الجـــــــــــــــــــمـهـوريـــــة الجـــــــــــــزائـريـة الديمـــــــقـراطيـة الـشـــــــــعبيـة

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

وزارة التـــــــــــــــــــــــــــعـليـم العـــــــالي و البـــــــــحث العـــــلـمـــي

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

جـــــــــــــــامعة أبي بكـــر بـلـقـايد– تـلمســـــــــــــان –

Université Aboubakr Belkaïd– Tlemcen –
Faculté de Technologie

MEMOIRE

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

En : Télécommunications

Spécialité : Systèmes de Télécommunications

Par :

BOUKHARI Aymen Abderrezzaq *et* BENNAHSENE Chahinez

Sujet

Etude et conception d'un nouveau générateur chaotique avec une enveloppe spectrale plate pour les systèmes de communication basée sur le chaos

Soutenu publiquement, le **09 / 06 / 2024**, devant le jury composé de :

Mr A. ABDELMALEK	Maitre de conférences B	Univ. Tlemcen	Président
Mme N. BENMOSTEFA	Maitre de conférences A	Univ. Tlemcen	Examinateur
Mr S. KAMECHE	Professeur	Univ. Tlemcen	Directeur de mémoire
Mr M. BENDAOUD	Doctorant	Univ. Tlemcen	Co-Directeur de mémoire

Année universitaire : 2023/2024

Dédicaces

DÉDICACES << AYMEN >>

Je tiens tout d'abord à remercier ALLAH pour la santé, la volonté et la patience qu'il m'a données pour accomplir ce modeste travail.

À mon père (Allah y Rahma) qui n'a pas pu voir mon travail.

Je remercie du fond de mon cœur, ma mère pour le soutien inconditionnel et les sacrifices qu'ils ont faits pour que je termine mes études.

À mes chers frères « Mohammed », « Khaled » et ma chère sœur « Amel ».

Merci à mes cousins « Djaafar », « Ismaïl » Et tous la famille BOUKHARI.

À mes meilleures amies

« Omar, Abdelbasset, Abdelghani, Abdennour, Zaki, Nory, Samir, Oussama, Khaled. »

A Tous mes amis d'enfance et du long parcours scolaire et universitaire.

Aymen

DÉDICACES << CHAHINEZ >>

Au nom du Dieu le tout puissant Je dédie ce travail :

A la raison de mon existence et le bonheur de ma vie, à la plus belle bénédiction de Dieu, mon cher père…

A la lumière de ma vie, ma chère et mon âme, à la plus belle bénédiction de Dieu, à ma très chère mère …

Mes chers parents, pour tous leurs sacrifices, leur amour, leur tendresse, leur soutien et leurs prières tout au long de mes études,

Merci d'être toujours là pour moi

À mes chers frères « Zakaria », « Oussama », « minouche Anes » ; pour leurs encouragements permanents, et leur soutien moral,

A tous mes amis de l'université, à mes sœurs « Wardchane », « Karima », «Aya» avec qui j'ai partagé les moments de joie et de tristesse des années universitaires dans une même résidence. ; « Marawa » et « Cherifa ». Ainsi que mes cousines « Assia » et « Khadîdja », et bien sûr merci pour mon binôme «Aymen»

Chahinez

Remerciements

Nous remercions notre Créateur Allah, Grand et Miséricordieux, Le Tout Puissant pour le courage qu'il nous a donné pour mener ce travail à terme.

Ce projet de fin d'études a été réalisé 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.

Nous tenons à exprimer notre profonde reconnaissance à notre encadreur, Monsieur KAMECHE Samir, Professeur à l'Université de Tlemcen, pour son encadrement actif, sa grande disponibilité, sa patience et surtout ses conseils avisés qui ont enrichi nos réflexions.

Nous remercions également chaleureusement notre co-encadreur, Monsieur BENDAOUD Mohammed, doctorant à l'Université de Tlemcen, pour son co-encadrement, sa disponibilité, son soutien moral et ses encouragements.

Nous souhaitons exprimer notre respect et notre profonde gratitude à Monsieur ABELMALEK Abdelhafid, Maître de Conférences classe B, qui nous a fait l'honneur de présider ce jury malgré ses nombreuses responsabilités. Nous remercions également Madame BENMOSTEFA Naima, Maître de Conférences classe A, pour avoir accepté d'examiner et d'évaluer ce mémoire.

Enfin, nous adressons nos remerciements les plus chaleureux à nos parents, nos familles et nos amis pour leur soutien et leurs encouragements constants. Nous leur en sommes profondément reconnaissants.

Résumé

Dans ce mémoire, un nouvel oscillateur à quatre dimensions basé sur la configuration de Colpitts avec une enveloppe spectrale presque plate est étudié. Le premier chapitre est dédié à la présentation et à l'explication des notions théoriques liées aux systèmes dynamiques chaotiques, telles que les exposants de Lyapunov, les espaces des phases et les diagrammes de bifurcation. Le deuxième chapitre aborde les différentes méthodes utilisées en cryptographie chaotique ainsi que les techniques de synchronisation des systèmes chaotiques. Le troisième chapitre examine un générateur chaotique capable de produire des oscillations chaotiques à des fréquences inférieures à 1 GHz avec un spectre presque plat. L'étude de cet oscillateur est d'abord réalisée sous Matlab pour résoudre le modèle mathématique, tracer le diagramme de bifurcation, les réponses temporelles chaotiques et les attracteurs étranges. Une deuxième simulation est effectuée sous ADS afin de confirmer les résultats obtenus sous Matlab et d'examiner les caractéristiques fréquentielles de l'oscillateur étudié.

Mots clés : *Configuration de Colpitts, Oscillateur chaotique, cryptographie, diagramme de bifurcation, BFG520.*

مـلـخــص

في هذا المذكرة، يتم دراسة مذبذب جديد رباعي الأبعاد يعتمد على تكوين كولبيتس مع غلاف طيفي شبه مسطح. يُخصص الفصل الأول لتقديم وشرح المفاهيم النظرية المتعلقة بالأنظمة الديناميكية الفوضوية، مثل مؤشرات ليابونوف، فضاءات الأطوار والمخططات التشعبية. يتناول الفصل الثاني الطرق المختلفة المستخدمة في التشفير الفوضوي وكذلك تقنيات تزامن الأنظمة الفوضوية. في الفصل الثالث، يتم دراسة مولد فوضوي قادر على إنتاج تذبذبات فوضوية بترددات أقل من 1 جيجاهرتز مع طيف شبه مسطح. يتم أولاً دراسة هذا المذبذب باستخدام Matlab لحل النموذج الرياضي ورسم المخطط التشعبي، الاستجابات الزمنية الفوضوية والجاذبات الغريبة. ثم يتم إجراء محاكاة ثانية باستخدام ADS لتأكيد النتائج التي تم الحصول عليها باستخدام Matlab ودراسة الخصائص الترددية للمذبذب المدروس.

الكلمات المفتاحية: *تكوين كولبيتس، مذبذب فوضوي، التشفير، مخطط التشعب، BFG520.*

Abstract

In this work, a four-dimensional oscillator based on the Colpitts configuration with an almost flat spectral envelope is studied. The first chapter is dedicated to presenting and explaining the theoretical principles of chaotic dynamical systems, such as Lyapunov exponents, phase spaces, and bifurcation diagrams. The second chapter addresses the different methods used in chaotic cryptography as well as techniques for synchronizing chaotic systems. The third chapter examines a chaotic generator capable of producing chaotic oscillations at frequencies below 1 GHz with an almost flat spectrum. The study of this oscillator is first conducted using Matlab to solve the ODE system and thus obtain the bifurcation diagram, chaotic time series, and strange attractors. A second simulation is performed using ADS to confirm the results obtained under Matlab and to analyze the frequency characteristics of the oscillator under study.

Keywords: *Colpitts configuration, chaotic oscillator, cryptography, bifurcation diagram, BFG520.*

Table des matières

Chapitre I : Notions théoriques

Chapitre II : Cryptographie chaotique

Chapitre III : Etude d'un oscillateur chaotique 4D

Sigles et abréviations

4D: 4-Dimensions

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

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

C: Capacitor**.**

CB: Common **B**ase.

L: Inductor**.**

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

PDE: Partial **D**ifferential **E**quation.

R: Resistor**.**

$\boldsymbol{R}$ **:** L'ensemble des réels.

$\boldsymbol{R^+}$ **:** L'ensemble des réels positifs.

$\boldsymbol{R^n}$ **:** espace vectoriel n dimensionnel sur le corps des réels.

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

Liste des figures

Chapitre I : Notions théoriques

Chapitre II : Cryptographie chaotique

Chapitre III : Etude d'un oscillateur chaotique 4D

Liste des tableaux

Chapitre I : Notions théoriques

Chapitre III : Etude d'un oscillateur chaotique 4D

Introduction générale

Introduction générale

Au fil des dernières années, l'évolution rapide des télécommunications a profondément transformé notre monde, modifiant non seulement notre quotidien, mais aussi la manière dont nous échangeons et stockons les informations. Des avancées telles que l'Internet, les smartphones et l'intelligence artificielle ont révolutionné les communications et la gestion des données. Cependant, cette prolifération technologique a également accru la vulnérabilité des informations sensibles face aux cyberattaques et aux accès non autorisés. Dans ce contexte, la cryptographie est devenue indispensable pour garantir la sécurité et la confidentialité des données échangées.

La cryptographie, ou science de l'encodage des informations, est essentielle pour protéger les communications dans un environnement numérique de plus en plus hostile. Les méthodes traditionnelles de cryptographie incluent la cryptographie symétrique, où une seule clé est utilisée pour le chiffrement et le déchiffrement des données, et la cryptographie asymétrique, qui repose sur une paire de clés publique et privée pour sécuriser les échanges. Ces techniques assurent la confidentialité, l'intégrité et l'authenticité des informations, formant la base de la sécurité numérique moderne.

En parallèle de ces méthodes classiques, la cryptographie chaotique a émergé comme une approche novatrice et prometteuse. Inspirée par la théorie du chaos, cette technique utilise les propriétés dynamiques et imprévisibles des systèmes chaotiques pour générer des clés de chiffrement robustes et résistantes aux attaques. Les systèmes chaotiques, avec leur sensibilité extrême aux conditions initiales, produisent des séquences aléatoires qui rendent les clés de chiffrement extrêmement difficiles à prédire ou à reproduire. Cette caractéristique rend la cryptographie chaotique une solution attractive pour les applications qui exigent un niveau élevé de sécurité.

Dans ce mémoire, nous visons à effectuer une étude détaillée d'un nouveau générateur chaotique basé sur la configuration de Colpitts, capable de produire des oscillations chaotiques avec une enveloppe spectrale presque plate. La recherche d'un générateur chaotique avec une enveloppe spectrale plate est motivée par son utilité dans de nombreuses applications de communication.

Pour atteindre l'objectif de ce mémoire, nous organiserons notre mémoire de la manière suivante :

- **Chapitre I :** Présentation des notions théoriques les plus importantes liées aux systèmes dynamiques chaotiques.
- **Chapitre II :** Explication du concept de chiffrement chaotique, en détaillant les techniques de chiffrement ainsi que les concepts généraux de la synchronisation des systèmes chaotiques.
- **Chapitre III :** Présentation de quelques circuits chaotiques célèbres et de leurs modèles mathématiques, suivie de l'étude d'un nouveau générateur chaotique à l'aide des simulateurs Matlab et ADS.

Chapitre I
Notions théoriques

I.1 Introduction

Le concept de chaos en tant que phénomène scientifique prend racine au 19e siècle, avec le mathématicien français Henri Poincaré reconnu comme l'un de ses précurseurs. Au cours des années 1880, Poincaré s'attelle au problème des trois corps en mécanique céleste, scrutant les trajectoires de trois corps célestes influencés par la gravité. Ses travaux révèlent une sensibilité extrême aux conditions initiales, défiant toute prédiction à long terme des trajectoires des corps et ébranlant ainsi l'idée de déterminisme absolu. Cette remise en question jette les fondements de la théorie du chaos [1].

Dans ce chapitre, nous allons présenter et détailler les notions théoriques les plus importantes liées aux systèmes dynamiques chaotiques.

I.2 Système dynamique

Un système dynamique est un ensemble de règles ou d'équations qui décrivent l'évolution dans le temps d'un système physique, biologique ou autre. Il est caractérisé par des états qui changent au cours du temps en réponse à des conditions initiales ou à des influences externes [2,3]. L'évolution d'un système dynamique dans le temps est à la fois causale et déterministe.

- **Causalité :** La causalité d'un système dynamique signifie que les états futurs du système sont déterminés par ses états actuels et ses conditions initiales. En d'autres termes, chaque changement observé dans le système est la conséquence directe des états précédents et des interactions entre ses composantes.
- **Déterminisme :** Le déterminisme d'un système dynamique signifie qu'il existe des relations mathématiques simples ou compliqués qui régi la dynamique de ce système. Cela implique que les états futurs du système peuvent être prédits avec certitude à partir de ses conditions initiales et des lois mathématiques qui le gouvernent.

I.2.1 Système dynamique continu

Les systèmes dynamiques continus sont des systèmes dans lequel les variables d'état évoluent de manière continue par rapport au temps. Cela signifie que les changements dans le système se produisent de manière fluide et continue à mesure que le temps s'écoule, sans aucun saut discret [4].

Mathématiquement, les systèmes dynamiques continus sont souvent décrits par des équations différentielles ordinaires (ODE) ou des équations aux dérivées partielles (PDE) de la forme :

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

Où : $f : R^+ \times R^n \rightarrow R^n$ décrit la dynamique du système dynamique, et x_0 représente l'état initial de système en t_0.

I.2.2 Système dynamique discret

Un système dynamique discret est un système dans lequel les changements dans les variables d'état se produisent à des instants de temps discrets et séparés. Contrairement aux systèmes dynamiques continus, où les variables évoluent de manière fluide et continue dans le temps, les systèmes dynamiques discrets fonctionnent par étapes discrètes [5,6].

Mathématiquement, les systèmes dynamiques discrets sont souvent décrits par des équations aux différences de la forme suivante :

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

Où : $g : R^n \times N \rightarrow R^n$ décrit la dynamique du système, et x_0 représente l'état initiale de système en k_0.

I.3 Système chaotique

Un système dynamique chaotique est défini par sa sensibilité aux conditions initiales et sa complexité intrinsèque, ce qui rend difficile la prédiction à long terme de son comportement, même avec des règles de comportement simples et déterministes.

Les systèmes chaotiques sont omniprésents dans notre monde, se manifestant dans une variété de domaines, allant de la météorologie à l'économie en passant par la biologie. Leur nature imprévisible et complexe en fait des modèles fascinants pour étudier les phénomènes dynamiques qui défient souvent une explication simple. Par exemple, les systèmes météorologiques, avec leur comportement turbulent et imprévisible, sont des exemples classiques de systèmes chaotiques. De même, les mouvements erratiques des particules dans un système solaire ou les fluctuations des marchés financiers sont également des manifestations de chaos dynamique. La capacité des systèmes chaotiques à reproduire une variété de phénomènes réels en fait des outils précieux pour la modélisation et la simulation dans de nombreux

domaines scientifiques et appliqués. En explorant les caractéristiques des systèmes chaotiques, nous enrichissons notre compréhension des processus complexes qui façonnent notre univers et nous ouvrons la voie à de nouvelles applications et découvertes dans divers domaines de la science et de la technologie.

I.3.1 Non-linéarité

La non-linéarité dans un système chaotique se signifie que les équations qui décrivent la dynamique de système ne sont pas linéaire, cela veut dire que l'évolution des variables d'état ne sont pas proportionnels aux entrées ou aux conditions initiales de manière simple et directe [7].

La non-linéarité est une caractéristique fondamentale des systèmes chaotiques et contribue à leur complexité intrinsèque. Elle est souvent responsable de la sensibilité aux conditions initiales, des bifurcations, des attracteurs étranges et d'autres phénomènes caractéristiques du chaos dynamique.

I.3.2 Déterminisme

Le déterminisme d'un système dynamique chaotique fait référence au fait que sa dynamique est régie par un ensemble d'équations différentielles ordinaires. Cela signifie que, bien que les systèmes dynamiques chaotiques semblent présenter un comportement aléatoire ou indéterminé en raison de leur complexité et de leur sensibilité aux conditions initiales, l'évolution de leurs variables d'état peut théoriquement être prédite avec précision si les conditions initiales et les paramètres du système sont parfaitement connus [8,9].

I.3.4 Aspect aléatoire

Cette caractéristique est bien détaillée dans la figure (I.1), où les états chaotiques du système de Rossler sont comparés avec un signal sinusoïdal. Cette figure permet de mettre en évidence la différence entre une évolution simple, périodique et prédictible et un autre système plus complexe, non périodique et non prédictible.

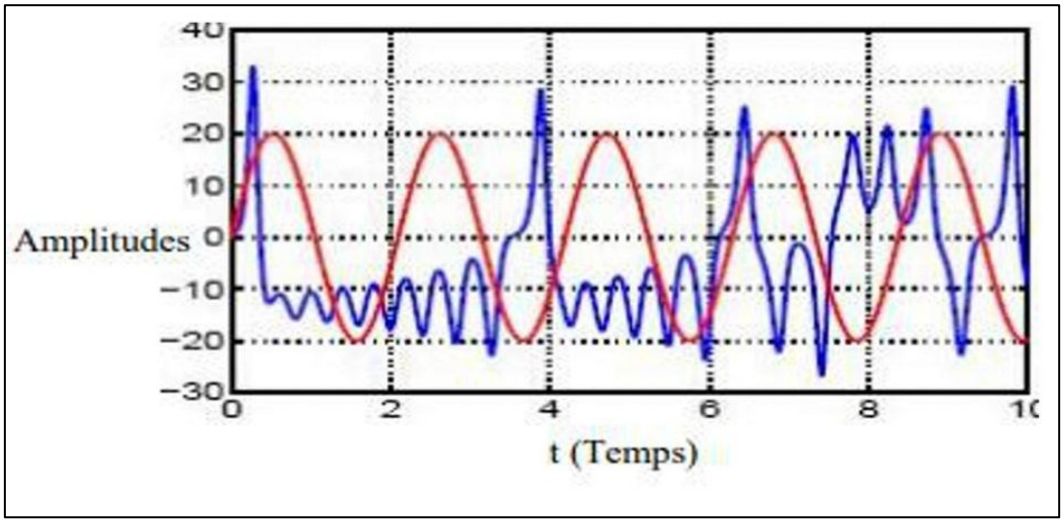


Figure I.1. Evolution temporelle chaotique de Rossler comparé à une sinusoïde.

I.3.4 Sensibilité aux conditions initiales

La sensibilité aux conditions initiales est considérée comme une caractéristique essentielle des systèmes chaotiques. Elle se réfère à la façon dont de petites variations dans les conditions initiales d'un système peuvent entraîner des différences drastiques dans son évolution à long terme. En d'autres termes, même de petits changements dans les conditions de départ peuvent conduire à des résultats radicalement différents. Ce phénomène est souvent illustré par l'analogie de l'effet papillon, où le battement d'ailes d'un papillon dans un endroit du monde pourrait éventuellement déclencher une série d'événements conduisant à un ouragan dans un autre endroit du monde. Les systèmes chaotiques peuvent sembler imprévisibles, mais ils suivent néanmoins des règles définies. Cependant, en raison de leur sensibilité aux conditions initiales, les prédictions à long terme deviennent extrêmement difficiles, voire impossibles, rendant le comportement de ces systèmes apparemment aléatoire [10-12]. Cette caractéristique est illustrée dans la figure (I.2).

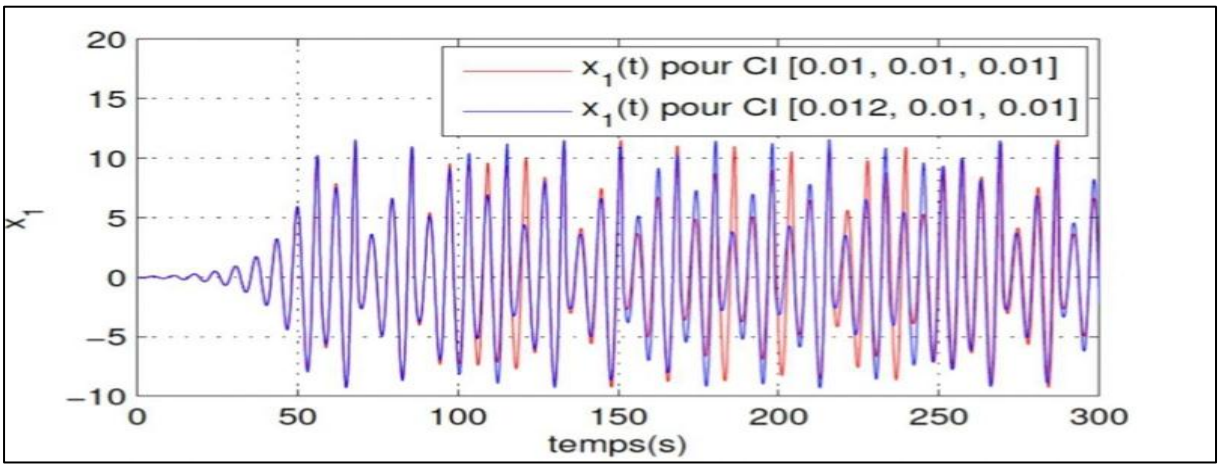


Figure I.2. Propriété de sensibilité aux conditions initiales.

I.4 Espace de phase

L'espace de phase d'un système dynamique est un concept essentiel en dynamique des systèmes. Il représente un espace abstrait où chaque état possible du système est représenté par un point unique. Chaque dimension de cet espace correspond à une variable d'état du système. Par exemple, dans un système à deux dimensions, comme un pendule simple, l'espace de phase serait représenté par un plan cartésien avec une dimension pour la position angulaire et une autre pour la vitesse angulaire. Les trajectoires dans cet espace de phase décrivent l'évolution du système au fil du temps, montrant comment les variables d'état changent en fonction les unes des autres [13-14]. Un aspect crucial de l'espace de phase est qu'il permet de visualiser les comportements dynamiques du système, y compris les points d'équilibre, les cycles périodiques et les trajectoires chaotiques. En analysant ces trajectoires, on peut comprendre en profondeur le comportement global du système et prédire son évolution future. L'espace de phase est ainsi un outil puissant pour explorer et comprendre la dynamique des systèmes complexes dans divers domaines : (la physique, biologie, et l'économie).

I.5 Notion d'attracteur

Dans les systèmes dynamiques, un attracteur est une notion centrale décrivant les états ou les trajectoires vers lesquels un système tend à évoluer au fil du temps. Ces états attracteurs peuvent être des points d'équilibre, des cycles périodiques ou même des trajectoires chaotiques. Un attracteur est ainsi un ensemble de valeurs vers lequel le système semble converger ou rester confiné, indépendamment de ses conditions initiales. Par exemple, un pendule simple a deux attracteurs : un point stable correspondant au pendule en position verticale et un cycle périodique représentant le pendule oscillant de manière régulière. La caractérisation des attracteurs est cruciale pour comprendre le comportement global d'un système dynamique. Elle permet d'identifier les états stables et les trajectoires prédominantes du système, facilitant ainsi les prédictions sur son évolution à long terme [15-17]. Dans les systèmes chaotiques, les attracteurs peuvent prendre des formes complexes, telles que des attracteurs étranges, dont la structure fractale reflète la complexité du comportement du système. Comprendre les attracteurs permet de saisir les motifs sous-jacents et les régularités cachées dans les systèmes dynamiques, offrant ainsi des perspectives précieuses dans de nombreux domaines, de la physique à la biologie en passant par l'économie. Les quatre types d'attracteurs les plus courants sont :

- **Attracteur ponctuel ou fixe :** un point d'équilibre stable vers lequel le système converge.

- **Attracteur cyclique :** une orbite périodique où le système oscille autour d'une trajectoire fermée.
- **Le tore supra Tr (r≥2) :** est un attracteur représentant un régime quasi-périodique caractérisé par la présence de r fréquences de base indépendantes.
- **Attracteur étrange :** un attracteur complexe associer à des systèmes chaotiques, caractérisé par une structure fractale et une sensibilité aux conditions initiales.

I.5.1 Attracteur étrange

L'attracteur étrange est un concept fascinant en théorie du chaos. Il décrit un système dynamique qui peut présenter un comportement chaotique, bien qu'il soit déterministe dans sa nature. Ce type d'attracteur est caractérisé par une sensibilité extrême aux conditions initiales, ce qui signifie que de petites différences dans le départ peuvent entraîner des résultats largement divergents. Cela rend la prédiction à long terme du comportement du système pratiquement impossible, d'où l'adjectif "étrange" pour décrire cet attracteur.

I.5.1.1 Attracteur étrange de Lorenz

Le modèle mathématique de Lorenz est défini par le système d'équations différentielles suivant [18-19]:

$$\begin{cases} \dfrac{dx}{dt} = \sigma(y - x) \\ \dfrac{dy}{dt} = x(\rho - z) - y \\ \dfrac{dz}{dt} = xy - \beta z \end{cases} \qquad \text{(I.3)}$$

Où β, ρ et σ sont les paramètres du système de Lorenz. L'attracteur étrange de Lorenz est obtenu en fixant les valeurs des paramètres comme suit : (σ = 10 ; ρ = 28 ; β = 8/3), avec les conditions initiales $x(0) = 0$, $y(0) = 1$, $z(0) = 20$. Les réponses temporelles et l'attracteur étrange de Lorenz obtenues sont illustrées dans la figure (I.3) et la figure (I.4).

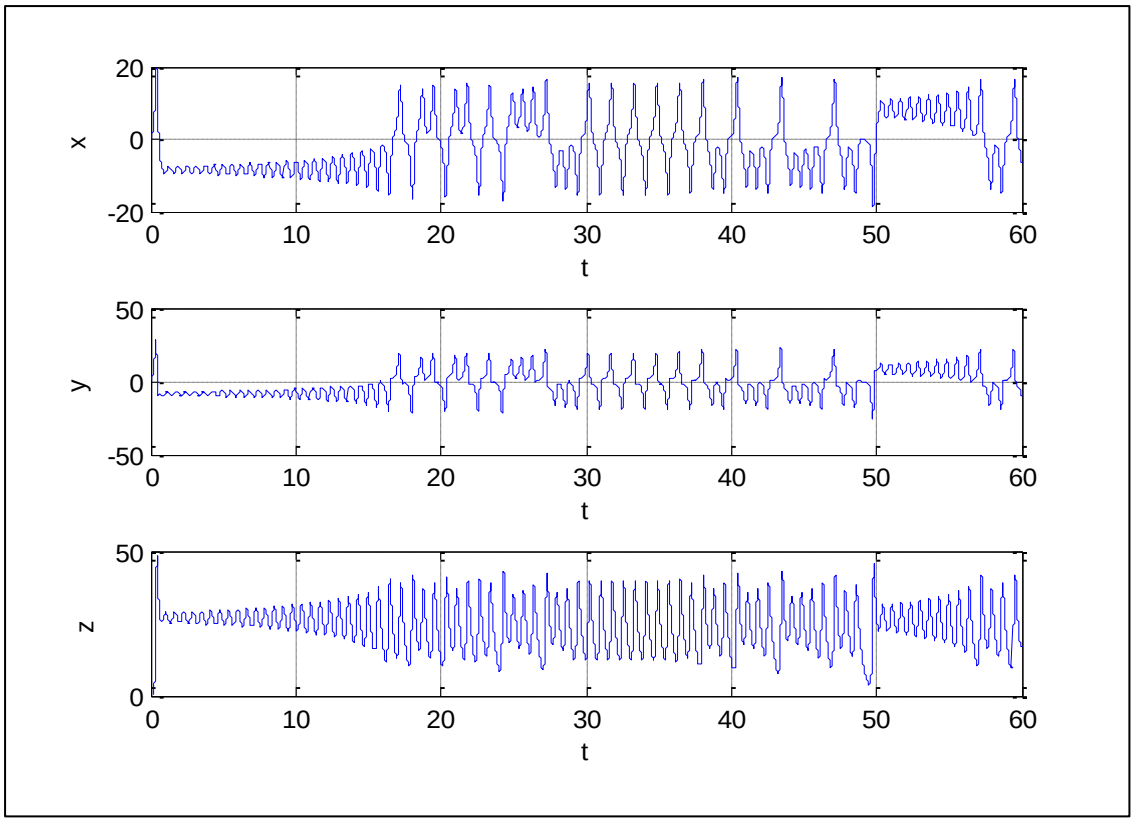


Figure I.3. Réponses temporelles de Lorenz *x(t)*, *y(t)* et *z(t)*.

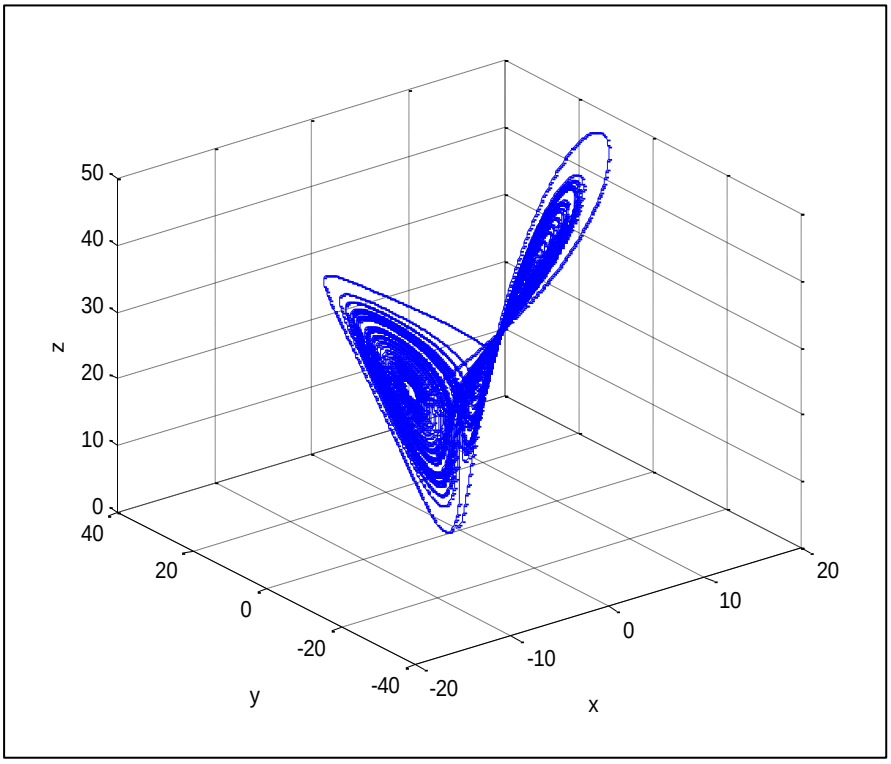


Figure I.4. Attracteur étrange de Lorenz *(x, y, z)*.

I.5.1.2 Attracteur étrange de Rossler

Le modèle mathématique de Lorenz est défini par le système d'équations différentielles suivant [20-21] :

$$\begin{cases} \dfrac{dx}{dt} = -y - z \\ \dfrac{dy}{dt} = x + ay \\ \dfrac{dz}{dt} = b + z(x - c) \end{cases} \quad \text{(I.4)}$$

Où β, ρ et σ sont les paramètres du système de Rossler. L'attracteur étrange de Rossler est obtenu en fixant les valeurs des paramètres comme suit : (a= 0.2 ; b= 0.2 ; c = 5.7), avec les conditions initiales $x(0) = 0.01$, $y(0) = 0.01$, $z(0) = 0.01$. Les réponses temporelles et l'attracteur étrange de Rossler obtenues sont illustrées dans la figure (I.5) et la figure (I.6).

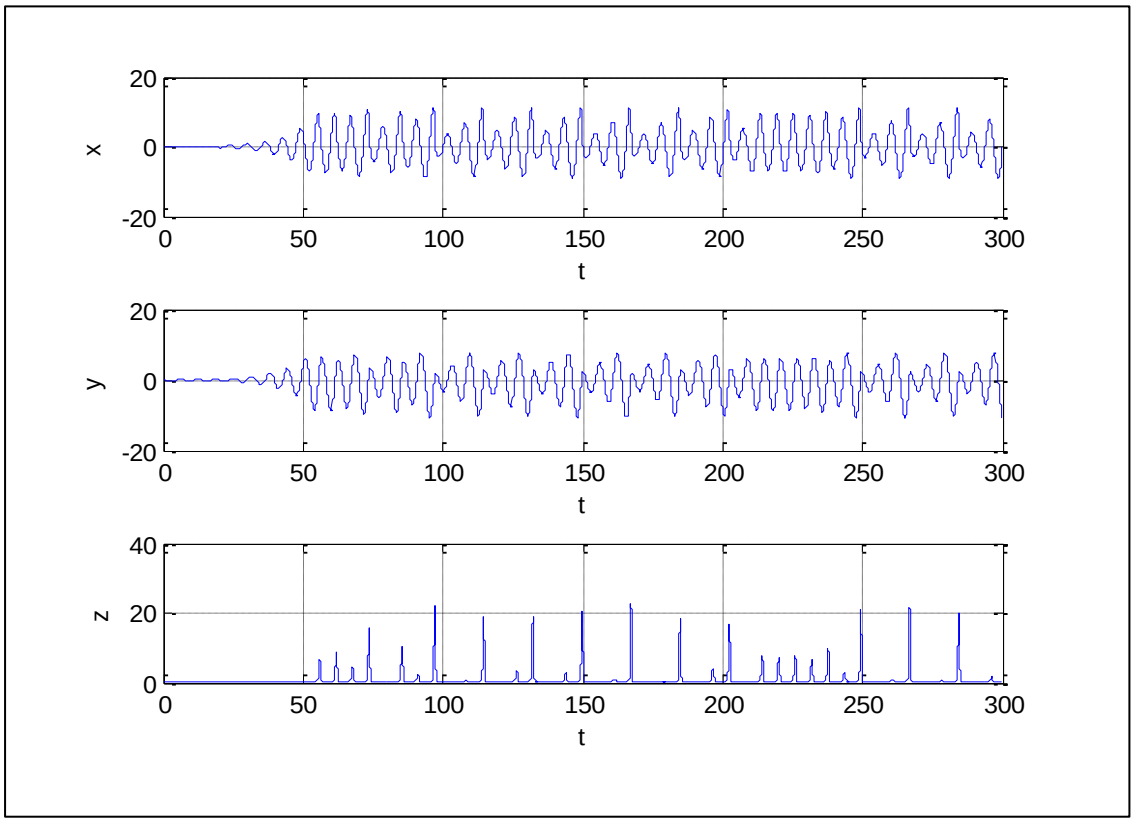


Figure I.5. Réponses temporelles de Rossler *x(t)*, *y(t)* et *z(t)*.

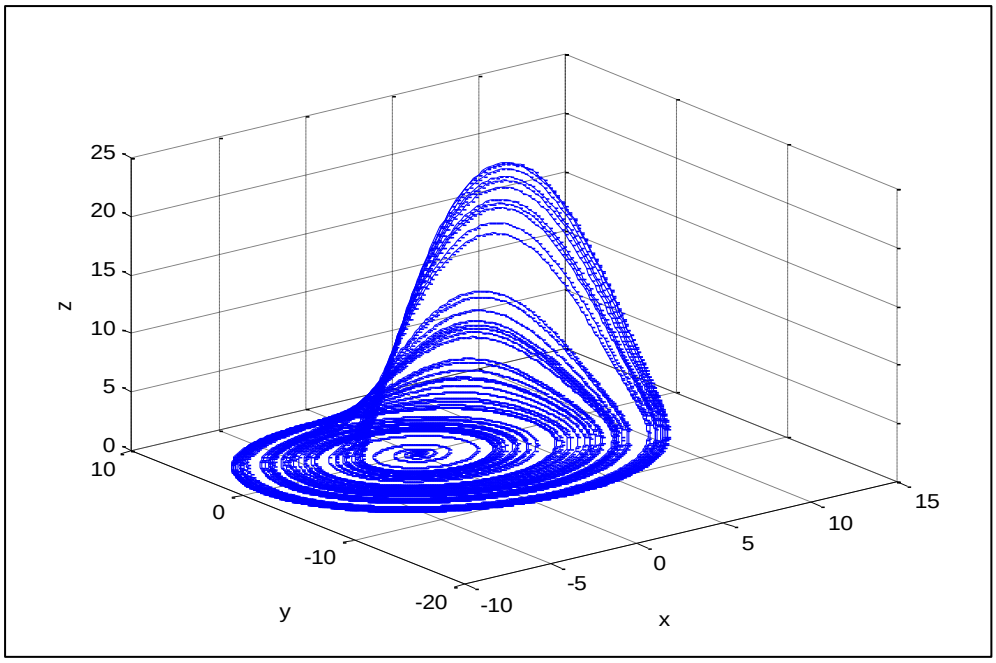


Figure I.6. Attracteur étrange de Rossler *(x, y, z)*.

I.5.2 Dimension de Hausdorff

La dimension de Hausdorff, introduite en 1918 par le mathématicien Felix Hausdorff, est un nombre réel positif ou nul qui caractérise un espace métrique, s'étendant dans l'intervalle $[0, \infty[$. Dans le contexte des attracteurs étranges, elle révèle une dimension fractale (non entière) d, avec $2 < d < n$, où n représente la dimension de l'espace de phase. De plus, un tel attracteur occupe un volume nul dans l'espace de phase [22].

I.6 Exposants de Lyapunov

Les exposants de Lyapunov fournissent une mesure cruciale pour quantifier la sensibilité aux conditions initiales dans les systèmes dynamiques. En théorie du chaos, ils déterminent si un système est déterministe mais erratique, ce qui signifie qu'il peut être très sensible aux petites variations initiales, rendant sa prédiction à long terme imprévisible. Les exposants de Lyapunov mesurent la vitesse à laquelle les trajectoires dans l'espace des phases divergent ou convergent. Un exposant positif indique une divergence exponentielle des trajectoires, signifiant un comportement chaotique, tandis qu'un exposant négatif indique une convergence vers une trajectoire stable. Ces exposants sont essentiels pour comprendre la stabilité des systèmes dynamiques, qu'il s'agisse du mouvement des planètes, des modèles climatiques ou de la dynamique des populations, offrant ainsi un outil puissant pour explorer les comportements complexes des systèmes naturels et artificiels [23-25]. Dans un système

dynamique, le nombre d'exposants de Lyapunov est égal au nombre de variables d'état. Ces exposants sont calculés en utilisant la formule suivante :

$$\lambda_i = \lim_{t\to\infty} \frac{1}{t} ln \frac{\delta_i(t)}{\delta_i(0)} \quad \text{(I.5)}$$

Avec *i*=1…*n*, et *n* est le nombre des variables d'état.

Le comportement d'un système peut être déduit à partir des valeurs des exposants de Lyapunov obtenues. Le tableau (I.1) résume les différents cas possibles.

Tableau I.1. Relation entre les valeurs des exposants de Lyapunov et l'attracteur de système.

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

I.7 Section de Poincaré

La section de Poincaré est une technique puissante utilisée dans l'étude des systèmes dynamiques. Elle consiste à réduire la dimension d'un système à plusieurs variables en le projetant sur un plan ou une surface de dimension inférieure. Cette projection est effectuée à travers des coupes transversales spécifiques, appelées sections de Poincaré, qui interagissent avec les trajectoires du système. En utilisant cette approche, les comportements complexes des systèmes dynamiques peuvent être analysés de manière plus accessible. Par exemple, dans le cas d'un système à trois dimensions, une section de Poincaré bidimensionnelle peut être utilisée pour étudier le comportement d'une trajectoire lorsque celle-ci traverse un plan spécifique dans l'espace des phases. Les points d'intersection entre la trajectoire et la section de Poincaré

fournissent des informations sur le comportement global du système, comme les points fixes, les orbites périodiques ou les trajectoires chaotiques. La section de Poincaré est un outil essentiel pour comprendre la structure et la dynamique des systèmes dynamiques, en permettant une visualisation claire et une analyse approfondie de leurs comportements. Elle est largement utilisée dans des domaines allant de la mécanique céleste à la biologie en passant par la théorie du chaos [26].

I.8 Bifurcation

Les bifurcations sont des points critiques dans la dynamique des systèmes dynamiques où un petit changement dans les paramètres du système entraîne un changement qualitatif dans son comportement. Elles sont souvent associées à des transitions majeures dans les propriétés du système, telles que l'apparition de nouvelles trajectoires, la création ou la destruction de cycles périodiques, ou l'émergence du chaos. Les bifurcations sont classées en différentes catégories en fonction de la nature du changement qui se produit. Par exemple, une bifurcation de selle est caractérisée par la création de trajectoires stables et instables à partir d'un point d'équilibre unique, tandis qu'une bifurcation de Hopf marque le passage d'une solution stable à une solution périodique stable à mesure qu'un paramètre est modifié. Les bifurcations sont cruciales pour comprendre la complexité des systèmes dynamiques et sont étudiées dans divers domaines, tels que la physique, la biologie, l'économie et la chimie, où elles fournissent des insights précieux sur les comportements non linéaires et les phénomènes émergents [27-29].

Un exemple très utilisé pour comprendre la notion de bifurcation est le diagramme de bifurcation de la fonction logistique représenté dans la figure (I.7), cette fonction logistique est définie par la fonction itérative suivante [30] :

$$\boldsymbol{f = [0,1] \rightarrow [0,1] x_{k+1} = f(x_k) = r.x_k(1 - x_k)} \quad \text{(I.4)}$$

Avec r est défini dans $0 : 4$.

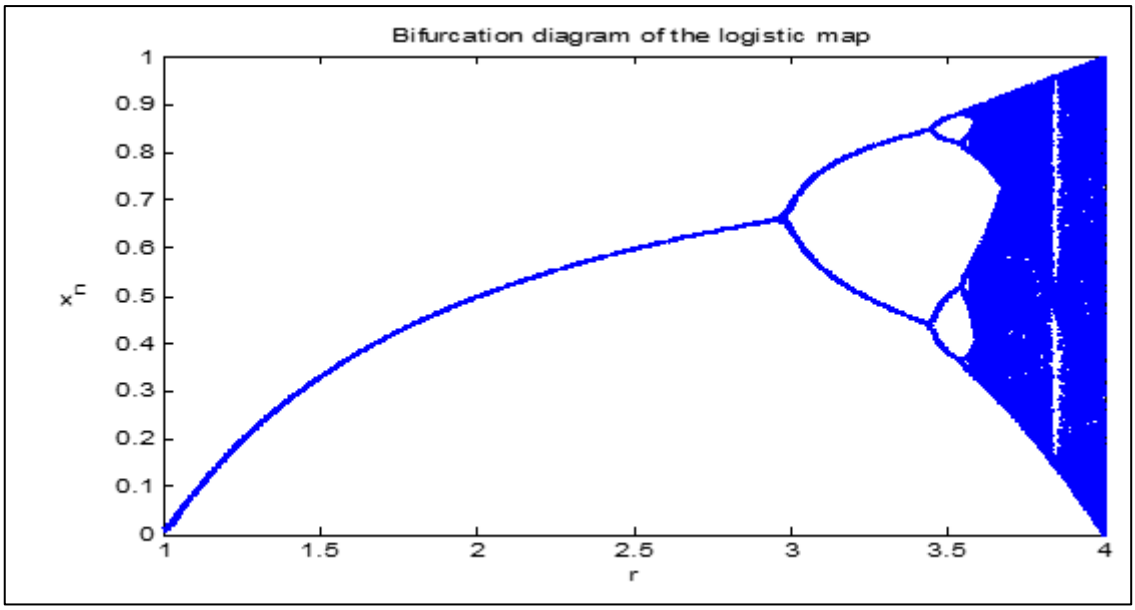


Figure I.7. Diagramme de bifurcation de la fonction logistique.

En observant le diagramme présenté dans la figure (I.7), on constate clairement que le système de la fonction logistique adopte un comportement périodique lorsque la valeur de *r* se situe entre 1 et 3, et un comportement quasi-périodique lorsque *r* est compris entre 3 et 3.373. Au-delà de 3.373, le système adopte un comportement chaotique.

I.9 Routes vers chaos

Les routes vers le chaos décrivent les différentes manières dont un système dynamique peut évoluer vers un comportement chaotique à mesure que ses paramètres sont modifiés. Une des routes les plus courantes est la route par bifurcation, où un système subit des bifurcations successives en modifiant un paramètre de contrôle. Par exemple, dans le cas de la fonction logistique, une série de bifurcations period-doubling se produit lorsque le paramètre de croissance *r* est augmenté. Cela conduit à des cycles de périodes doubles successives jusqu'à ce que le système bascule dans le chaos. Une autre route vers le chaos est par intermittence, où le système oscille entre des périodes de comportement périodique et chaotique à mesure que les paramètres varient. Ce phénomène peut se produire lorsque le système passe par des points critiques ou des bifurcations. Enfin, le chaos peut émerger de manière abrupte par une bifurcation de type "crise", où un petit changement dans les paramètres du système peut entraîner une transition soudaine vers le chaos. Comprendre les routes vers le chaos est crucial dans de nombreux domaines, de la physique à la biologie en passant par l'économie, car cela permet de prédire et de contrôler les comportements complexes des systèmes dynamiques [31-32].

I.9 Conclusion

Dans ce chapitre, nous avons détaillé les notions théoriques les plus importants liés aux systèmes dynamiques chaotiques, ainsi que les méthodes utilisées pour étudier ces systèmes, y compris les espaces des phases, les exposants de Lyapunov et diagramme de bifurcation. Le chapitre suivant sera consacré aux différentes techniques de chiffrement ainsi que les concepts généraux de la synchronisation des systèmes chaotiques.

Chapitre II
Cryptographie chaotique

II.1 Introduction

Dans le domaine des télécommunications, où les échanges de données multimédias connaissent une croissance rapide, il est crucial de disposer de systèmes sécurisés pour protéger les informations personnelles ou confidentielles et assurer la sécurité des transferts de données. Par conséquent, il est essentiel de développer des outils efficaces pour sécuriser les données transférées et les communications contre toute intrusion. Le cryptage des données est souvent la seule méthode efficace pour répondre à ces exigences. Il englobe toutes les techniques permettant de transmettre des informations confidentielles sur un réseau non sécurisé sans risque de divulgation par un intrus. Les anciens algorithmes de chiffrement, qu'ils soient basés sur une clé symétrique ou asymétrique, ont été compromis, rendant nécessaire l'utilisation de nouveaux algorithmes plus sûrs et plus efficaces. La cryptographie chaotique, qui exploite les principes du chaos, répond parfaitement aux besoins de sécurité et de confidentialité. Ce chapitre se consacre aux principes et aux techniques de la cryptographie chaotique.

II.2 Objectifs des crypto-systèmes

Les crypto-systèmes ont plusieurs objectifs fondamentaux pour garantir la sécurité et la confidentialité des informations échangées. Ces objectifs incluent :

- **Confidentialité :** Assurer que les informations transmises ne soient accessibles qu'aux destinataires autorisés. Cela empêche les intrus ou les parties non autorisées d'accéder au contenu des communications.
- **Intégrité :** Garantir que les données ne soient pas modifiées, altérées ou falsifiées durant la transmission. Cela permet de vérifier que les informations reçues sont exactement celles qui ont été envoyées, sans altération.
- **Authentification :** Vérifier l'identité des parties communicantes. Cela assure que les deux parties (l'émetteur et le récepteur) sont bien ceux qu'ils prétendent être, évitant ainsi les attaques par usurpation d'identité.
- **Non-répudiation :** Empêcher qu'une partie nie avoir envoyé ou reçu un message. Cela fournit une preuve que le message a bien été envoyé et reçu, ce qui est essentiel dans de nombreux contextes légaux et commerciaux.

II.3 Cryptographie

La cryptographie consiste à rendre un message illisible par un processus de chiffrement, nécessitant ensuite un déchiffrement pour le rendre compréhensible. Plusieurs algorithmes sont utilisés à cet effet, impliquant l'utilisation de clés pour assurer une communication sécurisée entre l'expéditeur et le destinataire. Certains algorithmes requièrent une clé commune, tandis que d'autres utilisent des clés distinctes pour le chiffrement et le déchiffrement. Même en connaissant l'algorithme, un espion ne peut pas décrypter le message sans la clé appropriée. On distingue deux types d'algorithmes : les algorithmes de chiffrement symétrique, où la même clé est utilisée pour le chiffrement et le déchiffrement, et les algorithmes de chiffrement asymétrique, où des clés différentes sont utilisées pour ces opérations.

II.3.1 Algorithme de chiffrement symétrique

L'algorithme de chiffrement symétrique, ou à clé secrète, consiste à utiliser une même clé pour chiffrer et déchiffrer un message. Dans ce type d'algorithme, la sécurité de la communication repose sur le secret partagé de la clé entre l'expéditeur et le destinataire. Avant la transmission des données, les deux parties doivent s'assurer que cette clé est échangée de manière sécurisée et confidentielle. Même si un tiers connaît l'algorithme utilisé, il ne pourra pas déchiffrer le message sans posséder la clé secrète. Ce type de chiffrement est généralement rapide et efficace, mais nécessite une gestion rigoureuse de la distribution et de la protection des clés [33-34]. Le concept de chiffrement symétrique est illustré dans La figure (II.1).

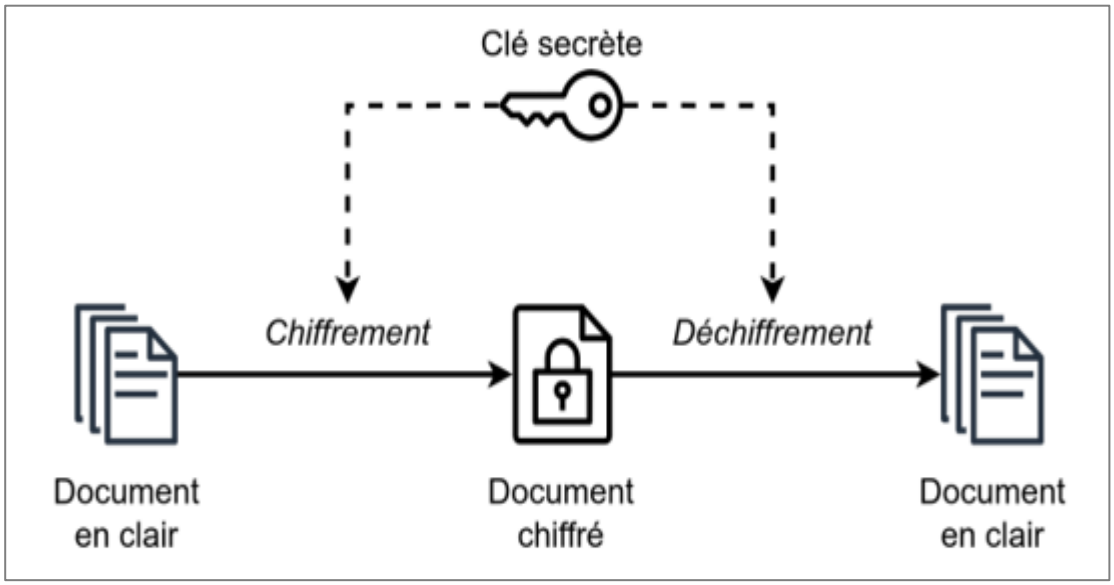


Figure II.1. Cryptographie symétrique.

II.3.2 Algorithme de chiffrement asymétrique

L'algorithme de chiffrement asymétrique, ou à clé publique, consiste à utiliser deux clés distinctes pour chiffrer et déchiffrer un message : une clé publique et une clé privée. La clé publique est accessible à tous et sert à chiffrer les messages, tandis que la clé privée est conservée secrète par le destinataire et est utilisée pour déchiffrer les messages. Dans ce type d'algorithme, même si un tiers connaît la clé publique et l'algorithme utilisé, il ne pourra pas déchiffrer le message sans posséder la clé privée. Ce modèle élimine le besoin de partager une clé secrète commune de manière sécurisée, résolvant ainsi le problème de la distribution des clés [35-36]. Cependant, les algorithmes asymétriques sont généralement plus lents et computationnellement intensifs que les algorithmes symétriques.

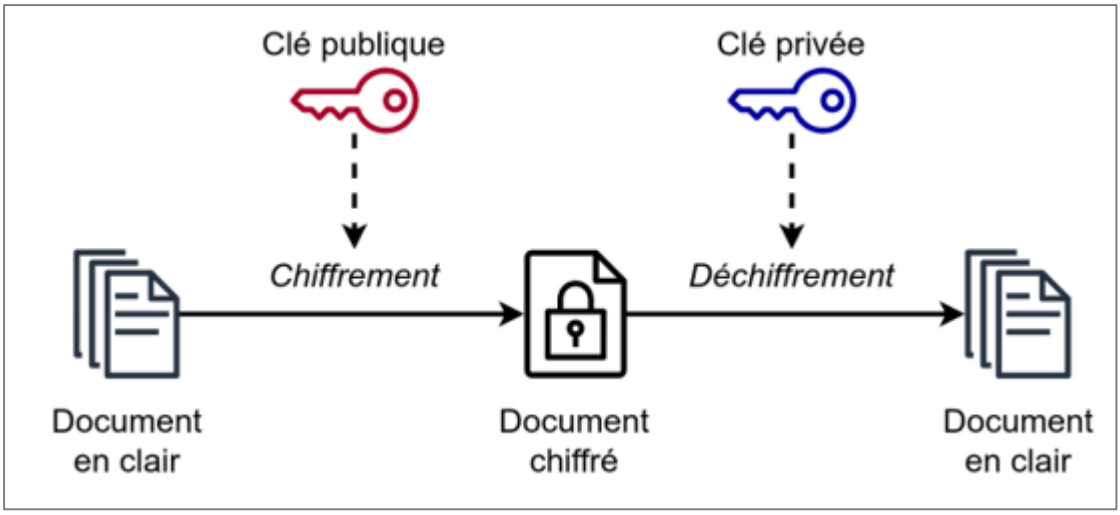


Figure II.2. Cryptographie symétrique.

II.4 Cryptanalyse

La cryptanalyse, à la fois un art et une science, consiste à étudier et à appliquer des techniques pour déchiffrer des messages chiffrés sans connaître la clé secrète. Elle vise à évaluer la sécurité des algorithmes de chiffrement en identifiant leurs faiblesses et en tentant de les exploiter. Les cryptanalystes utilisent diverses méthodes pour casser les codes, telles que l'analyse des fréquences, les attaques par force brute, l'ingénierie inverse et d'autres techniques mathématiques et informatiques avancées. Le but ultime de la cryptanalyse est de déterminer si un système de cryptographie est suffisamment robuste pour résister aux tentatives de décryptage non autorisées et de proposer des améliorations pour renforcer la sécurité des communications.

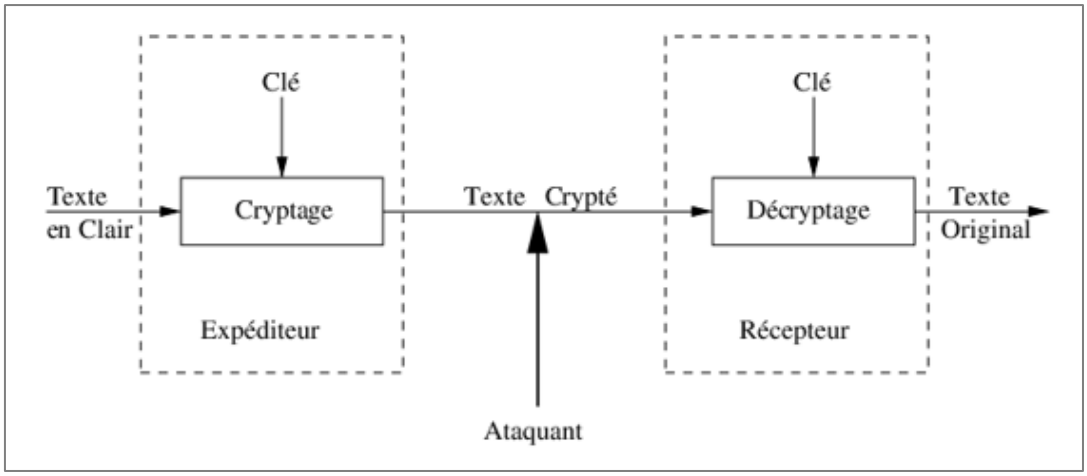


Figure II.3. Concept de cryptanalyse.

II.5 Techniques de chiffrement par chaos

Le chiffrement chaotique est une technique de cryptage utilisant des systèmes chaotiques pour produire des séquences de nombres pseudo-aléatoires, lesquelles servent à sécuriser les données. Son principe repose sur l'incorporation d'un signal chaotique, produit par un système dynamique chaotique, dans le message à transmettre. Ce signal agit comme une clé de chiffrement, transformant le texte en un format chiffré.

Généralement, le chiffrement chaotique s'effectue en trois étapes principales. Tout d'abord, un signal chaotique est généré à l'aide d'un système dynamique chaotique. Ensuite, ce signal est combiné avec le message à chiffrer pour produire le texte crypté. Enfin, ce texte crypté est transmis au destinataire, qui peut le déchiffrer en utilisant le même signal chaotique utilisé lors de l'émission.

Le chiffrement chaotique est considéré parmi les méthodes de chiffrement les plus efficaces, et cela est dû à la sensibilité aux conditions initiales qui caractérise les signaux chaotiques générés. En revanche, cette technique peut être fragile aux attaques si les paramètres de système chaotique ne sont pas configurés d'une manière correcte. De tout cela, on peut conclure qu'il est nécessaire de choisir des générateurs chaotiques adaptés aux applications à sécuriser afin de garantir un haut niveau de sécurité.

Dans ce qui suit, nous allons présenter et détailler les différentes méthodes de chiffrement chaotique.

II.5.1 Chiffrement par addition

La cryptographie chaotique par addition est une méthode de cryptage qui repose sur l'addition de valeurs chaotiques à un message clair pour produire un texte chiffré. Dans ce processus, un signal chaotique est généré à partir d'un système dynamique chaotique, puis il est combiné avec le message d'origine en utilisant une opération d'addition modulo. Cette opération crée un texte chiffré où chaque caractère est modifié de manière non linéaire en fonction du signal chaotique. Le destinataire peut ensuite utiliser le même signal chaotique pour effectuer l'opération inverse et récupérer le message d'origine. Cette méthode de cryptage est appréciée pour sa robustesse contre les attaques et sa capacité à générer des données chiffrées imprévisibles, ce qui en fait une solution prometteuse pour sécuriser les communications sensibles dans divers domaines, tels que les télécommunications, la sécurité des données et la confidentialité des informations [37-38]. Pour une illustration détaillée, référez-vous à la figure (II.4) montrant le principe du chiffrement par addition.

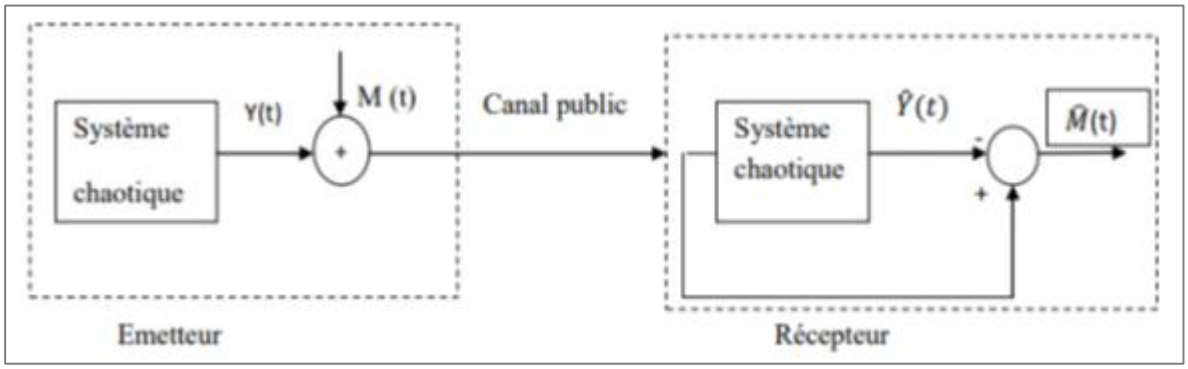


Figure II.4. Chiffrement chaotique par addition.

II.5.2 Chiffrement par commutation

La cryptographie chaotique par commutation est une méthode utilisée pour sécuriser le transfert de données binaires, généralement représentées par les valeurs 0 et 1. Ce système implique un émetteur composé de deux systèmes chaotiques ou plus. À chaque niveau du message m(t), l'un des systèmes transmet sa sortie via la ligne de transmission, alternant ainsi entre deux attracteurs étranges. Cette alternance crée un signal chaotique modulé qui transporte le message de manière sécurisée [39].

D’autre part, le dispositif récepteur est équipé de deux systèmes chaotiques, qui peuvent être soit identiques, soit totalement différents de ceux de l'émetteur, ainsi qu'un bloc de comparaison. Ce bloc joue un rôle crucial en déterminant la valeur du message m'(t) en

comparant la sortie du système chaotique du récepteur à celle de l'émetteur. Lorsque les deux signaux sont synchronisés, le bloc de comparaison peut alors identifier avec précision la valeur du message. Cette méthode offre un moyen robuste et sécurisé de transférer des données binaires sensibles, trouvant des applications dans divers domaines où la confidentialité et la sécurité des informations sont primordiales [40-41].

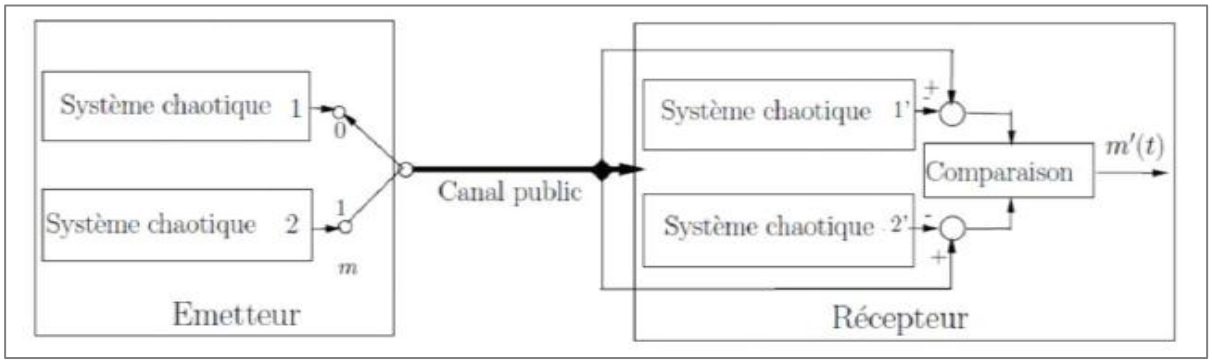


Figure II.5. Chiffrement chaotique par commutation.

II.5.3 Chiffrement par modulation

La cryptographie chaotique par modulation est une méthode sophistiquée qui utilise le message contenant l'information pour ajuster un ou plusieurs paramètres de l'émetteur chaotique. Ce schéma, représenté dans la figure (II.6), implique l'utilisation d'un contrôleur adaptatif pour garantir la synchronisation au niveau du récepteur tout en ajustant les variations des paramètres modulés. Au niveau de l'émetteur, la modulation des paramètres induit une évolution constante de la trajectoire à travers les attracteurs, ce qui rend le signal transmis beaucoup plus complexe qu'un signal chaotique conventionnel. Cependant, il est crucial que l'intégration du message et la fonction de modulation des paramètres ne compromettent pas le caractère chaotique du signal envoyé au récepteur. Cette approche exploite pleinement les caractéristiques des systèmes chaotiques pour garantir un niveau élevé de sécurité et de robustesse dans le transfert d'informations sensibles. Cette méthode offre ainsi une solution prometteuse pour sécuriser les communications dans divers domaines où la confidentialité et la fiabilité des données sont primordiales [42-43].

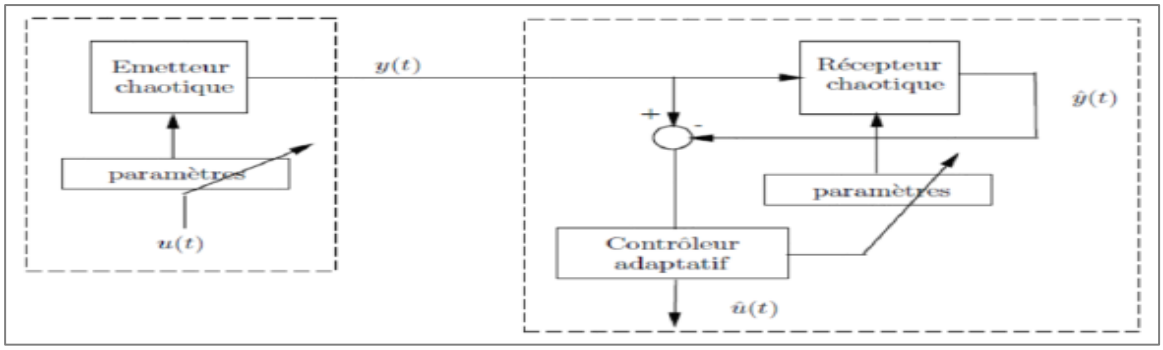


Figure II.6. Chiffrement chaotique par modulation.

II.6 Définition de la synchronisation

La synchronisation fait référence à un phénomène complexe où deux systèmes chaotiques, initialement indépendants, peuvent finir par évoluer de manière coordonnée ou synchronisée. Ce phénomène peut se produire même si les systèmes présentent des comportements chaotiques imprévisibles.

La synchronisation en système chaotique peut être observée lorsque les états dynamiques des systèmes deviennent corrélés, de sorte que des motifs de comportement similaires ou identiques émergent dans les deux systèmes. Cela peut se produire grâce à des mécanismes de couplage entre les systèmes qui permettent d'échanger des informations et d'influencer mutuellement leurs dynamiques.

II.7 Classes de synchronisation

Les classes de synchronisation sont déterminées par la direction de l'échange d'énergie, où l'on distingue la synchronisation par couplage unidirectionnel et celle par couplage bidirectionnel.

II.7.1 Synchronisation par couplage unidirectionnel

La synchronisation par couplage unidirectionnel vise à synchroniser un système "a" avec un système "b" sans que le système "b" influence le système "a". Ce type de synchronisation utilise un composant fonctionnant dans une seule direction, comme un circuit électrique suiveur (ou buffer en anglais), qui reproduit le signal d'entrée sans altération ni amplification, permettant ainsi de le transmettre sans perte à un autre système.

Dans ce contexte, le système "a" envoie son signal à travers un circuit suiveur, qui le transmet sans modification au système "b". Ainsi, le système "b" se synchronise avec le signal du système "a", tandis que le signal du système "b" n'affecte pas le système "a". Cette méthode

de couplage unidirectionnel peut être appliquée dans divers domaines en dehors de l'électronique, tels que la communication entre ordinateurs ou la synchronisation des mouvements entre robots industriels. Elle offre une solution efficace pour des scénarios où un flux d'information à sens unique est nécessaire pour garantir une synchronisation précise et stable. Le principe de ce couplage est illustré dans la figure (II.7).

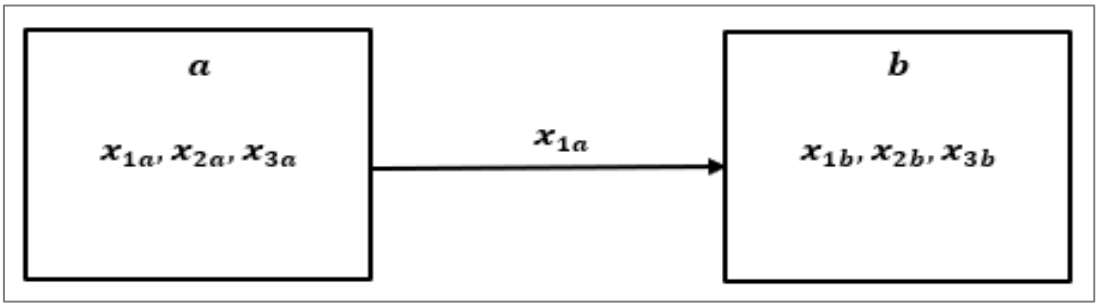


Figure II.7. Couplage unidirectionnel

II.7.2 Synchronisation par coulage bidirectionnel

La synchronisation par couplage bidirectionnel vise à synchroniser réciproquement deux systèmes "a" et "b" en permettant un échange d'énergie dans les deux directions. Pour ce faire, on utilise un composant qui facilite cet échange bidirectionnel, comme une simple résistance. Une résistance permet au courant de circuler dans les deux sens, ce qui permet aux systèmes de s'influencer mutuellement.

Lorsqu'on couple deux systèmes bidirectionnellement à l'aide d'une résistance, ils peuvent échanger de l'énergie et ainsi se synchroniser. Par exemple, si l'un des systèmes envoie un signal à l'autre, ce signal est reçu et utilisé par l'autre système pour ajuster sa propre sortie en conséquence. Ce processus d'ajustement mutuel continue jusqu'à ce que les deux systèmes atteignent une synchronisation parfaite.

Il est crucial de choisir le bon composant de couplage en fonction des caractéristiques spécifiques des systèmes à synchroniser. Outre les résistances, d'autres composants tels que les inductances et les capacités peuvent également être utilisés pour le couplage bidirectionnel, offrant diverses options pour optimiser la synchronisation en fonction des besoins spécifiques des systèmes en question.

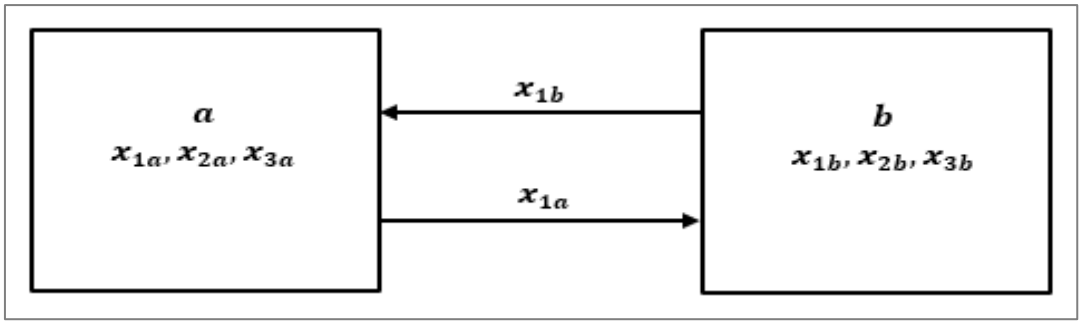


Figure II.8. Couplage bidirectionnel

II.8 Différents régimes de synchronisation

Parmi les nombreuses méthodes de synchronisation trouvées dans la littérature, nous allons citer quelques-unes des approches les plus courantes :

II.8.1 Synchronisation par décomposition de système

Cette méthode, couramment utilisée pour synchroniser des systèmes chaotiques, consiste à diviser le système chaotique en deux sous-systèmes : un maître et un esclave. Par le biais d'une rétroaction, le système esclave est synchronisé avec le système maître. Pecora et Carroll ont proposé une technique de synchronisation fondée sur un système chaotique [44-45], défini par l'équation de dynamique suivante :

$$x = f(x) \tag{II.1}$$

Où *x* est le vecteur d'état et *f* est une fonction non linéaire générant le comportement chaotique. En appliquant une fonction de sortie *h(x)*, le signal chaotique peut être converti en un signal de sortie *y* :

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

Utilisée pour assurer que le système esclave suive le comportement chaotique du système maître, cette méthode repose sur la rétroaction. Elle consiste à comparer les signaux de sortie des deux systèmes et à ajuster les paramètres du système esclave pour minimiser la différence entre eux.

II.8.2 Synchronisation retardée

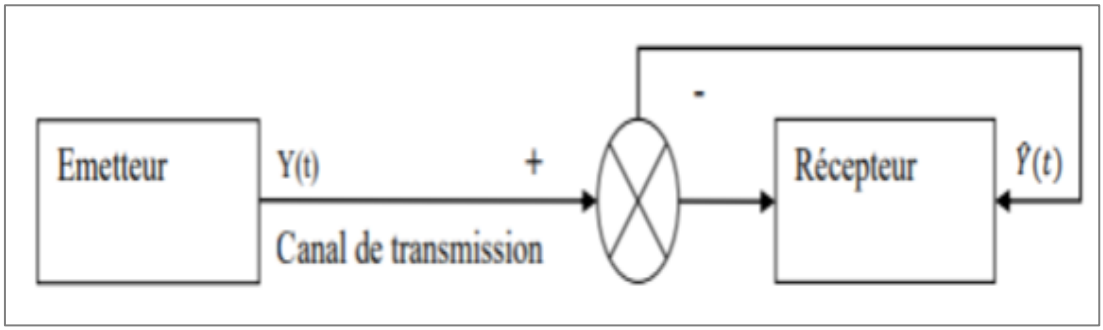
Dans ce processus de synchronisation, l'état du système esclave converge vers un état déphasé dans le temps par rapport au système maître, cela signifie :

$$\lim_{t\to\infty} \|x'(t) - x(t-\tau)\| = 0 \tag{II.3}$$

Dans cette expression, *x(t)* représente l'état du système émetteur, *x'(t)* correspond à l'état du système récepteur, et τ est un délai positif.

II.8.3 Synchronisation en boucle fermée

La synchronisation en boucle fermée est une méthode visant à synchroniser des systèmes où l'état du système récepteur est ajusté en temps réel en fonction de l'erreur mesurée entre le signal émis par le système principal et celui régénéré par le système secondaire. Ce processus consiste à comparer le signal du système principal avec celui reçu par le système secondaire, décalé dans le temps, afin de calculer l'erreur de synchronisation. Cette erreur est ensuite utilisée pour ajuster l'état du système secondaire, le synchronisant ainsi avec le système principal [46]. Une illustration simplifiée de ce processus est présentée dans la figure (II.9).



II.9. Synchronisation par boucle fermée

II.8.4 Synchronisation projective

Dans ce processus, le système émetteur envoie son état *x(t)* au système récepteur, qui utilise cette information pour ajuster sa propre sortie $\check{x}(t)$ à l'aide d'un contrôleur. Ce contrôleur introduit un délai positif τ, permettant ainsi à l'état du système émetteur d'être transmis au système récepteur avec un décalage temporel. De plus, un facteur d'échelle α est utilisé pour ajuster l'amplitude de la sortie du système récepteur afin qu'elle corresponde à celle du système émetteur. La condition de synchronisation dans cette méthode stipule que la différence entre l'état estimé $\hat{x}_1(t)$ du système récepteur et une version retardée $x(t-\tau)$ de l'état du système émetteur converge vers zéro lorsque le temps t tend vers l'infini [47-48].

II.8.5 Synchronisation de phase

Pour deux systèmes à phases périodiques $\emptyset 1$ et $\emptyset 2$, la synchronisation peut s'exprimer par l'équation suivante :

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

Avec *n* et *m* sont des entiers naturels *c* est une constante positive. La phase d'un système chaotique peut être définie grâce à ce mode de synchronisation. Le signal analytique est une fonction complexe définie comme suit :

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

Où $\tilde{\boldsymbol{s}}(\boldsymbol{t})$ est la transformée de Hilbert de la série temporelle *s(t), A(t)* est l'amplitude du signal *ψ(t)* et *Ø(t)* sa phase.

II.8.6 Anti synchronisation

Le système maître et le système esclave sont prêts à faire l'anti-synchronisation s'ils ont un contrôle *u (t; x; y)* comme indiqué dans l'équation :

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

Elle est satisfaite pour toutes les conditions initiales *x (0)* et *y (0)* des deux systèmes.

II.8.7 Synchronisation par observateur

Un observateur d'état est un système dynamique capable d'estimer l'état non mesuré d'un système en se basant sur ses entrées, ses sorties et la connaissance du modèle dynamique. En d'autres termes, les observateurs d'état nous permettent de reconstruire l'état interne d'un système à partir d'informations limitées sur celui-ci [49-51].

Dans le contexte de la synchronisation chaotique, des observateurs d'état sont utilisés pour estimer l'état du système maître en fonction de la sortie envoyée aux systèmes esclaves. Ensuite, le système esclave est ajusté en fonction de cette estimation pour reproduire le comportement chaotique du système maître. Cette approche de synchronisation chaotique a inspiré de nombreuses autres méthodes et techniques permettant de synchroniser des systèmes chaotiques dans des conditions plus générales et complexes. Théoriquement, le problème de la conception d'un observateur pour un système (non linéaire) est défini comme suit :

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

Où (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.

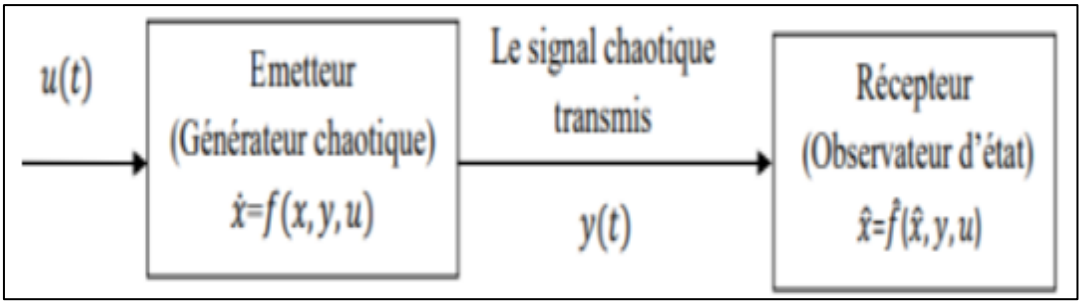


Figure II.10. Synchronisation à base d'observateurs

L'utilisation d'observateurs est une méthode courante pour estimer les états inconnus de systèmes dynamiques qui ne peuvent pas être mesurés directement. Ceci est particulièrement utile pour synchroniser des systèmes chaotiques dont l'état interne est difficile à mesurer avec précision.

Ces observateurs sont utilisés pour évaluer l'état du système maître en fonction de la sortie envoyée aux systèmes esclaves lors de la synchronisation chaotique. Le comportement chaotique du système maître est reproduit en ajustant le système esclave en fonction de cette estimation. Il y a plusieurs types d'observateurs : Observateur Luen berger, Observateur Kalman et Observateur adaptatif. Il est possible d'utiliser ces outils en fonction des caractéristiques du système observé. Il est possible de concevoir ces observateurs pour atteindre divers objectifs, tels que la stabilisation, l'observation d'états entiers ou partiels et même le contrôle.

L'utilisation d'observateurs peut être une méthode efficace de coordination de systèmes chaotiques, car elle permet de déduire l'état interne du système à partir de sa sortie et de l'adapter en conséquence.

II.9 Conclusion

Dans ce deuxième chapitre, nous avons d'abord exposé les objectifs des crypto-systèmes. Ensuite, nous avons décrit la cryptographie chaotique et mentionné les deux types de clés utilisés pour le chiffrement. Nous avons également présenté les diverses techniques de chiffrement basées sur le chaos analogique ainsi que les différents régimes de synchronisation.

Chapitre III

Etude d’un oscillateur chaotique 4D

III.1 Introduction

Dans la littérature, nous trouvons plusieurs circuits chaotiques proposés pour l'objectif de la génération de chaos, telles que le circuit de Chua [52], le circuit de Rossler [18], l'oscillateur de Colpitts [53], ce dernier étant considéré comme l'un des oscillateurs les plus connus et les plus utilisés, et cela est dû aux ses caractéristiques fréquentielles [54-60].

Nous allons commencer ce chapitre par présenter quelques structures chaotiques, puis nous allons faire une étude détaillée d'un oscillateur chaotique, qui peut générer des oscillations chaotiques avec un spectre plat jusqu'à 1 GHz.

III.2 Circuit de Chua

La figure (III.1) illustre le circuit de Chua, qui est un circuit électrique non linéaires utilisé comme exemple classique pour étudier le chaos et les systèmes dynamiques. Il comprend des composants linéaires : deux condensateurs C_1 et C_2, une inductance L, et une résistance R, ainsi qu'un composant non linéaire N_R appelé la diode de Chua (ou le morceau de Chua), cette diode est l'élément responsable sur la génération du chaos. Le modèle mathématique qui décrit la dynamique de ce circuit [52,61] :

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

Ou $f(x) = m_1 x + \frac{1}{2}(m_0 - m_1)(|x+1| - |x-1|)$ est une fonction linéaire par morceaux. L'attracteur chaotique de Chua est illustré dans la figure (III.2), il obtenu en fixant les paramètres de système comme suit : (α=15.8, β=28, m_0=-1.143, m_1=-0.714).

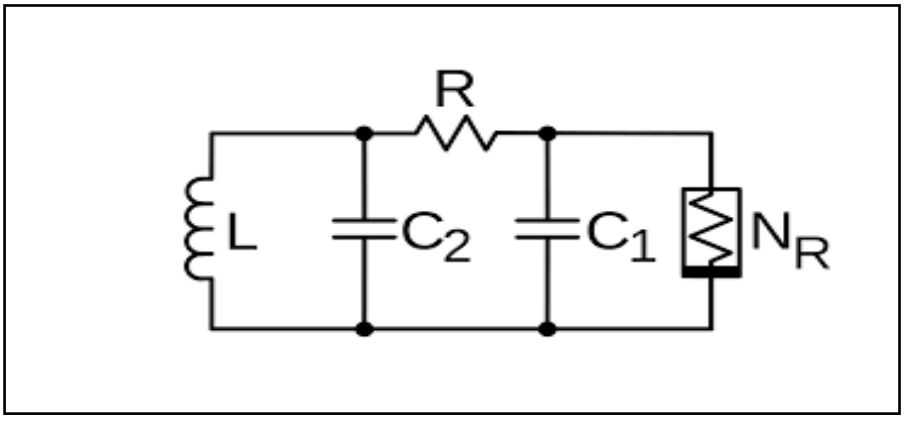


Figure III.1. Circuit de Chua.

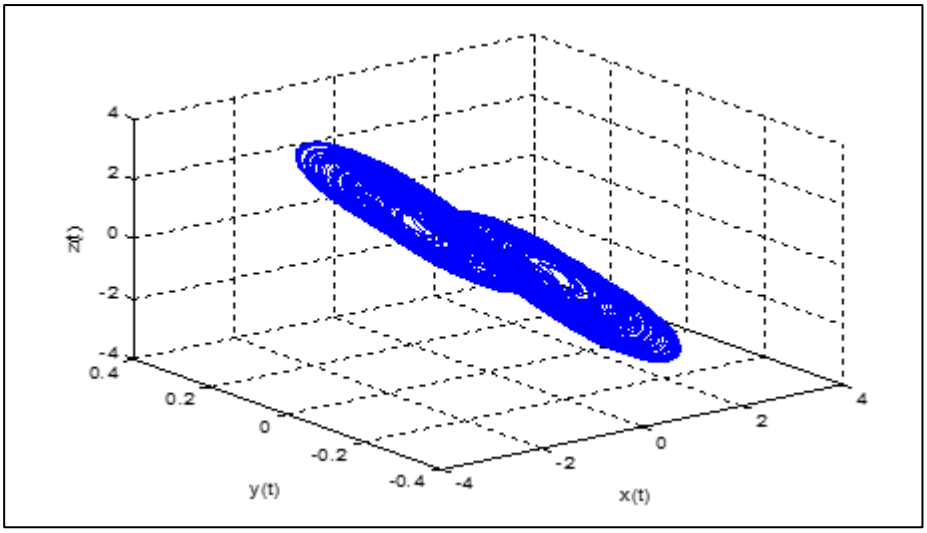


Figure III.2. Attracteur étrange de Chua (x, y, z).

III.3 Oscillateur Colpitts standard

Le schéma de l'oscillateur Colpitts est représenté dans la figure (III.3). Ce montage exploite une configuration en base commune du transistor Q, procurant un gain plus important et une bande passante plus étendue. Le circuit résonnant LC se trouve connecté entre le collecteur et la base du transistor. Une portion de la tension de ce circuit est réinjectée vers l'émetteur. Les sources V_0 et I_0 fixent le point de fonctionnement du transistor. La fréquence d'oscillation fondamentale est déterminée par les valeurs des composants du circuit résonnant.

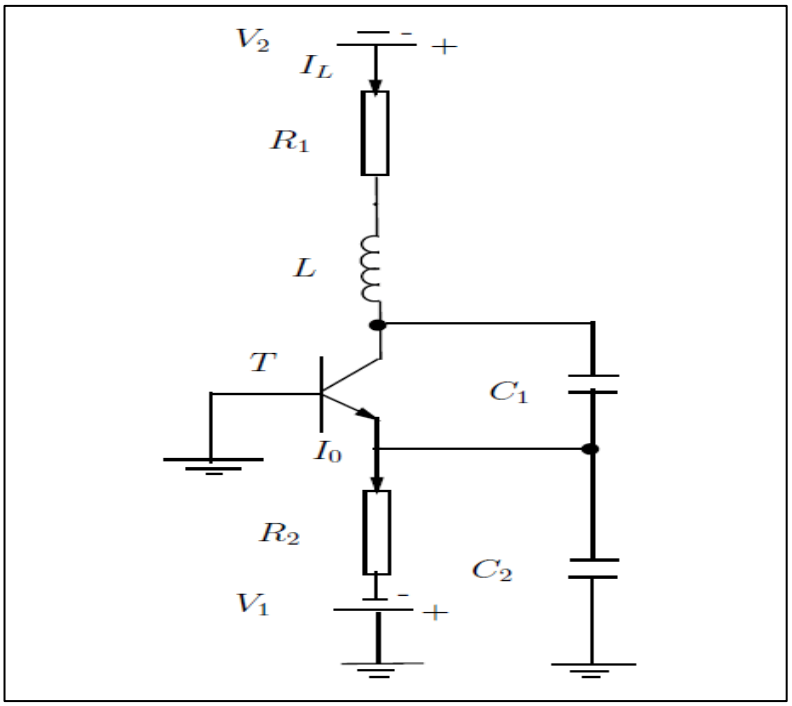


Figure III.3. Oscillateur Colpitts chaotique.

Les comportements dynamiques de l'oscillateur Colpitts sont décrit par le système d'équations différentielles [53,62,63] :

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

Avec $n\ (x_2) = exp\ (-x_2) - 1$ et $k = \frac{C_2}{C_1 + C_2}$. g correspond à la rétroaction de l'oscillateur quand le critère de Barkhausen est respecté. Le facteur de qualité du circuit LC déchargé est défini par $Q = \frac{\omega_0 L}{R}$. L'attracteur étrange (x_1, x_2) du circuit Colpitts est illustré dans la figure (III.3), où les valeurs des paramètres associés à cet attracteur sont : k=0.5, g=4.46, et Q=1.38.

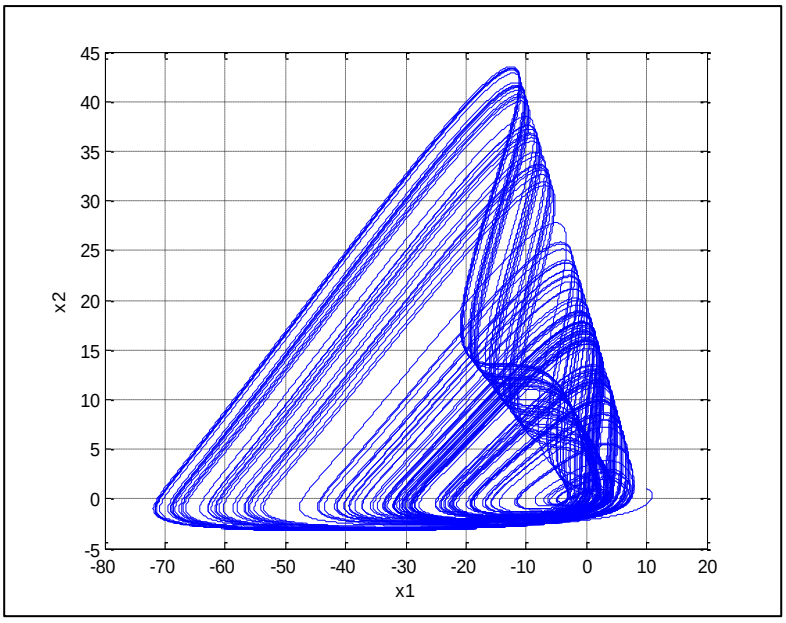


Figure III.4. Attracteur chaotique de l'oscillateur Colpitts (x_1, x_2).

III.4 Oscillateur Colpitts amélioré

Le circuit de l'oscillateur Colpitts amélioré est illustré dans la figure (III.5), il est presque identique à la version standard du Colpitts. La différence entre les deux c'est que l'inductance L est déplacée du collecteur vers la base du transistor bipolaire Q.

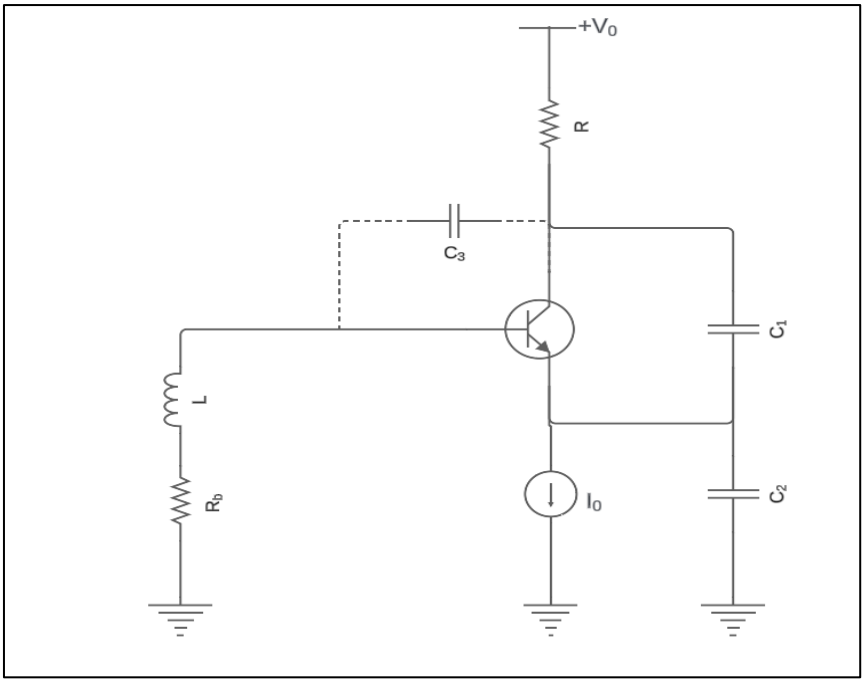


Figure III.5. Circuit de l'oscillateur Colpitts amélioré.

La dynamique de l'oscillateur Colpitts amélioré est décrit par le système des équations suivantes [64] :

$$\begin{cases} \dot{x}_1 = \sigma_1(-x_1 - x_2) + x_4 - \gamma\Psi(x_1, x_3) \\ \dot{x}_2 = \varepsilon_1\sigma_1(-x_1 - x_2) + \varepsilon_1 x_4 \\ \dot{x}_3 = \varepsilon_2(x_4 - (1-\alpha)\gamma\Psi(x_1, x_3)) \\ \dot{x}_4 = -x_1 - x_2 - x_3 - \sigma_2 x_4 \end{cases} \quad \text{(III.3)}$$

Où les paramètres de ce système sont définis comme suit :

$$\begin{aligned} & x_i V_T = V_{Ci} - V_{Ci}^0; (i = 1,2,3); x_4 V_T = \rho(I_L - I_L^0) \\ & t = \tau\sqrt{LC_1}, \rho = \sqrt{L/C_1}\,, \varepsilon_1 = C_1/C_2\,, \varepsilon_2 = C_1/C_3 \\ & \sigma_1 = \rho/R_C\,, \sigma_2 = R_B/\rho\,, \gamma = \rho I_0/V_T \end{aligned} \quad \text{(III.4)}$$

L'attracteur étrange (x_1, x_2) de l'oscillateur Colpitts amélioré est illustré dans la figure (III.6), où les valeurs des paramètres associés à cet attracteur sont : ε_1=1, ε_2=20, σ_1=1.49, σ_2=0.872, γ=86, α=255/256.

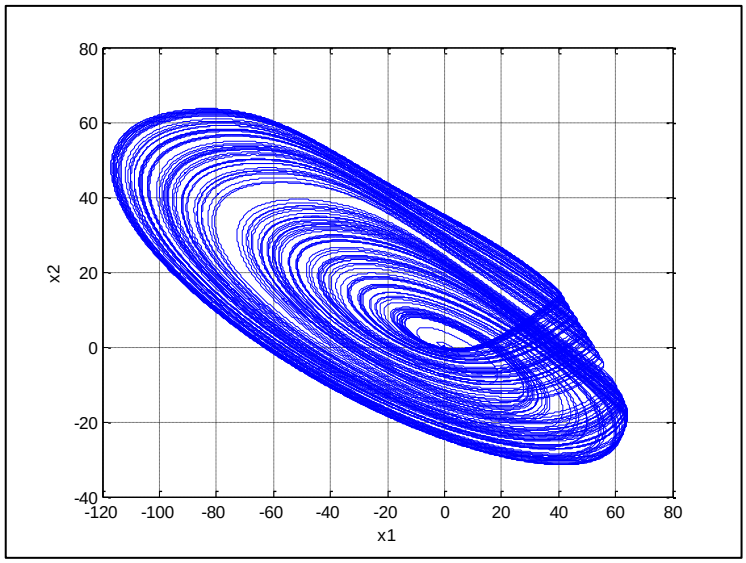


Figure III.6. Attracteur étrange de l'oscillateur Colpitts amélioré (x_1, x_2).

III.5 Oscillateur chaotique étudié

L'oscillateur chaotique étudié est illustré dans la figure (III.7), où il s'agit d'un oscillateur de type Colpitts réaménagé en ajoutant une cellule RLC à sa base, et en utilisant un transistor bipolaire à jonction (BJT) BFG520 avec une fréquence de seuil égale à 9 GHz comme élément actif non linéaire. La cellule RLC est une combinaison parallèle de branches RC et RL, où l'insertion de cette cellule vise d'obtenir un spectre presque plat, et aussi d'avoir plus de variables d'état [65].

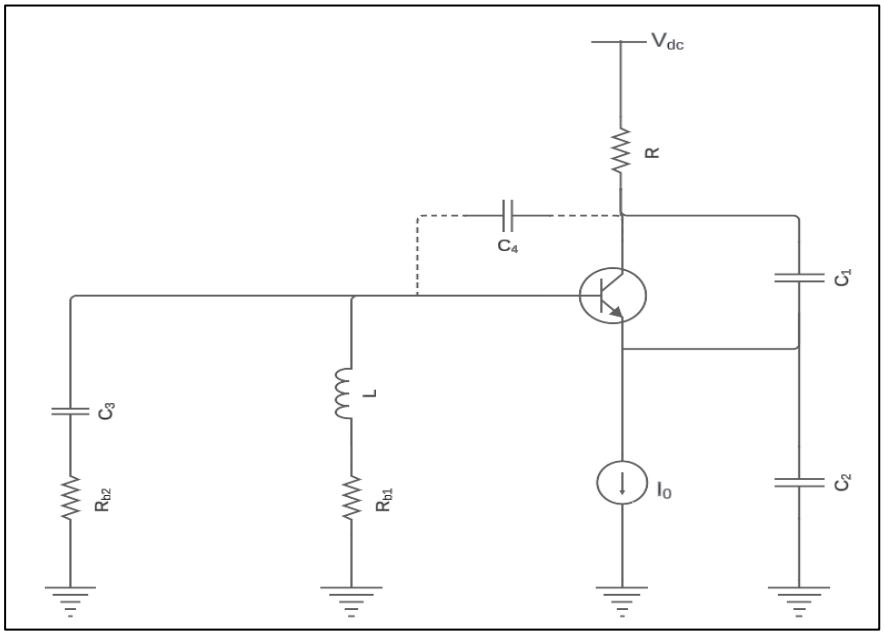


Figure III.7. Circuit de l'oscillateur chaotique étudié.

III.5.1 Modèle mathématique du circuit étudié

Pour qu'on puisse établir le modèle mathématique du circuit de la figure (III.7), il est nécessaire de modéliser le transistor bipolaire Q comme montré dans la figure (III.8), où la relation entre le courant de l'émetteur et la tension de la jonction Base-émetteur s'écrit comme suit [62-63] :

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

I_S est le courant de saturation de la jonction B-E, et V_T la tension thermique (V_T=26 mV pour T=300°K).

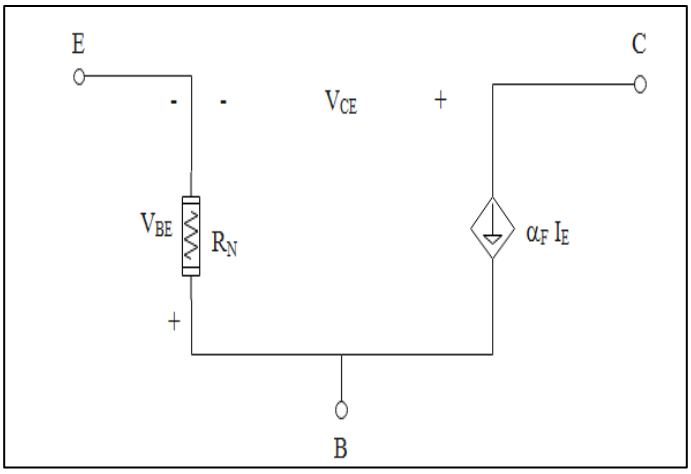


Figure III.8. Modèle de transistor en configuration Base Commune (CB).

Les équations d'états de l'oscillateur étudié sont obtenues après l'application des lois de Kirchhoff sur le circuit de l'oscillateur [65] :

$$\begin{cases} RC_1\dfrac{dV_{C_1}}{dt} = V_{dc} - \left(1 + \dfrac{R}{R_{b_2}}\right)(V_{C_1} + V_{C_2}) + \dfrac{R}{R_{b_2}}(V_{C_4} - V_{C_3}) + R_{I_L} - Rf(V_{C_1}, V_{C_4}) \\ RC_2\dfrac{dV_{C_2}}{dt} = V_{dc} - \left(1 + \dfrac{R}{R_{b_2}}\right)(V_{C_1} + V_{C_2}) + \dfrac{R}{R_{b_2}}(V_{C_4} - V_{C_3}) + R_{I_L} - RI_0 \\ R_{b_2}C_3\dfrac{dV_{C_3}}{dt} = V_{C_1} + V_{C_2} - V_{C_3} + V_{C_4} \\ L\dfrac{dI_L}{dt} = -V_{C_1} - V_{C_2} - V_{C_4} - R_{b_1}I_L \\ C_4\dfrac{dV_{C_4}}{dt} = I_L - \dfrac{1}{R_{b_2}}(V_{C_1} + V_{C_2} - V_{C_3} + V_{C_4}) - (1-\alpha)f(V_{C_1}, V_{C_4}) \end{cases} \quad \text{(III.6)}$$

Où la fonction non linéaire f (V_{C1}, V_{C4}) est exprimée comme suit [65]:

$$f\left(V_{C_1}, V_{C_4}\right) = I_S\left[e^{\frac{V_{C_1}+V_{C_4}}{V_T}} - 1\right] \tag{III.7}$$

V_{ci} représente la tension aux bornes de la capacité C_i, où $\boldsymbol{i} \in \{1,2,3,4\}$, et I_L est le courant qui traverse l'inductance L.

Le point de l'équilibre de système Eq. (III.6) s'écrit comme suit [65] :

$$\begin{cases} I_L^0 = I_0(1-\alpha) \\ V_{C_1}^0 = V_{dc} + V_T Ln\left(\dfrac{I_0+I_s}{I_s}\right) + I_0\left(R_{b_1}(1-\alpha) - \alpha R\right) \\ V_{C_2}^0 = -V_T Ln\left(\dfrac{I_0+I_s}{I_s}\right) - I_0 R_{b_1}(1-\alpha) \\ V_{C_3}^0 = -I_0 R_{b_1}(1-\alpha) \\ V_{C_4}^0 = -V_{dc} - I_0\left(R_{b_1}(1-\alpha) - \alpha R\right) \end{cases} \tag{III.8}$$

Pour obtenir un système des équation normalisé, nous adoptons les nouvelles variables d'état et paramètres suivants [65]:

$$\begin{cases} t = \grave{t}\sqrt{LC}, \quad \rho = \sqrt{\dfrac{L}{C_1}}, \quad \varepsilon_1 = \dfrac{C_1}{C_2}, \quad \varepsilon_2 = \dfrac{C_1}{C_3}, \quad \varepsilon_3 = \dfrac{C_1}{C_4} \\ \sigma_1 = \dfrac{\rho}{R}, \quad \sigma_2 = \dfrac{\rho}{R_{b_2}}, \quad \sigma_3 = \dfrac{R_{b_1}}{\rho}, \quad \gamma = \dfrac{I_0+I_s}{V_T}\sqrt{\dfrac{L}{C_1}}, \quad r = \left(1 + \dfrac{R}{R_{b_2}}\right) \\ x_1 = \dfrac{V_{C_1} - V_{C_1}^0}{V_T}, x_2 = \dfrac{V_{C_2} - V_{C_2}^0}{V_T}, x_3 = \dfrac{V_{C_3} - V_{C_3}^0}{V_T}, x_4 = \dfrac{V_{C_4} - V_{C_4}^0}{V_T} \quad x_5 = \sqrt{\dfrac{L}{c}}\dfrac{I_L - I_L^0}{V_T} \end{cases} \tag{III.9}$$

En conséquence, le système ODE qui décrit la dynamique de l'oscillateur étudié s'écrit comme suit [65] :

$$\begin{cases} \dot{x}_1 = -\sigma_1 r(x_1 + x_2) - \sigma_2 r(x_4 - x_3) + x_5 - \gamma\psi(x_1, x_4) \\ \dot{x}_2 = -\sigma_1\varepsilon_1 r(x_1 + x_2) - \sigma_2\varepsilon_1 r(x_4 - x_3) - \varepsilon_1 x_5 \\ \dot{x}_3 = \sigma_2\varepsilon_3(x_1 + x_2 - x_3 + x_4) \\ \dot{x}_4 = -\sigma_2\varepsilon_3(x_1 + x_2) - \sigma_2\varepsilon_3(x_4 - x_3) - \varepsilon_3 x_5 - \varepsilon_3(1-\alpha)\gamma\Psi(x_1, x_4) \\ \dot{x}_5 = -x_1 - x_2 - x_4 - \sigma_3 x_5 \end{cases} \quad \text{(III.10)}$$

Ici, $\dot{x}_k$: $k \in \{1,2,3,4,5\}$, représente la dérivée par rapport au temps normalisé, et $\Psi(x_1,x_4)$ défini par :

$$\Psi(x_1, x_4) = \{e^{x_1+x_4} - 1\} \quad \text{(III.11)}$$

III.5.3 Diagramme de bifurcation

Afin de tracer le diagramme de bifurcation de système étudié, nous devons résoudre le modèle mathématique Eq. (III.10) utilisant la méthode de Runge-Kutta d'ordre quatre, qui est une méthode spécialisée dans la résolution des systèmes ODE. L'objectif derrière le traçage de ce diagramme est d'identifier les différents comportements possibles de ce système et de déterminer l'intervalle où le système étudie se comporte chaotique.

Le diagramme de bifurcation est illustré dans la figure (III.9), où le paramètre de bifurcation γ varie de 0 jusqu'à 80. Les valeurs des autres paramètres sont fixées comme suit : $\mathcal{E}_1=0.88$, $\mathcal{E}_2=6.4$, $\mathcal{E}_3=6.4$, $\sigma_1=0.99$, $\sigma_2=0.0878$, $\sigma_3=0.033$, $r=1.094$, $\alpha=255/256$.

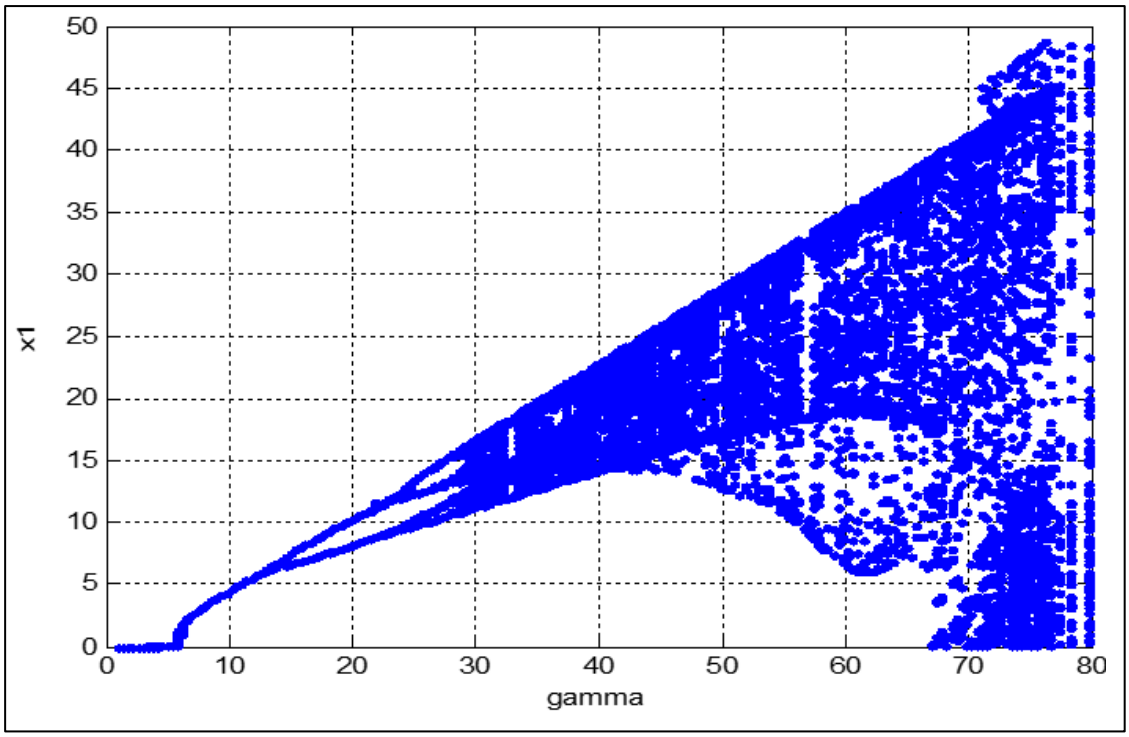


Figure III.9. Diagramme de bifurcation de système étudié.

A partir de diagramme de bifurcation obtenu, nous remarquons que le système étudié passe par plusieurs comportements différents avant qu'il arrive à son comportement chaotique. Dans l'intervalle où la valeur de γ est inférieure à 7, l'amplitude de x_1 est 0, ce qui veut dire qu'il n'y a pas des oscillations. Dans l'intervalle où la valeur de γ est entre 7 et 12, le système se comporte périodique (une seule période). Dans l'intervalle où la valeur de γ est entre 12 et 29, le comportement de système est quasi-périodique avec nombre bien précis des périodes. Pour la valeur de γ supérieure à 29, le comportement de système est chaotique avec un nombre infini des périodes, ce comportement est le comportement désiré dans notre travail.

III.5.4 Espaces des phases

Pour une meilleure identification de comportement chaotique de système étudié, nous allons tracer les réponses temporelles et les espaces des phases, ce comportement est obtenu en fixant la valeur de γ à 60. Les résultats de simulation sont illustrés dans les figures (III.10) et (III.11).

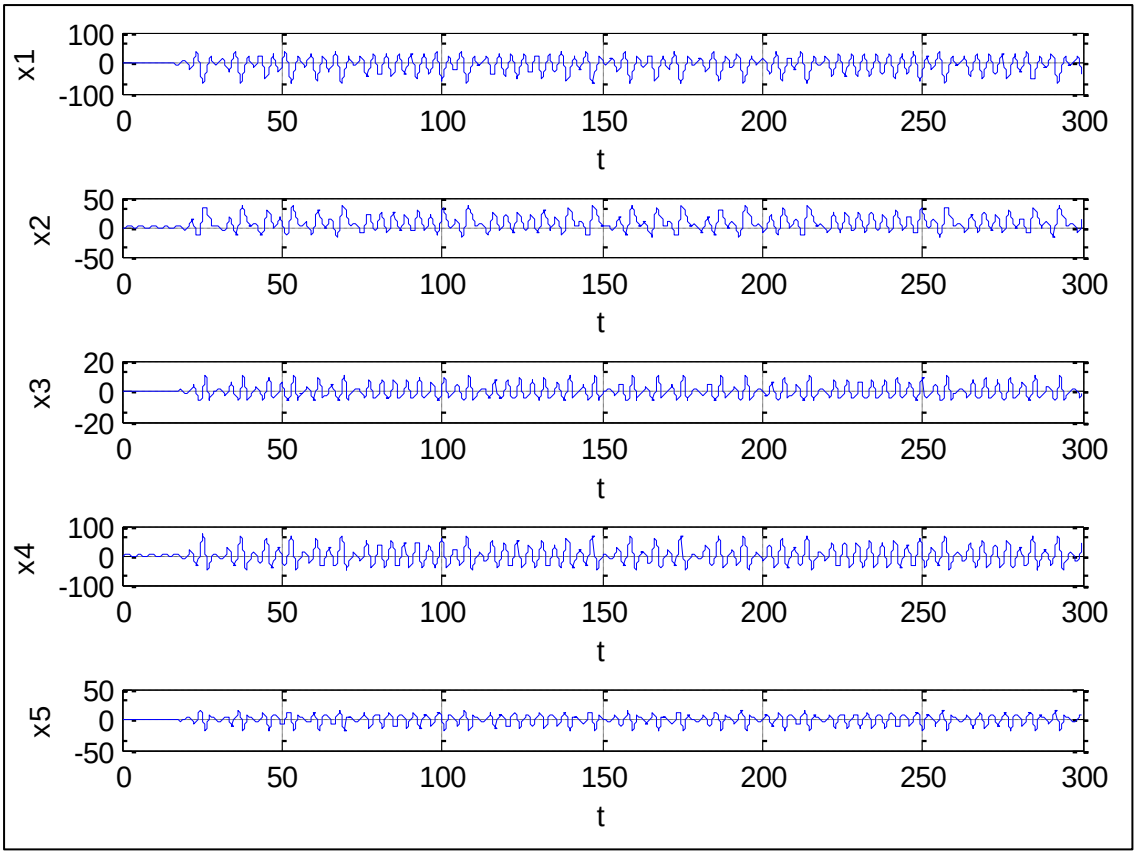


Figure III.10. Réponses temporelles de système étudié pour γ=60.

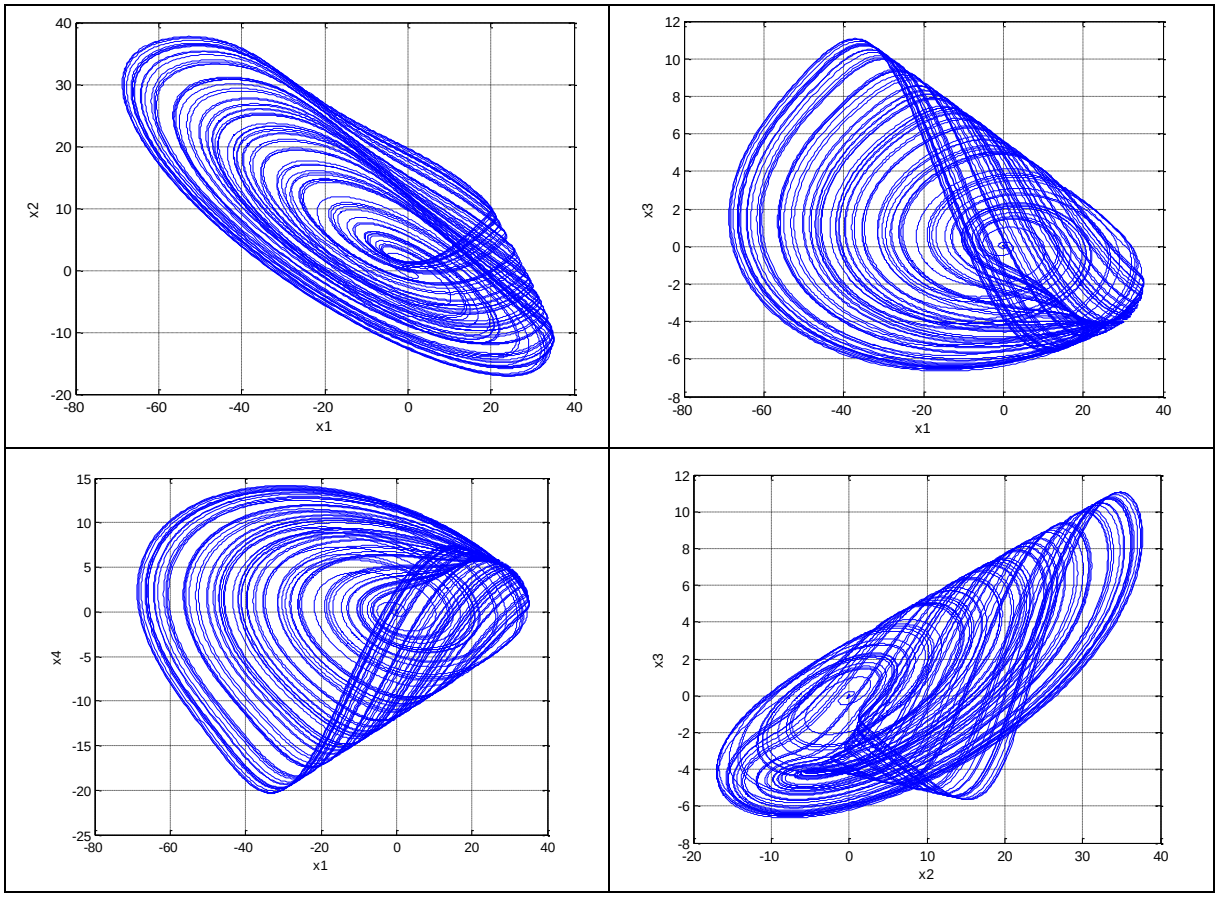


Figure III.11. Espaces des phases chaotiques obtenus sous Matlab pour γ=60.

III.5.4 Simulation sous ADS

Le circuit de l'oscillateur étudié est simulé sous ADS (Advanced Design System) pour confirmer les résultats de la première simulation et pour étudier les caractéristiques spectrales de cet oscillateur chaotique. Le circuit simulé est illustré dans la figure (III.12), où les valeurs des composantes utilisés dans cette simulation sont mentionnés dans le tableau (III.1). Dans cette simulation, nous utilisons le modèle Pspice de transistor bipolaire BFG 520 illustré dans la figure (III.13). Ce modèle complexe est utilisé Afin de modéliser le comportement réel du ce transistor aux hautes [66].

Tableau III.1. Données des éléments électroniques utilisés dans la simulation [65].

Composante	R_b	R_1	R_2=R_3	L	C_2	C_3	V_{dc}	V_{bias}
Valeur	10Ω	94Ω	1.0kΩ	49.4nH	2.6pF	1.0pF	10V	-9.6V

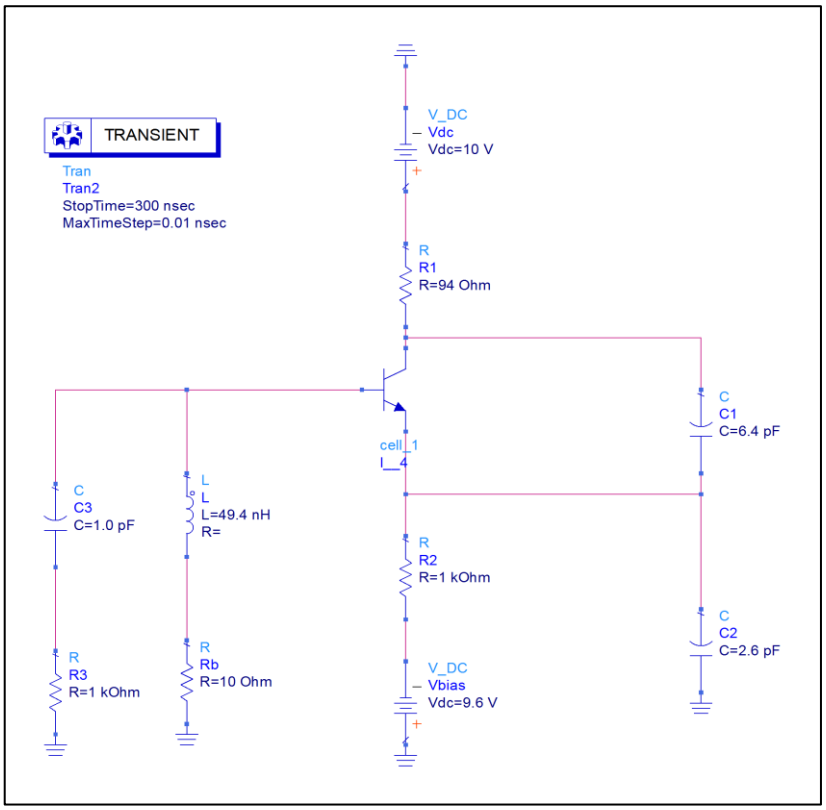


Figure III.12. Circuit de l'oscillateur étudié sous ADS.

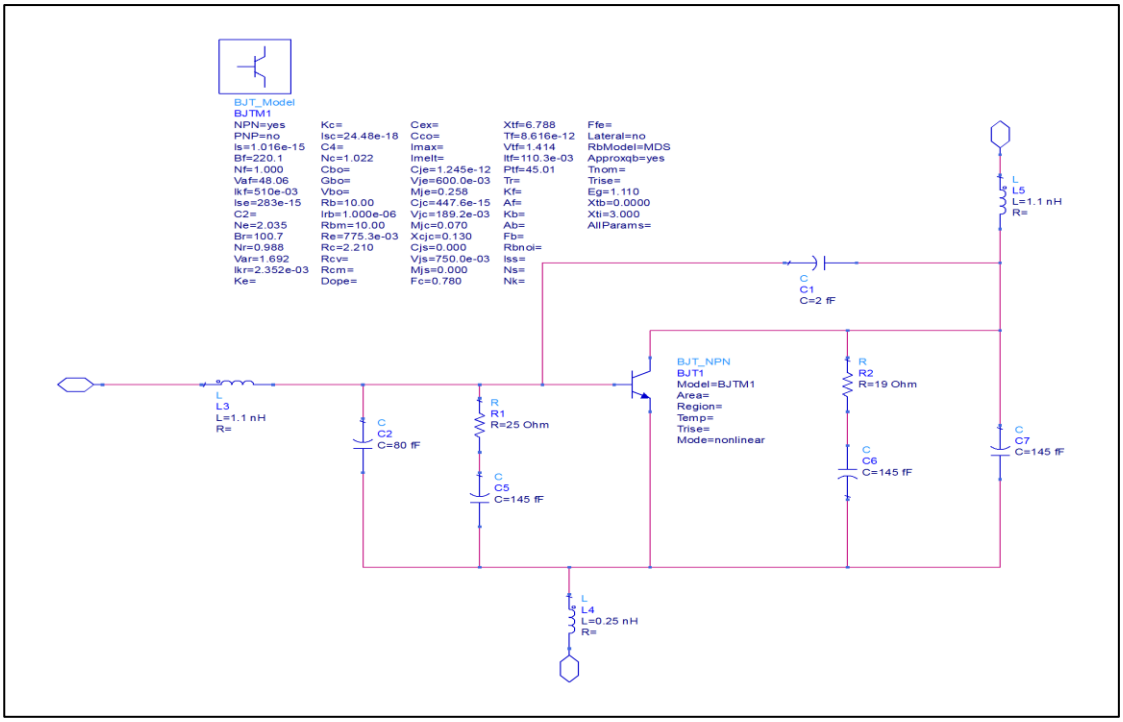
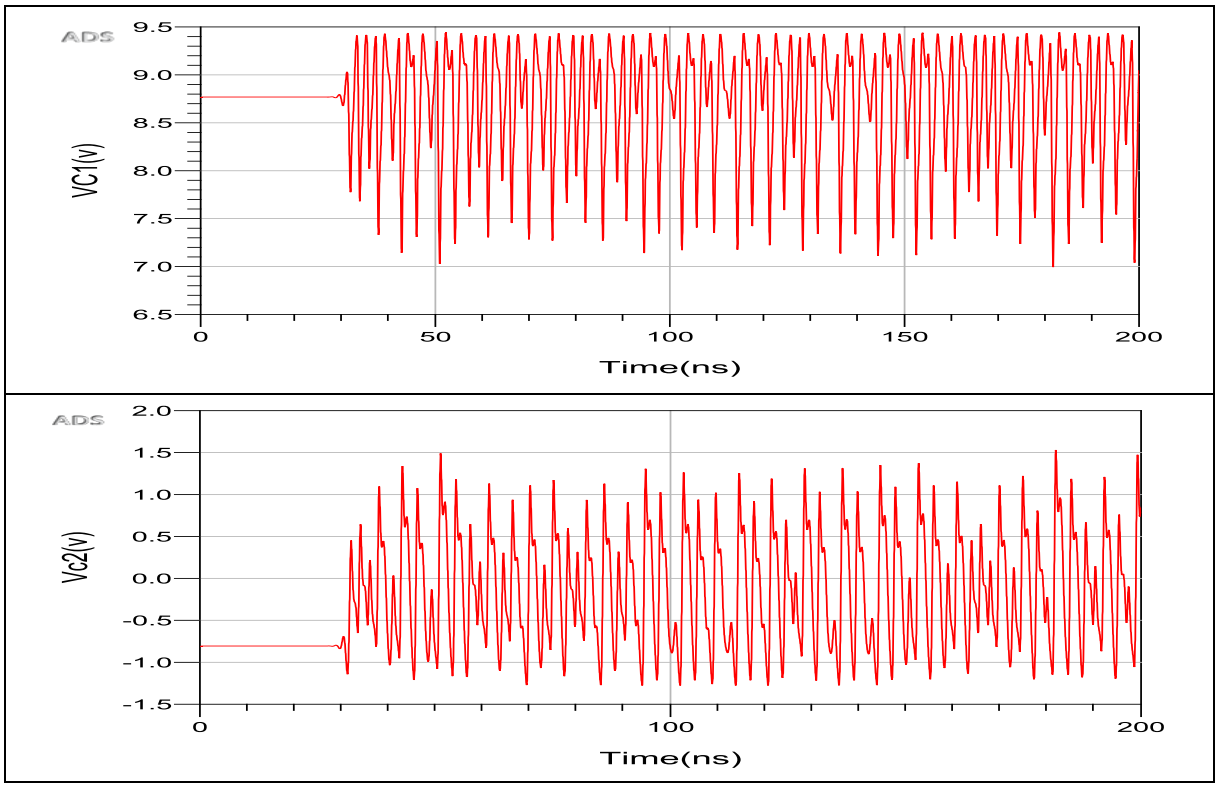


Figure III.13. Modèle Pspice de transistor bipolaire BFG520.

III.5.5 Résultats de simulation sous ADS

Les réponses temporelles et les espaces des phases obtenus après la simulation de circuit de l'oscillateur sous ADS sont montrés dans la figure (III.14) et la figure (III.15).



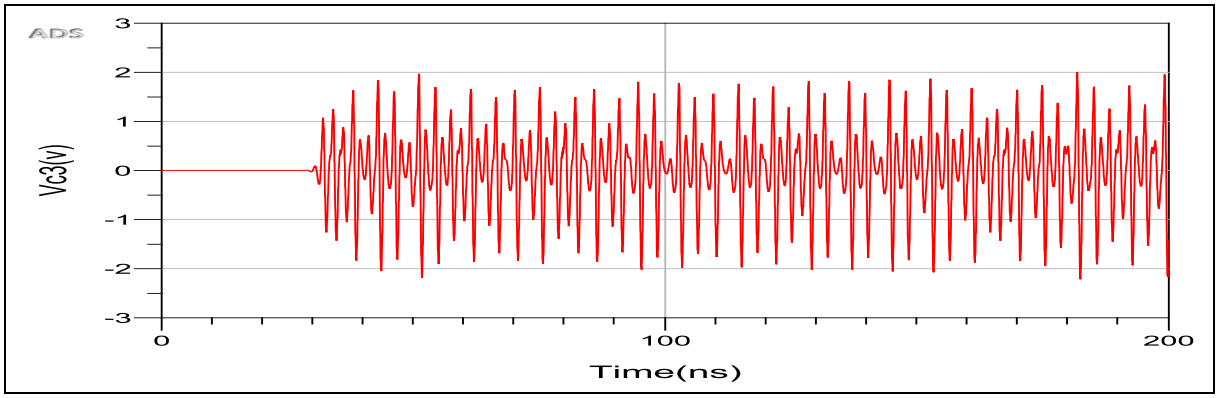


Figure III.14. Réponses temporelles chaotiques obtenues sous ADS : $V_{C1}(t)$, $V_{C2}(t)$, $V_{c3}(t)$.

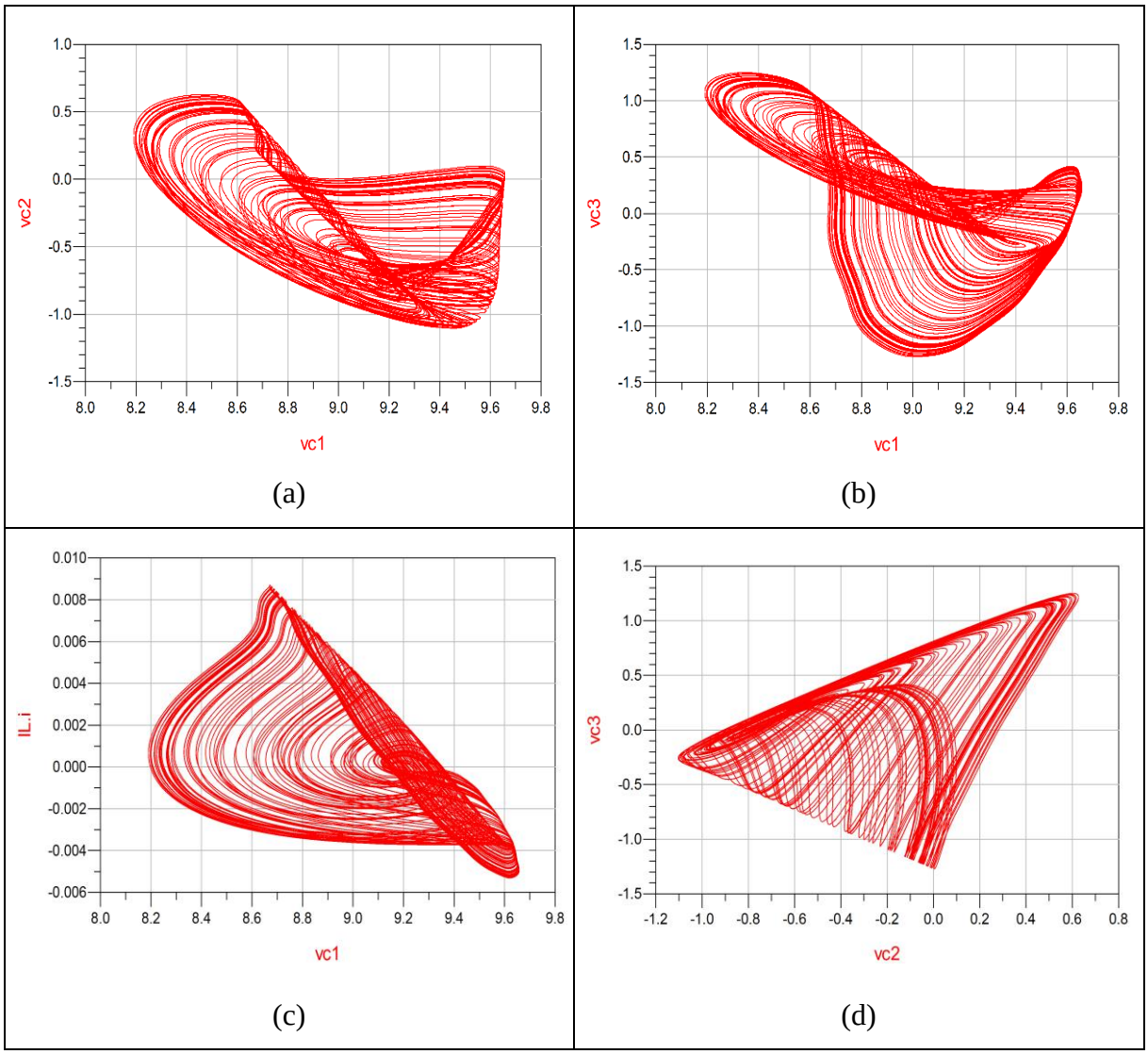


Figure III.15. Espaces des phases chaotiques obtenus sous ADS : (a) (V_{C1}, V_{C2}), (b) (V_{C1}, V_{C3}), (c) (V_{C1}, I_L), (d) (V_{C2}, V_{C3}).

En comparant les résultats des figures (III.11) et (III.15), il nous apparaît clairement qu'il existe une grande similitude entre eux, ce qui nous permet de valider le modèle mathématique établi dans la première partie de cette étude.

Afin d'étudier les caractéristiques fréquentielles de cet oscillateur, nous traçons sous ADS les réponses spectrales de V_{C1}, V_{C2}, et V_{C3}, ces réponses sont illustrées dans la figure (III.16).

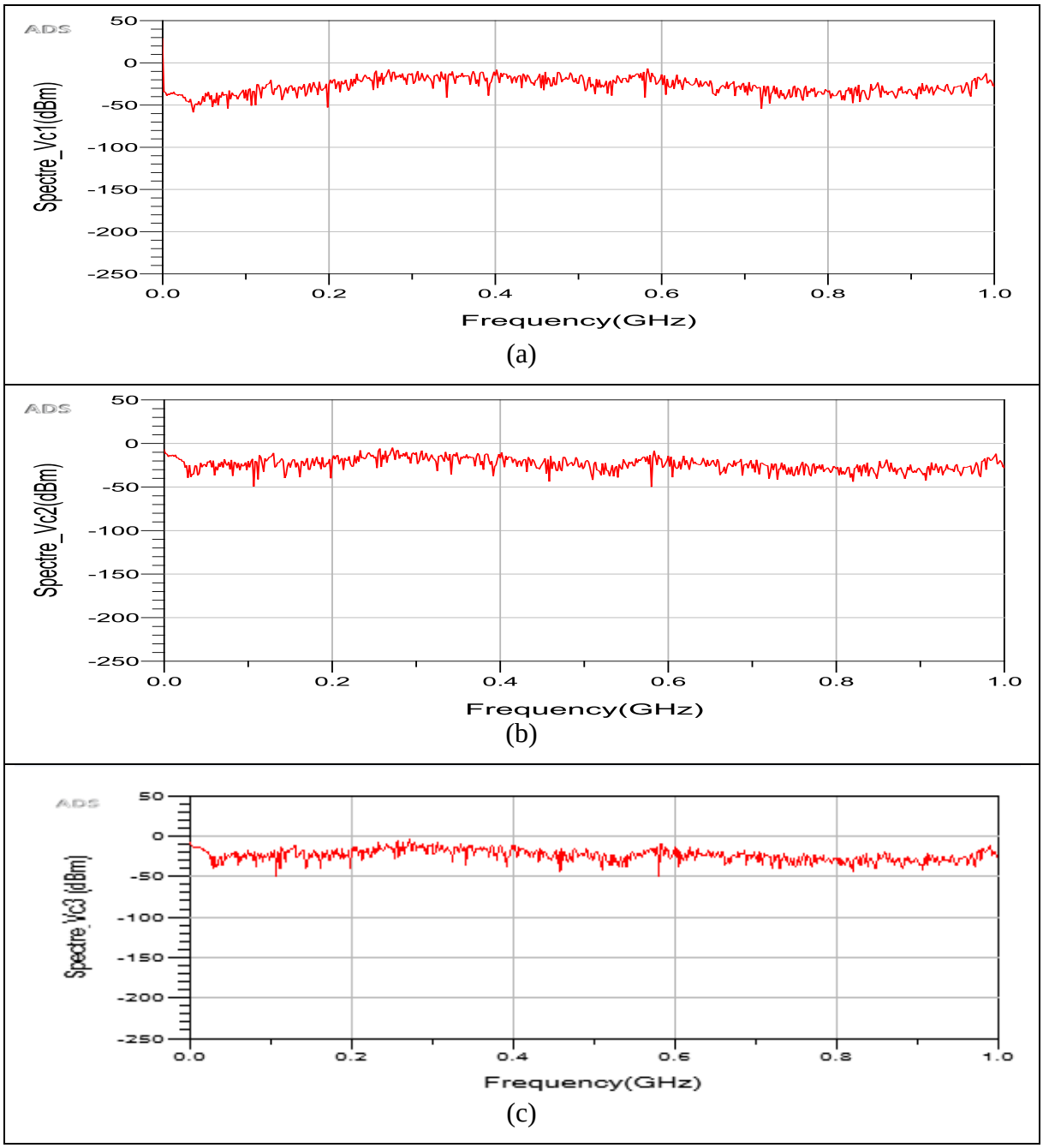


Figure III.16. Réponses spectrales de : (a) V_{C1} ; (b) V_{C2} ; (c) V_{C3}.

Nous remarquons que les spectres de V_{C1}, V_{C2}, et V_{C3} sont presque plat (lisses) dans la plage de fréquences allant jusqu'à 1GHz. Cette caractéristique spectrale rend l'oscillateur adapté à des applications de communication sans fil telles que la communication à spectre étalé basée sur le chaos, la communication chaotique directe, etc.

III.6 Conclusion

Dans ce chapitre, nous avons étudié un nouveau circuit chaotique à quatre dimensions basées sur la version améliorée de l'oscillateur Colpitts. Le modèle mathématique de cet oscillateur est étudié sous Matlab, où nous avons tracé le diagramme de bifurcation, les réponses temporelles chaotiques, et les espaces des phases chaotiques. Cette étude a été validée par une autre simulation sous le simulateur ADS. Les réponses spectrales obtenues montrent que le circuit peut générer des oscillations jusqu'à 1GHz avec une enveloppe spectrale presque plate.

Conclusion générale

Conclusion générale

Ce travail vise à étudier un nouveau générateur chaotique avec une enveloppe spectrale plate pour les systèmes de communications sécurisées par chaos. Pour atteindre l'objectif de cette étude on a divisé notre mémoire en trois chapitres :

Dans le premier chapitre, nous avons détaillé les notions fondamentales des systèmes dynamiques chaotiques, en mettant l'accent sur les systèmes chaotiques non linéaires. Nous avons expliqué les concepts essentiels de la théorie du chaos, tels que la sensibilité aux conditions initiales, le déterminisme et les attracteurs étranges. Ces propriétés rendent les systèmes chaotiques imprévisibles à long terme, ce qui les rend particulièrement adaptés pour sécuriser les transmissions. Nous avons également introduit des outils d'analyse, notamment les exposants de Lyapunov et les diagrammes de bifurcation, pour étudier ces systèmes.

Dans le deuxième chapitre, nous avons défini la cryptographie chaotique, puis nous avons détaillé les techniques utilisées pour crypter un message en utilisant ces systèmes, telles que la cryptographie chaotique par addition, la cryptographie chaotique par modulation et la cryptographie chaotique par commutation. La deuxième partie de ce chapitre est consacrée aux méthodes utilisées pour synchroniser les systèmes chaotiques, où nous avons cité : la synchronisation par décomposition de système, la synchronisation projective, la synchronisation par boucle fermée et la synchronisation par des observateurs.

Le troisième chapitre est consacré à l'étude détaillée d'un nouveau générateur chaotique. Nous avons d'abord commencé par la présentation et l'analyse des différents générateurs chaotiques trouvés dans la littérature. Ensuite, nous avons étudié un nouvel oscillateur chaotique basé sur l'oscillateur de Colpitts, en établissant un système d'équations différentielles décrivant ses comportements dynamiques. Ce système inclut un terme non linéaire pour assurer l'émergence du chaos. En utilisant la méthode Runge-Kutta d'ordre 4 sous Matlab, nous avons résolu ce modèle pour tracer les réponses temporelles et les espaces de phases chaotiques. Par la suite, nous avons utilisé ADS pour confirmer les résultats mathématiques obtenus sous Matlab, ainsi que pour tracer le spectre de cet oscillateur. Le spectre résultant de cette simulation indique que l'oscillateur étudié peut osciller jusqu'à 1 GHz avec un spectre presque plat.

Ce travail peut être amélioré dans l'avenir par :

- La proposition d'une méthode convenable pour synchroniser ce générateur chaotique.
- La réalisation pratique de cet oscillateur.

Bibliographie

Bibliographie

[1]. Sprott, J. C. (2000). Simple chaotic systems and circuits. *American Journal of Physics*, *68*(8), 758-763.

[2]. Luenberger, D. G. (1979). *Dynamic Systems* (p. 0007). J. Wiley Sons.

[3]. Close, C. M., Frederick, D. K., & Newell, J. C. (2001). *Modeling and analysis of dynamic systems*. John Wiley & Sons.

[4]. Thelen, E., & Smith, L. B. (2007). Dynamic systems theories. *Handbook of child psychology*, *1*.

[5]. Galor, O. (2007). *Discrete dynamical systems*. Springer Science & Business Media.

[6]. Robinson, R. C. (2012). *An introduction to dynamical systems: continuous and discrete* (Vol. 19). American Mathematical Soc.

[7]. Chernous' ko, F. L., Ananievski, I. M., & Reshmin, S. A. (2008). *Control of nonlinear dynamical systems: methods and applications*. Springer Science & Business Media.

[8]. McCauley, J. L. (1993). *Chaos, dynamics, and fractals: an algorithmic approach to deterministic chaos* (Vol. 2). Cambridge University Press.

[9]. Hobbs, J. (1991). Chaos and indeterminism. *Canadian Journal of Philosophy*, *21*(2), 141-164.

[10]. Galatolo, S. (2003). Complexity, initial condition sensitivity, dimension and weak chaos in dynamical systems. *Nonlinearity*, *16*(4), 1219.

[11]. Tsallis, C., & Borges, E. P. (2024). Nonlinear dynamical systems: Time reversibility versus sensitivity to the initial conditions. *Chaos, Solitons & Fractals*, *182*, 114743.

[12]. Alligood, K. T., Sauer, T. D., Yorke, J. A., & Chillingworth, D. (1998). Chaos: an introduction to dynamical systems. *SIAM Review*, *40*(3), 732-732.

[13]. Hale, J. K. (1968). *Dynamical systems and stability* (No. NASA-CR-95868).

[14]. Hirsch, M. W. (1984). The dynamical systems approach to differential equations. *Bulletin of the American mathematical society*, *11*(1), 1-64.

[15]. Auslander, J., Bhatia, N. P., & Seibert, P. (1964). *Attractors in dynamical systems* (No. NASA-CR-59858).

[16]. Dudkowski, D., Jafari, S., Kapitaniak, T., Kuznetsov, N. V., Leonov, G. A., & Prasad, A. (2016). Hidden attractors in dynamical systems. *Physics Reports*, *637*, 1-50.

[17]. Goldstein, J. (2011). Attractors and nonlinear dynamical systems. *Deeper Learning*, 1-17.

[18]. Rössler, O. E. (1977, May). Continuous chaos. In *Synergetics: A Workshop Proceedings of the International Workshop on Synergetics at Schloss Elmau, Bavaria, May 2–7, 1977* (pp. 184-197). Berlin, Heidelberg : Springer Berlin Heidelberg.

[19]. Rössler, O. E. (1976). Chaotic behavior in simple reaction systems. *Zeitschrift für Naturforschung A*, *31*(3-4), 259-264.

[20]. Lenz, H., & Obradovic, D. (1997). Robust control of the chaotic Lorenz system. *International Journal of Bifurcation and Chaos*, *7*(12), 2847-2854.

[21]. Yang, T., Yang, L. B., & Yang, C. M. (1997). Impulsive control of Lorenz system. *Physica D: Nonlinear Phenomena*, *110*(1-2), 18-24.

[22]. Keesling, J. (1986). Hausdorff dimension. In *Topology Proc* (Vol. 11, No. 2, pp. 349-383).

[23]. Sandri, M. (1996). Numerical calculation of Lyapunov exponents. *Mathematica Journal*, *6*(3), 78-84.

[24]. Abarbanel, H. D., Brown, R., & Kennel, M. B. (1991). Lyapunov exponents in chaotic systems: their importance and their evaluation using observed data. *International Journal of Modern Physics B*, *5*(09), 1347-1375.

[25]. Wolf, A. (1986). Quantifying chaos with Lyapunov exponents. *Chaos*, *16*, 285-317.

[26]. Holmes, P. (1990). Poincaré, celestial mechanics, dynamical-systems theory and "chaos". *Physics Reports*, *193*(3), 137-163.

[27]. Chen, Y., & Leung, A. Y. (2012). *Bifurcation and chaos in engineering*. Springer Science & Business Media.

[28]. Chen, G., & Moiola, J. L. (1994). An overview of bifurcation, chaos and nonlinear dynamics in control systems. *Journal of the Franklin Institute*, *331*(6), 819-858.

[29]. Wang, H. O., & Abed, E. H. (1995). Bifurcation control of a chaotic system. *Automatica*, *31*(9), 1213-1226.

[30]. Khmou, Y. (2017). A case study in bifurcation theory. *International Journal of Modern Physics C*, *28*(08), 1750104.

[31]. Chua, L. O., Wu, C. W., Huang, A., & Zhong, G. Q. (1993). A universal circuit for studying and generating chaos. I. Routes to chaos. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, *40*(10), 732-744.

[32]. Libchaber, A., Fauve, S., & Laroche, C. (1983). Two-parameter study of the routes to chaos. *Physica D : Nonlinear Phenomena*, *7*(1-3), 73-84.

[33]. Debraize, B. (2008). *Méthodes de cryptanalyse pour les schémas de chiffrement symétrique* (Doctoral dissertation, Versailles-St Quentin en Yvelines).

[34]. KHEBCHI, A. (2022). *An efficient and robust image encryption scheme tailored for modern applications requirements* (Doctoral dissertation).

[35]. Pointcheval, D. (2002). Le chiffrement asymétrique et la sécurité prouvée. *Habilitation à diriger des recherches, Université Paris VII*.

[36]. Huynh, P. (2020). *Analyse et conception d'algorithmes de chiffrement légers* (Doctoral dissertation, Université de Lorraine).

[37]. Kocarev, L. (2001). Chaos-based cryptography: a brief overview. *IEEE Circuits and Systems Magazine*, *1*(3), 6-21.

[38]. Carmen, P. L., & Ricardo, L. R. (2012, March). Notions of chaotic cryptography: sketch of a chaos-based cryptosystem. In *Applied cryptography and network security* (pp. 267-294). London : IntechOpen.

[39]. Kharel, R. (2011). *Design and implementation of secure chaotic communication systems* (Doctoral dissertation, Northumbria University).

[40]. Blackledge, J., & Ptitsyn, N. (2010). Encryption using deterministic chaos.

[41]. Chien, T. I., & Liao, T. L. (2005). Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization. *Chaos, Solitons & Fractals*, *24*(1), 241-255.

[42]. Corrochano, E. B., Mao, Y., & Chen, G. (2005). Chaos-based image encryption. *Handbook of Geometric Computing: Applications in Pattern Recognition, Computer Vision, Neuralcomputing, and Robotics*, 231-265.

[43]. Ranjan, R., Mukherjee, A., Rai, P., & Ahmad, K. (2019). Asymmetric Cryptography. In *Emerging Security Algorithms and Techniques* (pp. 119-137). Chapman and Hall/CRC.

[44]. Carroll, T. L., & Pecora, L. M. (1995). Synchronizing chaotic circuits. In *Nonlinear dynamics in circuits* (pp. 215-248).

[45]. Pecora, L. M., Carroll, T. L., Johnson, G. A., Mar, D. J., & Heagy, J. F. (1997). Fundamentals of synchronization in chaotic systems, concepts, and applications. *Chaos: An Interdisciplinary Journal of Nonlinear Science*, *7*(4), 520-543.

[46]. Kenouni, H., & Kemih, K. E. (2016). *Synchronisation des systèmes hyper-chaotiques à retard sous l'effet des perturbations : Application au chiffrement d'information* (Doctoral dissertation, Université de Jijel).

[47]. Chee, C. Y., & Xu, D. (2005). Secure digital communication using controlled projective synchronisation of chaos. *Chaos, Solitons & Fractals*, *23*(3), 1063-1070.

[48]. Vaidyanathan, S. (2014). Generalised projective synchronisation of novel 3-D chaotic systems with an exponential non-linearity via active and adaptive control. *International Journal of Modelling, Identification and Control*, *22*(3), 207-217.

[49]. Morgül, Ö., & Solak, E. (1996). Observer based synchronization of chaotic systems. *Physical Review E*, *54*(5), 4803.

[50]. Morgül, Ö., & Solak, E. (1996). Observer based synchronization of chaotic systems. *Physical Review E*, *54*(5), 4803.

[51]. Dimassi, H., & Loría, A. (2010). Adaptive unknown-input observers-based synchronization of chaotic systems for telecommunication. *IEEE Transactions on Circuits and Systems I : Regular Papers*, *58*(4), 800-812.

[52]. Chua, L. O. (1994). Chua's circuit 10 years later. *International Journal of Circuit Theory and Applications*, *22*(4), 279-305.

[53]. Kennedy, M. P. (1994). Chaos in the Colpitts oscillator. *IEEE Transactions on circuits and systems I: Fundamental Theory and Applications*, *41*(11), 771-774.

[54]. Tekam, R. B. W., Kengne, J., & Kenmoe, G. D. (2019). High frequency Colpitts' oscillator: A simple configuration for chaos generation. *Chaos, Solitons & Fractals*, *126*, 351-360.

[55]. Shi, Z. G., & Ran, L. X. (2006). Microwave chaotic Colpitts oscillator: design, implementation and applications. *Journal of Electromagnetic Waves and Applications*, *20*(10), 1335-1349.

[56]. Mykolaitis, G., Tamaševičius, A., Bumelienė, S., Baziliauskas, A., & Lindberg, E. J. E. I. E. (2004). Two-stage chaotic Colpitts oscillator for the UHF range. *Elektronika Ir Elektrotechnika*, *53*(4).

[57]. Li, J. X., Wang, Y. C., & Ma, F. C. (2013). Experimental demonstration of 1.5 GHz chaos generation using an improved Colpitts oscillator. *Nonlinear dynamics*, *72*, 575-580.

[58]. Bendaoud, M., Kamèche, S., & Ouslimani, A. (2023). Modeling and Analysis of a Novel Chaotic Oscillator up to 7.5 GHz. *Journal of Communications Technology and Electronics*, *68*(8), 903-909.

[59]. Hu, S., Yu, S., Hu, Y., Wang, Z., & Zhou, B. (2018, August). A novel 1–6 GHz chaotic signal oscillator for broadband communication systems. In *2018 Progress in Electromagnetics Research Symposium (PIERS-Toyama)* (pp. 1550-1554). IEEE.

[60]. Bendaoud, M., Kamèche, S., & Ouslimani, A. (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 (ICAECCS)* (pp. 1-4). IEEE.

[61]. Chua, L. O. (1994). Chua's circuit: An overview ten years later. *Journal of Circuits, Systems, and Computers*, *4*(02), 117-159.

[62]. De Feo, O., Maggio, G. M., & Kennedy, M. P. (2000). The Colpitts oscillator: Families of periodic solutions and their bifurcations. *International journal of bifurcation and chaos*, *10*(05), 935-958.

[63]. De Feo, O., & Maggio, G. M. (2003). Bifurcations in the Colpitts oscillator: from theory to practice. *International journal of bifurcation and chaos*, *13*(10), 2917-2934.

[64]. Tamaševičius, A., Mykolaitis, G., Bumelienė, S., Baziliauskas, A., Krivickas, R., & Lindberg, E. (2006). Chaotic Colpitts oscillator for the ultrahigh frequency range. *Nonlinear Dynamics*, *44*, 159-165.

[65]. Moundher, M., Hichem, B., Djamel, T., & Said, S. (2019, November). Novel four-dimensional chaotic oscillator for sub-1GHz chaos-based communication systems. In *2019 6th International Conference on Image and Signal Processing and their Applications (ISPA)* (pp. 1-5). IEEE.

[66]. NXP Semiconductors, NPN 9 GHz wideband transistor, BFG520; BFG520/X, BFG/XR, Product datasheet, 2007.