

الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي والبحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE



MEMOIRE

Présenté pour l'obtention du **diplôme de MASTER**

En : Télécommunication

Spécialité : Photonique et Réseaux Optiques de Télécommunications

Par : LAKEHAL Ilyes

Sujet

CRYPTOSYSTÈME CHAOTIQUE BASÉ SUR UNE DIOLE LASER A RÉTROACTION

Soutenu publiquement, le 24/06/2026 , devant le jury composé de :

M MERZOUGUI Rachid

Professeur

Université de Tlemcen

Président

Mme TALEB Sarra

MCB

Université de Tlemcen

Examinatrice

M ABDELMALEK Abdelhafid

MCB

Université de Tlemcen

Encadreur

Mme SLIMANE Zohra

Professeur

Université de Tlemcen

Co-Encadrante

Année universitaire : 2025/2026

Remerciements

Je tiens tout d'abord à remercier Monsieur **ABDELMALEK abdelhafid**, Maître de conférences à l'université de Tlemcen, et Mme **SLIMANE Zohra** Professeur à l'université de Tlemcen, pour m'avoir proposé ce sujet qui m'a permis de m'initier à la recherche scientifique. Leur suivi régulier de l'évolution de mon travail, leurs conseils et leurs encouragements m'ont permis de réaliser ce mémoire dans d'excellentes conditions de travail.

J'exprime ma gratitude à Monsieur **Merzougui Rachid**, Professeur à l'université de Tlemcen, pour l'honneur qu'il me fait en présidant mon Jury, ainsi qu'à Madame **TALEB Sara**, Maître de conférences à l'université de Tlemcen, pour l'honneur qu'elle me fait en participant à ce jury.

Je les remercie sincèrement pour le temps qu'ils ont consacré à la lecture et à l'évaluation de mon travail.

Bien entendu, il me serait impossible de terminer sans adresser une pensée chaleureuse à mes parents pour leur soutien et leurs encouragements pendant de longues années, sans qui je n'aurais pu arriver à ce niveau d'étude.

Dédicace

Je dédie ce travail à mes chers parents, dont l'amour, les sacrifices et les encouragements constants ont été le fondement de ma réussite. Aucun mot ne saurait traduire la reconnaissance et le respect que je leur port. Puisse Dieu leur accorder santé, bonheur et longue vie.

À tous les membres de ma famille, pour leur présence bienveillante, leur confiance et leur soutien indéfectible tout au long de notre parcours.

Enfin, à toutes les personnes qui ont cru en moi et m'ont encouragé à avancer malgré les difficultés, j'adresse ma profonde gratitude.

Liste des acronymes

Acronyme	Signification
AES	Advanced Encryption Standard
BER	Bit Error Rate (Taux d'Erreur Binaire)
CM	Chaos Masking (Masquage Chaotique)
CPM	Chaos Phase Modulation (Modulation par Décalage de Phase Chaotique)
CSK	Chaos Shift Keying (Modulation Chaotique par Décalage)
DDE	Delay Differential Equation (Équation Différentielle à Retard)
DFB	Distributed Feedback Laser (Laser à Rétroaction Distribuée)
DSP	Digital Signal Processing (Traitement Numérique du Signal)
FFT	Fast Fourier Transform (Transformée de Fourier Rapide)
GHz	Gigahertz
IA	Intelligence Artificielle
InGaAsP	Indium Gallium Arsenide Phosphide
LD	Laser Diode (Diode Laser)
LK	Lang-Kobayashi
MZM	Mach-Zehnder Modulator (Modulateur Mach-Zehnder)
NRZ	Non Return to Zero

Acronyme	Signification
OF	Optical Feedback (Rétroaction Optique)
OFC	Optical Feedback Chaos (Chaos par Rétroaction Optique)
OIC	Optical Injection Chaos (Chaos par Injection Optique)
PD	Photodiode
PSD	Power Spectral Density (Densité Spectrale de Puissance)
RF	Radio Frequency (Radiofréquence)
RNG	Random Number Generator (Générateur de Nombres Aléatoires)
SNR	Signal-to-Noise Ratio (Rapport Signal sur Bruit)
VCSEL	Vertical Cavity Surface Emitting Laser
WDM	Wavelength Division Multiplexing
QPSK	Quadrature Phase Shift Keying
DFB	Distributed Feedback Laser (<i>Doublon présent dans votre liste</i>)
QF	Facteur de Qualité (Quality Factor)
THz	Téraherertz
GHz	Gigahertz (<i>Doublon présent dans votre liste</i>)

Table des matières

Remerciements	2
Dédicace	3
Liste des acronymes	4
Table des matières	6
Listes des figures	8
Listes des tableaux	10
Introduction générale	11

CHAPITRE I : Systèmes Dynamiques et Chaos

I-1 Introduction	15
I-2 Systèmes dynamiques	16
I-3 Systèmes Dynamiques chaotiques.....	17
I-4 L'espace de phase	19
I-4-1 Notion d'attracteur	19
I-4-2 Dimension d'Hausdorff	21
I-4-3 Exposants de Lyapunov	22
I-4-4 Bifurcation et routes vers le chaos	23
I-5 Conclusion	25

CHAPITRE II : Chiffrement par Chaos : Cryptosystèmes Chaotiques Optiques

II-1 Introduction	27
II-2 Objectifs des crypto-systèmes	27
II-3 Communications Sécurisées par chaos	29
II-3-1 Principe des communications chaotiques	29
II-3-2 Synchronisation des systèmes chaotiques	29
II-3-3 Applications des communications chaotiques (notamment optiques)	30
II-4 Techniques de chiffrement par chaos.....	31
II-4-1 Masquage chaotique (Chaos Masking)	31
II-4-2 Modulation chaotique (Chaos Shift Keying - CSK)	32
II-4-3 Modulation par décalage de phase chaotique (Chaos Phase Modulation - CPM)	32
II-4-4 Cryptographie hybride chaos-numérique	33
II-5 Chiffrement par modulation	33
II-5-1 Masquage chaotique (Chaos Masking CM).....	34
II-5-2 Modulation chaotique (Chaos Shift Keying - CSK)	34
II-5-3 Modulation par décalage de phase chaotique (Chaos Phase Modulation - CPM)	35
II-6 Applications et perspectives	35
II-7 Conclusion	36

CHAPITRE III : Dynamique Chaotique d'une Diode Laser avec Rétroaction Optique : Chiffrement-déchiffrement

III-1 Introduction	38
III-2 Techniques de génération du chaos par diode laser	38
III-2-1 Chaos par rétroaction optique externe (Optical Feedback Chaos)	39
III-2-2 Chaos par injection optique (Optical Injection Chaos)	39
III-2-3 Chaos par modulation du courant d'injection	40
III-2-4 Chaos par couplage de lasers (Coupled Lasers Chaos)	40
III-2-5 Génération du chaos par cavité externe à fibre optique	40
III-3 Chaos par Diode Laser avec rétroaction optique	41
III-3-1 Modélisation Mathématique - Équations classiques d'une diode laser à semi-conducteur	42
III-3-2 Modèle avec Rétroaction : Formulation de Lang-Kobayashi	45
III-4 Caractérisation qualitative et quantitative - Résultats de simulation	47
III-4-1 Diagramme de bifurcation	47
III-4-2 Comportement périodique (Attracteur cycle limite) pour une rétroaction $k=10^9$	48
III-4-3 Comportement périodique (Attracteur cycle limite) pour une rétroaction $k=6.10^9$	52
III-4-4 Comportement quasi-périodique (Attracteur tore) pour une rétroaction $k=10^{11}$	54
III-4-5 Comportement chaotique (Attracteur étrange) pour une rétroaction $k=10^{11}$	58
III-5 Chiffrement-déchiffrement	61
III-5-1 Procédure de chiffrement au niveau de l'émetteur	62
III-5-2 Transmission du signal chiffré	65
III-5-3 Procédure de déchiffrement au niveau du récepteur	65
III-5-4 Analyse des performances du système	66
III-6 Conclusion	67
 Conclusion Générale	 68
Bibliographie	71
Annexe	73
Résumé	77

Listes des figures

Figure I.1 Attracteur de Lorenz dans l'Espace des phases, illustrant un comportement chaotique caractéristique des systèmes dynamiques non linéaires	20
Figure I.2 Exemples d'attracteurs	20
Figure I.3 Attracteur étrange de Lorentz	21
Figure I.4 Divergence de deux trajectoires dans le plan de phase	22
Figure II.1 Principe d'une communication sécurisée par chaos	30
Figure II.2 Principe d'une communication sécurisée par chaos (masquage chaotique)	31
Figure II.3 Modulation chaotique (Chaos Shift Keying - CSK)	32
Figure II.4 Principe de la modulation par décalage de phase chaotique (CPM)	33
Figure II.5 Cryptographie hybride chaos-numérique	33
Figure III.1 Schéma de principe d'une diode laser à semi-conducteur	42
Figure III.2 Diagramme de bifurcation en fonction du paramètre de contrôle k	48
Figure III.3 Représentation temporelle de l'intensité du signal optique pour $k=10^9$	49
Figure III.4 Représentation temporelle de l'intensité (zoom 50-300 ns) pour $k=10^9$	49
Figure III.5 Représentation temporelle de l'intensité (zoom 280-300 ns) pour $k=10^9$	49
Figure III.6 Densité spectrale de puissance pour $k=10^9$	50
Figure III.7 Diagramme de phase 3D pour $k=10^9$	50
Figure III.8 Diagramme de phase 2D pour $k=10^9$	51
Figure III.9 Représentation temporelle de l'intensité pour $k=6 \cdot 10^9$	51
Figure III.10 Représentation temporelle (zoom 280-300 ns) pour $k=6 \cdot 10^9$	52
Figure III.11 Densité spectrale de puissance pour $k=6 \cdot 10^9$	53
Figure III.12 Diagramme de phase 3D pour $k=6 \cdot 10^9$	54
Figure III.13 Diagramme de phase pour $k=6 \cdot 10^9$	54
Figure III.14 Représentation temporelle de l'intensité pour $k=10^{11}$	55
Figure III.15 Représentation temporelle (zoom 280-300 ns) pour $k=10^{11}$	55
Figure III.16 Densité spectrale de puissance pour $k=10^{11}$	56
Figure III.17 Densité spectrale de puissance (zoom 20-25 GHz) pour $k=10^{11}$	56
Figure III.18 Diagramme de phase 3D pour $k=10^{11}$	57
Figure III.19 Diagramme de phase 2D pour $k=10^{11}$	57
Figure III.20 Représentation temporelle de l'intensité pour $k=7,75735 \times 10^{11}$	58
Figure III.21 Représentation temporelle (zoom 280-300 ns) pour $k=7,75735 \times 10^{11}$	58
Figure III.22 Densité spectrale de puissance pour $k=7,75735 \times 10^{11}$	59
Figure III.23 Diagramme de phase 3D (attracteur étrange) pour $k=7,75735 \times 10^{11}$	60

Figure III.24 Diagramme de phase 2D (attracteur étrange) pour $k=7,75735 \times 10^{11}$	60
Figure III.25 Schéma du chiffrement-déchiffrement réalisé sous OptiSystem	62
Figure III.26 Message d'information émis, code NRZ	63
Figure III.27 Signal optique modulé par le message émis	63
Figure III.28 Spectre du signal optique modulé par le message émis	64
Figure III.29 Signal optique chiffré	64
Figure III.30 Message reçu déchiffré, code NRZ	66

Listes des tableaux

Tableau I.1 : Les types d'attracteurs.....	20
Tableau III.1 : Comparaison des cinq méthodes (de génération du chaos par diode laser)	42
Tableau III.2 : Valeurs pratiques de α (facteur de Henry)	45
Tableau III.3 : Valeurs pratiques du délai pour une cavité externe dans l'air ($n \simeq 1$)	47
Tableau III.4 : Valeurs pratiques du délai pour une fibre optique ($n \simeq 1.5$)	48

Introduction générale

L'essor des technologies numériques et des réseaux de communication a profondément transformé les modes d'échange et de transmission de l'information. Aujourd'hui, des volumes considérables de données transitent quotidiennement à travers des infrastructures de communication de plus en plus performantes, notamment les réseaux optiques à très haut débit. Cette évolution s'accompagne toutefois d'un besoin croissant de protection des informations contre les interceptions, les manipulations malveillantes et les accès non autorisés. La sécurité des communications est ainsi devenue un enjeu majeur dans de nombreux domaines tels que les télécommunications, les réseaux informatiques, les systèmes industriels, les applications militaires et les services financiers.

Les méthodes cryptographiques conventionnelles reposent principalement sur des algorithmes mathématiques utilisant des clés secrètes ou publiques afin d'assurer la confidentialité des données. Bien que ces techniques aient démontré leur efficacité, elles sont confrontées à des défis grandissants liés à l'augmentation de la puissance de calcul des systèmes informatiques, à l'émergence de nouvelles techniques d'attaque et aux perspectives offertes par l'informatique quantique. Dans ce contexte, de nouvelles approches de sécurisation de l'information ont été explorées, parmi lesquelles figure l'utilisation des systèmes chaotiques.

La théorie du chaos, développée au cours de la seconde moitié du 20^{ème} siècle, a révélé l'existence de comportements complexes dans certains systèmes dynamiques non linéaires. Ces systèmes présentent des propriétés remarquables telles que la sensibilité extrême aux conditions initiales, l'imprévisibilité à long terme, l'apparence aléatoire des signaux générés ainsi qu'une large richesse spectrale. Ces caractéristiques sont particulièrement intéressantes pour les applications cryptographiques puisqu'elles permettent de masquer efficacement une information au sein d'un signal difficile à prédire ou à reproduire sans une connaissance précise des paramètres du système.

Parallèlement, les progrès réalisés dans le domaine de la photonique et des communications optiques ont permis le développement de dispositifs capables de générer des comportements chaotiques à très

haute fréquence. Parmi ces dispositifs, les diodes laser à semi-conducteur occupent une place privilégiée en raison de leur simplicité de mise en œuvre, de leur faible coût, de leur compacité et de leur capacité à fonctionner à des vitesses extrêmement élevées. Lorsqu'une diode laser est soumise à une rétroaction optique externe, une partie de la lumière émise est réinjectée dans la cavité après un certain délai. Cette rétroaction introduit une non-linéarité supplémentaire ainsi qu'une mémoire temporelle dans le système, conduisant à l'apparition de régimes dynamiques complexes pouvant évoluer vers le chaos.

Les signaux chaotiques générés par une diode laser à rétroaction possèdent alors des propriétés particulièrement adaptées aux systèmes de communication sécurisée. Ils peuvent être utilisés comme porteuses de chiffrement afin de masquer un message d'information avant sa transmission. Grâce au phénomène de synchronisation chaotique, un récepteur disposant d'un générateur identique est capable de reconstruire localement le signal chaotique utilisé à l'émission et de récupérer ainsi l'information originale. Cette approche constitue une alternative prometteuse aux méthodes cryptographiques classiques, tout en offrant l'avantage d'une intégration naturelle dans les réseaux optiques modernes.

Cependant, la mise en œuvre d'un cryptosystème chaotique optique soulève plusieurs questions scientifiques et techniques. La première concerne les conditions permettant à une diode laser avec rétroaction de produire un chaos suffisamment développé pour assurer un niveau de sécurité élevé. La seconde porte sur la caractérisation de ce comportement chaotique à travers des outils d'analyse tels que les diagrammes de bifurcation, les portraits de phase, les spectres de puissance et les exposants de Lyapunov. Enfin, il est nécessaire d'évaluer la capacité de ces signaux chaotiques à assurer efficacement les opérations de chiffrement et de déchiffrement tout en garantissant une récupération fidèle du message transmis.

La problématique de ce travail peut ainsi être formulée comme suit : Comment exploiter le chaos généré par une diode laser à rétroaction optique pour concevoir un cryptosystème optique performant permettant d'assurer le chiffrement et le déchiffrement sécurisés d'une information, tout en garantissant une synchronisation efficace entre l'émetteur et le récepteur ?

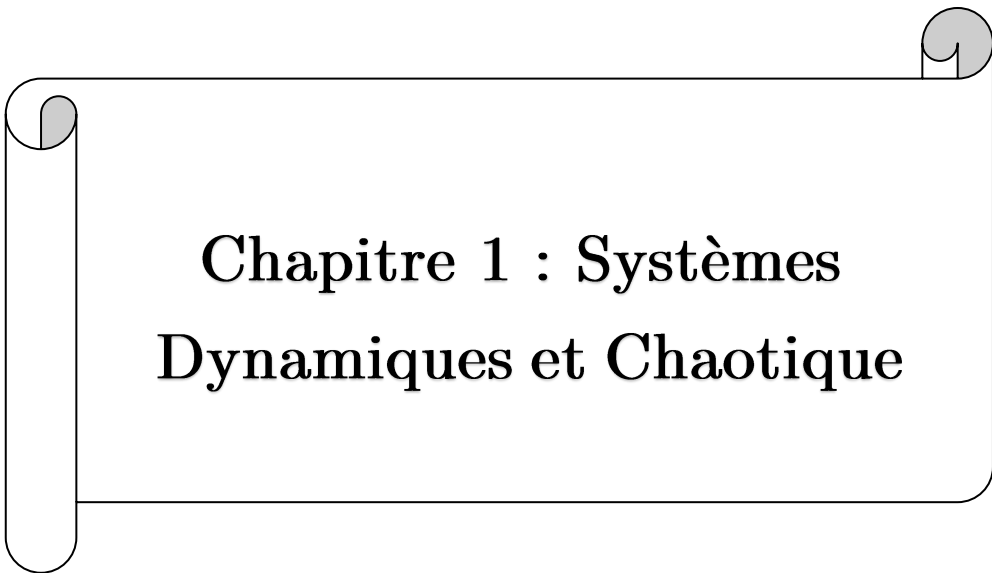
Pour répondre à cette problématique, ce mémoire a pour objectif principal la conception et la simulation d'un cryptosystème chaotique basé sur une diode laser à rétroaction optique. La génération du chaos est réalisée à partir du modèle de Lang-Kobayashi décrivant la dynamique d'une diode laser soumise à une rétroaction retardée. Les simulations sont effectuées sous MATLAB afin d'analyser les différents régimes dynamiques obtenus et d'identifier les conditions conduisant à l'apparition du chaos. Le signal chaotique ainsi généré est ensuite exploité dans un système de chiffrement optique simulé sous OptiSystem, où il sert à masquer un message d'information avant sa transmission. Le déchiffrement repose sur le principe de synchronisation chaotique permettant de reconstruire le signal initial au niveau du récepteur.

Afin d'atteindre ces objectifs, ce mémoire est structuré en trois chapitres.

Le premier chapitre présente les notions fondamentales relatives aux systèmes dynamiques et aux systèmes chaotiques. Les concepts essentiels tels que les systèmes non linéaires, l'espace des phases, les attracteurs, les bifurcations, la sensibilité aux conditions initiales et les exposants de Lyapunov sont introduits afin de fournir les bases théoriques nécessaires à la compréhension du chaos.

Le deuxième chapitre est consacré au chiffrement par chaos et aux crypto-systèmes chaotiques optiques. Après un rappel des objectifs fondamentaux de la cryptographie, les principes du chiffrement utilisant des signaux chaotiques sont présentés. Les avantages et les caractéristiques des systèmes optiques chaotiques appliqués à la sécurisation des communications sont également étudiés.

Enfin, le troisième chapitre traite de la dynamique chaotique d'une diode laser avec rétroaction optique ainsi que de son application au chiffrement et au déchiffrement des données. La modélisation mathématique du système est d'abord développée à travers le modèle de Lang-Kobayashi. Les résultats de simulation obtenus sous MATLAB sont ensuite analysés à l'aide de différents outils de caractérisation du chaos. Enfin, un système complet de chiffrement-déchiffrement basé sur le signal chaotique généré est proposé et évalué afin de démontrer la faisabilité et l'efficacité de cette approche pour les communications optiques sécurisées.



Chapitre 1 : Systèmes Dynamiques et Chaotique

Chapitre 1 : Systèmes Dynamiques et Chaotique

I-1 Introduction

Les systèmes dynamiques occupent une place fondamentale dans de nombreux domaines scientifiques tels que la physique, les mathématiques, l'ingénierie et les télécommunications. Ils permettent de décrire l'évolution d'un système au cours du temps en fonction d'un ensemble de règles ou d'équations déterministes. Dans certains cas, ces systèmes peuvent présenter des comportements complexes et imprévisibles appelés phénomènes chaotiques, qui relèvent du domaine de la Chaos théorie.

Le chaos se caractérise par une forte sensibilité aux conditions initiales, une évolution non linéaire et une apparente imprévisibilité, même lorsque les équations qui gouvernent le système sont parfaitement déterministes. Ces propriétés ont suscité un grand intérêt dans plusieurs applications modernes, notamment dans les systèmes de communication sécurisée et les techniques de chiffrement. En effet, les signaux chaotiques possèdent des caractéristiques telles que l'aléa, la complexité et la large bande spectrale, ce qui les rend particulièrement adaptés au domaine de la cryptographie.

Dans le contexte des systèmes optiques, les phénomènes chaotiques peuvent être générés à l'aide de dispositifs physiques tels que les Diode laser, notamment lorsque celles-ci sont soumises à un mécanisme de Optical feedback. Cette rétroaction peut produire des dynamiques non linéaires complexes capables de générer des signaux chaotiques exploitables pour la sécurisation des communications.

Ainsi, ce chapitre a pour objectif de présenter les notions fondamentales relatives aux systèmes dynamiques et au chaos. Il permettra de comprendre les principes théoriques qui sous-tendent la génération du chaos et constituera une base essentielle pour l'étude des systèmes de chiffrement chaotiques optiques abordés dans les chapitres suivants.

I-2 Systèmes dynamiques

Un Système dynamique est un modèle mathématique utilisé pour décrire l'évolution d'un système au cours du temps selon un ensemble de lois déterminées. Ces systèmes sont largement utilisés dans plusieurs domaines scientifiques tels que la physique, l'ingénierie, la biologie et les sciences de l'information afin d'analyser les comportements évolutifs des phénomènes naturels ou artificiels. De manière générale, un système dynamique est caractérisé par un ensemble de variables d'état qui décrivent l'état du système à un instant donné, ainsi que par une règle d'évolution qui détermine la manière dont ces variables changent avec le temps [1].

Mathématiquement, un système dynamique peut être représenté sous forme d'équations différentielles dans le cas des systèmes continus ou sous forme d'équations de récurrence pour les systèmes discrets. Dans un système dynamique continu, l'évolution est généralement décrite par une équation différentielle du type :

$$\frac{dx}{dt} = f(x, t)$$

Où x représente le vecteur d'état du système et f une fonction qui décrit la dynamique du système.

Les systèmes dynamiques peuvent être classés selon plusieurs critères. On distingue notamment les systèmes dynamiques linéaires, dont les équations obéissent au principe de superposition, et les 'Nonlinear dynamical systems', dans lesquels les relations entre les variables ne sont pas proportionnelles. Ces derniers sont particulièrement importants car ils peuvent produire des comportements complexes tels que les oscillations, les bifurcations et même le chaos.

Un autre aspect essentiel des systèmes dynamiques concerne la notion d'Espace des phases, qui représente graphiquement l'évolution du système dans un espace multidimensionnel défini par ses variables d'état. L'analyse de cet espace permet d'identifier les trajectoires du système, les points d'équilibre ainsi que les attracteurs qui déterminent la stabilité du comportement dynamique.

Dans le contexte des systèmes optiques et des communications sécurisées, l'étude des systèmes dynamiques non linéaires est particulièrement importante. En effet, certains dispositifs physiques comme les Diode laser peuvent présenter des dynamiques complexes lorsque des phénomènes tels que la Optical feedback sont introduits. Ces dynamiques peuvent conduire à l'apparition de comportements chaotiques exploitables dans le domaine de la cryptographie et des communications sécurisées.

Ainsi, la compréhension des systèmes dynamiques constitue une étape essentielle pour l'étude des phénomènes chaotiques et leur application dans les systèmes de chiffrement optiques basés sur les lasers.

I-3 Systèmes Dynamiques chaotiques

Les systèmes dynamiques chaotiques représentent une classe particulière de systèmes dynamiques non linéaires caractérisés par un comportement complexe et apparemment aléatoire. Malgré cette apparence d'irrégularité, ces systèmes sont entièrement déterministes, c'est-à-dire que leur évolution est régie par des équations mathématiques précises. Le chaos apparaît lorsque les interactions non linéaires entre les variables du système produisent des dynamiques très sensibles aux perturbations, ce qui rend la prédiction à long terme très difficile [1].

L'une des propriétés fondamentales des systèmes chaotiques est la sensibilité aux conditions initiales, souvent appelée « effet papillon ». Ce phénomène signifie qu'une très petite variation dans l'état initial d'un système peut entraîner une divergence rapide des trajectoires dans le temps. Cette caractéristique a été mise en évidence par les travaux du météorologue Edward Lorenz, qui a montré que des différences infinitésimales dans les paramètres initiaux d'un modèle météorologique pouvaient conduire à des résultats complètement différents. Cette découverte a constitué l'un des fondements de la Chaos théorie moderne [2].

Un autre aspect essentiel du chaos concerne la nature non linéaire des équations gouvernant le système.

Dans les ‘Nonlinear dynamical systems’, les interactions entre les variables sont complexes et ne suivent pas le principe de proportionnalité. Contrairement aux systèmes linéaires, ces systèmes peuvent produire des phénomènes dynamiques variés tels que les bifurcations, les oscillations irrégulières et l’émergence du chaos. Cette non-linéarité est donc une condition essentielle pour l’apparition du comportement chaotique dans les systèmes physiques et mathématiques

Les systèmes chaotiques sont également caractérisés par la présence d’un Strange attraction dans l’Espace des phases. Un attracteur étrange est une structure géométrique complexe vers laquelle les trajectoires du système convergent au cours du temps. Contrairement aux attracteurs simples comme les points d’équilibre ou les cycles périodiques, les attracteurs chaotiques possèdent généralement une structure fractale et reflètent la complexité du comportement dynamique du système. L’exemple le plus célèbre est l’attracteur de Lorenz, qui illustre parfaitement la dynamique chaotique et sa structure en forme d’ailes de papillon.

Par ailleurs, les systèmes chaotiques présentent souvent un spectre de fréquences large et une évolution temporelle irrégulière. Ces propriétés rendent les signaux chaotiques particulièrement intéressants pour certaines applications technologiques, notamment dans les domaines des télécommunications et de la cryptographie. En effet, l’imprévisibilité et la complexité des signaux chaotiques permettent de masquer efficacement l’information transmise, ce qui renforce la sécurité des communications [2].

Dans le domaine des systèmes optiques, le chaos peut être généré à l’aide de dispositifs physiques tels que les Diode laser. Lorsque ces lasers sont soumis à un mécanisme de Optical feedback, leur comportement peut devenir fortement non linéaire et produire des oscillations chaotiques. Ces signaux chaotiques peuvent ensuite être exploités dans les systèmes de communication sécurisée et dans les cryptosystèmes optiques, où ils servent à masquer ou à chiffrer les informations transmises [3].

I-4 L'espace de phase

L'Espace des phases est une représentation géométrique utilisée pour décrire l'évolution des Systèmes dynamiques. Dans cet espace, chaque état possible du système est représenté par un point unique, dont les coordonnées correspondent aux variables d'état du système (position, vitesse, intensité, etc.). Ainsi, l'évolution temporelle d'un système peut être représentée par une trajectoire appelée trajectoire de phase, qui décrit la succession des états du système au cours du temps. Cette représentation permet de transformer un problème dynamique dépendant du temps en une représentation géométrique plus facile à analyser. [4].

I-4-1 Notion d'attracteur

Dans un système dynamique, un attracteur est un ensemble de points de l'espace de phase vers lequel les trajectoires du système tendent à long terme. Autrement dit, quelle que soit la condition initiale (dans une certaine région), l'évolution du système finira par se rapprocher de cet ensemble. Les attracteurs représentent donc les états stables ou les comportements permanents du système [5].

On distingue généralement plusieurs types d'attracteurs :

Type d'attracteur	Description	Exemple
Point fixe	Le système converge vers un état unique stable	Système dissipatif
Cycle limite	Trajectoire périodique fermée	Oscillateur
Quasi-périodique	Mouvement sur un tore	Systèmes oscillants couplés
Attracteur étrange	Structure fractale associée au chaos	Systèmes chaotiques

Tableau I.1 : les types d'attracteurs (Point fixe, Cycle limite, Quasi-périodique, Attracteur étrange)

Dans les systèmes chaotiques, les trajectoires ne convergent pas vers un point ou un cycle simple, mais vers un « Strange attractor », caractérisé par une structure géométrique complexe et souvent fractale (Ott, 2002).

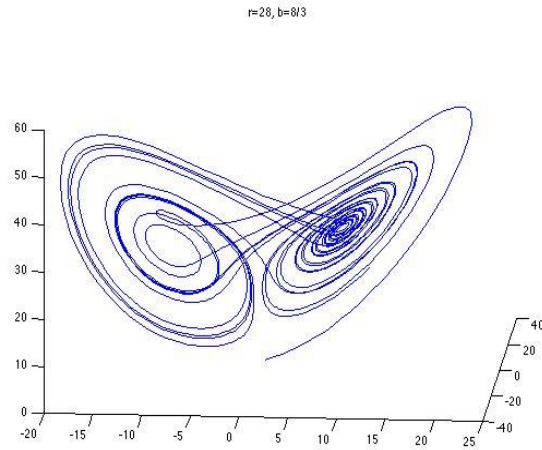


Figure I.1 - Attracteur de Lorenz dans l'Espace des phases, illustrant un comportement chaotique caractéristique des systèmes dynamiques non linéaires [6].

Cet attracteur célèbre illustre le comportement chaotique découvert par Edward Lorenz, où les trajectoires restent confinées dans une région de l'espace de phase tout en restant imprévisibles.

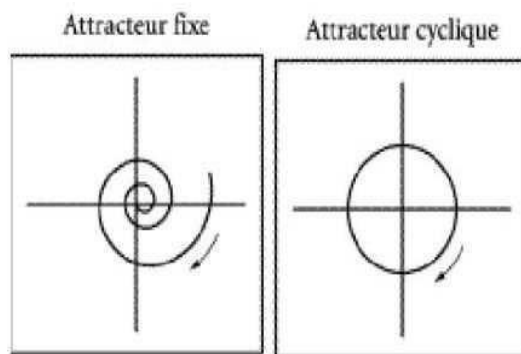


Figure I.2 - Exemples d'attracteurs

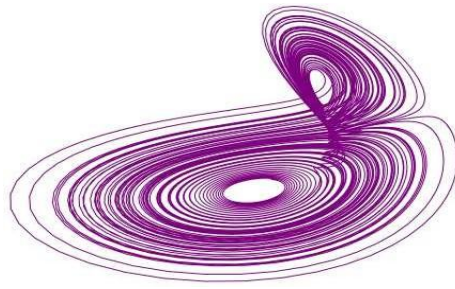


Figure I.3 - Attracteur étrange de Lorentz

I-4-2 Dimension d'Hausdorff

La Hausdorff dimension est une mesure mathématique utilisée pour caractériser la complexité géométrique d'un attracteur chaotique. Contrairement aux dimensions classiques (1D, 2D ou 3D), la dimension d'Hausdorff peut être fractionnaire, ce qui permet de décrire les structures fractales présentes dans les systèmes chaotiques.

Dans les systèmes dynamiques chaotiques, les attracteurs possèdent souvent une structure fractale. La dimension d'Hausdorff permet de quantifier cette structure en mesurant comment le nombre d'éléments nécessaires pour couvrir l'attracteur varie lorsque l'échelle d'observation change [7].

La dimension d'Hausdorff peut être exprimée de manière simplifiée par :

$$D_H = \lim_{\epsilon \rightarrow 0} \frac{\log N(\epsilon)}{\log \left(\frac{1}{\epsilon}\right)}$$

Où :

- $N(\epsilon)$: nombre de segments nécessaires pour couvrir l'ensemble
- ϵ : taille de l'échelle d'observation

Ainsi, la dimension d'Hausdorff permet de mesurer quantitativement la complexité des

attracteurs chaotiques et de distinguer un système régulier d'un système chaotique.

I-4-3 Exposants de Lyapunov

Les exposants de Lyapunov constituent un outil fondamental pour caractériser le chaos dans les systèmes dynamiques. Ils mesurent la vitesse à laquelle deux trajectoires initialement très proches dans l'espace des phases divergent au cours du temps. Un exposant positif indique que de petites différences dans les conditions initiales entraînent une divergence exponentielle des trajectoires, ce qui est la signature d'un comportement chaotique [7].

Mathématiquement, si deux trajectoires commencent séparées par une distance initiale δ_0 , leur séparation $\delta(t)$ après un temps t évolue approximativement selon :

Donc deux trajectoires dans le plan de phase initialement séparées par un taux Z_1 divergent après un temps $\Delta t = t_2 - t_1$ vers Z_2
tel que : $|Z_2| \approx \exp(\lambda \cdot \Delta t) |Z_1|$

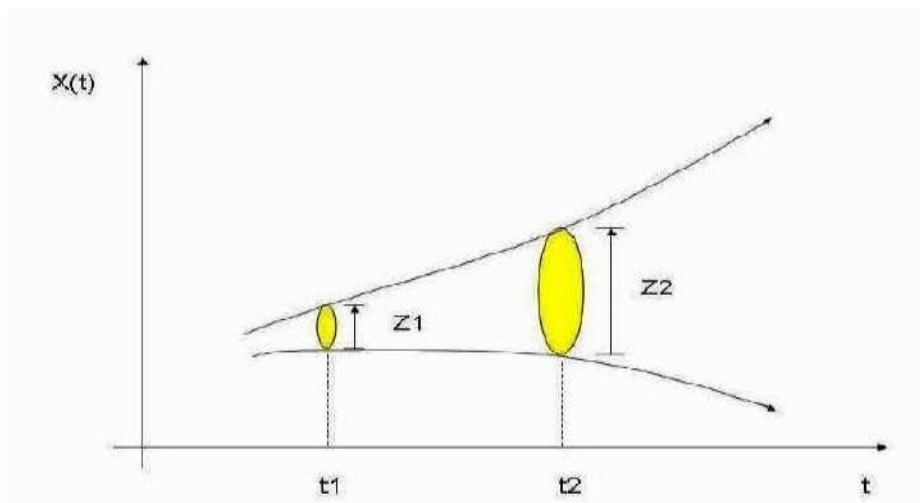


Figure I.4 - Divergence de deux trajectoires dans le plan de phase

Considérons un système dynamique dont l'espace des phases est de dimension n et prenons à $t=0$ une hyper sphère infiniment centrée en X appartenant à l'attracteur ($X \in \mathbb{R}^n$) avec un rayon ε_0 .

Au temps $t \gg 0$, cette hyper sphères transforme en une hyper-ellipsoïde demi-axes

$$\varepsilon_i(t) \approx \varepsilon_0 \exp(\lambda_i t) \quad i=1,2,\dots,n$$

Les exposants de Lyapunov sont tels que :

Soient deux trajectoires initialement proches dans l'espace des phases, séparées par un vecteur infini estimer $\delta X(0)$.

Après un temps t , leur séparation $\delta X(t)$ évolue approximativement selon :

$$\delta X(t) \approx \delta X(0) e^{\lambda t}$$

Où λ est l'exposant de Lyapunov.

- Si $\lambda > 0$, Les trajectoires divergent exponentiellement, indiquant un comportement chaotique.
- Si $\lambda = 0$, les trajectoires restent à distance constante, ce qui correspond à un mouvement périodique ou quasi-périodique.
- Si $\lambda < 0$, les trajectoires convergent vers un attracteur stable.

Ainsi, les exposants de Lyapunov quantifient de manière précise la sensibilité aux conditions initiales et permettent de caractériser la stabilité ou le chaos d'un système dynamique.

I-4-4 Bifurcation et routes vers le chaos

Dans l'étude des systèmes dynamiques, une bifurcation désigne un changement qualitatif du comportement d'un système lorsqu'un paramètre du système varie. Une modification continue de ce paramètre peut provoquer l'apparition ou la disparition de points fixes, de cycles limites ou d'attracteurs plus complexes. Ces transitions constituent souvent la première étape vers l'émergence du chaos, mettant en évidence la sensibilité du système aux conditions initiales [8].

Parmi les bifurcations les plus étudiées, on distingue les bifurcations locales et globales. Les bifurcations locales affectent directement la stabilité des points fixes ou des cycles limites. Par exemple, la bifurcation de pitchfork se produit lorsqu'un point fixe stable se divise en plusieurs points fixes, stables ou instables, tandis que la bifurcation de Hopf transforme un point fixe stable en un cycle limite stable lorsque les valeurs propres complexes d'un point fixe traversent l'axe imaginaire [9].

D'autres types, comme les bifurcations transcritiques ou tangentielle (saddle-node), jouent un rôle central dans l'apparition de comportements nouveaux. Les bifurcations globales, telles que les bifurcations homoclines, concernent l'ensemble du système et peuvent générer des attracteurs complexes par l'interaction de différentes orbites [10].

Les bifurcations sont directement liées aux routes vers le chaos, qui décrivent la transition progressive d'un système d'un comportement ordonné à un comportement chaotique. La route par cascade de périodes, observée dans le système logistique, illustre ce phénomène : à mesure que le paramètre du système augmente, la période d'un cycle stable double successivement (2, 4, 8, ...), conduisant finalement au chaos. La régularité de cette cascade est universelle et quantifiée par la constante de Feigenbaum. D'autres routes vers le chaos incluent la quasi-périodicité, où le système évolue sur un tore et devient instable lorsque des fréquences incommensurables interagissent et l'intermittence, caractérisée par l'alternance de phases régulières et chaotiques [11].

Enfin, les crises chaotiques apparaissent soudainement lorsque des attracteurs fusionnent ou disparaissent, entraînant un comportement chaotique abrupt.

Des exemples concrets illustrent ces concepts. L'attracteur de Lorenz montre comment un système simple de trois équations différentielles peut générer des trajectoires chaotiques par de petites variations des conditions initiales [12].

Le modèle logistique permet de visualiser la cascade de périodes et l'apparition du chaos à partir d'une équation itérative simple.

Enfin, des systèmes physiques comme les oscillateurs électroniques ou les lasers à rétroaction présentent des bifurcations et des transitions vers le chaos observables expérimentalement [13].

Ainsi, l'étude des bifurcations et des routes vers le chaos permet de comprendre comment des systèmes déterministes simples peuvent produire des comportements complexes et imprévisibles. Cette analyse est essentielle pour la modélisation, la prévision et le contrôle des systèmes physiques, biologiques ou économiques, tout en mettant en évidence la sensibilité aux conditions initiales et la structure fractale des attracteurs chaotiques.

I-5 Conclusion

Le présent chapitre a permis de poser les fondements théoriques relatifs aux systèmes dynamiques et aux phénomènes chaotiques. Il a été montré que les systèmes dynamiques constituent un outil puissant pour modéliser l'évolution temporelle de nombreux systèmes physiques, biologiques et technologiques. La distinction entre systèmes linéaires et non linéaires a souligné l'importance de la non-linéarité dans l'apparition de comportements complexes, notamment le chaos, qui se manifeste par une sensibilité extrême aux conditions initiales et par des évolutions imprévisibles malgré des équations déterministes [14].

L'étude de l'espace des phases a permis d'introduire la notion de trajectoires, de points fixes et d'attracteurs, en particulier les attracteurs étranges, qui représentent la signature géométrique des dynamiques chaotiques. La dimension d'Hausdorff a fourni un outil quantitatif pour mesurer la complexité fractale de ces attracteurs, tandis que les exposants de Lyapunov ont mis en évidence la vitesse à laquelle les trajectoires initialement proches divergent dans le temps, constituant un indicateur précis de la stabilité ou du chaos d'un système [15].

Enfin, l'analyse des bifurcations et des routes vers le chaos a permis de comprendre comment des changements progressifs de paramètres peuvent transformer un comportement ordonné en un comportement chaotique. Les différentes routes vers le chaos – par cascade de périodes, quasi-périodicité, intermittence ou crises – illustrent la diversité des mécanismes par lesquels le chaos peut apparaître dans des systèmes déterministes, comme dans le cas des lasers à rétroaction ou des oscillateurs électroniques [16].

En synthèse, ce chapitre a fourni les outils conceptuels et mathématiques nécessaires pour analyser la dynamique des systèmes non linéaires et comprendre l'apparition du chaos. Ces notions constituent une base essentielle pour l'étude des systèmes de chiffrement chaotiques optiques abordés dans les chapitres suivants, où les propriétés de sensibilité aux conditions initiales, d'imprévisibilité et de complexité seront exploitées pour la sécurisation des communications.

Chapitre 2 :
Chiffrement par Chaos :
Cryptosystèmes Chaotiques
Optiques

Chapitre 2 : Chiffrement par Chaos : Crypto-Systèmes Chaotiques Optiques

II-1 Introduction

Le développement rapide des technologies de l'information et de la communication a entraîné une augmentation considérable des besoins en sécurité des données. Les méthodes classiques de chiffrement, bien qu'efficaces, font face à de nouveaux défis liés à la complexité croissante des attaques et à l'évolution des capacités de calcul. Dans ce contexte, de nouvelles approches inspirées de phénomènes physiques et mathématiques ont émergé, parmi lesquelles le chiffrement par chaos.

Les systèmes chaotiques se distinguent par des propriétés essentielles telles que la sensibilité aux conditions initiales, l'imprévisibilité et le comportement pseudo-aléatoire, ce qui les rend particulièrement adaptés aux applications cryptographiques. En exploitant ces caractéristiques, les crypto-systèmes chaotiques offrent des mécanismes de chiffrement robustes et difficiles à décrypter sans connaissance précise des paramètres du système.

Par ailleurs, l'intégration de l'optique dans les systèmes de chiffrement a ouvert la voie à des techniques innovantes permettant de traiter l'information à très grande vitesse tout en assurant un haut niveau de sécurité. Les crypto-systèmes chaotiques optiques combinent ainsi les avantages du chaos et des technologies optiques pour proposer des solutions performantes, notamment dans le domaine du traitement et de la transmission d'images.

Ce chapitre a pour objectif de présenter les principes fondamentaux du chiffrement par chaos ainsi que les spécificités des crypto-systèmes chaotiques optiques. Il mettra en lumière leurs avantages, leurs mécanismes de fonctionnement et leurs domaines d'application, tout en abordant les enjeux liés à leur mise en œuvre [17].

II-2 Objectifs des crypto-systèmes

Les crypto-systèmes constituent un pilier fondamental de la sécurité de l'information. Leur objectif principal est de protéger les données contre les accès non autorisés, les altérations malveillantes et les utilisations frauduleuses.

Dans le contexte du chiffrement par chaos et des systèmes optiques, ces objectifs prennent une dimension encore plus importante en raison de la complexité et de la sensibilité des données traitées. Les principaux objectifs des crypto-systèmes peuvent être détaillés comme suit :

1. La confidentialité (Confidentialité des données) : La confidentialité vise à garantir que seules les personnes autorisées peuvent accéder à l'information. Elle est assurée par des techniques de chiffrement qui transforment les données lisibles (texte en clair) en une forme illisible (texte chiffré). Dans les crypto-systèmes chaotiques, cette propriété est renforcée par la nature imprévisible et sensible aux conditions initiales des systèmes chaotiques, rendant toute tentative de déchiffrement sans clé extrêmement difficile [18].

2. L'intégrité des données : L'intégrité consiste à s'assurer que les données n'ont pas été modifiées ou altérées, volontairement ou accidentellement, durant leur transmission ou leur stockage. Les crypto-systèmes utilisent des mécanismes comme les fonctions de hachage et les signatures numériques pour vérifier que l'information reçue est identique à celle envoyée (Menezes et al., 1996).

3. L'authentification : L'authentification permet de vérifier l'identité des entités communicantes (utilisateurs, systèmes, dispositifs). Elle garantit que l'émetteur et le récepteur sont bien ceux qu'ils prétendent être. Dans les systèmes chaotiques, des paramètres initiaux ou des clés secrètes peuvent servir de moyens d'authentification sécurisés [18].

4. La non-répudiation : La non-répudiation empêche un émetteur de nier ultérieurement avoir envoyé un message. Elle est généralement assurée par l'utilisation de signatures numériques, qui fournissent une preuve irréfutable de l'origine et de l'intégrité du message [19].

5. La disponibilité : La disponibilité garantit que les systèmes et les données sont accessibles aux utilisateurs autorisés lorsqu'ils en ont besoin. Bien que ce ne soit pas un objectif exclusivement cryptographique, les crypto-systèmes contribuent à la disponibilité en protégeant les systèmes contre certaines attaques, telles que les altérations ou les accès non autorisés [19].

6. La résistance aux attaques : Un objectif essentiel des crypto-systèmes modernes est leur capacité à résister à différents types d'attaques, telles que les attaques par force brute, les attaques statistiques ou les attaques différentielles. Les systèmes chaotiques offrent une forte résistance grâce à leurs propriétés non linéaires et à leur comportement complexe [20].

7. L'efficacité et la rapidité d'exécution : Les crypto-systèmes doivent également être performants afin de traiter de grandes quantités de données en temps réel. Dans le cas des crypto-systèmes optiques chaotiques, l'utilisation de technologies optiques permet d'atteindre des vitesses de traitement très élevées, ce qui constitue un avantage majeur pour les applications modernes, notamment dans le traitement d'images et de vidéos. [21].

II-3 Communications Sécurisées par chaos

Avant d'aborder en détail les différentes techniques des communications sécurisées par chaos, il convient de souligner que cette approche repose sur des principes innovants issus de la théorie des systèmes dynamiques non linéaires. Elle représente une alternative prometteuse aux méthodes classiques de cryptographie, en exploitant les propriétés intrinsèques du chaos pour assurer la sécurité des échanges. Dans ce qui suit, nous présenterons d'abord le principe général des communications chaotiques, puis le rôle fondamental de la synchronisation, avant de mettre en évidence les principales applications de ces systèmes, notamment dans le domaine optique [22].

II-3-1 Principe des communications chaotiques

Les communications sécurisées par chaos reposent sur l'utilisation de signaux chaotiques pour masquer l'information à transmettre. Un système chaotique est un système dynamique non linéaire caractérisé par une grande sensibilité aux conditions initiales, une évolution déterministe mais imprévisible et une apparence pseudo-aléatoire. Dans ce cadre, le message à transmettre est combiné avec un signal chaotique généré par un système dynamique, rendant le signal transmis difficilement interprétable sans connaissance préalable des paramètres du système.

Plusieurs techniques sont utilisées, telles que le masquage chaotique (chaos masking), où le message est ajouté à un signal chaotique, ou encore la modulation chaotique, où le message modifie directement les paramètres du système. Ces méthodes permettent d'assurer une certaine confidentialité, car le signal transmis ressemble à du bruit pour un observateur externe [23].

II-3-2 Synchronisation des systèmes chaotiques

La synchronisation est un élément central des communications chaotiques. Elle permet au récepteur de reproduire le signal chaotique généré par l'émetteur afin de récupérer le message initial. Malgré leur comportement imprévisible, deux systèmes chaotiques peuvent être synchronisés sous

certaines conditions, notamment lorsqu'ils partagent des paramètres communs et sont couplés de manière appropriée.

Ce concept a été introduit par Pecora et Carroll, qui ont démontré qu'il est possible d'obtenir une synchronisation stable entre systèmes chaotiques identiques. Cette propriété est exploitée dans les systèmes de communication pour assurer la récupération fiable du message. Toutefois, la synchronisation reste sensible aux perturbations, au bruit et aux erreurs de paramétrage, ce qui constitue un défi majeur pour les applications pratiques [24].

II-3-3 Applications des communications chaotiques (notamment optiques)

Les communications chaotiques trouvent des applications importantes dans plusieurs domaines, en particulier dans les systèmes de transmission à haut débit. Les systèmes optiques chaotiques, basés sur des lasers semi-conducteurs, permettent de générer des signaux chaotiques à très haute fréquence, offrant ainsi une large bande passante et une sécurité renforcée.

Ces techniques sont utilisées dans les réseaux de télécommunications, la transmission sécurisée d'images et de vidéos, ainsi que dans les domaines sensibles tels que les communications militaires et les systèmes bancaires. De plus, les communications chaotiques présentent une forte résistance aux attaques classiques grâce à la complexité du signal et à la difficulté de reproduire les conditions initiales exactes du système.

Cependant, malgré leurs avantages, ces systèmes présentent certaines limites, notamment la complexité de mise en œuvre, la sensibilité au bruit et les difficultés de synchronisation dans des conditions réelles [25].

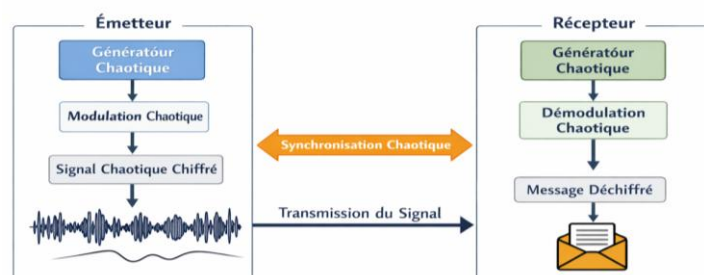


Figure II.5 - Principe d'une communication sécurisée par chaos

II-4 Techniques de chiffrement par chaos

Les techniques de chiffrement par chaos exploitent les propriétés dynamiques des systèmes chaotiques pour sécuriser l'information. Ces méthodes se distinguent par leur capacité à générer des signaux pseudo-aléatoires, sensibles aux conditions initiales et difficiles à reproduire, ce qui rend le déchiffrement sans connaissance exacte des paramètres quasi impossible. Les principales techniques utilisées peuvent être classées en plusieurs catégories, présentées ci-dessous avec leurs principes et références.

II-4-1 Masquage chaotique (Chaos Masking)

Le masquage chaotique consiste à ajouter le message à un signal chaotique généré par le système. Le signal chaotique agit comme une « clé dynamique » qui rend le message indéchiffrable pour un observateur non autorisé. À la réception, la synchronisation des systèmes chaotiques permet de récupérer le signal original et d'extraire le message. Cette technique est simple à mettre en œuvre mais nécessite un contrôle précis de la synchronisation [26].

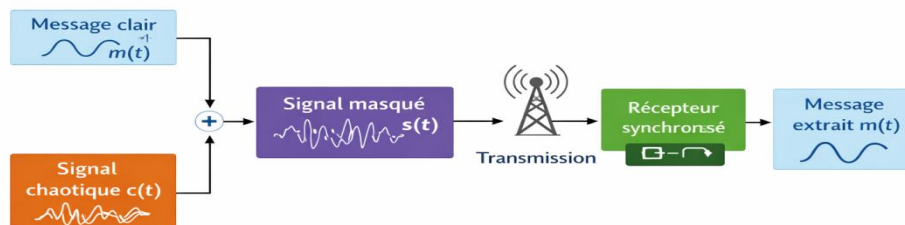


Figure II.6 - principe d'une communication sécurisée par chaos (masquage chaotique)

II-4-2 Modulation chaotique (Chaos Shift Keying – CSK)

Dans la modulation chaotique, le message influence directement l'évolution du système chaotique. Le signal chaotique change selon les bits du message, ce qui crée une corrélation complexe entre le message et le signal transmis. La démodulation au récepteur repose sur la synchronisation et la connaissance des paramètres exacts du générateur chaotique. CSK offre une n

quage [26].

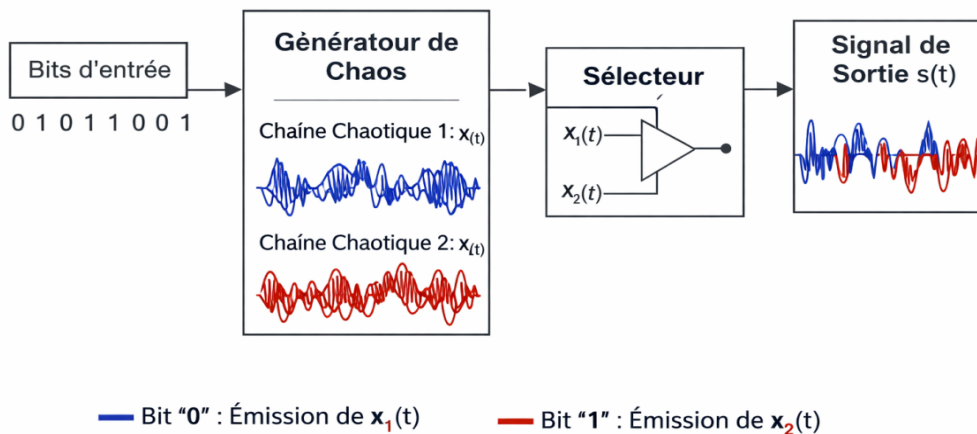


Figure II.7 - Modulation chaotique (Chaos Shift Keying - CSK)

II-4-3 Modulation par décalage de phase chaotique (Chaos Phase Modulation – CPM)

Cette technique consiste à coder l'information en modifiant la phase du signal chaotique. Chaque état du chaos correspond à un symbole du message. Le récepteur, synchronisé avec le générateur chaotique, peut reconstruire le signal et récupérer les données transmises. CPM permet une transmission efficace et sécurisée, notamment pour les communications optiques à haut débit [27].

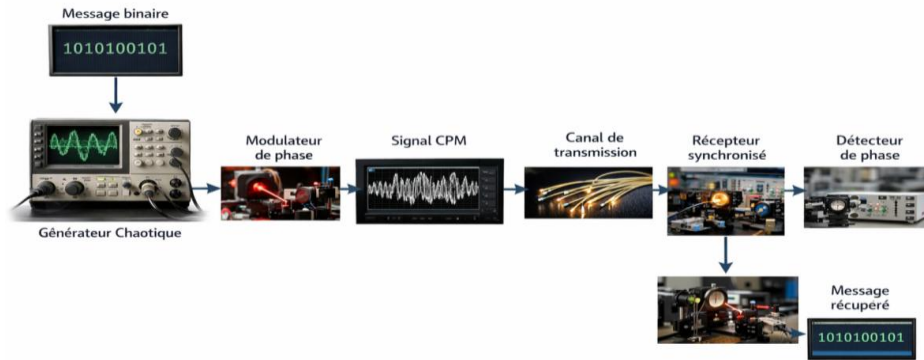


Figure II.8 - Principe de la modulation par décalage de phase chaotique (CPM)

II-4-4 Cryptographie hybride chaos-numérique

Certains systèmes combinent le chaos avec des méthodes de chiffrement numériques classiques pour renforcer la sécurité. Par exemple, un flux pseudo-aléatoire généré par un système chaotique peut être utilisé comme clé de chiffrement pour un algorithme de type AES. Cette approche hybride tire parti de la complexité du chaos et de la solidité des algorithmes cryptographiques traditionnels [27].

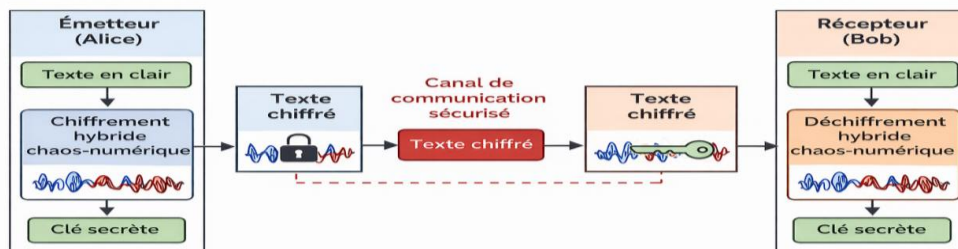


Figure II.9 - Cryptographie hybride chaos - numérique

II-5 Chiffrement par modulation

Le chiffrement par modulation est une technique de sécurité des communications qui repose sur la modulation d'un signal porteur selon un signal chaotique ou un signal porteur de données. Contrairement aux méthodes classiques de cryptographie, cette approche combine la théorie du chaos et les techniques de modulation pour coder les informations de manière

sécurisée. Elle est particulièrement utilisée dans les systèmes de communication optique et sans fil pour sa robustesse face aux interceptions et aux perturbations.

II-5-1 Masquage chaotique (Chaos Masking – CM)

Le masquage chaotique consiste à superposer le message à transmettre sur un signal chaotique généré par un système dynamique. Le signal chaotique agit comme une clé évolutive qui rend le message illisible pour tout observateur non autorisé [28].

Principe :

- Le message $m(t)$ est ajouté à un signal chaotique $x(t)$ $+m(t)$ pour créer le signal transmis
- À la réception, le récepteur synchronisé avec le générateur chaotique peut extraire $m(t)$ en soustrayant le signal chaotique reconstruit.

Avantages :

- Sécurité élevée grâce à la complexité du chaos.
- Résistance aux interférences et aux écoutes non autorisées.

II-5-2 Modulation chaotique (Chaos Shift Keying – CSK)

La modulation par décalage de chaos (CSK) utilise différents états chaotiques pour représenter des symboles binaires ou multivalués. Chaque état du chaos correspond à un symbole du message à transmettre.

Principe :

- Le message binaire détermine l'état initial du système chaotique.
- Le signal transmis est un signal chaotique dont l'évolution dépend du symbole courant.
- Le récepteur, synchronisé avec le générateur chaotique, peut identifier l'état correspondant à chaque symbole et reconstruire le message.

Avantages :

- Transmission sécurisée sans besoin de clés fixes.
- Adaptabilité aux canaux bruités grâce à la nature robuste des signaux chaotiques.

II-5-3 Modulation par décalage de phase chaotique (Chaos Phase Modulation – CPM)

Le CPM consiste à coder l'information en modifiant la phase d'un signal chaotique, plutôt que son amplitude ou sa fréquence.

Principe :

- Chaque symbole du message correspond à un changement de phase spécifique dans le signal chaotique.
- Le récepteur synchronisé peut détecter ces variations de phase et reconstruire le message transmis [29].

Avantages :

- Haute efficacité spectrale.
- Sécurité renforcée contre les attaques passives et actives.

II-6 Applications et perspectives

- Communications optiques sécurisées : transmission de données sensibles sur fibres optiques.
- Communications sans fil : résistance aux interceptions et brouillages.
- Cryptographie hybride : combinaison du chaos et des méthodes numériques pour renforcer la sécurité.

II-7 Conclusion

Le chiffrement par chaos représente une avancée significative dans le domaine de la sécurité des communications, offrant des solutions innovantes face aux limites des méthodes classiques de cryptographie. En exploitant les propriétés intrinsèques des systèmes chaotiques, telles que la sensibilité aux conditions initiales, l'imprévisibilité et le comportement pseudo-aléatoire, les crypto-systèmes chaotiques assurent un niveau de sécurité élevé, difficilement contournable par des attaques traditionnelles [30].

L'intégration de technologies optiques a permis de renforcer encore ces systèmes, en offrant des transmissions à très haut débit tout en maintenant une sécurité robuste. Les techniques de chiffrement par modulation, incluant le masquage chaotique (CM), la modulation chaotique (CSK) et la modulation par décalage de phase chaotique (CPM), démontrent la diversité et l'efficacité des approches basées sur le chaos pour coder l'information de manière sécurisée et résiliente face aux perturbations ou aux écoutes non autorisées. [31].

Par ailleurs, la cryptographie hybride chaos-numérique illustre le potentiel de combinaison entre le chaos et les méthodes classiques pour maximiser la sécurité et la performance des systèmes de communication. Ces innovations ouvrent des perspectives prometteuses pour les applications sensibles, notamment dans la transmission d'images et de vidéos, les communications militaires, les systèmes bancaires et les réseaux à haut débit.

Enfin, malgré leurs nombreux avantages, les systèmes chaotiques présentent encore des défis, tels que la complexité de mise en œuvre, la sensibilité au bruit et la nécessité d'une synchronisation précise entre émetteur et récepteur. Ces contraintes constituent des axes de recherche importants pour améliorer la fiabilité et l'adaptabilité des crypto-systèmes chaotiques dans des conditions réelles d'exploitation. [32].

En résumé, le chiffrement par chaos, et en particulier les crypto-systèmes chaotiques optiques, représentent une solution innovante et performante pour la sécurité des communications modernes, combinant rapidité, robustesse et confidentialité des données dans un contexte technologique en constante évolution [33].

Chapitre 3 :
Dynamique Chaotique d'une
Diode Laser avec Rétroaction
Optique :
Chiffrement-déchiffrement

Chapitre 3 :

Dynamique Chaotique d'une Diode Laser avec Rétroaction

Optique : Chiffrement-déchiffrement

III-1 Introduction

Le comportement chaotique d'une diode laser constitue aujourd'hui un axe de recherche majeur en raison de ses applications en communications sécurisées, génération de nombres aléatoires optiques, cryptographie physique et systèmes radar large bande.

Une diode laser est un système dynamique non linéaire décrit par les équations de taux (porteurs + photons). En régime normal, elle émet une lumière stable. Mais lorsqu'on introduit : un retard, une rétroaction, ou une modulation forte, le système peut entrer dans un régime chaotique caractérisé par : une sensibilité aux conditions initiales, un spectre large, et des oscillations imprévisibles.

La génération de chaos dans une diode laser repose donc essentiellement sur l'introduction de non-linéarité, de retard ou de rétroaction. Parmi toutes les techniques, la rétroaction optique externe reste la plus fondamentale, mais les approches modernes combinent souvent plusieurs mécanismes pour obtenir un chaos plus riche et contrôlable.

Dans ce chapitre, nous allons exposer quelques techniques de génération du chaos par diode laser, étudier le cas d'une dynamique chaotique d'une diode laser avec rétroaction et proposer et tester un crypto-système de chiffrement/déchiffrement utilisant cette approche.

III-2 Techniques de génération du chaos par diode laser

La génération du chaos dans les diodes laser peut être obtenue par plusieurs mécanismes non linéaires.

Les quatre voies les plus couramment étudiées dans la littérature sont les suivantes :

III-2-1. Chaos par rétroaction optique externe (Optical Feedback Chaos)

Cette méthode consiste à réinjecter dans la cavité laser une partie de la lumière émise après un retard temporel introduit par une cavité externe. La rétroaction modifie continuellement les conditions de fonctionnement du laser et peut conduire à des oscillations instables puis chaotiques lorsque l'intensité de la rétroaction dépasse un certain seuil. [26, 27]

Principe :

- Une fraction du faisceau laser est réfléchi par un miroir externe.
- Le signal réinjecté interagit avec le champ optique intracavité.
- Le retard de propagation introduit une dynamique de dimension élevée favorable au chaos.

Caractéristiques :

- Génération de chaos à large bande.
- Mise en œuvre relativement simple.
- Très utilisée pour les communications optiques sécurisées et les générateurs de nombres aléatoires.

Le modèle mathématique le plus utilisé pour décrire ce phénomène est celui de R. Lang et K. Kobayashi.

III-2-2. Chaos par injection optique (Optical Injection Chaos)

Dans cette configuration, un laser maître injecte son rayonnement dans un laser esclave. La compétition entre les fréquences des deux lasers et les non-linéarités du système peut conduire à des régimes chaotiques. [28, 29]

Principe :

- Un laser maître impose un champ optique au laser esclave.
- Le désaccord de fréquence et la puissance injectée jouent un rôle essentiel.
- Certaines combinaisons de paramètres provoquent des bifurcations menant au chaos.

Caractéristiques :

- Contrôle précis du régime chaotique.
- Large bande spectrale.
- Bonne stabilité expérimentale.

Cette technique est particulièrement adaptée aux systèmes de communication optique sécurisée.

III-2-3. Chaos par modulation du courant d'injection

Le courant d'alimentation du laser est modulé périodiquement par un signal électrique. Lorsque l'amplitude ou la fréquence de modulation deviennent suffisamment importantes, la dynamique du laser subit des bifurcations successives qui peuvent conduire au chaos. [30]

Principe :

- Modulation sinusoïdale ou périodique du courant.
- Apparition de bifurcations de période.

Caractéristiques :

- Mise en œuvre simple électroniquement.
- Faible coût expérimental.
- Bande chaotique généralement plus limitée que celle obtenue par rétroaction optique.

III-2-4. Chaos par couplage de lasers (Coupled Lasers Chaos)

Deux ou plusieurs lasers sont couplés optiquement ou électroniquement. Les interactions mutuelles entre les différents oscillateurs peuvent générer des comportements complexes et chaotiques. [31]

Principe :

- Échange d'énergie ou d'information entre plusieurs lasers.
- Synchronisation puis désynchronisation des oscillations.
- Apparition d'attracteurs chaotiques de grande dimension.

Caractéristiques :

- Chaos de forte complexité.
- Possibilité d'obtenir un hyper-chaos (plusieurs exposants de Lyapunov positifs).
- Utilisé dans les réseaux photoniques et les systèmes de cryptographie optique.

III-2-5. Génération du chaos par cavité externe à fibre optique

Une fibre optique longue est utilisée comme ligne de retard entre la sortie du laser et son entrée. Cette configuration augmente fortement la dimension du système chaotique.

Les avantages sont :

- Large bande spectrale ;
- Grande complexité ;
- Possibilité de synchronisation chaotique.

Les lasers à rétroaction par fibre sont largement étudiés pour les communications sécurisées [32].

Méthode	Complexité expérimentale	Largeur de bande chaotique	Possibilité d'hyper-chaos
Rétroaction optique	Faible à moyenne	Très élevée	Oui
Injection optique	Moyenne	Très élevée	Oui
Modulation du courant	Faible	Moyenne	Rare
Couplage de lasers	Élevée	Très élevée	Oui
Cavité externe à fibre optique	Élevée	Très élevée	Oui

Tableau III .1 : Comparaison des cinq méthodes :

En pratique, les méthodes les plus utilisées aujourd'hui pour générer un chaos à large bande sont la rétroaction optique externe et l'injection optique, car elles permettent d'obtenir des signaux chaotiques riches spectralement, particulièrement adaptés aux communications optiques sécurisées.

III-3 Chaos par Diode Laser avec rétroaction optique

Les lasers à semi-conducteur présentent une dynamique fortement non linéaire en raison du couplage intrinsèque entre la densité de porteurs et le champ optique intracavité. Lorsqu'une rétroaction optique externe est introduite, la dynamique devient encore plus complexe et peut conduire à des régimes instables, quasi-périodiques ou chaotiques.

Cette section présente la modélisation mathématique du système.

III-3-1 Modélisation Mathématique- Équations classiques d'une diode laser à semi-conducteur

La dynamique d'une diode laser est décrite par les équations de taux couplées suivantes (elles décrivent l'évolution temporelle du champ optique et de la densité de porteurs dans la région active du laser) :

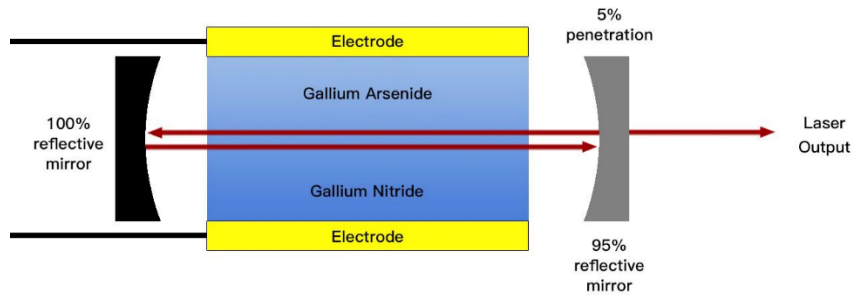


Figure III.1- Schéma de principe d'une diode Laser a semi-conducteur

a) Équation du champ optique

$$\frac{dE(t)}{dt} = \frac{1}{2}(1 + j\alpha) \left[G(N) - \frac{1}{\tau_p} \right] E(t)$$

b) Équation des porteurs

$$\frac{dN(t)}{dt} = \frac{I}{qV} - \frac{N(t)}{\tau_s} - G(N)|E(t)|^2$$

Paramètres physiques

- $E(t)$: amplitude complexe du champ optique
- $N(t)$: densité de porteurs
- I : courant d'injection
- q : charge électronique
- V : volume actif
- τ_p : temps de vie des photons
- τ_s : temps de vie des porteurs
- α : facteur de Henry (linewidth enhancement factor)
- $G(N)$: gain optique

Souvent on approxime :

$$G(N) = g(N - N_0)$$

où g est le gain différentiel et N_0 la densité de transparence.

➤ Signification physique dans l'équation du champ optique

L'équation indique que le champ optique est :

- Amplifié lorsque le gain $G(N)$ dépasse les pertes $\frac{1}{\tau_p}$,
- Atténué lorsque le gain est inférieur aux pertes.

Le terme : $G(N) - \frac{1}{\tau_p}$ représente donc le gain net.

Cas 1 : sous le seuil laser

$G(N) < \frac{1}{\tau_p}$ Alors : $\frac{dE(t)}{dt} < 0$: Le champ décroît exponentiellement.

Cas 2 : au seuil

$G(N) = \frac{1}{\tau_p}$: Le gain compense exactement les pertes.

Cas 3 : au-dessus du seuil

$G(N) > \frac{1}{\tau_p}$: Le champ augmente rapidement jusqu'à ce que les effets non linéaires stabilisent le laser.

➤ Rôle du facteur α (Facteur de Henry)

Le terme $(1 + j\alpha)$ couple :

- L'amplitude du champ,
- La phase du champ.

Le facteur de Henry explique :

- L'élargissement de la largeur de raie,
- Le chirp en modulation directe,
- Les oscillations de fréquence.

Type de laser	Valeurs typiques
DFB télécom	2 à 6
Fabry-Pérot	3 à 8
VCSEL	1 à 5
Quantum Dot	0.5 à 3

Tableau III.2 : Valeurs pratiques de α

➤ Interprétation des termes dans l'équation des porteurs :

Injection électrique : $\frac{I}{qV}$ représente le nombre de porteurs injectés par unité de volume et par seconde.

Recombinaison spontanée : $\frac{N(t)}{\tau_s}$ correspond aux pertes de porteurs dues aux recombinaisons

Émission stimulée : $G(N)|E(t)|^2$ traduit la conversion des porteurs en photons laser.

Lorsque la puissance optique augmente les porteurs sont davantage consommés.

➤ Approximation linéaire du gain

On écrit souvent :

$$G(N) = g(N - N_0)$$

– Densité de transparence

$$\text{À : } N = N_0 \quad \text{on a : } G = 0$$

Le matériau est transparent.

- Pas d'amplification.
- Pas d'absorption nette.

– Gain différentiel $g = \frac{dG}{dN}$

Il mesure la sensibilité du gain à une variation de densité de porteurs.

Plus g est grand :

- plus le laser répond vite,

- plus la fréquence de relaxation est élevée.

- Temps de vie des photons τ_p représente la durée moyenne de présence d'un photon dans la cavité.

Valeurs pratiques : Lasers télécom : $1 \text{ ps} \leq \tau_p \leq 10 \text{ ps}$

- Temps de vie des porteurs : τ_s temps moyen avant recombinaison.

Valeurs pratiques : Pour les lasers InGaAsP ou GaAs : $0.5 \text{ ns} \leq \tau_s \leq 5 \text{ ns}$

- Densité de porteurs : N nombre de porteurs par unité de volume. $N \approx 10^{17}$ à 10^{18} cm^{-3}

- Courant d'injection : I

Valeurs pratiques : pour une diode DFB le courant seuil est de 10-30 mA , celui du fonctionnement est de 30-100mA, fort au-delà de 100 mA.

III-3-2 Modèle avec Rétroaction : Formulation de Lang-Kobayashi

Lorsque la diode est soumise à une rétroaction optique externe, le modèle proposé par Roy Lang et Kobayashi introduit un terme retardé : [32, 33].

Équation du champ avec délai

$$\frac{dE(t)}{dt} = \frac{1}{2}(1 + j\alpha) \left[G(N) - \frac{1}{\tau_p} \right] E(t) + \kappa E(t - \tau) e^{-j\omega_0 \tau}$$

Équation des porteurs

$$\frac{dN(t)}{dt} = \frac{I}{qV} - \frac{N(t)}{\tau_s} - G(N)|E(t)|^2$$

Nouveaux paramètres

- κ : coefficient de rétroaction
- τ : délai externe (temps aller-retour)
- ω_0 : fréquence optique

La présence du terme retardé $E(t - \tau)$ transforme le système en équations différentielles à

retard ne (Delay Differential Equation, DDE), ce qui augmente considérablement la dimension dynamique effective et favorise l'apparition du chaos.

➤ Signification physique

Le modèle de Lang–Kobayashi est l'extension du modèle classique des équations de taux d'une diode laser lorsqu'une partie de la lumière émise est renvoyée vers la cavité par un réflecteur externe (miroir, fibre optique, surface réfléchissante, etc.).

Cette rétroaction introduit une mémoire temporelle dans le système : le laser dépend non seulement de son état actuel mais aussi de son état passé, ce qui explique l'apparition de dynamiques complexes (oscillations, bifurcations, chaos).

➤ Terme de rétroaction retardée $\kappa E(t - \tau)e^{-j\omega_0\tau}$

Le champ réinjecté $E(t - \tau)$ est celui qui a quitté la cavité un temps τ auparavant.

$$\tau = \frac{2L}{c/n}$$

où :

- L : longueur de la cavité externe,
- n : indice du milieu.

Distance miroir	τ
1 cm	67 ps
10 cm	0.67 ns
1 m	6.7 ns
10 m	67 ns

Tableau III.3 : Valeurs pratiques du délai pour une cavité externe dans l'air ($n \simeq 1$)

Longueur fibre	τ
1 m	10 ns
10 m	100 ns
100 m	1 μ s

Tableau III.4 : Valeurs pratiques du délai pour une fibre optique ($n \approx 1.5$)

➤ Interprétation du facteur de phase $e^{-j\omega_0\tau}$

Pendant le trajet extérieur, l'onde accumule une phase : $\phi = \omega_0\tau$

Cette phase détermine si la lumière réinjectée interfère constructivement ou destructivement avec le champ intracavité.

$$\omega_0 = 2\pi f_0 \quad , \quad f_0 = \frac{c}{\lambda}$$

Exemple pour $\lambda = 1550$ nm : $f_0 = 193.1 \times \text{THz}$

➤ Coefficient de rétroaction κ

Mesure la fraction du champ renvoyée vers le laser. Plus κ augmente, plus l'influence de la cavité externe devient importante. C'est le paramètre qui pilote le chaos.

○ Régimes pratiques

Faible rétroaction $107 \lesssim \kappa \lesssim 109$: laser quasi-stable

Rétroaction modérée $109 < \kappa \lesssim 1010$: oscillations périodiques

Rétroaction forte $1010 < \kappa \lesssim 1011$: quasi-périodicité

Rétroaction très forte $1010 < \kappa \lesssim 1012$: chaos

III-4 Caractérisation qualitative et quantitative - Résultats de simulation

Les simulations ont été conduites sous Matlab. Le code est donné en Annexe.

III-4-1 Diagramme de bifurcation

La bifurcation décrit le changement de régime dynamique lorsqu'un paramètre varie ; ici le paramètre de contrôle est le niveau de rétroaction. On observe souvent : un régime stable ; puis un régime périodique ; ensuite un doublement de période et enfin le chaos. Ce scénario est appelé route vers le chaos par cascade de doublement de période.

La figure III.2 illustre le diagramme de bifurcation de la diode laser en fonction du gain de rétroaction k . Les résultats montrent que l'apparition du chaos intervient à partir de $k = 7.75735 \times 10^{11}$. Par ailleurs, l'intensité du comportement chaotique s'accroît avec l'augmentation de k . Néanmoins, l'analyse n'a pas pu être étendue à des valeurs plus importantes de ce paramètre en raison des ressources de calcul limitées disponibles pour la réalisation des simulations.

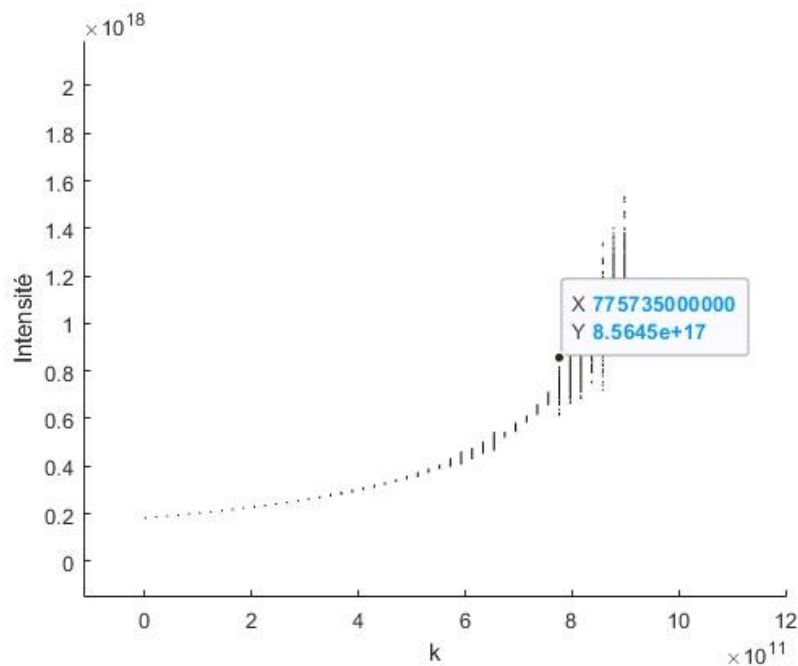


Figure III.2-Diagramme de bifurcation en fonction du paramètre de contrôle k

Nous présentons ci-après les résultats obtenus pour diverses valeurs de k , chacune caractérisant un régime de comportement particulier.

III-4-2 Comportement périodique (Attracteur cycle limite) pour une rétroaction $k = 10^9$

Le système présente un régime périodique, comme l'illustre l'évolution temporelle de l'intensité du signal optique à la sortie de la diode (Figure III.3, Figure III.4 et Figure III.5)

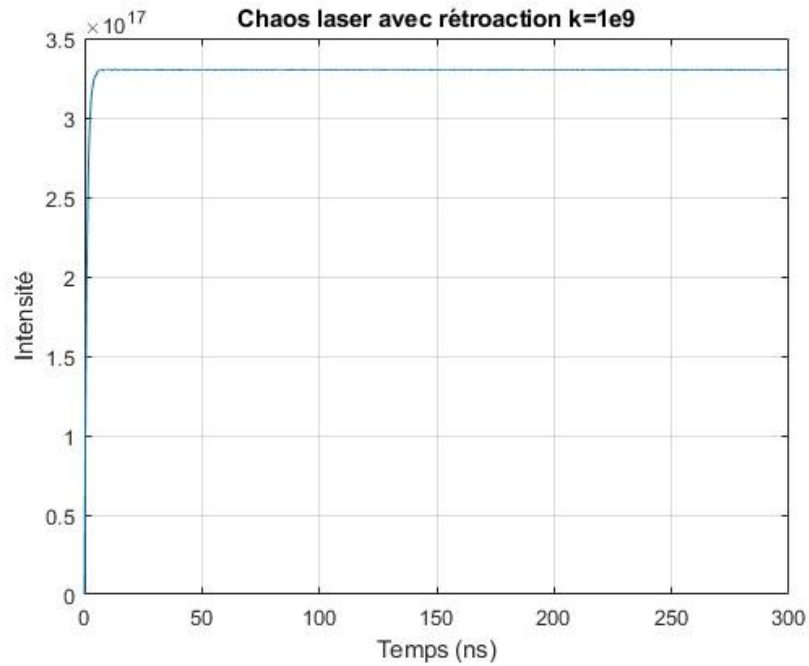


Figure III.3: Représentation temporelle de l'intensité du signal optique pour $k = 10^9$

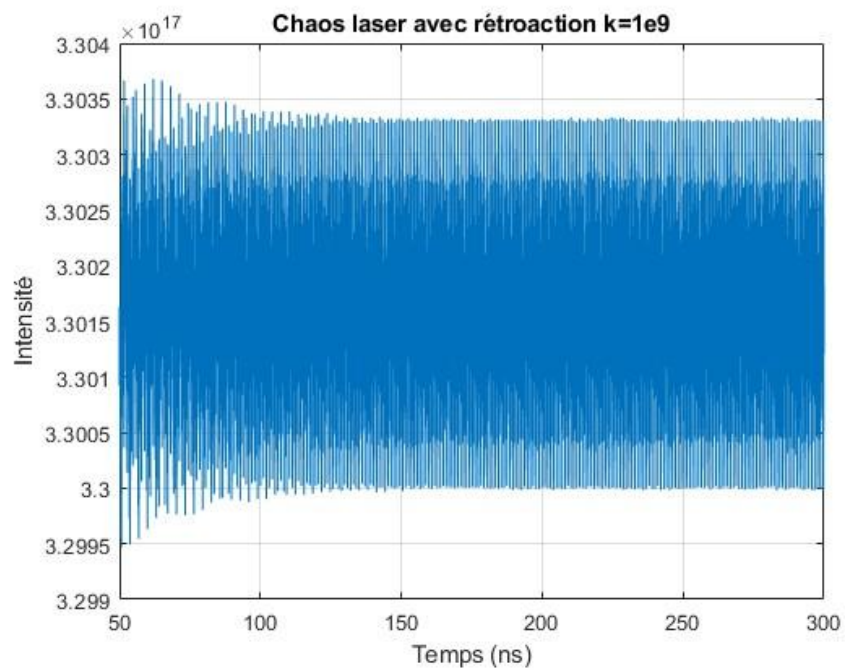


Figure III.4: Représentation temporelle de l'intensité du signal optique pour $k = 10^9$
Zoom 50-300 ns

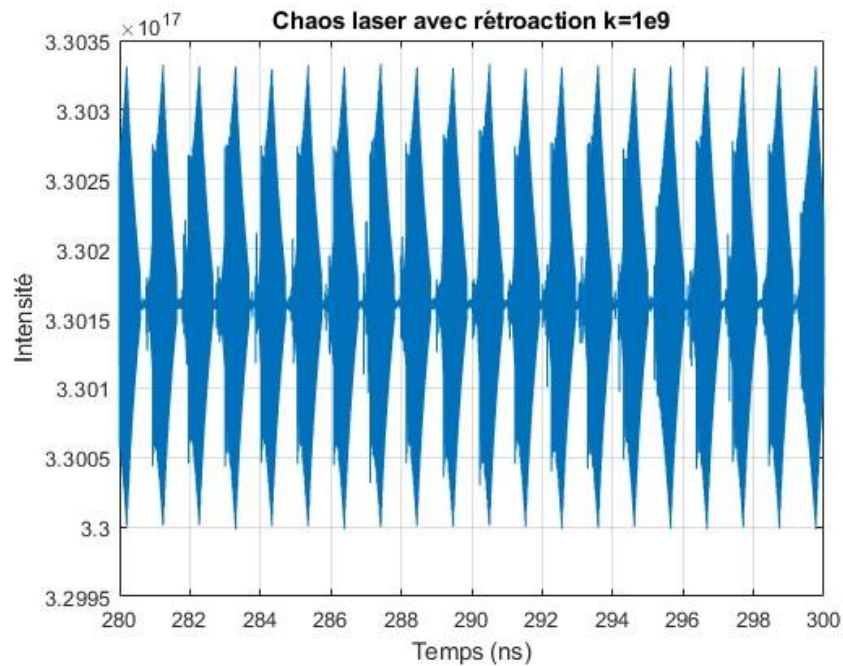


Figure III.5-Représentation temporelle de l'intensité du signal optique pour $k = 10^9$
Zoom 280-300 ns

Le spectre correspondant est marqué par la présence d'une fréquence, ce qui constitue une signature caractéristique d'un comportement périodique (Figure III.6).

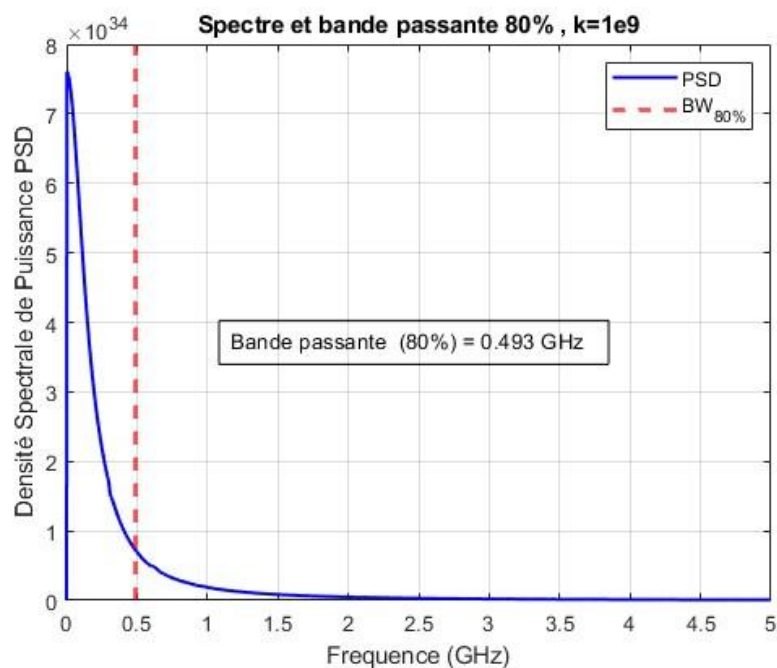


Figure III.6-Représentation de la densité spectrale de puissance de l'intensité du signal optique

pour $k = 10^9$

Par ailleurs, la représentation dans le plan de phase révèle un attracteur de type cycle limite (Figure III.8) confirmant ainsi la nature périodique de la dynamique du système.

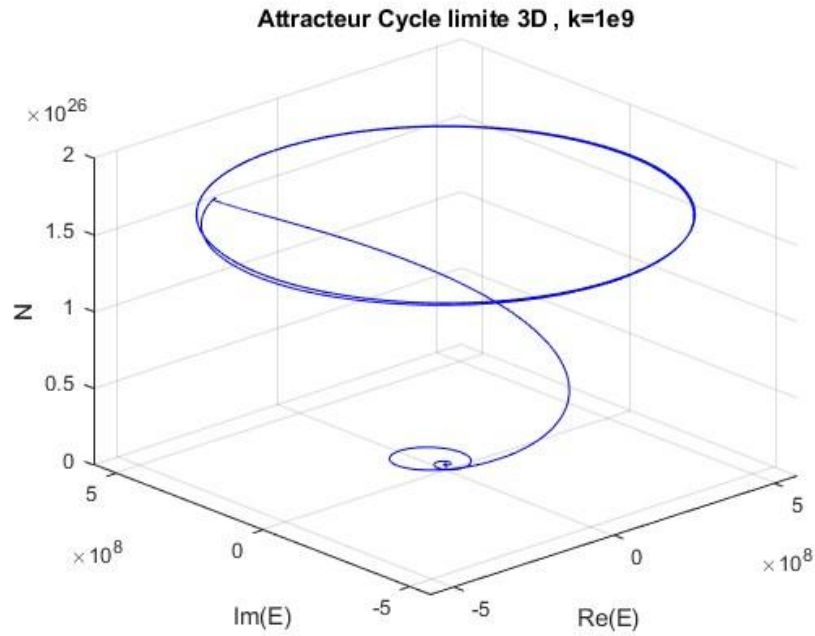


Figure III.7-Diagramme de phase 3D $k = 10^9$

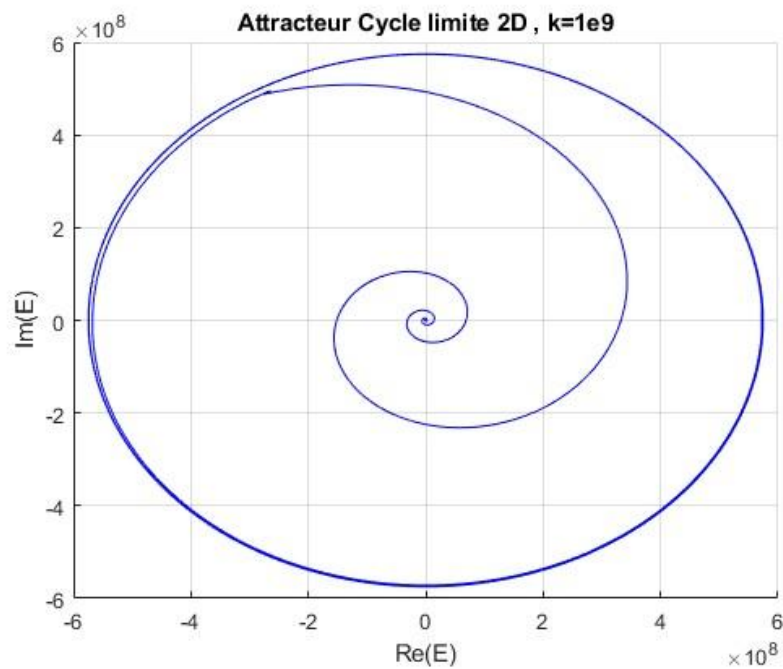


Figure III.8-Diagramme de phase 2D pour $k = 10^9$

III-4-3 Comportement périodique (Attracteur cycle limite) pour une rétroaction $k = 6.10^9$

À l'instar du cas précédent, les figures III.9 et III.10 montrent que l'intensité du signal optique à la sortie de la diode évolue selon un régime périodique.

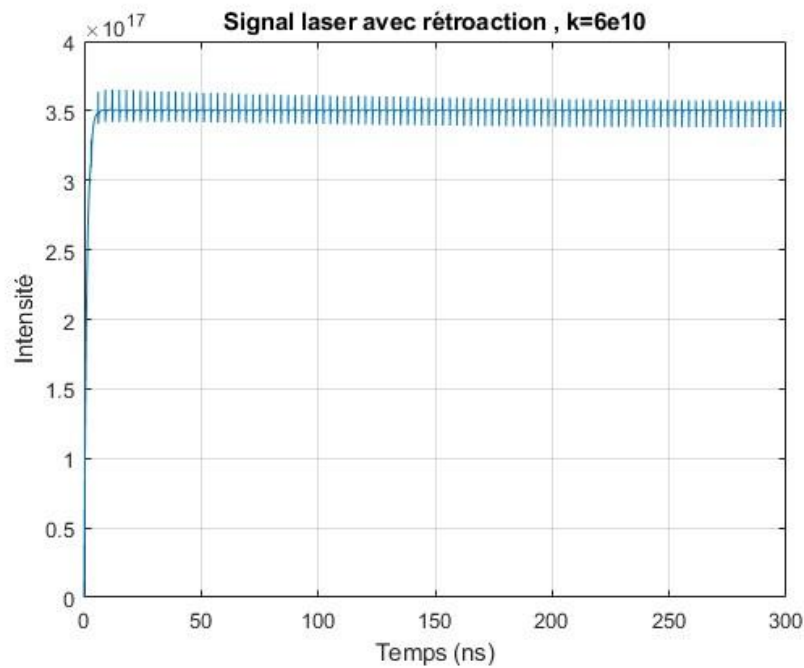


Figure III.9-Représentation temporelle de l'intensité du signal optique pour $k = 6.10^9$

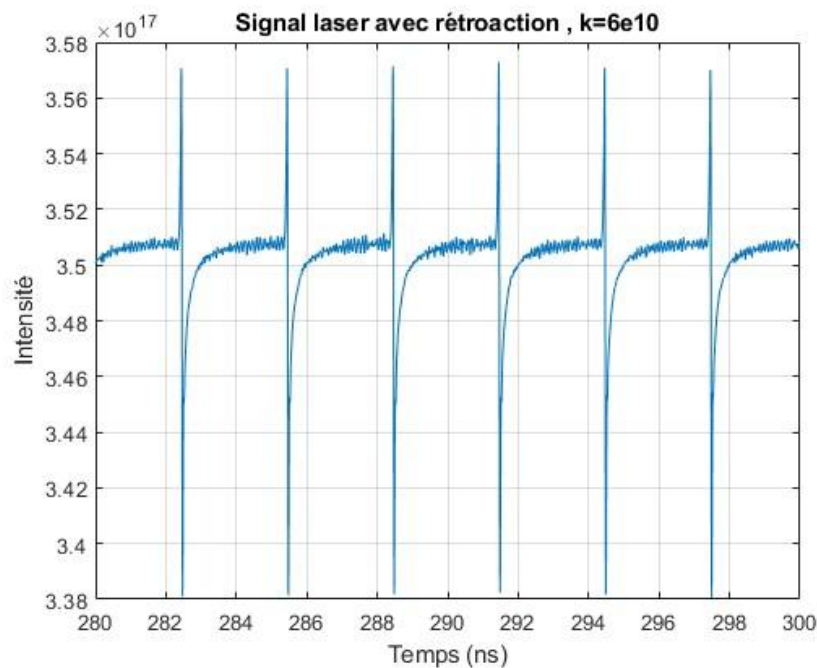


Figure III.10-Représentation temporelle de l'intensité du signal optique pour $k = 6.10^9$
Zoom 280-300 ns

Cette périodicité est confirmée par l'analyse spectrale (Figure III.11), qui met en évidence une fréquence fondamentale ainsi qu'un ensemble d'harmoniques.

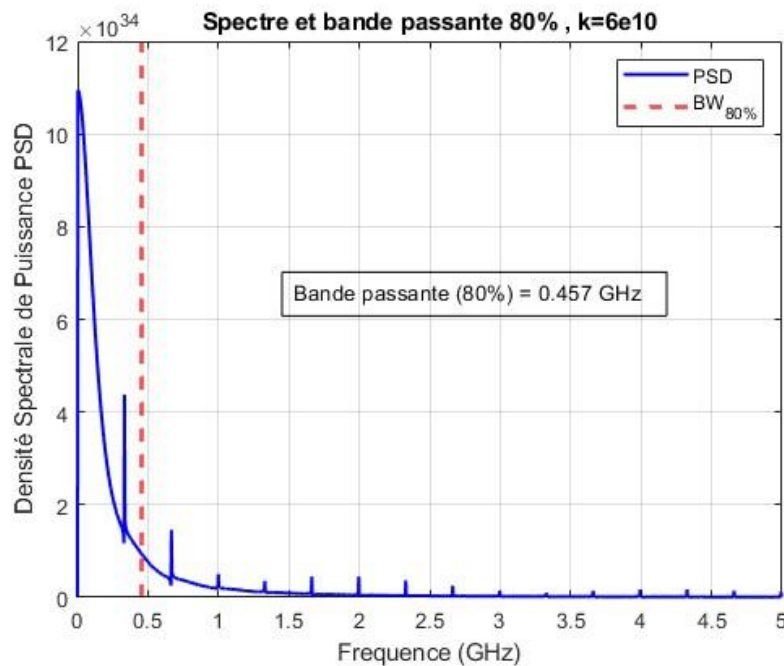


Figure III.11-Représentation de la densité spectrale de puissance de l'intensité du signal optique pour $k = 6.10^9$

En outre, l'attracteur observé dans le plan de phase (Figure III.13) prend la forme d'un cycle limite, caractéristique d'un comportement périodique stable.

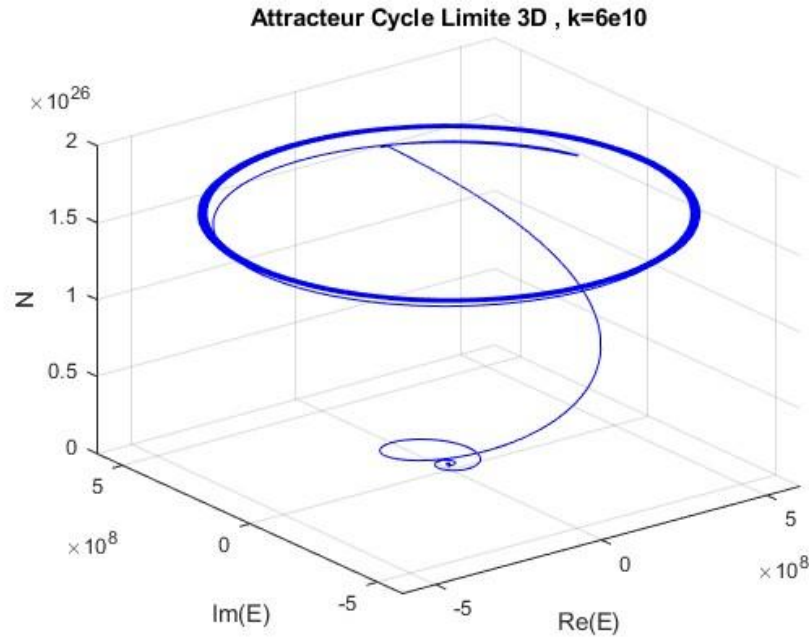


Figure III.12-Diagramme de phase 3D pour $k = 6.10^9$

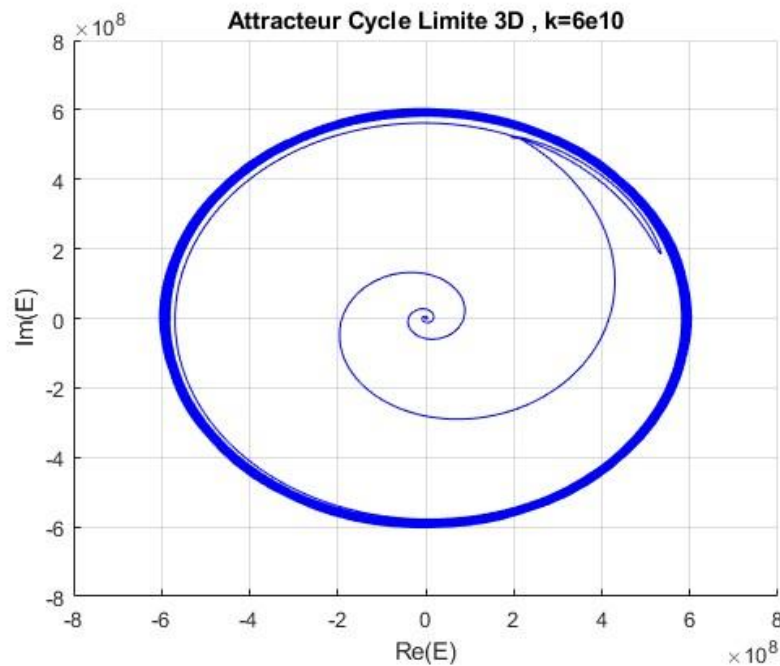


Figure III.13-Diagramme de phase 2D pour $k = 6.10^9$

III-4-4 Comportement quasi- périodique (Attracteur tore) pour une rétroaction $k = 10^{11}$

Les figures III.14 et III.15 mettent en évidence un régime quasi-périodique de l'intensité du signal optique à la sortie de la diode. Contrairement au régime périodique, où l'évolution temporelle est gouvernée par une seule fréquence fondamentale, le signal observé ici résulte de la superposition

de plusieurs oscillations de fréquences incommensurables. Cette caractéristique se traduit par une dynamique plus complexe, sans toutefois présenter le caractère imprévisible propre au chaos.

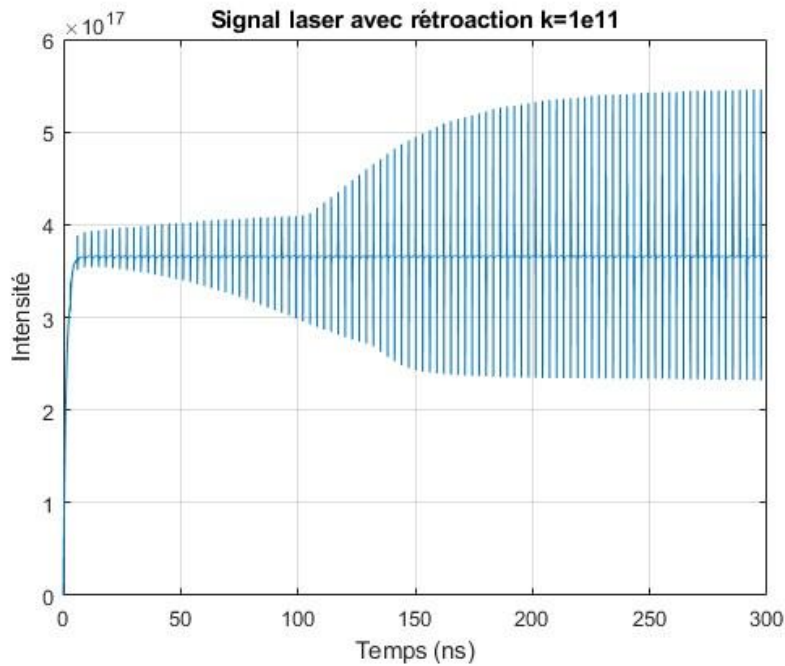


Figure III.14-Représentation temporelle de l'intensité du signal optique pour $k = 10^{11}$

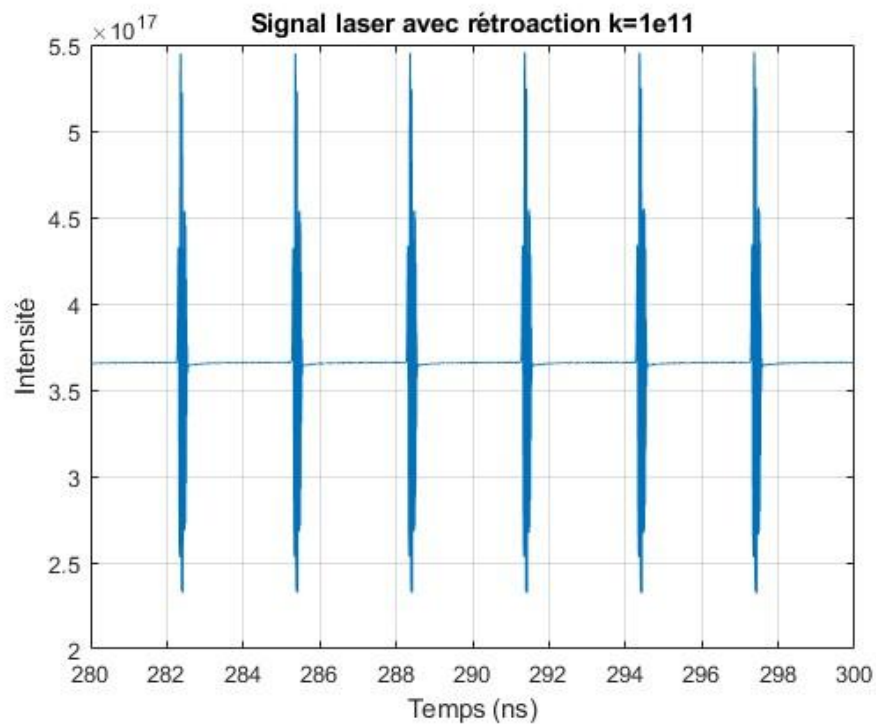


Figure III.15-Représentation temporelle de l'intensité du signal optique pour $k = 10^{11}$
Zoom 280-300 ns

L'analyse spectrale, présentée à la figure III.17, confirme ce comportement en révélant la présence de plusieurs fréquences fondamentales accompagnées de leurs harmoniques respectives. La coexistence de ces composantes fréquentielles traduit l'existence de plusieurs échelles temporelles dans la dynamique du système. Par ailleurs, l'apparition successive de nouvelles fréquences peut conduire à une complexification progressive du mouvement. Ce mécanisme constitue l'une des voies classiques menant au chaos, connue sous le nom de bifurcation par quasi-périodicité

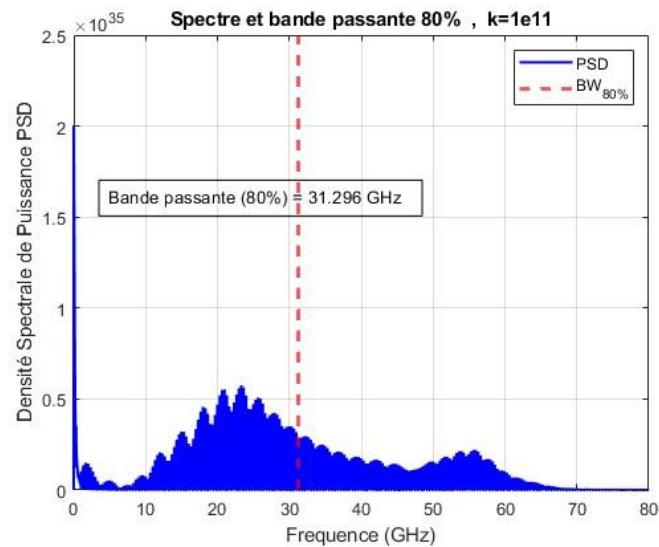


Figure III.16-Représentation de la densité spectrale de puissance de l'intensité du signal optique pour $k = 10^{11}$

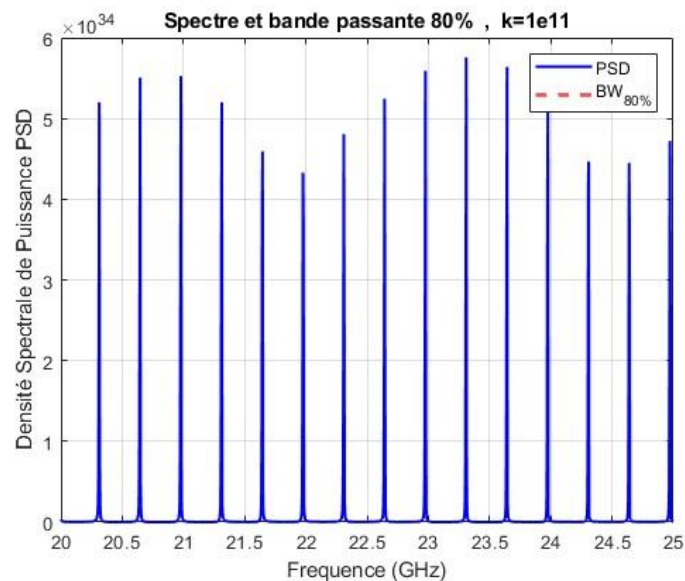


Figure III.17-Représentation de la densité spectrale de puissance de l'intensité du signal optique pour $k = 10^{11}$
Zoom 20-25 GHz

La représentation dans le plan de phase (figure III.19) apporte également des informations importantes sur la nature de la dynamique observée. L'attracteur obtenu présente une structure toroïdale, caractéristique d'un mouvement quasi-périodique. Plus précisément, il s'agit d'un attracteur de type tore de dimension supérieure ou égale à deux, traduisant l'interaction simultanée de plusieurs fréquences indépendantes. Cette géométrie confirme ainsi que le système se trouve dans un régime quasi-périodique, situé à la frontière entre le comportement périodique et le régime chaotique.

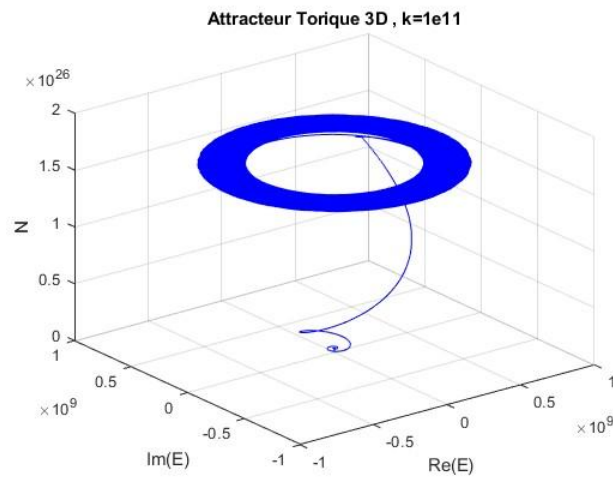


Figure III.18-Diagramme de phase 3D pour $k = 10^{11}$

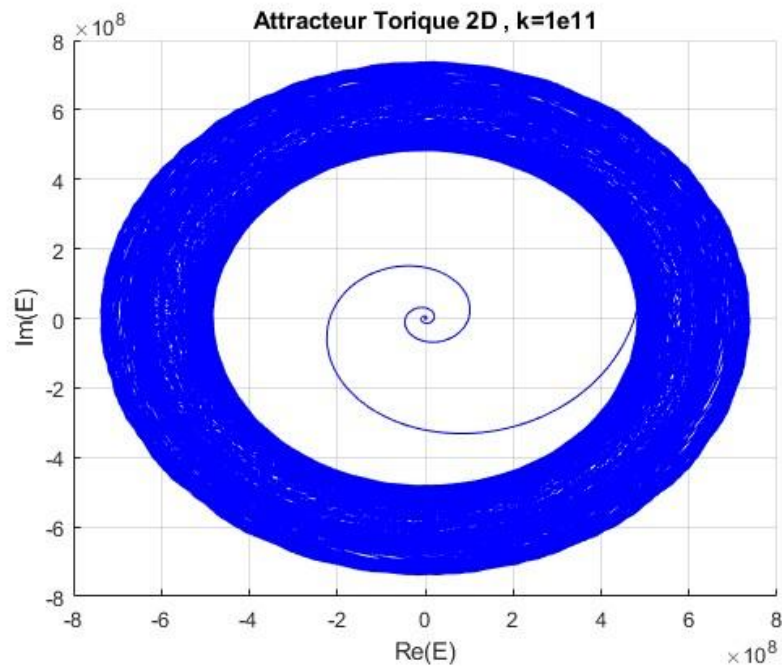


Figure III.19-Diagramme de phase 2D pour $k = 10^{11}$

III-4-5 Comportement chaotique (Attracteur étrange) pour une rétroaction $k = 10^{11}$

Les figures III.20 et III.21 mettent clairement en évidence que le système évolue dans un régime chaotique. Contrairement aux régimes périodiques ou quasi-périodiques étudiés précédemment, le signal optique présente ici des oscillations irrégulières et non répétitives, traduisant une dynamique complexe et fortement sensible aux conditions initiales. L'absence de périodicité apparente dans l'évolution temporelle constitue une première indication de la présence du chaos.

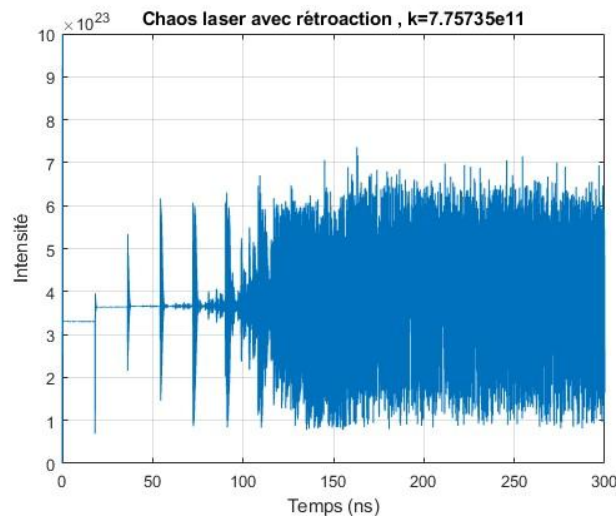


Figure III.20-Représentation temporelle de l'intensité du signal optique pour $k = 7.75735 \times 10^{11}$

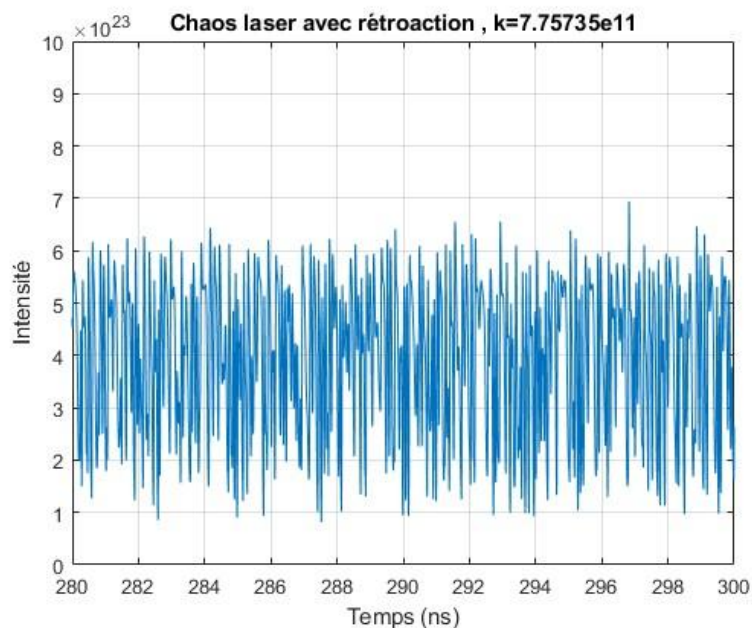


Figure III.21-Représentation temporelle de l'intensité du signal optique pour $k = 7.75735 \times 10^{11}$
Zoom 280-300 ns

Cette observation est appuyée par l'analyse fréquentielle du signal. En effet, la densité spectrale de puissance représentée à la figure III.22 présente un spectre continu et particulièrement dense, caractéristique des systèmes chaotiques. Contrairement aux régimes périodiques, où le spectre est composé d'un nombre limité de raies discrètes correspondant à la fréquence fondamentale et à ses harmoniques, le spectre observé ici couvre une large plage de fréquences, révélant une distribution énergétique étendue et complexe.

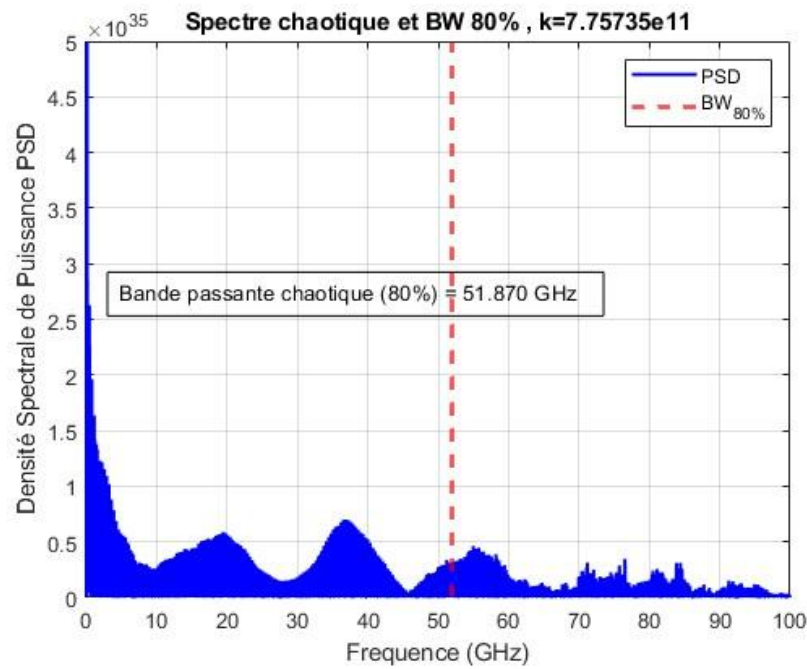


Figure III.22-Représentation de la densité spectrale de puissance de l'intensité du signal optique pour $k = 7.75735 \times 10^{11}$

L'étude du portrait de phase apporte également des informations essentielles sur la dynamique du système. L'attracteur présenté à aux figures III.23 et III.24 possède une géométrie complexe et non régulière, typique d'un attracteur étrange. Ce type d'attracteur est l'une des signatures fondamentales du chaos déterministe et traduit l'existence d'une dynamique bornée mais imprévisible à long terme.

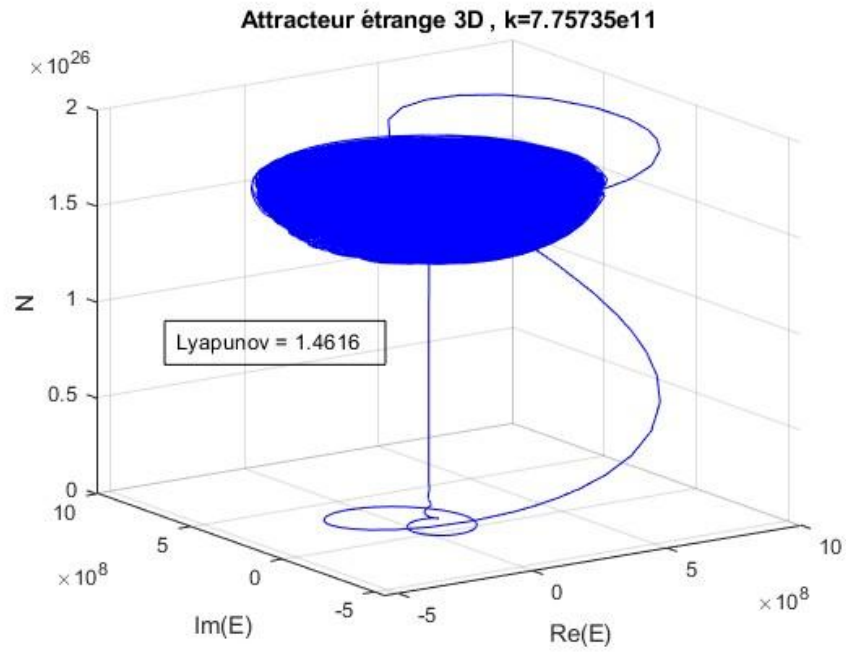


Figure III.23-Diagramme de phase 3D pour $k = 7.75735 * 10^{11}$

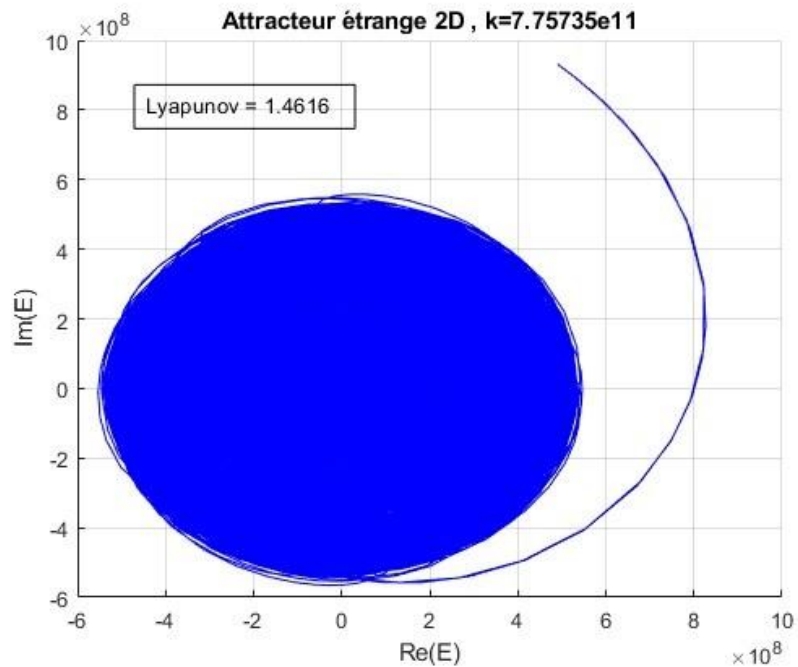


Figure III.24-Diagramme de phase 2D pour $k = 7.75735 * 10^{11}$

Toutefois, les analyses précédentes demeurent essentiellement qualitatives. Afin de caractériser de manière rigoureuse la complexité de la dynamique observée et de mettre en évidence son éventuel caractère hyper-chaotique, il est nécessaire de recourir à des indicateurs quantitatifs. Dans ce cadre, deux paramètres ont été déterminés : le plus grand exposant de Lyapunov et la largeur de bande chaotique.

Le plus grand exposant de Lyapunov constitue l'un des critères les plus utilisés pour détecter et quantifier le chaos. Il mesure la vitesse moyenne de divergence exponentielle de deux trajectoires initialement très proches dans l'espace des phases. Une valeur positive de cet exposant traduit une sensibilité aux conditions initiales et constitue ainsi une preuve directe de l'existence d'un comportement chaotique. Dans notre étude, la valeur obtenue est égale à $\lambda = 1,4616$. Cette valeur positive relativement élevée confirme sans ambiguïté la nature chaotique de la dynamique du système et témoigne d'un degré important de complexité dynamique.

Par ailleurs, la largeur de bande chaotique représente un indicateur complémentaire particulièrement pertinent pour l'évaluation des performances des systèmes photoniques chaotiques. Elle est définie comme l'intervalle de fréquences contenant 80 % de l'énergie totale du spectre de puissance du signal optique émis par le laser. Une largeur de bande élevée traduit une répartition énergétique sur une large gamme de fréquences et constitue généralement un indicateur de la richesse spectrale du signal chaotique.

Pour la valeur de rétroaction $k = 7,75735 \times 10^{11}$, la largeur de bande chaotique à 80 % a été estimée à environ 51,87 GHz. Cette valeur particulièrement importante met en évidence l'étendue spectrale du signal généré et confirme le fort niveau de complexité de la dynamique observée. Un tel résultat est particulièrement intéressant pour des applications telles que les communications sécurisées par chaos. L'ensemble des résultats obtenus, tant qualitatifs que quantitatifs, démontre ainsi que le système étudié est capable de produire un chaos développé, caractérisé par une forte sensibilité aux conditions initiales et une large extension fréquentielle.

III-5 Chiffrement-déchiffrement

Dans le système proposé, le procédé de sécurisation des données repose sur l'utilisation d'un signal chaotique généré optiquement et exploité comme porteuse de chiffrement. Cette technique permet de masquer efficacement l'information utile au sein d'un signal présentant un comportement complexe et

imprévisible, rendant ainsi son interception ou sa reconstruction extrêmement difficile pour un observateur non autorisé.

Les opérations de chiffrement et de déchiffrement ont été réalisées sous Optisystem (Figure III.25). Le même fichier contenant le signal chaotique généré sous Matlab est utilisé pour le chiffrement et le déchiffrement.

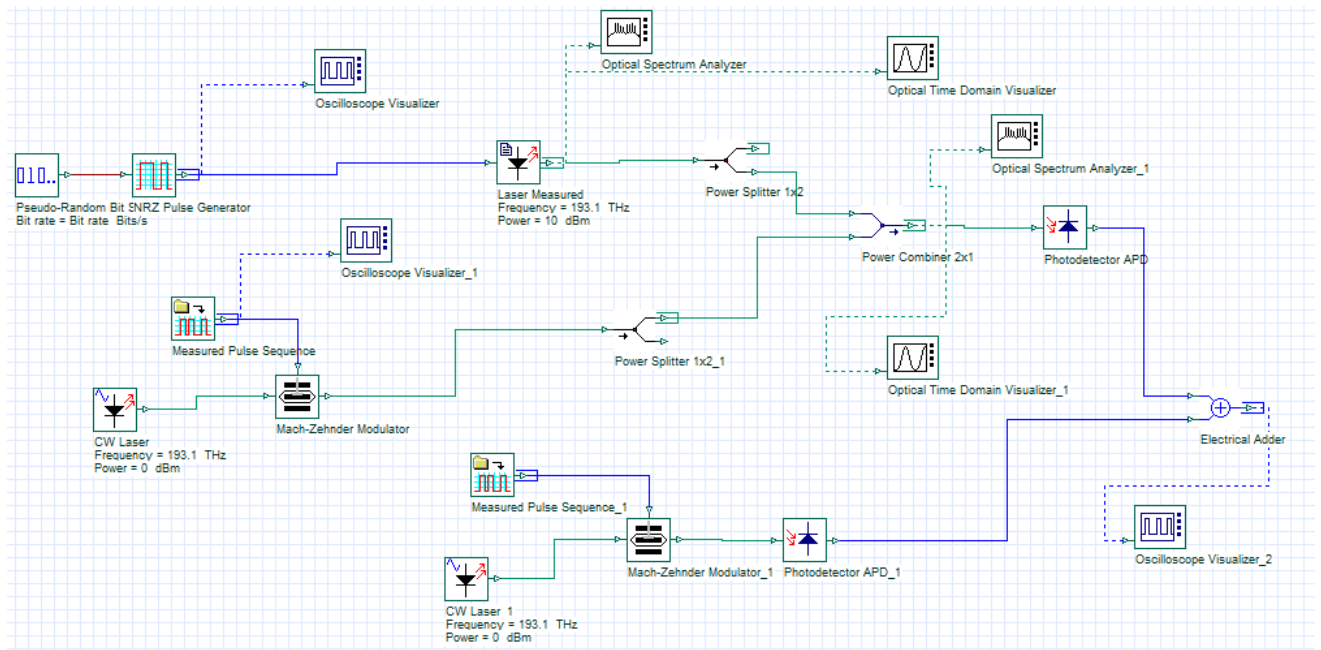


Figure III.25- Schéma du chiffrement-déchiffrement réalisé sous Optisystem

III-5-1 Procédure de chiffrement au niveau de l'émetteur

Le signal chaotique obtenu est appliqué à l'entrée d'un modulateur électro-optique de type Mach-Zehnder Modulator (MZM). Le rôle de ce composant est de convertir les variations électriques du signal chaotique en variations de phase ou d'intensité du signal optique propagé dans la fibre.

Parallèlement, le message d'information à transmettre module une source optique distincte. Le signal porteur de l'information est alors combiné optiquement avec le signal chaotique modulé. Cette opération de combinaison permet de masquer complètement l'information utile à l'intérieur de la dynamique chaotique. Les figures III.26, III.27 et III.29 présentent respectivement les différentes étapes de génération du message, de sa modulation et de combinaison optique des deux signaux chaotique et d'information.

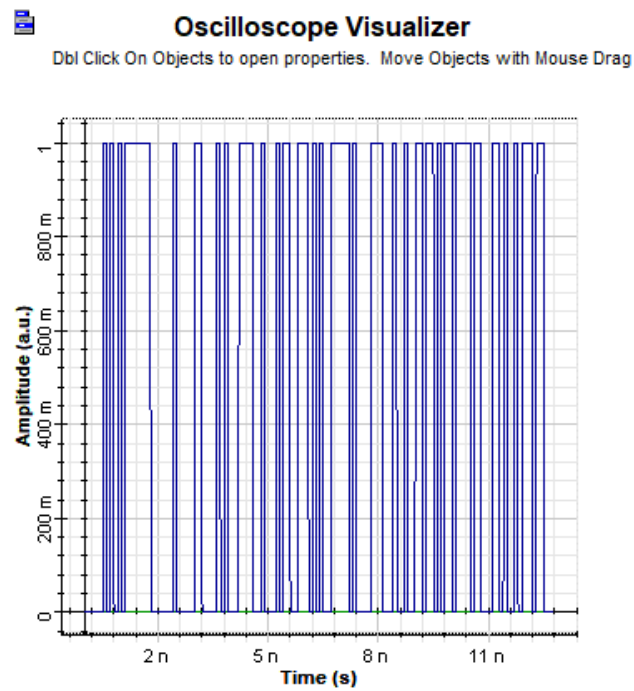


Figure III.26-Message d'information émis, code NRZ

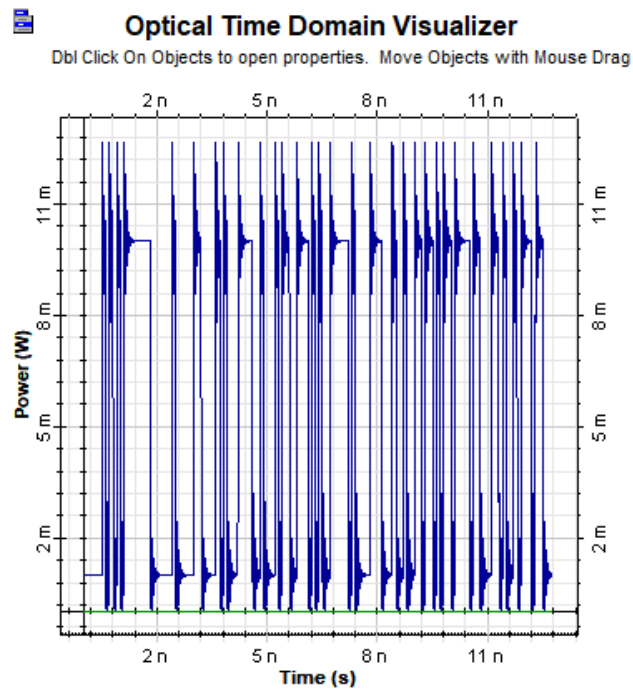


Figure III.27-Signal optique modulé par le message émis

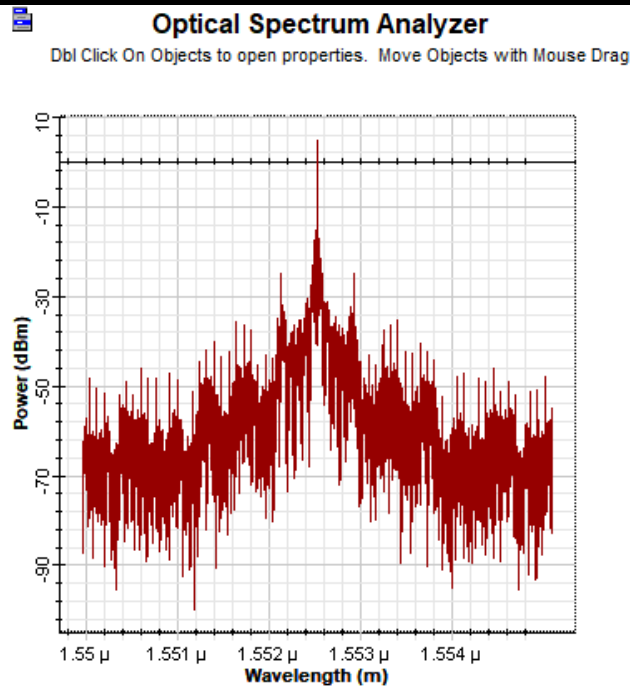


Figure III.28-Spectre du signal optique modulé par le message émis

Le résultat de cette opération est un signal optique chiffré dont l'apparence temporelle est fortement dominée par les caractéristiques du chaos. Ainsi, il devient pratiquement impossible de distinguer visuellement ou spectralement le message transmis. Le signal obtenu, représenté à la figure III.29, constitue le signal effectivement injecté dans le canal de transmission optique.

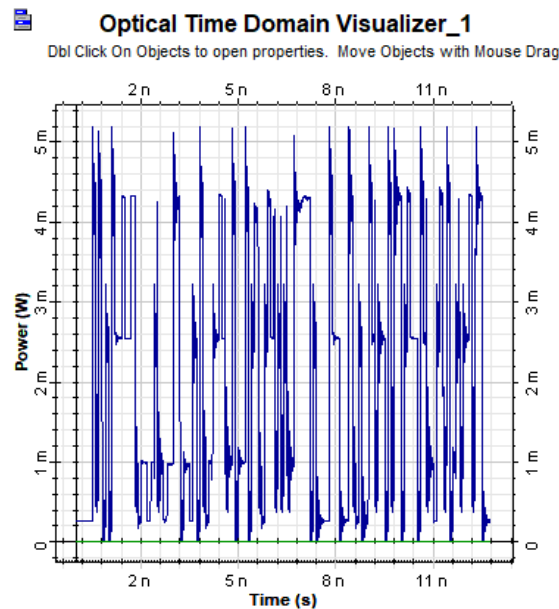


Figure III.29-Signal optique chiffré

L'utilisation du chaos comme masque de sécurité présente plusieurs avantages. D'une part, la nature déterministe mais imprévisible du signal chaotique garantit un niveau élevé de confidentialité. D'autre

part, la largeur de bande importante du chaos permet d'améliorer la robustesse du système face aux tentatives d'écoute ou d'analyse spectrale.

III-5-2 Transmission du signal chiffré

Après son élaboration, le signal optique chiffré est transmis à travers la liaison de communication. Durant cette phase, le message demeure totalement dissimulé sous l'enveloppe chaotique. Pour un observateur extérieur ne disposant pas des paramètres exacts du générateur chaotique utilisé à l'émission, le signal reçu apparaît comme un bruit complexe dépourvu d'information exploitable.

Cette propriété constitue le fondement même de la sécurité du système. En effet, la récupération du message nécessite non seulement la connaissance de l'architecture du système mais également une reproduction fidèle du signal chaotique utilisé lors du chiffrement.

III-5-3 Procédure de déchiffrement au niveau du récepteur

Au niveau du récepteur, le signal optique chiffré reçu est tout d'abord converti en signal électrique à l'aide d'une photodiode. Cette étape de détection optoélectronique permet d'obtenir une représentation électrique du signal transmis contenant simultanément la composante chaotique et le message masqué.

Afin de récupérer l'information originale, un second générateur chaotique identique à celui de l'émetteur est utilisé. Grâce au phénomène de synchronisation chaotique, ce générateur reproduit localement une réplique du signal chaotique ayant servi au chiffrement.

Le signal chaotique répliqué est ensuite appliqué à un second modulateur Mach-Zehnder. Après conversion et traitement appropriés, les signaux issus du canal de transmission et du générateur local sont combinés par addition algébrique.

Cette opération exploite le principe de compensation du chaos. Lorsque les conditions de synchronisation sont satisfaites, les deux composantes chaotiques sont pratiquement identiques mais de signes opposés. Leur combinaison conduit alors à leur annulation mutuelle, laissant apparaître uniquement le message d'information initial.

La figure III.30 illustre le signal récupéré après déchiffrement. On observe que la forme du message obtenu est très proche de celle du signal original transmis, démontrant ainsi l'efficacité du mécanisme de synchronisation et de compensation du chaos.

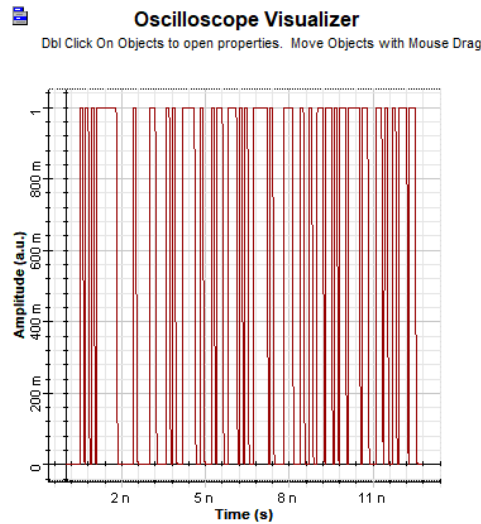


Figure III.30-Message reçu déchiffré, code NRZ

III-5-4 Analyse des performances du système

Les résultats obtenus montrent que les opérations de chiffrement et de déchiffrement sont réalisées avec succès. Le signal transmis est efficacement masqué par le chaos et demeure inintelligible durant toute la phase de propagation. Après réception et traitement, le message est correctement reconstruit grâce à la synchronisation entre les générateurs chaotiques de l'émetteur et du récepteur.

L'efficacité du système dépend toutefois fortement de la qualité de cette synchronisation. Une faible différence entre les paramètres des deux générateurs peut entraîner une dégradation significative de la qualité du signal récupéré. Par conséquent, le maintien d'une synchronisation précise constitue une condition essentielle au bon fonctionnement du procédé.

Les simulations réalisées démontrent également que le système présente une bonne résistance aux techniques classiques d'interception. En raison de la complexité intrinsèque du signal chaotique et de la difficulté de reproduire ses paramètres exacts, la récupération du message par un utilisateur non autorisé devient extrêmement complexe.

III-6 Conclusion

L'intérêt des diodes laser dans la génération de chaos optique complexe provient du fait qu'elles constituent des systèmes dynamiques non linéaires capables de produire des comportements chaotiques à très haute vitesse (GHz à plusieurs dizaines de GHz), tout en restant compactes, peu coûteuses et facilement intégrables.

En particulier, les diodes laser à retard permettent d'avoir un chaos particulièrement intéressant :

- Très grande bande passante : Les constantes de temps τ_p , τ_s sont extrêmement faibles ce qui conduit à des fréquences caractéristiques d'environ 50 GHz, voire davantage. Les systèmes électroniques classiques atteignent difficilement de telles vitesses.
- Grande dimension : Avec une rétroaction retardée $\tau \gg \tau_p$, le système devient effectivement de dimension très élevée avec une sensibilité aux conditions initiales élevée (hyperchaotique).

A travers cette étude, nous avons utilisé le système de Lang-Kobayashi pour montrer numériquement que l'introduction d'une rétroaction optique retardée transforme la dynamique d'une diode laser en un système capable de générer un chaos déterministe caractérisé par un attracteur étrange, un spectre continu large bande et un exposant de Lyapunov positif. Les paramètres clés de contrôle ont été identifiées.

Cette étude met également en évidence l'intérêt de l'utilisation des systèmes chaotiques dans les communications optiques sécurisées. Le procédé de chiffrement consiste à masquer le message à l'aide d'un signal chaotique généré à l'émission, tandis que le déchiffrement repose sur la reconstruction locale de ce même chaos au niveau du récepteur. Les résultats obtenus confirment la faisabilité et l'efficacité de cette approche pour la protection des informations transmises dans les réseaux optiques modernes.

Le succès des opérations de chiffrement et de déchiffrement repose néanmoins sur l'hypothèse fondamentale de synchronisation parfaite entre les systèmes chaotiques de l'émetteur et du récepteur. Lorsque cette condition est respectée, le message original peut être récupéré avec une très faible erreur, garantissant ainsi une transmission à la fois fiable et sécurisée.

Conclusion Générale

L'objectif principal de ce mémoire était d'étudier la génération de chaos optique à partir d'une diode laser à rétroaction et d'exploiter ce phénomène pour la réalisation d'un cryptosystème optique sécurisé. Cette démarche s'inscrit dans le contexte du développement de nouvelles solutions de sécurisation des communications capables de répondre aux exigences croissantes de confidentialité et de rapidité des réseaux modernes.

Dans un premier temps, nous avons présenté les fondements théoriques des systèmes dynamiques non linéaires et des systèmes chaotiques. Cette étude a permis de mettre en évidence les propriétés essentielles du chaos, notamment la sensibilité aux conditions initiales, l'imprévisibilité, les bifurcations et la présence d'attracteurs étranges. Ces caractéristiques constituent les éléments fondamentaux qui rendent les systèmes chaotiques particulièrement attractifs pour les applications cryptographiques.

Nous avons ensuite étudié les principes du chiffrement par chaos ainsi que les spécificités des cryptosystèmes chaotiques optiques. L'analyse bibliographique a montré que les signaux chaotiques possèdent plusieurs propriétés recherchées dans le domaine de la sécurité de l'information : comportement pseudo-aléatoire, large bande spectrale, forte complexité dynamique et difficulté de prédiction. Ces propriétés permettent de masquer efficacement les informations transmises tout en conservant des débits compatibles avec les systèmes de communication optiques actuels.

La partie centrale de ce travail a porté sur la modélisation et la simulation d'une diode laser à rétroaction optique à l'aide du modèle de Lang-Kobayashi. Les simulations réalisées sous MATLAB ont permis d'étudier l'influence du coefficient de rétroaction sur la dynamique du système. L'analyse du diagramme de bifurcation a montré une succession de régimes dynamiques comprenant des comportements périodiques, quasi-périodiques puis chaotiques lorsque le niveau de rétroaction augmente.

Les résultats obtenus ont notamment mis en évidence :

- Régime périodique stable pour des valeurs de rétroaction de l'ordre de $k = 10^9$ et $k = 6 \times 10^9$, caractérisé par un cycle limite dans le plan de phase et un spectre constitué de fréquences discrètes ;
- Régime quasi-périodique pour $k = 10^{11}$, associé à un attracteur toroïdal et à la présence de plusieurs fréquences fondamentales dans le spectre ;
- L'apparition du chaos pour une valeur critique du coefficient de rétroaction voisine de $k = 7,75735 \times 10^{11}$.

L'analyse qualitative du régime chaotique a révélé des oscillations irrégulières, un spectre continu à large bande et la présence d'un attracteur étrange dans l'espace des phases. Ces observations ont été confirmées quantitativement par le calcul du plus grand exposant de Lyapunov, dont la valeur obtenue est : $\lambda = 1,4616$

Cette valeur positive confirme sans ambiguïté la présence d'un comportement chaotique et traduit une forte divergence des trajectoires initialement voisines.

Par ailleurs, l'étude spectrale a permis d'évaluer la largeur de bande chaotique contenant 80 % de l'énergie totale du signal. Pour la valeur de rétroaction correspondant au régime chaotique développé, cette largeur de bande a été estimée à : $B_{80} \approx 51,87$ GHz

Cette bande passante particulièrement importante témoigne de la richesse fréquentielle du signal généré et constitue un atout majeur pour les applications de communication sécurisée à haut débit.

Dans la dernière partie de ce mémoire, le signal chaotique obtenu a été utilisé pour réaliser un système de chiffrement et de déchiffrement optique simulé sous OptiSystem. Le chaos généré a servi de masque pour dissimuler un message numérique codé en NRZ. Les résultats ont montré que le signal d'information devient totalement indiscernable après chiffrement, tandis que le processus de synchronisation chaotique permet une récupération correcte du message au niveau du récepteur. Les simulations ont ainsi démontré la faisabilité du procédé de chiffrement-déchiffrement ainsi que l'efficacité de la synchronisation pour restituer fidèlement l'information transmise.

L'ensemble des résultats obtenus confirme donc que la diode laser à rétroaction constitue une source efficace de chaos optique à large bande et que ce chaos peut être exploité avec succès dans des applications de cryptographie optique. Le système étudié combine à la fois une forte complexité dynamique, une grande sensibilité aux conditions initiales et une large extension fréquentielle, autant de propriétés favorables à la sécurisation des communications.

Les travaux réalisés dans ce mémoire ouvrent plusieurs perspectives de recherche particulièrement intéressantes.

Une première perspective consiste à développer un modèle complet de synchronisation entre deux diodes laser chaotiques distinctes, l'une utilisée à l'émission et l'autre à la réception. Une telle étude permettrait d'évaluer plus précisément l'influence des écarts paramétriques sur les performances du système et sur la qualité de récupération du message.

Une seconde perspective concerne l'évaluation quantitative des performances cryptographiques du système. Des indicateurs tels que le taux d'erreur binaire (BER), le facteur Q , le rapport signal sur bruit (SNR), la corrélation résiduelle ou encore la capacité de résistance aux attaques statistiques pourraient être étudiés afin de caractériser plus rigoureusement le niveau de sécurité obtenu.

Il serait également intéressant d'explorer des architectures plus complexes basées sur le couplage de plusieurs diodes laser ou sur l'utilisation de multiples boucles de rétroaction. Ces configurations pourraient conduire à la génération d'hyper-chaos caractérisé par plusieurs exposants de Lyapunov positifs et offrir ainsi un niveau de sécurité encore plus élevé.

Enfin, une validation expérimentale sur une plateforme photonique réelle représenterait une étape importante pour confirmer les résultats obtenus par simulation et évaluer les performances du cryptosystème dans des conditions pratiques de fonctionnement.

Ainsi, les travaux présentés dans ce mémoire démontrent que l'utilisation du chaos optique généré par une diode laser à rétroaction constitue une voie particulièrement prometteuse pour le développement de systèmes de chiffrement performants destinés aux communications optiques sécurisées de nouvelle génération.

Bibliographie

- [1] 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).
- [2] R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," *IEEE J. Quantum Electron.* vol. 16, pp. 347–355, 1980
- [3] V. Annovazzi-Lodi, S. Donati, and A. Scire, "Synchronization of chaotic lasers by optical feedback for cryptographic applications," *IEEE J. Quantum Electron.*, vol. 33, no. 9, pp. 1449– 1454, Sep. 1994.
- [4] M.S.Baptista, "Cryptography with Chaos", *Physics Letters A*, vol. 240, pp. 50–54, 1998.
- [5] L. Larger, J.-P. Goedgebuer, and F. Delorme, "Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator," *Phys. Rev. E*, vol. 57, no. 6, pp. 6618– 6624, Jun. 1998.
- [6] I. Fischer, Y. Liu, and P. Davis, "Synchronization of chaotic semiconductor laser dynamics on subnanosecond time scales and its potential for chaos communication," *Phys. Rev. A*, vol. 62, no. 1, pp. 011801-1 – 011801-4, Jun. 2000.
- [7] S. Sivaprakasam and K. A. Shore, "Message encoding and decoding using chaotic external- cavity diode lasers," *IEEE J. Quantum Electron.*, vol. 36, no. 1, pp. 35–39, Mar. 2000.
- [8] H. D. I. Abarbanel, M. B. Kennel, S. Illing, L. Tang, H. F. Chen, and J. M. Liu, "Synchronization and communication using semiconductor lasers with optoelectronic feedback," *IEEE J. Quantum Electron.*, vol. 37, no. 10, pp. 1301–1311, Oct. 2001.
- [9] Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I., García-Ojalvo, J., Mirasso, C. R., Pesquera, L. & Shore, K. A. Chaos-based communications at high bit rates using commercial fibre-optic links. *Nature* **438**, 343-346, 2005.
- [10] J.D.Farmer, Chaotic attractors of infinite-dimensional dynamical system, *Physica D*, 4, 366-393 (1982).
- [11] M. Nourine, M. Peil & L. Larger, Chaos g'en'er'e par une non linéarité 2D et une dynamique à retard, *Comptes-Rendu des Rencontres du Non Linéaire*, 12, 149–154, 2009.
- [12] Y.C. Kouomou, P. Colet, L. Larger & N. Gastaud, Mismatch-induced bit error-rate in optical chaos communication using semiconductor lasers with electro-optical feedback, *Physical Review E*, 41, 156–163 2005.
- [13] R. Noe, U. Rückert, Y.T. Achiam & H. Porte, European "synQPSK" Project : Toward Synchronous Optical Quadrature Phase Shift Keying with DFB Lasers, OSA, Amplifiers and Their Applications/COTA, pp. CThC4 (2006)
- [14] M. J. O'Mahoney, C. Politi, D. Klonidis, R. Nejabati, and D. Simeonidou, "Future optical networks," *J. Lightw. Technol.* , vol. 24, no. 12, pp. 4684–4696, Dec. 2006.
- [15] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photon. (London)*, vol. 2, no. 728–732, Dec. 2008.
- [16] M. C. Soriano, P. Colet, and C. R. Mirasso, "Security Implications of Open- and Closed-Loop Receivers in All-Optical Chaos-Based Communications," *IEEE Photon. Technol. Lett.* 21, 426- 428, 2009.

- [17] R. Lavrov, M. Jacquot, L. Larger, "Nonlocal nonlinear electro-optic phase dynamics demonstrating 10 Obis chaos communications," *IEEE J. Quant. Electron.*, 46 (10), 1435, 2010.
- [18] M. R. Nguimdo and P. Colet, "Electro-optic phase chaos systems with an internal variable and a digital key," *Optics Express*, vol. 20, pp. 25333–25344, November 2012.
- [19] Ponomarenko, V. I., et al. "Hidden data transmission based on time-delayed feedback system with switched delay time." *Technical Physics Letters* 38.1 , 2012.
- [20] Larger, Laurent. "Complexity in electro-optic delay dynamics: modelling, design and applications." *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 371.1999, 2013.
- [21] Hu, Hanping, et al. "Electro-optic intensity chaotic system with varying parameters." *Physics Letters A*, 2013.
- [22] L.F. Shampine , S. Thompson and J. Kierzenka. Solving Delay Differential Equations with dde23. The MathWorks, Inc. 2002.
- [23] M. Sciamanna, E. Mercier, D. Wolfersberger, "Nonlinear Dynamics in Semiconductor Lasers", *Abstract NDSL2016-p-0025*, Weierstrass Institute, 2016.
- [24] M.J. Wishon et al., "Revisiting the 'Quasi-Periodic' Route to Chaos", *Conference Paper*, 2017.
- [25] W. Wang et al., "Chaotic Behaviors of Bistable Laser Diodes and Its Application in Synchronization of Optical Communication", *Japanese Journal of Applied Physics*, vol. 40, n° 10, pp. 5914-5919, 2001 C. Juang et al., "Optoelectronic delayed-feedback and chaos in quantum-well laser diodes", *Optics Communications*, vol. 192, n° 1-2, pp. 77-81, 2001.
- [26] R. Lang and K. Kobayashi, "External optical feedback effects on semiconductor injection laser properties," *IEEE Journal of Quantum Electronics*, vol. 16, no. 3, pp. 347–355, 1980.
- [27] T. Heil, I. Fischer, W. Elsässer, J. Mulet and C. R. Mirasso, "Chaos synchronization and spontaneous symmetry-breaking in symmetrically delay-coupled semiconductor lasers," *Physical Review Letters*, vol. 86, pp. 795–798, 2001.
- [28] R. Lang, "Injection locking properties of a semiconductor laser," *IEEE Journal of Quantum Electronics*, vol. 18, pp. 976–983, 1982.
- [29] J. Ohtsubo, *Semiconductor Lasers: Stability, Instability and Chaos*, Springer, 2017.
- [30] H. G. Winful and L. Rahman, "Synchronized chaos and spatiotemporal dynamics in arrays of coupled lasers," *Physical Review Letters*, vol. 65, pp. 1575–1578, 1990.
- [31] C. R. Mirasso, P. Colet and P. Garcia-Fernandez, "Synchronization of chaotic semiconductor lasers: application to optical communications," *IEEE Photonics Technology Letters*, vol. 8, pp. 299–301, 1996.
- [32] I. Fischer, Y. Liu and P. Davis, "Synchronization of chaotic semiconductor laser dynamics on subnanosecond time scales," *Physical Review A*, vol. 62, 011801, 2000.
- [33] K. A. Shore and A. D. McCoy, "Chaos in semiconductor lasers," *Optical and Quantum Electronics*, vol. 24, pp. 917–925, 1992.

Annexes

Code Matlab:

Script chaos:

```
clc;clear;close all;
▪ %% Paramètres physiques
▪ q = 1.6e-19; % charge electron
▪ V = 3e-18; % volume actif
▪ tau_n = 1e-9; % temps de vie porteurs
▪ tau_p = 2e-12; % temps de vie photons
▪ Gamma = 0.3; % facteur confinement
▪ g0 = 1e-13; % gain différentiel
▪ N0 = 1e24; % densité transparence
▪ eps = 1e-13; % compression gain
▪ beta = 1e-5;
▪ %% Modulation du courant
▪ I0 = 40e-3; % courant moyen
▪ Im = 35e-3; % amplitude modulation
▪ fm = 10e9; % fréquence modulation
▪ %% Temps simulation
▪ tspan = [0 100e-9];
▪ %% Conditions initiales
▪ S0 = 1e15;
▪ N0_init = 1.1e24;
▪ X0 = [S0 N0_init];
▪ %% Résolution numérique
▪ [t,X] = ode45(@(t,X)laserChaos(t,X,q,V,tau_n,tau_p,Gamma,g0,N0,eps,beta,I0,Im,fm),
tspan, X0);
▪ %% Variables
▪ S = X(:,1);
▪ N = X(:,2);
▪ %% Affichage temporel
▪ figure (1);
▪ plot(t*1e9,S,'b');
▪ xlabel('Temps (ns)');
▪ ylabel('Photons S');
▪ title('Dynamique chaotique de la diode laser');
▪ grid on;
▪ %% Portrait de phase
▪ figure (2);
▪ dS = gradient(S,t);
▪ %plot3(N,S,dS,'r');
▪ plot(N,S,'r');
▪ xlabel('N porteurs');
▪ ylabel('S photons');
▪ title('Portrait de phase');
▪ grid on;
▪ %% Spectre fréquentiel
▪ Fs = 1/(t(2)-t(1));
▪ Y = fft(S-mean(S));
▪ f = Fs*(0:length(Y)-1)/length(Y);
▪ figure (3);
▪ plot(f/1e9,(abs(Y)).^2);
▪ xlim([0 20]);
▪ xlabel('Frequence (GHz)');
▪ ylabel('|FFT|');
▪ title('Spectre du chaos laser');
▪ grid on;
```

Fonction laser_chaos:

```
function dXdt = laserChaos(t,X,q,V,tau_n,tau_p,Gamma,g0,Ntr,eps,beta,I0,Im,fm)
    S = X(1);
    N = X(2);
    %% Courant modulé
    I = I0 + Im*sin(2*pi*fm*t);
    %% Gain non linéaire
    G = g0*(N - Ntr)/(1 + eps*S);
    %% Equations du laser
    dSdt = Gamma*G*S - S/tau_p + beta*N;
    dNdt = I/(q*V) - N/tau_n - G*S;
    dXdt = [dSdt;dNdt];
end
```

Script Lang Kobayashi:

```
clc;clear;close all;
%% Paramètres physiques
alpha = 4;
tau_p = 2e-12;
tau_n = 1e-9;
g0 = 1e-12;
Ntr = 1e24;
eps_gain = 1e-15;
q = 1.6e-19;
V = 3e-18;
%% Rétroaction optique
kappa = 1e10;
%kappa = 1e11;
%kappa = 7.75735e11;
tau = 3e-9;
omega0 = 2*pi*193.1e12;
%% Courant injection
I = 80e-3;
%% Historique initial
history = @(t)[1e3; 1e3; 1.1e24];
%% Temps simulation
tspan = [0 300e-9];
%% Résolution DDE
sol = dde23(@(t,y,Z) LK_equations(t,y,Z,...
    alpha,tau_p,tau_n,g0,Ntr,eps_gain,...
    q,V,I,kappa,omega0,tau),...
    tau,...
    history,...
    tspan);
%% Extraction
t = sol.x;
Er = sol.y(1,:);
Ei = sol.y(2,:);
N = sol.y(3,:);
%% Intensité optique
S = Er.^2 + Ei.^2;
%% Dynamique temporelle
figure;
plot(t*1e9,S);
xlabel('Temps (ns)');
ylabel('Intensité');
title('Chaos laser avec rétroaction');
grid on;
%% Attracteur étrange 3D
figure;
plot3(Er,Ei,N,'b');
xlabel('Re(E)');
ylabel('Im(E)');
zlabel('N');
title('Attracteur étrange 3D');
grid on;
```

```

▪ %% Spectre FFT
▪ %% Spectre FFT et bande passante chaotique 80 %
▪ t_uniform = linspace(t(1),t(end),length(t));
▪ S_uniform = interp1(t,S,t_uniform);
▪ Fs = 1/(t_uniform(2)-t_uniform(1));
▪ Nfft = length(S_uniform);
▪ Y = fft(S_uniform - mean(S_uniform));
▪ PSD = abs(Y).^2/Nfft;
▪ f = (0:Nfft-1)*(Fs/Nfft);
▪ %% Demi-spectre positif
▪ PSD = PSD(1:floor(Nfft/2));
▪ f = f(1:floor(Nfft/2));
▪ %% Puissance cumulée
▪ Ptot = sum(PSD);
▪ Pcumul = cumsum(PSD);
▪ %% Bande passante à 80 %
▪ idx80 = find(Pcumul >= 0.80*Ptot,1,'first');
▪ BW80 = f(idx80);
▪ fprintf('\n');
▪ fprintf('Bande passante chaotique (80%%) = %.3f GHz\n',BW80/1e9);
▪ fprintf('\n');
▪ %% Affichage
▪ figure (3);
▪ plot(f/1e9,PSD,'b','LineWidth',1.5);
▪ hold on
▪ xline(BW80/1e9,'r--','LineWidth',2);
▪ xlabel('Frequence (GHz)');
▪ ylabel('Densité Spectrale de Puissance PSD');
▪ title('Spectre chaotique et bande passante 80%');
▪ legend('PSD','BW_{80%}');
▪ grid on;
▪ %% Exposant de Lyapunov simplifié
▪ delta0 = 1e-9;
▪ history2 = @(t)[1e3+delta0; 1e3; 1.1e24];
▪ sol2 = dde23(@(t,y,Z) LK_equations(t,y,Z,...
▪ alpha,tau_p,tau_n,g0,Ntr,eps_gain,...
▪ q,V,I,kappa,omega0,tau),...
▪ tau,...
▪ history2,...
▪ tspan);
▪ t_common = sol.x;
▪ Y1 = deval(sol,t_common);
▪ Y2 = deval(sol2,t_common);
▪ S1 = Y1(1,:).^2 + Y1(2,:).^2;
▪ S2 = Y2(1,:).^2 + Y2(2,:).^2;
▪ delta_t = abs(S2 - S1);
▪ delta_t(delta_t < eps) = eps;
▪ lambda = mean(log(delta_t/delta0)) / t_common(end);
▪ disp(['Lyapunov = ',num2str(lambda*delta0)]);
▪

```

Fonction de Lang Kobayashi:

```

▪ function dydt = LK_equations(t,y,Z,...
▪ alpha,tau_p,tau_n,g0,Ntr,eps_gain,...
▪ q,V,I,kappa,omega0,tau)
▪ %% Variables actuelles
▪ Er = y(1);
▪ Ei = y(2);
▪ N = y(3);
▪ %% Variables retardées
▪ Er_tau = Z(1,1);
▪ Ei_tau = Z(2,1);
▪ %% Champ complexe
▪ E = Er + 1i*Ei;
▪ E_tau = Er_tau + 1i*Ei_tau;
▪ %% Gain optique

```

```

▪ G = g0*(N - Ntr)/(1 + eps_gain*abs(E)^2);
▪ %% Bruit spontané
▪ noise_amp = 1e8;
▪ Fn = noise_amp*(randn + 1i*randn);
▪ %% Equation Lang-Kobayashi
▪ dE = ((1 + 1i*alpha)/2)*(G - 1/tau_p)*E ...
▪       + kappa*E_tau*exp(-1i*omega0*tau) ...
▪       + Fn;
▪ %% Equation des porteurs
▪ dN = I/(q*V) - N/tau_n - G*abs(E)^2;
▪ %% Séparation réelle / imaginaire
▪ dydt = [real(dE);imag(dE);dN];
▪ end

```

Lyapunov:

```

▪ clc;clear;close all;
▪ %% Paramètres LK
▪ alpha = 4;
▪ tau_p = 2e-12;
▪ tau_n = 1e-9;
▪ g0 = 1e-12;
▪ Ntr = 1e24;
▪ eps_gain = 1e-14;
▪ q = 1.6e-19;
▪ V = 1e-17;
▪ I = 80e-3;
▪ kappa = 1e11;
▪ tau = 3e-9;
▪ omega0 = 2*pi*193.1e12;
▪ %% Paramètres Lyapunov
▪ delta0 = 1e-8;
▪ Trenorm = 5e-10;
▪ Nrenorm = 500;
▪ %% Historique
▪ history = @(t)[1e3;1e3;1.1e24];
▪ %% Initialisation
▪ Xref = history(0);
▪ Xpert = Xref + delta0*[1;0;0];
▪ sumlog = 0;
▪ for k = 1:Nrenorm
▪     tspan = [0 Trenorm];
▪     sol1 = dde23(@(t,y,Z) ...
▪         LK_eq2(t,y,Z,...
▪         alpha,tau_p,tau_n,g0,Ntr,...
▪         eps_gain,q,V,I,kappa,omega0,tau),tau,@(t)Xref,tspan);
▪     sol2 = dde23(@(t,y,Z) ...
▪         LK_eq2(t,y,Z,...
▪         alpha,tau_p,tau_n,g0,Ntr,...
▪         eps_gain,q,V,I,...
▪         kappa,omega0,tau),...
▪         tau,...
▪         @(t)Xpert,...
▪         tspan);
▪     X1 = sol1.y(:,end);
▪     X2 = sol2.y(:,end);
▪     delta = norm(X2-X1);
▪     sumlog = sumlog + log(delta/delta0);
▪     direction = (X2-X1)/delta;
▪     Xref = X1;
▪     Xpert = X1 + delta0*direction;
▪ end
▪ lambda = sumlog/(Nrenorm*Trenorm);
▪ fprintf('\n');
▪ fprintf('Plus grand exposant de Lyapunov = %.4e s^-1\n',lambda);
▪ fprintf('\n');

```

المخلص

تركز هذه الأطروحة على دراسة توليد الفوضى الضوئية في ثنائي ليزر شبه موصل مزود بتغذية راجعة ضوئية، وتطبيقها في تأمين الاتصالات الضوئية فائقة السرعة. تم نمذجة ديناميكيات ثنائي الليزر باستخدام نموذج لانغ-كوباياشي مع تضمين حد تغذية راجعة متأخرة. تُظهر عمليات المحاكاة التي أجريت في برنامج ظهورًا متتابعًا لأنظمة دورية، وشبه دورية، ثم فوضوية مع ازدياد معامل التغذية الراجعة. تظهر الفوضى عند قيمة حرجة للتغذية الراجعة تقارب MATLAB $10^{11} \times 7.75735$. تكشف النتائج عن جاذب غريب، وطيف متصل واسع النطاق، ومعامل ليابونوف موجب قدره 1.4616، مما يؤكد الطبيعة الفوضوية للنظام. يصل عرض النطاق الترددي الفوضوي المُقدَّر إلى حوالي 51.87 جيجاهرتز، وهو ما يُعد مناسبًا بشكل خاص للتطبيقات المقصودة. تُستخدم الإشارة الفوضوية يعتمد فك التشفير على مبدأ التزامن الفوضوي بين المرسل والمستقبل. تُظهر النتائج OptiSystem. المُولدة كقناع تشفير في نظام مُحاكى باستخدام برنامج استعادة دقيقة للرسالة المرسل، فضلاً عن مستوى عالٍ من السرية. تُبرهن هذه الدراسة على جدوى استخدام ثنائيات الليزر ذات التغذية الراجعة، وبالتالي تؤكد إمكاناتها كمصادر للفوضى في تطوير أنظمة التشفير البصري عالية الأداء والمكيفة مع شبكات الاتصالات الحديثة.

لكلمات المفتاحية: الفوضى البصرية، ثنائي الليزر ذو التغذية الراجعة، نموذج لانغ-كوباياشي، التزامن الفوضوي، التشفير البصري، الاتصالات الآمنة، الحساسية للشروط الأولية، اللاخطية، ليابونوف، التشعب، مخطط الطور

Résumé

Ce mémoire porte sur l'étude de la génération du chaos optique dans une diode laser à semi-conducteur avec rétroaction optique et son application à la sécurisation des communications optiques très hauts débits. La dynamique de la diode laser est modélisée à l'aide du modèle de Lang-Kobayashi intégrant un terme de rétroaction retardée. Des simulations réalisées sous MATLAB montrent l'apparition successive de régimes périodiques, quasi-périodiques puis chaotiques lorsque le coefficient de rétroaction augmente. Le chaos apparaît pour une valeur critique de rétroaction voisine de $7,75735 \times 10^{11}$. Les résultats obtenus révèlent un attracteur étrange, un spectre continu à large bande et un exposant de Lyapunov positif égal à 1,4616, confirmant le caractère chaotique du système. La largeur de bande chaotique estimée atteint environ 51,87 GHz, ce qui est particulièrement favorable au cadre des applications envisagées. Le signal chaotique généré est ensuite utilisé comme masque de chiffrement dans un système simulé sous OptiSystem. Le déchiffrement repose sur le principe de synchronisation chaotique entre l'émetteur et le récepteur. Les résultats démontrent une récupération fidèle du message transmis ainsi qu'un niveau élevé de confidentialité. Cette étude démontre la faisabilité et confirme ainsi l'intérêt des diodes laser à rétroaction comme sources de chaos pour le développement de systèmes de cryptographie optique performants et adaptés aux réseaux de communication modernes.

Mots-clés : Chaos optique, diode laser à rétroaction, modèle de Lang-Kobayashi, synchronisation chaotique, chiffrement optique, communications sécurisées, sensibilité aux conditions initiales, non-linéarité, Lyapunov, bifurcation, diagramme des phases

Abstract

This thesis investigates the generation of optical chaos in a semiconductor laser diode with optical feedback and its application to the security of ultra-high-speed optical communications. The laser diode dynamics are modeled using the Lang-Kobayashi equations, which incorporate a delayed optical feedback term. MATLAB simulations reveal the successive emergence of periodic, quasi-periodic, and chaotic regimes as the feedback coefficient increases. Chaos appears at a critical feedback value of approximately 7.75735×10^{11} . The obtained results exhibit a strange attractor, a broadband continuous spectrum, and a positive Lyapunov exponent equal to 1.4616, confirming the chaotic nature of the system. The estimated chaotic bandwidth reaches approximately 51.87 GHz, making it particularly suitable for the targeted communication applications. The generated chaotic signal is then used as an encryption mask in a communication system simulated using OptiSystem. The decryption process relies on the principle of chaotic synchronization between the transmitter and the receiver. The results demonstrate accurate recovery of the transmitted message while ensuring a high level of confidentiality. This study confirms the feasibility of the proposed approach and highlights the potential of feedback laser diodes as efficient chaos sources for the development of high-performance optical cryptography systems adapted to modern communication networks.

Keywords: Optical chaos, feedback laser diode, Lang-Kobayashi model, chaotic synchronization, optical encryption, secure communications, sensitivity to initial conditions, nonlinearity, Lyapunov exponent, bifurcation, phase-space diagram.