الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

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

En : **Télécommunications**

Spécialité : **Systèmes des Télécommunications**

Par :

BOUNAB Firras Abdelmounaim *et* OUADFEL Nadir

Sujet

Etude et conception d'un générateur chaotique pour sécuriser les communications sans fil allant jusqu'à 6 GHz

Soutenu publiquement, le **22 / 06 / 2022**, devant le jury composé de :

Mr M. FEHAM	Professeur	Université de Tlemcen	Président
Mr S. M. BAHRI	Maitre de Conférences-B	Université de Tlemcen	Examinateur
Mr S. KAMECHE	Professeur	Université de Tlemcen	Encadreur
Mr M. BENDAOUD	Doctorant	Université de Tlemcen	Co-Encadreur

Année universitaire : 2021 / 2022

الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التعليم العالي و البحث العلمي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جامعة أبي بكر بلقايد – تلمسان –

Université Aboubakr Belkaïd – Tlemcen –

Faculté de TECHNOLOGIE

MEMOIRE

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

En : **Télécommunications**

Spécialité : **Systèmes des Télécommunications**

Par :

BOUNAB Firras Abdelmounaim *et* OUADFEL Nadir

Sujet

Etude et conception d'un générateur chaotique pour sécuriser les communications sans fil allant jusqu'à 6 GHz

Soutenu publiquement, le **22 / 06 / 2022**, devant le jury composé de :

Mr M. FEHAM	Professeur	Université de Tlemcen	Président
Mr S. M. BAHRI	Maitre de Conférences-B	Université de Tlemcen	Examinateur
Mr S. KAMECHE	Professeur	Université de Tlemcen	Encadreur
Mr M. BENDAOUD	Doctorant	Université de Tlemcen	Co-Encadreur

Année universitaire : 2021 / 2022

Dédicaces

Dédicaces « Firas »

Merci « Allah » Dieu le tout puissant qui m'a donné le courage, la force et la patience pour réaliser ce travail.

Je dédie ce modeste travail en signe de respect et de reconnaissance

A

Mes parents, que j'aime beaucoup pour tous leurs nombreux sacrifices et qui ont toujours été à mes côtés pour me soutenir, m'encourager et me conseiller. Puisse Dieu, vous préservez et vous accordez santé et bonheur.

Mon frère « Soheyb », Mes sœurs « Yasmine » et « Douaa » Pour leur soutien et encouragements.

Toute ma famille.

Tous mes amis, je vous remercie infiniment pour votre aide ainsi que vos encouragements et votre fidélité.

Mon binôme et mon amis « Nadir » et sa famille.

Firas

Dédicaces « Nadir »

Merci « Allah » Dieu le tout puissant qui m'a donné le courage, la force et la patience pour réaliser ce travail.

Je dédie ce modeste travail en signe de respect et de reconnaissance

A

Mes parents, que j'aime beaucoup pour tous leurs nombreux sacrifices et qui ont toujours été à mes côtés pour me soutenir, m'encourager et me conseiller. Puisse Dieu, vous préservez et vous accordez santé et bonheur.

, Mes sœurs « Narimene » et « Meriem » Pour leur soutien et encouragements.

Toute ma famille.

Tous mes amis, je vous remercie infiniment pour votre aide ainsi que vos encouragements et votre fidélité.

Mon binôme et mon amis « Firas » et sa famille.

Nadir

Remerciements

Ce travail de recherche a été effectué au sein du laboratoire des Systèmes et Technologies de l'information et de la Communication (STIC) de la Faculté de Technologie à l'Université Abou-Bekr Belkaïd Tlemcen.

On voudrait tout d'abord remercier sincèrement notre Encadreur Monsieur Samir KAMECHE, Professeur à l'Université de Tlemcen, non seulement pour son encadrement actif mais aussi pour sa grande disponibilité, sa patience, ainsi que pour la générosité avec laquelle il a su partager ses connaissances et conseils.

Nous tenons aussi très chaleureusement à remercier notre Co-encadreur Monsieur BENDAOUD Mohammed, Doctorant à l'université de Tlemcen, d'avoir Co-encadré notre travail et su guider nos activités.

Nos remerciements les plus respectueux s'adressent à Monsieur Mohammed FEHAM, Professeur à l'Université de Tlemcen, pour avoir accepté de présider le jury de ce Mémoire.

Nous exprimons également notre reconnaissance à Monsieur Sidi Mohamed BAHRI, Maître de Conférences classe B à l'Université de Tlemcen, pour avoir accepté d'examiner et de juger les travaux de ce Mémoire.

Enfin, que nos parents, nos familles et nos amis trouvent à travers ces quelques lignes l'expression de notre profonde gratitude pour leur soutien et leurs encouragements de tous les instants. On vous en remercie chaleureusement.

Résumé

Résumé

Ce travail de mémoire consiste en l'étude et la conception d'un nouvel émetteur chaotique destiné aux transmissions sécurisées. Ce mémoire est composé de deux parties principales: la première partie concerne l'étude des systèmes chaotiques qui sont des systèmes caractérisés par le déterminisme, la non linéarité et une extrême sensibilité aux conditions initiales, ainsi quelques outils pour faciliter l'étude de ces systèmes comme les exposants de Lyapunov, l'espace des phases et le diagramme de bifurcation qui nous montre les différents comportements d'un système dynamique en passant par le comportement périodique jusqu'au comportement chaotique. L'étude des systèmes chaotiques est destinée à leur utilisation pour sécuriser les transmissions, c'est pourquoi nous avons expliqué les objectifs des crypto-systèmes et les différentes techniques de chiffrement par chaos, ainsi les différents régimes de synchronisation. La deuxième partie de ce travail comprend la conception d'un émetteur chaotique, qui a été réalisé en combinant deux versions de Colpitts à l'aide d'un transistor bipolaire de type BFG410W. Cette nouvelle structure a été simulée par deux logiciels de simulation, le premier c'est Matlab, afin de résoudre le modèle mathématique proposé et ainsi identifier les comportements possibles de cet émetteur, et le second est le logiciel ADS qui a été utilisé pour l'objectif de vérifier les résultats obtenus sous Matlab et donc validant le modèle mathématique établi, et traçant les réponses temporelles et fréquentielles. À travers cette dernière réponse, nous avons conclu que cet émetteur propose dans notre travail peut générer des signaux chaotiques allant jusqu'à 6 GHz.

Mots clés : *chaos, diagramme de bifurcation, l'espace de phase, Matlab, ADS, BFG410W.*

ملـخــص

ملخص

يهتم هذا العمل بدراسة وتصميم مرسل فوضوي جديد موجه لتأمين الاتصالات، ينقسم هذا العمل الى جزئين أساسيين: يتعلق الجزء الأول بدراسة الأنظمة الفوضوية والتي تتميز بالحتمية، اللاخطية، والحساسية المفرطة للشروط الابتدائية، وكذا بعض الوسائل المتاحة لتسهيل دراسة هاته الأنظمة مثل دلائل ليابونوف، مساحة الطور، ومخطط التشعب الذي يوضح لنا السلوكيات الممكنة للأنظمة الديناميكية انطلاقا من السلوك الدوري وصولا الى السلوك الفوضوي. تهدف دراسة الأنظمة الفوضوية إلى استخدامها لتأمين عمليات الاتصالات، ولهذا السبب قمنا بشرح أهداف أنظمة التشفير وتقنيات التشفير المختلفة بالفوضى، فضلاً عن أنظمة التزامن. يتضمن الجزء الثاني من هذا العمل تصميم مرسل فوضوي من خلال الجمع بين نسختين مختلفتين من مذبذب كولبيتس باستعمال ترانسيستور ثنائي القطب من نوع (BFG 410W)، تمت محاكات هذا الهيكل الجديد بواسطة برنامجين، الأول هو (Matlab) وهذا لحل النموذج الرياضياتي الخاص بهذا المرسل وبالتالي تحديد السلوكيات الممكنة له، أما البرنامج الثاني هو (ADS) والذي تم استعماله بغرض التحقق من النتائج الرياضية المتحصل عليها باستعمال (Matlab) وبالتالي التحقق من صحة النموذج الرياضياتي، ورسم الاستجابات الزمنية والترددية الخاصة بهذا المرسل. من خلال هاته الاستجابة الأخيرة، استنتجنا أن المرسل المقترح في عملنا بإمكانه توليد اشارات فوضوية تصل الى غاية 6 جيغا هرتز.

الكلمات المفتاحية: *الفوضى، منحنى التشعب، مساحة الطور، Matlab ، ADS، BFG410 W .*

Abstract

Abstract

This work consists in the study and the design of a new chaotic transmitter intended for secure transmissions. This memory is composed of two main parts: the first part concerns the study of chaotic systems which are systems characterized by determinism, non-linearity and extreme sensitivity to initial conditions, as well as some tools to facilitate the study of these systems such as Lyapunov exponents, phase space and the bifurcation diagram that shows us the different behaviors of a dynamic system through the periodic behavior to the chaotic behavior. The study of chaotic systems is intended for their use in securing transmissions, so we have explained the objectives of cryptosystems and the different techniques of encryption by chaos, as well as the different regimes of synchronization. The second part of this work includes the design of a chaotic emitter, which has been realized by combining two versions of Colpitts using a BFG410W bipolar transistor. This new structure has been simulated by two simulation software, the first is Matlab, in order to solve the proposed mathematical model and thus identify the possible behaviors of this emitter, and the second is the ADS simulator that has been used for the purpose of verifying the results obtained in Matlab and thus validating the established mathematical model, and plotting the temporal and frequency responses. Through this last response, we concluded that this transmitter proposed in our work can generate chaotic signals up to 6 GHz.

Keywords: *chaos, bifurcation diagram, phase space, Matlab, ADS, BFG410W.*

Table des matières

Chapitre II : Transmission chaotique

Sigles et abréviations

ADS: Advanced **D**esign **S**ystem simulator.

BJT: Bipolar **J**unction **T**ransistor.

CSK: Chaos **S**hift **K**eying.

DES: Data **E**ancryption **S**tandard.

ECC: Elliptic **C**urve **C**ryptography.

ISM: Industria**l, S**cientific and **M**edical band.

ODE: Ordinary **D**ifferential **E**quation.

$\boldsymbol{R}$ **:** Ensemble des nombres réels.

$\boldsymbol{R^+}$ **:** Nombres réels positifs ou nuls.

$\boldsymbol{R^n}$ **:** Espace vectoriel de dimension n construit sur le corps des réels.

RC4 : Rivest **C**ipher 4.

RED: Radio **E**quipment **D**irective.

RK-4: Runge-**K**utta d'ordre **4**

RSA : R**.R**ivest A**.S**hamir L**.A**dleman.

SCI : Sensibilité aux **C**onditions **I**nitiales.

UHF: Ultra **H**igh **F**requency.

WLAN: Wireless **L**ocal **A**rea **N**etwork.

$\dot{\boldsymbol{x}} = \frac{dx}{dt}$ **:** Dérivée de la variable x par rapport au temps.

Liste des figures

Chapitre I : Systèmes dynamiques et chaos

Chapitre II : Transmission Chaotique

Chapitre III : Conception et simulation d'un générateur pour les transmissions chaotiques

Liste des tableaux

Introduction générale

Introduction générale

Depuis l'antiquité, l'homme n'a pas cessé de chercher les différents moyens pour transmettre un message à son correspondant et pouvoir ainsi communiquer avec lui en toute sécurité. Tous ces efforts ont conduit à l'évolution des modes de communication et à leur développement continu à la recherche de débits plus élevés, d'une mobilité améliorée et surtout de la confidentialité des communications.

Les 20 dernières années ont été marquées par une révolution des systèmes de communication grâce au développement des technologies de l'information telles que les téléphones portables, les ordinateurs et autres périphériques informatiques utilisant des systèmes de réseaux sans fil, mais aussi plus récemment des capteurs sans fil et les systèmes d'identification par radiofréquence (RFID), envahissent progressivement notre quotidien et font l'objet d'un essor commercial grandissant. Cette révolution a permis un échange facile de millions de kilo-octets d'informations. Cependant, avec ces flux, des données confidentielles sont transmises via des canaux de communication non sécurisés, et les informations peuvent être interceptées à tout moment par des personnes indésirables.

La cryptographie ou l'Art de chiffrer est une science aussi vieille que le monde, elle a été cultivée, dès la plus haute antiquité, par les Chinois, les Perses, les Carthaginois ; elle était enseignée dans les écoles tactiques de la Grèce, et tenue en haute estime par les généraux romains les plus illustres. La cryptographie ancienne utilisait différents outils pour dissimuler une information ou un texte secret. Certains ont remplacé des mots par des chiffres, d'autres ont mélangé, décalé ou interverti des lettres, comme dans la substitution alphabétique inversée, pour rendre la lecture du message difficile ou impossible.

Les premiers principes de base de la cryptographie moderne reviennent à Auguste Kerkhoffs, Son essai « La Cryptographie militaire » (1883) constitue une référence de la cryptographie du 19ème siècle. À l'époque, l'une des préoccupations des cryptographes était de mettre en place un réseau de télégraphie sécurisé dont l'idée la plus importante est que la sécurité du chiffre ne doit pas dépendre de ce qui ne peut être facilement changer. En d'autres termes, aucun secret ne doit résider dans l'algorithme de cryptage mais plutôt dans la clé.

La cryptographie actuelle cherche à transformer de façon mathématique et algorithmique un message clair pour obtenir un autre chiffré et qui, à première vue, semble aléatoire. Plus l'inversion de la transformation est difficile plus la sécurité est élevée et vice versa. On cherche alors un phénomène d'apparence aléatoire, mais qui est déterministe à

l'origine pour le masquage d'information. Ainsi plusieurs moyens ont été développés, partant d'un système classique vers des systèmes numériques. L'utilisation des caractéristiques chaotique et hyper-chaotique a permis aussi le chiffrage des informations échangées entre un émetteur et un récepteur. La réussite de T.Peccora et L.Carroll en 1990 dans la synchronisation des deux signaux chaotiques offre la possibilité de développer de nouveaux systèmes de transmission sécurisée, la sécurisation de la transmission peut s'effectuer uniquement par l'intermédiaire des étages de modulation et de démodulation des systèmes de communication.

L'objectif de notre projet de fin d'études est la conception d'un générateur chaotique basé sur deux structures de Colpitts (standard et améliorée).

Ce travail décompose en trois chapitres :

- Le premier chapitre présente un état de l'art sur les systèmes dynamiques non linéaires en général et chaotiques en particulier.
- Le second chapitre présente le principe de cryptographie chaotique avec les méthodes de cryptage et décryptage, ainsi les généralités sur la synchronisation des systèmes chaotiques.
- Dans le troisième chapitre nous allons commencer par la présentation des applications qu'on veut les sécuriser, puis exposer quelques circuits chaotiques, ainsi que ses modèles mathématiques, en finalisant ce chapitre par la proposition d'un générateur chaotique basé sur l'utilisation les deux versions de Colpitts (standard et amélioré).

Chapitre I

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. À la fin du XIXe siècle, Henri 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 (calculer, les dates emplacement Initiale, la masse et la vitesse de trois corps sous réserve de l'influence de la mutuelle attraction gravitationnelle).

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 quantifier.

I.2 Systèmes dynamiques

Un système dynamique est une structure qui évolue au cours du temps de façon à la fois [1,2] :

• 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 finies [3].

I.2.1 Classification des systèmes dynamiques

Les systèmes dynamiques se classifient en fonction de leur façon d'évoluer dans le temps. Ainsi, il existe deux types de systèmes dynamiques :

• Les systèmes aléatoires, qui évoluent au hasard dans tout l'espace sans qu'aucune équation ne les régissent. Aucune prévision exacte dans le temps n'est possible.

• Les systèmes déterministes, régis par des lois mathématiques bien connues et dont on peut donc prévoir exactement leur évolution dans le temps.

Ces systèmes chaotiques, semblent suivre à la fois des lois déterministes et des lois aléatoires, ce qui rend toute prévision à long terme impossible [4].

I.2.2 Représentation des systèmes dynamiques

Partant de ces différentes classes de systèmes dynamiques, nous pouvons représenter l'évolution d'un système de deux formes possibles :

• Systèmes en temps continu ;

• Systèmes en temps discret.

I.2.2.1 Systèmes dynamiques continus

Les systèmes à temps continu sont caractérisés par l'utilisation d'équations différentielles décrivant l'évolution des variables dans le temps [5].

Les équations utilisées, reposant sur une approximation au premier ordre, possèdent la forme :

$$\dot{x} = \dot{x}(t) = f(x, t, v) \tag{I.1}$$

Avec $x(t)$ représentant l'évolution du système dans le temps et $\dot{x}(t)$ correspondant à l'état instantané du système. La fonction f dépend du temps, ainsi que des paramètres du système. Dans un système à *n* variables, l'expression (I.1) devient :

$$\begin{aligned}
\dot{x}_1 &= f_1(x_1, x_2, \ldots, x_n; t, v) \\
\dot{x}_2 &= f_2(x_1, x_2, \ldots, x_n; t, v) \\
&\ldots \\
&\ldots \\
\dot{x}_n &= f_n(x_1, x_2, \ldots, x_n; t, v)
\end{aligned} \tag{I.2}$$

Dont le système, $x_1, \ldots, x_n$ possèdent des conditions initiales connues $x_1(0), \ldots, x_n(0)$.

I.2.2.2 Systèmes dynamiques discrets

Pour les systèmes à temps discret, le système est décrit en utilisant une modélisation dont les instants sont répartis dans le temps de façon équidistante [6].

Afin de répondre aux critères de discrétisation du système dans le temps, deux possibilités s'offrent :

1- Les caractéristiques du système imposent leurs caractères discrets,

2- Le système est une version échantillonnée d'un système en temps continu.

Mais dans les deux cas, leurs représentations mathématiques utilisent des fonctions de récursivité. Une mise en équation via un système de premier ordre, est caractérisée de la façon suivante :

$$f(x+1) = f(x_n), n \geq 0 \tag{I.3}$$

I.3 Système 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 caractérisés par une

extrême sensibilité aux conditions initiales. Ils ne sont pas déterminés ou modélisés par des systèmes d'équations linéaires ni par les lois de la mécanique classique ; pourtant, ils ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités.

L'exemple suivant illustre les propriétés d'un système chaotique. Soit le modèle chaotique donné par Otto Rössler [7].

$$\begin{cases} \dot{x}_1 = -x_2 - x_3 \\ \dot{x}_2 = x_1 + a x_2 + 0.01 \ln(x_3) \\ \dot{x}_3 = c + x_3 (x_1 - b) \end{cases} \tag{I.4}$$

Où (x_1, x_2, x_3) est le vecteur d'état et a, b, c sont les paramètres du système. Ce système montre un comportement chaotique pour a = 0.2, b = 5.7, c = 0.2, avec les conditions initiales $x_1(0) = x_2(0) = x_3(0) = 0.01$.

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

I.3.1 Non linéaire

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 [8,9].

I.3.2 Déterministe

La notion de déterminisme signifie la capacité de « prédire » le futur d'un phénomène à partir d'un évènement passé ou présent. L'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités.

Dans les phénomènes aléatoires, il est absolument impossible de prévoir la trajectoire d'une quelconque particule. À l'opposé, un système chaotique a des règles fondamentales déterministes et non probabilistes.

I.3.3 L'aspect aléatoire

Une autre caractéristique des systèmes chaotiques peut être observée sur la figure (I.1). En effet, un système chaotique évolue d'une manière qui semble aléatoire. Cette figure permet de comparer une évolution simple, périodique et donc prédictible d'un système classique avec l'évolution plus complexe, non périodique et non prédictible d'un système chaotique.

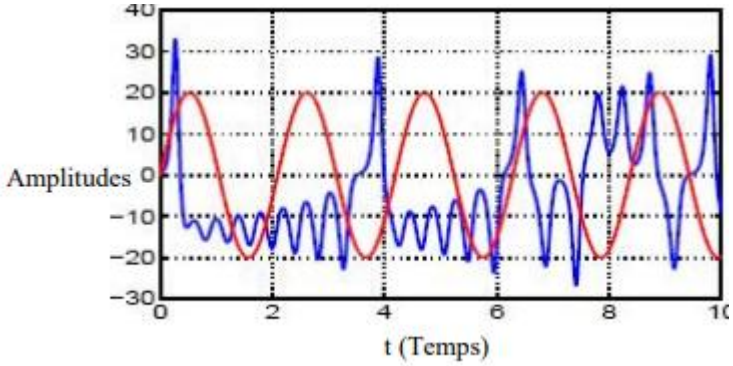


Figure I.1. Evolution dans le temps d'un système chaotique (Rossler), comparé à une sinusoïde.

I.3.4 Sensibilité aux conditions initiales

Tout d'abord, les systèmes chaotiques sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par l'effet papillon, popularisé par le météorologue Edward Lorenz. L'évolution d'un système dynamique chaotique est imprédictible dans le sens qu'elle est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est clair que la moindre erreur ou simple imprécision sur la condition initiale empêche de décider à tout le temps qu'elle sera la trajectoire effectivement suivie ; et par conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite des systèmes déterministes, il est impossible de prévoir à long terme leurs comportements. La seule manière est d'opérer effectivement l'évolution du système. Si cette simulation se fait informatiquement, un problème de précision sur les conditions initiales se pose alors : des petites erreurs d'arrondissement dues à la précision du type de la variable codant ces conditions initiales peuvent exponentiellement s'amplifier de telle sorte que la trajectoire de phases obtenue n'est pas représentative de la réalité.

Illustrons ce phénomène de SCI par une simulation numérique, on affecte à un système chaotique deux conditions initiales très proches. Dans un premier temps, les deux systèmes évoluent de la même manière ; mais très vite, leur comportement devient différent. Ceci est illustré dans la figure suivante :

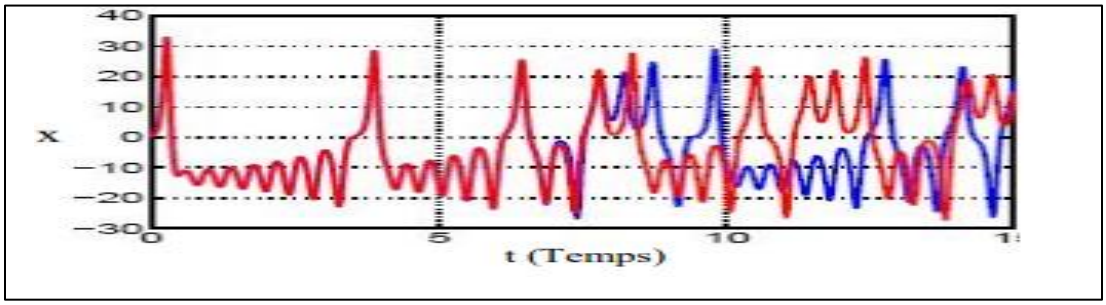


Figure I.2. Evolution temporelle pour deux conditions initiales très proches.

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 à cet état décrit une trajectoire, appelé également une orbite [10].

L'observation des divers régimes dynamiques possibles peut aussi se faire dans l'espace des phases. Dans le cas des dynamiques à retard, celui-ci est, a priori, infini, et ne peut être réellement utile pour une observation. A titre indicatif, nous avons quand même représenté dans la figure (I.3) trois exemples de régime dynamique dans un espace des phases reconstruit en dimension finie par la méthode dite des retards [11] ; les coordonnées de l'espace des phases correspondent à la variable dynamique retardée avec des valeurs différentes soient ω(t), ω(t -$T1$) et ω(t-$T2$) ($T1$= T, $T2$ = 2T, $T1$et $T2$ a priori quelconque).

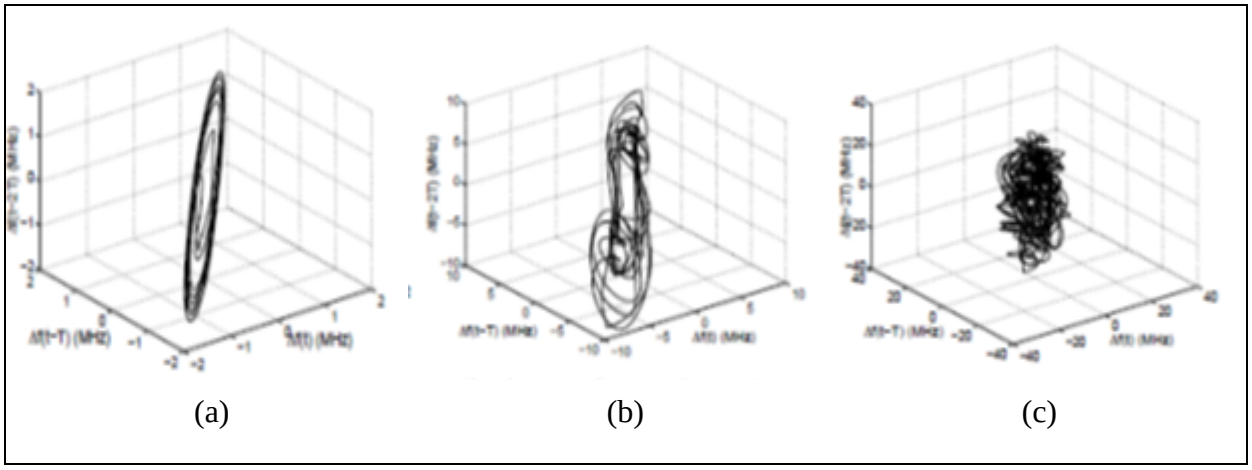


Figure I.3. Espaces des phases pour différents gains β et φ = π/4 rad : (a) périodique (β=1) ; (b) bi périodique (β=1.1) ; (c) chaotique (β=1.5).

I.5 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 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≥2) :** cet attracteur correspond à un régime quasi-périodique ayant r fréquences de base indépendantes (cas le plus simple r=2, dynamique bi périodique).

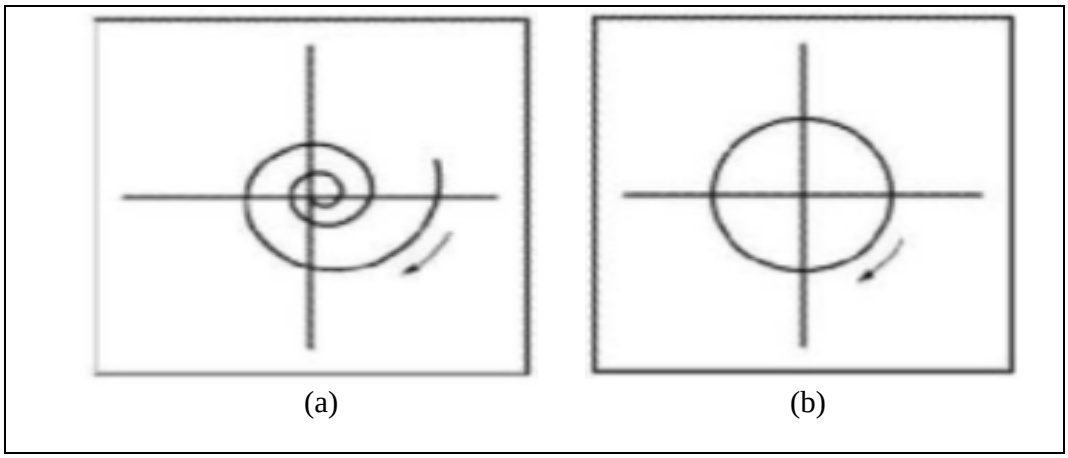
• **L'attracteur étrange :** cet attracteur est associé à un comportement quasi-aléatoire dit chaotique, caractérisé par un spectre de puissance continue et une fonction d'autocorrélation s'annulant très rapidement. Contrairement aux signaux périodiques (quasi-périodiques) pour laquelle la similitude 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'autocorrélation 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 inférieure à celle de l'espace des phases [12].

• Le chaos est caractérisé par la sensibilité aux conditions initiales.



(a) (b)

Figure I.4. Exemples d'attracteurs : (a) attracteur fixe ; (b) attracteur cyclique.

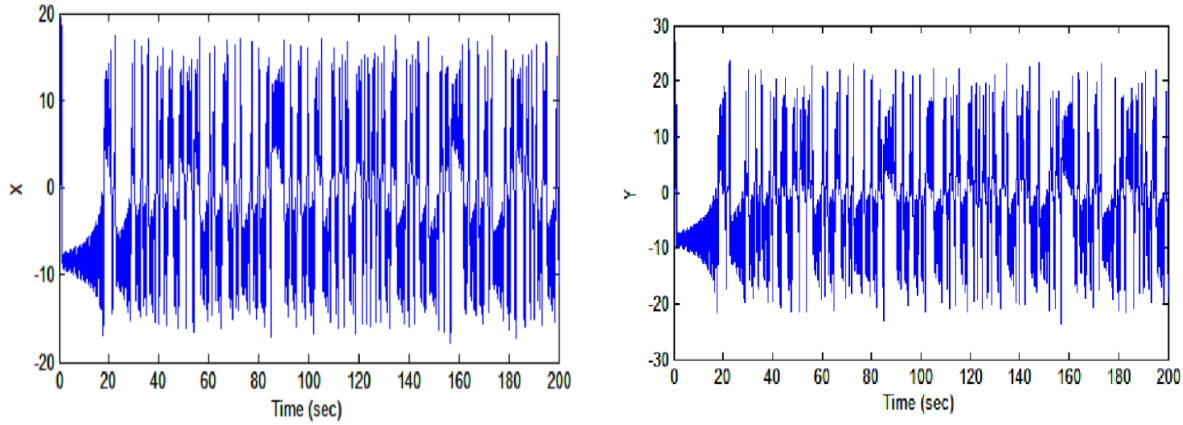
I.5.1. Attracteur étrange de Lorenz

Le météorologue Edward Lorenz a fait un système dynamique continu qui résume l'ensemble des prévisions météorologiques en trois équations différentielles qui sont :

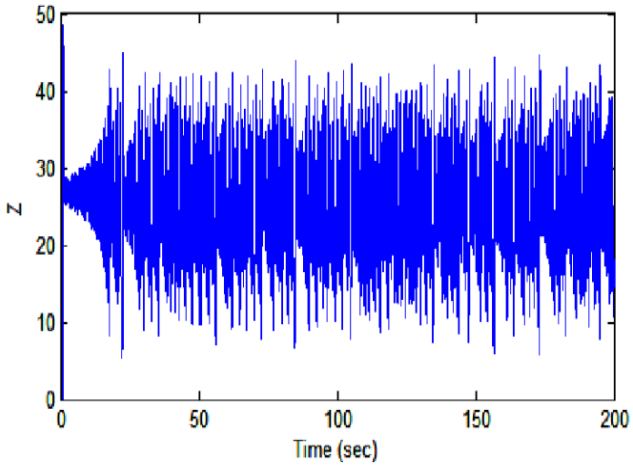
$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = x(\rho - z) - y \\ \dot{z} = xy - \beta z \end{cases} \tag{I.5}$$

Où x, y, z sont les variables d'état du système, et β, ρ, σ sont les paramètres de système [13].

La représentation graphique de ce système est donnée dans les figures (I.5) et (I.6), où on voit les états chaotiques, et l'attracteur du système de Lorenz. Pour (σ=10 ; ρ=28 ; β=83), et les conditions initiales [x (0) =0 ; y (0) = 1 ; z (0) =20].



(a) (b)



(c)

Figure I.5. Les états chaotiques du système de Lorenz : (a) la variable d'état x ; (b) la variable d'état y ; (c) la variable d'état z.

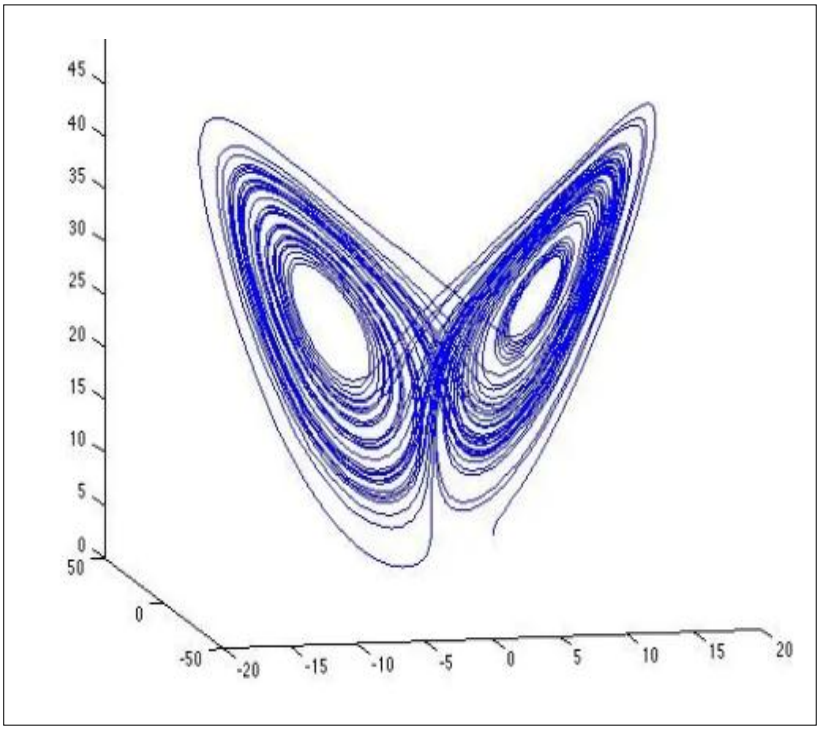


Figure I.6. Attracteur étrange de Lorenz.

I.5.2 Attracteur étrange de Rössler

Otto Rössler a conçu son attracteur en 1976 dans un but purement théorique, mais ces équations se sont avérées utiles dans la modélisation de l'équilibre dans les réactions chimiques. Physiquement, les états x, y et z représentent les concentrations des substances d'une réaction chimique. Les paramètres intervenants a, b et c sont positifs.

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \tag{1.6}$$

Où x, y, z est les variables d'état et a, b, c sont les paramètres du système [14]. La représentation graphique de ce système est donnée dans les figures (I.7) et (I.8), où on voit les états chaotiques et l'attracteur de Rössler pour $(a = 0.2; b = 0.2; c = 5.7)$, avec les conditions initiales $x(0) = y(0) = z(0) = 0.01$.

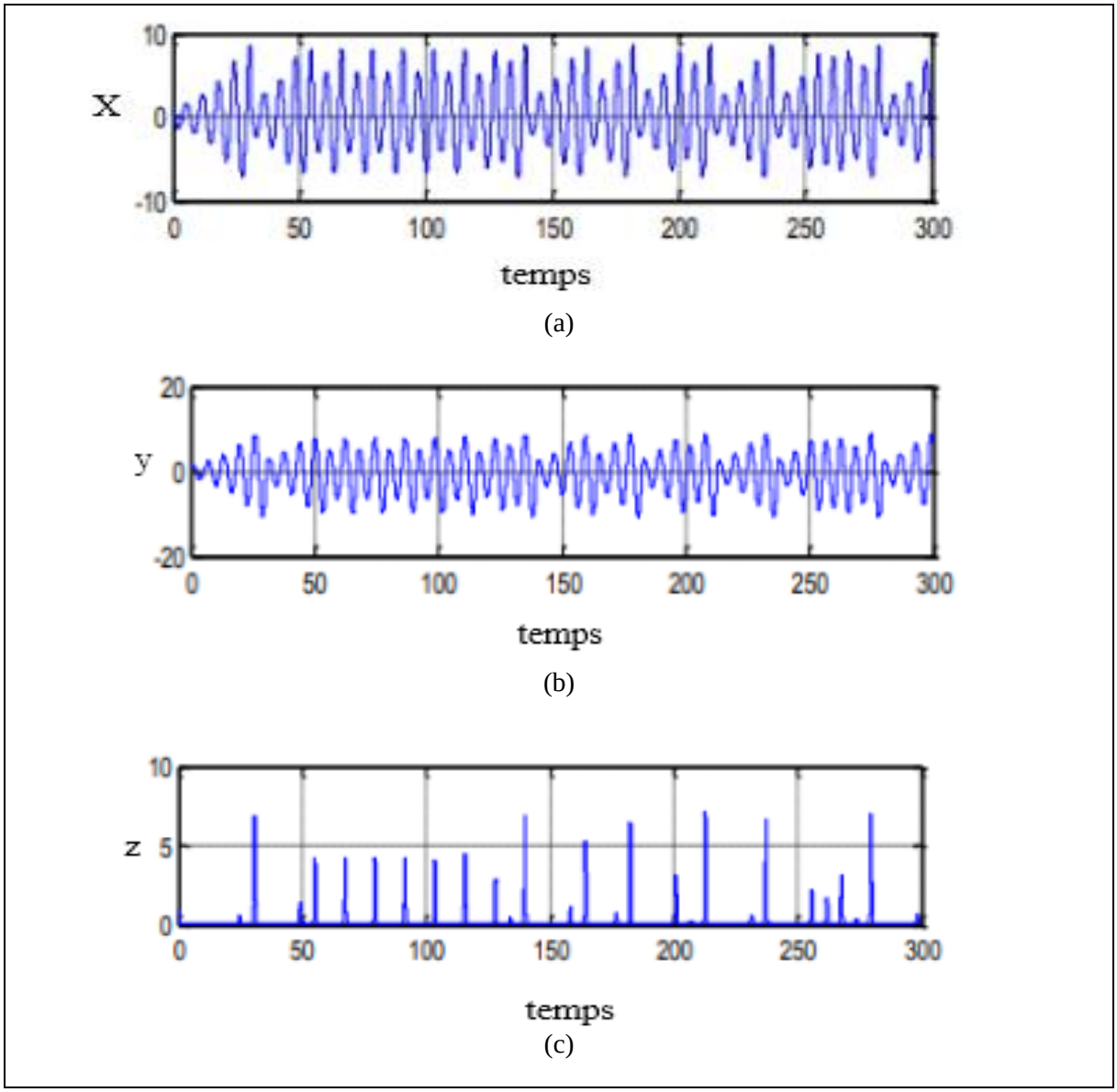


Figure I.7. Les états chaotiques du Rössler : (a) la variable d'état x ; (b) la variable d'état y ; (c) la variable d'état z.

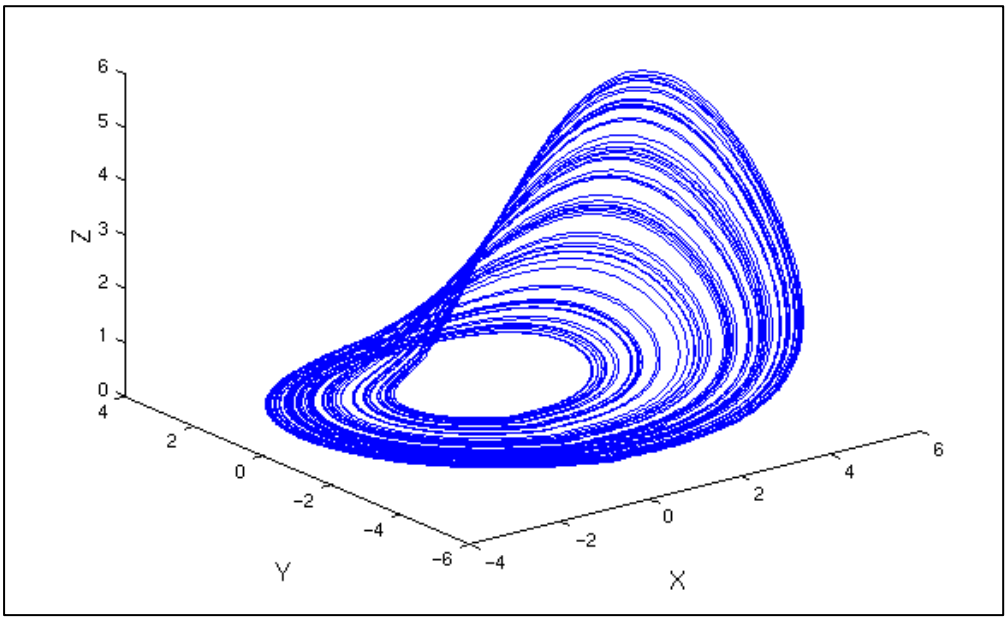


Figure I.8. Attracteur étrange de Rössler.

I.5.3 Dimension de 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 hypers cubés d'arrêter et examiner le nombre minimum N(ε) de cubes nécessaires à cette opération [15].

La dimension fractale de l'attracteur est donné par la dimension de Hausdorff Besicovutch.

$$D = \lim_{\varepsilon \to 0} \frac{\ln N(\varepsilon)}{ln\frac{1}{\varepsilon}} \qquad \text{(I.7)}$$

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'autocorrélation 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.6 Exposants de Lyapunov

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaie 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 [16,17].

Soit $f : \mathbb{R} \rightarrow \mathbb{R}$ une fonction de classe C_1. Pour chaque point x_0 on définit un exposant de Lyapunov (x_0) comme suit :

$$\lambda\,(x_0) = \lim_{n\to\infty} \sup \frac{1}{n} \log\,(|(\,f^n\,)'(\,x_0)\,|) = \lim_{n\to\infty} \sup \frac{1}{n} \sum_{j=0}^{n-1} \log(|f'(x_j)|), \qquad \text{(I.8)}$$

Avec $x_j = f_j\,(x_0)$

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 :

$$|Z_2| \approx e^{\lambda \Delta_t} |Z_1| \qquad \text{(I.9)}$$

Où λ est l'exposant de Lyapunov

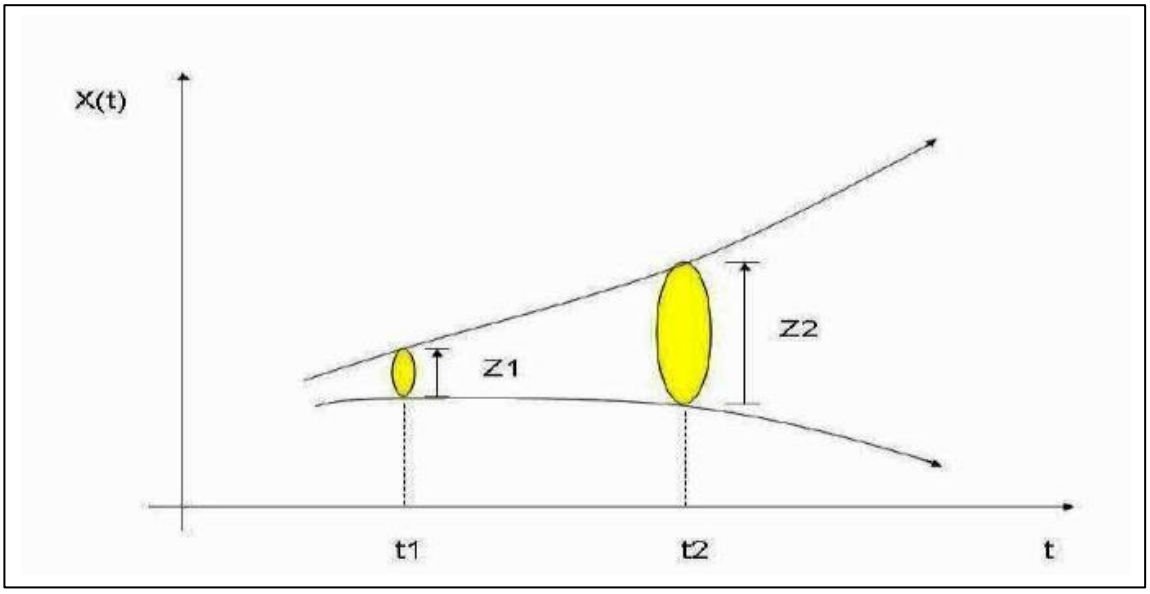


Figure I.9. Divergence de deux trajectoires dans le plan de phase.

Les exposants de Lyapunov sont une généralisation des valeurs propres pour le point fixe et des multiplieurs caractéristiques pour les solutions périodiques. 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 le tableau (I.1).

Tableau I.1. Classification des régimes permanents selon les exposants de Lyapunov.

Exposants de Lyapunov	**Attracteur**	**Dimension**
$\lambda_n \leq \cdots \leq \lambda_1 < 0$	L'existence d'un point fixe.	0
$\lambda_1 = 0\,; \lambda_n \leq \cdots \leq \lambda_2 < 0$	L'attracteur est une orbite fermée.	1
$\lambda_1 = \lambda_k = 0$; $\lambda_n \leq \cdots \leq \lambda_{k+1} < 0$	L'attracteur est quasi périodique (k fréquences).	K
$\lambda_1 > 0; \sum_{i=1}^{n} \lambda_i < 0$	L'attracteur est chaotique.	Non entier.
$\lambda_1 > \cdots > \lambda_k > 0$ $\sum_{i=1}^{n} \lambda_i < 0$	L'attracteur est hyper chaotique.	Non entier

I.7 Section de Poincaré

Henri Poincaré a apporté des contributions très utiles pour l'étude des systèmes chaotiques, parmi ces contributions on trouve les sections de Poincaré. Faire une section de Poincaré revient à couper la trajectoire dans l'espace des phases, afin d'étudier les intersections de cette trajectoire (en dimension trois, par exemple) avec un plan. On passe alors d'un système dynamique à temps continu à un système dynamique à temps discret. Les mathématiciens ont bien sûr démontré que les propriétés du système sont conservées après la réalisation d'une section de Poincaré judicieusement choisie [18].

I.8 Bifurcation et Route vers chaos

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique [17].

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. Pour une meilleure compréhension de cette partie,

nous allons présenter le diagramme de bifurcation de la fonction logistique, dont l'expression s'écrit comme suite [19] :

$$F=[0;1]\to[0;1]x_{k+1}=F(x_k)=r.x_k(1-x_k) \qquad \text{(I.10)}$$

Avec r est défini dans $[0;4]$, et $k=1,2,...$

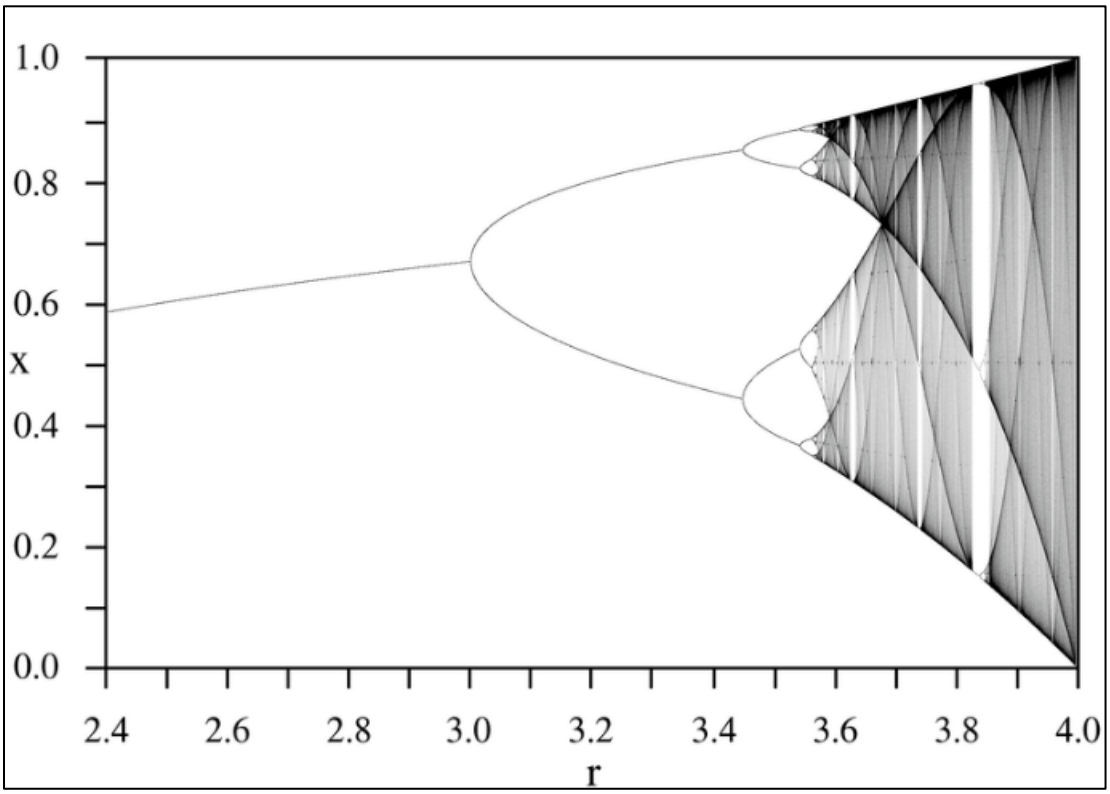


Figure I.10. Diagramme de bifurcation de la fonction logistique.

Dans le diagramme de bifurcation de la fonction logistique représenté dans la figure (I.10), on remarque que le système dynamique non linéaire se comporte périodiquement si $r\in[2.4;3]$, et se comporte quasi-périodiquement (plusieurs périodes) si $r\in]3;3.373]$. Dans le cas où $r\in]3.373;4]$, on remarque une infinité des périodes cela veut dire que le système se comporte chaotique.

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 ont permis de classer certains phénomènes expérimentaux comme chaotiques

déterministes. On obtient l'apparition du chaos en modifiant la valeur d'un paramètre du système que ça soit de manière théorique ou expérimentale.

I.8.1 Le doublement de période

L'augmentation d'un paramètre provoque, pour un système périodique, l'apparition d'un doublement de période, la période se multiplie ainsi en 2, 4, 8, 16, …

A partir d'une certaine valeur du paramètre, les doublements étant de plus en plus rapprochés, on tend vers un point auquel on obtiendrait hypothétiquement une fréquence infinie et c'est à ce moment que le chaos apparait.

I.8.2 L'intermittence

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière.

Le système conserve pendant un certain laps de temps un régime périodique ou pratiquement quasi-périodique, c'est à dire une certaine "régularité", et il se déstabilise, brutalement, pour donner lieu à un comportement chaotique. Il se stabilise de nouveau, pour donner lieu à une autre « explosion chaotique » plus tard.

La fréquence et la durée des phases chaotiques ont tendance à s'accroître plus on s'éloigne de la valeur critique de la contrainte ayant conduit à leur apparition.

I.8.3 La quasi périodicité

Ce troisième scénario fait intervenir pour un système périodique l'apparition d'une autre période dont le rapport avec la première n'est pas rationnel.

I.9 Conclusion

Dans le présent chapitre, quelques définitions et notions sur les systèmes chaotiques ont été présentées. Ces notions seront utilisées par la suite, lors de l'étude de différents comportements de générateur proposé dans le cadre de ce travail.

Chapitre II

Transmission chaotique

II.1 Introduction

La nouvelle révolution industrielle en informatique et dans les télécommunications a abouti au stockage et à la transmission de grandes quantités de données confidentielles et à un souci croissant d'en protéger l'accès. La cryptologie est un moyen de sauvegarder le caractère confidentiel des informations. Elle ne protège pas les communications mais plutôt leurs contenus, ils existent plusieurs méthodes de chiffrage qui sont connues depuis des milliers d'années.

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 devenus sans garantie. En effet, plus les ordinateurs sont puissants, plus les algorithmes de chiffrement sont vulnérables.

La cryptographie chaotique, en contrepartie, 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.

II.2 Objectifs des crypto-systèmes

Le crypto-système assure et garantit :

- **La confidentialité:** assurer que le contenu d'une communication ne peut pas être consulté par des personnes non autorisées.
- **L'authenticité:** fait référence pour la validation de la source du message pour assurer quel expéditeur est correctement identifié.
- **L'intégrité:** garantir que le message n'a pas été modifié pendant la transmission.
- **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.

II.3 Cryptographie

C'est l'ensemble des processus de verrouillage (sécurité des données) visant à protéger l'accès à certaines données, à garantir la confidentialité et l'intégrité des informations. La cryptographie recouvre les méthodes rendant des informations inaccessibles aux personnes non autorisées. L'émetteur d'une information peut ainsi être certain de l'identité du destinataire et vice versa. La cryptographie repose sur l'emploi de formules mathématiques souvent complexes, ainsi que des algorithmes. Ceux-ci servent à coder des informations qui seront ensuite décodées avec une clé, en utilisant des algorithmes, on verrouille les données, c'est-à-

dire qu'on les transforme, ou les inclut dans d'autres données pour les protéger [20]. Il existe deux classes de système de cryptographie :

II.3.1 Les systèmes symétriques ou la clé secrète

Dans cette classe, la même clé est utilisée pour encoder et décoder, appelé aussi (le chiffrement symétrique), est la plus ancienne forme de chiffrement, l'expéditeur et le destinataire utilisent des clés identiques. Cette clé est sélectionnée avant d'échanger les messages. Ainsi, si la clé est dévoilée, n'importe qui peut lire le message, la figure (II.1) présente le principe de chiffrement symétrique où l'algorithme à clé secrète.

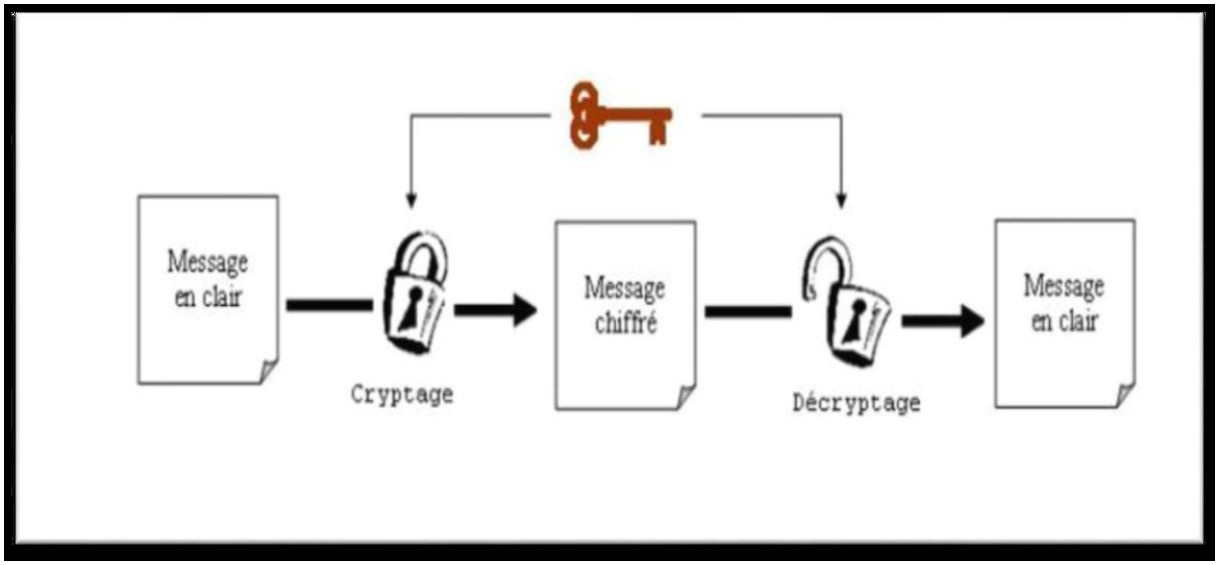


Figure II.1. Le principe de chiffrement symétrique.

II.3.2 Les systèmes asymétriques où la clé publique

La clé qui sert à coder est totalement différente de celle utilisée pour le décodage, appelé aussi (le chiffrement asymétrique), a été proposé par Diffie et Hellmanen en 1976 [21]. Cet algorithme utilise deux clés différentes, la clé de chiffrement peut être rendue publique, par contre dans la réception seule celui qui possède la clé de déchiffrement peut déchiffrer le message. La figure (II.2) présente le principe de chiffrement asymétrique.

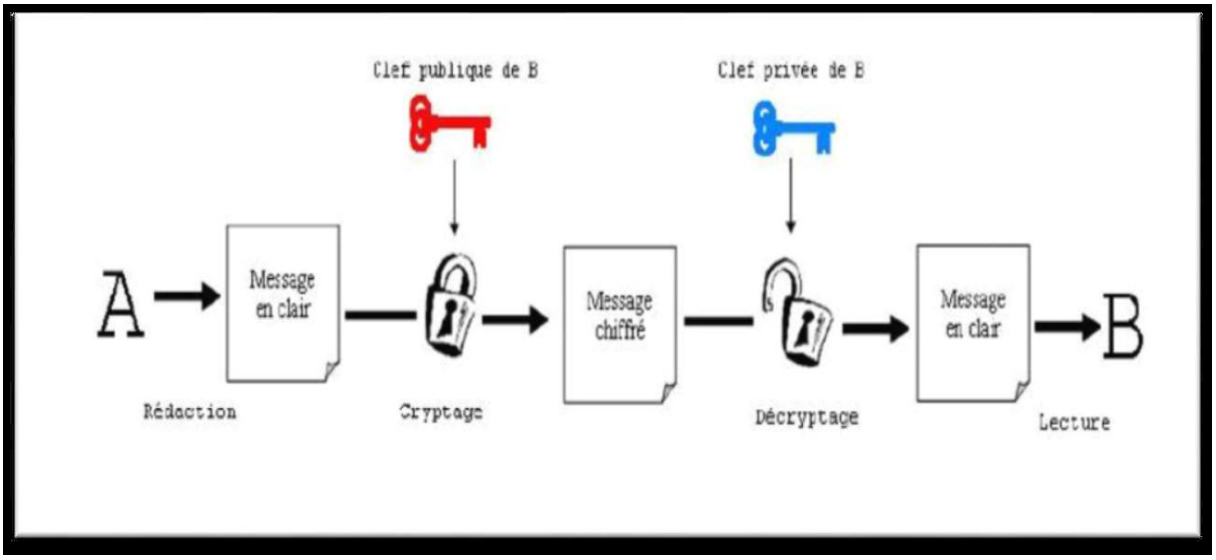


Figure II.2. Le principe de chiffrement asymétrique.

II.4 Cryptanalyse

La cryptographie permet de préserver les données confidentielles de l'indiscrétion des attaquants comme les adversaires, espions, décrypteurs, ou les ennemis. A l'inverse, la cryptanalyse est l'étude des probabilités de succès des attaques possible sur les systèmes cryptographiques dans le but de trouver leurs faiblesses [22].

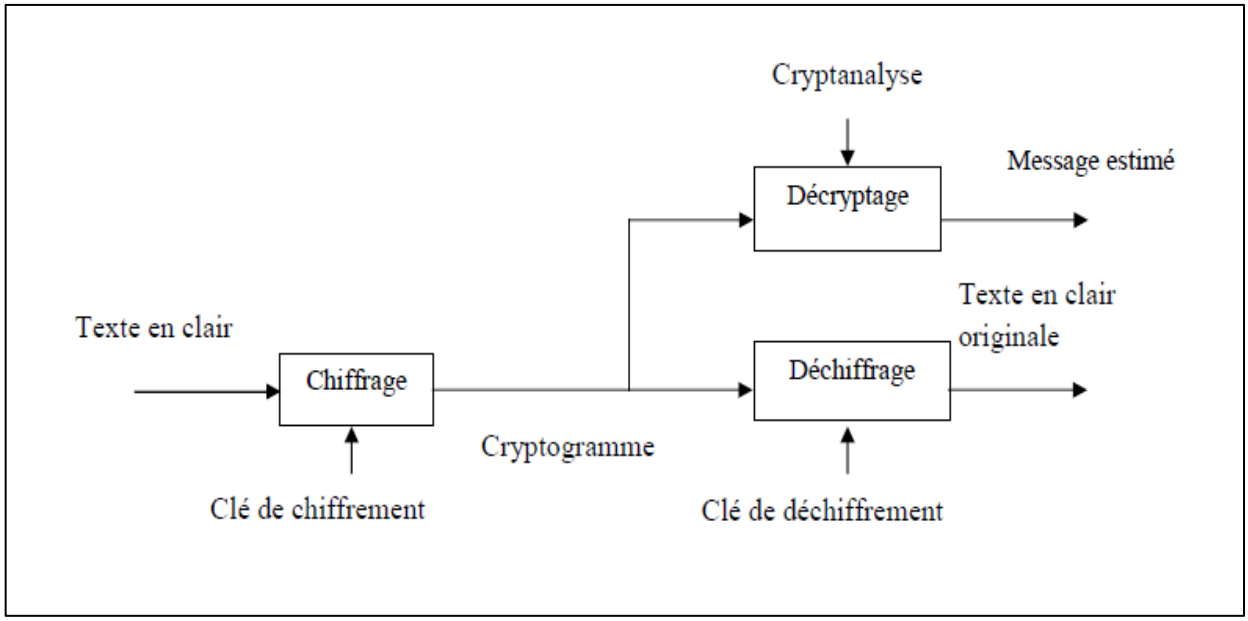


Figure II.3. Principe de cryptographie et de cryptanalyse.

II.5 Techniques de chiffrement par chaos

Dans cette partie, nous développons trois méthodes de chiffrement à base des systèmes chaotiques.

II.5.1 Chiffrement par addition

Dans le cryptage additif, le message est tout simplement additionné au signal chaotique, et le signal résultant est envoyé au récepteur. En conséquence, après la synchronisation, le message confidentiel peut être récupéré par une simple opération de soustraction entre la sortie du récepteur et le signal émis sur le canal public.

Le principal avantage de cette méthode réside dans la simplicité du cryptage, on peut souligner que cette technique peut être appliquée pour des messages continus ou discrets. Dans les deux cas, il est impératif que l'amplitude du message original soit plus petite que celle de la porteuse chaotique, d'une part pour ne pas perturber l'établissement de la synchronisation au niveau du récepteur, et d'autre part pour garantir le secret de la transmission [23].

Dans tous les cas, à cause de la présence du message, la synchronisation ne peut être parfaite. En outre, la fréquence du message doit être comprise dans le spectre du signal chaotique [24].

Un autre problème qui se pose naturellement concerne la présence d'un bruit additif au niveau du canal de transmission. Dans ce cas, il faut que l'amplitude du message soit plus grande que celle du bruit. Il y a donc un compromis à trouver entre la sécurité de la transmission, et la robustesse au bruit. La figure (II.4) montre en détails le principe de cryptage par addition [25].

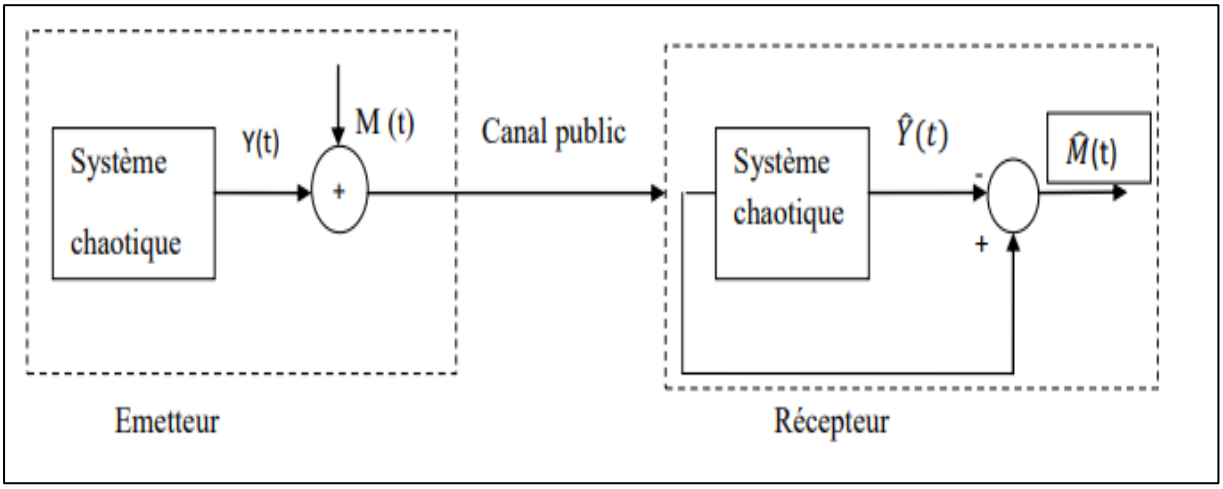


Figure II.4. Chiffrement par addition.

II.5.2 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 représenté dans la figure (II.5).

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre (s) impose à la trajectoire de changer continument 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 « classiques » [26].

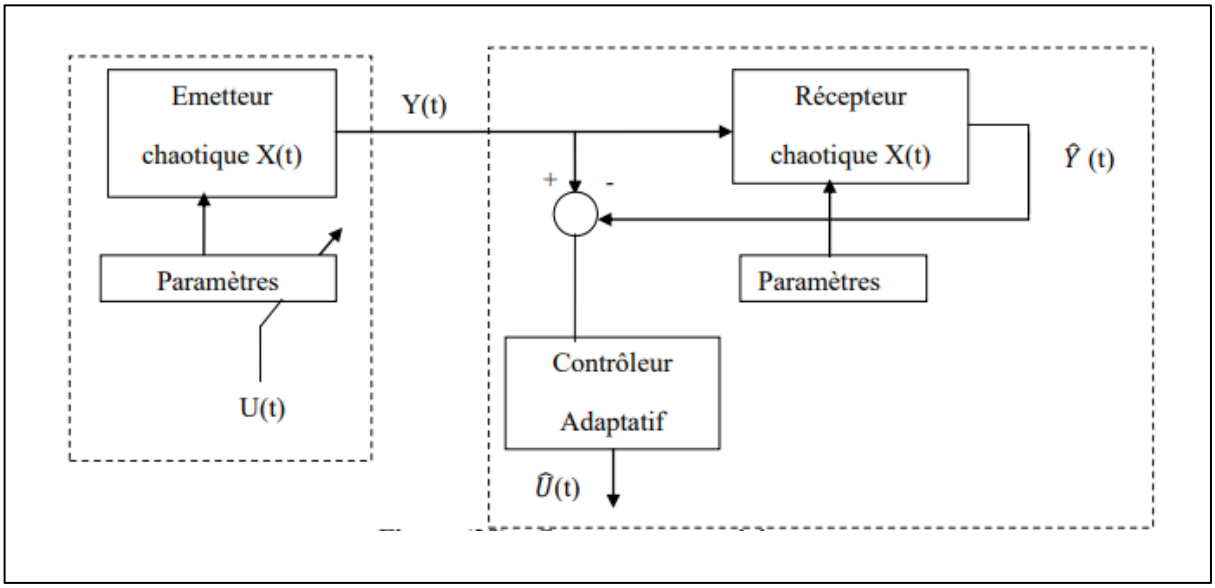


Figure II.5. Chiffrement par modulation.

II.5.3 Chiffrement par commutation

Cette méthode exige que le message à transmettre soit en binaire. Le diagramme de cette approche est illustré dans la figure (II.6) où une opération de commutation est employée selon la valeur du message binaire :

Si sa valeur est 0, alors le système chaotique 1 est choisi et le signal de sortie est transmis, sinon c'est la sortie du système chaotique 2 qui est transmise. Dans ce sens, le message binaire commute avec l'émetteur entre deux attracteurs étranges correspondants aux deux systèmes chaotiques [26].

Du coté récepteur, il y a deux sous-systèmes chaotiques 3 et 4 qui correspondent respectivement à 1 et 2. Supposant que le canal soit parfait, et que le signal transmis est 0 alors le sous-système 3 se synchronisera avec le système chaotique 1, mais le sous-système 4 ne pourra pas être synchronisé, selon les erreurs de synchronisation (1,3) et (2,4), le signal pourra être récupéré avec succès [27,28].

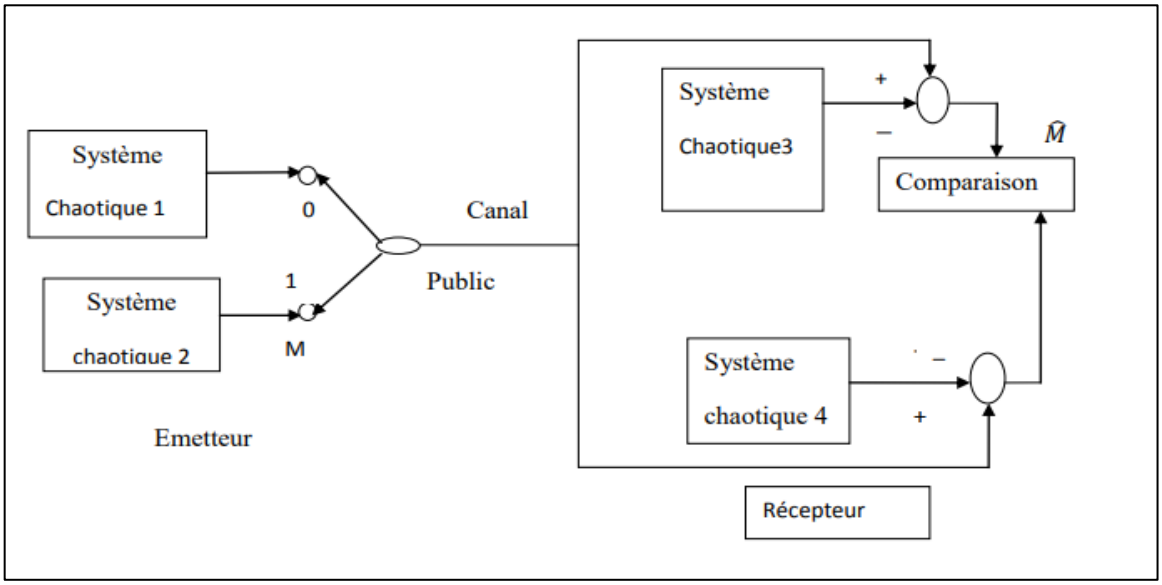


Figure II.6. Chiffrement par commutation.

II.6 Généralités sur la synchronisation des systèmes chaotiques

L'utilisation du chaos dans les systèmes de télécommunication a été rendue possible depuis la maitrise de la synchronisation des systèmes chaotiques. Un signal chaotique se présente sous forme d'un bruit blanc dans les deux domaines temporel et fréquentiel. Ce qui différencie un signal chaotique d'un bruit aléatoire est la notion de déterminisme. En effet, le bruit ne peut être décrit que comme un processus aléatoire alors qu'un système chaotique est représentable par des équations différentielles. Ainsi il est possible de synchroniser deux systèmes chaotiques.

La synchronisation c'est un phénomène qui se produit lorsque deux systèmes dynamiques identiques qui s'évoluant en fonction du temps, elle consiste à synchroniser est rapprocher les trajectoires des deux systèmes jusqu'à ce qu'ils deviennent confondus. La synchronisation obéis à la plus populaire des configurations de synchronisation ou cette dernière consiste à obliger un système dynamique dit esclave à se synchroniser (suivant la même trajectoire) avec un deuxième système dynamique dit maître [29].

II.6.1 Méthodes de synchronisation

Le concept de synchronisation repose sur le constat qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. Il est donc possible de construire une réplique identique à ce système et d'essayer de synchroniser de façon que les deux signaux chaotiques issus des deux exemplaires soient identiques.

Il existe deux classes de la synchronisation suivant la manière par laquelle les deux systèmes chaotiques sont couplés. Supposons qu'ils sont identiques oscillant de façon totalement indépendante. Les deux systèmes finiront par présenter un comportement commun : il est possible de coupler les systèmes chaotiques dans un sens (couplage unidirectionnel) ou dans les deux sens (couplage bidirectionnel).

II.6.1.1 Couplage unidirectionnel

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques ***a*** et ***b*** est réalisé à l'aide d'un élément fonctionnant dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur [30].

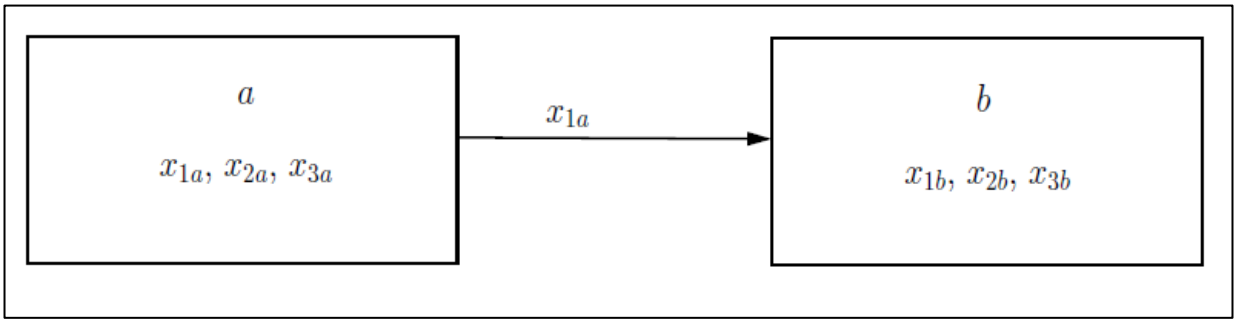


Figure II.7. Couplage unidirectionnel.

II.6.1.2 Couplage bidirectionnel

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques ***a*** et ***b*** est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance [10].

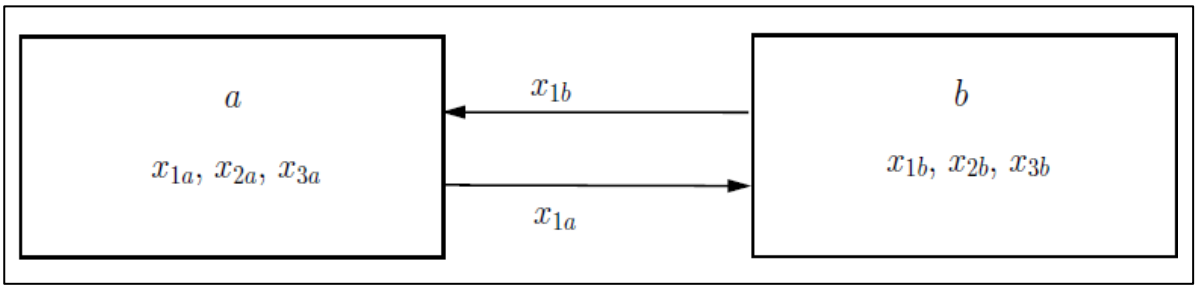


Figure II.8. Couplage bidirectionnel.

Les deux méthodes de synchronisation expliquées sont basées sur l'utilisation de systèmes identiques. Toutefois, ceci n'est pas toujours réalisable en pratique. Un petit écart peut jouer sur les comportements des deux circuits et détériorer le phénomène de synchronisation.

II.6.2 Différents régimes de synchronisation

II.6.2.1 Synchronisation généralisée

La synchronisation généralisée est considérée comme une généralisation de la synchronisation complète pour synchroniser des systèmes chaotiques de modèles différents. Elle se manifeste par une relation fonctionnelle entre deux systèmes chaotiques couplés [31].

II.6.2.2 Synchronisation retardée

Dans cette synchronisation l'état du système esclave tend vers l'état décalé dans le temps du système maitre c'est-à-dire :

$$\lim_{n\to\infty} \|x'(t) - x(t - \tau) = 0\| \qquad \text{(II.1)}$$

Où x(t) est l'état du système émetteur, x′ (t) est l'état du système récepteur et τ est un retard positif [32].

II.6.2.3 Synchronisation en boucle fermée

L'idée de la synchronisation par boucle fermée c'est de corriger le comportement du système récepteur en fonction d'une erreur qu'on injecte à ce dernier, cette erreur est due entre le signal transmis par le premier système et le signal régénéré par l'autre. La figure (II.9) indique un schéma simplifié de la synchronisation par boucle fermée.

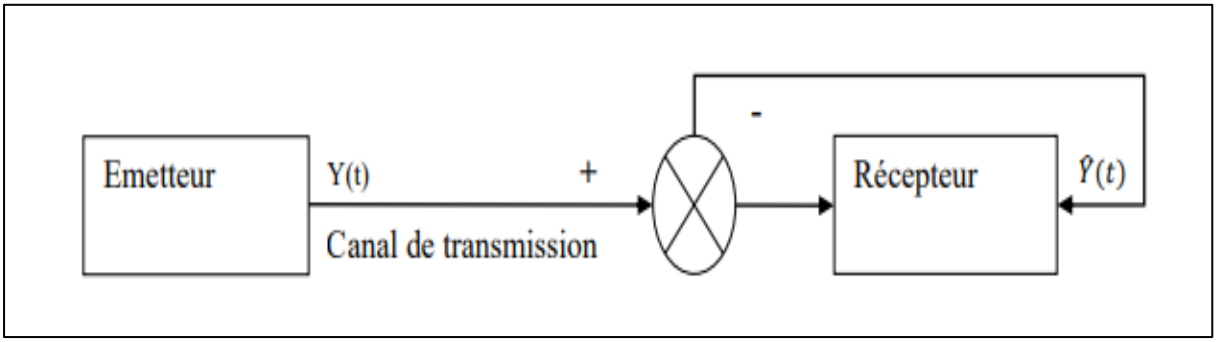


Figure II.9. Synchronisation par boucle fermée.

II.6.2.4 Synchronisation projective

Dans cette méthode, l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur, Donc il existe a et τ tell que :

$$\lim_{n\to\infty} \|\hat{x}1\,(t) - ax(t - \tau)\| = 0 \qquad \text{(II.2)}$$

Où a est le facteur d'échelle, x(t) est l'état du système émetteur, $\hat{x}(t)$ l'état du système récepteur, τ est un retard positif. Ce type de synchronisation est utilisé pour des systèmes partiellement linéaires et permet de synchroniser à un facteur prés les états qui ne peuvent être synchronisée.

II.6.2.5 Synchronisation de phase

Pour deux systèmes périodiques de phase $Ø_1$ et $Ø_2$, la synchronisation peut être exprimé par la relation suivante :

$$|nØ_1 - mØ_2| < c \qquad \text{(II.3)}$$

Avec *n*, *m* sont des entiers naturels et *c* est une constante positive. Ce mode de synchronisation permet de définir la phase d'un système chaotique. On peut mentionner le signal analytique et Ψ (t) une fonction complexe définie comme suit :

$$\Psi(t) = s(t) + j\dot{s}(t) = A(t)e^{jØ(\tau)} \qquad \text{(II.4)}$$

Où s(t) est la transformée de Hilbert de la série temporelle s(t), A(t) est l'amplitude du signal Ψ(t) et Ø(t) sa phase [33].

II.6.3 Synchronisation par observateur

La première approche de synchronisation chaotique a été proposée par Péccora et Carroll, et elle est basée sur la partition du système. Dans cette approche, le système maître est un

système chaotique quelconque et le système esclave est un observateur d'état. D'une manière générale : Un observateur ou reconstructeur d'état est un système dynamique qui permet d'obtenir une estimation de la valeur courante de l'état non mesuré d'un système à partir de ses entrées et sorties ainsi de la connaissance de son modèle dynamique qui sont les seules informations disponibles. Théoriquement, le problème de la conception d'un observateur pour un système (non linéaire) est défini comme suit :

$$\|\mathbf{x(t)} - \mathbf{\hat{x}(t)}\| \rightarrow \mathbf{0 \ \ Quand \ \ t} \rightarrow \infty \qquad \textbf{(II.5)}$$

Où $x(t)$ est l'état du système et $\hat{x}(t)$ est l'état estimé.

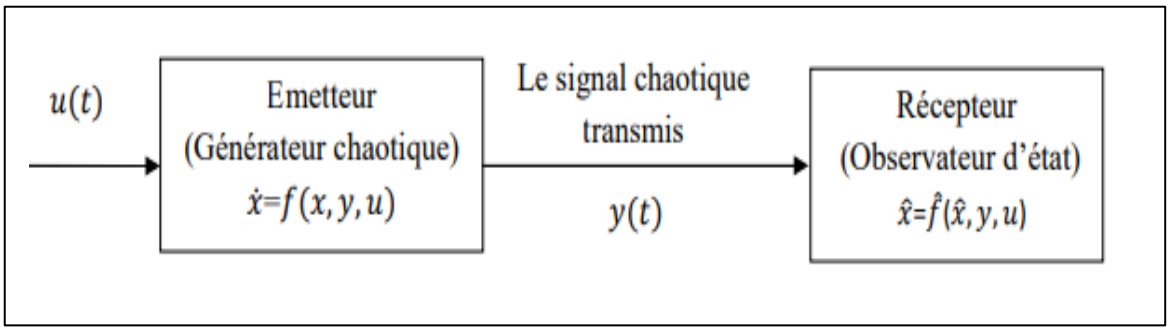


Figure II.10. Principe de synchronisation à base d'observateurs

La synchronisation peut également être réalisée en employant un observateur. L'observateur est une méthode typique afin d'estimer les états inconnus d'un système dynamique qui ne peuvent pas être mesurés directement.

Notre objectif consiste à concevoir un système de transmission sécurisée en utilisant les systèmes chaotiques. L'émetteur est composé d'un système chaotique en temps continu. Au niveau de la réception, un observateur impulsif en temps continu est conçu pour reconstituer les états chaotiques et récupérer le message envoyé.

Une fois que la synchronisation entre le récepteur et l'émetteur est réalisée, il est possible d'utiliser ce phénomène pour transmettre une information m(t). Il existe pour cela plusieurs techniques qui permettent de plus une transmission sécurisée. Il s'agit donc d'une méthode de cryptage basée sur l'utilisation des signaux générés par des systèmes dynamiques.

II.7 Conclusion

Ce chapitre a comme objectif de faire le lien entre les systèmes dynamiques chaotiques et le domaine des télécommunications. En première lieu, nous avons abordé la cryptographie chaotique et la cryptanalyse et aussi les différentes techniques utilisées dans ce domaine. En

dernier lieu, nous nous sommes intéressés à la synchronisation des systèmes chaotiques où nous avons présenté les différentes méthodes de synchronisation.

Chapitre III

Conception et simulation d’un gènèrateur pour les transmissions chaotiques

III.1 Introduction

Dans le premier et deuxième chapitre, nous avons passé en revue les caractéristiques les plus importantes des systèmes chaotiques et comment ils sont utilisés pour sécuriser les systèmes de communication. Grâce à ces propriétés uniques, ces systèmes sont devenus l'objet de nombreuses recherches. En 1983, le premier générateur chaotique proposé appelé circuit Chua, a été largement utilisé dans de nombreux domaines scientifiques tels que la médecine et l'économie ..., mais ce circuit n'a pas été largement utilisé dans le domaine de la sécurité des systèmes de communication, en raison de ses de faibles caractéristiques spectrales, ce qui est dû à sa conception, qui base principalement sur des amplificateurs opérationnels [34]. Afin d'améliorer les caractéristiques spectrales, le chercheur Kennedy en 1994 a exploité l'oscillateur de Colpitts comme un générateur chaotique, cet oscillateur a été construit sur la base d'un transistor bipolaire de type 2N2222, et donc il permettait de générer des oscillations chaotiques dans la gamme fréquentielle de 10 MHz jusqu'à 200 MHz [35]. Les résultats obtenus utilisant l'oscillateur n'étaient pas très convaincants, ce qui a conduit à lui apporter des modifications pour obtenir une nouvelle version améliorée plus efficace que la version standard en adoptant un transistor de type BFG520. Avec cette nouvelle version, des oscillations chaotiques étaient générées de 300 MHz jusqu'à 2 GHz [36,37]. Dans ce troisième chapitre, nous allons commencer tout d'abord par exposer les applications que nous viserons à les sécuriser. Ensuite nous présenterons quelques circuits chaotiques proposés dans la littérature, ainsi que ses modèles mathématiques, puis proposer un générateur chaotique basé sur la combinaison de deux versions de Colpitts (standard et amélioré). Ce nouvel oscillateur peut générer des oscillations chaotiques jusqu'à 6 GHz.

III.2 Les applications de communication visées

Dans cette partie, nous passerons en revue les applications les plus importantes que nous ciblons à sécuriser en utilisant l'oscillateur proposé dans le cadre de ce travail.

III.2.1 La téléphonie mobile

La téléphonie mobile, ou téléphonie cellulaire est un moyen de télécommunication, plus précisément de radiocommunication, par téléphone mobile. Ce moyen de communication s'est largement répandu à la fin des années 1990. La technologie associée bénéficie des améliorations des composants électroniques, notamment leur miniaturisation, ce qui permet aux téléphones d'acquérir des fonctions jusqu'alors réservées aux ordinateurs.

La téléphonie mobile est fondée sur la radiocommunication, c'est-à-dire la transmission de la voix et de données à l'aide d'ondes radioélectriques (fréquences dans les bandes UHF allant de 700 à 2 600 MHz) entre une station de base qui peut couvrir une zone de plusieurs dizaines de kilomètres de rayon et le téléphone mobile de l'utilisateur.

III.2.1 Les bandes ISM

Les bandes ISM (Industriel, Scientifique et Médical) sont des bandes de fréquences qui peuvent être utilisées dans un espace réduit pour des applications industrielles, scientifiques, médicales, domestiques ou similaires, à l'exception des applications de radiocommunication et de radiorepérage pour lesquels la directive RED est applicable . Les bandes de fréquences ISM sont aussi utilisées pour des applications de télécommunications, plus particulièrement de courte portée.

III.2.1.1 Bande 2.4 GHz

Dans l'Union européenne, la bande ISM principale utilisée est la bande de fréquence de la gamme des UHF allant de 2 400 à 2 483 MHz (bande S). Les réseaux WLAN et les dispositifs Bluetooth émettent dans la bande des 2,4 GHz. Outre le Wi-Fi, la bande des 2,4 GHz est réservée à de nombreuses applications publiques et grand public sans fil, les caméras de vidéo-surveillance professionnelles et domestiques, les webcams, les transmetteurs (émetteur/récepteur) de salon audio-vidéo...

III.2.1.2 Bande 5.8 GHz

La bande dite des 5,8 GHz (de 5 150 à 5 350 MHz et de 5 470 à 5 725 MHz) est désormais libre avec des PIRE limitées respectivement à 200 mW (intérieur) et 1 000 mW (extérieur/intérieur). Il y a également des réseaux et dispositifs WLAN dans la bande des 5 GHz (plus précisément 5,150 - 5,725 GHz en Europe) et à une puissance d'émission différente.

III.3 Circuit de Chua

Un circuit électronique doit respecter certaines conditions pour montrer un comportement chaotique, appelés critères chaotiques. Il doit contenir :

- Un élément non linéaire ou plus ;
- Une résistance localement active ou plus ;
- Trois éléments de stockage d'énergie ou plus.

En 1983, l'ingénieur Leon Ong Chua a mis au point le plus simple circuit électronique respectant ces critères. Il comporte deux condensateurs C_1 et C_2, une bobine L, une résistance active G et une diode de Chua N_R, cette diode joue le rôle de l'élément non linéaire dans le circuit de Chua et il est le premier responsable sur la génération du chaos. Quant à sa conception, il est conçu principalement à base des amplificateurs opérationnels [34,38].

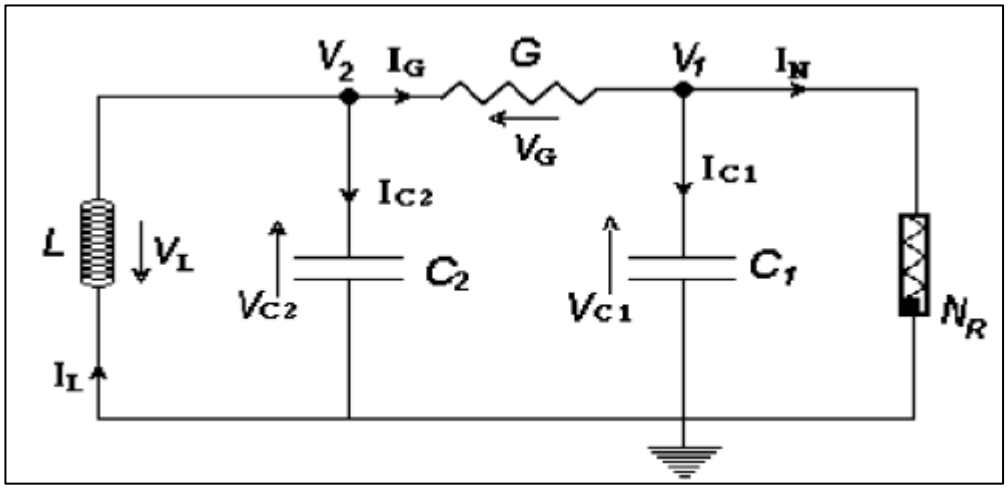


Figure III.1. Circuit de Chua.

En appliquant les lois de Kirchhoff au circuit de Chua représenté sur la figure (III.1), puis en normalisant les équations différentielles résultantes, nous trouvons le modèle mathématique du Chua représenté par l'ensemble d'équations différentielles d'ordre 3 [34] :

$$\begin{cases} \dot{x} = \alpha(y - x - g(x)) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y \end{cases} \quad \text{(III.1)}$$

Avec

$$g(x) = m_1 x + \frac{m_0 - m_1}{2}(|x+1| - |x-1|) \quad \text{(III.2)}$$

$g(x)$ Représente l'élément non linéaire du circuit [38].

III.4 L'oscillateur de Colpitts

La figure (III.2) représente le circuit diagramme de l'oscillateur de Colpitts, où on remarque que c'est une structure en base commune qui permet d'obtenir un gain plus élevé tout en autorisant une bande passante plus large. Le circuit résonant *L-C* est connecté entre le

collecteur et la base du transistor Q dont une fraction de la tension du circuit *L*-*C* est réinjectée au niveau de l'émetteur. Les sources V_0 et I_0 permettent de fixer le point de fonctionnement du transistor. Le choix des valeurs du circuit résonnant détermine la fréquence fondamentale de l'oscillateur.

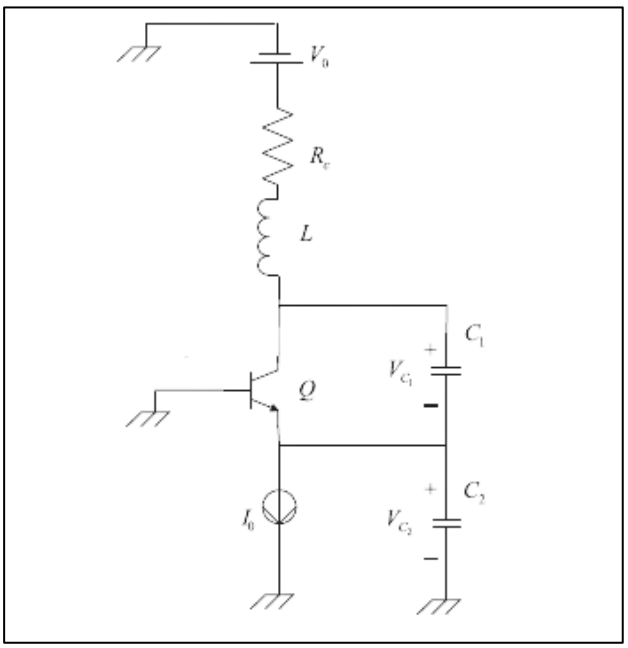


Figure III.2. Oscillateur de Colpitts.

Pour obtenir les équations d'état du l'oscillateur de Colpitts, on passe par les mêmes étapes qu'en appliquant les lois de Kirchhoff et en normalisant les équations obtenues, et donc on trouve le système suivant [35,39,40] :

$$\begin{cases} \dot{x}_1 = \dfrac{g}{Q(1-k)}[-n(x_2)+x_3] \\ \dot{x}_2 = \dfrac{g}{Qk}x_3 \\ \dot{x}_3 = -\dfrac{Qk(1-k)}{g}[x_1+x_2]-\dfrac{1}{Q}x_3 \end{cases} \quad \text{(III.3)}$$

Avec $n(x_2)=\exp(-x_2)-1$ et $k=\dfrac{C_2}{C_1+C_2}$. Le paramètre g est de la boucle de réaction de l'oscillateur lorsque le critère de Barkhausen est satisfait [6]. Et $Q=\dfrac{\omega_0 L}{R}$ est le facteur de qualité du circuit LC non chargé.

III.5 l'oscillateur de Colpitts amélioré

La configuration d'un oscillateur chaotique amélioré est illustrée à la figure (III.3). Nous pouvons voir qu'il est constitué d'un transistor bipolaire BJT comme élément de gain et d'un réseau résonnant comprenant une inductance L et une paire de condensateurs C_1 et C_2. La différence entre l'oscillateur de Colpitts conventionnel et la version améliorée est que l'inductance L est déplacée du collecteur à la base du transistor où elle est en série avec la résistance R_b [36]. Le mécanisme de base de la configuration améliorée est la diminution de l'influence négative du condensateur C_3 (capacité collecteur-base à polarisation nulle). Dans la version standard de Colpitts, le condensateur C_3 met à la masse le nœud du collecteur et agit comme un élément parasite détruisant les oscillations chaotiques. Dans cette nouvelle version, L et R_B protègent C_3 de la masse et réduisent son influence négative [41].

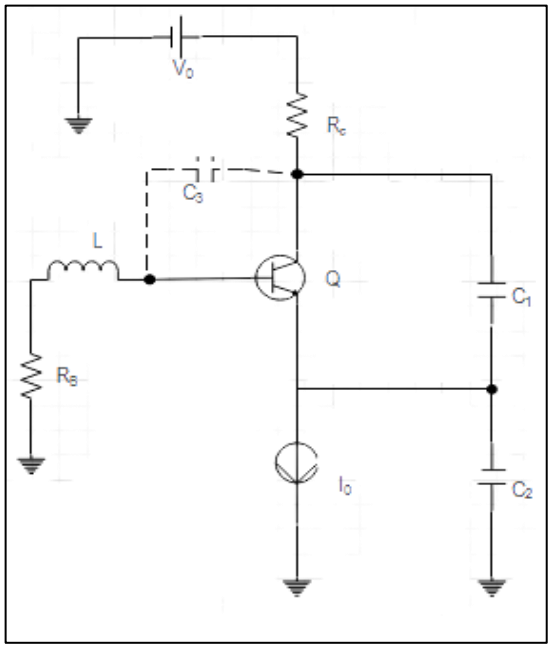


Figure III.3. Oscillateur de Colpitts amélioré.

Le modèle mathématique de cette nouvelle version de Colpitts s'écrit comme suite [36,42] :

$$\begin{cases} \dot{x}_1 = \sigma_1(-x_1 - x_2) + x_4 - \gamma\phi(x_1, x_3) \\ \dot{x}_2 = \varepsilon_1\sigma_1(-x_1 - x_2) + \varepsilon_1 x_4 \\ \dot{x}_3 = \varepsilon_2(x_4 - (1-\alpha)\gamma\phi(x_1, x_3)) \\ \dot{x}_4 = -x_1 - x_2 - x_3 - \sigma_2 x_4 \end{cases} \quad \text{(III.4)}$$

Avec : $\phi(x_1, x_3) = \exp(x_1 + x_3) - 1$, c'est le terme non linéaire pour ce système amélioré, et $t = \tau\sqrt{LC_1}, \rho = \sqrt{L/C_1}, \varepsilon_1 = C_1/C_2, \varepsilon_2 = C_1/C_3, \sigma_1 = \rho/R_C, \sigma_2 = R_B/\rho, \gamma = \rho I_0/V_T$.

III.6 l'oscillateur chaotique proposé

À travers ce travail, nous présenterons une nouvelle conception chaotique qui combine les deux versions précédentes de Colpitts, c'est-à-dire qu'il contient deux inductances la première L_c est placée dans le collecteur et la deuxième L_B dans la base, le circuit diagramme de circuit proposé est représenté dans la figure (III.4).

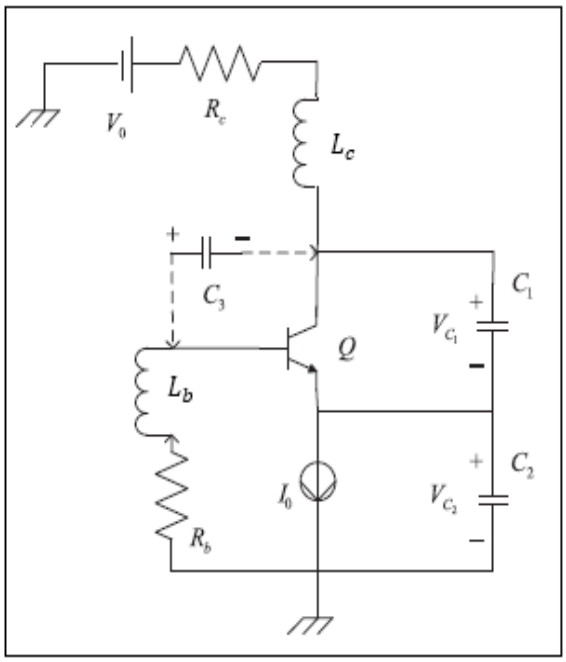


Figure III.4. L'oscillateur chaotique proposé.

III.6.1 Les équations d'états

Afin de dériver un modèle mathématique qui est traitable analytiquement et numériquement, certaines hypothèses utiles [39,43] sont prises en compte. Premièrement, nous supposons linéaires tous les condensateurs, inductances et résistances du réseau de l'oscillateur. Deuxièmement, le transistor Q est modélisé par une résistance non linéaire R_E et une source de courant linéaire contrôlée par le courant, comme le montre la figure (III.5). Nous modélisons la caractéristique du jonction base-émetteur (B-E) avec une fonction exponentielle s'écrit comme suite [43,45] :

$$I_E = \mathrm{f}(V_{BE}) = I_S[exp(V_{BE}/V_T) - 1] \qquad \text{(III.5)}$$

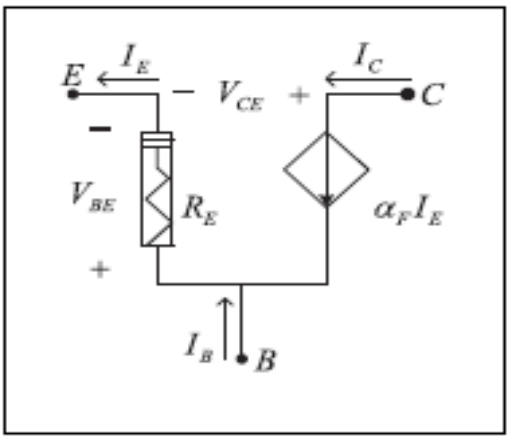


Figure III.5. Diagramme de circuit du modèle BJT.

Où I_E est le courant d'émetteur, V_{BE} est la tension aux bornes de la jonction B-E, α_F est le gain en courant de court-circuit direct de la base commune du transistor ($I_c = \alpha_F I_E$), V_T est la tension thermique, sachant que : V_T = 26 mV à la température (T=300°K).

En désignant par I_{Lc}, I_{Lb} le courant traversant l'inducteur L_c, L_b, et V_{c1}, V_{c2}, V_{c3} les tensions aux bornes des condensateurs C_1, C_2, C_3. Et par l'application des lois de Kirchhoff (La loi des nœuds, la loi des mailles) au schéma de la figure (III.4), on obtient l'ensemble d'équations d'états suivantes :

$$\begin{cases} \mathrm{C_1}\frac{\mathrm{dV_{C1}}}{\mathrm{dt}} = \mathrm{I_{Lc}} + \mathrm{I_{Lb}} - \mathrm{f(V_{BE})} \\ \mathrm{C_2}\frac{\mathrm{dV_{C2}}}{\mathrm{dt}} = \mathrm{I_{Lc}} + \mathrm{I_{Lb}} - \mathrm{I_0} \\ \mathrm{C_3}\frac{\mathrm{dV_{C3}}}{\mathrm{dt}} = \mathrm{I_{Lb}} - (1-\alpha_F)\mathrm{f(V_{BE})} \\ \mathrm{L_c}\frac{\mathrm{dI_{Lc}}}{\mathrm{dt}} = -V_0 - V_{c1} - V_{c2} - R_c\mathrm{I_{Lc}} \\ \mathrm{L_b}\frac{\mathrm{dI_{Lb}}}{\mathrm{dt}} = -V_0 - V_{c1} - V_{c2} - R_c\mathrm{I_{Lb}} \end{cases} \quad \text{(III.6)}$$

Où V_{BE} est la tension base-émetteur exprimée en termes de composantes du vecteur d'état comme suit : $V_{BE} = V_{C1}+V_{C3}$.

III.6.2 Le modèle mathématique normalisé

Afin de normaliser le système des équations différentielles (III.6), nous devons passer par ces étapes :

- Trouver le point d'équilibre ;
- Adopter des nouvelles variables d'états normalisée qui sont x_1, x_2, x_3, x_4, x_5.

Le système (III.6) a un seul point d'équilibre (V_{c1}^0 , V_{c2}^0 , V_{c3}^0, I_{Lc}^0 , I_{Lb}^0) qui est obtenu en mettant le côté droit de (III.6) à zéro, et donc les expressions suivantes sont obtenues :

$$\begin{cases} V_{c1}^0 = V_0 + V_T \ln\left(1 + \frac{I_0}{I_s}\right) + I_0((1-\alpha_F)R_b + \alpha_F R_c) \\ V_{c2}^0 = -V_T \ln\left(1 + \frac{I_0}{I_s}\right) + I_0(1-\alpha_F)R_b \\ V_{c2}^0 = -V_T \ln\left(1 + \frac{I_0}{I_s}\right) + I_0(1-\alpha_F)R_b \\ I_{Lc}^0 = -\alpha_F I_0 \\ I_{Lb}^0 = (1-\alpha_F)I_0 \end{cases} \quad \text{(III.7)}$$

Pour obtenir le système sans dimensions, nous adoptons le changement de variables et de paramètres suivants :

$$x_i V_T = V_{c_i} - V_{c_i}^0; i\epsilon\{1,2,3\}, x_4 V_T = \rho\left(I_{L_c} - I_{Lc}^0\right)$$

$$x_5 V_T = \rho\left(I_{L_c} - I_{Lc}^0\right), t = \tau\sqrt{L_c C_1}, \rho = \sqrt{\frac{L_c}{C_1}}, \varepsilon_1 = \frac{C_1}{C_2} \quad \text{(III.8)}$$

$$\varepsilon_2 = \frac{C_1}{C_2}, \varepsilon_3 = \frac{L_c}{L_b}, \sigma_1 = \frac{R_c}{\rho}, \sigma_2 = \frac{R_c}{\rho}, \gamma = \frac{\rho I_0}{V_T}$$

Et donc, le système ODE sans dimension est le suivant :

$$\begin{cases} \dot{x}_1 = x_4 + x_5 - \gamma\Psi(x_1, x_3) \\ \dot{x}_2 = \varepsilon_1(x_4 + x_5) \\ \dot{x}_3 = \varepsilon_2\left(x_5 + \gamma(1-\alpha)\Psi(x_1, x_3)\right) \\ \dot{x}_4 = -x_1 - x_2 - \sigma_1 x_4 \\ \dot{x}_5 = \varepsilon_3(-x_1 - x_2 - x_3 + \sigma_2 x_5) \end{cases} \quad \text{(III.9)}$$

Où les points indiquent les dérivés par rapport à τ (que nous renommons t dans la nouvelle échelle sans perte de généralité), et $\Psi(x_1, x_3)$ est le seul terme non linéaire dans notre modèle mathématique, exprimé par la formule suivante :

$$\Psi(x_1, x_3) = exp(x_1 + x_3) - 1 \quad \text{(III.10)}$$

III.6.3 Diagramme de bifurcation

On utilisera le diagramme de bifurcation comme moyen d'identifier les différentes transitions vers le chaos, après avoir résolu les équations différentielles précédentes (III.9) à l'aide du MATLAB. Le diagramme de bifurcation est une courbe utilisée pour suivre les différents comportements du système, qu'ils soient périodiques, quasi périodiques ou

chaotiques en modifiant le paramètre de contrôle (dans notre cas, on prend I_0 comme paramètre de contrôle).

Afin de tracer le diagramme de bifurcation de notre nouveau modèle 5D nous allons résoudre numériquement le système ODE (III.9) sous Matlab, en appliquant l'algorithme Runge-Kutta d'ordre 4 (RK-4) avec un pas de temps fixe de $\Delta t=0{,}001$, puis nous désignons les maximas locaux de la variable d'état x_1 en fonction du paramètre de contrôle de bifurcation γ (le seul paramètre directement lié au courant I_0) qui varie de 0 à 30 avec un pas de 0,03. Le reste des paramètres du système ont assigné les valeurs suivantes : $\varepsilon_1=1$, $\varepsilon_2=20$, $\varepsilon_3=0.5$, $\sigma_1=1.14$, $\sigma_2=0.32$, $\alpha=255/256$, avec les conditions initiales : $(x_1(0) ; x_2(0) ; x_3(0) ; x_4(0) ; x_5(0)) = (0.1 ; 0.1 ; 0.1 ; 0 ; 0)$.

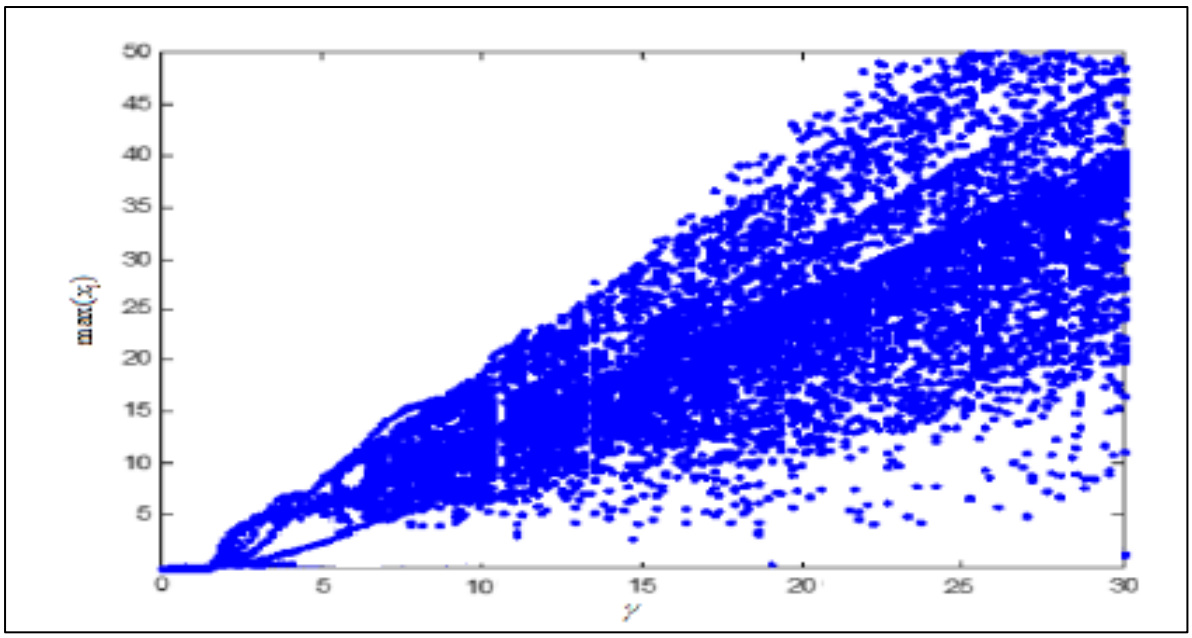


Figure III.6. Diagramme de bifurcation.

D'après le diagramme de bifurcation tracé sur la figure (III.6), nous pouvons conclure que notre système passe par de nombreux comportements pour atteindre le comportement chaotique. Lorsque γ est compris entre 0 et 2, le système n'a pas atteint les conditions de démarrage-oscillation. Lorsque γ est compris entre 2 et 10, cette région n'est pas dense et le comportement du système est soit périodique, soit quasi-périodique. Pour des valeurs γ supérieures à 10, la région est très dense, ce qui signifie que le comportement du système est chaotique.

III.6.4 Les résultats de simulation

Ce qui nous intéresse dans ce travail est le comportement chaotique de l'oscillateur proposé, où à travers le diagramme de bifurcation, il semble clair que si γ dépasse la valeur 10, le comportement de ce système devient chaotique. On prend par exemple la valeur γ=18.24, les réponses temporelles et les espaces des phases obtenus sont illustrés dans les figures (III.7) et (III.8)

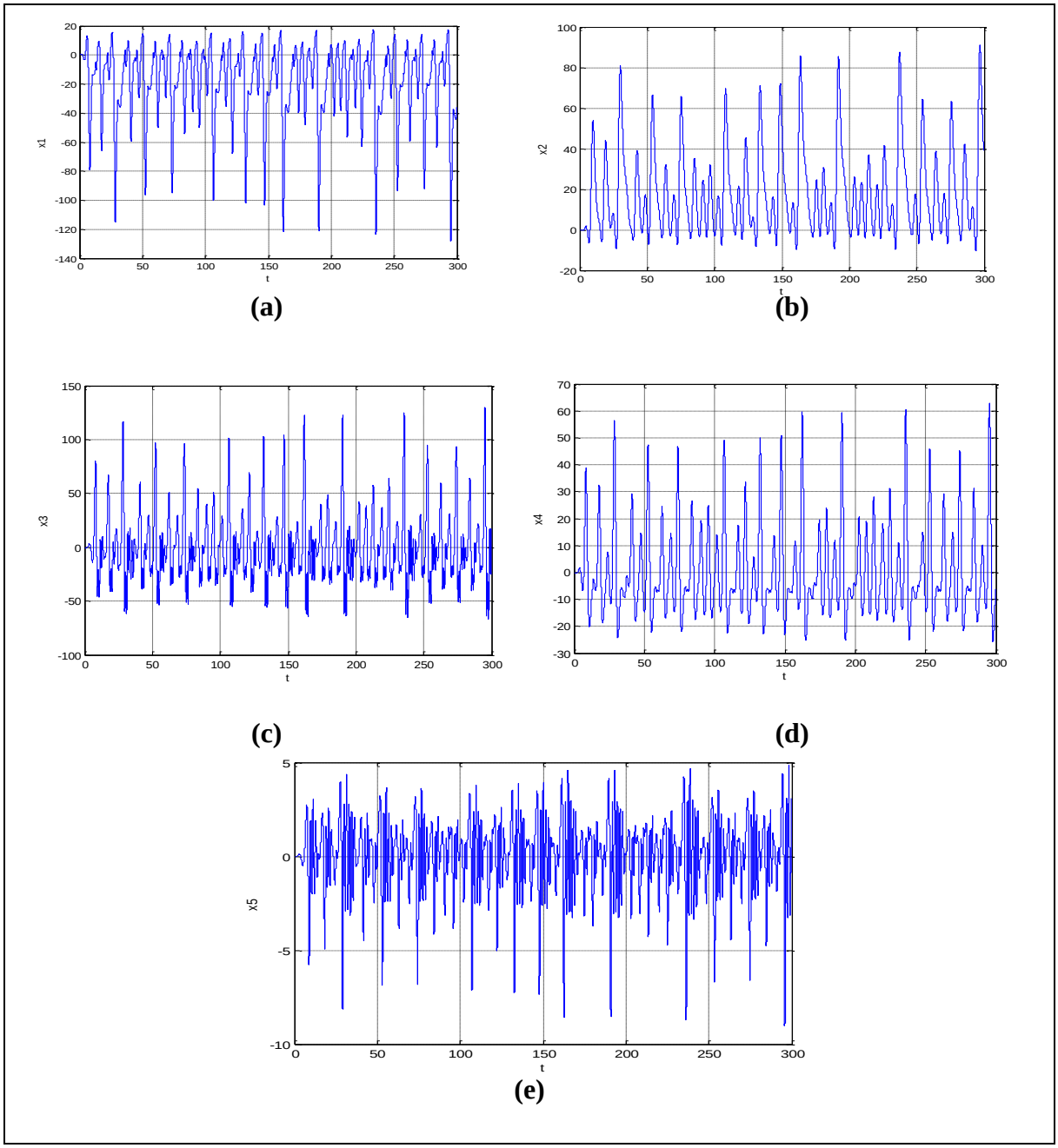


Figure III.7. Les réponses temporelles : **(a)** la variable d'état x_1 ; **(b)** la variable d'état x_2 ; **(c)** la variable d'état x_3 ; **(d)** la variable d'état x_4 ; **(e)** la variable d'état x_5.

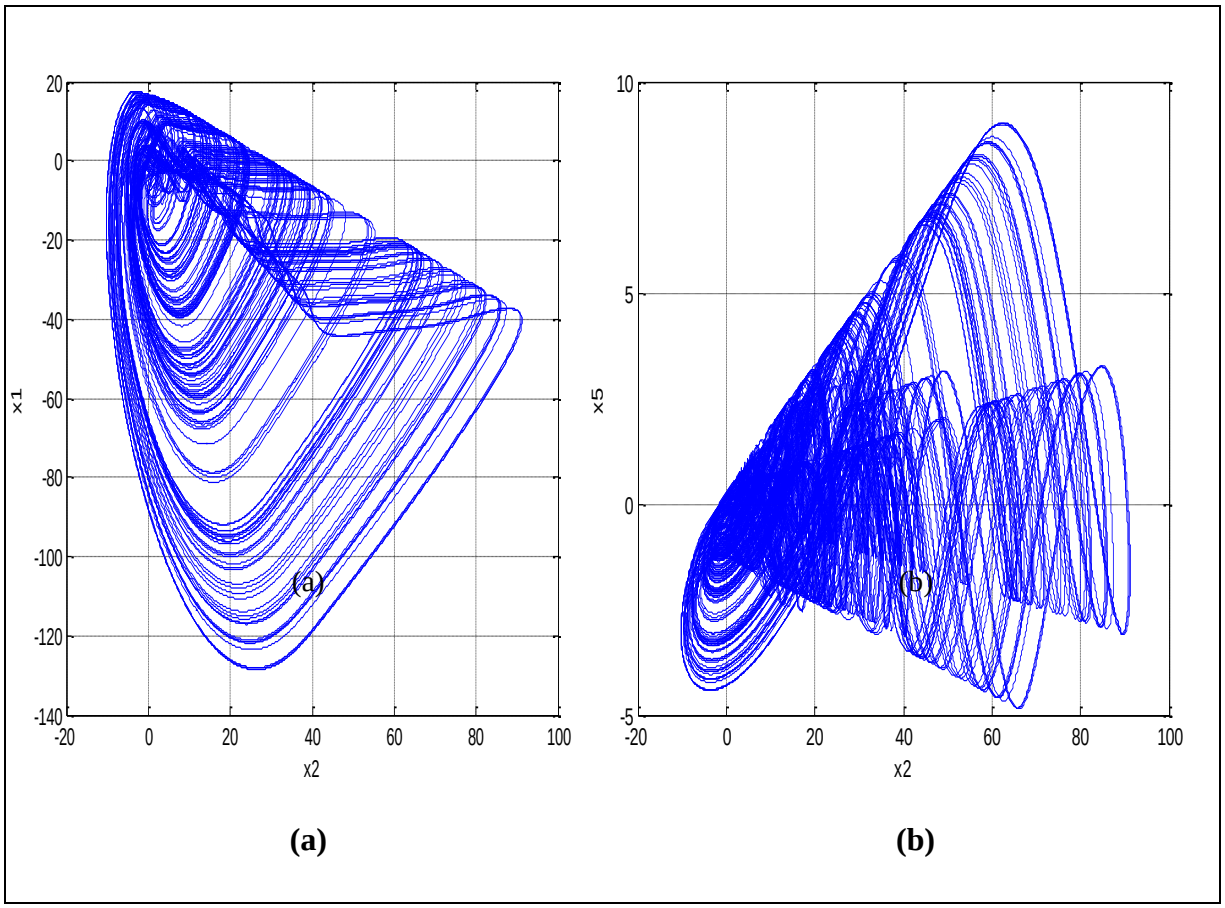


Figure III.8. Les espaces des phases : **(a)** (*x2*, *x1*) ; **(b)** (*x2*, *x5*).

III.6.5 Simulation sous ADS

Dans cette partie, nous visons à confirmer les résultats mathématiques obtenus sous Matlab, à travers une autre simulation à l'aide de l'outil ADS (Advanced Design System), le circuit simulé est représenté sur la figure (III.9), ce circuit est construit à l'aide du modèle Pspice de transistor bipolaire BFG410W qui est caractérisé par une fréquence de transition ($F_T = 22GHz$), l'utilisation du modèle Pspice de ce transistor qui est représenté dans la figure (III.10) vise à modéliser: des éléments parasites du boîtier (capacité, inductance et résistance) ; effets de température; temporisation; et d'autres paramètres qui affectent la dynamique de l'appareil. Les valeurs des composants du circuit sont mentionnées dans le tableau (III.1).

Tableau III.1. Les valeurs des composants utilisés dans la simulation sous ADS.

Composants	V_0	I_0	C_1=C_2	L_C	L_B	R_B	R_C
Valeurs	8 V	15mA	3 pF	3 nH	6 nH	10 Ω	36 Ω

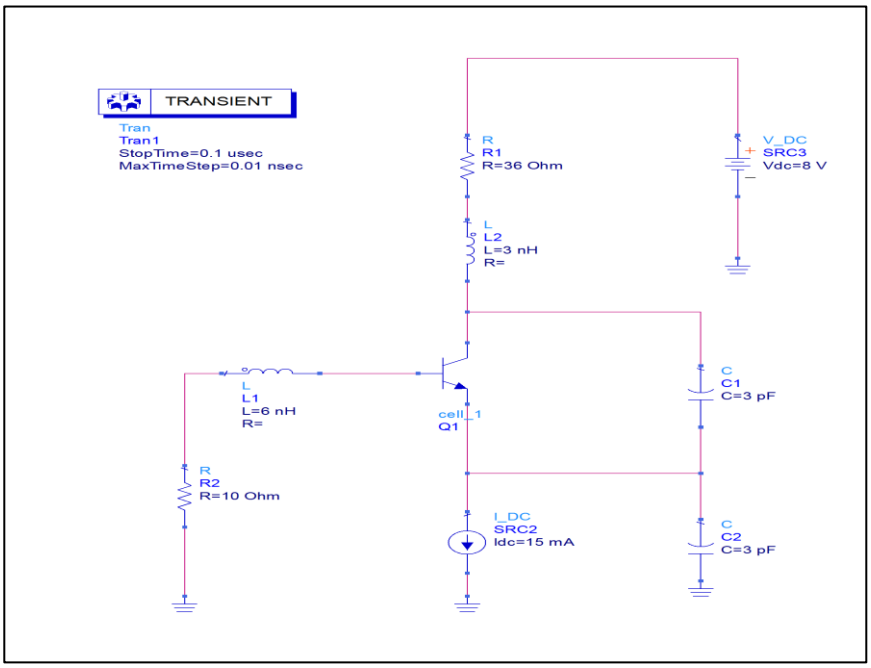


Figure III.9. Circuit simulé sous ADS.

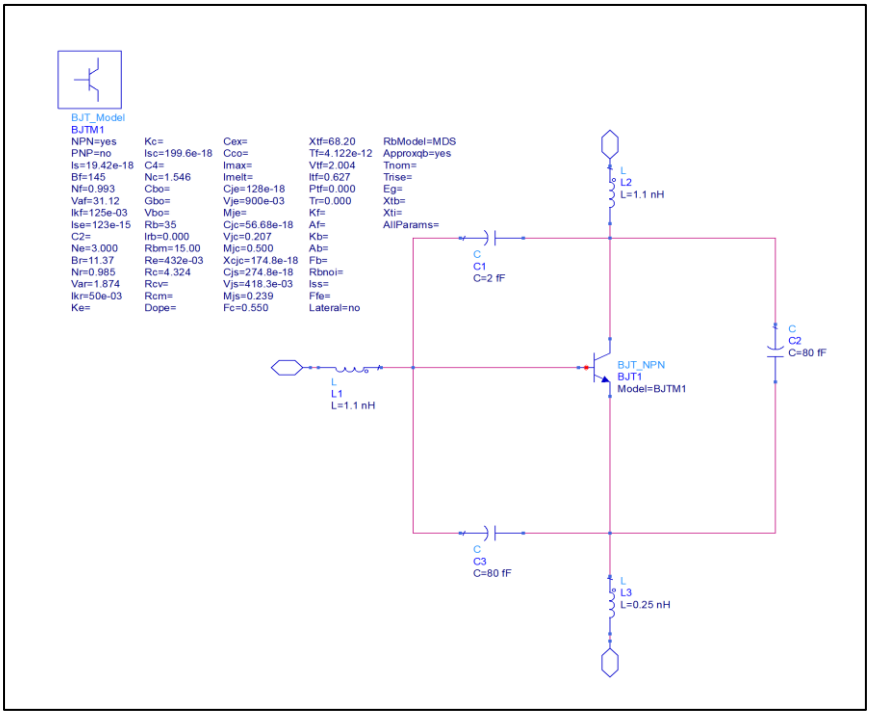


Figure III.10. Modèle Pspice de transistor bipolaire BFG410W.

Les figures (III.11) et (III.12) illustrent les réponses temporelles *(V_{C1})* et *(V_{C2})*, et les espaces des phases $V_{C1} = f(V_{C2})$, et $I_{LB} = f(V_{C2})$ trouvés après la simulation du circuit de l'oscillateur proposé sous le logiciel ADS en utilisant le simulateur transitoire *(TRANSIENT SIMULATOR)* avec un pas de temps égal à Δt=0,01 nsec.

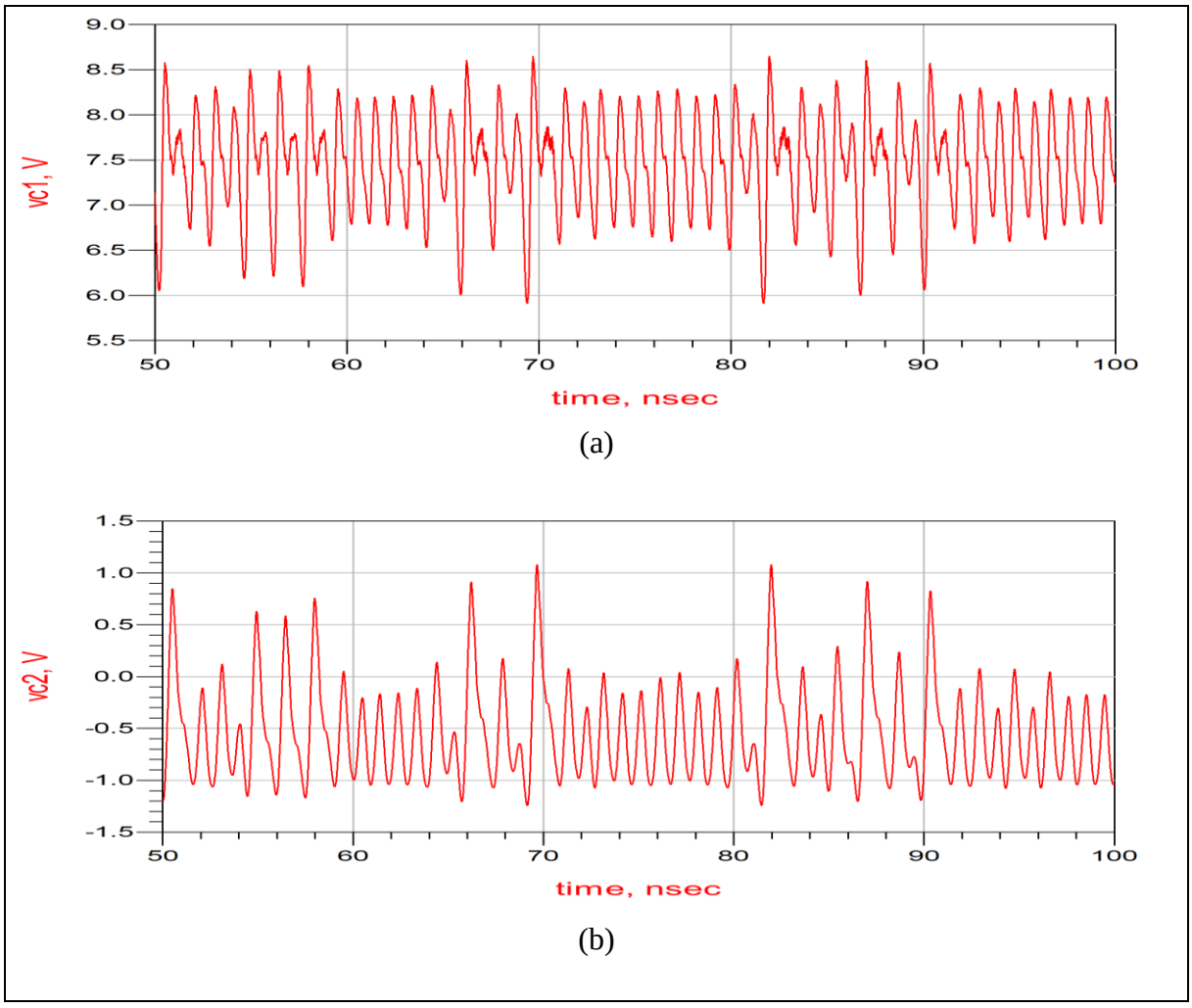


Figure III.11. Les réponses temporelles obtenus par la simulation sous ADS : **(a)** la variable d'état V_{C1} ; **(b)** la variable d'état V_{C2}.

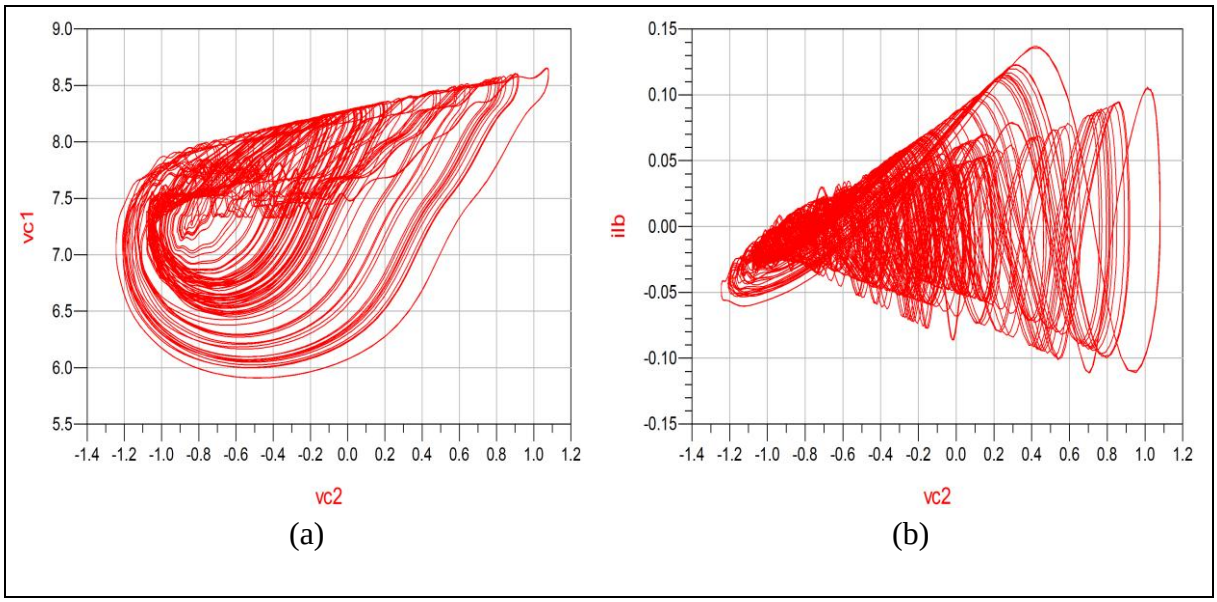


Figure III.12. Les espaces des phases obtenus par la simulation sous ADS : **(a)** (V_{C2}, V_{C1}) ; **(b)** (V_{C2}, I_{LB}).

Par la comparaison entre les espaces des phases mathématiques (obtenus sous Matlab) et les espaces des phases électriques (obtenus sous ADS), il est clair qu'il existe une bonne similitude entre eux. A partir de cette étroite similitude, nous pouvons valider le modèle mathématique (III.9) adopté pour notre oscillateur. Si V_{C1} est considéré comme une sortie de notre générateur, qui sera ensuite utilisée pour des applications de communication. En se basant sur la Figure (III.13) qui représente les caractéristiques spectrales de Vc_1, on remarque que son spectre de puissance est entre -10 dBm et -50dBm répartis sur une gamme de fréquence jusqu'à 6 GHz.

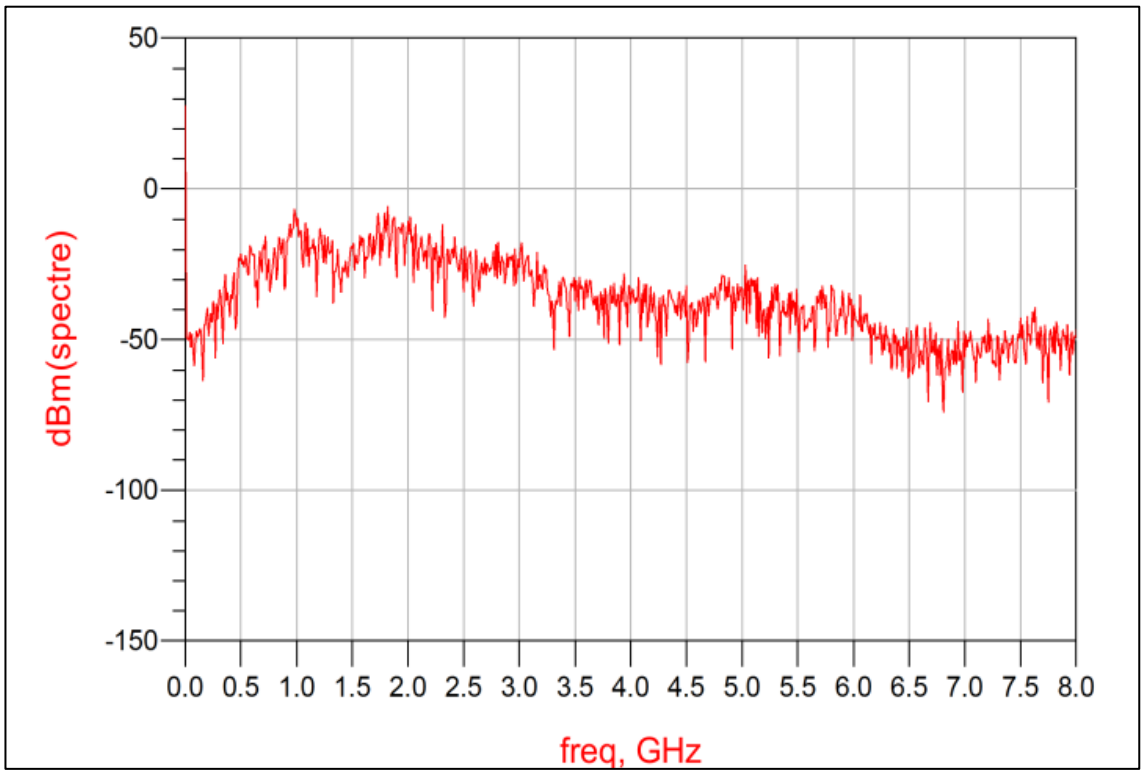


Figure III.13. Les caractéristiques spectrales de V_{c1}.

III.7 Conclusion

Dans ce troisième chapitre, nous avons présenté une nouvelle conception d'un oscillateur chaotique 5D basé sur la configuration Colpitts, ce nouvel oscillateur est conçu à l'aide d'un transistor bipolaire de type BFG410W en combinant deux versions de l'oscillateur Colpitts. Les résultats des simulations mathématique et électrique montrent que ce circuit peut osciller jusqu'à 6 GHz. Cela veut dire que l'oscillateur proposé dans le cadre de ce mémoire peut sécuriser les bandes de la téléphonie mobile (700 MHz – 2.6 GHz) et les bandes des applications ISM (la bande 2.4 GHz, et la bande 5.8 GHz).

Conclusion générale

Conclusion générale

Nous avons présenté dans ce mémoire une nouvelle conception d'un oscillateur chaotique 5D basé sur la configuration Colpitts utilisé pour sécuriser les communications sans fil allant jusqu'à 6 GHz, ce nouvel oscillateur combine deux versions de l'oscillateur Colpitts (standard et améliorée).

Dans le premier chapitre nous avons abordé quelques notions sur les systèmes dynamiques en temps continu ou en temps discret. Ensuite, nous nous sommes intéressés à une classe particulière de systèmes non linéaires dits chaotiques, avec quelques concepts et définitions introductifs à la théorie du chaos. Ces systèmes présentent plusieurs caractéristiques qui sont utilisées pour une transmission plus sécurisée. Nous pouvons citer parmi ces caractéristiques la sensibilité aux conditions initiales qui signifie qu'un moindre écart ou imprécision dans les conditions initiales engendre des évolutions totalement différentes, ce qui implique l'impossibilité de prédiction du comportement du système chaotique à long terme. Une autre propriété intéressante est le déterminisme qui signifie que ces systèmes sont régis par des règles fondamentales non probabilistes, donc c'est possible de reproduire le comportement chaotique. L'attracteur étrange est la troisième propriété qui est un attracteur dont la forme n'est pas une courbe ni une surface. Nous avons également défini quelques outils pour étudier ces systèmes, d'abord les exposants de Lyapunov pour vérifier le comportement d'un système dynamique, ensuite le diagramme de bifurcation qui nous permet d'observer les différents comportements possibles des systèmes chaotiques.

Dans le deuxième chapitre nous avons introduit la cryptographie chaotique, la cryptanalyse et les concepts de base d'un schéma de cryptage. Après, nous avons expliqué le cryptage par le chaos et les différentes techniques utilisées pour masquer l'information utile à transmettre par un signal chaotique. La première technique est le chiffrement par addition. La deuxième technique est le chiffrement par modulation qui utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. La dernière technique qu'on a citée est le chiffrement par commutation, cette dernière technique exige que le message à transmettre soit en binaire. Finalement nous avons clos le deuxième chapitre par la synchronisation chaotique, qui est une étape essentielle dans un système de transmission à base du chaos. Nous avons aussi présenté les différents régimes de synchronisation.

Le troisième chapitre, a été consacré à la conception et la simulation d'un émetteur pour les transmissions chaotiques. Dans la première partie de ce chapitre, nous avons exposé les différentes applications ciblées comme la téléphonie mobile et les applications des bandes ISM qui peuvent être sécurisées en utilisant le générateur chaotique proposé dans le cadre de ce Projet de Master.

Dans la deuxième partie, nous avons conçu un émetteur chaotique qui combine deux versions de l'oscillateur de Colpitts, cette nouvelle structure possède deux inductances : l'une L_C placée dans le collecteur, et l'autre L_B placée dans la base du transistor bipolaire utilisé. Ensuite, nous avons établi le modèle mathématique de cet oscillateur qui s'écrit sous la forme d'un système des équations différentielles ordinaires avec un terme non linéaire qui assure la présence de chaos dans ce modèle. La résolution de ce modèle sous Matlab par la méthode de Runge-Kutta d'ordre 4 nous permet de tracer le diagramme de bifurcation, les réponses temporelles, et les espaces des phases. Basant sur le diagramme de bifurcation tracé, on a conclu qu'à partir de la valeur $\gamma=10$ l'oscillateur se comporte de manière chaotique, ce comportement est illustré par la suite dans les réponses temporelles et les espaces des phases, où nous avons remarqué une infinité des périodes, et des attracteurs étranges dans les espaces des phases.

Dans la dernière partie de ce chapitre, nous avons simulé le circuit de l'oscillateur sous le logiciel ADS, et ceci afin de tracer les réponses temporelles, les espaces des phases, et aussi la réponse spectrale. Les réponses temporelles et les espaces des phases obtenus permettent de confirmer les résultats mathématiques obtenus sous Matlab et ainsi de valider le modèle mathématique établi. Le spectre obtenu dans cette simulation montre que la bande passante des oscillations chaotiques peut couvrir des fréquences allant jusqu'à 6 GHz avec une dynamique de chaos entre -10dBm et -50 dBm.

En perspectives, notre travail peut être complété par :

- L'augmentation de la fréquence d'oscillation.
- Réalisation pratique du générateur proposé.
- La proposition d'une méthode de synchronisation.

Bibliographie

Bibliographie

[1]. E. Ott , “Chaos in dynamical systems” , Cambridge University press , seconde edition, university of Maryland , 2002 .

[2]. R. L. DEVANEY, “An introduction to chaotic dynamical systems”, Westview Press, 2003.

[3]. P. Stavroulakis, “Chaos Applications In Telecommunications”, CRC Press, 2006.

[4]. Julio Alexander AGUILAR ANGULO, “Conception d’un Générateur de Valeurs aléatoires en Technologie CMOS AMS 0.35 μm”, Thèse de Doctorat, Universitè de Toulon, 2015.

[5]. F. Frédéric, “Cours de Systèmes dynamiques”, chaos et applications, 2018.

[6]. G. Oded, “Discrete Dynamical Systems”. Springer, 2007.

[7]. O. E. Rossler, “ An equation for continuos chaos”, Phys. Lett., 1976.

[8]. S. N. RASBAND, “Chaotic dynamics of non linear systems”, Wiley Professional, 1997.

[9]. S. H. STROGATZ, “Non linear dynamics and chaos : with applications to physics, biologie, chemistry and engineering”, *2000.*

[10]. Hamid Hamiche, ‘‘Inversion à Gauche Des Systèmes Dynamiques Hybrides Chaotiques Application à la Transmission Sécurisée de Données’’, Thèse de Doctorat, Université Mouloud Mammeri, 2011.

[11]. A. Pallavisini, ‘‘Système d'interférences radio fréquences pour la cryptographie par chaos appliquée aux transmissions hertziennes’’, Thèse de Doctorat, Université de Franche-Comté, 2007.

[12]. Cristina Morel, “Analyse et contrôle de dynamiques chaotiques, application à des circuits électroniques non-linéaires”, Thèse de Doctorat, Universitè d’Angers, 2005.

[13]. Edward N. Lorenz, “Deterministic nonperiodic flow ”, J. Atmos. Sci., vol. 20, no 2, 1963.

[14]. S. Malykh, Y. Bakhanova, A. Kazakov, K. Pusuluri, et A. Shilnikov, “Homoclinic chaos in the Rössler model ”, Chaos, 2020.

[15]. Dierk Schleicher, “Hausdorff dimension, its properties and its surprises”, Amer. Math. Monthly, vol. 114, p. 509-528, 2007.

[16]. A.J. Michaels, “Digital Chaotic Communications”, Thèse de Doctorat, Georgia Institute of Technology, 2009.

[17]. T. Yang, “Impulsive Control theory”, Springer Verlag, Lecture Notes in Control and Information sciences, 2001.

[18]. R. Gilmore, et M. Lefranc, "The Topology of Chaos", American Journal of Physics, 2003.

[19]. R. M. May, "Simple mathematical models with very complicated dynamics", Nature, vol. 261, no 5560, p. 459–467, 1976.

[20]. A. Ali Pacha, N. Hadj Said, « la Cryptographie et ses Principaux Systems : R.S.A et D.E.S » Vol 12, No 1, USTO-BP 1505,2002.

[21]. F. ANSTETT, « les systèmes dynamiques chaotiques pour le chiffrement: synthèse et cryptanalyse », Thèse de doctorat, Universitè de Henri Poincarè, *2006*.

[22]. N. Hamri, «La Synchronisation et le Contrôle du Chaos dans un Système Tridimensionnel», Proceedings Fractales 98, Séminaire National sur les Fractales dans la Compression des Images, pp. 48-57, 1998.

[23]. K. Veselyand J.Podolsky, « Chaos in a modified Hénon- Heiles system describing geodesics in gravitation waves », Phys. Leyy. 271, 368-376, 2000.

[24]. T. Hoet, B. Lorenz, S. Sahin « la cryptographie Chaotique », Mémoire de Licence IMACS INSA Toulouse, 2012.

[25]. M.Djemai, J-P Barbot and I. Belmouhoub, « Discrete-Time Normal From for Left Invertibilily problem », Eur, J.Control, Vol.15, p194-2014, 2009.

[26]. I. Belmouhoub, M. Demai and J.P. Barbot, « Observability quadtatic normal Form for discrete-Time système », IEEE Transactions on Automatic control, vol 50, July 2005.

[27]. A. Ouastaloup, J. Sabatier, and P.Lanusse. « From fractal robustness to the crone control», fractional Calculus and Applied nalysis, 2, 1999.

[28]. I. Ameur « Synchronisation Chaotification et Hyperchaotification des systèmes nonlinéaires : Méthodes et applications», thèse de Doctorat, Université Mentouri de Constantine, 2011.

[29]. L. M. Pecora, and T. L. Carroll, "Synchronization in chaotic systems," Physical Review Letters, vol. 64, no. 8, pp. 821–824, 1900.

[30]. Ge, Z. M., & Chen, Y. S,"Adaptive synchronization of unidirectional and mutual coupled chaotic systems". Chaos, Solitons & Fractals, *26*(3), 881-888. 2005.

[31]. Mihai Bogdan Luca « Apports du Chaos et des estimateurs d'état pour la transmission sécurisée de l'information », Thèse de Doctorat, Université de Bretagne Occidentale, 2006.

[32]. G.R. Cooper, R. W. Nettleton « Spectral efficiency in cellular Iand-mobile communications: a spread spectrum approach », final Report, TR- EE 78-44, Purdue University, West lafayette .Ind 1978.

[33]. E. Cherrier, « Estimation de l'Etat et des Entrées Inconnues pour une Classe de Systèmes non Linéaires », Thèse Doctorat, Nancy, France, 2006.

[34]. Matsumoto, Takashi , "A Chaotic Attractor from Chua's Circuit" . IEEE Transactions on Circuits and Systems. 31 (12): 1055–1058, 1983.

[35]. M. P. Kennedy, "Chaos in the Colpitts oscillator," IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, vol. 41, no. 11, pp. 771-774, 1994.

[36]. A. Tamasevicius, S. Bumeliene, et E. Lindberg, "Improved chaotic Colpitts oscillator for ultrahigh frequencies", Electronics Letters, 1569 – 1570, 2004.

[37]. X. Q. Nguyen, T. Q. Bui, V. Y. Vu, T. D. Nguyen and T. M. Hoang, "Simulation and implementation of improved chaotic Colpitts circuit for UWB communications," International Conference on Communications and Electronics 2010, 2010.

[38]. M. P. Kennedy,"Robust OP Amp Realization of Chua's Circuit" Frequenz, vol. 46, no. 3-4, pp. 66-80, 1992.

[39]. G. M. MAGGIO ,M. DI BERNARDO & M. P. KENNEDY, "Nonsmooth bifurcations in piecewise-linear model of the colpitts oscillator", IEEE Transactions on circuits and systems-I: Fundamental theory and apllications 47 ,p.1160-1177.2000.

[40]. M. BENDAOUD, " Etude et Conception d'un système chaotique basé sur l'oscillateur Colpitts pour les communications sécurisées", Mèmoire de Master, Universitè de Tlemcen, 2019.

[41]. M. Moundher, B. Hichem, T. Djamel and S. Said, "Novel Four-dimensional Chaotic Oscillator for Sub-1GHz Chaos-Based Communication Systems," 2019 6th International Conference on Image and Signal Processing and their Applications (ISPA), pp. 1-5, 2019.

[42]. J. Kengne, J. C. Chedjou, G. Kenne, et K. Kyamakya, "Dynamical properties and chaos synchronization of improved Colpitts oscillators", Communications in Nonlinear Science and Numerical Simulation, Vol.17, pp 2914-2923, 2012.

[43]. S. A. Maas, "Nonlinear microwave and RF circuits", 2nd ed. Artech. House, Inc. 2003.

[44]. G. M. Maggio, O. De Feo , M. P. Kennedy, "Nonlinear analysis of the Colpitts oscillator and application to design". IEEE Trans Circ Syst;46:1118–1130, 1999.

Résumé

Ce travail de mémoire consiste en l'étude et la conception d'un nouvel émetteur chaotique destiné aux transmissions sécurisées. Ce mémoire est composé de deux parties principales: la première partie concerne l'étude des systèmes chaotiques qui sont des systèmes caractérisés par le déterminisme, la non linéarité et une extrême sensibilité aux conditions initiales, ainsi quelques outils pour faciliter l'étude de ces systèmes comme les exposants de Lyapunov, l'espace des phases et le diagramme de bifurcation qui nous montre les différents comportements d'un système dynamique en passant par le comportement périodique jusqu'au comportement chaotique. L'étude des systèmes chaotiques est destinée à leur utilisation pour sécuriser les transmissions, c'est pourquoi nous avons expliqué les objectifs des crypto-systèmes et les différentes techniques de chiffrement par chaos, ainsi les différents régimes de synchronisation. La deuxième partie de ce travail comprend la conception d'un émetteur chaotique, qui a été réalisé en combinant deux versions de Colpitts à l'aide d'un transistor bipolaire de type BFG410W. Cette nouvelle structure a été simulée par deux logiciels de simulation, le premier c'est Matlab, afin de résoudre le modèle mathématique proposé et ainsi identifier les comportements possibles de cet émetteur, et le second est le logiciel ADS qui a été utilisé pour l'objectif de vérifier les résultats obtenus sous Matlab et donc validant le modèle mathématique établi, et traçant les réponses temporelles et fréquentielles. À travers cette dernière réponse, nous avons conclu que cet émetteur propose dans notre travail peut générer des signaux chaotiques allant jusqu'à 6 GHz.

Mots clés : *chaos, diagramme de bifurcation, l'espace de phase, Matlab, ADS, BFG410W.*

Abstract

This work consists in the study and the design of a new chaotic transmitter intended for secure transmissions. This memory is composed of two main parts: the first part concerns the study of chaotic systems which are systems characterized by determinism, non-linearity and extreme sensitivity to initial conditions, as well as some tools to facilitate the study of these systems such as Lyapunov exponents, phase space and the bifurcation diagram that shows us the different behaviors of a dynamic system through the periodic behavior to the chaotic behavior. The study of chaotic systems is intended for their use in securing transmissions, so we have explained the objectives of cryptosystems and the different techniques of encryption by chaos, as well as the different regimes of synchronization. The second part of this work includes the design of a chaotic emitter, which has been realized by combining two versions of Colpitts using a BFG410W bipolar transistor. This new structure has been simulated by two simulation software, the first is Matlab, in order to solve the proposed mathematical model and thus identify the possible behaviors of this emitter, and the second is the ADS simulator that has been used for the purpose of verifying the results obtained in Matlab and thus validating the established mathematical model, and plotting the temporal and frequency responses. Through this last response, we concluded that this transmitter proposed in our work can generate chaotic signals up to 6 GHz.

Keywords: *chaos, bifurcation diagram, phase space, Matlab, ADS, BFG410W.*

ملخص

يهتم هذا العمل بدراسة وتصميم مرسل فوضوي جديد موجه لتأمين الاتصالات، ينقسم هذا العمل الى جزئين أساسيين :يتعلق الجزء الأول بدراسة الأنظمة الفوضوية والتي تتميز بالحتمية، اللاخطية، والحساسية المفرطة للشروط الابتدائية، وكذا بعض الوسائل المتاحة لتسهيل دراسة هاته الأنظمة مثل دلائل ليابونوف، مساحة الطور، ومخطط التشعب الذي يوضح لنا السلوكيات الممكنة للأنظمة الديناميكية انطلاقا من السلوك الدوري وصولا الى السلوك الفوضوي. تهدف دراسة الأنظمة الفوضوية إلى استخدامها لتأمين عمليات الاتصالات، ولهذا السبب قمنا بشرح أهداف أنظمة التشفير وتقنيات التشفير المختلفة بالفوضى، فضلاً عن أنظمة التزامن. يتضمن الجزء الثاني من هذا العمل تصميم مرسل فوضوي من خلال الجمع بين نسختين مختلفتين من مذبذب كولبيتس باستعمال ترانسيستور ثنائي القطب من نوع(BFG 410W) ، تمت محاكات هذا الهيكل الجديد بواسطة برنامجين، الأول هو (Matlab) وهذا لحل النموذج الرياضياتي الخاص بهذا المرسل وبالتالي تحديد السلوكيات الممكنة له، أما البرنامج الثاني هو (ADS)والذي تم استعماله بغرض التحقق من النتائج الرياضية المتحصل عليها باستعمال (Matlab) وبالتالي التحقق من صحة النموذج الرياضياتي، ورسم الاستجابات الزمنية والترددية الخاصة بهذا المرسل. من خلال هاته الاستجابة الأخيرة، استنتجنا أن المرسل المقترح في عملنا بإمكانه توليد اشارات فوضوية تصل الى غاية 6 جيغا هرتز.

***الكلمات المفتاحية**: الفوضى، منحنى التشعب، مساحة الطور، Matlab، ADS، BFG410 W*