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

جـــــــــــــامعة 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 :

BENDAOUD Mouhamed

Sujet

Etude et Conception d'un système chaotique basé sur l'oscillateur Colpitts pour les communications sécurisées

Soutenu publiquement, le **01/07/ 2019** , devant le jury composé de :

Mr M. FEHAM	Professeur	Univ. Tlemcen	Président
Mr S. KAMECHE	Professeur	Univ. Tlemcen	Directeur de mémoire
Mr A. OUSLIMANI	Professeur	ENSEA. Cergy Pontoise- Paris	Co-Directeur de mémoire
Mr A. ABDELMALEK	Maître de Conférences	Univ. Tlemcen	Examinateur

Dèdicaces

Je dédie ce travail :

A ma mère et mon père,

Aucune dédicace ne saurait être assez éloquente pour exprimer ce que vous méritez, pour tous les sacrifices que vous n'avez cessé de me donner depuis ma naissance, durant mon enfance et même à l'âge adulte.

Je vous dédié ce travail en témoignage de mon profond amour. Puisse Dieu, le tout puissant, vous préservez et vous accordez santé, longue vie et bonheur.

A ma grande mère,

Zajia. Tu présentes pour moi le symbole de la bonté et la source de tendresse.

A la mémoire de mes grands-pères Mohammed et Elkhouane et ma grande mère Khadidja.

A mes beaux-frères,

Oussama, Aness, Yacine et Saleh. Je vous remercie infiniment pour votre aide ainsi que vos encouragements et votre fidélité.

A toute ma famille,

Ma belle-sœur Leila et mes oncles Khaled, Ismail, Nacer, Amara, Souad, Fouzia et Saliha. Je vous dédié ce travail avec tous mes vœux de bonheur et de santé.

A tous mes Amis(es),

Zaki Azizi et tous les sousta « mes frères », Zaki dahel et tous les Sanafir, a toute l'équipe de Jardin, Younes et tous l'équipe de rue 19 mars, Tarik et tous les amis de rue el kbir, ...

BENDAOUD Mohammed...

Remerciements

Je remercie tout d'abord, Allah le tout puissant qui m'a donné la force et le courage afin de parvenir à élaborer ce modeste travail.

J'exprime du profond de mon cœur les plus sincères remerciements à mon encadreur Monsieur S.KAMECHE Professeur à l'université de Tlemcen ainsi que mon Co-encadreur Monsieur A.OUSLIMANI Professeur à l'ENSEA de Cergy Pontoise-Paris, pour m'avoir proposé ce sujet qui m'a permis de m'initier à la recherche scientifique, pour leurs aides et les idées qui m'ont facilitées de nombreuses difficultés tout au long de mon travail, pour leurs encouragements qui m'ont permis de réaliser ce mémoire dans d'excellentes conditions de travail.

J'exprime ma gratitude à Monsieur M. FEHAM Professeur à l'université de Tlemcen, pour l'honneur qu'il me fait en présidant le jury de mon mémoire, ainsi qu'à Monsieur A. ABDELMALEK Maitre de conférences à l'université de Tlemcen d'avoir examiné mon travail.

Je tiens à remercier mes parents de m'avoir soutenu, et de m'avoir encouragé pendant de longues années, je ne serais jamais assez reconnaissant envers mes parents qui ont toujours tout mis en œuvre pour qu'on s'épanouisse dans tous ce qu'on entreprend.

Enfin, j'adresse mes respectueux remerciements à tous mes enseignants et toute personne qui m'ont aidés de près ou de loin durant mon travail et en particulier tous mes collègues de la promotion ST 2018/2019.

Résumé

Nous avons traité dans ce mémoire les systèmes chaotiques qui sont des systèmes caractérisés par le déterminisme, la non linéarité et une extrême sensibilité aux conditions initiales, ainsi que des outils disponibles pour faciliter l'étude de ces systèmes comme les exposants de Lyapunov, l'espace des phases et le diagramme de bifurcation, ce dernier nous montre les différents comportements possibles d'un système dynamique passant de comportement périodique jusqu'à le comportement chaotique. L'étude des systèmes chaotiques est destinée à leur utilisation pour sécurisation des transmissions, c'est pour cette raison nous avons expliqué les objectifs des crypto-systèmes et les différentes techniques de cryptographie chaotiques.

L'objectif principal de ce mémoire est la conception d'un générateur chaotique destiné aux transmissions sécurisées, nous avons donc choisi l'oscillateur Colpitts, pour cette tache ce choix peut être jugé par les avantages offerts par cet oscillateur, l'un de ces avantages c'est la simplicité de sa structure. Nous avons expliqué le principe de fonctionnement et déterminé la condition et la fréquence d'oscillation de cet oscillateur et aussi nous avons écrit et développé le modèle mathématique de l'oscillateur Colpitts en étudiant ses différents comportements par la variation de ses paramètres, cette étude est mise en évidence sous le simulateur MATLAB où nous avons calculé les exposants de Lyapunov qui justifient le comportement hyper chaotique pour certaines valeurs des paramètres, tracé les réponses temporelles pour les différents comportements et le diagramme de bifurcation de l'oscillateur Colpitts.

Mots clés : *système chaotique, exposant de Lyapunov, bifurcation, attracteur étrange, transmission sécurisée, cryptographie, l'oscillateur Colpitts, MATLAB*.

Table des matières

Chapitre II : Transmission Chaotique

Chapitre III : Conception d'un générateur chaotique

Sigles et abréviations

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

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

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

$\boldsymbol{Arg(A)}$ **:** l'argument de nombre complexe A.

$\boldsymbol{|A|}$ **:** le module de nombre complexe A.

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

$\boldsymbol{det(A)}$ **:** déterminant de la matrice A.

$\boldsymbol{I_{n\times n}}$ **:** matrice identité de dimension n.

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

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

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

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

FET : Field **E**ffect **T**ransistor.

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

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

Liste des Figures

Chapitre I

Chapitre II

Chapitre III

Liste des Tableaux

Introduction Générale

Dans les dernières années, le monde a été témoin d'un énorme développement dans les technologies de la communication en termes de qualité et quantité des services fournis comme l'augmentation de débit qui est devenu très élevé, la possibilité de transférer tous les contenus multimédias avec une haute définition et aussi le volume des moyens utilisés qui sont miniaturisées et sont devenus à la portée de tous. Ce développement comme il a beaucoup des avantages, il a posé un problème de sécurité (confidentialité, authenticité et intégrité), donc il est devenu indispensable de protéger les échanges des informations à travers les canaux publics de danger de piratage et d'exploitation malveillante. Et pour cet objectif on trouve les techniques de cryptographie qui ont le but de nous permet à envoyer un message à nos correspondants en toute sécurité.

La cryptographie, composée de deux mots grecs *kryptos* (caché et secret) et *graphien* (écrire), est la science des écritures secrètes. Elle recouvre l'étude et la conception des procèdes de chiffrement des informations de toute nature (écrites, paroles, images, données, …etc.). Le chiffrement désigne la transformation d'un texte (information) clair en un texte incompréhensible aux personnes non concernées, c'est-à-dire qui ne possèdent pas la « clef » de cryptage (connue uniquement par l'expéditeur et le destinataire). Le déchiffrement c'est l'opération inverse du chiffrement, il est l'art de retrouver l'information d'origine à partir du message chiffré.

Au départ de la cryptographie, l'homme a utilisé le remplacement des lettres par des signes ou d'autres lettres. Ensuite, à la renaissance, les lettres sont remplacées par des chiffres, dans des relations diplomatiques et militaires. Ainsi, les méthodes de chiffrement ont évolué au fil de temps, jusqu'on a arrivé aux premiers principes de base de la cryptographie moderne qui reviennent à Auguste Kirchhoff en 1883 et dont l'idée la plus importante est que la sécurité du chiffre ne doit pas dépendre de ce qui ne peut pas être facilement changer, plus le déchiffrement est difficile plus la sécurité est élevée.

Aujourd'hui, la cryptographie se base sur les mathématiques c'est-à-dire de transformer un message clair de façon mathématique et algorithmique pour le rendre incompréhensible (chiffré). Classiquement on distingue deux types d'algorithmes de chiffrement : symétrique et asymétrique. Les algorithmes de chiffrement symétriques utilisent la même clé partagée secrètement pour procéder au chiffrement et au déchiffrement comme l'algorithme DES (Data Encryption Standard). Les algorithmes de chiffrement asymétriques utilisent deux clés différentes. Une publique employée pour le chiffrement et une autre privée pour le déchiffrement comme l'algorithme RSA (dont le nom est formé des initiales de ses inventeurs : R. Rivest, A. Shamir, L. Adleman). Cependant, ces algorithmes restent insuffisants face à la montée en puissance des calculateurs pour garantir la sécurité parfaite de la communication. Une des solutions pour augmenter le niveau de sécurité c'est la cryptographie chaotique.

La réussite de T.Peccora et L.Carroll en 1990 dans la synchronisation des deux signaux chaotiques ouvre une grande porte de l'utilisation de ces signaux dans la sécurisation des

communications revient à ses propriétés (déterministe, sensibilité aux conditions initiales), et donc le but c'est de cacher le message à l'aide des systèmes chaotiques. Pour cela, des méthodes ont proposées, parmi lesquelles la méthode par addition, la commutation chaotique et la modulation chaotique.

Ce travail est organisé de la façon suivante : le premier chapitre présente un état de l'art sur les systèmes dynamiques non linéaires et les comportements chaotiques. Dans le second chapitre, nous introduisons la cryptographie chaotique. Nous présentons, en particulier les différentes techniques de cryptage par chaos. Le troisième chapitre constitue véritablement l'objet de notre contribution, ce chapitre consiste à :

- ✓ Faire une conception d'un émetteur chaotique.
- ✓ Ecrire son modèle mathématique.
- ✓ Chercher le comportement chaotique d'un paramètre.
- ✓ Tracer les réponses temporelles.
- ✓ Calculer les exposants de Lyapunov.
- ✓ Tracer le diagramme de bifurcation.

Les différentes simulations sont faites sous l'environnement MATLAB.

Chapitre I

Notions théoriques

I.1 Introduction

Pendant plusieurs siècles, le chaos était défini par le désordre et la confusion, et il est connu dans le domaine des mathématiques, mais c'est seulement au cours de la dernière décennie que les applications concrètes se sont multipliées.

Henry Poincaré fut l'un des premiers à entrevoir la théorie du chaos, Il découvrit la notion de sensibilité aux conditions initiales à travers le fameux problème de l'interaction de trois corps célestes (une étoile + 1 planètes).

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

I.2 Systèmes dynamiques

La notion de système dynamique est relative à tous les systèmes dont l'évolution dépend du temps ou de l'espace. Cette notion est donc générique et peut se retrouver dans divers domaines comme la physique, la chimie, la biologie, … [1]. L'évolution de système au cours du temps de façon à la fois :

- ✓ **Causal**, c'est-à-dire que l'avenir de système ne dépend que de phénomènes du passé ou du présent.
- ✓ **Déterministe**, c'est-à-dire qu'à une instante initiale donnée à l'instant présent va correspondre à chaque instant ultérieur et un seul état futur possible.

L'évolution du système peut donc se modéliser de deux façons différentes :

I.2.1 Système dynamique à temps continu

C'est-à-dire une évolution continue dans le temps, décrite par un système d'équations différentielles sous la forme :

$$\dot{x} = F(x(t), t) \qquad \text{(I.1)}$$

Où $F = R^n \times R^+ \rightarrow R^n$, désigne la dynamique du système continu.

I.2.2 Système dynamique à temps discret

C'est-à-dire une évolution discrète dans le temps, décrit par une équation aux différences finies sous la forme :

$$x_{i+1} = f(x_i\,, \alpha) \qquad \text{(I.2)}$$

Où f est une fonction continue où au moins continue par morceaux, $x_i \in R^i$ est le vecteur d'état à l'instant i ($i \in N$) et $\alpha \in R^r$ est celui des paramètres. L a fonction f peut dans certains cas, être inversée, ce qui introduit la notion de réversibilité qui permet de remonter dans le temps [2].

I.3 Système chaotique

Un comportement chaotique est un comportement particulier d'un système dynamique déterministe non linéaire plus complexe que les comportements habituels : oscillations périodiques, oscillations quasi périodiques, … etc, étudié théoriquement pour la première fois en 1963 par le météorologue américaine Edward LORENZ qui a mis en évidence que dans les systèmes non linéaires d'infimes différences dans les conditions initiales engendraient à long terme.

On appelle donc un système chaotique, un système qui dépend de plusieurs paramètres et qui est caractérisé par une extrême sensibilité aux conditions initiales. Il existe plusieurs systèmes physiques qui se comportent de manière chaotique, on peut citer l'atmosphère, un pendule excité dans le champ magnétique …etc. Par la suite, on va présenter quelques caractéristiques d'un système chaotique.

I.3.1 Non linéaire

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique. Le comportement chaotique d'un système dynamique non linéaire est dû aux non linéarités. En général, pour prévoir des phénomènes générés par les systèmes dynamiques, la démarche consiste à construire un modèle mathématique qui établit une relation entre un ensemble de causes et un ensemble d'effets. Si cette relation est une opération de proportionnalité, le phénomène est linéaire. Dans le cas d'un phénomène non linéaire, l'effet n'est pas proportionnel à la cause [3].

I.3.2 Déterministe

La Déterminisme veut dire qu'à partir d'un événement d'un phénomène (passé où présent) on peut prédire le futur de ce phénomène. Un système chaotique généralement régi par des équations différentielles non linéaires qui décrivent son comportement dynamique, et qui nous permet de prédire son évolution au cours du temps si on connait exactement son état initial.

I.3.3 Sensibilité aux conditions initiales

Est une propriété observée par le père de l'effet papillon Edward Lorenz lors de ses travaux en météorologie est connu sous le nom d'effet papillon, « un battement d'ailes de papillon à un endroit du monde peut provoquer une tempête à un autre endroit ». Donc on peut dire qu'une infime modification des conditions initiales peut entrainer des résultats imprévisibles sur le long terme, ça veut dire que l'existence d'une moindre erreur sur la condition initiale conduit à une divergence rapide des trajectoires au cours du temps. Ceci est illustré par la figure I.1 [4].

I.4 L'espace de phase

Un système dynamique est caractérisé par un certain nombre de variables d'états, qui ont la propriété de définir l'état du système à un instant donné. Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ces variables d'état. Cet espace est appelé l'espace de phase ou chaque point définit un état et le point associé à cet état décrit une trajectoire appelé également une orbite [3].

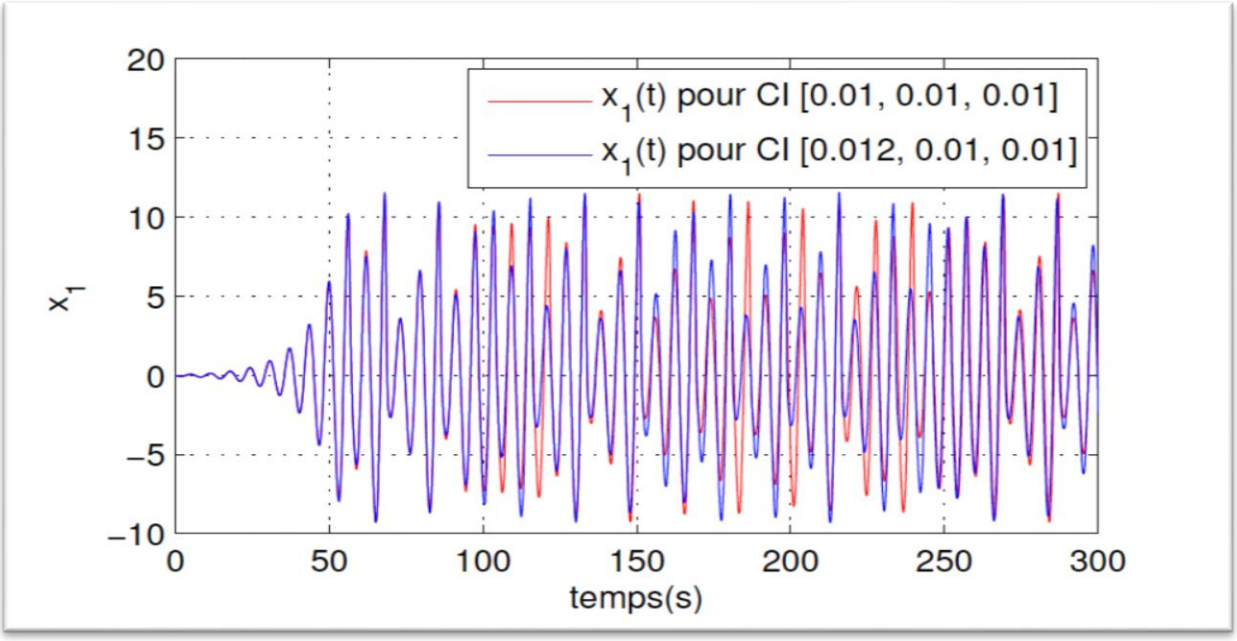


Figure I.1. Illustration de la propriété de sensibilité aux conditions initiales sur l'état x_1 (système de Rössler).

I.5 Notion d'attracteur

L'attracteur c'est la région de l'espace de phase vers laquelle convergent les trajectoires d'un système dynamique dissipatif. Les attracteurs sont des formes géométriques qui caractérisent l'évolution à long terme des systèmes dynamiques [5]. Il en existe quatre types distincts :

- ✓ **L'attracteur point fixe :** les trajectoires tendent vers un point de l'espace des phases donc on a une solution stationnaire constante (de fréquence nulle).
- ✓ **L'attracteur cycle limite :** les trajectoires tendent vers une trajectoire fermée dans l'espace des phases, donc on a une solution périodique (une seule fréquence).
- ✓ **L'attracteur « tore » :** correspond à un régime quasi-périodique ayant un nombre fini des fréquences.
- ✓ **L'attracteur étrange :** cet attracteur est associé à un comportement chaotique et c'est l'attracteur qui nous intéresse.

I.5.1 Attracteur étrange

C'est un attracteur associé à un comportement chaotique ; le terme attracteur étrange est utilisé pour la première fois par David Ruelle et Floris Taken en 1971[5], cette appellation d'attracteur étrange fait appel à ses propriétés (n'est pas une courbe ni une surface et aussi n'est pas continu). Il existe plusieurs attracteurs étranges par exemple (attracteur étrange de Lorenz, attracteur étrange de Rössler … etc.).

I.5.1.1 Attracteur étrange de Lorenz

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

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

Où x, y, z sont les variables d'état du système. β, ρ, σ Sont les paramètres de système [6].

La représentation graphique de ce système est donnée dans les figures suivantes, où on voit l'attracteur de Lorenz, et les états chaotiques du système de Lorenz. Pour ($\sigma = 10$; $\rho = 28$; $\beta = \frac{8}{3}$) , et les conditions initiales[$x(0) = 0$; $y(0) = 1$; $z(0) = 20$].

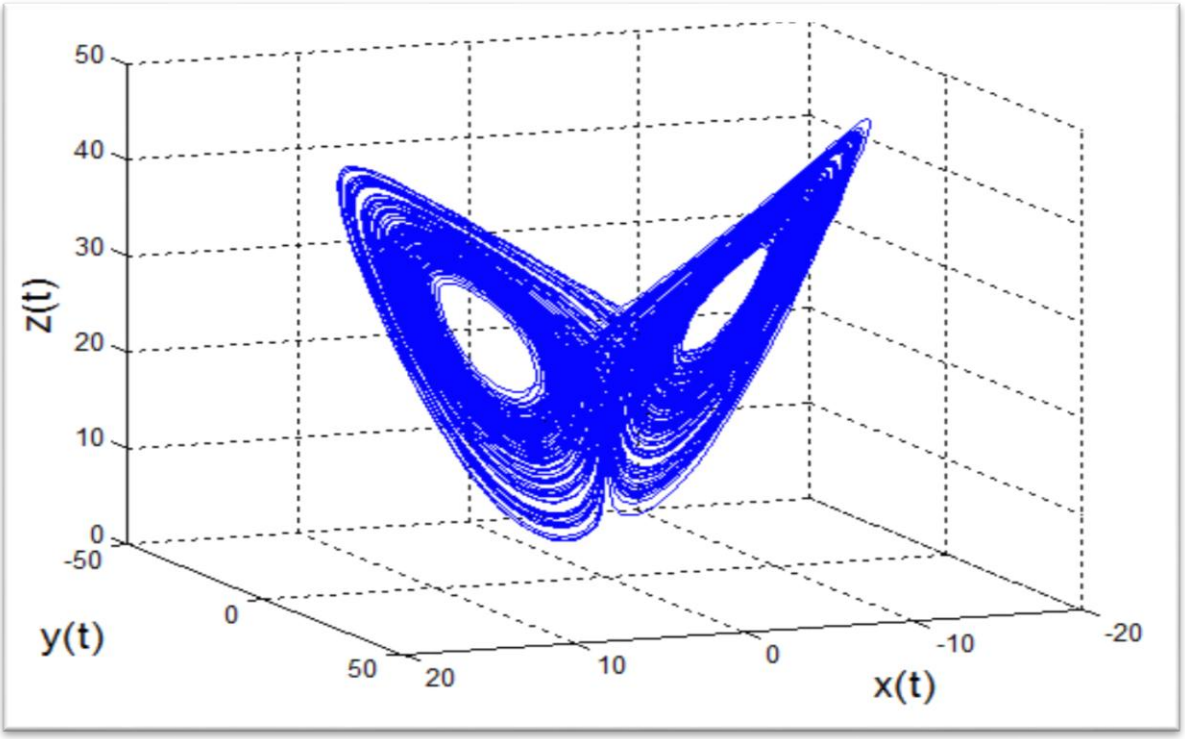


Figure I.2. Attracteur étrange de Lorenz.

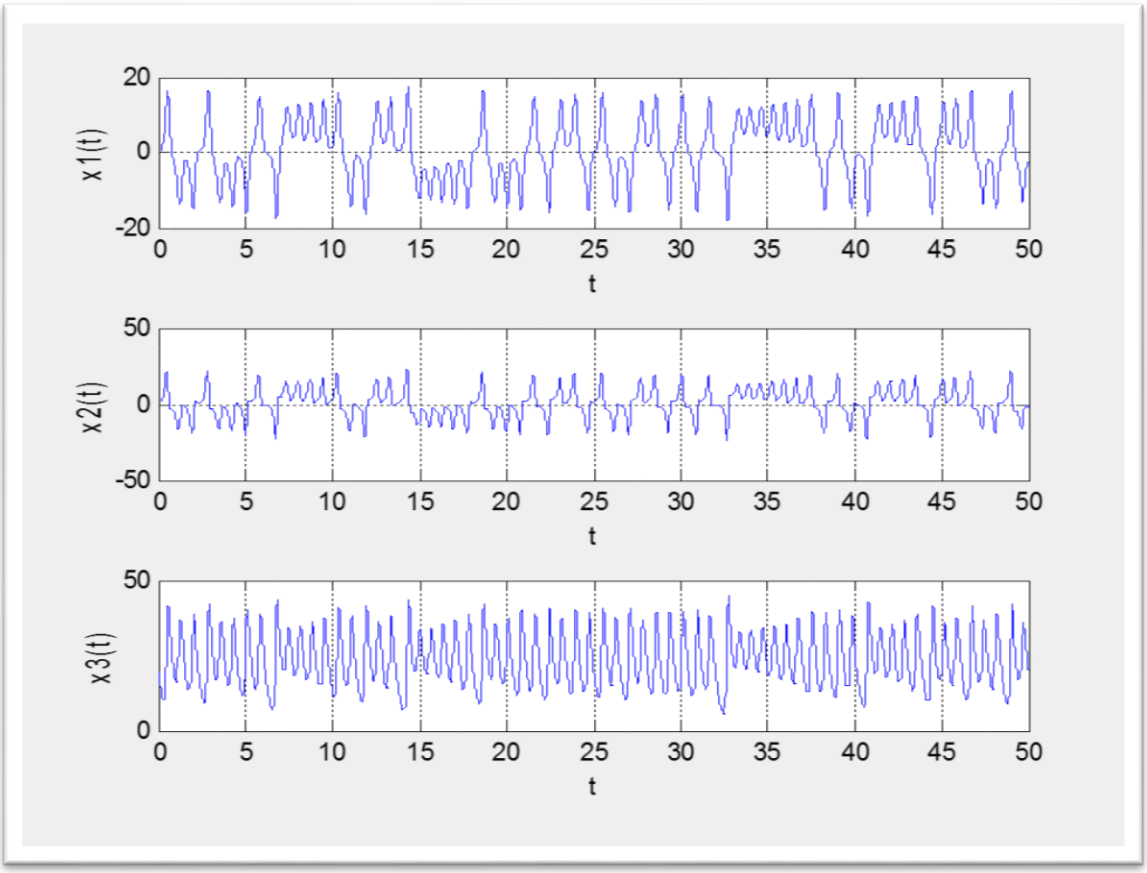


Figure I.3. Etats chaotiques du système de Lorenz.

I.5.1.2 Attracteur étrange de Rössler

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

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

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

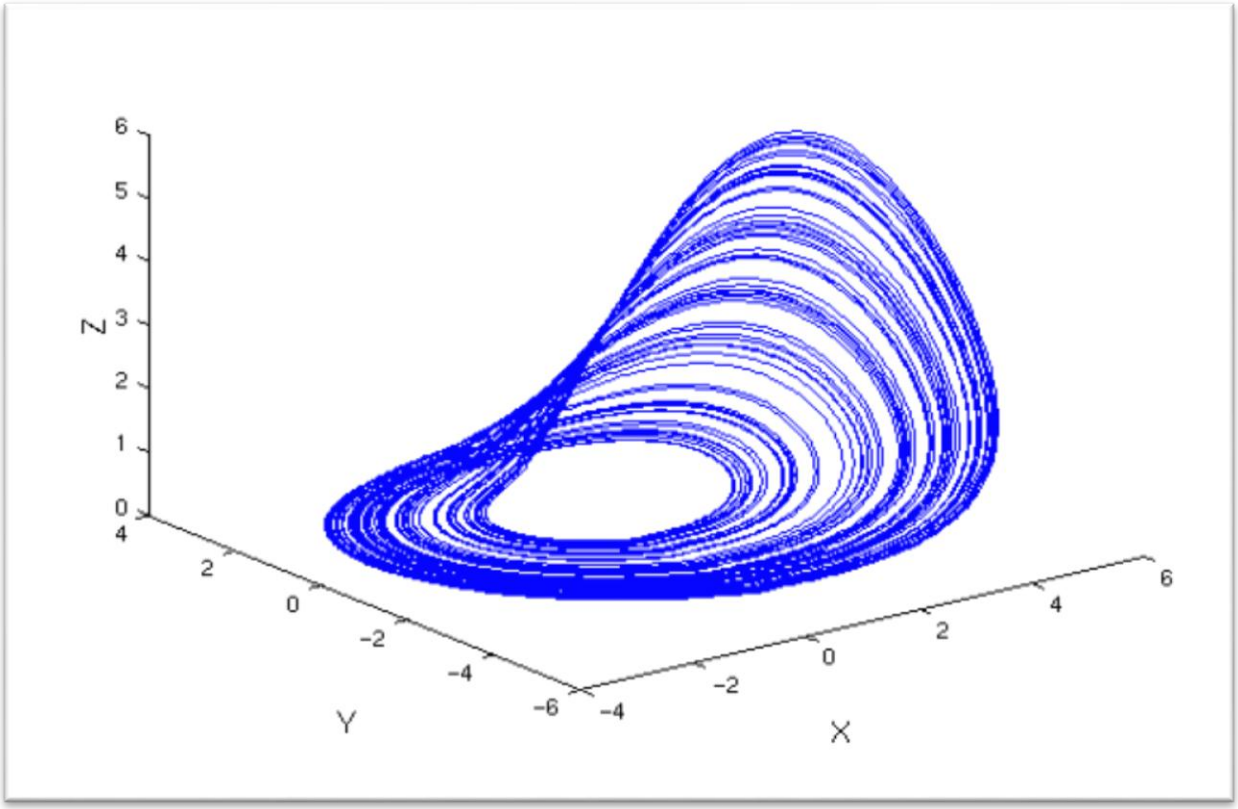


Figure I.4. Attracteur étrange de Rössler.

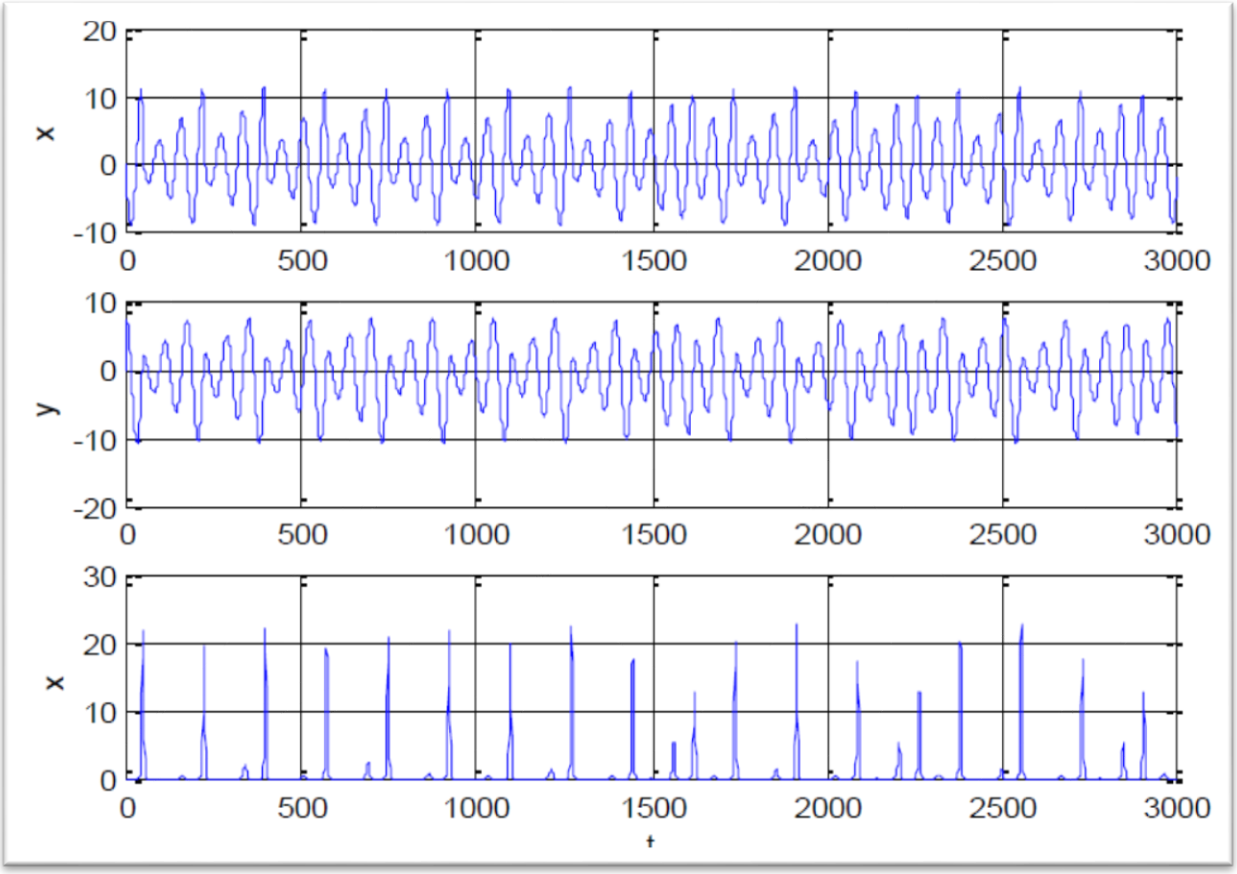


Figure I.5. Etats chaotique du système de Rössler.

I.5.2 Dimension de Hausdorff

La dimension de Hausdorff d'un espace métrique est un nombre réel positif ou nul, c'est-à-dire appartenant à l'intervalle[0 , ∞], introduite en 1918 par le mathématicien Felix Hausdorff [7 ,8].

Un attracteur étrange occupe un volume nul dans l'espace de phase, sa dimension est fractale (d non entière) avec $2 < d < n$, où n est la dimension de l'espace de phase.

I.6 Exposants de Lyapunov

Les exposants de Lyapunov, présentés par Oseledec pour la première fois en 1968, jouent un rôle important dans l'étude des systèmes dynamiques non linéaires notamment les systèmes chaotiques. Ils qualifient le degré de divergence des trajectoires d'un système dynamique non linéaire soumis à des conditions initiales différentes. Cette divergence est exprimée par les exposants de Lyapunov [9]. Ainsi le nombre d'exposants de Lyapunov est égal à la dimension de l'espace de phase et ils sont généralement indexés du plus grand au plus petit [6].

L'exposant de Lyapunov se définit alors comme :

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

Avec $i = 1, \dots, n$

L'existence d'un attracteur nécessite que la dynamique de ce système doit globalement dissipative

$$\sum_{i=1}^{n} \lambda_i < 0 \qquad \text{(I.6)}$$

En étudiant les exposants de Lyapunov d'un système dynamique non linéaire, on peut définir le comportement de ce système ou bien le type d'attracteur.

Tableau I.1. Exposants de Lyapunov et attracteur

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.6.1 Exemple

Les exposants de Lyapunov pour le système de Lorenz (I.3) sont calculés en utilisant MATLAB avec $(\sigma = 10; \rho = 28; \beta = \frac{8}{3})$, on trouve les résultats donnés dans la figure (I.6)

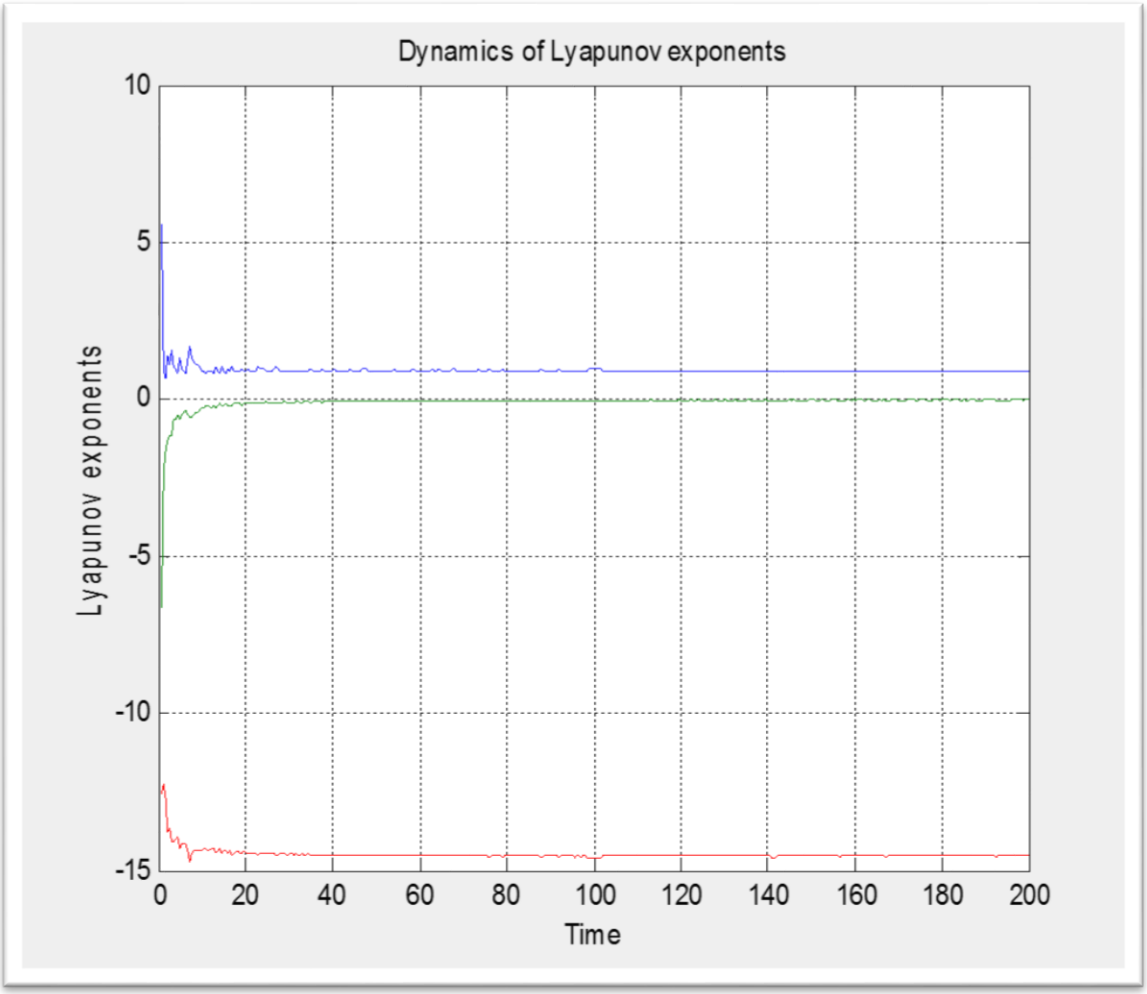


Figure I.6. Les exposants de Lyapunov pour Lorenz $\left(\sigma = 10, \rho = 28, \beta = \frac{8}{3}\right)$.

On a trouvé $(\lambda_1 = 0.895324\,, \lambda_2 = -0.011335\,, \lambda_3 = -14.547109)$, et puisque $\lambda_1 > 0$, on conclure que le système se comporte chaotique.

I.7 Section de Poincaré

En mathématiques, dans la théorie des systèmes dynamiques, la section de Poincaré est l'intersection d'une trajectoire (périodique, quasi-périodique ou chaotique) dans un espace d'au moins trois dimensions, avec un hyperplan d'une dimension inférieure. Ainsi, nous observons le retour de la trajectoire vers l'hyperplan qui commence à un certain point de celle-ci. L'ensemble des points marqués par la trajectoire sur l'hyperplan est appelé plan de Poincaré [9, 10, 11, 12]

I.8 Bifurcation

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique, une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents, les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation [3]. Donc une bifurcation c'est un diagramme qui montre les comportements possibles d'un système dynamique à long terme, en fonction des paramètres de bifurcation, la figure (I.6) nous donne un exemple de diagramme de bifurcation de la fonction logistique.

Le système dynamique non linéaire (la carte logistique) c'est un exemple des systèmes dynamiques unidimensionnels discrets qui est en fonction itérative définie par la fonction

$$f = [0,1] \rightarrow [0,1] x_{k+1} = f(x_k) = r.x_k(1 - x_k) \qquad \text{(I.7)}$$

Avec r est défini dans [0,4], et k=1,2, …

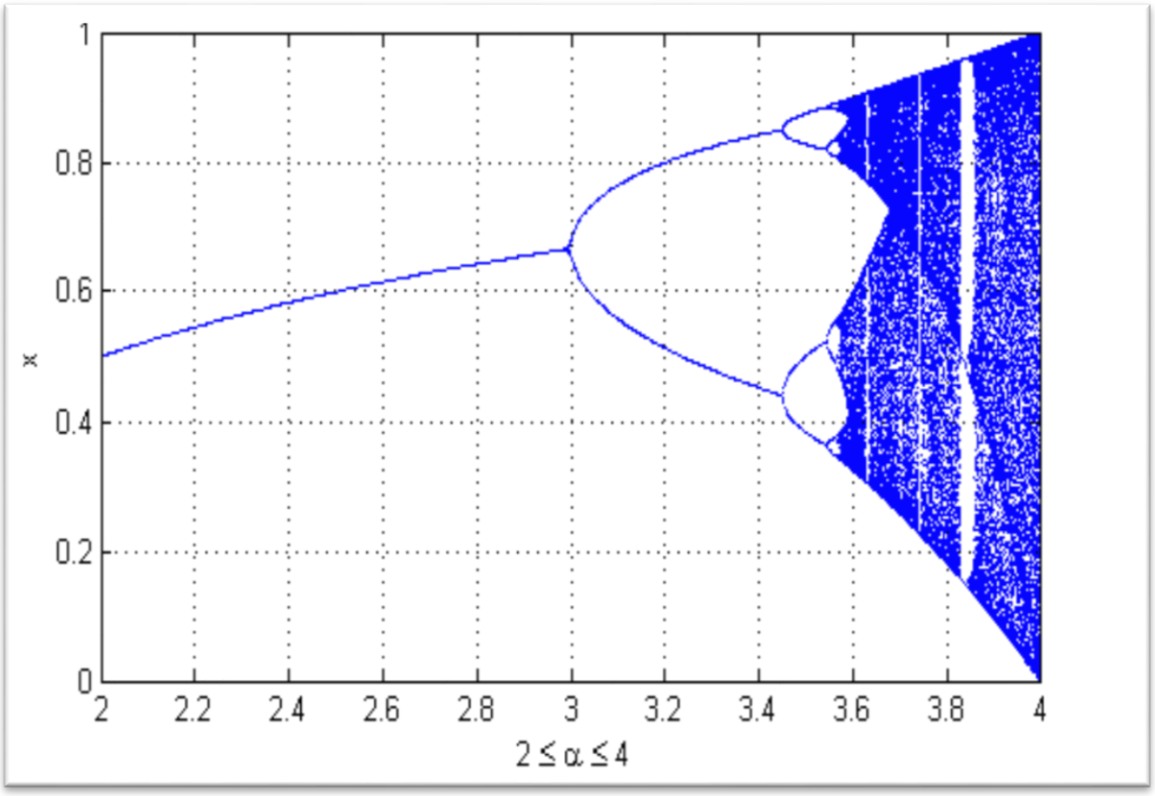


Figure I.7. Diagramme de bifurcation de la fonction logistique

r est responsable de comportement de cette dynamique :

Dans le diagramme de bifurcation de la fonction logistique figure (I.7), on remarque bien que le système dynamique non linéaire se comporte périodiquement pour certaines valeurs de paramètre r et

se comporte chaotique pour d'autres valeurs, on peut résumer les différents comportements possibles de ce système dans le tableau suivant :

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

La valeur de r	Le comportement de système
$1 \leq r < 3$	Le système possède un point fixe attractif
$3 \leq r < 3.373$	Le système se comporte périodiquement de période 2^m où m est un entier
$3.57 \leq r < 4$	Le système se comporte chaotique

I.9 Route vers chaos

Il existe plusieurs types d'évolution possible d'un système dynamique régulier vers le chaos, supposons que la dynamique étudiée dépend d'un paramètre de contrôle, lorsque on varie ce paramètre, le système peut passer d'un état stationnaire à un état périodique, puis au-delà d'un certain seuil, suivre un scénario de transition et devenir chaotique, on distingue trois scénarios théoriques d'évolution vers le chaos [13].

I.9.1 Le doublement de période

Ce scénario est le plus connu, par augmentation du paramètre de contrôle, la période se multiplie ainsi en 2,4, 8, 16, … jusqu'au on arrive à une certaine valeur du paramètre de contrôle où les doublements étant de plus en plus rapprochés, on tend vers un point auquel on obtiendrait hypothétiquement une fréquence infinie et c'est à ce moment que le chaos apparait.

I.9.2 L'intermittence

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière [4].

I.9.3 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.10 Conclusion

Dans le présent chapitre, quelques notions de base sur les systèmes dynamiques non linéaires notamment sur les systèmes chaotiques ont été décrites. Ces notions seront utilisées par la suite, lors de l'étude de différents comportements de l'oscillateur Colpitts qui sera utilisé en tant que générateur chaotique destiné à chiffrer un message confidentiel.

Chapitre II

Transmission Chaotique

II.1 Introduction

Dans le domaine des télécommunications, où les échanges d'informations multimédias se développent rapidement, il est indispensable de pouvoir disposer des systèmes sécurisés pour protéger les données à caractère personnel ou confidentiel et assurer la sécurité des transferts de données. Il est donc nécessaire de développer un outil efficace de protection des données transférées et des communications contre les intrusions arbitraires. Le cryptage des données est très souvent le seul moyen efficace pour répondre à ces exigences [14].

Le cryptage désigne l'ensemble des techniques permettant de transmettre des données confidentielles sur un milieu non sécurisé sans qu'un intrus ne puisse découvrir le contenu [15].

Les algorithmes de chiffrements utilisés avant soient à clé symétrique ou à clé asymétrique, ont déjà été cassés qu'impose l'obligation d'utiliser un algorithme plus sûr et plus efficace, c'est la cryptographie chaotique ou cryptage utilisant le chaos qui a répondu aux exigences de sécurité et de confidentialité. Dans ce chapitre, nous nous concentrons sur le principe et les techniques de la cryptographie chaotique.

II.2 Objectifs des crypto-systèmes

Le crypto-système assure et garantit :

- ✓ **La confidentialité**, garantir que le contenu d'une communication n'est pas accessible aux personnes non autorisées.
- ✓ **L'authentification**, fait référence pour la validation de la source du message pour assurer quel expéditeur est correctement identifié.
- ✓ **L'intégrité,** signe que le contenu d'une communication n'a pas été modifiée pendant la transmission.
- ✓ **La non-répudiation,** signée qu'un récepteur ne peut pas nier d'avoir reçu le message et l'expéditeur ne peut pas nier son émission.

II.3 Cryptographie chaotique

Le cryptage ou chiffrement c'est le processus qui transforme un message appelé « texte » de manière à le rendre incompréhensible. Par contre, le destinataire doit suivre un autre processus appelé « déchiffrement » ou « décryptage » pour récupérer le message original. Pour cet objectif il existe plusieurs algorithmes utilisés pour le chiffrement et déchiffrement du message. Et pour une communication sûre, l'expéditeur et le destinataire utilisent un élément appelé « clef » qui peut se présenter sous plusieurs formes (mots ou phrases), on peut classer les algorithmes en deux puisqu'il existe des algorithmes où l'expéditeur et le destinataire utilisent la même clef et d'autres algorithmes utilisent des clefs différentes pour le chiffrement déchiffrement. Avec ces algorithmes un espion même

s'il connait l'algorithme, ne peut pas déchiffrer le message s'il ne connait pas la clef. On distingue deux types d'algorithme :

- ✓ **Algorithme à clef secrète** appelé aussi (le chiffrement symétrique), est la plus ancienne forme de chiffrement, l'expéditeur et le destinataire utilisent des clefs identiques. Cette clef est sélectionnée avant d'échanger les messages. Ainsi, si la clef est dévoilée, n'importe qui peut lire le message, la figure (II.1) présente le principe de chiffrement symétrique ou l'algorithme à clef secrète.

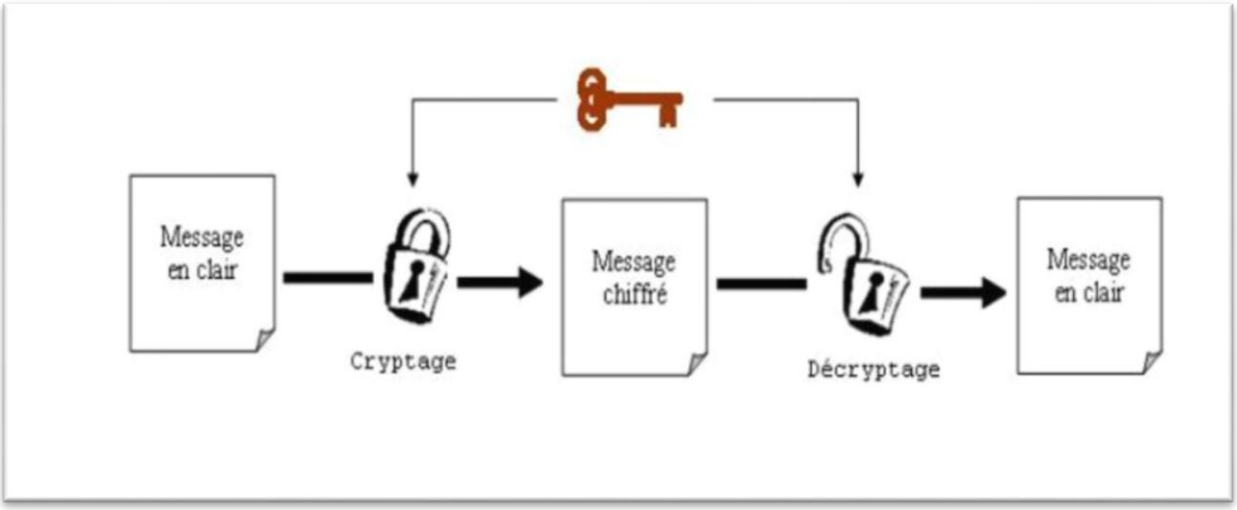


Figure II.1. Le principe de chiffrement symétrique.

- ✓ **Algorithme à clef publique** appelé aussi (le chiffrement asymétrique), a été proposé par Diffie et Hellmanen en 1976 [16]. Cet algorithme utilise deux clefs différentes, la clef de chiffrement peut être rendue publique, par contre dans la réception seule celui qui possède la clef de déchiffrement peut déchiffrer le message. La figure (II.2) présente le principe de chiffrement asymétrique.

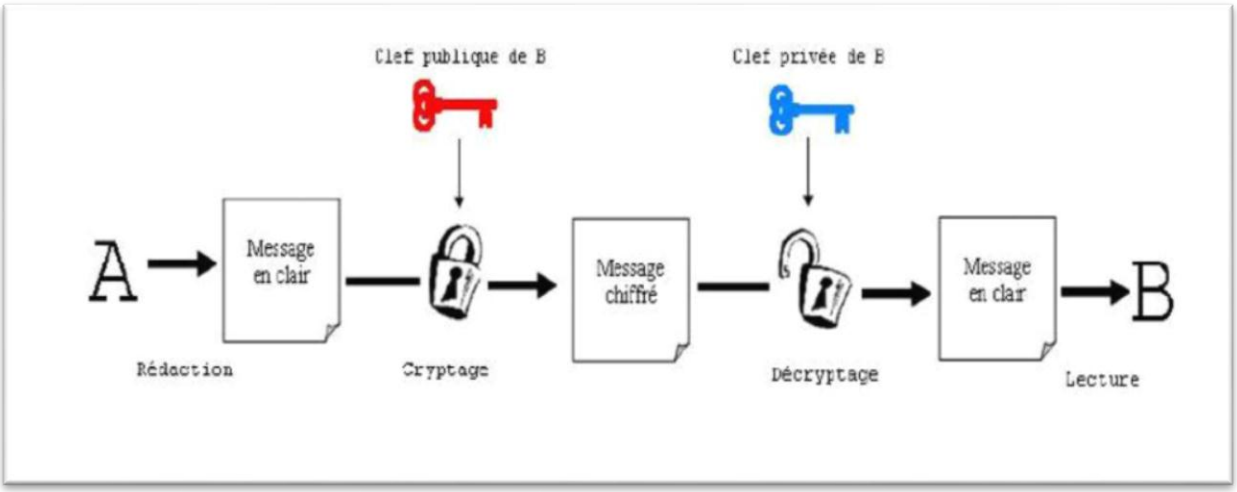


Figure II.2. Le principe de chiffrement asymétrique.

Depuis longtemps, les chercheurs ont l'idée d'utiliser les signaux aléatoires pour sécuriser les communications, cette idée a été mise en œuvre en 1926 par Vernam [17], cette idée a été développée dans le contexte des signaux chaotiques. A cause de la nature imprédictible à long terme du chaos, on a cru pendant longtemps que le chaos serait inutilisable et incontrôlable, mais depuis quelques décades, les chercheurs ont réussi à modéliser le chaos par des équations différentielles et montrer qu'il existe un coté déterministe dans ce phénomène qui apparait aléatoire à première vue. C'est cette nature semblable au bruit des signaux chaotiques qui a motivé les chercheurs d'essayer de camoufler un message confidentiel à l'aide d'un signal chaotique, de façon à ne pas distinguer. Ainsi, différentes techniques ont été proposées afin de masquer le message dans un système chaotique et ensuite de le restaurer. Ces techniques sont toutes basées sur la synchronisation des systèmes chaotiques et sont été améliorées au fil des années dans le but d'augmenter de plus en plus la sécurité et la rapidité de la transmission de l'information. Ces techniques sont parfois appelées méthodes de cryptographie chaotique, parmi elles on peut citer la technique par addition, la commutation chaotique, la modulation chaotique.

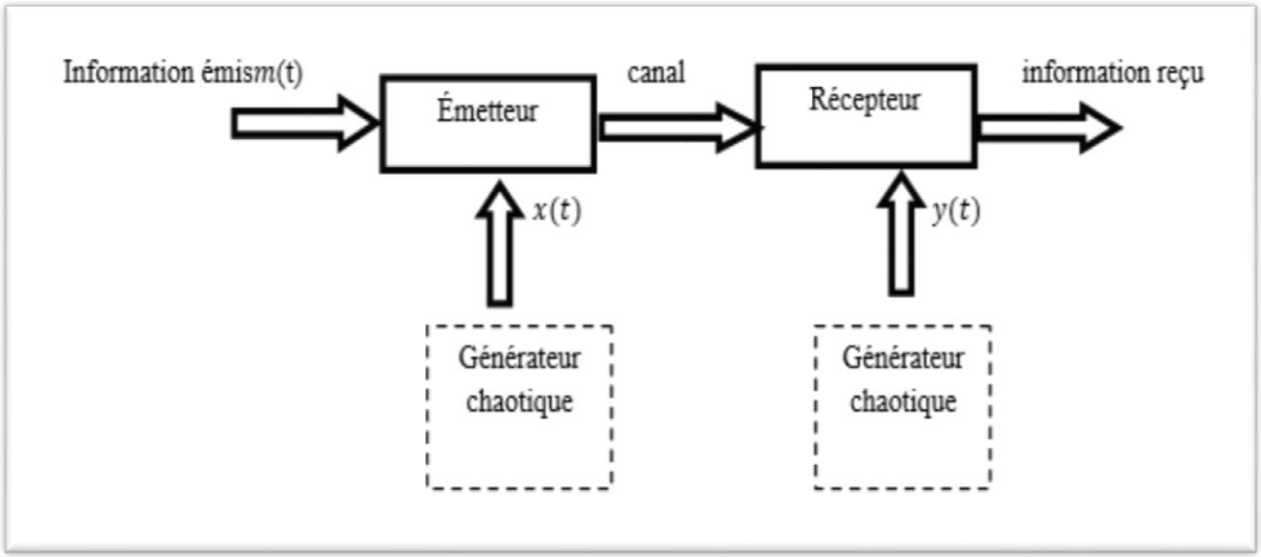


Figure II.3. Principe de transmission par chaos

II.4 Techniques de chiffrement par chaos

Dans la littérature, il existe plusieurs techniques pour l'injection de l'information dans un système chaotique ou bien pour masquer l'information dans le chaos, nous décrivons ici quelques-uns :

II.4.1 Chiffrement par addition

Cette méthode appelée aussi masquage chaotique, est la première chronologiquement à utiliser la synchronisation du chaos [18]. Dans cette méthode, l'émetteur est un système autonome dont le signal de sortie est ajouté au signal du message. La somme des deux signaux est transmise au

récepteur à travers le canal de transmission, qui est un canal public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur-récepteur), le message est extrait à l'aide d'une opération de soustraction [19, 20,21]. Notons que dans cette méthode, l'attracteur étrange du système chaotique n'est pas modifié par le message. Le principal avantage de cette méthode réside dans la simplicité de réalisation, on peut dire que cette technique peut être appliquée à des messages continus ou discrètes, inversement on souligne des inconvénients qui limitent l'application de cette technique comme le message doit être au moins de 20 à 30 dB inférieur à la sortie de l'émetteur pour garantir la synchronisation. Or en présence d'un bruit de canal d'une puissance proche de celle du message, il devient difficile de détecter l'information. De plus, cette méthode reste sensible aux attaques extérieures [22] et l'usage du canal de transmission est inefficace d'un point de vue de l'énergie transmise par rapport à la qualité d'information fournie [9]. Le schéma représentatif de cette méthode est donné dans la figure II.4

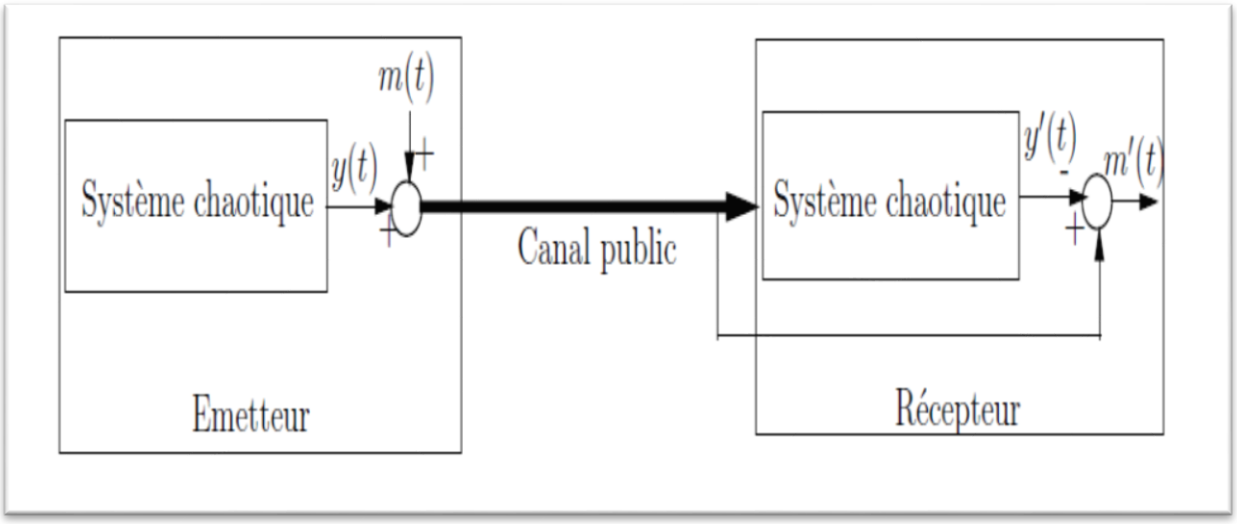


Figure II.4. Chiffrement par addition

II.4.2 Chiffrement par commutation

Cette méthode (en anglais Chaos Shift Keying, CSK) est utilisée principalement pour transmettre un message binaire (voir figure II.5), l'émetteur est composé de deux systèmes chaotiques et pour chaque niveau de message $m(t)$ (0 ou 1), l'un des systèmes envoie sa sortie sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étranges. Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur. Pour chaque valeur de message, l'un des deux systèmes se synchronise avec l'émetteur et un bloc de comparaison permet de relever la valeur de message notée $m'(t)$ [23,24]. Il est à noter que cette méthode reste sensible aux attaques par détection de rupture [25].

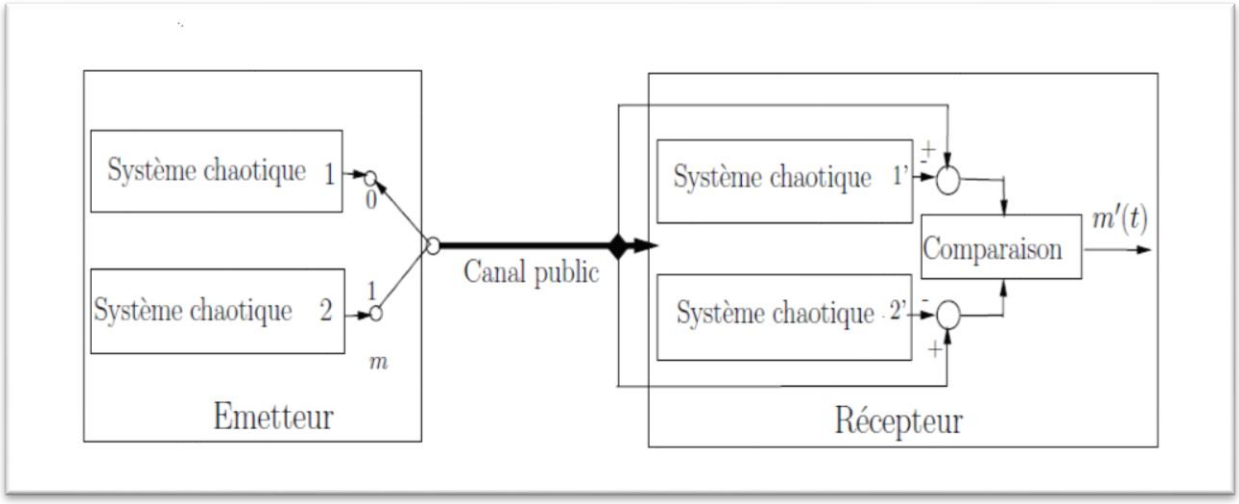


Figure II.5. Chiffrement par commutation

II.4.3 Chiffrement par modulation

Cette technique utilise le message contenant l'information pour moduler le paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure (II.6).

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètres (s) impose à la trajectoire de changer continument d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique « normal ». Cependant, la façon d'injecter le message est donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques. Elle n'a pas d'équivalent parmi les systèmes de communication « classique ». Cependant, le cryptage par modulation s'est avéré sensible à certaines attaques [26].

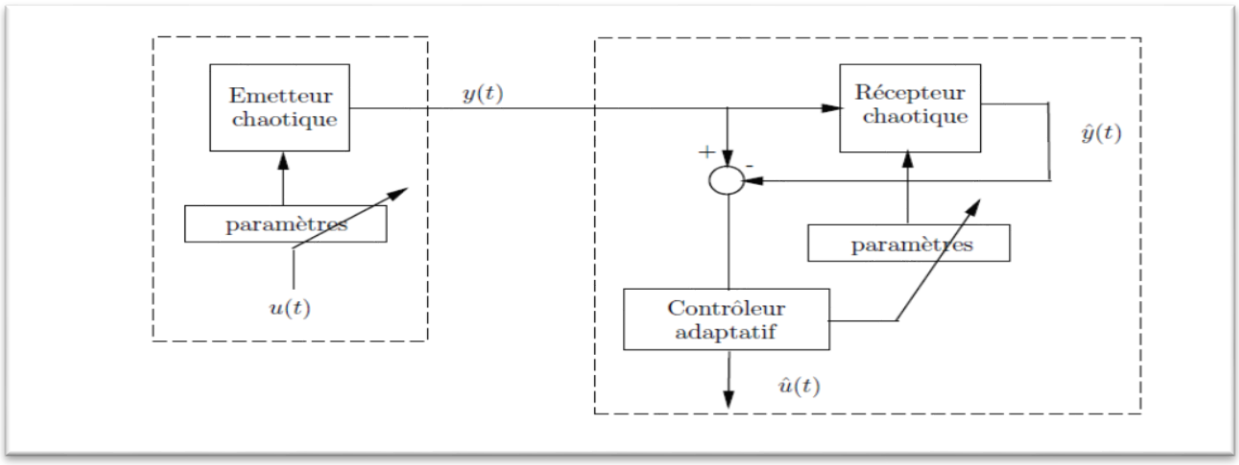


Figure II.6. Chiffrement par modulation

II.5 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 clefs utilisées dans le chiffrement. Aussi on a présenté les différentes techniques de chiffrement par chaos analogique. Dans le chapitre suivant on va présenter la conception de notre générateur de porteuse chaotique.

Chapitre III

Conception d’un Générateur Chaotique

III.1 Introduction

Aujourd'hui, dans la littérature on trouve plusieurs types d'oscillateurs pour la génération des signaux chaotiques [27, 28, 29, 30, 31, 32]. Parmi eux, certains sont des systèmes non autonomes utilisant un dipôle non linéaire dont la caractéristique est le plus souvent symétrique. Ces oscillateurs, qui diffèrent par leurs structures et/ou par leurs éléments électriques et/ou par la technologie utilisée, offrent la possibilité de générer des comportements chaotiques des plus basses fréquences aux plus hautes. Le point commun entre tous ces oscillateurs est la présence d'un élément non linéaire et d'un élément qui réinjecte de l'énergie.

Les oscillateurs sont généralement définis par des équations différentielles qui facilitent l'analyse explicite ou implicite de modèle mathématique. La caractéristique du chaos permet de l'utiliser dans plusieurs applications et en particulier dans le domaine des communications pour la sécurisation de l'information. Parmi les oscillateurs on trouve le circuit de Chua qui est très connu et réalisé ; et très utilisé pour l'étude des phénomènes chaotiques [17, 33]. L'oscillateur de Chua comme représenté sur la figure (III .1), est la réalisation physique d'un oscillateur développé par Leon Chua en 1983 – 1984 au cours de sa visite à l'Université Waseda (Tokyo, Japon) [34]. Ce circuit autonome est bien connu par la simplicité de sa structure qui est constituée d'une résistance négative non linéaire qui lui apporte de l'énergie (deux capacités et une inductance) [35]. Des choix appropriés de valeurs de ses paramètres électriques lui permettent de générer de différents comportements chaotiques. On trouve aussi un oscillateur qui est très utilisé pour la génération de signaux chaotiques est l'oscillateur Colpitts [36]. Cet oscillateur fait l'objet de nombreuses études [9, 37, 38, 39, 40, 41, 42, 43, 44, 45].

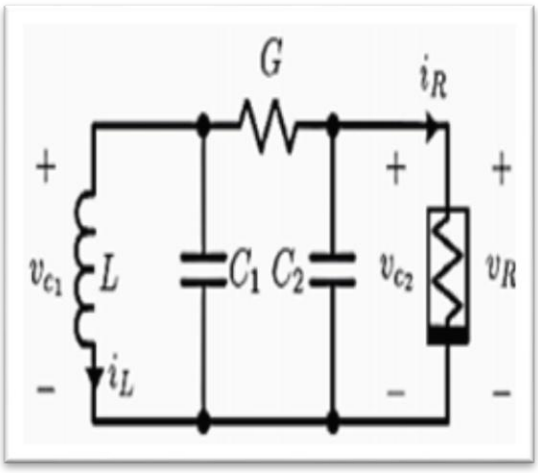


Figure III.1. Circuit de Chua.

Dans ce chapitre on va s'intéresser à l'explication de fonctionnement de l'oscillateur Colpitts qui sera utilisé par la suite comme générateur de porteuse chaotique. C'est pour cela on va détailler son comportement en différents régimes (périodiques, quasi-périodique et chaotique).

III.2 Choix de l'émetteur chaotique

Dans notre travail, nous avons choisi l'utilisation de l'oscillateur Colpitts en technologie bipolaire comme un générateur de signaux chaotiques. On peut juger notre choix par les arguments suivants :

- ✓ La simplicité de la structure de l'oscillateur Colpitts qui utilise un seul transistor et permet, comme nous allons le montrer dans les paragraphes suivants, de générer des comportements chaotiques en modifiant uniquement les conditions de fonctionnement du transistor. Les autres paramètres de l'oscillateur sont fixés à des valeurs appropriées.
- ✓ La possibilité de faire évoluer la fréquence fondamentale de l'oscillateur vers les fréquences élevées [46, 47]. Il suffit pour cela de choisir la technologie adéquate pour le transistor et d'inclure les effets liés à la montée en fréquence.
- ✓ La structure de l'oscillateur Colpitts possède une non linéarité intrinsèque due à la caractéristique exponentielle du transistor.
- ✓ L'utilisation de l'oscillateur Colpitts dans les systèmes de communications chaotiques a été démontrée pour la transmission de signaux binaires [48] et continus [49, 50, 51].

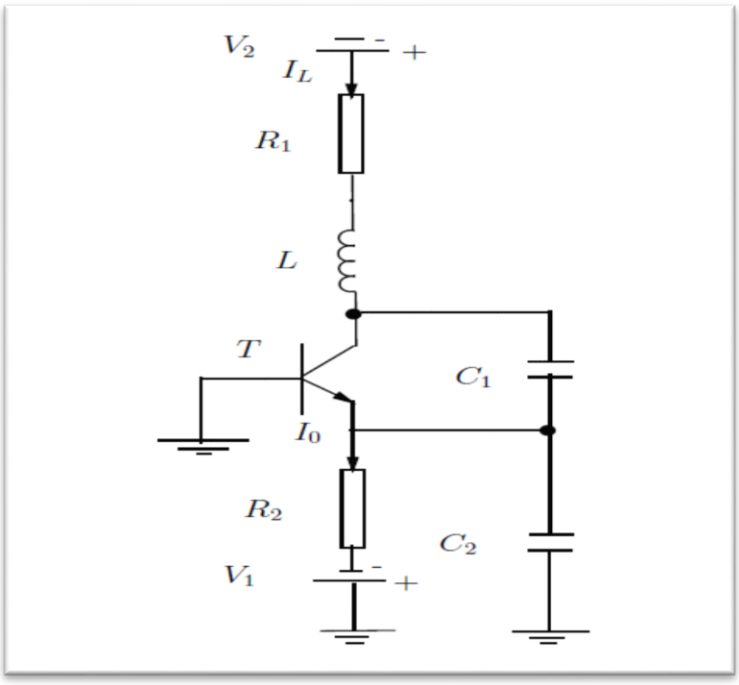


Figure III.2. Montage basses fréquences de l'oscillateur Colpitts.

($R_{1=}470\ Ohm$, $R_2 = 1\ kOhm$, $C_1 = C_2 = 470\ nF$, $L_1 = 1\ mH$, T: $2N2222.$)

En général, les oscillateurs constitués de transistor FET (Transistor à effet de champ ou « Field Effect Transistor ») ou BJT (Transistor Bipolaire ou « Bipolaire Junction Transistor ») et un circuit résonant LC sont souvent utilisés pour fonctionner dans des plages de quelques kHz à quelques

centaines de MHz. La structure qu'on va l'utiliser c'est une structure en base commune qui permet d'obtenir un gain plus élevé tout en autorisant une bande passante plus large [52]. Le transistor utilisé est un transistor bipolaire classique (BJT). Le circuit résonnant LC est connecté entre le collecteur et la base du transistor et une fraction de la tension du circuit LC est retournée à l'émetteur. Les tensions d'alimentation V_1 et V_2 permettent de fixer le point de fonctionnement du transistor. Le choix des valeurs du circuit résonnant détermine la fréquence fondamentale de l'oscillateur [53]. La figure III.2 montre le montage basses fréquences de l'oscillateur Colpitts.

III.3 Présentation de l'oscillateur Colpitts

III.3.1 Définition d'un oscillateur

Un oscillateur est un montage autonome (pas de signal de commande) qui génère spontanément un signal alternatif lors de la mise en tension.

III.3.2 Condition d'oscillation d'un oscillateur

Le schéma de la figure III.3 donne la structure d'un oscillateur qui comporte toujours de deux éléments : un élément actif (amplificateur opérationnel, transistor bipolaire …etc.) et un élément passif. Sa structure est celle d'un système bouclé dans lequel une fraction de signal de sortie est ramenée à l'entrée pour assurer l'auto entretien des oscillations.

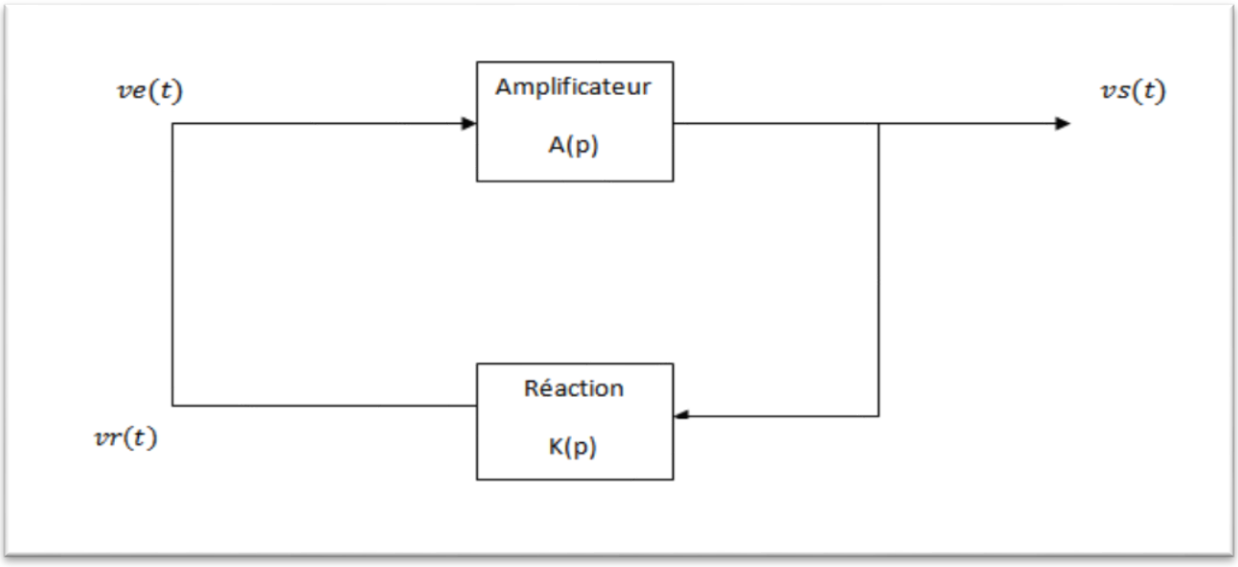


Figure III.3. Structure d'un oscillateur

Avec $A(p)$: est la fonction de transfert d'amplificateur, $K(p)$: est la fonction de transfert de réseau de réaction. $Ve(t)$ est le signal à l'entrée de l'amplificateur, $Vs(t)$ est le signal à la sortie de l'amplificateur, $Vr(t)$ est le signal à la sortie de réseau de réaction.

Si le signal $Vr(t)$ est identique à $Ve(t)$ alors on peut le refermer sur l'entrée de l'amplificateur, et on obtient $Vs(t)$ souhaité sans appliquer le signal de commande extérieur, cette condition n'est satisfaite que pour une condition d'oscillation bien définie appelée fréquence d'oscillation.

Pour trouver la condition d'oscillation d'un oscillateur on a :

$$Vs(t) = A(p)\,.Ve(t) \qquad \text{(III.1)}$$

$$Ve(t) = K(p).Vs(t) \qquad \text{(III.2)}$$

Et donc on trouve la condition suivante utilisant les équations (III.1) et (III.2) :

$$Vs(t)[1 - A(p).K(p)] = 0 \qquad \text{(III.3)}$$

Vs(t) = 0, pas d'oscillations. Donc la condition d'oscillation c'est la suivante :

$$A(p).K(p) = 1 \qquad \text{(III.4)}$$

En module $A\,.K = 1$, et en argument $\arg(A) + \arg(K) = 0 + 2k\pi$, ce qui signifie que le réseau de réaction doit compenser le déphasage éventuel par l'amplificateur. C'est la condition d'oscillation ou critère de Barkhausen.

III.3.2.1 Critère de Barkhausen

Pour qu'un système puisse osciller, l'amplitude du gain de la boucle doit être unitaire et sa phase doit être nulle.

III.3.3 Conditions d'oscillation de l'oscillateur Colpitts

Pour pouvoir déterminer la condition d'oscillation de l'oscillateur Colpitts, on donne son schéma de principe sur la figure suivante.

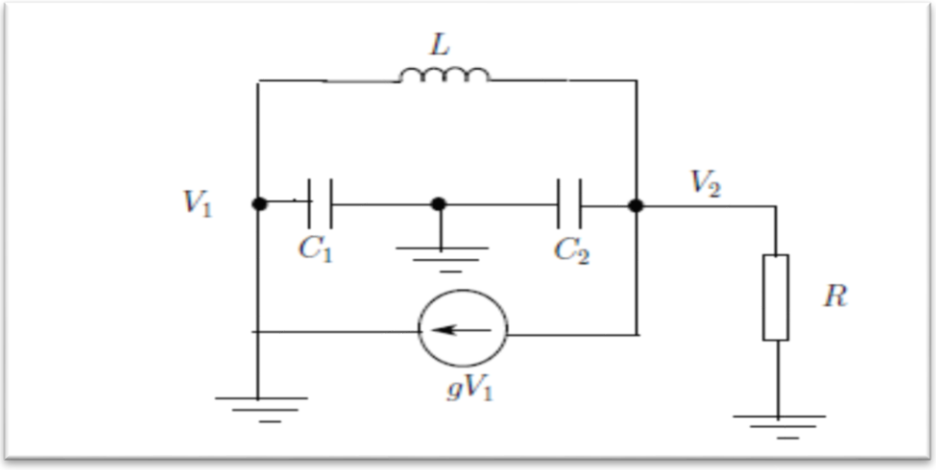


Figure III.4. Principe de l'oscillateur Colpitts.

$i_2 = g.V_2$ est défini la caractéristique de la résistance non linéaire qui peut être celle d'un amplificateur à base de transistor bipolaire où à effet de champ.

Utilisant la loi de Kirchhoff aux deux extrémités de l'inductance L, on écrit les équations suivantes du courant :

$$\begin{cases} -gv_1 - \frac{v_2}{R} - jC_2\omega v_2 + \frac{v_1 - v_2}{jL\omega} = 0 \\ \\ \frac{v_2 - v_1}{jL\omega} - jC_1\omega v_1 = 0 \end{cases} \quad \text{(III.5)}$$

En remplaçant la valeur de v_2 qui est déjà calculée à partir de la deuxième équation de (III.5), on obtient :

$$\left[-g + \frac{1}{jL\omega}\right]\frac{1}{jL\omega} - \left[jC_1\omega + \frac{1}{jL\omega}\right]\left[\frac{1}{R} + jC_2\omega + \frac{1}{jL\omega}\right] = 0 \quad \text{(III.6)}$$

Pour trouver la fréquence d'oscillation, on annule la partie imaginaire de (III.6), donc on trouve :

$$C_1C_2RL{\omega_0}^2 - (C_1 + C_2)R\omega_0^2 = 0 \quad \text{(III.7)}$$

Après qu'on résoudre l'équation précédente on trouve

$$\omega_0 = \frac{1}{\sqrt{L\frac{C_1C_2}{C_1+C_2}}} \quad \text{(III.8)}$$

Et la fréquence f_0 d'oscillation :

$$f_0 = \frac{1}{2\pi\sqrt{L\frac{C_1C_2}{C_1+C_2}}} \quad \text{(III.9)}$$

Pour trouver la condition d'oscillation de l'oscillateur Colpitts il faut annuler la partie imaginaire de l'équation (III.6), on obtient l'équation suivante :

$$-Rg + LC_1\omega^2 - 1 = 0 \quad \text{(III.11)}$$

Alors la condition d'oscillation de l'oscillateur Colpitts d'après l'équation (III.11) :

$$R = \frac{L\,C_1\omega^2 - 1}{g} \quad \text{(III.12)}$$

L'oscillation démarre lorsque la valeur de R est supérieure à la valeur obtenue par (III.12), si on remplace ω dans (III.12) on trouve la condition d'oscillation :

$$gR > \frac{C_1}{C_2} \quad \text{(III.13)}$$

III.3.4 Les équations d'états de l'oscillateur Colpitts

Afin de décrire le modèle mathématique de l'oscillateur Colpitts, nous écrivons ses équations d'état en considérant les variables d'états V_{C1} , V_{C2} et I_L appliquant la loi des mailles et la loi des nœuds sur le circuit de l'oscillateur Colpitts figure (III.2), donc on trouve les équations suivantes :

$$\begin{cases} \frac{dV_{C1}}{dt} = -\frac{1}{C_1} f(-V_{C2}) + \frac{1}{C_1} I_L \\ \frac{dV_{C2}}{dt} = \frac{1}{C_2} I_L - \frac{1}{C_2} I_0 \\ \frac{dI_L}{dt} = -\frac{1}{L_1} V_{C1} - \frac{1}{L_1} V_{C2} - \frac{R_1}{L_1} I_L + \frac{V_2}{L_1} \end{cases} \quad \text{(III.14)}$$

Où le terme $f(.)$ décrit la relation courant tension du transistor T, elle est fonction du courant de l'émetteur qui donné comme suit :

$$I_E = f(V_{BE}) = f(-V_{C2}) \cong I_S \left[\exp\left(\frac{V_{BE}}{V_T}\right)\right] \cong I_S \left[\exp\left(\frac{-V_{C2}}{V_T}\right)\right] \quad \text{(III.15)}$$

Où $V_T \approx 27\, m\, V$, et I_S désigne le courant de saturation inverse de la jonction base-émetteur (BE) du transistor T.

Dans [39,40], Maggio et al ont donné le modèle non linéaire du transistor bipolaire (figure III.5), où la relation courant tension (I_E , V_{BE}) est montrée par la résistance non linéaire R_E qui est l'élément générateur d'oscillations chaotiques.

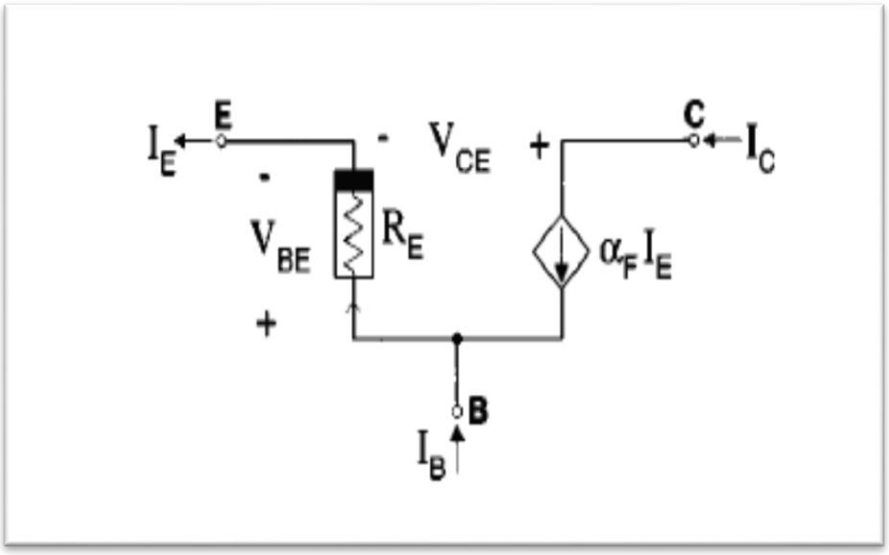


Figure III.5. Modèle non linéaire simple du transistor bipolaire.

Maggio et al dans [39,40] sont aussi présenté la normalisation de modèle mathématique de l'oscillateur Colpitts. Pour cela, la normalisation de temps, de courant et des tensions se fait par rapport à :

$$V_{ref} = V_T \ , \qquad I_{ref} = I_0 \ , t_{ref} = \frac{1}{\omega_0}$$

Avec $\omega_0 = \frac{1}{\sqrt{L\frac{C_1 C_2}{C_1+C_2}}}$ représente la fréquence centrale d'oscillation.

Le point d'opération du système (III.14) est la suivante [9, 39, 40] :

$$O: \begin{cases} V_{C_1O} = V_{CC} - \alpha R I_0 + V_T ln\left(\alpha \frac{I_0}{I_S}\right) \\ V_{C_2O} = -V_T ln\left(\alpha \frac{I_0}{I_S}\right) \\ I_{L_O} = \alpha I_0 \end{cases} \qquad \text{(III.16)}$$

On considère par la suite $\alpha = 1$, ce qui signifie que le courant de la base de transistor T est négligeable, donc les trois variables d'état sans dimensions(x_1, x_2, x_3), s'écrivent comme la suite :

$$\begin{cases} x_1(t) = \frac{1}{V_T}\left[V_{C1}(\omega_0 t) - V_{C_1O}\right] \\ x_2(t) = \frac{1}{V_T}\left[V_{C2}(\omega_0 t) - V_{C_2O}\right] \\ x_3(t) = \frac{1}{I_0}\left[I_L(\omega_0 t) - I_{L_O}\right] \end{cases} \qquad \text{(III.17)}$$

Et donc on obtient le système normalisé ci-dessous à partir de (III.14), (III.16) et (III.17) :

$$\begin{cases} \dot{x_1} = \frac{g}{Q(1-k)}\left[-n(x_2) + x_3\right] \\ \dot{x_2} = \frac{g}{Qk} x_3 \\ \dot{x_3} = -\frac{Qk(1-k)}{g}[x_1 + x_2] - \frac{1}{Q} x_3 \end{cases} \qquad \text{(III.18)}$$

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 de lorsque le critère de Barkhausen [52] est satisfait, et $Q = \frac{\omega_0 L}{R}$ est le facteur de qualité du circuit *LC* non chargé. Il y a alors des oscillations sinusoïdales lorsque $g = 1$.

Le paramètre g est calculé par [41] avec I_0 une source de courant idéale :

$$g = \frac{(R_1 + r_L)Q^2}{4V_T} I_0 \qquad \text{(III.19)}$$

Où r_L est l'impédance de l'inductanceL_1. Dans les simulations, on considère que cette impédance qui est contenue dans la résistanceR_1.

III.3.5 Linéarisation du système non linéaire normalisé

III.3.5.1 Définition du point d'équilibre d'un système

On considère le système dynamique non linéaire ci-dessous :

$$\begin{cases} \dot{x} = f(x, y) \\ \dot{y} = g(x, y) \end{cases} \qquad \text{(III.20)}$$

On appelle point d'équilibre du système précédente, le point x_e de l'espace des phases si :

$$f(x_e) = 0 \quad \text{Et} \quad g(x_e) = 0$$

III.3.5.2 Définition de la matrice Jacobienne

Pour un système dynamique non linéaire $\dot{x} = (f_1(x_1, x_2, \dots, x_n), \dots, f_p(x_1, x_2, \dots, x_p))$ la matrice jacobienne A en un point d'équilibre x_e est calculée de la façon suivante :

$$A = \begin{pmatrix} \frac{\partial f_1}{\partial x_1}(x_e) & \dots & \frac{\partial f_1}{\partial x_n}(x_e) \\ & \frac{\partial f_i}{\partial x_j}(x_e) & \\ \frac{\partial f_p}{\partial x_1}(x_e) & \dots & \frac{\partial f_p}{\partial x_n}(x_e) \end{pmatrix}$$

III.3.5.3 Théorème (Linéarisation du système)

Pour x petit, le comportement du système $\dot{x} = f(x)$ au voisinage du point d'équilibre est celui du système linèarisè [9] :

$$\dot{x}(t) = A(t)x(t) \qquad \text{(III.21)}$$

Où $A = \frac{\partial f}{\partial x}(x_e)$ est la matrice jacobienne du système au point d'équilibre x_e

III.3.5.4 Linéarisation du notre système

On commence d'abord par déterminer le point d'équilibre du système (III.18) en appliquant le changement de coordonnées indiquées en (III.17), donc on trouve que le point d'équilibre du système

(III.18) est situé à l'origine (0, 0, 0). Par conséquent on peut linéariser ce système autour du point d'équilibre en utilisant sa matrice jacobienne.

Donc on peut étudier le comportement du système linéarisé $\begin{pmatrix} \dot{x_1} \\ \dot{x_2} \\ \dot{x_3} \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$. La matrice jacobienne de (III.18) au point d'équilibre (0, 0, 0) est calculée par :

$$A = \begin{pmatrix} 0 & \frac{g}{Q(1-k)} & \frac{g}{Q(1-k)} \\ 0 & 0 & \frac{g}{Qk} \\ -\frac{Qk(1-k)}{g} & -\frac{Qk(1-k)}{g} & -\frac{1}{Q} \end{pmatrix} \qquad \text{(III.22)}$$

Le terme $n(x_2) = \exp(-x_2) - 1$ a disparu après la linéarisation car d'après le développement limité de la fonction $\exp(-x_2)$ pour y est proche de 0 :

$$e^{-x_2} = 1 + \frac{-x_2}{1!} + \frac{{-x_2}^2}{2!} + \frac{{-x_2}^3}{3!} + \cdots, \ -\infty < -x_2 < \infty \qquad \text{(III.23)}$$

On prend que la partie linéaire de (III.23) donc on trouve :

$$n(x_2) = 1 - x_2 - 1 = -x_2$$

On sait que l'équation caractéristique d'une matrice est égale à :

$$\text{èquation caractèristique}(\lambda) = \det(A - \lambda \mathrm{I})$$

Avec *A* : une matrice carrée de dimension $n \times n$, et *I* la matrice identité de dimension $n \times n$, λ est la variable de l'équation caractéristique.

Donc nous avons utilisé un programme MATLAB pour calculer l'équation caractéristique de la matrice A (III.22) et trouver ses valeurs propres, et l'équation trouvée ci-dessous :

$$\lambda^3 + \frac{\lambda^3}{Q} + \lambda + \frac{\mathrm{g}}{\mathrm{Q}} = 0 \qquad \text{(III.24)}$$

On remarque que pour $g = 1$, les valeurs propres de *A* sont :

$$\lambda_1 = +j\,, \qquad \lambda_2 = -j\,, \qquad \lambda_3 = -\frac{1}{Q}$$

Le point d'équilibre est caractérisé par des valeurs propres purement imaginaires (λ_1, λ_2) , ce qui justifie l'apparition des oscillations sinusoïdales pour $g = 1$.

III.3.6 Analyse des comportements chaotiques par simulation

Pour arriver à bien observer les différents comportements de l'oscillateur Colpitts, on a utilisé un programme MATLAB qui résoudre le système des équations différentielles ODE (III.18), et pour cela on a fixé les paramètres $L = 1\,mH\,, C_1 = C_2 = 470nF$. La fréquence d'oscillation est alors $f_0 = 10.38\,kHz$, la valeur de Q est obtenu en remplaçant les valeurs ci-dessus. Nous obtenons $Q = 1.38$ pour ces valeurs. Ainsi on fait varier le paramètre g qui lui dépend de I_0. Pour démarrer l'oscillation, nous avons fixé la valeur de g légèrement supérieur à 1 pour satisfaire la condition de Barkhausen. Les résultats obtenus pour différentes valeurs de g sont donnés par les figures suivantes (III.6), (III.7), (III.8), (III.9) et (III.10).

Pour $g = 1.0029$, la condition de Barkhausen est vérifiée, donc on a des oscillations sinusoïdales au niveau des réponses temporelle figure (III.6.a) et par conséquent un cycle limite dans le plan de phase $y - z$ figure (III.6.b).

En augmentant la valeur de g jusqu'à on arrive à $g = 2.13$, le système oscille sinusoïdalement avec deux périodes figure (III.7.a) correspondant à 2 cycles limites dans le plan de phase figure (III.7.b).

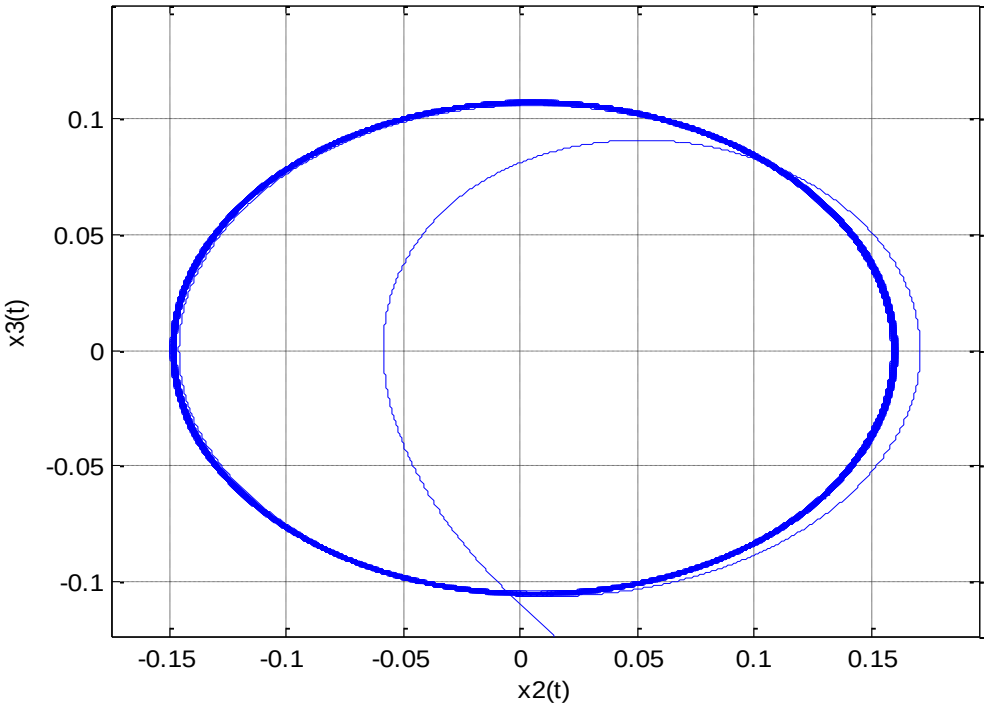
Pour $g = 2.4$ le système présent des oscillations à deux périodes figure (III.8.a) correspondant à 4 cycles limites dans le plan de phase figure (III.8.b).

Pour $g = 3.79$ le système oscille avec 8 périodes figure (III.9.a) correspondant à 8 cycles limites dans le plan de phase. Par contre pour $g = 4.46$ un comportement chaotique apparait correspondant à un attracteur étrange dans l'espace de phase.

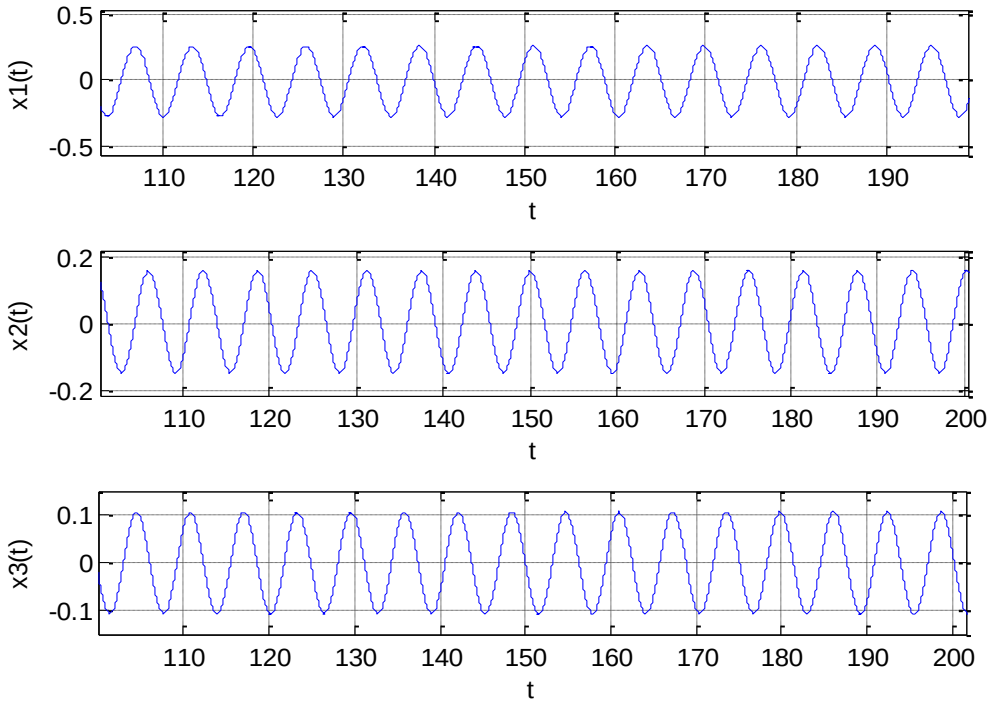
Pour $g = 4.46$ les valeurs propres de la matrice jacobienne A (les racines de l'équation caractéristique (III.24)), sont :

$$\lambda_1 = -1.49, \qquad \lambda_2 = 0.38 - 1.14j, \qquad \lambda_3 = 0.38 + 1.14j$$

On a trouvé que pour $g = 4.46$, le point d'équilibre possède deux valeurs propres à partie réelle positive. Cela justifie le comportement hyperchaotique de l'oscillateur Colpitts. Le chaos obtenu est appelé « chaos de Shil'nikov », qui en effet le résultat d'existence de deux valeurs propres complexes [41,42].

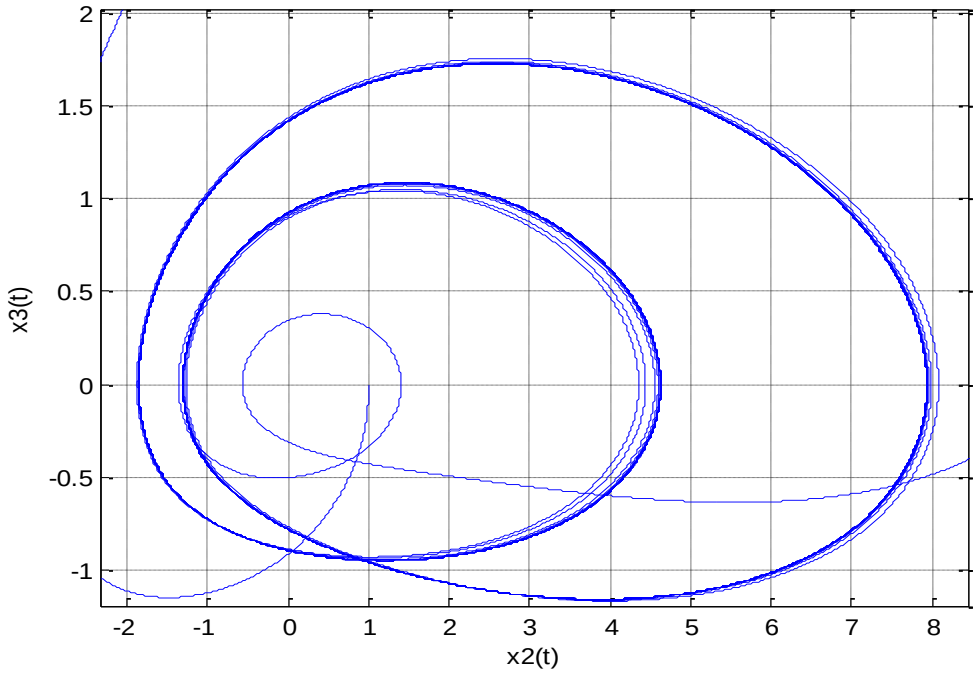


(a) Plan de phase

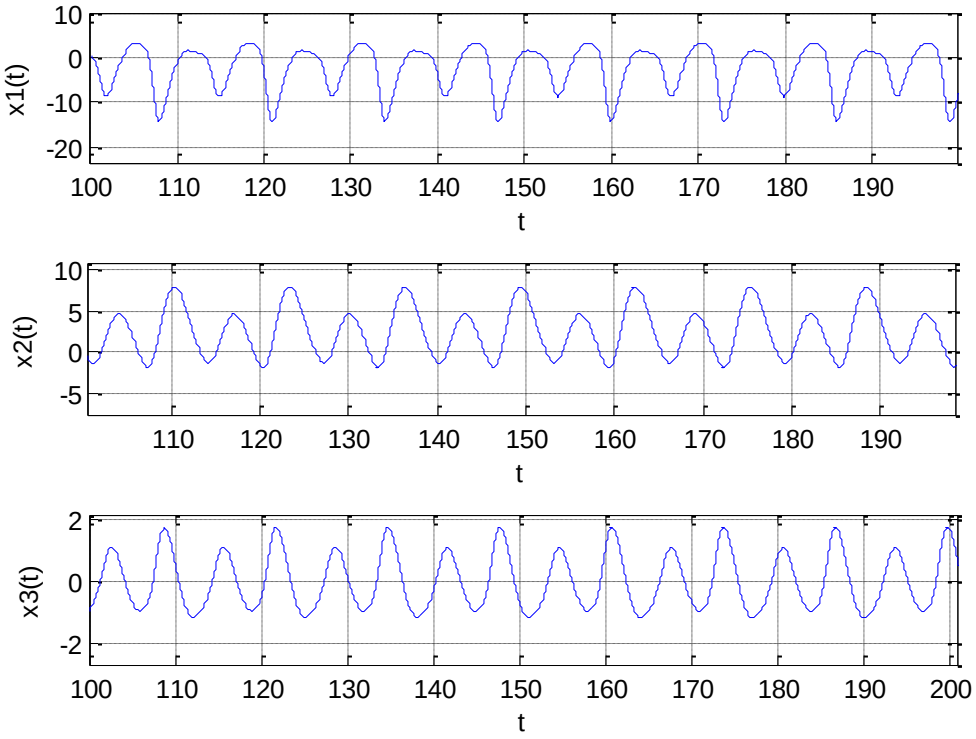


(b) Réponses temporelles

Figure III.6. Signaux et plans de phase obtenus pour l'oscillateur Colpitts (g=1.0029)

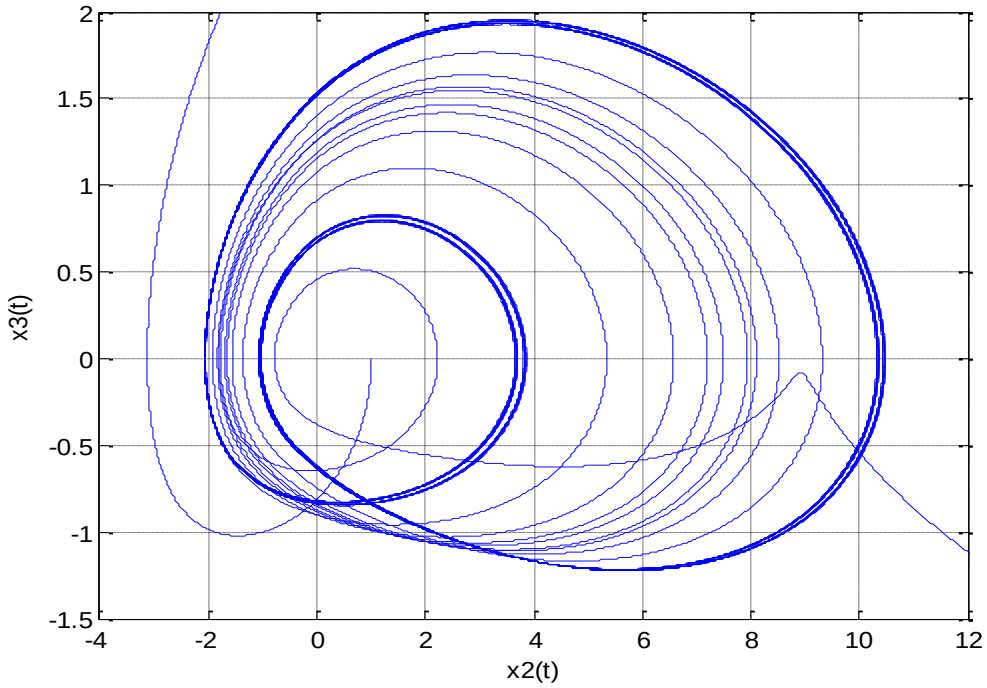


(a) Plan de phase

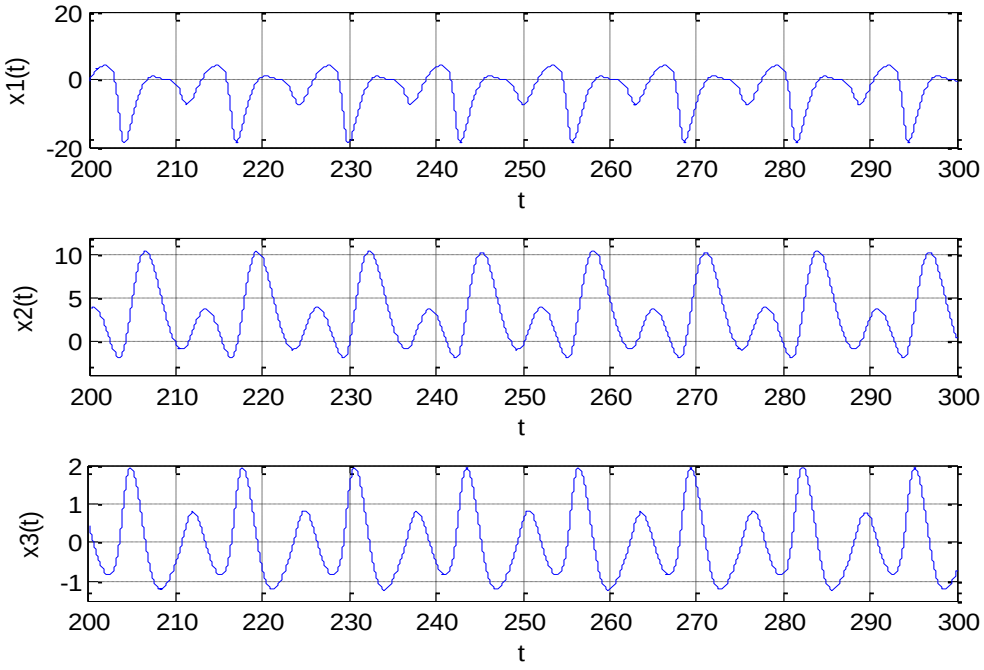


(b) Réponses temporelles

Figure III.7 Signaux et plans de phase obtenus pour l'oscillateur Colpitts (g=2.13)

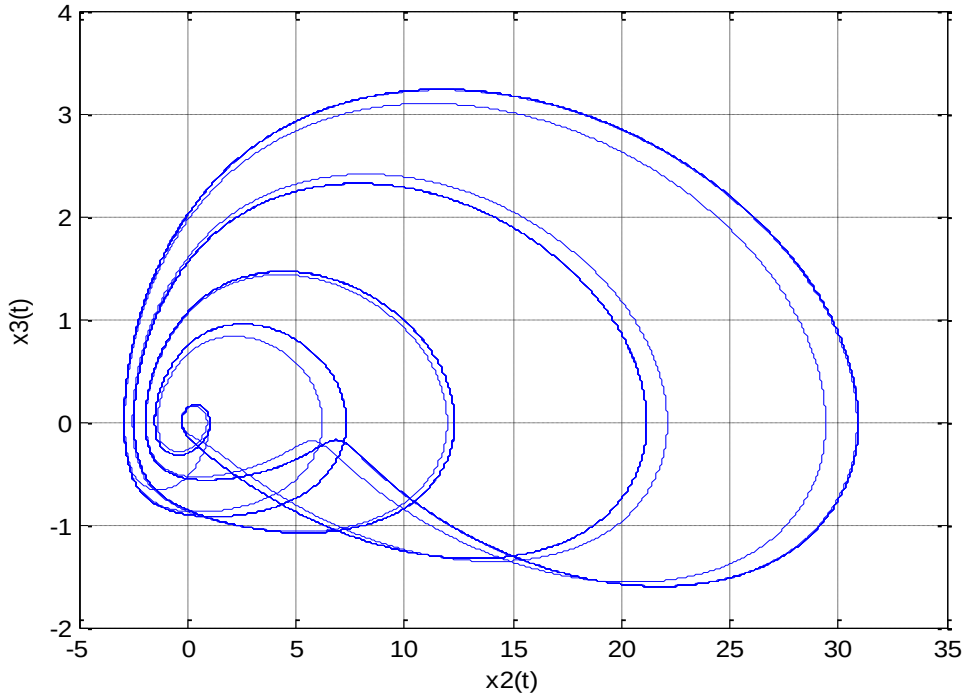


(a) Plan de phase

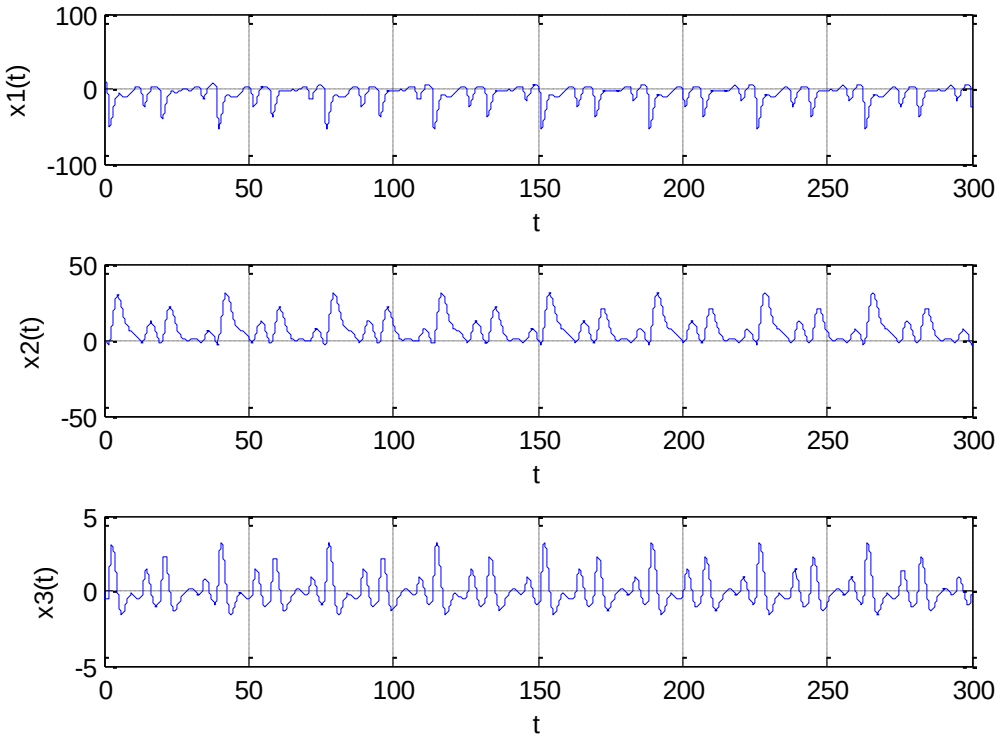


(b) Réponses temporelles

Figure III.8 Signaux et plans de phase obtenus pour l'oscillateur Colpitts (g=2.4)

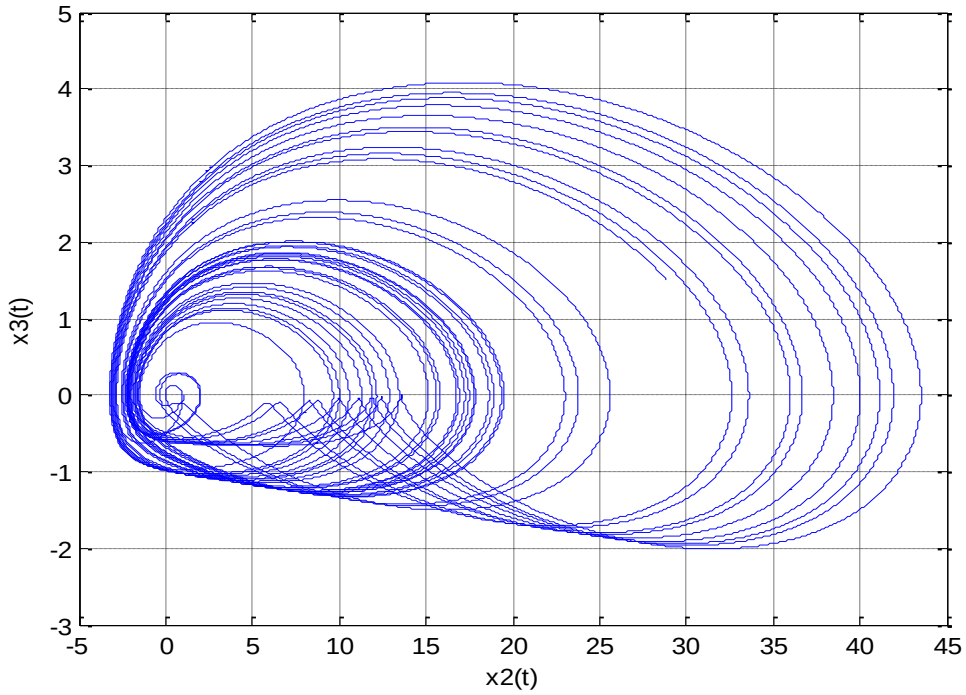


(a) Plan de phase

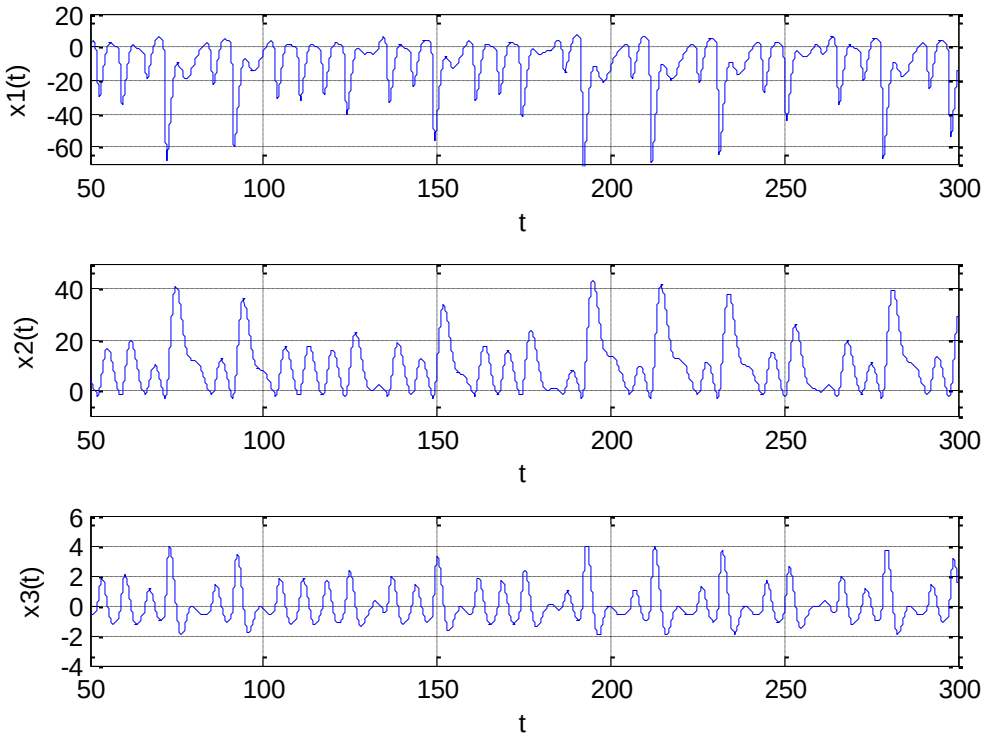


(b) Réponses temporelles

Figure III.9 Signaux et plans de phase obtenus pour l'oscillateur Colpitts (g=3.79)



(a) Plan de phase



(b) Réponses temporelles

Figure.III.10. Signaux et plans de phase obtenus pour l'oscillateur Colpitts (g=4.46)

III.3.7 Détermination des exposants de Lyapunov

Afin de déterminer les exposants de Lyapunov de l'oscillateur Colpitts en utilisant MATLAB, un algorithme proposé par A. Wolf, J.B.Swift, H.L.Swinney et J.A.Vastaro dans [54], en entrant les valeurs des paramètres g, Q, k , et les éléments de la matrice jacobienne, nous obtenons les exposants de Lyapunov. Et pour l'objectif de vérifier et justifier le comportement hyper chaotique de l'oscillateur Colpitts, on a pris les valeurs $Q = 1.38$, $g = 4.46$ et $k = 0.5$, nous obtenons :

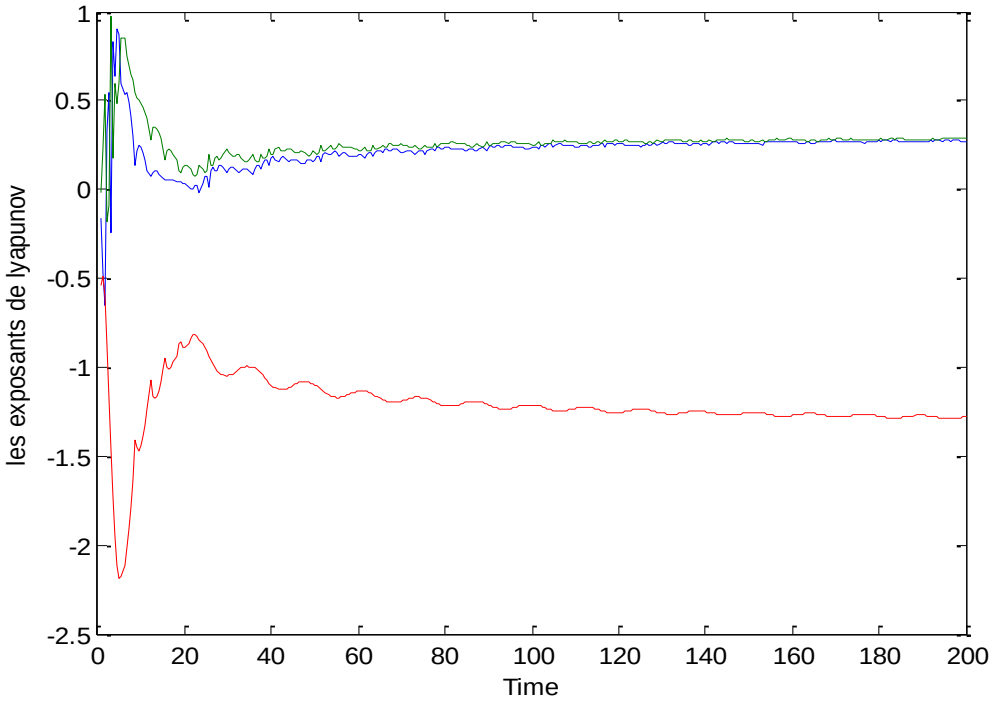


Figure III.11. Les exposants de Lyapunov pour $(g = 4.46, Q = 1.38, k = 0.5)$

Donc $\lambda_1 = 0.270528,\ \lambda_2 = 0.283822,\ \lambda_3 = -1.278999$, les deux premiers exposants sont positifs, donc ces résultats justifient le comportement hyperchaotique de l'oscillateur Colpitts trouvé déjà (figure III.10), ceci justifie aussi les résultats obtenus par le calcul des valeurs propres de la matrice jacobienne.

III.3.8 Section de Poincaré pour l'oscillateur de Colpitts

On a déjà dit que le point d'équilibre du système (III.18) est situé à l'origine $O(0,0,0)$ de plus ce point correspond au point d'opération du système. De plus l'espace de phase peut être devisé en deux régions distinctes correspondant aux différents modes d'opération du transistor BJT [40].

- ✓ Pour $x_2 \leq 1$ le transistor travaille dans sa région active.
- ✓ Pour $x_2 > 1$ le transistor travaille dans la région bloquée.

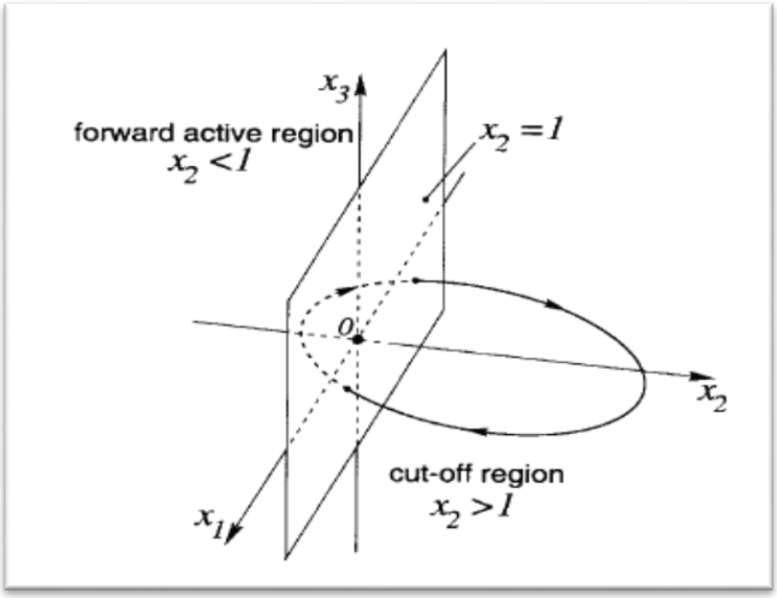


Figure III.12. Régions d'opération du transistor de l'oscillateur Colpitts

Dans la région active, les trajectoires sont accélérées par l'énergie fournie par le transistor, alors que dans la région non active, elles évoluent grâce aux oscillations naturelles du circuit LC non chargé. Donc on peut obtenir la section de Poincaré pour les différents comportements de l'oscillateur Colpitts. La section de Poincaré est obtenue dans un sens c'est-à-dire pour $\dot{x_2} > 0$. La section de Poincarè pour $g = 4.46$ (oscillations chaotiques) est donnée dans la figure (III.13), où on remarque que la section de Poincaré comprend plusieurs points, par contre au comportement périodique (cycle limite) qui aurait donné lieu à un seul point.

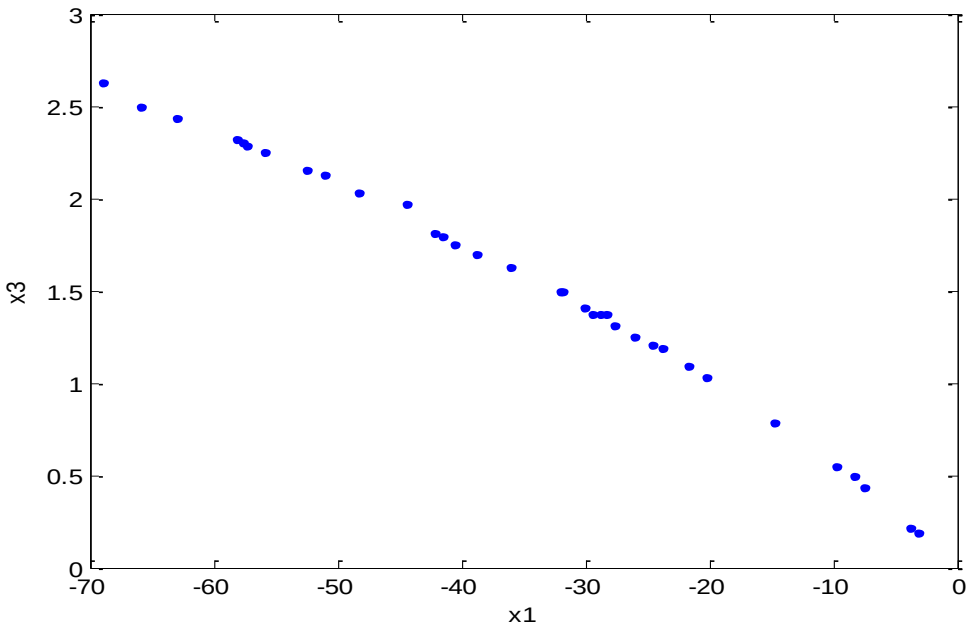


Figure III.12. Section de Poincaré de l'oscillateur Colpitts chaotique

III.3.9 Diagramme de bifurcation de l'oscillateur Colpitts

Pour bien visualiser et suivi les différents comportements de l'oscillateur Colpitts, on a tracé le diagramme de bifurcation en utilisant un programme MATLAB, dans ce programme on a fait varier le paramètre g de 0.5 jusqu'à 6 avec un pas de 0.01 et on a visualisé la variable d'état x_3 , ce diagramme (figure III.13) montre la route vers le chaos de l'oscillateur Colpitts, les zones denses dans la figure (III.13) indiquent le régime chaotique.

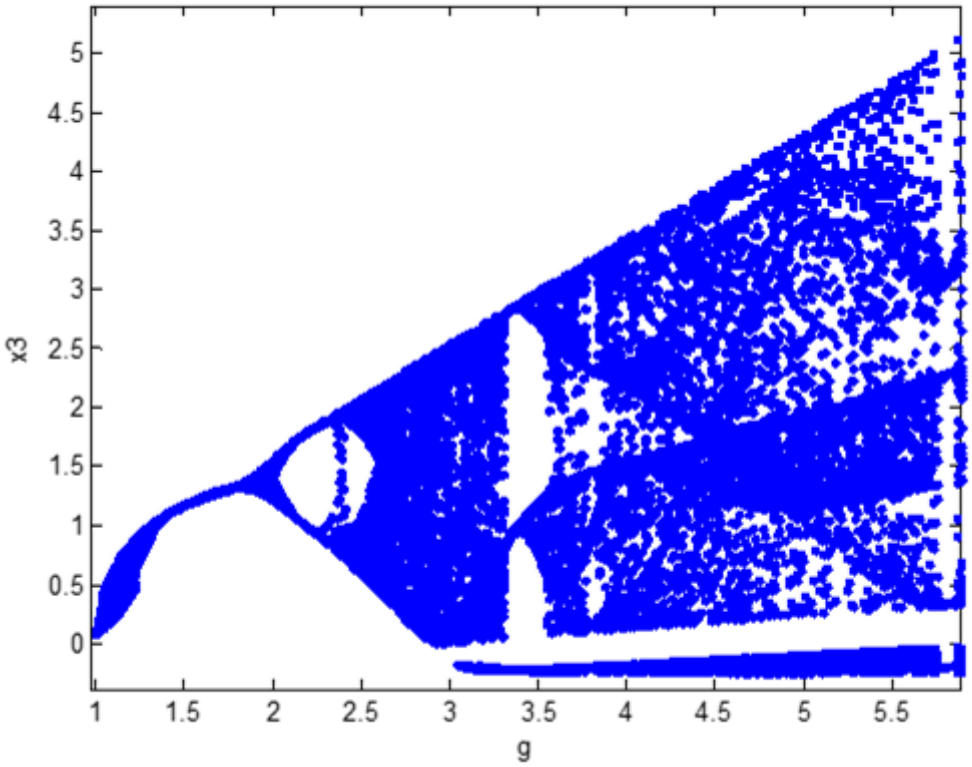


Figure III.13. Diagramme de bifurcations obtenu par la variation du paramètre g

III.4 Conclusion

Dans ce chapitre, nous avons expliqué le principe de fonctionnement de l'oscillateur Colpitts en étudiant les différents comportements de cet oscillateur en fonction de variations de ses paramètres. Ces études ont été mises en évidence à l'aide des simulations sous MATLAB. Nous avons ajusté les paramètres de l'oscillateur Colpitts afin d'obtenir un comportement chaotique.

Conclusion Générale

Nous avons abordé dans ce mémoire l'exploitation de chaos aux transmissions sécurisées ; qui malgré les nombreuses études et les avancées marquées dans ce domaine soulèvent encore de nombreux défis.

Dans le premier chapitre de ce mémoire, nous avons évoqué d'abord quelques notions et définitions théoriques sur les systèmes dynamiques et particulièrement sur les systèmes non linéaires qui sont dits chaotiques, ces systèmes présentent plusieurs caractéristiques dont l'utilisation aux transmissions sécurisées serait intéressante. On peut citer parmi eux le déterminisme qui signifie que ces systèmes régis par des règles non probabilistes. Une autre propriété intéressante, est la sensibilité aux conditions initiales. En effet, un moindre écart ou imprécision dans les conditions initiales engendre des évolutions totalement différentes. Ceci implique l'impossibilité de prédiction à long terme du comportement du système chaotique. Une troisième propriété c'est l'attracteur étrange, qui est un attracteur dont la forme n'est pas une courbe ni une surface et aussi n'est pas une courbe. Par la suite, nous avons défini les outils pour étudier ces systèmes où nous avons défini les exposants de Lyapunov qui ont la tache de vérifier le comportement d'un système dynamique, nous avons défini aussi le diagramme de bifurcation, ce dernier est très important dans l'étude des systèmes chaotique, il nous permet d'observer les différents comportements possibles.

Dans le deuxième chapitre du mémoire, nous avons exposé les objectifs des crypto-systèmes, et après nous avons récapitulé l'état de l'art des techniques utilisées pour injecter l'information dans un système chaotique. La première technique qu'on cite c'est le chiffrement par addition qui est une technique simple à réaliser. La deuxième technique c'est le chiffrement par commutation qui est utilisée principalement pour transmettre un message binaire. La dernière technique que nous avons définie c'est le chiffrement par modulation, cette technique utilise le message (information) pour la modulation de paramètre de l'émetteur chaotique.

Dans le dernier chapitre, nous avons développé un modèle mathématique déduit des équations des équations d'états de l'oscillateur Colpitts qui nous a conduit à un système de trois équations différentielles en fonctions de trois variables d'états et trois paramètres. A travers d'une étude mathématique sous MATLAB, nous avons cherché dans un premier temps à étudier les comportements dynamiques qui peut présenter en fonction de paramètre g. En utilisant MATLAB, nous avons tracé les réponses temporelles et le plan de phase $(y - z)$ pour chaque comportment, et pour vérifier les résultats obtenus nous avons calculé les exposants de Lyapunov, la positivité des deux premiers exposants confirme le comportement hyper chaotique pour $g = 4.46$. Afin de bien visualiser les changements qualitatifs de notre système on a tracé le diagramme de bifurcation en fonction de variation de paramètre g.

Ce travail peut être amélioré par l'évolution de la fréquence d'oscillation vers les fréquences élevées, il suffit pour cela de fixer les paramètres chaotiques $g = 4.46$, $Q = 1.38$, $k = 0.5$ et d'extraire les nouvelles valeurs de L_1, C_1, C_2.

Bibliographie

[1] M. NOURINE, Etude des communications optiques sécurisées par chaos intégrant une clé physique via un composant électro-optique dédié, *Thèse de doctorat, Université de Franche-Comté, 2010.*

[2] N. W. ABDERRAHIM, Etude et conception d'un modèle chaotique dédié aux transmissions chiffrés, *Thèse de doctorat, Université Abou Bakr Belkaid Tlemcen, 2014.*

[3] C. BENHABIB, Etude d'un système chaotique pour la sécurisation des communications optiques, *Mèmoire de master, Universitè Abou Bakr Belkaid Tlemcen , 2014.*

[4] O. MEGHERBI, Etude et rèalisation d'un système sècurisè a base de système chaotique, *Mèmoire de magister, Universitè Mouloud Mammeri, Tizi-ouzou, 2013.*

[5] D. RUELLE & F. TAKENS , On the nature of turbulence, *communications of mathematical physics 20(1971),p 167-192.*

[6] A. R. KIHAL, Système chaotique pour la transmission sècurisèe de donnèe, *Mèmoire de magister, Universitè Mohammed Khider, Biskra, 2013.*

[7] E. OTT, Chaos in dynamical systems, *2nd edition, Cambridge University Press, 2002.*

[8] D. V. HYUYEN & C.DELCARTE, Bifurications et chaos, *Ellipses editions marketing S.A, 2000.*

[9] M. L'HERNAULT-ZANGANEH, Faisabilitè d'un système d'èmission-rèception analogique pour les communications sècurisèes par le chaos, Thèse de Doctorat ; Universitè de Paris 6,2007.

[10] R. L. DEVANEY, An introduction to chaotic dynamical systems, *Westview Press, 2003.*

[11] S. N. RASBAND, Chaotic dynamics of non linear systems, *Wiley Professional, 1997.*

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

[13] T. HAMAIZIA, Système dynamique et chaos "application à l'optimisation a l'aide d'algorithme chaotique", *Thèse de doctorat, Universitè de Constantine 1, 2013.*

[14] Z. AMRANI ,S. CHITROUB et A. BOUKHARI, Cryptage d'images par chiffrement de vigenèrebasè sur le mixage des cartes chaotiques, *4th International conference on computer integrated manu facturing CIP ' 2007 03-04 November 2007*

[15] M. KOUADRI, Tests de validation pour les crypto-systèmes chaotiques, *Mèmoire de magister, Universitè Mohammed Boudiaf, Oran, 2013.*

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

[17] G. S. VERNAM, Cipher printing telegraph systems for secrets wire and telegraph communications, *J.Amer.Inst.Elec.Eng. 55(1926), p109.*

[18] E. CHERRIER, Estimation de l'ètat st des entrèes inconnues pour une classe de systèmes non linèaires, *Thèse de doctorat, Instiut National Polytechnique de Lorraine, 2006.*

[19] K. M. CUOMO &A. V. OPPENHEIM, Circuit implementation of synchronized chaos with applicatons to communications, *Phy, Rev, Lett.71(1993), p.65-68.*

[20] J. M. CRUZ & L. O. CHUA, A CMOSIC non linear resistor for chua's circuit, *IEEE transactions on circuits and systems I 39(1992).*

[21] A. V. OPPENHEIM, G. W. WORNELL, S. H. ISABELLE & K. M. CUOMO, Signal processing in the context of chaotic signals, *IEEE ICASSP(1992).p.IV-117-IV-120.*

[22] K. M. SHORT, Steps toward unmasking secure communications, *INT.J.of bifurcation and chaos4(1994),p.959-977.*

[23] N. CORRON, D. HAHS, A new approch to communication using chaotic signals, *IEEE Transactions on circuits and systems, Vol .44,pp.373-382, 1997.*

[24] H. DEDIEU, M. P. KENNEDY and M. HASLER, New block chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing chua's circuits, *IEEE Transactions on circuits and systems, circuits and systems II :Analog and digital signal processing,Vol.40,pp.634-642,1993.*

[25] M. FLIESS , C. JOIN, M. MBOUP & A. SEDOGLAVIC, Estimation des dèrivèes d'un signal multidimensionnel avec applications aux images et aux vidèos, *20ème colloque sur le traitement du signal et de l'image GRETSI , Belgique (2005).*

[26] H. HAMID, Inversion à gauche des systèmes dynamiques hybrides chaotiques, *Thèse de doctorat, Universitè Mouloud Mameri, Tizi-ouzou, 2001.*

[27] M. HASLER, Electrical circuits whith chaotic behavior, *Proc. IEEE 75 (1987), p.1009-1021.*

[28] T. MATSUMOTO , A chaotic attractor from chua's circuit, *IEEE Transcir. Sys. CAS-31(1984), p.1055-1058.*

[29] T. MATSUMOTO , Chaos in electronic circuits, *Proc. IEEE 75 (1987), p. 1033-1057.*

[30] T. MATSUMOTO, L. O. CHUA & S. TANKA, Simplest chaotic nonautonomous circuit, *Physical Review A 30 (1984), p.1155-1157.*

[31] T. MATSUMOTO, M. KOMURO, H. KOKUBU & R. TOKUNAGA , Bifurcation sights sounds and mathematics, *Ed Springer-Verlag Tokyo, 1993.*

[32] J. M. OGORAZTEK, Chaos and complexity in nonlinear electronic circuits, *World Scientific, Singapore, Series A, Vol.22,1997.*

[33] G. Q. ZHONG & F. AYROM, Experimental confirmation of chaos from chua's circuit, *Int. J. Circuit theory Appl.13 (1985), p.93-98.*

[34] M. ABDELFATTAH, Etude et Rèalisaion d'un système chaotique basè sur le circuit de Chua, Mèmoire de Master Professionnel, Universitè Mouloud Mammer, Tizi-Ouzou, 2014.

[35] M. P. KENNEDY, Robust OpAmp realization of chua's circuit, Frequenz 46 (1992), p.66-80.

[36] M. P. KENNEDY, Chaos in the Colpitts oscillator, *IEEE Trans. On circuits and systems-I 41(1994),p.771-774.*

[37] O. DEFEO & G. M. MAGGIO, Bifurcation phenomena in the colpitts oscilltor: A robustness analysis, *IEEE International symposiumon circuits and systems II (200), p 469-472*.

[38] O. DEFEO , G. M. MAGGIO & M. P. KENNEDY, The Colpitts oscillator: Families of periodic solutions and their bifurcations, *Int.J. Bifurcation and Chaos (2000).*

[39] G. M. MAGGIO ,M. DI BERNARDO & M. P. KENNEDY, Nonsmooth bifurcations in piecewise-linear model of the colpitts oscillator, *IEEE Transactions on circuits and systems-I: Fundamental theory and apllications 47 (2000),p.1160-1177*.

[40] G. M. MAGGIO & O. D. FEO, Nonlinear analysis of the Colpitts Oscillator and applications to Design, *IEEE Transactions on circuits and systems-I: Fundamental Theory and Applications 46 (1999).*

[41] G. M. MAGGIO ,C. KENNEDY & M .P. KENNEDY, Experimental manifestations of chaos in the colpitts oscillator, *Proc. NDES'96, Seville, Spain (1997),p.275-278*.

[42] G. M. MAGGIO & M. P. KENNEDY, Classification of steady state behavior of the colpitts oscillator, *in Proceedings of ICECS, 1999, p.811-814*.

[43] N. MAXIMOV, A. PANAS & S. STARKOV, Chaotic oscillators design with preassigned spectral carateristics, *ECCTD'01- European Conference on circuit theory and design (2001).*

[44] G. MYKOLAITIS, A. TAMASEVICIUS & S. BUMELIENE, Experimental demonstration of chaos from Colpitts oscillator in VHF and UHF ranges, *Electronics letters 40 (2004).*

[45] C. WEGENER ,G. M. MAGGIO & M. P. KENNEDY, Experimental manifestationof chaos I the Colpitts oscillator, *Proc. ISSC'97, Derry, Ireland (1996), p.235-242.*

[46] A. TAMASEVICIUS, G. MYKOLAITIS, S. BUMELIENE, A. CENYS, A. ANAGNOSTOPOULOS & E.LINDBERG, Two stage chaotic Colpitts oscillator, *Electronic letters 37(2001).*

[47] C. WEGENER & M. P. KENNEDY, RF chaotic Colpitts oscillator, *Proc. Of NDES'95,p.255-258.*

[48] V. RUBEZIC & R. OSTOJIC, Synchronisation of chaotic Colpitts oscilators with application to binary communications, *IEEE(1999).*

[49] M. L'HERNAULT, J. P. BARBOT & A. OUSLIMANI, Rèalisation èlectronique d'un observateur à mode glissants: application àa la cryptographie chaotique, *CIFA 2006, Bordeaux, France (2006).*

[50] M. L'HERNAULT, J. P. BARBOT & A. OUSLIMANI, Sliding mode observer for a chaotic communication system:experimental results, *1st IFAC conference on analysis and control of chaotic systems, Reims, France (2006).*

[51] M. L'HERNAULT, L. BOUTAT-BADDAS , J. P. BARBOT & A. OUSLIMANI, Chaotic frequency modulation in cryptography, *in International Workshop on Electronics and Systems Analysis, 2004, Bilbao, Spain.*

[52] A. S. SEDRA & K. C. SMITH, Microelectronic circuits, *Oxford, 1989.*

[53] Maryam L'Hernault, Achour Ouslimani, Jean-Pierre Barbot. Conception et réalisation d'un observateurà modes glissants pour un oscillateur de type Colpitts chaotique. *Alexandre Vautier, Sylvie Saget. MajecSTIC 2005 : Manifestation des Jeunes Chercheurs francophones dans les domaines des STIC, Nov 2005, Rennes, pp.232-237, 2005.*

[54] A. WOLF, J. B. SWIFT, H. L. SWINNEY & J. A. VASTANO, "Determining Lyapunov Exponents from a Time Series," Physica D, Vol. 16, pp. 285-317, 1985

Annexe

Programme MATLAB pour tracer le diagramme de bifurcation

```
%l'algorithme pour tracer le diagramme de bifurcation
clear all
close all
clc
for g=1:0.01:6 ;%l'intervalle de g
paramètre=[g;1.38;0.5];%les paramètres g,q,k
x0=[10;1;0];%les conditions initiales
dt=0.001;
tspan=dt:dt:300;
options=odeset('RelTol',1e-12,'AbsTol',1e-12*ones(1,3));
[t,x]=ode45(@(t,x)colpitts(t,x,paramètre),tspan,x0,options);%la
fonction qui résoudre le système des équations différentielles
for i=50000:299999
    if((x(i,3)>x(i-1,3))&&(x(i,3)>x(i+1,3)))
       plot(g,x(i,3),'.');xlabel('g');ylabel('x3');
       hold on
    end
end
end
```

```
%la fonction colpitts
function dx=colpitts(t,x,paramètre)
% x(1)=x;
%x(2)=y ;
%x(3)=z;
% paramètre(1)=g;
%paramètre(2)=q;
%paramètre(3)=k;
dx=[
    (paramètre(1)/( paramètre(2)*(1- paramètre(3))))*( exp(x(2)) +1
+x(3));
(paramètre(1)/( paramètre(2)* paramètre(3)))*x(3);
(-(paramètre(2)*(3)*(1- paramètre (3)))/( paramètre (1)))*
(x(1)+x(2))- (1/ paramètre(2))*x(3)
];
```

Résumé

Nous avons traité dans ce travail de mémoire les systèmes chaotiques qui sont des systèmes caractérisés par la déterminisme, la non linéarité et une extrême sensibilité aux conditions initiales, ainsi que des outils disponibles pour faciliter l'étude de ces systèmes comme les exposants de Lyapunov, l'espace des phases et le diagramme de bifurcation ce dernier qui nous montre les différents comportements possible d'un système dynamiques passant de comportement périodique jusqu'à le comportement chaotique. L'étude des systèmes chaotiques est destinée à leur utilisation pour sécurisation des transmissions, c'est pour ce raison nous avons expliqué les objectifs des crypto-systèmes et les différentes techniques de cryptographie chaotiques.

L'objectif principal de ce mémoire est la conception d'un générateur chaotique destiné aux transmissions sécurisées, nous avons donc choisi l'oscillateur de Colpitts pour cette tache ce choix peut être jugé par les avantages offrit par cet oscillateur, l'un de ces avantages c'est la simplicité de sa structure. Nous avons expliqué le principe de fonctionnement et déterminé la condition et la fréquence d'oscillation de cet oscillateur et aussi nous avons écrit et développé le modèle mathématique de l'oscillateur de Colpitts en étudiant ses différents comportements par la variation de ses paramètres, ces études est mise en évidence sous le simulateur MATLAB où nous avons calculé les exposants de Lyapunov qui justifient le comportement hyper chaotique pour certaines valeurs des paramètres, tracé les réponses temporelles pour les différents comportements et le diagramme de bifurcation de l'oscillateur de Colpitts.

Mots clés : *système chaotique, exposant de Lyapunov, bifurcation, attracteur étrange, transmission sécurisée, cryptographie, l'oscillateur de Colpitts, MATLAB.*

Abstract

In this work of thesis, we have treated the chaotic systems which are systems characterized by the determinism, the non-linearity and an extreme sensitivity to the initial conditions, as well as tools available to facilitate the study of these systems as the exponents of Lyapunov, the phase space and the bifurcation diagram which shows us the different possible behaviors of a dynamic system from periodic behavior to chaotic behavior. The study of chaotic systems is intended for their use for securing transmissions, which is why we explained the objectives of crypto-systems and the different chaotic cryptographic techniques.

The main objective of this thesis, is the design of a chaotic generator for secure transmissions, so we chose the Colpitts oscillator for this task this choice can be judged by the advantages offered by this oscillator, one of these advantages is the simplicity of its structure. We have explained the operating principle and determined the oscillator's condition and frequency of oscillation and also we have written and developed the mathematical model of the Colpitts oscillator by studying its different behaviors by the variation of its parameters, these studies is highlighted under the MATLAB simulator where we calculated the Lyapunov exponents that justify the hyper chaotic behavior for some parameter values, plot the temporal responses for the different behaviors and the bifurcation diagram of the Colpitts oscillator.

Keywords : *chaotic system, Lyapunov exponent, bifurcation, strange attractor, secure transmission, cryptography, Colpitts oscillator, MATLAB.*

ملخـــص

خلال هذا العمل المتمثل في مذكرة التخرج، قمنا بالتطرق الى الأنظمة الفوضوية التي تتميز بالحتمية، اللا خطية والحساسية الشديدة لظروف الأولية وكذا تم التطرق الى الوسائل المتاحة من اجل تسهيل دراسة هاته الأنظمة مثل أسس ليابونوف، مساحة الطور ومخطط التشعب هذا الأخير الذي يظهر لنا مختلف سلوكيات المحتملة لنظام ديناميكي من السلوك الدوري الى السلوك الفوضوي دراسة هاته الأنظمة راجع لاستعمالها في تامين الاتصالات، ولهذا السبب قمنا بشرح اهداف أنظمة التشفير ومختلف تقنيات التشفير الفوضوي

الهدف الرئيسي لهاته المذكرة هو تصميم مولد فوضوي من اجل تامين الاتصالات، ولهذا قمنا باختيار المذبذب Colpitts الاختيار يبرر بانه يمتلك الكثير من المزايا التي تتمثل احداهن في بساطة هيكله، واوضحنا مبدا التشغيل وحددنا شرط وتواتر تذبذبه من خلال دراسة سلوكياته المختلفة ودلك بتغيير قيم عناصره. هاته Colpitts وأيضا قمنا بكتابة وتطوير النموذج الرياضياتي للمذبذب الدراسات تمت محاكاتها بواسطة ماطلاب اين قمنا بحساب أسس ليابونوف التي تبرر السلوك الفوضوي المفرط للمذبذب وهذا من اجل بعض قيم عناصره كما قمنا برسم الاستجابات الزمنية لسلوكياته المختلفة ومخطط تشعبه

الكلمات المفتاحية: الأنظمة الفوضوية، أسس ليابونوف، التشعب، جاذب غريب، الاتصالات المؤمنة، التشفير، مذبذبColpitts ماطلاب.