Université Abou Bekr Belkaid
Tlemcen Algérie
جامعة أبي بكر بلقايد
تلمسان الجزائر

République Algérienne Démocratique et Populaire
Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Laboratoire STIC

MEMOIRE

Présenté

A L'UNIVERSITE DE TLEMCEN
FACULTE DE TECHNOLOGIE

Pour l'obtention du diplôme de

MASTER
TELECOMMUNICATIONS

Option : Photonique et Réseaux Optiques de Télécommunications

Par

BENHABIB Chouaib

ETUDE D'UN SYSTEME CHAOTIQUE POUR LA SECURISATION DES COMMUNICATIONS OPTIQUES

Soutenue en Juin 2014 devant le Jury:

Dr. KAMECHE Samir	Maitre de Conférences, Université de Tlemcen	Président
Dr. MERZOUGUI Rachid	Maitre de Conférences, Université de Tlemcen	Examinateur
Dr. ZERROUKI Elhadj	Maitre de Conférences, Université de Tlemcen	Examinateur
Dr. ABDELMALEK Abdelhafid	Maitre de Conférences, Université de Tlemcen	Encadreur

Remerciements

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

J'exprime ma gratitude à Monsieur KAMECHE Samir, Maitre de conférences à l'université de Tlemcen, pour l'honneur qu'il me fait en présidant mon Jury, ainsi qu'à Monsieur MERZOUGUI Rachid, Maitre de conférences à l'université de Tlemcen, et Monsieur ZERROUKI Elhadj, Maitre de conférences à l'université de Tlemcen, pour l'honneur qu'ils me font en participant à mon 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'études.

Résumé

Nous avons présenté dans ce mémoire un crypto-système optique basé sur le chaos en intensité. Le principe s'appuie sur une dynamique électro-optique non linéaire à retard, dont la non linéarité est réalisée grâce à un modulateur Mach Zehnder à une seule électrode. Le système comporte quatre modules, deux au niveau de l'émetteur : le générateur de chaos et le module de chiffrement, et deux au niveau du récepteur : les modules de synchronisation et de déchiffrement. Le système permet de disposer d'une part, d'une dynamique ultra-rapide jusqu'à des fréquences de plusieurs GHz, et d'autre part, de générer un chaos de grande dimension fractal. Nous avons développé un modèle mathématique pour le système étudié qui nous a conduits à une équation différentielle non linéaire du second ordre à retard. Au travers d'une étude numérique sous Matlab, nous avons cherché dans un premier temps à étudier les comportements dynamiques que peut présenter le générateur de chaos en fonction de divers paramètres, en particulier en fonction du gain de la boucle de rétroaction. A partir du diagramme de bifurcation, nous avons identifié les valeurs critiques de ce gain pour les quelles le chaos est capable de s'installer. L'évolution temporelle du signal généré, sa densité spectrale et le plan de phase nous ont permet de confirmer ces résultats. Le chaos généré par voie optique a été utilisé pour l'opération de chiffrement réalisée par addition d'intensité. Les opérations de chiffrement et déchiffrement ont été réalisées avec succès en utilisant dans Optisystem les données du signal chaotique obtenues par intégration numérique sous Matlab.

Mots clés : *Chaos, bifurcation, Exposant de Lyapunov, Attracteur étrange, stabilité, cascade sous-harmonique, quasi-périodicité, Dimension fractale, modulateur Mach Zhender, équation différentielle à retard, non linéaire, Synchronisation, Matlab, Optisystem.*

Table des matières

CHAPITRE III

Etude d'un Crypto-Système Chaotique à base de modulateur MZM à Rétroaction

Introduction générale

Les fibres optiques constituent, à l'heure actuelle, l'épine dorsale du réseau des télécommunications. La montée en débit réalisée ces dernières années a conduit au déploiement de réseaux SDH et WDM faisant office de réseaux de transport national, continental et intercontinental. Les données confidentielles : économiques, militaires ou diplomatiques ne doivent pas être captées simplement en interceptant le signal optique.

La sécurisation des données transportées par longueur d'onde est devenue donc une nécessité primordiale. Les méthodes classiques de chiffrement par des algorithmes mathématiques (AES, DES, DSA, RSA, ElGamal, ECC, ...) demeurent inadaptés pour le haut débit. D'une part, ces derniers deviennent de plus en plus fragiles face à la montée en puissance des calculateurs, et d'autre part ils sont très long pour fonctionner dans le domaine optique. Plus récemment, d'autres techniques de chiffrement matériel ont été introduits, telles que la cryptographie quantique et la cryptographie chaotique.

Dans le cadre de ce mémoire, nous investiguons les architectures de crypto-systèmes optiques chaotiques basé sur le chaos en intensité. Nous nous intéressons particulièrement aux systèmes à base de modulateur Mach-Zhender avec rétroaction. Ce travail comporte deux phases : une phase de conception et modélisation et une phase d'évaluation par méthodes numériques (Matlab & Optisystem) à défaut d'équipements pour l'expérimentation.

Il sera question de :

- La génération du chaos
- L'évaluation de la complexité du chaos généré (Densité spectrale, Espace des phases, Exposants de Lyapunov, Dimension fractale du chaos, ...)
- L'identification des paramètres de contrôle du système chaotique
- Le masquage de l'information
- La synchronisation du chaos et la restitution des messages d'origine

La suite de ce mémoire est organisée de la façon suivante : le premier chapitre présente un état de l'art sur les systèmes dynamiques non linéaires et les comportements chaotiques. Dans le second chapitre, nous introduisons la cryptographie chaotique. Nous présentons, en particulier, les différents types de crypto-systèmes chaotiques réalisés en longueur d'onde. Le troisième chapitre constitue véritablement l'objet de note contribution ayant trait à l'étude et l'évaluation d'un crypto-système électro-optique basé sur le chaos en intensité, réalisé autour d'un modulateur Mach Zhender à une seule rétroaction.

CHAPITRE 1

Systèmes Dynamiques et Chaos

I.1 Introduction

Depuis longtemps, le chaos était synonyme de désordre et de confusion. Il s'opposait à l'ordre et devait être évité. La science était caractérisée par le déterminisme, la prévisibilité et la réversibilité. Poincaré fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes.

Le terme chaos définit un état particulier d'un système dont le comportement ne se répète jamais qui est très sensible aux conditions initiales, et imprédictible à long terme. Des chercheurs d'horizons divers ont alors commencé à s'intéresser à ce comportement.

Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physiques que biologique, chimique ou économique. Ainsi, nous nous intéresserons principalement dans ce chapitre aux systèmes dynamiques chaotiques en nous attardant sur les espaces de phases, les attracteurs étranges et les scénarios de transition vers le chaos (appelés aussi bifurcations), lesquels nous permettront de mieux comprendre la nature du chaos.

L'objectif de ce chapitre est de donner quelques notions élémentaires sur les systèmes dynamiques afin de mieux appréhender ce qu'est le chaos : ses apparitions dans un système et la manière de le quantifie.

I.2 Systèmes dynamiques

Un système dynamique est une structure qui évolue au cours du temps de façon à la fois :

- Causale, où son avenir ne dépend que de phénomènes du passé ou du présent
- Déterministe, c'est-à-dire qu'à partir d'une condition initiale donnée à l'instant présent va correspondre à chaque instant ultérieur un et un seul état futur possible.

L'évolution déterministe du système dynamique peut alors se modéliser de deux façons distinctes

- Une évolution continue dans le temps, représentée par une équation différentielle ordinaire.
- Une évolution discrète dans le temps, l'étude théorique de ces modèles discrets est fondamentale, car elle permet de mettre en évidence des résultats importants, qui se généralisent souvent aux évolutions dynamiques continues. Elle est représentée par le modèle général des équations aux différences finie.

I.3 Systèmes Dynamiques chaotiques

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre; il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial.

On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales. Il n'est pas déterminé ou modélisé par des systèmes d'équations linéaires ni par les lois de la mécanique classique.

a) La non-linéarité

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique.

La notion de système dynamique est relative à tous les systèmes dont l'évolution dépend du temps. En général, pour prévoir des phénomènes réels générés par ces systèmes, la démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Si cette relation est une opération de proportionnalité, le phénomène est linéaire. Dans le cas d'un phénomène non linéaire, l'effet n'est pas proportionnel à la cause

b) Le déterminisme

Un système chaotique a des règles fondamentales déterministes et non probabilistes. Il est généralement régi par des équations différentielles non linéaires qui sont connues, donc par des lois rigoureuses et parfaitement déterministes.

c) Sensibilité aux conditions initiales

Certains phénomènes dynamiques non linéaires sont si sensibles aux conditions initiales que, même s'ils sont régis par des lois rigoureuses et parfaitement déterministes, les prédictions exactes sont impossibles.

Une autre propriété des phénomènes chaotiques est qu'ils sont très sensibles aux perturbations. L'un des premiers chercheurs à s'en être aperçu fut Edward Lorenz qui s'intéressait à la météorologie et par conséquent aux mouvements turbulents d'un fluide comme l'atmosphère. Lorenz venait de découvrir que dans des systèmes non linéaires, d'infimes différences dans les conditions initiales engendraient à la longue des trajectoires totalement différentes. Il a illustré ce fait par l'effet papillon. Le battement d'ailes d'un papillon aujourd'hui à Tlemcen engendrerait une tempête le mois prochain à Quebec.

Il est clair que la moindre erreur ou imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction sur l'évolution à long terme du système. Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant des taux de divergence des trajectoires.

I.4 L'espace de phase

Un système dynamique est caractérisé par un certain nombre de variables d'état, qui ont la propriété de définir complètement l'état du système à un instant donné. Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ces variables d'état. Cet espace est appelé l'espace de phase ou chaque point définit un état et le point associé a cet état décrit une trajectoire, appelé également une orbite.

I.4.1 Notion d'attracteur

L'étude du comportement asymptotique d'un système dynamique régi par un flot d'équations différentielles non linéaires révèle très souvent la notion d'attracteur, défini comme l'ensemble compact de l'espace des phases invariant par ce flot et vers lequel convergent toutes les trajectoires du système. Il existe quatre cas de figures correspondants à des solutions différentes du flot, mettant en évidence des attracteurs différents :

- Le point attracteur : correspondant à une solution stationnaire constante, donc de fréquence nulle.
- Le cycle limite attracteur : caractérisant un régime périodique, la solution possède une seule fréquence de base.
- Le tore supra Tr ($r \geq 2$) : cet attracteur correspond à un régime quasi-periodique ayant r fréquences de base indépendantes (cas le plus simple r=2, dynamique biperiodique).

- L'attracteur étrange : cet attracteur est associé à un comportement quasi-aléatoire dit chaotique, caractérisé par un spectre de puissance continue et une fonction d'auto-corrélation s'annulant très rapidement. Contrairement aux signaux périodiques (quasi-périodiques) pour laquelle la similitude reste présente pour autant que la périodicité n'est altérée ; ce qui a pour conséquence immédiate la périodicité du comportement du système, le caractère fini de la portée de la fonction d'auto-corrélation temporelle pour le régime chaotique met en évidence la perte progressive de la similitude interne et donc l'imprédictibilité. Cette perte de mémoire du signal est due au phénomène de contraction des volumes dans l'espace des phases des systèmes dynamiques dissipatifs, mais aussi et surtout au phénomène de dilatation directionnelle de ces volumes.

Notons quelques propriétés importantes des systèmes chaotiques :

- Trois degrés de liberté sont suffisants pour donner naissance au chaos.
- L'attracteur, qui en plus d'être invariant par le flot, est aussi de volume nul, d'où la conclusion sur sa dimension qui doit être inferieure à celle de l'espace des phases ($d<n$). On montre que cette dimension est fractale pour le cas d'attracteur étrange.
- Le chaos est caractérisé par la sensibilité aux conditions initiales

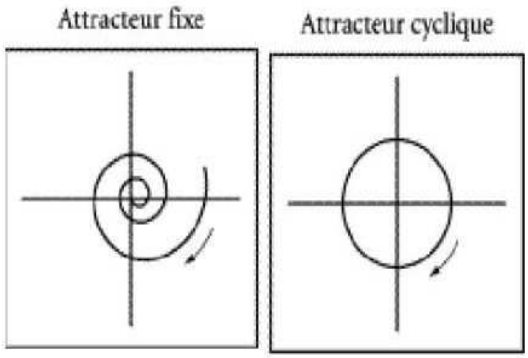


Figure 1.1 : Exemples d'attracteurs

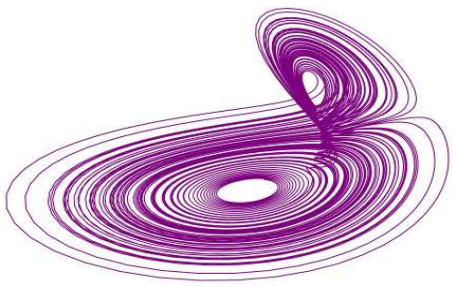


Figure 1.2 : Attracteur étrange de Lorentz

I.4.2 Dimension d'Hausdorff

Un attracteur occupe un volume nul dans l'espace des phases, sa dimension est donc inférieure à celle de l'espace en question, et elle est fractale plus précisément. Pour déterminer cette valeur une méthode simple consiste à recouvrir l'attracteur avec des hyper cubés d'arrête ε et examiner le nombre minimum $N(\varepsilon)$ de cubes nécessaires à cette opération.
La dimension fractale de l'attracteur est donné par la dimension de Hausdorff Besicovutch .

$$D = \lim_{\varepsilon \to 0} \frac{\ln N(\varepsilon)}{\ln (\frac{1}{\varepsilon})}$$

Quelques exemples :

- Pour un point, N (ε)=1 et D =0
- Pour un segment L, N (ε) $= \frac{L}{\varepsilon}$ $et\ D = 1$
- Pour un segment S, N (ε) $= \frac{S}{\varepsilon^2}$ $et\ D = 2$

Cette détermination permet de caractériser l'aspect d'auto-corrélation spatiale ou topologique de l'attracteur, qui ne donne aucun renseignement sur la façon dont une trajectoire va peupler les différentes parties de l'attracteur.
Pour mettre en évidence la dynamique du peuplement, on introduit la dimension d'information.

I.4.3 Exposants de Lyapunov

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaye si c'est possible de mesurer sinon d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches.

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 :
$|Z_2| \approx \exp(\lambda.\Delta t)\ |Z_1|$

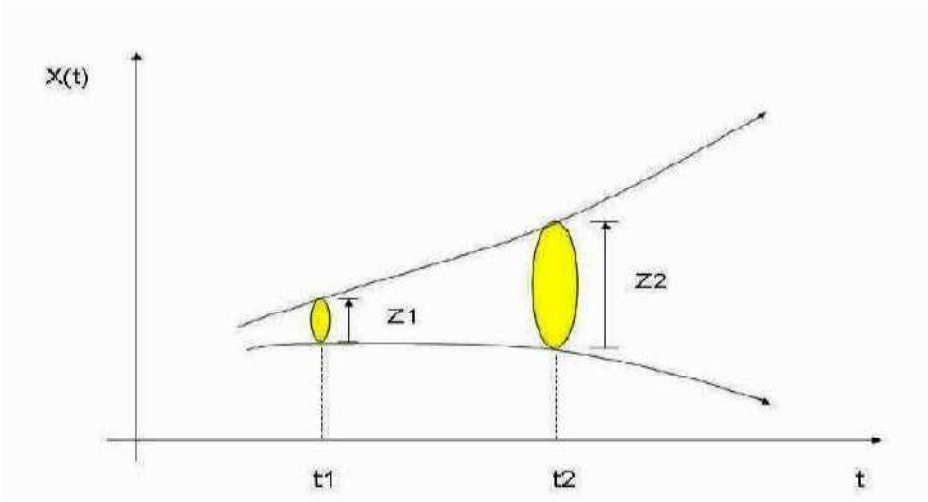


Figure 1.3 : Divergence de deux trajectoires dans le plan de phase

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

Au temps t >> 0, cette hyper sphère se transforme en une hyper-ellipsoïde de n demi-axes

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

Les exposants de Lyapunov sont tels que :

$$\lambda_i = \lim_{t\to\infty} \lim_{\varepsilon_0 \to 0} \frac{1}{t} \log\,(\frac{\varepsilon_i}{\varepsilon_0})$$

Ils caractérisent de façon assez précise la dynamique du système.

Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro et leur somme est négative. Un attracteur étrange possèdera toujours au moins trois exposants de Lyapunov, dont un au moins doit être positif (voir Tableau 1.1).

Tableau 1.1 : Exposants de Lyapunov et Dimensions

Etat	Attracteur	Dimension	Exposants de Lyapunov
Point d'équilibre	Point	0	$\lambda_n \leq \cdots \leq \lambda_1 \leq 0$
Périodique	Cercle	1	$\lambda_1 = 0$ $\lambda_n \leq \cdots \leq \lambda_2 \leq 0$
Période d'ordre 2	Tore	2	$\lambda_1 = \lambda_2 = 0$ $\lambda_n \leq \cdots \leq \lambda_3 \leq 0$
Période d'ordre K	K-Tore	K	$\lambda_1 = \cdots = \lambda_k = 0$ $\lambda_n \leq .. \leq \lambda_{1k+1} \leq 0$
Chaotique		Non entier	$\lambda_1 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$
Hyper chaotique		Non entier	$\lambda_1 > 0 \;\; \lambda_2 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$

I.4.4 Bifurcation et routes vers le chaos

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique. Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation.

Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation.

I.5 Conclusion

Dans le présent chapitre, quelques définitions et notions sur les systèmes chaotiques ont été présentées. Nous allons éclaircir leur utilisation à des fins de chiffrement de données. En effet, les systèmes chaotiques possèdent des propriétés proches de celles requises en cryptographie usuelle. Le prochain chapitre introduit la notion de la cryptographie et présente les différents schémas de chiffrement basés sur l'utilisation des systèmes dynamiques chaotiques.

CHAPITRE 2

Chiffrement par Chaos : Crypto-Systèmes Chaotiques Optiques

II.1 Introduction

L'informatique et les réseaux de communication sont devenus des composantes indispensables de la vie personnelle et professionnelle d'un nombre croissant de personnes. Leur bon fonctionnement est donc vital. La notion de bon fonctionnement des ordinateurs et des réseaux de communication se situe à deux niveaux du point de vue de la sécurité. Elle comprend :

- les obligations légales : la protection des données à caractère personnel
- les obligations professionnelles : fiabilité, disponibilité, performances, protection des données (intégrité et confidentialité), protection des accès (authentification), assurance sur l'interlocuteur (authentification, signature), il faut donc définir des politiques de sécurité.

Les algorithmes de chiffrement actuels qu'ils soient à clé symétrique ou asymétrique tels que RSA, DES, ECC, RC4, ont déjà été cassés et sont donc devenus sans garantie. En effet, plus les ordinateurs sont puissants, plus la méthode Brute Force est efficace et plus les algorithmes de chiffrement sont vulnérables.

La cryptographie chaotique, en contre partie, répond aux exigences de sécurité et aux contraintes, à savoir une résistance très grande à la cryptanalyse combinée au maintien de tous les attributs nécessaires aux algorithmes de chiffrement.

Dans ce chapitre, nous nous concentrons sur les propriétés des systèmes optoélectroniques non linéaires pour la sécurisation des communications optiques par chaos. En particulier, nous examinons les trois plus configurations utilisées: les lasers à semi-conducteurs (systèmes tout optique), chaos en intensité (systèmes électro-optiques à retard), et le chaos en phase des systèmes électro-optiques également.

II.2 Objectifs des crypto-systèmes

Le crypto système assure et garantit : la confidentialité, l'authenticité, l'intégrité et la non-répudiation.

- La confidentialité signe qu.une personne non autorisée n.ait accès aux informations.

- L'authenticité fait référence pour la validation de la source du message pour assurer quel expéditeur est correctement identité.

- L'intégrité fournit l'assurance que le message n'a pas été modifié pendant la transmission, accidentellement ou intentionnellement.

- La non-répudiation signée qu'un expéditeur ne peut pas nier d'avoir envoyé le message et le récepteur ne peut pas nier sa réception.

Si une personne envoie un message, puis plus tard, il prétend qu'il n'a pas envoyé le message, il s'agit d'un acte de répudiation. Quand un mécanisme de cryptage prévoit la non- répudiation, cela signifie que l'expéditeur ne peut pas nier d'avoir envoyé le message et le récepteur ne peut pas nier sa réception.

II.3 Communications Sécurisées par chaos

Protéger les informations sensibles de l'interception indésirable a toujours attiré l'attention dans les réseaux de communication. Traditionnellement, la confidentialité et l'authentification de l'information sont réalisées grâce à des algorithmes mathématiques. Plus récemment, d'autres techniques de cryptage ont été introduits, tels que des clés quantiques la distribution et de la communication par chaos.

Comme il a été déjà mentionné dans le premier chapitre, le chaos déterministe peut générer des comportements dynamiques d'apparences aléatoires. Il serait donc intéressant d'utiliser ces derniers comme porteuses d'informations en télécommunication.

Le diagramme principal de la communication sécurisée par le chaos est montré sur la figure 2.1. Le principe est de masquer une information par des signaux chaotiques et de l'envoyer vers le récepteur sur un canal public. L'information cryptée est récupérée au niveau du récepteur.

La clé du système de transmission est l'ensemble des paramètres des deux générateurs chaotiques à l'émission et à la réception qui doivent être synchronisés, c'est à dire X = Y.

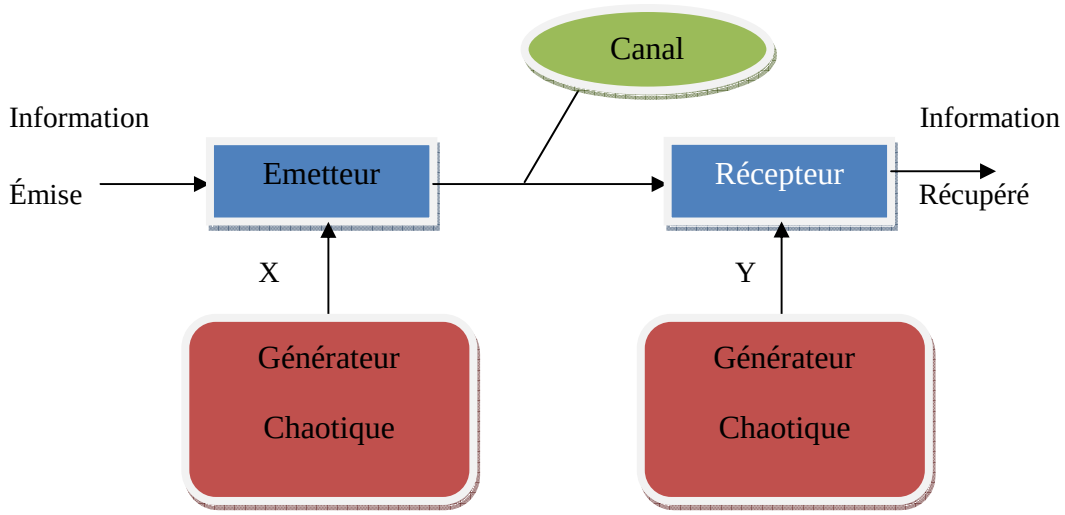


Figure 2.1 : Principe d'une communication sécurisée par chaos

Dans certain cas, la cryptanalyse peut se baser sur la respectabilité du signal transmis car les algorithmes de cryptage sont des suites de nombres pseudo aléatoires. Il est alors possible de reconstruire la clé à partir du signal crypté. Pour éviter ce type de faille, il faut donc que la clé ait une dimension suffisamment complexe pour que même à long terme, on ne puisse pas remonter au code. Le principe serait alors de se servir d'un bruit aléatoire évoluant dans le temps dont on connaît les caractéristiques en guise de clé.

Le chiffrement d'un message par le chaos s'effectue donc en superposant à l'information initiale un signal chaotique. On envoie par la suite le message noyé dans le chaos à un récepteur qui lui connaît les caractéristiques du générateur de chaos. Il ne reste alors plus au destinataire qu'à soustraire le chaos de son message pour retrouver l'information. Si la génération du chaos et le cryptage du message ne présente pas de problèmes majeurs, on va voir par la suite que du fait de la nature même du chaos, le décryptage va quant à lui présenter des étapes critiques notamment pour recréer la composante chaotique du message (synchronisation) et la soustraire.

II.4 Techniques de chiffrement par chaos

Il existe plusieurs techniques qui peuvent servir comme moyen de masquage de l'information dans le chaos, nous décrivons ici quelques uns :

II.4.1 Chiffrement par addition

Dans cette méthode appelée, masquage chaotique, l'émetteur est un système chaotique autonome dont le signal de sortie y(t) est ajouté au signal du message m(t). La somme de deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotique (émetteur et récepteur), le message est extrait a l'aide d'une opération de soustraction.(Figure 2.2)

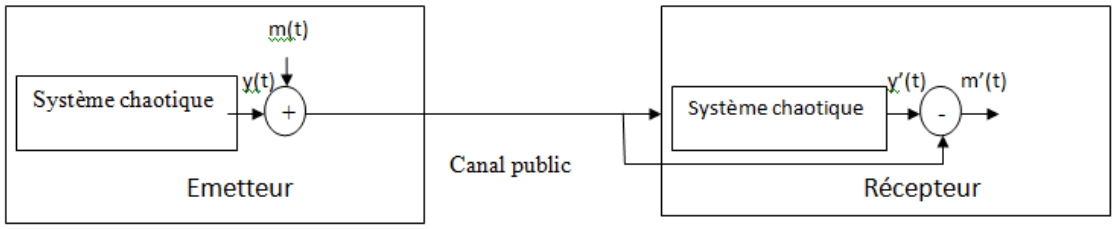


Figure 2.2 : Principe du chiffrement chaotique par addition

II.4.2 Chiffrement par commutation

Cette méthode (en anglais Chaos Shift Keying, CSK) est utilisée pour transmettre un message binaire (voir figure 2.3). L'émetteur est composé de deux systèmes chaotiques et pour chaque niveau de message m(t) (0 ou 1), l'un des systèmes envoi sa sortie sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étrange.

Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur et un bloc de comparaison permet de relever la valeur du message noté m'(t).

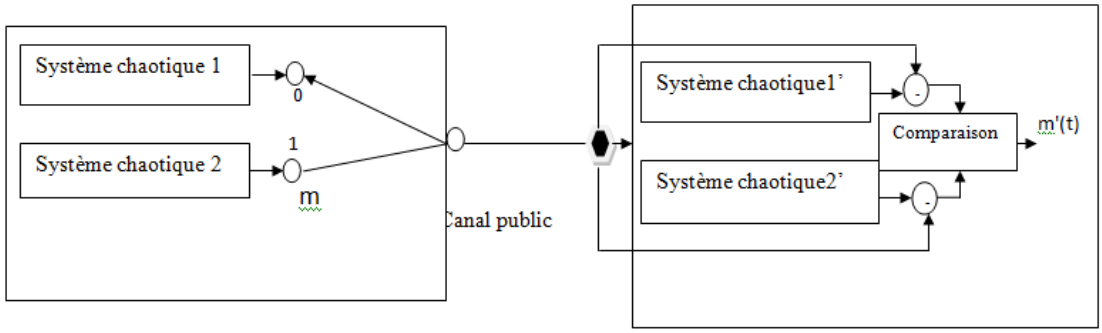


Figure 2.3 : Principe du chiffrement chaotique par commutation

II.4.2 Chiffrement par modulation

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure.

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus Complexe qu'un signal chaotique normal. Cependant, la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques. Elle n'a pas d'équivalent parmi les systèmes de communication classique. Cependant, le cryptage par modulation s'est avéré sensibles à certaines attaques.

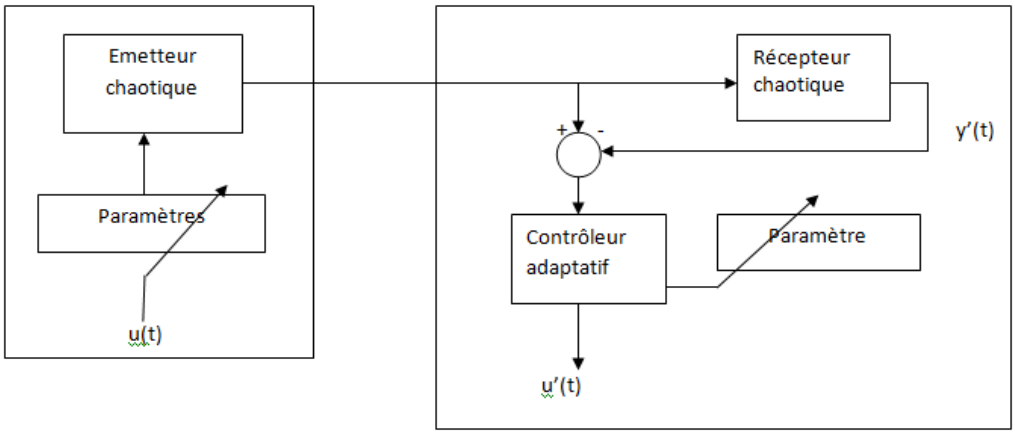


Figure 2.3 : Principe du chiffrement chaotique par modulation

II.5 Crypto-systèmes optiques basé sur le chaos

Les générateurs optiques de chaos utilisent des dynamiques engendrées par des oscillateurs non linéaires à retard. Une des principales études sur ce genre de système a été réalisée en 1979 par le physicien japonais Kensuke Ikeda. Celui-ci a analysé numériquement les variations de la puissance optique à la sortie d'une cavité optique non linéaire en forme d'anneau. Une cavité de ce type porte le nom de boucle à retard (appelé aussi anneau d'Ikeda). Elle est constituée d'un anneau optique en matériau non linéaire dans lequel on injecte un faisceau laser dont la puissance est constante. Au bout d'un tour dans la cavité, le faisceau interfère avec lui-même. La propriété intéressante des matériaux non linéaires est d'avoir un indice de réfraction variable avec l'intensité

optique. L'interférence créant alors une variation de l'intensité lumineuse dans la cavité va provoquer une modification de l'indice de réfraction de la boucle. Le retard optique va se trouver modifié et par conséquent, l'intensité lumineuse va varier de par la dépendance des interférences à la différence de marche optique. Un chaos d'intensité lumineuse va donc s'installer au fur et à mesure que le rayon tournera dans l'anneau.
Le comportement dynamique de tels systèmes est décrit par des équations différentielles à retard appelées aussi équations d'Ikeda de la forme : $x(t+T)=f(x'(t))$
Le retard T va jouer le rôle d'une mémoire capable de stocker un grand nombre d'oscillation. Plus ce retard sera grand devant le temps de réponse du système plus le chaos créé sera complexe.

Ces dernières années, le progrès dramatique dans les communications chaotiques a été fait avec des expériences dans les réseaux réalistes. En particulier, deux démonstrations réussies impliquant la transmission de l'information à plusieurs gigabits dans un réseau optique installé distant de plusieurs dizaines de kilomètres. Pendant la transmission, les messages ont été cachés dans un signal chaotique produit par des lasers à semi-conducteur à rétroaction tout-optique ou par les systèmes électro-optiques à rétroaction.
Les performances courantes des systèmes tout-optiques pour les transmissions sécurisées sont limitées à 2.5 Gb/s en raison de la largeur de bande du signal chaotique. Tandis que les systèmes électro-optiques sont capables de développer un chaos fort avec une largeur de bande qui peut atteindre plusieurs dizaines de gigahertz. Dans de tels systèmes électro-optiques, le chaos a été induit dans l'intensité. Encouragé par ce succès, d'autres systèmes électro-optiques induisant le chaos en phase ont été proposés.

On distingue donc en général trois types de crypto-systèmes optiques permettant de générer le chaos : une diode laser à rétroaction générant un chaos en intensité, un modulateur électro-optique à rétroaction générant soit un chaos en intensité soit un chaos en phase.

CHAPITRE 3

Etude d'un Crypto-Système Chaotique à base de modulateur MZM à Rétroaction

III.1 Introduction

L'un des systèmes appartenant à la convenable classe de systèmes chaotiques capables de développer une grande complexité a été proposé en 2002 par Goedgebuer et al. Ce système utilise une rétroaction non linéaire à retard, avec une source Laser CW à semi-conducteur. La non-linéarité est mise en œuvre par l'intermédiaire d'un Modulateur de Mach-Zehnder à niobate de lithium (LiNbO)3. Dans ce travail, nous nous sommes intéressés à cette configuration simple, pour mettre en évidence la possibilité de chiffrement chaotique dans le domaine optique.

III.2 Rappel sur le Modulateur Mach-Zehnder (MZM)

Le modulateur Mach-Zehnder (MZM) est, dans sa version la plus simple, un interféromètre constitué généralement d'un bras de référence et d'un bras dans lequel une variation de phase est induite par effet électro-optique (variation de l'indice de réfraction du cristal).

Ces deux bras sont deux guides optiques parallèles et de longueurs égales. Si aucune tension n'est appliquée aux guides d'ondes, la lumière incidente est divisée de manière égale entre les deux bras de l'interféromètre. La recombinaison des ondes provenant des bras conduit à une figure d'interférence (Figure 3.1).

Si une tension est appliquée à l'un des bras de sorte que la différence de phase entre les deux faisceaux de sortie est un multiple impair de l'interférence est destructif : l'interféromètre a une transmission nulle. L'interféromètre de MZM constitue donc un modulateur d'intensité. En utilisant ce type de composant, il est possible de réaliser un émetteur optique par modulation d'amplitude. L'intensité à la sortie peut être de façon générale, représentée par :

$$I_{out}/I_{in} = cos^2(\frac{\pi V}{2V_\pi})$$

Où : V est la tension appliquée au borne des électrodes

Vπ est la tension demi-onde du modulateur MZM , c'est la tension pour laquelle on a une sortie nulle.

Il faut noter que la tension demi-onde est différente suivant qu'on est en statique ou en dynamique. Généralement, il existe deux valeurs : $V_{\pi DC}$ et $V_{\pi RF}$. (Figure 3.2).

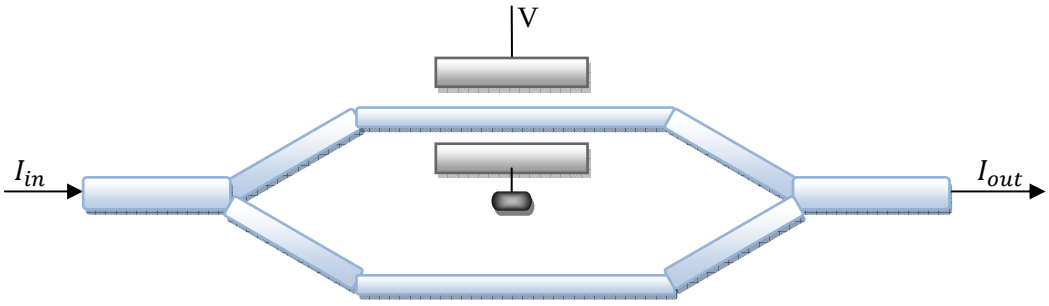


Figure 3.1 : Principe de fonctionnement du modulateur Mach-Zehnder

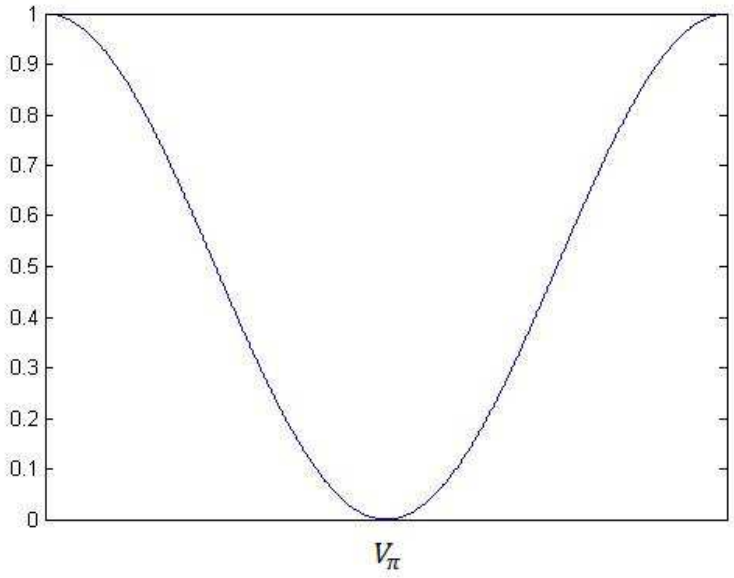


Figure 3.2 : Fonction de transfert d'un modulateur Mach-Zehnder

III.3 Crypto-système chaotique à base de modulateurs MZM à rétroaction

On se propose dans cette partie d'étudier et évaluer les performances du crypto-système représenté par les figures 3.3 et 3.4.

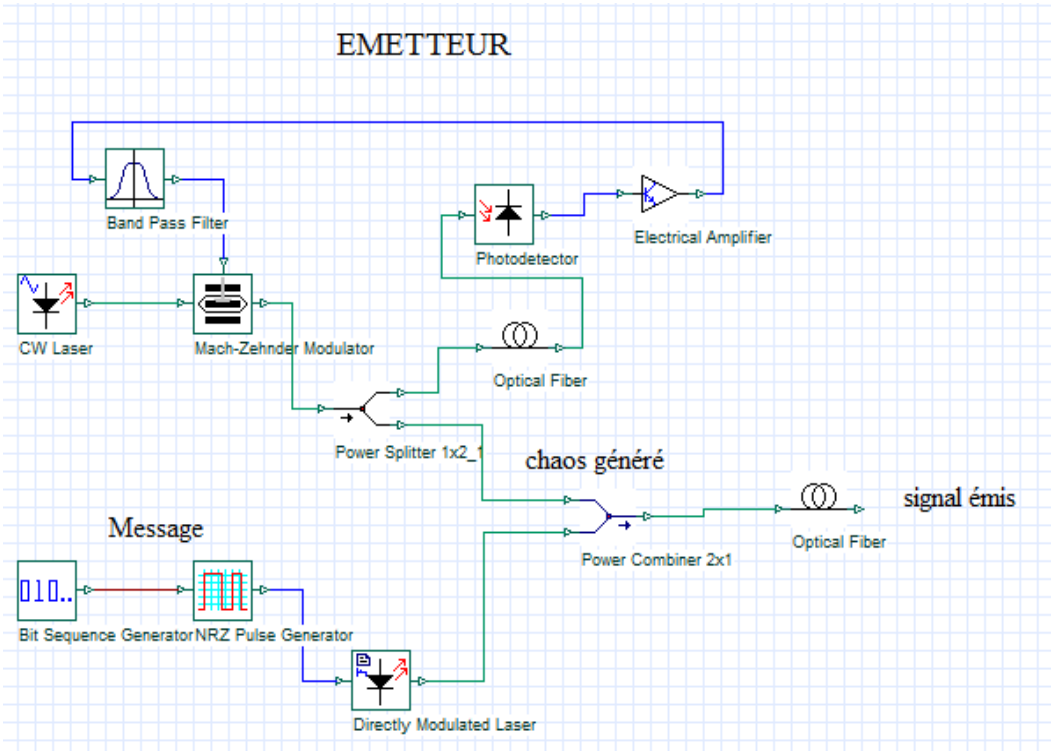


Figure 3.3 : Crypto-système chaotique basé sur un MZM à rétroaction : Emetteur

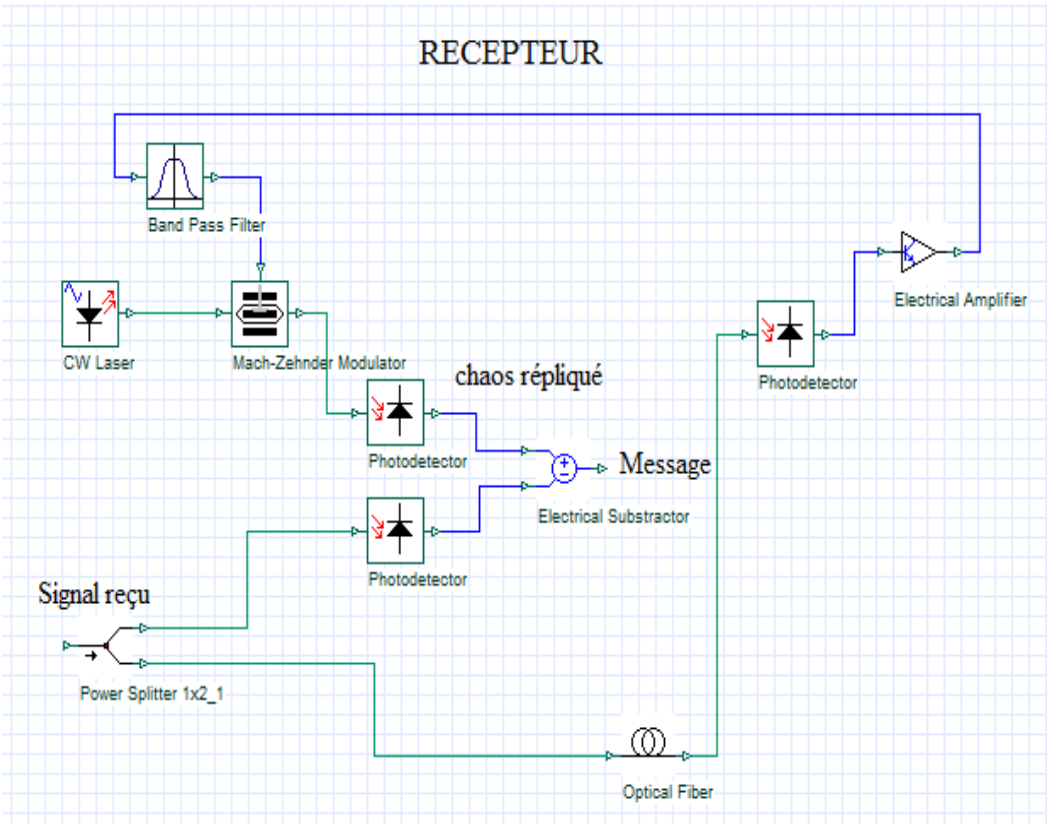


Figure 3.4 : Crypto-système chaotique basé sur un MZM à rétroaction : Récepteur

Le système se compose au niveau de l'émetteur :

- d'un module pour la génération de chaos optique
- d'un module pour le chiffrement chaotique par un combiner optique

Au niveau du récepteur, nous avons :

- un module pour la synchronisation du chaos
- un module pour le déchiffrement

III.3.1 Modélisation du système

Dans ce qui suit, nous présentons les composantes du module générateur de chaos.

- Un laser CW à semi-conducteur (SL) délivrant une puissance constante $P_0 = h\gamma I$ (où h représente la constante de Planck, γ est la fréquence d'émission de photons et I le nombre de photons.

- Un modulateur Mach Zehnder (MZM) : La lumière provenant de la SL est uniformément divisée en deux branches du MZM et interfère à sa sortie. La réfraction de l'indice d'un bras est modulée par la tension de sortie d'un conducteur électronique. La tension appliquée a deux composantes: une composante constante de V_{DC} qui permet de sélectionner le point de fonctionnement du modulateur et la composante radiofréquence RF, V(t) qui est utilisé pour générer le chaos. L'enveloppe complexe du champ électrique à la sortie MZM peut s'écrire :

$$E(t) = \frac{1}{2} E_0 \left\{1 + e^{j\left(\frac{\pi V(t)}{V_{\pi RF}} + \frac{\pi V_{DC}}{V_{\pi DC}}\right)}\right\}$$

Où $V_{\pi RF}$ et $V_{\pi DC}$ sont synonymes de la tension demi-onde RF et de la tension demi-onde de l'électrode de polarisation respectivement et E_0 est l'amplitude de la sortie SL. La puissance de sortie optique est donnée par :

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

Où $P_{0=} E_0{}^2$

- une ligne à retard à fibre utilisée pour retarder le signal optique dans le temps. La fibre est supposée non dispersive (indépendant de la fréquence du signal retardé), de sorte que le retard T est donné par : T = L/ Vi, où L est la longueur de la fibre et Vi est la vitesse de groupe.

- Une photodiode avec une sensibilité S pour détecter le signal optique (intensité) et le convertir en un signal électrique.

- Un amplificateur de gain G.

- Un filtre RF qui peut être passe-bas, passe-haut ou passe-bande de n'importe quel ordre. Le Tableau 3.1 survole les principaux filtres 1er ordre. Ici, on suppose un filtre passe-bande de 1er ordre de fréquence de coupure basse F_1 et de fréquence de coupure haute F_2.

La fonction de transfert $H_F(p)$ du filtre, dans le domaine de Laplace, est donnée par :

$$H_F(p) = \frac{\tau_2\ p}{(1+\tau_2 p)(1+\tau_1 p)}$$

Où : $\tau_1 = \frac{1}{2\pi F_1}$ et $\tau_2 = \frac{1}{2\pi F_2}$

Filtrer	Type de représentation dans le domaine temporel	bande passante
Passe-bas de 1er ordre	$x(t) + \tau \frac{dx(t)}{dt}$	$[0, f_H = \frac{1}{(2\pi\tau)}]$
passe-haut 1er ordre	$x(t) + \frac{1}{\tau}\int_{t_0}^{t} x(t')\,dt'$	$[f_B = \frac{1}{2\pi\tau}, \infty]$
passe-bande de 1er ordre	$(1+\frac{\tau 1}{\tau 2})x(t) + \tau 1\ \frac{d\,x(t)}{dt} + \frac{1}{\tau 2}\int_{t_0}^{t} x(t')dt'$	$[f_B, f_H]$

Tableau 3.1 : Filtres et leurs équations correspondantes

Ainsi, le système peut être décrit par la tension de sortie RF en tant que :

$$\left(1+\frac{\tau_1}{\tau_2}\right) V(t) + \tau_1 \frac{dV}{dt}(t) + \frac{1}{\tau_2}\int_{t_0}^{t} V(t')dt' = GSP(t-T)$$

Par dérivation, nous obtenons :

$$\left(1+\frac{\tau_1}{\tau_2}\right) \dot{V}(t) + \tau_1 \ddot{V}(t) + \frac{1}{\tau_2} V(t) + \frac{\pi}{2}\frac{GSP_0}{V_{\pi RF}}\dot{V}(t-T)sin\left[\pi\frac{V(t-T)}{V_{\pi RF}} + \pi\frac{V_{DC}}{V_{\pi DC}}\right] = 0$$

Il s'agit donc d'un système dynamique régi par une équation différentielle non linéaire du second ordre à retard.

Posons : $\frac{\pi}{2}\frac{GSP_0}{V_{\pi RF}} = \beta$ et $\pi\frac{V_{DC}}{V_{\pi DC}} = \varphi$,

Il s'en suit :

$$\left(1+\frac{\tau_1}{\tau_2}\right) \dot{V}(t) + \tau_1 \ddot{V}(t) + \frac{1}{\tau_2} V(t) + \beta\dot{V}(t-T)sin\left[\pi\frac{V(t-T)}{V_{\pi RF}} + \varphi\right] = 0$$

III. 3.2 Paramètres du modèle

Les paramètres du système sont facilement identifiés :

τ_1 , τ_2 , β , $T, V_{\pi RF}$ et φ .

Dans ce travail, nous avons fixé les valeurs de τ_1 , τ_2 , $T, V_{\pi RF}$ et φ , et nous avons étudié l'évolution du système en fonction de β.

Le tableau 3.2 résume ces valeurs :

$\tau_1(\mu s)$	τ_2(ns)	T(ns)	$V_{\pi RF}(V)$	φ (rad)
$\frac{1}{2\pi}$	$\frac{1}{2\pi}$	10	5	$\frac{\pi}{4}$

Le choix de $\varphi = \frac{\pi}{4}$ a été fait de façon à avoir une non linéarité forte.

A noter qu'en pratique les valeurs de ces paramètres doivent être non triviales et confidentielles, puisqu'elles représentent la clé du crypto-système.

III. 4 Evaluation du système- Résultats de Simulation

III. 4.1 Méthodologie

Faute d'équipements pour l'expérimentation, l'évaluation des performances et la validation du modèle que nous venons de présenter a été conduite par voie de simulation. Dans un premier temps, nous avons tenté d'utiliser le simulateur connu Optisystem, mais très vite nous avons heurté un obstacle. En effet, Optisystem ne prend pas en charge la simulation des rétroactions, une fonction essentielle dans notre modèle.

Nous nous sommes retournés donc vers Matlab, et cette fois-ci nous avons été amenés à procéder à une intégration numérique d'équations différentielles non-linéaires du second ordre à retard.

A) Méthodes de résolutions numériques

Les méthodes d'intégration numérique des équations différentielles peuvent être classées en deux types: les méthodes explicites et les méthodes implicites. Une méthode est dite explicite si la valeur

X_{i+1} peut être calculée directement à l'aide des valeurs précédentes X_i (ou d'une partie d'entre elles). Une méthode est dite implicite si la valeur X_{i+1} n'est définie que par une relation implicite fonction de X_i .

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

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

- Méthode d'Euler

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

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

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

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

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

$$X_{i+1} = X_i + h\,.F(x_i, t_i) + O(h^2)$$

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

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

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

- Méthode de Runge-Kutta d'ordre 4

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

$$X_{i+1} = X_i + \frac{h}{6}\,.(k_1 + 2.k_2 + 2.k_3 + k_4) + O(h^5)$$

Avec :

$$k_1 = F(x_i, t_i)$$
$$k_2 = F(x_i + \frac{h}{2}.k_1, t_i + \frac{h}{2})$$
$$k_3 = F(x_i + \frac{h}{2}.k_2, t_i + \frac{h}{2})$$
$$k_4 = F(x_i + h, t_i + h)$$

Cette méthode est à pas constant, très utilisée pour réaliser les intégrations numériques. Elle a le principal avantage d'avoir une précision en h^4, et converge rapidement. Néanmoins, elle reste assez coûteuse en temps de calcul car, elle nécessite d'évaluer de manière itérative 4 fois la fonction F.

B) Implémentation sous Matlab

Nous avons utilisé pour cela la fonction DDE23 qui repose sur l'algorithme de Runge Kutta.

A partir de l'équation du second ordre, on passe à un système à deux équations du premier ordre. On pose pour cela :

$$V(t) = y_2(t)$$

Il s'en suit :

$$\left(1 + \frac{\tau_1}{\tau_2}\right) \dot{y_2}(t) + \tau_1 \ddot{y_2}(t) + \frac{1}{\tau_2} y_2(t) + \beta \dot{y_2}(t-T) sin\left[\pi \frac{y_2(t-T)}{V_{\pi RF}} + \varphi\right] = 0$$

Ensuite :

$$\dot{y_2}(t) = y_1(t)$$

D'où le système du 1er ordre :

$$\dot{y_1}(t) = -\left(\left(\frac{1}{\tau_1} + \frac{1}{\tau_2}\right) y_1(t) + \frac{1}{\tau_1 \tau_2} y_2(t) + \frac{\beta}{\tau_1} y_1(t-T) sin\left[\pi \frac{y_2(t-T)}{V_{\pi RF}} + \varphi\right]\right)$$

$$\dot{y_2}(t) = y_1(t)$$

C) **Caractérisation du chaos**

Nous avons procédé dans ce travail à la détermination des caractéristiques suivantes :

- le diagramme de bifurcation

Le script Matlab pour la détermination du diagramme de bifurcation est le suivant :

```
%Diagramme de bifurcation
bmin=0.0001;
bmax=0.01;
bint=0.0001;

brange=[bmin bint bmax];
bifurcation(brange);

end

function output=bifurcation(range)

D=[];

for b=range(1):range(2):range(3)

    fprintf('b=%g...\n',b);

    solb = dde23(@chaosf,10*10^-9,[10^-3;0],[0,2*10^-7],[],b);

    for i=2:length(solb.y(2,:))-1
        if((solb.y(2,i)>solb.y(2,i-1))&&(solb.y(2,i)>solb.y(2,i+1)))
            D=[D; b solb.y(2,i)];
        end
    end
end

figure(3)
plot(D(:,1),D(:,2),'ro','MarkerEdgeColor','b','MarkerFaceColor','b','MarkerSize',1.5)
```

- l'évolution temporelle du signal chaotique

Le script Matlab pour l'intégration numérique et la représentation temporelle du signal est le suivant :

```
function sol = chaos
% chaos-optique

T=3e-6; %durée du signal
b=1.5;
sol = dde23(@chaosf,10*10^-9,[10^-6;0],[0,T],[],b);

%representation temporelle
figure(1)
plot(sol.x,sol.y(2,:));

end
%-------------------------------------------------------------------------
function yp = chaosf(t,y,Z,b)

%paramétres du chaos

phi=pi/4;
to1=1/(2*pi*10^9);
to2=1/(2*pi*10^6);
Vprf=5.0;

%equations
ylag1 = Z(:,1);
yp = zeros(2,1);
yp(2) = -((1/to1)+(1/to2))*y(2)-(1/(to1+to2))*y(1)-(b/to1)*ylag1(2)*sin(((pi*ylag1(1))/Vprf)+phi);
yp(1) = y(2);
y(2)

end
```

- la densité spectrale de puissance

Le script Matlab pour le calcul de densité spectrale de puissance est :

```
%Spectre

Te=0.01e-9;

Fe=1/Te;
N=round((T/Te)/2);


t = linspace(T/2,T,N);
y = deval(sol,t);

f=0:Fe/N:Fe/2-Fe/N;

dsp=(abs(fft(y(2,:)))).^2);
plot(f,10*log(dsp(1:length(f))+0.0000000001))
```

- le plan de phase

Le script Matlab pour la représentation de l'espace et le plan de phase est :

```
%Espace de phase 3D
figure(6)
tau=0.3*10^-6;
t = linspace(2*tau,T,10000);
y = deval(sol,t)/0.5e-6;
yy = deval(sol,t - tau)/0.5e-6;
yyy= deval(sol,t - 2*tau)/0.5e-6;
plot3(y(2,:),yy(2,:),yyy(2,:),'.')

%Plan de phase
figure(5)
 plot(y(2,:),yy(2,:),'.')
```

D) **Chiffrement-déchiffrement**

Les opérations de chiffrement et déchiffrement ont été réalisées sous Optisystem. A défaut de générer, sous Matlab, à la réception un réplica du chaos par synchronisation, nous avons procédé comme suit :

Le signal chaotique à l'émission a été généré sous Matlab par intégration numérique, puis enregistré dans un fichier .dat. Ce fichier est utilisé sous Optisystem pour le chiffrement et le déchiffrement conformément à la figure 3.5.

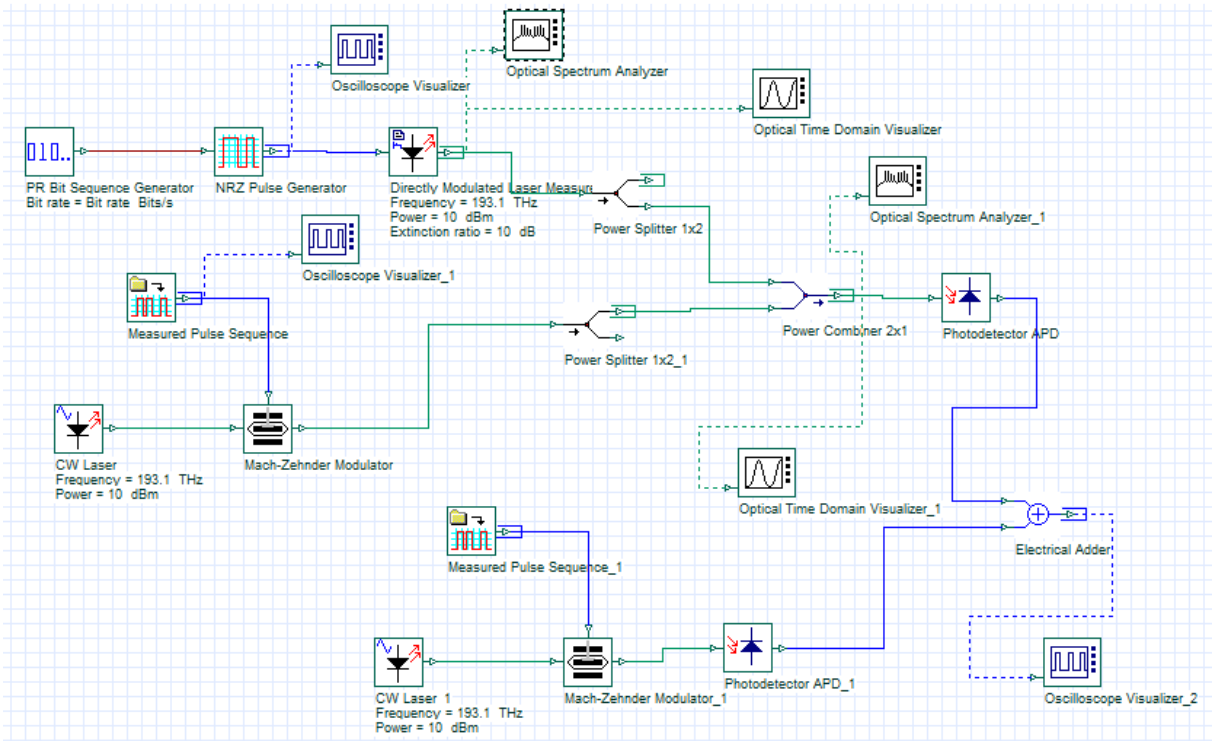


Figure 3.5 : Schéma du chiffrement-déchiffrement

III.4.2 Résultats de simulation

1) Diagramme de bifurcation

La figure 3.6 montre le diagramme de bifurcation du système en fonction du gain de rétroaction beta.

Nous constatons que le chaos commence à s'installer à partir de beta=0.13. On peut voir également que pour les grandes valeurs de beta, le système est fortement chaotique. Malheureusement, on n'a pas pu aller plus loin pour les valeurs de beta, à cause de la faible puissance de calcul des machines utilisées.

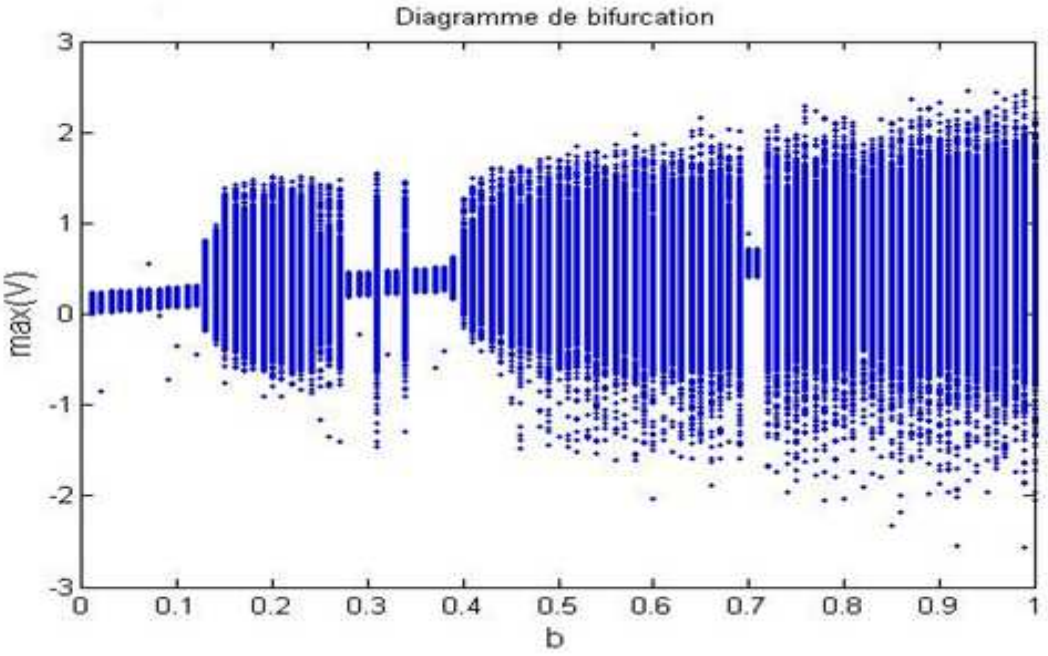


Figure 3.6 : Diagramme de bifurcation en fonction du paramètre de contrôle beta

Dans ce qui suit nous allons présenter les résultats, pour quelques valeurs de beta donnant chacune un comportement différent.

2) Etude pour β=0.1

On a un régime périodique, comme on peut le voir sur la représentation temporelle du signal v(t) récupéré à la sortie du filtre passe bande (figures 3.7 et 3.8).

Le spectre est caractérisé par la présence d'une seule fréquence fondamentale et plusieurs harmoniques (figure 3.9). Sur la figure 3.10, on remarque dans le plan de phase un attracteur cycle limite mettant en évidence un comportement périodique.

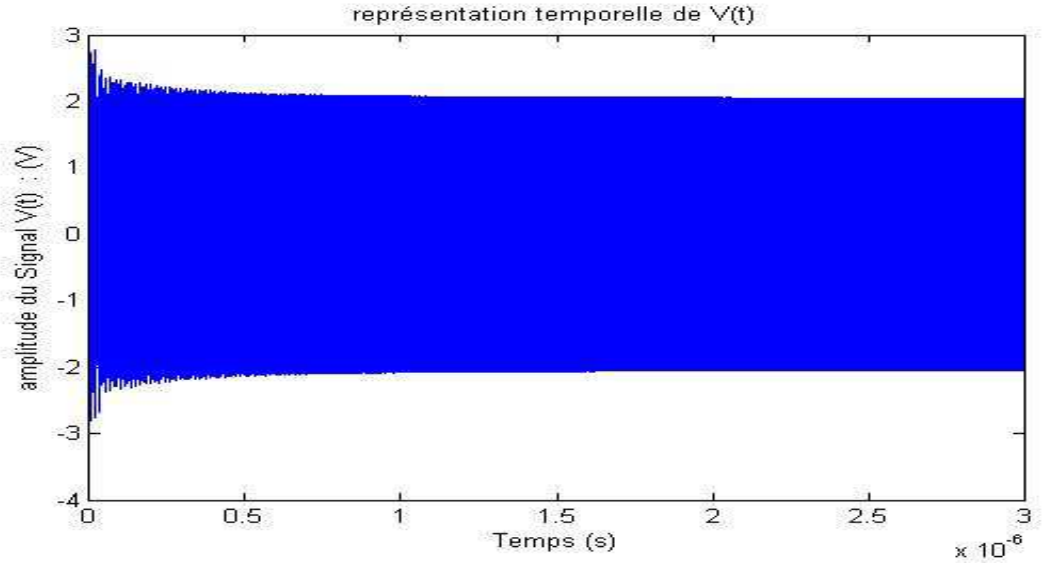


Figure 3.7 : Représentation temporelle du signal V(t) , beta=0.1

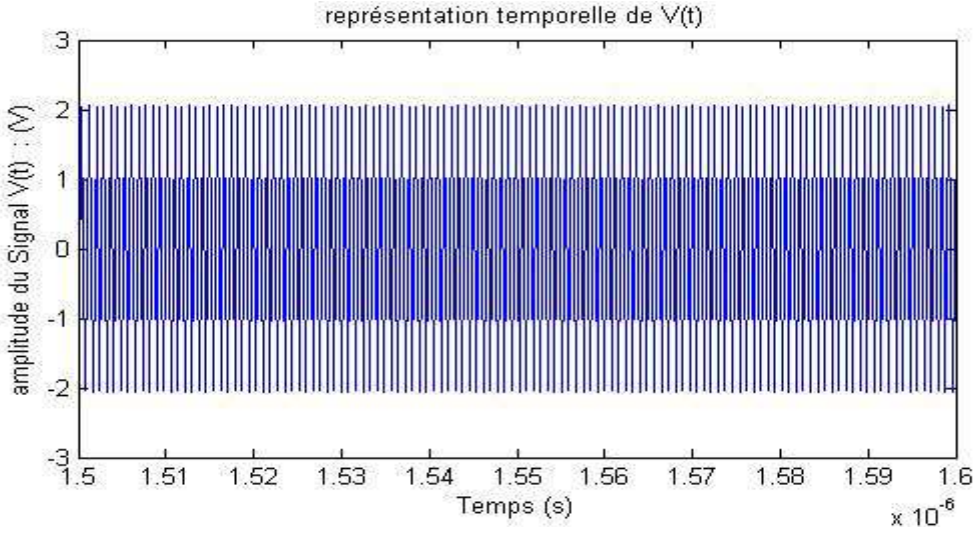


Figure 3.8 : Zoom sur le représentation temporelle du signal V(t) , beta=0.1

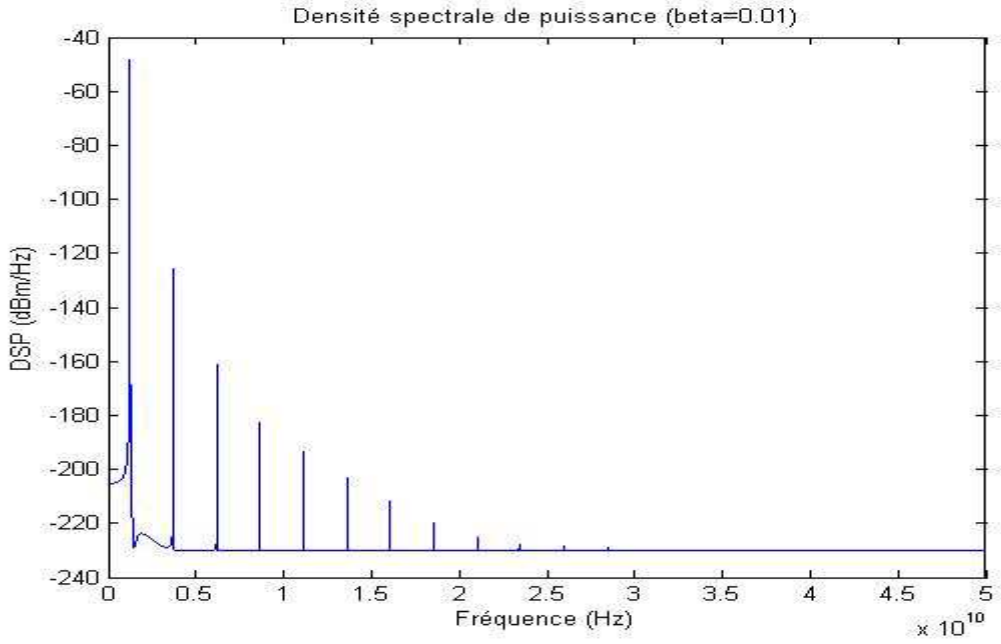


Figure 3.9 : Représentation de la densité spectrale de puissance du signal V(t) , beta=0.1

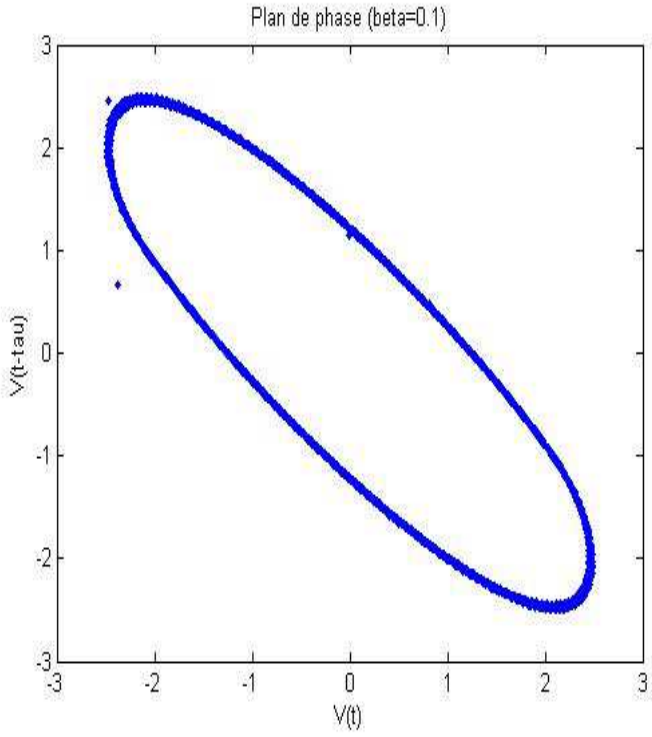


Figure 3.10 : Plan de phase (beta=0.1 , tau=300 ns)

3) Etude pour β=0.127

On constate que le signal est quasi-périodique (figures 3.11 et 3.12). Le spectre est formé de plusieurs fréquences de base avec leurs harmoniques (figure 3.13).

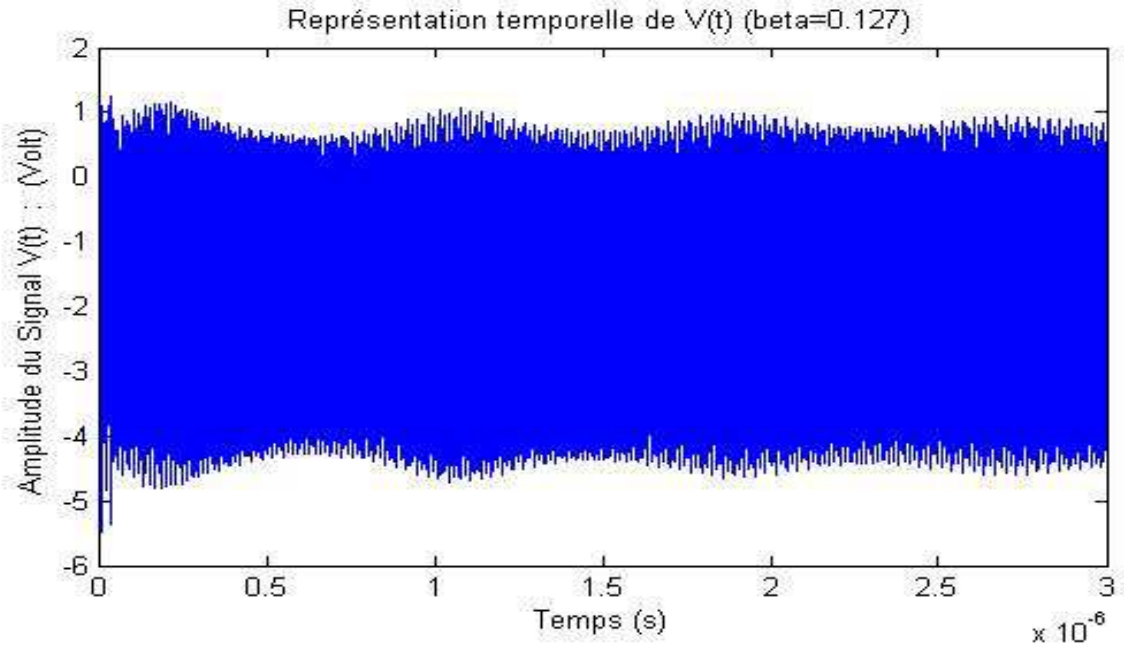


Figure 3.11 : Représentation temporelle du signal V(t) , beta=0.127

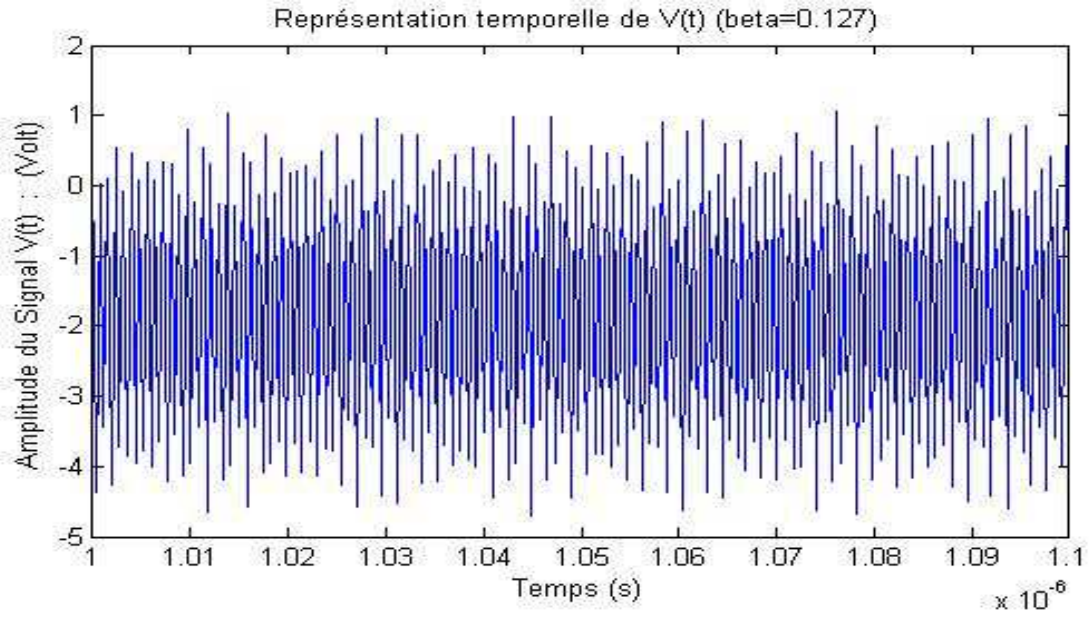
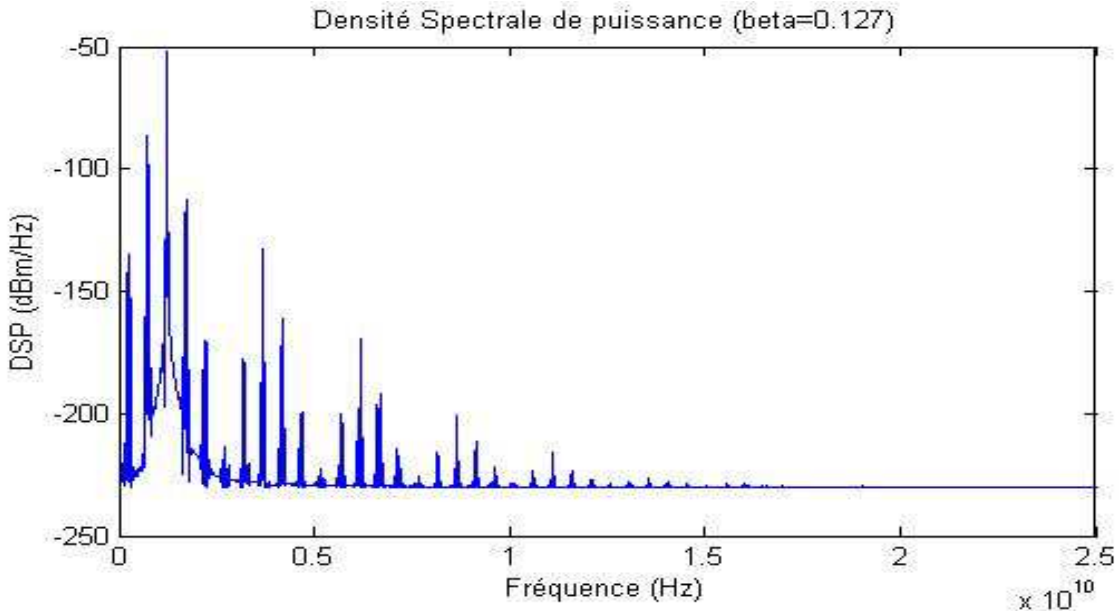


Figure 3.12 : Zoom sur le représentation temporelle du signal V(t) , beta=0.127

Sur la figure 3.14, on note un attracteur de type tore supra de dimension >= 2.

Il faut noter que la multiplication successive des fréquences de base engendre le chaos, ce qui est appelé bifurcation par quasi-périodicité.



3.13 : Représentation de la densité spectrale de puissance du signal V(t)

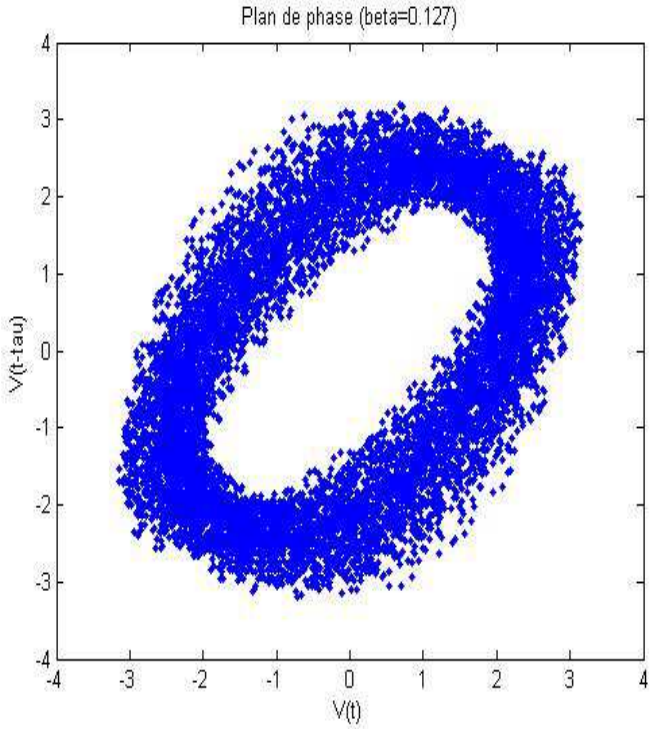


Figure 3.14 : Plan de phase (beat=0.127, tau=300 ns)

4) Etude pour β=0.2

Il est fort de constater que le signal est dans ce cas chaotique (figures 3.15 et 3.16). Ceci est confirmé par la courbe de la densité spectrale de puissance qui apparait très dense (figure 3.17). L'attracteur sur la figure 3.18 sera qualifié d'étrange.

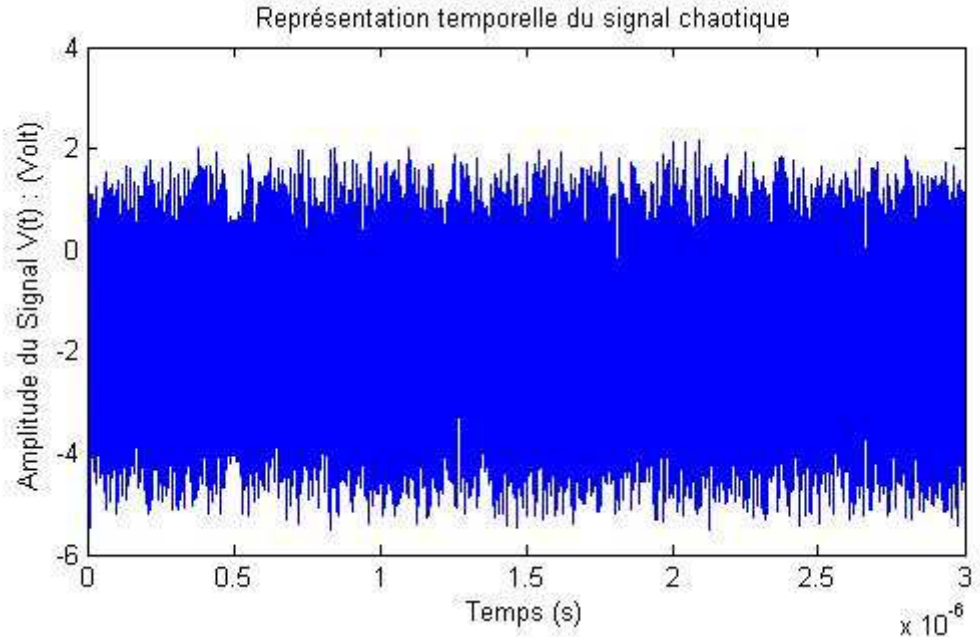


Figure 3.15 : Représentation temporelle du signal V(t) , beta=0.2

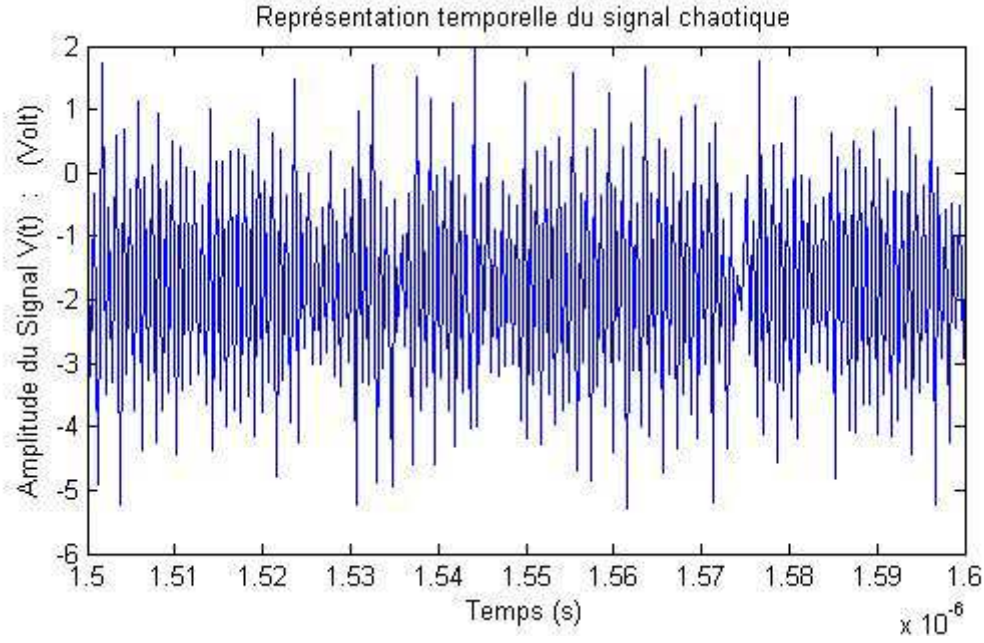


Figure 3.16 : Zoom sur le représentation temporelle du signal V(t) , beta=0.2

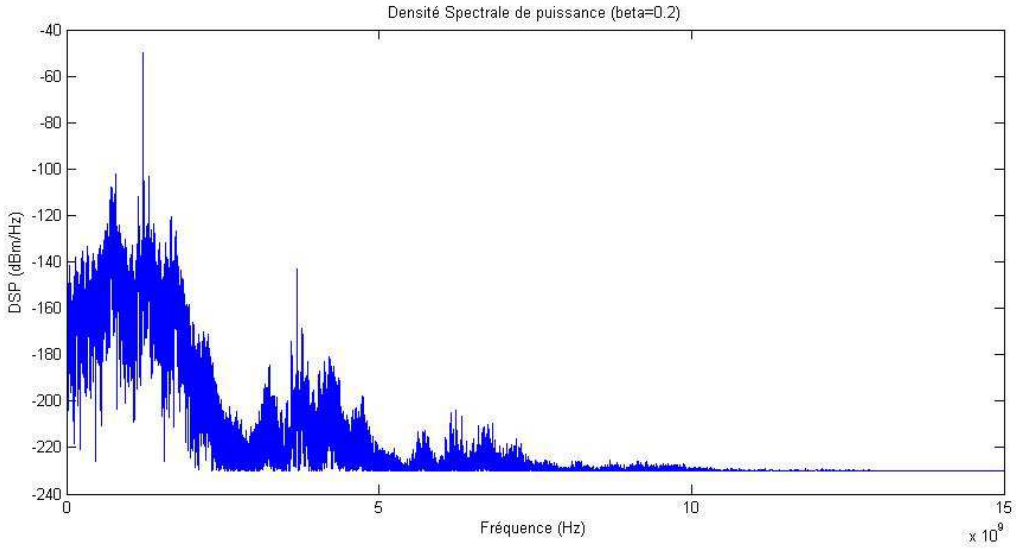


Figure 3.17 : Représentation de la densité spectrale de puissance du signal V(t) , beta=0.2

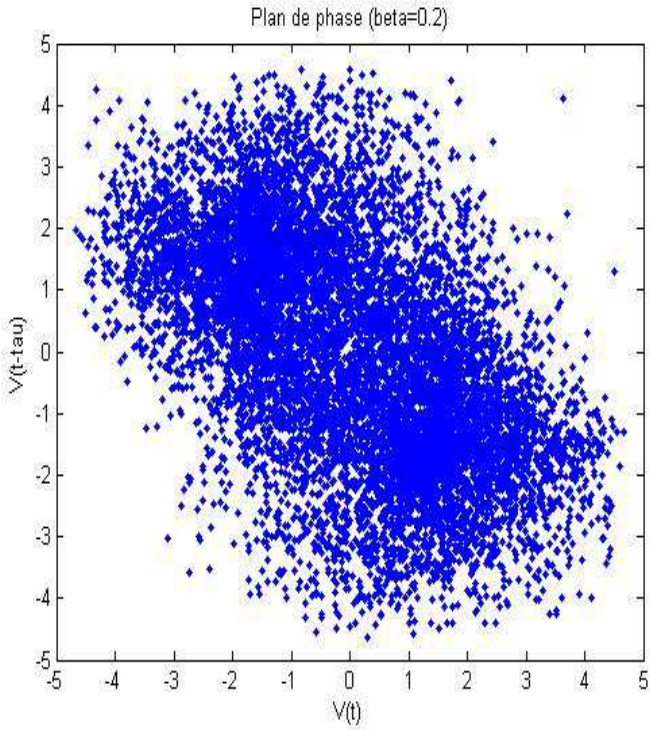


Figure 3.18 : Plan de phase (beta=0.2, tau=300 ns)

Bien sûr, nous avons présenté jusqu'à présent une caractérisation qualitative. Pour mettre, en évidence la complexité du chaos et donc le caractère hyper-chaotique, il faut passer par une

caractérisation quantitative, c'est-à-dire déterminer les exposants de Lyapunov et la dimension fractale de l'attracteur étrange. Chose qui n'a pas abouti à cause toujours du même problème calculatoire. Elle reste donc une perspective.

5) Chiffrement-déchiffrement

Comme nous l'avons déjà signalé, les opérations de chiffrement et de déchiffrement ont été réalisées sous Optisystem. Le même fichier contenant le signal chaotique généré sous Matlab est utilisé pour le chiffrement et le déchiffrement;

Le signal chaotique vient attaquer le MZM, puis est combiné optiquement au signal optique modulé par le message d'information (figures 3.19, 3.20 et 3.21). Ensuite le signal optique chiffré (figure 3.22) passe par la photodiode.

Le signal répliqué du chaos attaque un autre MZM polarisé en opposition de phase. Après détection, les deux signaux sont additionnés, et le message est déchiffré (figure 3.23).

Les opérations de chiffrement et déchiffrement sont réalisées avec succès, sous l'hypothèse, bien sûr, de synchronisation au niveau du récepteur.

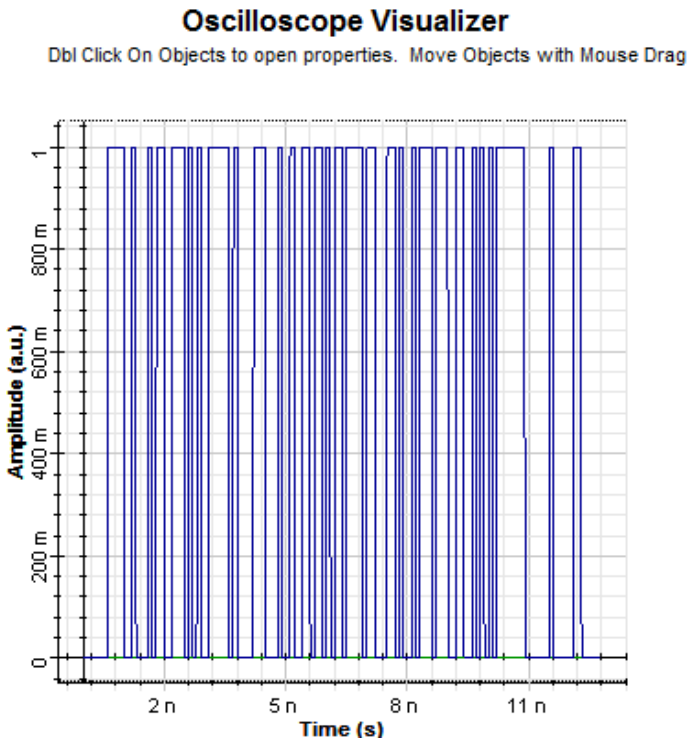


Figure 3.19 : Message émis, code NRZ

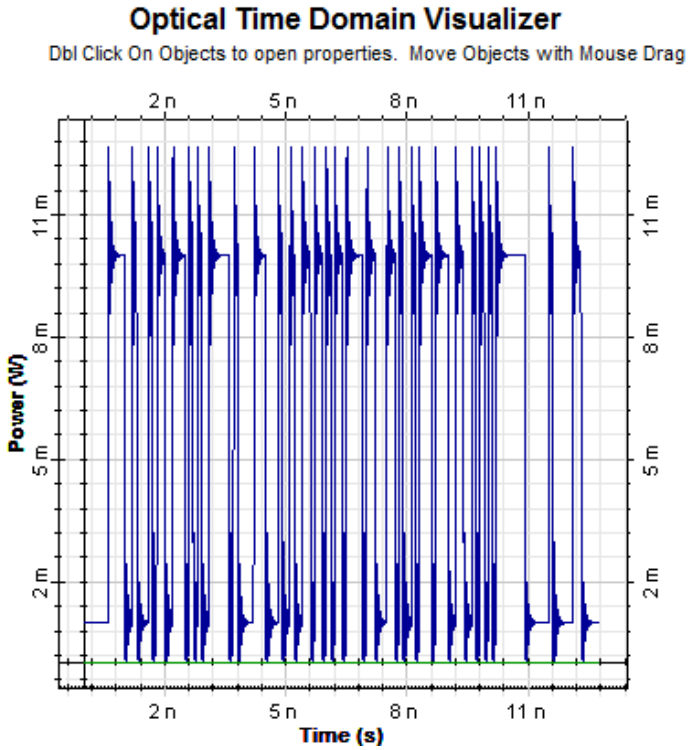


Figure 3.20 : Signal optique modulé par le message émis

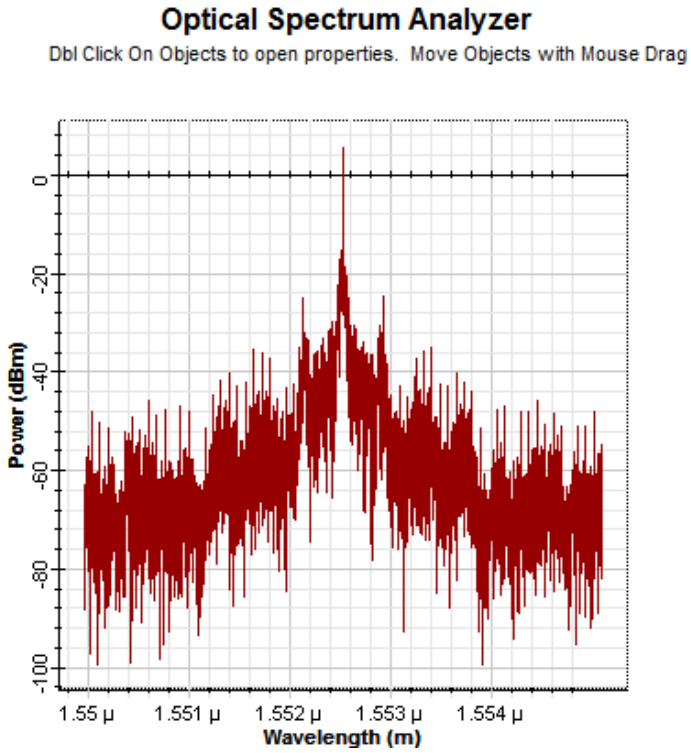


Figure 3.21 : spectre du signal optique modulé par le message émis

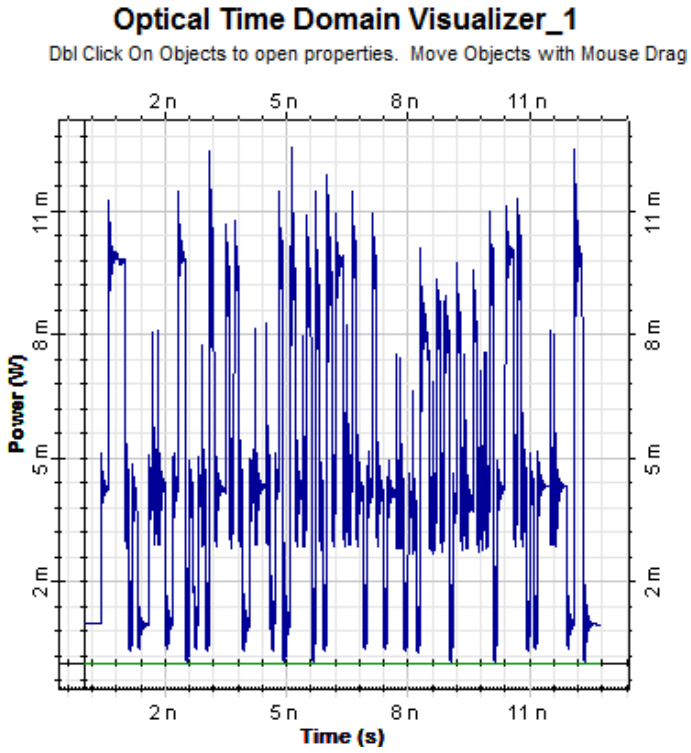


Figure 3.22 : Signal optique chiffré

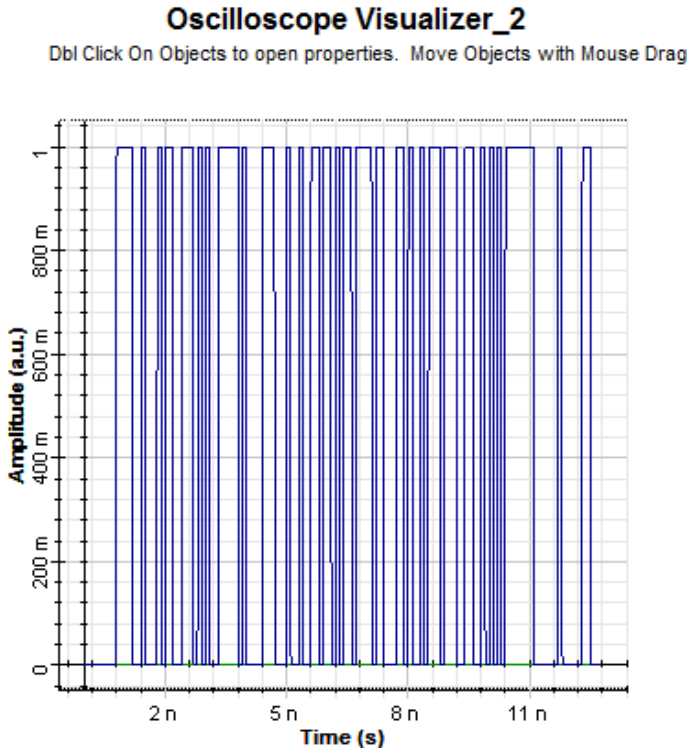


Figure 3.19 : Message reçu déchiffré, code NRZ

Conclusion générale

Nous avons présenté dans ce mémoire un crypto-système optique basé sur le chaos en intensité. Le principe s'appuie sur une dynamique électro-optique non linéaire à retard, dont la non linéarité est réalisée grâce à un modulateur Mach Zehnder à une seule électrode. Le système comporte quatre modules, deux au niveau de l'émetteur : le générateur de chaos et le module de chiffrement, et deux au niveau du récepteur : les modules de synchronisation et de déchiffrement. Le système permet de disposer d'une part, d'une dynamique ultra-rapide jusqu'à des fréquences de plusieurs GHz, et d'autre part, de générer un chaos de grande dimension fractal.

Nous avons développé un modèle mathématique pour le système étudié qui nous a conduits à une équation différentielle non linéaire du second ordre à retard.
Au travers d'une étude numérique sous Matlab, nous avons cherché dans un premier temps à étudier les comportements dynamiques que peut présenter le générateur de chaos en fonction de divers paramètres, en particulier en fonction du gain de la boucle de rétroaction.

A partir du diagramme de bifurcation, nous avons identifié les valeurs critiques de ce gain pour les quelles le chaos est capable de s'installer. L'évolution temporelle du signal généré, sa densité spectrale et le plan de phase nous ont permet de confirmer ces résultats.

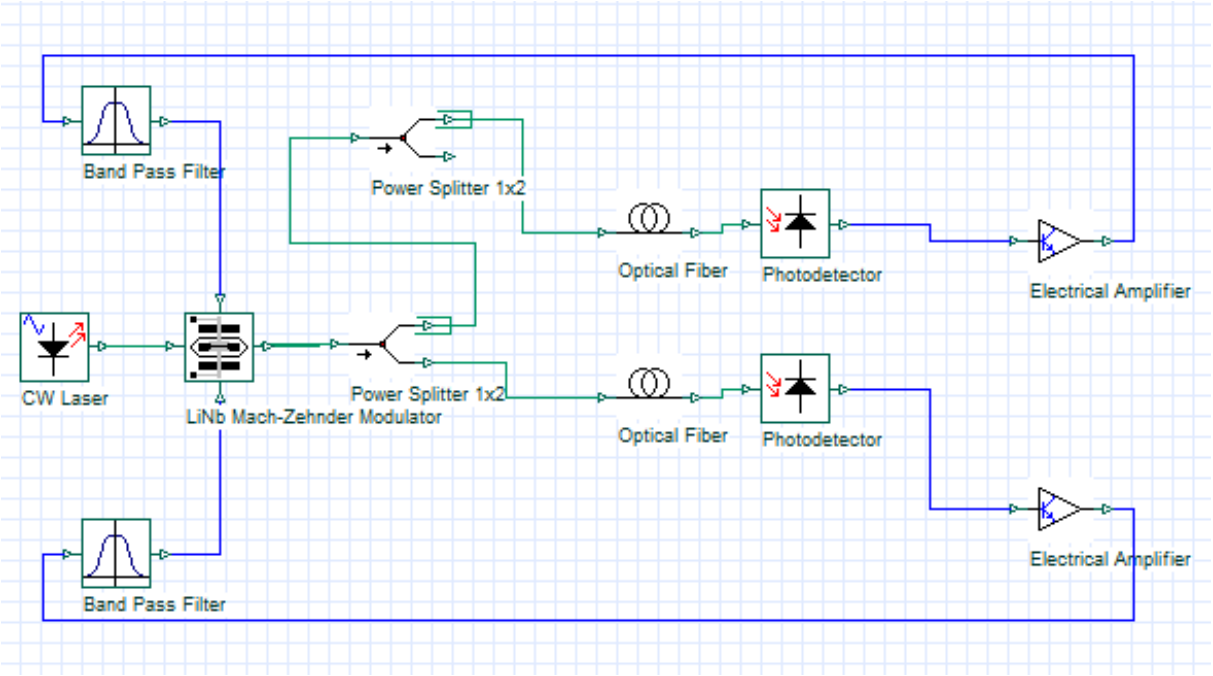
La caractérisation quantitative du chaos généré en termes d'exposants de Lyapunov et dimension fractale, qui nous peuvent renseigner sur la complexité du chaos, n'a pas abouti et nous a amené à constater une difficulté sérieuse pour l'aboutissement au convergence, en raison de la faible puissance des calculateurs disponibles. C'est d'ailleurs notre premier prochain objectif dans la continuité à ce travail.

Le chaos généré par voie optique a été utilisé pour l'opération de chiffrement réalisée par addition d'intensité. Les opérations de chiffrement et déchiffrement ont été réalisées avec succès en utilisant dans Optisystem les données du signal chaotique obtenues par intégration numérique sous Matlab. La synchronisation quant à elle reste une issue pour le système considéré, et représente pour nous une

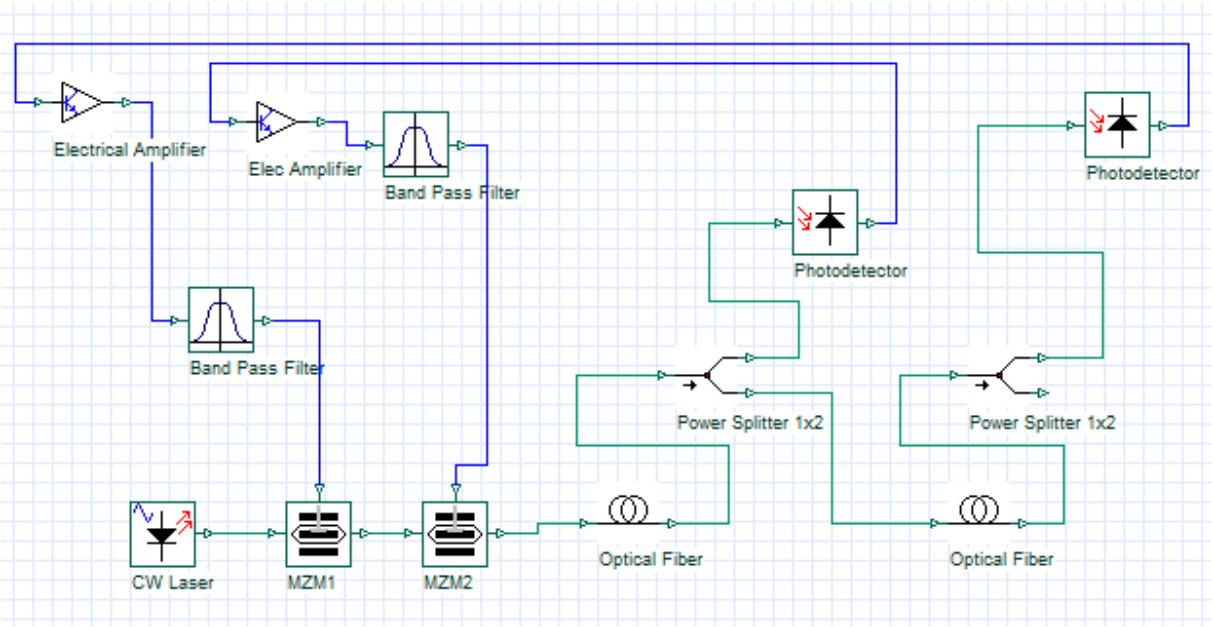
autre perspective. Comme prolongement également à ce travail, dans le cas où la caractérisation quantitative est possible, nous proposons d'étudier et évaluer les performances de deux autres systèmes à double retard

- Crypto-système chaotique à double retard utilisant un seul modulateur MZM à deux électrodes.
- Crypto-système chaotique à double retard utilisant deux modulateurs MZM à une seule électrode.

(a)



(b)



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-dimentional 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. R¨uckert, 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.