récepteur. Un exemple de ces résultats est illustré sur la figure 3.32, où les niveaux « 0 » et « 1 » sont reconnus correctement si les CI sont identiques (figure 3.32b), alors que dans le cas contraire ces niveaux ne sont plus distinguables (figure 3.32c).

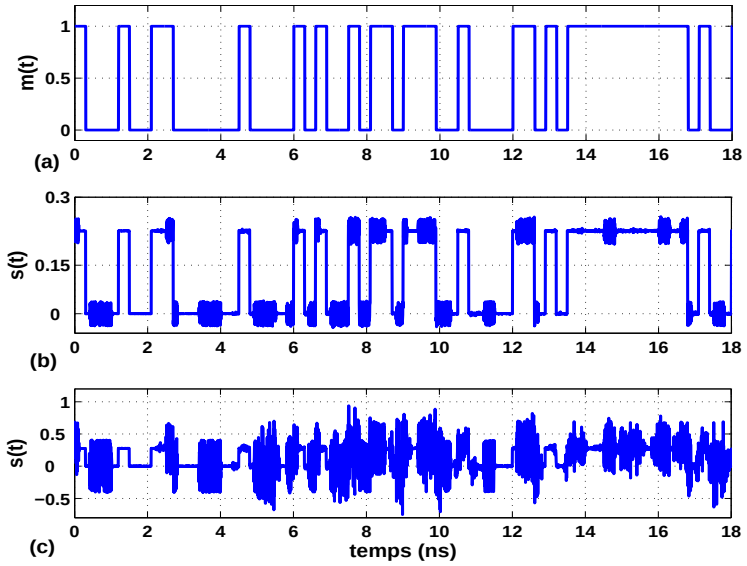



Figure 3.32 – *Exemple de décryptage d'un message binaire codé NRZ avec le récepteur en boucle fermée* ($C = 0,9$) ; *Paramètres de simulation* : $\alpha \approx 1,6\%$ ; $\beta_a = 10$ ; $\beta_b = 0,5$ ; (*a*) *Le message.* (*b*) *CI identiques.* (*c*) *CI différentes.*

À partir des difficultés que nous venons d'évoquer, nous privilégierons pour la suite le couplage total entre l'émetteur et le récepteur ($C = 1$). Physiquement, ce type de couplage signifie que la boucle ($\widetilde{A}$) est ouverte (voir la figure 3.33). Un exemple de décodage dans ces conditions est donnée sur la figure 3.34, où le message utile peut être restitué correctement, même si les CI sont différentes et avec un taux de masquage important.

Nous allons voir maintenant, après avoir choisi le couplage total, comment l'erreur évolue en fonction du gain de l'une des boucles du système (le gain considéré est toujours $\beta_b$). Les origines physiques de cette erreur sont diverses (bruits thermiques des composants, bruits du canal de transmission... etc), mais pour nos investigations, nous ne considèrerons que la différence des états initiaux de fonctionnement, et les désaccords de paramètres entre l'émetteur et le récepteur. Nous avons cherché à estimer cette erreur dans deux cas différents : le premier est lorsque seules les CI de l'émetteur et du récepteur sont différentes, et le second lorsque certains paramètres de l'émetteur sont en désaccords d'environ $\pm$ 1% par rapport à ceux du récepteur. Les paramètres en questions sont les gains des boucles et

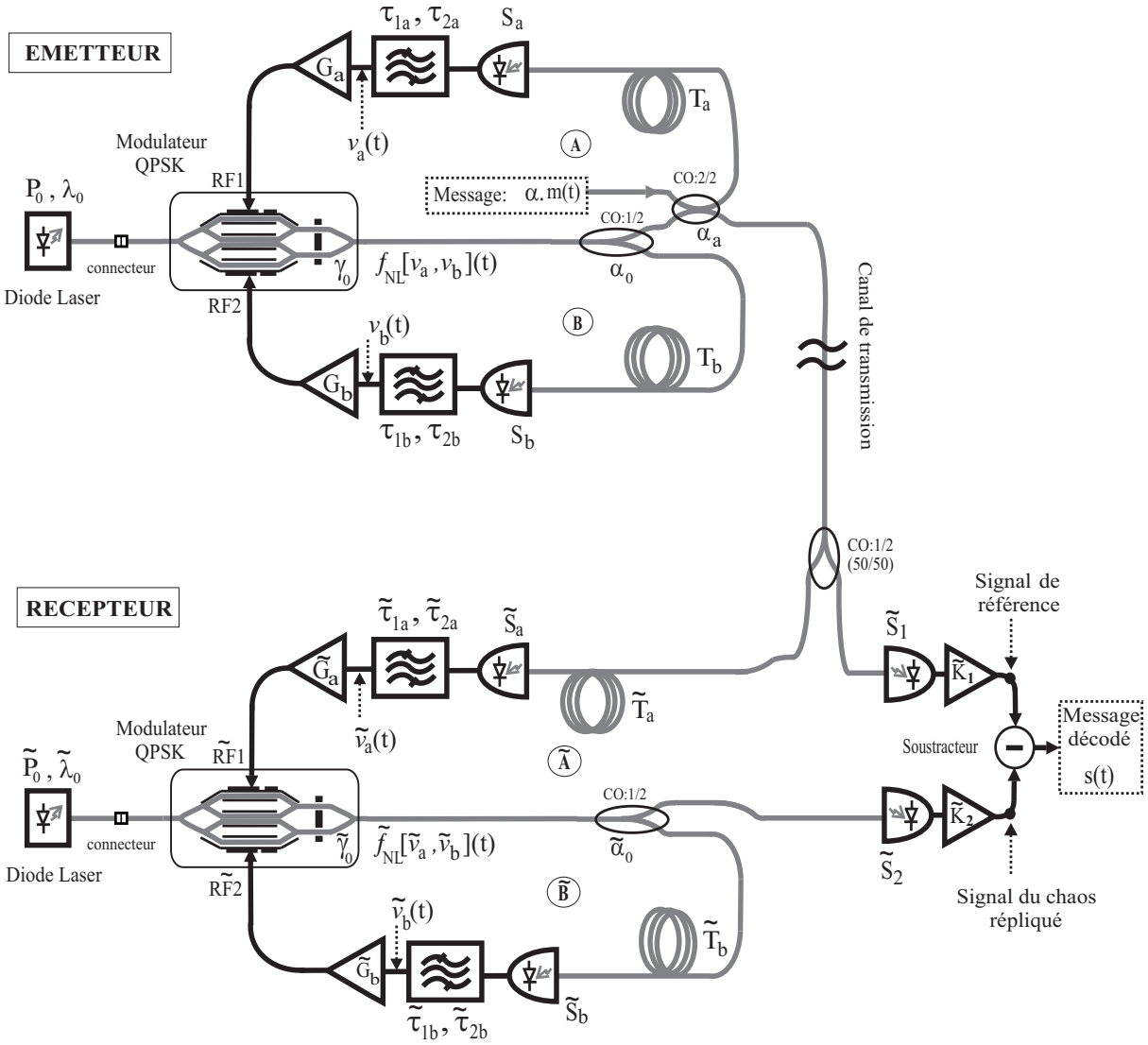



FIGURE 3.33 – *Schéma de principe du système cryptographique complet. Le récepteur est couplé en boucle ouverte.*

les fréquences de coupure des filtres passe-bandes. La figure 3.35 montre les résultats ainsi obtenus. Nous constatons que globalement l'erreur de synchronisation a tendance à s'annuler lorsque $\beta_b$ est faible. Cette tendance est plus nette lorsque seule les CI sont différentes, qu'en incluant les désaccords de paramètres.

Nous constatons aussi que l'erreur devient non négligeable au delà de $\beta_b \approx 3$. Celle-ci peut être réduite par contre par un réglage plus minutieux de certains paramètres par exemple. Cette solution est tout à fait possible, car comme nous allons le voir dans la section suivante, la sensibilité de la synchronisation est différente d'un paramètre à l'autre.

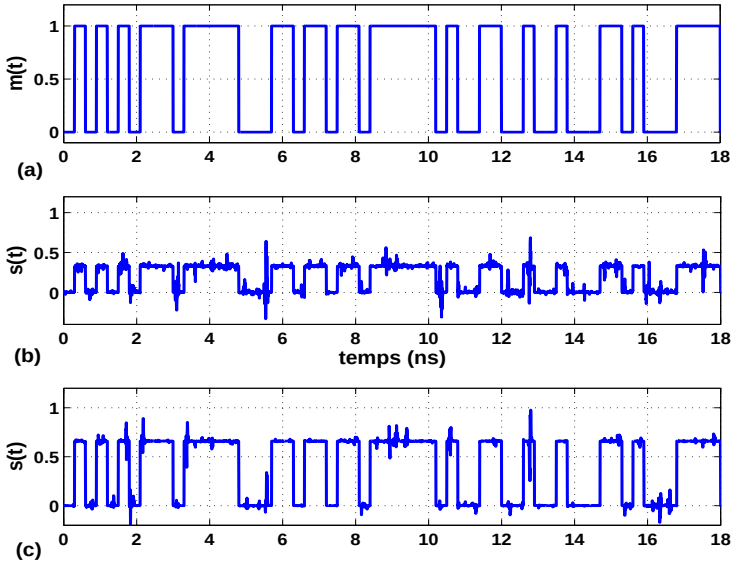



Figure 3.34 – *Exemple de décryptage d'un message binaire codé NRZ avec le récepteur à boucle ouverte* ($C = 1$) ; *Paramètres de simulation* : $\beta_a = 10$ ; $\beta_b = 2,2$ ; (*a*) *Le message.* (*b*) *CI différentes et* $\alpha = 10\%$. (*c*) *CI différentes et* $\alpha = 20\%$.

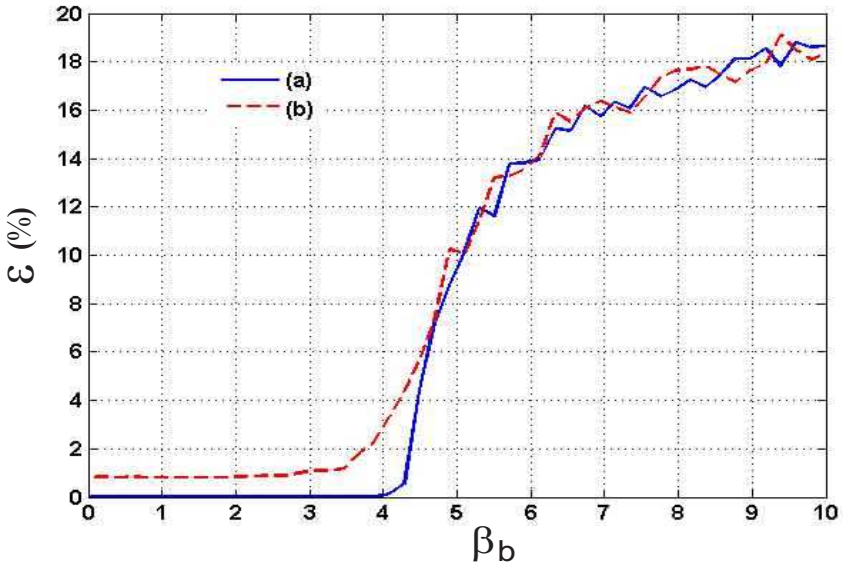



Figure 3.35 – *Évolution de l'erreur de synchronisation en fonction du gain* $\beta_b$. (*a*) *CI différentes.* (*b*) *CI différentes, et désaccords de paramètres.*

### 3.4.4 Étude de la sensibilité de la synchronisation

Pour réduire le plus possible l'erreur de synchronisation, nous allons étudier la sensibilité de celle-ci par rapport au désaccord de chacun des paramètres. Nous signalons par avance que cette étude est numérique, et limitée aux paramètres ajustables expérimentalement. Ces paramètres sont ceux cités à la section précédente avec en plus les phases des modulateurs QPSK et les retards temporels. Cette étude est inspirée de la référence [116] où le lecteur peut trouver des éléments de réponse théorique. L'influence d'un désaccord du paramètre $p$ est effectuée sous l'hypothèse que tous les autres paramètres sont parfaitement accordés.

#### Désaccord des gains globaux des boucles :

Les conditions de ces simulations se limitent à nouveau au cas le plus favorable, où un gain d'une boucle est élevé ($\beta_a = 10$) et l'autre faible ($\beta_b = 1,5$). C'est aussi autour de ces deux valeurs que la suite de l'étude va se poursuivre.

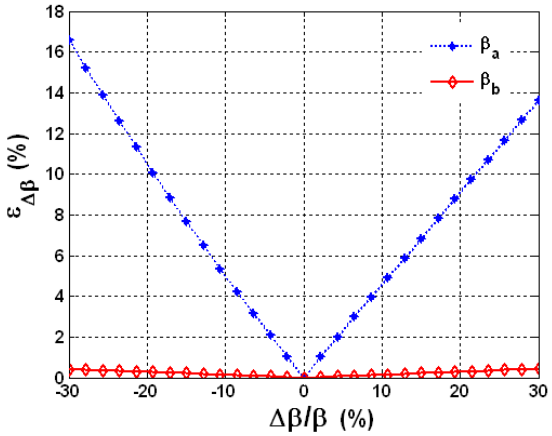



Figure 3.36 – *Influence du paramètre "gain de boucle" sur la synchronisation.*

La figure 3.36 présente les résultats obtenus en ce qui concerne l'influence d'un désaccord de gain de boucle sur la synchronisation. Nous constatons que l'évolution de l'erreur est linéaire. Nous remarquons aussi que les pentes relatives à l'écart autour de $\beta_a$ sont nettement plus grandes à ceux relatives à $\beta_b$. En d'autres termes, un écart autour de $\beta_a$ engendre une erreur plus conséquente qu'un écart autour de $\beta_b$, comme on peut s'y attendre. Nous constatons également que l'erreur n'est pas symétrique par rapport à l'axe qui définit une fonction d'amplification identique ($\Delta\beta/\beta = 0$). Ceci est dû probablement à la condition d'interférence au point de repos du modulateur QPSK.

**Désaccord des fréquences de coupure :**

Nous rappelons que les fréquences de coupure des filtres sont liées directement aux constantes de temps du système (relations (1.17)). Intuitivement, nous pouvons prévoir qu'un écart de ces fréquences entre l'émetteur et le récepteur va perturber les bandes passantes du chaos généré. Ce qui va se traduire par une perturbation du spectre chaotique et engendrer un bruit supplémentaire de décodage. Et comme nous avons pour chaque partie émetteur et récepteur 2 filtres soumis à des gains différents, nous avons voulu savoir si l'erreur est aussi dépendante du gain de la boucle où se trouve le filtre.

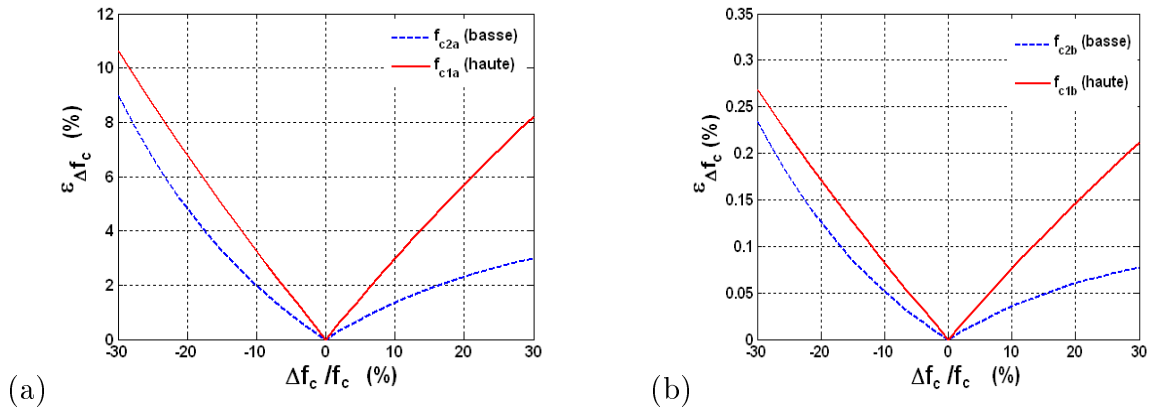



FIGURE 3.37 – *Influence de la différence des fréquences de coupure sur la synchronisation.* (*a*) *Filtre de la boucle* (*A*). (*b*) *filtre de la boucle* (*B*).

La figure 3.37 montre les résultats obtenus. Globalement, ces résultats confirment la dépendance de l'erreur en fonction du gain de la boucle. Plus le gain est fort plus l'erreur produite est conséquente. L'erreur engendrée par le désaccord de la fréquence de coupure haute est plus grande que celle produite par la fréquence de coupure basse. Dans la pratique, il est raisonnable de considérer des erreurs sur ces fréquences de coupure d'au plus quelques %, ce qui entraine au plus 1 % d'erreur de synchronisation.

**Désaccord des phases des modulateurs QPSK :**

L'origine d'un tel désaccord peu être liée à une différence de chemin optique résiduelle à l'intérieur des modulateurs QPSK, où encore à un mauvais réglage du point de fonctionnement du modulateur du récepteur par rapport à celui de l'émetteur.

Les résultats obtenus sont représentés sur la figure 3.38. Nous constatons que globalement l'erreur varie linéairement, et celle engendrée par un désaccord de $\phi_1$ est aussi plus conséquente que celle produite par l'écart de $\phi_2$, où encore de $\phi_3$. Le gain élevé de la boucle du côté de $\phi_1$ ($\beta_a = 10$) est probablement à l'origine de cet effet.

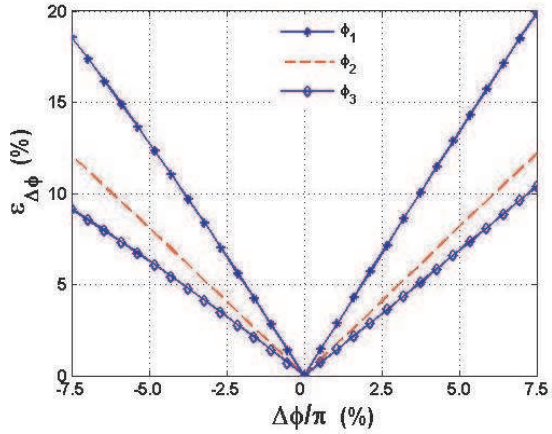



Figure 3.38 – *Influence de la différence des phases sur la synchronisation.*

En résumé, nous retenons donc que le système est très sensible aux désaccords des phases des modulateurs QPSK, et que le réglage du point de fonctionnement du récepteur doit être le plus proche possible de celui de l'émetteur, avec un soin particulier à la phase du modulateur du côté récepteur où le gain de boucle est élevé.

**Désaccord des retards temporels :**

Avec la rapidité des oscillations chaotiques par rapport aux retards temporels de l'oscillateur (ces derniers sont très grands devant les constantes de temps rapides du systèmes : $T_b/\tau_b \approx 5000 \gg 1$), nous pouvons nous attendre à ce qu'un faible désaccord de retard induise une dégradation importante de la synchronisation. Cette conséquence est clairement confirmée par les résultats donnés sur la figure 3.39.

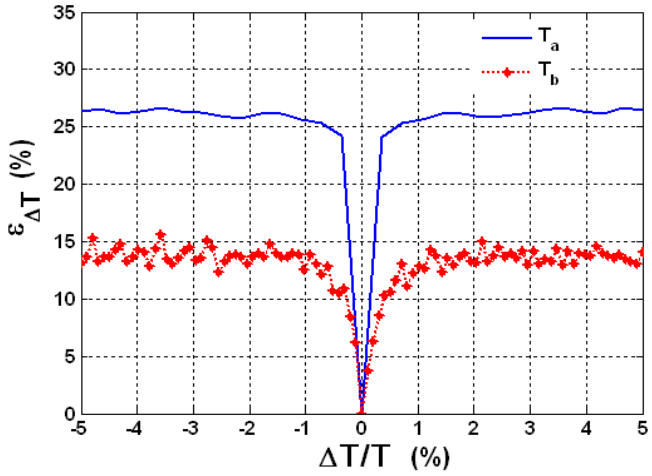



Figure 3.39 – *Influence de la différence des délais sur la synchronisation.*

Nous observons deux plateaux de désynchronisation, avec un creux en forme de " V " se terminant par un point anguleux de forte synchronisation. Nous constatons aussi que l'erreur induite par un écart de $T_a$ est visiblement très grande par rapport à celle engendrée par $T_b$. Cette différence est liée probablement encore aux gains différents des boucles. Nous concluons donc que l'erreur est très sensible à un désaccord de délai du système.

Un exemple d'une estimation approximative de l'erreur de synchronisation due à un désaccord de 1% de paramètre est donnée au tableau récapitulatif 3.2. L'objectif de cet exemple est de faire une comparaison de la sensibilité de la synchronisation par rapport à l'ensemble des paramètres que nous venons de voir. L'ordre de grandeur de l'erreur est donné à titre indicatif.

| **Boucle (A)** | | **Boucle (B)** | | **Modulateur QPSK** | |
|---|---|---|---|---|---|
| Paramètre | $\varepsilon_{\Delta p}$ (%) | Paramètre | $\varepsilon_{\Delta p}$ (%) | Paramètre | $\varepsilon_{\Delta p}$ (%) |
| $\beta_a$ | $\approx 0{,}4$ | $\beta_b$ | $\approx 0{,}05$ | $\phi_1$ | $\approx 2{,}4$ |
| $f_{c1a}$ | $\approx 0{,}3$ | $f_{c1b}$ | $\approx 0{,}008$ | $\phi_2$ | $\approx 1{,}6$ |
| $f_{c2a}$ | $\approx 0{,}2$ | $f_{c2b}$ | $\approx 0{,}004$ | $\phi_3$ | $\approx 1{,}2$ |
| $T_a$ | $\approx 27$ | $T_b$ | $\approx 12$ | | |

TABLE 3.2 – *Exemple récapitulatif de l'estimation de l'erreur de synchronisation $\varepsilon_{\Delta p}$ à 1% de désaccord d'un paramètre du système.*

Ainsi, nous pouvons tirer deux conclusions à partir de ce tableau : la première est que la synchronisation du récepteur sur l'émetteur est particulièrement sensible à l'écart des retards temporels ; et la seconde est générale : l'erreur de synchronisation due aux désaccords des paramètres se trouvants dans une boucle à gain global élevé est plus conséquente que celle engendrée par des paramètres d'une boucle à gain faible.

## 3.5 Conclusion

L'ensemble de ce chapitre a été consacré à l'étude du système cryptographique. Au travers des analyses numériques, nous avons montré que la nouvelle architecture du générateur du chaos en intensité à modulateur QPSK est capable de générer des dynamiques chaotiques en une seule boucle, comme en double boucle de rétroaction. Nous avons ensuite effectué une analyse temporelle, statistique et spectrale de quelques régimes d'oscillations du système. Cette analyse nous a permis de révéler qu'il suffit qu'un gain d'une boucle soit élevé, avec un choix adéquat du point de fonctionnement du modulateur QPSK, pour que la dynamique générée soit chaotique. Le tracé des diagrammes de bifurcation, de l'entropie et l'analyse dans l'espace des phases nous ont aussi confirmé ces conclusions dans les deux configurations du système en une seule, ou en double boucle.

Dans une deuxième partie, nous avons cherché à explorer l'architecture du système sans rentrer trop dans les détails. Ainsi, nous avons étudié l'influence des bias du modulateur QPSK sur la multitude des régimes que peut acquérir le système. Cette étude a révélé l'importance de la condition d'interférence au point de repos du QPSK par rapport à la complexité du chaos généré. Une seconde étude de l'influence des délais du système nous a permis de comprendre que le délai le plus grand du système doit être dans la boucle dont le gain est le plus élevé, afin d'éviter la présence de fortes composantes périodiques dans le spectre. Et enfin, une troisième étude de l'influence des bandes passantes des filtres a permis de mettre en évidence la réduction de la bande passante du chaos généré lorsque les filtres limitant la dynamique du système sont différents.

La troisième partie de ce chapitre a été consacrée au système complet de cryptographie émetteur/récepteur. Nous avons présenté deux architectures différentes par leur aspect de boucle fermée ou de boucle ouverte du récepteur. Une étude de la sensibilité de la synchronisation en fonction du taux de couplage entre l'émetteur et le récepteur, nous a permis de privilégier l'architecture du récepteur en boucle ouverte, et donc d'opter pour un couplage total de la boucle à fort gain. Une autre étude (désaccords de paramètres) nous a montré que les délais du système sont particulièrement les paramètres les plus sensible pour réaliser l'opération de synchronisation. Ainsi, les applications à la cryptographie par chaos ont pu être validées à l'aide des simulations numériques présentées. Le chapitre suivant permettra ainsi de vérifier la validité de notre modèle théorique du générateur de chaos au travers des résultats expérimentaux.

# Chapitre 4

# Résultats expérimentaux

Dans les chapitres précédents, nous avons décrit et étudié numériquement le principe de fonctionnement du générateur de chaos à modulateur QPSK, et aussi le système complet de cryptage par chaos. Tous ces résultats ont été entrepris dans la perspective d'une réalisation expérimentale. Dans ce chapitre, nous allons mettre en œuvre le système proposé et exposer l'ensemble des résultats expérimentaux obtenus.

Ce chapitre est divisé en cinq parties, dont la première sera consacrée entièrement à la fonction non linéaire bidimensionnelle du système. Nous savons à présent que celle-ci est représentée par la fonction de transfert du modulateur QPSK, que nous pouvons considérer comme le cœur de cet oscillateur chaotique. Dans une première étape, nous allons d'abord décrire le dispositif expérimental, puis nous analyserons les résultats obtenus. Nous décrirons aussi les dispositifs de mesure des différents paramètres caractérisant le modulateur QPSK. Ensuite dans une seconde étape, nous effectuerons une étude comparative entre l'expérience et les simulations numériques. Cette étude nous permettra de valider le modèle analytique de la fonction non linéaire du système proposé.

La deuxième et la troisième partie de ce chapitre seront dédiées à la caractérisation de tous les composants de l'oscillateur chaotique. Comme le système est hybride (opto-électronique), certains composants seront caractérisés dans une chaîne de fonctionnement, alors que d'autres seront caractérisés séparément. Cette partie nous permettra de définir les paramètres de fonctionnement effectifs de notre oscillateur chaotique.

La quatrième partie aura pour objet la mise en œuvre expérimentale du générateur de chaos avec une architecture à une seule boucle. L'obtention des différents régimes dynamiques prévus par le modèle théorique sera vérifiée, et des comparaisons seront proposées entre des simulations des solutions et les régimes observés pratiquement. Cette partie nous permettra de valider le modèle dynamique théorique, ainsi que la capacité du générateur à produire des dynamiques chaotiques complexes.

Enfin, la dernière partie sera consacrée à l'étude et à l'analyse du système en architecture à double boucle. Un ensemble relativement exhaustif des dynamiques non linéaires générées seront explorées et analysées en vue d'une application à la cryptographie par chaos.

## 4.1 La non linéarité du système

Nous savons que les électrodes RF d'un modulateur permettent d'acheminer des signaux électriques de modulation, qui interagissent avec la lumière se propageant dans les guides optiques. Le modulateur agit donc comme une interface entre les signaux électriques et le signal lumineux. Pour un fonctionnement efficace, les électrodes dites à ondes progressives doivent présenter des pertes électriques faibles, et être adapté en impédance afin d'éviter les réflexions parasites, et aussi pour que la vitesse de l'onde micro-onde dans la ligne soit égale à la vitesse de l'onde lumineuse dans le guide optique (condition d'isochronisme). Ainsi, cette adaptation garantit un fonctionnement optimal sur une large bande de fréquences.

Une photographie du modulateur QPSK utilisé pour réaliser la fonction non linéaire du système est représentée sur la figure 4.1. Les électrodes RF de celui-ci ont des impédances caractéristiques de $35\,\Omega$.
Cette terminaison non rigoureusement adaptée a une conséquence pratique. C'est la diminution de la tension électro-optique effective, d'un facteur $35/(35+50) \simeq 0,411$ au lieu du facteur habituel $1/2$ de l'adaptation d'impédance (il faut donc appliquer un facteur correctif de $0,82$ aux amplitudes des tensions délivrées par les sources des modulations électro-optiques, ce qui correspond à $-1,7\,\mathrm{dB}$ de perte RF). Cette contrainte expérimentale et notamment la dépendance des tensions demi-ondes $V_{\pi RF1,2}$ de la fréquence, comme le montre le tableau 4.10, nous a incité à choisir une méthode de mesure statique pour évaluer la fonction non linéaire expérimentale.


Figure 4.1 – *Photographie du modulateur QPSK.*

Le principe de cette méthode consiste à appliquer deux signaux électriques alternatifs, dont l'évolution temporelle est rapide pour l'une des électrodes et lente pour l'autre. En d'autres termes, on effectue un balayage semblable à celui d'un écran cathodique. Nous avons donc réalisé un montage — figure 4.2 — permettant de mesurer cette non linéarité en fonction des valeurs des amplitudes des tensions variables appliquées aux électrodes RF. Comme on peut le voir sur ce montage, les différents appareils de commande et de contrôle sont reportés. Ce dispositif de mesure est composé, en plus du modulateur QPSK et des câbles de connexions, des éléments suivants :

- 1 diode laser pour alimenter en continue l'entrée optique du modulateur.
- 2 générateurs de fonctions pour délivrer les signaux lents et rapides.
- 1 alimentation fournissant 3 tensions continues indépendantes pour ajuster les valeurs des bias du modulateur. Pour des raisons de clarté du dispositif, celle-ci n'apparaît pas sur la figure.
- 1 photodiode DSC40S (sensibilité 18 mV/mW, à adapter sur 50 Ω, bande passante $> 10$ GHz), pour détecter l'intensité optique à la sortie du modulateur QPSK.
- 2 oscilloscopes, un pour l'enregistrement des variations de la puissance pour une période lente complète, l'autre en haute impédance pour contrôler l'amplitude des signaux lents et rapides appliqués au QPSK.
- 2 Tés BNC.

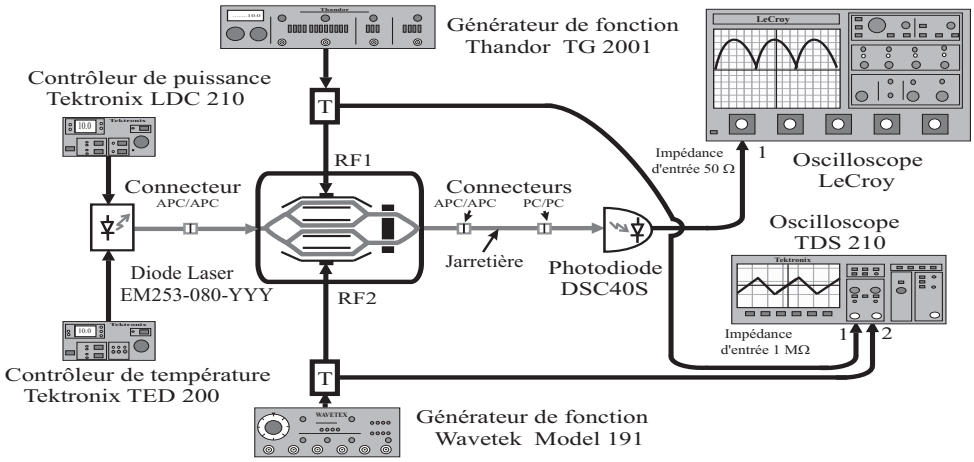



Figure 4.2 – *Dispositif de mesure de la fonction non linéaire.*

L'ensemble du montage peut se décrire de la manière suivante : la diode laser est monomode, sa longueur d'émission est 1550 nm. Elle est contrôlée et commandée par deux équipements différents. Le premier est un contrôleur de température qui maintient la source laser à une température constante, de l'ordre de 25 °C. Le second équipement assure à la diode un asservissement en courant où en puissance optique. Pour des raisons de bon fonctionnement et des contraintes de seuils des autres composants (le modulateur et le photodétecteur), nous avons fixé par ce dernier équipement un asservissement en courant de 146,7 mA, ce qui correspond à une puissance optique de 24,8 mW.

L'injection de la puissance optique dans le modulateur QPSK s'effectue par simple connexion FC APC/APC des fibres optiques, à maintien[1] de polarisation. À la sortie de celui-ci, la puissance optique convertie en tension est mesurée par un oscilloscope à impédance d'entrée 50 Ω (oscilloscope LeGroy), avec un pas d'échantillonnage de 5 ns/point.

[1]La diode laser utilisée émet naturellement une lumière polarisée linéairement, qui peut être maintenue grâce à un pigtail utilisant de la fibre à maintien de polarisation. Ce même type de fibre équipe bien sûr le pigtail d'entrée du modulateur QPSK, celui-ci étant sensible à la polarisation.

Aux électrodes RF du modulateur, deux tensions alternatives délivrées par 2 générateurs de fonctions différents sont appliquées. Pour chacune de ces tensions, une partie est prélevée, *via* un Té BNC, pour y être mesurée par un oscilloscope à impédance d'entrée 1 MΩ, réalisant ainsi un pont de diviseur de tension chargé (figure 4.3). Cette technique permet de contrôler l'amplitude des tensions réelles appliquées aux électrodes adaptées 35 Ω.

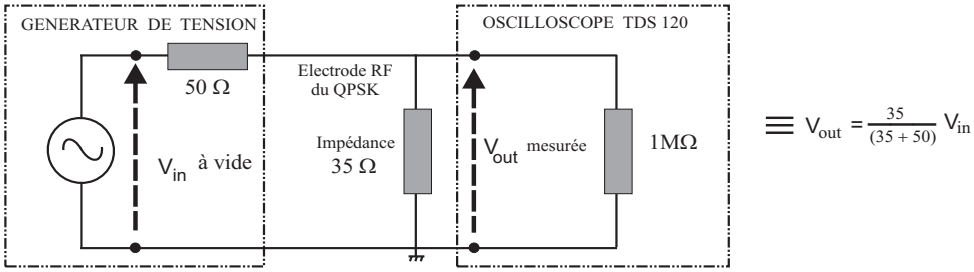



FIGURE 4.3 – *Schéma élémentaire d'un pont diviseur de tension.*

Ces tensions ont les caractéristiques suivantes :

- **Sur l'électrode RF1** est appliquée une tension alternative triangulaire $v_1(t)$, de fréquence $f_1 = 1$ MHz. Cette tension est fournie par un GBF capable de délivrer des amplitudes de tension allant au maximum à 25 $V_{pp}$ à vide. L'amplitude maximum mesurée aux bornes de l'électrode est de l'ordre de 8,7 $V_{pp}$ ; cette chute de tension s'explique par l'impédance 35 Ω de l'électrode RF du modulateur.
- **Sur l'électrode RF2** est appliquée une tension alternative triangulaire $v_2(t)$, de fréquence $f_2 = 10$ kHz. Pour un maximum de tension fournie de 30 $V_{pp}$, l'amplitude de la tension disponible sur l'électrode est de 12,2 $V_{pp}$ .

Comme les signaux appliqués aux électrodes sont périodiques, il est judicieux de représenter le balayage de la non linéarité par rapport à une période de chacun de ces signaux. À titre d'illustration, la figure 4.4 montre les évolutions temporelles périodiques des signaux $v_1(t)$ et $v_2(t)$ mesurés expérimentalement, ainsi que celle de $P_s(t)$. Ce dernier signal représente la puissance optique à la sortie du modulateur QPSK, mesurée indirectement par l'oscilloscope LeCroy. L'acquisition des données depuis l'oscilloscope vers l'ordinateur s'est effectuée à l'aide d'une interface LabVIEW conçue spécialement.

La figure 4.5 montre l'allure de la fonction non linéaire bidimensionnelle obtenue expérimentalement, en fonction des amplitudes des signaux appliqués aux électrodes RF du modulateur QPSK. Nous rappelons que pour obtenir une dynamique chaotique, une condition nécessaire sur la non linéarité est de présenter un extrémum dans l'intervalle de variation des variables d'entrées. Cette condition nous paraît bien remplie, d'après la figure 4.5a, par la fonction de transfert du modulateur QPSK.

La vue de dessus — figure 4.5b — révèle que la périodicité 2D de la fonction non linéaire n'est pas atteinte. Pour pouvoir observer par exemple 2 minima successifs de la puis-

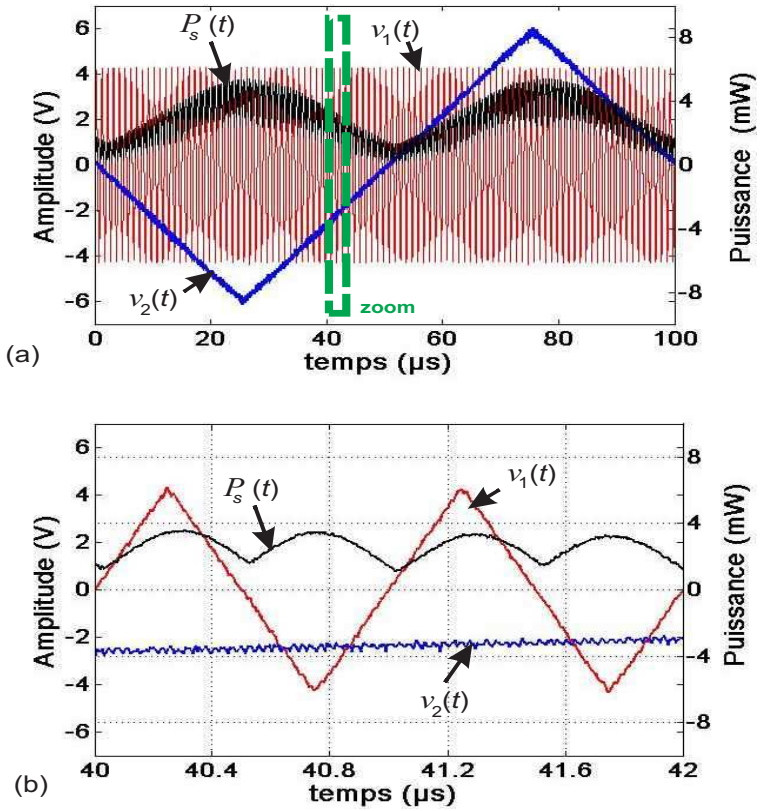



FIGURE 4.4 – *Évolution temporelle des tensions appliquées aux électrodes RF et de la puissance optique à la sortie du modulateur QPSK.* (*b*) *est le zoom de la zone en pointillés de* (*a*).

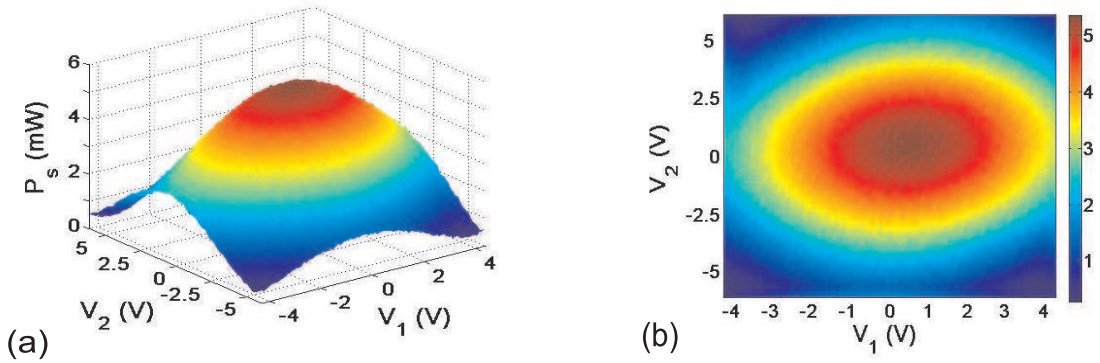



FIGURE 4.5 – *Allure de la fonction non linéaire bidimensionnelle expérimentale.* $\phi_1 = 5,3$ ; $\phi_2 = 4,8$ ; $\phi_3 = 3,0$ ; (*a*) *une vue en* 3D. (*b*) *une vue de dessus.*

puissance optique, il faudrait appliquer 2 fois $V_{\pi RF}$ ; c'est une tâche que les générateurs de fonction utilisés ne peuvent assurer (ils sont aux limites d'amplitudes de ce qu'ils peuvent fournir). La conséquence de cette contrainte physique est de ne pas pouvoir mesurer directement le $V_\pi$ par sa définition, c'est-à-dire l'amplitude de tension qui fait passer la condition d'interférence de constructif à destructif.

### 4.1.1 Mesure des caractéristiques du modulateur QPSK

À présent, nous allons décrire les méthodes de mesure expérimentales des paramètres caractérisant le modulateur QPSK. Selon le paramètre à mesurer, nous donnerons les détails du principe de la mesure ou directement le résultat obtenu. L'ensemble des valeurs numériques est donné sous forme d'un tableau récapitulatif en fin de cette sous-section.

**Mesure des paramètres $V_{\pi DC1,\,2,\,3}$**

Pratiquement, les tensions demi-ondes statiques ($V_{\pi DC1,\,2,\,3}$) du modulateur sont les paramètres les plus simples à mesurer. Le dispositif expérimental permettant de les estimer, dans les mêmes conditions de fonctionnement que l'expérience précédente, est schématisé sur la figure 4.6.

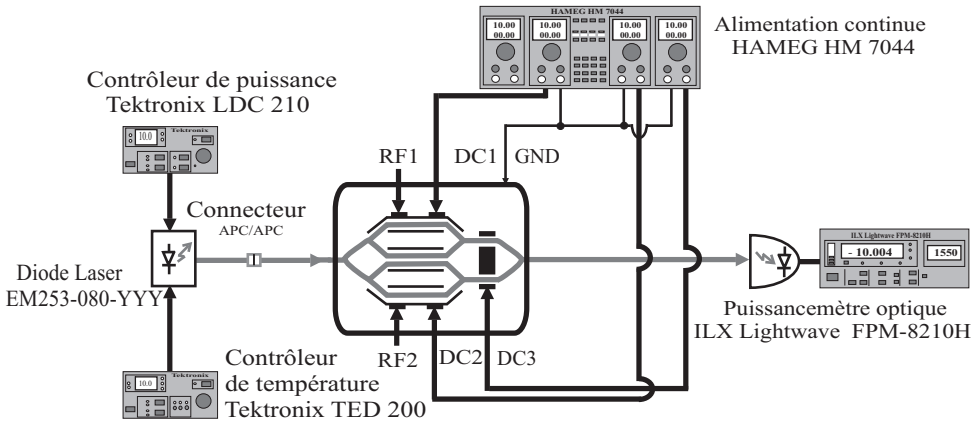



Figure 4.6 – *Dispositif de mesure des paramètres $V_{\pi DC1,\,2,\,3}$ du modulateur QPSK.*

Le principe de la méthode consiste à calculer la différence entre les 2 tensions, du même bias, qui correspondent à maximum, puis à un minimum de puissance optique à la sortie du modulateur. Pour retrouver ces tensions, il existe différentes manières de procéder, parmi lesquelles celle qui s'effectue en statique. Son principe consiste à tracer la variation de la puissance optique en fonction de la tension d'un seul bias. Si ce n'est de rester pendant la mesure constant, cette méthode n'exige aucune condition particulière sur les 2 autres bias. Un exemple de résultats obtenus par ce procédé est illustré sur la figure 4.7, et ainsi, la détermination des paramètres $V_{\pi DC1,\,2,\,3}$ peut se faire sans grandes difficultés.

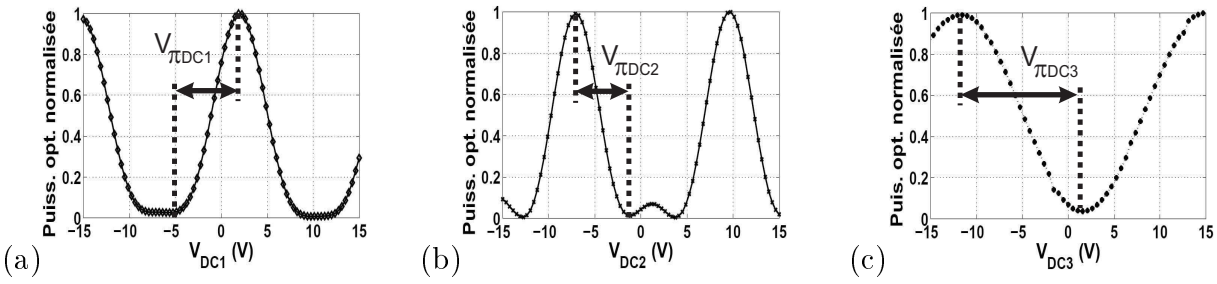



FIGURE 4.7 – *Mesure en statique des paramètres $V_{\pi DC1,2,3}$ du modulateur QPSK.*

**Mesure des paramètres $V_{\pi RF1,2}$**

En général, le principe de la mesure d'une tension demi-onde dynamique consiste à appliquer à l'entrée RF d'un modulateur un signal alternatif, de fréquence donnée et d'amplitude suffisante, qui permet d'observer en sortie une demi-période de la cannelure. Le modulateurs QPSK se caractérise par 2 tensions demi-ondes dynamiques différentes ($V_{\pi RF1}$ et $V_{\pi RF2}$). La mesure du $V_{\pi RF2}$ par exemple s'effectue dans des conditions d'extinction de l'interféromètre $MZ_1$, qui s'obtient par un réglage minutieux du bias $V_{DC1}$. Cette extinction peut être vérifiée par la non variation de la puissance optique mesurée, lorsqu'une action sur le bias $V_{DC3}$ est opérée. En plus de cette condition sur le $MZ_1$, nous avons connecté à l'entrée de l'électrode RF1 un bouchon de 50 Ω. Cette précaution a pour but d'éviter un possible dépôt de charges électrostatiques sur cette électrode. La puissance optique en sortie du QPSK dépend alors essentiellement de la tension sur RF2.

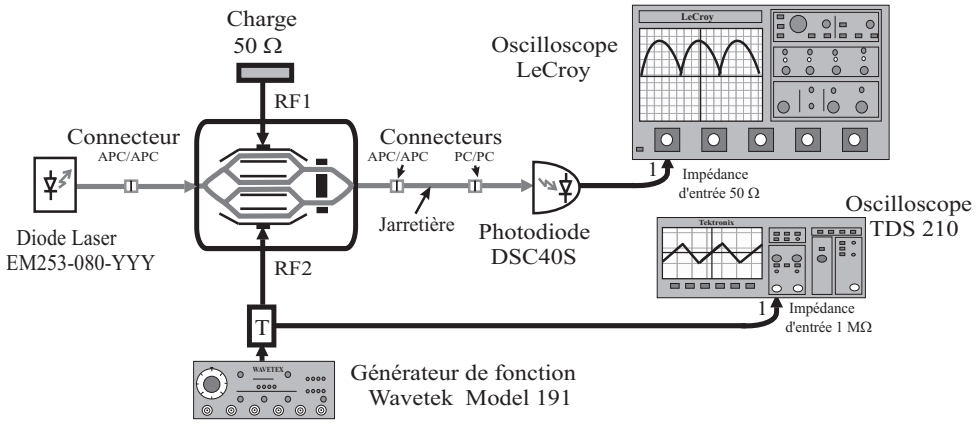



FIGURE 4.8 – *Dispositif de mesure du paramètre $V_{\pi RF2}$ du modulateur QPSK.*

Après ces étapes préparatoires, nous avons mesuré le $V_{\pi RF2}$ correspondant à 4 fréquences de modulation différentes (1 k, 50 k, 1 M et 1 GHz). Pour réaliser la quatrième mesure, malheureusement des contraintes expérimentales se sont imposées. En effet, le générateur de fonction (voir la figure 4.8) et l'oscilloscope à impédance d'entrée 1 MΩ sont limités en fréquences, respectivement à 20 MHz et 60 MHz maximum. À cause de ces

limitations, nous les avons changé respectivement par un Agilent E4420B (fréquence ajustable : 250 kHz–2 GHz), et une entrée électrique de l'oscilloscope LeCroy qui a nécessité une photodiode (une Miteq), pour la conversion du signal optique en électrique.

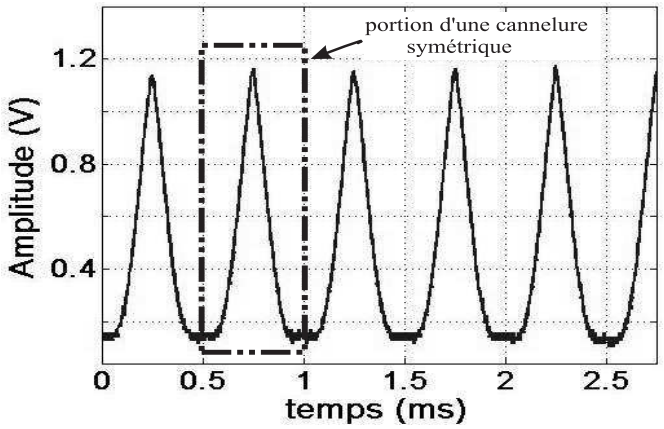



Figure 4.9 – *Allure d'une cannelure symétrique sur l'oscilloscope LeCroy.*

À titre d'exemple, la procédure de la mesure du $V_{\pi RF2}$ à la première fréquence 1 kHz est la suivante : on applique un signal triangulaire sur l'électrode RF2, puis on augmente son amplitude jusqu'à l'obtention d'une demi-cannelure sur l'oscilloscope LeCroy (un exemple de cannelure symétrique est représenté sur la figure 4.9). Ainsi, le paramètre $V_{\pi RF2}$ est déterminé par la mesure, sur l'oscilloscope à impédance d'entrée 1 M Ω, de l'amplitude de la tension triangulaire appliquée.

| Paramètre mesuré | | Valeur (V) |
|---|---|---|
| $V_{\pi DC1}$ | | 7,40 |
| $V_{\pi DC2}$ | | 7,14 |
| $V_{\pi DC3}$ | | 14,24 |
| $V_{\pi RF1}$ | @ 1 kHz | 2,81 |
| | @ 50 kHz | 4,27 |
| | @ 1 MHz | 5,84 |
| | @ 1 GHz | 6,31 |
| $V_{\pi RF2}$ | @ 1 kHz | 2,50 |
| | @ 50 kHz | 4,18 |
| | @ 1 MHz | 6,08 |
| | @ 1 GHz | 6,42 |

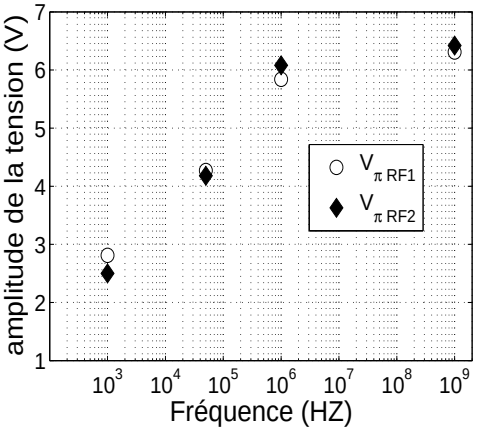



Figure 4.10 – *Tableau récapitulatif des paramètres du modulateur QPSK.*
*(à droite) Variation des $V_{\pi RF1,2}$ en fonction de la fréquence de modulation.*

Les valeurs mesurées jusqu'à présent de l'ensemble des paramètres du modulateur QPSK sont données au tableau 4.10. Ces valeurs sont globalement très proches de celles données par le constructeur du composant. Nous constatons d'après ces mesures que les $V_{\pi RF1,2}$ dépendent de la fréquence de modulation, plus particulièrement lorsque celle-ci est basse, comme le montre la figure de droite. Heureusement, lors d'une mesure par l'analyseur de réseau, que nous allons présenter au paragraphe suivant, ces tensions demi-ondes ne varient pas significativement dès qu'on s'éloigne de cette gamme de basses fréquences.

### Mesure des bandes passantes du modulateur QPSK

La figure 4.11 montre le dispositif expérimental utilisé pour la mesure des bandes passantes du modulateur QPSK. Une conversion optique-électrique est nécessaire dans ce montage car le port d'entrée de l'analyseur de réseau est électrique, alors que la sortie du QPSK est optique. Cette conversion est réalisée par une photodiode de type Miteq, dont le choix n'est pas arbitraire. En effet, cette photodiode est celle qui sera utilisée par la suite dans la boucle de rétroaction, et donc sa bande passante sera aussi incluse dans la mesure.

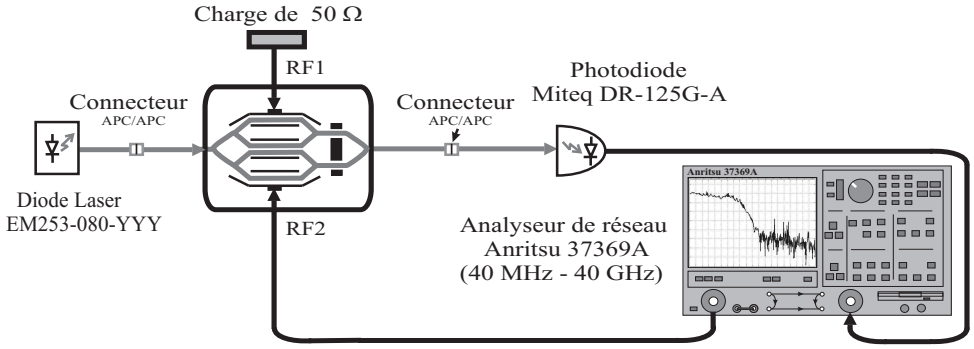



Figure 4.11 – *Dispositif de mesure des bandes passantes du modulateur QPSK.*

Après avoir pris soin de bien calibrer l'analyseur de réseau, et les réglages appropriés à l'extinction de l'un des MZ simples, les résultats que nous avons obtenus sont représentés sur la figure 4.12. D'après ces résultats, on remarque que les courbes ressemblent au diagramme de Bode d'un filtre passe bas, où la fréquence de coupure haute est mesurée pour chacun des 2 interféromètres MZ−photodétecteur à environ 13 GHz.

Cependant avec le dispositif de la figure 4.11, nous n'avons pas pu mesurer la fréquence de coupure basse de l'ensemble modulateur – photodétecteur, car l'analyseur de réseau utilisé est limité en fréquence inférieure à 40 MHz. Cette limite est loin de celle du photodétecteur Miteq, qui est mesurée en section 4.3.3.

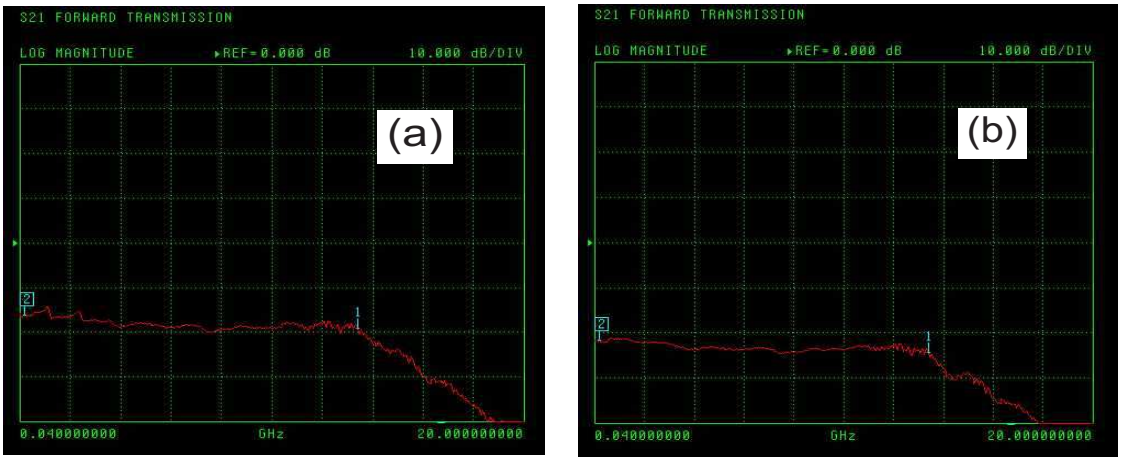



Figure 4.12 – *Mesure de bandes passantes du modulateur QPSK et photodétecteurs (a) Interféromètre $MZ_1$ et photodiode (b) Interféromètre $MZ_2$ et photodiode.*

**Mesure des pertes optiques $\gamma_0$**

Pratiquement, la mesure des pertes optiques du modulateur QPSK est très simple. Pour les estimer, nous avons utilisé le montage de la figure 4.6, en procédant de la manière suivante : à travers les réglages des trois bias du modulateur, on cherche une condition d'interférence permettant une transmission maximale de la puissance optique à la sortie du QPSK. Ensuite, cette puissance optique de sortie est comparée par rapport à celle en entrée du modulateur. Ainsi, les pertes optiques $\gamma_0$ estimées expérimentalement sont de l'ordre de $-7,2$ dB ; cette valeur est proche de celle indiquée par le fabriquant du composant ($-6,7$ dB).

Nous venons de décrire les méthodes de mesure et l'évaluation des différents paramètres du modulateur QPSK. Nous allons maintenant vérifier que lorsqu'on injecte ces paramètres dans le modèle théorique de la fonction non linéaire, étudié au chapitre 2, cette fonction correspond bien aux conditions expérimentales.

### 4.1.2 Comparaison des non linéarités expérimentale/théorique

Dans ce qui suit, la comparaison entre les fonctions non linéaires expérimentale et théorique se fera en deux parties. Nous exposerons dans la première certaines précautions à prendre en compte, avant d'entamer la comparaison proprement dite dans la seconde partie. Ces précautions sont relatives au point de fonctionnement du QPSK, où une procédure de calibrage est nécessaire.

**a. Mesures de précaution :**

Nous rappelons ici l'expression analytique de la fonction non linéaire, donnée par (2.15).

$$f_{NL}[v_a, v_b] = \frac{1}{4}\Big\{ \cos(\psi_3)\Big[\cos(\psi_3) + 2\cos\big(\psi_1 + \psi_2\big)\cos\big(\psi_2 + \psi_3 - \psi_1\big)\Big] + \cos^2\big(\psi_2 + \psi_3 - \psi_1\big)\Big\} \tag{4.1}$$

avec :

$$\psi_1 = \frac{\varphi_1(t)}{2}; \qquad \psi_2 = \frac{\varphi_2(t)}{2}; \qquad \psi_3 = \frac{\phi_3}{2}; \tag{4.2}$$

et :

$$\begin{cases} \varphi_{1,2}(t) = \pi \cdot \dfrac{v_{a,b}(t)}{V_{\pi RF_{1,2}}} + \phi_{1,2} & \text{(4.3a)} \\ \phi_m = \pi \cdot \dfrac{V_{DC_m}}{V_{\pi DC_m}}; \qquad (m = 1,\ 2,\ 3) & \text{(4.3b)} \end{cases}$$

D'après la relation (4.3b), les déphasages statiques nuls sont induits par des tensions de bias nulles, ce qui n'est pas forcément le cas en expérience. Les tolérances de fabrication du modulateur et la légère dérive de son point de fonctionnement au cours du temps sont autant de raisons, parmi d'autres, qui expliquent cette différence.

Pour remédier à ce problème, il suffit d'effectuer un calibrage des tensions $V_{DC_m}$ avant de les injecter dans le modèle (4.1). Le calibrage dans ce contexte consiste à ajouter des offsets $\phi_{m0}$ aux déphasages théoriques (4.2). Ainsi, on obtient les relations suivantes :

$$\psi_1 = \frac{\varphi_1(t)}{2} + \phi_{10}; \qquad \psi_2 = \frac{\varphi_2(t)}{2} + \phi_{20}; \qquad \psi_3 = \frac{\phi_3}{2} + \phi_{30}; \tag{4.4}$$

La détermination de ces offsets peut se faire de différentes manières, parmi lesquelles on peut citer l'ajustement des paramètres par la méthode des moindres carrés, bien connue dans la littérature, ou encore celle que nous avons pratiquement utilisée : faire coïncider les extrema des non linéarités expérimentale et théorique. Le principe de cette dernière méthode se base essentiellement sur 2 critères :

- avoir les mêmes contrastes optiques.
- les déphasages statiques, aboutissant à un maximum de puissance optique en expérience, correspondent à ceux d'un maximum de la non linéarité (4.1).

**Le contraste optique :**

Le contraste est le rapport entre la variation d'une fonction et sa valeur moyenne, indiquant la capacité d'un système optique à faire ressortir ces variations par rapport au fond continu [117]. Ramené au modulateur QPSK, celui-ci est défini par :

$$c_m = \frac{P_{max} - P_{min}}{P_{max} + P_{min}} \tag{4.5}$$

où $P_{max}$ et $P_{min}$ sont respectivement les puissances optiques maximale et minimale en sortie du QPSK. Celles-ci dépendent en général des trois tensions de bias du modulateur,

comme le montre l'exemple[2] de la figure 4.13a, mais plus particulièrement de la tension $V_{DC3}$ qui agit sur le contraste de la figure d'interférences.

Lorsque le critère de même contraste optique est respecté, un exemple de courbes expérimentale et théorique est représenté sur la figure 4.13b. On peut remarquer sur cette figure qu'il y a une sorte de décalage entre les deux courbes, d'où la nécessité d'effectuer une calibration.

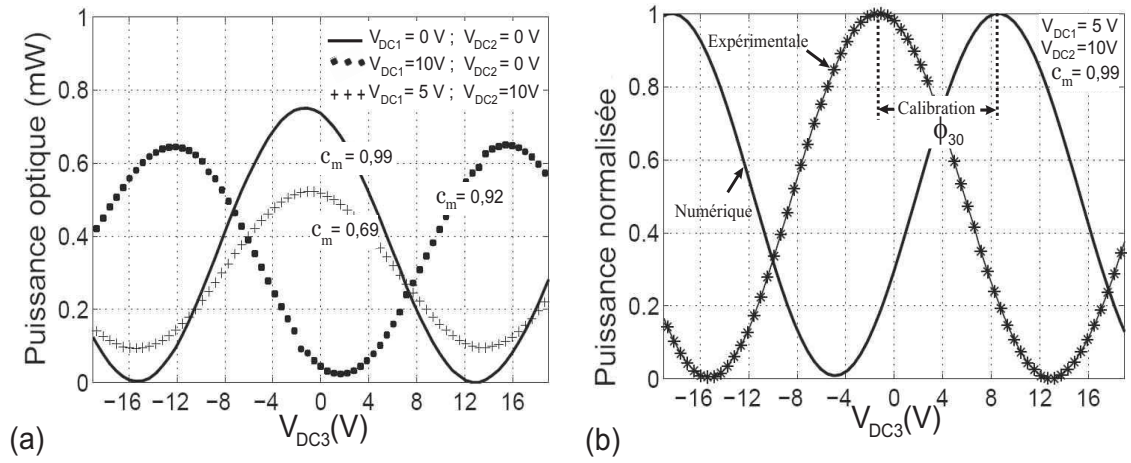



FIGURE 4.13 – *Contraste optique en fonction des tensions de bias du modulateur QPSK. (a) Mesures expérimentales de différents contrastes. (b) Comparaison d'interférences de même contraste optique.*

### Recherche d'extrema de la fonction non linéaire

L'intérêt de localiser les points critiques — points max, min et col — de $f_{NL}[v_a, v_b]$ est double. Le premier est de nous permettre d'identifier de manière analytique le point de fonctionnement du modulateur QPSK, et le second est d'établir une correspondance théorie/expérimentale du modèle associé. Les développements mathématiques détaillés pour la recherche de ces extrema sont disponibles en annexe, et nous soulignons seulement ici, que ces points critiques obéissent aux conditions de dérivées partielles premières nulles, autrement dit, ils vérifient les relations suivantes :

$$\begin{cases} \dfrac{\partial f_{NL}}{\partial v_a}(v_a, v_b) = \dfrac{\partial f_{NL}}{\partial \psi_1}(\psi_1, \psi_2) \cdot \dfrac{\partial \psi_1}{\partial v_a}(v_a) = 0 & \text{(4.6a)} \\ \dfrac{\partial f_{NL}}{\partial v_b}(v_a, v_b) = \dfrac{\partial f_{NL}}{\partial \psi_2}(\psi_1, \psi_2) \cdot \dfrac{\partial \psi_2}{\partial v_b}(v_b) = 0 & \text{(4.6b)} \end{cases}$$

Il vient après calcul de (4.6a) et (4.6b), que ces extrema sont les solutions du système d'équations suivant :

[2]Le dispositif expérimental utilisé est donné sur la figure 4.6.

$$\begin{cases} \sin(2\psi_2 - 2\psi_1 + 2\psi_3) - 2\cos(\psi_3)\sin(2\psi_1 - \psi_3) = 0 & \text{(4.7a)} \\ \sin(2\psi_2 - 2\psi_1 + 2\psi_3) + 2\cos(\psi_3)\sin(2\psi_2 + \psi_3) = 0 & \text{(4.7b)} \end{cases}$$

Suivant la procédure décrite aussi en annexe, le type de point critique est identifié ensuite numériquement, comme le montre l'exemple déjà vu de la figure 2.8b page 55. Ainsi, après la localisation numérique d'un maximum de $f_{NL}[v_a, v_b]$ (pour le cas étudier ici, les déphasages sont donnés au tableau 4.1), la suite du calibrage consiste tout simplement à faire correspondre les déphasages induisant ce maximum, avec ceux qui permettent d'avoir un maximum de puissance optique en expérience.

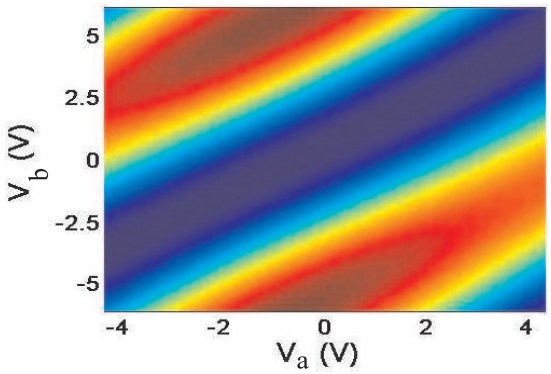
| Déphasages expérimentaux (rad) | Déphasages théoriques (rad) | Calibrage (rad) |
|---|---|---|
| $\begin{pmatrix} \phi_1 \\ \phi_2 \\ \phi_3 \end{pmatrix} = \begin{pmatrix} 5,3 \\ 4,8 \\ -0,2 \end{pmatrix}$ | $\begin{pmatrix} \phi_1 + \phi_{10} \\ \phi_2 + \phi_{20} \\ \phi_3 + \phi_{30} \end{pmatrix} = \begin{pmatrix} 0,1 \\ 6,2 \\ 1,9 \end{pmatrix}$ | $\begin{pmatrix} \phi_{10} \\ \phi_{20} \\ \phi_{30} \end{pmatrix} = \begin{pmatrix} -5,2 \\ 1,4 \\ 2,1 \end{pmatrix}$ |

Table 4.1 – *Calibration des déphasages statiques par les tensions de bias.*

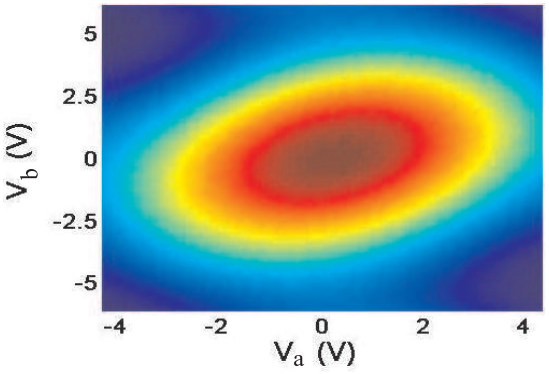
### b. Comparaison des non linéarités expérimentale et théorique

La figure 4.14a illustre la fonction non linéaire théorique sans aucun calibrage (les paramètres expérimentaux du tableau 4.1 sont injectés directement dans le modèle (4.1)). D'après cette figure, le résultat obtenu est très différent de celui de l'expérience (figure 4.14c). Par contre, lorsque le calibrage est effectué selon la procédure décrite précédemment, plusieurs points de similitude sont alors identifiés (figures 4.14b et 4.14c), parmi lesquels au moins deux exemples peuvent être relevés : présence d'un extrémum clairement identifiable, satisfaisant ainsi la condition nécessaire sur la non linéarité pour permettre de générer une dynamique chaotique, et une cannelure incomplète dont l'origine a déjà été évoqué. Globalement, il y a donc une bonne concordance entre la théorie et l'expérience, ce qui permet de valider le modèle théorique de la non linéaire proposé.

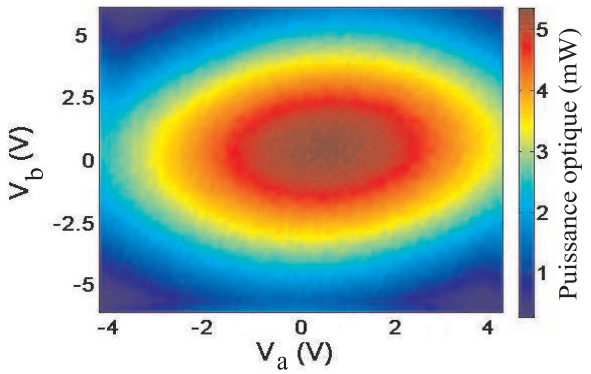
Néanmoins, comme aucun modèle théorique ne décrit avec une exactitude absolue un phénomène physique, on constate que la correspondance expérience−théorie présente aussi quelques points de différence. À titre d'exemple, la forme théorique de la non linéarité — figure 4.14b — est légèrement inclinée vers le bas comparée à celle obtenue expérimentalement (figure 4.14c). Cet exemple dont l'origine exacte n'a pas été identifié nécessite d'autres tests et d'autres études. On peut supposer que la cause de cette différence est liée aux erreurs d'estimation des nombreux paramètres du QPSK, dont il est tout à fait possible que lorsqu'on remonte au modèle théorique global, ces erreurs peuvent s'accumuler.




(a) Simulation : sans calibrage




(b) Simulation : avec calibrage




(c) Expérimentale

Figure 4.14 – *Comparaison des fonctions non linéaires théorique et expérimentale*

## 4.2 Caractérisation des composants

### 4.2.1 La source laser

La source laser utilisée est une diode laser de type DFB[3]. Pour donner une brève description de ce type de laser, nous pouvons informer qu'il possède un élément de rétroaction distribué (un réseau périodique) qui est gravé directement sur sa région active. Le rôle de ce réseau est de sélectionner un seul mode longitudinal de propagation (laser monomode). Grâce à leur stabilité en longueur d'onde, leur stabilité en puissance et leur fiabilité, ces lasers sont les plus répandus dans les télécommunications optiques.

Cette diode laser est un produit de la société EM4, Inc portant la référence EM253-080-YYY. D'après les indications du constructeur, le numéro (080) signifie que la puissance maximale émise par cette diode est de 80 mW. L'étiquetage (YYY) indique que la longueur d'onde d'émission centrale peut être sélectionnée, avant la fabrication, dans la fenêtre 1515 – 1600 nm. Cette longueur d'onde peut être contrôlée soit par le courant d'injection, soit par la température.

[3]DFB signifie Distributed Feedback.

En effet, le laser est connecté à un dispositif d'asservissement en température et à un autre en courant. Leur rôle est de garantir une très bonne stabilité de la longueur centrale d'émission. En changeant le courant d'injection dans le semi-conducteur (InGaAsP/InP), celà revient à changer le nombre de porteurs dans la cavité laser, ce qui modifie l'indice de réfraction. De même, en changeant la température de la jonction, l'indice de réfraction est modifié. Par conséquent, ces modifications entraînent un changement d'un point de vue de la longueur du parcours optique, ce qui induit un glissement[4] de la longueur d'onde émise d'environ $0,1$ nm/ °C, et de $2,8$ pm/mA.

À la température de fonctionnement arbitraire de 24,8 °C, la figure 4.15 montre la courbe de la puissance de sortie du laser en fonction du courant d'injection. Nous avons relevé sur cette caractéristique une efficacité de 0,27 mW/mA, et un courant seuil de 55 mA.

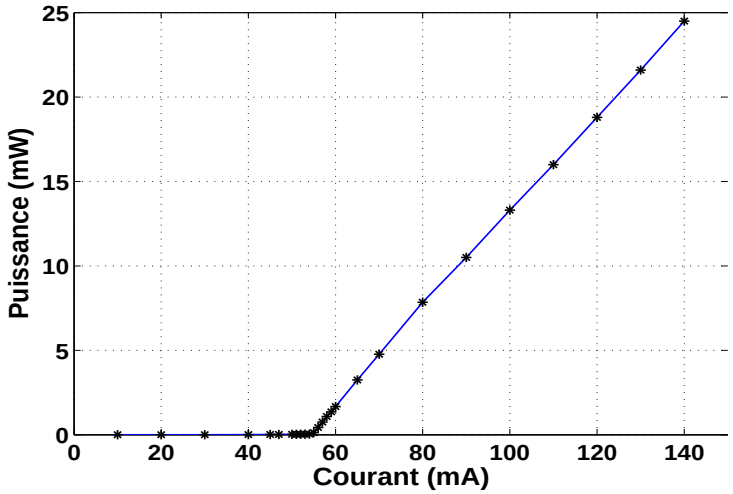



Figure 4.15 – *Puissance de sortie de la diode laser en fonction du courant d'injection.*

### 4.2.2 La chaîne d'amplification et de filtrage RF

En plus de deux coupleurs optiques (50/50), chaque boucle de rétroaction du système est formée par une chaîne d'amplification et de filtrage RF ; elle est composée de deux éléments principaux : un photodétecteur muni d'un amplificateur, et un amplificateur RF large bande.

**Photodétecteurs :**

Nous avons utilisé dans les deux boucles de rétroaction 2 photodiodes pré–amplifiées de même type (Miteq DR-125G-A), avec un gain de conversion de l'ordre de $2\,\mathrm{V/mW}$. La valeur typique fournie par le fabriquant (lorsque celles-ci sont chargées sur $50\,\Omega$) est de $1,9\,\mathrm{V/mW}$. Leur bande passante a été déjà donnée — figure 4.12 — en faisant entrer en jeu le modulateur QPSK.

[4]Les mesures sont effectuées à l'aide d'un analyseur de spectre optique Anritsu MS 9710B.

**Amplificateurs RF :**

Pour permettre d'atteindre des gains suffisants et des amplitudes de modulation d'au moins de l'ordre des $V_{\pi RF}$ afin de générer des signaux chaotiques complexes, 2 amplificateurs de puissance RF sont utilisés :

- Le premier est un SHF 2100CPS, qui se caractérise par un gain de 18 dB (amplification x8) capable de délivrer près de 22 dBm (environ 8V crête à crête). Cet amplificateur est inséré dans la boucle (A) du système, sa bande passante analogique – figure 4.16a – est d'environ 25 GHz, et sa fréquence de coupure basse (mesurée à l'aide du dispositif de la figure 4.21) vaut environ 50 kHz.

- Le second amplificateur est un SHF 100CP, utilisé dans la boucle (B) de l'oscillateur. Son gain vaut aussi 18 dB, mais sa puissance de saturation est de 26dBm (équivalent à 12,6V crête à crête). Sa bande passante — figure 4.16b — est d'environ 26 GHz. La fréquence de coupure basse (déterminée aussi par le dispositif de la figure 4.21) est d'environ 30 kHz.

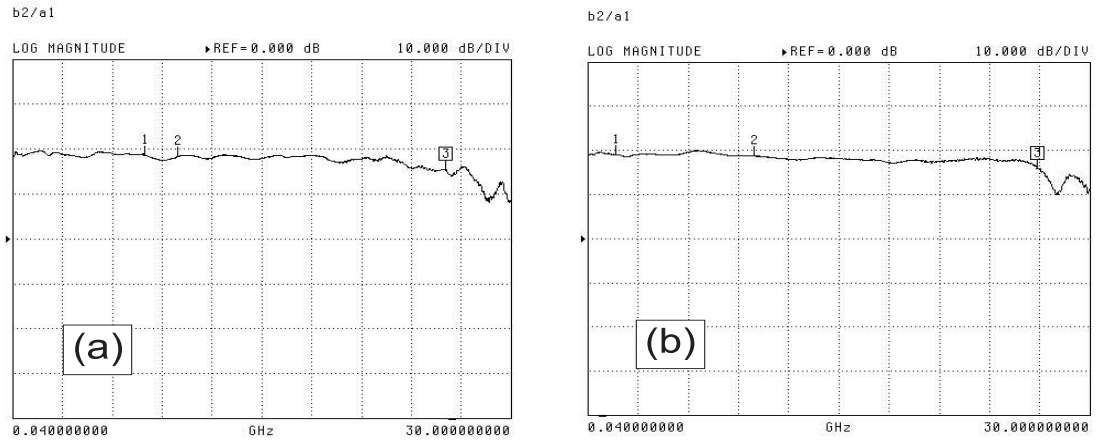



FIGURE 4.16 – *Paramètres $S_{21}$ des amplificateurs de puissance RF.* (*a*) *Amplificateur* SHF 2100CPS. (*b*) *Amplificateur* SHF 100CP.

Par rapport à la bande passante de notre générateur de chaos, nous allons voir par la suite que pratiquement, les fréquences de coupure basses sont celles des amplificateurs RF, et les fréquences hautes sont celles des photodétecteurs.

## 4.3 Mesures en boucle ouverte

Le nombre d'éléments formant l'ensemble expérimental de l'oscillateur chaotique étant assez important, il n'est pas intéressant de mesurer les caractéristiques de chacun, puis de calculer le résultat pour remonter au modèle global théorique de l'oscillateur. Dans ces

conditions, les erreurs de mesure sur chaque élément s'accumuleraient, et deviendraient trop importantes. Nous allons donc mesurer certains paramètres du système — les retards, les gains de boucle et les bandes passantes — en considérant cette fois-ci toute la chaîne des composants électro-optiques et optoélectroniques formant la boucle de rétroaction.

### 4.3.1 Les retards temporels

Le dispositif expérimental de la mesure des retards temporels est représenté sur la figure 4.17. Nous avons pris soin à ce que la mesure s'effectue dans des conditions optimales en terme de précision, car comme nous l'avons vu dans la partie théorique, la synchronisation émetteur−récepteur en dépend fortement. Expérimentalement, le retard temporel est le temps de parcours par le signal de l'ensemble des composants électro-optiques et optoélectroniques constituant la boucle de rétroaction.

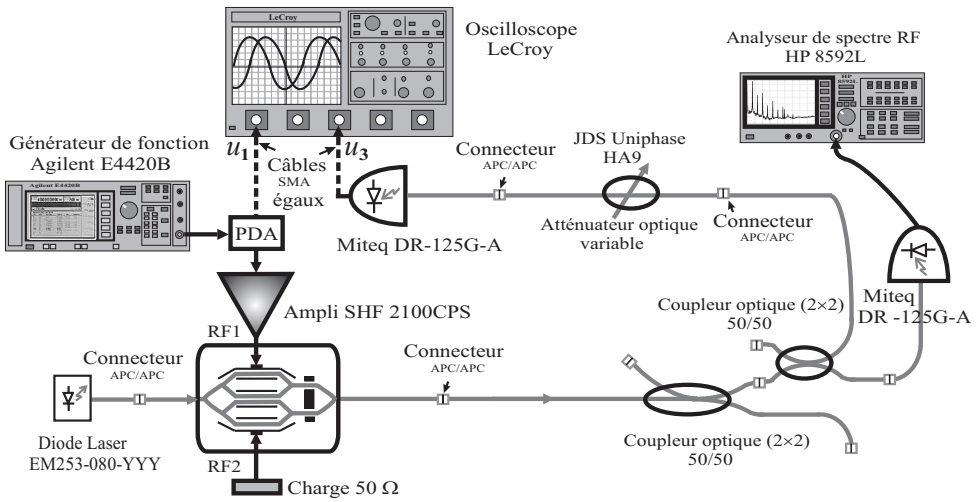



FIGURE 4.17 – *Dispositif de mesure des retards temporels.*

Le principe de la mesure consiste à injecter, dans une boucle ouverte de rétroaction, un signal électrique sinusoïdal de fréquence ajustable. Comme on peut le voir sur la figure 4.17, ce signal est introduit à travers l'une des deux sorties d'un coupleur RF[5] (1 entrée / 2 sorties). L'autre sortie du coupleur permet d'avoir le signal de référence $u_1(t)$, que l'on peut visualiser sur l'oscilloscope LeCroy. Ce signal est ensuite comparé au signal électrique retardé $u_3(t)$ issu du photodétecteur.

Les 2 signaux (référence + retardé) sont donc observables simultanément sur l'oscilloscope : $u_3(t) =\propto u_1(t-T)$ ; $T$ étant le retard temporel. La suite consiste à augmenter la fréquence du signal de référence jusqu'à ce que les 2 signaux soient en phase : $\Delta\varphi = \pi = 2\pi T/T_0$ ; avec $(T = T_0/2)$ la demi-période de la sinusoïde. À cette condition, on note la fréquence correspondante que l'on peut, soit lire directement sur l'afficheur du générateur de fonction, soit obtenir de l'analyseur de spectre RF. Mais afin d'obtenir

[5]Représenté sur la figure 4.17 par PDA (Power Divider de marque Anritsu).

une bonne précision de la mesure, on continue à augmenter la fréquence du signal de référence, tout en notant le nombre de fois " $\kappa$ " que les 2 signaux sont encore en phase : $\Delta\varphi = 2\pi\kappa = 2\pi T\Delta f$ ; avec $\Delta f$ est l'écart entre les fréquences correspondant au premier et au dernier cas des 2 signaux en phase. Finalement, le délai $T$ de la boucle est calculé par le rapport suivant :

$$T = \frac{\kappa}{\Delta f} \tag{4.8}$$

Ainsi, dans des conditions d'extinction de l'interféromètre MZ simple de la boucle non concernée, nous avons mesuré ($\pm\,0{,}1$ ns ; $\kappa = 10$ fois) les retards temporels suivants :

$$T_a = 61,3 \text{ ns} \quad ; \quad T_b = 60,4 \text{ ns}$$

### 4.3.2 Les gains de boucles

La figure 4.18 montre le dispositif expérimental utilisé pour la mesure du gain, lorsqu'on met bout à bout les composants coupleurs optiques, photodétecteur et amplificateur RF relatifs à la boucle (A) du système. La source laser utilisée est un laser DFB intégré, avec un modulateur à électro-absorbant (EA). Ce modulateur est commandé par une tension $V_{EA}$ fournie par une alimentation continue.

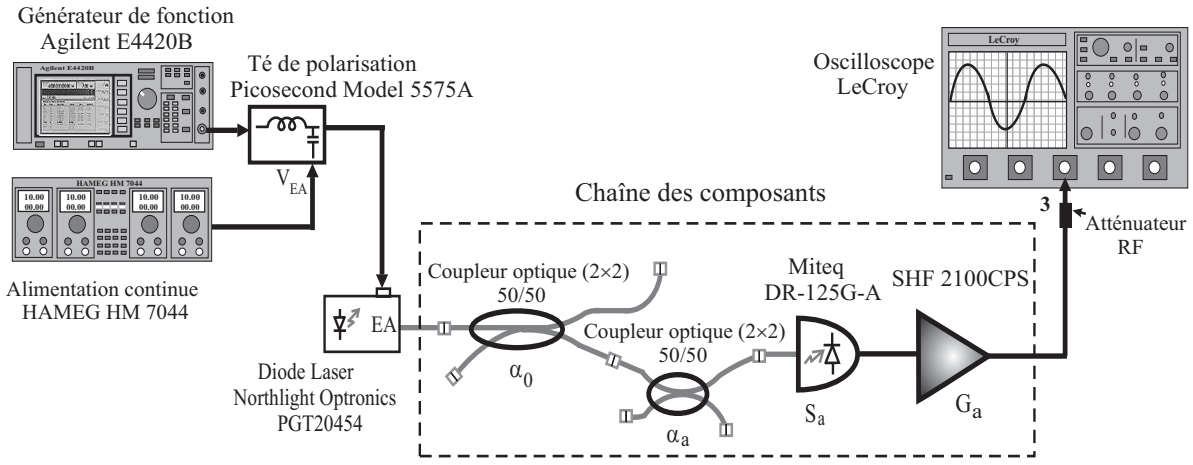



FIGURE 4.18 – *Dispositif de mesure du gain de la boucle (A).*

Le principe de la mesure consiste à appliquer un signal sinusoïdal, à travers le modulateur EA, pour moduler l'intensité lumineuse guidée à l'entrée de la chaîne. En sortie de cette dernière, l'oscilloscope LeCroy permet de visualiser le signal ainsi modulé. La valeur du gain, dont les expressions théoriques[6] relatives à chaque boucle de rétroaction sont rappelées en (4.9), est obtenue par le rapport des amplitudes des signaux à la sortie et à

[6]La définition de chaque paramètre est donné page 60.

l'entrée de la chaîne. Cette valeur dépend bien sûr de la puissance optique fournie par le laser, mesurée à la sortie du modulateur QPSK.

$$K_a = \pi \cdot \alpha_0 \cdot \alpha_a \cdot S_a \cdot G_a \qquad ; \qquad K_b = \pi \cdot \alpha_0 \cdot S_b \cdot G_b \tag{4.9}$$

En utilisant cette méthode, nous avons mesuré à la fréquence 500 MHz les gains des deux boucles du système suivants :

$$K_a = 4,22 \text{ V/mW} \qquad ; \qquad K_b = 8,58 \text{ V/mW}$$

Enfin, comme il est décrit en théorie page 61, ces gains sont normalisés par rapport aux tensions demi-ondes du QPSK ($V_{\pi RF1} = 5,84V$ et $V_{\pi RF2} = 6,08V$), leurs[7] expressions sont :

$$\beta_a = \frac{P_0 \cdot \gamma_0 \cdot K_a}{2V_{\pi RF1}} = 0,35\ P_s \qquad ; \qquad \beta_b = \frac{P_0 \cdot \gamma_0 \cdot K_b}{2V_{\pi RF2}} = 0,71\ P_s \tag{4.10}$$

avec : $P_s = P_0 \cdot \gamma_0$ ; est la puissance optique à la sortie du modulateur QPSK.

### 4.3.3 Les fréquences de coupure de la chaîne globale

**Fréquences de coupure haute :**

La solution la plus simple et la plus efficace pour la mesure de la bande passante est d'utiliser l'analyseur de réseau. Cette solution a été envisagée dès le premier essai, mais comme nous l'avons signalé précédemment, l'Anritsu 37369A est limité en fréquences basses à 40 MHz. Avec cet appareil, nous avons réussi cependant à mesurer la partie des fréquences hautes du système, en utilisant le dispositif expérimental de la figure 4.19. Pour

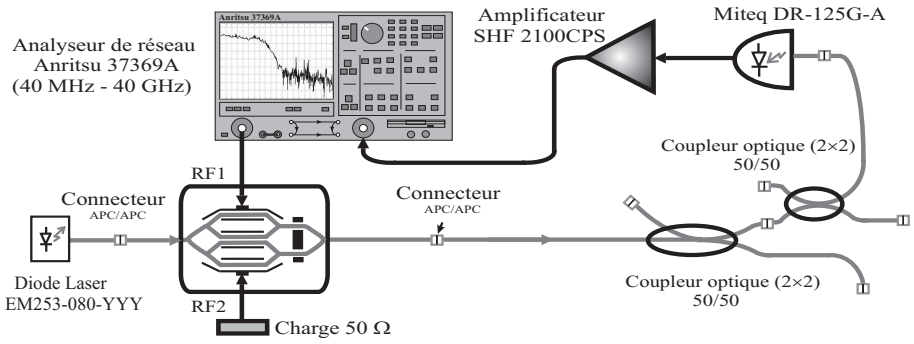



FIGURE 4.19 – *Dispositif de mesure de la fréquence de coupure haute.*

[7] Des informations complémentaires sont données en page 134.

une puissance optique de -2,78 dBm ($\approx$ 0,52 mW : mesurée juste avant l'entrée de la photodiode) et une puissance de modulation de -7 dBm ($\approx$ 0,28 $V_{pp}$) à l'entrée de l'électrode RF du QPSK, les résultats obtenus sont représentés sur la figure 4.20.

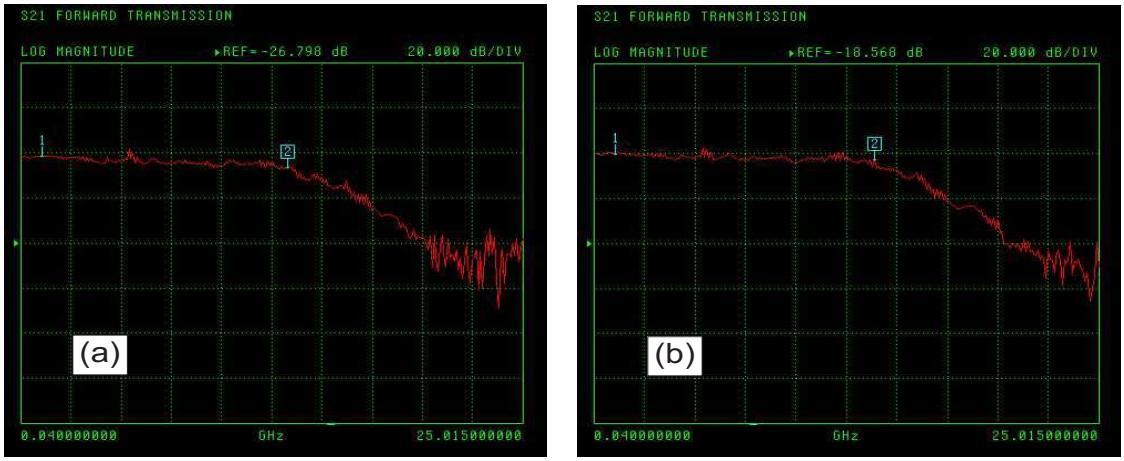



Figure 4.20 – *Paramètres $S_{21}$ de la chaîne des composants en hautes fréquences. (a) Composants de la boucle (A). (b) Composants de la boucle (B).*

C'est à partir des courbes représentées sur les figures 4.20a et 4.20b, que nous avons pu déterminer les fréquences de coupure haute du système. Ces fréquences sont d'environ 13 GHz, ce qui correspond à des constantes de temps de l'ordre de 12,2 ps. L'origine de celles-ci se confirme ici, elles sont liées aux photodétecteurs Miteq.

En effet, la présence dans la chaîne de mesure des autres composants (coupleurs optiques et amplificateur RF), n'ont rien modifié par rapport aux bandes passantes mesurées sans ces composants (figures 4.12a et 4.12b). Les valeurs typiques fournies par le constructeur indiquent aussi que la bande passante de ces photodétecteurs est aux alentours de cette fréquence de coupure.

**Fréquences de coupure basse :**

La figure 4.21 montre le montage expérimental utilisé pour la mesure des fréquences de coupure basses du système. Le principe de la méthode consiste à appliquer sur l'électrode RF du modulateur QPSK un signal sinusoïdal d'amplitude suffisante et constante, puis de mesurer sur l'oscilloscope LeCroy l'amplitude du signal en sortie de la chaîne. La fréquence de ce signal est ajustable par un générateur de basses fréquences (fréquences disponibles : $0 - 80$ MHz), mais les pertes électriques dues aux câbles et au connecteur BNC (en forme de T sur la figure) empêchent cependant d'aller plus loin en fréquences.

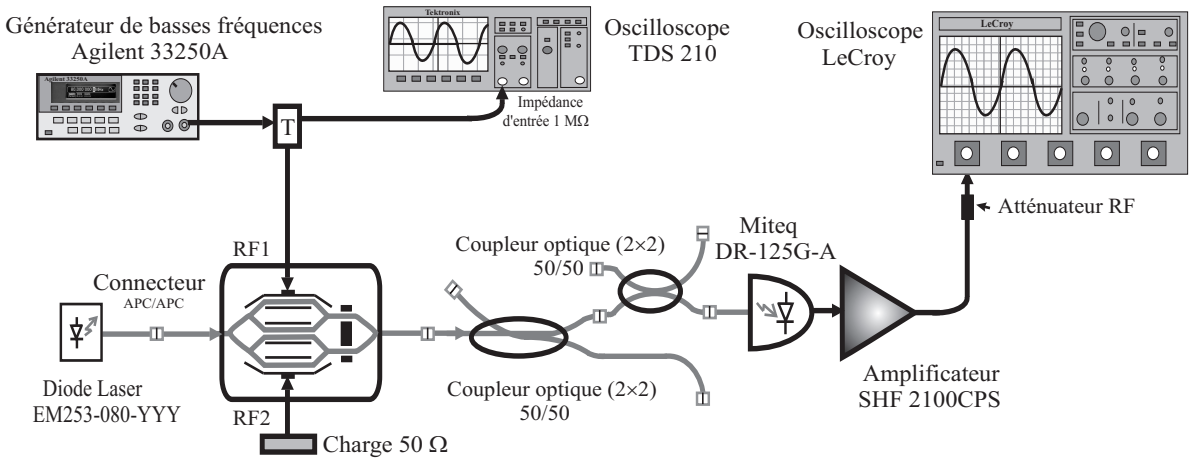



Figure 4.21 – *Dispositif de mesure de la fréquence de coupure basse.*

Les résultats obtenus de ces mesures sont représentés sur la figure 4.22. La fréquence de coupure basse pour la chaîne des composants de la boucle (A) est d'environ 50 kHz, et celle de la boucle (B) est d'environ 30 kHz. En effectuant des mesures[8] avec et sans amplificateurs RF, nous avons déduit que ces composants sont à l'origine de ces fréquences de coupure basses.

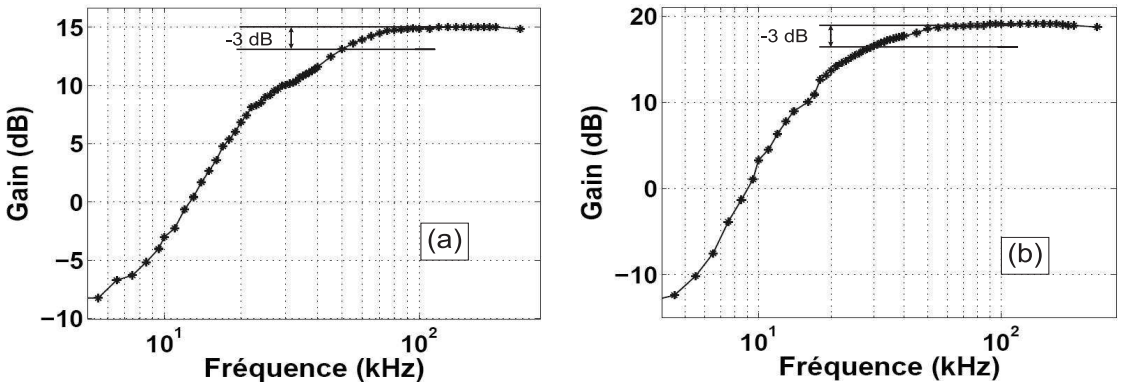



Figure 4.22 – *Diagrammes de Bode de la chaîne des composants en basses fréquences.* (*a*) *Composants de la boucle* (*A*). (*b*) *Composants de la boucle* (*B*).

Avec les caractéristiques en boucle ouverte que nous venons de décrire, l'oscillateur est prêt à être bouclé sur lui-même. Dans ce qui suit, nous allons l'étudier expérimentalement en commençant par son architecture à une seule boucle, puis à deux boucles. Des comparaisons des résultats expérimentaux aux résultats de l'intégration du modèle théorique seront aussi données.

[8]Le dispositif expérimental utilisé est le même que celui de la figure 4.21.

## 4.4 Système à une seule boucle de rétroaction

La photographie 4.23 représente le générateur de chaos tel qu'il a été réalisé expérimentalement. Les atténuateurs optiques variables HA9 et HA11 permettent de contrôler optiquement les gains des boucles de rétroaction. Ainsi par simple blocage de l'un de ces atténuateurs, le fonctionnement du système passe en simple boucle. Cette souplesse expérimentale présente l'avantage de pouvoir faire basculer facilement le système, et d'observer rapidement ses régimes dynamiques en fonction de l'une comme de l'autre de ses boucles. Les résultats que nous allons présenter dans cette section sont réalisés soit en bloquant l'atténuateur HA11, soit en ouvrant la boucle (B) au niveau d'un connecteur.

Nous signalons aussi un détail expérimental lié à l'utilisation du second coupleur optique ($50 \times 50$) de la boucle (A). En effet, la puissance optique à la sortie du QPSK est divisée pratiquement en 2 par le premier coupleur optique. Ensuite à l'aide du second coupleur, la puissance de l'une des sorties du premier coupleur est encore divisée en 2 (celle qui est destinée à la boucle (A)), alors que l'autre ne l'est pas (celle qui est destinée à la boucle (B)). Pour disposer de plus de puissance optique dans la boucle (A) et afin de protéger les composants optoélectroniques du générateur (essentiellement les photodiodes Miteq), nous avons donc inséré le second coupleur optique dans la boucle (B). Les délais du système sont ensuite ajustés au moyen de jarretières optiques, ce qui ne change absolument rien de la configuration initiale de l'oscillateur, à l'exception des gains de boucle qui se retrouvent affectés par le facteur de couplage $\alpha_a = 0,5$ (c'est-à-dire : $2\beta_a$ et $\beta_b/2$). Ainsi, les expressions (4.10) des gains globaux deviennent :

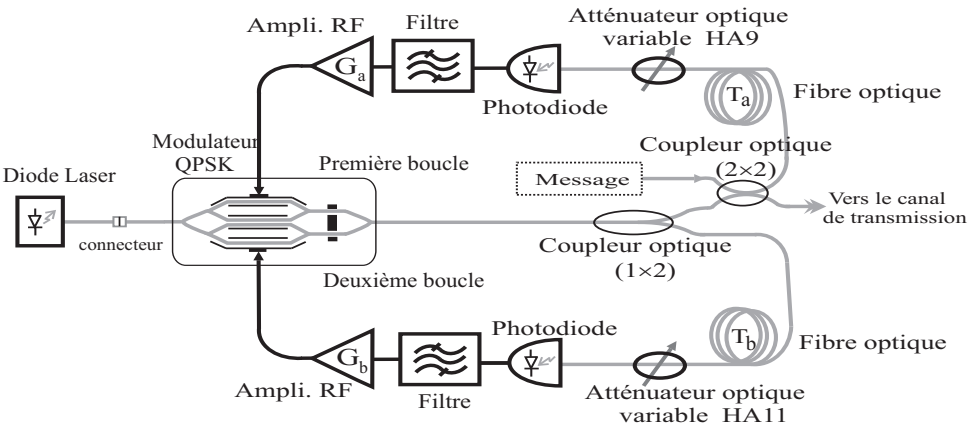
$$\beta_a = 0,71\ P_s \qquad ; \qquad \beta_b = 0,36\ P_s \tag{4.11}$$

### 4.4.1 Évolution temporelle

Les traces temporelles observées expérimentalement sont enregistrées avec l'oscilloscope LeCroy (photographie 4.24). Ces traces sont obtenues en augmentant le paramètre de bifurcation, qui correspond au gain de la boucle opto-électronique d'amplification et de filtrage ($\beta_a$). Ce gain est ajusté optiquement au moyen de l'atténuateur variable HA9.

Lorsque le montage est mis en route, l'atténuateur HA9 doit se trouver en atténuation très forte ($-50\,\mathrm{dB}$ par exemple). Cette précaution expérimentale est nécessaire, car d'une part c'est pour protéger les composants optoélectroniques formant la chaîne de contre-réaction, et d'autre part, pour avoir au lancement un gain de retour $\beta_a$ quasi-nul.

Pour une puissance optique moyenne d'environ $7,3\,\mathrm{mW}$ (mesurée à la sortie du modulateur QPSK), l'augmentation du paramètre de bifurcation $\beta_a$, jusqu'à l'obtention d'un régime dynamique chaotique, s'effectue en diminuant l'atténuation de HA9. La figure 4.25 (à droite) montre la courbe de variation de ce paramètre — relation (4.11) — en fonction de la puissance optique.



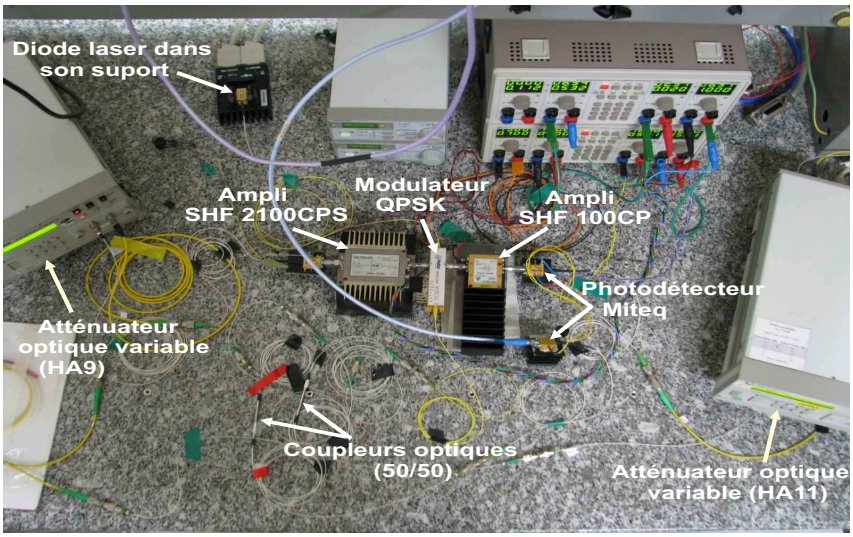




Figure 4.23 – *Schéma et photographie du générateur de chaos à modulateur QPSK.*

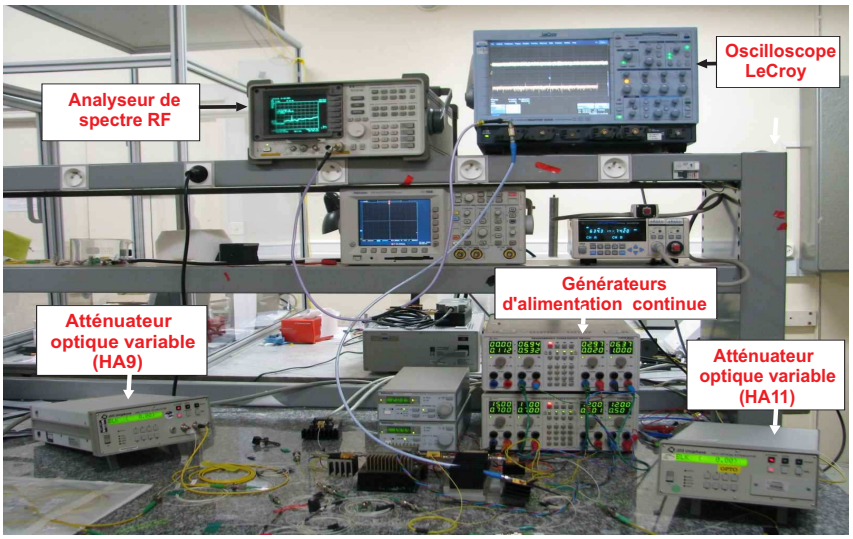



Figure 4.24 – *Dispositif de mesure des évolutions temporelles et spectrales.*

| Boucle (A) | | |
|---|---|---|
| Symbole | Valeur | Unité |
| $T_a$ | 61,3 | ns |
| $f_{c1a}$ | 13 | GHz |
| $f_{c2a}$ | 50 | kHz |
| $\tau_{1a} = (2\pi f_{c1a})^{-1}$ | 12,2 | ps |
| $\tau_{2a} = (2\pi f_{c2a})^{-1}$ | 3,2 | $\mu$s |
| $P_s = P_0 \cdot \gamma_0$ | 7,3 | mW |
| $\beta_a$ | 0–5,25 | |
| $\phi_1$ | 1,3 | rad |
| $\phi_2$ | 2,9 | rad |
| $\phi_3$ | -0,1 | rad |

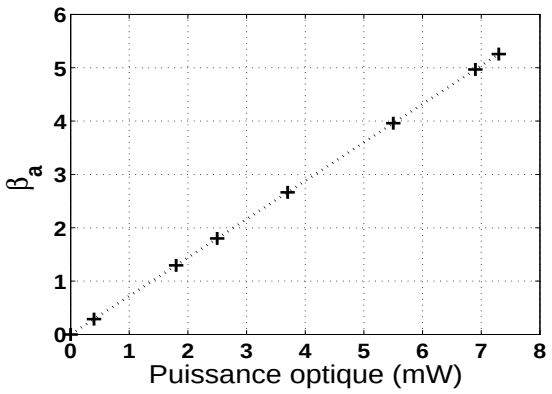



Figure 4.25 – *Paramètres de fonctionnement du système à une seule boucle ($\beta_b = 0$). (à droite) Variation du gain $\beta_a$ en fonction de la puissance $P_s$ en sortie du QPSK.*

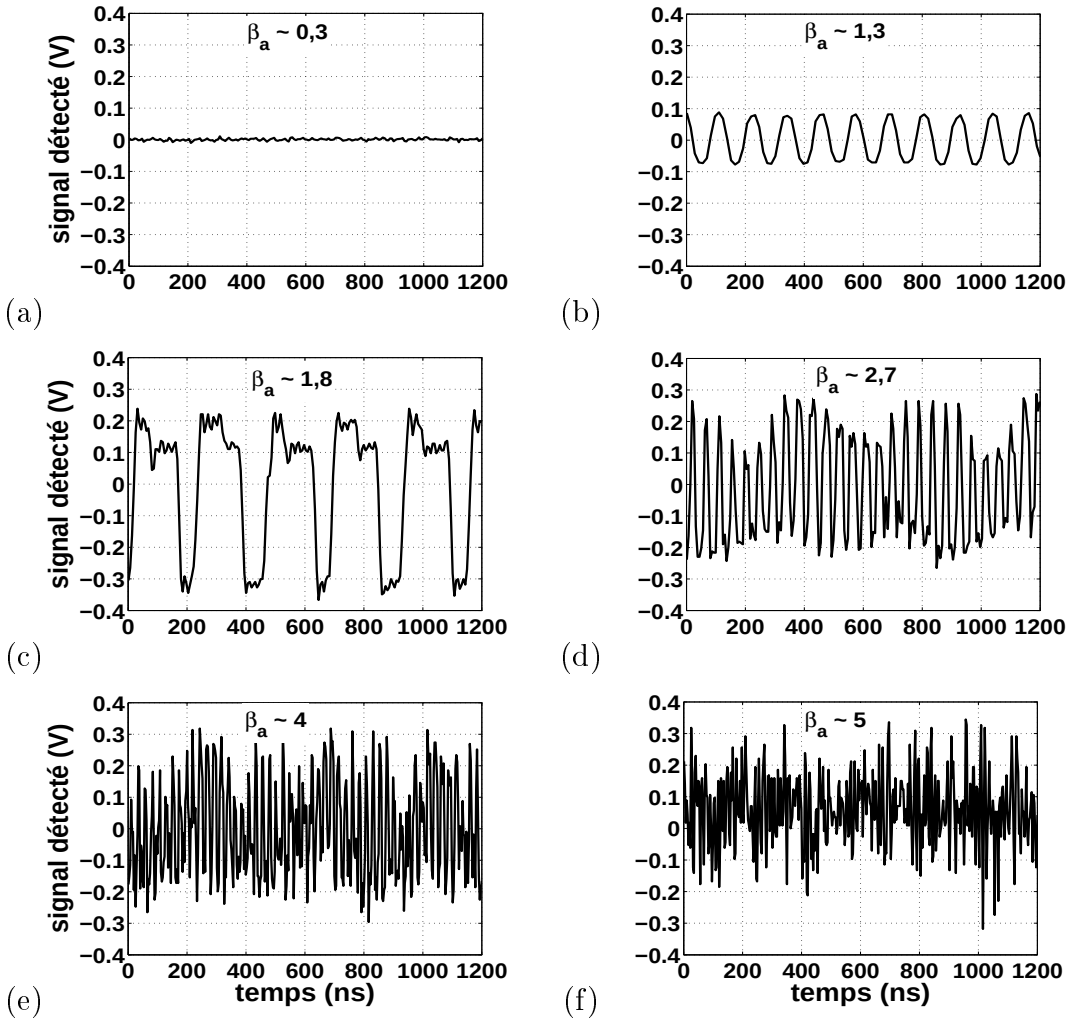



Figure 4.26 – *Traces temporelles du système expérimental à une seule boucle.*

La figure 4.26 représente les traces temporelles observées pour différentes valeurs croissantes de $\beta_a$. Les oscillations correspondantes sont représentatives de l'ensemble des régimes dynamiques du système, depuis le point fixe stable jusqu'à un régime chaotique entièrement développé.

Dans la mesure où on s'intéresse plus particulièrement aux régimes chaotiques, il est intéressant de connaître la bande de fréquence qui peut être couverte par le spectre du signal chaotique produit. Plus large sera cette bande, plus la quantité d'information pouvant être noyée dans le chaos sera grande. L'analyseur de spectre RF utilisé est visible sur la photographie 4.24. Cet appareil est un HP 8592L capable de mesurer des signaux entre 9 kHz et 22 GHz.

### 4.4.2 Étendue spectrale du chaos

La figure 4.27a donne le profil statistique correspondant à la trace temporelle expérimentale 4.26b. On peut noter que cette répartition de la densité de probabilité est la caractéristique d'un régime dynamique périodique (oscillation sur deux niveaux). La fréquence d'oscillation de ce régime est localisée sur le spectre — figure 4.27b — aux alentours de 8 MHz. Cet harmonique correspond approximativement à l'inverse du double du retard temporel du système ($1/2\,T_a = 1/(2 \cdot 61,3\,\text{ns}) = 8,1\,\text{MHz}$). Ce résultat est en très bon accord avec la simulation (voire le spectre de la figure 3.4c page 70), pour laquelle nous avons retrouvé une valeur très proche de cet harmonique.

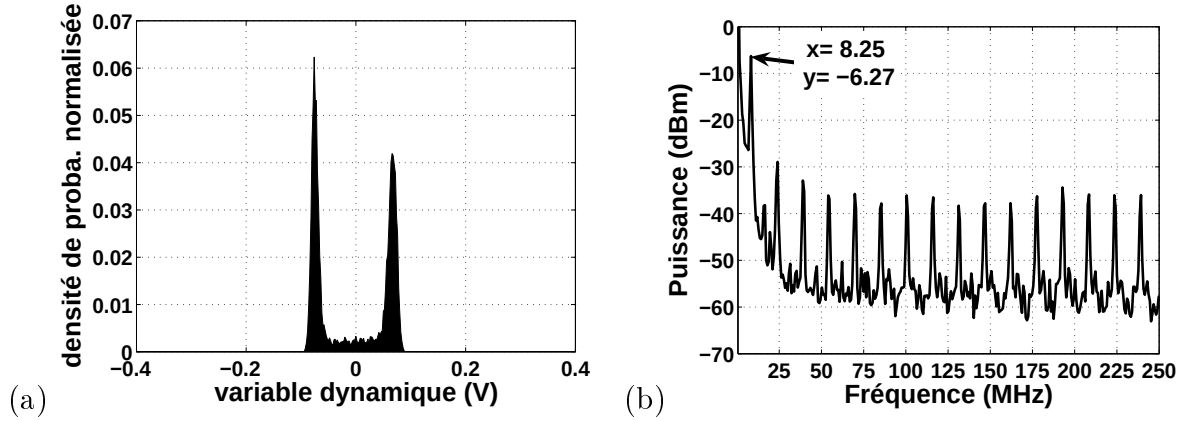



Figure 4.27 – *Régime périodique expérimental du système à une seule boucle* ($\beta_a \sim 1,3$). (*a*) *Densité de probabilité correspondante.* (*b*) *Spectre correspondant.*

La figure 4.28b montre le spectre observé relatif au régime chaotique de la figure 4.26f. Cette figure et notamment la répartition relativement gaussienne de la densité de probabilité associée (figure 4.28a), permettent d'affirmer qu'on a en sortie du système une trace temporelle avec une signature statistique classique d'un bruit quelconque, et avec une signature spectrale de type bruit blanc (si ce n'est bien sûr la limitation en bande passante qui les différencie, dont la fréquence de coupure haute est bien autour de 13 GHz).

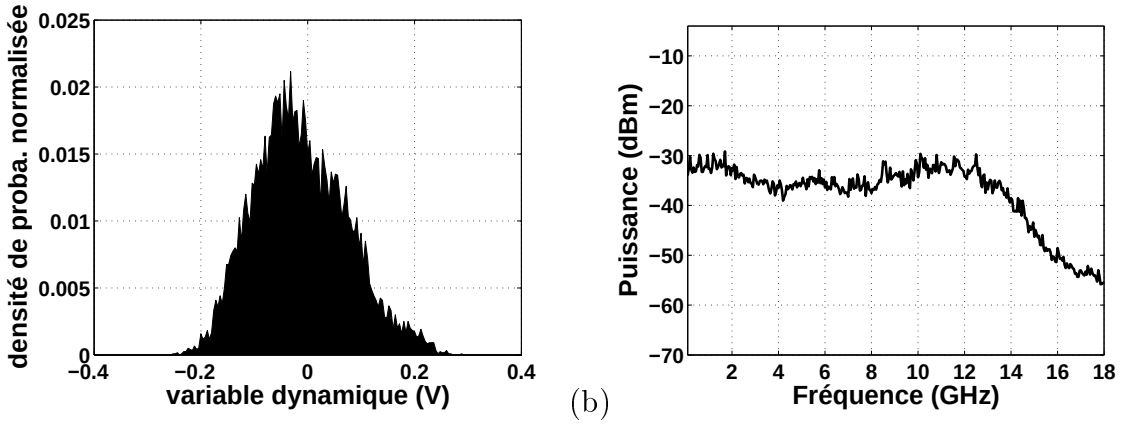



Figure 4.28 – *Régime chaotique expérimental du système à une seule boucle* ($\beta_a \sim 5$). (*a*) *Profil gaussien de la densité de probabilité.* (*b*) *Spectre large bande.*

Les régimes dynamiques que nous venons d'étudier sont deux exemples expérimentaux choisis parmi la multitude des régimes dynamiques que peut engendrer l'oscillateur. Un diagramme de bifurcation permet d'avoir une vue globale de l'ensemble de ces régimes.

### 4.4.3 Diagramme de bifurcation

Un schéma et une photographie du dispositif expérimental de traçage des diagrammes de bifurcation sont donnés sur la figure 4.29. Le principe de la mesure consiste à faire varier l'atténuateur optique variable HA9, et à observer en même temps le profil de la densité de probabilité obtenue sur un oscilloscope numérique de type Tektronix CSA8000. Les deux équipements (l'atténuateur HA9 + CSA8000) sont reliés par l'intermédiaire d'un câble GPIB, et ils sont commandés depuis un PC *via* une interface LabVIEW spécialement conçue. Une interface USB/GPIB permet de relier le PC et les deux équipements. L'acquisition des données de mesure depuis le CSA8000 vers le PC s'effectue donc d'une manière automatique.

Pour l'exemple choisi, les conditions de fonctionnement de l'oscillateur restent les mêmes que celles utilisées pour l'enregistrement des traces temporelles (section 4.4.1). L'interface LabVIEW est conçue de telle sorte à commander l'atténuateur HA9 entre le blocage total (100%) de l'onde optique jusqu'à une atténuation nulle, ou encore inversement (atténuation croissante ou décroissante). Pour l'ensemble des diagrammes de bifurcation expérimentaux qui seront présentés, nous avons échantillionné ce paramètre avec 400 pas entre ces deux limites.

La figure 4.30a donne le premier diagramme de bifurcation du système à une seule boucle, obtenu expérimentalement dans les conditions que nous venons de citer. Ce diagramme nous montre que lorsqu'on fait croître le gain $\beta_a$, la variable dynamique passe d'un régime de point fixe à un régime périodique au moyen d'une bifurcation de Hopf. Puis,

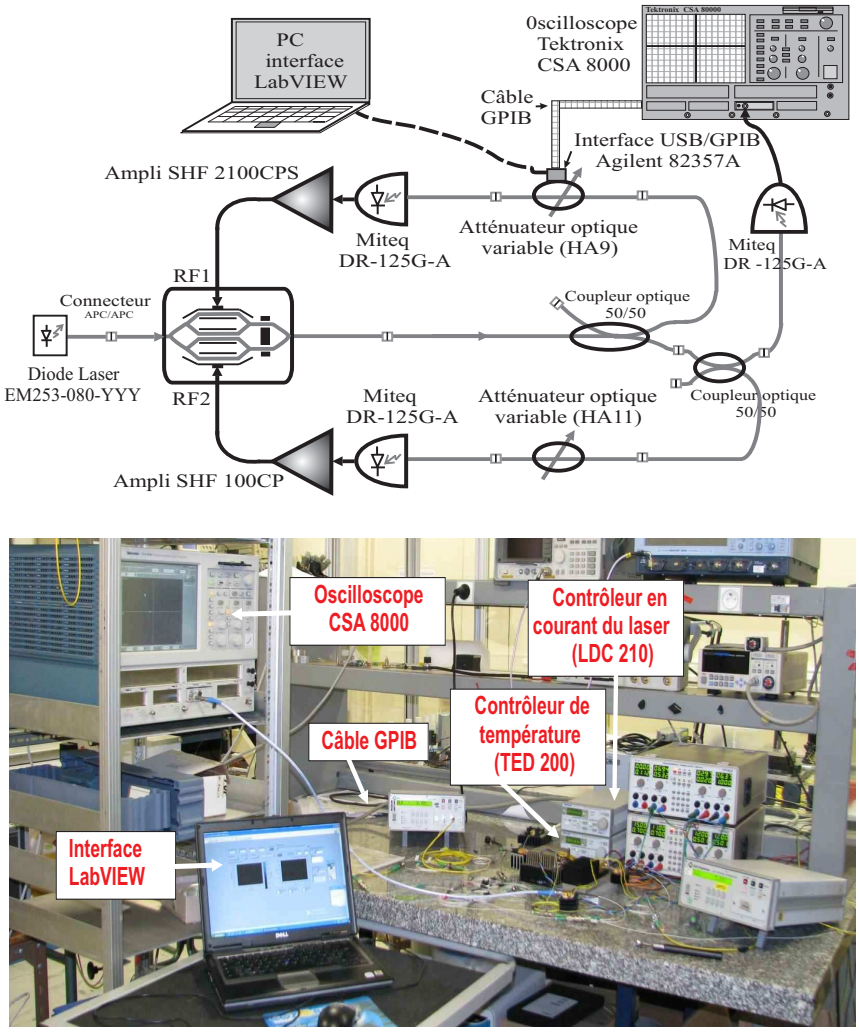
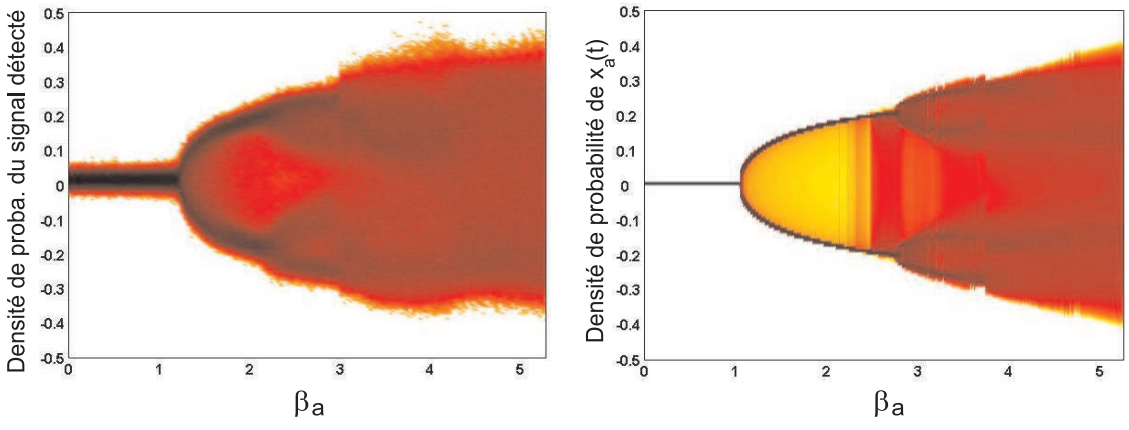



FIGURE 4.29 – *Schéma et photographie du dispositif de traçage des diagrammes de bifurcation.*




(a) Expérimental (b) Simulation

FIGURE 4.30 – *Diagrammes de bifurcation du système à une seule boucle de rétroaction.*

lorsque le gain est encore augmenté, les régimes périodiques évoluent vers des régimes chaotiques de plus en plus développés. Ce diagramme est intéressant dans le sens où il représente notre référence, car comme nous l'avons déjà signalé dans la partie théorique, le système à une seule boucle est largement décrit dans la littérature [52, 53, 118]. C'est la raison aussi pour laquelle nous n'allons pas détailler l'étude de l'oscillateur dans ce cas de configuration.

Un diagramme de bifurcation numérique, obtenu dans les mêmes conditions que le diagramme expérimental, est donné sur la figure 4.30b. En comparant ces deux diagrammes, on constate qu'il y a de très grandes similitudes entre les résultats numériques et expérimentaux [119]. Cette comparaison nous permet de valider le modèle théorique associé à la configuration du système à une seule rétroaction. Cependant, une validation entière de ce modèle passe inévitablement par la comparaison des résultats (simulations/expérimentaux) du système à double boucle de rétroaction.

## 4.5 Système à double boucle de rétroaction

Le basculement du système pour un fonctionnement à double boucle de rétroaction se fait tout simplement par déblocage de l'atténuateur optique variable HA11, ou encore par fermeture de la seconde boucle si elle était ouverte (figure 4.23). Le HA11 doit être en atténuation très forte (−30 dB par exemple) non seulement, pour protéger les composants optoélectroniques formant la seconde boucle, mais aussi pour assurer au lancement du système un état correspondant à $\beta_b$ minimum.

### 4.5.1 Évolutions temporelles et spectrales

Nous avons utilisé le même dispositif que celui de la figure 4.24 pour enregistrer les évolutions temporelles et spectrales de la variable dynamique du système. Le spectre est

| **Boucle (A)** | | | **Boucle (B)** | | |
|---|---|---|---|---|---|
| Symb. | Valeur | Unité | Symb. | Valeur | Unité |
| $T_a$ | 61,3 | ns | $T_b$ | 60,4 | ns |
| $f_{c1a}$ | 13 | GHz | $f_{c1b}$ | 13 | GHz |
| $f_{c2a}$ | 50 | kHz | $f_{c2b}$ | 30 | kHz |
| $\tau_{1a}$ | 12,2 | ps | $\tau_{1b}$ | 12,2 | ps |
| $\tau_{2a}$ | 3,2 | $\mu$s | $\tau_{2b}$ | 5,3 | $\mu$s |
| $\beta_a$ | 0 – 5,25 | | $\beta_b$ | 0 – 2,55 | |
| **Autres paramètres** | | | | | |
| $P_s$ | 7,3 | mW | $\phi_2$ | 0,7 | rad |
| $\phi_1$ | 1,2 | rad | $\phi_3$ | -0,2 | rad |

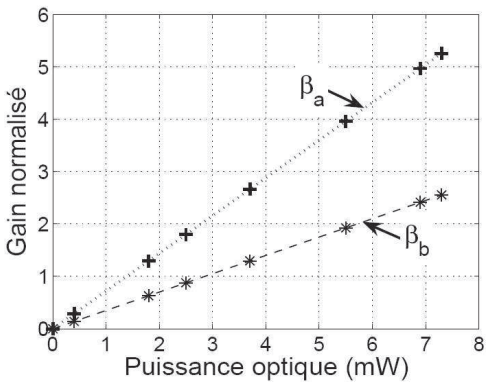
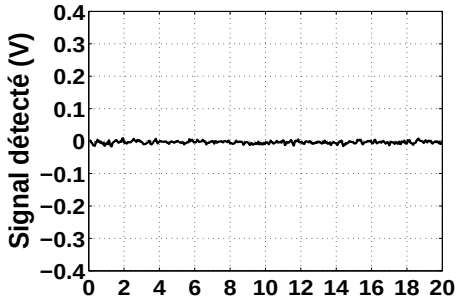
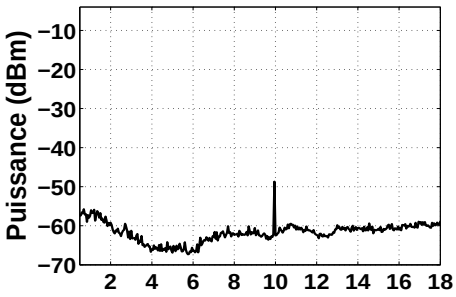



Figure 4.31 – *Paramètres de fonctionnement du système à double boucle.* (*à droite*) *Variation des gains en fonction de la puissance $P_s$ en sortie du QPSK.*

$\beta_a \sim 0,5$

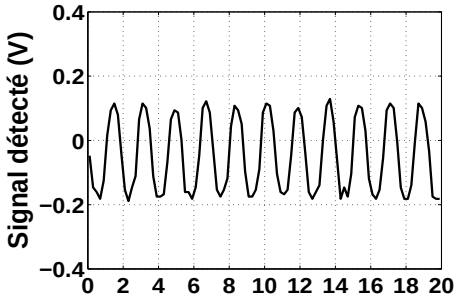



(a)

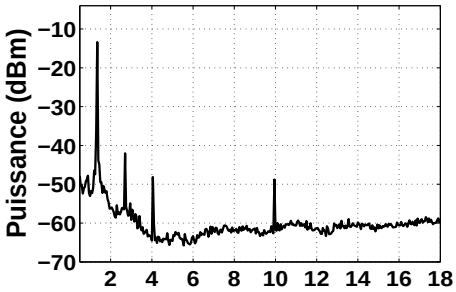



(b)

$\beta_a \sim 1,2$

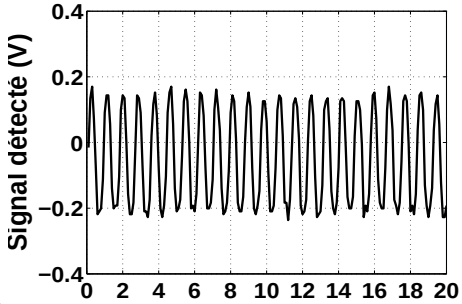



(c)

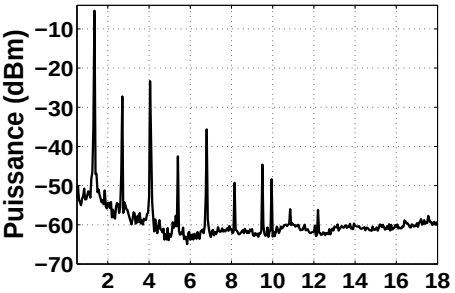



(d)

$\beta_a \sim 2,9$

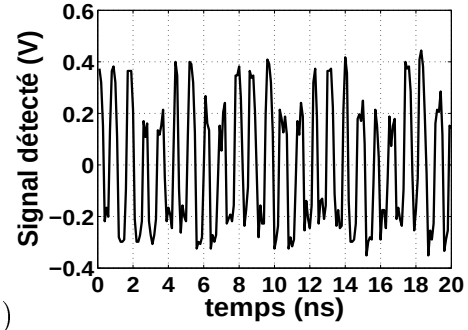



(e)

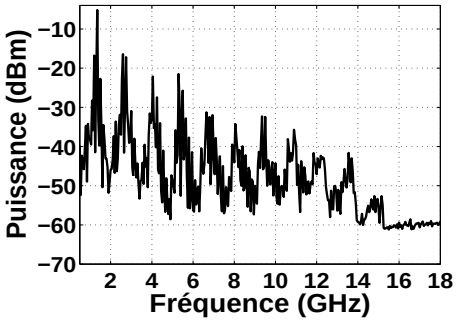



(f)

$\beta_a \sim 3,5$




(g)




(h)

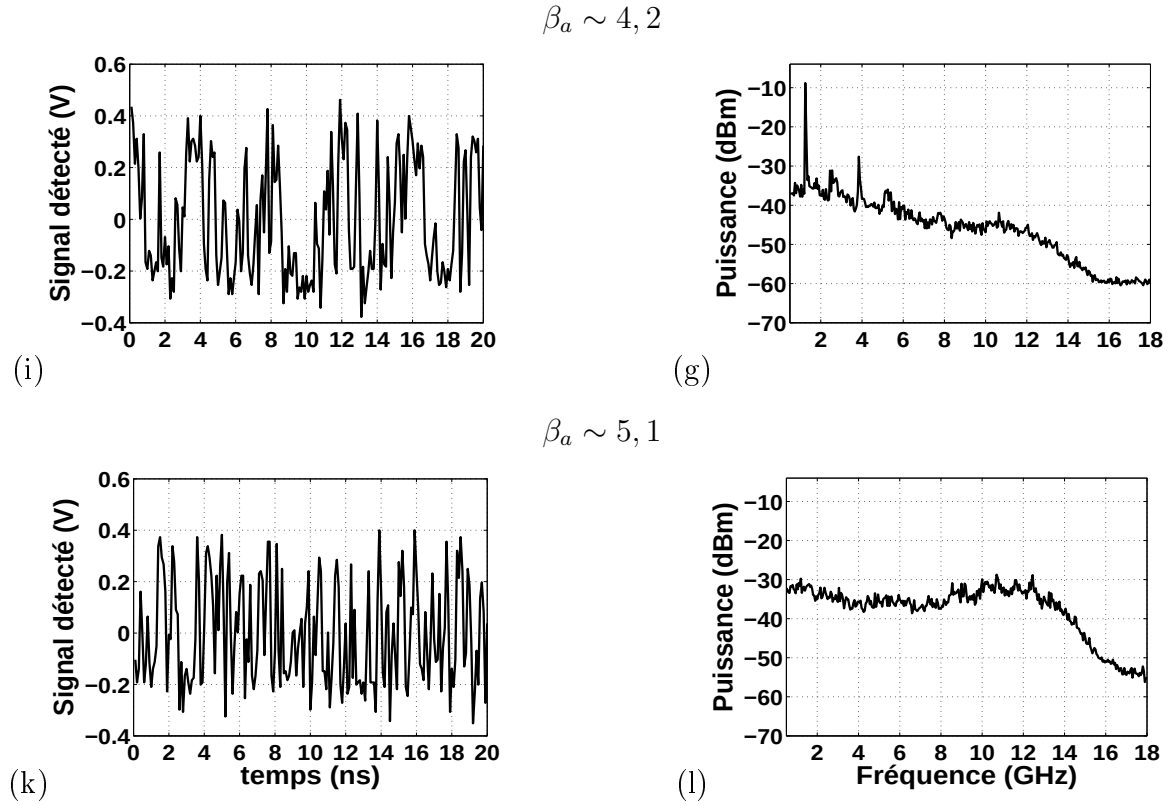



Figure 4.32 – *Évolutions temporelles et spectrales du système expérimental à double boucle de rétroaction* ($\beta_b \sim 0{,}4$).

visualisé sur une bande large allant de $0,5$ à $18\,\text{GHz}$, et les paramètres expérimentaux de fonctionnement sont donnés au tableau 4.31. Le point de fonctionnement du modulateur QPSK est choisi de telle sorte que les interférences soient constructives. L'atténuateur optique HA11 est fixé à une valeur de $-14,1\,\text{dB}$ (ce qui correspond à environ $\beta_b = 0,4$ que nous considérons faible).

La figure 4.32 représente les chronogrammes et les spectres observés pour différentes valeurs décroissantes de l'atténuation contrôlée par HA9. Ces chronogrammes montrent la route vers le chaos, qui commence au début par un régime stationnaire stable, en raison du faible gain de retour ($\beta_a = 0,5$). Alors qu'à la fin, lorsque $\beta_a$ est poussé vers les plus hautes valeurs accessibles expérimentalement, la dynamique observée est hyperchaotique. Cette dernière se caractérise par un spectre large bande et un niveau d'amplitude élevé, comme le montre l'exemple des figures 4.32k et 4.32l.

Par ailleurs, on peut noter que le premier régime périodique observé — figure 4.32c — est d'ordre 2, comme le confirme son profil statistique donné sur la figure 4.33a ; sa période[9] est d'environ 1,7 ns. En comparant cette période à celle d'un régime du même ordre dans le cas du système à une seule boucle[10] (figure 4.26b), nous pouvons déduire que 1,7 ns correspondrait au double de la différence des 2 délais du système, c'est-à-dire : $2(T_a - T_b) = 2 \cdot (61,3 - 60,4)$ ns $= 1,8$ ns. Lorsque la bande de fréquences observées sur l'analyseur est réduite pour une meilleure résolution de 30 kHz, l'inverse de cette

[9] Cette période a été mesurée sur l'oscilloscope LeCroy avec un pas d'échantillonnage de 100 ps.
[10] La période d'un tel régime était $2\,T_a = 124,4$ ns.

période (*i.e* fréquence : 1/(1,7 ns)= 0,5 GHz) est bien localisée sur le spectre enregistré (figure 4.33b). Celle-ci est conforme à nos simulations numériques, comme le montre le pic du spectre 3.15c page 83.

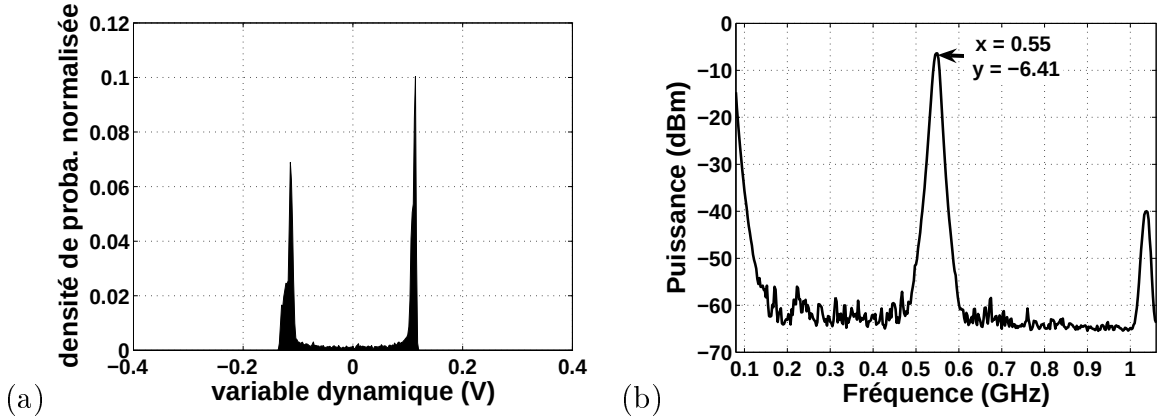



Figure 4.33 – *Régime périodique expérimental du système en double boucle* ($\beta_a \sim 1{,}2$). *(a) Profil statistique. (b) Spectre correspondant.*

## 4.5.2 Diagrammes de bifurcation

Grâce à la souplesse du montage expérimental, nous avons pu effectuer un premier relevé de diagramme de bifurcation du système à double boucle (figure 4.34a). Nous retrouvons à nouveau une route vers le chaos assez classique pour les systèmes à retard : stationnaire, périodique et enfin chaotique.

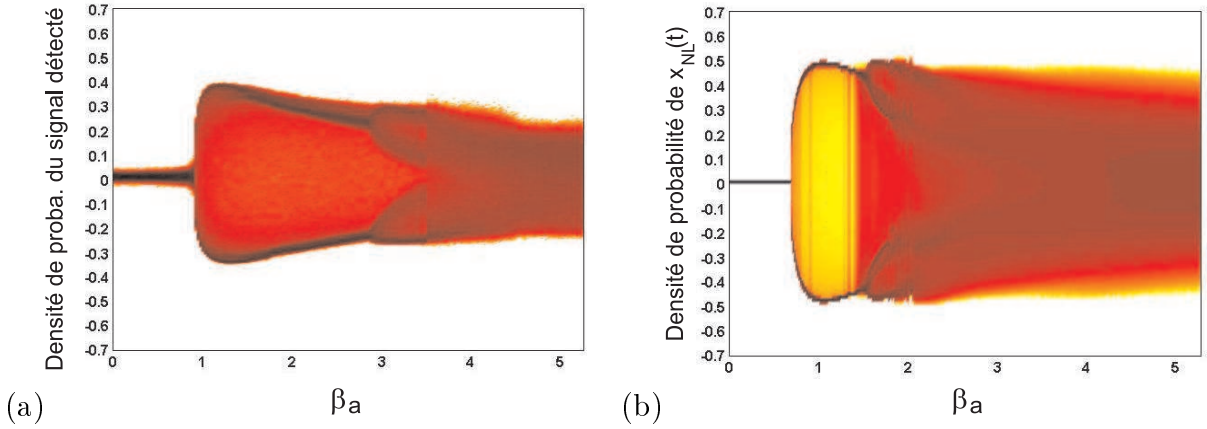
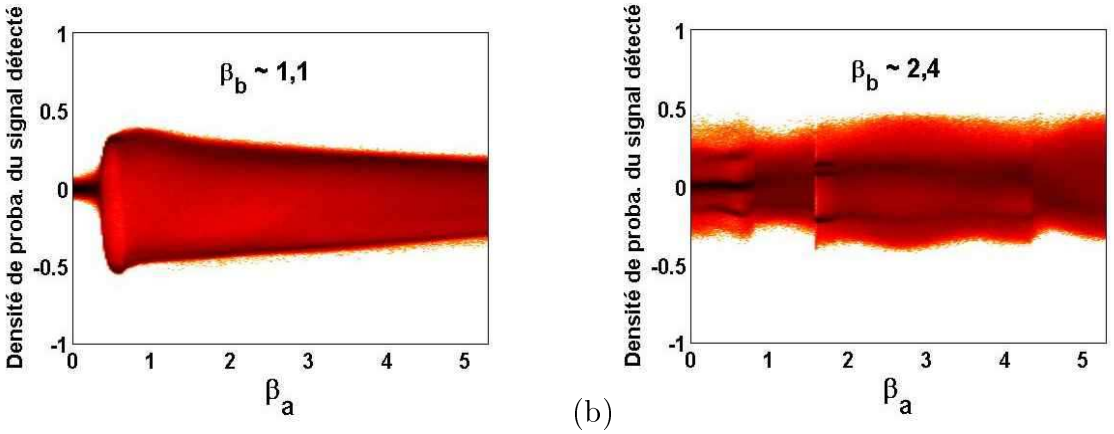



Figure 4.34 – *Diagrammes de bifurcation du système à double boucle de rétroaction. Le gain de la seconde boucle est considéré faible* ($\beta_b \sim 0{,}4$) *; voir tableau* 4.31 *pour les autres paramètres.*

À titre de comparaison, un diagramme de bifurcation numérique est représenté à la figure 4.34b. Les paramètres utilisés pour avoir ce diagramme correspondent à ceux mesurés dans le cas du diagramme expérimental. Une bonne adéquation peut être relevée entre les résultats numériques et expérimentaux, confirmant ainsi le bon comportement du système expérimental par rapport au modèle dynamique à retards initialement espéré [119].




(a) (b)

Figure 4.35 – *Diagrammes de bifurcation expérimentaux du système à double boucle. Le gain de la seconde boucle est (a) moyen et (b) élevé.*

Les figures 4.35a et 4.35b correspondent aux relevés expérimentaux dans le cas où le gain de la seconde boucle $\beta_b$ est augmenté. D'après ces diagrammes, on peut remarquer que les régimes périodiques ne sont plus observables, et que les dynamiques chaotiques sont rapidement atteintes. Intuitivement, cette remarque nous paraît évidente dans le cas du gain $\beta_b$ élevé, car le système se trouve initialement dans un état de régime chaotique. On constate aussi, plus particulièrement sur la figure 4.35a, qu'il y a un phénomène d'amincissement du diagramme de bifurcation. L'origine exacte de celui-ci n'est pas identifié ; il pourrait s'agir de phénomènes de saturation des photodiodes amplifiées.

L'influence des conditions initiales et des phases (donc du point de fonctionnement du modulateur QPSK) peut être mise en évidence dans un diagramme de bifurcation par le phénomène d'hystérésis [120]. L'évolution croissante ou décroissante du paramètre de bifurcation $\beta_a$ conduit à des résultats différents (figure 4.36). La première explication qui peut être mise en avant est le changement d'attracteur étrange dans l'espace des phases. Ce changement d'attracteur pousse à une dynamique différente dans le cas d'une variation croissante ou décroissante du paramètre de bifurcation [121]. L'hystérésis ne suscite pas un grand intérêt dans l'analyse de notre système en vue d'une application à la cryptographie. Cependant, ce phénomène physique peut être intéressant dans la compréhension des mécanismes de bifurcation des dynamiques à retard passe-bande [57].

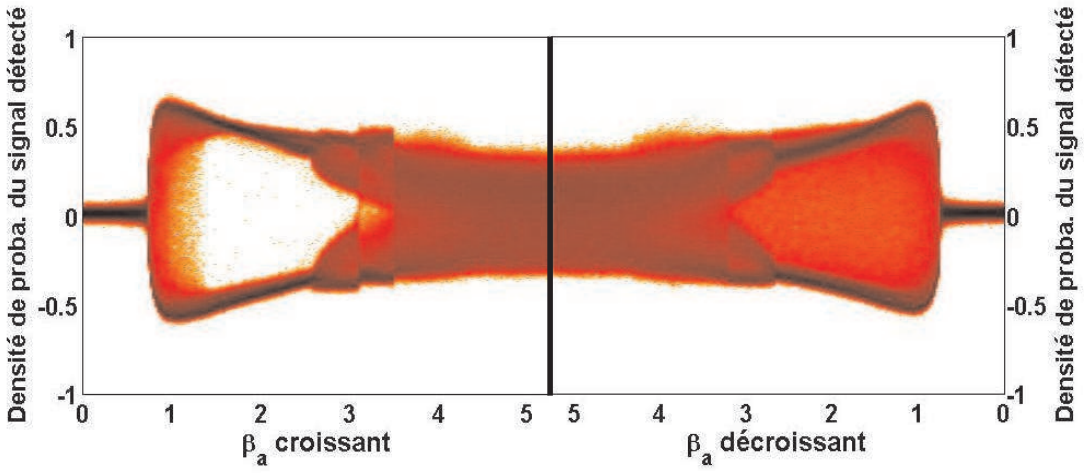



Figure 4.36 – *Hystérésis du système en double boucle de rétroaction* ($\beta_b \sim 0{,}5$).

Nous venons de décrire expérimentalement le générateur de chaos à modulateur QPSK. Pour prouver la viabilité du système cryptographique proposé, il reste maintenant à réaliser le *système complet* « Emetteur−Récepteur » permettant de décrypter un message. Par manque de temps, cette réalisation n'a pu être menée à terme, mais elle constitue l'une des perspectives de cette thèse.

## 4.6 Conclusion

Dans ce dernier chapitre, nous avons présenté et étudié expérimentalement le générateur de chaos à modulateur QPSK. Au cours de la première partie, l'étude expérimentale du modulateur nous a permis de valider la fonction non linéaire bidimensionnelle théorique du système. Les méthodes de mesure de l'ensemble des paramètres caractérisant ce modulateur ont été aussi brièvement décrites.

Nous avons ensuite, dans une deuxième et troisième partie, caractérisé tous les éléments constituant l'oscillateur chaotique. Cette caractérisation est effectuée pour chaque composant, soit indépendamment des autres, soit dans l'ensemble en boucle ouverte. La quatrième partie a été consacrée à l'étude expérimentale des dynamiques générées par cet oscillateur en architecture à une seule boucle. Cette étude nous a permis de mettre en évidence la production de signaux chaotiques et la validation quantitative du modèle théorique du système.

Enfin, l'étude du système en double boucle a été également validée. L'oscillateur peut exhiber des dynamiques non linéaires complexes, dont le chaos s'étale sur plusieurs GHz de bande passante (environ 13 GHz). La suite de ce travail va consister à mettre au point le dispositif complet de *cryptographie par chaos*, qui aura pour variable dynamique l'intensité optique.

# Conclusion générale et perspectives

Ces travaux de thèse ont permis la mise en œuvre de nouvelles architectures optoélectroniques pour la génération du chaos en intensité. Leur principe s'appuie sur une dynamique électro-optique non linéaire à retard, dont la non linéarité est particulière par sa nature bidimensionnelle. Cette dernière est construite grâce à modulateur QPSK, qui n'est autre qu'un interféromètre à 4 ondes réalisé en optique intégrée, et disposant de 2 électrodes de modulation indépendantes. Ce modulateur a permis de relier deux boucles de rétroaction, qui sont formées essentiellement de composants optoélectroniques largement utilisés dans les transmissions des télécommunications optiques actuelles. Ainsi, un nouveau système générateur de chaos est réalisé, original par son architecture, et robuste par le nombre de paramètres physiques de sa clé cryptographique. Le montage a permis aussi de disposer d'une part, d'une dynamique ultra-rapide jusqu'à des fréquences de plusieurs GHz (environ 13 GHz), et d'autre part de générer un chaos de grande dimension destiné au cryptage physique de données optiques.

Au travers d'une étude numérique et expérimentale, nous avons cherché à analyser certains des nombreux comportements dynamiques que peut présenter cet oscillateur à modulateur QPSK, en fonction de divers paramètres physiques du montage : régimes de point fixes stables, périodiques, et chaotiques. La mise en œuvre du montage expérimental a permis de valider le modèle théorique adopté pour les simulations. Ainsi, la production de signaux chaotiques a pu être mise en évidence dans 2 configurations différentes par leur architecture à une seule boucle, puis par deux boucles de rétroaction.

Après avoir réussi à maîtriser le fonctionnement du générateur de chaos à modulateur QPSK, nous avons étudié numériquement le système de cryptage complet, en modulant chaotiquement une information binaire à plus de 3 Gbit/s. Ainsi, la restitution du message au niveau du récepteur, dont le principe est basé sur la synchronisation de chaos initialement introduit par Pecora et Carroll, nous a permis de montrer la faisabilité du système global de cryptographie par chaos proposé.

Cette étude nous a aussi aidé à fixer les paramètres de fonctionnement (un des gains de boucle est élevé et l'autre faible ; la condition d'interférence doit être fixée autour du maximum de transmission du QPSK), et de définir les conditions optimales (synchronisation en boucle ouverte ; le plus grand des délais du système doit être inséré dans la boucle à gain élevé), afin d'avoir toutes les chances, d'une part de restituer un message décodé de bonne qualité, et d'autre part d'augmenter la sécurité de la transmission.

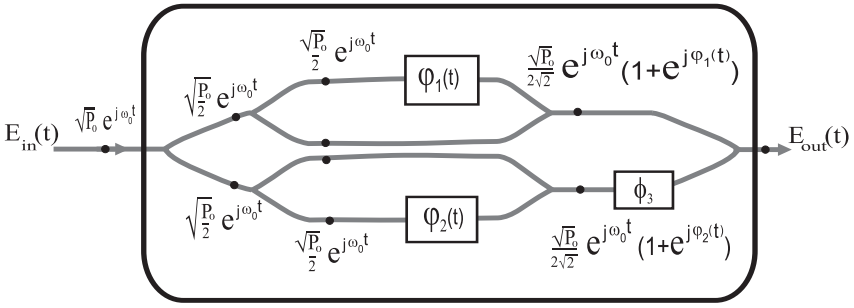
Il reste bien sûr encore beaucoup de points à développer, dont certains sont déjà évoqués tout au long de ce manuscrit. En effet, bien qu'il soit un cas particulier, correspondant à une clé cryptographique particulière, nous avons vu à travers la fonction d'autocorrélation que lorsque les délais du système sont égaux, certaines composantes périodiques liées à ces délais n'apparaissent plus, autrement dit la confidentialité est améliorée. Cette configuration précise du système mérite plus d'investigations et d'explorations, tant sur les plans numérique, analytique et expérimental. Certes la confidentialité est une caractéristique encore mal connue précisément pour ce type de cryptographie, car il n'existe que très peu de travaux publiés [122] sur la cryptanalyse des systèmes de codage par chaos, mais le degré de complexité est un paramètre objectif qui est souvent pris en compte dans l'estimation du degré de confidentialité. La mesure de la complexité en terme d'entropie d'informations a été faite numériquement, mais elle reste à faire sur la base du comportement expérimental, à partir de séries temporelles. Ainsi, à partir de mesures de dimensions de Lyapounov sur des signaux expérimentaux, il serait possible de mieux caractériser la confidentialité effective. La crypto-analyse est bien sûr l'une des perspectives de cette thèse.

Le potentiel de décodage du système proposé a été certes mis en évidence numériquement, mais il reste encore à le réaliser d'une manière expérimentale. De plus, le point d'insertion du message informatif n'a pas été discuté. En effet, de part la nature de ce message (électrique ou optique) et de l'endroit de son injection, on peut penser que plusieurs possibilités sont à envisager. L'architecture du système à double boucle nous permet aussi d'imaginer que des transmissions bidirectionnelles peuvent êtres réalisées, pour lesquelles des protocoles de distribution de clés ont été proposés [123].

Enfin, un dernier exemple de perspective est la suite donnée à l'intégration sur le $LiNbO_3$ d'un tout nouveau composant [124], encore au stade de tests (année 2009), qui est un modulateur DQPSK (Dual-QPSK) disposant de 4 électrodes de modulation. Une utilisation de ce composant permettra de réaliser peut être une non linéarité 4D. Ainsi, la mise en œuvre d'une nouvelle architecture de générateur de chaos, à 4 boucles de rétroaction avec des retards multiples, peut être une autre solution pour augmenter encore plus significativement la taille de la clé cryptographique.

# Annexe A : Fonction non linéaire

Cette annexe donne les détails du principe de calcul de la fonction non linéaire $f_{NL}[x_a, x_b]$, aboutissant à la relation (2.15).




– L'expression de $f_{NL}[x_a, x_b]$ est obtenue par le calcul de la moyenne — relation (12) — du module au carré du champ électrique résultant $E_{out}(t)$.

$$f_{NL}[v_a, v_b](t) = \langle |E_{out}(t)|^2 \rangle \tag{12}$$

– Le champ électrique $E_{out}(t)$ en sortie du modulateur QPSK est donné par :

$$E_{out}(t) = \frac{\sqrt{P_0}}{4}\Big[1 + e^{j\varphi_1(t)} + \big[1 + e^{j\varphi_2(t)}\big]e^{j\phi_3}\Big]e^{jw_0 t} \tag{13}$$

– Il vient donc :

$$f_{NL}[v_a, v_b] = E_{out}(t) \cdot E^*_{out}(t) \tag{a1}$$

$$= \frac{P_0}{16}\Big[1 + e^{j\varphi_1} + \big[1 + e^{j\varphi_2}\big]e^{j\phi_3}\Big] \cdot \Big[1 + e^{-j\varphi_1} + \big[1 + e^{-j\varphi_2}\big]e^{-j\phi_3}\Big], \tag{a2}$$

$$= \frac{P_0}{16}\Big\{4 + \underbrace{e^{j\varphi_1} + e^{-j\varphi_1}} + \underbrace{e^{j\varphi_2} + e^{-j\varphi_2}} + \underbrace{e^{j\phi_3} + e^{-j\phi_3}} + \underbrace{e^{j(\varphi_1-\phi_3)} + e^{-j(\varphi_1-\phi_3)}} + \underbrace{e^{j(\varphi_2+\phi_3)} + e^{-j(\varphi_2+\phi_3)}} + \underbrace{e^{j(\varphi_2+\phi_3-\varphi_1)} + e^{-j(\varphi_2+\phi_3-\varphi_1)}}\Big\}, \tag{a3}$$

$$= \frac{P_0}{16}\Big\{4 + 2\cos\varphi_1 + 2\cos\varphi_2 + 2\cos\phi_3 + 2\cos(\varphi_1 - \phi_3) + 2\cos(\varphi_2 + \phi_3) + 2\cos(\varphi_2 + \phi_3 - \varphi_1)\Big\}, \quad \text{(a4)}$$

$$= \frac{P_0}{4}\Bigg\{1 + \frac{1}{2}\Big[\cos\varphi_1 + \cos\varphi_2 + \cos\phi_3\Big] + \frac{1}{2}\Big[\cos(\varphi_1 - \phi_3) + \cos(\varphi_2 + \phi_3)\Big] + \frac{1}{2}\Big[2\cos^2\Big(\frac{\varphi_2 + \phi_3 - \varphi_1}{2}\Big) - 1\Big]\Bigg\}, \quad \text{(a5)}$$

$$= \frac{P_0}{4}\Bigg\{\frac{1}{2} + \frac{1}{2}\Big[2\cos\Big(\frac{\varphi_1 + \varphi_2}{2}\Big)\cos\Big(\frac{\varphi_1 - \varphi_2}{2}\Big) + \cos\phi_3\Big] + \frac{1}{2}\Big[2\cos\Big(\frac{\varphi_1 + \varphi_2}{2}\Big)\cos\Big(\frac{\varphi_1 - \varphi_2 - 2\phi_3}{2}\Big)\Big] + \cos^2\Big(\frac{\varphi_2 + \phi_3 - \varphi_1}{2}\Big)\Bigg\}, \quad \text{(a6)}$$

$$= \frac{P_0}{4}\Bigg\{\frac{1}{2}[1 + \cos\phi_3] + \cos\Big(\frac{\varphi_1 + \varphi_2}{2}\Big)\cos\Big(\frac{\varphi_1 - \varphi_2}{2}\Big) + \cos\Big(\frac{\varphi_1 + \varphi_2}{2}\Big)\cos\Big(\frac{\varphi_1 - \varphi_2 - 2\phi_3}{2}\Big) + \cos^2\Big(\frac{\varphi_2 + \phi_3 - \varphi_1}{2}\Big)\Bigg\}, \quad \text{(a7)}$$

$$= \frac{P_0}{4}\Bigg\{\cos^2\Big(\frac{\phi_3}{2}\Big) + \cos\Big(\frac{\varphi_1 + \varphi_2}{2}\Big)\Big[\cos\Big(\frac{\varphi_1 - \varphi_2}{2}\Big) + \cos\Big(\frac{\varphi_1 - \varphi_2 - 2\phi_3}{2}\Big)\Big] + \cos^2\Big(\frac{\varphi_2 + \phi_3 - \varphi_1}{2}\Big)\Bigg\}, \quad \text{(a8)}$$

$$= \frac{P_0}{4}\Bigg\{\cos^2\Big(\frac{\phi_3}{2}\Big) + \cos\Big(\frac{\varphi_1 + \varphi_2}{2}\Big)\Big[2\cos\Big(\frac{\varphi_1 - \varphi_2 - \phi_3}{2}\Big)\cos\Big(\frac{\phi_3}{2}\Big)\Big] + \cos^2\Big(\frac{\varphi_2 + \phi_3 - \varphi_1}{2}\Big)\Bigg\}, \quad \text{(a9)}$$

$$= \frac{P_0}{4}\Bigg\{\cos\Big(\frac{\phi_3}{2}\Big)\Big[\cos\Big(\frac{\phi_3}{2}\Big) + 2\cos\Big(\frac{\varphi_1 + \varphi_2}{2}\Big)\cos\Big(\frac{\varphi_1 - \varphi_2 - \phi_3}{2}\Big)\Big] + \cos^2\Big(\frac{\varphi_2 + \phi_3 - \varphi_1}{2}\Big)\Bigg\}, \quad \text{(a10)}$$

En opérant les changements de variables suivants :

$$\psi_1 = \frac{\varphi_1(t)}{2}; \qquad \psi_2 = \frac{\varphi_2(t)}{2}; \qquad \psi_3 = \frac{\phi_3}{2};$$

nous obtenons enfin l'expression de la fonction non linéaire, en les remplaçant dans (a10).

$$\boxed{f_{NL}[v_a, v_b] = \frac{P_0}{4}\Big\{\cos(\psi_3)\Big[\cos(\psi_3) + 2\cos\big(\psi_1 + \psi_2\big)\cos\big(\psi_2 + \psi_3 - \psi_1\big)\Big] + \cos^2\big(\psi_2 + \psi_3 - \psi_1\big)\Big\},}$$

## Condition d'extinction d'un modulateur MZ simple ($\phi_{1,2} = \pm\,\pi$) :

**Exemple** : extinction du $\mathrm{MZ}_2$ pour $\phi_2 = \pi$ ;

La fonction non linéaire $f_{NL}[v_a, v_b]$ devient, à cette condition, semblable à celle d'un MZ simple, et le déphasage $\phi_3$ n'a pas d'influence. Voici la démonstration analytique :

$$f_{NL}[v_a, v_{b0}] = \frac{P_0}{4}\Big\{\cos\psi_3\Big[\cos\psi_3 + 2\cos\Big(\psi_1 + \frac{\pi}{2}\Big)\cos\Big(\psi_1 - \frac{\pi}{2} - \psi_3\Big)\Big] + \cos^2\Big(\psi_1 - \frac{\pi}{2} - \psi_3\Big)\Big\}, \quad \text{(b1)}$$

$$= \frac{P_0}{4}\Big\{\cos\psi_3\Big[\cos\psi_3 - 2\sin\psi_1\sin(\psi_1 - \psi_3)\Big] + \sin^2(\psi_1 - \psi_3)\Big\}, \quad \text{(b2)}$$

$$= \frac{P_0}{4}\Big\{\cos\psi_3\Big[\cos\psi_3 - 2\sin\psi_1\Big(\sin\psi_1\cos\psi_3 - \cos\psi_1\sin\psi_3\Big)\Big] + \Big(\sin\psi_1\cos\psi_3 - \cos\psi_1\sin\psi_3\Big)^2\Big\}, \quad \text{(b3)}$$

$$= \frac{P_0}{4}\Big\{\cos^2\psi_3 - 2\sin^2\psi_1\cos^2\psi_3 + \underbrace{2\cos\psi_3\sin\psi_1\cos\psi_1\sin\psi_3} + \sin^2\psi_1\cos^2\psi_3 - \underbrace{2\sin\psi_1\cos\psi_3\cos\psi_1\sin\psi_3} + \cos^2\psi_1\sin^2\psi_3\Big\}, \quad \text{(b4)}$$

$$= \frac{P_0}{4}\Big\{\cos^2\psi_3 - \sin^2\psi_1\cos^2\psi_3 + \cos^2\psi_1\sin^2\psi_3\Big\}, \quad \text{(b5)}$$

$$= \frac{P_0}{4}\Big\{\cos^2\psi_3 - \big(1 - \cos^2\psi_1\big)\cos^2\psi_3 + \cos^2\psi_1\sin^2\psi_3\Big\}, \quad \text{(b6)}$$

$$= \frac{P_0}{4}\Big\{\cos^2\psi_1\Big(\cos^2\psi_3 + \sin^2\psi_3\Big)\Big\}, \quad \text{(b7)}$$

$$= \frac{P_0}{4}\cos^2\psi_1, \quad \text{(b9)}$$

En résumé :

$$\text{Si } \phi_2 = \pi \text{ (extinction du MZ}_2\text{)} \implies f_{NL}[v_a, v_{b0}] = \frac{P_0}{4}\cos^2\psi_1 \ ; \ \forall\ \phi_3 \in \mathbb{R}$$

**Remarque** : idem pour $\phi_1 = \pm\pi$

**Quelques rappels mathématiques :**

$$\cos x + \cos y = 2\cos\left(\tfrac{x+y}{2}\right)\cos\left(\tfrac{x-y}{2}\right);$$

$$\cos 2x = 2\cos^2 x - 1;$$

# Annexe B : Mise en évidence de la fréquence propre en $(T_a - T_b)^{-1}$

Le modèle dynamique de chacune des 2 variables normalisées $x_a(t)$ et $x_b(t)$ correspondant aux tensions de modulation RF électro-optique, est celui qui est typiquement adopté pour un filtre passe-bande, et ceci pour chacune des 2 boucles de contre-réaction sur le modulateur QPSK (temps de réponse court $\tau_{1i}$ du passe-bas, et temps d'intégration lent du passe-haut, $\tau_{2i} \gg \tau_{1i}$). La contre-réaction non linéaire à retard est définie par la non linéarité 2D du QPSK, et par un retard qui dépend de la boucle de contre-réaction considérée.

$$x_i(t) + [\tau_{1i} + \tau_{2i}]\frac{dx_i}{dt}(t) + \tau_{1i}\tau_{2i}\frac{d^2x_i}{dt^2}(t) = \beta_i\tau_{2i}\frac{d}{dt}\Big[f_{NL}(x_a, x_b)\Big]_{(t-T_i)},$$

où $i = a, b$ selon qu'il s'agit de la boucle (A) ou de la boucle (B). On cherche ensuite une oscillation périodique au seuil du démarrage, donc en régime quasi-linéaire, où le terme non linéaire à retard peut être approximé par sa variation linéaire, autour du point d'équilibre qui est $(x_a, x_b) = (0, 0)$ dans le cas du filtre passe-bande :

$$f_{NL}(x_a, x_b) \simeq x_a\frac{\partial f_{NL}}{\partial x_a} + x_b\frac{\partial f_{NL}}{\partial x_b} = S_a\ x_a + S_b\ x_b,$$

où $S_a$ et $S_b$ sont les sensibilités linéaires de la fonction non linéaire 2D respectivement par rapport à $x_a$ et $x_b$. Une solution harmonique de pulsation $\omega$ du système à 2 retards aura alors la forme suivante (l'hypothèse de linéarité implique que la pulsation d'oscillation sera la même pour $x_a$ et $x_b$) :

$$x_i = \delta_i e^{j\omega t},$$

En injectant ce modèle dans les équations de la dynamique de $x_a$ et $x_b$, on obtient un système à 2 équations :

$$\delta_a\left[1 + j(\tau_{2a} + \tau_{1a})\omega - \tau_{2a}\tau_{1a}\omega^2\right] = j\tau_{2a}\beta_a\left(\delta_a S_a + \delta_b S_b\right)e^{-j\omega T_a}$$
$$\delta_b\left[1 + j(\tau_{2b} + \tau_{1b})\omega - \tau_{2b}\tau_{1b}\omega^2\right] = j\tau_{2b}\beta_b\left(\delta_a S_a + \delta_b S_b\right)e^{-j\omega T_b}$$

En supposant que les 2 filtres sont quasiment identiques ($\tau_{1a} \simeq \tau_{1b}$ et $\tau_{2a} \simeq \tau_{2b}$), et en faisant le rapport des 2 équations, on met clairement en évidence une solution pour la pulsation d'oscillation $\omega$ qui est en $(T_a - T_b)^{-1}$ :

$$\frac{\delta_b}{\delta_a} = \frac{\beta_b}{\beta_a} e^{j\omega(T_a - T_b)}$$

Cette expression rapidement obtenue permet d'explique, au moins qualitativement dans un premier temps, l'origine de l'oscillation observée à la fréquence $(T_a - T_b)^{-1}$ lors de la bifurcation de Hopf.

# Annexe C : Extrema de la fonction non linéaire

**Théorème : Extréma des fonctions à deux variables [125, 126]**

Soit une fonction $f : \mathbb{R}^2 \to \mathbb{R}$, de classe $C^2$. On suppose que les dérivées partielles secondes de $f(x, y)$ sont continues. Un point $A(x_0, y_0)$ est un extrémum de $f(x, y)$, c'est-à-dire que $A(x_0, y_0)$ est un point critique si :

1. au point $A(x_0, y_0)$, les dérivées $\dfrac{\partial}{\partial x} f(x, y)$ et $\dfrac{\partial}{\partial y} f(x, y)$ sont nulles.

2. En utilisant les notations de Monge :

$$r = \frac{\partial^2}{\partial x^2} f(x, y) \quad ; \quad s = \frac{\partial^2}{\partial x \partial y} f(x, y) \quad ; \quad t = \frac{\partial^2}{\partial y^2} f(x, y)$$

   - si $s^2 - rt < 0$ et $r > 0$ : alors $f(x, y)$ admet un minimum local en $A(x_0, y_0)$ ;
   - si $s^2 - rt < 0$ et $r < 0$ : alors $f(x, y)$ admet un maximum local en $A(x_0, y_0)$ ;
   - si $s^2 - rt > 0$ : alors $f(x, y)$ admet un point selle (ou col) en en $A(x_0, y_0)$ ;
   - si $s^2 - rt = 0$ : alors on ne peut rien dire sur $A(x_0, y_0)$, le test n'est pas concluant, c'est-à dire $f(x, y)$ peut avoir un maximum local, minimum local ou même un point col.

**Application à la fonction non linéaire du modulateur QPSK**

Nous rappelons ici l'expression analytique de la fonction non linéaire du générateur de chaos, donnée par la relation (2.15).

$$f_{NL}[v_a, v_b](t) = \frac{P_0}{4} \Big\{ \cos(\psi_3) \Big[ \cos(\psi_3) + 2\cos\big(\psi_1 + \psi_2\big) \cos\big(\psi_2 + \psi_3 - \psi_1\big) \Big] + \cos^2\big(\psi_2 + \psi_3 - \psi_1\big) \Big\} \quad (14)$$

avec :

$$\psi_1 = \frac{\varphi_1(t)}{2} \; ; \qquad \psi_2 = \frac{\varphi_2(t)}{2} \; ; \qquad \psi_3 = \frac{\phi_3}{2} \; ;$$

et :

$$\begin{cases} \phi_m = \pi \cdot \dfrac{V_{DC_m}}{V_{\pi DC_m}} \; ; \qquad (m = 1,\ 2,\ 3) & \text{(15a)} \\ \varphi_{1,2}(t) = \pi \cdot \dfrac{v_{a,b}(t)}{V_{\pi RF_{1,2}}} + \phi_{1,2} & \text{(15b)} \end{cases}$$

**Remarque :**

La non linéarité – relation (14) – est en fonction des tensions $v_a(t)$ et $v_b(t)$, mais par souci de simplification des écritures, nous la considérons en fonction de $\psi_1$ et de $\psi_2$, avec en plus $P_0 = 1$.

$$f_{NL}[\psi_1, \psi_2] = \underbrace{\frac{1}{4}\cos^2(\psi_3)}_{X} + \underbrace{\frac{1}{2}\cos(\psi_3)\cos\big(\psi_1 + \psi_2\big)\cos\big(\psi_2 + \psi_3 - \psi_1\big)}_{Y} + \underbrace{\frac{1}{4}\cos^2\big(\psi_2 + \psi_3 - \psi_1\big)}_{Z} \qquad (16)$$

On constate que : $f_{NL}[\psi_1 + \pi, \psi_2 + \pi] = f_{NL}[\psi_1, \psi_2] \Rightarrow$ la fonction $f_{NL}[\psi_1, \psi_2]$ est périodique, de période $2\pi$. Par conséquent, l'intervalle de l'étude de la fonction sera réduit à une demi-période, soit par exemple l'intervalle $[-\pi/2, \pi/2]$.

**Recherche des points critiques :**

Nous calculons d'abord les expressions des dérivées partielles premières de la fonction non linéaire – relation (14) – correspondant à la condition 1 du théorème :

$$\begin{cases} \dfrac{\partial f_{NL}}{\partial v_a}(v_a, v_b) = 0 \;\Leftrightarrow\; \dfrac{\partial f_{NL}}{\partial \psi_1}(\psi_1, \psi_2) \cdot \dfrac{\partial \psi_1}{\partial v_a} = \dfrac{\partial f_{NL}}{\partial \psi_1}(\psi_1, \psi_2) = 0 \quad ; \quad \text{car : } \dfrac{\partial \psi_1}{\partial v_a} = \dfrac{\pi}{2V_{piRF1}} & \text{(17a)} \\ \dfrac{\partial f_{NL}}{\partial v_b}(v_a, v_b) = 0 \;\Leftrightarrow\; \dfrac{\partial f_{NL}}{\partial \psi_2}(\psi_1, \psi_2) \cdot \dfrac{\partial \psi_2}{\partial v_b} = \dfrac{\partial f_{NL}}{\partial \psi_1}(\psi_1, \psi_2) = 0 \quad ; \quad \text{car : } \dfrac{\partial \psi_2}{\partial v_b} = \dfrac{\pi}{2V_{piRF2}} & \text{(17b)} \end{cases}$$

♦ Calcul de $\dfrac{\partial f_{NL}}{\partial \psi_1}(\psi_1, \psi_2)$ à partir de (16) :

$$\begin{cases} \dfrac{\partial X}{\partial \psi_1} = 0 & \text{(18a)} \\ \dfrac{\partial Y}{\partial \psi_1} = \dfrac{1}{2}\cos(\psi_3)\left[\cos(\psi_1 + \psi_2)\sin(\psi_2 - \psi_1 + \psi_3) - \sin(\psi_1 + \psi_2)\cos(\psi_2 - \psi_1 + \psi_3)\right] & \text{(18b)} \\ \dfrac{\partial Z}{\partial \psi_1} = \dfrac{1}{2}\cos(\psi_2 - \psi_1 + \psi_3)\sin(\psi_2 - \psi_1 + \psi_3) & \text{(18c)} \end{cases}$$

Avec de simples arrangements[11] trigonométriques, ce système d'équations peut se ré-

[11] $\sin(a - b) = \sin a \cos b - \cos a \sin b$ ; $\quad \cos a \sin a = \frac{1}{2}\sin(2a)$ ;

écrire sous la forme :

$$\begin{cases} \dfrac{\partial X}{\partial \psi_1} = 0 & \text{(19a)} \\ \dfrac{\partial Y}{\partial \psi_1} = -\dfrac{1}{2}\cos(\psi_3)\sin(2\psi_1 - \psi_3) & \text{(19b)} \\ \dfrac{\partial Z}{\partial \psi_1} = \dfrac{1}{4}\sin(2\psi_2 - 2\psi_1 + 2\psi_3) & \text{(19c)} \end{cases}$$

d'où la dérivée partielle première de la non linéarité par rapport à $\psi_1$ :

$$\frac{\partial f_{NL}}{\partial \psi_1}(\psi_1, \psi_2) = -\cos(\psi_3)\sin(2\psi_1 - \psi_3) + \frac{1}{2}\sin(2\psi_2 - 2\psi_1 + 2\psi_3) = 0 \qquad (20)$$

♦ Calcul de $\dfrac{\partial f_{NL}}{\partial \psi_2}(\psi_1, \psi_2)$ à partir de (16) :

$$\begin{cases} \dfrac{\partial X}{\partial \psi_2} = 0 & \text{(21a)} \\ \dfrac{\partial Y}{\partial \psi_2} = -\dfrac{1}{2}\cos(\psi_3)\sin(2\psi_2 + \psi_3) & \text{(21b)} \\ \dfrac{\partial Z}{\partial \psi_2} = -\dfrac{1}{4}\sin(2\psi_2 - 2\psi_1 + 2\psi_3) & \text{(21c)} \end{cases}$$

donc la dérivée partielle première de la non linéarité par rapport à $\psi_2$ est :

$$\frac{\partial f_{NL}}{\partial \psi_2}(\psi_1, \psi_2) = -\cos(\psi_3)\sin(2\psi_2 + \psi_3) - \frac{1}{2}\sin(2\psi_2 - 2\psi_1 + 2\psi_3) = 0 \qquad (22)$$

La recherche des points critiques de $f_{NL}(\psi_1, \psi_2)$ revient donc à résoudre le système des deux équations (20) et (22). Cette résolution peut se faire, par exemple, en effectuant la somme de ces deux équations. Nous obtenons dans ce cas l'équation suivante :

$$\cos(\psi_3)\big[\sin(2\psi_1 - \psi_3) + \sin(2\psi_2 + \psi_3)\big] = 0 \qquad (23)$$

qui peut aussi se simplifier – équation (24) – en la réécrivant sous la forme d'un produit[12] de trois termes.

$$\cos(\psi_3)\sin(\psi_1 + \psi_2)\cos(\psi_1 - \psi_2 - \psi_3) = 0 \qquad (24)$$

Il suffit maintenant de trouver les solutions de l'équation (24) pour localiser les points critiques de $f_{NL}(\psi_1, \psi_2)$. Dans l'intervalle $[-\pi/2, \pi/2]$, ces solutions sont données par :

[12] Nous avons utilisé la relation : $\sin a + \sin b = 2\ \sin(\frac{a+b}{2})\cos(\frac{a-b}{2})$

$$\begin{cases} \psi_1 + \psi_2 = 0 & (25a) \\ \psi_1 - \psi_2 - \psi_3 = \pm\dfrac{\pi}{2} & (25b) \\ \psi_3 = \pm\dfrac{\pi}{2} & (25c) \end{cases}$$

Dans ce qui suit, nous allons étudier les solutions (25a) et (25b), puis nous analyserons le type de point critique obtenu (point min, max ou col). Enfin, nous donnerons un exemple numérique d'application.

**1er cas, la solution (25a) :** $\psi_1 + \psi_2 = 0 \;\Rightarrow\; \psi_1 = -\psi_2$ ;

En remplaçant $\psi_1$ dans l'équation (22), on obtient :

$$\sin(2\psi_2+\psi_3)\,[\cos(\psi_3)+\cos(2\psi_2+\psi_3)] = 0 \Rightarrow \begin{cases} \sin(2\psi_2+\psi_3) = 0 \cdots\cdots\cdots\cdots\cdots\cdots (*) \\ \quad \text{où} \\ \cos(2\psi_2+\psi_3) = -\cos(\psi_3) \;\cdots\cdots\cdots\cdots (**) \end{cases}$$

On déduit donc :

$$(*) \Rightarrow \begin{cases} 2\psi_2+\psi_3 = \pi & \Rightarrow \psi_2 = \frac{\pi}{2} - \frac{\psi_3}{2} \; ; & \longrightarrow a_1 \\ 2\psi_2+\psi_3 = 0 & \Rightarrow \psi_2 = -\frac{\psi_3}{2} \; ; & \longrightarrow a_2 \\ 2\psi_2+\psi_3 = -\pi & \Rightarrow \psi_2 = -\frac{\pi}{2} - \frac{\psi_3}{2} \; ; & \longrightarrow a_3 \end{cases}$$

$$(**) \Rightarrow \begin{cases} 2\psi_2+\psi_3 = \arccos(-\cos(\psi_3)) \; ; & \longrightarrow a_4 \\ 2\psi_2+\psi_3 = -\arccos(-\cos(\psi_3)) \; ; & \longrightarrow a_5 \end{cases}$$

les points critiques $a_1$, $a_2$, $a_3$, $a_4$ et $a_5$ (voir le tableau 2 pour les coordonnées de chaque point).

**2ieme cas, la solution (25b) :** $\psi_1 - \psi_2 - \psi_3 = \pm\frac{\pi}{2} \;\Rightarrow\; \psi_1 = \pm\frac{\pi}{2} + \psi_2 + \psi_3$ ;

En remplaçant $\psi_1$ dans l'équation (22), on obtient :

$$-\cos(\psi_3)\sin(2\psi_2+\psi_3) = 0 \Rightarrow \begin{cases} 2\psi_2+\psi_3 = 0 \; ; & \longrightarrow a_6 \\ 2\psi_2+\psi_3 = \pi \; ; & \longrightarrow a_7 \end{cases}$$

et en remplaçant $\psi_2$ dans l'équation (20), on obtient :

$$-\cos(\psi_3)\sin(2\psi_1-\psi_3) = 0 \Rightarrow \begin{cases} 2\psi_1-\psi_3 = 0 \; ; & \longrightarrow a_8 \\ 2\psi_1-\psi_3 = \pi \; ; & \longrightarrow a_9 \end{cases}$$

**3ieme cas, la solution (25c) :** Cette solution est un cas particulier des solutions précédentes (elles dépendent toutes de $\psi_3$ ; voir le tableau 2).

### Détermination du type de point critique

Les expressions des notations de Monge ($r$, $s$, $t$) sont calculés selon la condition 2 du théorème de recherche d'extréma. Leur expressions sont données par :

$$\begin{cases} r = \dfrac{\partial^2 f_{NL}}{\partial \psi_1^2}(\psi_1, \psi_2) = -\cos(\psi_3)\cos(2\psi_1 - \psi_3) - \dfrac{1}{2}\cos(2\psi_2 - 2\psi_1 + 2\psi_3); & \text{(26a)} \\ s = \dfrac{\partial^2 f_{NL}}{\partial \psi_1 \partial \psi_2}(\psi_1, \psi_2) = \dfrac{1}{2}\cos(2\psi_2 - 2\psi_1 + 2\psi_3); & \text{(26b)} \\ t = \dfrac{\partial^2 f_{NL}}{\partial \psi_2^2}(\psi_1, \psi_2) = -\cos(\psi_3)\cos(2\psi_2 + \psi_3) - \dfrac{1}{2}\cos(2\psi_2 - 2\psi_1 + 2\psi_3); & \text{(26c)} \end{cases}$$

***Exemple*** : pour $\psi_3 = \frac{\pi}{5}$

| **Point critique** | $s^2 - r \cdot t$ | $r$ | **Type du point** |
|---|---|---|---|
| $a_1 \left(-\frac{\pi}{2} + \frac{\psi_3}{2}, \frac{\pi}{2} - \frac{\psi_3}{2}\right)$ | 0,1 | | col |
| $a_2 \left(\frac{\psi_3}{2}, -\frac{\psi_3}{2}\right)$ | -1,4 | -1,3 | max |
| $a_3 \left(\frac{\pi}{2} + \frac{\psi_3}{2}, -\frac{\pi}{2} - \frac{\psi_3}{2}\right)$ | 0,1 | | col |
| $a_4 \left(-\frac{\arccos(-\cos(\psi_3))}{2} + \frac{\psi_3}{2}, \frac{\arccos(-\cos(\psi_3))}{2} - \frac{\psi_3}{2}\right)$ | -0,2 | 0.5 | min |
| $a_5 \left(\frac{\arccos(-\cos(\psi_3))}{2} + \frac{\psi_3}{2}, -\frac{\arccos(-\cos(\psi_3))}{2} - \frac{\psi_3}{2}\right)$ | -0,2 | 0.5 | min |
| $a_6 \left(\frac{\pi}{2} + \frac{\psi_3}{2}, -\frac{\psi_3}{2}\right)$ | 0,6 | | col |
| $a_7 \left(-\frac{\pi}{2} + \frac{\psi_3}{2}, -\frac{\psi_3}{2}\right)$ | 0,6 | | col |
| $a_8 \left(\frac{\psi_3}{2}, -\frac{\pi}{2} - \frac{\psi_3}{2}\right)$ | 0,6 | | col |
| $a_9 \left(\frac{\psi_3}{2}, \frac{\pi}{2} - \frac{\psi_3}{2}\right)$ | 0,6 | | col |

Table 2 – *Points critiques de la fonction non linéaire.*

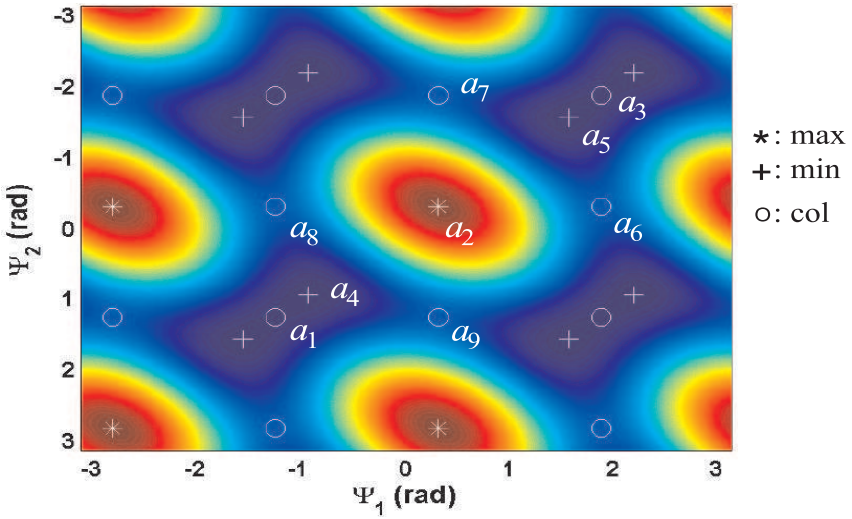



Figure 37 – *Exemple de localisation des points critiques* ($\psi_3 = \frac{\pi}{5}$).

# Bibliographie


[1] C.H. Bennet and G. Brassard. *Quantum Cryptography : Public Key Distribution and Coin Tossing. In Proc. of IEEE International Conference on Computers, Systems, and Signal Processing*, pages :175–179, 1984.

[2] L. M. Pecora and T. L. Carroll. *Synchronization in chaotic systems. Phys. Rev. Lett*, 64(8) :821–824, 1990.

[3] H. Poincaré. *Sciences et méthodes.* Ernest Flamarion édition, 1908.

[4] J. Gleick. *La théorie du Chaos : vers une Nouvelle Science.* Flamarmarion éditition, 1999.

[5] P. Bergé, Y. Pomeau, and C. Vidal. *L'ordre dans le chaos : vers une approche déterministe de la turbulence.* Ed. Hermann, 1988.

[6] J. B. Cuenot. *Système optoélectronique de communication sécurisé par chaos en longueur d'onde.* PhD thesis, Université de Franche-Comté, 2002.

[7] X. Bavard. *Numérisation du chaos et applications aux systèmes de communication sécurisés par chaos en longueur d'onde.* PhD thesis, Université de Franche-Comté, 2004.

[8] E. N. Lorenz. *Deterministic nonperiodic flow. J. Atmospheric Sci*, 20 :130–141, 1963.

[9] H. K. Khalil. *Nonlinear Systems.* Prentice Hall, 1996.

[10] I. Prigogine. *Les lois du chaos.* Edition Flammarion, 2008.

[11] A. Dahan Dalmedico, J.-L. Chabert, and K. Chemla. *Chaos et déterminisme.* Edition du Seuil, 1992.

[12] D. Ruelle and F. Takens. *On the nature of turbulence. Commun. Math. Phys.*, 20 :167–192, 1971.

[13] L. Larger. *Cryptage de signaux par chaos en longueur d'onde.* PhD thesis, Université de Franche-Comté, 1997.

[14] H. Kantz and T. Schreiber. *Nonlinear time series analysis.* Ed. Cambridge University Press, 2000.

[15] S. Roman. *Coding and information theory.* Springer, 1992.

[16] P. Manneville. *Structure dissipatives, chaos et turbulence.* Collection Aléa-Saclay, 1991.

[17] R. M. May. *Simple mathematical models with very complicated dynamics. Nature*, 261 :459 – 467, 1976.

[18] E. R. Hunt. *Stabilizing high-period orbits in a chaotic system : The diode resonator. Phys. Rev. Lett*, 67(15) :1953–1955, 1991.

[19] T. Matsumoto, L. O. Chua, and M. Komuro. *Birth and death of the double scroll. Physica D : Nonlinear Phenomena*, 24(Issues 1-3) :97–124, 1987.

[20] M. Hasler. *Engineering Chaos for Encryption and Broadband Communication. Philosophical Transactions of the Royal Society*, 353(1701) :115–126, 1995.

[21] F. A. Hopf, D. L. Kaplan, H. M. Gibbs, and R. L. Shoemaker. *Bifurcations to chaos in optical bistability. Phys. Rev. A*, 25(4) :2172–2182, 1982.

[22] K. Ikeda and O. Akimoto. *Instability Leading to Periodic and Chaotic Self-Pulsations in a Bistable Optical Cavity. Phys. Rev. Lett.*, 48(9) :617–620, 1982.

[23] Q. Alfio, S. Riccardo, and S. Fausto. *Méthodes Numériques : Algorithmes, analyse et applications.* Ed. Springer, 2007.

[24] R. Hegger, M. J. Bünner, H. Kantz, and A. Giaquinta. *Identifying and Modeling Delay Feedback Systems. Phys. Rev. Lett.*, 81(3) :558–561, 1998.

[25] M. Schatzman. *Analyse numérique : une approche mathématique.* Ed. Dunod, 2001.

[26] C. Le Bris. *Systèmes multi-échelles.* Edition Springer, 2005.

[27] M. T. Darvishia, F. Khanib, and A. A. Solimanc. *The numerical simulation for stiff systems of ordinary differential equations. Computers and Mathematics with Applications*, 54(7-8) :1055–1063, 2007.

[28] K. Ikeda. *Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system. Optics Communications*, 30(2) :257–261, 1979.

[29] T. Erneux, L. Larger, M.W. Lee, and J.-P. Goedgebuer. *Ikeda Hopf bifurcation revisited. Physica D*, 194 :49Ũ64, 2004.

[30] H. Nakatsuka, S. Asaka, H. Itoh, K. Ikeda, and M. Matsuoka. *Observation of Bifurcation to Chaos in an All-Optical Bistable System. Phys. Rev. Lett*, 50(2) :109–112, 1983.

[31] H. M. Gibbs, F. A. Hopf, D. L. Kaplan, and R. L. Shoemaker. *Observation of Chaos in Optical Bistability. Phys. Rev. Lett.*, 46(7) :474–479, 1981.

[32] A. Neyer and E. Voges. *Dynamics of electrooptic bistable devices with delayed feedback. IEEE J. Quantum Electronics*, 18(12) :2009–2015, 1982.

[33] R. Vallée and C. Delisle. *Route to chaos in an acousto-optic bistable device . Physical Review A*, 31(4) :2390–2396, 1985.

[34] P. Celka. *Chaotic synchronization and modulation of nonlinear time-delayed feedback optical systems. IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 42(8) :455–463, 1995.

[35] L. Larger, J.-P. Goedgebuer, and J.-M. Merolla. *Chaotic Oscillator in Wavelength : a new setup for investigating differentiel difference equations describing nonlineair dynamics. IEEE J. of Quantum Electronics*, 34(34) :594–601, 1998.

[36] K. Ikeda and M. Mizuno. *Modeling of nonlinear Fabry-Perot resonators by difference-differential equations. IEEE J. Quantum Electronics*, 21(9) :1429–1434, 1985.

[37] Y. Liu and J. Ohtsubo. *Chaos in an active interferometer. J. Opt. Soc. Am. B*, 9(2) :261–265, 1992.

[38] T. Heil, J. Mulet, I. Fischer, C. R. Mirasso, M. Peil, P. Colet, and W. Elsä$\beta$er. *ON/OFF Phase Shift Keying for Chaos-Encrypted Communication Using External-Cavity Semiconductor Lasers. IEEE J. Quantum Electronics*, 38(9) :1162–1170, 2002.

[39] J. Mork, B. Tromborg, and J. Mark. *Chaos in semiconductor lasers with optical feedback : Theory and experiment. IEEE J. of Quantum Electronics*, 28(1) :93–108, 1992.

[40] S. J. 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 Electronics*, 37(3) :329–336, 2001.

[41] A. T. Ryan, G. P. Agrawal, G. R. Gray, and E. C. Cage. *Optical feedback−induced chaos and its control in multimode semiconductor lasers. IEEE J. Quantum Electron*, 30(3) :668–679, 1994.

[42] N. Kikuchi, Y. Liu, and J. Ohtsubo. *Chaos control and noise suppression in external-cavity semiconductor lasers. IEEE J. Quantum Electronics*, 33(1) :56–65, 1997.

[43] I. Fischer, O. Hess, W. Elsä$\beta$er, and E. Göbel. *High-Dimensional Chaotic Dynamics of an External Cavity Semiconductor Laser. Phys. Rev. Lett.*, 73(16) :2188–2191, 1994.

[44] S. Anoovazzi-Lodi, S. Donati, and A. Scirè. *Synchronisation of chaotic injected-laser systems and its amplification to optical cryptography. IEEE J. Quantum Electron*, 32(6) :953–959, 1996.

[45] A. M. Kul'minskii, V. N Severikov, and A. P. Voitovich. *Polarization chaos in a vector nonautonomous class-A laser. J. of Optics B : Quantum and Semiclassical*, 1(2) :294–298, 1999.

[46] P. Glorieux and A. Le Floch. *Nonlinear polarization dynamics in anisotropic lasers. Optics Communications*, 79(3-4) :229–234, 1990.

[47] Y. Hong, P. S. Spencer, S. Bandyopadhyay, P. Rees, and K. A. Shore. *Polarisation-resolved chaos and instabilities in a vertical cavity surface emitting laser subject to optical injection. Optics Communications*, 216(1-3) :185–189, 2003.

[48] M. Sciamanna, A. Valle, P. Mégret, M. Blondel, and K. Panajotov. *Nonlinear polarization dynamics in directly modulated vertical-cavity surface-emitting lasers. Phys. Rev. E*, 68(1) :016207(1–4), 2003.

[49] A. Argyris, M. Hamacher, K. E. Chlouverakis, A. Bogris, and D. Syvridis. *Photonic Integrated Device for Chaos Applications in Communications. Phys. Rev. Lett.*, 100(19) :194101(1–4), 2008.

[50] K. E. Chlouverakis, A. Argyris, A. Bogris, and D. Syvridis. *Hurst exponents and cyclic scenarios in a photonic integrated circuit. Phys. Rev. E*, 78(6) :066215(1–5), 2008.

[51] L. Larger, J.-P. Goedgebuer, and F. Delorme. *Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator. Phys. Rev. E*, 57(6) :6618–6624, 1998.

[52] P. Levy. *Télécommunications cryptées par chaos*. PhD thesis, Université de Franche-Comté, 2004.

[53] N. Gastaud. *Système de communication haut débit sécurisé par chaos en intensité*. PhD thesis, Université de Franche-Comté, 2006.

[54] M. W. Lee. *Etude des comportements chaotiques en modulation de cohérence et application à la cryptographie*. PhD thesis, Université de Franche-Comté, 2002.

[55] J.-P. Goedgebuer and A. Hamel. *Coherence multiplexing using a parallel array of electrooptic modulators and multimode semiconductor lasers. IEEE J. Quantum Electronics*, 23(12) :2224–2237, 1987.

[56] L. Larger, M. W. Lee, J.-P. Goedgebuer, W. Elflein, and T. Erneux. *Chaos in coherence modulation : bifurcations of an oscillator generating optical delay fluctuations. J. Opt. Soc. Am. B*, 18(8) :1063–1068, 2001.

[57] A. Pallavisini. *Système d'interférences radiofréquences pour la cryptographie par chaos appliquée aux transmissions hertziennes.* PhD thesis, Université de Franche-Comté, 2007.

[58] A. Pallavisini, L. Larger, V. S. Udaltsov, J.-M. Merolla, R. Quéré, N. Butterlin, and J.-P. Goedgebuer. *RF-Interferences generate chaotic GHz FM-Carrier for communications. IEEE journal of quantum electronics*, 43(5) :426–433, 2007.

[59] E. Genin. *Etude et réalisation d'un générateur de chaos optoélectronique sur la phase pour les télécommunication cryptées haut-débit.* PhD thesis, Université de Franche-Comté, 2003.

[60] E. Genin, L. Larger, J.-P. Goedgebuer, M. W. Lee, R. Ferrière, and X. Bavard. *Chaotic Oscillations of the Optical Phase for Multigigahertz-Bandwidth Secure Communications. IEEE J. Quantum Electronics*, 40(3) :294–298, 2004.

[61] L. Larger, V. S. Udaltsov, S. Poinsot, and E. Genin. *Optoelectronic phase chaos generator for secure communication. J. Optical Technology (A Translation of Opticheskii Zhurnal)*, 72(5) :378–382, 2005.

[62] 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*, 80(2) :026207(1–9), 2009.

[63] J.-P. Goedgebuer, M. Li, and H. Porte. *Demonstration of bistability and multistability in wavelength with a hybrid acoustooptic device. IEEE J. of Quantum Electronics*, 23(2) :153–157, 1987.

[64] J. Duvernoy, J.-P. Goedgebuer, and H. Porte. *Bistabilité, multistabilité et chaos en longueur d'onde. Annales des Telecommunications*, 42(5-6) :315–323, 1987.

[65] J.-P. Goedgebuer, L. Larger, H.i Porte, and F. Delorme. *Chaos in wavelength with a feedback tunable laser diode. Phys. Rev. E*, 57(3) :2795–2798, 1998.

[66] N. Gastaud, S. Poinsot, L. Larger, J.-M. Merolla, M. Hanna, J.-P. Goedgebuer, and F. Malassenet. *Electro-optical chaos for multi-10 Gbit/s optical transmissions. Electronics Letters*, 40(14) :898–899, 2004.

[67] J. P. Goedgebuer, P. Levy, and L. Larger. *Laser cryptography by optical chaos. Proceedings of SPIE - The International Society for Optical Engineering*, 5135 :14–20, 2002.

[68] J.-P. Goedgebuer, P. Levy, L. Larger, C.-C. Chen, and W.T. Rhodes. *Optical communication with synchronized hyperchaos generated electrooptically. IEEE J. Quantum Electronics*, 38(9) :1178–1183, 2002.

[69] 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*, 80(10) :2249–2252, 1998.

[70] G. D. VanWiggeren and R. Roy. *Communicating with chaotic lasers. Science*, 279(3) :1198–1200, 1998.

[71] S. Tang, H. F. Chen, S. K. Hwang, and J. M. Liu. *Message encoding and decoding through chaos modulation in chaotic optical communications. IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, 49(2) :163–169, 2002.

[72] 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*, 86(9) :1892–1895, 2001.

[73] O. Morgil and M. Feki. *A chaotic masking scheme by using synchronized chaotic systems. Phys. Lett. A*, 251 :169– I76, 1999.

[74] V. I. Ponomarenko and M. D. Prokhorov. *Extracting information masked by the chaotic signal of a time-delay system. Phys. Rev. E*, 66 :026215 (1–7), 2002.

[75] S. Sivaprakasam and K. A. Shore. *Signal masking for chaotic optical communication uing external cavity diode lasers. Opt. Lett*, 24(17) :1200–1202, 1999.

[76] K. M. Cuomo and A. V. Oppenhein. *Circuit implementation of synchronised chaos with applications to communications. Phys. Rev. Lett*, 71(1) :65–68, 1993.

[77] J. B. Cuenot, L. Larger, J.-P. Geodgebuer, and W. T. Rhodes. *Chaos shift keying with an optoelectronic encryption system using chaos in wavelength. IEEE J. of Quantum Electronics*, 37(7) :849–855, 2001.

[78] 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 Transactions on Circuits and Systems II : Analog and Digital Signal Processing*, 40(10) :634–642, 1993.

[79] T. Yang. *A Survey of Chaotic Secure Communication Systems. International Journal of Computational Cognition*, 2(2) :81–130, 2004.

[80] F. C. M. Lau, M. M. Yip, C. K. Tse, and S. F. Hau. *A multiple-access technique for differential chaos-shift keying. IEEE Trans. Circuits and Systems I : Fundamental Theory and Applications*, 49(1) :96–104, 2002.

[81] G. Kolumbán, M.P. Kennedy, Z. Jako, and G. Kis. *Chaotic communications with correlator receivers : theory and performance limits. Proceedings of the IEEE*, 90(5) :711–732, 2002.

[82] G. Kolumbán, G. Kis, Z. Jákó, and M. P. Kennedy. *FM-DCSK : A robust modulation scheme for chaotic communications. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, E81-A(9) :1798–1802, 1998.

[83] R. Noé, U. Rückert, Y. Achiam, F. J. Tegude, and H. Porte. *European "synQPSK" Project : Toward Synchronous Optical Quadrature Phase Shift Keying with DFB Lasers.* In *OSA, Amplifiers and Their Applications/COTA, CThC*4, 2006.

[84] M.-C. Oh, H. Zhang, C. Zhang, H. Erlig, Y. Chang, B. Tsap, D. Chang, A. Szep, W. H. Steier, H. R. Fetterman, and L. R. Dalton. *Recent Advances in Electrooptic Polymer Modulators Incorporating Highly Nonlinear Chromophore. IEEE J.on Selected Topics in Quant. Electronics*, 7(5) :826–835, 2001.

[85] S. Khalfallah, P. Dubreuil, R. Legros, C. Fontaine, A. Munoz-Yague, B. Beche, H. Porte, R. Warno, and M. Karpierz. *Highly unbalanced GaAlAs-GaAs integrated Mach-Zehnder interferometer for coherence modulation at* 1.3 $\mu m$. *Optics Communications*, 167(1) :67–76, 1999.

[86] N. Courjal, H. Porte, J. Hauden, P. Mollier, and N. Grossard. *Modeling and Optimization of Low Chirp $LiNbO_3$ Mach-Zehnder Modulators With an Inverted Ferroelectric Domain Section. J. Lightwave Technology*, 22(5) :1338–1343, 2004.

[87] M. Bouvrot. *Micro Modulateurs de lumière à base de cristaux électro-optiques à coefficients géants.* PhD thesis, Université de Franche-Comté, 2010.

[88] T. G. Nguyen, A. Mitchell, and Y. S. Visagathilagar. *Investigation of Resonantly Enhanced Modulators on $LiNbO_3$ Using FEM and Numerical Optimization Technique. J. of Lightwave Technology*, 22(2) :526–533, 2004.

[89] S. Oikawa, F. Yamamoto, J. Ichikawa, S. Kurimura, and K. Kitamura. *Zero-Chirp Broadband Z-Cut Ti :$LiNbO_3$ Optical Modulator Using Polarization Reversal and Branch Electrode. J. of Lightwave Technology*, 23(9) :2756–2760, 2005.

[90] N. Courjal. *Modulateur $LiNbO_3$ à faible chirp par inversion de domaine ferroélectrique.* PhD thesis, Université de Franche-Comté, 2002.

[91] J. Kondo, A. Kondo, K. Aoki, M. Imaeda, T. Mori, Y. Mizuno, S. Takatsuji, Y. Kozuka, O. Mitomi, and M. Minakata. 40-*Gb/s X-Cut $LiNbO_3$ Optical modulator with two-step back-slot structure. J. of Lightwave Technology*, 20(12) :2110–2114, 2002.

[92] K. Noguchi, O. Mitomi, and H. Miyazawa. *Millimeter-Wave Ti :$LiNbO_3$ Optical Modulators. J. of Lightwave Technology*, 16(4) :615–619, 1998.

[93] E. Wooten, K. M. Kissa, A. Yi-Yan, E. J. Murphy, D. A. Lafaw, P. F. Hallemeier, D. Maack, D. V. Attanasio, D. J. Fritz, G. J. McBrien, and D. E. Bossi. *A Review of Lithium Niobate Modulators for Fiber-Optic Communications Systems. IEEE J. of Selected Topics in Quantum Electronics*, 6(1) :69–82, 2000.

[94] L. Terlevich, S. Balsamo, S. Pensa, M. Pirola, and G. G. Senior. *Design and Characterization of a 10-Gb/s Dual-Drive Z-Cut Ti :$LiNbO_3$ Electrooptical Modulator. J. of Lightwave Technology*, 24(6) :2355–2361, 2006.

[95] R. Valois. *Contribution de l'analyse électromagnétique et outils associés à la conception de modules de communications millimétriques et optoélectroniques.* PhD thesis, Université de Limoges, 2005.

[96] T. Pfau, S. Hoffmann, R. Peveling, S. Ibrahim, O. Adamczyk, M. Porrmann, S. Bhandare, R. Noé, and Y. Achiam. *Synchronous QPSK transmission at 1.6 Gbit/s with standard DFB lasers and real-time digital receiver. Eectronics Letters*, 42(20) :1175–1176, 2006.

[97] N. Grossard, J. Hauden, H. Porte, P. Mollier, S.K. Ibrahim, and R. Noe. *Low chirp QPSK modulator integrated in poled Z-cut $LiNbO_3$ substrate for $2\times$MultiGb/s transmission.* 33*rd European Conference and Exhibition on Optical Communication - ECOC*, pages 1035–1036, Berlin 17-19, 2007.

[98] R. Noé, T. Pfau, O. Adamczyk, R. Peveling, V. Herath, S. Hoffmann, M. Porrmann, S. K. Ibrahim, and S. Bhandare. *Real-time Digital Carrier & Data Recovery for a Synchronous Optical Quadrature Phase Shift Keying Transmission System.* In *Proc. IMS*2007*, TH*2*E*-01, 2007.

[99] T. Pfau, S. Hoffmann, O. Adamczyk, R. Peveling, V. Herath, M. Porrmann, and R. Noé. *Coherent optical communication : Towards realtime systems at 40 Gbit/s and beyond. OSA Optics Express*, 16(2) :866–872, 2008.

[100] G. Charlet, J. Renaudier, H. Mardoyan, P. Tran, O. Bertran Pardo, F. Verluise, M. Achouche, A. Boutin, F. Blache, J. Dupuy, and S. Bigo. *Transmission of* $16.4Tbit/s$ *Capacity over* $2,550km$ *Using PDM QPSK Modulation Format and Coherent Receiver. in National Fiber Optic Engineers Conference, OSA Technical Digest*, page PDP3, San Diego, 24-28 Feb, 2008.

[101] C. Laperle, B. Villeneuve, Z. Zhang, D. McGhan, H. Sun, and M. O'Sullivan. *WDM Performance and PMD Tolerance of a Coherent* 40*-Gbit/s Dual-Polarization QPSK Transceiver. J. of Lightwave Technology*, 26(1) :168–175, 2008.

[102] Y. Chembo, P. Colet, L. Larger, and N. Gastaud. *Chaotic breathers in delayed electro-opyical systems . Phys. Rev. Lett*, 95(20) :203903 (1–4), 2005.

[103] E. Darbellay. *Le temps et la forme.* Recherches et Rencontres, Publications de la Faculté des lettres de Genève, DROZ, 1998.

[104] M. Peil, M. Jacquot, Y. Chembo, L. Larger, and T. Erneux. *Routes to chaos and multiple time scale dynamics in broadband bandpass nonlinear delay electro-optic oscillators. Phys. Rev. E*, 79(2) :026208(1–15), 2009.

[105] N. H. Packard, J. P. Crutchfield, J. D. Farmer, and R. S. Shaw. *Geometry from a time series. Phys. Rev. Lett*, 45(9) :712–716, 1980.

[106] A. Locquet. *Analyse numériques de dynamiques chaotiques dans des systèmes optiques à délai : propriétés de synchronisation et extraction du déterminisme.* PhD thesis, Université de Franche-Comté, 2004.

[107] G. Millerioux, J. M. Amigo, and J. Daafouz. *A connection between chaotic and conventional cryptography. IEEE Trans. On Circuits and Systems I : Regular Papers*, 55(6) :1695–1703, 2008.

[108] N. F. Rulkov, L. S. Tsimring, and H. D. I Abarbanel. *Tracking unstable orbits in chaos us ing dissipative feedback control. Phys. Rev. E*, 50(1) :314–324, 1994.

[109] N. F. Rulkov, M. M. Sushchik, L. S. Tsimring, and H. D. Abarbanel. *Generalized synchronization of chaos in directionally coupled chaotic systems. Phys. Rev. E*, 51(2) :980–993, 1995.

[110] L. Kocarev and U. Parlitz. *General approach for chaotic synchronization with applications to communication. Phys. Rev. Lett.*, 74(25) :5028–5031, 1995.

[111] M. G. Rosenblum, A. S. Pikovsky, and J. Kurths. *Phase synchronization in driven and coupled chaotic oscillators. IEEE Trans. Circuits Syst. I*, 44(10) :874–881, 1997.

[112] A. Volkovskii. *Synchronization of chaotic systems using phase control. IEEE Trans. Circuits Syst. I*, vol. 44(10) :pp. 913–917, 1997.

[113] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares, and C.S. Zhou. *The synchronization of chaotic systems. Physics Reports*, 366 :1–101, 2002.

[114] L. M. Pecora and T. L. Carroll. *Driving systems with chaotic signals. Phys. Rev. A*, 44(4) :2374–2383, 1991.

[115] M. Nourine, L. Larger, Y.K. Chembo, K. Volyanskiy, and M. Peil. *Générateur de chaos optoélectronique à double retard pour les télécommunications optiques sécurisées à haut débits. Compte-Rendus de la* 13*ème Rencontre du Non Linéaire*, pages 127–132, 2010.

[116] Y. Chembo, 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*, 69 :056226 (1–15), 2004.

[117] E. Hecht. *Optique*. Ed. Pearson Education, 2005.

[118] L. Larger, J.-P. Geoddgebuer, and V. Udaltsov. *Ikeda-based nonlenear delayed dynamics for application to secure optical transmission systems using chaos. C. R. Physique*, 5 :669–681, 2004.

[119] M. Nourine, M. Peil, and L. Larger. *Chaos généré par une non linéarité* 2*D et une dynamique à retard. Compte-Rendus de la* 12*ème Rencontre du Non Linéaire*, pages 146–154, 2009.

[120] C. Tresser, P. Coullet, and A. Arneodo. *On the existence of hysteresis in a transition to chaos after a single bifurcation. J. Physique Lett*, 41 :243–246, 1980.

[121] A. Prasad, L. D. Iasemidis, S. Sabesan, and K. Tsakalis. *Dynamical hysteresis and spatial synchronization in coupled non-identical chaotic oscillators. Pramana - Journal of Physics*, 64(4) :513–523, 2005.

[122] F. Anstett, G. Millerioux, and G. Bloch. *Chaotic Cryptosystems : Cryptanalysis and Identifability. Chaotic Cryptosystems : Cryptanalysis and Identifiability, IEEE Trans. On Circuits and Systems I : Regular Papers*, 53(12) :2673–2680, 2006.

[123] M. Peil, L. Larger, and I. Fischer. *Versatile and robust chaos sychronization phenomena imposed by delayed shared feedback coupling. Phys. Rev. E*, 76(4) :045201(1–4), 2007.

[124] J. Hauden, N. Grossard, A. Mottet, H. Porte, B. Ftaich-Frigui, and D. Baillargeat. *Modulation DQPSK* $2\times20GB/S$ *avec un modulateur* $LiNbO_3$ *Dual électrodes (*$LiNbO_3$ *DMZ−DE). 28e Journées Nationales d'Optique Guidée (JNOG)*, pages 342–343, 2009.

[125] J. Stewart. *Analyse : concepts et contextes. Volume 2, Fonctions de plusieurs variables.* Edition : De Boeck, 2001.

[126] F. Delmer. *Fonctions de plusieurs variables et intégration.* Edition : Dunod, 1997.

[127] H. D. Abarbanel, Z. Gills, C. Liu, and R. Roy. *Nonlinear-time-series analysis of chaotic laser dynamics. Physical Review A*, 53(1) :440–453, 1996.

[128] K. T. Alligood, T. D. Sauer, and J. A. Yorke. *Chaos an introduction to dynamical systems.* Ed. Springer, 2000.

[129] 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*, 438 :343–346, 2005.

[130] P. Colet and R. Roy. *Digital communication with sychronized chaotic lasers. Opt. Lett*, 19(24) :2056–2058, 1994.

[131] 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*, 35(1) :328–339, 1987.

[132] J. D. Farmer. *Chaotic attractors of infinite-dimentional dynamical system. Physica D*, 4 :366–393, 1982.

[133] I. Fischer, Y. Liu, and P. Davis. *Synchronisation of chaotic semiconductor laser dynamics on sub-ns timescales and its potential for communication. Phys. Rev. A*, 62(1) :1–4, 2000.

[134] C.-M. Kim, K.-S. Lee, J. M. Kim, S.-O. Kwon, C.-J. Kim, and J.-M. Lee. *Route to chaos through the type I intermittency of a gain-modulated* $CO_2$ *laser caused by the discharge instability at low frequency. J. Opt. Soc. Am. B*, 10(9) :1651–1654, 1993.

[135] Lj. Kocarev, K.S. Halle, K. Eckert, L.O. Chua, and U. Parlitz. *Experimental demonstration of secure communication via chaotic synchronization. International Journal of Bifurcation and Chaos*, 2(3) :709–713, 1992.

[136] M. Le Berre, E. Ressayre, A. Tallet, and Y. Pomeau. *Dynamic system driven by a retarded force acting as colored noise. Phys. Rev. A*, 41(12) :6635–6646, 1990.

[137] M. W. Lee, L. Larger, V. Udaltsov, E. Genin, and J.-P. Goedgebuer. *Demonstration of a chaos generator with two time delays. Optics Letters*, 29(4) :325–327, 2004.

[138] M. Nazarathy, J. Berger, A. J. Ley, I. M. Levi, and Y. Kagan. *Progress in externally modulated AM CATV transmission systems. J. of Lightwave Technology*, 11(1) :82–105, 1993.

[139] U. Parlitz, L. O. Chua, L. Kocarev, K.S. Halle, and A. Shang. *Transmission of digital signals by chaotic synchronization. International Journal of Bifurcation and Chaos*, 2(4) :973–977, 1992.

[140] J.-P. Pérez. *Optique : fondements et applications.* Ed. Masson, 1996.

[141] B. Schneier. *Cryptographie appliquée : algorithmes, protocoles et codes source en C.* Ed. Wiley, 1996.

[142] D. Stinson. *Cryptographie : théorie et pratique.* Ed. International Thomson publishing, 1996.

[143] A. Uchida, S. Yochimori, M. Shinozuka, T. Ogawa, and F. Kannari. *Chaotic on-off keying for secure communications. Opt. Lett*, 26(12) :866–868, 2001.

[144] V. S. Udaltsov, L. Larger, J.-P. Goedgebuer, M. W. Lee, E. Genin, and W. T. Rhodes. *Bandpass chaotic dynamics of electronic oscillator operating with delayed nonlinear feedback. IEEE Transactions on Circuits and Systems I*, 49(7) :1006–1009, 2002.