REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE ABOU BAKR BELKAID-TLEMCEN
FACULTE DE TECHNOLOGIE
DEPARTEMENT DE TELECOMMUNICATION

MEMOIRE DE FIN D'ETUDE POUR L'OBTENTION Du DIPLOME DE MASTER
EN
TELECOMMUNICATIONS
OPTION
Photoniques Réseau Optique de Télécommunication

THEME

Laser à semi-conducteur dans les communications optiques sécurisées par Chaos

Soutenu le15 juin 2015

Présenté par :

Mme. MESLI Fatima Zohra
Melle. BENBARKA Imane

Devant les membres du jury composés de :

Mr. O.SEDDIKI	**Professeur**	**Président**
Mr. A.R.BORSALI	**Maitre de conférences classe « A »**	**Examinateur**
Mme. F.Z.BENMANSOUR	**Maitre de conférences classe « B »**	**Encadreur**

Année universitaire: 2014– 2015

DEDICACE

Par la grâce de dieu Je dédie ce travail…✍

Je dédie ce travail à mes chers parents qui m'ont encouragé, aidés et soutenus.

Je voudrais remercier mon mari pour son soutient ; sa présence et son courage et d'avoir toujours été à mes côtés.

Je dédier ce travail aussi à :

Mes filles ***Nesrine*** *et* ***Chahinez****, et à ma tante* ***Badia****.*

A toutes mes amies

A toute la famille ***MESLI*** *et* ***KHEDIM***

A toute ma promotion deuxième année master télécommunication

2014-2015

Et a tous ceux qui me portent dans leurs cœurs

FATIMA ZOHRA

DEDICACE

Par la grâce de dieu Je dédie ce travail… ✍

A mes chers parents qui m'ont encouragés, aidés et soutenus et d'avoir été à mes côtés, sans vous je n'aurais jamais atteint ce jour.

A L'être la plus chère : ***ma mère*** *pour son amour, ses sacrifices, sa bienveillance et surtout son soutien tout au long de mon cycle d'étude.*

A mon mari ***RIAD*** *pour son soutient ; sa présence et son courage*

Je dédie ce travail aussi à :

Mes sœurs ***WASSILA*** *et* ***SARAH***

Mes frères ***CHAKIB****et* ***EL HADI***

A toutes mes amies

A mes collègues de travail et le Président Directeur Général

A toute ma promotion deuxième année master télécommunication

2014-2015

Et à tous ceux qui me porte dans leurs cœurs

IMANE

REMERCIMENTS

*Nous voudrons remercier **ALLAH** tout puissant qui nous a donné le courage et la patience pour faire ce modeste travail.*

*Nous exprimons notre gratitude à notre encadreur, Madame **BENMANSOUR F.Z.** pour sa confiance et sa patience qu'elle nous a témoignée, et pour tous les conseils et les idées qu'elle nous a partagées.*

*Nous exprimons notre connaissance au Monsieur **SEDDIKI O.** d'avoir accepté de présider ce jury. Egalement, nous sommes très reconnaissantes à Monsieur BORSALI **R.** qui a bien voulu témoigné son intérêt pour ce travail en tant qu'examinateur.*

Finalement, nos remerciements vont aussi à tous nos professeurs qui ont participés à notre formation, ainsi à toutes les personnes qui nous ont aidées, de prés ou de loin, pour finaliser ce modeste travail.

Table des matières

Liste des figures

Liste des abréviations

$\boldsymbol{\nu_{21}}$ **:** Fréquence
$\boldsymbol{\Delta E}$ **:** D'énergie
$\boldsymbol{h}$ **:** Constante de Planck
$\boldsymbol{R1}$ **:** Indice de réflexion
$\boldsymbol{R2}$ **:** Indice de réflexion
$\boldsymbol{I_s}$ **:** Courant de seuil
$\boldsymbol{N_s}$ **:** Densité des porteurs injectés
$\boldsymbol{P_{pop}(I)}$ **:** La puissance optique délivrée par une facette d'une diode laser
$\boldsymbol{\eta_d}$ **:** représente l'efficacité quantique différentielle
$\boldsymbol{n_g}$: Indice du groupe
$\boldsymbol{\lambda}$ **:** longueur d'onde
$\boldsymbol{h}$ **:** Constante de Planck
$\boldsymbol{\nu}$ **:** Fréquence optique
$\boldsymbol{e}$ **:** Charge de l'électron
$\boldsymbol{I}$ **:** Courant injecté
$\boldsymbol{n}$ **:** L'indice de la cavité
$\boldsymbol{L}$**:** Longueur de la cavité
$\boldsymbol{M}$: Un nombre entier.
$\boldsymbol{\lambda_B}$: longueur d'onde de Bragg
$\boldsymbol{n_{eff}}$ **:** L'indice effectif du guide dans la zone de réseau
$\boldsymbol{V}$ **:** Tension appliquée au borne des électrodes
$\boldsymbol{V\pi}$ **:** tension demi-onde du modulateur MZM
LD : diode laser
Dj : diviseur de tension
RF : filtre passe-bande
DFB : distributed feedback
MEA : modulateur électro-absorbant
MZM : modulateur de Mach-Zehnder
OEO : Oscillateur Electro-Optique
CSK: Chaos Shift Keying
CDMA : code-division multiple access

Introduction Générale

Introduction Générale

Les technologies optoélectroniques ont fortement contribué au développement des télécommunications optiques modernes (par exemple, sources laser, amplificateurs performants et compacts, et fibres optique). Ces réseaux possèdent une structure par couches, comme définie par la représentation OSI (open system interconnexion), comprenant une couche physique de bas niveau (associée au support physique du signal, optique ou électrique), et des couches haut niveaux : liaison de données, réseau, transport, session, présentation et application. Cette architecture modulaire offre cependant de nombreuses failles de sécurité menaçant l'intégrité du réseau de communication.

L'essentiel des efforts de protection des systèmes de communication s'est attaché à l'utilisation et à l'amélioration constante de techniques de cryptographie mathématique. Dans cette approche, un algorithme mélange un message clair (plain text) avec une clé (key) afin que deux parties légitimes (dénomées traditionellement Alice et Bob) puissent échanger des données cryptées (ciphertext) difficilement interprétables par un espion (dénommé Eve). Ce n'est que récemment que la couche physique a suscité l'intérêt de la communauté scientifique.

Il est à présent possible d'utiliser directement les propriétés physiques du signal porteur d'information afin d'apporter un niveau de confidentialité supplémentaire. Deux solutions ont été largement étudiées :

• Les Communications Quantiques utilisant la nature probabiliste des photons (assurée par la mécanique quantique) afin de transmettre des informations sensibles tout en garantissant une sécurité inconditionnelle (au sens de la théorie de l'information).

• Les Communications Chaotiques utilisant les instabilités existant dans certaines sources optiques afin de générer des signaux pseudo-aléatoires de forte complexité dans lesquels des informations seront cachées. Cette approche garantit une sécurité algorithmique similaire à celle produite par certaines méthodes mathématiques (RSA et PGP par exemple).

A l'heure actuelle, les systèmes de communication quantiques, malgré leur haut degré de confidentialité, n'offrent malheureusement que des débits limités (quelques kbit/s) sur de courtes distances (quelques dizaines de km) et sont essentiellement utilisés pour l'échange de clés (quantum key distribution ou QKD).

Les systèmes optiques chaotiques, au contraire, ont de larges bandes passantes, permettant l'échange de données à haut-débit (plusieurs Gbit/s) sur de larges distances.

Une architecture de communication par chaos optique comprend deux oscillateurs chaotiques structurellement identiques (paramètres et non-linéarité) propriétés respectives d'Alice et Bob, et situés à chacune des extrémités d'un canal de communication optique. En début de chaîne, Alice encode son message et l'incorpore au moyen d'une méthode appropriée au signal chaotique avant d'injecter le résultat de l'encryption dans le canal. En fin de chaîne, le récepteur de Bob se synchronise uniquement sur le chaos produit par Alice (la partie déterministe du signal) et une opération de soustraction est ensuite utilisée pour extraire les données chiffrées.

Le développement des communications chaotiques optiques résulte de trois phénomènes physiques: (i) l'émission stimulée mise en évidence par Einstein (le principe physique utilisé dans les lasers), (ii) la théorie du chaos donnant un cadre mathématique aux comportements erratiques de certains systèmes non-linéaires, et enfin, (iii) la synchronisation des systèmes chaotiques.

Malgré leurs performances en terme de complexité algorithmique et leurs larges bandes passantes, les communications par chaos optique demeurent marginales principalement en raison des difficultés à caractériser leur sécurité et à les utiliser dans un contexte multi-utilisateurs.

Le travail présenté dans ce mémoire s'organise autour de trois chapitres :

Le premier chapitre aborde les généralités sur les lasers à semi-conducteurs ainsi que les transmissions optiques sécurisées, les principes des lasers ainsi que leurs compositions sont abordés pour aboutir à la réalisation d'un OEO à rétroaction utilisant deux circuits Mach Zenhder générant une onde Lasers chaotique

Le second chapitre présente la théorie du chaos, et comment l'obtenir à partir des systèmes dynamiques non linéaire, à partir de la non linéarité des lasers à semi-conducteur on a réalisé un générateur de chaos qui sera utilisé pour le chiffrement de l'information

Dans le dernier chapitre, on a réalisé une chaine de transmission sous Optisystem cette chaîne comprenant un générateur de chaos à l'émission et le même à la réception qui vont servir une fois au chiffrement côté émetteur puis au déchiffrement côté récepteur. D'autres résultats tels que le diagramme de bifurcation et le chiffrement d'une image à partir d'un algorithme sous Matlab sont présenté en fin du chapitre III.

Le travail ainsi mené s'achève par une conclusion générale.

Chapitre I

Introduction aux lasers à semiconducteur

I. Introduction :

Ces dernières années L'invention du laser a permis une utilisation potentielle de l'optique dans une transmission de données. Le mot laser est devenu un terme commun à l'origine un acronyme pour Light amplification by stimulated émission of radiation c'est-à-dire Amplification de lumière par émission stimulée.

II. Généralités sur les transmissions optiques :

Comme tous les systèmes de communications, les liaisons optiques se basent sur trois blocs fondamentaux pour effectuer le transfert de l'information : l'élément d'émission, le canal de communication et le récepteur. La particularité de ce système provient des éléments utilisés pour effectuer le transport de l'information. Le bloc d'émission est constitué d'un dispositif diode laser ou source laser qui permet de convertir un signal sinusoïdal électrique en un signal optique. Le canal de transmission (la fibre optique) transporte une porteuse optique modulée contenant l'information. Enfin, le récepteur (le photodétecteur) récupère le signal électrique véhiculé en opérant une conversion optique-électrique.

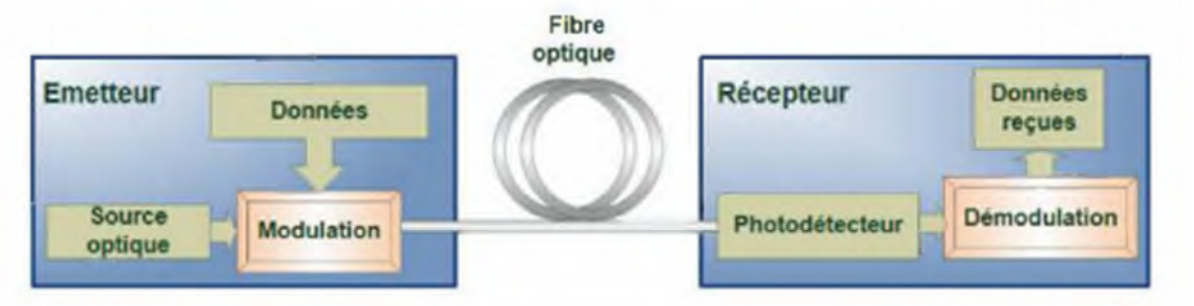


Figure I.1 Synoptique général d'un système de communications par fibre optique

II.1 Le bloc d'émission :

Dès le commencement des télécommunications par fibre optique, le choix des sources optiques s'est appuyé sur les émetteurs à semi-conducteur dont l'évolution des structures s'est faite de manière parallèle aux autres types de lasers. Avec de nombreux avantages :

- Petites dimensions 1.510^{-3}mm^3 en rapport avec celles du coeur des fibres optiques.

- Excellente capacité de modulation en agissant sur le courant
- Couverture spectrale importante (0,4 µm< λ < 30 µm) avec un spectre optique relativement étroit.
- Faible coût de fabrication avec une très bonne fiabilité.
- Alimentation très commode avec une faible consommation énergétique pour donner une puissance pouvant atteindre plusieurs Watts en continu, et donc un bon rendement.
- Facilité d'intégration avec d'autres composants optoélectroniques.

II.1.1 Source laser :

Une source laser associe un amplificateur optique basé sur l'effet laser à une cavité optique, encore appelé résonateur, généralement constituée de deux miroirs, dont au moins l'un des deux est semi-réfléchissant c'est-à-dire qu'une partie de la lumière sort de la cavité et l'autre partie est réinjectée vers l'intérieur de la cavité laser comme il est schématisé dans la figure I.2.

Les caractéristiques géométriques de cet ensemble imposent que le rayonnement émis soit d'une grande pureté spectrale, c'est-à-dire temporellement cohérent. Le spectre du rayonnement contient en effet un ensemble discret de raies très fines, à des longueurs d'ondes définit par la cavité et le milieu amplificateur. La finesse de ces raies est cependant limitée par la stabilité de la cavité et par l'émission spontanée au sein de l'amplificateur (bruit quantique).

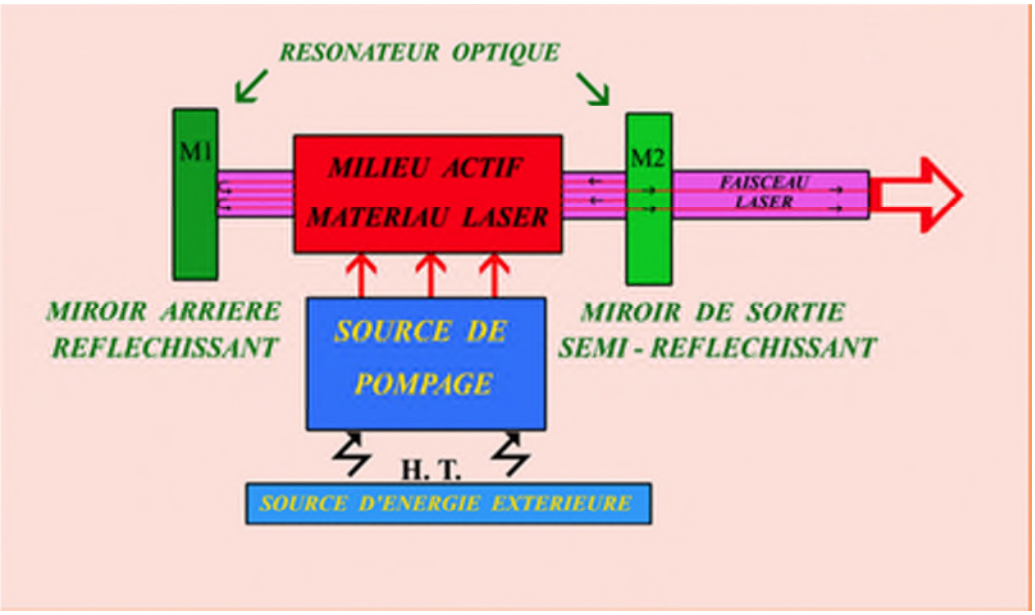


Figure I.2 Principe de fonctionnement d'un laser

II.1.1.1 laser à semi-conducteur :

Les lasers utilisés dans les liaisons optiques actuelles sont les lasers à semi-conducteurs .Le principal matériau utilisé est : L'alliage quaternaire $In_{1-x}Ga_xAs_yP_{1-y}$sur substrat ***InP***. L'alliage ***InGaAsP*** est utilisé dans les applications de télécommunications à cause de ça bande interdite (***gap***) réglable en fonction des valeurs de $\boldsymbol{x}$ et y, qui lui permet d'émettre entre $1\ et\ 1.65\mu m$.

- **Jonction P-N :** Lorsque deux semi-conducteurs type ***P*** et type ***N*** sont mis en contact, ils forment une jonction ***PN.*** Les porteurs libres de chaque région vont être diffusés dans la région de signe opposée, en se recombinant éventuellement dans la zone amoindrie. Et donc une région amoindrie de porteurs libres est formée de deux côtés de la jonction, ainsi le courant de diffusion dure jusqu'à l'équilibre

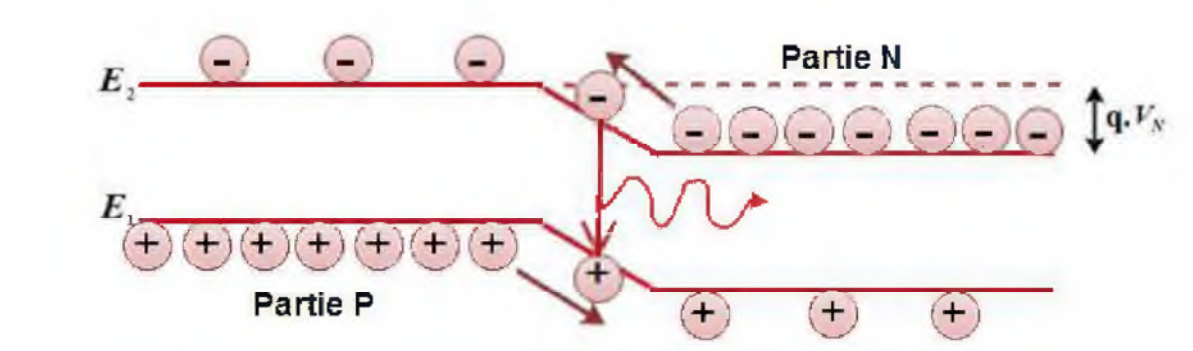


Figure I.3. La jonction P-N dans un laser

Dans le cas idéal chaque porteur minoritaire doit générer un photon. Mais ce qui se passe dans le cas réel est que seule une fraction de ces porteurs se recombine d'une manière radiative et émettent un photon. L'efficacité associée s'appelle efficacité quantique et elle représente le nombre de photon générés par chaque porteur minoritaire.
Le nombre de photons générés, noté ***P,*** est relié directement au courant d'injection ***I*** :

$$P = \eta_{ext} I \frac{h\nu}{e} \simeq \eta_{ext} I \frac{E_g}{e} \qquad \text{(I.1)}$$

II.1.1.1.1 Principe d'un laser à semi-conducteur :

L'effet photoélectrique est une première manifestation du caractère discontinu des phénomènes électromagnétiques qui se révèle dans l'interaction entre la lumière et la matière.

en 1917, EINSTEIN mit en évidence les trois processus d'interaction entre un atome dit «à deux niveaux» et un rayonnement électromagnétique Ces processus sont désignés par les termes l'absorption, l'émission spontanée et l'émission stimulée Ces différents types d'interactions se déroulent au sein d'un milieu pouvant être atomique, ionique ou moléculaire, constitué de deux niveaux d'énergie possibles E_m et$E_n(E_m < E_n)$pour les atomes constituant ce milieu comme présenté dans la (figure I.4). On pourra désigner le niveau 1 par le terme de «niveau fondamental» et le niveau 2 par celui de «niveau excité», lorsque le niveau 2 est plus peuplé d'atomes que le niveau 1, on dit qu'il y a inversion de population.

a) Absorption :

Lors du processus d'absorption, un atome situé sur le niveau inférieur $\boldsymbol{Em}$ va absorber un photon d'énergie $\boldsymbol{h\nu = En - Em}$ et monte au niveau excité grâce à la présence d'un photon de fréquence $\boldsymbol{\nu_{21}}$ et d'énergie $\boldsymbol{\Delta E}$.
Il ya disparition du photon qui transfère son énergie au milieu environnement .Ce phénomène est représenté à la figure **I.4.a**

b) Émission spontanée :

L'émission spontanée consiste à la désexcitation du milieu considéré par passage d'un atome du niveau supérieur $\boldsymbol{En}$ vers le niveau inférieur $\boldsymbol{Em}$. Le milieu va donc perdre une quantité d'énergie égale **à** $\boldsymbol{\Delta E = En - Em}$, entraînant ainsi la création d'un photon d'énergie $\boldsymbol{\Delta E}$ et de fréquence :

$$\boldsymbol{\nu_{21} = \frac{En - Em}{h}} \qquad \text{(I.2)}$$

h est la constante de Planck. Ce phénomène est illustré à la figure **I.4.b**

c) Émission stimulé :

Dans cet état, le milieu se trouve au préalable dans un état excité. Cherchant naturellement à minimiser sa quantité d'énergie, un atome du niveau 2, il va se désexciter vers le niveau 1. À la différence de l'émission spontanée, l'émission stimulée nécessite la présence d'un photon d'énergie ΔE et de fréquence ν_{21}.

Ce photon sera en effet reproduit, on obtient à l'issu deux photons parfaitement similaires en terme d'énergie, fréquence, direction de propagation. Cette création d'un second photon résulte d'un couplage entre l'onde incidente et le système atomique s'apparentant aux résonances rencontrées dans les phénomènes vibratoires Le système atomique recevant un photon en fournit un second : il agit donc en amplificateur de rayonnement. C'est ce processus de l'émission stimulée qui est à l'origine du principe du laser. L'émission stimulée est montré à la figure **I.4.c**, l'onde optique ainsi passe par une cavité optique ou résonateur.

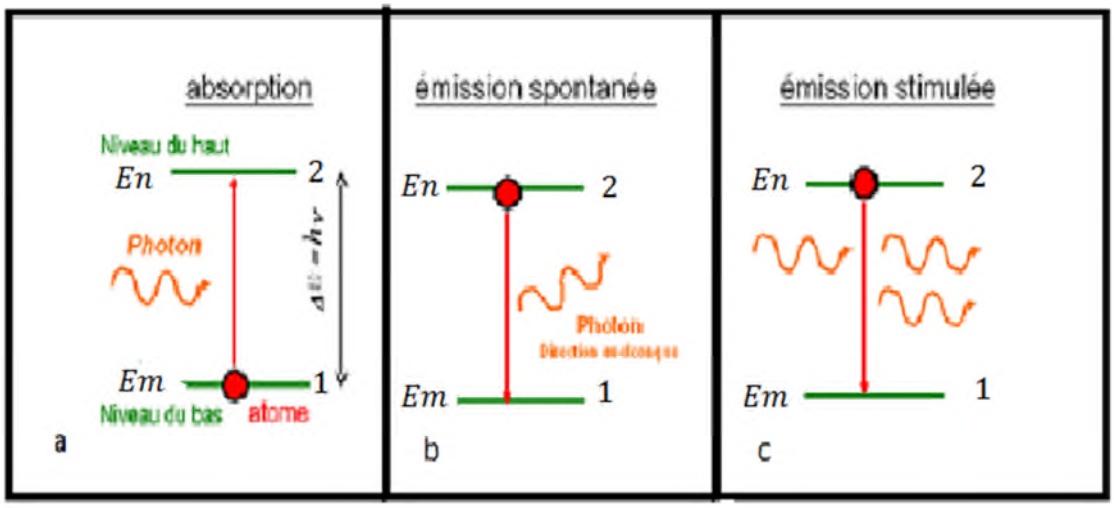


Figure I.4 Représentation schématique des transitions électroniques possibles dans un modèle à deux niveaux

II.1.1.2 Cavité résonante :

Le résonateur est constitué de deux miroirs parallèles entre lesquels est placé le milieu actif. Le premier miroir, le réflecteur, est totalement réfléchissant alors que le second, le coupleur, est semi-transparent. Il permet ainsi à la lumière de sortir de la cavité, le résonateur contribue en grande partie à l'amplification de la lumière dans le laser. Les photons en étant réfléchis par les miroirs, peuvent traverser plusieurs fois le milieu actif et provoquer l'émission stimulée d'un plus grand nombre de photons.

Lorsque le processus d'amplification se produit dans le laser, on dit qu'il oscille. On trouve deux types de cavités des cavités linéaires et des cavités en anneau.

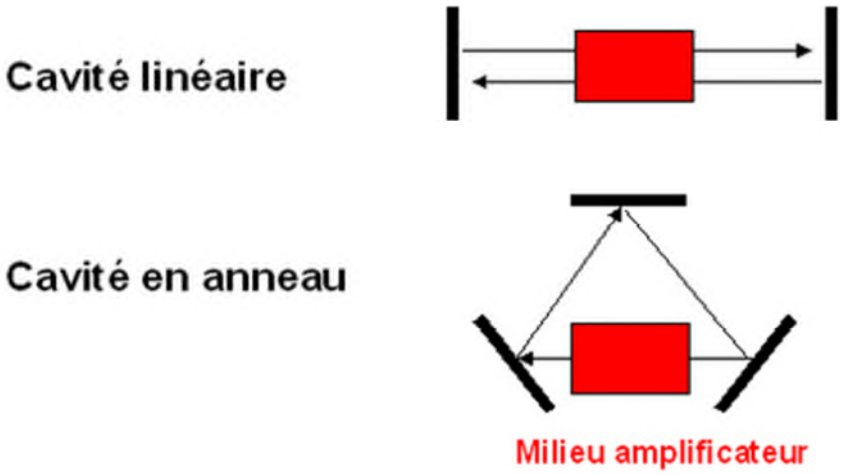


Figure I.5 Type de cavité

Nous allons décrire différents types de cavités utilisées pour réaliser des lasers :

II.1.1.3 Laser Fabry-Perot :

Le fonctionnement de la diode laser fait appel à la contre réaction optique qui permet de passer d'un comportement amplificateur en oscillateur, Ceci est obtenu en plaçant le milieu actif à l'intérieur d'une cavité optique. Cette cavité est constituée de deux miroirs partiellement réflectifs avec indice de réflexion $R1$ et $R2$ comme le montre la figure I.6 :

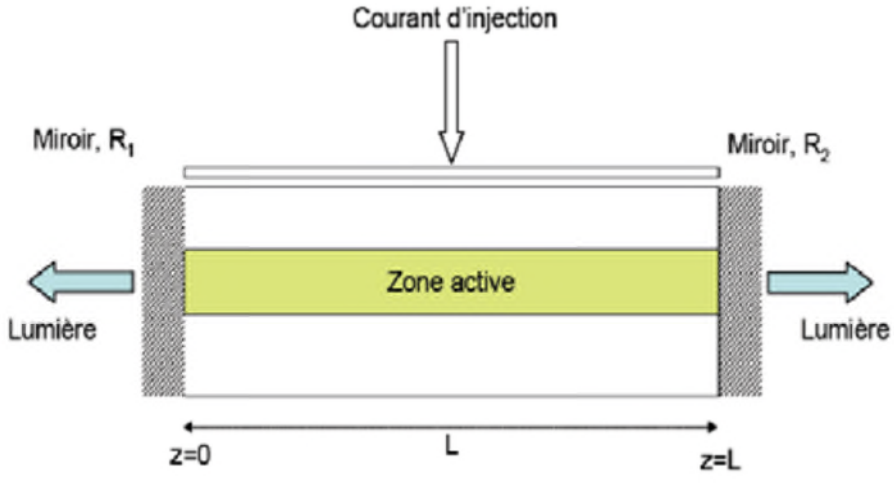


Figure I.6 Structure d'une diode laser à une cavité de résonance Fabry-Perot.

La contre-réaction positive est déterminée par les réflexions aux extrémités de la cavité. L'onde optique générée à l'intérieur de la zone active effectue autant d'allers retours à l'intérieur de la cavité que de passages dans le milieu amplificateur.
Pour que l'oscillation de l'onde optique puisse démarrer à l'intérieur de la cavité, le gain optique doit compenser au moins les pertes internes à cette dernière. Il doit en effet dépasser la valeur seuil de densité des porteurs injectés N_s correspond au courant de seuil I_s.
La puissance optique délivrée par une facette d'une diode laser est la suivant :

$$\boldsymbol{P_{pop}(I) = \eta_d \left(\frac{hv}{2.e}\right)(I - I_S)} \qquad \textbf{(I.3)}$$

η_d : représente l'efficacité quantique différentielle

h : Constante de Planck
v : Fréquence optique
e : Charge de l'électron
I : Courant injecté
Une cavité optique assure :

* le gain nécessaire pour l'émission des photons
*consiste à réaliser une sélectivité en fréquence ou en longueur d'onde.

Ce sont des ondes stationnaires crées à l'intérieur de la cavité après chaque aller et retour suivant l'axe de propagation. Ces ondes sont renforcées par l'interférence constructive après la réflexion sur les surfaces des miroirs, et les autres ondes subissent toutes entre elles des
Interférences destructives.
Dans cette cavité résonnante seulement les modes longitudinaux qui se propage les ondes optiques qui satisfont à la condition de propagation :

$$\boldsymbol{\lambda = \lambda_m = \frac{2.n.L}{M}} \qquad \textbf{(I.4)}$$

n : L'indice de la cavité,
L: Longueur de la cavité

M: Un nombre entier.

Le nombre de ces modes dépend de :
- l'énergie introduite dans le laser
- la longueur de la cavité
- la distribution spectrale du gain et des pertes
- du type de gain
- L'espacement entre deux modes longitudinaux qui donné par :

$$\boldsymbol{\delta\lambda = \lambda_{m-}\lambda_{m+1} = \frac{\lambda_m^2}{2.n_g.L}} \qquad \textbf{(I.5)}$$

n_g: Indice du groupe,

$\delta\lambda$ Varie de 0.5 à 1nm pour L variant de 200 à 400 nm

II.1.1.4 laser DFB:

La contre-réaction dans les lasers DFB (distributed feedback), lasers les plus courants, est distribuée sur toute la longueur de la cavité et donc n'est pas localisée seulement sur les côtés. Ce résultat est obtenu avec un réseau gravé tout autour de la zone active qui détermine une variation périodique de l'indice de mode. Ce type de contre-réaction se base sur le principe de la diffraction de Bragg. La sélectivité de modes pour un laser DFB est reliée à la condition de Bragg.

En effet le couplage entre les ondes qui se propagent en sens direct ou inverse se réalise seulement pour celles dont la longueur d'onde λ_B (longueur d'onde de Bragg) satisfait la condition suivant :

$$\boldsymbol{\lambda_M = \frac{2An_{eff}}{M}} \qquad \textbf{(I.6)}$$

A : est la période du miroir de Bragg

n_{eff} : L'indice effectif du guide dans la zone de réseau

M : Un entier correspondant à l'ordre de diffraction du réseau

II.1.1.5 Laser DBR :

Dans le cas de lasers DBR la contre-réaction ne se réalise pas à l'intérieur du milieu actif. En effet les extrémités d'un laser DBR se comportent comme des miroirs

dont la réflectivité est maximale pour une longueur d'onde λB qui satisfait l'équation précédente.
Les structures des lasers DFB et DBR sont montrées sur la figure I.7 suivante :

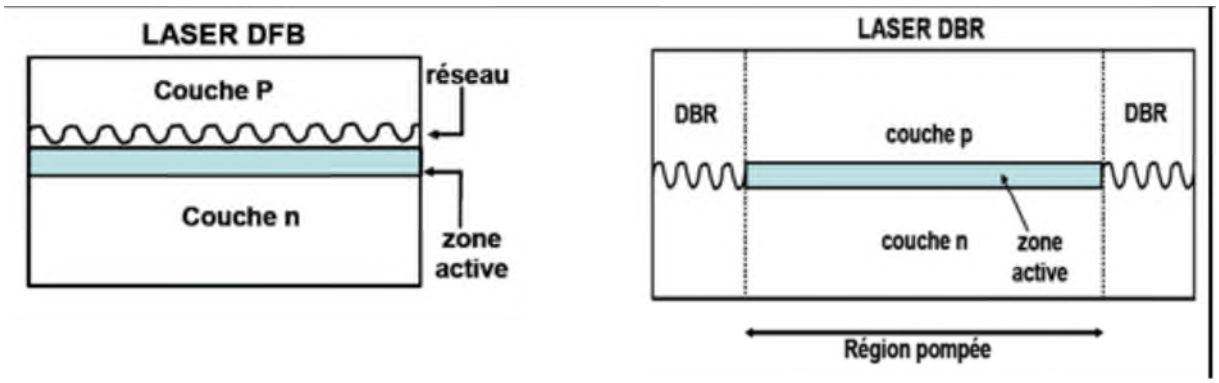
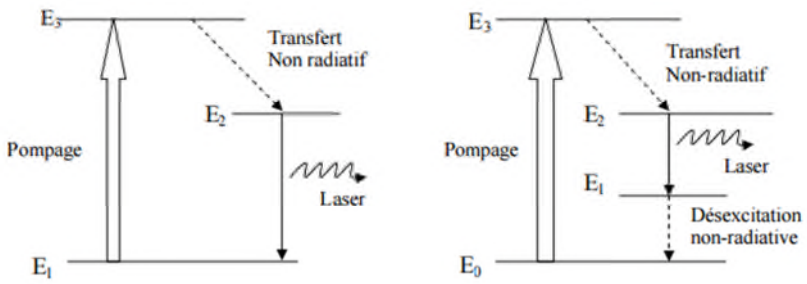


Figure I.7 Structure des lasers DFB et DBR.

II.1.2 pompage otique :

Lorsque le milieu actif d'un laser comprenait seulement deux niveaux l'état fondamental et un état excité, il serait impossible de placer la majorité des atomes dans l'état excité, la raison pour laquelle les systèmes atomiques utilisés fonctionnent sur trois niveaux, soit sur quatre niveaux, soit un transfert résonant d'énergie La figure I.8 résume ces trois principaux systèmes atomiques rencontrés dans les lasers.



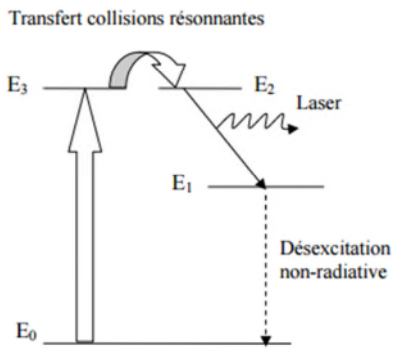


Figure I.8 Schéma général sur le processus du pompage

II.1.3 Technique de modulation :

La transmission des données numériques au sein d'un système de télécommunications optique impose d'écrire ces dernières sur un signal lumineux, c'est ce qu'on appelle une modulation.

Il existe deux méthodes pour moduler les ondes optiques des

Télécommunications : la modulation directe (ou interne) et la modulation externe.

II.1.3.1 La modulation directe :

Dans cette technique, la modulation du courant qui traverse le laser entraine directement la modulation en intensité. Le générateur émet les données à transmettre à un débit précis (<2.5 Gb/s), le laser est alimenté à un circuit de modulation de courant qui permet de moduler

La puissance du laser, la lumière modulée est couplée dans la fibre optique de transmission.

Cette modulation est satisfaisante jusqu'à 15GHz environ, mais qu'au-delà, elle n'est plus applicable. Trop de dégradations (oscillations de relaxation, chirp, bruit, ...) apparaissent et limitent les capacités de transmissions.

II.1.3.2 La modulation externe :

Ce type de modulation consiste à écrire les données électriques sur un signal optique continu. Elle est obtenue en modulant directement le faisceau lumineux en sortie du laser et non plus le courant d'alimentation à l'entrée du laser. Ainsi les défauts de la modulation directe qui incombent au laser ne seront plus présents dans le signal optique.

Le signal optique continu émis par le laser alimenté par un courant constant est pur et peu dégradé. En traversant le modulateur, il subit les modifications du facteur de transmission et le signal de sortie se trouve modulé selon **v(t)**.

Dans les systèmes de communications optiques, plusieurs types de modulateurs sont utilisés. Nous présenterons les deux types de modulateurs optiques les plus utilisés

dans les systèmes de transmission à fibre optique : le modulateur à électro-absorption et le modulateur de Mach-Zehnder.

II.1.3.2.1 Le modulateur électro-absorbant (MEA)

Le principe de fonctionnement des modulateurs à électro-absorption repose sur les modifications du spectre d'absorption d'un matériau semi-conducteur soumis à un champ électrique. Leur particularité intéressante est qu'ils peuvent être facilement intégrés avec les diodes lasers pour créer des sources optiques compactes et à très large bande de modulation.

II.1.3.2.2 Le modulateur de 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.

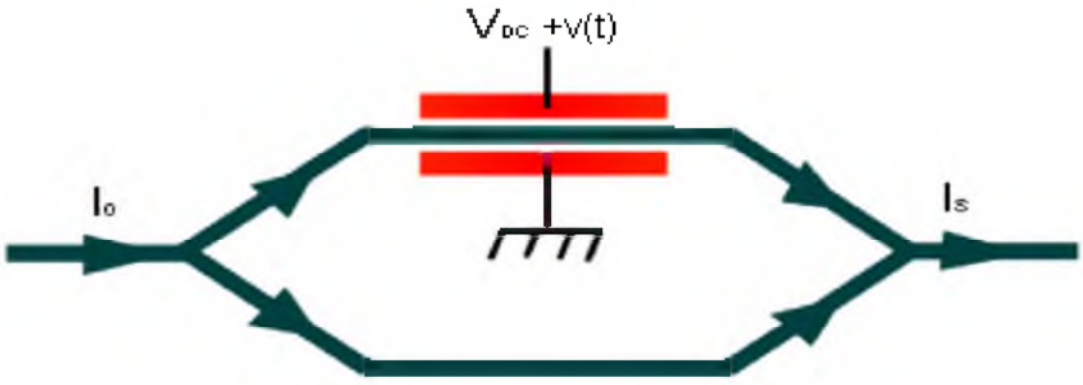


Figure I.9 Schéma simplifié d'un modulateur de Mach-Zehnder

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

$$\frac{I_{out}}{I_{int}} = cos^2(\frac{\pi V}{2V_\pi}) \qquad \textbf{(I.7)}$$

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.

II.2 Bloc de réception

Le récepteur est sensiblement le même que l'émetteur, il est constitué d'un photodétecteur qui joue le rôle de préamplificateur optique ce dernier détecte le signal à la sortie de la fibre optique.
Le signal obtenu est ensuite démodulé pour récupérer les données transmises par cette chaîne de transmissions optique.

Conclusion :

Dans ce chapitre on a présenté une chaine de transmission, on a accentué notre étude sur les lasers à semi-conducteur. Le chapitre suivant on abordera les cryptosystèmes en générale pour aboutir à une configuration d'un cryptosystème optique.

Chapitre II

Générateur De Chaos Optique

I. Introduction

Le besoin de dissimuler les informations préoccupe l'homme depuis le début de la civilisation. La confidentialité apparait notamment nécessaire lors des luttes pour l'accès au pouvoir. Puis elle se développe énormément à des fins militaires et diplomatiques. Aujourd'hui, de plus en plus d'applications dites civiles nécessitent la sécurité des données transitant entre deux interlocuteurs ou plusieurs, via un canal de transmission d'informations comme les réseaux de télécommunications actuels.

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 :

- la cryptographie quantique
- la cryptographie par chaos.

Dans notre travail on détaille uniquement la technique de cryptographie par Chaos

II. Système dynamique et chaos

II.1 Le chaos

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. Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physiques que biologique, chimique ou économique.

Le terme chaos définit un état particulier d'un système dont le comportement ne se répète jamais qui est très sensible aux conditions initiales.

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

L'exemple suivant illustre les propriétés d'un système dynamique chaotique. Soit le modèle chaotique donné par Otto de Rossler.

$$\begin{cases} X'_1 = -x_2 - x_3 \\ X'_2 = -x_1 + ax_2 + 0.01x_1 \ln(x_3) \\ X'_3 = -c + x_3 (x_1 - b) \end{cases} \quad \text{(II.1)}$$

Ou (x_1, x_2, x_3) est le vecteur d'état et a, b, c sont les paramètres du système. Le système de Rossler montre un comportement chaotique pour a = 0.2, b = 5.7, c = 0.2. Avec les conditions initiales x_1 (0) = 0.01, x_2 (0) = 0.01 et x_3 (0) =0.01

Les définitions et propriété suivantes permettent de comprendre qualitativement les points marquants des systèmes chaotiques.

a) La non-linéarité

Un système chaotique est un système dynamique non linéaire. 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) L'aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires. La figure suivante illustre l'aspect aléatoire du système de Rossler.

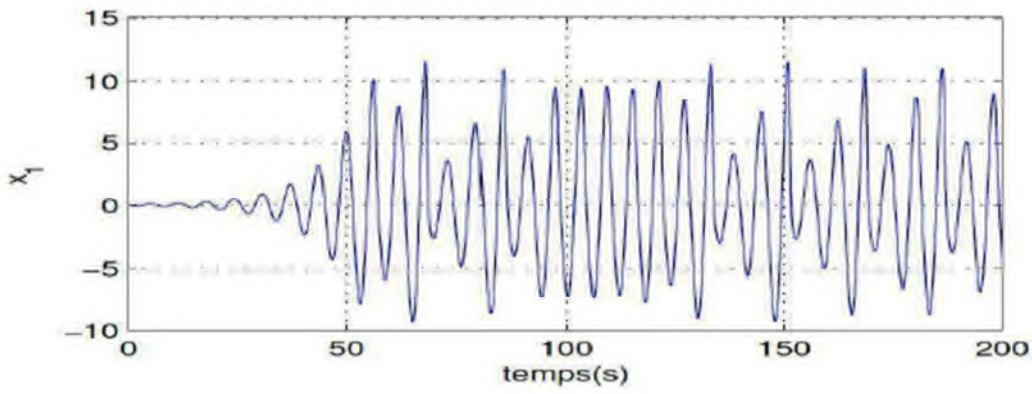


Figure II.1. État chaotique x1 du système de Rossler

d) 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. Comme la plupart des phénomènes sont non linéaire

On comprend alors l'importance de la découverte de Lorenz 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.

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.

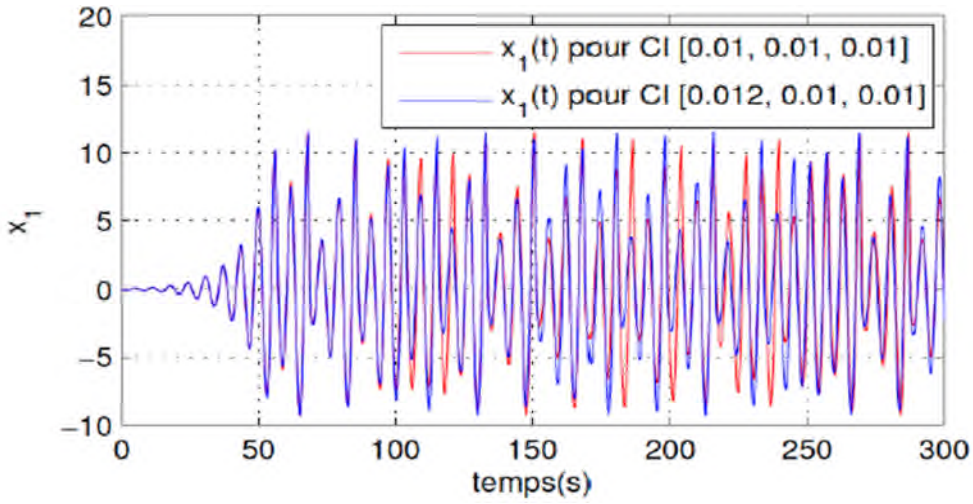


Figure II.2. Illustration de la propriété de sensibilité aux conditions initiales sur l'état x_1

II.2. Détermination du chaos :

Les signaux produits par ces systèmes dynamiques non linéaires conviennent à plusieurs types d'application grâce à leurs caractéristiques particulières. Par exemple, les séquences chaotiques sont intéressantes pour l'analyse du signal, la synthèse de signaux et pour les communications numériques et analogiques. Parmi les propriétés

des signaux chaotiques qui les rendent si intéressants, on peut citer leur génération facile et une faible probabilité de détection. Par conséquent, il n'est pas surprenant qu'ils aient été utilisés depuis longtemps dans les communications sécurisées et la cryptographie.
L'intérêt d'utiliser des signaux chaotiques dans ces systèmes réside dans trois propriétés fondamentales des signaux et systèmes chaotiques :

- un signal chaotique est obtenu à partir d'un processus purement déterministe; il est donc possible de le reconstituer en se plaçant dans les mêmes conditions que celles qui ont contribué à le créer ;

- un système chaotique engendre un signal à large spectre et peut donc permettre de transmettre des signaux très variés.

- Deux trajectoires de signaux chaotiques issues d'un même système chaotique, mais obtenues à partir de conditions initiales différentes, ont une inter-corrélation très faible.

II.3. Caractéristiques d'un système chaotique :

II.3.1 L'espace de phase :

Il est possible de suivre l'évolution de l'état d'un système physique dans le temps. En construisant l'espace des phases, cet espace est une notion purement mathématique qui comporte autant de dimensions qu'il y a de paramètres dans le système dynamique étudié. Ainsi on pourrait très bien imaginer se retrouver à manipuler un espace de phases à *216* dimensions si le système dynamique analysé implique *216* paramètres (toute difficulté géométrique mise à part...). En considérant un espace des phases à *3* dimensions, on ne peut tracer qu'un graphique.

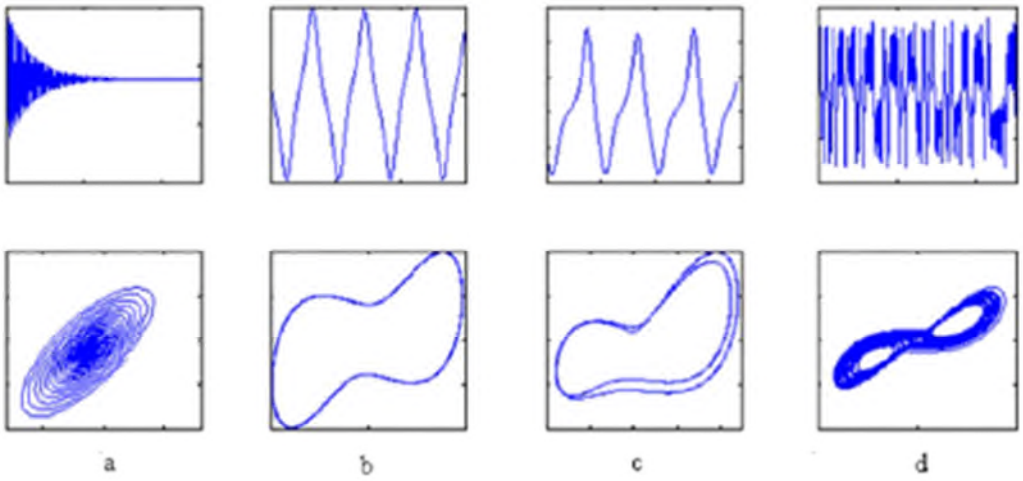


Figure II.3. Séries temporelles en haut et espaces de phase correspondant

II.3.2. Attracteurs :

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évoluent un système, quelles que soient ses conditions initiales.

Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques. Les attracteurs étranges semblent inclure à la fois des lois déterministes et des lois aléatoires, ce qui rend impossible toute prévision à long terme

3- Attracteurs régulier :

Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de deux sortes :

* ***Un point fixe :*** ou état stationnaire, du système. Ce sont les valeurs de la variable pour les quelles elle n'évolue plus avec le temps. Un élément x de E est un point fixe de f si $f(x) = x$.

Un cycle limite: Ce sont les valeurs de la variable pour lesquelles la trajectoire de phase se referme sur elle-même. L'évolution temporelle est alors cyclique.

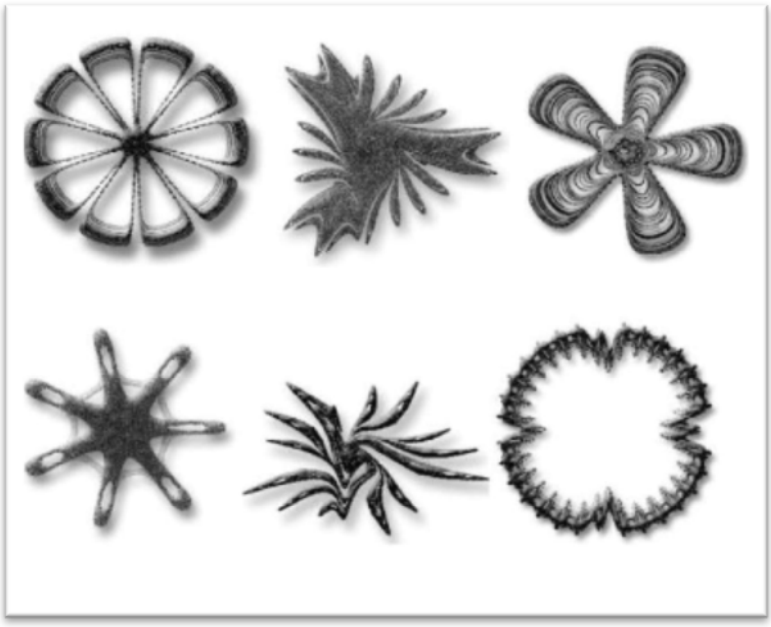
Pour tous les attracteurs réguliers, c'est à dire pour tous les systèmes non-chaotiques, des trajectoires qui partent de "points" proches l'un de l'autre dans l'espace de phase restent indéfiniment voisines. On sait donc prévoir l'évolution de ces systèmes, à partir d'une situation connue

4- **Attracteurs étranges :**

Ils sont caractéristiques de l'évolution des systèmes chaotiques c'est-à-dire qu'au bout d'un certain temps, tous les points de l'espace des phases donnent des trajectoires qui tendent à former l'attracteur étrange.

Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver à deux extrémités opposées de l'attracteur (conditions finales). Cela traduit le comportement divergent des phénomènes chaotiques

On obtient ainsi des attracteurs différents (en fonction des systèmes étudiés), qui présentent des formes diverses et surprenantes



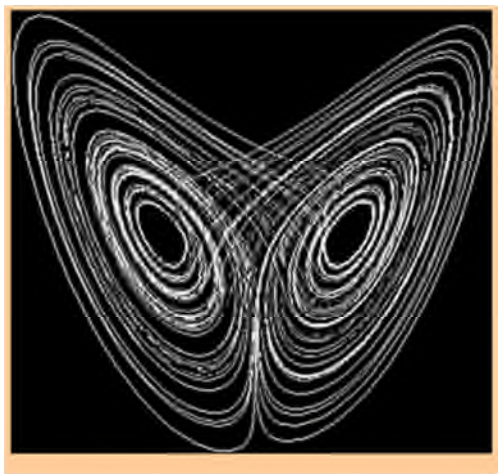


Figure II.4. Attracteurs étranges

II.3.3 Les exposants de Lyapunov :

Certains systèmes dynamiques sont très sensibles aux variations de leurs conditions initiales, ces variations peuvent rapidement prendre d'énormes proportions. Le mathématicien russe Alexander Markus-Lyapunov (1857-1918) s'est penché sur ce phénomène et a développé une quantité permettant de mesurer la vitesse à laquelle ces petites variations peuvent s'amplifier, cette quantité appelée « exposant de Lyapunov » mesure en fait le degré de sensibilité d'un système dynamique, autrement dit, le taux de divergence entre l'évolution de trajectoires issues de conditions initiales proches.

II.3.4 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

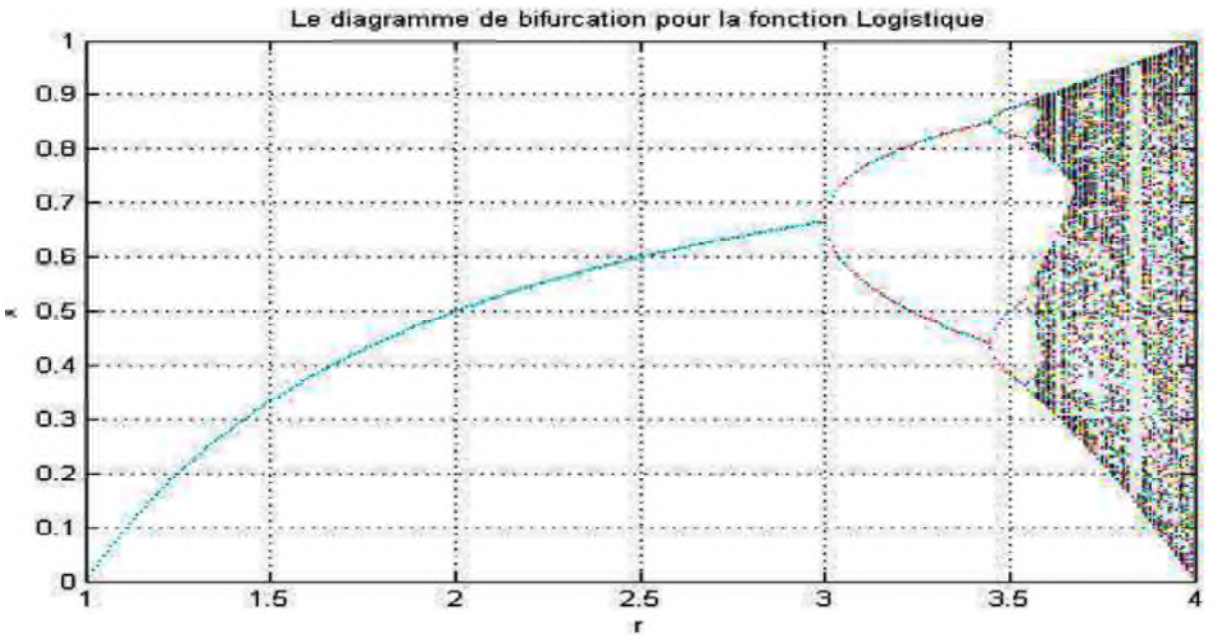


Figure II.5. Diagramme de bifurcation de la fonction logistique

Dans les équations de Lorenz par exemple, la résolution du système n'apporte pas toujours le chaos. Ce régime n'apparaît que pour certaines valeurs des paramètres. Pour caractériser le chaos.

Il peut être intéressant d'étudier l'apparition du chaos (ce qu'on appelle le scénario ou la route vers le chaos).

On distingue trois scénarios théoriques d'évolution vers le chaos. Toutes ces évolutions sont permises de classer certains phénomènes expérimentaux comme chaotiques déterministes.

III. Système de cryptographie par le chaos :

Le schéma principal de la communication sécurisée par le chaos est montré sur la figure II.6. 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 qui a permis de crypter l'information à l'émetteur est utilisée pour décryptée à la réception les conditions initiales permettent de synchroniser les deux générateurs

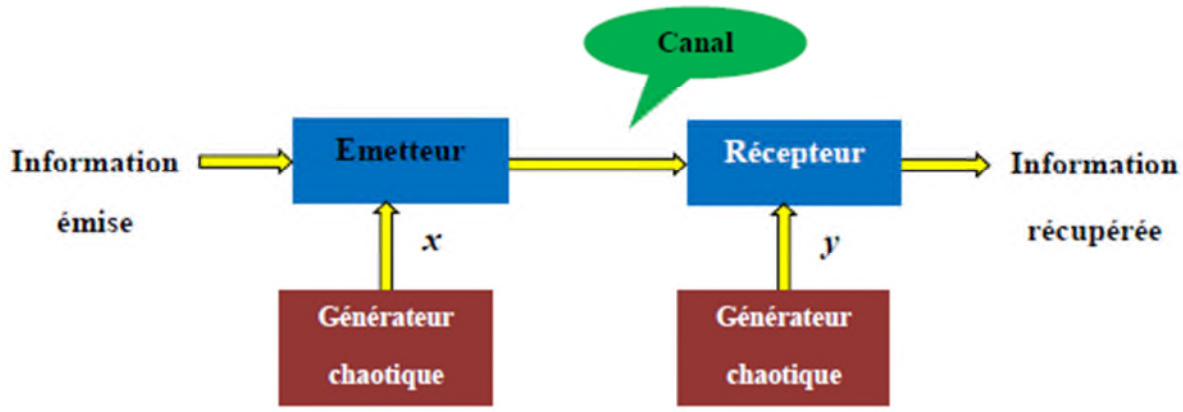


Figure II.6. Principe de la communication sécurisée à base du chaos

Dans le cas analogique, le principe de cryptage consiste à générer une porteuse chaotique dont l'étalement spectral couvre la totalité de celui de l'information analogique. Dans le cas du numérique, la largeur spectrale du chaos est liée au débit binaire, dont le spectre doit également pouvoir être masque par la porteuse chaotique. En termes de qualité de la liaison cryptée, une transmission analogique mettra en avant le rapport signal sur bruit du décodage par synchronisation entre chaos. Une transmission numérique se réfère quant à elle à la valeur du BER6 après synchronisation et suppression de la porteuse chaotique par le récepteur. Pour avoir une image concrète sur la qualité du décodage d'une information numérique, nous tracerons un diagramme de l'œil.

IV. Principe de la cryptographie par chaos

IV.1. Masquage additif :

Ce principe consiste à effectuer une simple addition entre l'information à transmettre m_k et le signal de sortie x_k du générateur de chaos

Le générateur de chaos du coté émetteur et récepteur ont pour représentation d'état

$$\begin{cases} X_{k+1} = f(x_k) \\ y_k = h(x_k) + m_k \end{cases} \qquad \text{(II.2)}$$

$$\begin{cases} \end{cases}$$

$\hat{x}_{k+1}$= f($\hat{x}_k$) (II.3)

$\hat{y}_k$ = h($\hat{x}_k$)

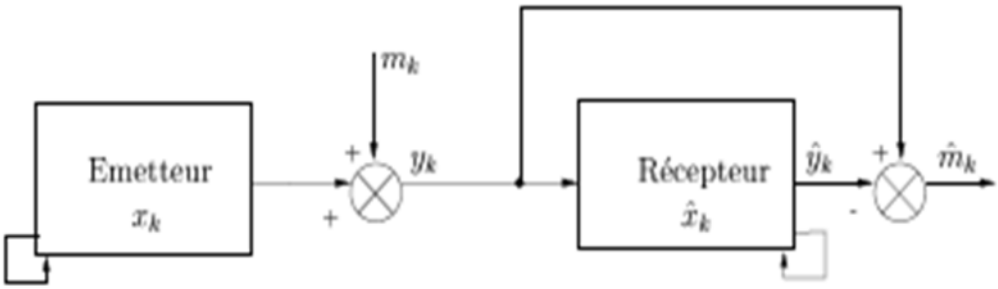


Figure II.7 Principe du chiffrement chaotique par addition

La reconstruction de l'information nécessite la synchronisation de l'émetteur et du récepteur l'information et alors récupérer on soustrayant la sortie du récepteur avec celle de l'émetteur

IV.2 Chiffrement par commutation :

Méthode (en anglais Chaos Shift Keying, CSK) est utilisée pour transmettre un message binaire. 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).

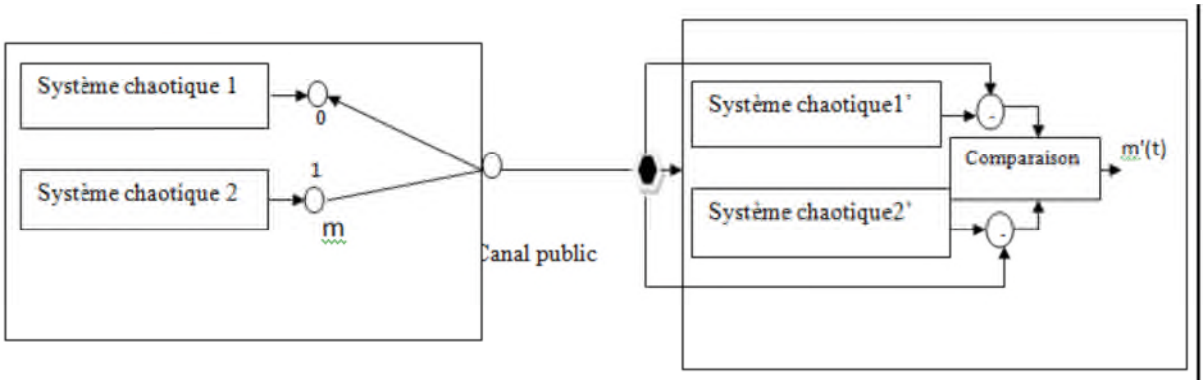


Figure II.8. Principe du chiffrement chaotique par commutation

IV.3 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 par la figure II.9.
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.

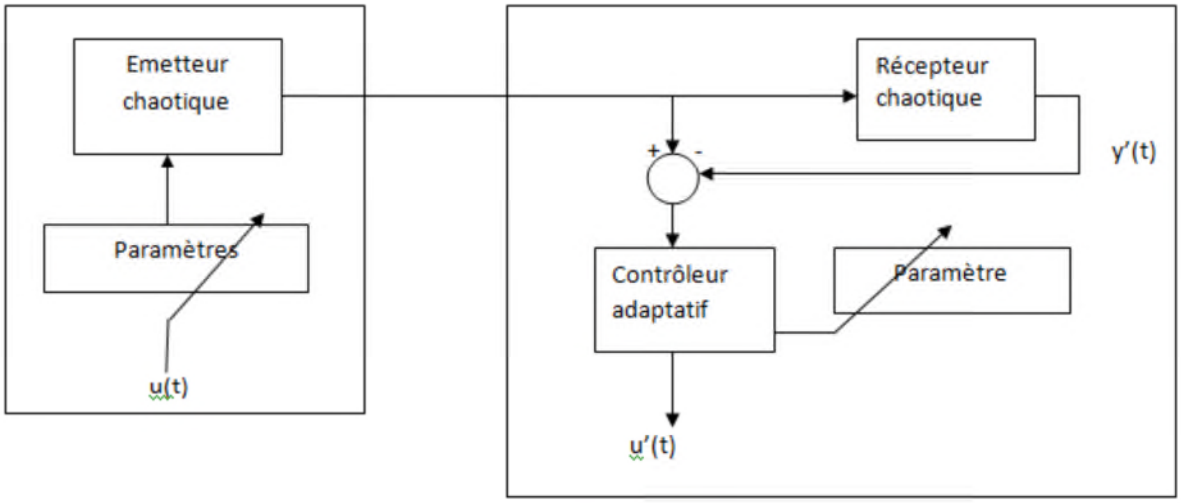


Figure II.9. Principe du chiffrement chaotique par modulation

V. Communication optique et chaos :

Les technologies optoélectroniques ont fortement contribué au développement des télécommunications optiques modernes (par exemple, sources laser, amplificateurs performants et compacts, et fibres optique). L'essentiel des efforts de protection des systèmes de communication s'est attaché l'utilisation et à l'amélioration constante de techniques de cryptographie mathématique. Il est à présent possible d'utiliser directement les propriétés physiques du signal porteur d'information afin d'apporter un niveau de confidentialité supplémentaire. Deux solutions ont été largement étudiées :

• **Les Communications Quantiques** utilisant la nature probabiliste des photons (assurée par la mécanique quantique) afin de transmettre des informations sensibles

tout en garantissant une sécurité inconditionnelle (au sens de la théorie de l'information)

• **Les Communications Chaotiques** utilisant les instabilités existant dans certaines sources optiques afin de générer des signaux pseudo-aléatoires de forte complexité dans lesquels des informations seront cachées. Cette approche garantit une sécurité algorithmique similaire à celle produite par certaines méthodes mathématiques (RSA et PGP par exemple)

Les systèmes optiques chaotiques, ont de larges bandes passantes, permettant l'échange de données à haut-débit (plusieurs Gbit/s) sur de larges distances. Une architecture de communication par chaos optique comprend deux oscillateurs chaotiques structurellement identiques (paramètres et non-linéarité), et situés à chacune des extrémités d'un canal de communication optique. En début de chaîne, le message est incorporé au moyen d'une méthode appropriée au signal chaotique avant d'injecter le résultat du chiffrement dans le canal de transmission. En fin de chaîne, le récepteur se synchronise uniquement sur le chaos produit par l'émetteur (la partie déterministe du signal) et une opération de soustraction est ensuite utilisée pour extraire les données

Plusieurs architectures à base d'oscillateur électro-optique (OEO) à boucles de rétroactions retardées sont possibles. Elles sont représentées en Figure II.10. On distingue deux classes, l'une utilisant un seul photodétecteur (Configuration 1) et l'autre en utilisant plusieurs (Configurations 2a et 2b).

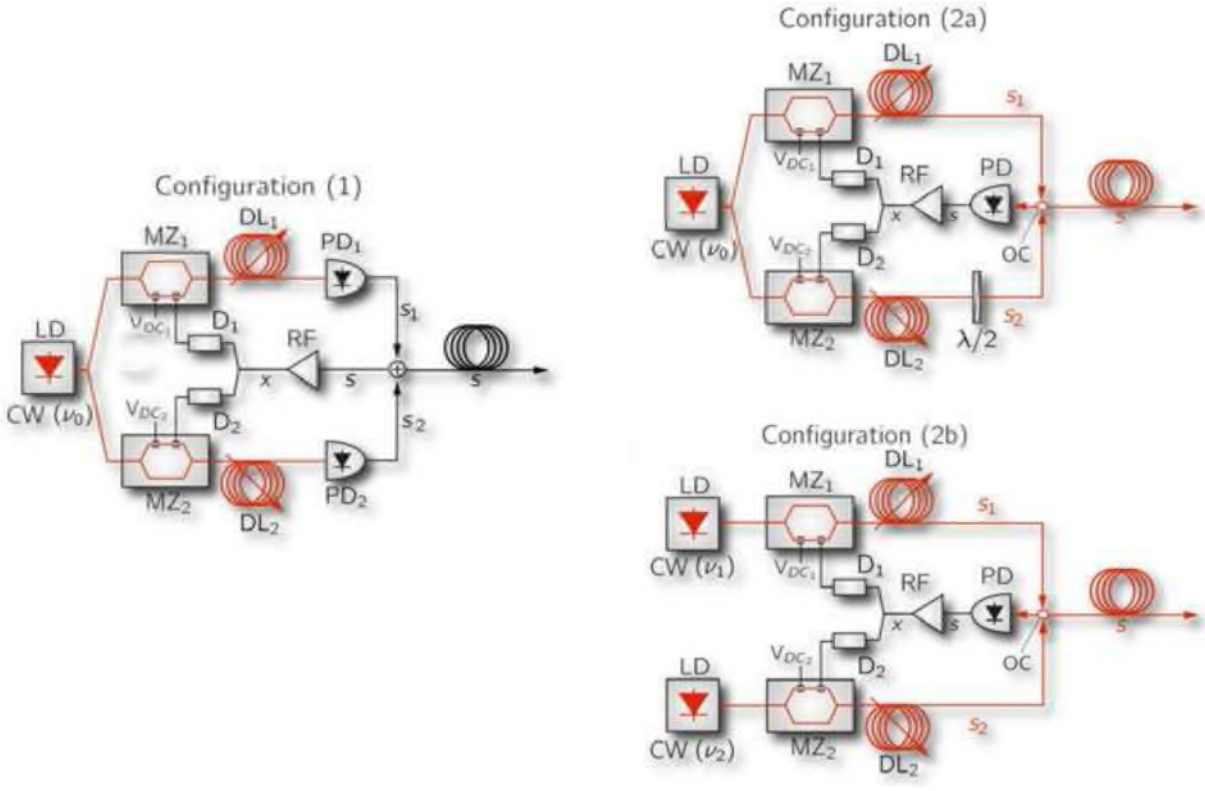


Figure II.10. Oscillateur électro-Optique : Emission Laser chaotique

La Configuration (1) possède deux photodétecteurs alors que les Configurations (2a)-(2b) n'en ont qu'un. LD : diode laser, MZj=1,2 : modulateur de Mach-Zehnder, DLj=1,2 : ligne à retard optique, PDj=1,2 : photodétecteur, RF : filtre RF passe-bande, Dj=1,2 : diviseur de tension associé au facteur d'atténuation gj=1,2 < 1.

Dans la Configuration 1, l'émetteur est composé d'une source laser CW monochromatique (LD) d'une puissance optique P qui est divisée dans plusieurs bras optiques. Dans chacun d'eux, la lumière est modulée en amplitude par un modulateur de Mach Zehnder (MZi) polarisé par la tension constante

Ceci nous permettra par la suite de générer des signaux chaotiques sous forme de séquences chaotiques orthogonale et de transmettre de façon sécurisée plusieurs messages simultanément tout en garantissant un décryptage de complexité linéaire. En adoptant une philosophie identique à celle utilisée dans les méthodes de multiplexage par code (code-division multiple access ou CDMA), les signaux chaotiques générés par des modulateurs de Mach Zehnder (présents dans chaque boucle) sont utilisés comme séquences d'étalement orthogonales (ou codes). Bien que la notion d'orthogonalité parfaite (ou décorrelation totale) entre chaque code ne soit pas nécessaire dans les approches de type CDMA, elle demeure une propriété essentielle à la simplicité algorithmique du décryptage. La transposition du CDMA en utilisant des signaux chaotiques est ambitieuse. Au niveau du récepteur, la synchronisation du chaos est utilisée pour reproduire les codes chaotiques afin de pouvoir réaliser une détection par corrélation.

Il est possible de déterminer un modèle mathématique pour la Configuration de la figure. II.10 :

$$\tau\dot{x}(t) + x(t) + \frac{1}{\theta}\int_{t_0}^{t} x(u)du = \sum_{i-1}^{n} \beta_i \cos^2(\omega_i x(t - T_i) + \phi o_i) \qquad (II.4)$$

Avec :

$x(t) = \pi g_1 V(t)/2V_{\pi_{rf_1}}$: la variable d'état du système

$xT_{i=}\, x(t - T_i)$: La variable d'état retardée

$\theta = (2\pi f_L)^{-1}$, $\tau = (2\pi f_H)^{-1}$, $\beta_i = g_1 GSP_{i\pi}/2V_{\pi_{rf_1}}$: Le gain non linéaire

$\phi o_i = \pi\, V_{dc1}/2V_{\pi dc1}$: Un offset de phase

$\omega_i = g_i/g_1 V_{\pi_{rf_1}}/2V_{\pi_{rf_1}}$: Un gain interne modifiant la fréquence de la non-linéarité de la boucle de rétroaction.

Une liaison optique dépendent des performances, des dispositifs utilisés pour les conversions électrique/optique, et optique électrique et de la technique de modulation optique choisie et des amplificateurs utilisés, la qualité et nature de la fibre optique et finalement, de la topologie choisie pour réaliser le système entier

Conclusion

Dans ce chapitre on a présenté tout d'abord les systèmes dynamiques non linéaire qui sous certaines conditions pouvaient produire du chaos, qui va être utilisé pour chiffrer l'information à transmettre, avant de terminer par la présentation d'un générateur de chaos optique utilisant une rétroaction. Ce modèle sera réalisé sous Optisystem dans une chaîne de transmission dans le chapitre simulation.

Chapitre III

Simulation et Résultat

I. Introduction :

Ce chapitre est dédié à la réalisation d'un système de transmission basé sur le chaos optique. L'architecture proposée est issue d'un générateur de chaos en intensité. Dans notre cas, on utilise une structure à base d'OEO avec boucles de rétroaction retardées sous Optisystem.

Le logiciel Optisystem permet de simuler et d'analyser des systèmes de transmission optique. La diversité des systèmes simulés peut être étendue par la possibilité d'insérer des fonctions réalisées par l'utilisateur sous Matlab et qui peuvent être insérées aux systèmes simulés

II. Conception d'une chaîne de transmission optique :

Cette première chaîne figure III.1 nous permet de nous familiariser avec le logiciel Optisystem, ainsi on peut voir la longueur d'onde émise par la diode laser figure III.1 donnée par l'analyseur de spectre optique

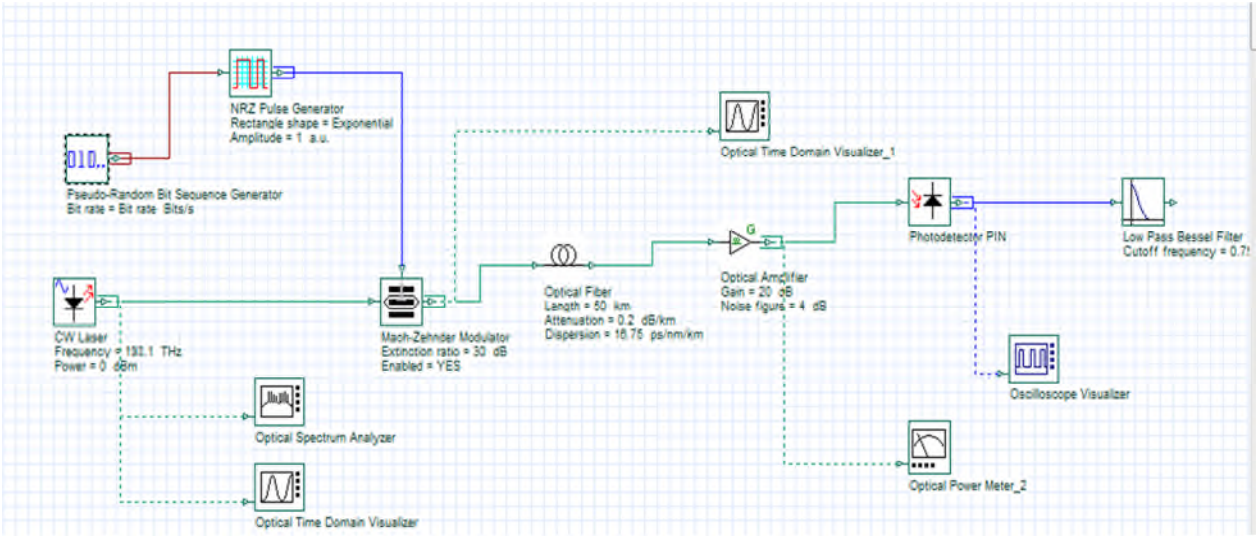


Figure III.1 une chaine de transmission d'une liaison optique

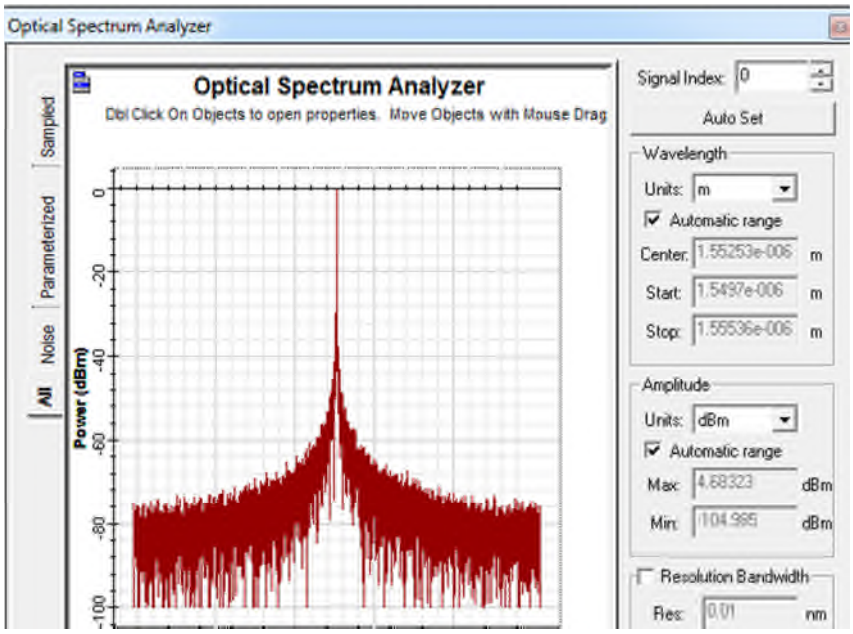


Figure III.2 longueur d'onde

La figure III.3 nous donne la sortie du modulateur Mach Zehnder ou le signal laser est modulé par la sortie d'un générateur NRZ

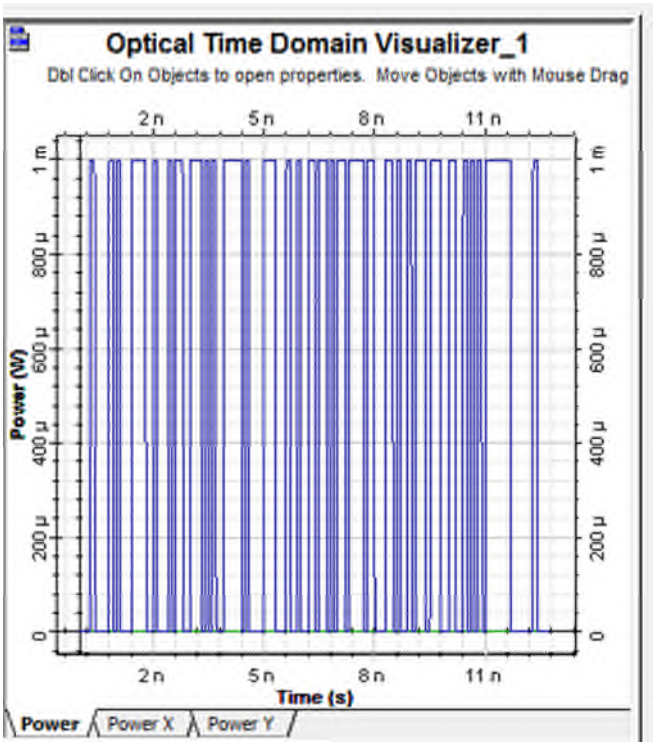


Figure III.3 Signal optique modulé par un code NRZ

II.1 Bifurcations :

Sont les changements qualitatifs dans la dynamique du système**.** Les valeurs des paramètres à laquelle ils se produisent sont appelés **points de bifurcation.**
Dans notre exemple, on considère une suite logistique:

$$x_{n+1} = rx_n(1 - x_n) \qquad \text{(III.1)}$$

Pour les valeurs de paramètre r juste en dessous de 3,0 orbites convergent vers un point fixe stable. Lorsque la valeur de r dépasse 3 le point fixe devient instable, et les orbites convergent vers une multiplication de point d'équilibre période de 2 orbite, qui est créé à $r = 3{,}0$. Par conséquent, nous disons que $r = 3.0$ est Le *point* où la suite logistique *a des bifurcations.*

II.1.1 Construction d'un diagramme de bifurcation :

Afin d'étudier les bifurcations des systèmes dynamiques, il est commode de visualiser les bifurcations qui se produisent à différentes valeurs de paramètres r.

le programme qui nous donne le diagramme de bifurcation pour la suite logistique avec le paramètre r dans la gamme de $2{,}5$ à 4 est construit programme dans un sous Matlab

Programme :

```
Npre = 200; Nplot = 100;
x = zeros(Nplot,1);
for r = 2.5:0.005:4.0,
   x(1) = 0.5;
   for n = 1:Npre,
      x(1) = r*x(1)*(1 - x(1));
   end,
   for n = 1:Nplot-1,
      x(n+1) = r*x(n)*(1 - x(n));
   end,
   plot(r*ones(Nplot,1), x, '.', 'markersize', 2);
   hold on;
end,
title('Bifurcation diagram of the logistic map');
xlabel('r');  ylabel('x_n');
set(gca, 'xlim', [2.5 4.0]);
hold off;
```

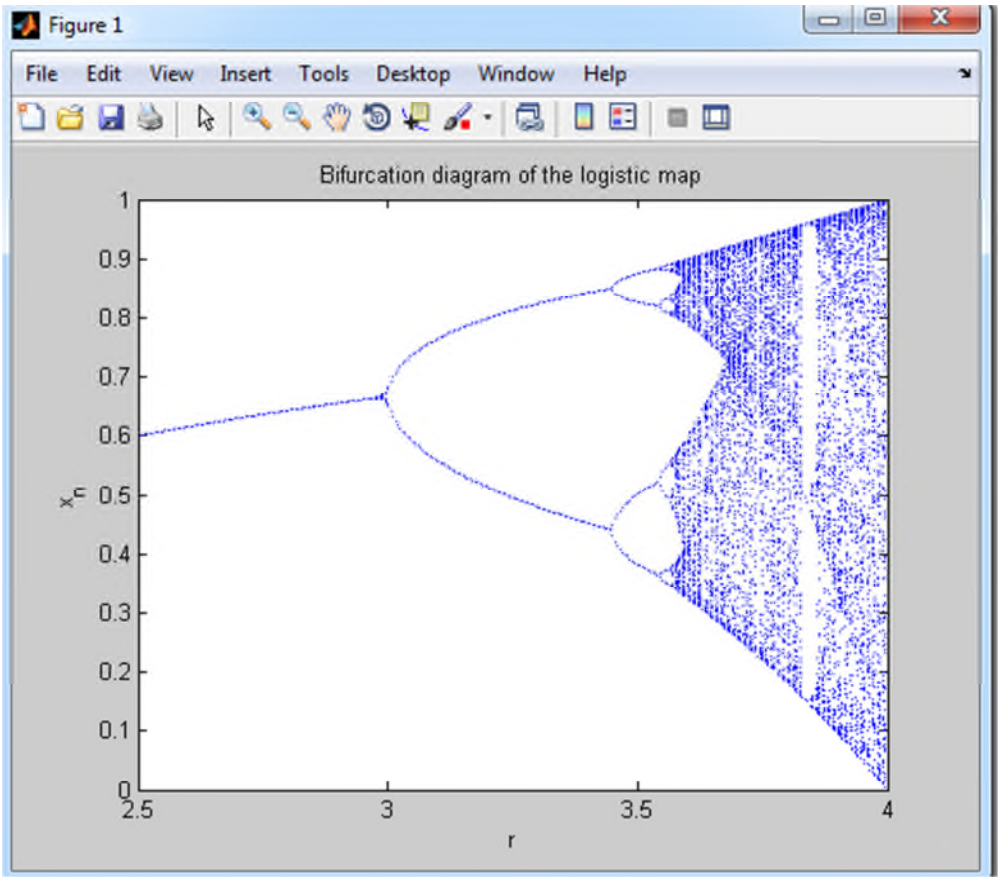


Figure III.4 le diagramme de biffurcation

II.2 Attracteur

Pour l'attracteur étrange de Lorenz est aussi construit sous Matlab il permet de tracer l'attracteur dans l'espace X, Y, Z

```
% plot final MF's on x, y, z, u
for input_index=1:4,
    subplot(2,2,input_index)
    [x,y]=plotmf(trn_fismat,'input',input_index);
    plot(x,y)
    axis([-inf inf 0 1.2]);
    xlabel(['Input ' int2str(input_index)],'fontsize',10);
end
% error curves plot
close all;
epoch_n = 10;
plot([trn_error chk_error]);
hold on; plot([trn_error chk_error], 'o'); hold off;
xlabel('Epochs','fontsize',10);
ylabel('RMSE (Root Mean Squared Error)','fontsize',10);
title('Error Curves','fontsize',10);
input = [trn_data(:, 1:4); chk_data(:, 1:4)];
anfis_output = evalfis(input, trn_fismat);
index = 125:1124;
plot(time(index), [x_t(index) anfis_output]);
xlabel('Time (sec)','fontsize',10);
diff = x_t(index)-anfis_output;
plot(time(index), diff);
xlabel('Time (sec)','fontsize',10);
title('ANFIS Prediction Errors','fontsize',10);
```

```
load mgdata.dat
a = mgdata;
time = a(:, 1);
x_t = a(:, 2);
plot(time, x_t);
xlabel('Time (sec)','fontsize',10); ylabel('x(t)','fontsize',10);
title('Mackey-Glass Chaotic Time Series','fontsize',10);
trn_data = zeros(500, 5);
chk_data = zeros(500, 5);

% prepare training data
trn_data(:, 1) = x_t(101:600);
trn_data(:, 2) = x_t(107:606);
trn_data(:, 3) = x_t(113:612);
trn_data(:, 4) = x_t(119:618);
trn_data(:, 5) = x_t(125:624);

% prepare checking data
chk_data(:, 1) = x_t(601:1100);
chk_data(:, 2) = x_t(607:1106);
chk_data(:, 3) = x_t(613:1112);
chk_data(:, 4) = x_t(619:1118);
chk_data(:, 5) = x_t(625:1124);

index = 119:1118; % ts starts with t = 0
plot(time(index), x_t(index));

xlabel('Time (sec)','fontsize',10); ylabel('x(t)','fontsize',10);
title('Mackey-Glass Chaotic Time Series','fontsize',10);
fismat = genfis1(trn_data);


% The initial MFs for training are shown in the plots.
for input_index=1:4,
    subplot(2,2,input_index)
    [x,y]=plotmf(fismat,'input',input_index);
    plot(x,y)
    axis([-inf inf 0 1.2]);
    xlabel(['Input ' int2str(input_index)],'fontsize',10);
end
% load training results
load mganfis
```

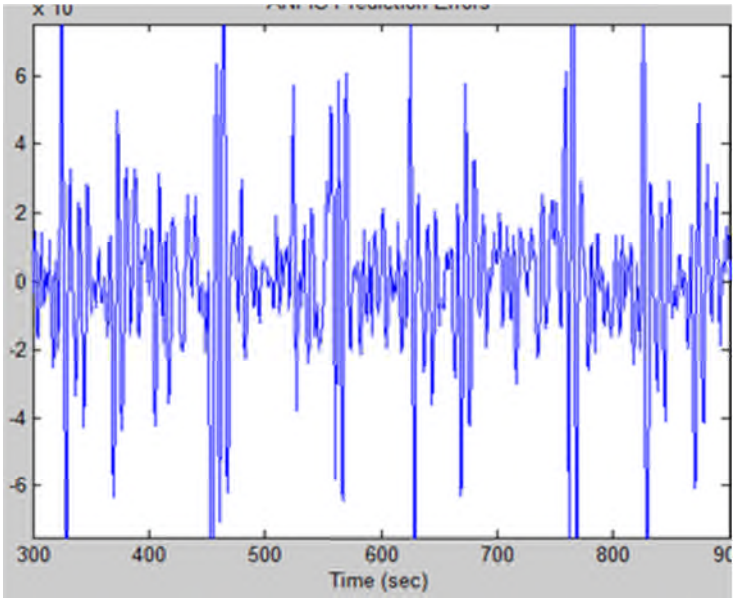


Figure III.5 : le mouvement des lobes sinus et cosinus

La figure suivant montre un mouvement des lobes sinus et cosinus qui se superposent et se succèdent anarchiquement comme si la période changeait sans arrêt.

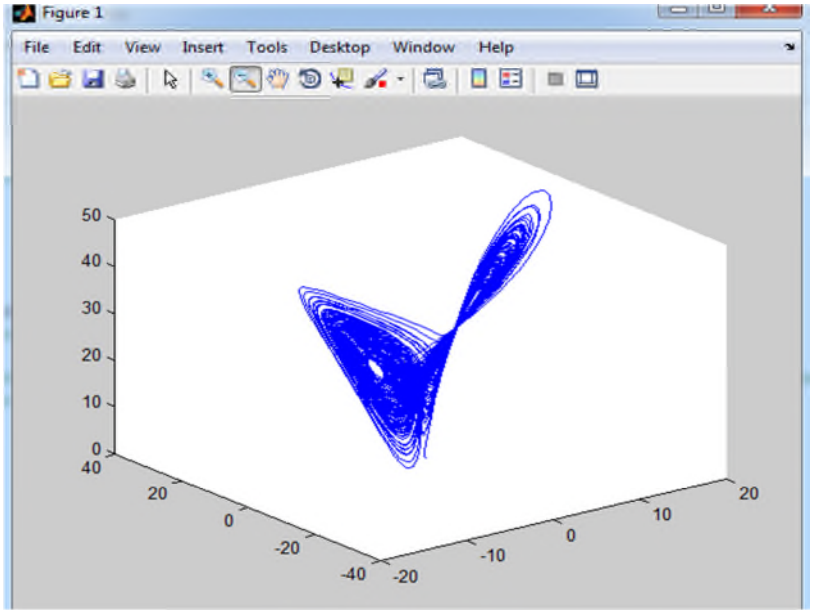


Figure III.6 : Attracteur de Lorenz

II.3 Conception du générateur chaotique optique :

La Configuration réalisée est composé d'une source laser CW monochromatique (LD) d'une puissance optique P qui est divisée dans deux bras optiques. Dans chacun d'eux, la lumière est modulée en amplitude par un modulateur de MachZehnder (MZi) polarisé par une tension constante, puis une contre réaction est effectuée. A la sortie on obtient une onde chaotique

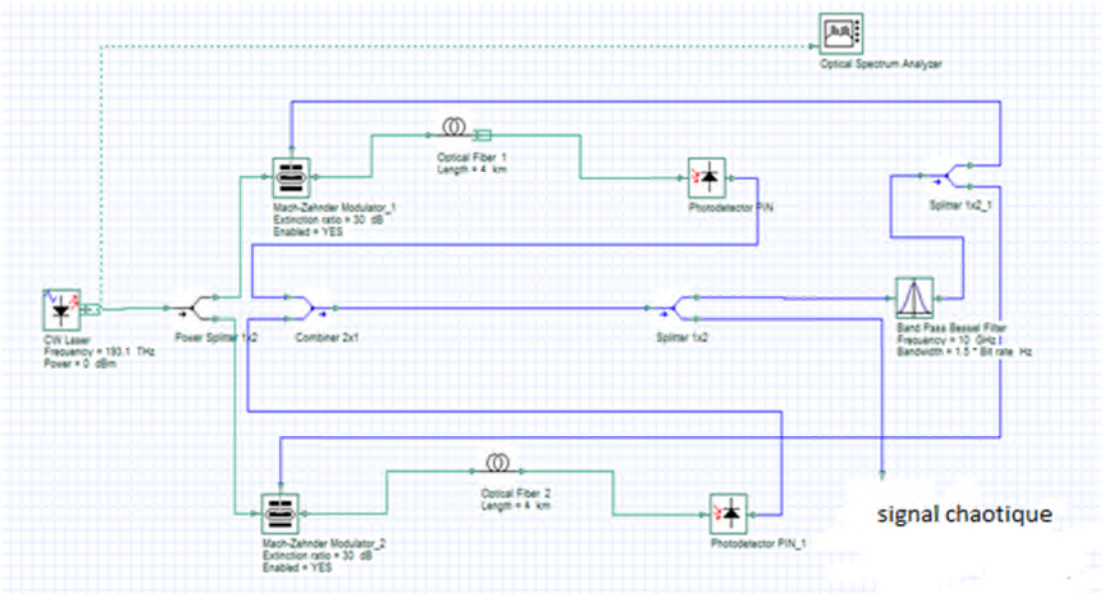


Figure III.6 réalisation d'un générateur chaotique à base de rétroaction

- **Le signal en sortie**

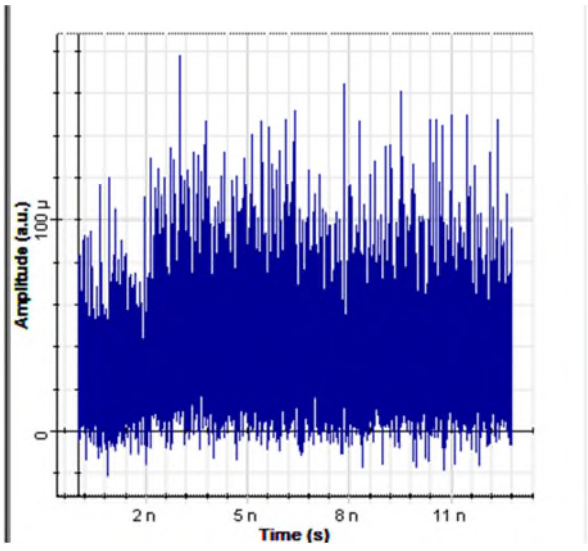


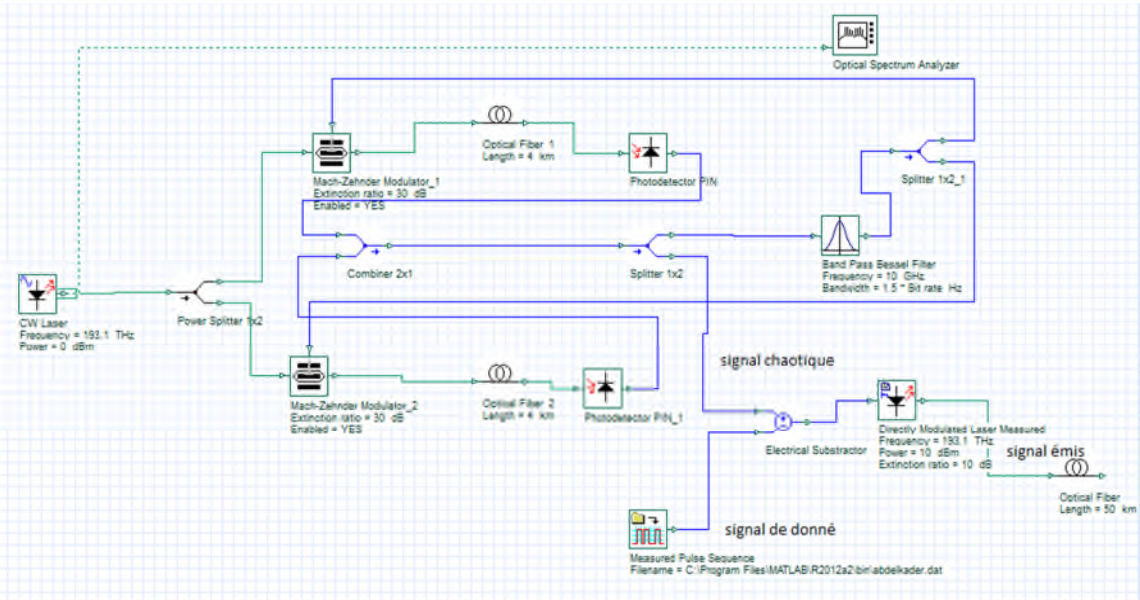
Figure III.7 représentation du signal de sortie chaotique

II.4 Modélisation du système de transmission sécurisée par chaos optique :

Dans cette chaîne on retrouve le générateur de la figure 6 qui va être utilisé deux fois du coté émetteur et en réception (donc pour le chiffrement puis le déchiffrement).

Dans ce qui suit, nous présentons les composantes du module émission de la chaîne de transmission modélisée sous Optisystem.

A - L'émetteur



Le système se compose au niveau de l'émetteur :

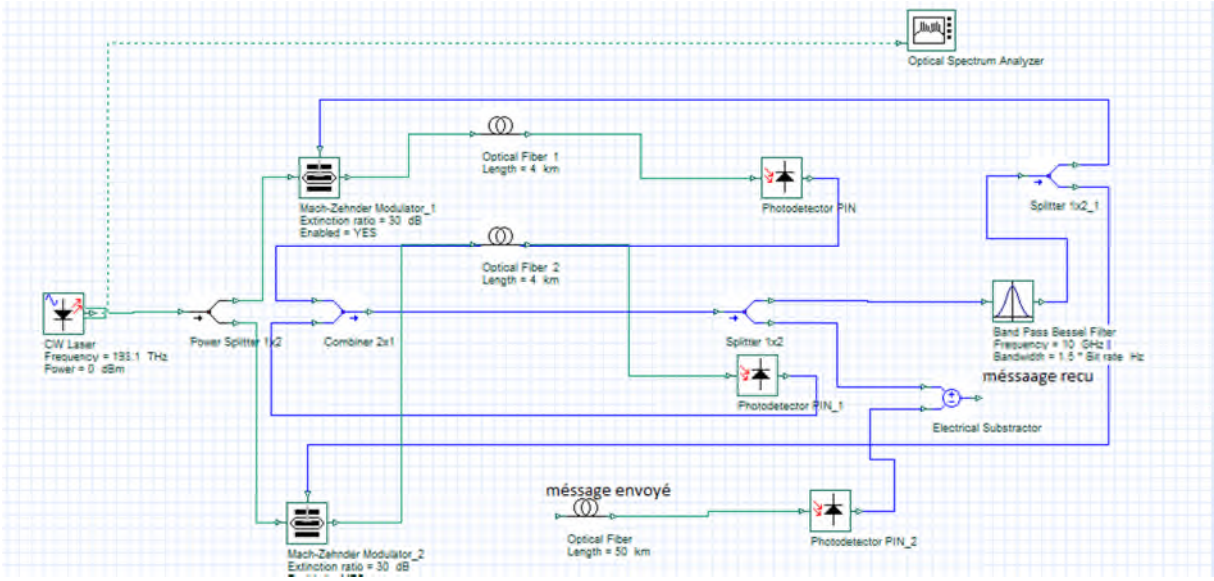
• d'un module pour la génération de chaos optique

• d'un module pour le chiffrement chaotique

Le module du générateur de chaos est celui présenté plus haut composé d'une source Laser à semi-conducteur dont la puissance est divisée en deux branches chacune appliquée à l'entrée d'un MZN à l'autre entrée on applique une rétroaction obtenue après une photo détection.

Le chiffrement est une simple addition suivi d'une modulation directe effectuée par un laser à semi conducteur qui transmets alors le message chiffré au canal de transmission qui est représenté ici par une fibre optique.

B- Le récepteur :



Le récepteur est constitué du même générateur de chaos optique que l'émetteur ceci pour la simple raison qu'on voulait éviter les problèmes de synchronisation qui ne sont pas évidente à réaliser.
Le message obtenu à la sortie du canal de transmission est alors détecté par un photodétecteur puis on lui soustrait le chaos qui été rajouté avant l'émission pour obtenir finalement le message déchiffré.

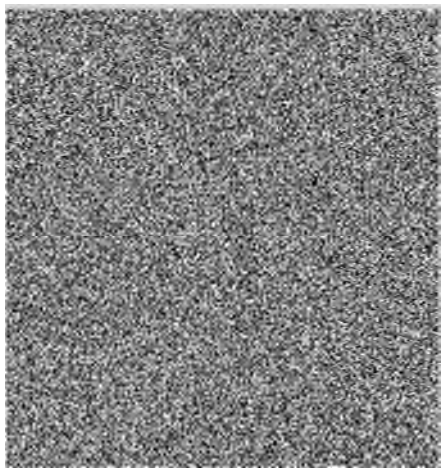
II.5 Chiffrement et déchiffrement de l'image

Dans notre travail on a aussi réalisé un algorithme de génération de séquences chaotiques à partir d'une suite logistique. Ces séquences sont utilisées comme clé de chiffrement un puis de déchiffrement de l'image et il nous donne aussi l'histogramme correspondant à l'image original puis celui de l'image chiffrée

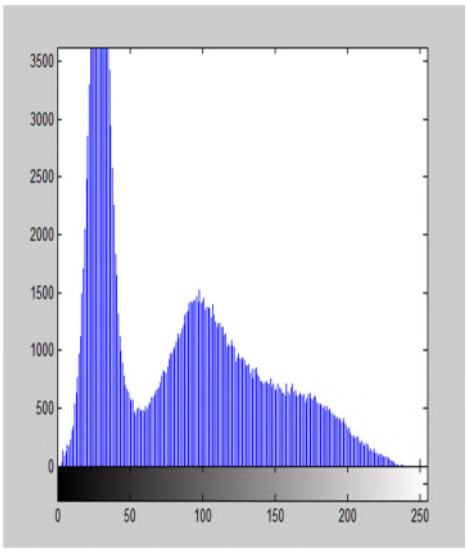
L'image originale est celle de l'émir Abdelkader

Sur cette image on va effectuer un premier traitement en passant aux nuances de gris, image qui va servir comme base pour le chiffrement puis le déchiffrement

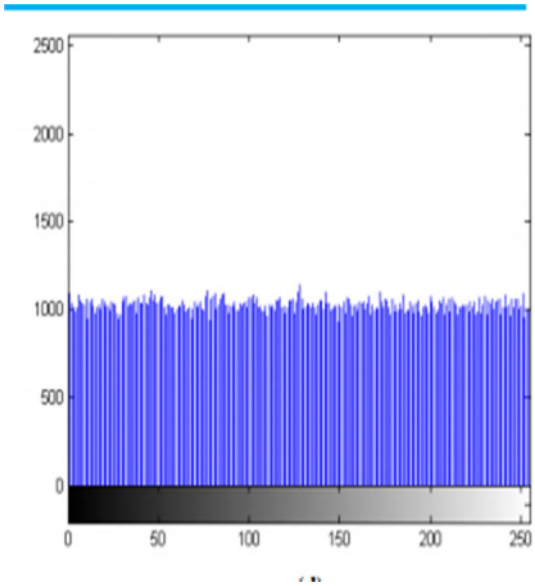
(a)



(b)



(c)



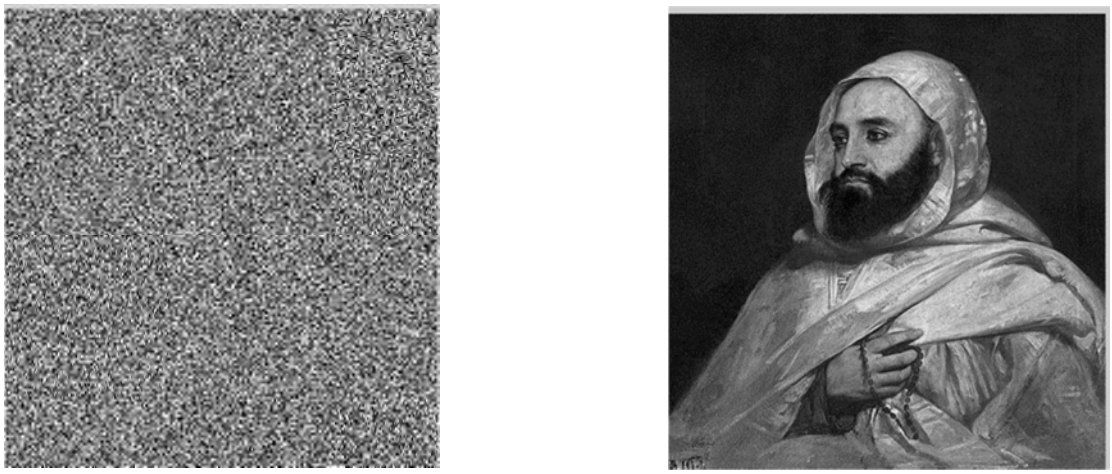
(d)

Figure III.8 Chiffrement de l'image

a) Image originale
b) Image chiffrée
c) Histogramme d l'image originale

d) Histogramme d l'image chiffrée

❖ Pour le déchiffrement le résultat était le suivant



(a) (b)

Figure III.9 Déchiffrement de l'image

a) Image chiffrée

b) Image originale

Conclusion

A travers cette étude nous avons présenté un cryptosystème réalisé autour d'un générateur de chaos a base de suite logistique qui nous a permet de voir les différentes propriétés du chaos ; avant de réaliser une chaine de transmission optique sous optisystem ou le générateur chaotique était basée sur les lasers a semi-conducteur

Conclusion Générale

Conclusion Générale

Ce mémoire consiste à réaliser un système de transmission de données et 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.

Dans le premier chapitre de ce mémoire, nous avons présenté une chaine de transmission et nous avons intensifié notre étude sur les lasers à semi-conducteur, cette thèse porte sur l'estimation de l'état et des entrées inconnues pour une classe des systèmes non linéaires. De façon plus particulière, le problème est abordé sous l'angle de la conception d'un système de transmission sécurisée d'informations exploitant les propriétés des systèmes chaotiques. Les travaux présentés traitent trois points principaux : le choix de l'émetteur, le développement du récepteur, et la mise au point du processus de transmission de l'information ou du message.

Dans le deuxième chapitre, nous avons évoqué d'abord quelques notions sur les systèmes dynamiques qu'ils soient en temps continu où en temps discret.par la suit, nous nous sommes intéressés à une classe particulière de système non linéaire qui est dit chaotique.

Ces systèmes présentent plusieurs caractéristiques dont l'exploitation serait intéressante pour la transmission de données. Parmi ces caractéristiques que nous avons développées avec plus de détails, nous pouvons citer le déterminisme qui signifie que ces systèmes sont régis par des règles fondamentales non probabilistes. Il est alors possible de reproduire le comportement chaotique. Une autre propriété intéressante de ces systèmes est la sensibilité aux conditions initiales.

En effet, un moindre écart ou imprécision dans les conditions initiales engendre des évolutions totalement différentes. Ceci implique l'impossibilité de prédiction à long terme du comportement du système chaotique, et pour chaque catégorie nous avons donné des exemples de systèmes chaotiques utilisés par la communauté scientifique.

Dans le troisième chapitre du mémoire, nous avons fais une simulation avec Le logiciel optisyteme qui nous sa permis de simuler notre système de transmission

optique en utilisant le langage de programmation MATLAB pour l'insertion de quelques fonctions. 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 le logiciel Optisystem. Les données du signal chaotique ont été obtenues par l'intégration numérique sous Matlab.

Bibliographie

Bibliographie

(1) Adams et al, 1993 C. M. Adam, S.E. Tavares, “Designing S-boxes for ciphers resistant to differential cryptanalysis“, Proceedings of the 3rd Symposium on State and Progress of Research in Cryptography, Rome, Italy, pp. 181–190, 1993. [Addabbo et al, 2004 .

(2) Alvarez 06a G. Alvarez & S. Li. *Some Basic Cryptographic Requirements for Chaos-Based*

(3) Álvarez 06b Gonzalo Álvarez & Shujun Li. *Some basic cryptographic requirements for chaosbased cryptosystems*. accepted by International Journal of Bifurcation and Chaos

(4) Amigo et al, 2007J. M. Amigó, L. Kocarev , J. Szczepanski, “Theory and practice of chaotic cryptography“, Physics Letters A, Vol. 366, pp. 211–216 , 2007.

(5) [Canteaut, 2001] A. Canteaut, “Cryptographic functions and design criteria for block ciphers“, In Proceedings of Indocrypt, Springer, 2001.

(6) [Chen et al, 2004] G. Chen, Y. Mao, Charles K. Chui, “A symmetric image encryption scheme based on 3D chaotic cat maps “, Chaos, Solitons Fractals, Vol. 21, pp. 749-761, July 2004.

(7) [Cherrier et al, 2010] E. Cherrier, M. M′Saad, M. Farza, “High-gain observer synchronization for a class of time-delay chaotic systems, Application to secure communications”, Journal of Nonlinear Systems and Applications, pp. 102-112, 2010.

(8) [Dachselt et Schwarz, 2001] F. Dachselt, W. Schwarz, “Chaos and cryptography”, IEEE Trans.Circuits and Systems–I, Vol. 48, pp. 1498–1509, 2001.

(9) [Dachselt et Schwarz, 2001] F. Dachselt, W. Schwarz, “Chaos and cryptography”, IEEE Trans. Circuits and Systems–I, Vol. 48, pp. 1498–1509, 2001.

(10) [Dawson 92] D.M. Dawson, Z. Qu & J.C. Carroll. *On the state observation and output feedback problems for nonlinear uncertain dynamic systems*. Systems & Control Letters,

(11) [Femat 01] R. Femat, R.Jauregui-Ortiz & G. Solís-Perales. *A chaos-based communication*

(12) [Fournier et al, 2011] D. Fournier, P. Chargé, L. Gardini, ″Border Collision Bifurcations and Chaotic Sets in a Two-Dimensional Piecewise

Linear Map″, Communications in Nonlinear Science and Numerical Simulation Vol. 16, no. 2, pp. 916-927, February 2011.

(13) [Ha 04] Q.P. Ha & H. Trinh. *State and input simultaneous estimation for a class of nonlinear systems*. Automatica, vol. 40, pages 1779–1785, 2004.

(14) [Haeri 06] M. Haeri & B. Khademian. *Comparison between different synchronization methods of identical chaotic systems*. Chaos, Solitons and Fractals, vol. 29, no. 4,

(15) [Inoue 01] E. Inoue & T. Ushio. *Chaos communication using unknown input observers*.

(16) "Synchronization and communication using semiconductor lasers with optoelectronic

(17) 1807, 2001.

(18) à très haut débit, 7KqVH_GH_GRFWRUDW_GH_O¶8QLYHUVLWp_GH_5HQQHV_, 2004.

(19) Access Techniques and Performance. Elsevier, 2006.

(20) Addabbo, M. Alioto, S. Bernardi, A. Fort, S. Rocchi, V. Vignoli, "The digital tent map: performance analysis and optimized design as a source of pseudo-random bits", IEEE

(21) Annovazzi-Lodi, S. Donati, and A. Scire, "Synchronization of chaotic lasers by optical

(22) 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.

(23) Chapin. D.M, fuller C.S, pearson G.L.A new silicon pn junction photocell for converting solar radiation into electric power.J.Appl.Phys. 1954, vol25,pp.676-677.

(24) *Cryptosystems*. International Journal of Bifurcation and Chaos, vol. 16, no. 8,

(25) D . Ankri, " Transport électronique en régime de survitesse dans les composants à semi-conducteurs III-V", L'Echo des Recherches, No. 118, 1984.

(26) David Aubin, Amy Dahan. "Systemes dynamiques et Chaos : Convergences et recompositions, un apercu historique". Apparu dans Chaos & Systemes dynamiques: elements pour un epistemologie, dir. Sara Franceschelli, Tatiana Roque & Michel Paty. Paris: Hermann, (11 decembre 2007), pp. 327-356.

(27) demonstrating 10 Obis chaos communications," IEEE J. Quant. Electron., 46 (10), 1435, 2010.

(28) digital key," *Optics Express*, vol. 20, pp. 25333–25344, November 2012. doi:10.1093/bjps/axn053

(29) Ecole d'eté d'optoélectronique ; PHISIQUE DES SEMICONDUCTEURS III- V ; S.S LAVAL, Institut d'Electronique Fondamentale, CNRS (URA 022), Bat. 220. University Paris Sud, F-91405 Orsay Cedex, France (2002).

(30) Electronics and Communications in Japan, vol. J82-A, no. 12, pages 1801– Encyclopedia Universalis. et Application à la cryptographie. PhD in Engineering Sciences, Université de feedback for cryptographic applications," *IEEE J. Quantum Electron.*, vol. 33, no. 9, pp. 1449– 1454, Sep. 1994. feedback," *IEEE J. Quantum Electron.*, vol. 37, no. 10, pp. 1301–1311, Oct. 2001.µ 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. Franche-Comté, 2002.

(31) G.P. William, Chaos Theory Tammed. Taylor & Francis, 1997.

(32) H. D. I. Abarbanel, M. B. Kennel, S. Illing, L. Tang, H. F. Chen, and J. M. Liu,

(33) H. Mathieu. Physique des semi-conducteurs et des composants électroniques 1996 .

(34) I, vol. 48, no. 10, pages 1161–1169, 2001. in May 2005, tentatively scheduled for publication in vol. 16, no. 7, 2006, preprint available online at http://www.hooklee.com/pub.html, 2006.

(35) J. D. Farmer, Chaotic attractors of infinite-dimentional dynamical system, Physica D, 4, 366-393 (1982).

(36) Jiang 02 Z.-P. Jiang. *A note on chaotic secure communication systems*. IEEE Transactions on Circuits and Systems I, vol. 49, no. 1, pages 92–96, 2002.

(37) 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).

(38) L. Bramerie, 'Etude de la régénération optique dans les systèmes de transmissions

(39) 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.

(40) L. Vegard Z. Phys. 5.17 (1921).

(41) M. Hasler. Engineering chaos for encryption and broadband communication. *Phil. Trans.*

(42) 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.

(43) M. R. Nguimdo and P. Colet, “Electro-optic phase chaos systems with an internal variable and a

(44) M. S. Baptista, “Cryptography with Chaos”, *Physics Letters A*, vol. 240, pp. 50–54, 1998.

(45) M.W. Lee, Etudes de Comportements Chaotiques en Modulation de Cohérence pages 1002–1022, 2006. pages 2129–2151, 2006.

(46) R. Lang and K. Kobayashi, “External optical feedback effects on semiconductor injection laser properties,” IEEE J. Quantum Electron. vol. 16, pp. 347–355, 1980

(47) R. Lavrov, M. Jacquot, L. Larger, "Nonlocal nonlinear electro-optic phase dynamics

(48) R.M. Gagliardi et S. Karp, ‘Optical communications’, Wiley-intersciences, 1976. *Royal Soc. London*, A, 353 :115–126, 1995.

(49) S. Sivaprakasam and K. A. Shore, “Message encoding and decoding using chaotic externalcavity diode lasers,” *IEEE J. Quantum Electron.*, vol. 36, no. 1, pp. 35–39, Mar. 2000.

(50) *scheme via robust asymptotic feedback*. IEEE Transactions on Circuits and Systems Scientiic Conference on Physics and Control (PhysCon 2007), (2007).

(51) Secure Communications and Cryptanalysis: A Brief Survey, 3rd International IEEE

(52) Shujun Li , Gonzalo Alvarez, Zhong Li and Wolfgang A. Halang, Analog Chaos-based

(53) Transactions on Instrumentation and Measurement, Vol. 2, pp. 1301-1304, May 2004.

(54) vol. 18, pages 217–222, 1992.

(55) W.M. Tam, F.C.M. Lau, and C.K. Tse, Communications with Chaos: Multiple

(56) Werndl, Charlotte (2009). "What are the New Implications of Chaos for Unpredictability?". The British Journal for the Philosophy of Science 60 (1): 195–220.

(57) Wikiversity (28 July 2011). "1972/Lorenz". Wikipedia. Retrieved 8 April 2014.

Résumé

Utilisation de la théorie du chaos pour transmettre de l'information via fibre optique en toute sécurité est possible. Le système permet en effet de camoufler des données au sein d'ondes chaotiques afin de les rendre indéchiffrables.

L'objectif de ce travail est de présenté un système de transmission chaotique, et permettre l'envoi et la réception de messages d'une manière stable par réseau optique. La lumière, transmise par des lasers, étant non-linéaire, le générateur de chaos est réalisé à partir d'une émission laser appliqué à un OEO à rétroaction retardée cette onde chaotique nous permet de chiffrer l'information et de la transmettre au récepteur où on a le même générateur qui va servir pour déchiffrer et revenir à l'information initiale.

L'élément clé de d´encodage réside dans la capacité du système récepteur à reproduire le plus fidèlement possible les oscillations chaotiques de l'émetteur.

Mots clés : Laser à semi-conducteur , générateur de Chaos optique, transmission sécurisée, chiffrement, déchiffrement d'image.

Abstract

Using chaos theory to send information via optical fiber is safely possible. The system makes it possible to hide data within the chaotic waves to make them indecipherable.

The objective of this work is presented a chaotic transmission system, and allow sending and receiving messages in a stable manner by optical network. The light transmitted by the laser, being nonlinear, chaos generator is made from a laser emission applied to a feedback OPA delayed this chaotic wave allows us to encrypt information and transmit it to the receiver where we have the same generator that will be used to decrypt and return to the initial information.

The key element of d'encodage is the receiver system's ability to reproduce as faithfully as possible the chaotic oscillations of the issuer.

Keywords: semiconductor laser, optical chaos generator, secure transmission, encryption, image decryption.

ملخص

باستخدام نظرية الفوضى لإرسال المعلومات عبر الألياف الضوئية من الممكن بأمان. نظام يجعل من الممكن لإخفاء البيانات داخل موجات الفوضى لجعلها عويص.

ويرد الهدف من هذا العمل نظام نقل الفوضى، وتسمح إرسال واستقبال الرسائل بطريقة مستقرة من قبل الشبكة البصرية .ضوء تنتقل عن طريق الليزر، ويجري غير الخطية، وتتكون مولد الفوضى من انبعاث الليزر تطبيقها على OPAردود الفعل تأخر هذه الموجة الفوضوية تسمح لنا لتشفير المعلومات وإحالته إلى المتلقي حيث لدينا نفس المولدات التي سيتم استخدامها لتشفير والعودة إلى المعلومات الأولية والعنصر الأساسي encodage هو قدرة النظام المتلقي لإعادة إنتاج بأكبر قدر من الأمانة التذبذبات الفوضوية للمصدر.

الكلمات المفتاحية: ليزر أشباه الموصلات، مولد الفوضى البصرية، نقل آمنة، والتشفير، صورة فك التشفير.