

**République Algérienne Démocratique et Populaire**  
**Ministère de l'Enseignement Supérieur et de la Recherche Scientifique**  
**Université Mouloud MAMMERY, Tizi-Ouzou**



**Faculté de Génie Electrique et d'Informatique**  
**Département d'Automatique**

**Mémoire de Fin d'Etudes**

En vue de l'obtention du diplôme

*Master académique en automatique*  
*Option commande des systèmes*

***Thème***

***Réalisation d'une transmission  
sécurisée de données par chaos***

**Proposé et dirigé par :**

M. Kara

M. Hamiche

Soutenu le : 17 / 10 /2012

**Présenté par :**

M<sup>elle</sup> Meghezzi Rabia

M. Larbi Mohand Saïd

***Promotion 2012***

## *Remerciements*

*Nous remercions notre créateur tout puissant pour nous avoir donné la force et le courage pour accomplir ce travail.*

*Nos vœux vont d'abord à nos promoteurs M. KARA et M. HAMICHE qui ont suivi l'évolution de notre projet, et pour leur aide précieuse, nous tenons à leur exprimer notre profonde gratitude et reconnaissance.*

*Nous tenons à remercier chaleureusement les membres du jury de nous faire l'honneur d'accepter d'évaluer ce projet.*

*Nos remerciements vont également à tous les Enseignants du Département Automatique et M. BERCHICHE le responsable du laboratoire Maquette qui nous a orienté dans le développement de notre maquette, ainsi que nos camarade M'hena et Samir.*

*Enfin, que tous ceux, qui de près ou de loin, ont participé à l'élaboration de ce travail trouvent ici l'expression de nos meilleurs remerciements.*

## Sommaire

Introduction générale.....	1
Chapitre I : Généralités sur les systèmes chaotiques	
I.1 Introduction.....	3
I.2 Historique de la théorie du chaos.....	3
I.3 Notions de systèmes dynamiques .....	5
I.3.1 Définition d'un système dynamique.....	6
a. En temps discret.....	6
b. En temps continu.....	7
I.1.2 Autonomie.....	7
I.3.3 Déterminisme.....	8
I.3.4 Trajectoire et flot.....	8
I.3.5 Espace des phases.....	8
I.3.7 Attracteurs.....	9
I.3.7. Comportement des systèmes dynamiques non linéaires .....	10
a. Point d'équilibre.....	10
b. Régime périodique.....	11
c. Régime quasi-périodique.....	12
d. Régime chaotique.....	13
I.4 Définition et caractéristiques des systèmes chaotiques.....	14
I.4.1 Définition d'un système chaotique.....	14
I.4.2 Caractéristiques des systèmes chaotiques.....	14
a. La Sensibilité aux conditions initiales.....	14
b. L'attracteur étrange .....	16
c. L'exposant de Lyapunov .....	20
d. Le déterminisme et l'imprédictibilité.....	23

e. L'aspect aléatoire.....	24
f. Le spectre de puissance .....	25
g. La fonction d'autocorrélation.....	26
I.5 Les sections de Poincaré .....	27
I.6 Notions bifurcation et transition vers le chaos .....	29
I.7 Conclusion.....	33

## Chapitre II synchronisation du chaos et transmission sécurisée

II.1 Synchronisation du chaos.....	35
II.1.1 Introduction.....	35
II.1.2 La synchronisation du chaos.....	35
II.1.2.1 Positionnement du problème.....	36
II. 1.2.2 Techniques de synchronisation du chaos.....	38
Synchronisation à l'aide d'observateur .....	39
a. Observabilité des systèmes.....	40
b. Observateur de Luenberger .....	42
c. Observateur à grand gain .....	43
d. Commande par retour d'état.....	45
II.2 Généralité sur la transmission sécurisée.....	49
II.2.1 Introduction à la communication sécurisée.....	49
a. Cryptologie.....	49
b. Cryptographie par chaos.....	51
II.2.2 Technique de cryptage.....	51
a.Cryptage par addition.....	51
b.Cryptageparinclusion.....	52
c.Cryptage par modulation.....	53
II.2.3 Transmission à deux voies.....	53
II.2.4 Conclusion.....	54

## Chapitre III : synchronisation du système de Qi

III.1 Introduction.....	55
III.2 Emetteur.....	55
III.2.1 Oscillateur électronique.....	55
III.2.2 Structure générale d'un oscillateur.....	56
III.2.3 Système hyperchaotique de Qi .....	57
III.2.3.1 Caractérisation du chaos dans le système de Qi.....	57
a.    Exposants de Lyapunov.....	58
b.    Spectre de puissance.....	58
c.    Schéma électronique du système.....	59
d.    Etude du montage électrique.....	60
III.2.4 Simulation sous Matlab.....	63
a.    Visualisation des états.....	64
b.    Visualisation des attracteurs.....	66
c.    Visualisation des attracteurs en trois dimension.....	67
III.3 Récepteur.....	68
III.3.1 Condition du rang d'observabilité .....	68
III.3.2 Synchronisation du système de Qi .....	70
III.3.3 Simulation sous Matlab.....	76
a.    Visualisation des états estimé.....	77
b.    Visualisation des écarts entre les états des deux systèmes.....	79
c.    Récupération du message.....	80
III.4 Conclusion.....	81

## Chapitre IV : Réalisation électronique

IV.1 Introduction.....	82
IV.2 Simulation sous le logiciel de traitement de texte pour schémas électriques.....	82

IV.3 Modification de l'oscillateur de Qi.....	89
IV.4 Etapes de réalisation d'un circuit imprim.....	90
IV.4.1 L'insolation.....	93
IV.4.2 La révélation.....	93
IV.4.3 La gravure.....	93
IV.4.4 Perçage.....	94
IV.4.5 Implantation des composants.....	94
IV.4.6 La soudure.....	94
IV.5 Résultats expérimentaux.....	96
IV.6 conclusion.....	100
Conclusion générale.....	101

Annexe A : Datasheet des composants électriques

Annexe B : Schémas de Simulation sur Matlab

## Notations

$\mathbb{R}$ : Ensemble des nombres réels.

$\mathbb{R}^+$ : Ensemble des nombres positifs.

$\mathbb{R}^n$ : Espace vectorielles de dimension  $n$ .

$\mathbb{R}^P$ : Espace vectorielles de dimension  $P$ .

$\mathbb{N}$ : Ensemble des nombres naturels.

$\mathbb{N}^*$ : Ensemble des entiers naturels non nuls.

$\mathbb{Z}^+$ : Ensemble des nombres relatifs (entiers négatifs et positifs)

$L_f h(x) = \sum_{i=1}^n f_i(x) \frac{\partial h}{\partial x_i}(x)$ : la dérivée de  $h$  long de  $f$ .

$L_f^i h$ :  $i$ ème dérivée du vecteur d'état.

$dL_f^i h$ : Le différentiel de  $L_f^i h$ .

$\dot{X}$ : Dérivée du vecteur d'état  $X$ .

$\lambda_i$ : Variation d'exposant de Lyapunov selon  $i$ .

$\hat{x}$ : Vecteur  $x$  estimé.

$\dot{\hat{x}}$ : Dérivée du vecteur  $x$  estimé.

$\|x\|$ : Norme euclidienne du vecteur  $x$ .

## Introduction générale

La sécurisation de la chaîne de transmission devient de plus en plus nécessaire avec l'évolution des communications en termes de nombre d'utilisateurs et nature d'information à transmettre. Actuellement, tout système de communication performant nécessite un système de sécurisation afin de le protéger envers les attaques possibles. Pour cela, de nouvelles méthodes de cryptage sont développées. Le cryptage des informations est maintenant utilisé pour interdire l'accès ou la modification des informations sensibles et garantir la confidentialité dans les communications. Certaines de ces nouvelles méthodes utilisent le chaos dans les systèmes de transmission.

La théorie du chaos déjà entrevue par Hadamard et Poincaré au début du XXe siècle a été définie à partir des années soixante par Lorenz et plusieurs autres scientifiques. On appelle chaotiques, des systèmes dynamiques, dépendants de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales qui les rend imprédictibles à long terme et leur donne un aspect aléatoire. En effet, un signal chaotique se présente comme un bruit blanc, mais ce qui différencie le signal chaotique du bruit blanc est le déterminisme.

Plusieurs scientifiques se sont intéressés de près à la théorie du chaos et ont défini ses caractéristiques ainsi que des méthodes de contrôle du chaos, comme l'élaboration de systèmes chaotiques ayant une dynamique plus complexe appelés «système hyperchaotique ». Cependant, l'exploitation du chaos n'a été rendue possible que depuis la synchronisation de deux systèmes chaotiques établie pour la première fois par Pecora et Carroll. Cette découverte a ouvert la porte à l'utilisation du chaos dans plusieurs domaines, notamment la sécurisation des transmissions de données.

Dans ce travail, nous utiliserons le chaos pour chiffrer une information dans une transmission sécurisée que nous allons concevoir théoriquement et réaliser sur une carte électronique. Pour ce faire, nous utiliserons un système hyperchaotique appelé système de Qi. Deux systèmes de Qi identiques seront donc utilisés comme émetteur et récepteur de signaux chaotiques. L'émetteur étant un générateur de signaux chaotiques et le récepteur sera un circuit identique à l'émetteur, les deux systèmes seront synchronisés à l'aide d'observateur afin de récupérer en sortie le signal chaotique généré par l'émetteur. Pour sécuriser un message à l'aide de ce système de transmission, nous allons noyer ce message (signal sinusoïdal dans notre cas) dans le signal chaotique généré par l'émetteur, en l'additionnant à un des états de l'émetteur. Le signal reçu par le récepteur sera donc un signal chaotique dans

lequel le message est caché. L'extraction du message se fera alors par sa soustraction du signal chaotique.

Le chapitre I est une introduction à la théorie du chaos, partant de ses différentes propriétés et de son comportement spécifique.

Dans le chapitre II nous allons, dans une première partie, étudier la technique de synchronisation que nous utiliseront pour concevoir notre transmission, qui se fera à l'aide d'observateur. En deuxième partie nous allons donner des généralités sur la transmission sécurisée et les méthodes de cryptage pouvant s'appliquer à notre système.

Le chapitre III est consacré à l'étude théorique du système hyperchaotique de Qi, puis la conception du récepteur et l'insertion du message puis son extraction. Le système de transmission sécurisée obtenu sera simulé sous Matlab pour anticiper la possibilité du fonctionnement de la réalisation pratique.

Dans le quatrième chapitre, nous allons réaliser en pratique la transmission du système simulé dans le chapitre III sur deux cartes électroniques, émetteur et récepteur.

Nous terminons par une conclusion générale et perspectives.

**« I.1 Introduction**

Nos ancêtres ont découvert il y a fort longtemps que le futur était difficile à prédire, et que des petites causes pouvaient avoir de grands effets. Ce qui est relativement neuf, c'est la démonstration que pour certains systèmes déterministes, une petite variation de condition initiale peut changer complètement le comportement du système, ce qui rend ces systèmes bien qu'ils soient déterministes, imprédictibles à long terme et à aspect désordonné et aléatoire. On appelle ce phénomène : *la théorie du chaos* ou encore le *chaos déterministe* pour le distinguer des phénomènes aléatoires.

Découvert par Henri Poincaré et médiatisé par Lorenz sous le nom d'*effet papillon*, le chaos déterministe avait attiré l'attention de scientifiques de divers domaines et avait fait l'objet d'études approfondies, qui ont mis au point des méthodes de caractérisation du comportement chaotique des systèmes ainsi que des perspectives d'exploitation de ce type de comportement.

Dans ce chapitre nous allons donner la chronologie de la découverte du chaos, une première façon d'explicitier le comportement chaotique. Ensuite, nous allons donner ses caractéristiques et méthodes d'études, illustrés par simulation de deux modèles de systèmes chaotiques, sur Matlab.

**I.2 Historique de la théorie du chaos**

La signification scientifique du chaos n'a été citée qu'à la fin du XIXe siècle par Henri Poincaré (1854-1912), car depuis les travaux d'Isaac Newton (1642 - 1727), la Science était dominée par le déterminisme. Moyennant la connaissance des conditions initiales d'un système donné, les scientifiques pensaient pouvoir prédire complètement et précisément le futur du système en question. Un siècle après Newton, Pierre-Simon Laplace (1749-1827) définit le sens absolu du déterminisme, il affirmait que l'état présent de l'Univers permettait en principe de prédire complètement son futur. Mais Poincaré allait donner tort à Laplace, il avait en effet montré que, malgré un caractère déterministe, le problème des trois corps en mécanique céleste (exemple Terre-Lune-Soleil) ne pouvait pas donner lieu à la prédiction.

On a ainsi pu tester la stabilité de ce système en comparant les trajectoires suivies par un des corps à partir de deux positions initiales très proches : ces trajectoires restent proches l'une de l'autre à court terme et on peut donc prédire les éclipses, mais elles deviennent complètement différentes à long terme, une toute petite différence initiale a donc produit un effet considérable. C'est dans cette extrême sensibilité aux conditions initiales que réside l'origine de l'imprédictibilité du chaos déterministe. Poincaré avait remarqué cet effet puisqu'il a écrit : "*Une cause très petite, qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir et alors nous disons que cet effet est dû au hasard.*". [1]

L'idée que les petites causes peuvent avoir quelquefois de grands effets a été notée par les historiens et autres depuis longtemps, par exemple dans la fameuse expression "*pour manque d'un clou un royaume a été perdu*". En 1860 James Maxwell a discuté comment les collisions entre molécules dures de la sphère pourraient mener à l'amplification progressive du rendement aléatoire microscopique dans les gaz.

En 1898 Jacques Hadamard a noté la divergence générale de trajectoires dans l'espace, et Pierre Duhem a discuté la signification générale possible de ceci en 1908, il a donné le résultat qu'on ne peut jamais atteindre une prédiction complète du système chaotique, et cela à cause des conditions initiales aléatoires nécessairement présentes dans le théorème de Hadamard.

En 1961, Edward Lorenz, météorologue et professeur de mathématiques au MIT (Massachusetts Institut of Technology) observa par hasard le phénomène qui s'appellera plus tard la théorie du chaos ou le chaos déterministe, à la suite de calculs visant à prévoir les phénomènes météorologiques. Ces prévisions nécessitaient un grand nombre de calculs d'équations différentielles complexes à très grand nombre de variables impossible à faire à la main, il a utilisé alors un ordinateur, son Royal Mcbee LGP-300 qui est entré dans l'histoire de la théorie du chaos, et qui a fait de Lorenz le père officiel de cette théorie puisque les calculs des systèmes chaotiques régissant ces phénomènes étaient difficiles à comprendre et à simuler sans ordinateur. Après plusieurs heures de calculs, Lorenz avait obtenu une série de résultats et a décidé de repasser une deuxième fois ces données dans l'ordinateur pour s'assurer du résultat. Pour gagner du temps, il avait entré les variables avec trois chiffres après la virgule au lieu de six, il pensait qu'une faible variation dans les variables à la base d'un

calcul aurait une incidence du même ordre de grandeur sur le résultat final, mais à sa grande surprise les résultats étaient totalement différents de la première série. Il venait de découvrir le comportement chaotique d'un système non linéaire ; soit, d'infimes différences dans les conditions initiales d'un système déterministe entraîneraient des résultats complètement différents. Pour mieux comprendre l'importance de cette sensibilité aux conditions initiales Lorenz a eu recours à une métaphore qui contribua au succès médiatique de la théorie du chaos : « *le simple battement d'aile de papillon au Brésil pourrait déclencher une tornade au Texas* » [2].

En 1971, le physicien belge David Ruelle et le mathématicien néerlandais Floris Takens ont également publié un article dans lequel ils avaient analysé les états finals des modèles mathématiques de systèmes qui dissipent une partie de leur énergie en chaleur. Les résultats ont montré que l'ensemble des états finals d'un tel système a une nature fractale : c'est un attracteur étrange. Le mouvement sur un tel attracteur dépend énormément des conditions initiales ; c'est la propriété appelée effet papillon par Lorenz. En appelant bifurcation le point où une faible variation d'un paramètre induit un changement qualitatif de la solution d'une équation, Ruelle et Takens ont montré qu'un tout petit nombre de bifurcations suffit à produire un comportement chaotique et donc à engendrer la turbulence. Quatre ans plus tard, l'étude expérimentale d'un fluide en rotation par les physiciens Jerry Gollub et Harry Swinney, du City College de New York, montrait que l'apparition de la turbulence suit bien dans ce cas la description de Ruelle et Takens mais le mot chaos n'a pas encore été utilisé ; il était introduit par le mathématicien Yorke en 1975 et la théorie du chaos déterministe sera alors appliquée à l'étude de phénomènes dans divers domaines scientifiques, de la physique à la biologie.

### **I.3 Notions de systèmes dynamiques [3] [4]**

Le chaos est défini généralement comme un comportement particulier d'un système dynamique déterministe non-linéaire. Du point de vue mathématique la notion générale de système dynamique est défini à partir d'un ensemble de variables qui forment le vecteur d'état. Ces variables ont la propriété de caractériser complètement l'état instantané du système dynamique. En associant en plus un système de coordonnées on obtient l'espace d'état qui est appelé également l'espace des phases. Conjointement avec l'espace d'état un système

dynamique est défini aussi par une loi d'évolution, généralement désignée par *dynamique*, qui caractérise l'évolution de l'état du système en temps. La notion de déterminisme provient du fait que le système considéré est complètement caractérisé par son état initial et sa dynamique.

### I.3.1 Définition d'un système dynamique

On appelle système dynamique en temps continu, tout système décrit par un système d'équations différentielles alors qu'en temps discret on parle d'équations aux différences finies.

#### a. En temps continu

Comme il a été précisé, le système dynamique est représenté dans ce cas par des équations différentielles :

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

Où :

$x(t) = [x_1(t) \ x_2(t) \ \dots \ x_n(t)]^T$  est le vecteur d'état du système.

$x_1(t) \ x_2(t) \ \dots \ x_n(t)$  sont les états du système.

$n$  est la dimension appelée aussi degré de liberté.

$u \in \mathbb{R}^p$  représente l'entrée du système et  $t$  la variable temporelle.

$x_0$  l'état du système à l'instant initial  $t_0$ .

$f: \mathbb{R}^+ \times \mathbb{R}^n \times \mathbb{R}^p \rightarrow \mathbb{R}^n$  est une fonction non linéaire désignant un champ de vecteurs.

$h: \mathbb{R}^+ \times \mathbb{R}^n \times \mathbb{R}^p \rightarrow \mathbb{R}^p$  une fonction éventuellement non linéaire qui désigne le vecteur de sortie.

- Si le système ne dépend pas de l'entrée l'équation devient alors :

$$\dot{x} = f(t, x(t)) \quad x(t_0) = x_0 \quad (I.2)$$

### b. En temps discret

Dans ce cas le système est représenté par des équations aux différences finies, avec le modèle général suivant :

$$\begin{cases} x(k+1) = G(k, x(k), u(k)) \\ y(k+1) = h(k, x(k), u(k)) \end{cases} \quad x(k_0) = x_0 \quad (I.1)$$

Où  $G: \mathbb{Z}^+ \times \mathbb{R}^n \times \mathbb{R}^p \rightarrow \mathbb{R}^n$  désigne la dynamique du système en temps discret.  $x(k)$  le ve  $x_0$  est l'état du système à l'instant initial  $k_0$ .

### I.1.2 Autonomie

Un système dynamique non linéaire est dit *autonome* lorsqu'il ne dépend pas explicitement du temps. Un système autonome est donné ci-dessous :

$$\dot{x} = f(x) \quad (I.4)$$

Où  $x \in \mathbb{R}^n$  est un système autonome et indépendant du temps initial, alors qu'un système non autonome ne l'est pas. Dans un système autonome, tout instant peut être considéré comme instant initial, et tout état  $x(t)$  du système peut être considéré comme un état initial.

### I.3.3 Déterminisme

Soit  $D$  l'ensemble des conditions initiales du système (I.4), et soit  $x_0 \in D$ , si pour tout  $x_0$  il existe une solution  $\varphi(t, x_0)$  et que cette solution est unique, alors le système est *déterministe*.

### I.3.4 Trajectoire et flot

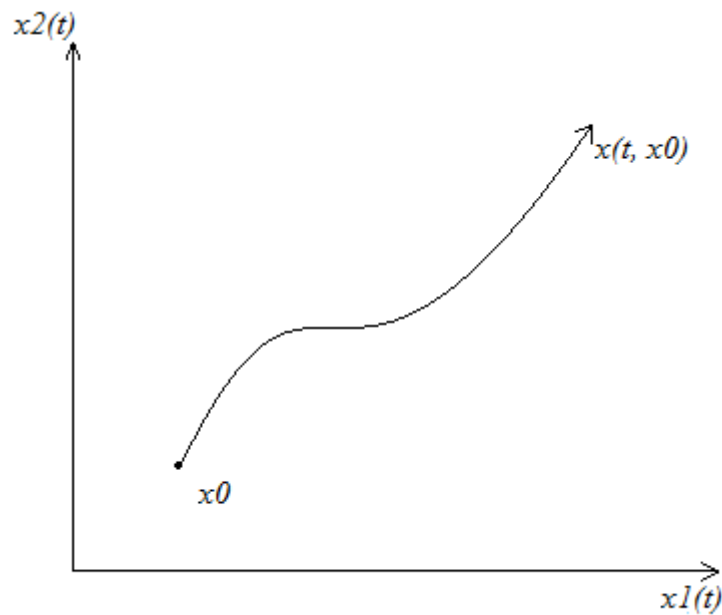
Pour chaque  $x_0$  fixé,  $t \rightarrow \varphi(t, x_0) = x(t, x_0)$  est une solution de l'équation différentielle (I.4).

Le chemin parcouru par le système est appelé *trajectoire de phase* ou *orbite du système*, et l'ensemble des trajectoires est appelé *flot*.

### I.3.5 Espace des phases (d'état) [3]

Il n'est toujours pas possible de déterminer une solution analytique exacte des équations différentielles non linéaires, cependant il est utile de déterminer les évolutions possibles à long terme ou d'avoir une vue d'ensemble des comportements dynamiques. Pour remédier à ce problème Poincaré a pensé à une représentation géométrique du système dans laquelle il élimine le temps, appelée l'espace des phases qui est un espace à 2 ou 3 dimensions dans lequel chaque coordonnée de l'espace correspond à une variable d'état du système. Dans le cas où  $n=2$  l'espace des phases est dit *plan des phases*.

La figure suivante illustre le plan des phases et une trajectoire de phase pour le système (I.4).



**Figure (I.1)** Plan des phases et trajectoire de phase

### I.3.7 Attracteurs

Dans l'espace des phases, il est possible de situer l'ensemble des points qui forment une trajectoire décrivant géométriquement toute l'évolution du système, cette trajectoire est appelée *attracteur*. C'est donc un objet géométrique vers lequel tendent un ensemble de trajectoires des points de cet espace, c'est-à-dire une situation ou un ensemble de situations vers lesquelles évolue un système dynamique pour un ensemble de conditions initiales. On peut avoir plusieurs attracteurs dans un même espace des phases. Il existe deux types d'attracteurs : les attracteurs réguliers (le point fixe, le cycle limite, le tore et les attracteurs étranges (chaotiques)). En outre, le type de l'attracteur dépend du comportement du système . Nous allons voir ces types dans les sections suivantes.

### I.3.7. Comportement des systèmes dynamiques non linéaires [3] [4]

A partir d'un état initial  $x_0$  et après un régime transitoire, la trajectoire d'un système dynamique non linéaire atteint une région limitée de l'espace des phases. Ce comportement asymptotique obtenu pour  $t \rightarrow \infty$  est une des caractéristiques les plus importantes des systèmes dynamiques. Si dans le cas d'un système linéaire la solution asymptotique est indépendante de la condition initiale, en présence de non linéarités, il existe une plus grande variété de régimes permanents parmi lesquelles on trouve par ordre de complexité : points d'équilibre, solutions périodiques, solutions quasi-périodiques et chaos. Il faut préciser que cette fois le comportement développé par un système dynamique particulier est fortement dépendant de la condition initiale choisie. Ces solutions correspondent à différents types d'attracteurs dans l'espace des phases.

#### a. Point d'équilibre

Dans ce cas, la solution asymptotique est représentée par un point, sa valeur étant déterminée en fonction de la condition initiale choisie. Ainsi, pour des conditions initiales différentes on peut retrouver plusieurs points d'équilibres.

Il existe plusieurs types de points d'équilibre (nœud, foyer, col, puits, centre). De même ces points peuvent être stables ou instables suivant que les trajectoires voisines convergent ou divergent entre-elles. Dans l'espace des phases l'attracteur correspondant à une solution d'équilibre est *un point fixe*, c'est la catégorie la plus simple d'attracteurs parce qu'elle n'évolue plus dans le temps.

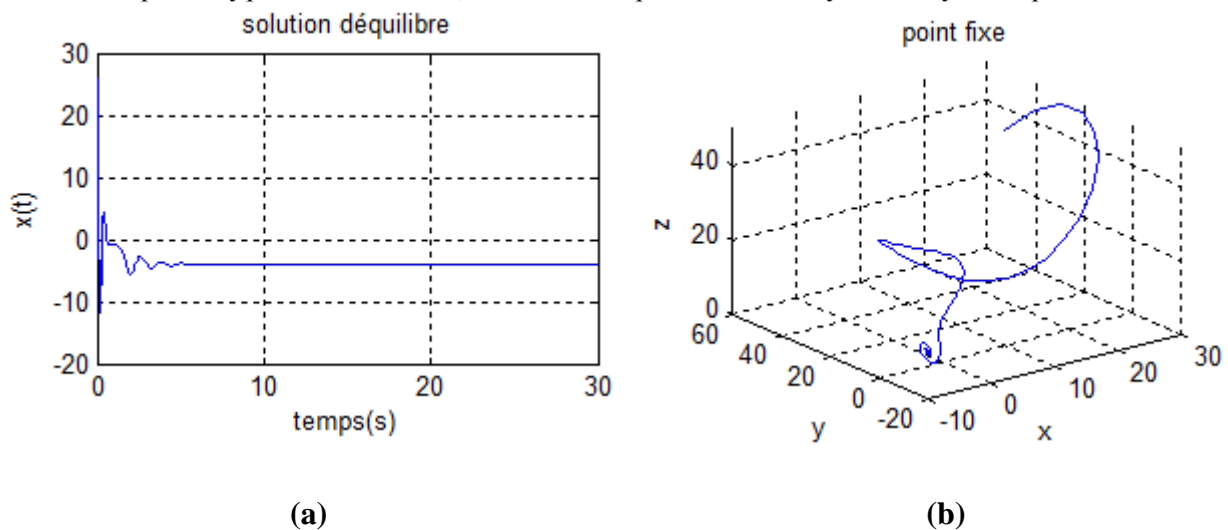
On appelle point fixe ou point d'équilibre du système autonome(I.4), le point  $x^*$  tel que :

$$x^* = f(x^*) = 0 \quad (\text{I.5})$$

#### Exemple

La figure suivante représente une solution d'équilibre d'un système non linéaire, dans l'espace des temps (figure a) et le point fixe qui lui correspond dans l'espace des phases (figure b).

Il existe quatre types d'attracteurs, selon le comportement du système dynamique



**Figure (I.2)** Exemple de point fixe.

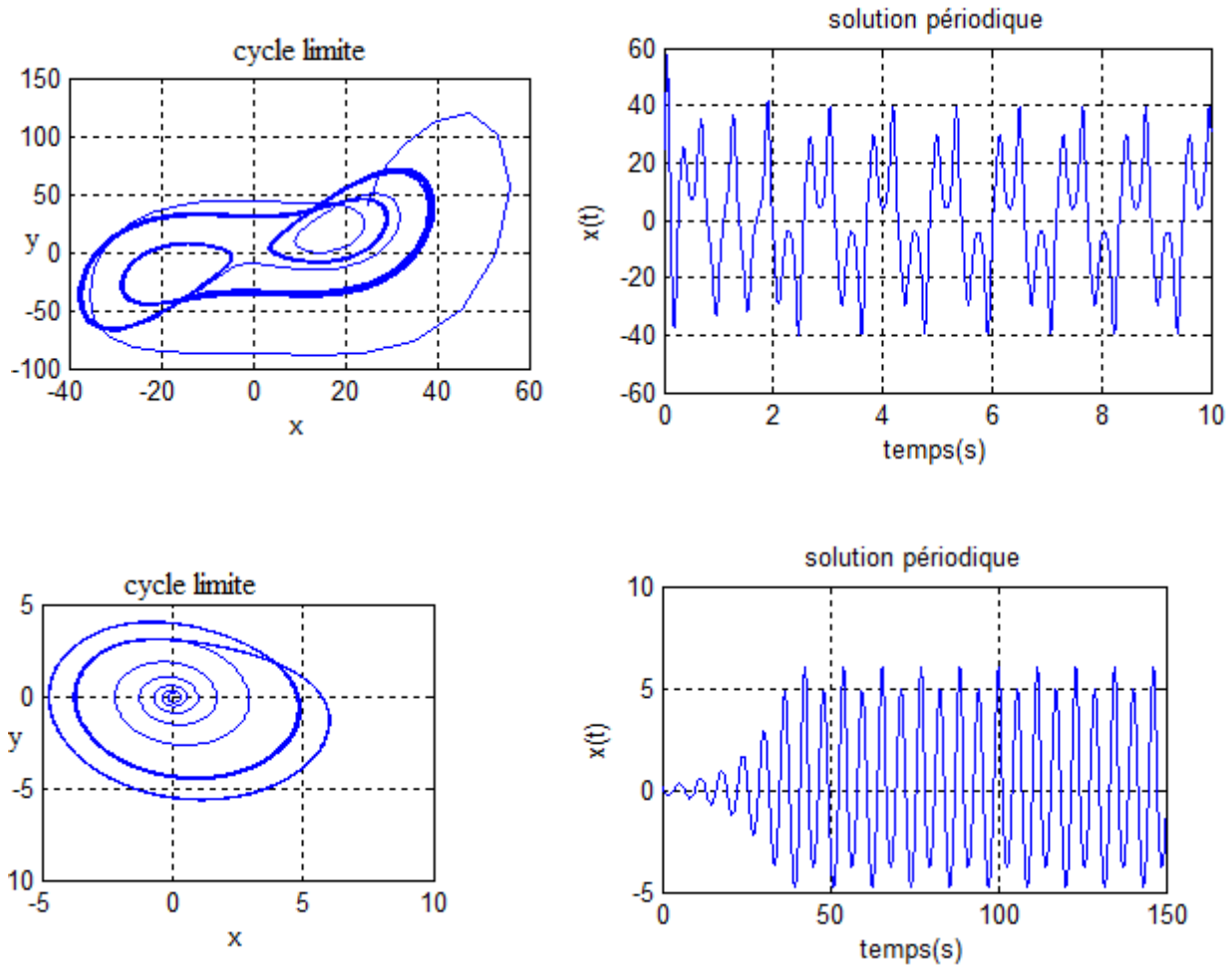
### b. Régime périodique

Le régime asymptotique permanent périodique correspond à une trajectoire dont les répliques d'une portion élémentaire sont espacées à des intervalles  $nT$ ,  $n \in \mathbb{N}^+$ ,  $T$  désignant la période.

Un comportement périodique dans le temps représente *un cycle limite* dans l'espace des phases, c'est une trajectoire de phases fermée associée à un nombre fini de fréquences. Connaissant l'état du système à un instant donné, on est en mesure de prévoir son état à un instant ultérieur.

### Exemple

La figure suivante montre une solution périodique et le cycle limite qui lui correspond pour deux modèles différents de systèmes non linéaires.



**Figure(I.3)** Exemple de solutions périodiques et cycles limites correspondants.

**c. Régime quasi-périodique**

Soit  $x(t, x_0)$  une solution du système dynamique (1.4) et soit  $T = \{T_1, T_2, \dots, T_k\}$ ,  $k \in \mathbb{N}$  un ensemble fini de réels linéairement indépendants.

On dit que  $x(t, x_0)$  est une solution quasi-périodique de (1.4) si elle est périodique pour chacune des périodes  $T_i$  de  $T$ . La solution  $x(t, x_0)$  est également dite  $k$ -périodique.

L'attracteur correspondant dans l'espace des phases est une surface appelée *tore* de dimension  $k$  ou d'ordre  $k$ .

L'état du système demeure calculable à partir d'une condition initiale.

#### d. Régime chaotique

Le régime chaotique est par définition tout régime permanent qui n'appartient à aucune des classes présentées antérieurement. Une telle solution a une trajectoire asymptotique bornée avec une extrême sensibilité aux conditions initiales. Ainsi deux trajectoires générées à partir de CI (conditions initiales) très proches, vont diverger très vite l'une par rapport à l'autre. Cette sensibilité par rapport aux CI traduit aussi le comportement en apparence stochastique des générateurs chaotiques, de telle sorte qu'une prévision à long terme du comportement du système est impossible. L'attracteur correspondant au régime chaotique dans l'espace des phases est appelé *attracteur étrange* à cause de sa forme géométrique particulière.

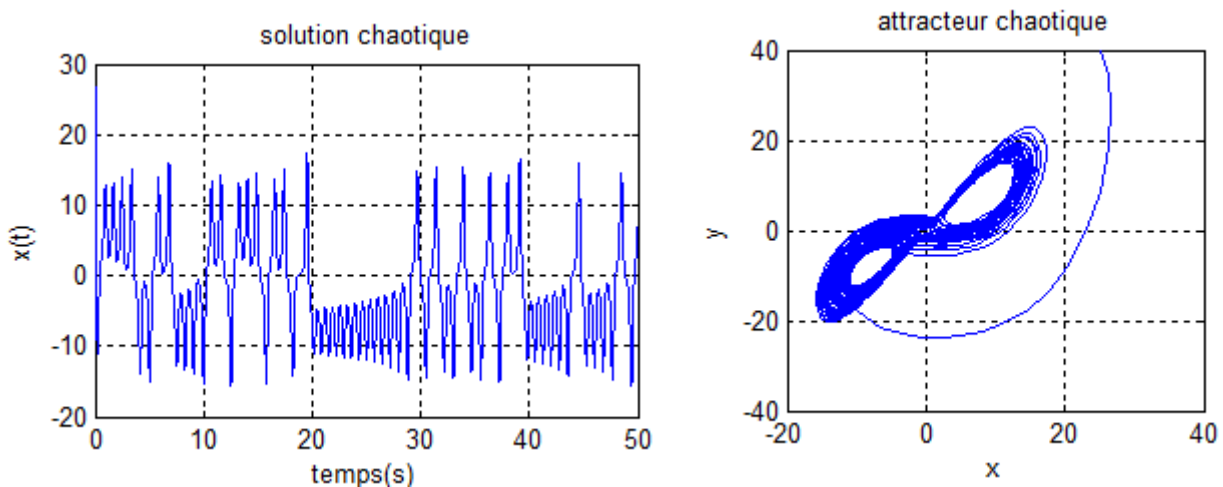
Sachant qu'il n'existe pas de définition à la fois formelle et générale du chaos, il peut donc être défini par défaut des autres types de solutions

#### Remarque

Un système dynamique peut présenter des solutions chaotiques instables. Celles-ci ne pouvant être ni observées ni même simulées, nous ne traiterons que des solutions chaotiques stables.

#### Exemple

La figure suivante représente une solution chaotique et l'attracteur correspondant à cette solution.



**Figure (I.4)** Solution chaotique et attracteur correspondant

## I.4 Définition et caractéristiques des systèmes chaotiques

### I.4.1 Définition d'un système chaotique

En première approximation, le chaos est un comportement particulier des systèmes dynamiques. Un système dynamique est dit chaotique ses les solutions se trouvent dans un ensemble borné de l'espace des phases et qui présente plusieurs caractéristiques fondamentales.

Pratiquement, une dynamique chaotique peut être identifiée, en première analyse, par la reconnaissance de ses propriétés caractéristiques :

- Une extrême sensibilité aux conditions initiales, ce qui se traduit par des trajectoires très proches l'une de l'autre qui divergent de façon exponentielle.
- Il présente au moins un exposant de Lyapunov positif.
- C'est un système déterministe à aspect aléatoire et imprédictible à long terme.
- A l'infini, Sa fonction d'autocorrélation tend vers 0.
- Son spectre de puissance est continu.
- Sa représentation sur l'espace des phases est un attracteur étrange.

### I.4.2 Caractéristiques des systèmes chaotiques

#### a. La Sensibilité aux conditions initiales [5]

La caractéristique principale des systèmes chaotique est la sensibilité aux conditions initiales; pour deux conditions initiales arbitraires très voisines initialement; les deux trajectoires correspondantes à ces données initiales divergent exponentiellement, par suite les deux trajectoires sont incomparables, Ce qui rend les systèmes chaotiques imprédictibles à long terme.

Comme nous l'avons cité dans les paragraphes précédant, ce phénomène a été découvert par Henri Poincaré et popularisé plus tard par Lorenz.

Nous avons cité également dans la chronologie du chaos déterministe le modèle de Lorenz qui fut le premier modèle d'équations différentielles à illustrer les caractéristiques du chaos déterministe.

Ces équations de Lorenz se caractérisent par leur sensibilité aux conditions. Cette propriété est aussi connue sous le nom d'effet papillon « un simple battement d'aile de papillon au Brésil pourrait déclencher une tornade au Texas », c'est -à - dire que d'infimes modifications dans les conditions initiales provoquent des solutions totalement divergentes. Malgré ceci, les solutions sont d'une remarquable simplicité géométrique.

### Exemple

Dans cet exemple, nous allons étudier l'effet papillon i.e. comment une petite modification dans les conditions initiales engendre des solutions totalement divergentes.

Modèle de Lorenz

$$\begin{cases} \frac{dx}{dt} = a(x - y) \\ \frac{dy}{dt} = bx - y - xz \\ \frac{dz}{dt} = xy - cz \end{cases} \quad (1.4)$$

Avec  $(x, y, z)^T$  le vecteur d'état.

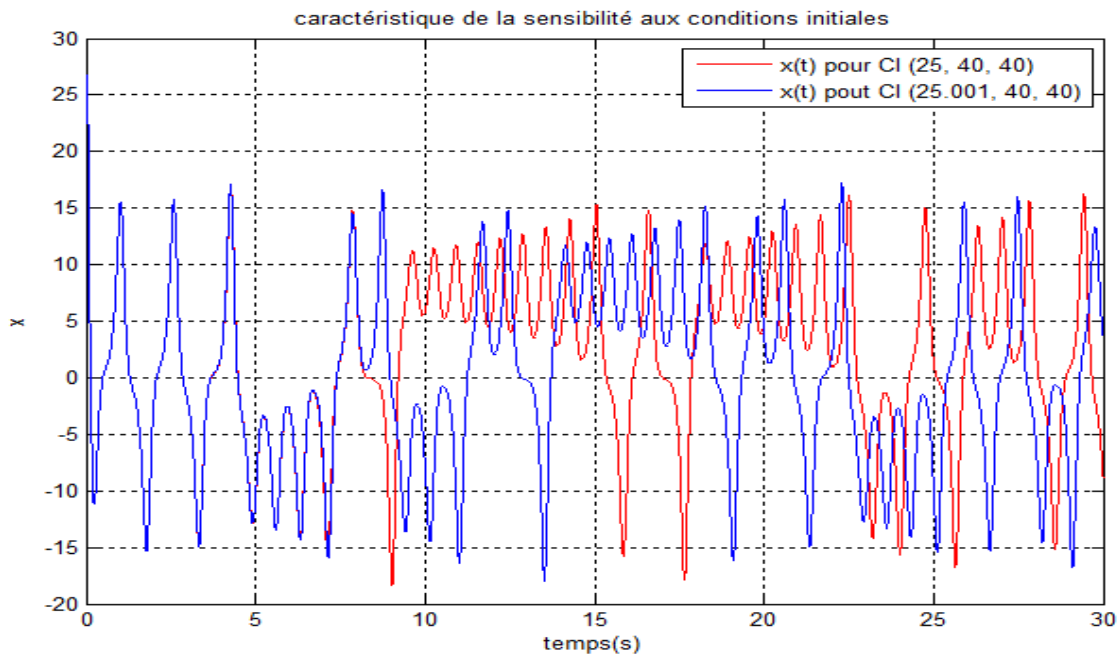
a, b et c des paramètres du système, a=10, b=28 et c=8/3 sont les valeurs pour lesquels le système présente un aspect aléatoire.

$$(x_0, y_0, z_0) = (25, 40, 40) \quad \text{et} \quad (x_0, y_0, z_0) = (25.001, 40, 40)$$

Pour l'illustration nous allons simuler ce modèle sous Matlab pour deux conditions initiales très proches

Soit

$$(x_0, y_0, z_0) = (25, 40, 40) \quad \text{et} \quad (x_0, y_0, z_0) = (25.001, 40, 40)$$



**Figure (I.6)** : tracé de deux solutions du modèle de Lorenz pour des conditions initiales très proches

La figure montre l'extrême sensibilité aux conditions initiales du modèle de Lorenz. En effet, pour deux conditions initiales très proches  $(25, 40, 40)$  et  $(25.001, 40, 40)$ , les deux trajectoires évoluent au départ de la même manière ensuite et très rapidement elles divergent. En outre, l'évolution de  $x(t)$  présente une allure aléatoire.

### b. L'attracteur étrange [5]

Après avoir découvert le chaos, Lorenz entreprit de présenter graphiquement la solution de son système au moyen de son ordinateur, il vit alors apparaître sa deuxième découverte : les attracteurs. En effet il traça la courbe avec deux jeux de conditions initiales très proches, il s'attendait à ce que les deux courbes divergent, mais à sa grande surprise les deux courbes étaient plus ou moins identiques, pas point par point mais dans l'ensemble, elles ressemblaient à deux ailes de papillon.

Le physicien David RUELLE qui s'est penché sur la question et a qualifié cette figure « d'attracteur étrange » en remarquant que les trajectoires ne se coupent jamais, et pourtant

semblent évoluer au hasard formant des boules pas tout à fait concentriques, pas tout à fait sur le même plan mais formant des figures indiscutablement reconnaissables.

Par conséquent, lorsque le régime d'un système est chaotique, l'attracteur correspondant est un attracteur étrange qui a des propriétés topologiques différentes de celles d'un point fixe, cycle limite ou d'un tore appelés communément attracteurs simples cités précédemment.

Un attracteur est caractérisé par :

- Son bassin d'attraction.
- Sa dimension fractale.

### ➤ **Le bassin d'attraction**

L'ensemble de points  $x_0$  de l'espace des phases définissant la condition initiale de chacune des trajectoires qui convergent asymptotiquement vers l'attracteur est appelé le bassin d'attraction.

### ➤ **Dimension fractale [5]**

En géométrie fractale, la dimension fractale,  $D$ , est une grandeur qui a vocation à traduire la façon qu'a un ensemble fractal de remplir l'espace.

Soit un ensemble de points situés dans un espace à  $p$  dimension. Cherchons à recouvrir cet ensemble par des cubes de côté  $\varepsilon$ , soit  $N(\varepsilon)$  le nombre minimal de cubes nécessaire à cette opération.

Par définition la dimension de Hausdorff-Beiscovitch  $D$  est la limite, si elle existe, de l'expression :

$$D = \lim_{\varepsilon \rightarrow 0} \frac{\ln N(\varepsilon)}{\ln \left(\frac{1}{\varepsilon}\right)} \quad (I.7)$$

$D$  est la dimension fractale quand  $\varepsilon$  tend vers 0.

Autrement dit, pour  $\varepsilon$  petit, le nombre minimal de cubes nécessaires pour recouvrir l'ensemble de point varie avec  $\varepsilon$  comme  $\varepsilon^{-D}$ . Dans le cas où l'ensemble se réduit à un point unique.

$$N(\varepsilon) = 1 \quad (I.8)$$

Donc  $D = 0$  est la dimension de Hausdorff du point.

Si l'ensemble est celui des points d'un segment de longueur  $L$ .

$$N(\varepsilon) = L\varepsilon^{-1} \quad (I.9)$$

D'où :  $D = 1$ , alors que pour l'ensemble des points d'une surface d'aire  $S$  :

$$N(\varepsilon) = S\varepsilon^{-2} \quad (I.10)$$

D'où :  $D = 2$

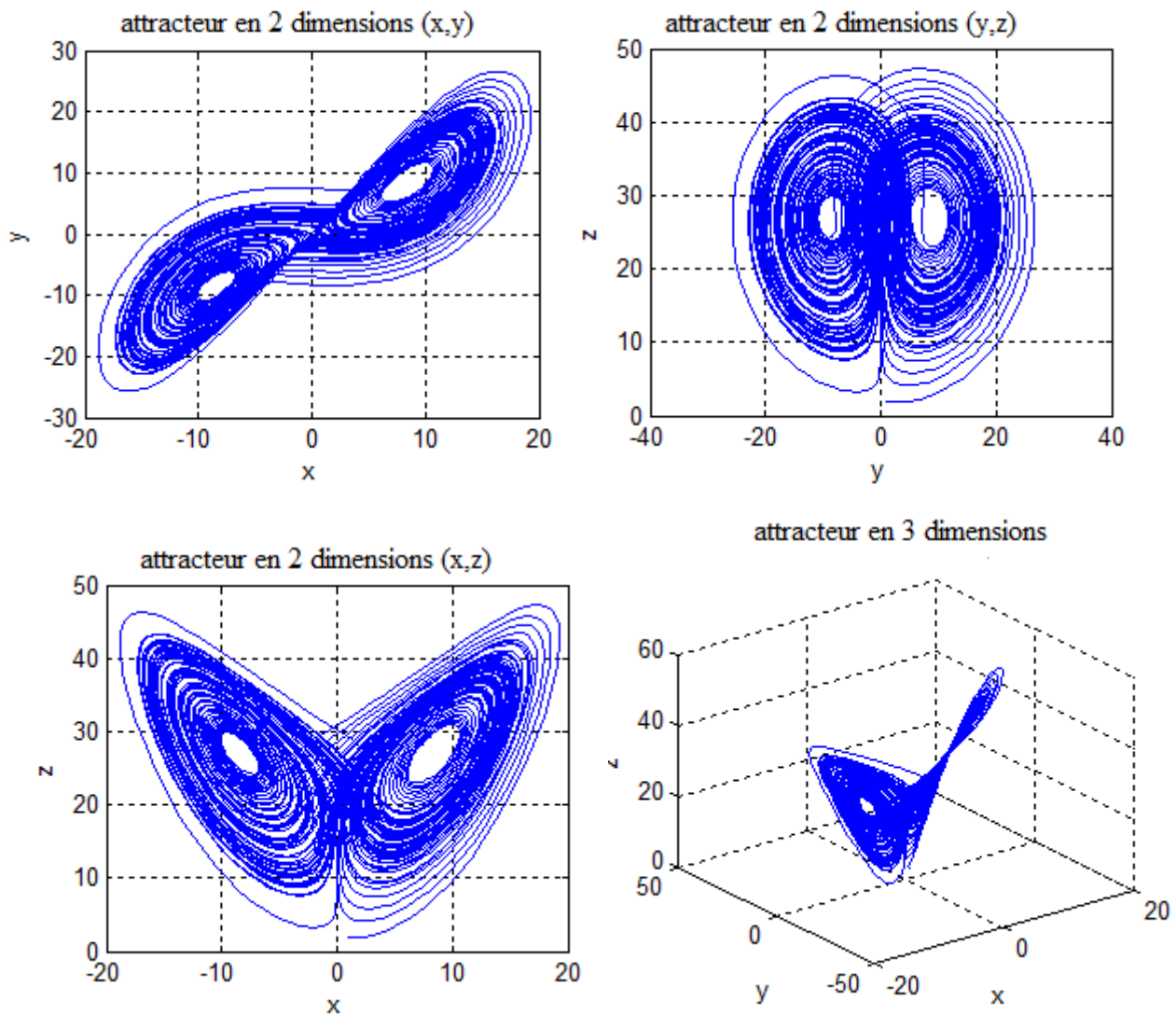
Par conséquent, le point fixe a une dimension nulle, une oscillation périodique stable est de dimension 1, et un attracteur de période 2 a une dimension 2.

C'est parce que la structure de ces attracteurs est très régulière que leur dimension soit entière. Par contre la dimension d'un attracteur étrange est non entière par exemple la dimension de l'attracteur de Lorenz est de 2.06.

### Exemples d'attracteur étrange :

#### Exemple 1

Pour illustrer cette caractéristique des systèmes chaotiques, nous avons choisi l'attracteur de Lorenz, nous allons donc simuler sur Matlab le système d'équations (I. 6).



Figure(I.7) : attracteur de Lorenz en 2 et 3 dimensions

**Exemple 2**

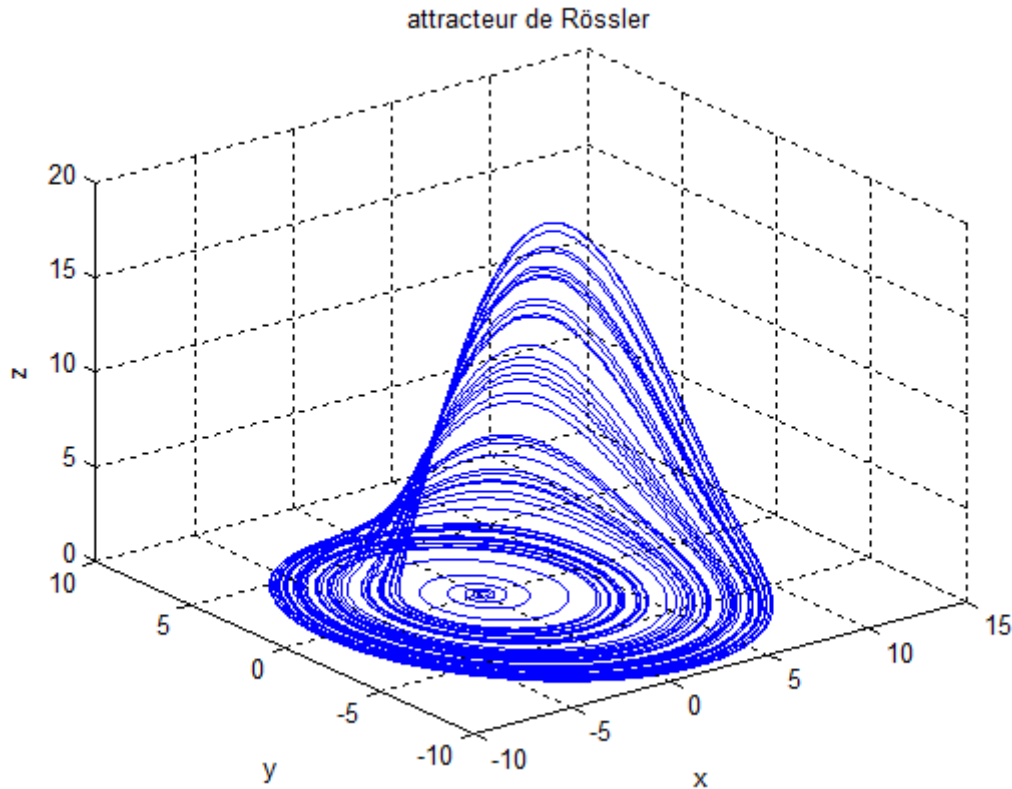
Un autre type d'attracteur qui est l'attracteur de Rössler décrit par le système d'équations suivant

$$\begin{cases} \frac{dx}{dt} = -(y + z) \\ \frac{dy}{dt} = x + ay \\ \frac{dz}{dt} = b + z(x - c) \end{cases} \quad (I.11)$$

Avec  $(x, y, z)$  le vecteur d'état et  $a, b, c$  les paramètres du système.

Le système de Rössler montre un comportement chaotique pour  $a=b=0.2$ ,  $c=5$ .

Les conditions initiales choisies comme suit  $(x_0, y_0, z_0) = (0.2, 2, 1)$



**Figure(I.8)** : attracteur chaotique de Rössler

### c. L'exposant de Lyapunov [6], [3]

En régime chaotique, la distance entre deux trajectoires initialement proches tend à augmenter à une vitesse exponentielle, puis à se stabiliser lorsque la distance atteint une valeur limite de l'ordre du diamètre de l'attracteur. Le temps que mettent deux conditions initiales à atteindre cette valeur limite constitue l'horizon prédictif du système. Les exposants dits de **Lyapunov** permettent de mesurer ce *taux de divergence* et donc de mesurer la sensibilité aux conditions initiales.

**Définition** un exposant de Lyapunov est le taux exponentiel moyen de divergence ou de convergence de trajectoires voisines de l'espace des phases d'un système dynamique non linéaire soumis à des conditions initiales différentes.

Cette mesure est faite suivant un des axes de l'espace des phases. En outre, Si un exposant de Lyapunov est positif alors les trajectoires divergent, et s'il est négatif elles convergent. L'apparition du chaos exige l'existence d'un exposant positif selon au moins un axe. Les exposants de Lyapunov caractérisent ainsi les attracteurs ou le comportement du système dynamique non linéaire, notamment son caractère chaotique ou hyperchaotique, par exemple si le système présente un exposant de Lyapunov positif alors le système est chaotique et s'il a deux exposants de Lyapunov positifs alors le système est hyper chaotique.

#### ➤ Calcul de l'exposant de Lyapunov

Les valeurs propres de la matrice d'état  $A$  d'un système linéaire permettent de caractériser les points d'équilibre et leur stabilité. Les exposants de Lyapunov sont une généralisation de ces valeurs propres pour les systèmes non linéaires et caractérisent les attracteurs comme cité antérieurement. Cela se fait par la mesure de la distance Euclidienne de deux évolutions du système à partir de deux conditions initiales différentes, cette mesure nécessite d'itérer la dynamique du modèle pour deux conditions initiales très proches, et de mesurer au bout d'un temps fini la distance entre ces deux trajectoires. Pour que ce calcul soit valable, il faut bien sûr que ces deux conditions initiales soient situées à proximité de l'attracteur. Cette distance peut être approximée par  $e^{\lambda t+a}$  où  $a$  est une constante et  $\lambda$  une constante réelle appelée exposant de Lyapunov.

Pour le calcul de ces exposants, il existe différentes méthodes, par contre, il est difficile de le déterminer par les méthodes analytique, c'est pour cela qu'on a recours aux simulations numériques.

#### Remarque

Le nombre des exposants de Lyapunov est égal à la dimension du système.

➤ **Comportement d'un système dynamique non linéaire en fonction des exposants de Lyapunov [3]**

$\lambda_n \leq \dots \leq \lambda_1 < 0$  : Des exposants de Lyapunov négatifs montrent l'existence d'un point fixe.

$\lambda_1 = 0, \lambda_n \leq \dots \leq \lambda_2 < 0$  : L'attracteur est un cycle limite ( régime périodique).

$\lambda_1 = \lambda_2 = 0, \lambda_n \leq \dots \leq \lambda_3 < 0$  : L'attracteur est un tore d'ordre 2 (Régime quasi-périodique à 2 fréquences)

$\lambda_1 = \dots = \lambda_k = 0, \lambda_n \leq \dots \leq \lambda_{k+1} < 0$  : L'attracteur est un tore d'ordre k (Régime quasi-périodique à k fréquences).

$\lambda_1 > 0, \lambda_n \leq \dots \leq \lambda_2 < 0$  : L'attracteur est chaotique.

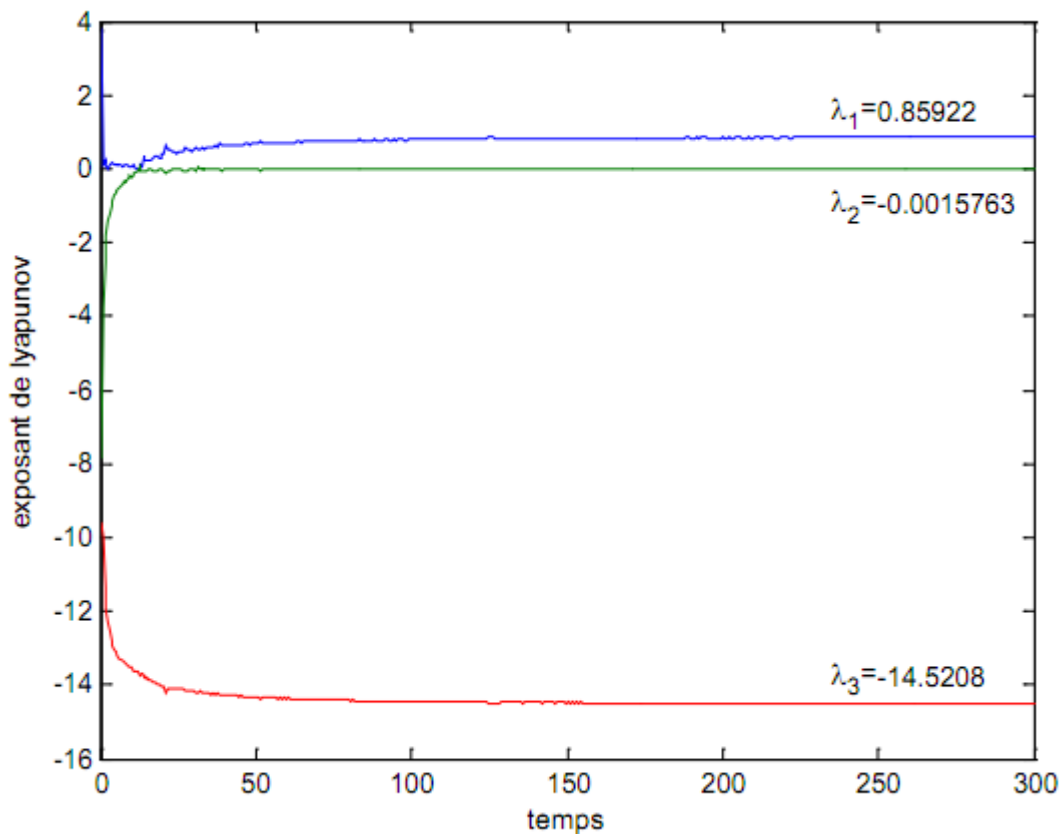
$\lambda_1 > \dots > \lambda_k > 0, \lambda_n \leq \dots \leq \lambda_{k+1} < 0$  : L'attracteur est hyperchaotique.

**Remarque**

On constate ici que le nombre d'exposants de Lyapunov nuls indique la dimension d'un attracteur non chaotique. Ainsi, un point fixe est de dimension 0, un cycle limite est de dimension 1 et un tore d'ordre k de dimension k.

Illustration :

Pour illustrer cette caractéristique nous avons choisi le système de Lorenz décrit par le système d'équations(I.6), la figure suivante montre l'évolution des trois exposants de Lyapunov du système de Lorenz



**Figure(I.9) :** exposants de Lyapunov du système de Lorenz

On remarque que la trajectoire qui décrit l'exposant de Lyapunov positif  $\lambda_1$  augmente à une vitesse exponentielle au début, puis se stabilise à une valeur fixe. Ce qui traduit la divergence exponentielle des deux trajectoires du système issues de deux conditions initiales différentes, utilisées pour la mesure de l'exposant.

#### d. Le déterminisme et l'imprédictibilité

Pour un système déterministe, si l'on connaît l'état du système à un instant donné, on est en mesure de prévoir son état à un instant ultérieur puisque il existe une seule solution pour chaque condition initiale. Cependant, deux conditions initiales très proches peuvent avoir des évolutions complètement différentes. L'évolution du système devient alors imprédictible car une petite erreur de mesure ou un simple arrondi conduit à des résultats complètement faux au bout d'un certain temps. C'est *le chaos déterministe*. A long terme, on ne peut pas savoir, même approximativement, quelle sera la valeur d'un système chaotique.

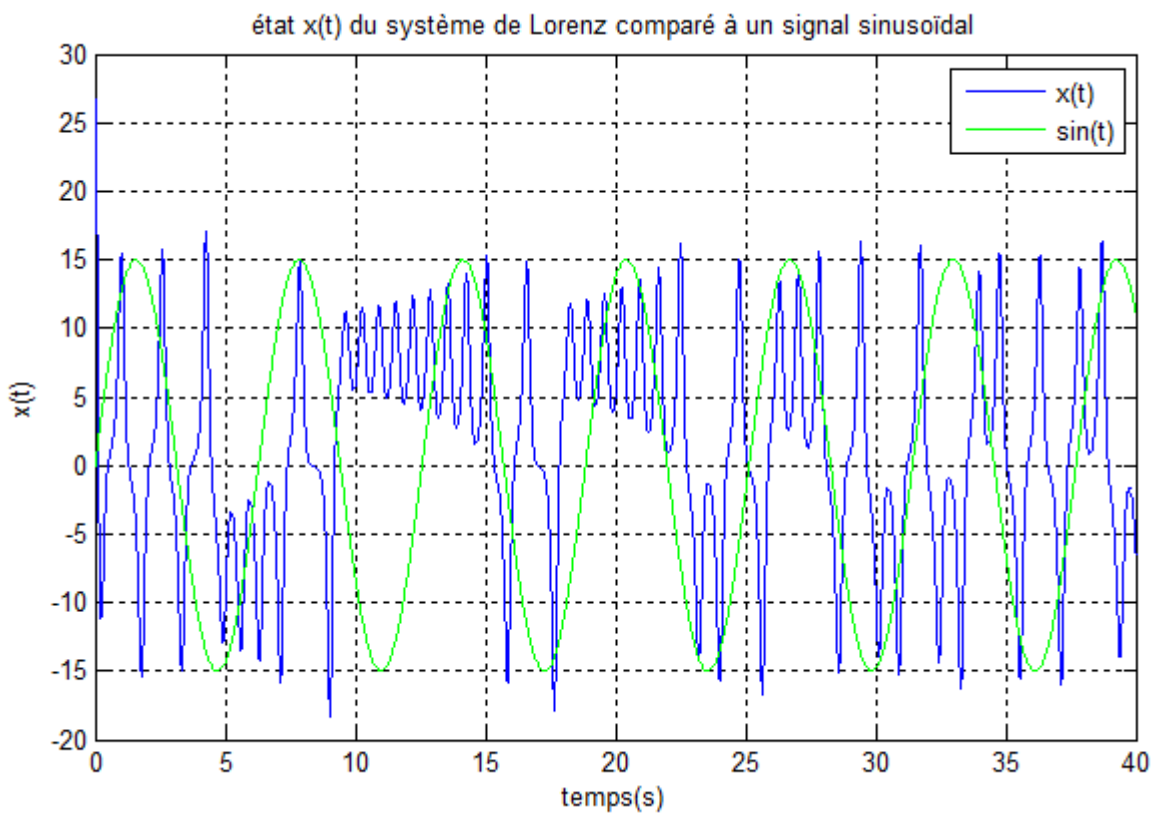
Donc ce qui différencie le chaos des phénomènes aléatoires est son déterminisme mais sa sensibilité aux conditions initiales le rend imprédictible à long terme.

### e. L'aspect aléatoire

Les solutions d'un système chaotique correspondant à des conditions initiales légèrement différentes sont éloignées les unes des autres de façon désordonnée, ce qui donne un aspect aléatoire au système chaotique. Il est donc difficile de distinguer un comportement chaotique d'un comportement aléatoire sur les trajectoires des solutions dans l'espace des temps.

Illustration

Pour illustrer l'aspect aléatoire des systèmes chaotiques nous allons observer l'aspect d'un état du système de Lorenz décrit par le système d'équations (I. 6), comparé à un signal périodique (sinusoïdal).



Figure(I.10) état  $x(t)$  du système de Lorenz comparé à un signal périodique (sinusoïde)

### f. Le spectre de puissance [7]

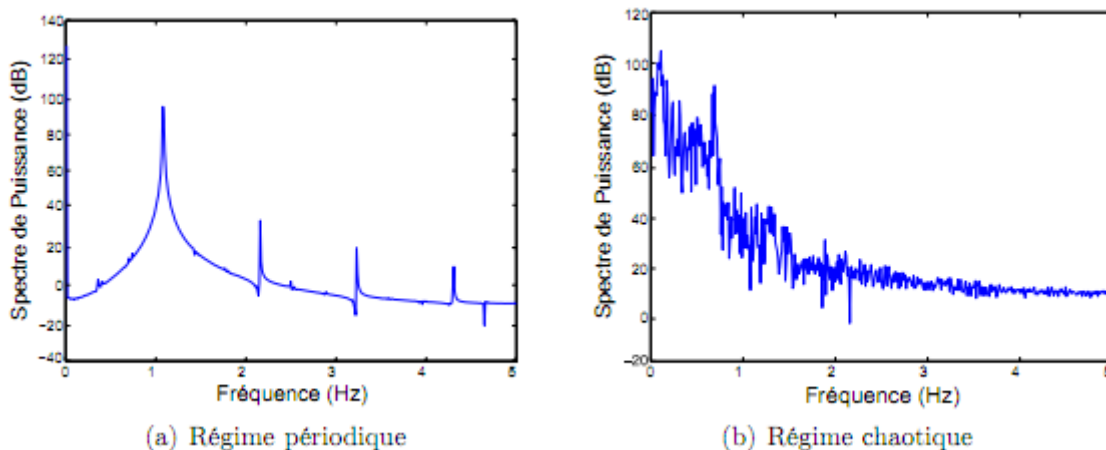
Une approche pratique et porteuse d'information est le calcul du spectre du signal. Il s'agit de l'extraction des composantes fréquentielles d'un signal. Elle utilise la transformée de Fourier. La fréquence, l'amplitude et la phase de chaque composante sinusoïdale sont calculées en fonction du signal temporel selon la relation suivante en faisant intervenir les deux variables réciproques,  $t$  le temps, et  $f$  la fréquence :

$$\tilde{x}(f) = \int_{-\infty}^{+\infty} x(t)e^{-2j\pi ft} dt \quad (I.12)$$

La transformée de Fourier  $\tilde{x}(f)$  est complexe. Le module de cette grandeur représente le spectre d'amplitude, l'argument le spectre de phase et le spectre de puissance représente le carré du module  $|\tilde{x}(f)|^2$ .

Une façon simple de caractériser le chaos consiste à calculer le spectre de Fourier de l'évolution temporelle d'une des variables du système. Le spectre de Fourier d'un signal périodique ou quasi-périodique est constitué de raies distinctes correspondant aux périodes et harmoniques du système. Pour un signal chaotique on obtient un spectre continu.

Illustration :



Figure(I.11) : spectre de puissance d'un système en régime périodique et en régime chaotique

Nous voyons dans la figure (I.11) le spectre d'amplitude des oscillations d'un système dynamique en régime périodique. Le spectre présente des raies à la fréquence fondamentale ainsi qu'à celles des harmoniques.

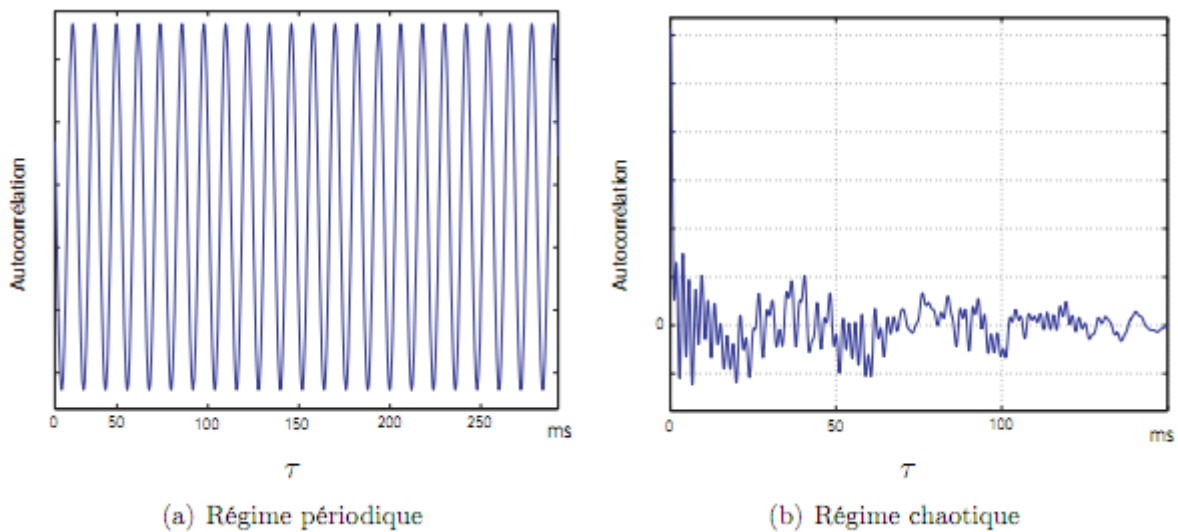
En régime chaotique le spectre ne présente plus des raies discrètes, mais un continuum de fréquences, signe d'une grande richesse dans la dynamique.

### g. La fonction d'autocorrélation [7]

Le spectre de puissance est la transformée de Fourier de la fonction d'autocorrélation notée  $C(\tau)$ , cette fonction mesure la ressemblance de la variable  $x$  à l'instant donné  $t$  avec sa valeur à l'instant ultérieur  $t + \tau$ . La fonction d'autocorrélation  $C(\tau)$  est obtenue en faisant la moyenne arithmétique d'un grand nombre de  $x(t)x(t + \tau)$ .

$$C(\tau) = \frac{1}{t_2 - t_1} \int_{t_1}^{t_2} x(t)x(t + \tau) dt \quad (I.13)$$

La fonction d'autocorrélation est donc construite en faisant varier progressivement l'intervalle  $\tau$ . Par conséquent, si  $x(t)$  est constant, périodique ou quasi-périodique  $C(\tau)$  reste non nul quand  $\tau \rightarrow \infty$  car le spectre de puissance est formée de raies distinctes. En particulier, pour des oscillations périodiques,  $C(\tau)$  oscille entre 1 et -1. En revanche, dans le cas des oscillations chaotiques, ou le spectre de puissance comporte une partie continue,  $C(\tau) \rightarrow 0$  quand  $\tau$ , et cela de manière exponentielle, ainsi un processus chaotique est tel que sa fonction de corrélation décroît vers 0 quand l'horizon tend vers l'infini. Cette propriété assure que les solutions divergent les unes des autres. Si la fonction de corrélation est nulle pour des horizons non nuls, alors c'est un processus non corrélé, et on parle de « bruit blanc déterministe ».



**Figure(I.12) :** autocorrélation d'un système en régime périodique et en régime chaotique

La figure (b) montre que la similitude temporelle du signal chaotique avec lui-même diminue, et disparaît quasiment à des instants suffisamment éloignés l'un de l'autre. La connaissance de  $x(t)$  pendant un laps de temps aussi long que l'on veut ne permet plus de prédire le comportement futur de  $x(t)$ . Nous retrouvons l'imprédictibilité du régime chaotique par perte progressive de sa similitude interne. Cette imprédictibilité est aussi à l'origine de l'écartement de deux trajectoires initialement voisines : elles perdent toute similitude au bout d'un temps fini. Nous retrouvons la sensibilité aux conditions initiales.

### I.5 Les sections de Poincaré [6]

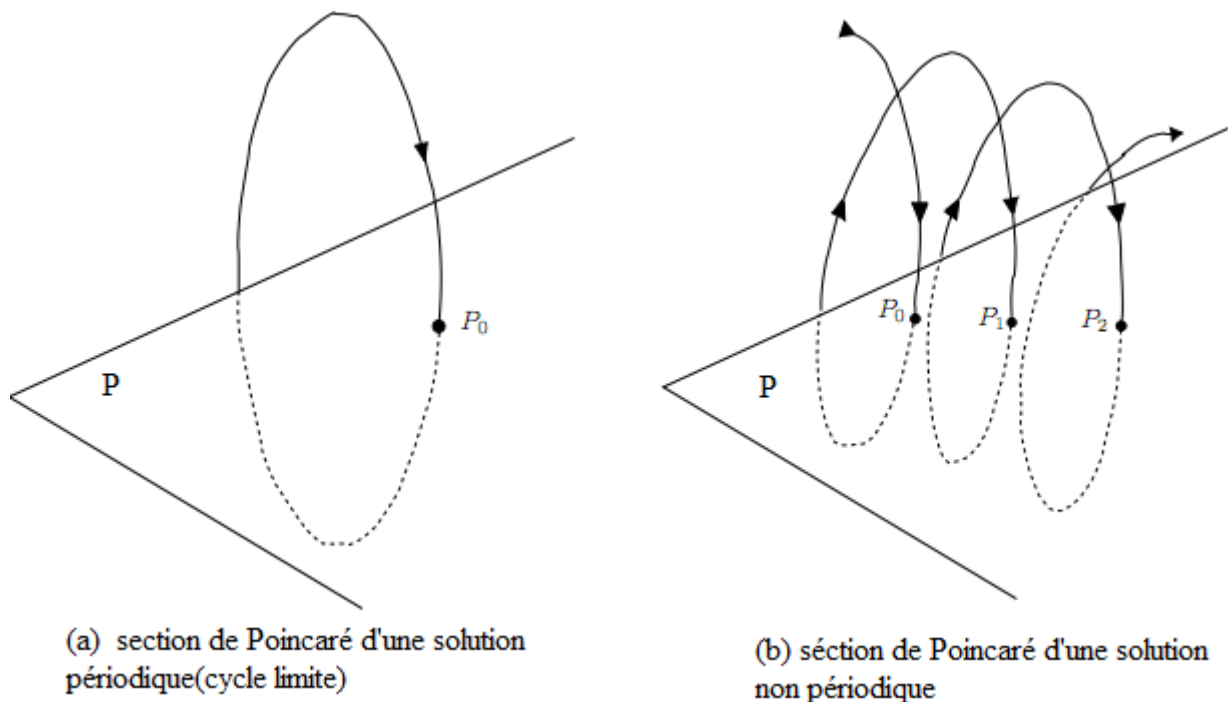
Henri Poincaré a apporté une contribution très utile pour l'étude des systèmes chaotiques. Parmi ces contributions on trouve les sections de Poincaré. Faire une section de Poincaré revient à couper la trajectoire dans l'espace des phases par un plan en dimension 3 ou par une droite en dimension 2, afin d'étudier les intersections de cette trajectoire avec ce plan ou cette droite, ces intersections sont faites avec un sens prédéfini. On passe alors d'un système dynamique à temps continu à un système dynamique à temps discret via une réduction d'une unité de l'ordre du système. Les mathématiciens ont bien sûr démontré que

les propriétés du système sont conservées après la réalisation d'une section de Poincaré judicieusement choisie.

On constate qu'à chaque type d'attracteur correspond un seul type de topologie dans le plan. L'avantage des sections de Poincaré dans l'étude des systèmes dynamiques est le passage d'une dynamique à temps continu à une dynamique à temps discret, ce qui facilite l'analyse.

Le plan de la section doit être choisi de manière à garantir l'existence d'intersections avec la trajectoire et de telle sorte que celle-ci le traverse alternativement dans un sens puis dans l'autre.

La figure suivante montre le principe de la section de Poincaré, pour une solution périodique et une solution non périodique.

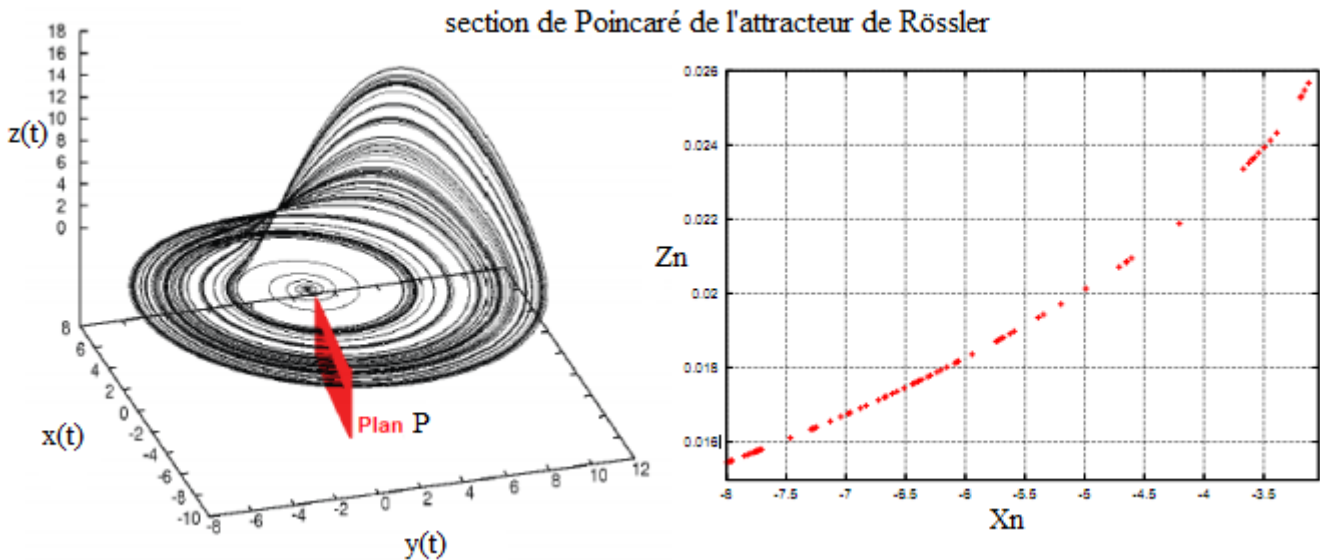


**Figure(I.13) :** principe de la section de Poincaré

En effectuant une section de Poincaré, on peut identifier le régime de fonctionnement d'un système dynamique en observant l'allure obtenue sur cette section. Par exemple, lorsque le régime est périodique, la section de Poincaré est un point (l'attracteur est un cycle limite), pour un régime bipériodique la section de Poincaré est une courbe fermée (l'attracteur est un tore) et lorsque le régime est chaotique les points de la section sont répartis sur une surface.

Ils sont donnés par une structure complexe mais bien définie. Lorsque le flot est très dissipatif, la section est pratiquement une ligne (segment, arc,...).

### Exemple



**Figure(I.14) :** Intersections de la trajectoire de l'attracteur de Rössler avec un plan P d'équation  $y = 0$  ( $x \leq 0$ )

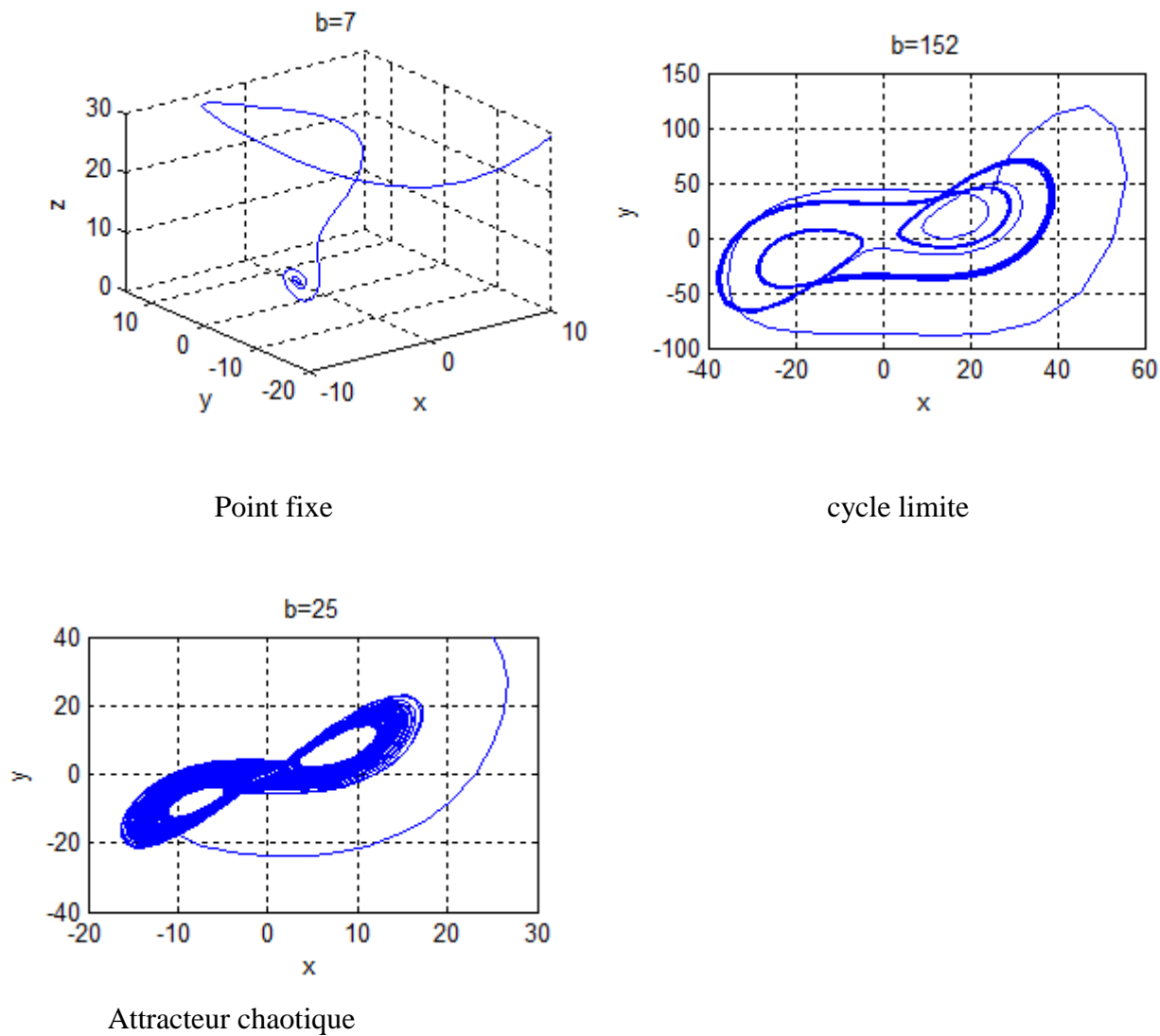
La section de Poincaré obtenue par l'intersection de l'attracteur de Rössler en trois dimensions avec un plan est un arc assimilable à une parabole.

### I.6 Notions bifurcation et transition vers le chaos [7]

Un système dynamique non-linéaire peut présenter de multiples comportements (point fixe, oscillations périodiques, quasi-périodiques, chaos) en fonction de la valeur de ses paramètres. Il passe d'un comportement à un autre en fonction des changements de certains paramètres importants du système. Les transitions entre régimes dynamiques se font par bifurcation, et le paramètre dont la modification entraîne le changement de régime dynamique est appelé *paramètre de bifurcation*. L'ensemble de l'évolution dynamique d'un système peut se représenter sous la forme d'un *diagramme de bifurcation*.

## Illustration

Le modèle de Lorenz décrit par les équations (I.6) présente des comportements différents suivant la valeur du paramètre  $b$  comme le montre la figure suivante.



**Figure(I.15)** : attracteurs du modèle de Lorenz pour différentes valeurs de  $b$ .

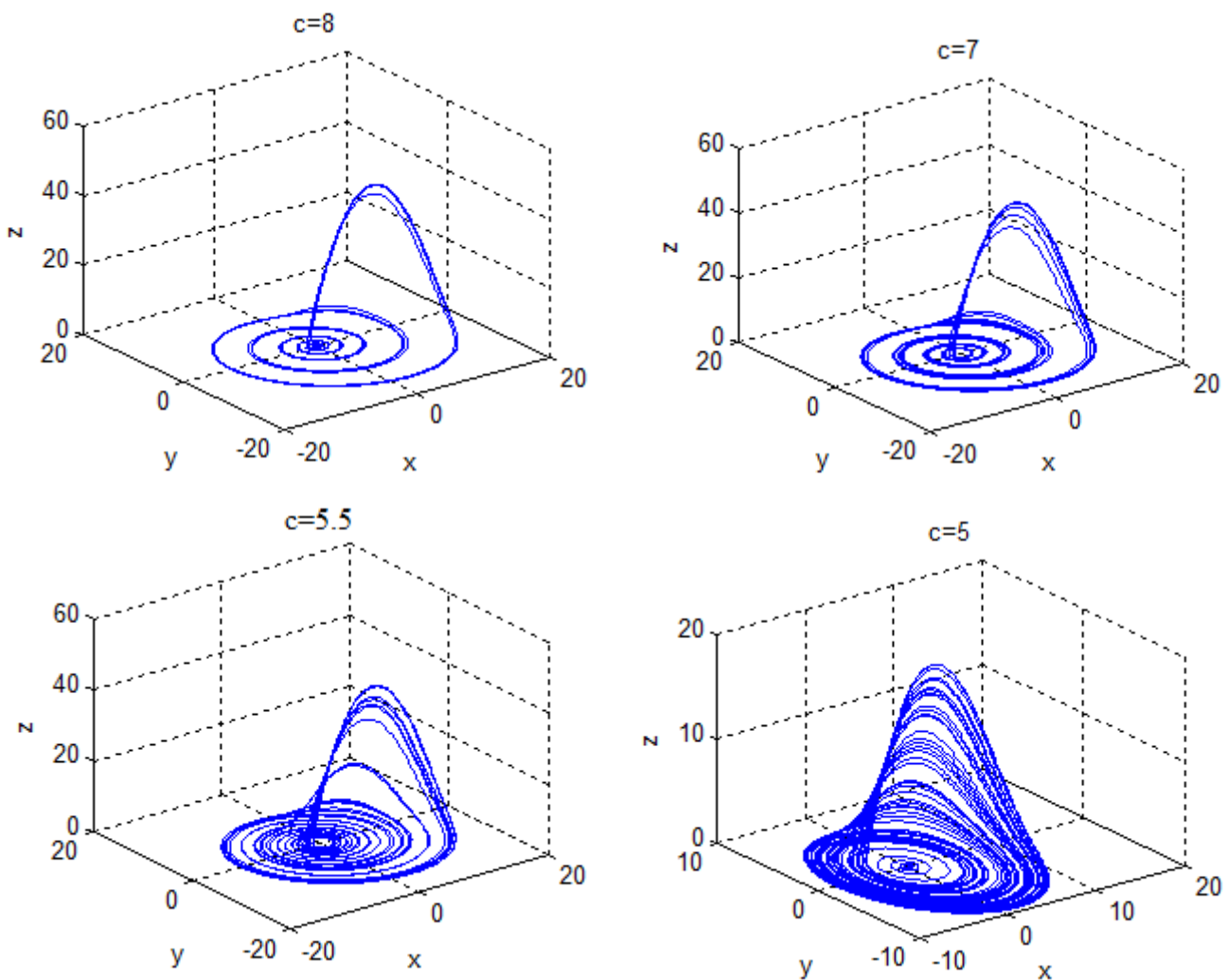
On remarque que pour le même système, différents types d'attracteurs sont obtenus, par le changement du paramètre  $c$ , un point fixe pour  $b=7$ , un cycle limite pour  $b=152$  et un attracteur chaotique pour  $b=25$ .

➤ **Exemple scénario de transition vers le chaos : Le dédoublement de période**

Il existe différents enchaînements types de régimes dynamiques lorsque le paramètre de bifurcation est augmenté. Ces enchaînements sont parfois appelés «route vers le chaos».

Il existe plusieurs types de route vers le chaos, parmi lesquels nous donnerons comme *exemple* *Le dédoublement de période* ou *route de Feigenbaum*. Par variation du paramètre de bifurcation d'un modèle des solutions de période  $2T$ ,  $4T$  apparaissent successivement, on parle alors de cascade sous harmonique ou cascade de dédoublement de période.

La figure suivante représente le dédoublement de période du modèle de Rössler décrit par les équations (I.11), par variation du paramètre  $c$ .



**Figure(I.16)** : dédoublement de période de l'attracteur du modèle de Rössler

➤ **Diagramme de bifurcation [6]**

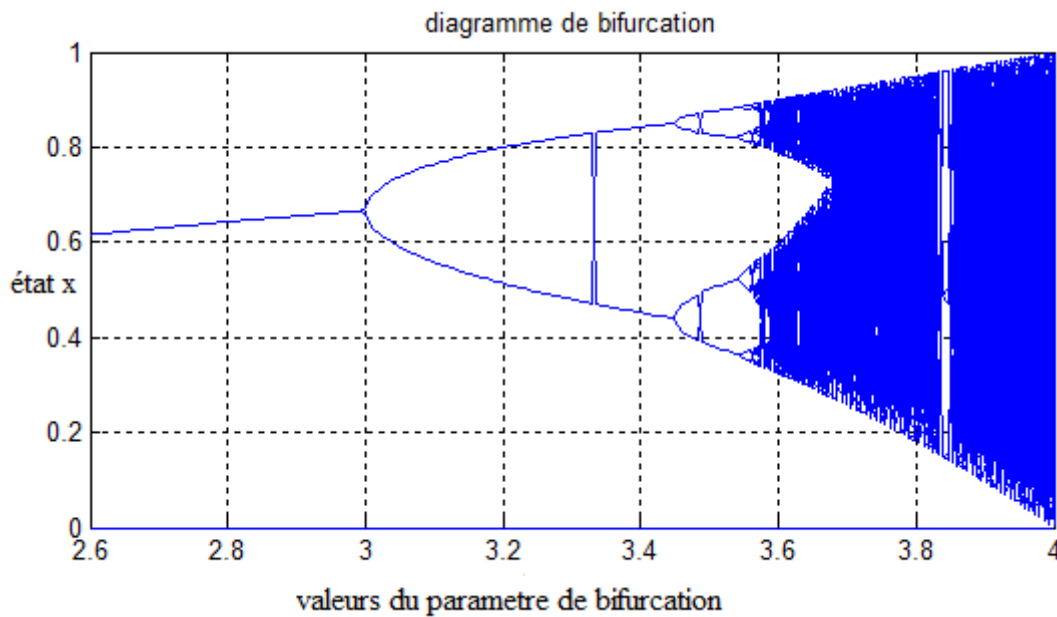
Le diagramme de bifurcations est un tracé repérant la nature des différentes solutions du système et leur stabilité lorsqu'un paramètre varie.

Il est composé d'intervalles sur lesquelles les solutions asymptotiques (ou les ensembles limites qui leur correspondent) évoluent continûment avec le paramètre. Il classe donc les valeurs du paramètre sur l'axe abscisses et des valeurs particulières d'une des variables d'état sur l'axe des ordonnées. C'est un outil efficace pour évaluer rapidement l'ensemble des solutions possibles d'un système en fonction des variations de l'un de ses paramètres. Il permet de repérer les valeurs particulières du paramètre qui induisent des bifurcations.

Dans le cas d'un système autonome, ces valeurs particulières peuvent être obtenues en travaillant avec une section de Poincaré. Pour un système excité par une fonction périodique du temps, elles peuvent l'être en échantillonnant la variable à la fréquence d'excitation. On obtient ainsi pour chaque valeur du paramètre la suite des états discrets de la variable lorsque le régime asymptotique est atteint.

### Propriétés

- Un seul point sur une verticale indique un fonctionnement périodique fondamental. En effet, si pour une valeur donnée du paramètre le régime est périodique, la variable échantillonnée à la fréquence fondamentale  $f$  prend une valeur unique. Les  $N$  points correspondants à la même abscisse se superposent donc exactement.
- Un ensemble de  $q$  points distinct est la marque d'un régime sous harmonique de rang  $q$ , la fréquence de la variable en ce point est  $f/q$ .
- Lorsque les points se répartissent densément sur un segment de la verticale, on peut en déduire que la solution est apériodique mais il n'est pas possible de préciser si elle est quasi périodique ou chaotique.



Figure(I.17) : exemple de diagramme de bifurcation

## I.7 Conclusion

C'est lors d'une étude météorologique que la théorie du chaos a été mise à jour. Un système est chaotique s'il est régi par des lois déterministes, mais que son évolution échappe à toutes prévisions à long terme. L'origine de ce phénomène est la dépendance aux conditions initiales qui est la caractéristique principale du chaos déterministe. Les systèmes chaotiques ont un comportement infiniment complexe, leur représentation dans l'espace des phases est une figure géométrique de structure également infiniment complexe : l'attracteur étrange.

D'autres caractéristiques sont également induites par la sensibilité aux conditions initiales. En effet, un système chaotique est un système déterministe à aspect aléatoire, qui a au moins un exposant de Lyapunov positif, un spectre de puissance continu, une fonction d'autocorrélation qui à l'infini tend vers zéro. Nous avons explicité ces caractéristiques par des exemples de célèbres modèles de systèmes chaotiques : le modèle de Lorenz et le modèle de Rössler que nous avons simulé sous Matlab.

Dans ce chapitre nous avons vu aussi les sections de Poincaré, un autre outil de caractérisation et d'étude des systèmes chaotiques, ainsi que la bifurcation vers le chaos, et un

scénario de transition vers le chaos que nous avons observé lors des simulations du modèle de Lorenz connu sous le nom de dédoublement de période ou cascades harmoniques.

## **II.1 Synchronisation du chaos**

### **II.1.1 Introduction**

L'utilisation du chaos dans les systèmes de télécommunication a été rendue possible depuis la maîtrise de la synchronisation des systèmes chaotiques. Un signal chaotique se présente sous la forme d'un bruit blanc que ce soit dans le domaine temporel ou le domaine fréquentiel. Ce qui différencie un signal chaotique d'un bruit aléatoire est la notion de déterminisme. En effet, le bruit ne peut être décrit que comme un processus aléatoire alors qu'un système chaotique est représentable par des équations différentielles, il est alors possible de synchroniser deux systèmes chaotiques. Pecora et Carroll ont été les premiers en 1989 à synchroniser deux systèmes chaotiques.

Un aspect intéressant de l'utilisation du chaos dans la transmission sécurisée réside dans le fait que les signaux chaotiques peuvent être générés en utilisant des circuits simples et peu coûteux. Un autre avantage non négligeable concerne la confidentialité des transmissions. Un message codé par un système chaotique possédant plusieurs exposants de Lyapunov positifs sera très difficile à déchiffrer pour un récepteur non autorisé.

Ce chapitre se décompose en deux parties. La première section présente le concept de synchronisation du chaos.

La seconde partie de ce chapitre expose les principales implémentations utilisant des systèmes chaotiques pour les communications.

### **II.1.2 La synchronisation du chaos**

La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre système.

D'une façon générale, la synchronisation peut être décrite de la manière suivante :

Considérons les deux systèmes suivants :

$$\begin{cases} \dot{x} = f(x, u) \\ \dot{\hat{x}} = f(\hat{x}, u) \end{cases} \quad (2.1)$$

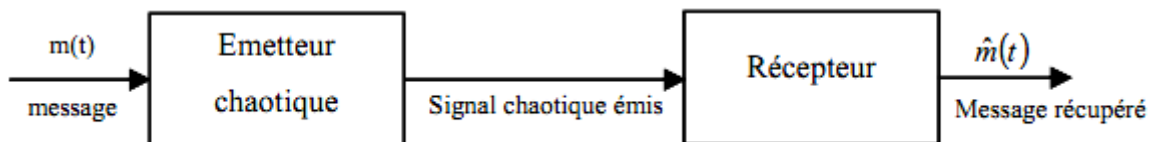
Avec  $x \in \mathbb{R}^n$ ,  $\hat{x} \in \mathbb{R}^n$ , dans lesquels  $f_i: \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}^n$  sont des champs de vecteurs non linéaires, les deux systèmes sont dit synchronisés si :

$$e = |\hat{x}(t) - x(t)| \rightarrow 0 \text{ quand } t \rightarrow \infty \quad (2.2)$$

Où  $e$  représente l'erreur de synchronisation.

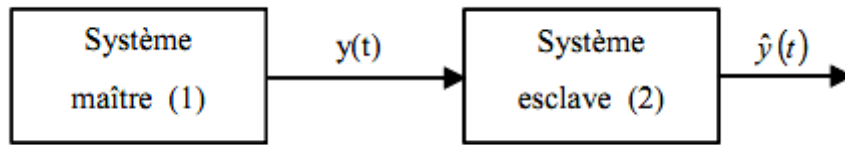
### II.1.2.1 Positionnement du problème

La figure suivante présente l'architecture générale d'un système de communication basé sur le chaos. Un signal  $m(t)$  contenant l'information à transmettre est injecté à l'entrée d'un émetteur présentant un comportement chaotique. Celui-ci génère un signal  $y(t)$  chaotique qui est transmis au récepteur.



**Figure(II.1) :** Système de communication chaotique

Le récepteur est piloté par le signal  $y(t)$  et réalise l'opération inverse de celle effectuée à l'émission afin de récupérer le message transmis. L'émetteur, pour transmettre le message, mélange celui-ci avec un signal chaotique (différentes techniques pour coder le message avec un signal chaotique seront abordées dans un paragraphe ultérieur). De ce fait, il apparaît difficile pour le récepteur de récupérer l'information contenue dans le signal chaotique. Le récepteur est en général similaire à l'émetteur. Pour pouvoir extraire l'information du signal reçu, il est nécessaire de synchroniser les deux systèmes.



**Figure (II.2) :** Système maître esclave pour la communication chaotique

La notion de synchronisation est en général liée à un mouvement périodique. Deux signaux sont synchronisés si leur période ainsi que leur phase sont identiques. Cette définition n'est plus valable dans le cas de signaux chaotiques. Deux signaux chaotiques seront dits synchronisés s'ils sont asymptotiquement identiques.

Considérons la figure (II.2) dans laquelle, le système (2), dit système esclave, sera synchronisé avec le système (1) (système maître) si :

$$\lim_{t \rightarrow \infty} |\hat{y}(t) - y(t)| = 0 \quad (II.3)$$

et ce, quel que soit l'état initial des deux systèmes.

A priori, il paraît impossible d'arriver à synchroniser deux exemplaires d'un même système chaotique. D'une part parce que dans les systèmes réels, il est extrêmement difficile de construire deux circuits à l'identique à cause de la tolérance sur les composants ainsi que du bruit présent dans tout système électronique.

D'autre part, en supposant que l'on dispose de deux circuits identiques, il se pose le problème de la sensibilité aux conditions initiales. Une infime différence entre les conditions initiales des deux circuits conduira à des signaux totalement différents. Cela signifie que reproduire ces conditions initiales dans un système réel est impossible.

Cependant, dans le cas de la Figure (II.2), c'est le signal pilote  $y(t)$  qui force le système esclave à suivre le comportement du système maître ce qui permet, à terme, une

synchronisation entre les systèmes (1) et (2). Nous allons maintenant présenter une méthode basée sur la notion de "maître - esclave" qui permet de réaliser cette synchronisation.

### II. 1.2.2 Techniques de synchronisation du chaos [3]

Les méthodes traditionnelles de synchronisation chaotiques sont en générale basées sur l'utilisation des circuits identiques. Supposons deux systèmes chaotiques identiques oscillant de façon totalement indépendante. Si par un moyen quelconque, on leur permet d'échanger de l'énergie, action que le nomme 'couplage', les deux systèmes finiront par céder la place à un comportement commun : ils se synchronisent. Il est possible de coupler les systèmes chaotiques dans un sens (couplage unidirectionnel) ou dans les deux sens (couplage bidirectionnel). Dans le cas d'un couplage unidirectionnel, l'énergie est transférée d'un système à l'autre, à l'aide d'un élément de couplage fonctionnant dans un seul sens comme par exemple *un suiveur*. Par contre, dans le couplage bidirectionnel, l'élément de couplage permet l'échange de l'énergie dans les deux sens. Ceci peut être par exemple une simple résistance.

Les deux types de couplages, unidirectionnel et bidirectionnel, peuvent aussi être appliqués aux systèmes non identiques. Le couplage bidirectionnel de circuits non identiques ne sera pas traité dans ce mémoire.

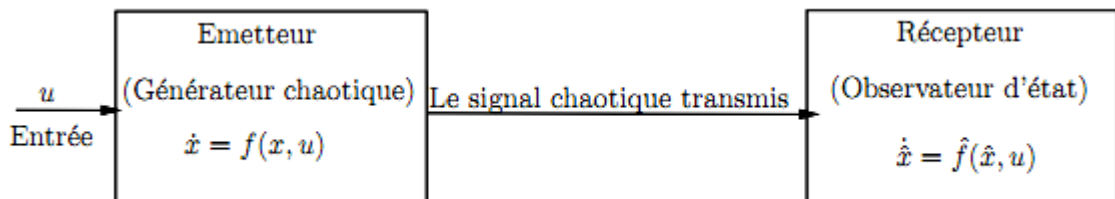
En plus du couplage simple (la résistance ou suiveur), d'autres méthodes ont été proposées pour la synchronisation des systèmes chaotiques. Ainsi pour la synchronisation unidirectionnelle on peut citer la méthode par décomposition en sous systèmes, la synchronisation impulsive ou la synchronisation par la boucle fermée.

Dans la majorité des cas, les deux systèmes doivent avoir des structures identiques, ce qui n'est pas tout à fait réalisable en pratique. Un petit écart entre les valeurs des composants peut entraîner un écart considérable entre les comportements des deux circuits et détruire le phénomène de synchronisation.

La méthode utilisée dans notre mémoire est un couplage unidirectionnel par observateur.

➤ **Synchronisation à l'aide d'observateur [8]**

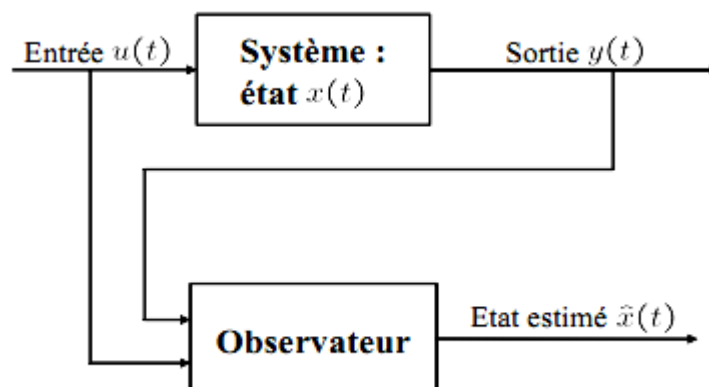
Après la découverte de Pecora-Carroll de la possibilité de synchronisation du chaos, le problème de synchronisation a été rapidement relié au problème plus général de l'observation d'état non linéaire classique. Dans cette approche, Le système maître est un système chaotique quelconque et le système esclave est un observateur d'état correspondant.



**Figure(II.3) :** principe de la synchronisation à base d'observateurs

**Définition** De manière générale, un observateur est un système dynamique qui permet la reconstruction de l'état d'un système dynamique, à partir de ses entrées, de ses sorties, et de la connaissance de son modèle, qui sont les seules informations disponibles. C'est une méthode typique afin d'estimer les états inconnus d'un système dynamique qui ne peuvent pas être mesurées directement : soit par ce qu'ils sont inaccessible, soit par économie.

Ce principe est illustré par la Figure (II.4)



**Figure (II.4) :** Principe de l'observateur

Théoriquement, le problème de la conception d'un observateur pour un système (non linéaire) donné est posé comme suit.

$$\| x(t) - \hat{x}(t) \| \rightarrow 0 \text{ quand } t \rightarrow \infty \quad (\text{II.4})$$

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

### a. Observabilité des systèmes

#### ➤ Observabilité d'un système linéaire

Considérons le système linéaire défini par les équations suivantes :

$$\begin{cases} \dot{x}(t) = Ax \\ y(t) = Cx \end{cases} \quad (\text{II.5})$$

Où  $x \in \mathbb{R}^n$  et  $y \in \mathbb{R}^p$  et  $A, C$  sont des matrices de dimensions appropriées. Le système est observable, c'est-à-dire qu'on peut retrouver les états d'origine du système à partir de ses sorties, lorsque :

$$\text{rang}(O) = \text{rang} \begin{pmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{pmatrix} = n \quad (\text{II.6})$$

#### ➤ Observabilité d'un système non linéaire [3]

Considérons maintenant le système non linéaire :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \quad (\text{II.7})$$

Avec  $t \geq 0$

$x \in \mathbb{R}^n$  est le vecteur d'état,  $y \in \mathbb{R}^p$  est le vecteur de sortie, les fonctions  $f, h$  sont des vecteurs de fonctions analytiques de dimensions appropriées.

### Conditions du rang d'observabilité

Pour donner la condition du rang d'observabilité il faut d'abord définir la dérivée de Lie, qui est une notion largement utilisée dans l'étude d'observabilité des systèmes non linéaires.

#### Définition (dérivée de Lie)

Considérons  $h$  une fonction  $C^\infty$  de  $\mathbb{R}^n$  dans  $\mathbb{R}$ . On définit la dérivée de Lie de  $h$  dans la direction de  $f$ , notée  $L_f h$ , la dérivée de  $h$  le long de la courbe intégrale de  $f$  en  $t = 0$  :

$$L_f h(x) = \sum_{i=1}^n f_i(x) \frac{\partial h}{\partial x_i}(x) \quad (II.8)$$

Par définition on écrit :  $L_f^0 h = h$  et  $L_f^k h = L_f(L_f^{k-1} h), \forall k \geq 1$ .

Le système (3.13) satisfait la condition du 'rang d'observabilité' si :

$$\text{Rang} \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1}(h) \\ \vdots \\ dL_f^\infty h \end{pmatrix} = n \quad (II.9)$$

Si la condition du rang d'observabilité est vérifiée en  $x, \forall x \in U, U$  étant un voisinage de  $x^0$ , le système (II.7) est localement faiblement observable en  $x^0$ .

Pour l'application non linéaire, nous définissons la condition du rang d'observabilité 'pratique' comme suit :

$$\text{Rang} \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{pmatrix} = n \quad (II.10)$$

### b. Observateur de Luenberger [9]

La théorie de l'observation de Luenberger repose essentiellement sur des techniques de placement de pôles.

Soit le système linéaire :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \end{cases} \quad (II.11)$$

Où

$x(t) \in R^n$  ,  $u(t) \in R^m$ ,  $y(t) \in R^p$ , Les matrices du système sont de dimensions appropriées, et les conditions initiales sont définies par  $x(t_0) = x_0$ .

Luenberger propose l'observateur suivant pour le système (II.11)

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + K(y(t) - C\hat{x}(t)) \\ \hat{y}(t) = C\hat{x}(t) \end{cases} \quad (II.12)$$

Où

$\hat{x}(t)$  est l'estimé de  $x(t)$

$\hat{y}(t)$  est l'estimé de  $y(t)$

La dynamique de l'erreur d'estimation  $e(t) = x(t) - \hat{x}(t)$  a pour expression :

$$\dot{e}(t) = (A - KC) e(t) \quad (II.13)$$

En utilisant une technique de placement de pôles, il suffit alors de choisir le gain  $K$  de l'observateur de telle sorte que les valeurs propres de la matrice  $A - KC$  soient dans le demi-plan complexe gauche.

### Remarque

L'utilisation de ce type d'observateur dans le cas non linéaire nécessite une transformation dont le but est de se rapprocher du cas linéaire, que l'on sait traiter. Pour ce faire, il existe plusieurs approches. Ces approches font appel à des transformations non linéaires de l'état d'un système afin de rendre la dynamique de l'erreur d'estimation linéaire. Ainsi l'erreur d'estimation converge linéairement ou quasi linéairement dans un espace d'état qui est une transformation non linéaire du système de coordonnées original. On utilise alors des techniques linéaires pour construire un observateur linéaire, puis on applique la transformation inverse pour obtenir un observateur non linéaire pour le système de départ. L'application de ces transformations met le système initial sous la forme canonique d'observabilité généralisée : cela généralise la forme canonique d'observabilité définie dans le cas linéaire.

#### c. Observateur à grand gain [9], [17], [18]

Les techniques dites "à grand gain" peuvent être appliquées sans transformation du système initial : dans ce cas, la conception de l'observateur se fait directement à partir de la structure du système.

Considérons l'émetteur (système maître) comme suit :

$$\begin{cases} \dot{x} = f(x) = Ax + f(x) \\ y = h(x) = Cx \end{cases} \quad (II. 14)$$

est un d'observateur possible (système esclave) peut être conçu de la façon suivante

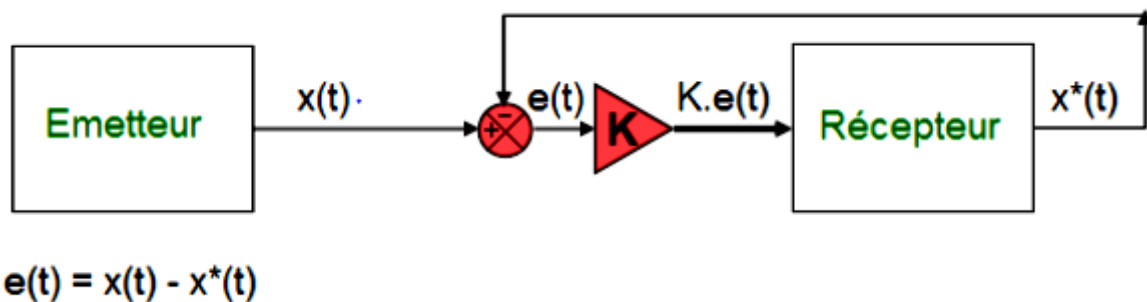
$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) = A\hat{x} + f(\hat{x}) + K(y - \hat{y}) \\ \hat{y} = h(\hat{x}) = C\hat{x} \end{cases} \quad (II.15)$$

En définissant l'erreur d'estimation  $e = x - \hat{x}$ , nous pouvons obtenir

$$\dot{e} = (A - KC)e + f(x) - f(\hat{x}) \quad (II.16)$$

Dans ce cas, le problème de la synchronisation devient celui de la stabilité au voisinage du point fixe : 0, du système (II.16). Si nous pouvons trouver un gain appropriée : K afin de garantir la stabilité du système (II.16), alors la synchronisation entre l'émetteur et le récepteur peut être réalisée.

Cette approche peut également être regardée comme un type de synchronisation par la boucle fermée puisque nous employons l'erreur entre l'émetteur et le récepteur pour corriger le comportement du récepteur afin de réaliser la synchronisation, comme le montre la figure(II.5) :



**Figure(II.5) :** Principe de la synchronisation par boucle fermée

#### d. Commande par retour d'état

Pour stabiliser l'écart  $\dot{e}(t)$  nous utiliserons dans ce travail un retour d'état ;

#### Définition de la commandabilité

La commandabilité d'un système caractérise sa capacité à voir son comportement dynamique évoluer sous l'action du signal de commande  $u(t)$ . Un système linéaire est commandable s'il est possible de le conduire, en appliquant un signal d'entrée admissible  $u(t)$ .

Soit le système linéaire décrit par les équations (II.11)

$$\begin{cases} \dot{x}(t) = A(t)x + B(t)u(t) \\ y(t) = C(t)x(t) \end{cases}$$

La matrice de contrôlabilité  $M$  est :

$$M = [B \quad AB \quad \dots \quad A^{n-1}B]$$

Le système est commandable si le rang de la matrice de commandabilité est égal à la dimension du système,  $\text{rang}(M)=n$  ou encore le déterminant de  $M$  est différent de 0.

#### Retour d'état

L'objectif est de stabiliser le système (s'il n'est pas stable) ou de modifier son comportement dynamique en introduisant une contre-réaction déterminée à partir du vecteur d'état  $x(t)$ . En supposant que l'on a accès à toutes les variables d'état (variables mesurées). En désignant par  $v(t)$  le signal de référence (consigne), la loi de commande s'exprime de la manière suivante :

$$u(t) = -kx(t) + v(t) \quad (II.17)$$

Compte tenu de l'expression de la commande  $u(t)$  et du modèle du système en boucle ouverte, celui en boucle fermée est donné par :

$$\begin{cases} \dot{x}(t) = (A - Bk)x + B(t)v(t) \\ y(t) = (c - Dk)x(t) + Dv(t) \end{cases} \quad (II.18)$$

Le problème posé ici consiste à trouver un vecteur de gain  $K$  (gain de retour d'état) de telle sorte que la matrice d'état du système en boucle fermée  $(A - Bk)$  possède les valeurs propres désirées. Pour la stabilisation les valeurs propres doivent être dans la partie complexe négative (valeurs propres à partie réelle négative). Pour ce faire, on utilise souvent la méthode de placement de pôles.

### Exemple de placement de pôles

Les valeurs propres désirées  $(A - Bk)$ :  $\mu_1, \mu_2, \dots, \mu_n$  des valeurs à Parties réelles négatives et  $k$  la matrice de gain.

Soit le système

$$A = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -1 & -5 & -6 \end{bmatrix} \quad B = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

Etape 1 : Vérifier si le système est commandable

Matrice de commandabilité

$$M = [B \quad AB \quad A^2B] = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & -6 \\ 1 & -6 & 31 \end{bmatrix}$$

Rang(M) = 3 = n  $\rightarrow$  système commandable

Etape 2 : Du polynôme caractéristique de la matrice  $A$ , déterminer les coefficients  $a_1, a_2, \dots, a_n$  :

Polynôme caractéristique.

$$\det(sI - A) = s^n + a_1s^{n-1} + \dots + a_{n-1}s + a_n$$

$$\det(sI - A) = s^3 + 6s^2 + 5s + 1$$

Donc

$$a_1 = 6$$

$$a_2 = 5$$

$$a_3 = 1$$

Construire la matrice de transformation  $T = MW$ .

Matrice  $W$

$$W = \begin{bmatrix} a_{n-1} & \cdots & a_1 & 1 \\ \vdots & & a_1 & 1 & 0 \\ a_1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

Construire la matrice  $W$  :

$$W = \begin{bmatrix} a_2 & a_1 & 1 \\ a_1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 6 & 1 \\ 6 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

Obtenir la matrice de transformation  $T = MW$

$$T = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Etape 4

Choisir les valeurs propres désirées : Pôles en boucle fermée.

Écrire le polynôme caractéristique correspondant.

$$(s - \mu_1)(s - \mu_2) \cdots (s - \mu_n) = s^n + \alpha_1 s^{n-1} + \cdots + \alpha_{n-1} s + \alpha_n$$

Ce qui mène aux coefficients  $\alpha_1 \quad \alpha_2 \quad \cdots \quad \alpha_n$

Donc, si on choisi les pôles suivants:

$$s = -2 \pm 4j$$

$$s = -10$$

Cela mène à

$$(s + 2 - 4j)(s + 2 + 4j)(s + 10) = s^3 + 14s^2 + 60s + 200$$

Etape 5 : calcul de la matrice de gain  $K$

$$K = -[(\alpha_n - a_n) \quad (\alpha_{n-1} - a_{n-1}) \quad \cdots \quad (\alpha_1 - a_1)]T^{-1}$$

Dans l'exemple

$$K = -[(200-1) \quad (60-5) \quad (14-6)] \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$
$$= -[199 \quad 55 \quad 8]$$

## II.2 Généralité sur la transmission sécurisée

La capacité de synchronisation, dérivant de la théorie plus générale du contrôle du chaos, a ouvert la voie à de nombreuses applications, parmi lesquelles : les systèmes de communications sécurisées. Une discipline qui connaît un essor important depuis son passage du secret des laboratoires militaires au domaine public. En effet, les années 1990 ont été marquées par l'explosion des systèmes de communication qui a nécessité l'amélioration des techniques de sécurisation de ces communications. La cryptographie est alors devenue une véritable science dans le domaine universitaire.

### II.2.1 Introduction à la communication sécurisée

#### Communication sécurisée

Dès que l'on désire communiquer de manière secrète, deux problèmes se posent. Il faut s'assurer :

- que l'information ne va pas être reçue par une personne autre que son destinataire légitime (menace contre la confidentialité de l'information).
- que l'information ne provient pas d'une personne autre que son véritable auteur, ou n'a pas été modifiée durant son transfert (menace contre l'intégrité de l'information).

La confidentialité est assurée en chiffrant le message envoyé, c'est-à-dire en le transformant de manière à le rendre illisible pour toute personne ne connaissant pas la clé de déchiffrement, tandis que l'intégrité est garantie par une signature électronique du message.

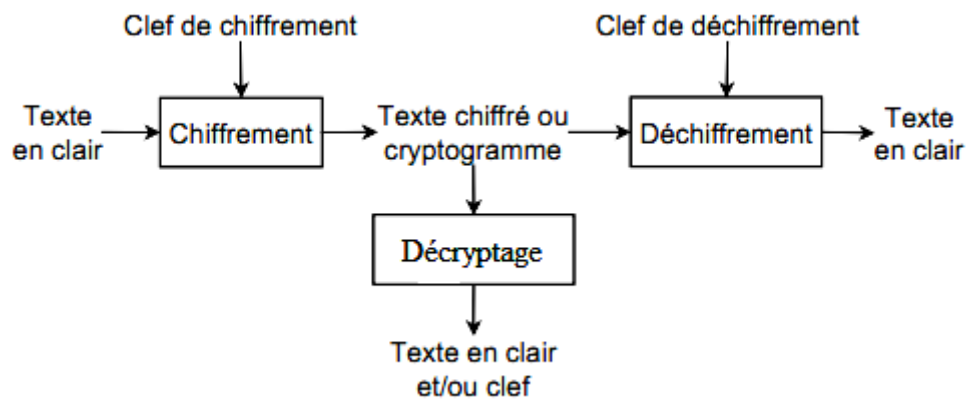
#### ➤ Cryptologie

La cryptologie (du grec (kryptos) : caché et (graphein) : écrire) est une science mathématique qui comporte deux branches : la cryptographie et la cryptanalyse.

La cryptographie traditionnelle est l'étude des méthodes permettant de transmettre des données de manière confidentielle. Afin de protéger un message, on lui applique une

transformation qui le rend incompréhensible ; c'est ce qu'on appelle le chiffrement, qui, à partir d'un texte en clair, donne un texte chiffré ou cryptogramme. Inversement, le déchiffrement est l'action qui permet de reconstruire le texte en clair à partir du texte chiffré. Dans la cryptographie moderne, les transformations en question sont des fonctions mathématiques, appelées algorithmes cryptographiques, qui dépendent d'un paramètre appelé clef.

La cryptanalyse, à l'inverse, est l'étude des procédés cryptographiques dans le but de trouver des faiblesses et, en particulier, de pouvoir décrypter des textes chiffrés. Le décryptement est l'action consistant à retrouver le texte en clair sans connaître la clef de déchiffrement.



**Figure (II.6) :** Cryptographie et cryptanalyse

### Remarque

Les termes "cryptage" et "crypter" sont des anglicismes, dérivés de l'anglais *to encrypt*, souvent employés à la place de chiffrement et chiffrer. Le "cryptage" pourrait être défini comme l'inverse du décryptage, c'est-à-dire comme l'action consistant à obtenir un texte chiffré à partir d'un texte en clair sans connaître la clef.

### ➤ **Cryptographie par chaos**

Dans les différentes applications actuellement envisagées, les signaux chaotiques servent soit à véhiculer l'information soit à réaliser le cryptage de données.

Nous nous intéressons au cryptage de données à transmettre et plus particulièrement dans un contexte de transmission sécurisée. En effet, un signal chaotique apparaît comme un « bruit » pseudo-aléatoire. Il peut donc être utilisé lors du cryptage de données, pour masquer les informations dans une transmission sécurisée : il suffit de le « mélanger » de manière appropriée au message à envoyer confidentiellement.

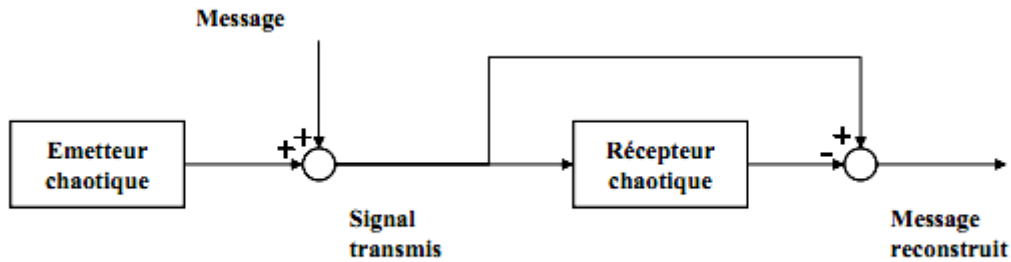
## **II.2.2 Technique de cryptage [8] [9]**

### **a. Cryptage par addition**

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

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

Dans tous les cas, à cause de la présence du message, la synchronisation ne peut être parfaite. En outre, la fréquence du message doit être comprise dans le spectre du signal chaotique. Un autre problème qui se pose naturellement concerne la présence d'un bruit additif au niveau du canal de transmission. Dans ce cas, il faut que l'amplitude du message soit plus grande que celle du bruit. Il y a donc un compromis à trouver entre la sécurité de la transmission, et la robustesse au bruit. Ce compromis va s'exprimer dans toutes les techniques que nous présentons dans ce mémoire.



**Figure (II.7)** Principe du cryptage par addition

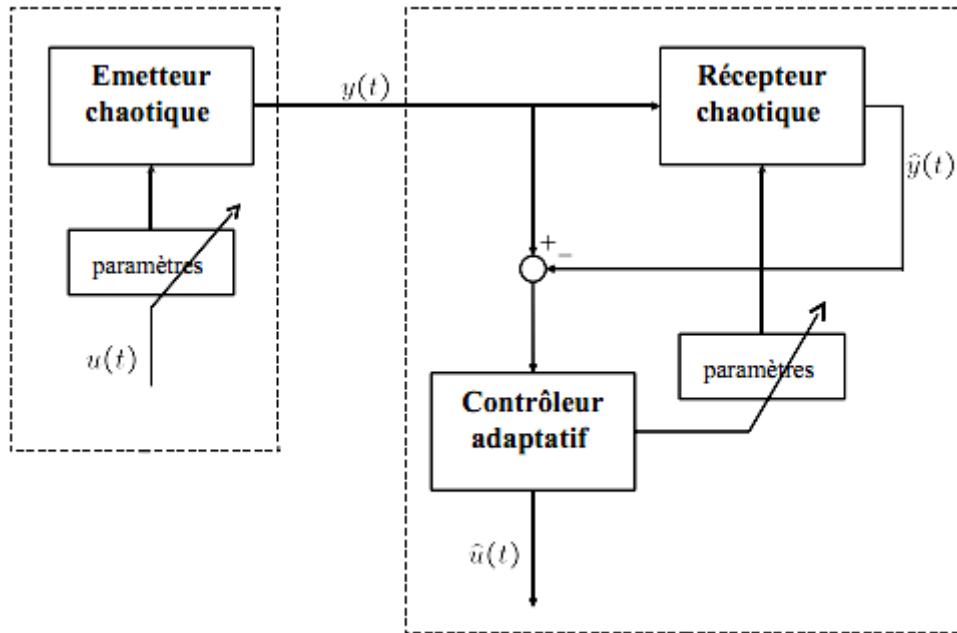
### b. Cryptage par inclusion

Dans le cryptage par inclusion, le message source est inclus dans la structure du système chaotique du côté de l'émission. Dans ce cas, un observateur doit être utilisé à la réception pour récupérer le message original. Cette méthode nécessite un seul canal de transmission.

### c. Cryptage par modulation

Cette technique utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la (II.8).

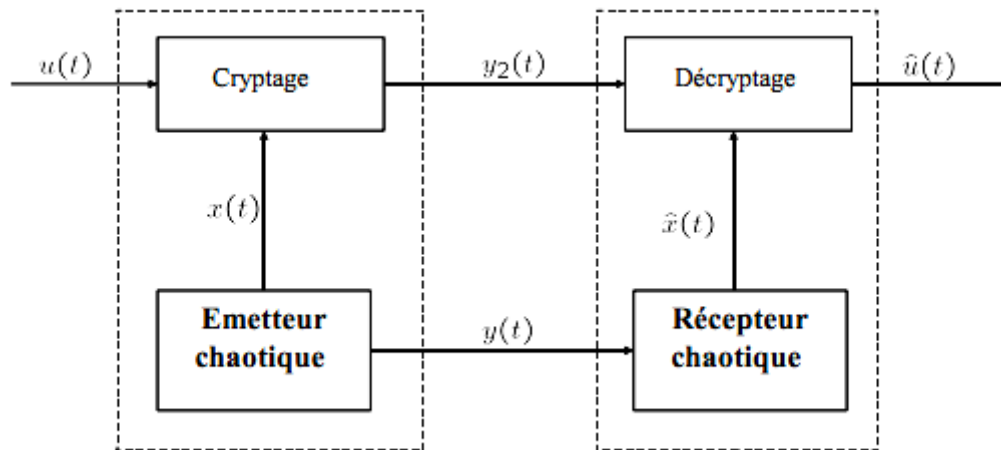
Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique "normal". Cependant, la façon d'injecter le message et donc la fonction de modulation des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



**Figure (II.8)** Cryptage par modulation

### II.2.3 Transmission à deux voies

Dans le schéma présenté à la figure (II.9), l'émetteur envoie deux signaux au récepteur. Le premier,  $y$ , est une fonction à valeurs réelles de l'état  $x$  du système chaotique émetteur, dont l'unique but est de permettre la synchronisation du récepteur. Le second,  $y_2$  envoyé éventuellement sur un autre canal - est un signal chaotique qui contient l'information à transmettre. Parmi les avantages de cette méthode, on peut souligner d'une part que le signal  $y$  ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale. D'un autre côté, le second signal  $y_2$  contient l'information qui peut être soit cryptée par une fonction non linéaire de l'état  $x$ , soit simplement masquée par un signal chaotique généré par l'émetteur, qui sert de porteuse. On peut noter également que les deux étapes de synchronisation et de cryptage étant totalement indépendantes, le décryptage n'est pas nécessairement effectué, au niveau du récepteur, en même temps que la synchronisation.



**Figure (II.9) :** Transmission à deux voies

#### II.2.4 Conclusion

La découverte de la possibilité de synchronisation du chaos avait permis l'utilisation du chaos dans divers domaines notamment la transmission sécurisée de données. Pour ce faire, il existe diverse méthodes de synchronisation du chaos, parmi lesquelles : la synchronisation à l'aide d'observateur présenté dans la première partie de ce chapitre.

Dans la deuxième partie nous avons donné des notions de transmission sécurisée des données en utilisant le chaos. En exposant d'abord la terminologie utilisée en transmission sécurisée puis quelques méthodes de cryptage.

### III.1 Introduction

Ce chapitre est consacré à la synchronisation de deux systèmes chaotiques identiques (émetteur et récepteur). Pour cela, nous allons appliquer un retour d'état afin de réaliser leur synchronisation à l'aide d'observateur.

Dans un premier, temps nous allons définir un oscillateur, ensuite étudier a un oscillateur appelé « système de Qi », par la caractérisation de chaos dans ce dernier par les exposants de Lyapunov et le spectre de puissance. Ensuite nous allons synthétiser un observateur en linéarisant le système d'erreur par un retour d'état, puis nous définiront les équations mathématiques de notre récepteur. Par la suite nous le simulerons sur Matlab.

### III.2 Emetteur

Afin de générer un signal chaotique et envoyer un message, nous avons besoin d'un oscillateur électronique.

#### III.2.1 Oscillateur électronique

Un oscillateur électronique est un montage électronique autonome, dont la fonction principale est de produire un signal périodique lors de sa mise sous tension, la forme du signal peut être sinusoïdale, carrée, voire en dents de scie, ou quelconque.

### III.2.2 Structure générale d'un oscillateur

Un oscillateur comporte toujours un élément actif (circuit amplificateur) associé à circuit passif (un filtre). L'élément actif est souvent un transistor bipolaire ou un amplificateur opérationnel.

Sa structure est celle d'un système bouclé dans lequel une fraction du signal de sortie est ramenée à l'entrée pour assurer l'auto entretien des oscillations. D'une façon générale, un oscillateur est représenté par le schéma bloc ci-dessous :

Si le signal  $V_r(t)$  est identique à  $V_e(t)$ , alors peut le boucler à l'entrée de l'amplificateur et pour obtenir  $V_s(t)$  souhaité sans appliquer de signal de commande extérieur.

Cette condition n'est satisfaite que pour une fréquence bien définie appelée fréquence d'oscillation. La structure d'un tel oscillateur se reconnaît par le fait que la sortie de l'amplificateur est rebouclée sur l'entrée via le réseau de réaction qui est, rappelons le, un circuit passif.

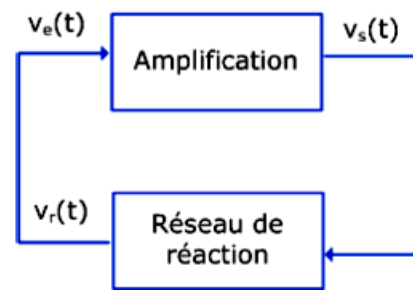


Figure (III.1)

Cependant, dans la pratique, les oscillations prennent naissance à partir de fluctuations qui sont amplifiées, ce qui nécessite un gain plus grand que l'unité.

### III.2.3 Système hyperchaotique de Qi [10]

L'oscillateur que nous allons étudier est le système de Qi, ce dernier est régi par les équations suivantes

$$\dot{x}_1 = a(x_2 - x_1) + x_2x_3 \quad (\text{III.3})$$

$$\dot{x}_2 = b(x_1 + x_2) - x_1x_3 \quad (\text{III.4})$$

$$\dot{x}_3 = -cx_3 - ex_4 + x_1x_2 \quad (\text{III.5})$$

$$\dot{x}_4 = -dx_4 + fx_3 + x_1x_2 \quad (\text{III.6})$$

Où

$x_i$  ( $i= 1, 2, 3, 4$ ) sont des variables d'état.

$a, b, c, d, e, f$ , sont des constantes positives.

#### III.2.3.1 Caractérisation du chaos dans le système de Qi

Le chaos est défini par caractéristiques qui le différencie des autres signaux et permet de le classer autant que chaos ou bien hyper chaos.

##### a. Exposants de Lyapunov

La figure (III.2) représente l'exposant de Lyapunov avec  $15.425 \leq b \leq 27$ ,  $a = 50$ ,  $c = 13$ ,  $d = 8$ ,  $e = 33$  et  $f = 30$

On peut observer qu'il y a deux exposants de Lyapunov positifs sur tout un intervalle de valeurs de paramètres. Pendant que le paramètre  $b$  varie, comme on le voit sur la figure, le premier exposant  $L_1$  est très grand ( $8.3585 \leq L_1 \leq 13.4632$ ) le deuxième exposant de Lyapunov  $L_2$  est assez grand ( $12 \leq 20.1L_2 \leq 3.4781$ ), le troisième exposant est approximativement nul, et le quatrième est négatif ( $L_4 < -60$ ).

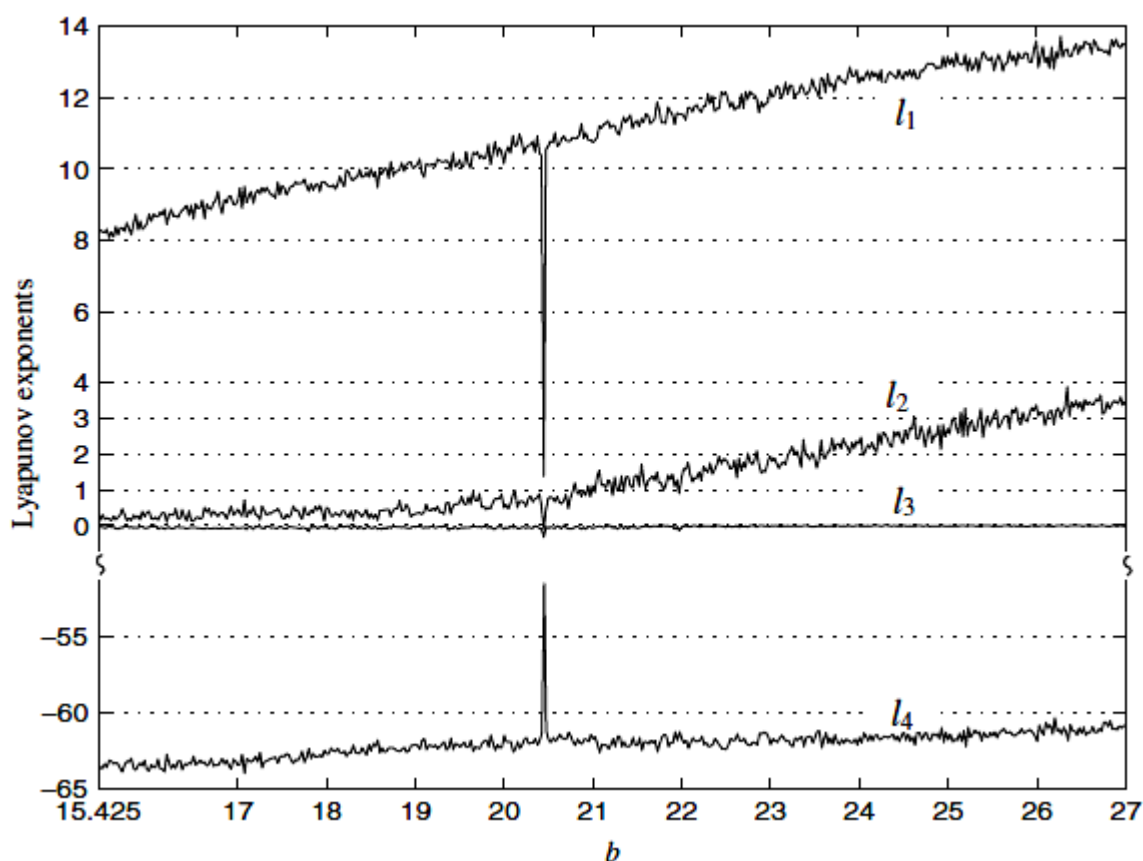


Figure (III.2) : graphe des exposants de Lyapunov [10]

### b. Spectre de puissance

Comme nous l'avons vu dans le chapitre précédent, le spectre de puissance est la transformée de Fourier de la fonction d'autocorrelation.

Le spectre de puissance d'un système chaotique est continu et évolue de manière exponentielle vers zéro comme le montre la figure (III.4)

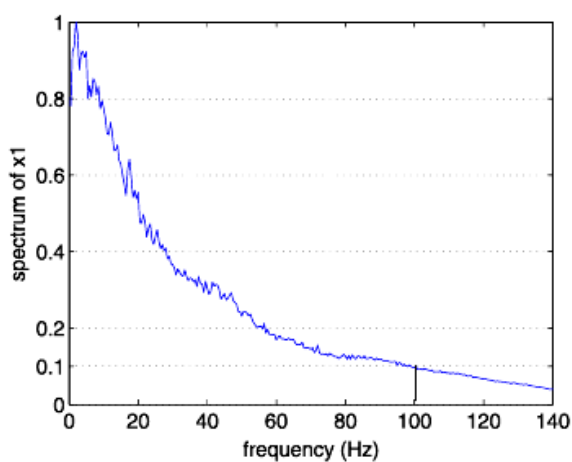
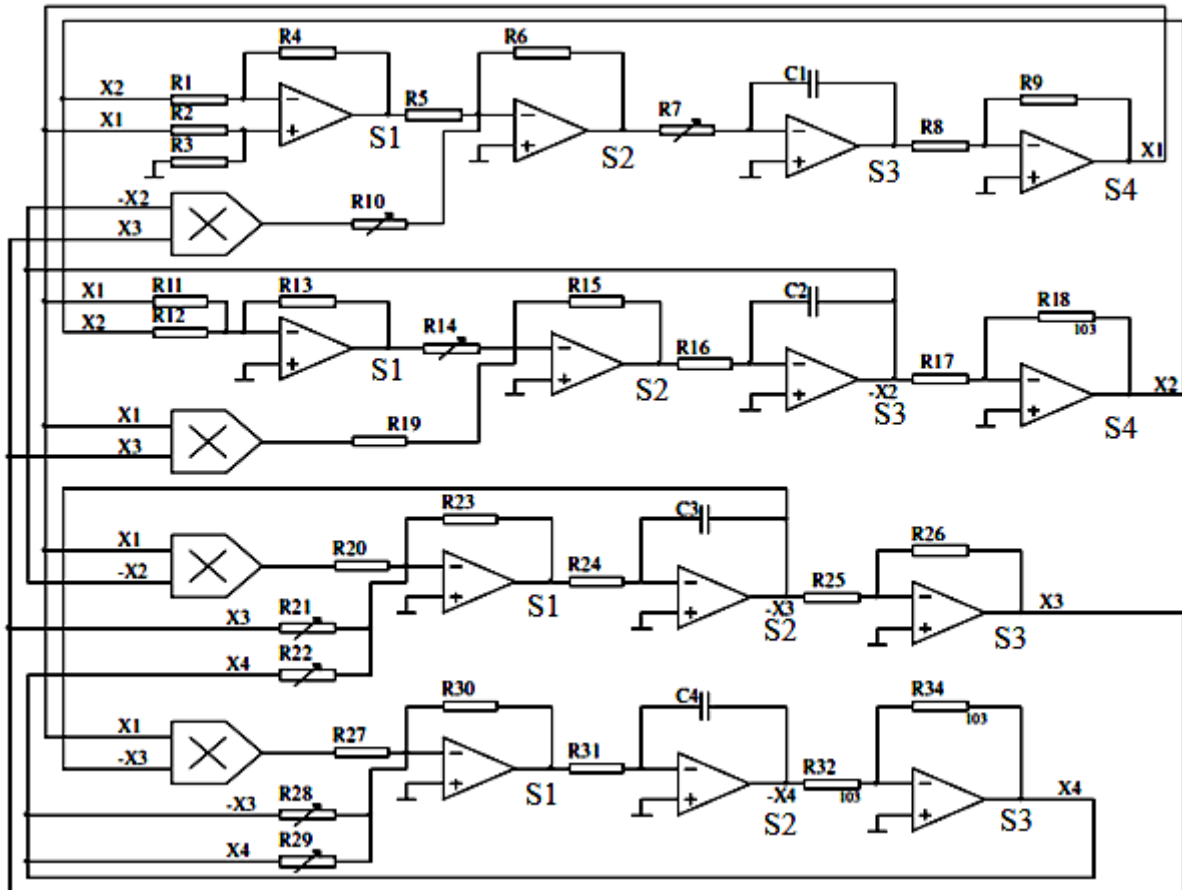


Figure (III.4) : Spectre de puissance du Système de Qi [10]

## c. Schéma électronique du système

Le schéma suivant représente la réalisation des équations précédentes sous forme de circuit électronique :



**Figure (III.5)** : schéma de réalisation du système hyperchaotique de Qi [10]

Avec :

$R_1, R_2, R_3, R_4, R_5, R_6, R_8, R_9, R_{11}, R_{12}, R_{13}, R_{15}, R_{17}, R_{18}, R_{23}, R_{25}, R_{26}, R_{30}, R_{32}, R_{33} = 10\text{k}\Omega$  ;  $R_{16}, R_{24}, R_{31} = 100\text{k}\Omega$  ;  $R_7 = 20\text{k}\Omega$  ;  $R_{14} = 4.17\text{k}\Omega$  ;  $R_{21} = 7.69\text{k}\Omega$  ;  $R_{22} = 3.03\text{k}\Omega$  ;  $R_{28} = 3.33\text{k}\Omega$  ;  $R_{29} = 12.5\text{k}\Omega$  ;  $R_{10} = 500\Omega$  ;  $R_{19}, R_{20}, R_{27} = 100\Omega$  ;  $C_i = 5$  (N-F),  $i = 1, \dots, 4$ .

#### d. Etude du montage électrique

➤ Pour le premier étage :

**NB** : ( $S_1$  sortie du premier AOP,  $S_2$  sortie du deuxième AOP, et ainsi de suite)

$$V^+ = \frac{R_3}{R_2 + R_3} x_1 \quad (1)$$

Avec : ( $R_2 = R_3$ )

$$\text{L'équation (1) devient : } V^+ = V^- = \frac{1}{2} x_1 \quad (2)$$

$$S_1 - V^- = R_4 \cdot i \quad (3)$$

$$x_2 - V^- = R_1 \cdot i \Rightarrow i = \frac{x_2 + V^-}{R_1} \quad (4)$$

On remplace (4) dans (3):

$$S_1 = V^- - R_4 \frac{x_2 + V^-}{R_1} \quad (5)$$

On remplace (2) dans (5):

$$S_1 = \frac{1}{2} x_1 - (x_2 - \frac{1}{2} x_1) = (x_2 - x_1)$$

$$S_2 = R_6 \cdot i$$

On a:  $i = i_1 + i_2$

$$\text{Avec: } i_1 = \frac{S_2}{R_5}, \quad i_2 = \frac{x_2 x_3}{R_{10}}$$

$$i = \frac{(x_1 - x_2)}{R_5} + \frac{x_2 x_3}{R_{10}}$$

$$S_2 = -\frac{R_6}{R_5} (x_2 - x_1) + \frac{R_6}{R_{10}} x_2 x_3$$

$$S_3 = -\frac{1}{C} \int i \, dt, \quad i = \frac{S_2}{R_7}$$

$$\dot{x}_1 = \frac{R_6}{R_5} (x_2 - x_1) + \frac{R_6}{R_{10}} (x_2 x_3) \quad (7)$$

$$x_1 = -\frac{1}{R_7 C_1} \int \left( \frac{R_6}{R_5} (x_2 - x_1) + \frac{R_6}{R_{10}} (x_2 x_3) \right) dt$$

➤ **Pour le deuxième étage :**

$$S_1 = R_{13} \cdot i \quad (8) \quad , \quad i = i_1 + i_2 \quad (9)$$

Avec:

$$i_1 = \frac{X_1}{R_4} \quad , \quad i_2 = \frac{X_2}{R_{12}}$$

On remplace (9) dans (8) et on obtient :

$$S_1 = R_{13} \left( \frac{X_1}{R_4} + \frac{X_2}{R_{12}} \right) = -(x_1 + x_2)$$

$$S_2 = R_{15} \cdot i \quad (10)$$

$$i = i_1 + i_2 \quad (11)$$

Avec

$$i_1 = \frac{S_2}{R_{14}}$$

$$i_2 = \frac{X_1 X_3}{R_{19}}$$

On remplace (11) dans (10) et on obtient :

$$S_2 = R_{15} \left( \frac{S_2}{R_{14}} + \frac{X_1 X_3}{R_{19}} \right)$$

$$S_3 = -\frac{1}{C} \int i \, dt$$

$$\dot{x}_2 = \frac{R_{15}}{R_{14}} (x_1 + x_2) - \frac{R_{15}}{R_{19}} (x_1 x_3) \quad (12)$$

$$x_2 = -\frac{1}{R_{16} C_2} \int \left( \frac{R_{15}}{R_{14}} (x_1 + x_2) - \frac{R_{15}}{R_{19}} (x_1 x_3) \right) dt$$

➤ **Pour le troisième étage :**

$$S_1 = R_{23} \cdot i \quad (13)$$

$$i = i_1 + i_2 + i_3 \quad (14)$$

Avec:

$$i_1 = \frac{X_1 X_2}{R_{20}}$$

$$i_2 = \frac{X_3}{R_{21}}$$

$$i_3 = \frac{X_4}{R_{22}}$$

On remplace (14) dans (13) et on obtient :

$$S_1 = R_{23} \left( \frac{X_1 X_2}{R_{20}} + \frac{X_3}{R_{21}} + \frac{X_4}{R_{22}} \right)$$

$$S_2 = -\frac{1}{C} \int i \, dt$$

$$\dot{x}_3 = -\frac{R_{23}}{R_{20}} x_3 - \frac{R_{23}}{R_{22}} x_4 + \frac{R_{23}}{R_{20}} (x_1 x_2) \quad (15)$$

$$x_3 = -\frac{1}{R_{24} C} \int \left( -\frac{R_{23}}{R_{20}} x_3 - \frac{R_{23}}{R_{22}} x_4 + \frac{R_{23}}{R_{20}} (x_1 x_2) \right) dt$$

► Pour le quatrième étage :

$$S_1 = -R_{30} i \quad (16)$$

$$i = i_1 + i_2 + i_3 \quad (17)$$

Avec

$$i_1 = -\frac{X_1 X_2}{R_{27}}$$

$$i_2 = -\frac{X_3}{R_{28}}$$

$$i_3 = \frac{X_4}{R_{29}}$$

On remplace (17) dans (16) et on obtient :

$$S_1 = R_{30} \left( -\frac{X_1 X_2}{R_{27}} - \frac{X_3}{R_{28}} + \frac{X_4}{R_{29}} \right)$$

$$S_2 = -\frac{1}{C} \int i \, dt$$

$$\dot{x}_4 = +\frac{R_{30}}{R_{28}} x_3 + \frac{R_{30}}{R_{29}} x_4 - \frac{R_{30}}{R_{27}} (x_1 x_2) \quad (18)$$

$$\dot{x}_4 = -\frac{1}{R_{31}C_4} \int \left( +\frac{R_{30}}{R_{28}} x_3 + \frac{R_{30}}{R_{29}} x_4 - \frac{R_{30}}{R_{27}} (x_1 x_2) \right) dt$$

Notre oscillateur comporte quatre étages et on a pu extraire ses équations :

$$\dot{x}_1 = \frac{R_6}{R_5} (x_2 - x_1) + \frac{R_6}{R_{10}} (x_2 x_3) \quad (\text{III.7})$$

$$\dot{x}_2 = \frac{R_{15}}{R_{14}} (x_1 + x_2) - \frac{R_{15}}{R_{19}} (x_1 x_3) \quad (\text{III.8})$$

$$\dot{x}_3 = -\frac{R_{23}}{R_{20}} x_3 - \frac{R_{23}}{R_{22}} x_4 + \frac{R_{23}}{R_{20}} (x_1 x_2) \quad (\text{III.9})$$

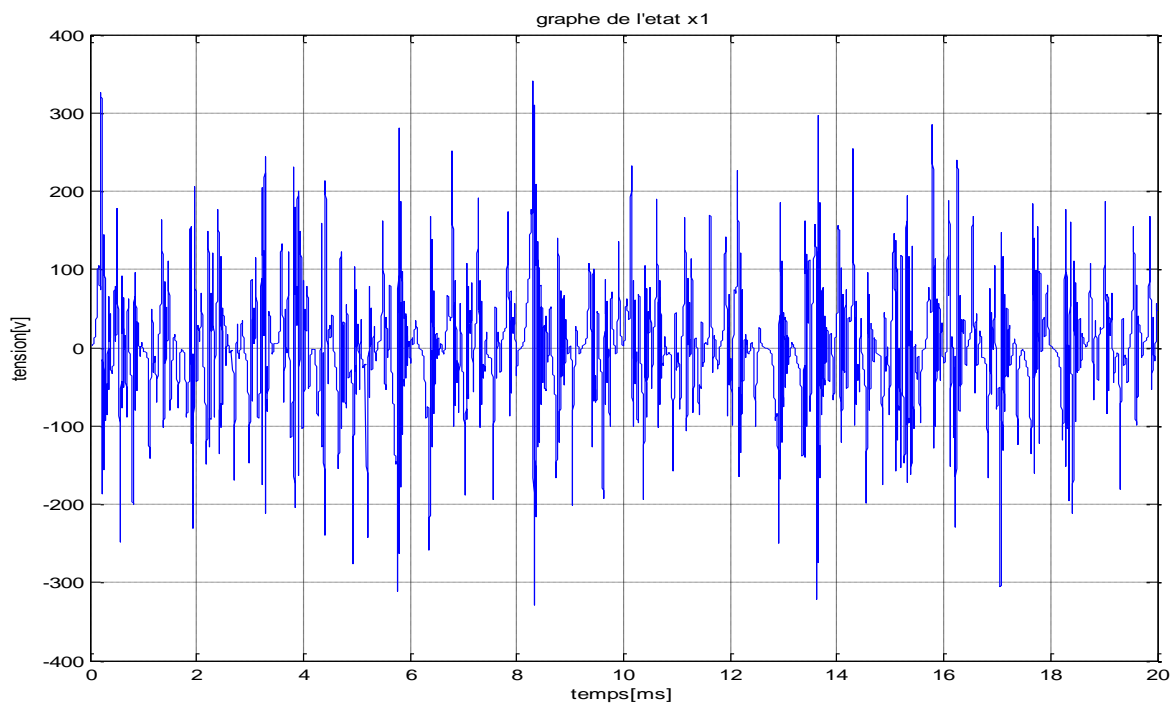
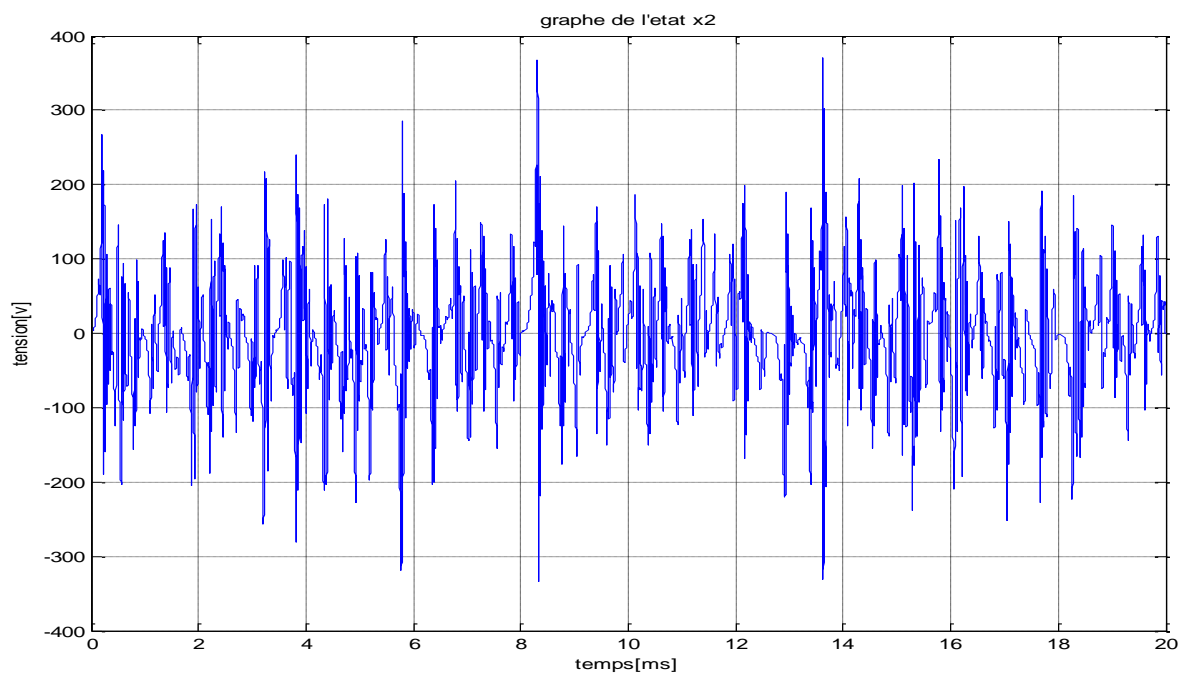
$$\dot{x}_4 = +\frac{R_{30}}{R_{28}} x_3 + \frac{R_{30}}{R_{29}} x_4 - \frac{R_{30}}{R_{27}} (x_1 x_2) \quad (\text{III.10})$$

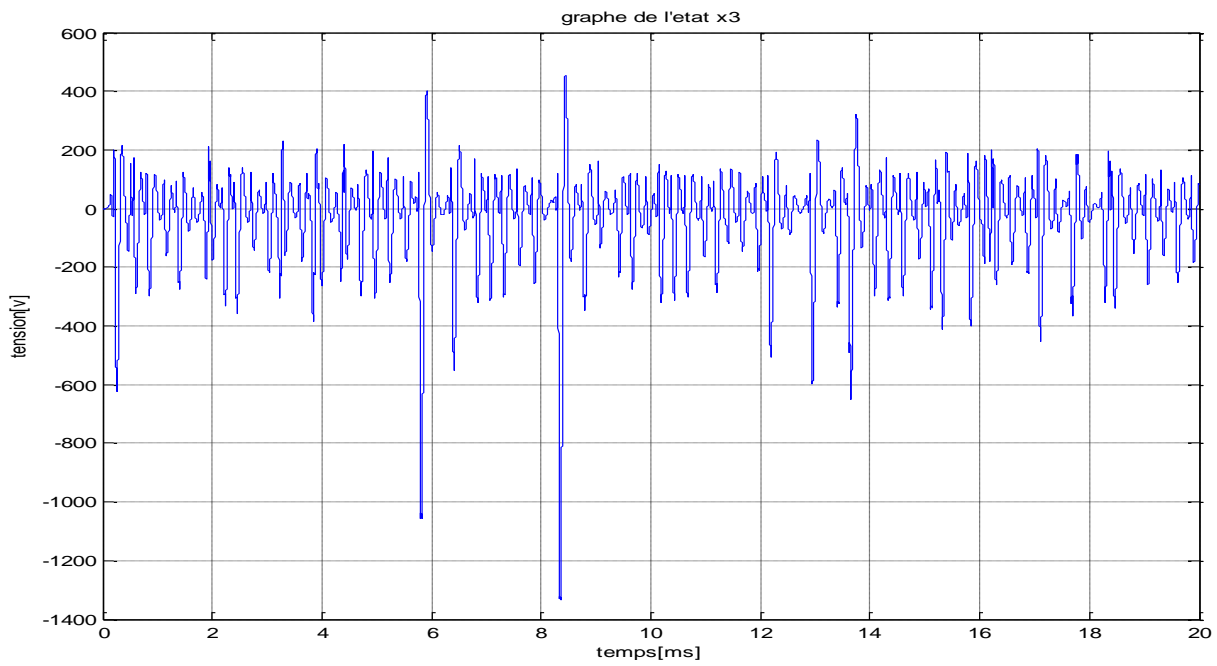
Et on jouant sur les valeurs des résistance variable on obtient les mêmes coefficients que les équations autonomes (III.3), (III.4), (III.5), (III.6) du système de Qi

### III.2.4 Simulation sous Matlab

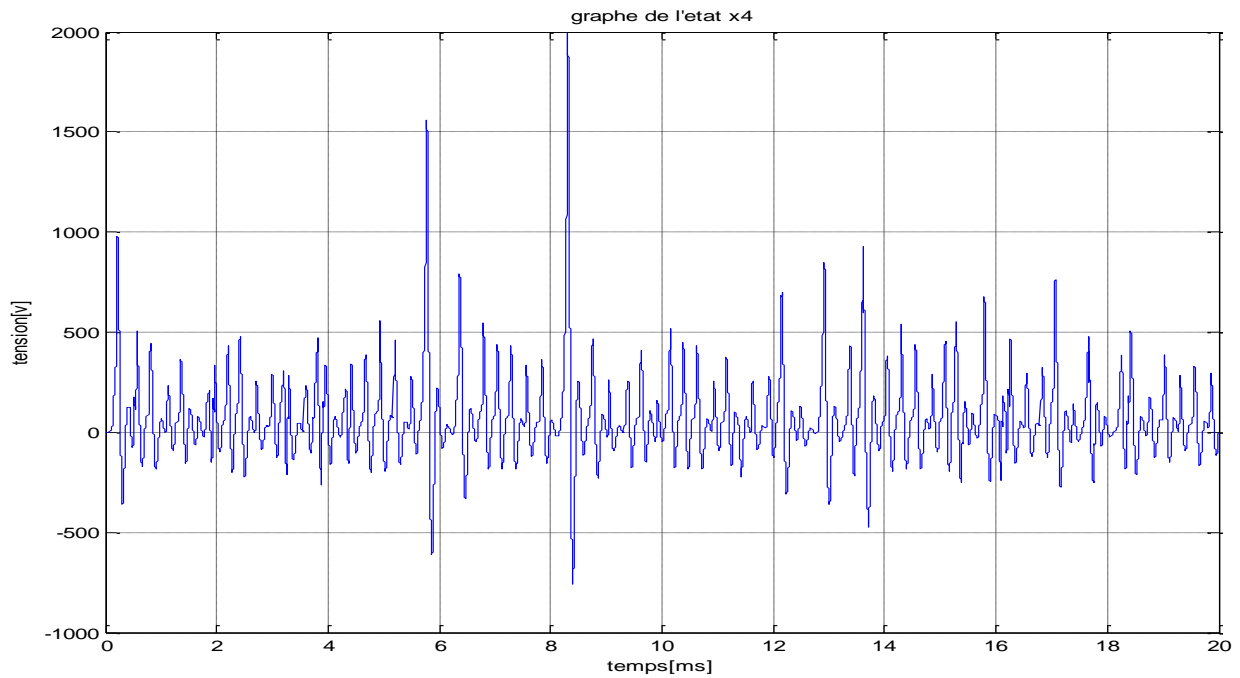
On insère les équations autonomes (III.3), (III.4), (III.5), (III.6) du système de Qi dans Matlab sur le schéma de la figure (2.1) (annexe B) et on observe le comportement de chaque étage durant la simulation.

La simulation se fera pour a=50; b=20; c=13; d=8; e=33; f=30;

**a. Visualisation des états****Figure (III.6) :** graphe de l'état  $x_1(t)$  du système de Qi**Figure (III.7) :** graphe de l'état  $x_2(t)$  du système de Qi



**Figure (III.8)** : graphe de l'état  $x_3(t)$  du système de Qi

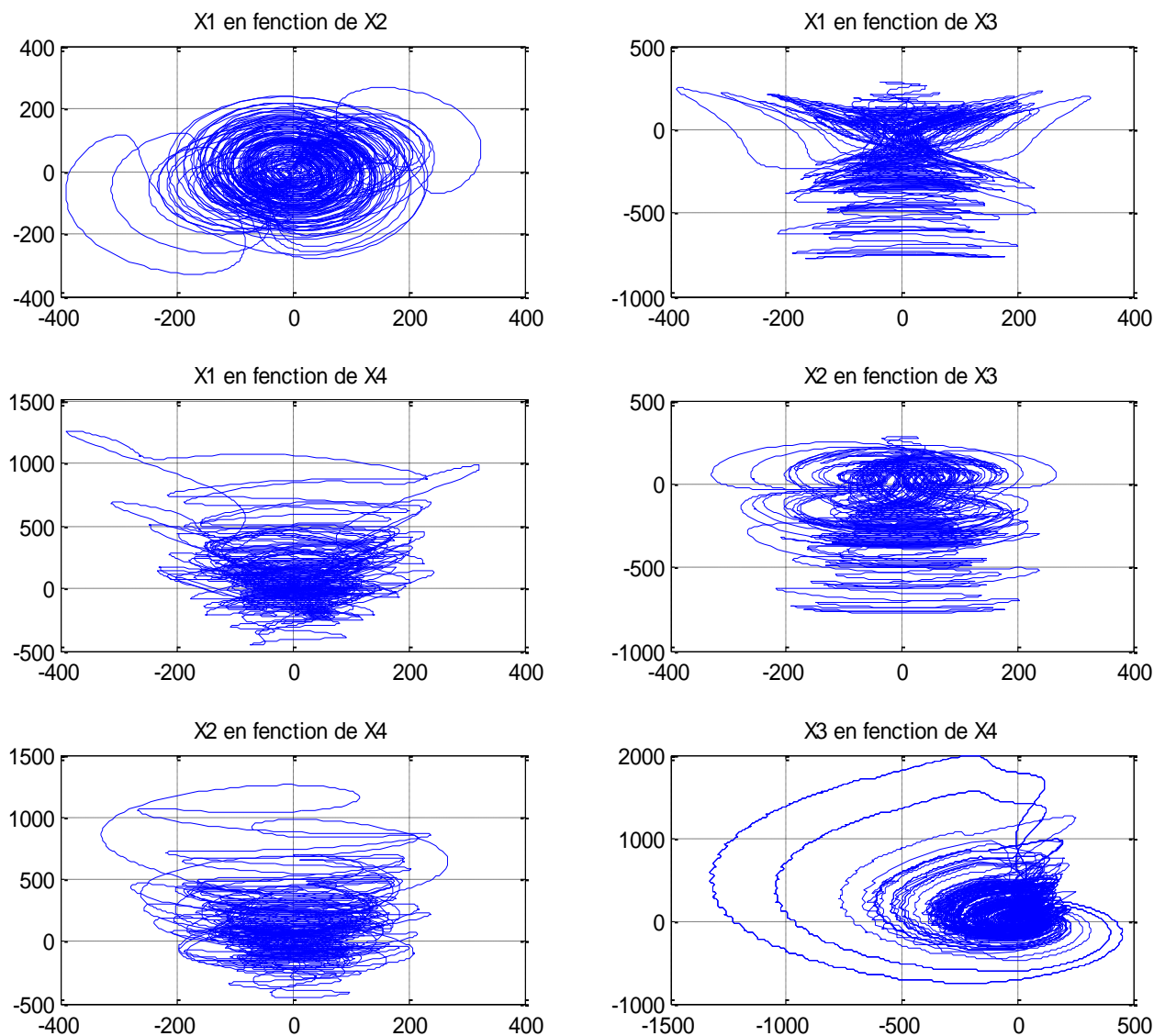


**Figure (III.9)** : graphe de l'état  $x_4(t)$  du système de Qi

Nous remarquons la présence d'oscillations irrégulières et apériodiques dans ces quatre dernières figures, les signaux  $x_1$ ,  $x_2$ ,  $x_3$ ,  $x_4$  sont des signaux chaotiques.

### b. Visualisation des attracteurs

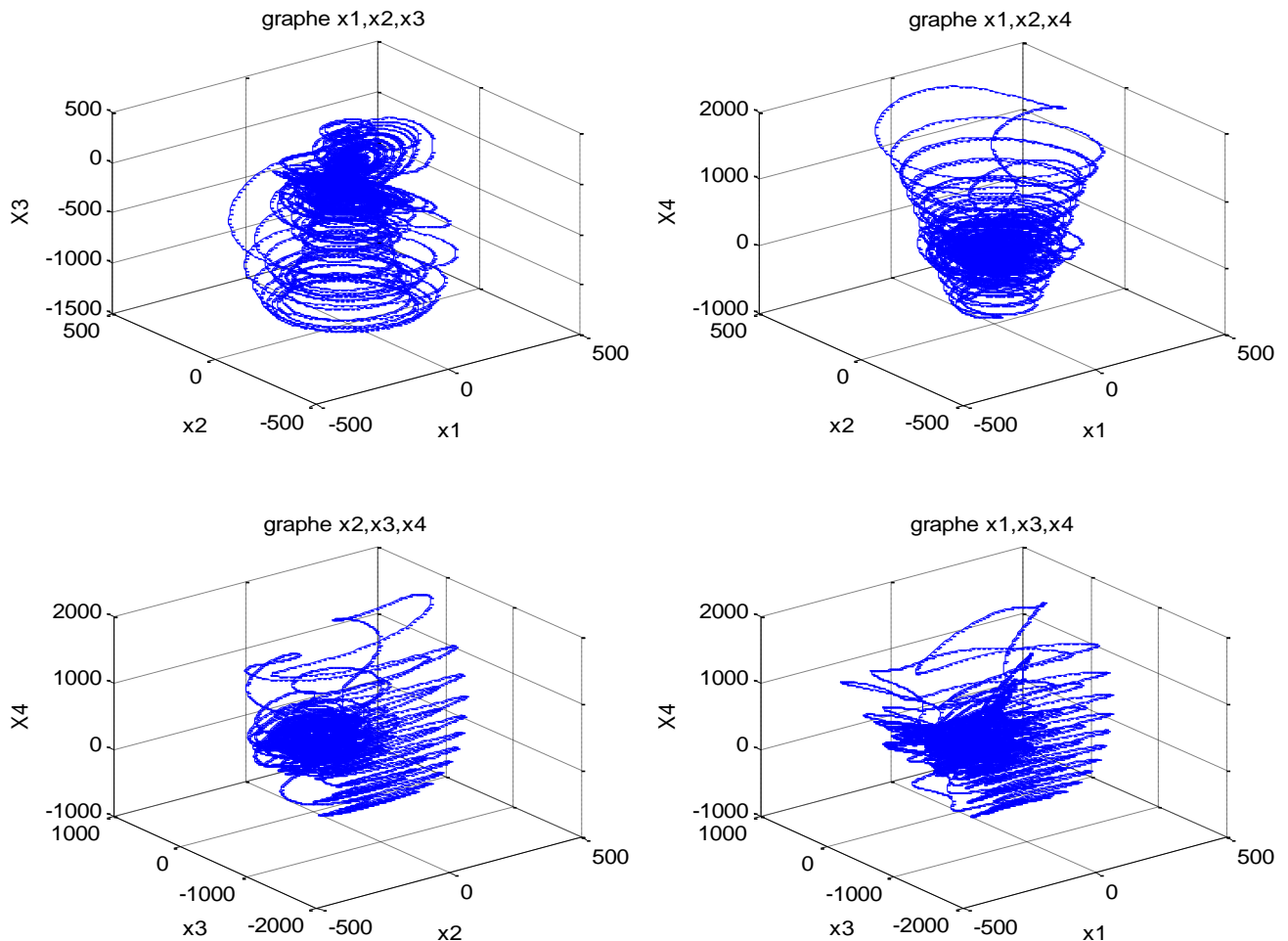
Nous allons maintenant observer les attracteur obtenus du système :



**Figure (III.10)** : les attracteurs de phase du système de Qi observés sous matlab

### c. Visualisation des attracteurs en trois dimension

Les orbites des états sont définies dans ces figures-ci :



**Figure (III.11) :** attracteur en trois dimension

Les figures ci-dessus démontrent l'aspect hyperchaotique du système de Qi, et que L'observation de ses attracteurs se fait à partir de plusieurs paramètres très sensible aux changements.

### III.3 Récepteur

L'utilisation d'observateurs est proposée pour estimer les états inconnus d'un système qui ne sont pas mesurables directement. Un système dynamique est dit observable si on peut récupérer toutes ses grandeurs par une combinaison de mesures et de leurs dérivées. En 1997, Nijmeijer et Mareels ont montré que la synchronisation unidirectionnelle de deux systèmes chaotiques peut être considérée comme un problème d'observateur non linéaire et par conséquent les théories d'automatique peuvent être utilisées afin d'analyser ce phénomène.

#### III.3.1 Condition du rang d'observabilité [3], [11]

Afin de vérifier si notre système est observable on applique la dérivé de Lie, si le rang de la matrice obtenue et égale au rang du système étudie alors ce dernier se révèle être observable.

$$\begin{cases} \dot{x} = f(x) \\ y = c(x) = h(t) \end{cases} \quad L_f h = \frac{dh}{dx} \cdot f \quad , \quad O = \begin{pmatrix} dH \\ dL_f H \\ dL_f^2 H \\ \vdots \\ dL_f^{n-1} H \end{pmatrix} \quad , \quad \text{rang}(O) = n$$

Considérons le système non linéaire défini par les équations suivantes :

$$f(x) = \begin{pmatrix} a(x_2 - x_1) + x_2 x_3 \\ b(x_1 + x_2) - x_1 x_3 \\ -cx_3 - ex_4 + x_1 x_2 \\ -dx_4 + fx_3 + x_1 x_2 \end{pmatrix} \quad , \quad y = (0 \ 0 \ x_3 \ 0) = h(t)$$

On a :

$$h(t) = x_3$$

$$L_f h(t) = x_1 x_2 - cx_3 - ex_4$$

$$L_f^2 h(t) = -x_1^2 x_3 + x_2^2 x_3 - 26x_1 x_2 + 20x_1^2 - 169x_3 + 533x_4$$

$$L_f^2 h(t) = -x_1^3 x_2 + x_2^2 x_1 + 83x_1^2 x_3 - 2000x_1^2 - 8x_4 x_1^2 + x_3 x_2^2 - 8x_4 x_2^2 - 102x_1 x_2 x_3^2 + 2224x_1 x_2 - 60x_1 x_2 x_3 + 500x_3 + 296x_4$$

Pour  $i = 1, \dots, 4$

$$\diamond dh/dx_i = (dh/dx_1 \quad dh/dx_2 \quad dh/dx_3 \quad dh/dx_4)$$

$$\diamond dL_f h/dx_i = (dL_f h/dx_1 \quad dL_f h/dx_2 \quad dL_f h/dx_3 \quad dL_f h/dx_4)$$

$$\diamond dL_f^2 h/dx_i = (dL_f^2 h/dx_1 \quad dL_f^2 h/dx_2 \quad dL_f^2 h/dx_3 \quad dL_f^2 h/dx_4)$$

$$\diamond dL_f^3 h/dx_i = (dL_f^3 h/dx_1 \quad dL_f^3 h/dx_2 \quad dL_f^3 h/dx_3 \quad dL_f^3 h/dx_4)$$

$$dh/dx_1 = 0$$

$$dh/dx_2 = 0 \quad (19)$$

$$dh/dx_3 = 1$$

$$dh/dx_4 = 0$$

$$dL_f h/dx_1 = x_2$$

$$dL_f h/dx_2 = x_1 \quad (20)$$

$$dL_f h/dx_3 = -13$$

$$dL_f h/dx_4 = -33$$

$$dL_f^2 h/dx_1 = (-2x_1 x_3 - 26x_2 + 40x_1)$$

$$dL_f^2 h/dx_2 = (2x_2 x_3 - 26x_1) \quad (21)$$

$$dL_f^2 h/dx_3 = (-x_1^2 + x_2^2 - 169)$$

$$dL_f^2 h/dx_4 = (533)$$

$$dL_f^3 h/dx_1 = (3x_1^2 x_2 + x_2^3 + 166x_1 x_3 - 4000x_1 - 16x_4 x_1 - 102x_2 x_3^2 + 2224x_2 - 60x_2 x_3)$$

$$dL_f^3 h/dx_2 = (x_1^3 + 3x_2^2 + 16x_4 x_2 - 108x_2 - 102x_1 x_3^2 + 2224x_1 - 60x_1 x_3) \quad (22)$$

$$dL_f^3 h/dx_3 = (83x_1^2 + x_1^2 + x_2^3 + 204x_1 x_2 x_3 - 60x_1 x_2 + 500)$$

$$dL_f^3 h/dx_4 = (-8x_2^2 + 296)$$

et avec les résultats obtenues (19) (20) (21) (22), on les réunit dans une matrice et on vérifie si son rang est égale au rang de notre système.

$$\begin{bmatrix} dh/dxi \\ dL_f h/dxi \\ dL_f^2 h/dxi \\ dL_f^3 h/dxi \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ x_2 & x_1 & -13 & -33 \\ dL_f^2 h/dx_1 & dL_f^2 h/dx_2 & dL_f^2 h/dx_3 & dL_f^2 h/dx_4 \\ dL_f^3 h/dx_1 & dL_f^3 h/dx_2 & dL_f^3 h/dx_3 & dL_f^3 h/dx_4 \end{bmatrix}.$$

Le rang du système est de 4 donc il vérifie le théorème de lie, et par conséquent notre système est observable.

### III.3.2 Synchronisation du système de Qi [3]

Dans cette section nous allons réaliser la synchronisation entre deux systèmes de Qi identiques définis comme émetteur et récepteur.

On choisira comme notation système maître « système de Qi » et système esclave comme notation pour le récepteur, pour se faire on appliquera la commande active.

- **Système maître :**

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) + x_2 x_3 \\ \dot{x}_2 &= b(x_1 + x_2) - x_1 x_3 \\ \dot{x}_3 &= -c x_3 - E x_4 + x_1 x_2 \\ \dot{x}_4 &= -d x_4 + f x_3 + x_1 x_2 \end{aligned} \quad (\text{III.11})$$

- **Système esclave :**

$$\begin{aligned} \hat{x}_1 &= a(\hat{x}_2 - \hat{x}_1) + \hat{x}_2 \hat{x}_3 + U_1 \\ \hat{x}_2 &= b(\hat{x}_1 + \hat{x}_2) - \hat{x}_1 \hat{x}_3 + U_2 \\ \hat{x}_3 &= -c \hat{x}_3 - E \hat{x}_4 + \hat{x}_1 \hat{x}_2 + U_3 \\ \hat{x}_4 &= -d \hat{x}_4 + f \hat{x}_3 + \hat{x}_1 \hat{x}_2 + U_4 \end{aligned} \quad (\text{III.12})$$

Avec :  $U(t) = [U_1(t), U_2(t), U_3(t), U_4(t)]^T$  vecteur de commande.

Pour réaliser la synchronisation du système maître défini en (III.11) avec le système esclave défini en (III.12). On applique une commande afin de forcer le système (III.12) à suivre le second système (III.11)

Définissant d'abord les écarts entre les états de l'esclave et du maître comme suit :

$$\begin{cases} e1 = \hat{x}1 - x1 \\ e2 = \hat{x}2 - x2 \\ e3 = \hat{x}3 - x3 \\ e4 = \hat{x}4 - x4 \end{cases} \quad (\text{III.13})$$

Après la soustraction de l'équation (III.11) de l'équation (III.12) on obtient le système suivant :

$$\dot{\hat{x}}1 - \dot{x}1 = -a(\hat{x}1 - x1) + a(\hat{x}2 - x2) - x2x3 + \hat{x}2\hat{x}3 + U1$$

$$\dot{\hat{x}}2 - \dot{x}2 = +b(\hat{x}1 - x1) + b(\hat{x}2 - x2) - \hat{x}1\hat{x}3 + x1x3 + U2 \quad (\text{III.14})$$

$$\dot{\hat{x}}3 - \dot{x}3 = -c(\hat{x}3 - x3) - E(\hat{x}4 - x4) + \hat{x}1\hat{x}2 - x1x2 + U3$$

$$\dot{\hat{x}}4 - \dot{x}4 = f(\hat{x}3 - x3) - d(\hat{x}4 - x4) + \hat{x}1\hat{x}2 - x1x2 + U4$$

$$y(x) = [x1 \ x2 \ x3 \ 0]$$

Nous appliquons la commande qui linéarisera le système (III.14)

$$U1 = x2x3 - \hat{x}2\hat{x}3 + V1$$

$$U2 = \hat{x}1\hat{x}3 - x1x3 + V2 \quad (\text{III.15})$$

$$U3 = x1x2 - \hat{x}1\hat{x}2 + V3$$

$$U4 = x1x2 - \hat{x}1\hat{x}2 + V4$$

Avec :  $U(t) = [U1(t), U2(t), U3(t), U4(t)]^T$  vecteur de commande.

En remplaçant (III.15) dans (III.14) on obtient le système suivant :

$$\dot{\hat{x}}_1 - \dot{x}_1 = -a(\hat{x}_1 - x_1) + a(\hat{x}_2 - x_2) + V_1$$

$$\dot{\hat{x}}_2 - \dot{x}_2 = +b(\hat{x}_1 - x_1) + b(\hat{x}_2 - x_2) + V_2$$

$$\dot{\hat{x}}_3 - \dot{x}_3 = -c(\hat{x}_3 - x_3) - E(\hat{x}_4 - x_4) + V_3$$

$$\dot{\hat{x}}_4 - \dot{x}_4 = f(\hat{x}_3 - x_3) - d(\hat{x}_4 - x_4) + V_4$$

Donc :

$$\dot{e}_1 = -a(e_1) + a(e_2) + V_1$$

$$\dot{e}_2 = +b(e_1) + b(e_2) + V_2 \quad (\text{III.16})$$

$$\dot{e}_3 = -c(e_3) - e(e_4) + V_3$$

$$\dot{e}_4 = f(e_3) - d(e_4) + V_4$$

Alors le système (III.16) à commander est un système linéaire en boucle ouverte qui peut s'écrire sous la forme de :

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \\ \dot{e}_4 \end{bmatrix} = \begin{bmatrix} -a & a & 0 & 0 \\ b & b & 0 & 0 \\ 0 & 0 & -c & -e \\ 0 & 0 & f & -d \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix} + \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} V_1 \\ V_2 \\ V_3 \\ V_4 \end{bmatrix} \quad (\text{III.17})$$

Pour assurer la synchronisation entre les deux systèmes maître et esclave, il faut stabiliser le système (III.16), en convergeant exponentiellement le système (III.13) vers zéro quand t tend vers l'infini pour ca on applique la commande par retour d'état.

Nous choisisant k comme une matrice à coefficients constants :

$$K = \begin{bmatrix} 1 - a & a & 0 & 0 \\ b & 1 + b & 0 & 0 \\ 0 & 0 & 1 - c & -e \\ 0 & 0 & f & 1 - d \end{bmatrix}$$

Alors  $V = -K e$

$$\begin{bmatrix} V1 \\ V2 \\ V3 \\ V4 \end{bmatrix} = \begin{bmatrix} 1-a & a & 0 & 0 \\ b & 1+b & 0 & 0 \\ 0 & 0 & 1-c & -e \\ 0 & 0 & f & 1-d \end{bmatrix} \begin{bmatrix} e1 \\ e2 \\ e3 \\ e4 \end{bmatrix} \quad (\text{III.18})$$

On remplace le système (III.18) dans le système (III.17) et on a :

$$\begin{bmatrix} \dot{e}1 \\ \dot{e}2 \\ \dot{e}3 \\ \dot{e}4 \end{bmatrix} = \begin{bmatrix} -a & a & 0 & 0 \\ b & b & 0 & 0 \\ 0 & 0 & -c & -e \\ 0 & 0 & f & -d \end{bmatrix} \begin{bmatrix} e1 \\ e2 \\ e3 \\ e4 \end{bmatrix} - \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1-a & a & 0 & 0 \\ b & 1+b & 0 & 0 \\ 0 & 0 & 1-c & -e \\ 0 & 0 & f & 1-d \end{bmatrix} \begin{bmatrix} e1 \\ e2 \\ e3 \\ e4 \end{bmatrix}$$

$$\begin{bmatrix} \dot{e}1 \\ \dot{e}2 \\ \dot{e}3 \\ \dot{e}4 \end{bmatrix} = \begin{bmatrix} -50 & 50 & 0 & 0 \\ 20 & 20 & 0 & 0 \\ 0 & 0 & -13 & -33 \\ 0 & 0 & 30 & -8 \end{bmatrix} \begin{bmatrix} e1 \\ e2 \\ e3 \\ e4 \end{bmatrix} - \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 49 & 50 & 0 & 0 \\ 20 & 21 & 0 & 0 \\ 0 & 0 & -12 & -33 \\ 0 & 0 & 30 & -7 \end{bmatrix} \begin{bmatrix} e1 \\ e2 \\ e3 \\ e4 \end{bmatrix}$$

$$\begin{bmatrix} \dot{e}1 \\ \dot{e}2 \\ \dot{e}3 \\ \dot{e}4 \end{bmatrix} = \begin{bmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} e1 \\ e2 \\ e3 \\ e4 \end{bmatrix}$$

$$\dot{e}_1 = -e_1 \quad \text{on a : } \frac{\dot{e}_1}{e_1} = -1 \quad ; \ln e_1 = -t \Rightarrow e_1 = e^{-t} \quad (\text{III.19})$$

La matrice donnée ci-dessus présente quatre valeurs propres négatives ce qui implique que tous les écarts du système convergent exponentiellement vers zéro en un temps fini. Donc, la synchronisation de ses deux systèmes (III.11) et (III.12) est réalisée.

Et comme dans notre mémoire on a une réalisation pratique, faire une commande à chaque étage se révèle un peu coûteuse, et vu que notre système comporte plusieurs variables d'état, l'alternative consiste à mesurer qu'un nombre réduit de variables d'état.

Alors il faut opter pour une commande passive afin de réduire le coût de la réalisation, par la suite on adopte pour une synchronisation unidirectionnel entre les deux systèmes qui on la

même architecture électronique afin d'assurer une meilleure synchronisation et permettre à l'émetteur de piloter le récepteur et résoudre du même coup le problème de non linéarité :

$$\begin{aligned}
 \dot{\hat{x}}_1 &= a(\hat{x}_2 - \hat{x}_1) + x_2x_3 \\
 \dot{\hat{x}}_2 &= b(\hat{x}_1 + \hat{x}_2) - x_1x_3 + U \\
 \dot{\hat{x}}_3 &= -c\hat{x}_3 - E\hat{x}_4 + x_1x_2 \\
 \dot{\hat{x}}_4 &= -d\hat{x}_4 + f\hat{x}_3 + x_1x_2
 \end{aligned} \tag{III.20}$$

Par soustraction des équations du système (III.11) et celles du système (III.20) on obtient :

$$\begin{aligned}
 \dot{\hat{x}}_1 - \dot{x}_1 &= -a(\hat{x}_1 - x_1) + a(\hat{x}_2 - x_2) \\
 \dot{\hat{x}}_2 - \dot{x}_2 &= +b(\hat{x}_1 - x_1) + b(\hat{x}_2 - x_2) + U \\
 \dot{\hat{x}}_3 - \dot{x}_3 &= -c(\hat{x}_3 - x_3) - E(\hat{x}_4 - x_4) \\
 \dot{\hat{x}}_4 - \dot{x}_4 &= f(\hat{x}_3 - x_3) - d(\hat{x}_4 - x_4)
 \end{aligned} \tag{III.21}$$

On applique le système d'écart (III.13) sur (III.21) et on a

$$\begin{aligned}
 \dot{e}_1 &= -a(e_1) + a(e_2) \\
 \dot{e}_2 &= +b(e_1) + b(e_2) + U \\
 \dot{e}_3 &= -c(e_3) - e(e_4) \\
 \dot{e}_4 &= f(e_3) - d(e_4)
 \end{aligned}$$

Représentation d'état

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \\ \dot{e}_4 \end{bmatrix} = \begin{bmatrix} -a & a & 0 & 0 \\ b & b & 0 & 0 \\ 0 & 0 & -c & -e \\ 0 & 0 & f & -d \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix}$$

$$V = -Ke$$

$$\begin{bmatrix} \dot{e}_1 \\ \dot{e}_2 \\ \dot{e}_3 \\ \dot{e}_4 \end{bmatrix} = \begin{bmatrix} -50 & 50 & 0 & 0 \\ 20 & 20 & 0 & 0 \\ 0 & 0 & -13 & -33 \\ 0 & 0 & 30 & -8 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & -K & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} e_1 \\ e_2 \\ e_3 \\ e_4 \end{bmatrix}$$

$$\dot{e}_1 = -50(e_1) + 50(e_2)$$

$$\dot{e}_2 = +20(e_1) + 20(e_2) - K(e_2) \quad (\text{III.22})$$

$$\dot{e}_3 = -13(e_3) - 33(e_4)$$

$$\dot{e}_4 = 30(e_3) - 8(e_4)$$

Donc notre récepteur aura pour équations

$$\dot{\hat{x}}_1 = a(\hat{x}_2 - \hat{x}_1) + x_2x_3$$

$$\dot{\hat{x}}_2 = b(\hat{x}_1 + \hat{x}_2) - x_1x_3 - K(\hat{x}_2 - x_2) \quad (\text{III.23})$$

$$\dot{\hat{x}}_3 = -c\hat{x}_3 - E\hat{x}_4 + x_1x_2$$

$$\dot{\hat{x}}_4 = -d\hat{x}_4 + f\hat{x}_3 + x_1x_2$$

Dans le système (III.23) nous avons construit un observateur avec un gain correctif. Dans ce cas, le problème de la synchronisation est devenu celui de la stabilité du système d'erreur, Si nous pouvons trouver un gain K appropriée, afin de garantir la stabilité du système d'erreur, alors la synchronisation entre l'émetteur et le récepteur peut être réalisée.

Donc on va chercher pour quelle valeur de K le système est stable, dans un premier lieu on détermine les polynômes caractéristiques du système.

$$\Delta(A) = \det(SI - (A - BK)) = \begin{bmatrix} S & 0 & 0 & 0 \\ 0 & S & 0 & 0 \\ 0 & 0 & S & 0 \\ 0 & 0 & 0 & S \end{bmatrix} - \begin{bmatrix} -50 & 50 & 0 & 0 \\ 20 & 20 + K & 0 & 0 \\ 0 & 0 & -13 & -33 \\ 0 & 0 & 30 & -8 \end{bmatrix}$$

$$\Delta(A)=\det (SI-(A-BK))=\begin{bmatrix} S+50 & 50 & 0 & 0 \\ 20 & S-20-K & 0 & 0 \\ 0 & 0 & S+13 & -33 \\ 0 & 0 & 30 & S+8 \end{bmatrix}$$

$$\Delta(A)=S^4 + (51-K) S^3 + (-71.K-267) S^2 + (-2144 K-9180) S - 54700 K - 218800$$

On appliquant le critère de Routh

$$\begin{cases} K - 51 > 0 \\ 71K + 267 > 0 \\ -54700K + 218800 > 0 \end{cases} \Rightarrow K \in [51, +\infty [$$

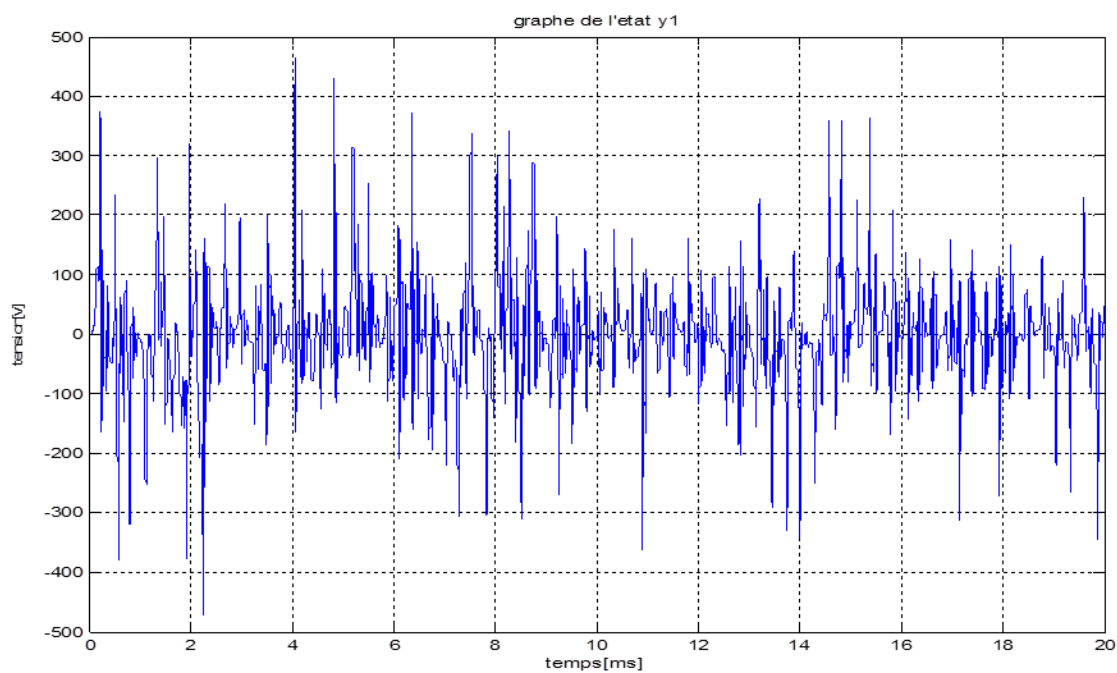
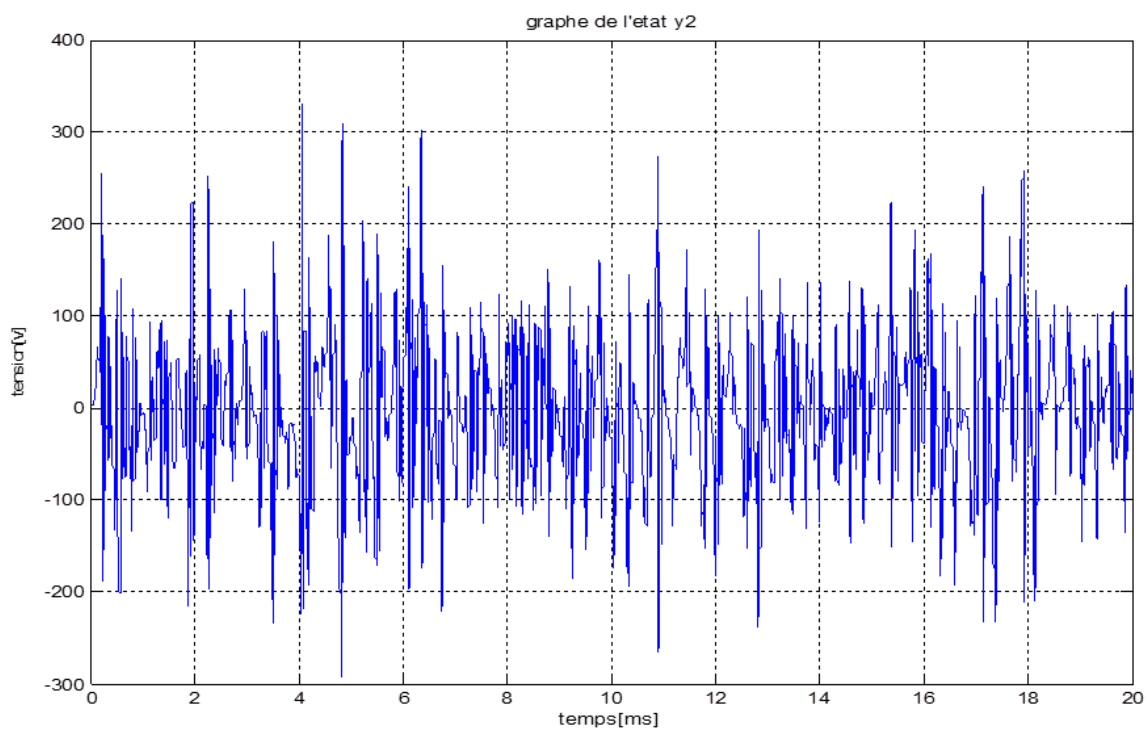
### III.3.3 Simulation sous Matlab

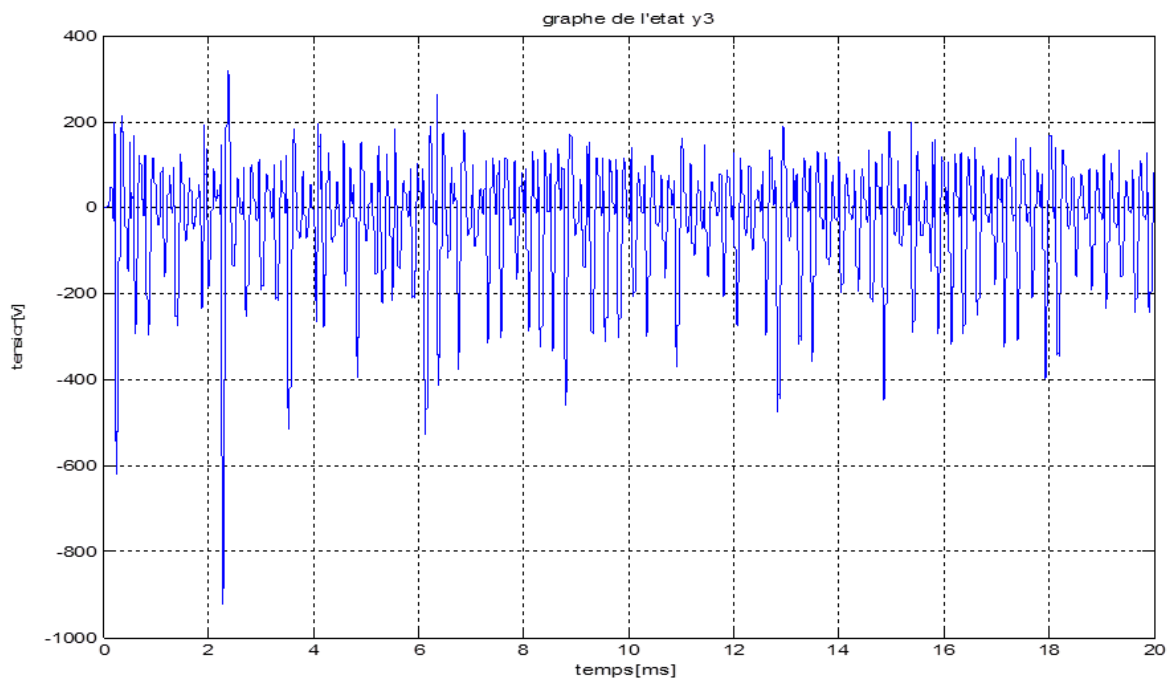
On insère les équations autonomes (III.23), (III.24), (III.25), (III.26) du récepteur dans Matlab sur la figure (3.2) (Annexe C) tout on le combinant à la figure (3.1) (Annexe C) sauf que cette dernière on lui additionne un message dans l'un des étages et on observe le comportement de chaque étage du récepteur.

Vu que le message (signal sinusoïdal) sera ajouté dans le troisième étage ( $x_3$ ) de l'émetteur, et que les deux systèmes présentent la même architecture électronique une simple opération de soustraction des deux variables d'état ( $x_3, \hat{x}_3$ ) permettra la récupération du message.

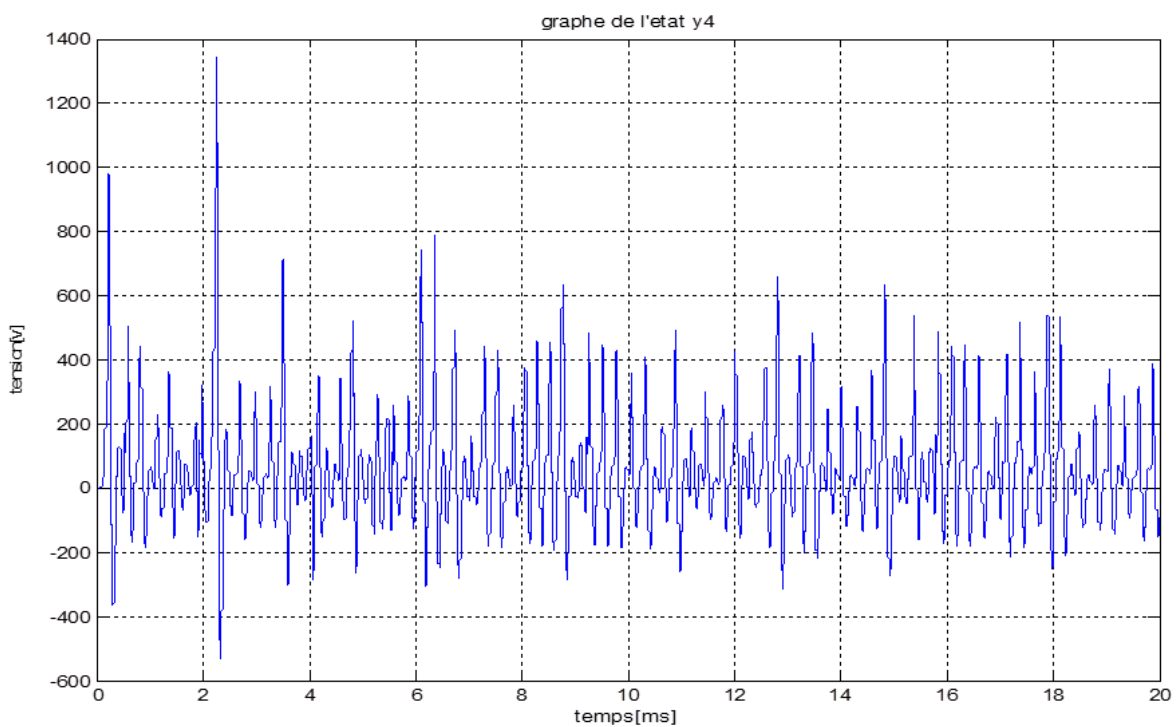
La simulation se fera pour  $a=50$ ;  $b=20$ ;  $c=13$ ;  $d=8$ ;  $e=33$ ;  $f=30$ ;  $K=100$ ;

## a. Visualisation des états estimé

Figure (III.12) : graphe de l'état  $\hat{x}_1(t)$ Figure (III.13) : graphe de l'état  $\hat{x}_2(t)$



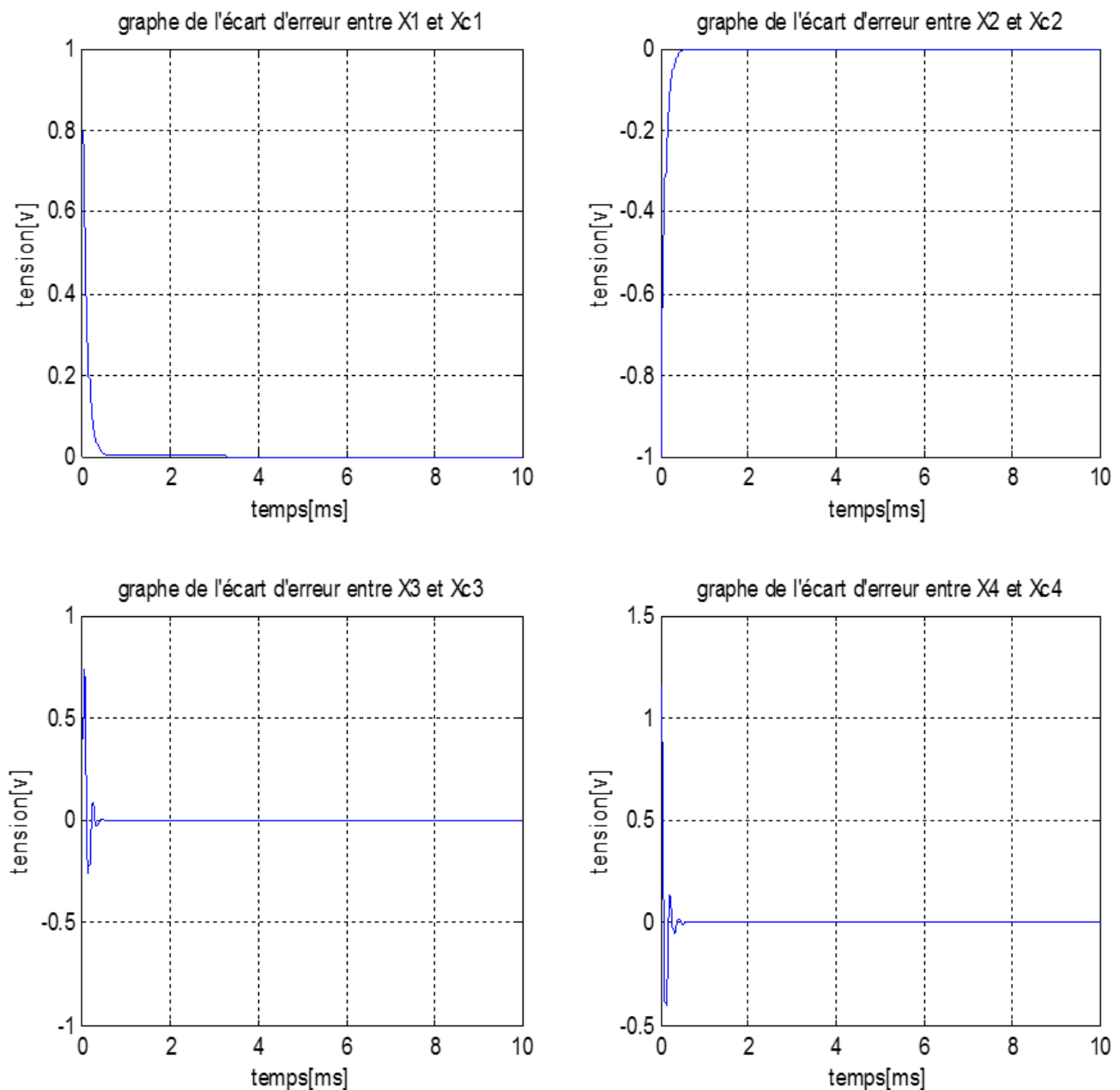
**Figure (III.14) :** graphe de l'état  $\hat{x}_3(t)$



**Figure (III.15) :** graphe de l'état  $\hat{x}_4(t)$

Nous remarquons la présence d'oscillations irrégulières et apériodiques dans ces quatre dernières figures, les signaux  $\hat{x}_1$ ,  $\hat{x}_2$ ,  $\hat{x}_3$ ,  $\hat{x}_4$  sont des signaux chaotiques.

### b. Visualisation des écarts entre les états des deux systèmes

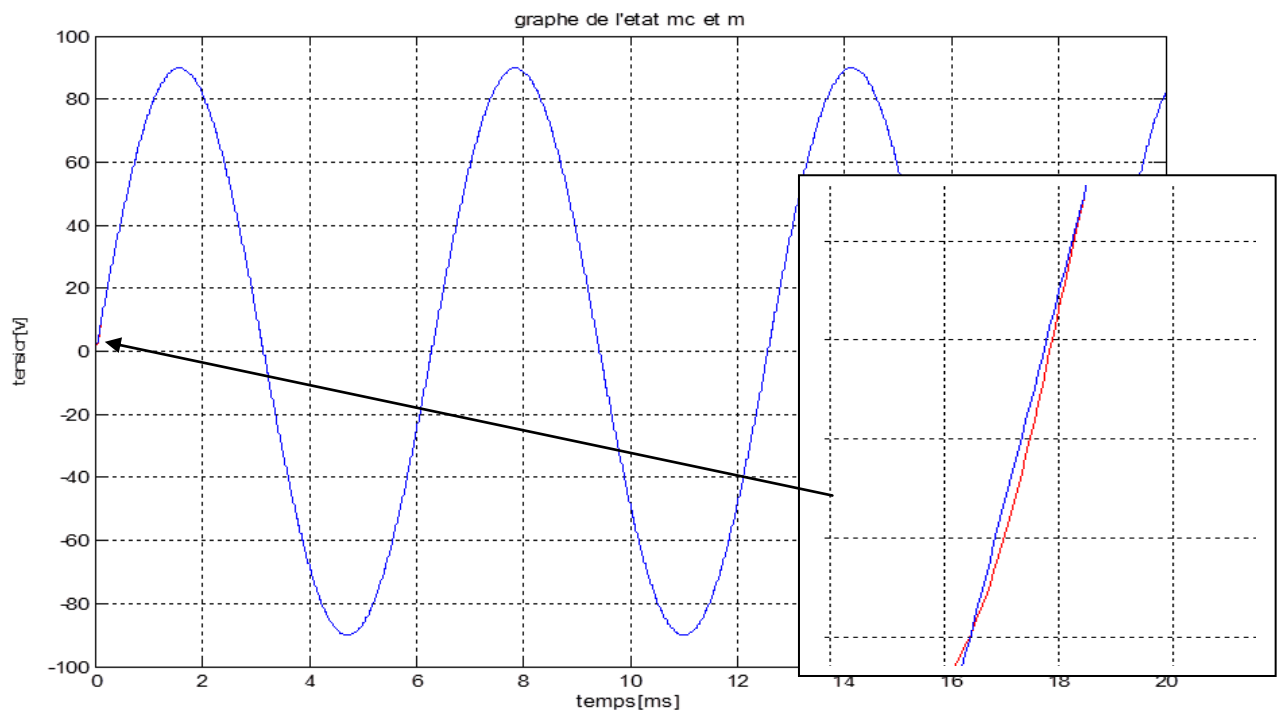


**Figure (III.16) :** allures des erreurs entre les états des deux systèmes

La figures (III.16) nous montre la convergence des erreurs d'état vers zéro quand  $t$  tend vers l'infini, ce qui démontre la synchronisation des deux systèmes.

### c. Récupération du message

On récupère le message on faisant une soustraction entre les états similaire à savoir  $x_3$  et  $\hat{x}_3$



**Figure (III.17) :** comparaison entre le message et la sortie du récepteur

La figure(III.17) montre très bien que le message envoyé a été belle et bien récupéré se qui prouve l'efficacité de l'approche.

### III.4 Conclusion

Dans ce chapitre nous avons pu faire connaissance avec l'oscillateur hyperchaotique de Qi et définir ses caractéristiques, puis nous avons synchronisé deux systèmes de Qi à l'aide d'un observateur, afin de réaliser un émetteur et un récepteur de signaux chaotiques pour une transmission sécurisée de données. Cela s'est fait en noyant par addition le message (signal sinusoïdal) dans le signal chaotique généré par l'émetteur, et la récupération du message s'est faite par soustraction entre le signal émis et le signal reçu. Les résultats obtenus par Matlab prouvent la possibilité du procédé et montre que la récupération du message est possible.

Dans le chapitre suivant nous allons réaliser électroniquement le système émetteur-récepteur obtenu.

### IV.1 Introduction

La conception théorique de notre transmission étudiée au chapitre précédent nous offre la possibilité de la réaliser en pratique à l'aide de deux cartes électroniques, émetteur et l'autre récepteur.

Ce chapitre se répartit en plusieurs parties. La première concerne la simulation du système sur un logiciel de simulation de circuits électronique, ensuite nous allons présenter les étapes nécessaires à la réalisation d'un circuit imprimé utilisées dans notre travail. En fin, nous passerons à l'acquisition de données sur oscilloscope numérique afin d'illustrer les résultats expérimentaux.

### IV.2 Simulation sous le logiciel de simulation de schémas électriques

Avant d'arriver à la réalisation de la carte imprimée il est primordiale d'utiliser un logiciel de simulation schémas électriques, et réalisé le lay out du circuit simple et à double face.

Ce dernier comporte une bibliothèque de composants traditionnels et une pour CMS (Composants à Montage de Surface ou SMD en anglais) mais là aussi on peut développer ses propres package (ou macro) et même de dessiner automatiquement le plan de masse autour des pistes qui s'avère très utile pour les circuits sensibles.

Nous avons une large gamme de logiciels de simulation comme Protel, Eagle, Multisim, et Proteus ..., notre choix en premier lieux s'est porté sur Protéus pour sa maniabilité, ses interphases, il est facile à utiliser, intuitif, inclue toutes les fonctions utiles, facile et en plus de ça qui permet la simulation de montages électriques.

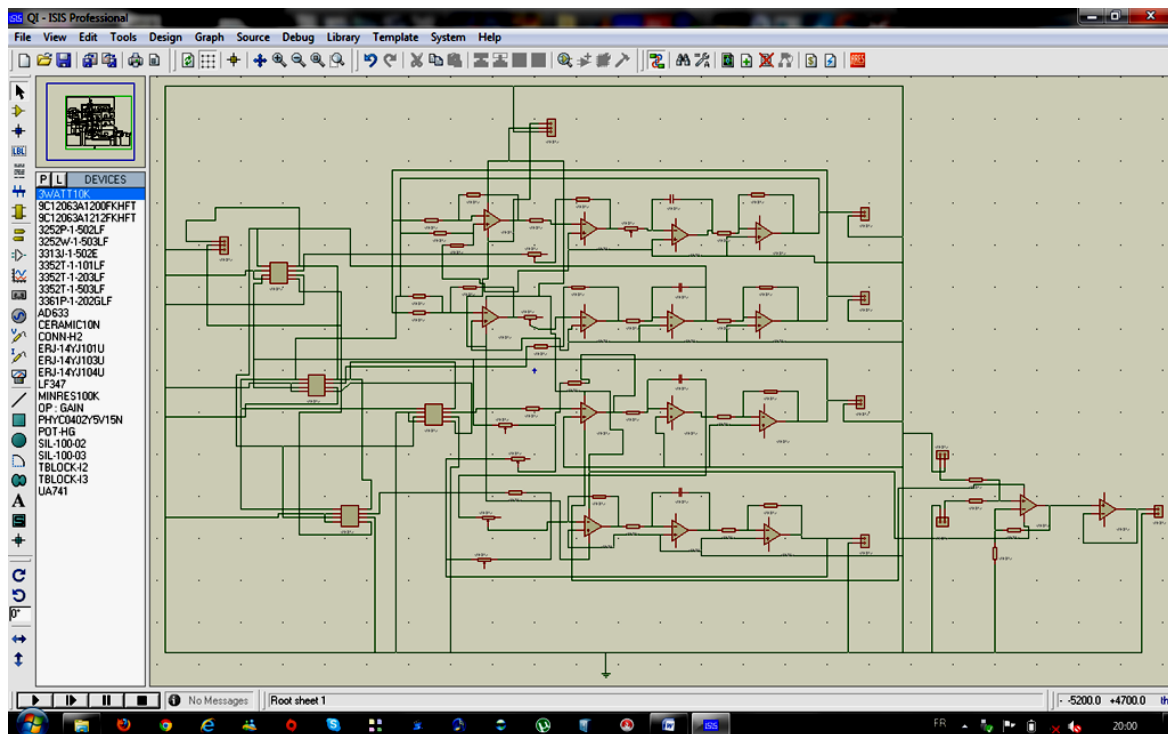


Figure (IV.1) : interface de Proteus

Mais malheureusement après plusieurs essais on n'a pas pu simuler notre schéma vu la complexité des paramètres de simulation de ce dernier.

Pour cela on s'est tourné vers Multisim de « international instruments » qui se révèle plus puissant et contient un programme de rectification automatique des paramètres de simulation.

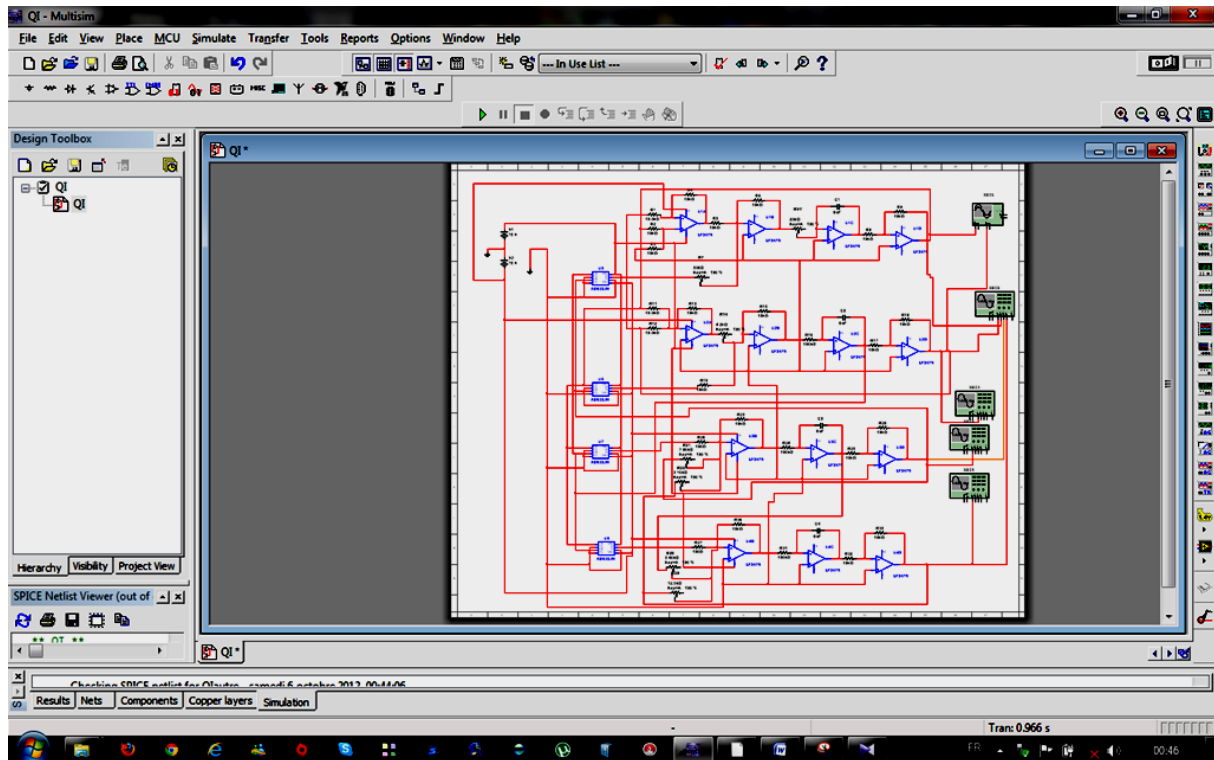


Figure (IV.2) : Schéma de l'oscillateur de Qi sous Multisim

La première étape est de mettre le schéma du montage dans la plate forme ci-dessus figure (IV.2), elle nous permet de faire le montage désiré ainsi que la simulation.

Les figures ci-dessous montrent les différents comportements de l'oscillateur de Qi obtenus lors de la simulation sous le logiciel Multisim pour une tension fixe à 15V qui alimente les amplificateurs et les multiplieurs.

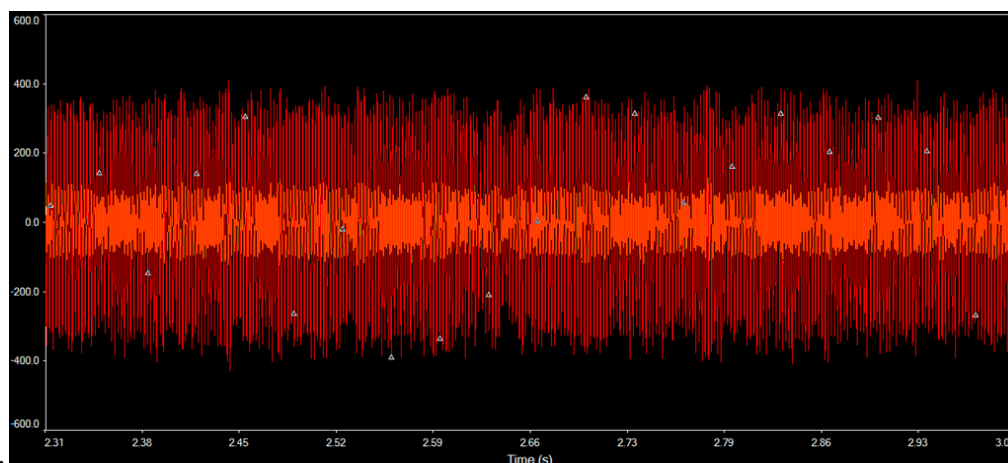


Figure (IV.3) : signaux chaotique observé sous multisim.

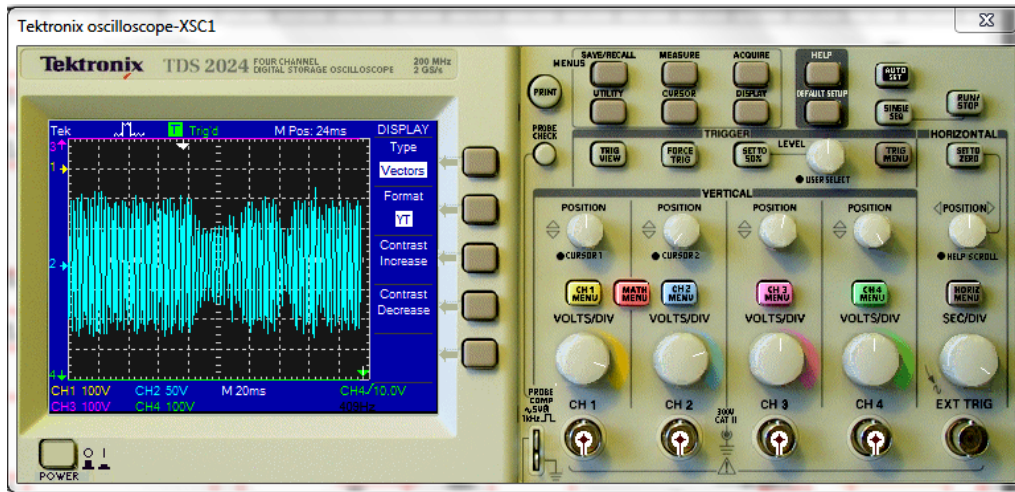


Figure (IV.4) : l'allure de l'état x1



Figure (IV.5) : l'allure de l'état x2

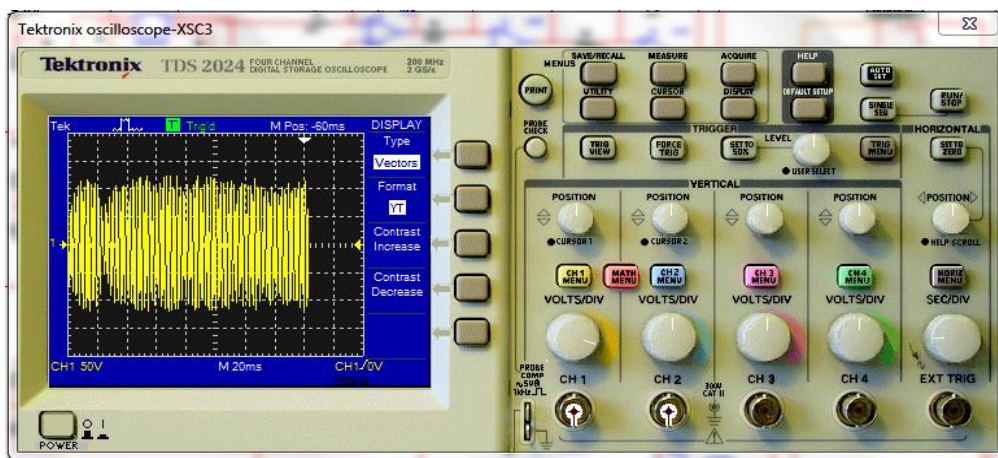


Figure (IV.6) : l'allure de l'état x3

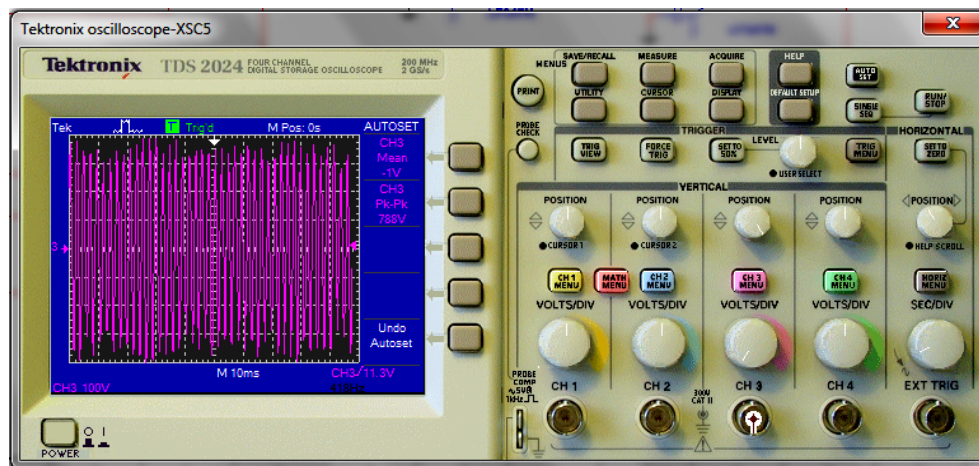


Figure (IV.7) : l'allure de l'état x4

Après avoir observé les états de notre oscillateur on passe à l'observation des attracteurs étranges :

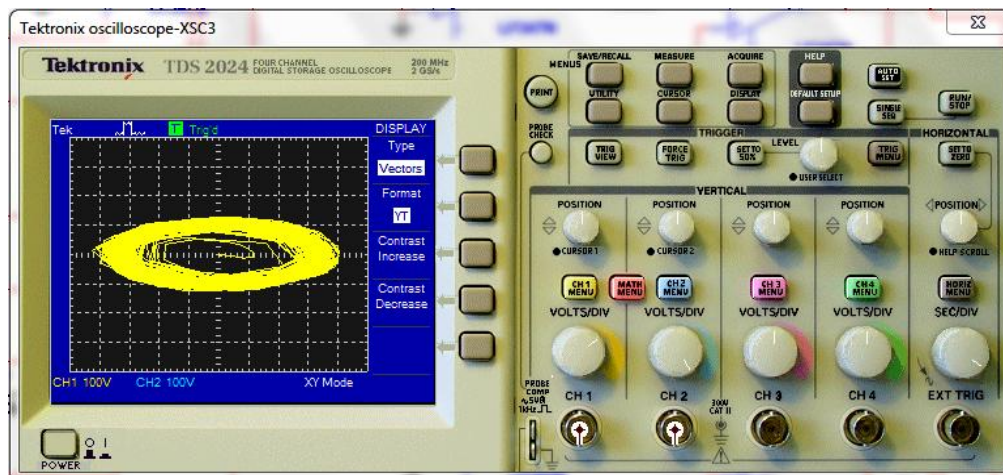


Figure (IV.8) : l'attracteur x1x2

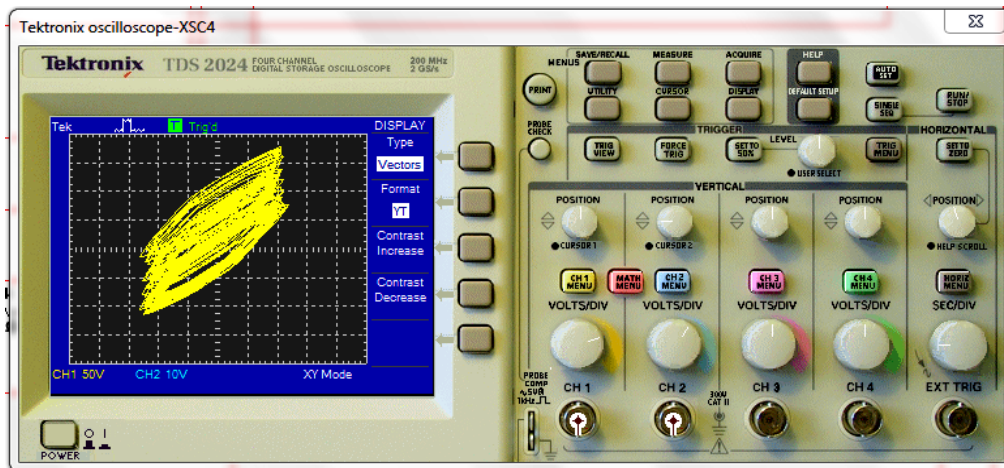


Figure (IV.9) : l'attracteur x1x3

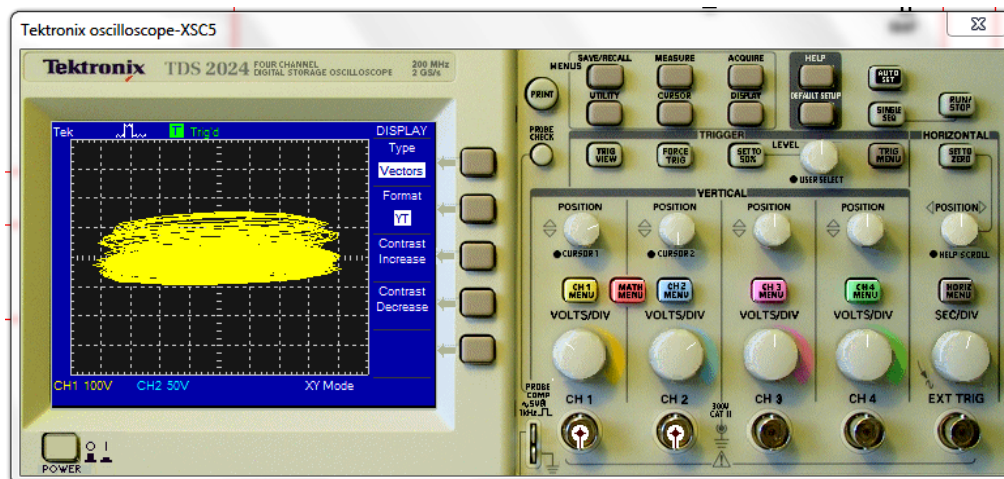
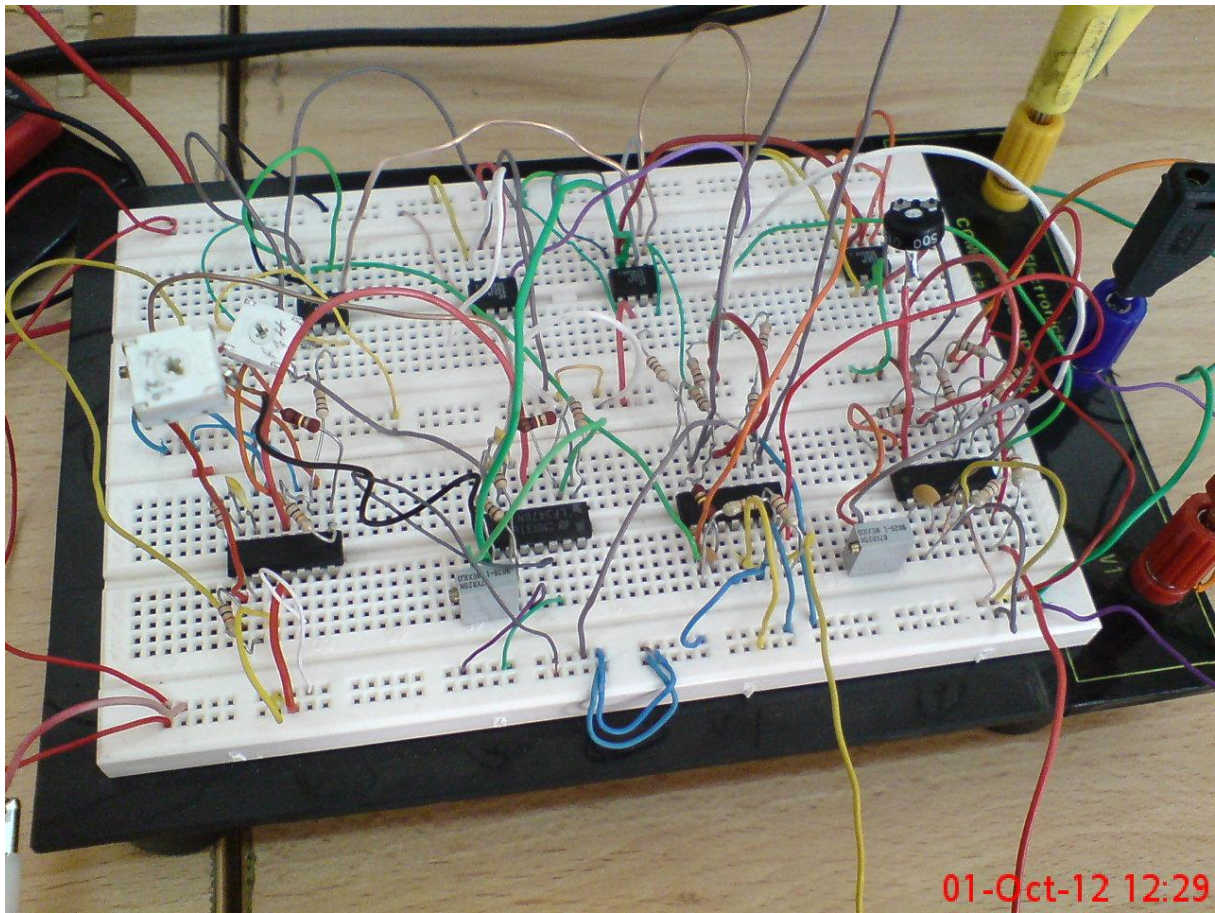


Figure (IV.10) : l'attracteur x2x3

Les attracteurs sont loin de ressembler aux attracteurs obtenus sur matlab, et comme on a une partie réalisation avant de s'aventurer dans la conception de celle-ci il est primordiales de tester le bon fonctionnement du schéma électrique de l'oscillateur de Qi.

Pour cela, on le fait à l'ancienne en utilisant un « lab. d'essai » que montre la figure (IV.11)



**Figure (IV.11) :** l'oscillateur de Qi sur un lab. d'essai

Après avoir terminé le raccordement de tous les composants, on teste le circuit. Après avoir pris un long moment à chercher les paramètres de l'oscillateur celui-ci donne des résultats qui nous permettent de réaliser le circuit imprimé.

IV.3 Modification de l'oscillateur de Qi

L'ajout d'un additionneur et un suiveur permet d'ajouter un message et l'incorporer dans notre signal chaotique comme le montre la figure (IV.12)

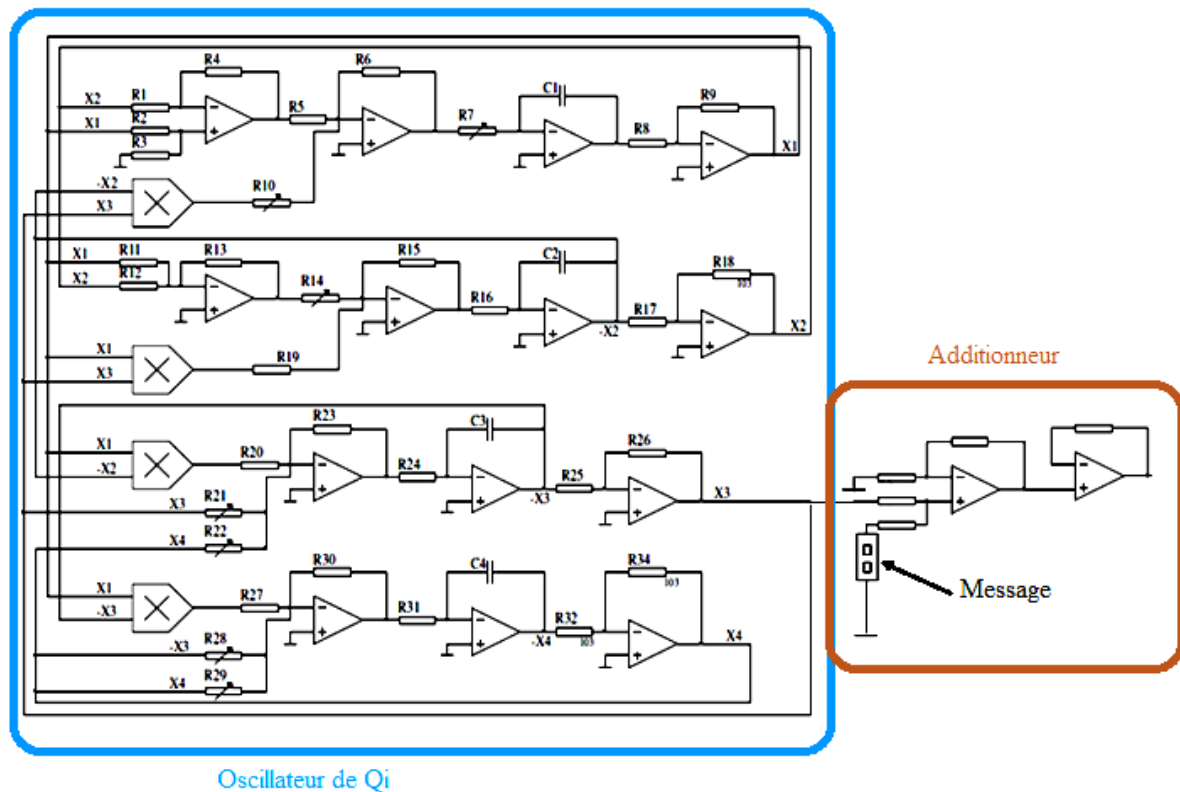


Figure (IV.12) : l'oscillateur de Qi modifié « émetteur »

Et pour notre récepteur figure (IV.13) on lui ajoute un additionneur pour  $x_2$  et  $\hat{x}_2$  et un amplificateur non inverseur avec une résistance variable afin d'ajuster le gain K.

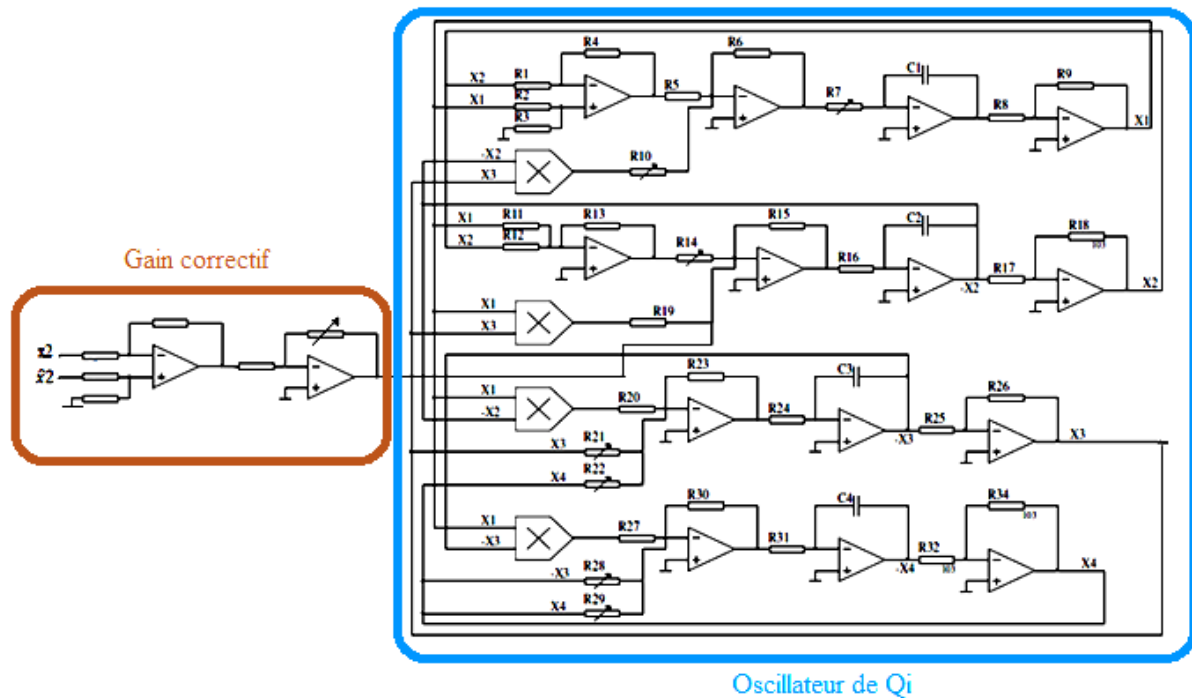
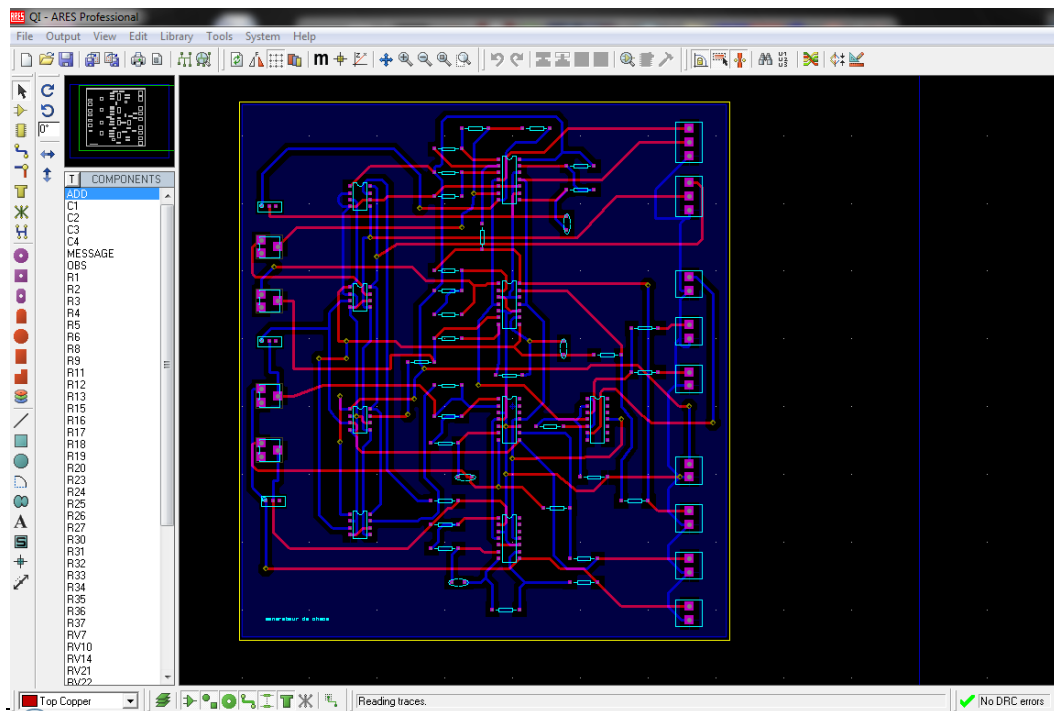


Figure (IV.13) : l'oscillateur de Qi modifié « récepteur »

#### IV.4 Etapes de réalisation d'un circuit imprimé

Maintenant on passe à la réalisation de notre circuit imprimé, pour cela on revient à Proteus pour créer notre plaque imprimée.

La première étape est de mettre le schéma du montage figure (IV.13) dans la plateforme de la figure (IV.1), elle nous permet de faire le dessin ainsi que la simulation, une fois terminé et qu'on est sûr des résultats obtenus, on passe à la réalisation du schéma professionnel final à l'aide de la touche rouge en haut et à droite de la figure (ARES) et on obtient la figure (IV.14) ci-dessous.



**Figure (IV.14) :** Lay-out sous protégés

On peut voir le typon qui sera la feuille transparente, sur laquelle est dessiné en noir le dessin du circuit imprimé

L'intérêt de ces deux logiciels est qu'ils vérifient la cohérence entre le typon réalisé et le schéma. Ils possèdent également des fonctions d'auto routage qui permettent de laisser le logiciel faire les pistes entre les composants. Cette méthode est rapide mais donne souvent des résultats moyens qu'il faut corriger à la main.

Une fois le typon prêt, on passe à l'impression du négatif sur du film transparent figure (IV.15) (papier calque 90 mg).

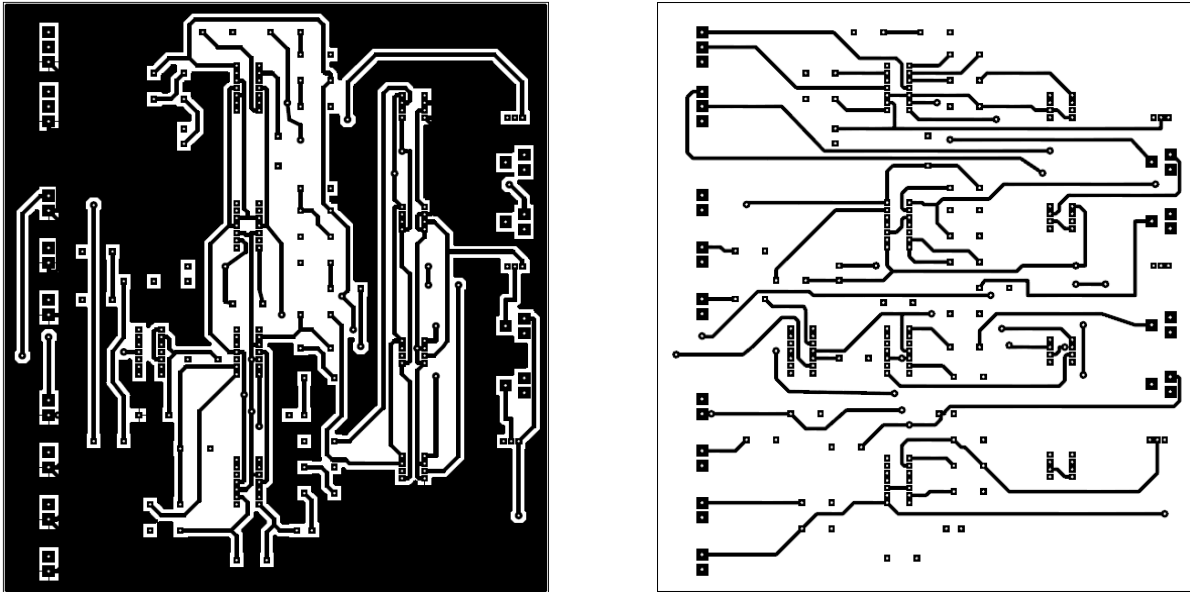


Figure (IV.15) : typon ou négatif du circuit

Maintenant que nous avons obtenu notre typon on passe au laboratoire pour la réalisation pratique et pour cela on aura besoin de matériel entre autre une plaque vierge pour circuits-imprimés. Cette dernière se compose d'une plaque d'isolant (époxy, fibre de verre, téflon) d'une épaisseur variable (de 0.1 à 1.5 mm) recouverte d'une couche de cuivre de 35 microns en général et en fin d'une couche de résine pré-sensibilisé au UV comme le montre la Figure (IV.16)

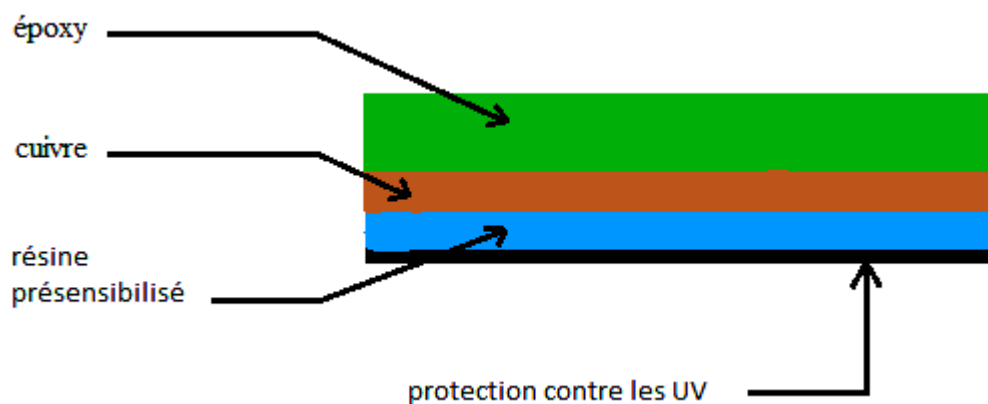


Figure (IV.16) : la plaque vierge

La réalisation d'un circuit imprimé se déroule en plusieurs étapes importantes :

#### IV.4.1 L'insolation

Après avoir retiré le papier noir qui protège la couche photosensible de la lumière, le typon est placé d'une façon adéquate sur la face sensible au UV avec quatre clips afin que le tout tienne bien en place, et tout en exposant ce côté au rayonnement d'un néon ultra-violet, la couche photosensible sera atteinte par le rayonnement à travers les parties transparentes du typon. Par contre, les parties noires ne laisseront rien passer et la couche photosensible restera vierge. Cette opération dure environ deux minutes

Enfin, la résine non protégée par l'encre du typon est attaquée par les rayonnements UV.

#### IV.4.2 La révélation

La révélation est un bain de soude dans le quel on laisse tremper la plaque insolée. Néanmoins ce produit chimique est assez dangereux et impose le port de gants. Il se trouve sous forme liquide prêt à l'emploi ou sous forme de poudre à diluer avec de l'eau.

Donc on verse notre soude dans une bassine puis on met la plaque dans cette dernière et nous voyons apparaître petit à petit le cuivre nu aux endroits exposés aux UV, c'est à dire aux endroits qui ne devront pas subsister à l'étape de gravure finale, alors que les pistes protégées précédemment par le typon apparaissent en bleu.

#### IV.4.3 La gravure

La gravure chimique consiste à dissoudre une partie du cuivre de la plaque du circuit imprimé, en plongeant pendant un certain temps la plaque dans un produit corrosif appelé perchlorure de fer (C'est un acide qui attaque les métaux et notamment le cuivre), il ne doit rester que le cuivre correspondant au dessin du circuit imprimé car l'encre protège contre la gravure, tout le reste doit disparaître.

La couche pré-sensibilisée de la résine qui recouvre le cuivre formant les pistes et pastilles du circuit imprimé doit être éliminée, ce procédé peut se faire par utilisation de l'acétone. Ou bien, en exposant une seconde fois la plaque au rayonnement UV puis la laver à l'eau courante.

#### IV.4.4 Perçage

Le perçage des trous s'effectue à l'aide d'une perceuse rapide et de forets en métal dur. Ce matériau est obligatoire car la fibre de verre use très vite une mèche en acier normal.

Bien sûr avant d'entamer le perçage, les pistes sont testées à l'aide d'un multimètre afin de vérifier leur continuité et s'assurer de la non présence de microcoupure.

#### IV.4.5 Implantation des composants

Les composants électroniques sont introduits dans la plaque et soudés à leur place. On commence en général par les composants peu encombrants, pour ne pas être gêné pour les soudures suivantes.

On peut également commencer par implanter les straps (ponts de fils entre deux points de la plaque pour les circuits imprimés à double faces) et les supports de circuits intégrés. L'intérêt de ces derniers est de pouvoir tester aisément si les pins des circuits intégrés sont correctement liés entre eux, sans être gêné lors des mesures par les autres composants, et aussi donnent la possibilité de changer aisément les composants endommagés.

#### IV.4.6 La soudure

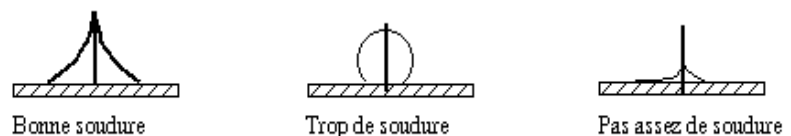
Placer la panne du fer à souder de façon à ce qu'elle soit en contact avec le cuivre de la plaque et avec la patte du composant. Laisser chauffer ainsi quelques secondes. Ajouter de la soudure au niveau du contact.

Laisser la panne encore quelques secondes afin que la soudure s'étale bien.

retirer le fer à souder.

La quantité de soudure

Apportée est un facteur décisif pour la qualité de la soudure.



**Figure (IV.17) : soudure**

On voit à la forme de la soudure si la quantité est la bonne figure (IV.16). Une bonne soudure apporte une meilleure tenue mécanique du circuit, évite les faux contacts et améliore aussi le contact électrique.

On a pour résultats les figures (IV.18) et (IV.19)

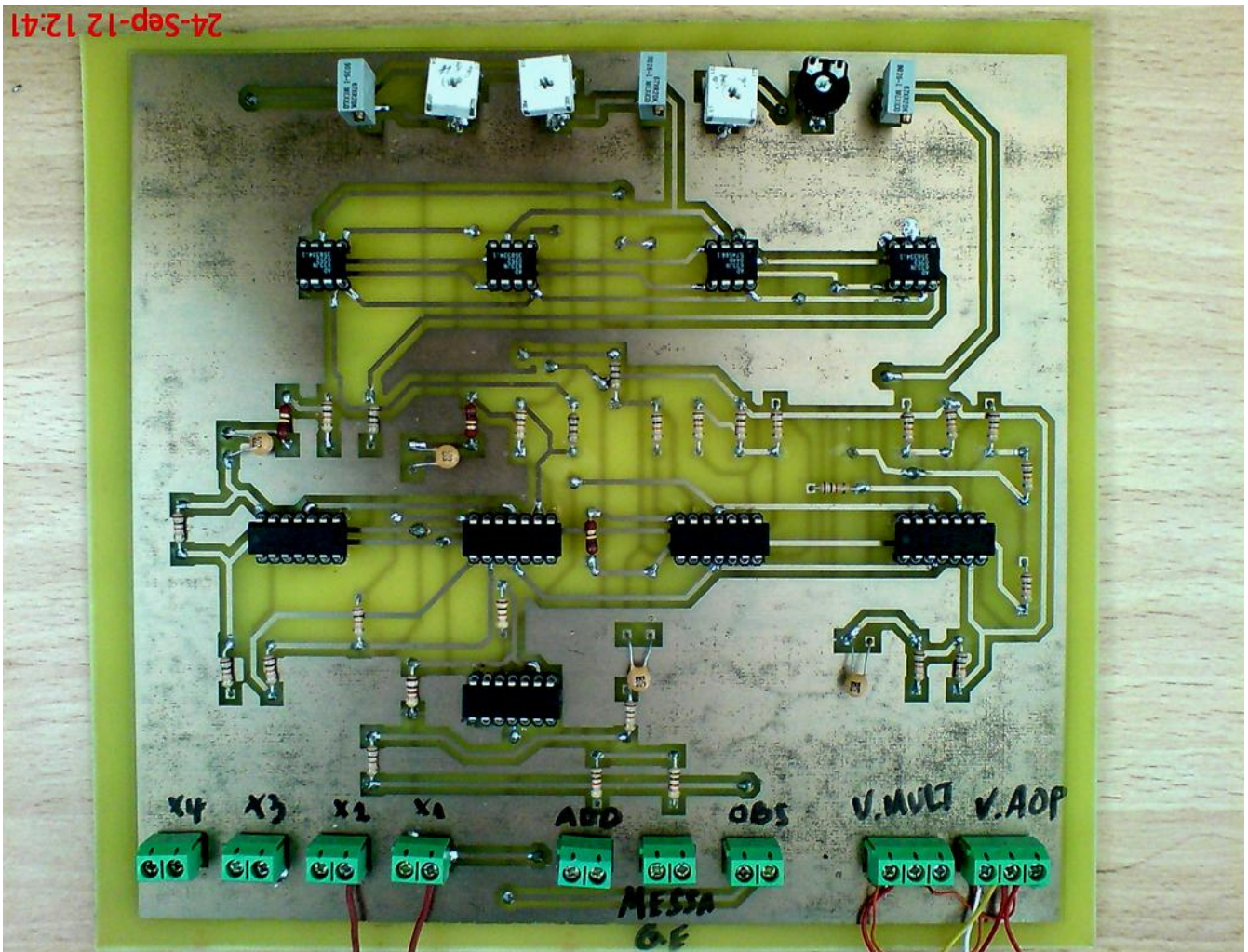


Figure (IV.18) : émetteur

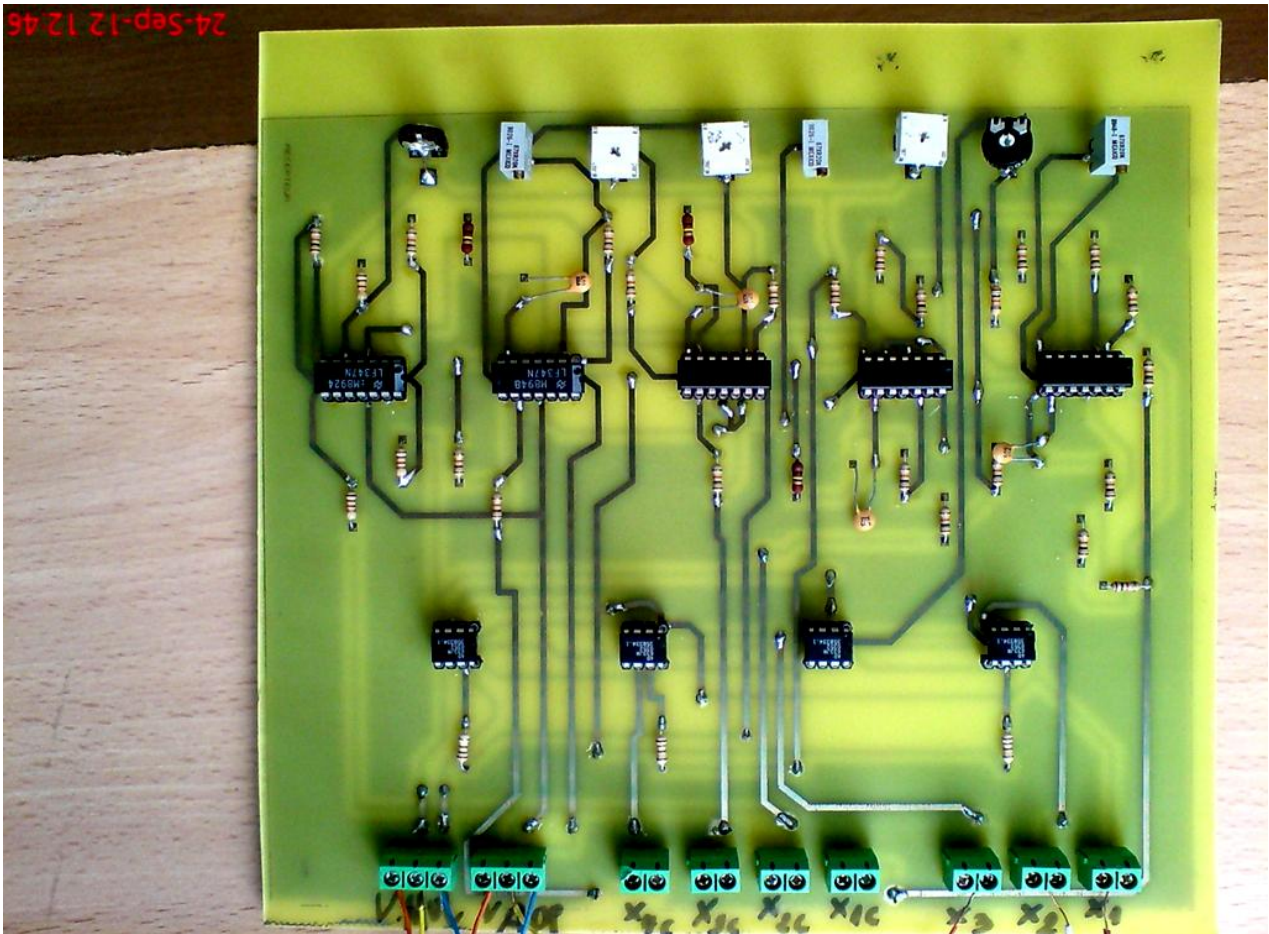


Figure (IV.19) : récepteur

#### IV.5 résultats expérimentaux

Les figures ci-dessous montrent les différents comportements de l'oscillateur de QI obtenus lors de l'expérience pour une tension fixée à 15V.

Les mesures temporelles des signaux de sorties sont visualisées sur un oscilloscope numérique.

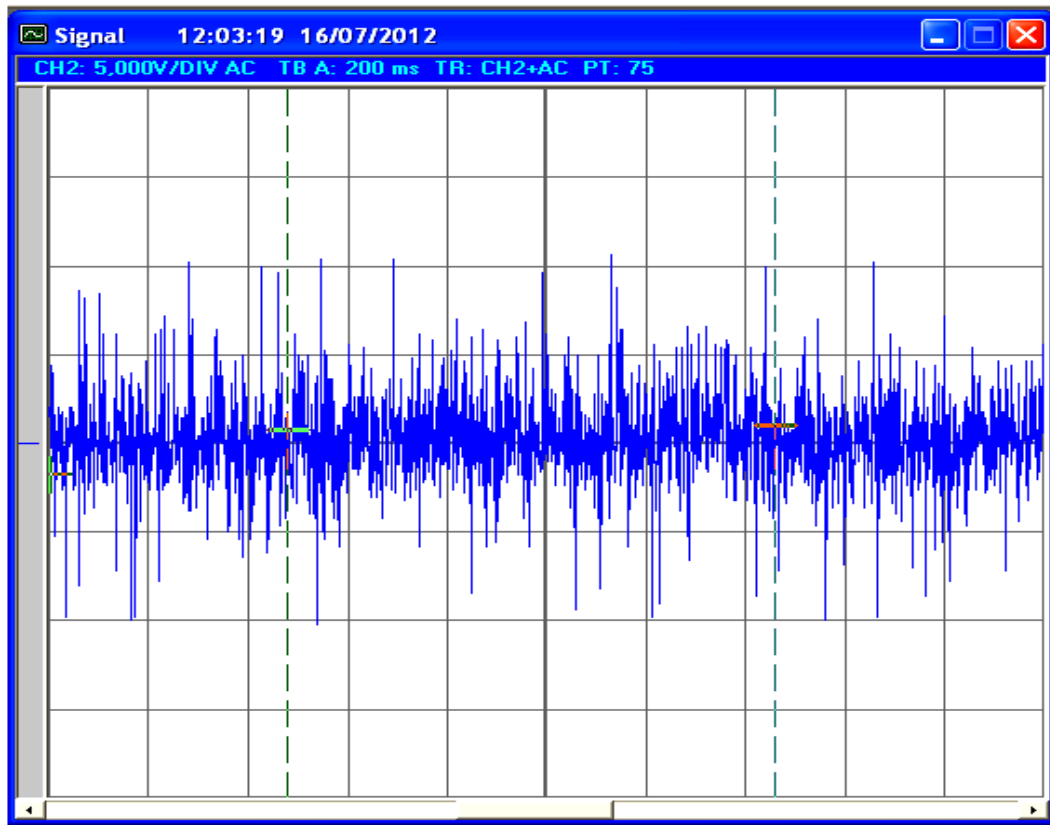


Figure (IV.20) : graphe de l'état x1

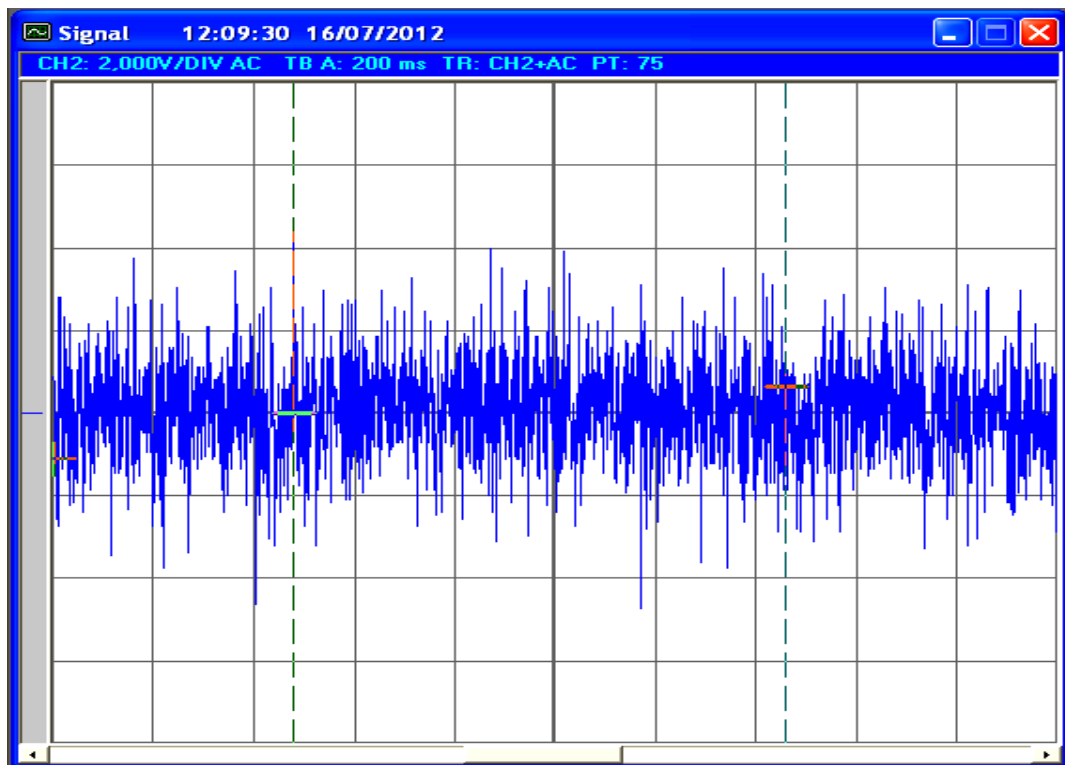


Figure (IV.21) : graphe de l'état x2

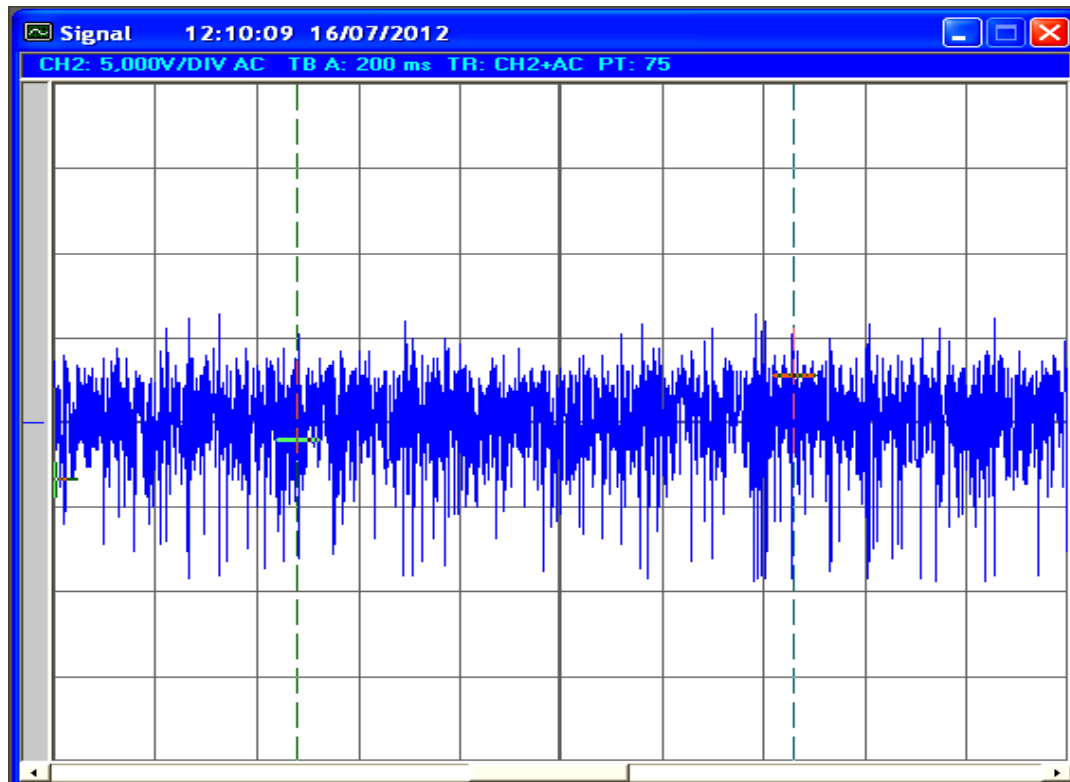


Figure (IV.22) : graphe de l'état x3

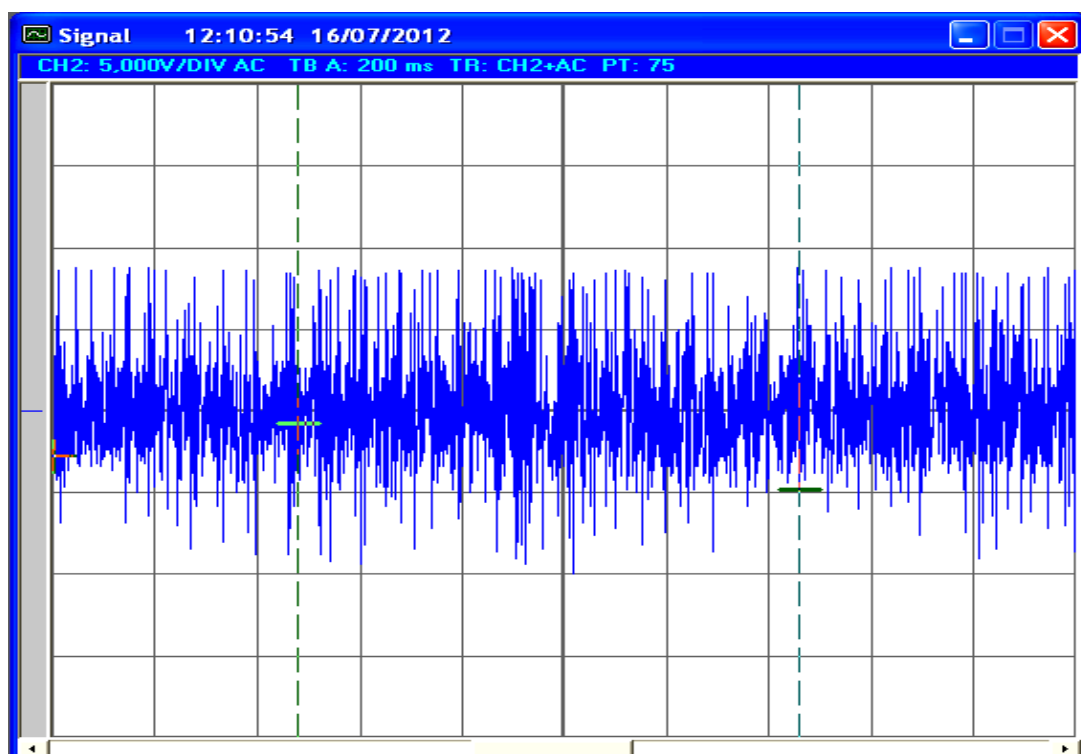


Figure (IV.23) : graphe de l'état x4

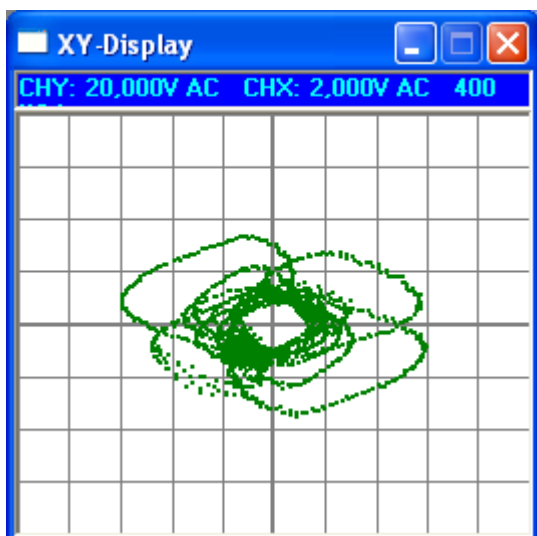


Figure (IV.24) : attracteur x1x2

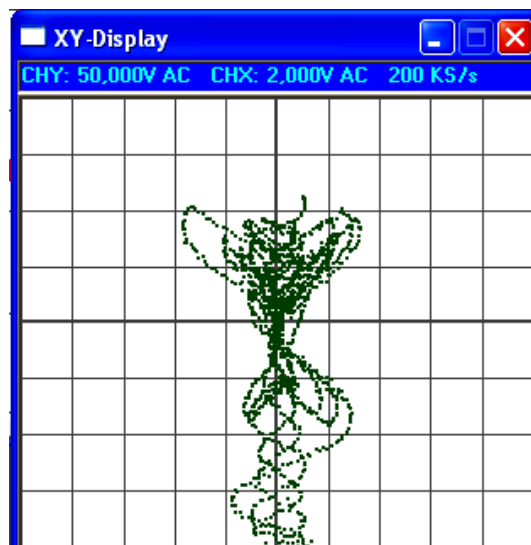


Figure (IV.25) : attracteur x1x3

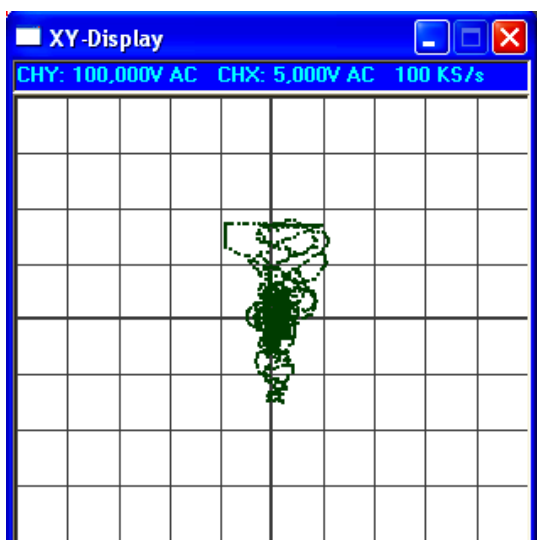


Figure (IV.26) : attracteur x1x4

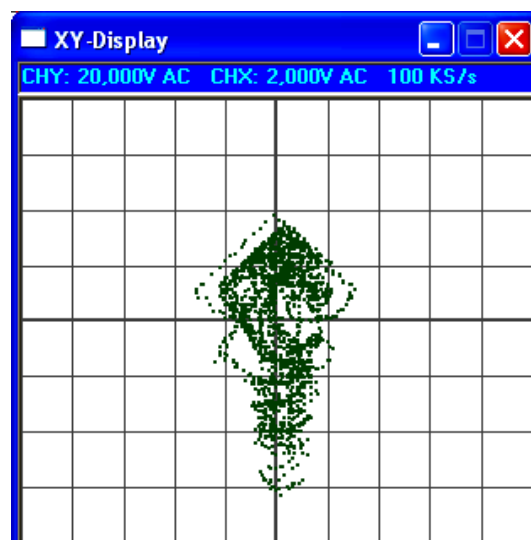


Figure (IV.27) : attracteur x2x3

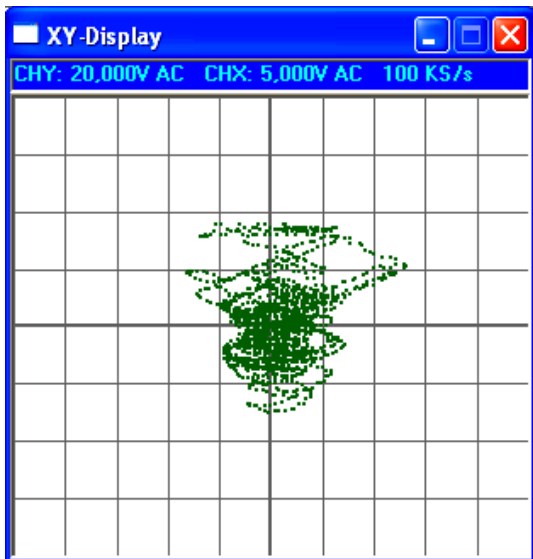


Figure (IV.28) : attracteur x2x4

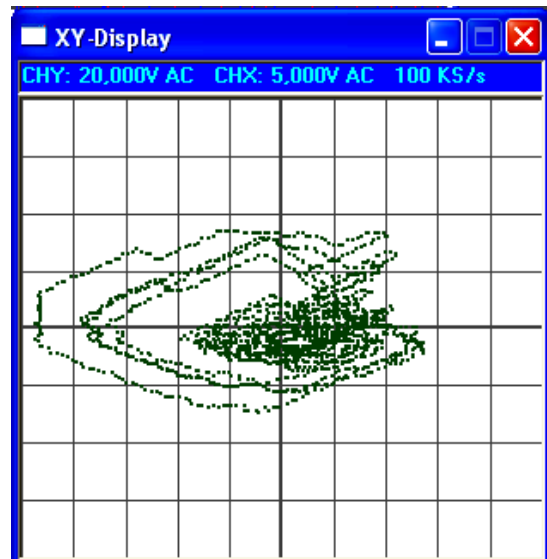


Figure (IV.29) : attracteur x1x3

Les résultats des figures ci-dessus montrent bien que notre émetteur marche parfaitement est concorde avec les résultats trouvés sur Matlab.

Malheureusement, pour des raisons techniques on n'a pas pu vérifier la synchronisation entre l'émetteur et le récepteur.

#### IV.6 Conclusion

Dans ce chapitre nous avons pu simuler l'oscillateur de Qi sur un logiciel de traitement de schéma électronique, nous avons aussi modifié notre oscillateur afin qu'on puisse ajouter un message par la méthode par addition et une autre fois nous l'avons configuré afin qu'il puisse recevoir le message. Par la suite, nous avons donné une idée sur les différentes étapes à suivre pour réaliser un circuit imprimé.

En pratique, nous avons pu faire fonctionner l'émetteur d'où l'acquisition de données sur oscilloscope, quant au récepteur, uniquement deux étages ont fonctionné à cause d'un dysfonctionnement dans le circuit imprimé.

## **Conclusion générale**

Dans ce travail, nous avons conçu et réalisé une transmission sécurisée par chaos. Ce qui nous a permis de toucher à un domaine difficile qui est le chaos déterministe, ainsi que la transmission sécurisée, la commande des systèmes et l'électronique.

Le premier chapitre est consacré à l'étude des systèmes chaotiques par leurs caractéristiques et leur comportement.

Le deuxième chapitre expose la synchronisation du chaos dans une première partie et quelques rappels sur la transmission sécurisée dans une deuxième partie.

Pour la réalisation, nous avons d'abord élaboré les équations différentielles régissant le système de transmission dans un troisième chapitre. Nous avons utilisé comme émetteur un système hyperchaotique de Qi, décrit par des équations différentielles. La conception du récepteur s'est faite par un circuit de Qi identique à l'émetteur que nous avons synchronisé à l'aide d'observateur. Nous avons ensuite inséré un message dans l'émetteur en l'additionnant à un de ses états. Nous avons simulé Le système obtenu sur Matlab et nous avons récupéré le message par cette simulation en utilisant une fonction de soustraction.

La réalisation pratique exposée dans le quatrième chapitre s'est faite par deux cartes électroniques, la première pour l'émetteur et la deuxième pour le récepteur. Nous avons pu obtenir sur l'émetteur les mêmes résultats obtenus sous Matlab, quant au récepteur, uniquement deux étages sur quatre ont fonctionnés.

Nos résultats prouvent que les transmissions sécurisées par chaos, étudiées avant par simulation uniquement, fonctionnent en pratique et ouvrent une possibilité de développement de ces méthodes dans le futur dans le domaine de la communication.

Comme perspectives à ce travail il est possible de changer le type d'observateur utilisé pour la synchronisation et la méthode de cryptage.

## Bibliographie

[1] H. Poincaré, « La Science et l'Hypothèse, Le calcul des probabilités », Ed. La Bohème (1902)

[2]: E.N.Lorenz , « The essence of chaos » Ed Kindle, (1995)

[3] H. Hamiche, « Inversion à gauche des systèmes dynamiques hybrides chaotiques. Application à la transmission sécurisée de données », Thèse doctorat, UMMTO, Algérie, (2011).

[4] M.B. Luca, « Apport du chaos et des estimateurs d'états pour la transmission sécurisée de l'information », Thèse doctorat. Université de Bretagne occidentale. (2006)

[5] P. Bérge, Y. Pomeau et C. Vidal, « L'ordre dans le chaos ». Hermann, éditeur des sciences et des arts, (1988)

[6] I. Aneur, « Synchronisation, chaotification et hyperchaotification des systèmes non-linéaires : Méthodes et Applications », Thèse doctorat, Université Mentouri de Constantine, Algérie, (2011).

[7] N.R.Gastaud Galagher, « Système de communication haut débit sécurisé par chaos et intensité », Thèse doctorat, Université de Franche-Comté, (2006).

[8] G. Zheng, « Formes normales d'observabilité paramétrées par les sorties : Applications au cryptage par synchronisation de systèmes chaotiques », Thèse doctorat. Université de Cergy-Pontoise (2006).

[9] E. Cherrier, « Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires », Thèse Doctorat. Institut National Polytechnique de Lorraine, (2006).

- [10] Guoyuan Qi, Michael Antonie van Wyk, Barend Jacobus Van Wyk, Guanrong Chen, « A new hyperchaotic system and its circuit implementation », *Chaos solutions & fractals*, pages (2545-2549), (2007).
- [11] D. Boutat, « la notion d'observateur pour les systèmes non linéaires », ENSI de Bourges institut prisme, (2010).
- [12] D. Ruelle, « Hasard et chaos », Odile Jacob sciences, (1991).
- [13] F. Anstett, « Les systèmes dynamiques chaotiques pour le chiffrement, synthèse et cryptanalyse », Thèse doctorat, Université de Henri Poincaré, Nancy1, 2006.
- [14] A. Layec, « Développement de modèles de CAO pour la simulation système des systèmes de communication. Application aux communications chaotiques. », thèse doctorat, université de Limoges, (2006)
- [15] A. Zemouche, « Sur l'observation de l'état des systèmes dynamiques non linéaires », Thèse doctorat, université Louis Pasteur Strasbourg, (2007).
- [16] B. Boulaïd, « Estimation de l'état des systèmes non linéaires à temps discret. Application à une station d'épuration », Thèse doctorat, Université Henri Poincaré Nancy1, (2008).
- [17] F.E. Thau, Observing the state of non-linear dynamic systems, *International Journal of Control*, vol. 17, no. 3, pages 471–479, 1973.
- [18] S.R. Kou, D.L. Elliott & T.J. Tarn, Exponential observers for nonlinear dynamic systems, *Information and Control*, vol. 29, pages 204–216, 1975.
- [19] T.L. Carroll and L.M. Pecora, Synchronization in chaotic systems, *Physicals review and letters*, 1990.

[20] H. Nijmeijer, Iven H.Y. Marceels , an observer looks at synchronization, IEEE transaction on circuits and systems: Fundamental theory and applications, vol. 44, October 1997.

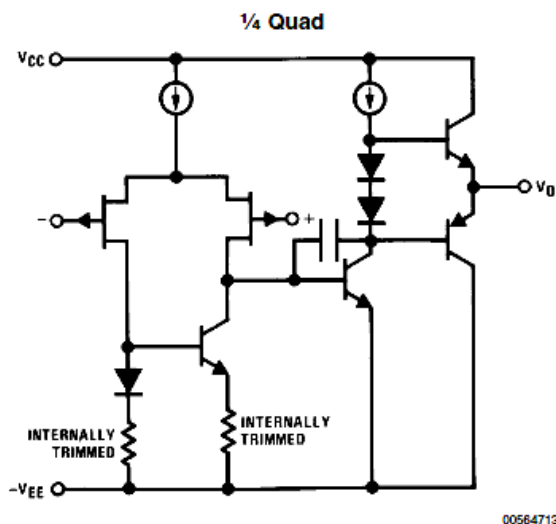
[21] H. Hammiche, K. Kemih, M. Ghanes, G. Zhang and S. Djenoun, Passive and impulsive synchronization of new four-dimensional chaotic system, Non linear analysis: theory, methods, applications, vol.74, no. 4 pp. 1146-1154, 2011.

## Datasheet des composants électriques :

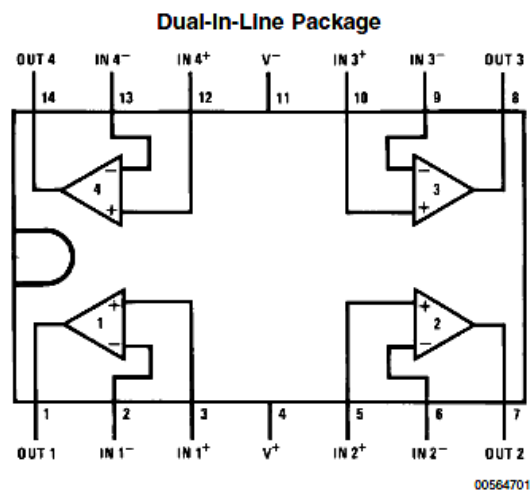
## 1 LF347

Le LF347 est un circuit intégré comportant quatre AMP-OP

## Simplified Schematic



## Connection Diagram



Note 1: LF147 available as per JM38510/11906.

## Top View

Order Number LF147J, LF147J-SMD, LF347M,  
LF347BN, LF347N, LF147J/883,  
or JL147 BCA (Note 1)  
See NS Package Number J14A, M14A or N14A

Figure (1) : amplificateur opérationnel LF347

## Absolute Maximum Ratings (Note 2)

If Military/Aerospace specified devices are required, please contact the National Semiconductor Sales Office/ Distributors for availability and specifications.

	LF147	LF347B/LF347
Supply Voltage	±22V	±18V
Differential Input Voltage	±38V	±30V
Input Voltage Range (Note 3)	±19V	±15V
Output Short Circuit Duration (Note 4)	Continuous	Continuous
Power Dissipation (Notes 5, 11)	900 mW	1000 mW
$T_j$ max	150°C	150°C
$\theta_{JA}$		
Ceramic DIP (J) Package		70°C/W
Plastic DIP (N) Package		75°C/W
Surface Mount Narrow (M)		100°C/W
Surface Mount Wide (WM)		85°C/W

	LF147 (Note 6)	LF347B/LF347 (Note 6)
Operating Temperature Range		
Storage Temperature Range		-65°C ≤ T <sub>A</sub> ≤ 150°C
Lead Temperature (Soldering, 10 sec.)	260°C	260°C
Soldering Information		
Dual-In-Line Package		
Soldering (10 seconds)		260°C
Small Outline Package		
Vapor Phase (60 seconds)		215°C
Infrared (15 seconds)		220°C
See AN-450 "Surface Mounting Methods and Their Effect on Product Reliability" for other methods of soldering surface mount devices.		
ESD Tolerance (Note 12)		900V

**DC Electrical Characteristics** (Note 7)

Symbol	Parameter	Conditions	LF147			LF347B			LF347			Units
			Min	Typ	Max	Min	Typ	Max	Min	Typ	Max	
$V_{OS}$	Input Offset Voltage	$R_S=10\text{ k}\Omega$ , $T_A=25^\circ\text{C}$ Over Temperature		1	5		3	5		5	10	mV mV
$\Delta V_{OS}/\Delta T$	Average TC of Input Offset Voltage	$R_S=10\text{ k}\Omega$		10			10			10		$\mu\text{V}/^\circ\text{C}$
$I_{OS}$	Input Offset Current	$T_J=25^\circ\text{C}$ , (Notes 7, 8) Over Temperature		25	100		25	100		25	100	pA nA
$I_B$	Input Bias Current	$T_J=25^\circ\text{C}$ , (Notes 7, 8) Over Temperature		50	200		50	200		50	200	pA nA
$R_{IN}$	Input Resistance	$T_J=25^\circ\text{C}$		$10^{12}$			$10^{12}$			$10^{12}$		$\Omega$
$A_{VOL}$	Large Signal Voltage Gain	$V_S=\pm 15\text{V}$ , $T_A=25^\circ\text{C}$ $V_O=\pm 10\text{V}$ , $R_L=2\text{ k}\Omega$ Over Temperature	50	100		50	100		25	100		V/mV V/mV
$V_O$	Output Voltage Swing	$V_S=\pm 15\text{V}$ , $R_L=10\text{ k}\Omega$	$\pm 12$	$\pm 13.5$		$\pm 12$	$\pm 13.5$		$\pm 12$	$\pm 13.5$		V
$V_{CM}$	Input Common-Mode Voltage Range	$V_S=\pm 15\text{V}$	$\pm 11$	+15 -12		$\pm 11$	+15 -12		$\pm 11$	+15 -12		V V
CMRR	Common-Mode Rejection Ratio	$R_S \leq 10\text{ k}\Omega$	80	100		80	100		70	100		dB
PSRR	Supply Voltage Rejection Ratio	(Note 9)	80	100		80	100		70	100		dB
$I_S$	Supply Current			7.2	11		7.2	11		7.2	11	mA
	Amplifier to Amplifier Coupling	$T_A=25^\circ\text{C}$ , $f=1\text{ Hz}-20\text{ kHz}$ (Input Referred)		-120			-120			-120		dB
SR	Slew Rate	$V_S=\pm 15\text{V}$ , $T_A=25^\circ\text{C}$	8	13		8	13		8	13		V/ $\mu\text{s}$
GBW	Gain-Bandwidth Product	$V_S=\pm 15\text{V}$ , $T_A=25^\circ\text{C}$	2.2	4		2.2	4		2.2	4		MHz
$e_n$	Equivalent Input Noise Voltage	$T_A=25^\circ\text{C}$ , $R_S=100\Omega$ , $f=1000\text{ Hz}$		20			20			20		$\text{nV}/\sqrt{\text{Hz}}$
$i_n$	Equivalent Input Noise Current	$T_J=25^\circ\text{C}$ , $f=1000\text{ Hz}$		0.01			0.01			0.01		$\text{pA}/\sqrt{\text{Hz}}$
THD	Total Harmonic Distortion	$A_V=+10$ , $R_L=10\text{k}$ , $V_O=20\text{ Vp-p}$ , $\text{BW}=20\text{ Hz}-20\text{ kHz}$		<0.02			<0.02			<0.02		%

Tableau (1) : caractéristiques électrique du LF347

## 1.2 AD633

C'est un composant intégré comportant trois

AMP-OP comme le montre la figure (2)

Ca sortie se calcule tel que :

$$W = \frac{((x_1 - x_2)(y_1 - y_2))}{10} + Z$$

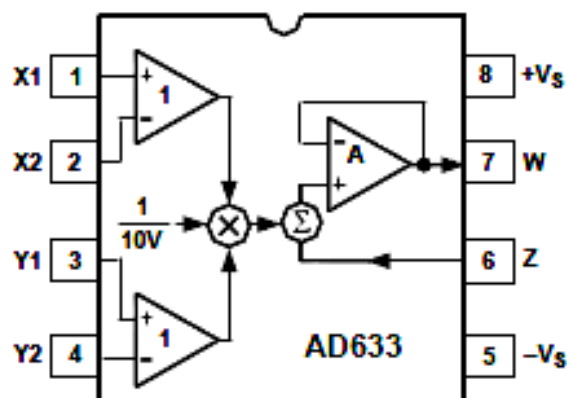


Figure (2) : multiplieur AD633

## AD633—SPECIFICATIONS ( $T_A = +25^\circ\text{C}$ , $V_S = \pm 15\text{ V}$ , $R_L \geq 2\text{ k}\Omega$ )

Model		AD633J, AD633A			
TRANSFER FUNCTION		$W = \frac{(X_1 - X_2)(Y_1 - Y_2)}{10\text{ V}} + Z$			
Parameter	Conditions	Min	Typ	Max	Unit
<b>MULTIPLIER PERFORMANCE</b>					
Total Error	$-10\text{ V} \leq X, Y \leq +10\text{ V}$		$\pm 1$	$\pm 2$	% Full Scale
$T_{\text{MIN}}$ to $T_{\text{MAX}}$			$\pm 3$		% Full Scale
Scale Voltage Error	SF = 10.00 V Nominal		$\pm 0.25\%$		% Full Scale
Supply Rejection	$V_S = \pm 14\text{ V}$ to $\pm 16\text{ V}$		$\pm 0.01$		% Full Scale
Nonlinearity, X	$X = \pm 10\text{ V}$ , $Y = +10\text{ V}$		$\pm 0.4$	$\pm 1$	% Full Scale
Nonlinearity, Y	$Y = \pm 10\text{ V}$ , $X = +10\text{ V}$		$\pm 0.1$	$\pm 0.4$	% Full Scale
X Feedthrough	Y Nulled, $X = \pm 10\text{ V}$		$\pm 0.3$	$\pm 1$	% Full Scale
Y Feedthrough	X Nulled, $Y = \pm 10\text{ V}$		$\pm 0.1$	$\pm 0.4$	% Full Scale
Output Offset Voltage			$\pm 5$	$\pm 50$	mV
<b>DYNAMICS</b>					
Small Signal BW	$V_O = 0.1\text{ V rms}$		1		MHz
Slew Rate	$V_O = 20\text{ V p-p}$		20		V/ $\mu\text{s}$
Settling Time to 1%	$\Delta V_O = 20\text{ V}$		2		$\mu\text{s}$
<b>OUTPUT NOISE</b>					
Spectral Density			0.8		$\mu\text{V}/\sqrt{\text{Hz}}$
Wideband Noise	$f = 10\text{ Hz}$ to $5\text{ MHz}$		1		mV rms
	$f = 10\text{ Hz}$ to $10\text{ kHz}$		90		$\mu\text{V rms}$
<b>OUTPUT</b>					
Output Voltage Swing		$\pm 11$			V
Short Circuit Current	$R_L = 0\ \Omega$		30	40	mA
<b>INPUT AMPLIFIERS</b>					
Signal Voltage Range	Differential	$\pm 10$			V
	Common Mode	$\pm 10$			V
Offset Voltage X, Y			$\pm 5$	$\pm 30$	mV
CMRR X, Y	$V_{\text{CM}} = \pm 10\text{ V}$ , $f = 50\text{ Hz}$	60	80		dB
Bias Current X, Y, Z			0.8	2.0	$\mu\text{A}$
Differential Resistance			10		M $\Omega$
<b>POWER SUPPLY</b>					
Supply Voltage			$\pm 15$		V
Rated Performance				$\pm 18$	V
Operating Range		$\pm 8$		6	V
Supply Current	Quiescent		4		mA

Tableau (2) : caractéristique du AD633

### 1.3 Amplificateur inverseur

Ce type de montage permet d'amplifier un signal en l'inversant et le gain  $A_v$  c'est a dire la valeur par laquelle on multiplie la tension d'entrée pour obtenir celle de la sortie se calcule en divisant la valeur de la résistance  $R_2$  par  $R_1$  avec le signe - car le signal est inversé.

$$A_v = \frac{V_s}{V_e} = -\frac{R_2}{R_1}$$

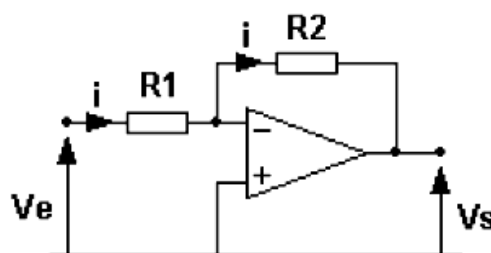


Figure (3) : Amplificateur inverseur

### 1.4 Amplificateur non inverseur

Voici une autre configuration typique avec un gain  $A_v$  positif.

$$A_v = \frac{V_s}{V_e} = 1 + \frac{R_2}{R_1}$$

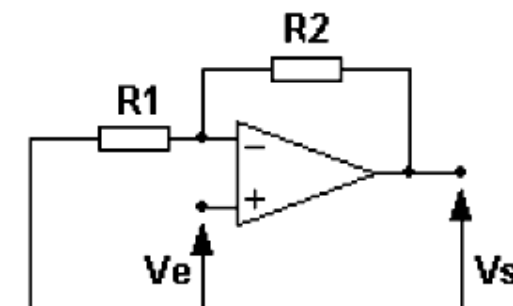


Figure (4) : Amplificateur non inverseur

### 1.5 Montage suiveur

L'amplificateur séparateur ou suiveur, la valeur du signal d'entrée suit celle du signal de sortie .Ce circuit peut sembler inutile car

le gain  $A_v = 1$  ; or il sera très pratique dans le cas où l'on a un signal d'entrée avec un certain niveau de tension mais un faible courant , en sortie de

l'amplificateur la tension sera conservé mais nous disposerons alors du courant nécessaire pour commander la suite du circuit.

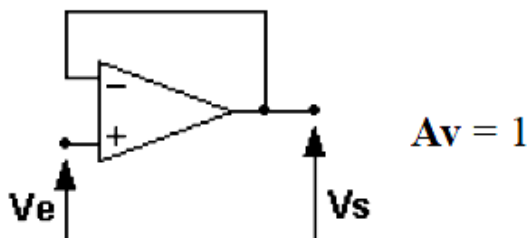


Figure (5) : suiveur

## 1.6 Montages opérationnels

### 1.6.1 Additionneur inverseur

L'ampli-op facilite le montage d'additionneurs. Comme son nom l'indique, l'additionneur est un circuit dont la tension de sortie est égale à la somme des tensions appliquées à chacune de ces entrées. L'appellation "mélangeur" s'applique au circuit qui "mélange" des signaux alternatifs, il est fort utilisé en audio.

$$V_s = -(V_{e1} + V_{e2} + V_{e3})$$

Si le gain est différent pour chaque entrée :

$$V_s = \left( V_{e1} \frac{R}{R_1} + V_{e2} \frac{R}{R_2} + V_{e3} \frac{R}{R_3} \right)$$

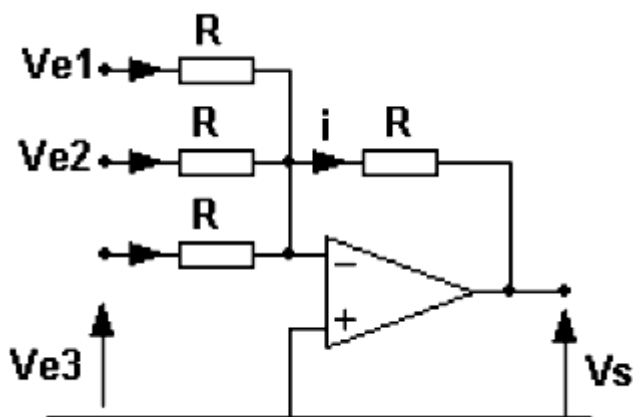


Figure (6) : Additionneur inverseur

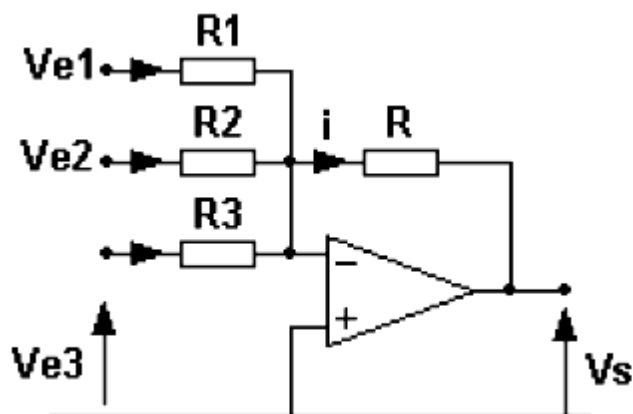


Figure (7) : Additionneur inverseur

### 1.6.2 Montage soustracteur (différentiel)

Ce montage permet d'amplifier la différence de deux signaux. C'est un montage de base très important en mesures. Tel quel, ce montage n'est pas un ampli de différence ; il faut imposer des conditions sur les résistances.

Si on pose :  $K = \frac{R_2}{R_1} = \frac{R_4}{R_3}$ , on obtient  $V_s = K (V_{e1} - V_{e2})$

On a bien en sortie la différence des deux signaux d'entrée multipliée par le gain  $k$ .

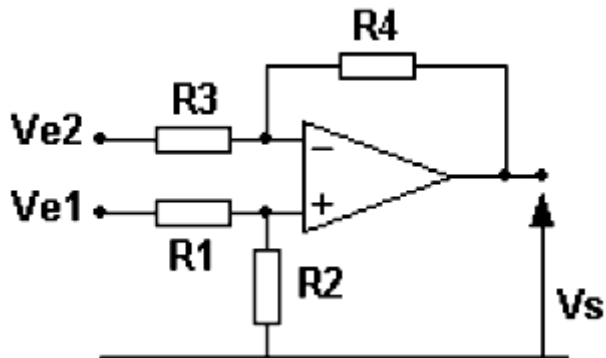
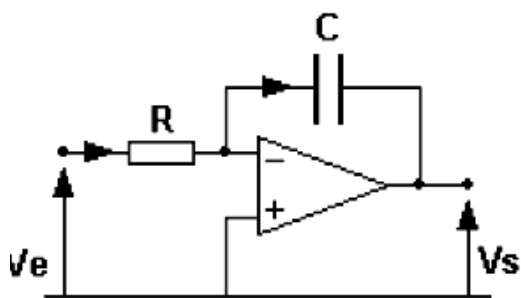


Figure (8) : Montage soustracteur

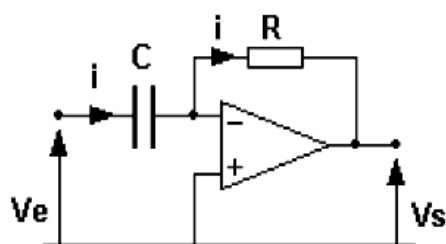
### 1.6.3 Montage intégrateur



$$V_s = \frac{1}{RC} \int V_e dt$$

Figure (9) : Montage intégrateur

### 1.6.4 Montage dérivateur



$$V_s = RC \frac{dV_e}{dt}$$

Figure (10) : Montage dérivateur

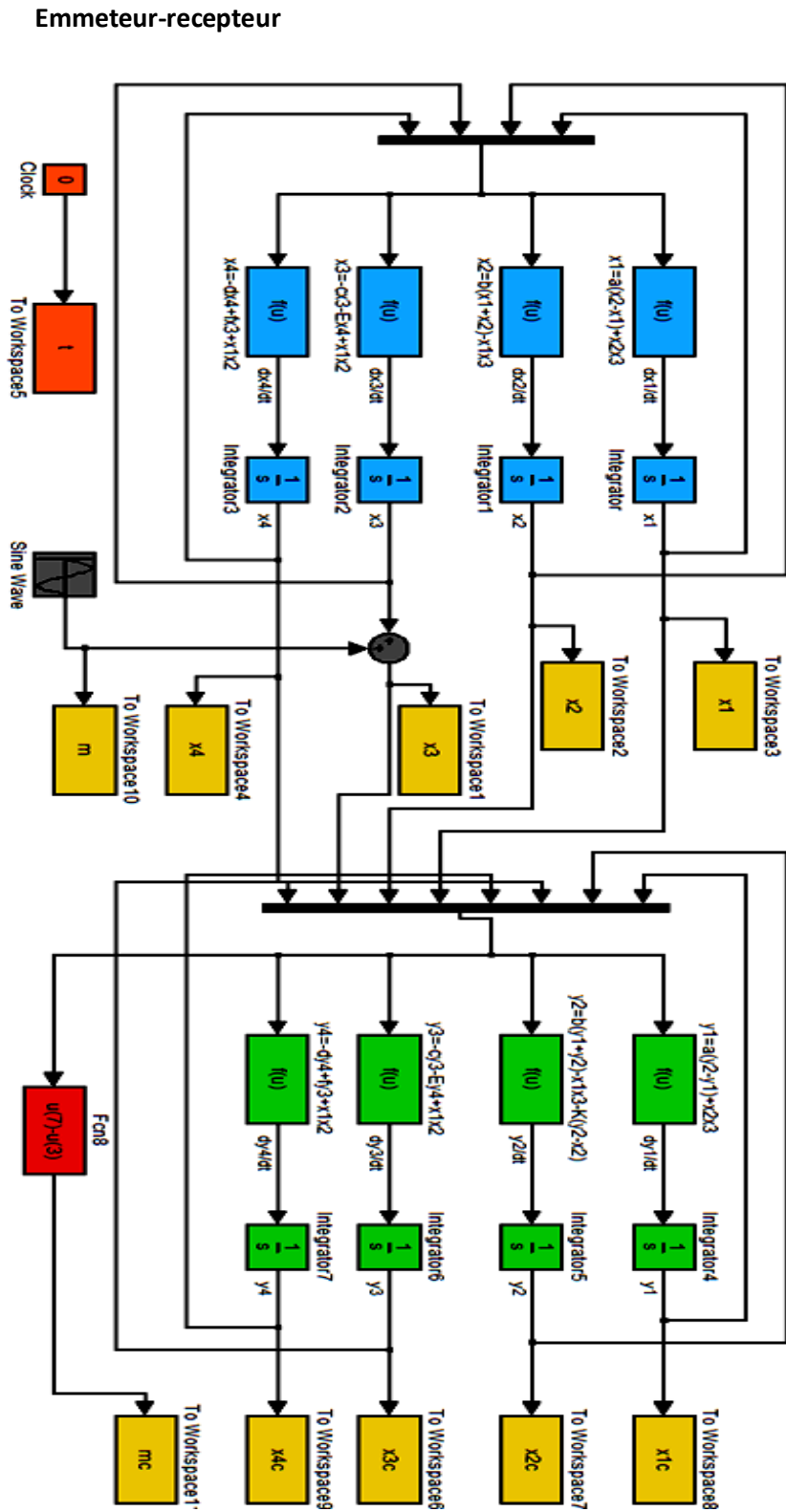


Figure (2) : schéma de simulation émetteur-récepteur

## Emetteur

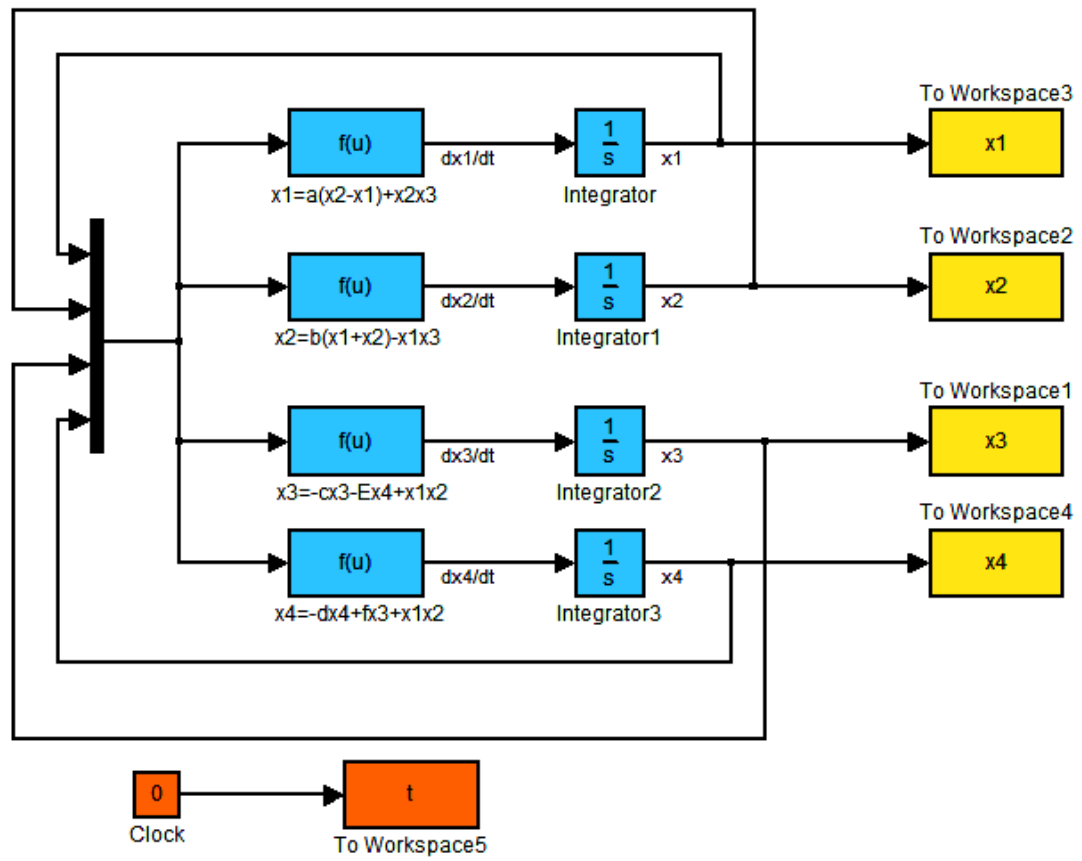


Figure (3.1) : schéma de simulation émetteur-récepteur