

الجمهورية الجزائرية الديمقراطية الشعبية

**REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE**

وزارة التعليم العالي والبحث العلمي

**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**

جامعة أبو بكر بلقايد - تلمسان

Université Aboubakr Belkaïd - Tlemcen -

Faculté de TECHNOLOGIE



## **MEMOIRE**

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

**En** : Télécommunications

**Spécialité** : Systèmes de Télécommunications

**Par** :

BENAZOUZ Manel *et* BELDJELIL Khawla

**Sujet**

**Etude de la dynamique et la synchronisation d'un nouveau  
générateur chaotique dédié aux systèmes de communication  
sécurisé par chaos**

Soutenu publiquement, le **21/06/2023**, devant le jury composé de :

Mr A. BOUACHA	Professeur	Univ. Tlemcen	Président
Mr A. R. BORSALI	Professeur	Univ. Tlemcen	Examineur
Mr S. KAMECHE	Professeur	Univ. Tlemcen	Directeur de mémoire
Mr M.BENDAOUZ	Doctorant	Univ. Tlemcen	Co-Directeur de mémoire

Année universitaire : 2022/2023

## Dédicaces

### *Dédicaces « Manel »*

*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 ma chère mère,*

*A mon cher père,*

*Qui n'ont jamais cessé, de formuler des prières à mon égard, de me soutenir et de m'épauler pour que je puisse atteindre mes objectifs,*

*A mon frère Nasreddine,*

*A mes sœurs Hafsa et Nesrine,*

*Pour son soutien moral et leurs conseils précieux tout au long de mes études,*

*A toute ma famille.*

*A mes chères amies Ikram et chaimaa, je vous remercie infiniment pour votre aide ainsi que vos encouragements et votre fidélité.*

*Mon binôme et mon amie « Khawla » et sa famille.*

***Manel***

## ***Dédicaces « Khawla »***

*A ma mère et mon père,*

*Qui n'ont jamais cessé, de formuler des prières à mon égard, de me soutenir et de pour tous les sacrifices que vous n'avez cessé de me donner m'épauler pour que je puisse atteindre mes objectifs. Puisse Dieu, le tout puissant, vous préserver et vous accordez santé, longue vie et bonheur.*

*Mes sœurs « Ikram » et « Ilham », « merwa » et « nada » Pour leur soutiens et encouragements.*

*A ma chère tante Naima et toute ma famille, mon grand-père et ma grand-mère. Je vous dédié ce travail avec tous mes vœux de bonheur et de santé.*

*A ma chère binôme, « Manel » Pour son entente et sa sympathie.*

*A tous mes Amis(es), qui m'a aidé et supporté dans les moments difficiles.*

***Khawla***

## 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 et surtout ses judicieux conseils qui ont contribués à alimenter nos réflexions.*

*Nous tenons aussi très chaleureusement à remercier notre Co-encadreur Monsieur BENDAOUH Mohammed, Doctorant à l'université de Tlemcen, d'avoir co-encadré notre travail et sa grande disponibilité et son soutien moral, ses encouragements.*

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

*Nous exprimons également notre reconnaissance à Monsieur BORSALI Ahmed Riad Professeur 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 de notre profonde gratitude pour leur soutien et leurs encouragements de tous les instants. On vous en remercie chaleureusement.*

## ملخص

### ملخص

تهتم مذكرة التخرج هاته بدراسة وتصميم مولد فوضوي جديد يتم استغلاله في حماية أنظمة الاتصالات. حيث يتألف هذا العمل من جزئين رئيسيين: الجزء الأول يعرض المفاهيم النظرية المتعلقة بالأنظمة الفوضوية، مثل مؤشرات لياونوف ومساحة المراحل ومنحنى التفرع، الذي يوضح السلوك المختلف للنظام الديناميكي، بدءًا من السلوك الدوري وحتى السلوك الفوضوي. يهدف دراسة الأنظمة الفوضوية إلى استخدامها في تأمين الاتصالات، ولهذا السبب قمنا بتعريف أنظمة التشفير ومختلف تقنيات التشفير الفوضوي وأنظمة المزامنة المختلفة. الجزء الثاني من هذا العمل يركز على تصميم مرسل فوضوي اعتمادا على النسخة المحسنة من مذبذب كولبيتس المحسن باستخدام الترانزيستور الثنائي BFP420، تمت محاكاة هذا المذبذب باستخدام برنامجين، الأول هو ماطلاب والذي قمنا من خلاله بحل النموذج الرياضي للمذبذب المقترح وبالتالي رسم الاستجابات الزمنية الفوضوية وكذا مساحات الطور الفوضوية. كما قمنا بمحاكاة دارة المذبذب باستعمال برنامج ثاني هو ADS والذي قمنا من خلاله بتأكيد النتائج الرياضية المتحصل عليها سابقا وكذا رسم الاستجابة الترددية للمذبذب المقترح. انطلاقا من الاستجابة الأخيرة، استنتجنا بأن المذبذب المقترح في هذا العمل بإمكانه توليد إشارات فوضوية تصل الى 11.2 جيجا هرتز.

**الكلمات المفتاحية:** مولد فوضوي، الاتصالات المؤمنة، Matlab، ADS، BFP420، التزامن.

## Abstract

---

### **Abstract**

This memory work consists of researching and designing a new chaotic generator for secure chaos-based transmissions. This work is composed of two main parts: the first part presents theoretical concepts related to chaotic systems, such as Lyapunov exponents, phase space, and the bifurcation diagram, which illustrates the different behaviors of a dynamical system ranging from periodic to chaotic behavior. The study of chaotic systems aims to use them for secure transmissions, which is why we have defined cryptographic systems and various chaotic encryption techniques, as well as different synchronization regimes. The second part of the work focuses on the design of a chaotic transmitter based on the improved Colpitts oscillator using a bipolar transistor BFP420. This new structure was simulated using two simulation programs: the first one is Matlab, used to solve the proposed mathematical model and plot the different chaotic time responses and chaotic phase spaces. The second one is the ADS software, used to verify and validate the results obtained in Matlab and also to plot the frequency response of the proposed oscillator. Based on this frequency response, we have concluded that the transmitter proposed in our work can generate chaotic signals up to 11.2 GHz. And we concluded our work by proposing a synchronization method using nonlinear feedback control.

**Keyword:** *chaotic generator, secure communications, MATLAB, ADS, BFP420, chaotic synchronization.*

# Résumé

## Résumé

Ce travail de mémoire consiste à rechercher et concevoir un nouveau générateur chaotique pour les transmissions sécurisées par chaos. Ce travail se compose de deux parties principales : la première partie expose des notions théoriques concernant les systèmes chaotiques, comme les exposants de Lyapunov, l'espace des phases, et le diagramme de bifurcation, qui nous montre les différents comportements d'un système dynamique, allant du comportement périodique au comportement chaotique. L'étude des systèmes chaotiques vise à les utiliser pour sécuriser les transmissions, c'est pourquoi nous avons défini les systèmes cryptographiques et les différentes techniques de chiffrement chaotique ainsi que les différents régimes de synchronisation. La deuxième partie du travail porte sur la conception d'un émetteur chaotique à base du l'oscillateur Colpitts amélioré utilisant un transistor bipolaire BFP420. Cette nouvelle structure a été simulée par deux programmes de simulation : le premier est Matlab, pour résoudre le modèle mathématique proposé et donc tracer les différentes réponses temporelles chaotiques, et les espaces de phases chaotiques. Le second est le logiciel ADS qui est utilisé pour vérifier et valider les résultats obtenus sous Matlab, et aussi pour tracer la réponse fréquentielle de l'oscillateur proposé. Grâce à cette dernière réponse, nous sommes arrivés à la conclusion que l'émetteur proposé dans notre travail peut générer des signaux chaotiques jusqu'à 11.2 GHz. Et nous avons fini notre travail par proposer une méthode de synchronisation à l'aide d'un contrôle rétroaction non linéaire.

**Mots clés :** *Générateur chaotique, communications sécurisées, MATLAB, ADS, BFP420, synchronisation chaotique.*

## Table des matières

Dédicaces .....	i
Remerciements .....	iii
Résumés .....	iv
Table des matières .....	v
Sigles et Abréviations.....	viii
Liste des figures .....	ix
Liste des tableaux .....	xi
Introduction Générale.....	2

### Chapitre I : Généralités sur les systèmes dynamiques chaotiques

I.1 Introduction.....	5
I.2 Systèmes dynamiques .....	5
I.2.1 Systèmes dynamiques continus.....	5
I.2.2 Systèmes dynamiques discrets .....	6
I.2.3 Systèmes dynamiques autonomes et non-autonomes .....	6
I.3 Systèmes chaotiques .....	6
I.3.1 Non linéaire.....	7
I.3.2 Déterministe .....	7
I.3.3 L'aspect aléatoire .....	7
I.3.4 Sensibilité aux conditions initiales.....	8
I.4 Application du chaos.....	8
I.5 L'espace de phase .....	9
I.6 Notion d'attracteurs .....	9
I.6.1 Les différents types d'attracteurs .....	9
I.6.2 Des différents exemples d'attracteurs .....	10

I.6.2.1	Attracteur étrange de Lorenz .....	10
I.6.2.2	Attracteur étrange de Rossler .....	12
I.7	Exposants de Lyapunov .....	13
I.7.1	Exemple .....	14
I.8	Section de Poincaré .....	15
I.9	Bifurcation .....	15
I.10	Route vers chaos .....	16
I.10.1	Le doublement de période .....	16
I.10.2	L'intermittence .....	16
I.10.3	La quasi périodicité .....	17
I.11	Conclusion .....	17

**Chapitre II : Transmission chaotique**

II.1	Introduction .....	19
II.2	Objectifs des crypto-systèmes .....	19
II.3	Cryptographie .....	19
II.3.1	Les systèmes symétriques ou la clé secrète .....	20
II.3.2	Les systèmes asymétriques où la clé publique .....	21
II.4	Cryptanalyse .....	21
II.5	Techniques de chiffrement par chaos .....	22
II.5.1	Chiffrement par addition .....	23
II.5.2	Chiffrement par commutation .....	24
II.5.3	Chiffrement par modulation .....	24
II.6	Définition de la synchronisation .....	25
II.7	Classes de synchronisation .....	25
II.7.1	Synchronisation par couplage unidirectionnel .....	25
II.7.2	Synchronisation par couplage bidirectionnel .....	26
II.8	Différents régimes de synchronisation .....	27
II.8.1	Synchronisation par décomposition de système .....	27
II.8.2	Synchronisation retardée .....	27
II.8.3	Synchronisation en boucle fermée .....	28
II.8.4	Synchronisation projective .....	28

II.8.5 Synchronisation de phase.....	28
II.8.6 Anti-synchronisation.....	29
II.8.7 Synchronisation par observateur.....	29
II.7 Conclusion.....	30

**Chapitre III : Conception et synchronisation d'un générateur chaotique**

III.1 Introduction.....	32
III.2 Les bandes fréquentielles visées.....	32
III.2.1 La bande L [1 à 2 GHz].....	32
III.2.2 La bande S [2 à 4 GHz].....	32
III.2.3 La bande C [4 à 8 GHz].....	33
III.2.4 La bande X [8 à 12 GHz].....	33
III.3 Circuit de Chua.....	33
III.4 L'oscillateur Colpitts standard.....	35
III.5 L'oscillateur Colpitts amélioré.....	36
III.5.1 Le circuit de l'oscillateur.....	36
III.5.2 Le modèle mathématique de Colpitts amélioré.....	37
III.5.3 Les résultats de simulation numérique.....	38
III.5.4 Les résultats de simulation sous ADS.....	40
III.6 Synchronisation à l'aide d'un contrôle rétroaction non linéaire.....	44
III.7 Conclusion.....	48
Conclusion Générale.....	50
Bibliographie.....	53

## Sigles et abréviations

---

**ADS:** Advanced Design System simulator.

**BJT :** Bipolar Junction Transistor.

**CSK:** Chaos Shift Keying.

**DES :** Data Encryption Standard.

**ECC:** Elliptic Curve Cryptography.

**GPS:** Global Positioning System

**LTE:** Long Term Evolution

**NASA:** National Aeronautics and Space Administration

**ODE :** Ordinary Differential Equation.

**$\mathbf{R}$  :** ensemble des nombres réels.

**$\mathbf{R}^+$  :** nombres réels positifs ou nuls.

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

**RC4:** Rivest Cipher 4.

**RK-4:** Runge-Kutta d'ordre 4

**RSA :** R.Rivest A.Shamir L.Adleman.

**SCI :** Sensibilité aux Conditions Initiales.

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

## Liste des figures

### Chapitre I : Généralités sur les systèmes dynamiques chaotiques

<b>Figure I.1.</b> État chaotique $x_I$ du système de Rossler. ....	7
<b>Figure I.2.</b> Illustration de la propriété de sensibilité aux conditions initiales de la variable d'état $x_I$ (système de Rossler). ....	8
<b>Figure I.3.</b> Attracteur étrange de Lorenz .....	11
<b>Figure I.4.</b> États chaotiques du système de Lorenz .....	11
<b>Figure I.5.</b> Attracteur étrange de Rossler. ....	13
<b>Figure I.6.</b> États chaotiques du système de Rossler .....	13
<b>Figure I.7.</b> Les exposants de Lyapunov pour Lorenz ( $\sigma = 10$ ; $\rho = 28$ ; $\beta = \frac{8}{3}$ ) .....	14
<b>Figure I.8.</b> Diagramme de bifurcation de la fonction logistique .....	15

### Chapitre II : Transmission Chaotique

<b>Figure II.1.</b> Le principe de chiffrement symétrique .....	20
<b>Figure II.2.</b> Le principe de chiffrement asymétrique .....	21
<b>Figure II.3.</b> Principe de cryptanalyse. ....	22
<b>Figure II.4.</b> Chiffrement par addition. ....	23
<b>Figure II.5.</b> Chiffrement par modulation. ....	24
<b>Figure II.6.</b> Chiffrement par commutation. ....	25
<b>Figure II.7.</b> Couplage unidirectionnel .....	26
<b>Figure II.8.</b> Couplage bidirectionnel .....	27
<b>Figure II.9.</b> Synchronisation par boucle fermée. ....	28
<b>Figure II.10.</b> Principe de synchronisation à base d'observateurs. ....	29

**Chapitre III : Conception et synchronisation d'un générateur chaotique**

<b>Figure III.1.</b> Circuit de Chua.....	34
<b>Figure III.2.</b> L'attracteur étrange 3D de Chua. ....	34
<b>Figure III.3.</b> Le circuit de l'oscillateur Colpitts chaotique standard.....	35
<b>Figure III.4.</b> L'attracteur étrange 3D de Colpitts standard. ....	36
<b>Figure II.5.</b> Le circuit de l'oscillateur Colpitts amélioré. ....	37
<b>Figure III.6.</b> Les différentes réponses temporelles chaotique de l'oscillateur Colpitts amélioré.....	39
<b>Figure III.7.</b> Les différentes réponses temporelles chaotique de l'oscillateur Colpitts amélioré.....	39
<b>Figure III.8.</b> L'attracteur étrange 3D de Colpitts amélioré.....	40
<b>Figure III.9.</b> Le Circuit simulé sous ADS.....	41
<b>Figure III.10.</b> Le modèle Pspice de transistor bipolaire BFP420. ....	41
<b>Figure III.11.</b> Réponses temporelle ( $V_{c1}$ ), et ( $V_{c2}$ ). ....	42
<b>Figure III.12.</b> L'espace de phase ( $V_{c2}$ , $V_{c1}$ ). ....	42
<b>Figure III.13.</b> L'espace de phase ( $V_{c1}$ , $V_{c2}$ ). ....	43
<b>Figure III.14.</b> Les caractéristiques spectrales de $V_{c1}$ . ....	43
<b>Figure III.15.</b> Graphiques des erreurs de synchronisation avec temps normalisé .....	47

## Liste des tableaux

---

<b>Tableau I.1.</b> Classification des comportements selon les exposants de Lyapunov.....	14
<b>Tableau I.2.</b> Les différents comportements possibles de la fonction logistique .....	16
<b>Tableau III.1.</b> Les valeurs des composants utilisés dans la simulation sous ADS .....	40

# **Introduction Générale**

## **Introduction générale**

Depuis l'antiquité, l'homme a recherché divers moyens de communication pour transmettre des messages de manière sécurisée. Au fil du temps, ces modes de communication ont connu une évolution significative, tant sur le plan technologique que sur celui de la sécurité des échanges.

A mesure que les technologies de communication se sont développées, les risques de piratages, de vol de données et de violations de la confidentialité ont également augmenté. Les cyberattaques sont devenues plus sophistiquées et les cybercriminels sont constamment à la recherche de moyens de compromettre les systèmes de communication. Pour répondre à ce besoin, des mesures de sécurité ont été mises en place pour protéger les informations échangées. La cryptographie, par exemple, est une technique couramment utilisée pour sécuriser les données en les chiffrant de manière à ce qu'elles ne puissent être comprises que par les destinataires autorisés.

Les crypto systèmes modernes reposent sur le principe d'Auguste Kirchhoff. Il a conduit à une approche de conception de systèmes cryptographiques plus transparentes et à une plus grande confiance dans les algorithmes publics. De nos jours, la plupart des algorithmes de chiffrement et de signature numérique utilisés sont des normes ouvertes et publiques, ce qui permet une analyse approfondie de leur sécurité et favorise la confiance dans leur utilisation.

Le chaos présente un certain nombre de caractéristiques, notamment la sensibilité aux conditions initiales et l'imprévisibilité, ce qui rend les systèmes chaotiques très intéressants pour le cryptage des données.

L'utilisation des systèmes chaotiques pour sécuriser les communications est une approche innovante qui exploite les propriétés complexes et imprévisibles des systèmes chaotiques. En utilisant des algorithmes de chiffrement basés sur le chaos, les signaux de communication peuvent être mélangés de manière à rendre les messages chiffrés difficiles à décoder sans la connaissance du système chaotique utilisé. De plus, les systèmes chaotiques peuvent être utilisés pour générer des clés de chiffrement aléatoires et pour synchroniser les émetteurs et les récepteurs. Cependant, cette approche présente des défis tels que la synchronisation précise et la conception de schémas de chiffrement robustes, ce qui nécessite une expertise spécialisée pour garantir la sécurité des communications. Malgré ces défis,

l'utilisation des systèmes chaotiques offre un potentiel prometteur pour renforcer la confidentialité et la sécurité des échanges d'information.

Le but de notre mémoire est basé sur la conception et la synchronisation d'un générateur chaotique (Colpitts amélioré).

Ce mémoire est divisé en trois chapitres :

- Le premier chapitre présente des généralités sur les systèmes dynamiques chaotiques.
- Le second chapitre présente le principe de cryptographie chaotique avec les techniques de chiffrements, ainsi quelques notions sur la synchronisation des systèmes chaotiques.
- Dans le troisième chapitre nous allons commencer par la présentation de quelques circuits chaotiques, ainsi que ses modèles mathématiques, en finalisant ce chapitre par la proposition d'un générateur chaotique à base de l'oscillateur Colpitts amélioré.

**Chapitre I**  
**Généralités sur les systèmes dynamiques**  
**chaotiques.**

## I.1 Introduction

La découverte du chaos en tant que phénomène scientifique remonte au 19<sup>e</sup> siècle. Le mathématicien français Henri Poincaré est considéré comme l'un des pionniers de l'étude du chaos. Dans les années 1880, Poincaré a entrepris des recherches sur le problème des trois corps en mécanique céleste, qui consiste à étudier les mouvements de trois corps célestes sous l'influence de la gravité. Poincaré a découvert que le système présentait une sensibilité extrême aux conditions initiales, rendant impossible la prédiction précise à long terme des trajectoires des corps. Ce résultat a remis en question l'idée traditionnelle de déterminisme absolu et a jeté les bases de la théorie du chaos [1].

Les systèmes dynamiques chaotiques se retrouvent dans de nombreux domaines scientifiques, tels que la physique, les sciences de la vie, l'économie et la météorologie. Par exemple, le mouvement des planètes du système solaire, la croissance des populations d'animaux, les fluctuations des marchés financiers et les modèles climatiques peuvent tous exhiber des comportements chaotiques.

## I.2 Système dynamique

Un système dynamique est un système qui évolue dans le temps. Plus précisément, c'est un ensemble de règles mathématiques qui décrivent comment l'état d'un système change en fonction de temps et des entrées, où l'évolution d'un système dynamique est de la manière suivante :

- Causal, dont la sortie de système dépend uniquement des entrées actuelles et passées, ainsi que l'état actuel du système. En d'autres termes, la sortie à tout moment ne dépend que des entrées et de l'état du système à des moments antérieurs, cela implique que l'effet d'une entrée sur la sortie ne peut pas précéder la cause qui l'a produite.
- Déterministe, c'est-à-dire les résultats futurs peuvent être prédits avec certitude à partir des conditions initiales et des lois mathématiques qui régissent le système. Autrement dit, dans un système déterministe, si les conditions initiales sont connues avec précision, l'état futur du système peut être calculé de manière exacte à partir des lois mathématiques qui le régissent sans aucune incertitude ou aléatoire.

### I.2.1 Systèmes dynamiques continus

Un système dynamique continu est représenté par un système des équations différentielles de la forme :

$$\begin{cases} \dot{x}(t) = f(t, x(t)) \\ x(t_0) = x_0 \end{cases} \quad (\text{I.1})$$

Où :  $f : \mathbb{R}^+ \times \mathbb{R}^n \rightarrow \mathbb{R}^n$  représente la dynamique du système en temps continu, et  $x_0$  représente l'état initial en  $t_0$ .

### I.2.2 Systèmes dynamiques discrets

Un système dynamique discret est représenté par un système de équations aux différences de la forme [2]:

$$\begin{cases} x(k+1) = g(x(k), k) \\ x(k_0) = k_0 \end{cases} \quad (\text{I.2})$$

Où :  $g : \mathbb{R}^n \times \mathbb{N} \rightarrow \mathbb{R}^n$  représente la dynamique du système en temps discret, et  $x_0$  représente l'état initial en  $k_0$ .

### I.2.3 Systèmes dynamiques autonomes et non-autonomes

Lorsque le champ de vecteur  $f$  ne dépend pas explicitement du temps, on dit que le système dynamique est autonome [3].

$$\begin{cases} \dot{x}(t) = f(x(t)) \\ x(t_0) = x_0 \end{cases} \quad (\text{I.3})$$

Par contre le système est non autonome si le champ de vecteur  $f$  dépend de temps  $t$  :

$$\begin{cases} \dot{x}(t) = f(x(t), t) \\ x(t_0) = x_0 \end{cases} \quad (\text{I.4})$$

## I.3 Système chaotique

Un système dynamique chaotique est un système qui présente un comportement complexe et imprévisible à long terme malgré des règles de comportement simples et déterministes. Cela signifie que de petites différences dans les conditions initiales peuvent conduire à des résultats très différents à long terme, rendant difficile la prédiction précise du comportement du système à long terme. Les exemples courants de systèmes dynamiques chaotiques comprennent le système météorologique, le système solaire, le mouvement d'un pendule double, les attracteurs de Lorenz, et bien d'autres. Ces systèmes ont une importance théorique et pratique, car ils peuvent modéliser un large éventail de phénomènes physiques, biologiques et économiques [4]. Dans ce qui suit, nous passerons en revue les caractéristiques les plus importantes des systèmes chaotiques

### I.3.1 La non-linéarité

Un système chaotique est un exemple de système dynamique non linéaire. Les systèmes linéaires sont caractérisés par des relations linéaires entre les variables, ce qui signifie que si l'on double l'entrée, la sortie sera également doublée. En revanche, les systèmes non linéaires ont des relations plus complexes et souvent non prévisibles entre les variables, ce qui peut conduire à des comportements chaotiques. Les systèmes chaotiques sont sensibles aux conditions initiales et peuvent afficher des comportements imprévisibles même si leurs équations sous-jacentes sont déterministes.

### I.3.2 Déterministe

Le déterminisme se réfère à l'idée qu'à partir d'un événement ou d'un phénomène, il est possible de prédire son futur en utilisant des lois ou des principes physiques. Dans le cas des systèmes chaotiques, bien qu'ils soient déterministes (leurs équations sous-jacentes sont connues et décrivent leur comportement dynamique), leurs comportements à long terme peuvent être extrêmement difficiles à prédire, même si leur état initial est connu avec une grande précision [5].

### I.3.3 Aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires. La figure (I.1) illustre l'état chaotique  $x_1$  du système de Rossler [6].

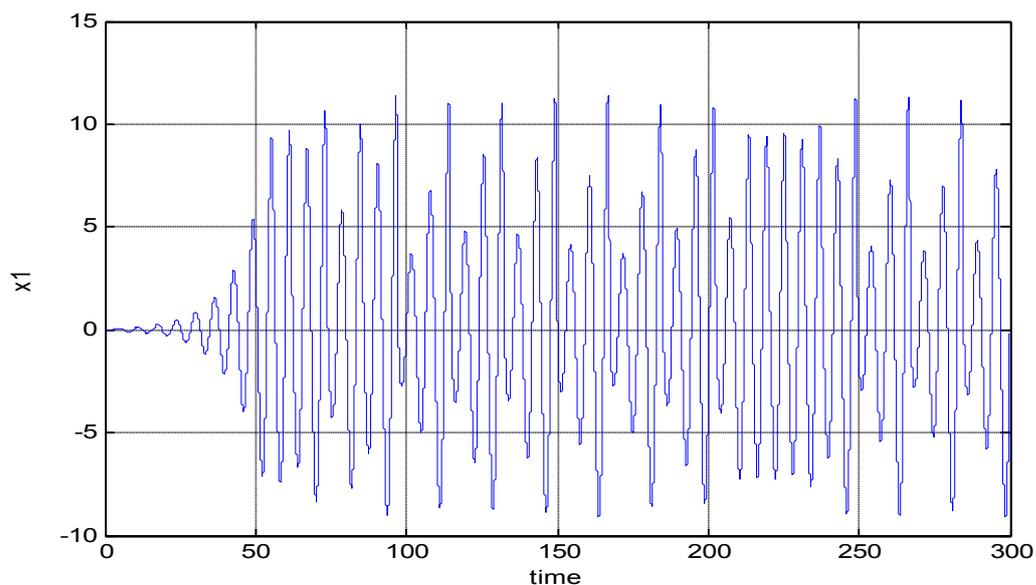
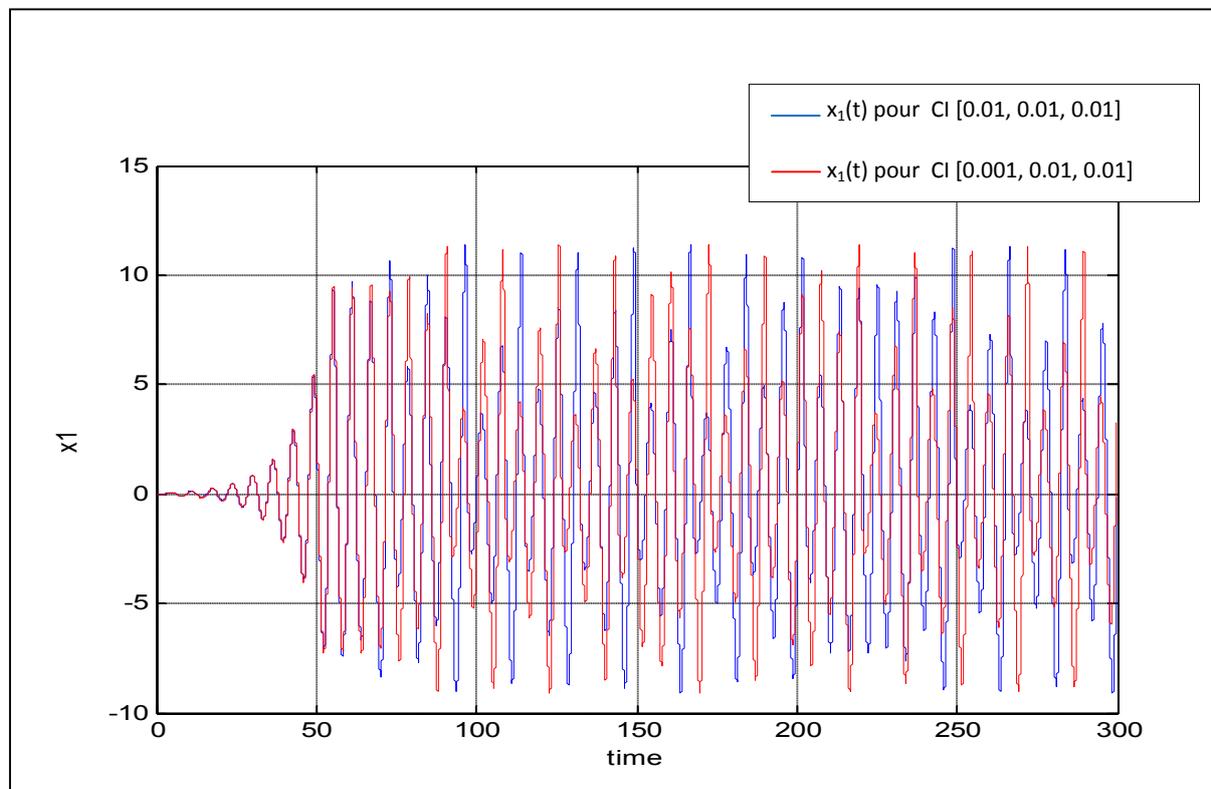


Figure I.1. Etat chaotique  $x_1$  du système de Rossler.

### I.3.4 Sensibilité aux conditions initiales

Les systèmes chaotiques, comme le système météorologique, sont extrêmement sensibles aux conditions initiales, ce qui signifie que de petites perturbations dans les conditions initiales peuvent entraîner des résultats très différents dans l'évolution du système à long terme. L'effet de papillon fait référence à l'idée que de petits changements dans un système complexe peuvent avoir des effets disproportionnés et imprévisibles sur le système à long terme. En raison de cette sensibilité aux conditions initiales, il est souvent impossible de prédire avec précision l'évolution à long terme des systèmes chaotiques. Cette propriété est l'une des caractéristiques clés des systèmes chaotiques et a des implications importantes dans de nombreux domaines.



**Figure I.2.** Illustration de la propriété de sensibilité aux conditions initiales de la variable d'état  $x_1$  (système de Rossler).

### I.4 Application du chaos

Le chaos peut s'appliquer dans des diverses applications, on peut mentionner les applications suivantes :

- **Contrôle** : en effet, l'une des premières applications du chaos a été dans le domaine du contrôle des systèmes dynamiques non linéaires tels que les circuits électriques et les systèmes mécaniques. Les systèmes chaotiques peuvent avoir des comportements imprévisibles, mais ils présentent également des motifs récurrents appelés attracteurs étranges. Ces attracteurs étranges peuvent être utilisés pour contrôler et stabiliser les systèmes chaotiques en leur donnant une trajectoire d'évolution particulière.
- **Synchronisation** : le chaos a également des applications dans la communication sécurisée, le cryptage et les systèmes de radio.
- **Traitement d'information** : les systèmes chaotiques présentent des propriétés uniques qui ont des applications potentielles dans la cryptographie, la communication sécurisée, le stockage d'informations et les circuits électroniques.
- **Prédiction à court terme** : les maladies contagieuses, température, économie[7].

### I.5L'espace de phase

L'espace de phase est un outil mathématique utilisé pour décrire l'évolution d'un système dynamique au fil du temps. Il est défini comme un ensemble de toutes les configurations possibles du système à un instant donné, représentées par des vecteurs dans un espace de dimension égale au nombre de variables d'état du système. Chaque vecteur dans l'espace de phase représente une configuration du système à un instant donné. L'évolution du système dans le temps peut être représentée par une trajectoire dans cet espace de phase, qui est décrite par une courbe continue reliant les vecteurs représentant l'état du système à des instants différents [8.9]

### I.6 Notion d'attracteurs

Un attracteur est une région de l'espace des états vers laquelle les trajectoires du système convergent ou restent confinées au fil du temps. Il représente un ensemble de valeurs ou une configuration stable que le système tend à atteindre ou autour duquel il oscille [10].

#### I.6.1 Les différents types d'attracteurs

On distingue deux types d'attracteurs :

- ✓ **Attracteurs réguliers** : Les attracteurs réguliers caractérisent l'évolution de systèmes non chaotiques, et peuvent être de trois sortes [11].

- **Point fixe** :Lorsque l'on dit que le système tend à se comporter de manière statique, cela signifie que le système a une faible capacité à changer ou à s'adapter aux nouvelles situations.
- **Cycle limite** :Lorsque l'on dit que le système présente un comportement oscillatoire qui se maintient sur le long terme, cela signifie que le système suit un cycle répétitif de fluctuations qui se répètent à intervalles réguliers.
- **Attracteur quasi-périodique** : Lorsqu'un système est identifié avec un tore dans l'espace de phase, cela signifie que le comportement du système suit un motif en forme de tore dans l'espace de phase.
- ✓ **Attracteur étrange** :Un attracteur étrange, également connu sous le nom d'attracteur chaotique, est un concept issu de la théorie du chaos en mathématiques et en dynamique des systèmes. Il se réfère à un ensemble de points dans l'espace des phases d'un système dynamique non linéaire qui exhibe un comportement chaotique. L'attracteur étrange est généralement fractal, ce qui signifie qu'il présente une structure répétitive à différentes échelles. Il peut avoir des formes complexes et asymétriques, avec des boucles, des plis, des spirales ou d'autres motifs géométriques. Les trajectoires des points dans l'attracteur étrange peuvent sembler erratiques, mais elles restent confinées à l'attracteur et ne s'échappent pas. Les attracteurs étranges sont étudiés dans divers domaines scientifiques, notamment la physique, la biologie, l'économie et la météorologie. Ils jouent un rôle important dans la modélisation de phénomènes complexes et dans la compréhension des systèmes dynamiques chaotiques [12].

## I.6.2 Des différents exemples d'attracteurs

### I.6.2.1 Attracteur étrange de Lorenz

Le système de Lorenz est décrit par un ensemble de trois équations différentielles ordinaires, qui résumel'ensemble des prévisions météorologiques. Les équations sont les suivantes :

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

Dans ces équations,  $x$ ,  $y$  et  $z$  sont les variables d'état du système,  $t$  représente le temps, et  $\sigma$ ,  $\rho$  et  $\beta$  sont des paramètres qui contrôlent le comportement du système [13].Les résultats de la

résolution de ce système sont donnés dans les figures (I.3) et (I.4), où on voit les états chaotiques  $x(t)$ ,  $y(t)$ ,  $z(t)$ , et l'attracteur du système de Lorenz  $(x,y,z)$ . Pour  $(\sigma=10 ; \rho=28 ; \beta=8/3)$ , et les conditions initiales  $[x(0)=0 ; y(0)=1 ; z(0)=20]$ .

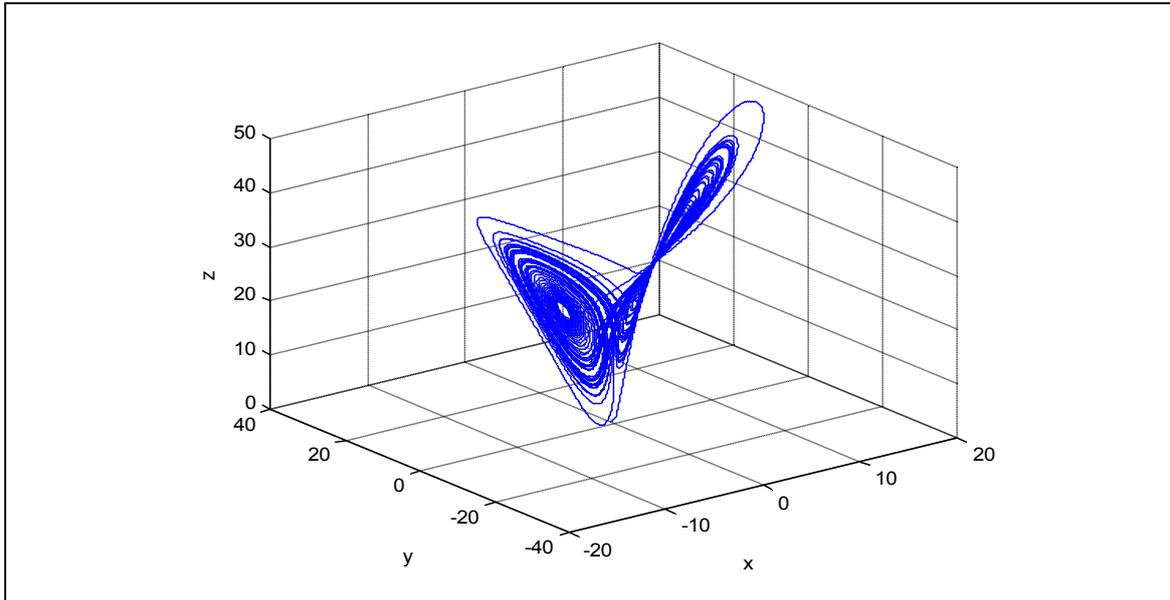


Figure I.3. Attracteur étrange de Lorenz

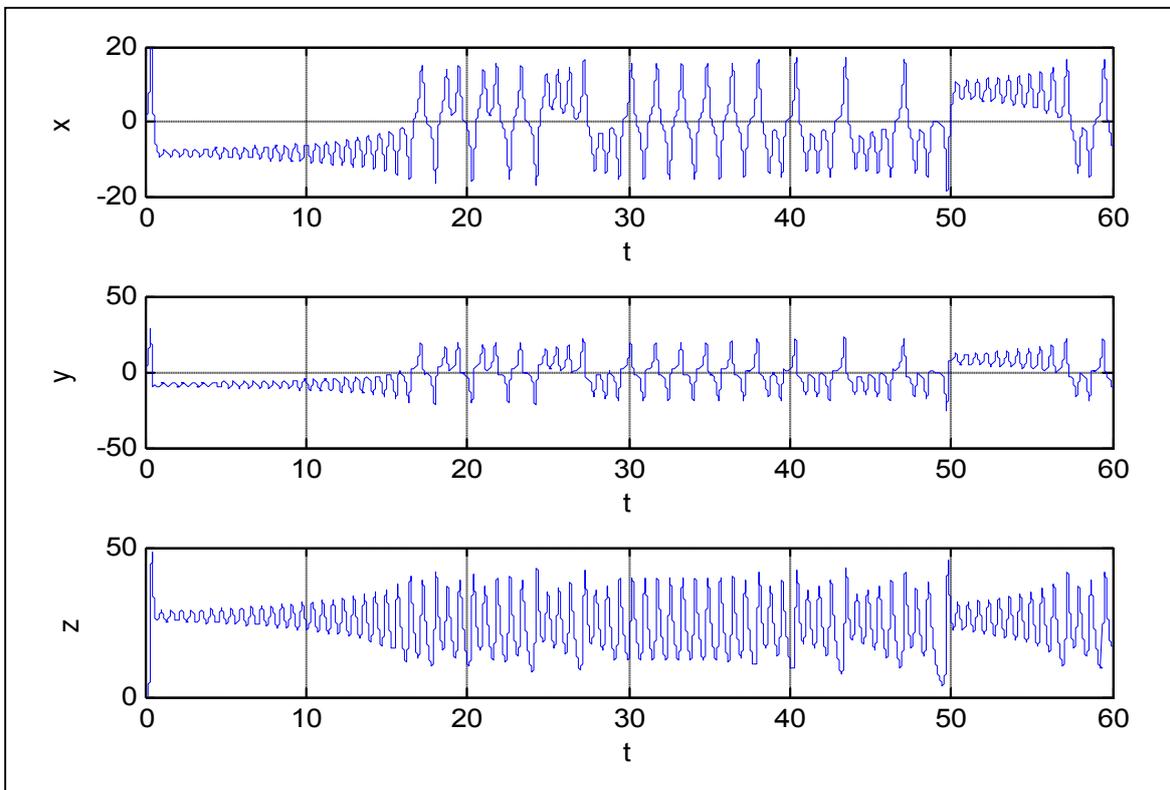


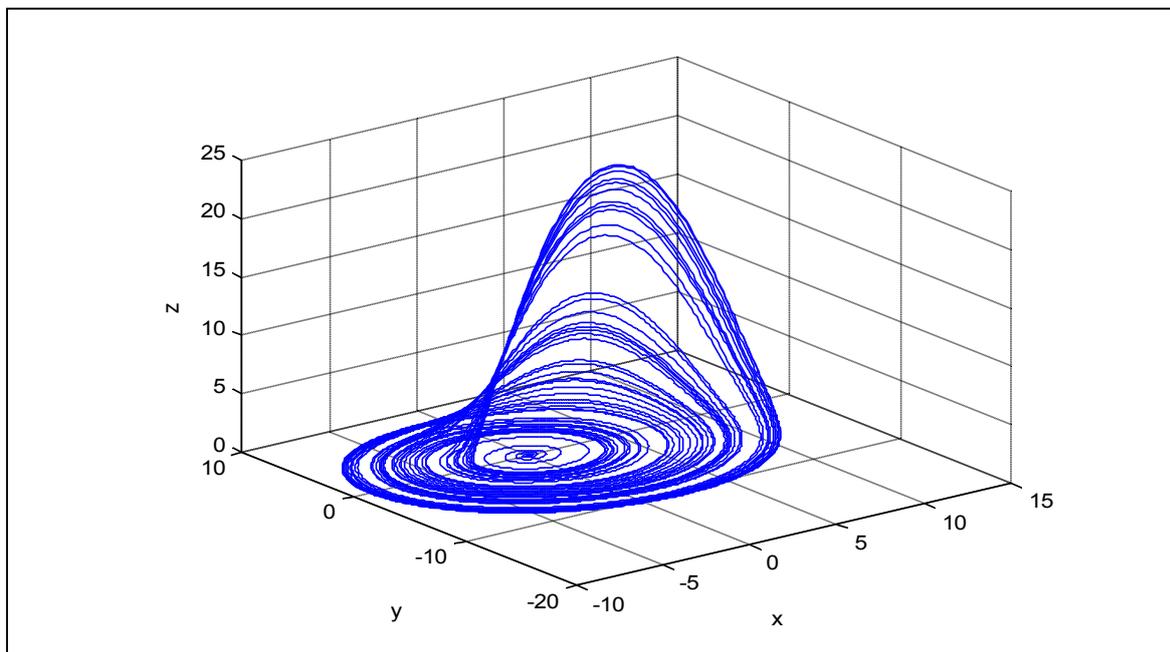
Figure I.4. États chaotiques du système de Lorenz

### I.6.2.1 Attracteur étrange de Rossler

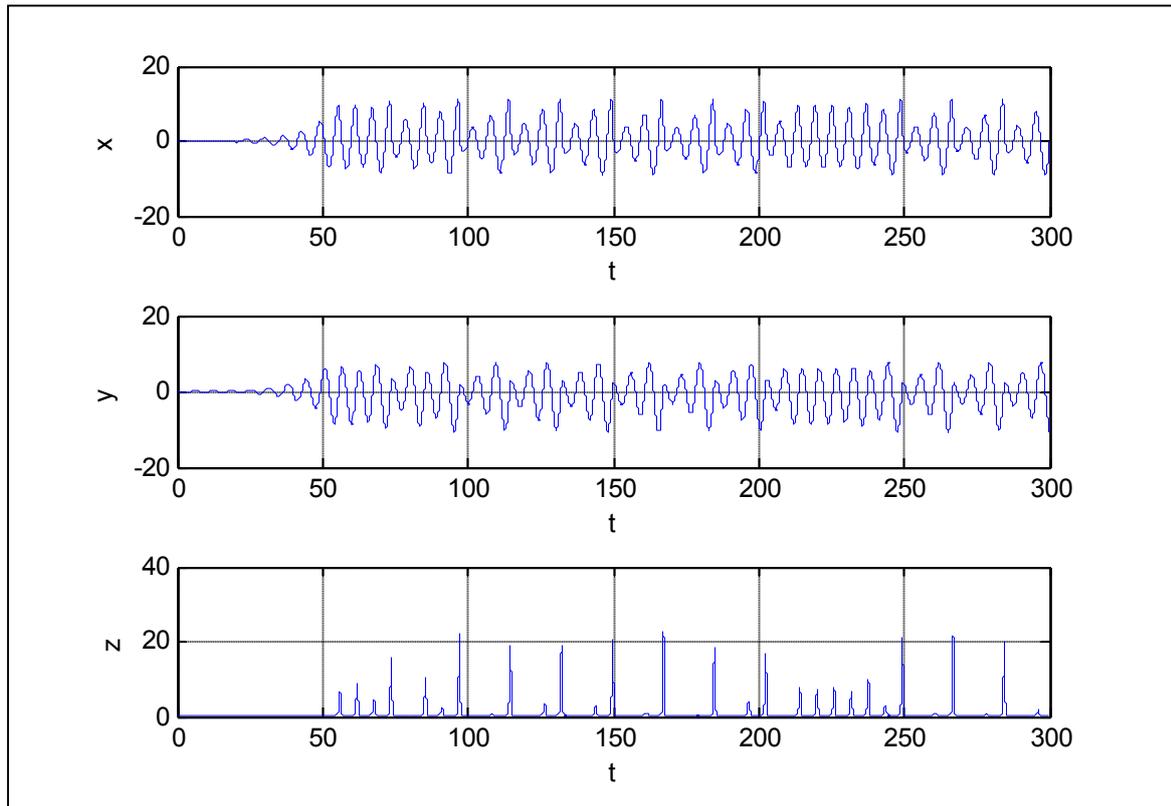
L'attracteur de Rossler est un exemple d'un attracteur chaotique produit par un système dynamique constitué de trois équations différentielles ordinaires introduites par Otto Rossler en 1976 [13]. Les équations sont les suivantes :

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \quad (\text{I.6})$$

Où  $x$ ,  $y$  et  $z$  sont les variables d'état du système, et  $a$ ,  $b$  et  $c$  sont les paramètres de ce système. Le terme non linéaire  $z(x - c)$  est ce qui introduit le comportement chaotique dans le système. Le comportement chaotique du système peut être visualisé en traçant l'attracteur de Rossler dans l'espace des phases (c'est-à-dire en traçant  $x$ ,  $y$  et  $z$  les uns contre les autres). L'attracteur de Rossler ressemble à un papillon ou à une figure en forme de huit, avec des oscillations chaotiques de trois dimensions. La représentation graphique de ce système est donnée dans la figure (I.5) et figure (I.6), où on voit l'attracteur de Rossler, et les états chaotique de système Rossler pour ( $a=0.2$  ;  $b=0.2$  ;  $c=5.7$ ), et les conditions initiales [ $x(0)=0.01$  ;  $y(0)=0.01$  ;  $z(0)=0.01$ ].



**Figure I.5.** Attracteur étrange de Rossler



**Figure I.6.** Etats chaotique du système de Rossler

### I.7 Exposants de Lyapunov

Les exposants de Lyapunov sont une mesure de la vitesse à laquelle les trajectoires d'un système dynamique se séparent les unes des autres, cette mesure est utilisée pour quantifier le niveau de chaos dans un système dynamique. Les exposants de Lyapunov ont été introduits pour la première fois par le mathématicien russe Aleksandr Oseledec en 1968. Ils sont nommés d'après le mathématicien russe Mikhaïl Lyapunov, qui a également travaillé sur la théorie du chaos.

L'exposant de Lyapunov est utilisé pour évaluer la stabilité d'un système et permet de mesurer la sensibilité aux conditions initiales d'un système chaotique. Le nombre d'exposants de Lyapunov est égal à la dimension de l'espace de phase, et ils sont généralement classés par ordre décroissant, du plus grand au plus petit [14].

L'exposant de Lyapunov se définit alors comme :

$$\lambda_i = \lim_{t \rightarrow \infty} \frac{1}{t} \ln \left( \frac{\delta_i(t)}{\delta_i(0)} \right), i = 1, \dots, n \quad (\text{I.7})$$

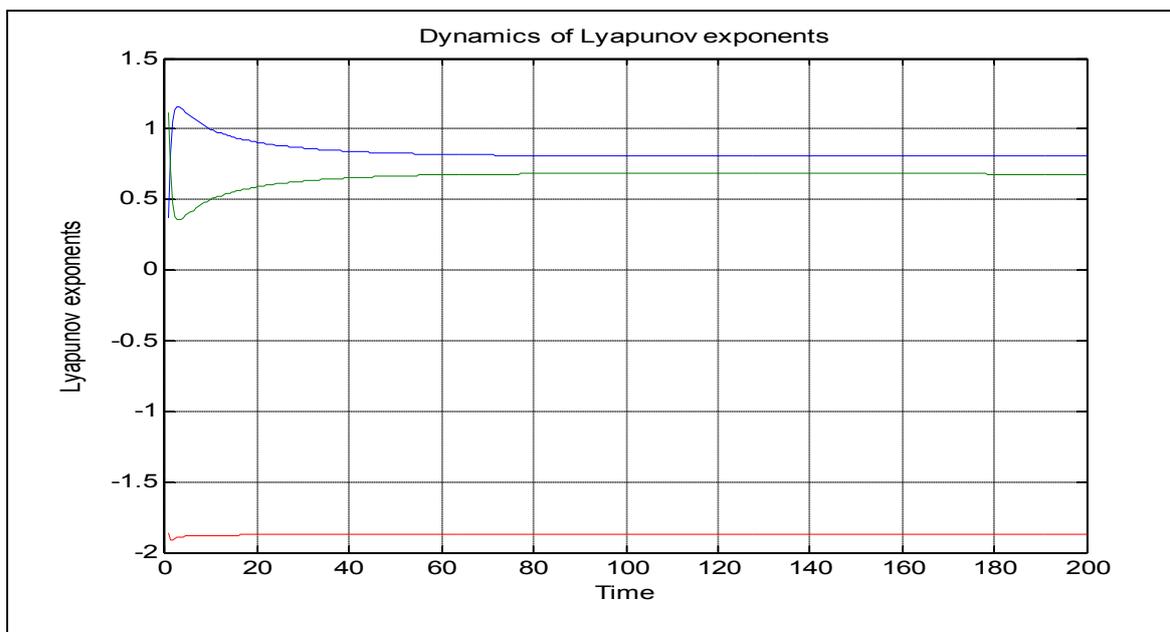
Le tableau (II.1) illustre la classification des comportements des systèmes dynamiques en fonction des exposants de Lyapunov [15].

LE	L'attracteur	Dimension
$\lambda_n \leq \dots \leq \lambda_1 < 0$	Un point fixe.	<b>0</b>
$\lambda_1 = 0 ; \lambda_n \leq \dots \leq \lambda_2 < 0$	Une orbite fermée.	<b>1</b>
$\lambda_1 = \lambda_k = 0 ;$ $\lambda_n \leq \dots \leq \lambda_{k+1} < 0$	L'attracteur est quasi périodique (k fréquences)	<b>K</b>
$\lambda_1 > 0 ; \sum_{p=1}^n \lambda_p < 0$	L'attracteur est chaotique (attracteur étrange)	<b>Non entier.</b>
$\lambda_1 > \dots > \lambda_k > 0$ $\sum_{p=1}^n \lambda_p < 0$	L'attracteur est hyper chaotique (attracteur étrange)	<b>Non entier.</b>

**Tableau I.1.** Classification des comportements de système selon les exposants de Lyapunov.

### I.7.1 Exemple

Utilisant un programme Matlab, les exposants de Lyapunov pour le système de Lorenz sont calculés. Les résultats sont donnés dans la figure (I.7). Réf[ Tableau I.1].



**Figure I.7.** Les exposants de Lyapunov pour Lorenz ( $\sigma = 10 ; \rho = 28 ; \beta = \frac{8}{3}$ ).

D'après la figure (I.7), On a trouvé ( $\lambda_1 = 0.895324$ ,  $\lambda_2 = -0.011335$ ,  $\lambda_3 = -14.547109$ ), et donc on conclure que le comportement est chaotique.

### I.8 Section de Poincaré

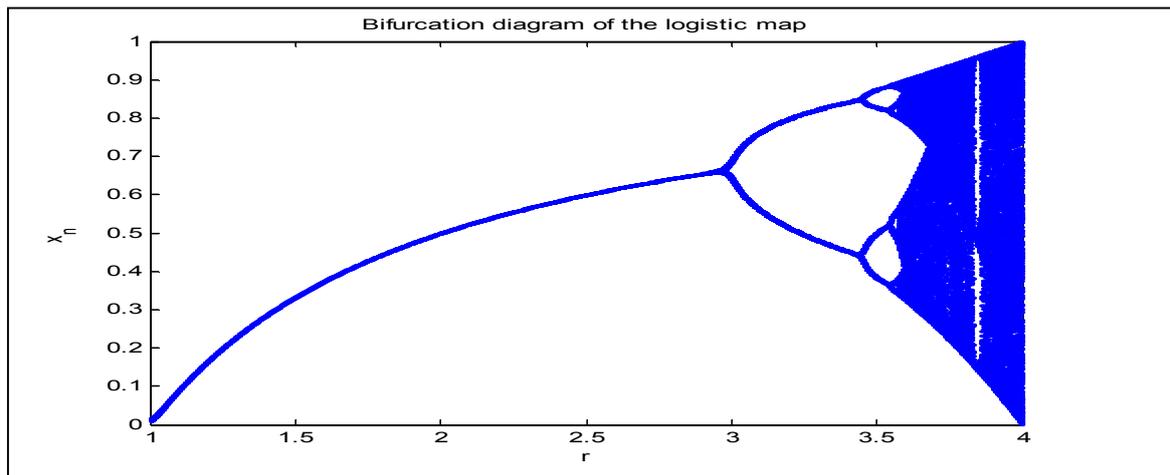
La section de Poincaré d'un système dynamique est une construction mathématique utilisée pour étudier le comportement d'un système à travers une surface de coupe fixe. Cette surface de coupe est généralement choisie de manière à traverser périodiquement l'orbite du système. En examinant les points d'intersection entre l'orbite et la surface de coupe, on peut analyser les propriétés dynamiques du système, telles que la stabilité, la périodicité ou le chaos. La section de Poincaré permet ainsi de simplifier l'étude d'un système dynamique en réduisant sa dimensionnalité tout en conservant les informations essentielles sur son comportement [16,17,18,19].

### I.9 Bifurcation

Un diagramme de bifurcation est un outil graphique utilisé pour visualiser les bifurcations et les transitions de comportement d'un système dynamique en fonction d'un paramètre de contrôle. Il représente les valeurs stables ou périodiques des états d'équilibre du système en fonction de ce paramètre [20]. Pour construire un diagramme de bifurcation, on fixe les conditions initiales du système et on fait varier le paramètre de contrôle. On observe alors les valeurs stables ou périodiques atteintes par le système à chaque valeur du paramètre. Ces valeurs sont généralement représentées sur l'axe vertical du diagramme, tandis que les valeurs du paramètre de contrôle sont représentées sur l'axe horizontal. Le diagramme de bifurcation permet d'identifier les bifurcations, c'est-à-dire les points où le système passe d'un comportement stable à un comportement périodique, ou d'un comportement périodique à un comportement chaotique. Il peut également révéler des motifs de répétition, des points de stabilité ou d'instabilité, et d'autres caractéristiques intéressantes du système dynamique. La figure (I.8) illustre le diagramme de bifurcation de la fonction logistique, qui est un exemple des systèmes dynamiques unidimensionnels discrets définie par la fonction :

$$f: [0; 1] \rightarrow [0; 1] x_{k+1} = f(x_k) = rx_k(1 - x_k) \quad (I.8)$$

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



**Figure I.8.** Diagramme de bifurcation de la fonction logistique

$r$  est responsable de comportement de cette dynamique.

Le diagramme de bifurcation de la fonction logistique figure (I.8) illustre que le système dynamique non linéaire présente des comportements périodiques pour certaines valeurs du paramètre  $r$ , tandis que pour d'autres valeurs, il devient chaotique. Les divers comportements possibles de ce système peuvent être résumés dans le tableau ci-dessous :

**Tableau I.2.** Les différents comportements possibles de la fonction logistique

La valeur de $r$	Le comportement de système
$1 \leq r < 3$	Le comportement de système est périodique
$3 \leq r < 3.373$	Le comportement est quasi-périodique avec $2^m$ périodes, ou $m$ est un entier
$3.57 \leq r < 4$	Le comportement de système est chaotique

### I.10 Routes vers chaos

Routes vers le chaos font référence aux différentes voies par lesquelles un système dynamique peut passer d'un comportement périodique à un comportement chaotique. On distingue trois scénarios théoriques d'évolution vers le chaos [21].

### **I.10.1. Le doublement de période**

Dans ce scénario, l'augmentation d'un paramètre de contrôle pour un système périodique permet de l'apparition d'un doublement de période (2, 4, 8, 16,...), les doublements étant de plus en plus convergés jusqu'à l'obtention d'un nombre infini des périodes.

### **I.10.2. L'intermittence**

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière[22].

### **I.10.3. La quasi périodicité**

Ce scénario intervient pour un système périodique quand un deuxième oscillateur le perturbe et dont le rapport des deux  $n$ 'est pas rationnel.

## **I.11 Conclusion**

Dans ce premier chapitre, nous avons présenté quelques notions théoriques sur les systèmes dynamiques chaotiques. Ces notions seront utilisées par la suite, lors de l'étude de la dynamique de l'oscillateur Colpitts amélioré.

**Chapitre II**  
**Transmission chaotique**

## II.1 Introduction

L'utilisation des systèmes chaotiques dans les transmissions sécurisées est devenue une pratique courante au cours des dernières décennies. Les systèmes chaotiques offrent une sécurité accrue en raison de leur comportement aléatoire et de leur hypersensibilité aux conditions initiales, ce qui les rend difficiles à prédire et à intercepter. Cette caractéristique ouvre des perspectives applicatives importantes pour la sécurité des transmissions de données confidentielles.

La cryptologie est un domaine qui s'intéresse à la protection des informations confidentielles dans les systèmes informatiques et de télécommunications. Le cryptage est une technique de sécurité qui permet de transmettre des données confidentielles sur un réseau non sécurisé sans que des tiers puissent y accéder. Les algorithmes de chiffrement actuels, qu'ils soient à clé symétrique ou asymétrique, sont largement utilisés pour protéger les informations et pour garantir l'intégrité, l'authentification et la non-répudiation des données.

En résumé, l'utilisation de systèmes chaotiques dans les transmissions sécurisées est une pratique prometteuse pour renforcer la sécurité des données confidentielles. La cryptologie et les algorithmes de chiffrement actuels sont des outils importants pour la protection de l'information et pour répondre aux préoccupations croissantes en matière de sécurité des données dans l'ère de la nouvelle révolution industrielle en informatique et dans les télécommunications.

## II.2 Objectifs des crypto-systèmes

Le crypto-système assure et garantit :

- **La confidentialité**, assuré 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**, elle consiste en l'assurance qu'une action sur la donnée réalisée au nom d'un utilisateur (après l'authentification).

## II.3 Cryptographie

La cryptographie est l'étude et la pratique de techniques visant à sécuriser la communication et à protéger l'information contre des tiers non autorisés. Elle utilise des algorithmes mathématiques pour chiffrer les données, c'est-à-dire les rendre illisibles, afin que seules les personnes disposant de la clé appropriée puissent les déchiffrer et les comprendre

[23]. La cryptographie est utilisée dans de nombreux domaines, tels que les communications en ligne, les transactions financières, la protection des données sensibles et la sécurité des systèmes informatiques. Son objectif principal est de garantir la confidentialité, l'intégrité et l'authenticité des informations échangées [24]. Il existe deux classes de système de cryptographie :

### II.3.1 Les systèmes symétriques ou la clé secrète

La cryptographie symétrique, également connue sous le nom de cryptographie à clé secrète, est une méthode de chiffrement où la même clé est utilisée pour chiffrer et déchiffrer un message. Cette technique est considérée comme la plus ancienne forme de chiffrement et est toujours largement utilisée de nos jours.

L'utilisation d'une clé commune pour chiffrer et déchiffrer les messages implique que si la clé est compromise, tout le contenu chiffré avec cette clé devient vulnérable. Cela signifie que si quelqu'un parvient à accéder à la clé, il peut facilement déchiffrer tous les messages chiffrés avec cette même clé. C'est pourquoi il est essentiel de conserver la clé secrète et de la protéger de manière adéquate.

Dans la cryptographie symétrique, il existe plusieurs algorithmes de chiffrement, tels que le chiffrement par blocs et le chiffrement par flux. Les algorithmes de chiffrement par blocs chiffrent le message en blocs de taille fixe, tandis que les algorithmes de chiffrement par flux chiffrent le message en continu.

Bien que la cryptographie symétrique soit une technique de chiffrement très efficace et rapide, elle présente des limites en termes de sécurité, notamment en ce qui concerne la distribution et la gestion des clés. C'est pourquoi la cryptographie asymétrique (ou à clé publique) a été développée pour pallier à ces problèmes, la figure (II.1) présente le principe de chiffrement symétrique ou l'algorithme à la clé secrète.

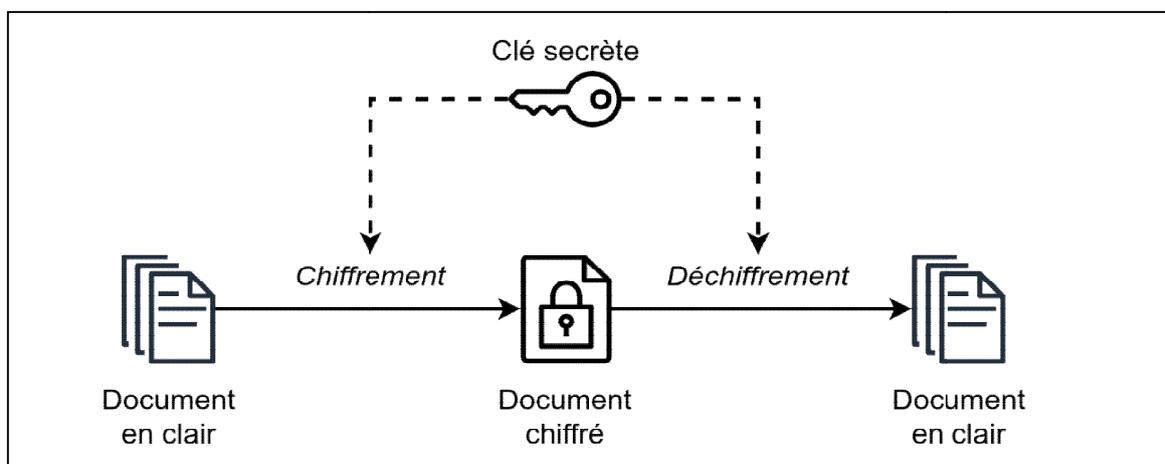


Figure II.1.Principe de chiffrement symétrique

### II.3.2 Les systèmes asymétriques ou la clé publique

Le système de chiffrement asymétrique, également appelé cryptographie à clé publique, a été inventé dans les années 1970 par Winfield Diffie et Martin Helmand [25]. Dans ce système, chaque utilisateur dispose d'une paire de clés, une clé publique et une clé privée. La clé publique est disponible pour tout le monde et peut être utilisée pour chiffrer des messages à destination de l'utilisateur, tandis que la clé privée est conservée secrète et utilisée pour déchiffrer les messages chiffrés avec la clé publique.

Le chiffrement asymétrique est considéré comme plus sûr que la cryptographie symétrique, car même si la clé publique est compromise, le contenu des messages reste protégé car seul le possesseur de la clé privée peut les déchiffrer. Cependant, ce type de chiffrement est plus lent et plus complexe que la cryptographie symétrique.

Le chiffrement asymétrique est utilisé dans de nombreuses applications, notamment pour les transactions en ligne, les échanges d'informations sensibles et les signatures électroniques. La figure (II.2) présente le principe de chiffrement asymétrique.

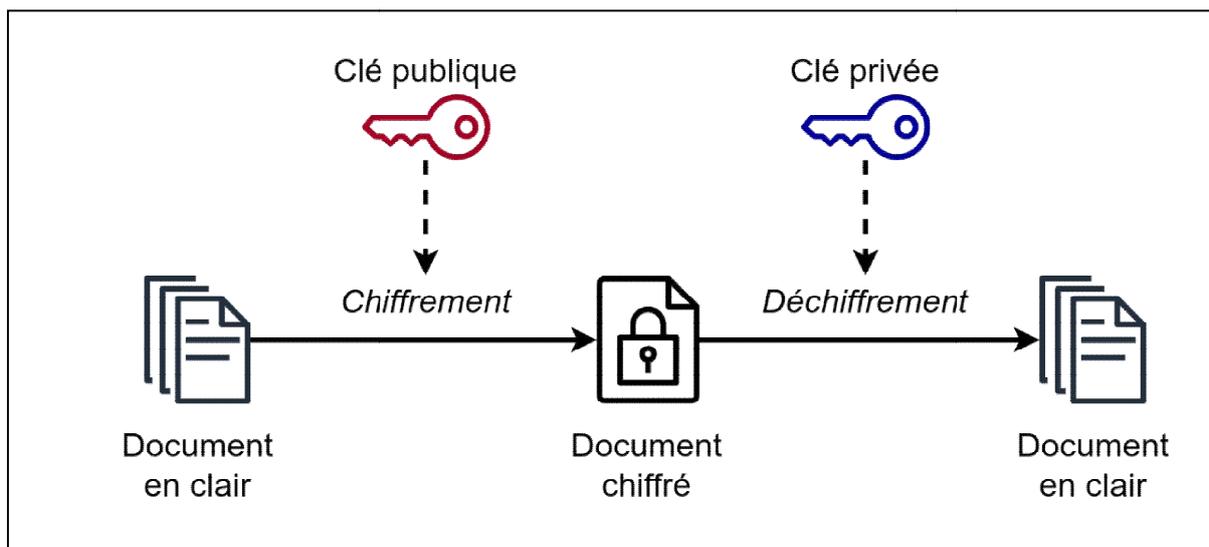


Figure II.2.Principe de chiffrement asymétrique

### II.4 Cryptanalyse

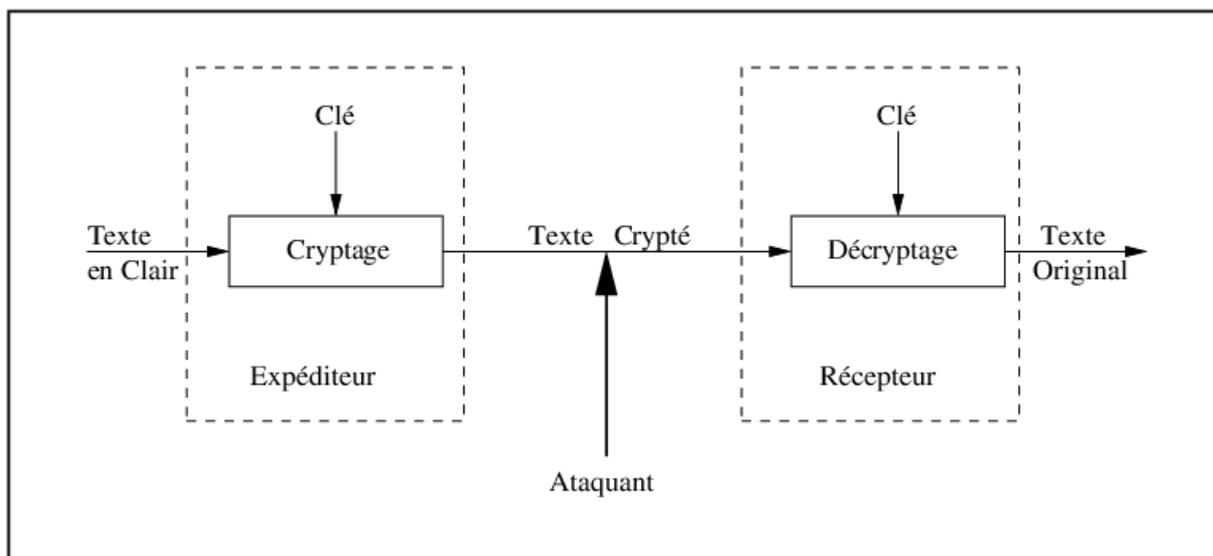
La cryptanalyse est l'art et la science de décoder des messages cryptés sans avoir connaissance de la clé secrète utilisée pour le chiffrement. Elle implique l'analyse systématique des caractéristiques des messages chiffrés et l'application de techniques mathématiques, statistiques et informatiques pour révéler les informations originales.

La cryptanalyse vise à découvrir des faiblesses dans les algorithmes de chiffrement, les protocoles de sécurité ou les systèmes cryptographiques afin de récupérer les données

protégées. Elle peut être utilisée dans un contexte défensif, pour évaluer la sécurité d'un système cryptographique et identifier les vulnérabilités potentielles, ou dans un contexte offensif, pour tenter de casser des codes et accéder à des informations confidentielles.

La cryptanalyse utilise différentes méthodes et techniques, telles que l'analyse de fréquence, l'analyse des motifs, l'attaque par force brute, l'attaque par recherche exhaustive, l'attaque par dictionnaire, l'attaque par faute, l'attaque par canal auxiliaire, la cryptanalyse différentielle, la cryptanalyse linéaire, etc. Ces méthodes peuvent varier en fonction du type de chiffrement utilisé, qu'il s'agisse de chiffrement symétrique ou asymétrique.

En résumé, la cryptanalyse est l'ensemble des techniques et des méthodes utilisées pour analyser et décoder des messages cryptés, dans le but de comprendre leur contenu et de contourner les mécanismes de sécurité mis en place par le chiffrement. Le principe de cryptanalyse est illustré dans la figure (III.3).



**Figure II.3.** Principe de cryptanalyse

### II.5 Techniques de chiffrement par chaos

Le chiffrement par chaos est une méthode de cryptage qui utilise des systèmes chaotiques pour générer des séquences de nombres pseudo-aléatoires qui sont utilisées pour chiffrer les données. Le principe de chiffrement par chaos consiste à ajouter au message à transmettre un signal chaotique généré par un système dynamique chaotique. Ce signal chaotique est utilisé comme clé de chiffrement pour transformer le message en un texte chiffré.

Le processus de chiffrement par chaos est généralement réalisé en trois étapes principales. La première étape consiste à générer un signal chaotique en utilisant un système

dynamique chaotique. La deuxième étape consiste à combiner le signal chaotique avec le message à chiffrer, ce qui produit le texte chiffré. La troisième étape consiste à envoyer le texte chiffré au destinataire, qui peut le déchiffrer en utilisant le signal chaotique comme clé de déchiffrement.

Le chiffrement par chaos est considéré comme une méthode de cryptage très efficace, car les séquences de nombres générées par les systèmes chaotiques sont très difficiles à prédire. Cependant, il est important de souligner que cette méthode peut être vulnérable à des attaques si les systèmes chaotiques ne sont pas correctement choisis ou si les paramètres ne sont pas correctement configurés. Par conséquent, il est important de prendre en compte les bonnes pratiques de sécurité lors de l'utilisation de cette méthode pour garantir une protection efficace des données.

Dans la partie suivante, nous allons présenter les différentes méthodes de chiffrement par les systèmes chaotiques.

### **II.5.1 Chiffrement par addition**

Dans cette méthode, un système chaotique autonome est utilisé comme émetteur. Son signal de sortie  $y(t)$  est additionné avec le message  $m(t)$ , et le signal résultant après la sommation des deux signaux est transmise au récepteur à travers un canal de transmission public. Le récepteur est composé d'un système chaotique identique à celui de l'émetteur et d'un simple soustracteur.

Après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message peut être extrait à l'aide d'une opération de soustraction. Cette méthode est appelée "masquage chaotique" car le signal chaotique généré par l'émetteur "masque" le signal du message, ce qui le rend difficile à détecter pour les personnes qui interceptent le canal de transmission.

Cette méthode est souvent utilisée dans les communications sécurisées, car elle utilise la complexité du chaos pour rendre le message difficile à intercepter et à décoder. Cependant, cette méthode présente également des inconvénients, tels que la difficulté de synchroniser les deux systèmes chaotiques et la vulnérabilité aux attaques par rétroaction [26]. La figure (II.4) montre en détails le principe d'un chiffrement par addition.

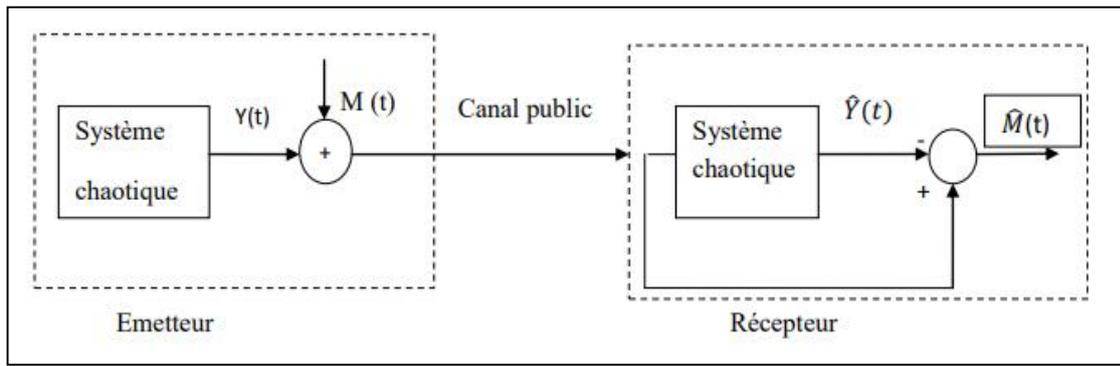


Figure II.4. Chiffrement par addition

II.5.2 Chiffrement par commutation

Cette méthode est utilisée pour transmettre des messages binaires, c'est-à-dire des messages qui prennent seulement deux valeurs, généralement 0 et 1. L'émetteur de cette méthode est composé de deux ou plusieurs systèmes chaotiques. Pour chaque niveau de message  $m(t)$ , l'un des systèmes envoie sa sortie sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étranges, créant un signal chaotique modulé qui contient le message. Le récepteur est constitué de deux systèmes chaotiques identiques ou totalement différents de ceux de l'émetteur, ainsi qu'un bloc de comparaison. Ce bloc permet de relever la valeur du message  $m'(t)$  en comparant la sortie du système chaotique du récepteur avec celle du système chaotique de l'émetteur. Si les deux signaux sont synchronisés, le bloc de comparaison peut déterminer la valeur du message.

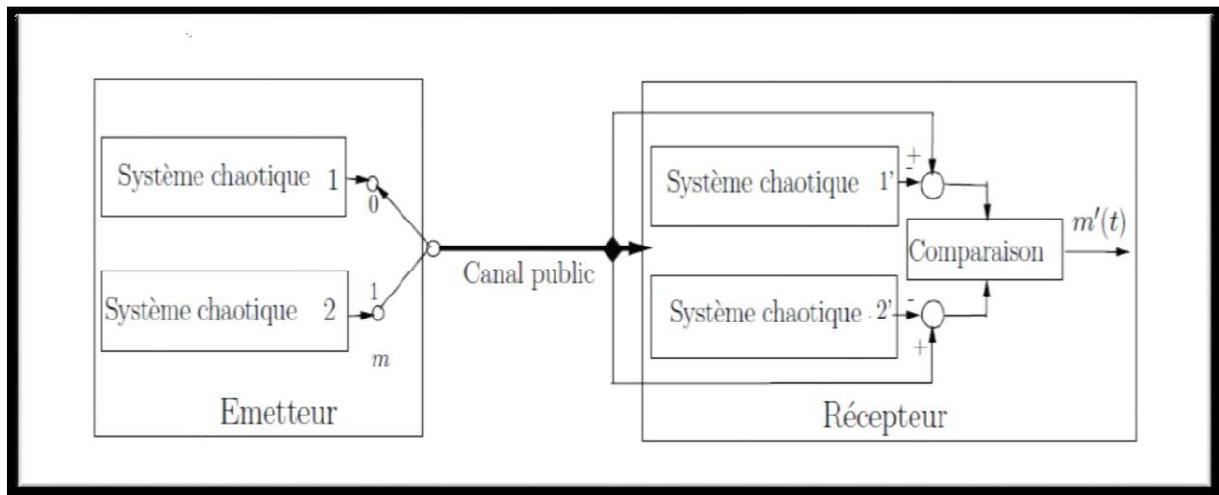


Figure II.5. Chiffrement par commutation

### II.5.3 Chiffrement par modulation

Dans cette technique, le message contenant l'information est utilisé pour moduler un ou plusieurs paramètres de l'émetteur chaotique. Le schéma correspondant est représenté dans la figure (II.6).

Un contrôleur adaptatif est utilisé pour maintenir la synchronisation au niveau du récepteur tout en suivant les changements des paramètres modulés. Au niveau de l'émetteur, la modulation des paramètres force la trajectoire à changer continuellement d'attracteur, ce qui rend le signal transmis plus complexe qu'un signal chaotique "normal".

Cependant, la façon dont le message est injecté et donc la fonction de modulation des paramètres ne doit 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.

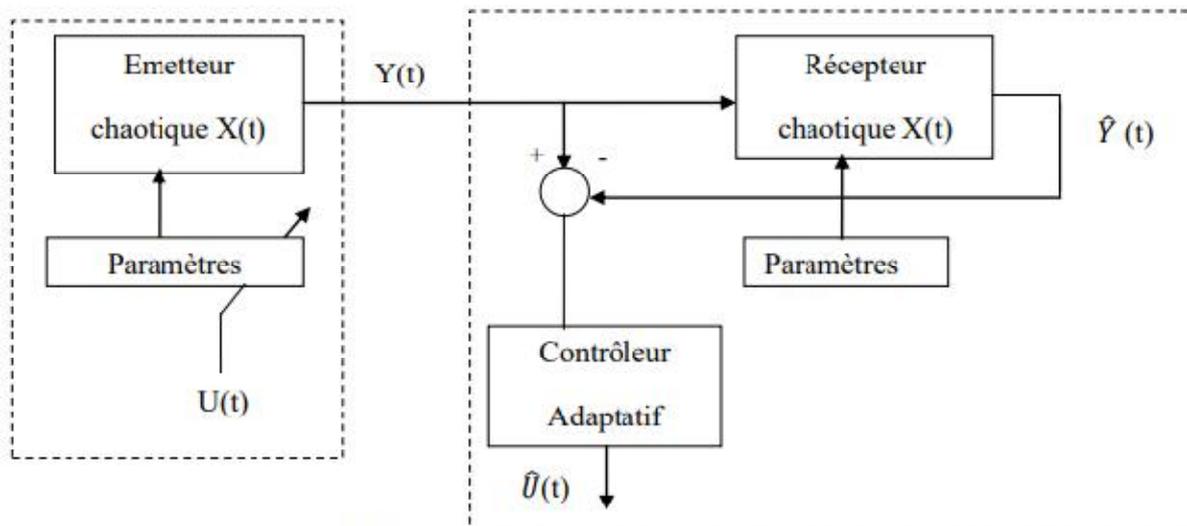


Figure II.6. Chiffrement par modulation

### II.6 Définition de la synchronisation

**Définition (1) :** (Larousse) Synchronisation est un mot grec décomposé en deux parties: Syn. signifie ensemble, et Chrono signifie temps. C'est l'action de mettre en phase pour créer une simultanéité entre plusieurs opérations, en fonction du temps [27].

**Définition (2) :** (générale) La synchronisation est un moyen de maintenir un mouvement périodique (ou chaotique). La synchronisation de deux systèmes dynamiques signifie que chaque système se développe en suivant le comportement de l'autre système [28].

Ce concept repose sur le fait qu'un système chaotique est déterministe et possède un ou plusieurs exposants positifs de Lyapunov et qu'il est instable, si par n'importe quel moyen, deux systèmes puissent échanger de l'énergie, action que l'on nomme couplage, alors la

synchronisation va éventuellement se produire [29]. Plus précisément, deux signaux chaotiques seront dits synchronisés s'ils sont asymptotiquement identiques lorsque  $t$  tend vers l'infini.

## II.7 Classes de synchronisation

Il existe deux classes de synchronisation suivant le sens dont l'énergie est échangée entre les deux systèmes chaotiques ; on distingue la synchronisation par couplage unidirectionnel et la synchronisation par couplage bidirectionnel.

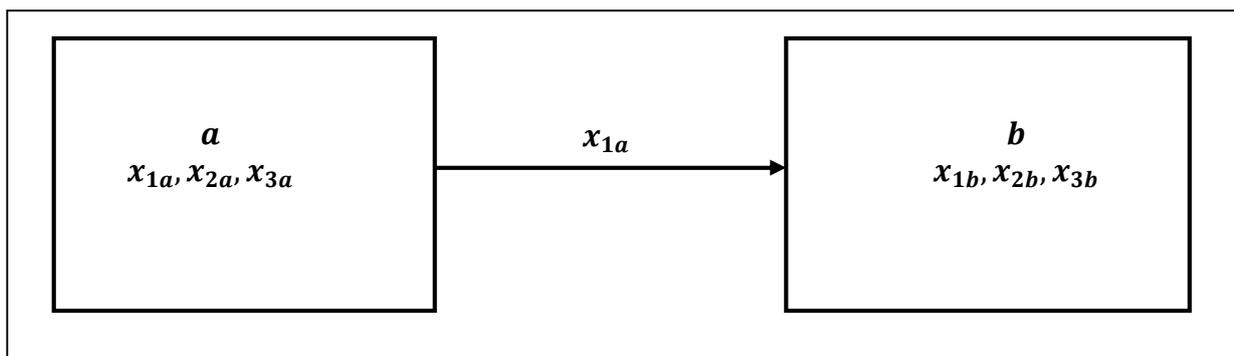
### II.7.1 Synchronisation par couplage unidirectionnel

Dans le cas d'une synchronisation unidirectionnelle, où l'on veut synchroniser un système " $a$ " avec un système " $b$ ", mais pas nécessairement l'inverse, on peut utiliser un couplage unidirectionnel à l'aide d'un élément fonctionnant dans un seul sens.

Un exemple courant de ce type d'élément est le circuit électrique suiveur [30] (ou buffer en anglais), qui permet de répliquer le signal d'entrée sans le modifier ou l'amplifier, et donc de le transmettre sans perte à un autre système.

Dans ce cas, le système " $a$ " envoie son signal à travers le circuit suiveur, qui transmet ce signal sans le modifier au système " $b$ ". Ainsi, le système " $b$ " est synchronisé avec le signal du système " $a$ ", mais le signal du système " $b$ " n'affecte pas le système " $a$ ".

Il est important de noter que ce type de couplage unidirectionnel peut être utilisé dans de nombreux autres domaines que l'électronique, comme la communication entre ordinateurs ou la synchronisation de mouvements entre des robots industriels.



**Figure II.7.** Couplage unidirectionnel

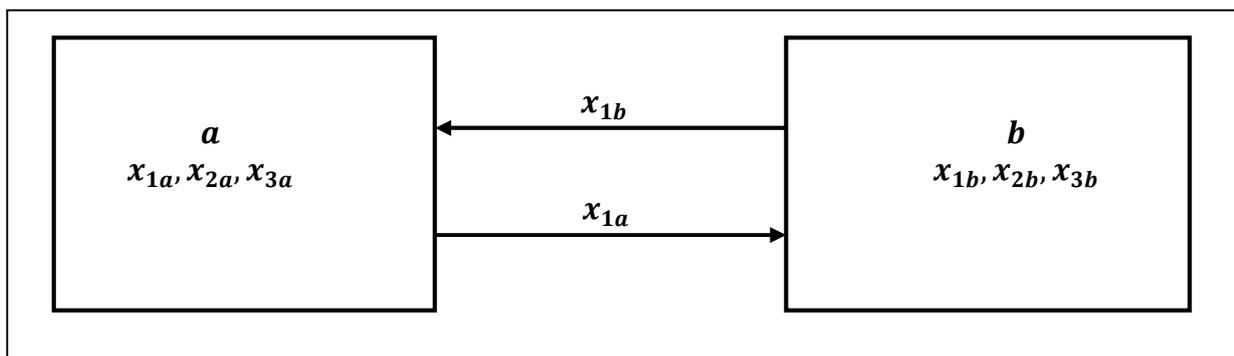
### II.7.2 Synchronisation par couplage bidirectionnel

Dans le cas d'une synchronisation bidirectionnelle, où l'on veut synchroniser deux systèmes " $a$ " et " $b$ " de manière réciproque, on peut utiliser un couplage bidirectionnel à l'aide d'un élément permettant l'échange d'énergie dans les deux sens.

Un exemple courant de ce type d'élément est une simple résistance [31], qui permet d'échanger de l'énergie entre les deux systèmes "a" et "b" dans les deux sens. En utilisant une résistance, le courant peut circuler dans les deux sens, ce qui permet aux deux systèmes de s'influencer mutuellement.

Lorsque les deux systèmes sont couplés bi-directionnellement à travers une résistance, ils peuvent échanger de l'énergie et se synchroniser. Par exemple, si l'un des systèmes commence à envoyer un signal à l'autre, ce signal sera reçu par l'autre système et sera utilisé pour ajuster sa propre sortie en conséquence. Ce processus d'ajustement mutuel peut continuer jusqu'à ce que les deux systèmes soient parfaitement synchronisés.

Il est important de noter que le choix de l'élément de couplage dépendra des caractéristiques spécifiques des systèmes à synchroniser, et que d'autres éléments, tels que les inductances et les capacités, peuvent également être utilisés pour le couplage bidirectionnel.



**Figure II.8.** Couplage bidirectionnel

## II.8 Différents régimes de synchronisation

Il existe de nombreuses méthodes de synchronisation proposées dans la littérature. Voici quelques approches courantes :

### II.8.1 Synchronisation par décomposition de système

La méthode de la synchronisation par répartition du système est une méthode couramment utilisée pour synchroniser des systèmes chaotiques. Cette méthode consiste à diviser le système chaotique en deux sous-systèmes, un maître et un esclave, et à utiliser une rétroaction pour synchroniser le système esclave avec le système maître. Peccora et Carroll ont proposé un système chaotique pour cette méthode de synchronisation, qui est décrit par l'équation de dynamique :

$$\dot{x} = f(x) \quad (\text{II.1})$$

Où  $x$  est le vecteur d'état et  $f$  est une fonction non linéaire qui génère le comportement chaotique. En utilisant une fonction de sortie  $h(x)$ , le signal chaotique peut être transformé en un signal de sortie  $y$  :

$$y = h(x) \quad (\text{II.2})$$

Ce signal de sortie est utilisé pour entraîner le système esclave à suivre le comportement chaotique du système maître. La rétroaction est réalisée en comparant le signal de sortie du système maître avec le signal de sortie du système esclave et en ajustant les paramètres du système esclave pour minimiser la différence entre les deux signaux.

### II.8.2 Synchronisation retardée

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

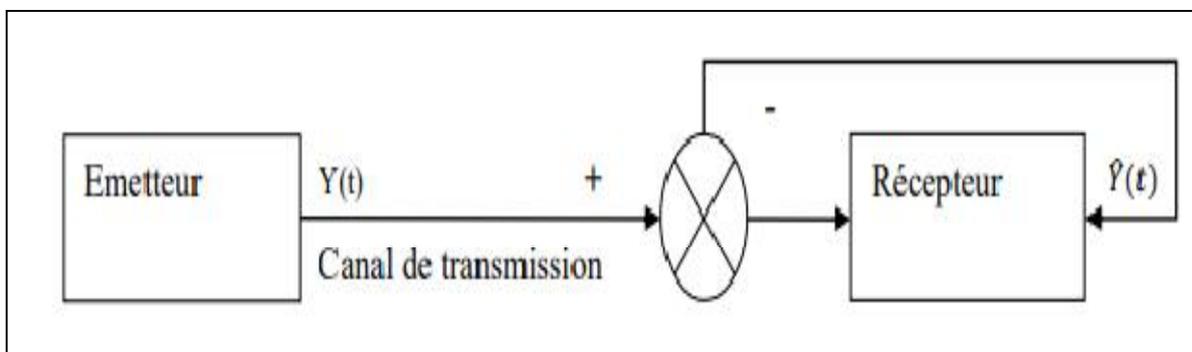
$$\lim_{t \rightarrow \infty} \|x'(t) - x(t - \tau)\| = 0 \quad (\text{II.3})$$

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

### II.8.3 Synchronisation en boucle fermée

La synchronisation par boucle fermée est une méthode de synchronisation de systèmes où l'état du système récepteur est corrigé en temps réel en fonction d'une erreur mesurée entre le signal émis par le système maître et le signal régénéré par le système esclave.

Le fonctionnement de la synchronisation par boucle fermée consiste à comparer le signal émis par le système maître avec le signal reçu par le système esclave décalé dans le temps. La différence entre ces signaux est l'erreur de synchronisation, qui est ensuite utilisée pour ajuster l'état du système esclave afin qu'il se synchronise avec le système maître. La figure (II.9) indique un schéma simplifié de la synchronisation par boucle fermée.



II.9. Synchronisation par boucle fermée

### II.8.4 Synchronisation projective

Le système émetteur envoie son état  $x(t)$  au système récepteur, qui utilise cet état pour ajuster sa sortie  $\hat{x}(t)$  via un contrôleur. Le contrôleur utilise un retard positif  $\tau$  pour permettre à l'état du système émetteur d'être transmis au système récepteur avec un décalage temporel.

Le facteur d'échelle  $\lambda$  est utilisé pour ajuster l'amplitude de la sortie du système récepteur afin de correspondre à celle du système émetteur. La condition de synchronisation dans cette méthode est que la différence entre l'état estimé  $\hat{x}(t)$  du système récepteur et une version retardée à  $x(t-\tau)$  de l'état du système émetteur converge vers zéro lorsque le temps  $t$  tend vers l'infini.

### II.8.5 Synchronisation de phase

Pour deux systèmes périodiques de phase  $\theta_1$  et  $\theta_2$ , la synchronisation peut être exprimé par la relation suivante :

$$|n\phi - m\phi| < c \quad (\text{II.4})$$

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  $\psi(t)$  une fonction complexe définie comme suit :

$$\Psi(t) = s(t) + j\tilde{s}(t) = A(t).e^{j\phi(t)} \quad (\text{II.5})$$

Où  $\tilde{s}(t)$  est la transformée de Hilbert de la série temporelle  $s(t)$ ,  $A(t)$  est l'amplitude du signal  $\psi(t)$  et  $\phi(t)$  sa phase [33].

### II.8.6 Anti synchronisation

Le système maître et le système esclave sont dits prêts pour effectuer l'anti-synchronisation entre ces deux systèmes, s'il existe un contrôle  $u(t; x; y)$  tel que l'équation :

$$\lim_{t \rightarrow \infty} |y(t) + x(t)| = 0 \quad (\text{II.6})$$

Est satisfaite, pour toutes conditions initiales  $x(0)$  et  $y(0)$  des deux systèmes.

### II.8.7 Synchronisation par observateur

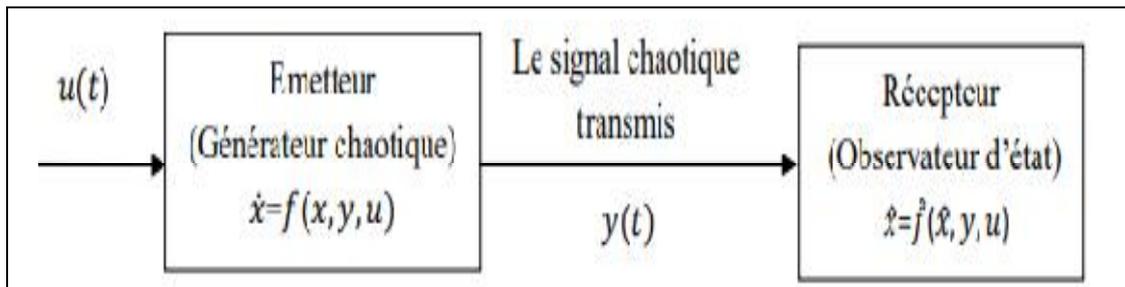
L'observateur d'état est un système dynamique qui permet d'estimer l'état non mesuré d'un système à partir de ses entrées et sorties, ainsi que de la connaissance de son modèle dynamique. En d'autres termes, l'observateur d'état permet de reconstruire l'état interne d'un système à partir d'informations limitées sur ce système.

Dans le cas de la synchronisation chaotique, l'observateur d'état est utilisé pour estimer l'état du système maître à partir de ses sorties, qui sont transmises au système esclave. Le système esclave est ensuite ajusté en fonction de cette estimation pour reproduire le comportement chaotique du système maître.

Cette approche de synchronisation chaotique a ouvert la voie à de nombreuses autres méthodes et techniques de synchronisation, qui ont permis de synchroniser des systèmes chaotiques dans des conditions plus générales et plus complexes. Théoriquement, le problème de la conception d'un observateur pour un système (non linéaire) est défini comme suit :

$$\|x(t) - \hat{x}(t)\| \rightarrow 0 \text{ Quand } t \rightarrow \infty \quad (\text{II.7})$$

Où  $x(t)$  est l'état du système et  $\hat{x}(t)$  est l'état estimé. La figure suivante présente le principe de synchronisation à base d'observateurs.



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

L'utilisation d'un observateur est une méthode courante pour estimer les états inconnus d'un système dynamique qui ne peuvent pas être mesurés directement. Cela peut être particulièrement utile pour la synchronisation de systèmes chaotiques, où les états internes peuvent être difficiles à mesurer avec précision.

Dans le contexte de la synchronisation chaotique, l'observateur est utilisé pour estimer l'état du système maître à partir de ses sorties, qui sont transmises au système esclave. Le système esclave est ensuite ajusté en fonction de cette estimation pour reproduire le comportement chaotique du système maître. Il existe plusieurs types d'observateurs, tels que les observateurs de Luenberger, les observateurs de Kalman et les observateurs adaptatifs, qui peuvent être utilisés en fonction des caractéristiques du système à observer. Ces observateurs peuvent être conçus pour atteindre différents objectifs, tels que la stabilisation, l'observation de l'état complet ou partiel, ou encore la régulation.

En somme, l'utilisation d'un observateur peut être une approche efficace pour réaliser la synchronisation de systèmes chaotiques, en permettant d'estimer les états internes des systèmes à partir de leurs sorties et de les ajuster en conséquence.

## II.9 Conclusion

Dans ce chapitre on a exposé les objectifs des crypto-systèmes, et après on a décrit la cryptographie chaotique où on a cité les deux types des clés utilisées dans le chiffrement. Aussi on a présenté les différentes techniques de chiffrement par chaos analogique ainsi que les différents régimes de synchronisations.

## **Chapitre III**

### **Conception et synchronisation d'un générateur chaotique**

### III.1. Introduction

Lors de la recherche de structures chaotiques responsables de la génération du chaos, on trouve de nombreux travaux dans la littérature à travers lesquels des circuits chaotiques ont été proposés, en commençant par le circuit de Chua, qui est considéré comme le premier circuit électronique ayant introduit le chaos au début des années quatre-vingt [34]. Ce circuit a été largement utilisé malgré ses faibles caractéristiques fréquentielles par rapport à l'oscillateur Colpitts, qui a été exploité comme générateur chaotique pour la première fois par le chercheur Kennedy [35], ce dernier oscillateur chaotique a été conçu utilisant un transistor bipolaire (BJT). Une version améliorée de Colpitts chaotique a également été proposée dans le but d'améliorer ses caractéristiques fréquentielles, où une légère modification a été apportée à la version traditionnelle susmentionnée [36]. Dans le présent chapitre, nous commencerons par exposer les différentes bandes fréquentielles que nous viserons à les sécuriser, ensuite nous passerons en revue les oscillateurs chaotiques : (circuit de Chua, et l'oscillateur de Colpitts), puis nous étudierons numériquement la version améliorée de Colpitts à l'aide du programme MATLAB, et nous simulerons électriquement son circuit sous ADS (Advanced Design System) pour connaître la bande passante des oscillations chaotiques. Nous terminerons également ce chapitre en synchronisant cet oscillateur à l'aide d'un contrôle rétroaction non linéaire.

### III.2. Les bandes fréquentielles visées

#### III.2.1. La bande L [1 à 2 GHz]

La bande L est la partie du spectre électromagnétique définie par les fréquences de 1 GHz à 2 GHz, elle est attribuée aux services de radioastronomie à des fins de recherches spatiales et scientifiques. Cette bande est utilisée aussi par les systèmes de positionnement américain (GPS), européen (Galileo), russe (GLONASS) et chinois (Beidou). La partie haute de cette bande de fréquence est utilisée pour la téléphonie mobile (LTE 1800).

#### III.2.2. La bande S [2 à 4 GHz]

La bande S est une bande de fréquences définie sur la partie du spectre électromagnétique allant de 2 à 4 GHz. Cette bande S est notamment utilisée dans les applications suivantes :

- Radars météorologiques et certains radars militaires de surveillance aérienne (exemple AN/SPY-1 ou SAMPSON)

- Quelques satellites de télécommunications, spécialement ceux que la NASA emploie pour communiquer avec leurs navettes spatiales et la station spatiale internationale.
- Certains transmetteurs audio/vidéo de puissance maximale 20 mW.
- Les réseaux sans fil utilisant le protocole Wi-Fi (2400 à 2485 MHz).
- Les réseaux mobiles LTE (2500 à 2690 MHz) et 5G (3400 à 3800 MHz).

### III.2.3. La bande C [4 à 8 GHz]

La bande C situe généralement entre 4 et 8 gigahertz (GHz), elle est utilisée pour diverses applications de télécommunication terrestre, y compris les liaisons point à point et les réseaux cellulaires. Elle est aussi utilisée dans des applications scientifiques telles que la recherche en radioastronomie et la télédétection. Cette bande C est utilisée même pour les communications maritimes et aéronautiques, y compris les communications par satellite pour les navires en mer et les avions en vol.

### III.2.4 La bande X [8 à 12 GHz]

Les applications de télécommunication dans la bande X, qui se situe généralement entre 8 et 12 GHz, sont principalement liées aux communications par satellite, aux radars et à certaines technologies sans fil à haut débit. Voici quelques-unes des utilisations courantes :

- Les satellites de communication utilisent souvent la bande X pour les communications descendantes, c'est-à-dire la transmission de signaux depuis le satellite vers les récepteurs au sol.
- La bande X est utilisée dans de nombreux systèmes radar, y compris les radars météorologiques, les radars de contrôle du trafic aérien, les radars de surveillance maritime et les radars utilisés dans les applications militaires.
- Certaines technologies sans fil à haut débit, telles que le WiMAX (Worldwide Interoperability for Microwave Access) et certaines variantes de la 4G et de la 5G, peuvent utiliser la bande X pour fournir des connexions internet rapides et à large bande passante.

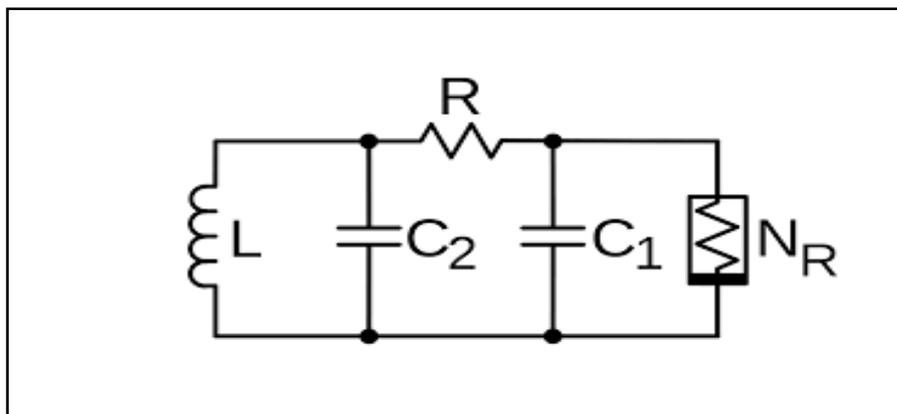
## III.3. Circuit de Chua

Le circuit de Chua représenté dans la figure (III.1) est inventé en 1983 par Leon Chua [34, 37], c'est le circuit électronique le plus simple qui présente le chaos. Il comporte deux condensateurs  $C_1$  et  $C_2$ , une bobine  $L$ , une résistance active  $R_{et}$  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 [37]. Le circuit classique de Chua peut être décrit par les équations différentielles suivantes :

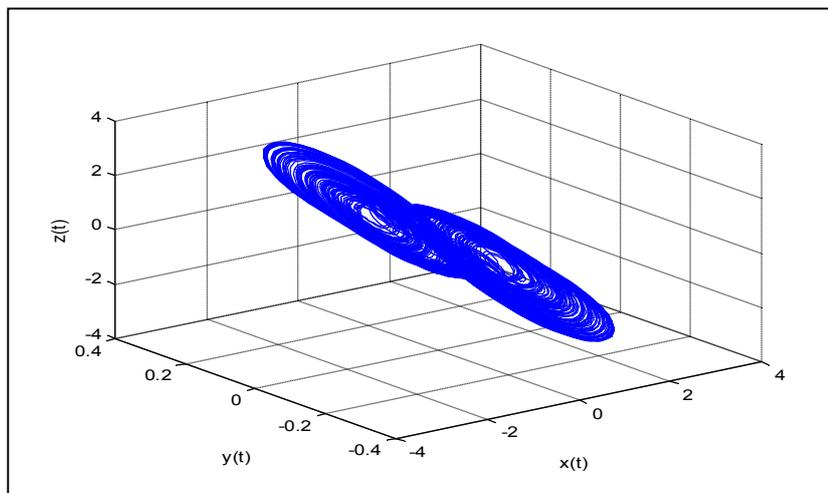
$$\begin{cases} \dot{x} = \alpha(y - x) - \alpha f(x) \\ \dot{y} = x - y + z \\ \dot{z} = -\beta y \end{cases} \quad (\text{III.1})$$

Où  $f(x) = m_1 x + \frac{1}{2}(m_0 - m_1)(|x + 1| - |x - 1|)$  est la caractéristique tension-courant linéaire par morceaux, ici  $x, y, z$  sont des variables d'état ; les paramètres  $m_0, m_1$  caractérisent une caractéristique linéaire par morceaux d'un élément non linéaire ; les paramètres  $\alpha$ , et  $\beta$  caractérisent la résistance, les deux condensateurs et l'inductance.



**Figure III.1.** Circuit de Chua.

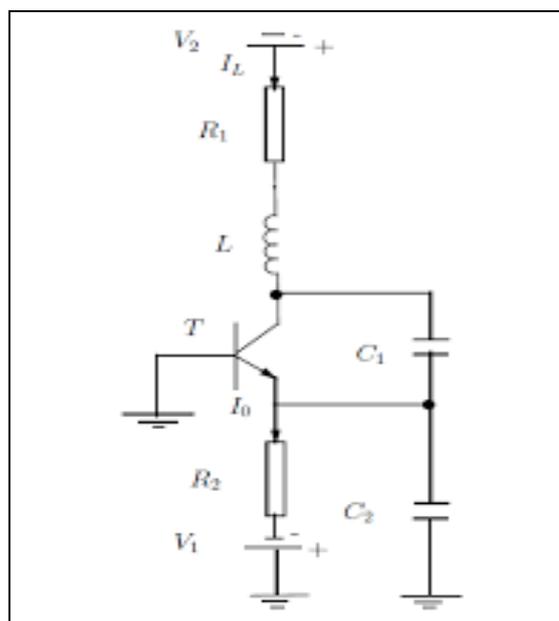
L'attracteur chaotique correspondant au circuit de Chua est représenté dans la figure (III.2), cet attracteur est obtenu utilisant les valeurs des paramètres suivantes ( $\alpha=15.8$ ,  $\beta=28$ ,  $m_0=-1.143$ ,  $m_1=-0.714$ ).



**Figure III.2.** L'attracteur étrange3D de Chua.

### III.4. L'oscillateur Colpitts standard

La figure (III.3) représente le circuit diagramme de l'oscillateur 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.

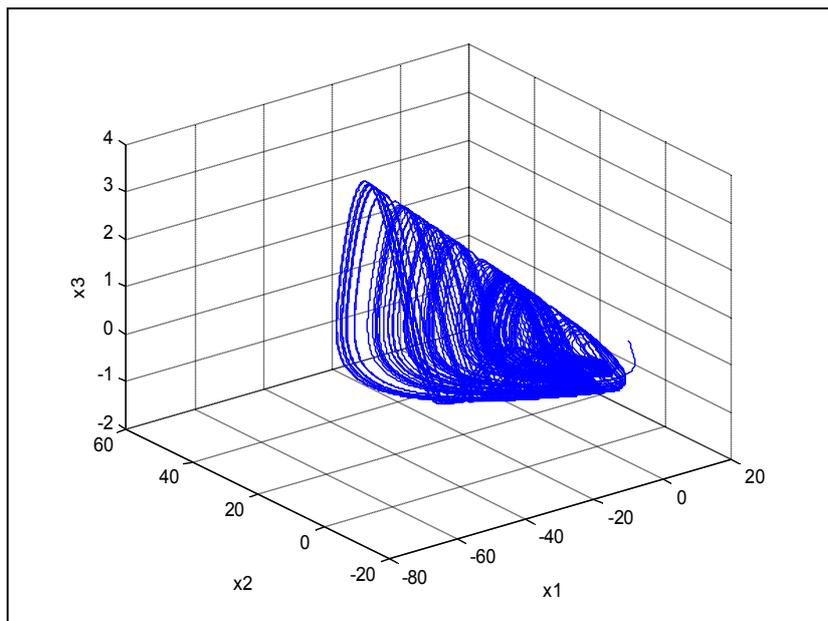


**Figure III.3.**Le circuit de l'oscillateur Colpitts chaotique standard.

La dynamique de l'oscillateur Colpitts est décrite par le système des équations différentielles suivant [35,38,39] :

$$\begin{cases} x_1 = \frac{g}{Q(1-k)} [-n(x_2) + x_3] \\ x_2 = \frac{g}{Qk} x_3 \\ x_3 = -\frac{Qk(1-k)}{g} [x_1 + x_2] - \frac{1}{Q} x_3 \end{cases} \quad (\text{III.2})$$

Avec  $n(x_2) = \exp(-x_2) - 1$  et  $k = \frac{C_2}{C_1 + C_2}$ . Le paramètre  $g$  est de la boucle de réaction de l'oscillateur lorsque le critère de Barkhausen est satisfait [38,39]. Et  $Q = \frac{\omega_0 L}{R}$  est le facteur de qualité du circuit LC non chargé. L'attracteur étrange de Colpitts obtenu en fixant les valeurs des paramètres comme suite ( $k=0.5$ ,  $g=4.46$ ,  $Q=1.38$ ) est illustré dans la figure (III.4).



**Figure III.4.** L'attracteur étrange 3D de Colpitts standard.

### III.5. L'oscillateur Colpitts amélioré

#### III.5.1 Le circuit de l'oscillateur

La configuration de l'oscillateur chaotique amélioré est représentée sur la figure (III.5). On voit qu'il est constitué d'un transistor bipolaire BJT en tant qu'élément amplificateur et d'un réseau résonnant contenant une inductance  $L$  et trois condensateurs  $C_1, C_2$ , et  $C_3$ . La différence entre l'oscillateur Colpitts traditionnel et la version améliorée est que l'inductance  $L$  est déplacé du collecteur à la base du transistor où elle est connectée en série avec la résistance  $R_B$ . Dans la version Colpitts standard, le condensateur  $C_3$  met à la terre le nœud collecteur et agit comme un élément parasite pour annuler les oscillations chaotiques dans les hautes fréquences. Dans cette nouvelle version,  $L$  et  $R_b$  protègent le  $C_3$  du sol et réduisent ses effets négatifs. Les études et les simulations menées sur les deux versions prouvent que la version traditionnelle de Colpitts ne peut pas générer des oscillations chaotiques dans les fréquences supérieures à 1 GHz, contrairement à la version améliorée qui peut générer des signaux chaotiques dans les trois bandes de fréquences suivantes : [0.3 GHz → 1 GHz], [1 GHz → 2 GHz], et [2 GHz → 4 GHz] [36,40,41,42,43,44]. Dans notre travail, nous allons exploiter la version améliorée de Colpitts pour générer des signaux chaotiques jusqu'à 12 GHz, en adoptant le transistor bipolaire BFP420 qui est caractérisé par une fréquence de transition égale à 25 GHz.

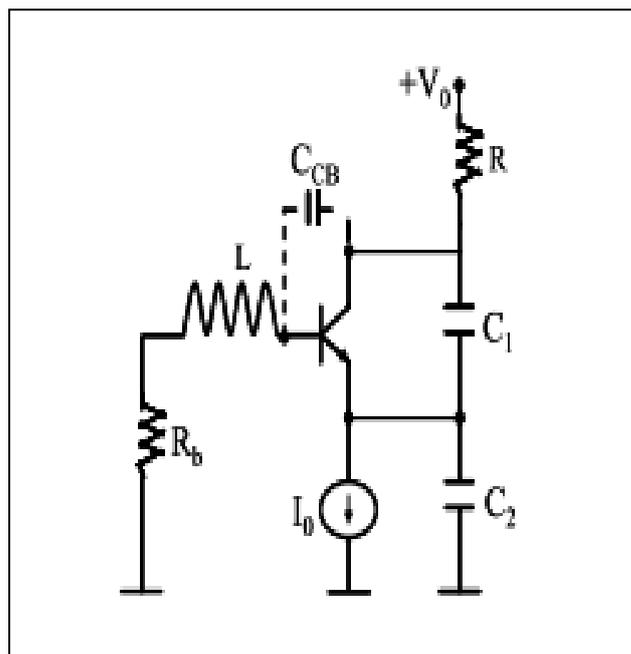


Figure III.5. Le circuit de l'oscillateur Colpitts amélioré.

### III.5.2 Le modèle mathématique de Colpitts amélioré

Pour trouver les équations d'état de l'oscillateur Colpitts chaotiques améliorés, on doit appliquer les lois de Kirchhoff sur son circuit représenté dans la figure (III.5), et donc on obtient le système suivant :

$$\left\{ \begin{array}{l} RC_1 \frac{dV_{C1}}{dt} = V_0 - V_{C1} - V_{C2} + RI_L - R(\beta + 1)I_B \\ RC_2 \frac{dV_{C2}}{dt} = V_0 - V_{C1} - RI_0 + RI_L \\ L \frac{dI_L}{dt} = -R_b I_L - V_{BE} - V_{C2} \\ RC_1 \frac{dV_{BE}}{dt} = V_0 - V_{C1} - V_{C2} + R \left(1 + \frac{C_1}{C_{CB}}\right) I_L - R \left(1 + \frac{C_1}{C_{CB}} + \beta\right) I_B \end{array} \right. \quad (\text{III.3})$$

Où  $I_B$  est le courant de base et  $I_C$  le courant de collecteur dans le BJT,  $I_B$  est défini par la relation suivante [45] :

$$I_B = \begin{cases} \frac{V_{BE} - V^*}{r}, & V_{BE} > V^* \\ 0, & V_{BE} \leq V^* \end{cases} \quad (\text{III.4})$$

Ici  $V^*$  est la tension de rupture ( $V^* \cong \mathcal{O}V$ ) de la caractéristique  $I-V$ ,  $r$  est la résistance différentielle de la jonction base-émetteur (B-E), et  $\beta$  est le gain de courant direct du

dispositif. Pour une analyse numérique pratique, nous introduisons l'ensemble suivant de variables d'état sans dimension :

$$\left\{ \begin{array}{l} x = \frac{V_{C1}}{V^*}, \quad y = \frac{\rho I_L}{V^*}, \quad z = \frac{V_{C2}}{V^*}, \\ v = \frac{V_{BE}}{V^*}, \quad t = \frac{t}{\tau}, \\ \rho = \sqrt{\frac{L}{C_1}}, \quad \varepsilon = \frac{C_2}{C_1}, \quad \tau = \sqrt{LC_1}, \\ a = \frac{\rho}{r}, \quad b = \frac{R}{\rho}, \quad c = \frac{V_0}{V^*}, \quad d = \frac{\rho I_0}{V^*}, \\ \alpha = \frac{R_b}{\rho}, \quad \gamma = 1 + \frac{C_1}{C_{CB}}, \end{array} \right. \quad (\text{III.6})$$

Par conséquent, les équations ci-dessus sont réécrites dans la forme sans dimension comme :

$$\left\{ \begin{array}{l} \dot{x} = \frac{c}{b} - \frac{1}{b}(x+z) + y - a(\beta+1)F(v) \\ \dot{y} = -\alpha y - z - v \\ \varepsilon \dot{z} = \frac{c}{b} - \frac{1}{b}(x+z) + y - d \\ \dot{v} = \frac{c}{b} - \frac{1}{b}(x+z) + \gamma y - a(\gamma+\beta)F(v) \end{array} \right. \quad (\text{III.7})$$

Où la fonction non linéaire est donnée comme suite :

$$F(v) = \begin{cases} v - 1, & v > 1 \\ 0, & v \leq 1 \end{cases} \quad (\text{III.8})$$

### III.5.3 Les résultats de simulation numérique

Pour résoudre le système des équations différentielles ordinaires (III.7) sous Matlab, nous avons utilisé l'algorithme d'Euler avec un pas  $\Delta\tau=0.01$ , sachant que les valeurs des paramètres pour que le comportement de ce système soit chaotique sont les suivantes :  $a=0.8$ ,  $b=0.67$ ,  $c=30$ ,  $d=0.96$ ,  $\alpha=0.87$ ,  $\gamma=21$ , et  $\beta=100$  avec les conditions initiales  $(x(0), y(0), z(0), v(0)) = (0.3, 0.1, 1, 0.7)$ . Les réponses temporelles, les différents espaces de phase et l'attracteur étrange 3D obtenus après la résolution de ce système sont illustrés dans les figures (III.6), (III.7), et (III.8).

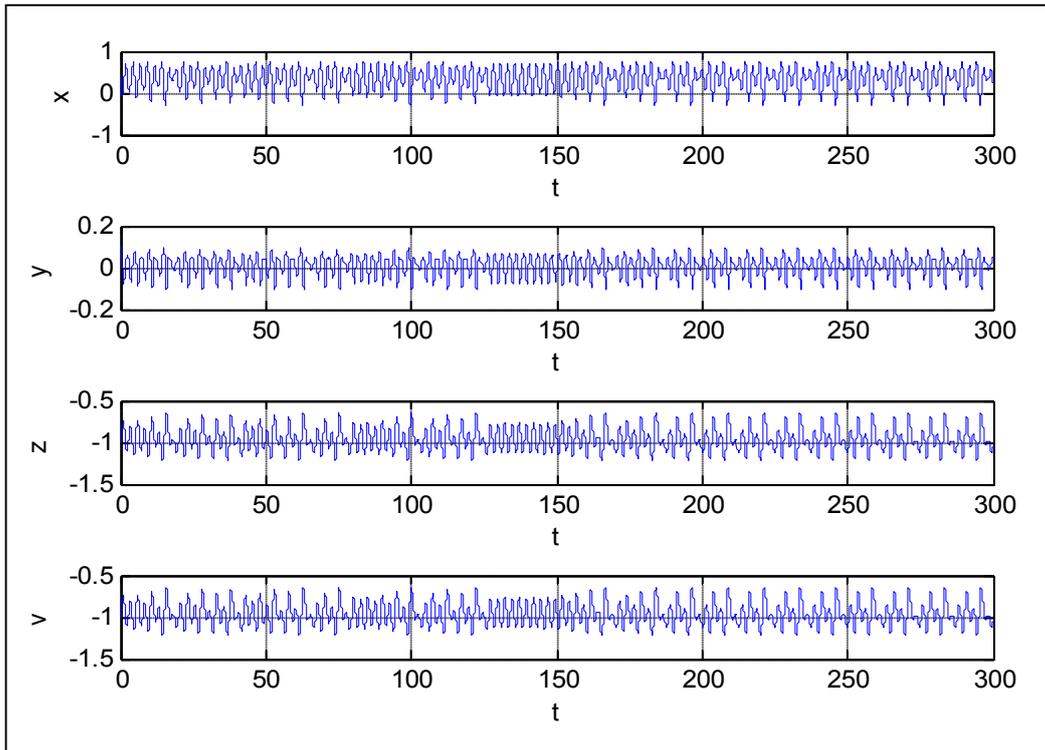


Figure III.6. Les différentes réponses temporelles chaotique de l'oscillateur Colpitts amélioré.

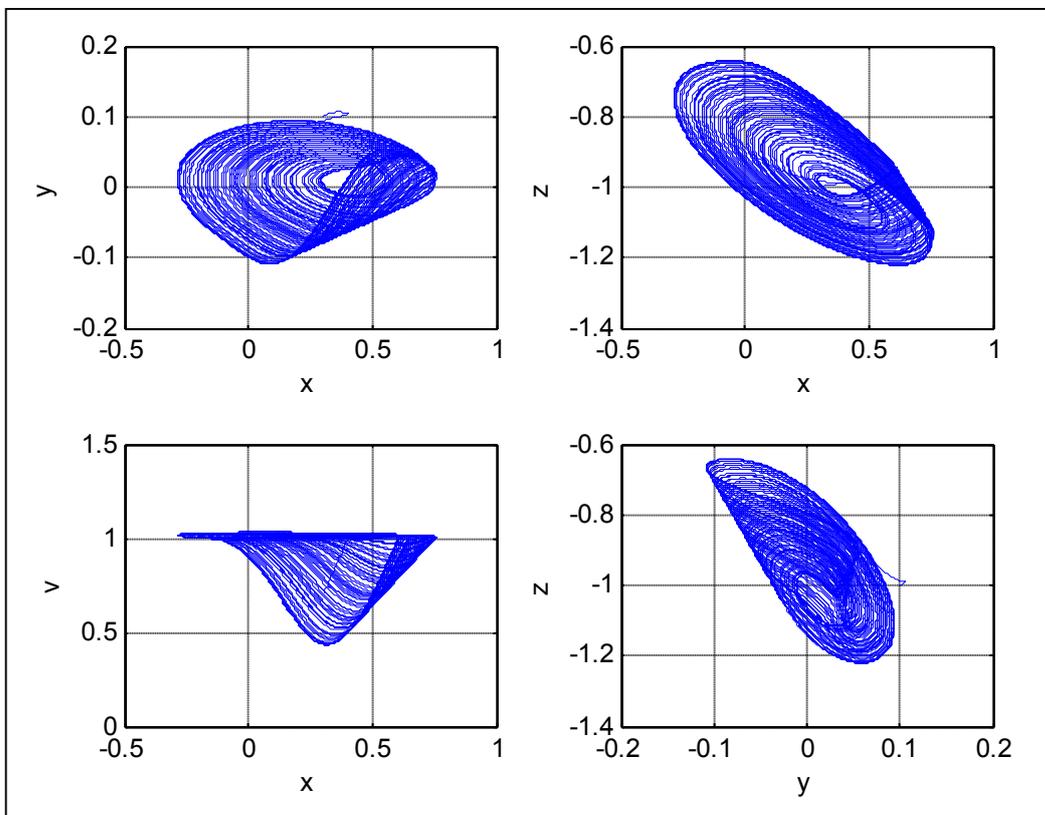
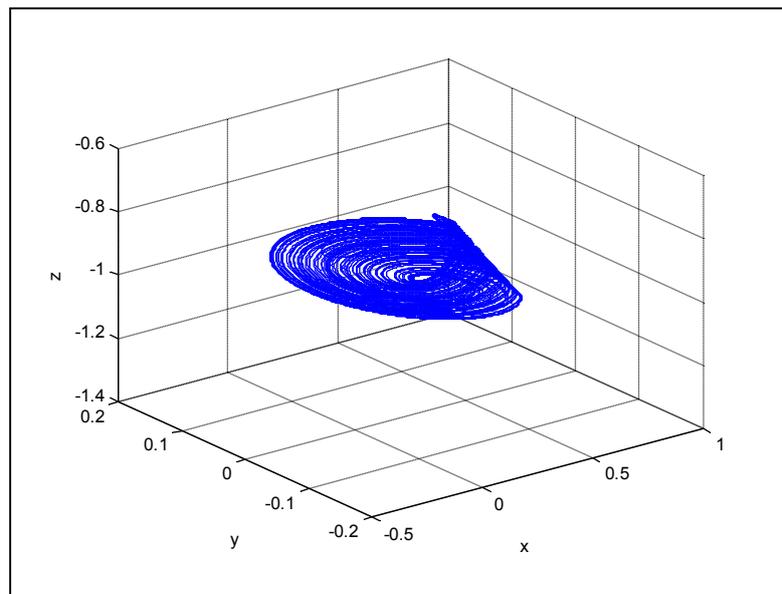


Figure III.7. Les différentes réponses temporelles chaotique de l'oscillateur Colpitts amélioré.



**Figure III.8.** L'attracteur étrange 3D de Colpitts amélioré.

### III.5.4 Les résultats de simulation sous ADS

Afin de confirmer les résultats numériques obtenus dans la partie de simulation sous Matlab, nous simulons le circuit de l'oscillateur Colpitts amélioré représenté dans la figure (III.9) utilisant le logiciel ADS. Le circuit simulé dans ce travail est construit à base d'un modèle Pspice de transistor bipolaire BFP420 avec une fréquence de transition égale à 25 GHz, l'utilisation de modèle Pspice d'un transistor bipolaire vise à modéliser : les éléments parasites du boîtier (capacité, inductance, et résistances), effets de température, et d'autres paramètres qui affectent la dynamique de l'appareil dans les hautes fréquences [46]. Pour augmenter la valeur de la fréquence fondamentale des oscillations chaotiques, on doit diminuer la valeur de l'inductance  $L$  qui va être dans ce cas-là très petite et comparable avec la valeur de l'inductance interne  $L_{BO}$  de. Nous proposons dans ce cas-là d'éliminer l'inductance  $L$  et d'exploiter l'inductance  $L_{BO}$ .

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

Composants	$V_0=V_1$	$I_0$	$C_1=C_2$	$R_1$	$R_2$	$R_3$
Valeurs	10V	20 mA	1.8pF	$3.5\Omega$	$35\Omega$	$400\Omega$

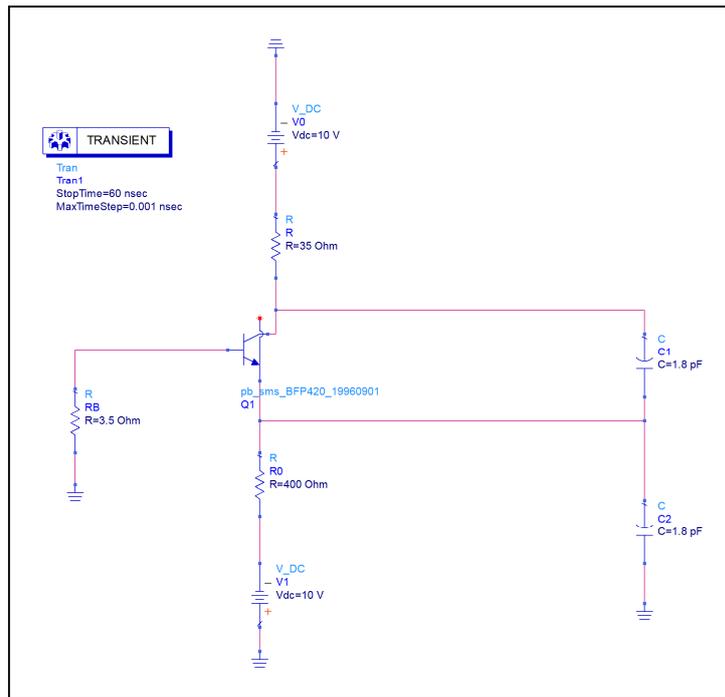


Figure III.9. Le Circuit simulé sous ADS.

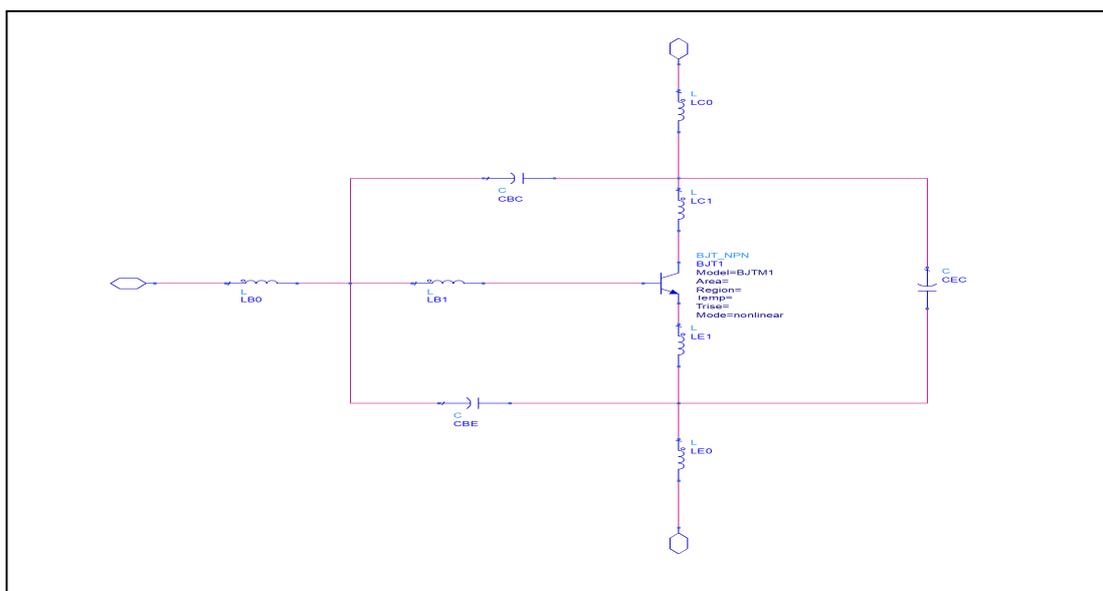


Figure III.10. Le modèle Pspice de transistor bipolaire BFP420.

Les résultats des simulations sont illustrés dans les figures (III.11), (III.12), et (III.13), où les réponses temporelles chaotiques ( $V_{C1}$ ) et ( $V_{C2}$ ) sont représentés dans la figure (III.11). Les deux espaces des phases chaotiques  $V_{C1} = f(V_{C2})$ , et  $V_{C2} = f(V_{C1})$  trouvés après la simulation du circuit de l'oscillateur Colpitts amélioré sous le logiciel ADS en utilisant une simulation transitoire (TRANSIENT SIMULATOR) avec les paramètres suivants : (Start

time= 0nsec, Stop time= 60nsec, et  $\Delta t=0,001nsec$ ) sont illustrés aussi dans les figures (III.12), et (III.13).

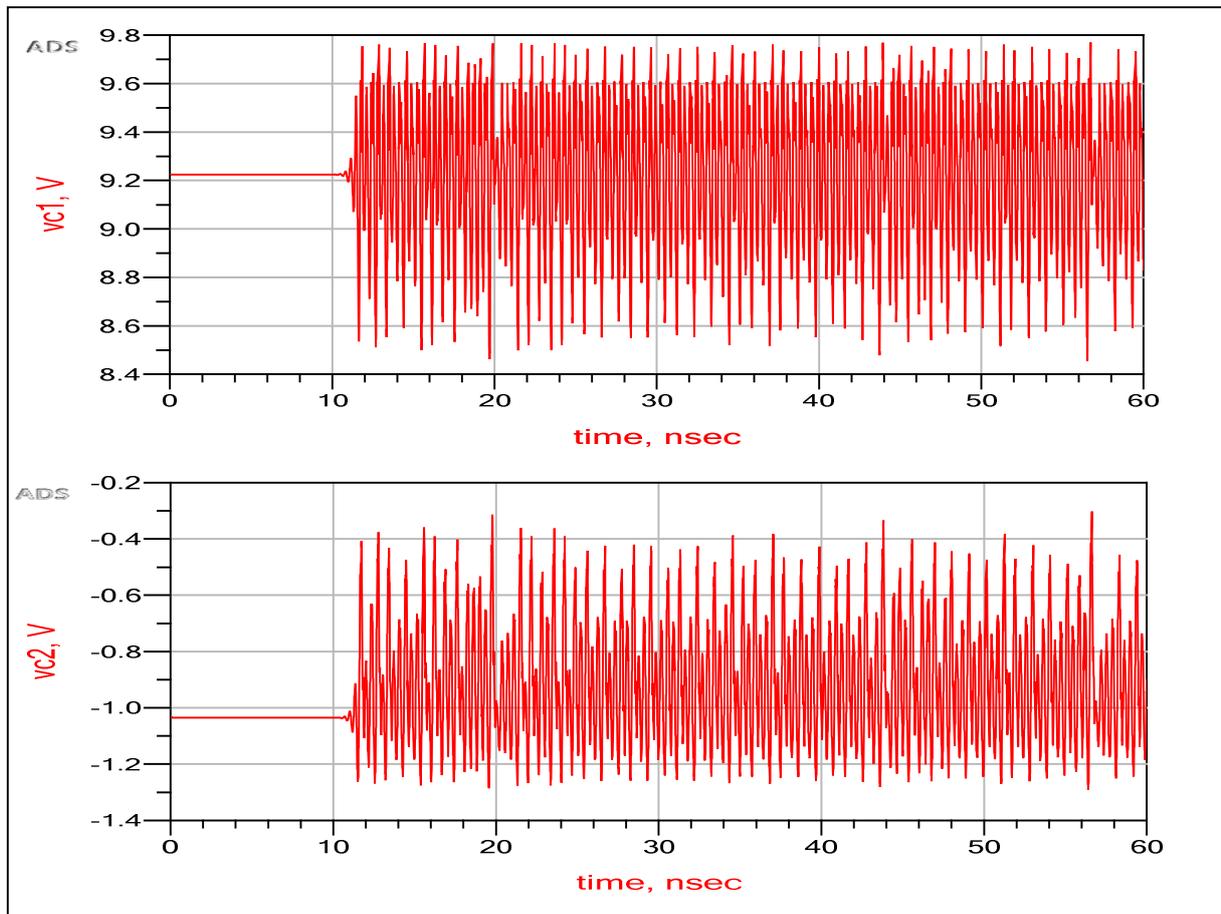


Figure III.11. Réponses temporelle ( $V_{c1}$ ), et ( $V_{c2}$ ).

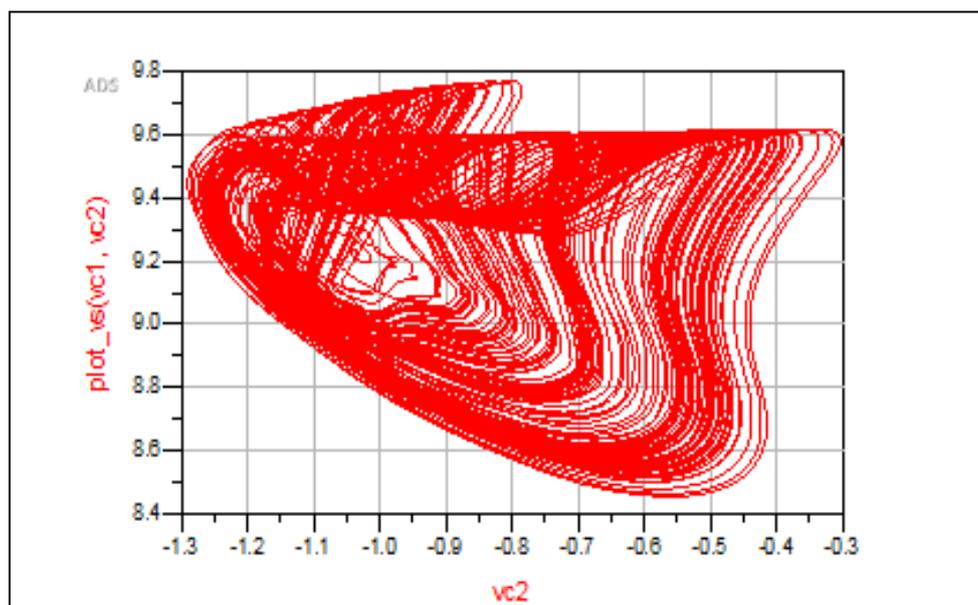


Figure III.12. L'espace de phase ( $V_{c2}, V_{c1}$ ).

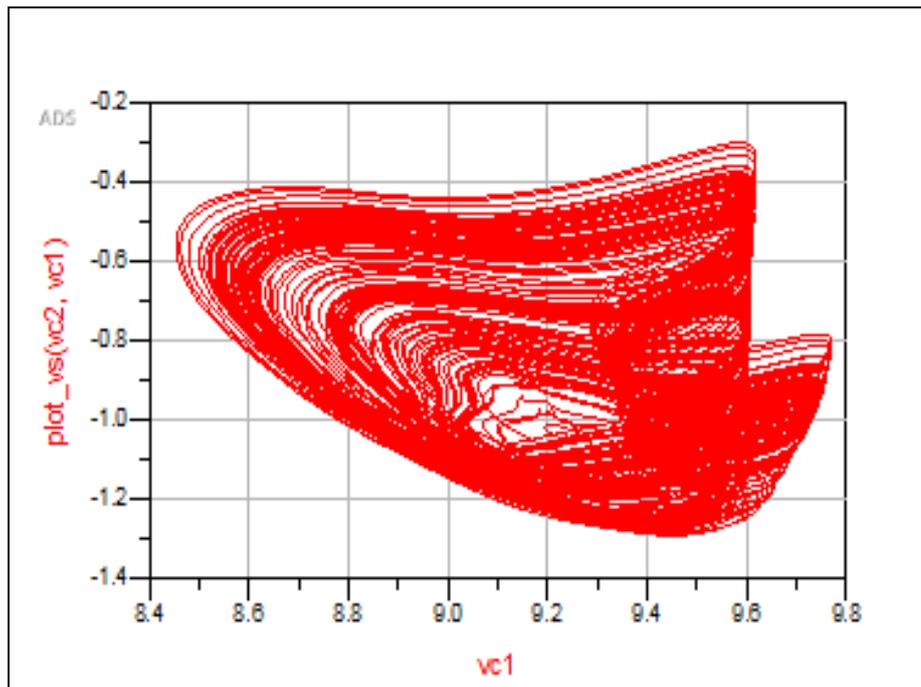


Figure III.13. L'espace de phase ( $V_{c1}, V_{c2}$ ).

Par la comparaison entre l'espace de phases mathématiques obtenu sous Matlab ( $x, y$ ) et l'espace de phases électriques obtenu sous ADS ( $V_{c1}, V_{c2}$ ), il est clair qu'il existe une bonne similitude entre eux. A partir de cette étroite similitude, nous pouvons valider le modèle mathématique (III.7) adopté pour notre oscillateur. En se basant sur la Figure (III.14) qui représente les caractéristiques spectrales de  $V_{c1}$ , on remarque que son spectre de puissance est étendu de 1 GHz jusqu'à 11.2 GHz avec une dynamique de chaos entre -10 et -60 dB.

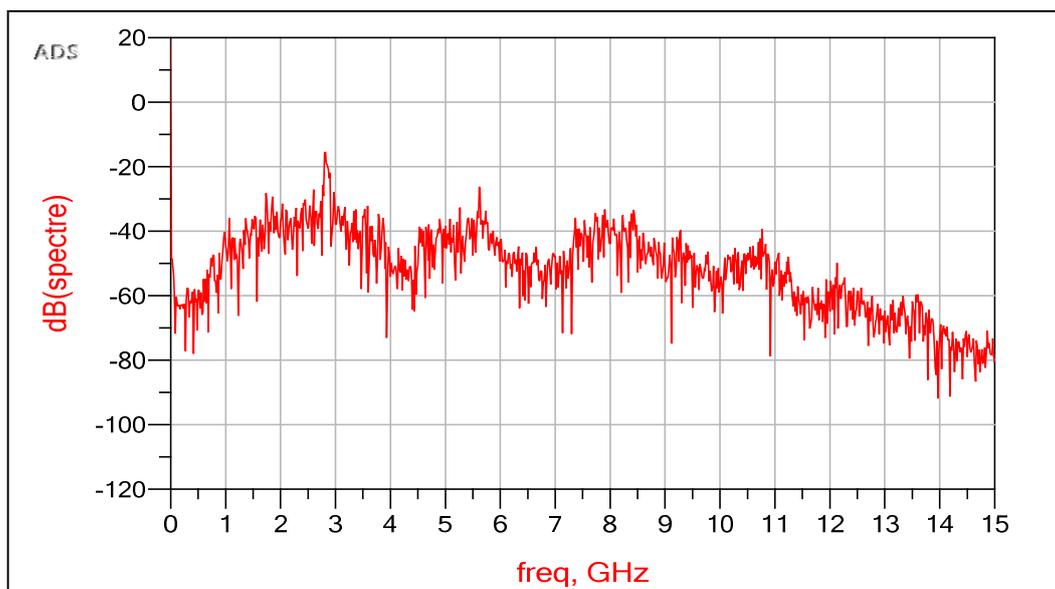


Figure III.14. Les caractéristiques spectrales de  $V_{c1}$ .

### III.6. Synchronisation à l'aide d'un contrôle rétroaction non linéaire :

À partir de l'analyse et les simulations susmentionnées, nous avons constaté que le système d'équations (III.7) peut présenter un comportement chaotique pour certains paramètres particuliers. Considérons maintenant les deux systèmes suivants :

$$\begin{cases} \dot{x}_1 = -\frac{1}{b}(x_1 + z_1) \pm a(\beta + 1)F(v_1), \\ \dot{y}_1 = -\alpha y_1 - z_1 - v_1, \\ \dot{z}_1 = -\frac{1}{b}(x_1 + z_1) + y_1 - d, \\ \dot{v}_1 = -\frac{1}{b}(x_1 + z_1) + \gamma y_1 - a(\gamma + \beta)F(v_1), \end{cases} \quad (\text{III.9})$$

Le système de réponse est :

$$\begin{cases} \dot{x}_2 = -\frac{1}{b}(x_2 + z_2) + y_2 - a(\beta + 1)F(v_2) + u_1(t) \\ \dot{y}_2 = -\alpha y_2 - z_2 - v_2 + u_2(t) \\ \dot{z}_2 = -\frac{1}{b}(x_2 + z_2) + y_2 - d + u_3(t) \\ \dot{v}_2 = -\frac{1}{b}(x_2 + z_2) + \gamma y_2 - a(\gamma + \beta)F(v_2) + u_4(t) \end{cases} \quad (\text{III.10})$$

Où  $u(t) = [u_1(t), u_2(t), u_3(t), u_4(t)] \in \mathbb{R}^{4 \times 1}$  est le contrôleur non linéaire ajouté au système de réponse. Avant l'ajout de  $u(t)$ , les systèmes (III.9) et (III.10) ne sont pas synchrones.

**Théorème 1 :** Les systèmes (III.9) et (III.10) peuvent être synchronisés si le contrôleur est de la forme suivante [47,48] :

$$u(t) = -G(v_1, v_2, a, \beta) + W(t) \quad (\text{III.11})$$

Où  $G(v_1, v_2, a, \beta)$  et  $W(t)$  sont définis comme suite :

$$G(v_1, v_2, a, \beta) = \begin{bmatrix} -a(\beta + 1)[F(v_2) - F(v_1)] \\ 0 \\ 0 \\ -a(\beta + 1)[F(v_2) - F(v_1)] \end{bmatrix} \quad (\text{III.12})$$

$$W(t) = \begin{bmatrix} 0 & -1 & \frac{1}{b} & 0 \\ 0 & 0 & 1 & 1 \\ \frac{1}{b} & -1 & 0 & 0 \\ \frac{1}{b} & -\gamma & \frac{1}{b} & -1 \end{bmatrix} e(t) \quad (\text{III.13})$$

Introduire  $e(t) = [e_1(t), e_2(t), e_3(t), e_4(t)] \in R^{4 \times 1}$  comme variables d'erreur des deux systèmes :

$$\begin{cases} e_1 = x_2 - x_1 \\ e_2 = y_2 - y_1 \\ e_3 = z_2 - z_1 \\ e_4 = v_2 - v_1 \end{cases} \quad (\text{III.14})$$

Nous séparons les deux systèmes (III.9) et (III.10) en termes linéaires et termes non linéaires, et donc les deux systèmes deviennent :

$$\begin{cases} \dot{x}_1 = f_{11} + f_{21} \\ \dot{y}_1 = f_{12} + f_{22} \\ \dot{z}_1 = f_{13} + f_{23} \\ \dot{v}_1 = f_{14} + f_{24} \end{cases} \quad (\text{III.15})$$

$$\begin{cases} \dot{x}_2 = g_{11} + g_{21} + u_1(t) \\ \dot{y}_2 = g_{12} + g_{22} + u_2(t) \\ \dot{z}_2 = g_{13} + g_{23} + u_3(t) \\ \dot{v}_2 = g_{14} + g_{24} + u_4(t) \end{cases} \quad (\text{III.16})$$

Où  $f_{1j}, g_{1j}$  ( $j = 1, \dots, 4$ ) sont des termes linéaires et  $f_{2j}, g_{2j}$  ( $j = 1, \dots, 4$ ) sont respectivement des termes non linéaires. Les termes  $f_{1j}$  sont les suivants :

$$\begin{cases} f_{11} = -\frac{1}{b}(x_1 + z_1) + y_1 \\ f_{12} = -\alpha y_1 - z_1 - v_1 \\ f_{13} = -\frac{1}{b}(x_1 + z_1) + y_1 \\ f_{14} = -\frac{1}{b}(x_1 + z_1) + \gamma y_1 \end{cases} \quad (\text{III.17})$$

Les termes  $f_{2j}$  sont :

$$\begin{cases} f_{21} = -\alpha(\beta + 1)F(v_1) \\ f_{22} = 0 \\ f_{23} = -d \\ f_{24} = \alpha(\gamma + \beta)F(v_1) \end{cases} \quad (\text{III.18})$$

Les termes  $g_{1j}$  sont :

$$\begin{cases} g_{11} = -\frac{1}{b}(x_2 + z_2) + y_2 \\ g_{12} = -\alpha y_2 - z_2 - v_2 \\ g_{13} = -\frac{1}{b}(x_2 + z_2) + y_2 \\ g_{14} = -\frac{1}{b}(x_2 + z_2) + \gamma y_2 \end{cases} \quad (\text{III.19})$$

Les termes  $g_{2j}$  sont :

$$\begin{cases} g_{21} = -a(\beta + 1)F(v_2) \\ g_{22} = 0 \\ g_{23} = -d \\ g_{24} = -a(\gamma + \beta)F(v_2) \end{cases} \quad (\text{III.20})$$

Alors les différences linéaires entre les deux systèmes sont :

$$\begin{cases} g_{11} - f_{11} = -\frac{1}{b}(e_1 + e_3) + e_2 \\ g_{12} - f_{12} = -\alpha e_2 - e_3 - e_4 \\ g_{13} - f_{13} = -\frac{1}{b}(e_1 + e_3) + e_2 \\ g_{14} - f_{14} = -\frac{1}{b}(e_1 + e_3) + \gamma e_2 \end{cases} \quad (\text{III.21})$$

Et les différences non linéaires entre les deux systèmes sont :

$$\begin{cases} g_{21} - f_{21} = -a(\beta + 1)[F(v_2) - F(v_1)] \\ g_{22} - f_{22} = 0 \\ g_{23} - f_{23} = 0 \\ g_{24} - f_{24} = -a(\beta + 1)[F(v_2) - F(v_1)] \end{cases} \quad (\text{III.22})$$

Supposons que le contrôleur non linéaire est déterminé comme suit :

$$\begin{cases} u_1(t) = a(\beta + 1)[F(v_2) - F(v_1)] + w_1(t) \\ u_2(t) = w_2(t) \\ u_3(t) = w_3(t) \\ u_4(t) = a(\beta + 1)[F(v_2) - F(v_1)] + w_4(t) \end{cases} \quad (\text{III.23})$$

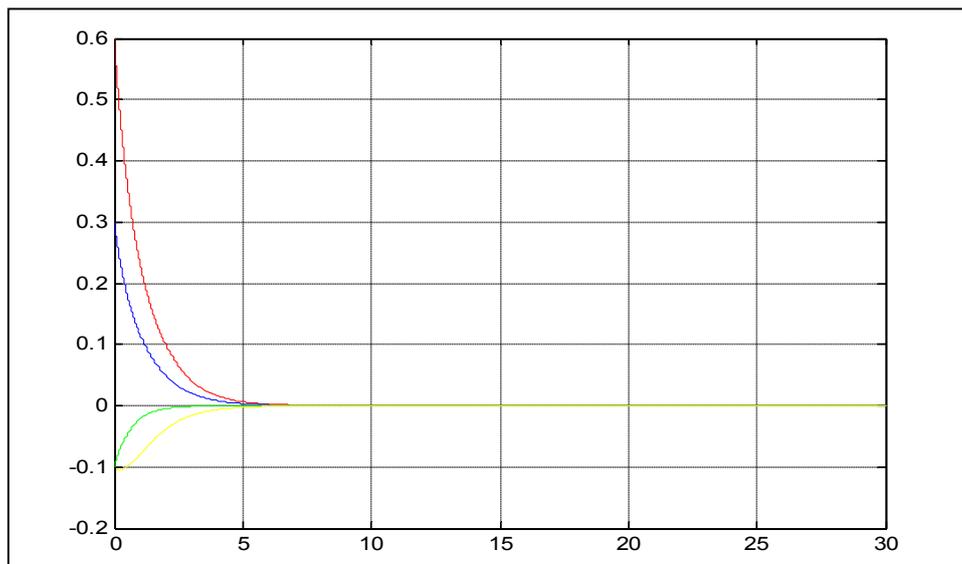
D'après les équations dynamiques (III.9) et (III.10), l'équation de l'erreur des deux systèmes,

$$\begin{cases} \dot{e}_1 = -\frac{1}{b}(e_1 + e_3) + e_2 + w_1(t) \\ \dot{e}_2 = -\alpha e_2 - e_3 - e_4 + w_2(t) \\ \dot{e}_3 = -\frac{1}{b}(e_1 + e_3) + e_2 + w_3(t) \\ \dot{e}_4 = -\frac{1}{b}(e_1 + e_3) + \gamma e_2 + w_4(t) \end{cases} \quad (\text{III.24})$$

La fonction de contrôle  $W(t) = [w_1(t), w_2(t), w_3(t), w_4(t)]^T$  est une fonction de  $e_1, e_2, e_3, e_4$ . Si  $\lim_{t \rightarrow \infty} e(t) = 0$  et que le système d'erreur dans (III.24) a quatre valeurs propres avec des parties réelles négatives, alors la synchronisation peut être réalisée [47,49]. Pour ce faire, on choisit parmi de nombreux choix possibles de  $W(t)$  :

$$\begin{cases} w_1(t) = -e_2 + \frac{1}{b}e_3 \\ w_2(t) = e_3 + e_4 \\ w_3(t) = -e_2 + \frac{1}{b}e_1 \\ w_4(t) = \frac{1}{b}(e_1 + e_3) - \gamma e_2 - e_4. \end{cases} \quad (\text{III.25})$$

Par conséquent dans ce cas, les quatre valeurs propres du système (III.24)  $(-\frac{1}{b}, -\alpha, -\frac{1}{b}, -1)$  sont tous négatifs. Et donc selon la théorie de la stabilité de Hurwitz, la synchronisation des deux systèmes chaotiques est réalisée. Afin de vérifier l'efficacité des mesures proposées méthode de contrôle de rétroaction non linéaire, choisissons le système d'entraînement avec l'état initial (0.3, -0.1, -0.4, 0.3) et système de réponse avec condition initiale (0.7, 0.2, -0.5, 0.2). Les paramètres  $a = 1,15, b = 0,67, d = 0,96, \alpha = 0,87, \gamma = 21, \beta = 100$  sont identiques pour les deux systèmes et sont maintenus constants lors des calculs actuels. La figure (III.15) affiche les résultats. Des simulations numériques montrent que l'erreur entre les deux systèmes tend vers zéro, et donc la synchronisation est réalisée avec succès.



**Figure III.15.** Graphiques des erreurs de synchronisation avec temps normalisé ( $e_1$  en rouge,  $e_2$  en bleu,  $e_3$  en vert, et  $e_4$  en jaune).

Au final, ce contrôleur sera facilement implémenté pour fonctionner aux hautes fréquences du circuit. En effet, plus récemment le concept d'observateur non linéaire a été appliqué pour concevoir les contrôleurs de rétroaction pour réaliser la synchronisation Entre un émetteur et un récepteur [47, 48]. Dans [49], Qiao et al. ont étudié la possibilité d'appliquer des signaux chaotiques micro-ondes et la synchronisation du chaos dans construire un nouveau type de RADAR UWB, en utilisant Oscillateur Colpitts. En outre, les chercheurs de Réf. [50] ont démontré la faisabilité de réaliser la synchronisation du chaos à très hautes fréquences.

### **III.7. Conclusion**

Dans ce troisième chapitre nous avons exploité l'oscillateur Colpitts chaotique amélioré pour générer des oscillations chaotiques jusqu'à 11.2 GHz, utilisant un transistor bipolaire de type BFP420. L'étude numérique de cet oscillateur est faite sous Matlab en résolvant son modèle mathématique pour tracer les différents espaces des phases chaotiques. La simulation de son circuit sous le simulateur ADS vise à confirmer les résultats numériques obtenus, et à étudier ses caractéristiques fréquentielles. La deuxième partie de chapitre est consacrée à synchroniser deux systèmes de Colpitts amélioré en utilisant la méthode de Contrôle rétroaction non linéaire.

# **Conclusion Générale**

## Conclusion générale

Ce mémoire consiste à étudier la dynamique et la synchronisation d'un nouveau générateur chaotique basé sur l'oscillateur de Colpitts amélioré destiné à sécuriser les systèmes de communication.

Dans le premier chapitre nous avons introduit quelques notions de systèmes dynamiques en temps continu ou discret. Ensuite, nous avons porté notre attention particulière sur une classe spécifique de systèmes non linéaires appelés chaotiques, avec quelques concepts et définitions d'introduction à la théorie du chaos. Ces systèmes ont plusieurs fonctionnalités conçues pour assurer une transmission plus sécurisée. Ces caractéristiques incluent la sensibilité aux conditions initiales, en ce sens qu'un léger écart ou une inexactitude dans les conditions initiales produira des développements extrêmement différents, ce qui signifie qu'il est impossible de prédire le comportement à long terme d'un système chaotique. Une autre propriété intéressante est le déterminisme, ce qui signifie que ces systèmes sont régis par des règles fondamentales de non-probabilité, permettant de reproduire un comportement chaotique. L'attracteur étrange est la troisième propriété, qui est un attracteur dont la forme est une courbe ni une surface. Nous avons également défini plusieurs outils pour étudier ces systèmes, d'abord des exposants de Lyapunov pour vérifier le comportement d'un système dynamique, puis le diagramme de bifurcation qui permet d'observer les différents comportements possibles de systèmes chaotiques.

Dans le deuxième chapitre de notre étude, nous avons abordé plusieurs sujets liés à la cryptographie chaotique, la cryptanalyse et les concepts de base d'un schéma de cryptage. Nous avons ensuite expliqué en détail le cryptage par le chaos et les différentes techniques utilisées pour masquer l'information utile lors de la transmission d'un signal chaotique. La première technique que nous avons mentionnée est le chiffrement par addition. Cette méthode consiste à ajouter le message à chiffrer à un signal chaotique. Le résultat est ensuite transmis comme signal chiffré. Cette technique offre une certaine sécurité, mais elle peut être vulnérable à certaines attaques cryptographiques. La deuxième technique que nous avons présentée est le chiffrement par modulation. Cette approche utilise le message contenant l'information à transmettre pour moduler un paramètre du système émetteur chaotique. En modifiant ce paramètre de manière contrôlée, le signal chaotique résultant transporte l'information sous une forme cryptée. Cette méthode présente des avantages en termes de sécurité et de robustesse. Enfin, nous avons mentionné la technique de chiffrement par

commutation. Cette méthode exige que le message à transmettre soit converti en une séquence binaire. Le signal chaotique est ensuite utilisé pour effectuer des commutations entre les bits du message binaire, ce qui crée un signal chiffré. Cette technique offre une bonne résistance aux attaques, mais elle nécessite une conversion préalable du message en format binaire. Pour conclure le deuxième chapitre, nous avons abordé le sujet de la synchronisation chaotique, qui est une étape essentielle dans les systèmes de transmission basés sur le chaos. La synchronisation permet de garantir que l'émetteur et le récepteur sont en phase et peuvent décoder correctement le signal chaotique transmis. Différents régimes de synchronisation chaotique ont été étudiés et utilisés dans diverses applications de cryptographie.

Le troisième chapitre de notre recherche porte sur la conception et la simulation d'un générateur chaotique. Dans la première partie de ce chapitre, nous avons présenté le circuit de Chua et l'oscillateur Colpitts, qui sont considérés comme les générateurs les plus utilisés et les plus célèbres. Dans la deuxième partie, nous avons exploité l'oscillateur Colpitts amélioré pour générer des oscillations chaotiques. Où 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 d'Euler nous permet de tracer les réponses temporelles et les espaces des phases chaotiques. Nous avons aussi confirmé les résultats mathématiques obtenus sous Matlab à partir d'une autre simulation à l'aide de l'outil ADS. Le spectre obtenu dans cette deuxième simulation montre que la bande passante des oscillations chaotiques peut couvrir des fréquences allant jusqu'à 11.2 GHz avec une dynamique de chaos entre -10dBm et -60 dBm. Dans la dernière partie de ce chapitre, nous avons proposé une méthode de synchronisation à l'aide de rétroaction non linéaire contrôlée.

#### Perspectives

ce travail peut être amélioré par:

L'augmentation de la fréquence d'oscillation

Réalisation pratique de générateur proposé

La proposition d'une autre méthode de synchronisation

# **Références bibliographiques**

- 
- [1]. E. Cherrier. Estimation de l'état et des entrées inconnues pour une classe de système non linéaire. Thèse de doctorat, 2006.
- [2]. O. Megherbi, 'Etude et réalisation d'un système sécurisé à base de système chaotique', thèse De magister, université Mouloud Mammeri Tizi-Ouzou, 10/10/2013.
- [3]. H. Dang-Vu, c. Del carte, 'Bifurcation et chaos : introduction à la dynamique contemporaine Avec des programmes en Pascal, Fortan et Mathematica', Ed. Ellipses, Paru en septembre 2000.
- [4]. C. Morel, 'Analyse et contrôle de dynamique chaotique, application à des circuits Électroniques Non linéaires', université D'Angers, Décembre 2005.
- [5]. H. Kenouni, 'synchronisation des systèmes Rye-chaotiques à retard sous l'effet des Perturbations : application au chiffrement d'information', mémoire de master, Université de Jijel, 2016.
- [6]. HAMATT, « étude et réalisation d'un système chaotique base sur le circuit de Chua », Mémoire de Master, Tizi-Ouzou : université Mouloud Mammeri, 2014.
- [7]. Hamaizia, systèmes dynamiques et chaos 'application à l'optimisation à l'aide d'algorithmes chaotiques', thèse pour l'obtention de doctorat, université de Constantine, 2013, pp.22.
- [8]. D. Peltier, T Nguyen Hoang, D. P. Tran. O. Abdelmalki, K. Alaoui et K. Lerouse, 'Etude d'un système physique non dissipatif « chaotiques », projet de physique P6-3 Stpi /pg-3/2009.
- [9]. G. Assel, L. Blaizot et G. Huizinga, 'la théorie du chaos', saint Eloi. 2013.
- [10]. H. Azira, M. Khetta, 'analyse et implémentation du système chaotique de Qi', Université de Saad Dahlab de Blida, thèse de master, 2015.
- [11]. I. Talbi, 'système dynamique non linéaires et phénomènes de chaos', thèse de Master, Université Mentour de Constantine 29/06/2010.
- [12]. E. N. Lorenz, 'Deterministic no periodic flow', journal of atmospheric sciences, 20 :130-141,1963.
- [13]. E. Ott, chaos in dynamical systems, 2nd editions, Cambridge university press, 2002.
- [14]. D.V. Huynen and C. Delcarte, bifurcation et chaos, ellipse editions marketing S.A ,2000.
- [15]. A.R.Kihal, système chaotique pour la transmission sécurisé de donnée Mémoire de Magister, Université Mohammed Khider, Biskra, 2013.

- [16]. D. RUELLE & F. TAKENS, On the nature of turbulence, *communications of mathematical physic* 20(1971), p 167-192.
- [17]. M. BENDAOU, “ Etude et Conception d’un système chaotique basé sur l’oscillateur Colpitts pour les communications sécurisées”, Mémoire de Master, Université de Tlemcen, 2019.
- [18]. E. OTT, Chaos in dynamical systems, *2nd Edition, Cambridge University Press, 2002.*
- [19]. D. V. HYUYEN & C. DELCARTE, Bifurcations et chaos, *Ellipses editions marketing S.A, 2000.*
- [20]. T. Yang, “Impulsive Control theory”, Springer Verlag, Lecture Notes in Control and Information sciences, 2001.
- [21]. O. MEGHERBI, Etude et réalisation d’un système sécurisé à base de système Chaotique, *Mémoire de magister, Université Mouloud Mammeri, Tizi-Ouzou, 2013.*
- [22]. Mr Medjahdi Nasreddine « Cryptage Chaotique Basé sur L’attracteur Clifford », Université Abou Baker Belkaid. Tlemcen, 02 Juillet 2017.
- [23]. Cristina Morel, « Analyse et contrôle de dynamiques chaotiques, Application à des Circuit électroniques non-linéaires », Thèse de Doctorat, Université de Franche-Comté, 2007.
- [24]. F. Anstett, « les systèmes dynamiques chaotique pour le chiffrent : synthèse et Cryptanalyse », thèse de doctorat, Université de Henri Poincaré, 2006.
- [25]. B. Chouaib, « Etude d’un système chaotique pour la sécurisation des communications Optiques, Mémoire de Master Télécommunication Université d’Abou Baker Belkaid, Juin, 2014.
- [26]. Kara Ali, Djamila. (2007). Synchronisation de quelques systèmes chaotiques. Mémoire De Magister, Université de Constantine.
- [27]. Menacer, Tidjani (26/05/2014). Synchronisation des systèmes dynamiques chaotiques À Dérivées fractionnaires. Doctorante sciences en Mathématiques Université Constantine.
- [28]. Megherbi, ouerdia. (2013). Etude et réalisation d’un système sécurisé à base des Systèmes Chaotiques. Mémoire de magister en automatique, université Mouloud Marameri Tizi- Ouzou.
- [29]. Ge, z, M, Chen, Y. S, ‘Adaptative synchronization of unidirectionnel and mutual Coupled Chaotic systems. Chao, solitons & fractals, 26(3), 881\_888.2005.

- [30]. Hamid Hamiche, « Inversion à Gauche des systèmes dynamiques hybrides chaotiques Application à la transmission sécurisée de données », thèse de doctorat, université Miloud Mammeri, 2011.
- [31]. G.R. Cooper, R.W. Nettleton 'spectral efficiency in cellular lan-mobile Communications: a spread Spectrum approach', final report, TR- EE 78-44, purdue University, West Lafayette. TND 1978.
- [32]. E. charrier, « Estimation de l'état et des entrées inconnues pour une classe de systèmes Non linéaires », thèse Doctorat, Nancy, France, 2006.
- [33]. M. ABDELFAH, Etude et Réalisation d'un système chaotique basé sur le circuit De Chua, Mémoire de Master Professionnel, Université Mouloud Mammer, Tizi-Ouzou, 2014.
- [34]. Chua, L. O. (1994). Chua's circuit 10 years later. *International Journal of Circuit Theory and Applications*, 22(4), 279-305.
- [35]. M. P. KENNEDY, Chaos in the Colpitts oscillator, *IEEE Trans. On circuits and systems-I* 41(1994), p.771-774.
- [36]. A. Tamasevicius, S. Bumeliene, et E. Lindberg, "Improved chaotic Colpitts oscillator For ultrahigh frequencies", *Electronics Letters*, 1569 – 1570, 2004.
- [37]. M. P. KENNEDY, Robust OpAmp realization of chua's circuit, *Frequenz* 46 (1992), p.66-80.
- [38]. O. DE. FEO & G. M. MAGGIO, Bifurcation phenomena in the Colpitts oscillator: A Robustness analysis, *IEEE International symposiumon circuits and systems II (200)*, p 469-472.
- [39]. O. DE.FEO, G. M. MAGGIO & M. P. KENNEDY, The Colpitts oscillator: Families of Periodic solutions and their bifurcations, *Int.J. Bifurcation and Chaos (2000)*.
- [40]. CNTA
- [41]. 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.
- [42]. A. TAMASEVICIUS, G. MYKOLAITIS, S. BUMELIENE, A. CENYS, A. ANAGNOSTOPO- ULOS & E.LINDBERG, Two stage chaotic Colpitts oscillator, *Electronic letters* 37(2001).

- 
- [43]. C. WEGENER & M. P. KENNEDY, RF chaotic Colpitts oscillator, *Proc. Of NDES'95*, p.255-258.
- [44]. Mohammed, B., Samir, K., & Achour, O. (2023, March). Analysis of a Novel 4D Chaotic Oscillator for Communication Systems Up to 6 GHz. In 2023 International Conference on Advances in Electronics, Control and Communication Systems (ICAEECS) (pp. 1-4). IEEE.
- [45]. 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 applications* 47, p.1160-1177.2000.
- [46]. Philips NXP Semiconductors. Data sheet BFP420 NPN 25 GHz, wideband transistor.
- [47]. Kyarginsky, B.E., Maximov, N.A., Panas, A.I., Starkov, S.O.: Wideband microwave chaotic oscillators. In: 1st IEEE International Conference on Circuits and Systems for Communications, pp. 296–299 (2002).
- [48]. Feki, M., Robert, B.: Observer-based chaotic synchronization in the presence of unknown input. *Chaos Solitons Fractals* 15, 831–840 (2003)
- [49]. Liao, T.L., Huang, N.S.: An observer-based approach for chaotic synchronization with applications to secure communications. *IEEE Trans. Circuits Syst. I* 46, 1144–1150(1999).
- [50]. Qiao, S., Shi, Z.G., Chen, K.S., Cui, W.Z., Ma, W., Jiang, T., Ran, L.X.: A new architecture of UWB radar utilizing microwave chaotic signals and chaos synchronization. *Prog. Electromagn. Res.* 75, 225–237 (2007).