الجمهورية الجزائرية الديمقراطية الشعبية
**République Algérienne démocratique et populaire**

وزارة التعليم العالي و البحث العلمي
**Ministère de l'enseignement supérieur et de la recherche scientifique**

جامعة سعد دحلب البليدة
**Université SAAD DAHLAB de BLIDA**

كلية التكنولوجيا
**Faculté de Technologie**

قسم الإلكترونيك
**Département d'Électronique**

# Mémoire de Projet de Fin d'Études

Présenté par

OUKSOUM Ryma

&

BOUMESSID Hanane

Pour l'obtention du diplôme de Master en Electronique

Spécialité : Télécommunications et Réseaux.

Thème

# Transmission sécurisée par modulation CSK (Chaos Shift Keying)

Proposé par : Mr.CHIKHI Mohamed Lazhar

Année Universitaire 2015-2016

## Remerciements

Nous tenons tout d'abord à remercier « DIEU » qui nous a donné le courage, la confiance et l'opportunité de mener à bien ce travail.

Notre profonde gratitude et nos sincères remerciements vont à notre promoteur « Mr.CHIKHI Mohamed Lazhar » pour son encadrement, ses conseils, sa présence et son soutien tout le long de ce mémoire.

On adresse nos sincères remerciements à toute l'équipe du laboratoire « LABSET » où nous avons travaillé durant toute la période de préparation de ce mémoire, ainsi qu'à tous les enseignants de notre cursus d'avoir enrichi nos connaissances et de nous avoir guidé durant toutes ces années.

On exprime toute notre gratitude aux membres du jury, qui ont accepté d'évaluer notre travail.

Finalement, nous tenons aussi à remercier nos très chers parents pour leur soutien et leur confiance, ainsi qu'à nos sœurs et frères et nos amis(e).

## Dédicaces

*Que ce travail témoigne de mes respects :*

*A mes parents :*

*Grâce à leurs tendres encouragements et leurs grands sacrifices, ils ont pu créer le climat affectueux et propice à la poursuite de mes études.*

*Aucune dédicace ne pourrait exprimer mon respect, ma considération et mes profonds sentiments envers eux.*

*Je prie le bon Dieu de les bénir, de veiller sur eux, en espérant qu'ils seront toujours fiers de moi.*

*A ma sœur « LILY » et à mes chers frères « LYES » & « ANOUAR ».*

*A ma famille « OUKSOUM » & « SLIMANI ».*

*Ils vont trouver ici l'expression de mes sentiments de respect et de reconnaissance pour le soutien qu'ils n'ont cessé de me porter.*

*A ma chère binôme « HANANE » avec qui j'ai passé de très bons moments.*

*A tous mes professeurs :*

*Leur générosité et leur soutien m'oblige de leurs témoigner mon profond respect et ma loyale considération.*

*A tous mes amis (e) et mes collègues :*

*Ils vont trouver ici le témoignage d'une fidélité et d'une amitié infinie.*

*RYMA OUKSOUM*

# Dédicaces

*Je dédie ce mémoire :*

*A mes très chers parents pour leur amour inestimable, leur confiance, leur soutien, leurs sacrifices et toutes les valeurs qu'ils ont su m'inculquer. Je vous remercie pour tout ce que vous avez fait pour moi. Que ce modeste travail soit l'exaucement de vos vœux tant formulés que dieu vous accorde santé, bonheur et longue vie*

*A mes sœurs « FERIAL » & « AMINA» sans oublier ma très chère « AROURA » pour leurs précieux encouragements*

*Je vous souhaite beaucoup de bonheur et de réussite.*

*A toute ma famille, à tous mes cousins & cousines.*

*A mes amis (e) qui m'ont soutenue de près ou de loin*

*A ma chère binôme « RYMA » qui a supporté mon humeur tout au long du travail et avec qui j'ai passé de très bons moments merci du fond de cœur.*

*A tous les étudiants avec qui j'ai parcouru mon cursus universitaire.*

*HANANE BOUMESSID*

**ملخص**: يتمثل هذا العمل في تحقيق إرسال مطمئن عبر تقنيات CSK (إدخال تحول فوضوي), جهاز الإرسال يتكون من جهاز شديد الفوضىQI حيث تم إجراء تحليل الخصائص الأولية على مستوى جهاز الإستقبال التزامن بحلقة مغلقة من أجل إسترداد الرسالة ( مثال الصورة المشفرة ) التنفيد لجهاز شديد الفوضىQI على بطاقة FPGA و الحصول على الإرشادات المتوافقة مع التي تحصلنا على مستوى MATLAB (Simulink)

**كلمات المفاتيح** : دليل تزامن, تشفير , تشعيب , بطاقة FPGA . نظام QI, إشارة فوضوية, المزامنة بحلقة مغلقة

**Résumé :** Ce travail consiste à réaliser une transmission sécurisée par modulation CSK (Chaos Shift Keying).L'émetteur est construit autour du système hyper-chaotique de Qi dont les principales propriétés sont analysées. Au niveau du récepteur, la synchronisation par boucle fermée a été utilisée pour la récupération du message (exemple d'une image cryptée). Une implémentation sur circuit FPGA Virtex-5 en virgule flottante du système hyper-chaotique de Qi a été réalisée, et les différents signaux ainsi obtenus ont été visualisés sur oscilloscope numérique montrant une bonne concordance avec ceux obtenus par simulation sous Matlab-Simulink d'une part et sous ModelSim d'autre part.

**Mots clés :** signal chaotique; cryptage; synchronisation ; boucle fermée ; système de Qi ; FPGA.

**Abstract:** This work is to realize a secure transmission by modulation CSK (Chaos Shift Keying). The transmitter is built around The hyper-chaotique system of Qi whose main properties are analyzed. At the receiver, the synchronization by closed loop was used for the recovery of the message (for example encrypted image). An implementation in the FPGA circuit Virtex-5 by using floating point of the Qi hyper chaotic system has been realized, and the different Signals obtained were visualized on digital oscilloscope show a good concordance with those obtained by simulation under Matlab Simulink and ModelSim.

**Keywords:** chaotic signal; encryption; synchronization, closed loop; Qi system; FPGA circuit.

## Listes des acronymes et abréviations

ASK : Amplitude Shift Keying.

FSK : Frequency Shift Keying.

PSK : Phase Shift Keying.

CSK : Chaos Shift Keying.

CAN: Convertisseur Analogique Numérique.

CNA: Convertisseur Numérique Analogique.

CLB: Configurable Logic Block.

CPLD : Complex Programmable Logic Device.

CAO : Conception Assistée par Ordinateur.

BER : Bit Error Rate.

DES : Data Encryption Standard.

D$\mathcal{F}$(x) : Matrice du système.

DSP : Digital Signal Processor.

EEPROM: Electrically Erasable Programmable Read-Only Memory.

EPROM : Erasable Programmable Read-Only Memory.

FPGA: Field Programmable Gate Array.

HDL: Hardware Description Language.

IOB: Input Output Block.

ISE: Integrated Software Environment.

SRAM: Static Random Access Memory.

USB: Universal Serial Bus.

DVI: Digital Visual Interface.

LCD: Liquid-Crystal Display.

VHDL: Very High Density Logic.

VLSI : Very Large Scale Integration.

m(t) : Message informatif.

Mk : $k^{ième}$ point d'intersection de la trajectoire avec le plan de coupe.

a,b,c,d,e,f : Paramètres du système de Qi.

m'(t) : Message récupéré.

r(t) : Signal crypté.

x(t) : Signal chaotique.

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

$R^n$ : Ensemble des nombres réels.

$R^+$: Ensemble des nombres réels positifs.

$R_n$ : Espace vectoriel de dimension n construit dans le corps des réels.

$Z^+$ : Ensemble des nombres rationnels positifs.

$x_0$ : L'état initial.

$x_k$ : L'état x au temps t=k.

$x_{k+1}$ : L'état de x au temps t=k+1.

$\overline{x}$ : Point fixe.

$\xi$ : La différence entre l'état x et le point fixe.

$\theta$ : L'orbite périodique.

$\omega$ : L'angle de l'orbite.

$\lambda i$ : Valeurs propres de la matrice jacobienne ou exposant de Lyapunov d'ordre i.

$r$ : Le paramètre de contrôle dans une bifurcation.

$\mu$ : Le paramètre de contrôle dans une bifurcation.

$\tau$ : Un retard positif.

$a^{(i)}$ : Le vecteur propre.

# Table des matières

# Liste des figures

# Liste des tableaux

# Introduction générale

L'échange de données (paroles, images, signes, signal etc.....) pour l'homme est une nécessité. La sécurité de cette opération devient parfois plus qu'une exigence. Ainsi, le chiffrement de certains messages a toujours été un besoin afin de les cacher à tout intrus non autorisé de façon à s'abriter d'un éventuel usage malveillant. De nos jours, L'ensemble de ces méthodes a été regroupé dans une branche appelée la cryptographie [11].

Les techniques de cryptographie classique sont basées sur la théorie des nombres. Nous pouvons aussi citer les deux algorithmes bien connus : DES, RSA. Néanmoins, avec la révolution de l'informatique, ces algorithmes proposés ne sont pas assez sécurisés. Pour cette raison plusieurs chercheurs essayent de mettre en œuvre d'autres « crypto-systèmes ». Durant ces dernières décennies, la théorie des systèmes non linéaires a été appliquée à la cryptographie afin d'augmenter le degré de sécurité. Notamment, après le travail de Pecora et Carroll, des applications du chaos ont attiré beaucoup d'attention [5].

La transmission chaotique est un mode de communication à clé secrète. La connaissance de cette clé est nécessaire du côté de l'émetteur du message ainsi que du récepteur pour le chiffrement et le déchiffrement du message. On doit alors disposer au niveau du récepteur, d'un signal chaotique identique à la porteuse pour pouvoir récupérer le message masqué.

Le travail de ce mémoire qui consiste à réaliser un système de transmission sécurisée à base du chaos est organisé de la façon suivante :

Le premier chapitre présente des définitions importantes concernant les systèmes dynamiques et les systèmes chaotiques. Ces définitions seront utilisées pour la conception de l'émetteur chaotique.

Le second chapitre consiste à étudier l'émetteur qui est composé de l'oscillateur hyper chaotique de Qi.

Dans le troisième chapitre, on va parcourir les différents types de la synchronisation du chaos, On mettra en évidence la méthode qu'on va utiliser pour récupérer notre message crypté émis. Ainsi les différentes méthodes d'insertion du message.

Le quatrième chapitre présente un aperçu sur la technologie FPGA et avec laquelle on va implémenter notre émetteur hyper chaotique de Qi en utilisant le langage VHDL.

# Chapitre 1 Les systèmes dynamiques chaotiques

## 1.1 Introduction :

Les systèmes dynamiques chaotiques sont depuis longtemps connus dans le domaine des mathématiques mais c'est seulement au cours de la dernière décennie que les applications concrètes se sont multipliées. Nous nous intéresserons principalement dans ce chapitre aux systèmes dynamiques chaotiques en nous attardant sur les espaces de phases, les attracteurs étranges et les scénarios de transition vers le chaos (appelés aussi bifurcations), lesquels nous permettront de mieux comprendre la nature du chaos. Notre étude va se focaliser sur l'usage du chaos pour transmettre de l'information. Ainsi, l'objectif de ce chapitre est de donner quelques notions élémentaires sur les systèmes dynamiques afin de mieux appréhender ce qu'est le chaos : ses apparitions dans un système et la manière de le quantifier [3] [1].

## 1.2 Les systèmes dynamiques :

### 1.2.1 Définition d'un système dynamique :

Un système dynamique consiste en un espace de phase abstrait ou un espace d'état dont les coordonnées décrivent l'état dynamique du système à n'importe quel moment et dont une règle dynamique spécifie la tendance future immédiate de toutes les variables d'état composant le système, donnée par la valeur présente de ces mêmes variables d'état.

Mathématiquement, un système dynamique est décrit par un problème où seules sont données les valeurs de départ des variables d'état sont données. Il peut y avoir une composante de temps "discrète" ou "continue".

Ce système est décrit par un ensemble d'équations différentielles ordinaires du premier ordre du type [6] :

$$\frac{dx}{dt} \stackrel{\text{def}}{=} \dot{x} = f(x,t) \tag{1.1}$$

### 1.2.2 Système dynamique à temps continu :

Un système à temps continu est décrit par un système d'équations différentielles :

$$\dot{x}(\mathrm{t}) = \mathrm{F}\ (x(\mathrm{t}),t) \tag{1.2}$$

Où $\mathrm{F} : \mathrm{R}^{\mathrm{n}} \mathrm{X}\ \mathrm{R}^{+} \longrightarrow \mathrm{R}^{\mathrm{n}}$ désigne la dynamique du système.

Si on associe à cette dynamique un état initial : $x_0 = x(t_o)$, pour chaque couple choisi ($x_0$ , $t_0$) on peut identifier une solution unique de F.

On considère l'exemple du célèbre système de Lorenz donné par les équations suivantes :

$$\begin{aligned} \frac{dx}{dt} &= \sigma(y-x) \\ \frac{dy}{dt} &= x(\rho - z) - y \\ \frac{dz}{dt} &= xy - bz \end{aligned} \tag{1.3}$$

Les paramètres pour l'exemple de trajectoire donné dans la figure (1.1) ont été choisis de la manière suivante :$\sigma$= 10, $\rho$ = 28, $b$ = 8⁄3 avec la condition initiale

($x_0$, $y_0$, $z_0$) = $(2, 5, 20)$.

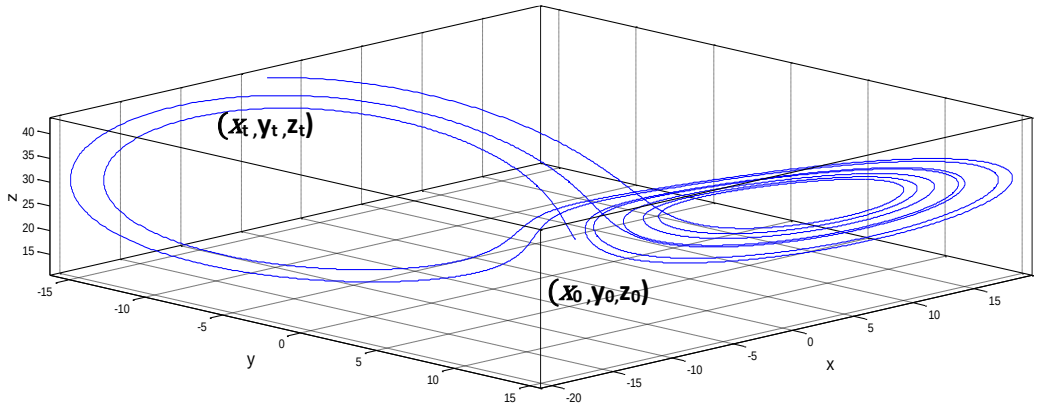



**Figure 1.1**: Exemple de trajectoire du système de Lorenz.

### 1.2.3 Système dynamique à temps discret :

Un système dynamique dans le cas discret est représenté par des équations aux différences finies, avec le modèle général suivant :

$$x_{k+1} = G(x_k, k) \tag{1.4}$$

Où G : $R^n$ X $Z^+$ ⟶ $R^n$ indique la dynamique du système en temps discret.

De même qu'en temps continu, si on associe à cette dynamique un état initial : $x_0 = x(k_0)$, pour chaque couple choisi ($x_0$, $k_0$) on peut identifier une solution unique de $G$[3].

### 1.2.4 Système autonome et non autonome :

Soit le système dynamique suivant :

$$\dot{x} = \frac{dx}{dt} = f(x, t) \tag{1.5}$$

Lorsque le champ de vecteur f ne dépend pas explicitement du temps, on dit que le système dynamique est autonome. Dans le cas contraire il est non autonome.

Dans un système autonome, la trajectoire ne dépend pas du temps initial $t$, alors que dans un système non autonome elle dépend de t[4].

## 1.3 Le chaos :

### 1.3.1 Définition du chaos :

On dit qu'un système est chaotique lorsque son évolution dans le temps est très sensible aux conditions initiales. Ainsi, deux trajectoires générées à partir des conditions initiales très proches, vont diverger très rapidement l'une par rapport à l'autre. Cette sensibilité par rapport aux conditions initiales traduit aussi le comportement en apparence stochastiques des générateurs chaotiques de telle sorte qu'une prévision à long terme du comportement du système devienne impossible [5].

### 1.3.2 Caractéristiques du chaos :

Les phénomènes chaotiques ne sont pas aléatoires mais obéissent au contraire à des lois déterministes, parfois assez simple dans leur représentation mathématique. Les phénomènes traités par les lois du chaos se caractérisent par des propriétés génériques fondamentales en plus de la sensibilité aux conditions initiales [5], les définitions et propriétés suivantes permettent de comprendre qualitativement les points marquants des systèmes chaotiques [7] :

- **La non-linéarité :**

  Un système chaotique est décrit par un ensemble d'équations dynamiques non linéaires et déterministes. Bien que ces équations définissent complètement son évolution, il est imprédictible à long terme [5].

- **Le déterministe :**

  La notion de déterminisme signifie la capacité de « prédire » le futur d'un phénomène à partir d'un évènement passé ou présent.

  L'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités [7].

- **L'aspect aléatoire :**

Tous les états d'un système chaotique présentent des aspects aléatoires. La figure 1.2 représente l'état chaotique x1 du système de Lorenz :

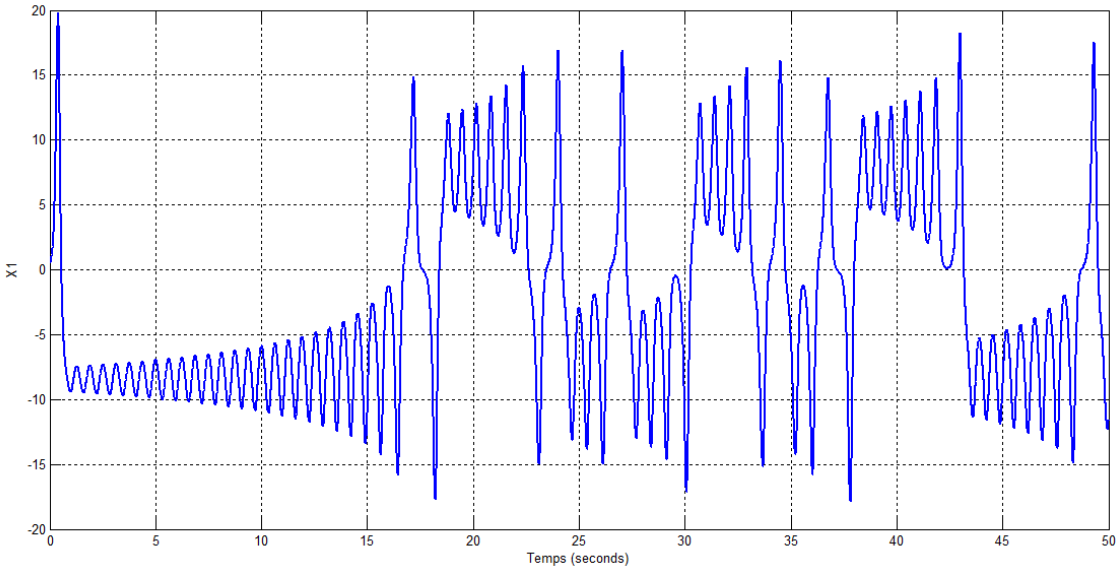



**Figure 1.2**: Etat chaotique x du système de Lorenz.

- **La sensibilité aux conditions initiales :**

Certains phénomènes dynamiques non linéaires sont si sensibles aux conditions initiales que, même s'ils sont régis par des lois rigoureuses et parfaitement déterministes, les prédictions exactes sont impossibles. Il est clair que la moindre erreur ou imprécision sur la condition initiale interdit de décider à tout temps quelle serait la trajectoire effectivement suivie et de faire une prédiction sur l'évolution à long terme du système.

Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant des taux de divergence des trajectoires. Ceci est illustré par la figure 1.3 [9].

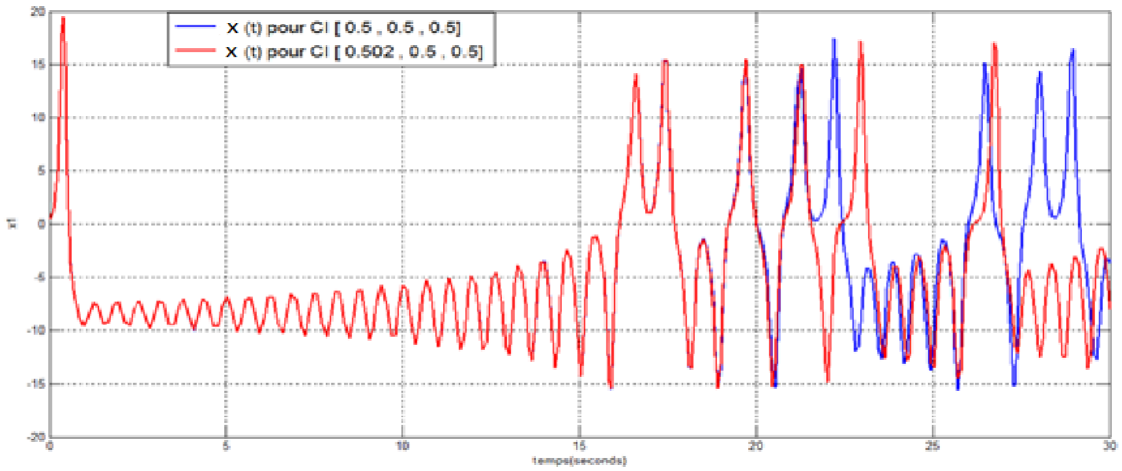



**Figure 1.3 :** Illustration de la propriété de sensibilité aux conditions initiales sur l'état x.

### 1.3.3 L’histoire du chaos :

Edward Lorenz, professeur de mathématiques est le fondateur officiel de la théorie du chaos. Il observa le phénomène en 1961 et l'ironie du sort a voulu qu'il découvre ce qui s'appellera plus tard la théorie du chaos par hasard, à la suite de calculs visant à prévoir les phénomènes météorologiques.

Ces prévisions nécessitaient un nombre très important de calculs. En effet les phénomènes météorologiques obéissent aux lois de Newton, aux trajectoires des corps, etc….. Et donc au calcul d'équations différentielles très complexes du fait du nombre astronomique de variables entrant en jeu. Pour résoudre ces équations, Lorenz les a tout d'abord simplifiées au maximum, jusqu'à obtenir un système de trois équations avec trois inconnues, mais les calculs restaient impossibles à faire à la main, Il utilisa donc un ordinateur .après plusieurs heures de calcul l'ordinateur retourna sous forme de colonnes de chiffres les résultats des équations, Lorenz décida alors de repasser une deuxième fois ces données dans l'ordinateur pour s'assurer des résultats. Mais au lieu d'entrer les variables à six chiffres après la virgule il décida de n'en garder que trois pour gagner du temps. Il pensait, comme beaucoup de mathématiciens à l'époque, qu'une faible variation dans les variables à la base d'un calcul aussi complexe aurait une incidence du même ordre de grandeur sur le résultat final. Seulement voilà, les résultats obtenus étaient totalement différents.

Il venait de découvrir le comportement chaotique d'un système non linéaire, soit que d'infimes différences dans les conditions initiales d'un système déterministe entraînaient des résultats complètement différents. On appellera plus tard cette théorie, la théorie du chaos. Ce nom, fut trouvé par le mathématicien Yorke, en 1975. Lorenz entreprit alors de représenter 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 d'évolution de son système météorologique avec deux jeux de valeurs initiales très proches, et comme il s'y attendait les trajectoires des deux courbes semblaient identiques au départ mais divergeaient de plus en plus. Par contre ce à quoi Lorenz ne s'attendait pas, c'est que les deux courbes soient plus ou moins identiques, non pas point par point mais dans leur ensemble. Les deux courbes ressemblaient aux ailes déployées d'un papillon. Il eut beau

recommencer l'expérience autant de fois qu'il le voulait, il obtenait toujours le même résultat.

Des années plus tard Mandelbrot découvrit la géométrie fractale et vit que l'attracteur de Lorenz en était une, comme la grande majorité des attracteurs étranges.
Pour mieux faire comprendre l'importance de cette sensibilité aux conditions initiales, Lorenz eut recours à une métaphore qui contribua au succès médiatique de la théorie du chaos : "le simple battement d'ailes d'un papillon au Brésil pourrait déclencher une tornade au Texas". Ainsi une donnée infime, imperceptible, pouvait aboutir à une situation totalement différente de celle calculée sans tenir compte de cette donnée infime [15].

## 1.4 Plan de phase :

Un système dynamique est caractérisé par un certain nombre de variables d'état, qui ont la propriété de définir complètement l'état du système à un instant donné. Le comportement dynamique du système est ainsi relié à l'évolution de chacune de ces variables d'état. Cet espace est appelé l'espace de phase où chaque point définit un état et le point associé à cet état décrit une trajectoire, appelée également une orbite [1].

Le portrait de phase d'un système dynamique est une représentation graphique de plusieurs trajectoires représentatives dans l'espace des phases. Etant donné un système dynamique, $\dot{x}$ = f (x,t), sans résoudre les équations, on peut toujours, à un instant t donné, représenter graphiquement (à l'aide des flèches) le champ des $\dot{x}$ (x est la coordonnée du champ des vitesses). La lecture de cette représentation graphique sera très utile pour se faire une idée du comportement du système. Il s'agit d'un espace de dimensions 2 ou 3 dans lequel chaque coordonnée est une variable d'état du système considéré. Il permet de distinguer un comportement chaotique d'un comportement purement aléatoire à l'aide des conditions initiales.
La figure 1.4 représente un exemple d'un plan de phase [8].

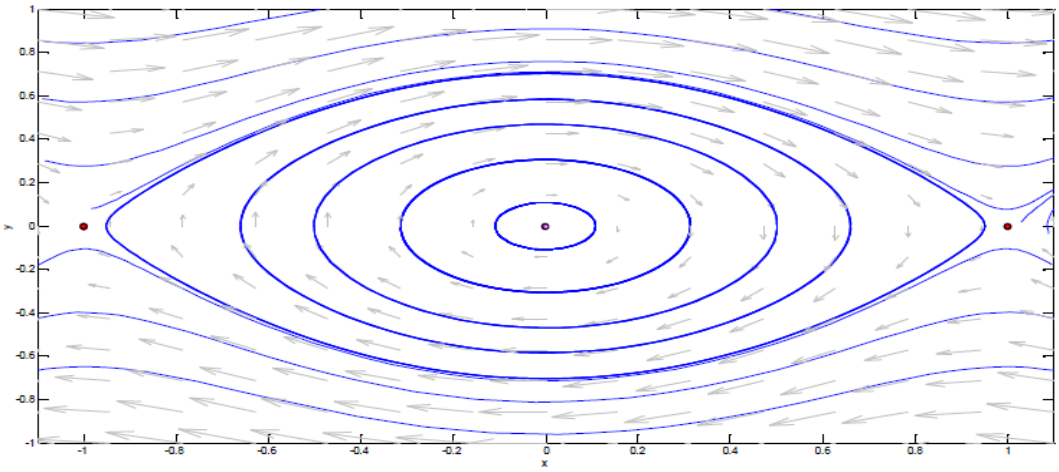


**Figure 1.4 :** Exemple d'un plan de phase [8].

## 1.5 Les points fixes :

On appelle également point fixe, point stationnaire, point d'équilibre ou point critique, le point $\bar{x}$ de l'espace des phases obtenu en annulant le second membre de la fonction dynamique F :

$$F(\bar{x})=0 \tag{1.6}$$

Par le changement de variables $\xi=x-\bar{x}$, on peut ramener le point $\bar{x}$ à l'origine [8].

### 1.5.1 Stabilité des points fixes :

Un point fixe $\bar{x} \in R^n$ est stable si :

$$\forall \varepsilon>0, \exists \delta>0 \; telque \qquad \|x(0)-\bar{x}\|<\delta \rightarrow \|x(t)-\bar{x}\|<\varepsilon \tag{1.7}$$

Où $\|\|$désigne la norme dans $R^n$.

Si de plus, il existe $\delta_0$ avec $0< \delta_0< \delta$ tel que :

$$\|x(0)-\bar{x}\|<\delta_0 \rightarrow \lim_{t\to\infty} x(t)= \bar{x} \tag{1.8}$$

$\bar{x}$ est asymptotiquement stable [8].

### 1.5.2 Stabilité du système linéarisé (valeurs propres) :

La matrice $D\mathcal{F}(x)$ est la matrice jacobéenne de $\mathcal{F}$(x) :

$$D\mathcal{F}(x)\equiv\frac{\partial\mathcal{F}i(x)}{\partial xj} \tag{1.9}$$

Son déterminant est le jacobien.

Pour x petit, le comportement du système au voisinage de 0 est celui du système linéarisé :

$$\dot{x}=D\mathcal{F}(0)\text{x} \tag{1.10}$$

Dans le cas où la matrice : $\mathcal{F}$(0) possède n valeurs propres $\lambda_i$,=1,…, n distinctes, la solution est :

$$x=\sum_{i=1}^{n} c_{\text{i}}a^{(\text{i})}\exp\lambda_{\text{i}}\text{t} \tag{1.11}$$

Où $a^{\text{i}}$ est le vecteur propre correspondant à la valeur propre $\lambda_i$ et les $c_i$, $i$=1,2,..., n sont des constantes (déterminées par les conditions initiales).On en déduit que :

a) Si toutes les valeurs propres $\lambda_i$ ont leur partie réelle négative, le point fixe est asymptotiquement stable.
b) Si une ou plusieurs valeurs propres sont des imaginaires pures, les autres valeurs propres ayant leur partie réelle négative, le point fixe est un centre ou un point elliptique (stable mais pas asymptotiquement stable).
c) Si une des valeurs propres a sa partite réelle positive le point fixe est instable.
d) Si $D\mathcal{F}$(0) n'a pas de valeur nulle ou purement imaginaire, le point fixe est un point hyperbolique. Dans le cas contraire, il est non-hyperbolique.
e) S'il existe $iet j$ tels que $\Re\lambda_i$<0 et $\Re\lambda_{\text{j}}$>0, le point fixe est un seul point selle.
f) Si toutes les valeurs propres de $D\mathcal{F}$(0) sont réelles et de même signe, le point fixe est un nœud [8].

## 1.6 Bifurcation :

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique. Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système tels que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation. Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation. Il existe plusieurs types de bifurcation [1] :

### 1.6.1 Bifurcation nœud–col :

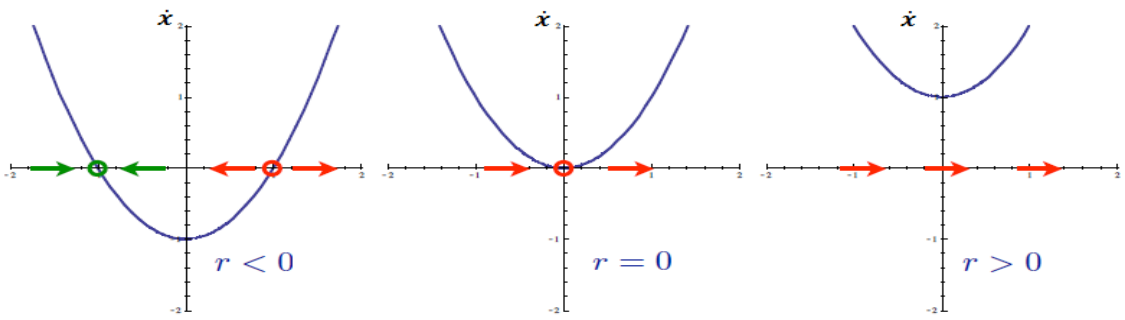
C'est la bifurcation associée à l'équation du premier ordre

$$\dot{x}=r+x^2 \tag{1.12}$$

Avec r le paramètre de contrôle.

Quand r<0, on aura deux points fixes, un point stable et l'autre instable. A chaque fois que r tend vers 0, la parabole se déplace vers le haut et les deux points fixes se déplacent l'un vers l'autre jusqu'à ce qu'ils se rejoignent en un point fixe demi stable. Ce dernier disparaît dès que r> 0.

La figure 1.5 illustre la bifurcation nœud-col.




**Point fixe stable et instable**

**Figure1.5 :** Bifurcation nœud-col.

### 1.6.2 Bifurcation Trans-critique :

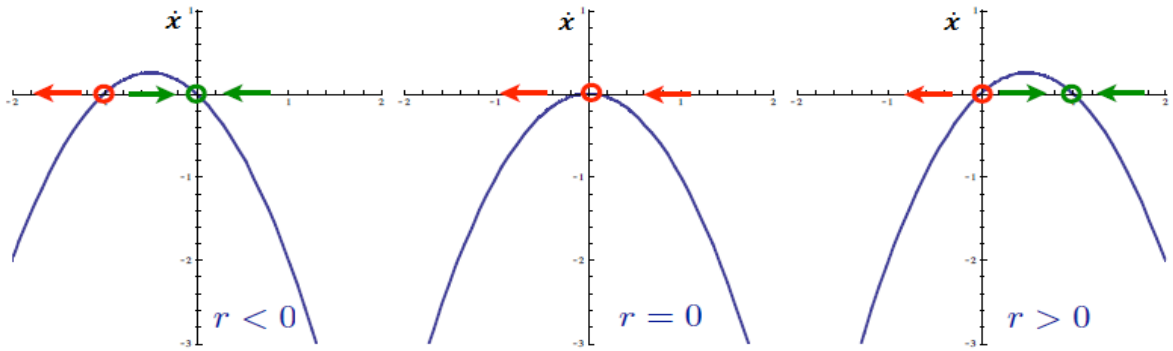
C'est la bifurcation associée à l'équation du premier ordre :

$$\dot{x}=rx-x^2 \qquad (1.13)$$

Il y a deux points fixes $\overline{x}$=0 et $\overline{x}$=r.

- Pour r <0, le point fixe $\overline{x}$=0 est donc stable tandis que le point fixe $\overline{x}$=r est instable.
- Pour r=0, il y a qu'un seul point fixe demi stable $\overline{x}$=0 (même raisonnement que celui de la bifurcation noud-col). Il y a donc échange de stabilité en r=0.
- Pour r>0, le point fixe $\overline{x}$=0 est donc instable tandis que le point fixe $\overline{x}$=r est stable.

La figure 1.6 illustre la bifurcation trans-critique.




**Point fixe stable et instable**

**Figure1.6 :** Bifurcation Trans-critique.

### 1.6.3 Bifurcation fourche :

C'est la bifurcation associée à l'équation du premier ordre :

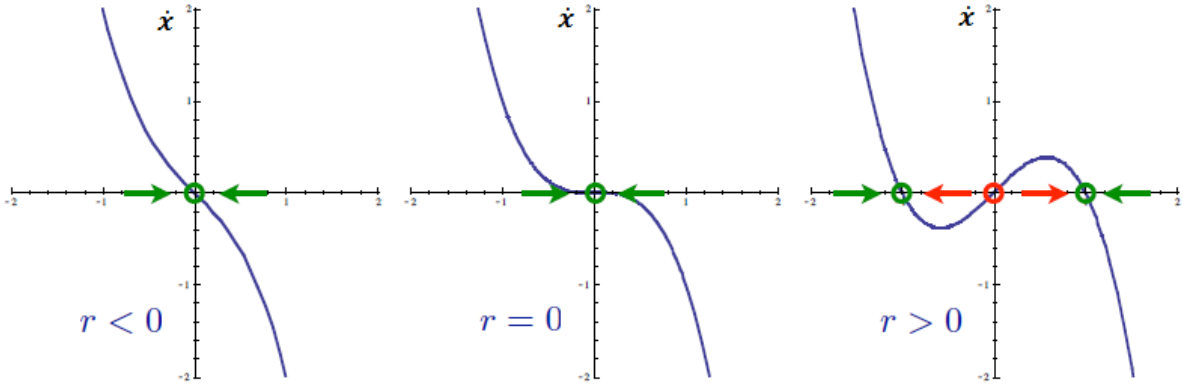
$$\dot{x} = rx - x^3 \qquad (1.14)$$

Il y a trois points fixes : $\overline{x} = \pm\sqrt{r}$ et $\overline{x}$=0.

- Pour r<0, il y a un seul point fixe stable $\overline{x}$=0.
- Pour r=0, il y a qu'un seul point fixe demi stable$\overline{x}$=0 (même raisonnement que celui de la bifurcation nœud-col), il y a donc ralentissement critique en r=0.

- Pour r>0, il y a trois points fixes. Les deux points fixes $\bar{x} = \pm\sqrt{r}$sont stables tandis que le point fixe $\bar{x} = 0$ est instable.

La figure 1.7 illustre la bifurcation fourche




**Point fixe stable et instable**

**Figure 1.7** : Bifurcation fourche.

### 1.6.4 Bifurcation de Hopf :

C'est la bifurcation associée à l'équation dans le plan complexe :

$$z'(t) = \mathcal{F}(z(t)) = (\mu + i\omega)z(t) - |z|^2 z(t) \qquad (1.15)$$

Pour étudier cette équation, on écrit la variable z sous la forme $z(t) = x(t)e^{i\theta(t)}$.

L'équation s'exprime sous forme d'un système :

$$x' = rx - x^3 \qquad (1.16)$$

$$\theta' = \omega \qquad (1.17)$$

La première équation n'est autre qu'une bifurcation fourche de paramètre de contrôle$\mu$.

La figure 1.8 représente le diagramme de bifurcation de Hopf

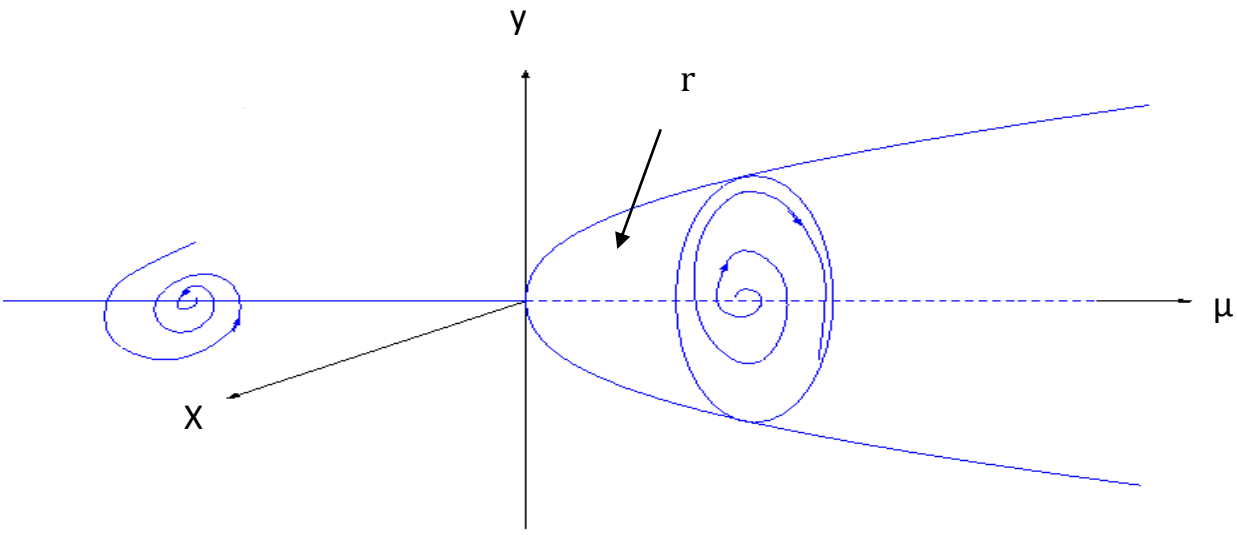



**Figure 1.8** : Diagramme de bifurcation de Hopf.

Nous partons d'un système où le paramètre $r$est négatif. Le système possède un point d'équilibre stable qui correspond ici à un point puits : les trajectoires s'enroulent en spirale vers l'origine. Lorsque $r$=0, ce point d'équilibre perd sa stabilité, puis lorsque $r$>0, il se forme alors une trajectoire périodique stable ou cycle limite.
La bifurcation de Hopf correspond à une instabilité oscillatoire.

## 1.7 Section de Poincaré :

Faire une section de Poincaré revient à couper la trajectoire dans l'espace des phases, afin d'étudier les intersections de cette trajectoire avec, par exemple en dimension trois, un plan. On passe alors d'un système dynamique à temps continu à un système dynamique à temps discret. Les mathématiciens ont bien évidemment démontré que les propriétés du système sont conservées après la réalisation d'une section de Poincaré judicieusement choisie. Dans un premier temps nous allons voir quelles sont les différentes sections de Poincaré utilisées en général [2].

- L'application ponctuelle T dans $\mathcal{R}^2$ définie ainsi $M_{\mathcal{K}+1}$=T ($M_{\mathcal{K}}$) où $M_{\mathcal{K}}$ est le k$^{ième}$ point d'intersection de la trajectoire avec le plan de coupe.
- L'application g dite de premier retour définie ainsi $x_{\mathcal{K}+1}$=($x_{\mathcal{K}}$) où $x_{\mathcal{K}}$ est l'abscisse du k$^{nième}$ point d'intersection de la trajectoire avec les plans de coupe.

❖ **Les cas typiques observés :**

- la solution périodique dans $\mathcal{R}^n$ (c'est un cycle limite) : la section de Poincaré est un point.
- la solution est quasi-périodique à deux fréquences $f_1$ et $f_2$. On distingue deux cas selon que le rapport $r=f_1/f_2$ soit rationnel ou pas :
  - ✓ **si r n'est pas rationnel :** la section de Poincaré est une courbe fermée.
  - ✓ **si r est rationnel :** la section de Poincaré se compose de quelque points.
- la solution est apériodique : la section de Poincaré est un nuage de points.

La figure 1.9montre un exemple d'une section de Poincaré du système de Lorenz.

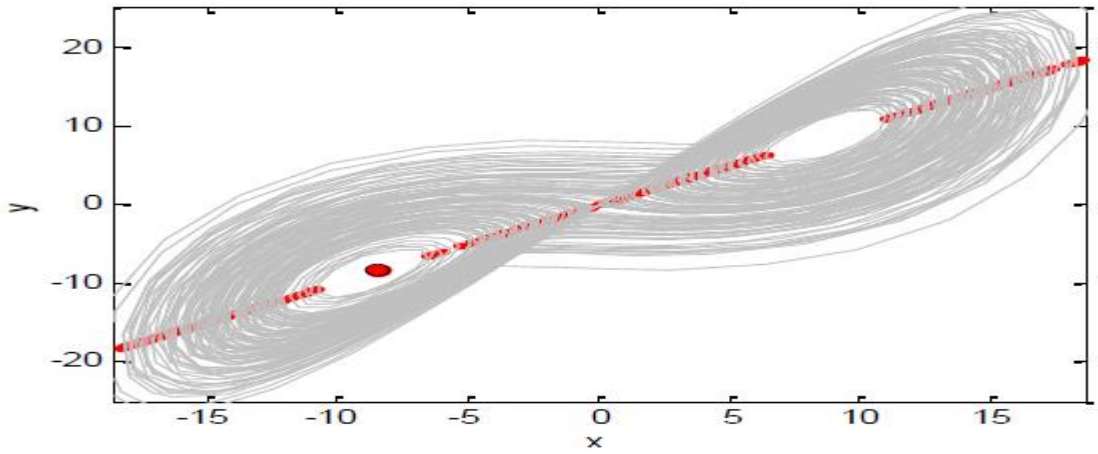



**Figure 1.9 :** Section de Poincaré du système de Lorenz [8].

❖ Le graphe de la section Poincaré peut être :

- **un unique point:** le système est périodique.
- **un petit nombre de points:** le système est périodique.
- **une courbe fermée:** le système est quasi-périodique.
- **un nuage de points:** le système est chaotique.

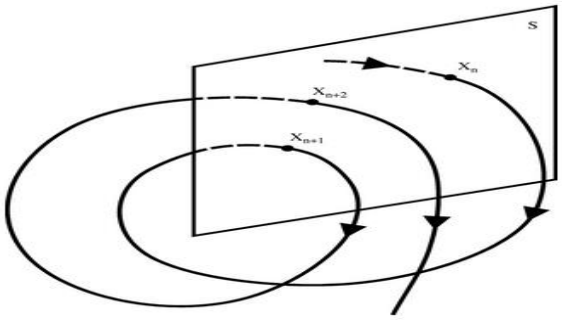



**Figure 1.10 :** Principe de la section Poincaré [9].

## 1.8 Les exposants de Lyapunov :

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaye si possible de mesurer sinon d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches**.**

- **Les exposants de Lyapunov pour des attracteurs non chaotiques :**

Pour un attracteur non chaotique, les exposants de Lyaponov sont tous négatifs ou nuls: $\lambda_{\mathcal{K}} \leq 0 \forall t$, $\mathcal{K}$ et leur somme est négative :$\sum_{k=1}^{n} \lambda_k$ <0. Les attracteurs non chaotiques sont classés en quatre catégories :

Point d'équilibre asymptotiquement stable : $\lambda\kappa < 0$ pour $\kappa$=1,…,n.

- Cycle limite stable : $\lambda_1 1 = 0$ et $\lambda\kappa < 0$ pour k= 2,…,n.
- Tore d'ordre 2 asymptotiquement stable : $\lambda_1 = 0$, $\lambda_2 2 = 0$ et $\lambda\kappa < 0$ pour k =3,…, n.
- Tore d'ordre K asymptotiquement stable : $\lambda_1 1 = \ldots \lambda_\kappa = 0$, $\lambda_2 2 = 0$ et $\lambda_\kappa k < 0$ pour k = k + 1,…, n.

- **Les exposants de Lyapunov pour un attracteur étrange (systèmes chaotiques) :**

Une des particularités du chaos est son extrême sensibilité aux conditions initiales. Un attracteur étrange possèdera toujours au moins un exposant de Lyapunov positif avec la propriété$\sum_{k=1}^{n} \lambda_k$ <0. De plus, pour un attracteur étrange, un des exposants de Lyapunov est toujours nul. Cela signifie que pour respecter la condition $\sum_{k=1}^{n} \lambda_k$<0, un

attracteur étrange doit avoir au minimum trois exposants de Lyapunov. Donc, un système continu dans le temps doit être au moins de dimension trois pour produire du chaos.

La figure 1.11 représente les exposants de Lyapunov de l'attracteur étrange de Lorenz :

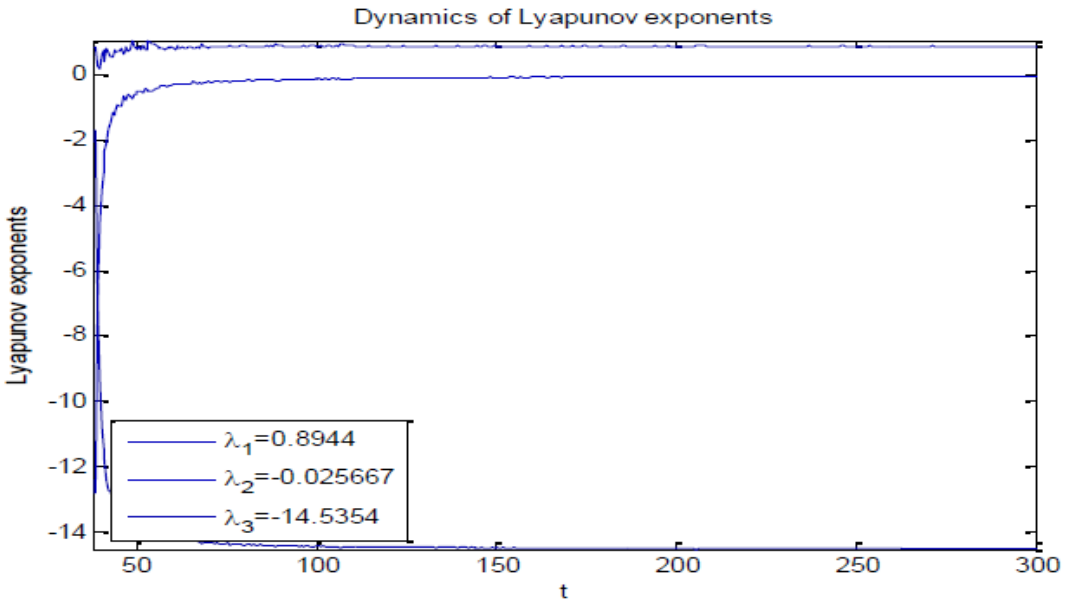



**Figure1.11 :** La dynamique des exposants de Lyapunov.

## 1.9 Les attracteurs étranges :

Dans la représentation des systèmes chaotiques, les attracteurs sont des courbes plus complexes qui présentent une symétrie interne: si l'on pratique un "zoom" avant ou arrière sur l'attracteur, on y retrouve la même forme, la même structure. À chaque échelle, il est semblable à lui-même. Les attracteurs sont des courbes fractales rendues célèbres par le mathématicien Benoît Mandelbrot. Le désordre est dans le système, mais l'ordre fractal, en revanche, apparaît dans ses représentations géométriques. Le chaos déterministe est caractérisé par ce type d'attracteurs, que les mathématiciens appellent attracteurs étranges, voici quelques exemples [14] :

### 1.9.1 Attracteur de Lorenz :

L'attracteur de Lorenz tient son nom du météorologue Edward Lorenz qui l'a étudié le premier. C'est une simplification à l'extrême d'équations régissant les mouvements

atmosphériques. Lorenz les a étudiées afin de mettre en évidence sur un système simple la sensibilité aux conditions initiales qu'il avait observé. Les équations de ce système sont les suivantes :

$$\begin{aligned} \frac{dx}{dt} &= a(y - x) \\ \frac{dy}{dt} &= \mathrm{b}x - \mathrm{y} - x\mathrm{z} \\ \frac{dz}{dt} &= x\mathrm{y} - \mathrm{cz} \end{aligned} \qquad (1.18)$$

On prendra : a= 10, b = 28 et c = 8/3.

La figure 1.12 représente l'attracteur étrange de Lorenz

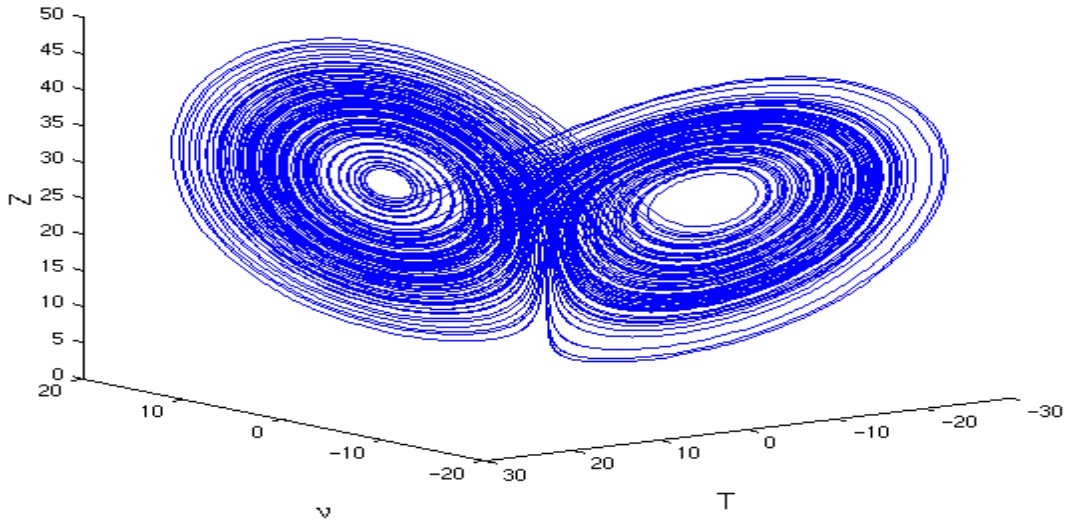



**Figure 1.12 :** Attracteur étrange de Lorenz [8].

### 1.9.2 Attracteur de Rössler:

Proposé par l'Allemand Otto Rössler en 1974, l'attracteur de Rössler ne provient pas de l'étude d'un système physique, du moins pas directement. Il résulte d'un effort de simplification pour étudier plus facilement la "chute" d'une trajectoire dans un bassin d'attraction.

Les équations de ce système sont les suivantes :

$$\frac{dx}{dt} = -y - z$$
$$\frac{dy}{dt} = x + ay \qquad (1.19)$$
$$\frac{dz}{dt} = b + xz - cz$$

On prendra : $a = 0.398$, $b = 2$ et $c = 4$.

La figure 1.13 représente l'attracteur étrange de Rössler [8] :

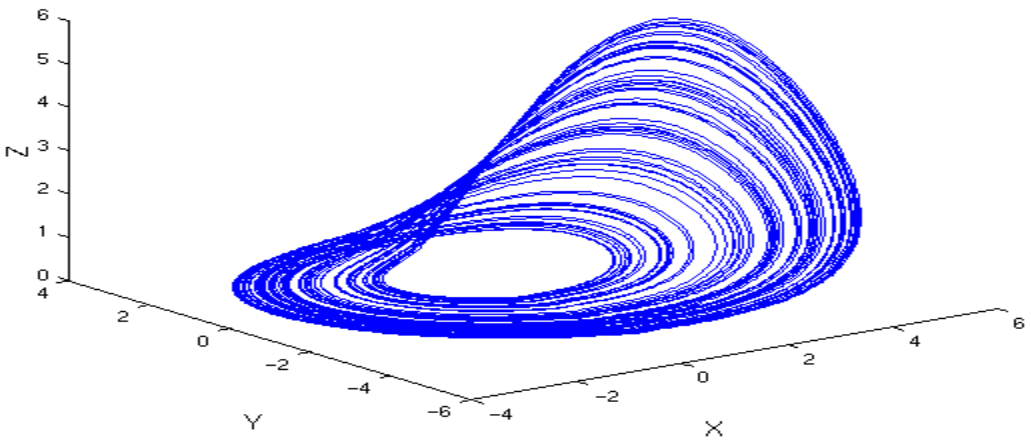



**Figure 1.13 :** Attracteur étrange de Rössler[8].

### 1.9.3 Attracteur de Chua :

Proposé par le professeur chinois LeonOng Chua en 1993, cet attracteur provient de l'étude de l'oscillateur chaotique de Chua. Les équations de ce système sont les suivantes :

$$\frac{dx}{dt} = \alpha^{*}(y - x - c^{*}x)$$
$$\frac{dy}{dt} = x - y + z \qquad (1.20)$$
$$\frac{dz}{dt} = -\beta^{*}y$$

On prendra : $\alpha$=10, $c$=−0.143, $\beta$=16.

La figure 1.14 représente l'attracteur étrange de Chua :

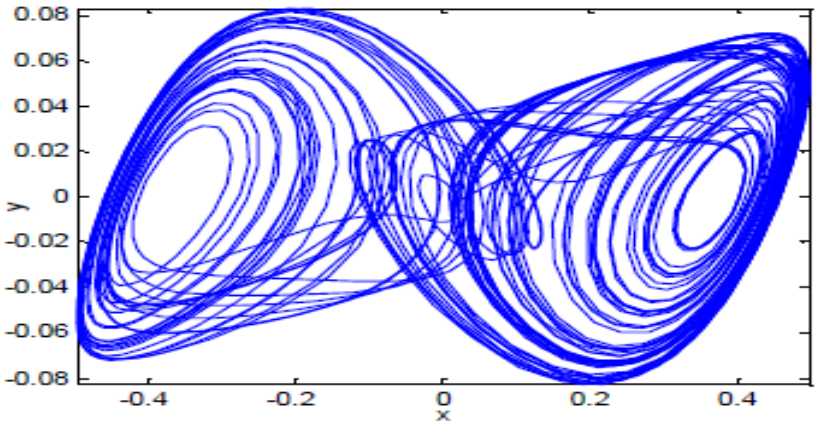



**Figure 1.14 :** Attracteur étrange de Chua [8].

## 1.10 Conclusion :

Dans ce chapitre, nous avons présenté les principales caractéristiques des systèmes dynamiques chaotiques.

Nous avons mis en relief certaines propriétés à savoir : les points d'équilibre, le diagramme de Bifurcation, le plan de phase, la section de Poincaré, les exposants de Lyapunov et l'attracteur étrange.

Ces notions nous seront très utiles pour l'analyse du système hyper chaotique de Qi dont le développement sera détaillé dans le prochain chapitre.

# Chapitre 2 Etude de l'oscillateur hyper chaotique de Qi

## 2.1 Introduction :

Les oscillations chaotiques sont déterministes mais fortement sensibles aux conditions initiales et présentent une allure « pseudo-aléatoire ». Ces propriétés peuvent être affinées pour simuler les caractéristiques d'un bruit blanc ou d'un autre signal « aléatoire », ce qui fait du chaos un phénomène très intéressant pour cacher des signaux d'informations afin de les transmettre d'une manière « sécurisée ».

Dans ce chapitre nous allons étudier le système hyper chaotique de Qi qui constitue l'élément essentiel de l'émetteur.

## 2.2 Description du système :

Le système hyper chaotique de Qi est donné par :

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) + x_2 x_3 \\ \dot{x}_2 &= b(x_1 + x_2) - x_1 x_3 \\ \dot{x}_3 &= -cx_3 - ex_4 + x_1 x_2 \\ \dot{x}_4 &= -dx_4 + fx_3 + x_1 x_2 \end{aligned} \tag{2.1}$$

Où $x_1, x_2, x_3, x_4$ sont des variables d'état, et $a, b, c, d, e, f$ sont des constantes réelles.

Pour $a = 50, b = 24, c = 13, d = 8, e = 33, f = 30,$ le système a un comportement chaotique.

## 2.3 Etude du système hyper chaotique de Qi :

### 2.3.1 Etude des points fixes :

On a un point fixe si :

$$\frac{dx}{dt} = f(x) = 0 \tag{2.2}$$

C'est-à-dire :

$$\begin{aligned} \dot{x}_1 &= a(x_2 - x_1) + x_2x_3 = 0 \\ \dot{x}_2 &= b(x_1 + x_2) - x_1x_3 = 0 \\ \dot{x}_3 &= -cx_3 - ex_4 + x_1x_2 = 0 \\ \dot{x}_4 &= -dx_4 + fx_3 + x_1x_2 = 0 \end{aligned} \tag{2.3}$$

On obtient alors une seule solution :$x_1 = x_2 = x_3 = x_4 = 0$.

Pour étudier la stabilité de ce point fixe, on détermine les valeurs propres de la matrice Jacobienne.

Pour le système de Qi, la matrice Jacobienne au point d'équilibre est donnée par :

$$D(0\,0\,0\,0) = \begin{bmatrix} -a & a & 0 & 0 \\ b & b & 0 & 0 \\ 0 & 0 & -c & -e \\ 0 & 0 & f & -d \end{bmatrix} \tag{2.4}$$

Les valeurs propres sont données par les solutions de l'équation :

$$D - \lambda I = 0 \tag{2.5}$$

Où $\lambda I$ est donnée par :

$$\lambda I = \begin{bmatrix} \lambda & 0 & 0 & 0 \\ 0 & \lambda & 0 & 0 \\ 0 & 0 & \lambda & 0 \\ 0 & 0 & 0 & \lambda \end{bmatrix} \quad (2.6)$$

Avec : $\lambda$ valeur propre de la matrice et $I$ la matrice identité.

L'équation caractéristique est donnée par : *det* (D ( 0 0 0 0 ) –λ$I$) = 0 , soit :

$$[ (-c-\lambda ) (-d-\lambda) + ef ] [ (-a-\lambda ) ( b-\lambda ) - ab ]=0 \quad (2.7)$$

La résolution de l'équation caractéristique nous donne les racines suivantes :

λ1= - 10.5 – 31.36 i , λ2= - 10.5 + 31.36 i , λ3= 37.685 , λ4= -63.68 .

On a quatre valeurs propres :

- Deux valeurs purement réelles dont l'une négative et l'autre positive.
- Deux valeurs complexes dont leurs parties réelles sont négatives et leurs parties imaginaires sont de différents signes (positifs, négatifs).

Donc on a un point fixe instable, Comme cela a été expliqué dans le premier chapitre.

### 2.3.2 Evolution du système de Qi en fonction du temps :

Nous avons utilisé MATLAB Simulink pour visualiser des différents signaux issus du système de Qi, tels que : les états $x_i$ en fonction du temps, les plans de phase et le tracé de l'attracteur chaotique en 3D.

Pour cela, on a simulé sous Matlab-Simulink, le système hyper chaotique de Qi à partir des équations (2.1).

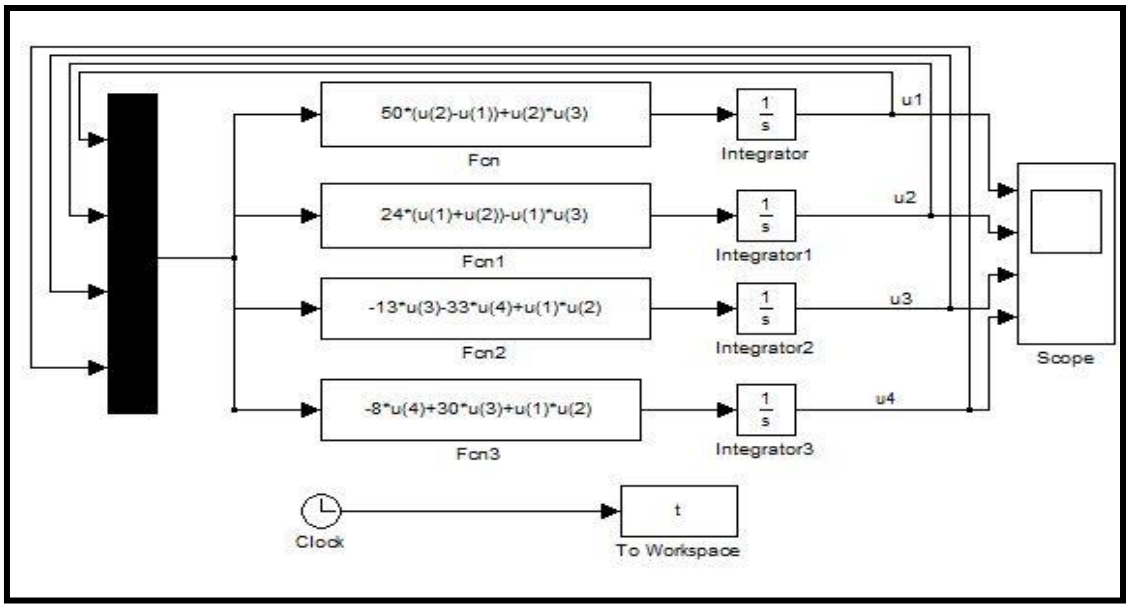



**Figure 2.1 :** Représentation du système de Qi sous MATLAB (Simulink).

Les figures de 2.2 à 2.6 représentent les courbes des états $x_1$ , $x_2$ , $x_3$ , $x_4$ en fonction du temps.

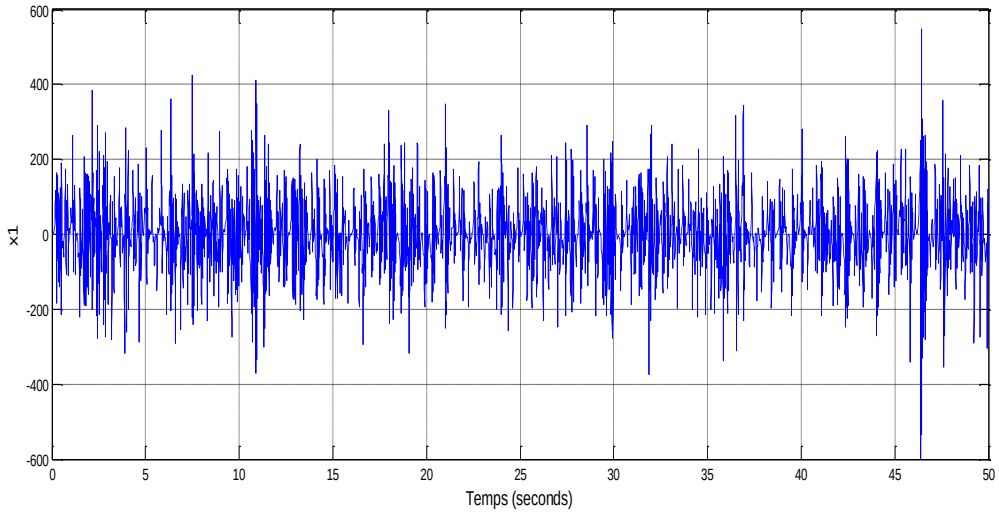



**Figure 2.2 :** L'état $x_1$ en fonction du temps t.

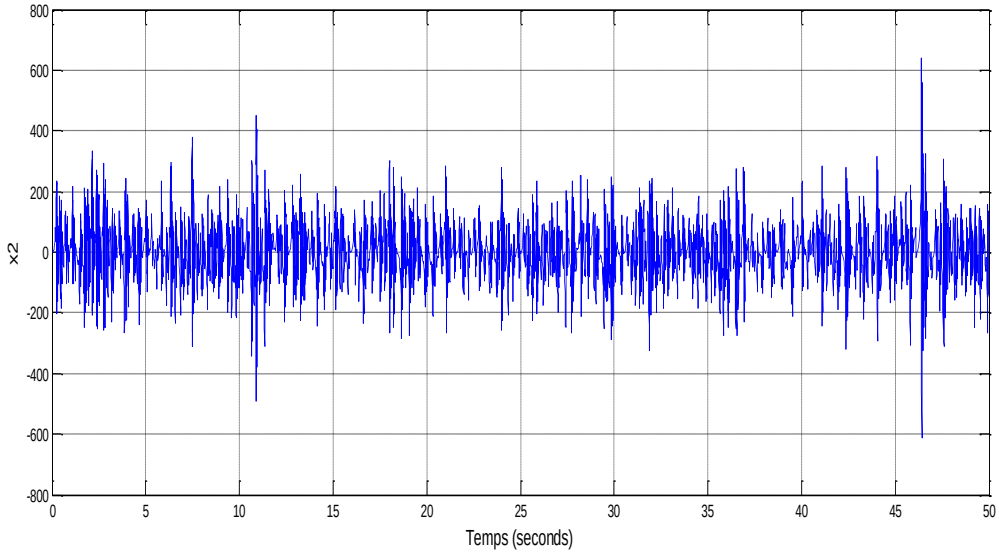



**Figure 2.3 :** L'état $x_2$ en fonction du temps t.

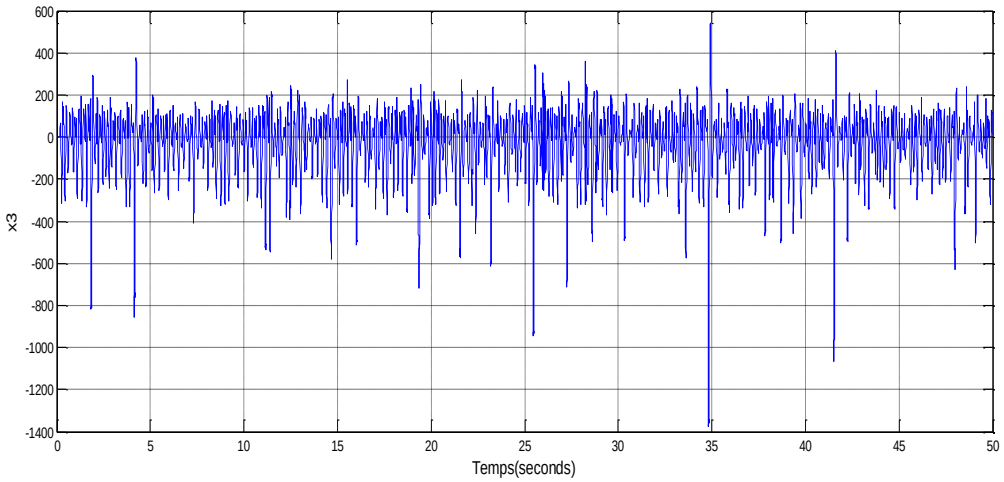



**Figure 2.4 :** L'état $x_3$ en fonction du temps t.

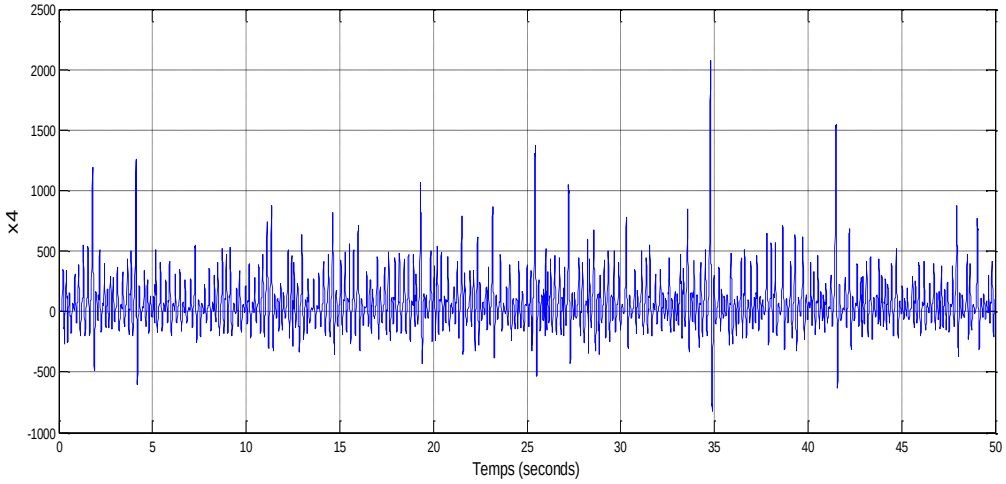



**Figure 2.5 :** L'état $x_4$ en fonction du temps t.

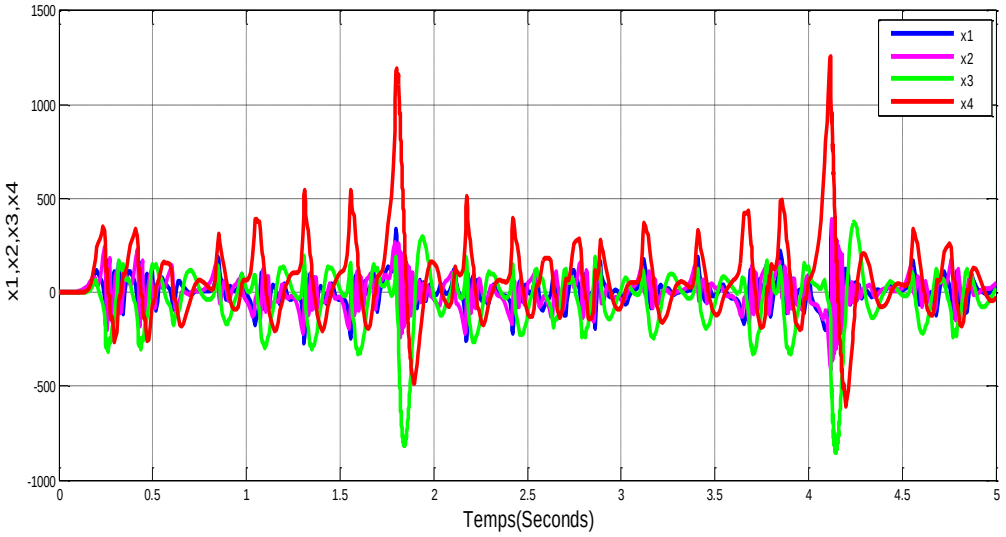



**Figure 2.6 :** Les états $x_1$ , $x_2$ , $x_3$ , $x_4$ en fonction du temps.

### 2.3.3 Sensibilité aux conditions initiales :

La figure 2.7 illustre une des propriétés essentielles du chaos, à savoir l'extrême sensibilité aux conditions initiales.

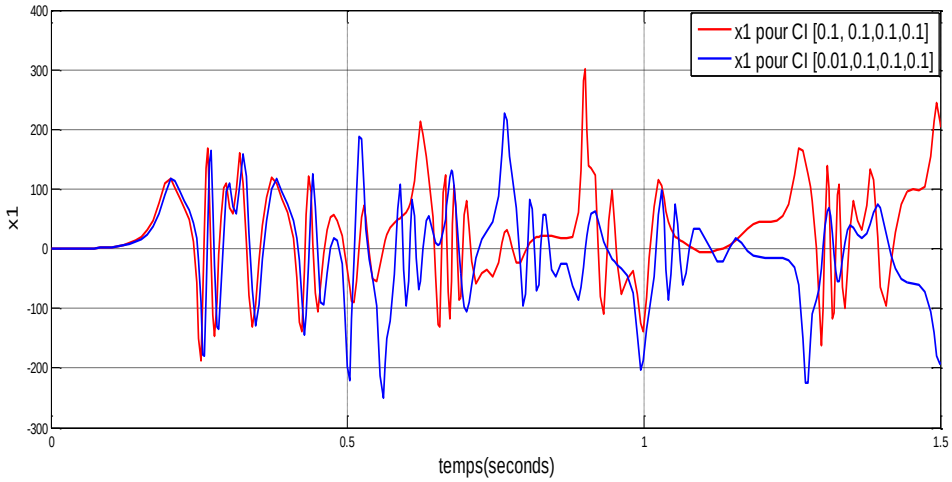



**Figure 2.7 :** Illustration de la propriété de sensibilité aux conditions initiales sur l'état x1.

### 2.3.4 Plan de phase :

Les figures 2.8 à 2.13 représentent les différents plans de phase du système hyper chaotique de Qi.

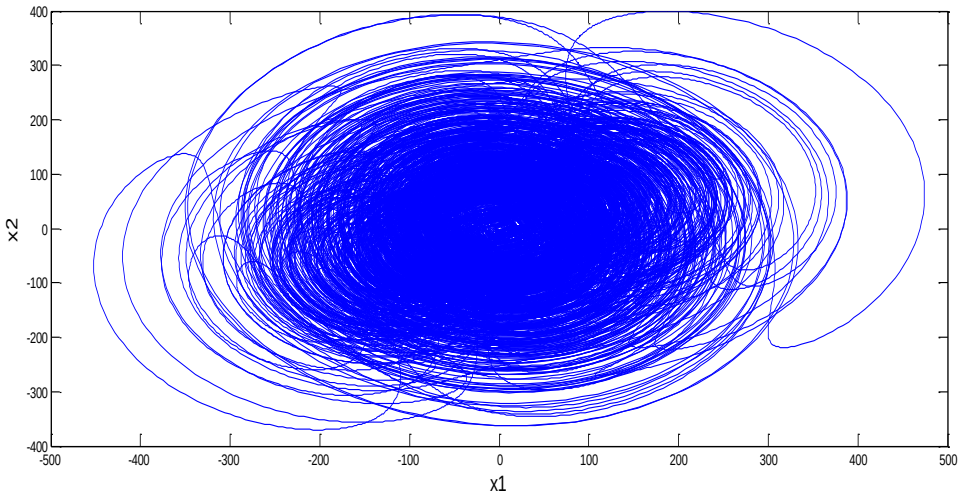



**Figure 2.8 :** Plan de phase $x_2$ en fonction de $x_1$ du système de Qi.

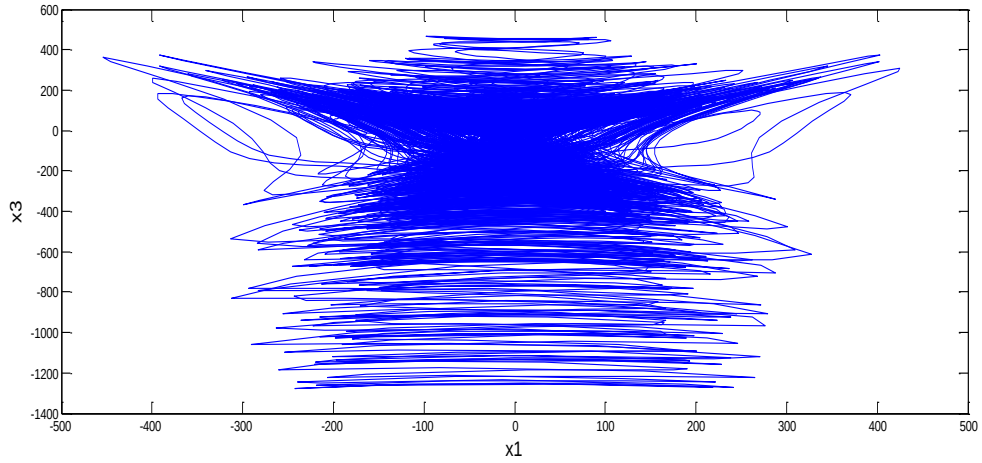



**Figure 2.9 :** Plan de phase $x_3$ en fonction de $x_1$ du système de Qi.

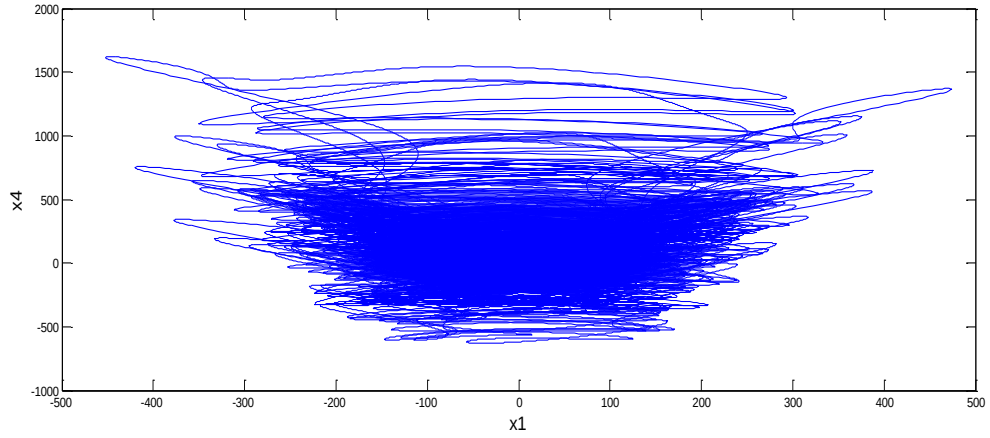



**Figure 2.10 :** Plan de phase $x_4$ en fonction de $x_1$ du système de Qi.

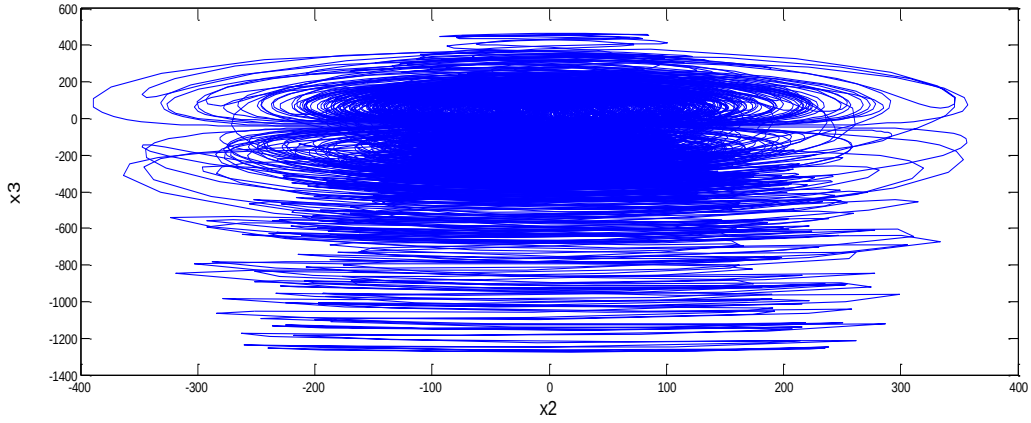



**Figure 2.11:** Plan de phase $x_3$ en fonction de $x_2$ du système de Qi.

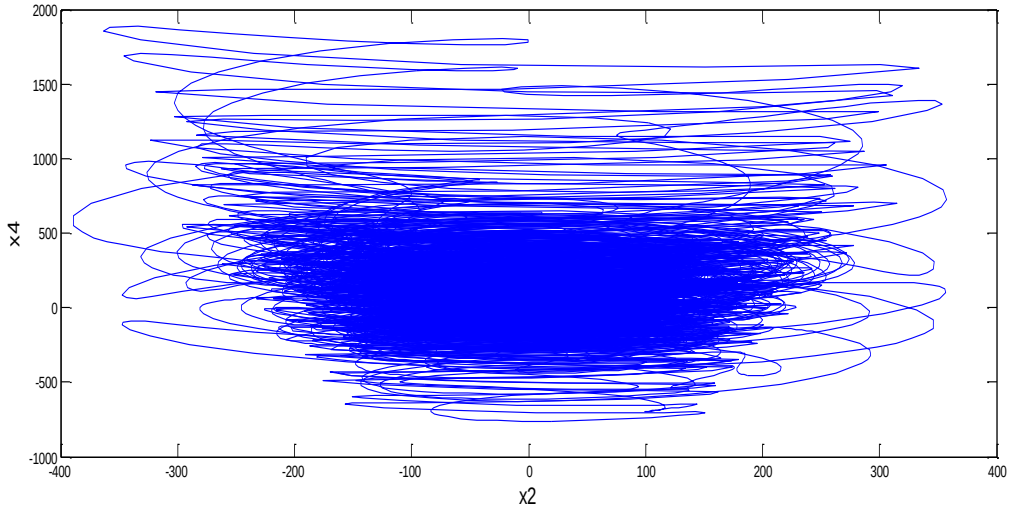



**Figure 2.12 :** Plan de phase $x_4$ en fonction de $x_2$ du système de Qi.

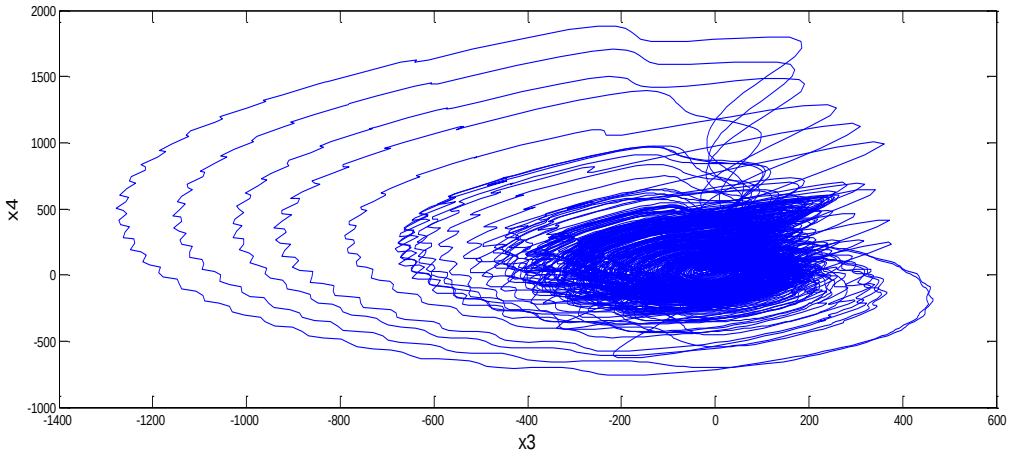



**Figure 2.13:** Plan de phase $x_4$ en fonction de $x_3$ du système de Qi.

### 2.3.5 Attracteur étrange (chaotique) :

Les figures 2.14 à 2.17 représentent les différents attracteurs étranges du système hyper chaotique de Qi.

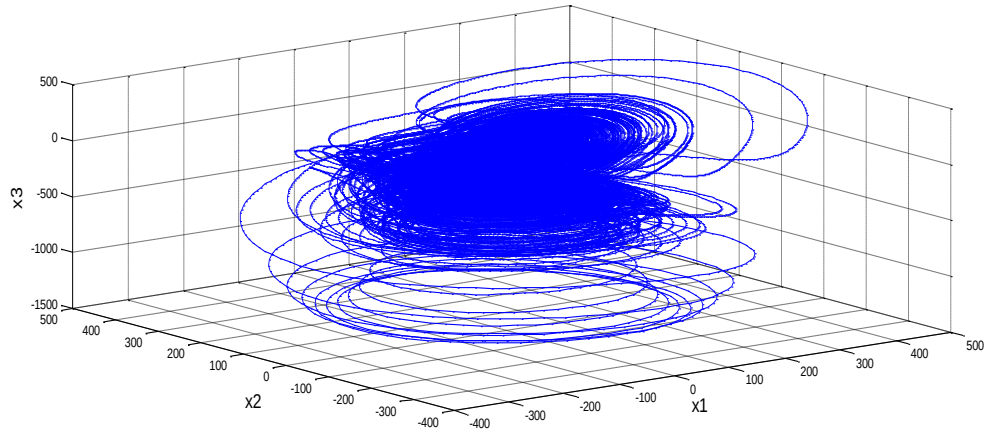



**Figure 2.14 :** Attracteur étrange de Qi en fonction de$x_1$ , $x_2$ $et$ $x_3$.

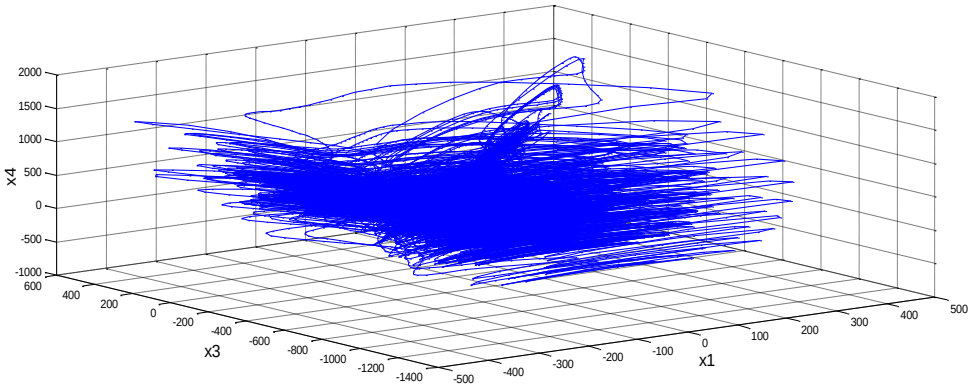



**Figure 2.15:** Attracteur étrange de Qi en fonction de $x_1$ , $x_3$ $et$ $x_4$.

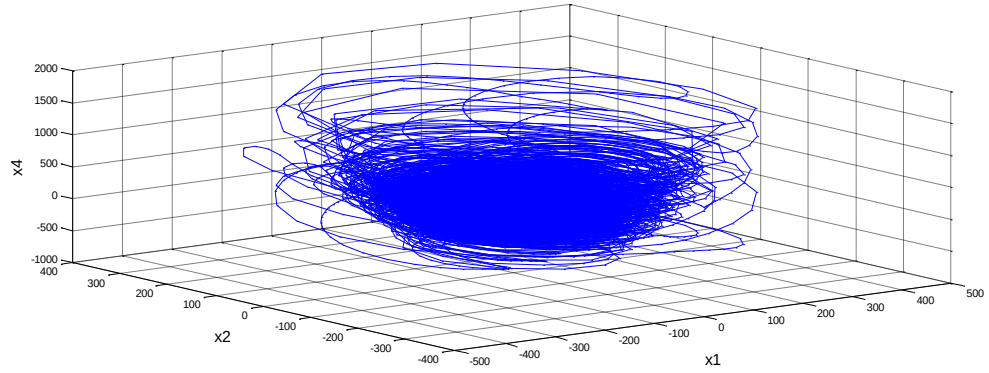



**Figure 2.16 :** Attracteur étrange de Qi en fonction de $x_1$ , $x_2$ $et$ $x_4$.

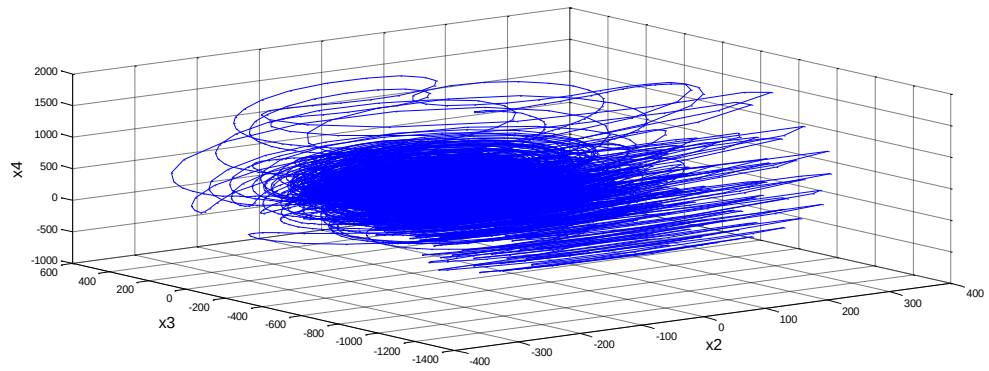



**Figure 2.17:** Attracteur étrange de Qi en fonction de $x_2$ , $x_3$ $et$ $x_4$.

### 2.3.6 Densité de probabilité :

L'histogramme de la densité de probabilité peut statistiquement montrer les propriétés stochastiques d'un signal généré par le système de Qi. Et comme le système de Qi est très semblable au bruit blanc gaussien donc il est assez aléatoire à utiliser dans le chiffrement [17].

La figure suivante représente la densité de probabilité du système de Qi.

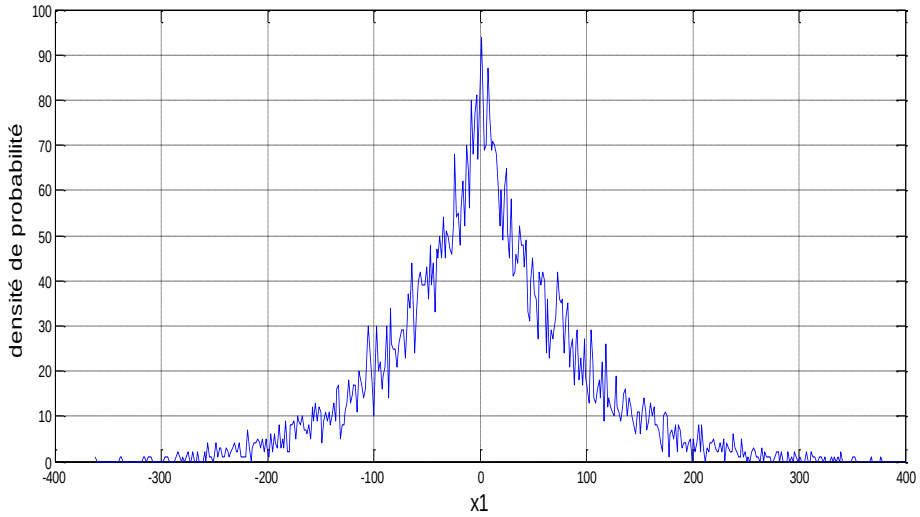



**Figure 2.18 :** La densité de probabilité du système de Qi.

### 2.3.7 Exposants de Lyapunov :

Nous allons utiliser l'outil MATDS qui travaille sous MATLAB, et qui nous permet d'étudier des systèmes dynamiques.

Tout d'abord, on va commencer par la représentation de l'outil MATDS :

- Lorsqu'on lance le MATDS la fenêtre suivante va apparaitre :

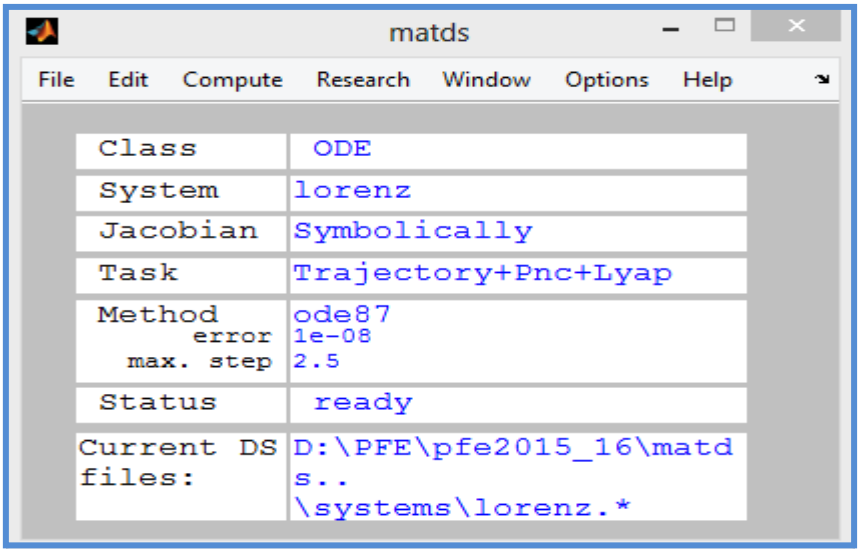



**Figure 2.19 :** L'interface de l'outil MATDS.

- On va créer par la suite notre système hyper chaotique de Qi en faisant entrer les équations (2.1) et les paramètres suivants :$a = 50, b = 24, c = 13, d = 8, e = 33, f = 30.$

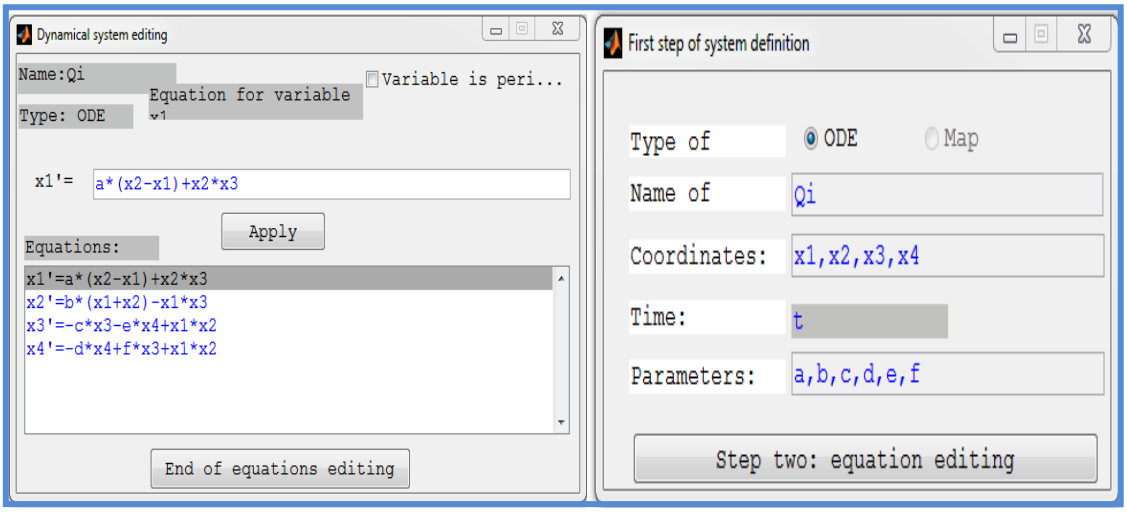



**Figure 2.20 :** Création du système de Qi en MATDS.

Le MATDS nous permet de visualiser les exposants de Lyapunov et la section de Poincaré.

On sait que pour un attracteur étrange (hyper chaotique), il faut que la somme des exposants de Lyapunov soit négative et qu'au moins deux de ses exposants soient positifs. Pour notre système hyper chaotique de Qi, les exposants de Lyapunov sont représentés sur la figure suivante.

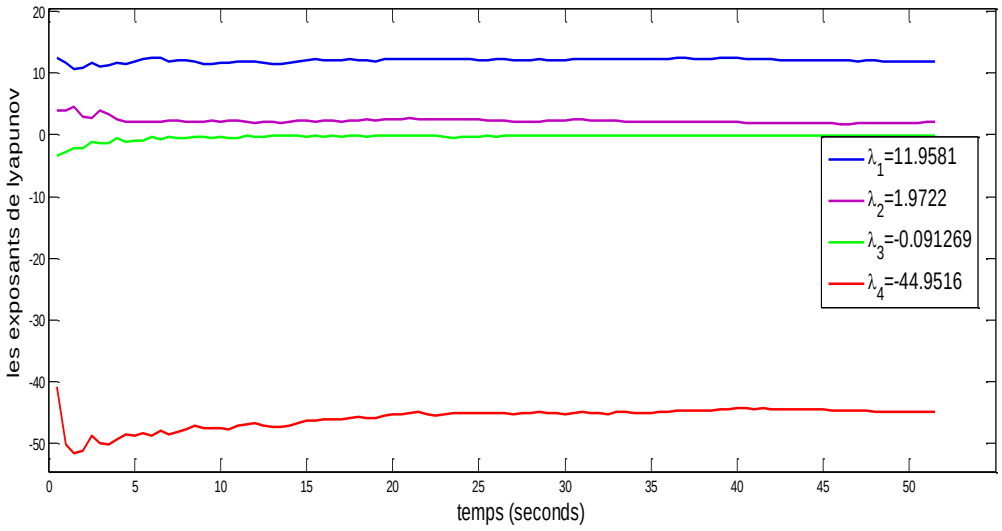


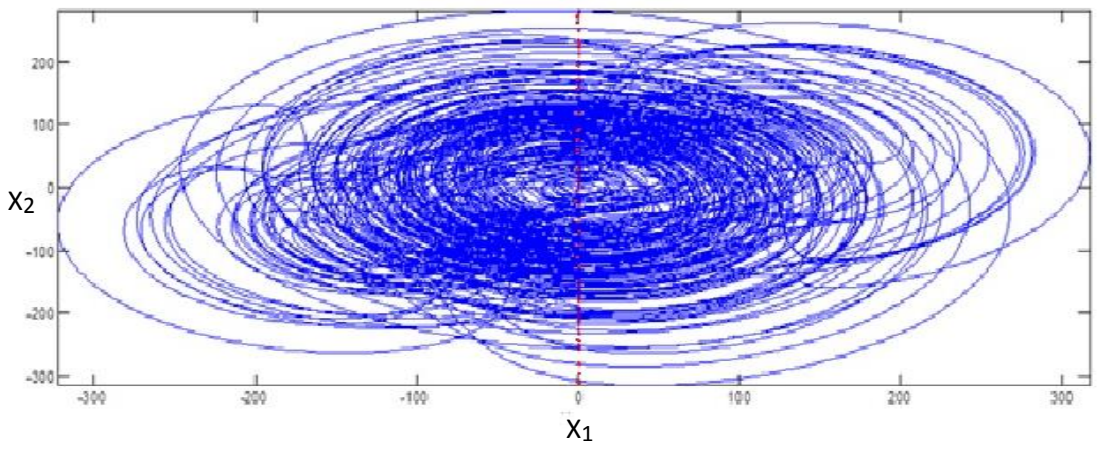

**Figure 2.21 :** La dynamique des exposants de Lyapunov du système de Qi.

Notre système hyper chaotique de Qi a quatre équations différentielles donc on obtient quatre exposants de Lyapunov :

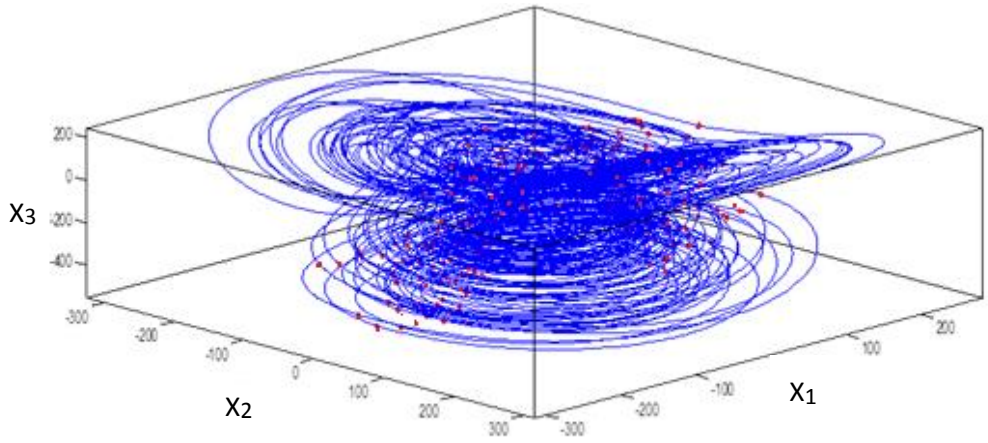
$\lambda_1$= 11.9581 , $\lambda_2$= 1.9722 , $\lambda_3$=-0.091269 , $\lambda_4$= -44.9516.

### 2.3.8 Section de Poincaré :

Dans le premier chapitre nous avons définit la section de Poincaré qui permet de différencier un système chaotique d'un système périodique. Pour cela, on détermine par exemple l'intersection du plan d'équation $x_1$=0 et de l'attracteur étrange.



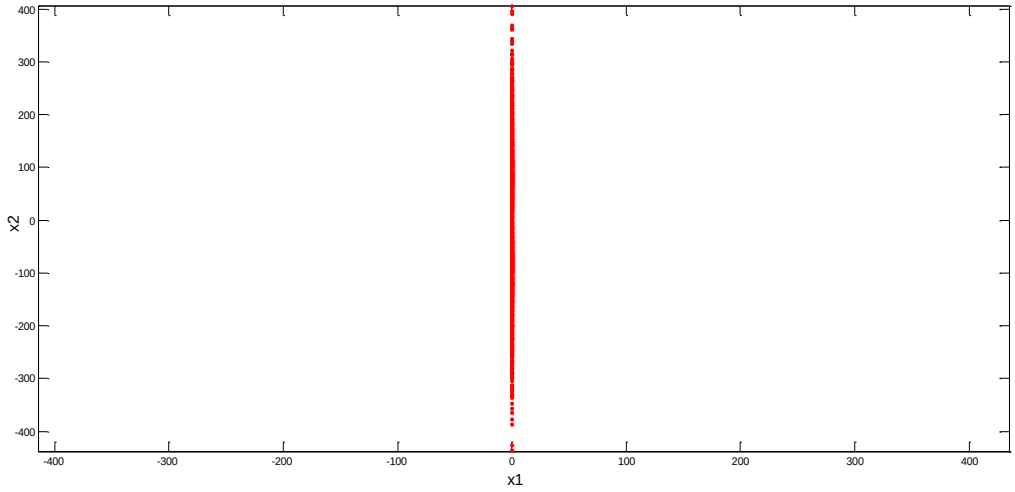

**a) La section de Poincaré dans le plan de phase en 2D**



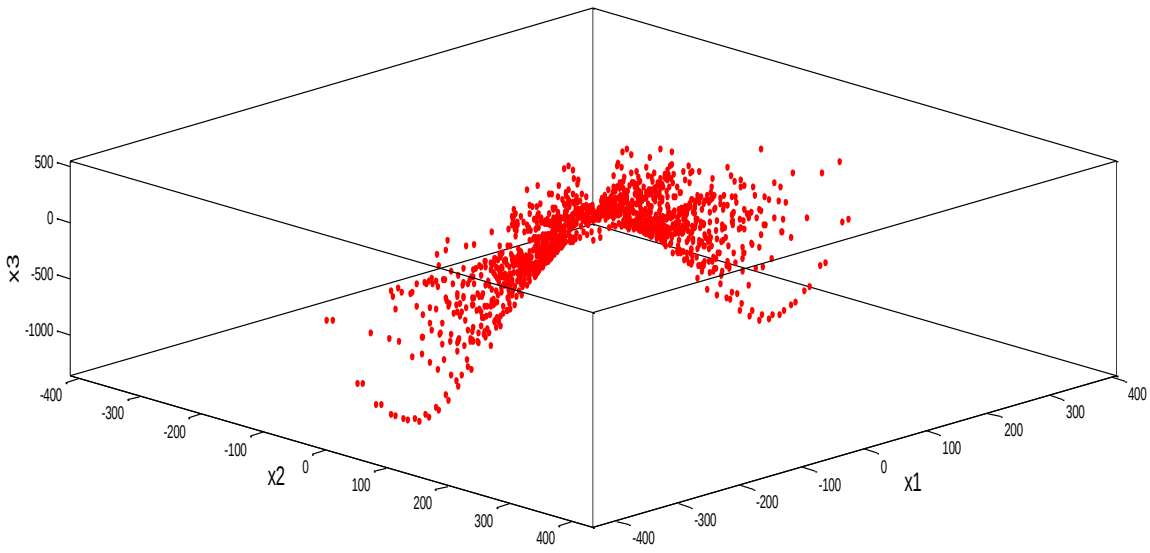

**b) La section de Poincaré sur l'attracteur étrange en 3D**

**Figure 2.22 :** Représentation de la section de Poincaré dans a) le plan de phase et b) l'attracteur étrange du système de Qi.

On a supprimé les trajectoires pour n'obtenir que la section de Poincaré représentée sur la figure 2.23.




**a) La section de Poincaré du système de Qi en 2D**




**b) La section de Poincaré du système de Qi en 3D**

**Figure 2.23** : Section de Poincaré du système de Qi.

### 2.3.9 Diagramme de bifurcation :

Pour tracer le diagramme de bifurcation, un programme sous MATLAB a été écrit et les résultats obtenus sont représentés sur la figure 2.24 .Le paramètre variable utilisé est b.

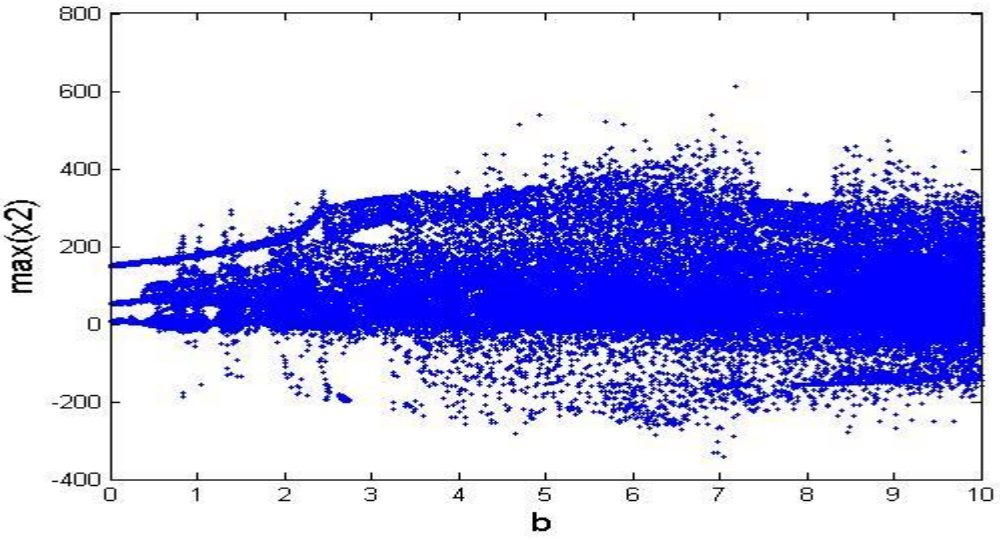



**Figure 2.24 :** Diagramme de bifurcation de x2 en fonction de b.

On remarque par exemple que pour b=0.102, le système présente un caractère périodique comme le montre les figures 2.25 et 2.26.

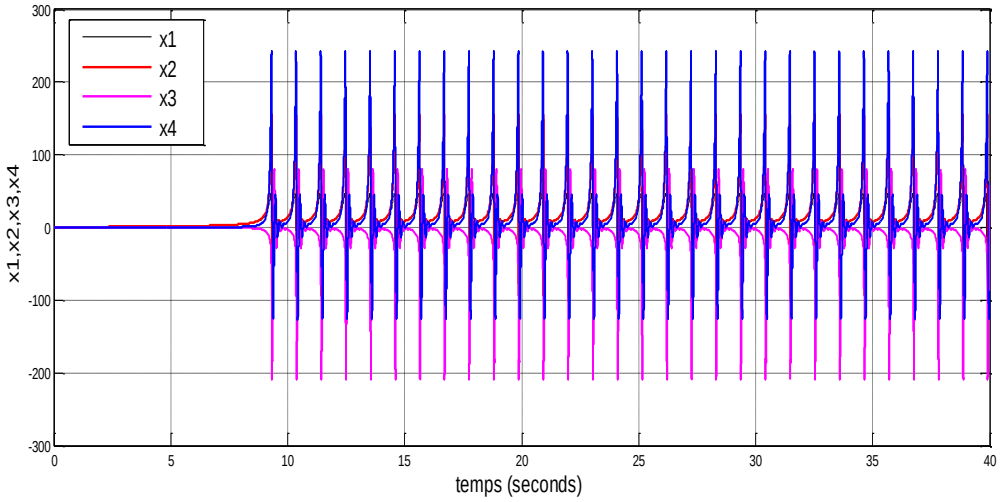



**Figure 2.25 :** Les états $x_1$ , $x_2$ , $x_3$ , $x_4$ sont périodiques lorsque b=0.102.

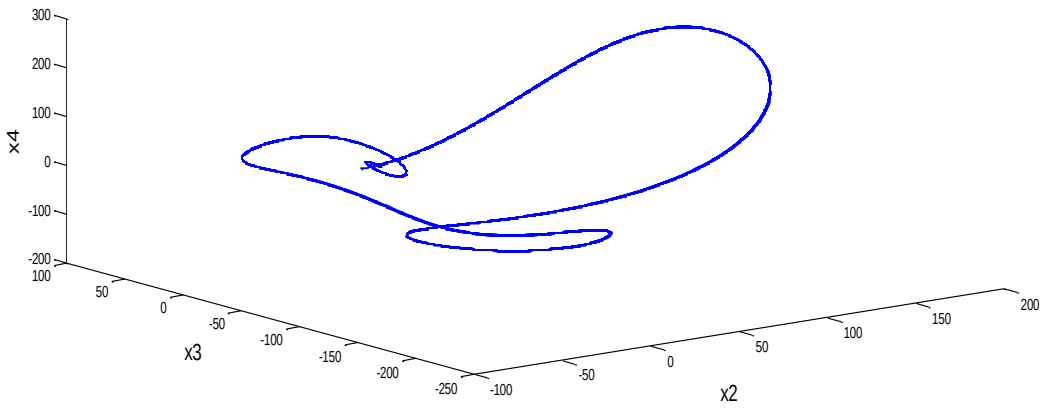



**Figure 2.26 :** Attracteur étrange pour b= 0.102.

## 2.4 Conclusion :

Dans ce chapitre, les principales caractéristiques et propriétés de l'oscillateur hyper chaotique de Qi ont été développées en mettant en évidence son caractère hyper chaotique .Il sera ainsi utilisé aussi bien au niveau de l'émetteur que du récepteur pour la transmission sécurisée par modulation CSK (Chaos Shift Keying) et dont l'analyse détaillée sera développée dans le prochain chapitre.

# Chapitre 3 Cryptage par modulation CSK (Chaos Shift Keying)

## 3.1 Introduction :

Cacher des informations particulières à certaines personnes a toujours été l'un des intérêts principaux de l'Homme. On a ainsi cherché à établir des techniques dites de « cryptage » afin de rendre ces informations incompréhensibles à ceux qui n'ont pas accès à une « clé » secrète [12].

Ainsi la découverte par Pecora et Carroll que deux systèmes chaotiques peuvent être synchronisés, a déclenché un certain intérêt pour le développement des systèmes de communication sécurisés basés sur le chaos durant les trois décennies passées [13].

L'idée de base est de brouiller un message adéquatement avec le chaos au niveau de l'émetteur, afin de le dissimuler des intrus, avant de le transmettre à sa destination qui sera la seule capable de le déchiffrer [13].

Cependant, les difficultés issues de la synchronisation en temps continu ont mené certains chercheurs à mettre au point d'autres techniques de « synchronisation » comme la modulation par Chaos Shift Keying(CSK) [12].

## 3.2 Les classes de synchronisation :

Le concept de synchronisation repose sur le constat qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. Il est donc possible de construire une réplique identique à ce système et

d'essayer de le synchroniser de façon que les deux signaux chaotiques issus des deux exemplaires soient identiques.

Il existe deux classes de synchronisation suivant la manière avec laquelle les deux systèmes chaotiques sont couplés : unidirectionnelle et bidirectionnelle [8].

### 3.2.1 Synchronisation unidirectionnelle :

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément qui fonctionne dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur. La figure 3.1 représente le couplage unidirectionnel.

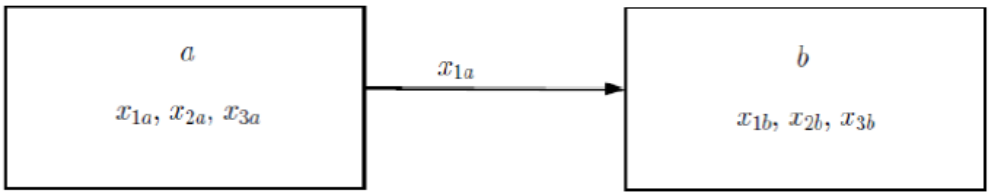



**Figure 3.1**: Couplage unidirectionnel [8].

### 3.2.2 Synchronisation bidirectionnelle :

Dans le cas d'une synchronisation bidirectionnelle figure 3.2, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance.

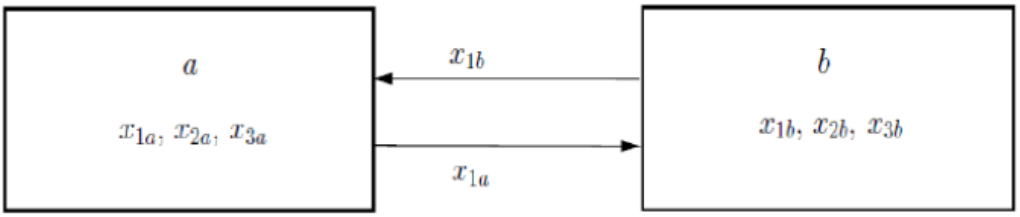



**Figure 3.2**: Couplage bidirectionnel [8].

## 3.3 Méthodes de synchronisation :

Plusieurs méthodes de synchronisation ont été proposées dans la littérature. Dans ce qui suit nous citerons quelques approches en expliquant leurs principes et avantages [8].

### 3.3.1 Synchronisation par boucle fermée :

La synchronisation des systèmes chaotiques par les méthodes en boucle ouverte implique une sensibilité aux variations paramétriques. Pour y remédier, de nouvelles techniques basées sur un bouclage par contre-réaction ont été proposées.

L'idée est d'appliquer une correction au système en fonction de l'erreur entre le signal transmis par le premier système et le signal régénéré par l'autre. Cette erreur est ainsi injectée en contre-réaction d'où l'appellation de l'approche.

Cette technique permet également la synchronisation entre des paires différentes de systèmes chaotiques. La figure 3.3 indique un schéma simplifié de la synchronisation par boucle fermée [8].

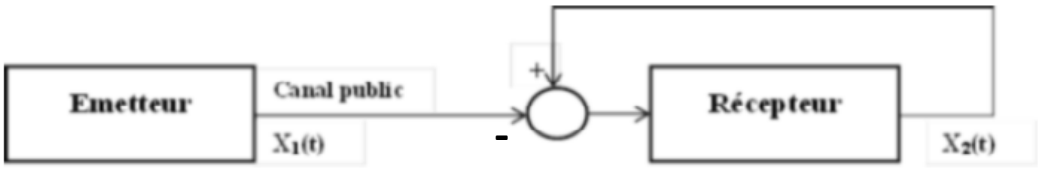



**Figure 3.3**: Synchronisation par boucle fermée [8].

### 3.3.2 Synchronisation généraliste :

Cette méthode est une généralisation du concept de synchronisation identique.

Les deux systèmes se synchronisent au sens généralisé, s'il existe une transformation M telle que

$$\lim_{t\to\infty} \| y(t) - M\,(x(t)) \| = 0 \qquad (3.1)$$

où : $x(t)$ est l'état du système émetteur et $y(t)$ est l'état du système récepteur.

Les conditions initiales ne sont pas tenues en compte dans ce cas. Si M est inversible, alors $M^{-1}(y)$ fournit une estimation de l'état x ; dans le cas contraire, il serait impossible de fournir une estimation de l'état x. Ceci présente alors un inconvénient majeur pour les techniques de communication utilisant l'état de l'émetteur pour décrypter le message transmis.

### 3.3.3 Synchronisation retardée :

Dans la synchronisation retardée, l'état du système esclave converge vers l'état décalé dans le temps du système maitre.

$$\lim_{t\to\infty} \| y(t) - x(t-\tau) \| = 0 \qquad (3.2)$$

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

### 3.3.4 Synchronisation projective :

Dans cette méthode, l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur. Soit $\alpha$ et $\tau$ tels que :

$$\lim_{t\to\infty} \| y(t) - \alpha x(t-\tau) \| = 0 \qquad (3.3)$$

Où $\alpha$ est le facteur d'échelle, x($t$) est l'état du système émetteur, y($t$) est l'état du système récepteur et $\tau$ est un retard positif.

Cette approche est utilisée pour des systèmes partiellement linéaires et permet de synchroniser à un facteur près les états qui ne peuvent être synchronisés.

### 3.3.5 Synchronisation impulsive :

Dans un schéma de transmission usuel, un des états du système dynamique est transmis afin de réaliser la synchronisation par le récepteur. Dans le but de réduire la redondance du signal transmis, la synchronisation impulsive a été proposée.

Le contrôle impulsif d'un système signifie qu'à des moments choisis, les états du système changent soudainement.

Dans ce schéma de synchronisation, on considère un système maître de la forme générale suivante :

$$\dot{x}(t)=f(x(t)) \tag{3.4}$$

On définit un signal impulsif qui consiste en une suite d'instants discrets auxquels un signal y(t) = Cx(t) est envoyé par le système maître au système esclave, dont les variables d'état subissent un saut et un changement d'état. La figure 3.4 représente le schéma synoptique de la synchronisation impulsive [8].

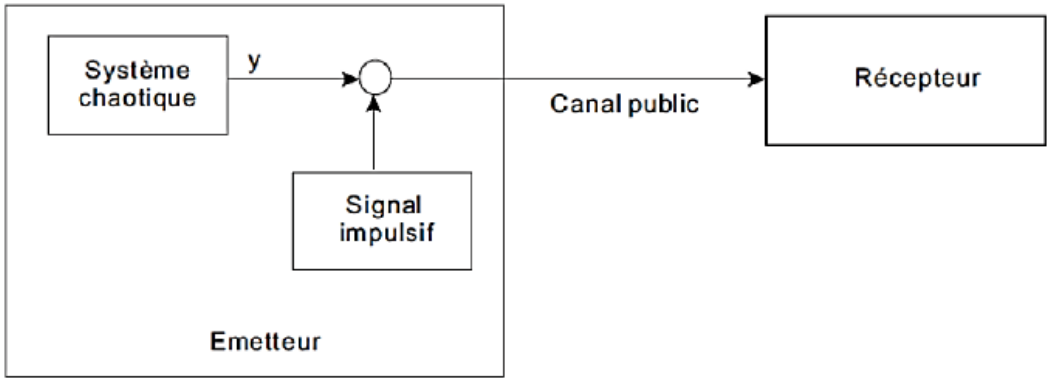



**Figure 3.4**: Synchronisation impulsive [8].

## 3.4 Techniques de cryptage par le chaos :

Les systèmes chaotiques constituent une classe particulière de systèmes non linéaires, il est donc possible de leur appliquer toutes les méthodes relatives aux systèmes non linéaires.

Un système de communication utilisant le chaos représente une application prometteuse de l'estimation d'état des systèmes non linéaires.

A partir d'un message contenant l'information, l'émetteur génère un signal qui est transmis au récepteur par l'intermédiaire du canal. Le récepteur reconstruit alors le message original grâce à une « clé » partagée avec l'émetteur [8].

Il existe plusieurs techniques qui peuvent servir comme moyen de masquage de l'information dans le chaos ; nous en décrivons ici quelques unes [1]:

### 3.4.1 Cryptage par addition :

Le principe de cette méthode est d'additionner directement notre signal informatif m(t) avec le signal x(t) de notre oscillateur chaotique de Qi et de le récupérer ensuite par synchronisation chaotique figure 3.5. Le même oscillateur est utilisé à la fois au niveau de l'émetteur et au niveau du récepteur, avec la différence que le récepteur est contrôlé par le signal reçu de l'émetteur pour obtenir la synchronisation.

Au niveau du récepteur après synchronisation grâce au signal reçu, on récupère le message original par une simple soustraction.

Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal s(t) (porteuse chaotique plus le message). Donc il ne cherchera pas à appliquer des techniques de décryptage.

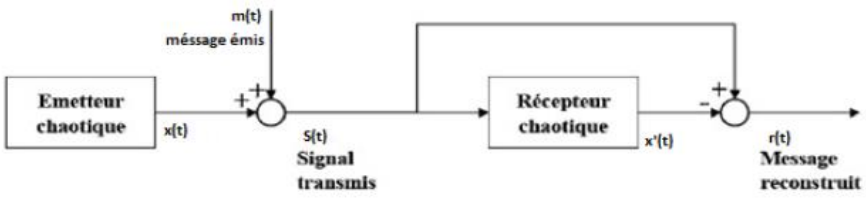



**Figure 3.5** : Cryptage par addition [8].

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.

L'inconvénient de cette méthode est qu'afin de garantir la synchronisation, le message doit être au moins de 20 à 30 dB inférieur à la sortie de l'émetteur. Toutefois, en présence d'un bruit de canal d'une puissance proche à celle du message, il devient difficile de détecter l'information. De plus, cette méthode reste sensible aux attaques extérieures [8].

### 3.4.2 Cryptage par modulation paramétrique :

L'approche par modulation utilise le message contenant l'information pour moduler un ou plusieurs paramètres θ de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant le changement du paramètre modulé. Le schéma correspondant est présenté par la figure 3.6.

Au niveau de l'émetteur, le fait de moduler un ou plusieurs paramètres impose à la trajectoire un changement continu de l'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 démodulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur [8].

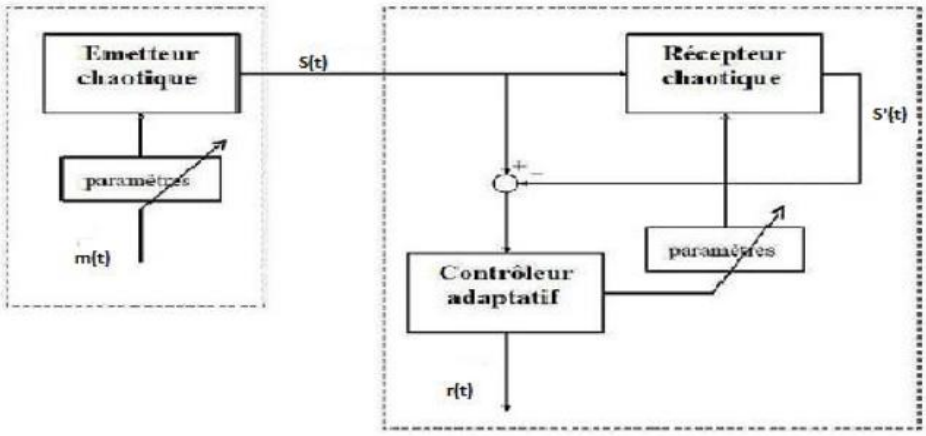



**Figure 3.6** : Cryptage par modulation paramétrique [8].

### 3.4.3 Cryptage par inclusion :

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur.

La restauration de l'information se fait principalement par deux techniques, se basant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur. Cette méthode présente beaucoup d'avantages et reste très utilisée en pratique [8].

### 3.4.4 Cryptage par décalage chaotique (CSK) :

L'apparition de cette technique, est considérée comme une conséquence des problèmes d'application pratique du masquage par addition. Elle a été proposée pour la première fois par le groupe de Kocarev, et sa dénomination actuelle est connue sous l'acronyme ''Chaos Shift Keying : CSK''[13] .

La CSK définie comme une modulation numérique est inspirée des techniques de modulation classique telles que la FSK (Frequency Shift Keying), la ASK (Amplitude Shift Keying) et la PSK (Phase Shift Keying).Ainsi, le système de masquage par CSK est constitué par un modulateur CSK au niveau de l'émetteur et d'un démodulateur CSK au niveau du récepteur raccordés par un canal routeur du signal comme cela est représenté sur la figure 3.7[13].

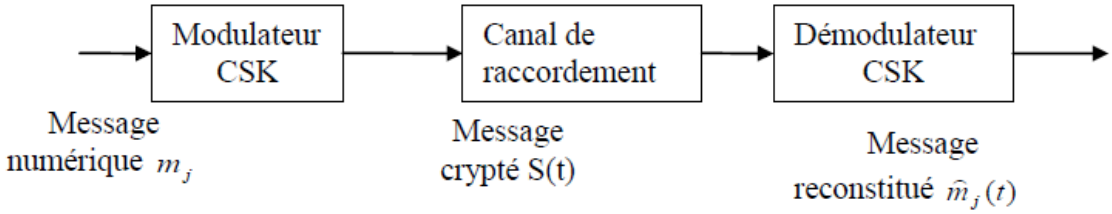



**Figure 3.7 :** Schéma de principe simplifié d'un système de cryptage CSK [13].

#### a) Le modulateur CSK :

Son idée de base est la même que celle de la modulation numérique classique, c'est-à-dire associer à chaque symbole du message à transmettre non pas une porteuse sinusoïdale, mais une porteuse chaotique différente, en se déplaçant dans une période de durée T. Ainsi en utilisant la notation la plus générale, les éléments de l'ensemble d'un signal message numérique décrits dans un espace de symboles à M niveaux et modulés par CSK sont définis par [13] :

$$\boldsymbol{S(t) = \sum_{j=1}^{N} m_j\, g_i\,(t)} \qquad (3.5)$$

Où : $m_j$ sont les éléments du vecteur signal message et $g_i(t)$ sont les porteuses chaotiques où : $j$ =1,2.....$N$ ; $i$ =1,2.....$M$ ; $N \leq M$ et $m_j$ =1 si $i = j$ et $m_j$=0 si $i \neq j$. Le signal $S(t)$ peut être généré selon le schéma représenté sur la figure 3.8 [13]:

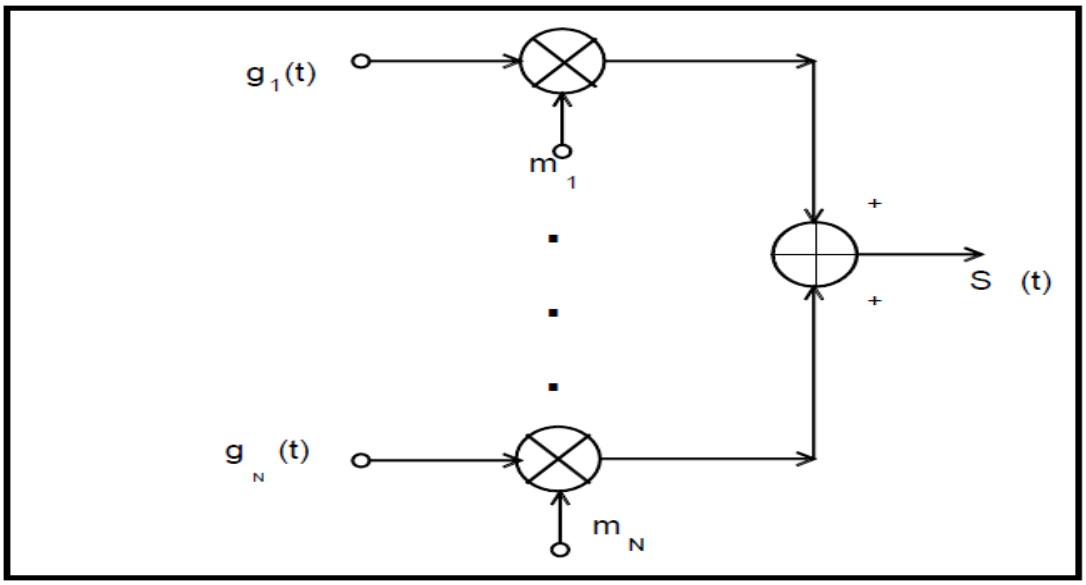



**Figure 3.8 :** Principe de la modulation CSK [13].

### b) Le démodulateur CSK :

La récupération du message émis du côté du récepteur se fait par la méthode suivante :

- **Démodulation basée sur la synchronisation et le calcul d'erreur :**

A ce niveau les porteuses chaotiques $g_i$, utilisées pour la modulation, seront reconstruites en utilisant des unités de synchronisation chaotiques. Le nombre de ces unités est égal au nombre des porteuses chaotiques $g_i$, Ainsi dans cette configuration, le signal reçu va essayer de synchroniser toutes les unités de synchronisation. Alors si on suppose que le signal transmis $S(t)=g_i(t)$ , on n'aura donc la synchronisation qu'avec la i-ème unité. De cette façon on va avoir une convergence de $g_i(t)$ vers la sortie de l'unité $\hat{g}_i(t)$ et une divergence pour les autres unités. L'estimation des symboles $m_j$ du message sera faite après le calcul des erreurs de synchronisation dans le bloc de décision. Les paramètres des unités de synchronisation et le temps symbole peuvent être considérés comme la clé de décryptage [13]. La figure 3.9 représente la démodulation basée sur la synchronisation et le calcul d'erreur :

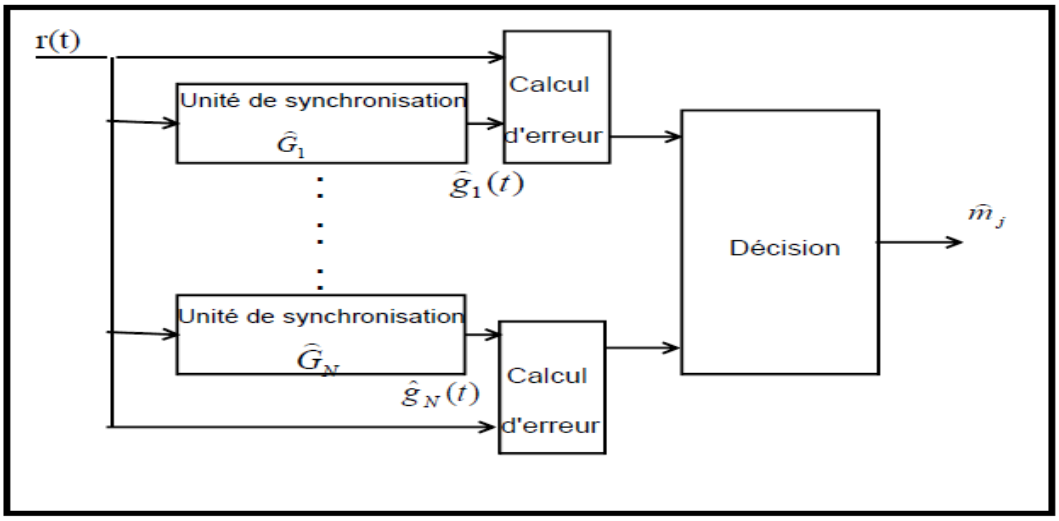



**Figure 3.9 :** Démodulation basée sur la synchronisation et le calcule d'erreur [13].

## 3.5 Etude de l'émetteur chaotique CSK :

L'émetteur hyper chaotique du système Qi est représenté par les équations suivantes :

$$\begin{cases} \frac{dx_1}{dt} = a(x_2 - x_1) + x_2x_3 \\ \frac{dx_2}{dt} = b(x_1 + x_2) - x_1x_3 \\ \frac{dx_3}{dt} = -cx_3 - ex_4 + x_1x_2 \\ \frac{dx_4}{dt} = -dx_4 + fx_3 + x_1x_2 \end{cases} \quad (3.6)$$

Où $x_1, x_2, x_3, x_4$ sont des variables d'état et $a, b, c, d, e, f$ sont des paramètres positifs du système. La figure 3.10 représente l'émetteur chaotique avec l'insertion du message par modulation CSK implémenté sous MATLAB :

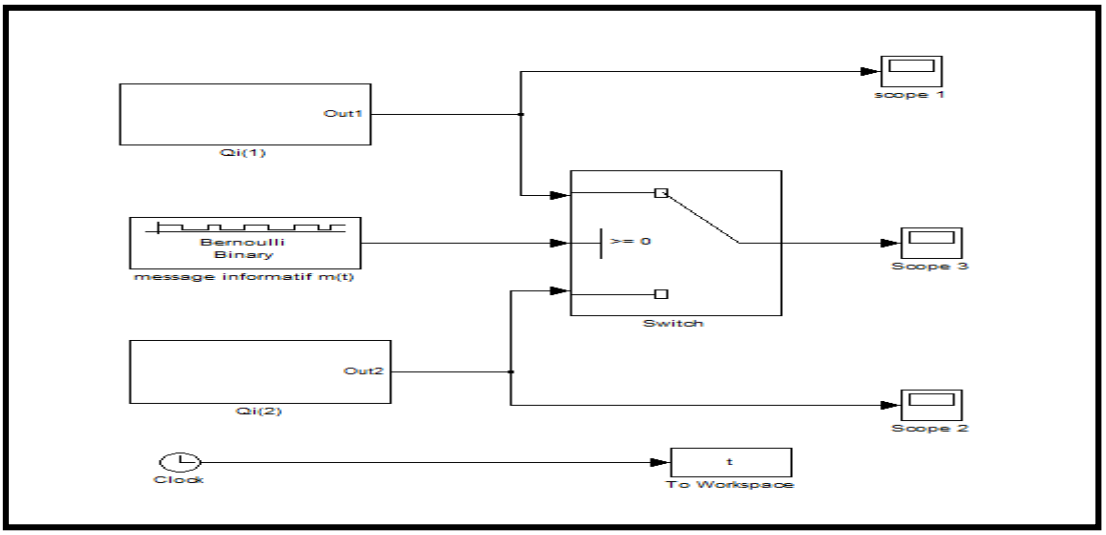



**Figure 3.10 :** Emetteur chaotique et modulation CSK sous MATLAB (Simulink).

La figure 3.11 représente le message informatif émis :

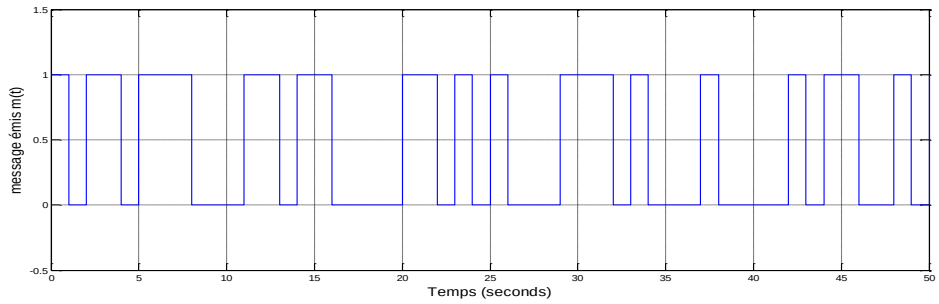



**Figure 3.11 :** Le message informatif émis $m(t)$.

La figure 3.12 représente le message crypté :

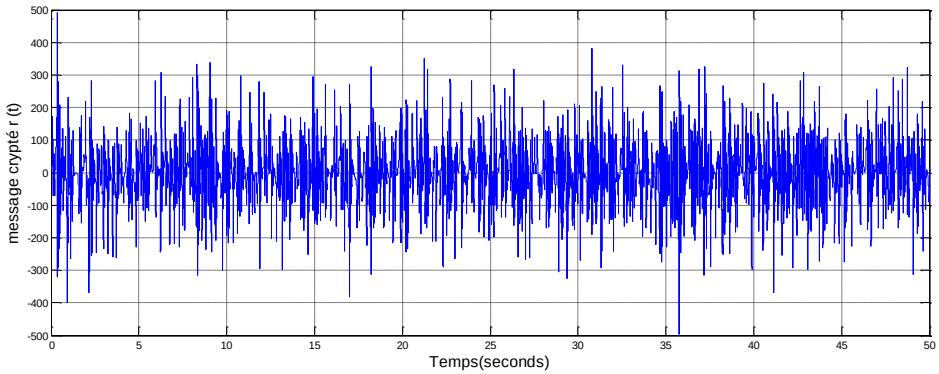



**Figure 3.12 :** Le message crypté r(t).

## 3.6 Etude du récepteur chaotique :

### 3.6.1 Récepteur chaotique :

Le schéma synoptique de la transmission sécurisée basée sur la modulation Chaos Shift Keying et la synchronisation par boucle fermée est représenté sur la figure 3.13 :

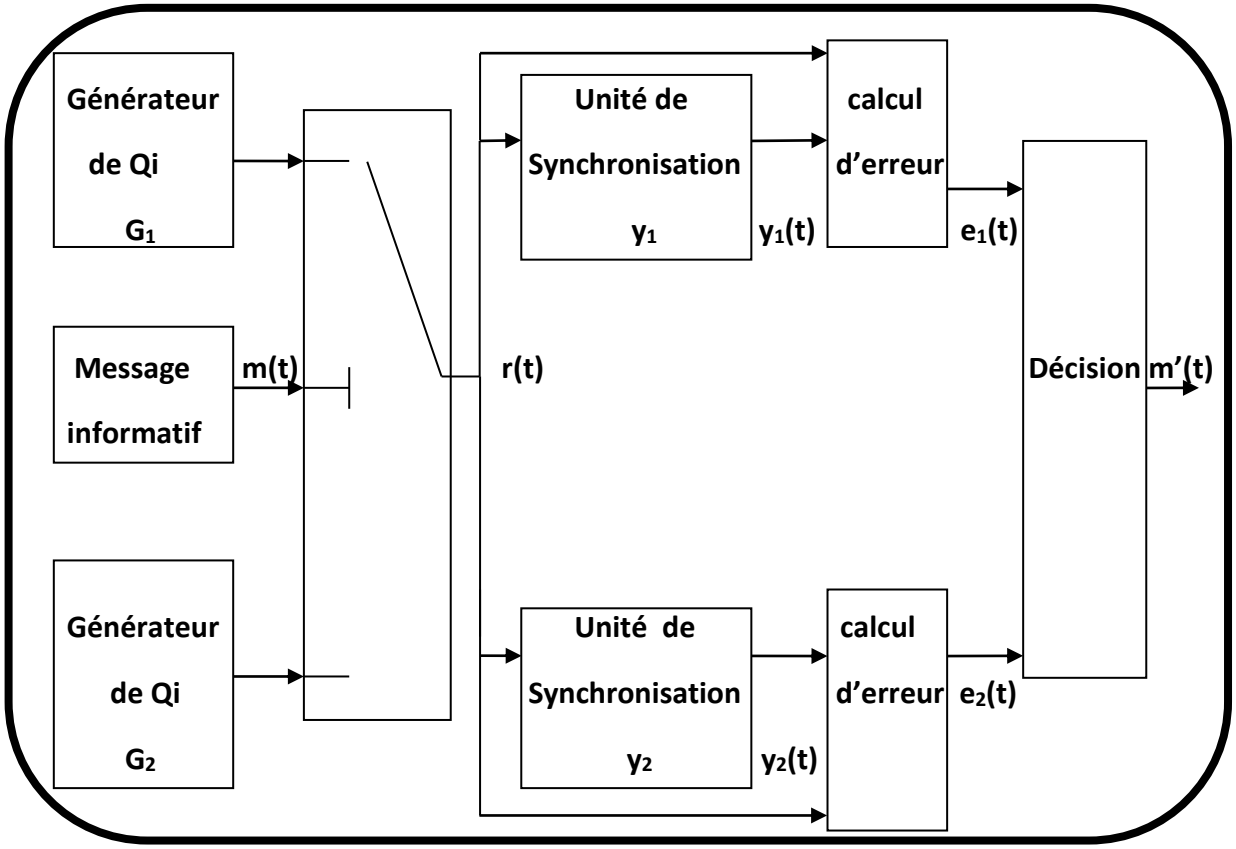



**Figure 3.13 :** Schéma synoptique d'une transmission sécurisée par CSK.

La figure 3.14 représente le récepteur chaotique :

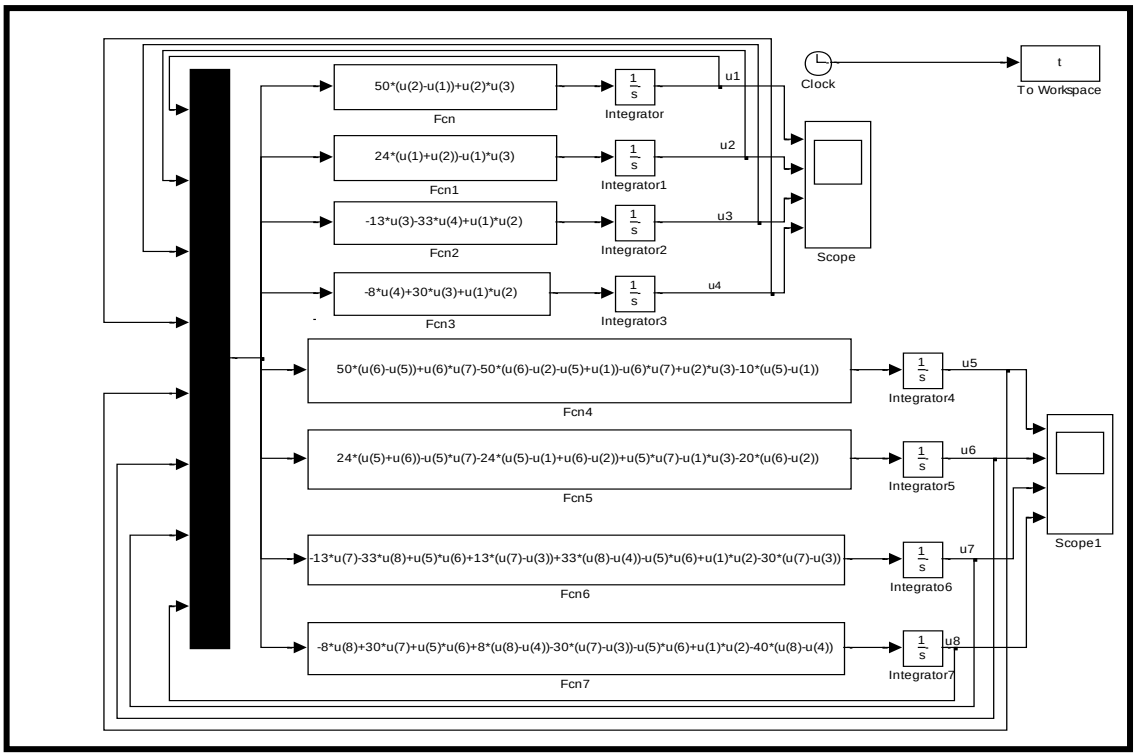



**Figure 3.14 :** Récepteur chaotique sous MATLAB (simulink).

La figure 3.15 représente l'implémentation du bloc de synchronisation par boucle fermée :

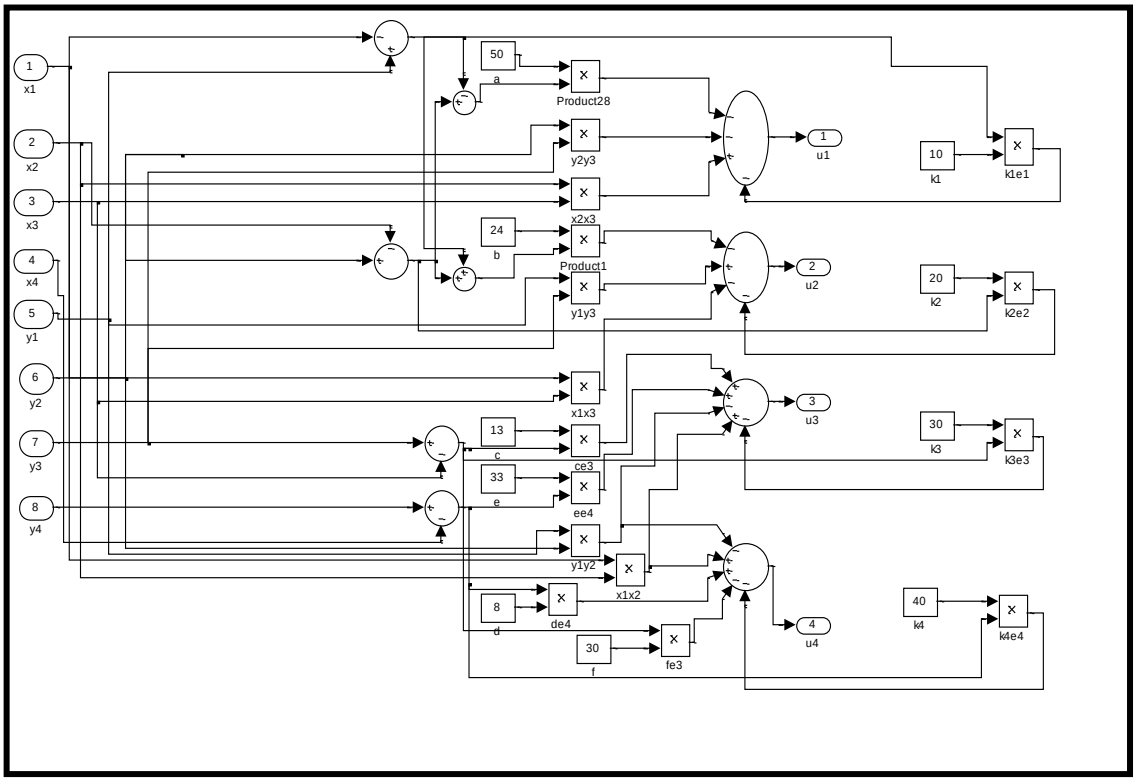



**Figure 3.15 :** Bloc de synchronisation par boucle fermée.

La figure 3.16 représente le schéma complet de la transmission sécurisée par modulation CSK en utilisant le système hyper chaotique de Qi :

- **Bloc 1 :** Système émetteur hyper chaotique de Qi.
- **Bloc 2 :** Système récepteur hyper chaotique de Qi.
- **Bloc 3 :** Synchronisation (par boucle fermée).
- **Bloc 4 :** Calcul d'erreur et décision.

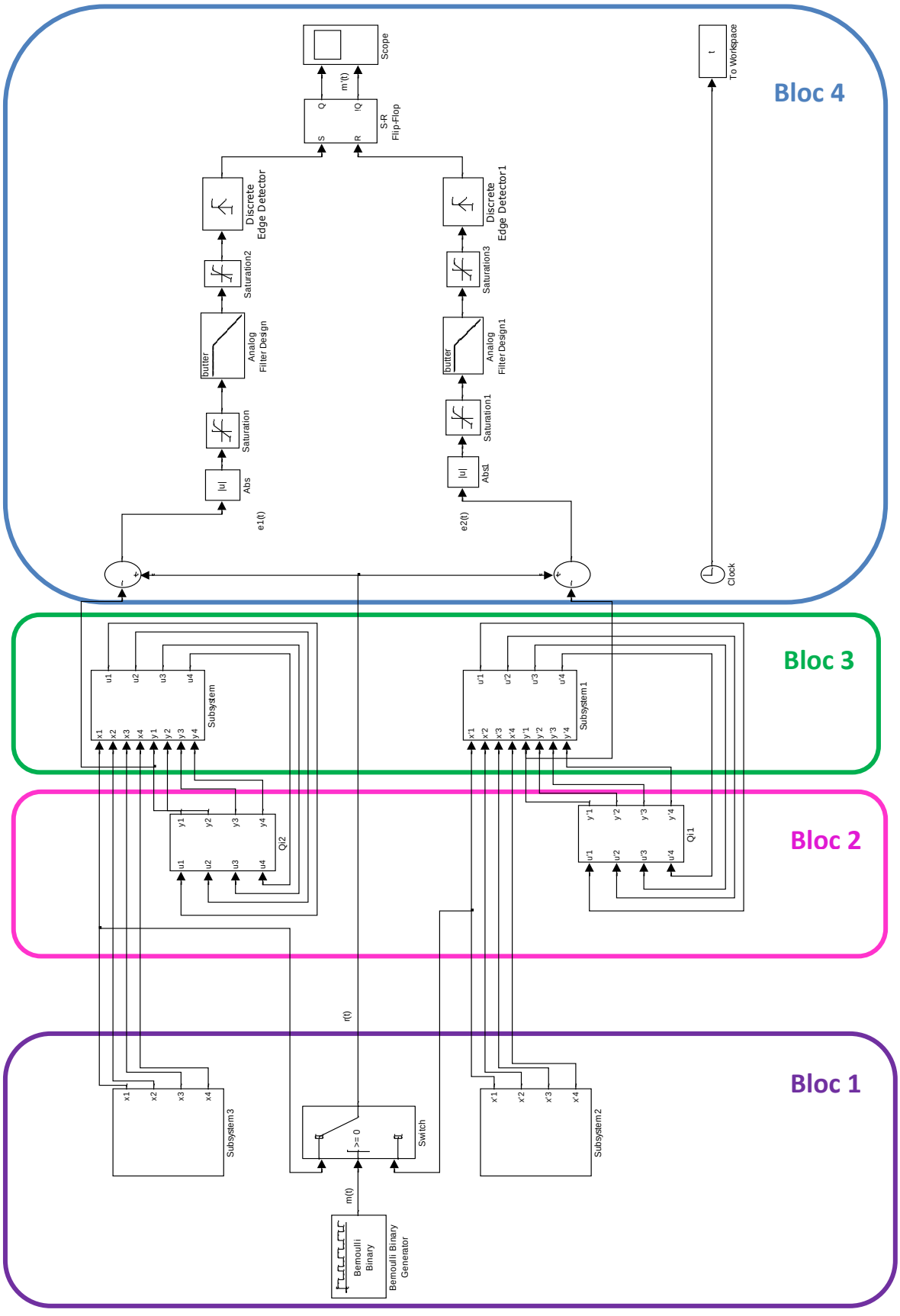



**Figure 3.16 :** Transmission sécurisée par modulation CSK**.**

### 3.6.2 Analyse de la synchronisation :

Le système de récepteur est décrit par les hyper chaotiques dynamiques de Qi contrôlées suivantes :

$$\begin{cases} \frac{dy_1}{dt} = a(y_2 - y_1) + y_2y_3 + U_1 \\ \frac{dy_2}{dt} = b(y_1 + y_2) - y_1y_3 + U_2 \\ \frac{dy_3}{dt} = -cy_3 - ey_4 + y_1y_2 + U_3 \\ \frac{dy_4}{dt} = -dy_4 + fy_3 + y_1y_2 + U_4 \end{cases} \quad (3.7)$$

Où $y_1, y_2, y_3, y_4$ sont des variables d'état et $U_1, U_2, U_3, U_4$ sont des systèmes de contrôles non linéaires actifs qui doivent être déterminés.

L'erreur de synchronisation « e » est définie par :

$$e_i = y_i - x_i \quad , i = (1, 2, 3, 4) \quad (3.8)$$

La dynamique d'erreur est obtenue par les relations suivantes :

$$\begin{aligned} \frac{de_1}{dt} &= a(e_2 - e_1) + y_2y_3 - x_2x_3 + U_1 \\ \frac{de2}{dt} &= b(e_1 + e_2) - y_1y_3 + x_1x_3 + U_2 \\ \frac{de_3}{dt} &= -ce_3 - ee_4 + y_1y_2 - x_1x_2 + U_3 \\ \frac{de_4}{dt} &= -de_4 + fe_3 + y_1y_2 - x_1x_2 + U_4 \end{aligned} \quad (3.9)$$

En utilisant le contrôleur non linéaire actif suivant:

$$\begin{aligned} U_1 &= -a(e_2 - e_1) - y_2y_3 + x_2x_3 - k_1e_1 \\ U_2 &= -b(e_1 + e_2) + y_1y_3 - x_1x_3 - k_2e_2 \\ U_3 &= ce_3 + ee_4 - y_1y_2 + x_1x_2 - k_3e_3 \\ U_4 &= de_4 - fe_3 - y_1y_2 + x_1x_2 - k_4e_4 \end{aligned} \quad (3.10)$$

Où les gains du retour $k_1, k_2, k_3, k_4$ sont des constantes positives,

et en remplacent 3.10 dans 3.9 la dynamique de l'erreur s'écrit:

$$\frac{de_1}{dt} = -k_1 e_1$$

$$\frac{de_2}{dt} = -k_2 e_2 \qquad (3.11)$$

$$\frac{de_3}{dt} = -k_3 e_3$$

$$\frac{de_4}{dt} = -k_4 e_4$$

Nous considérons la fonction de Lyapunov quadratique définie par :

$$V(e) = \frac{1}{2} e^T e = \frac{1}{2}( e_1^2 + e_2^2 + e_3^2 + e_4^2) \qquad (3.12)$$

Où : $V(e)$est une fonction définie positive sur $R^4$.

La dérivation par rapport à l'erreur dynamique :

$$\dot{V}(e) = -k_1 e_1^2 - k_2 e_2^2 - k_3 e_3^2 - k_4 e_4^2 \qquad (3.13)$$

Où :$\dot{V}$ est une fonction définie négative sur $R^4$.

$$\dot{V}(e) < 0 \qquad pour\ k_i > 0\ , \{i= 1, 2, 3 ,4\} \qquad (3.14)$$

Selon la théorie de Lyapunov, l'inégalité V(t) <0 indique que V(t) converge vers zéro et qu'elle est bornée quelque soit t. Il est noté que $e(t) \to 0$ quand t $\to \infty$ .

On en déduit que : $e_1 \to 0, e_2 \to 0, e_3 \to 0, e_4 \to 0$ si t $\to \infty$

$$\lim_{t\to\infty} ||e|| = 0 \qquad (3.15)$$

On en conclue que les systèmes Qi hyper chaotiques identiques 3.6 et 3.7 sont globalement et de façon exponentielle synchronisés pour toutes conditions initiales avec le contrôleur non linéaire actif défini par 3.10.

### 3.6.3 Etude des cas particuliers:

- La figure 3.17 représente le cas où l'émetteur et le récepteur ne sont pas synchronisés avec $k_1$= -1, $k_2$= -10, $k_3$= -5, $k_4$= -8.

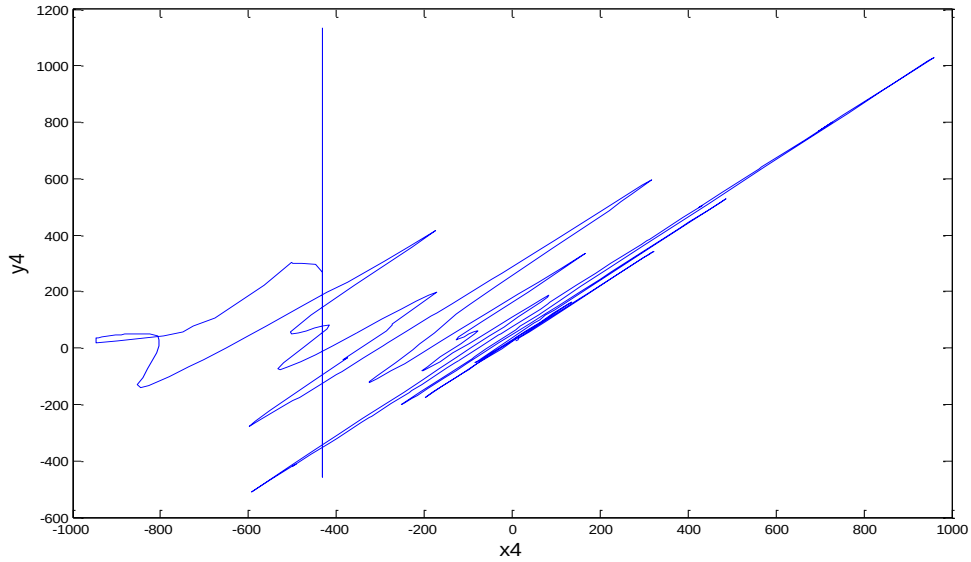



**Figure 3.17 :** Le signal $y_4$ en fonction de $x_4$ (non synchronisé).

On ne peut jamais reconstituer le message informatif émis si l'émetteur et le récepteur ne sont pas synchronisés.

La figure 3.18 représente le message informatif émis et reçu dans le cas où on n'a pas de synchronisation.

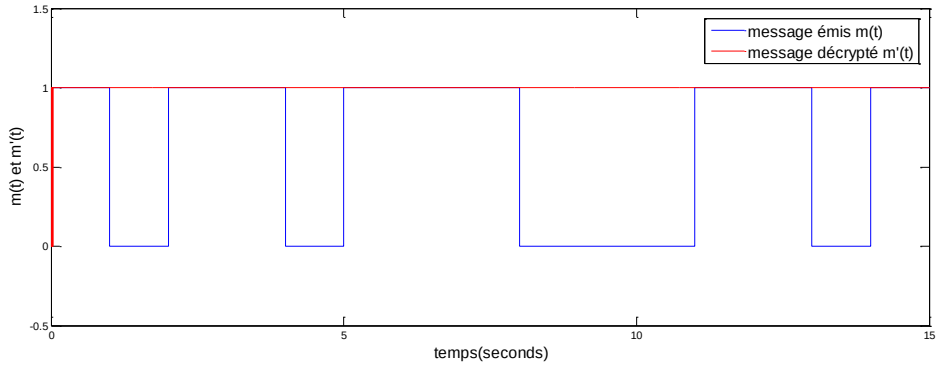



**Figure 3.18 :** Le message informatif émis et le message décrypté.

Lorsque le signal émis et le signal reçu ne sont pas synchronisés, l'erreur ne tend pas vers zéro.

La figure 3.19 représente l'erreur $e_1(t)$ entre l'émetteur et le récepteur dans le cas de non synchronisation.

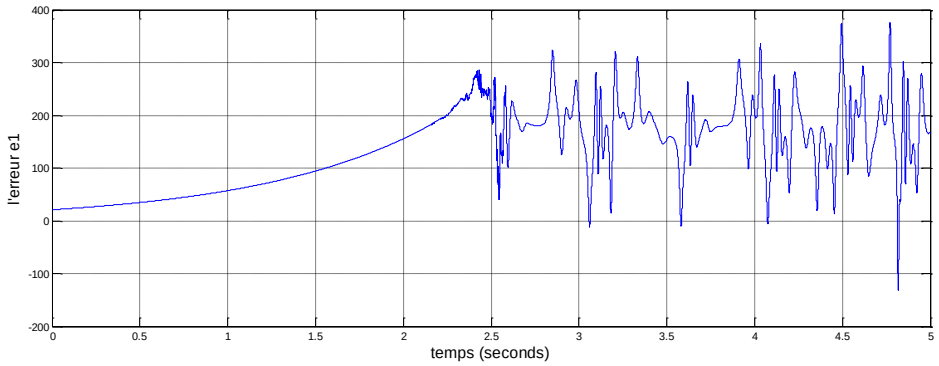



**Figure 3.19 :** L'erreur $e_1(t)= y_1(t) – x_1(t)$ pour la non synchronisation.

### 3.6.4 Visualisation des signaux :

Les figures de 3.20 à 3.23 représentent les différents signaux obtenus lorsque l'émetteur et le récepteur sont synchronisés :

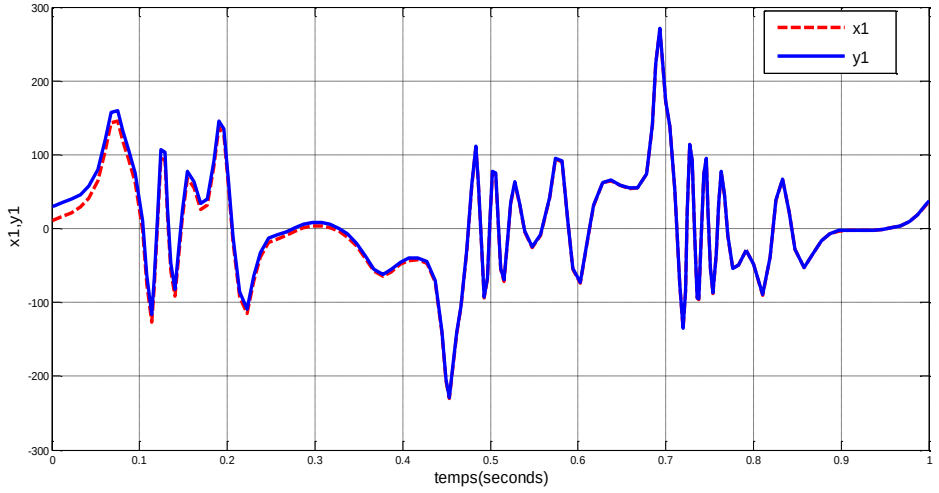



**Figure 3.20 :** Le signal émis $x_1(t)$ et le signal reçu $y_1(t)$.

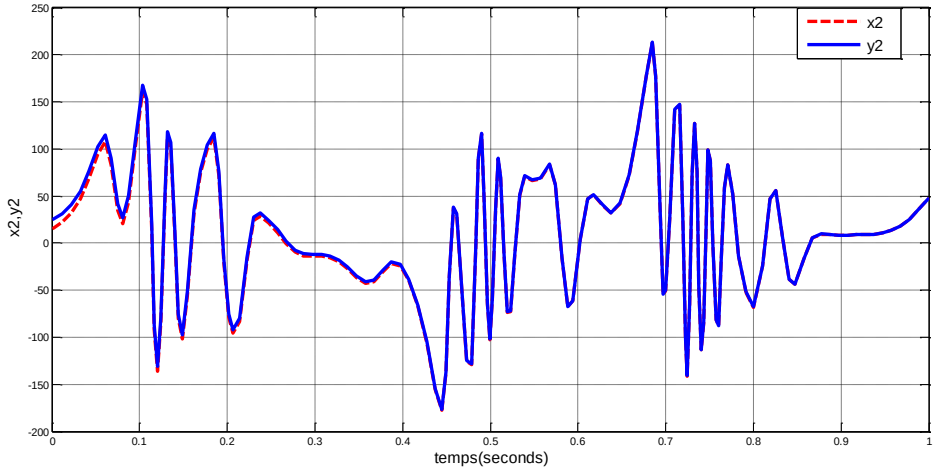



**Figure 3.21 :** Le signal émis $x_2(t)$ et le signal reçu $y_2(t)$.

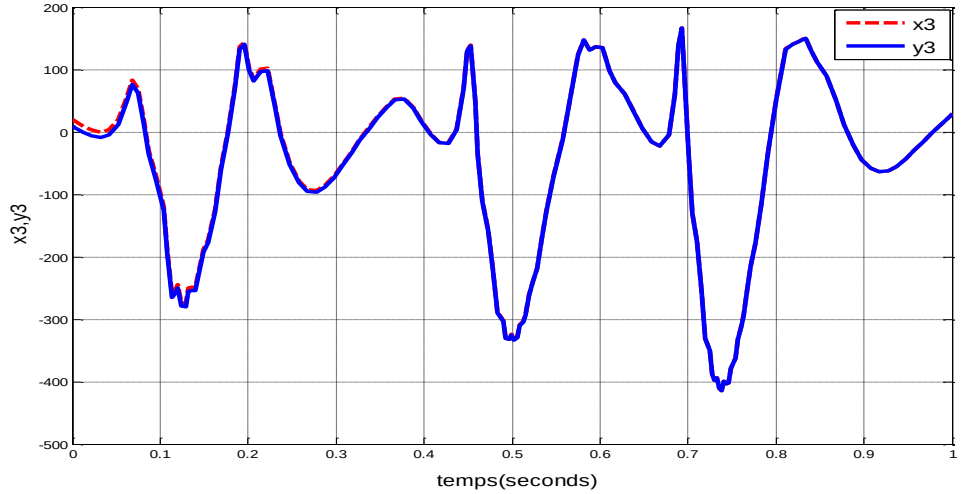



**Figure 3.22 :** Le signal émis $x_3(t)$ et le signal reçu $y_3(t)$.

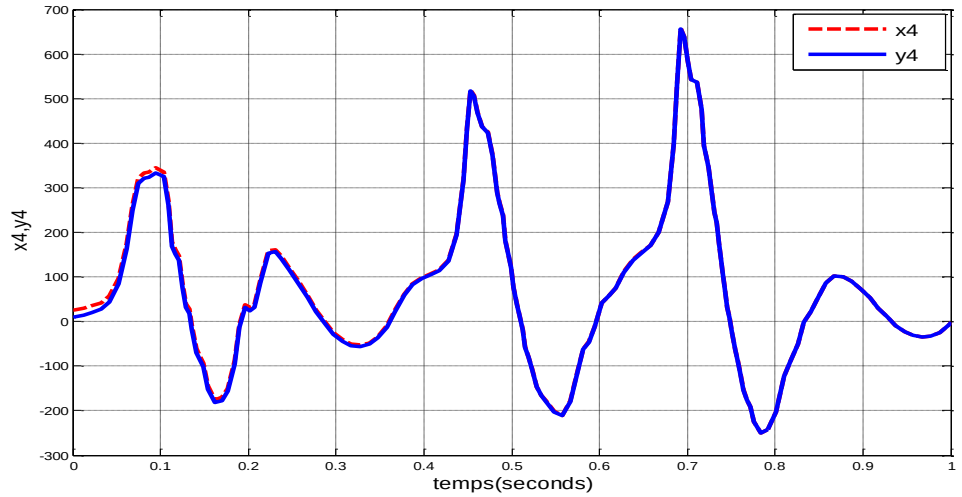



**Figure 3.23 :** Le signal émis $x_4(t)$ et le signal reçu $y_4(t)$.

Lorsque les signaux émis et les signaux reçus sont synchronisés :

- On obtient une droite quand on représente l'état reçu en fonction de l'état émis et l'erreur tend vers zéro.

La figure 3.24 représente l'état du signal reçu en fonction de l'état du signal émis :

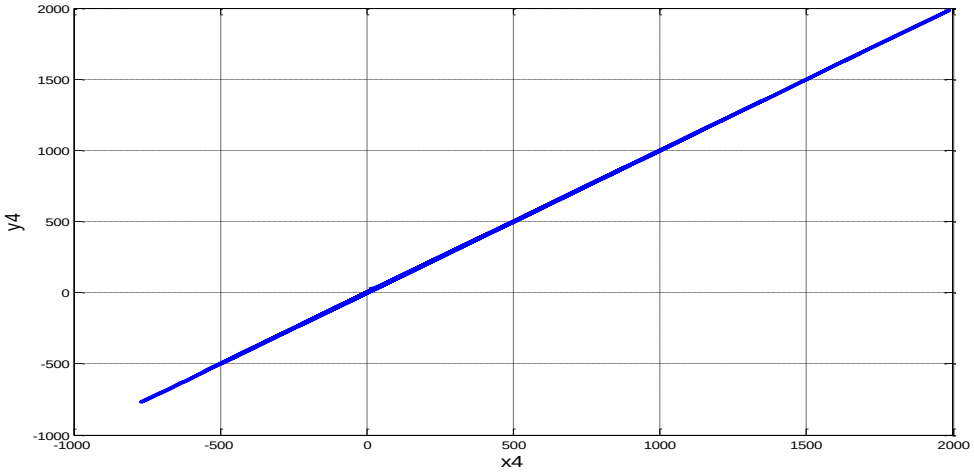



**Figure 3.24 :** Signal $y_4$ en fonction de $x_4$ avec $K_4$=50.

La figure 3.25 représente les erreurs : $e_1(t) = y_1(t)-x_1(t)$, $e_2(t)=y_2(t)-x_2(t)$, $e_3(t)=y_3(t)-x_3(t)$ et $e_4(t)=y_4(t)-x_4(t)$.

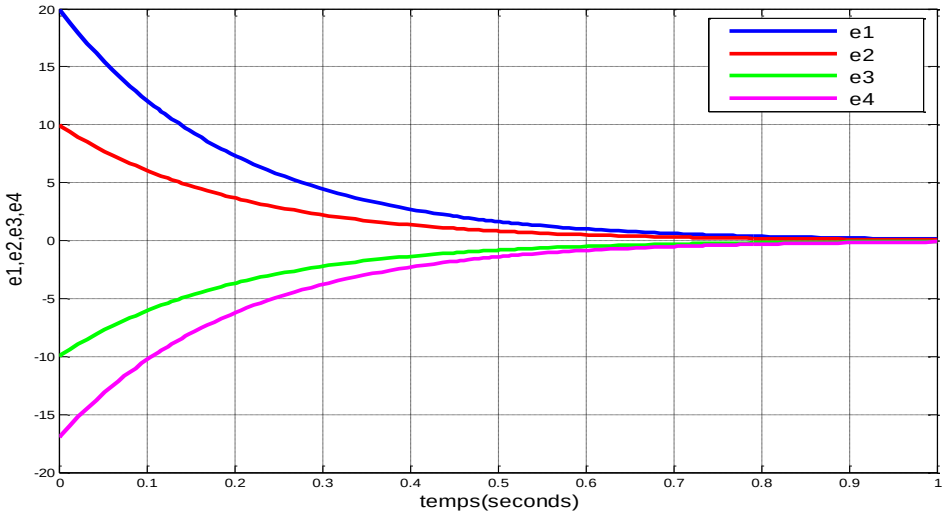
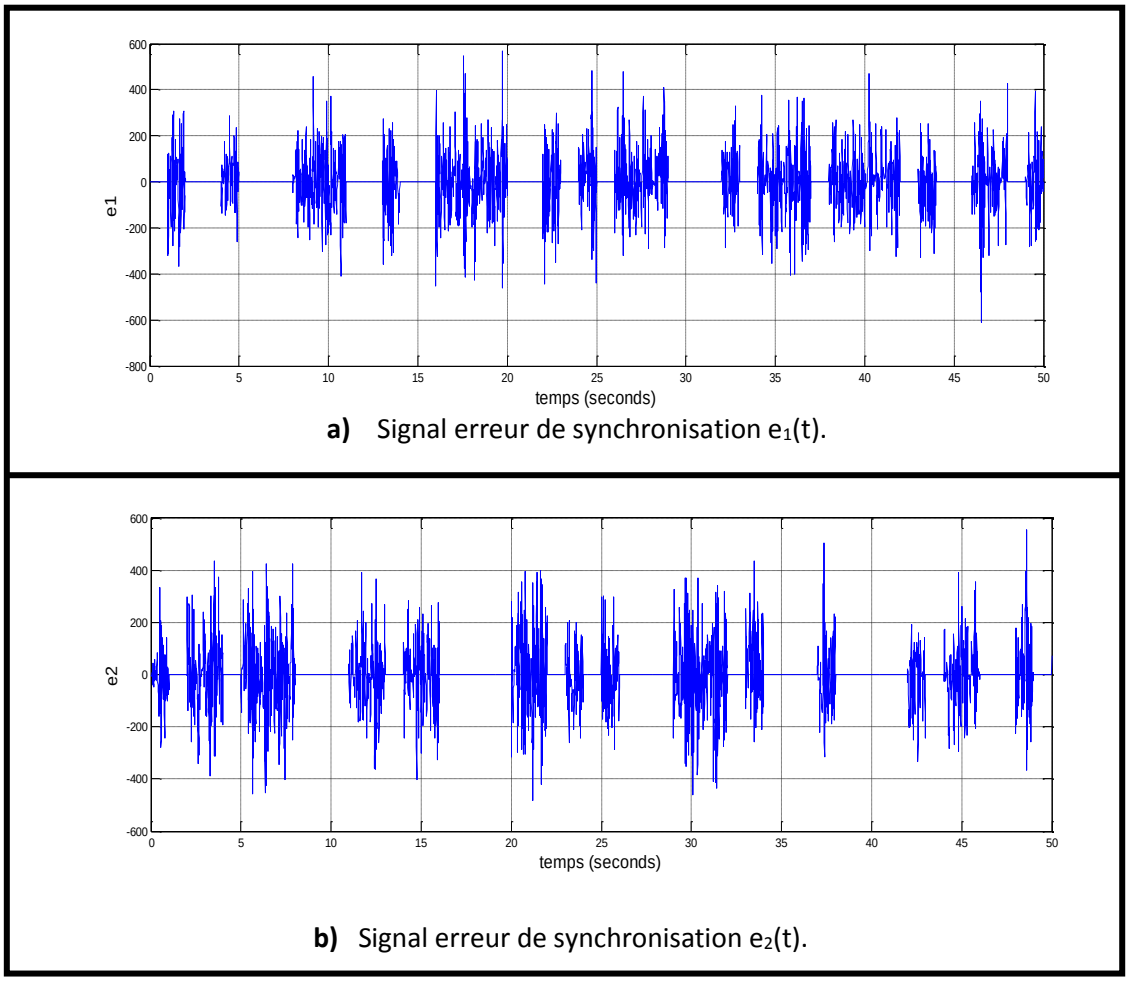



**Figure 3.25 :** Les erreurs $e_1(t)$, $e_2(t)$, $e_3(t)$ et $e_4(t)$ en fonction du temps.

La figure 3.26 représente le signal d'erreur de synchronisation $e_1(t)$ et $e_2(t)$:




**a)** Signal erreur de synchronisation $e_1(t)$.

**b)** Signal erreur de synchronisation $e_2(t)$.

**Figure 3.26 :** a) signal erreur de synchronisation $e_1(t)$, b) signal erreur de synchronisation $e_2(t)$.

La figure 3.27 représente les deux erreurs de synchronisation e1(t) et e2(t) :

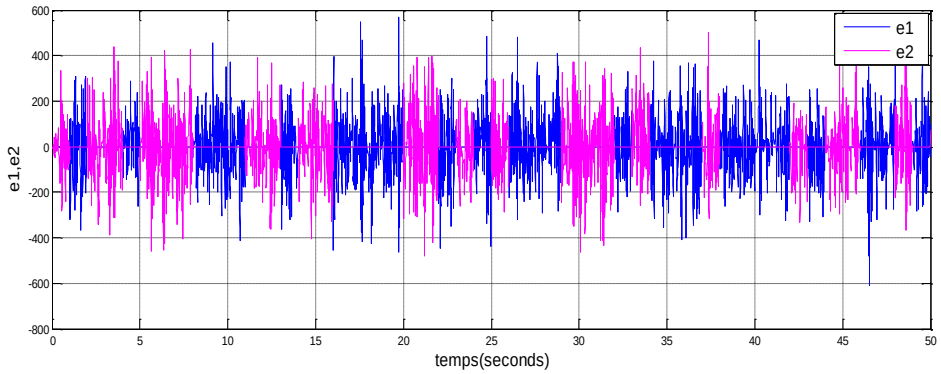
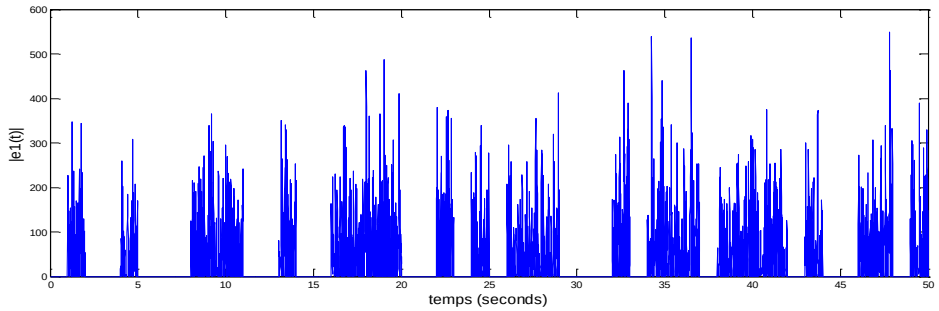
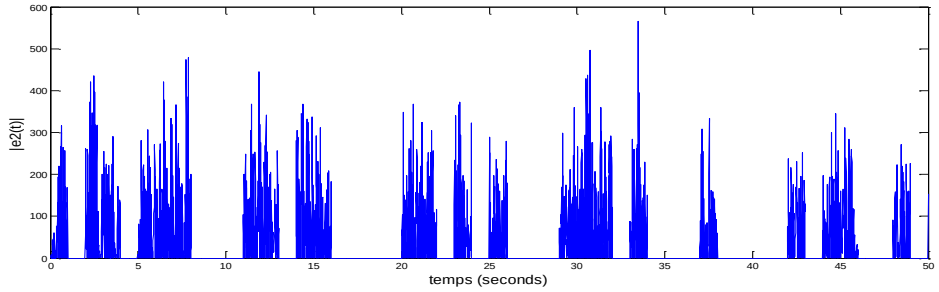



**Figure 3.27 :** Les erreurs $e_1(t)$ et $e_2(t)$ en fonction du temps.

La figure 3.28 représente les valeurs absolues des signaux erreurs de synchronisation $e_1(t)$ et $e_2(t)$ :



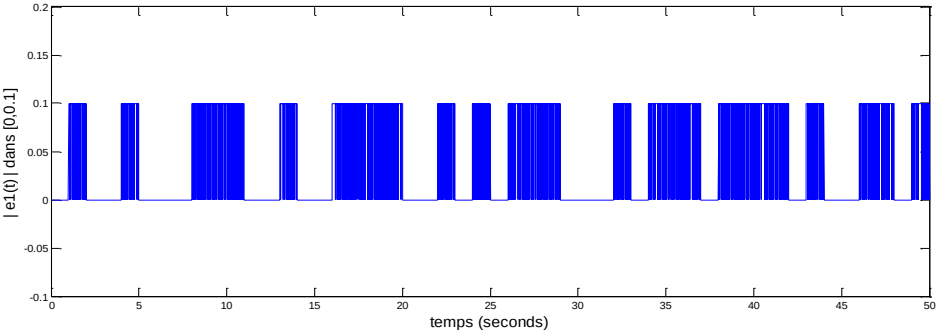

**a)** La valeur absolue du signal erreur $e_1(t)$.



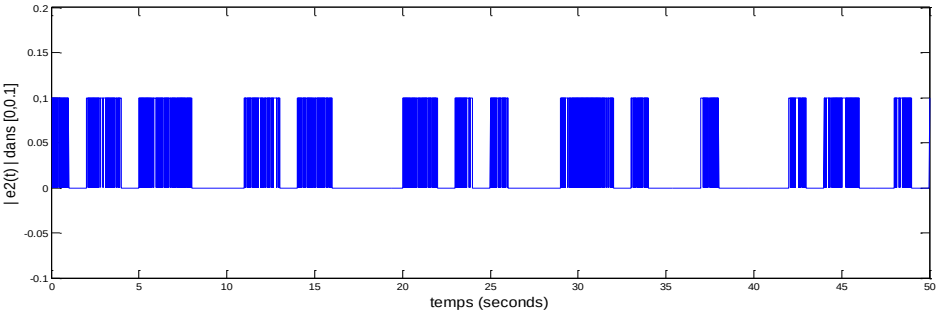

**b)** La valeur absolue du signal erreur $e_2(t)$.

**Figure 3.28** : Représente les valeurs absolues des signaux erreurs de synchronisation.

La figure 3.29 représente les valeurs limitées des signaux erreur de synchronisation $e_1(t)$ et $e_2(t)$ :



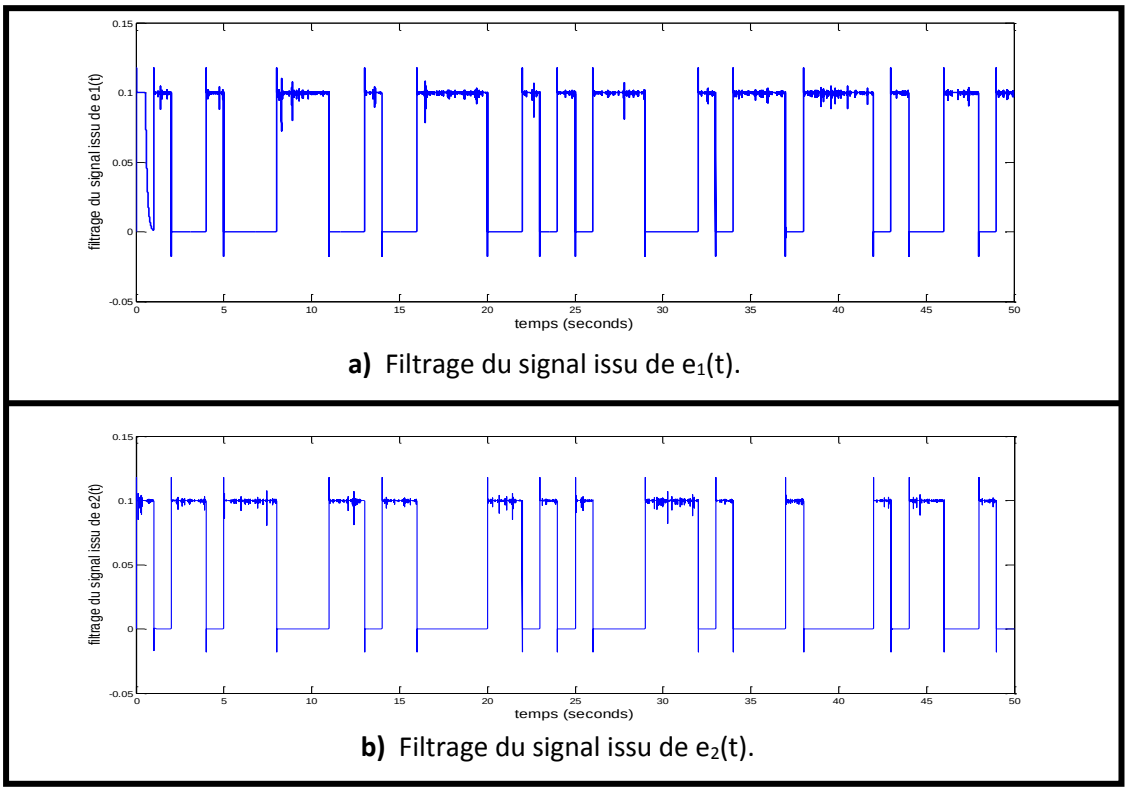

**a)** Limitation du niveau du $|e_1(t)|$dans [0,0.1].




**b)** Limitation du niveau du $|e_2(t)|$ dans [0,0.1].

**Figure 3.29** : Valeurs limitées des valeurs absolues des signaux erreurs de synchronisation.

La figure 3.30 représente le filtrage des signaux issus de $e_1(t)$ et $e_2(t)$ :

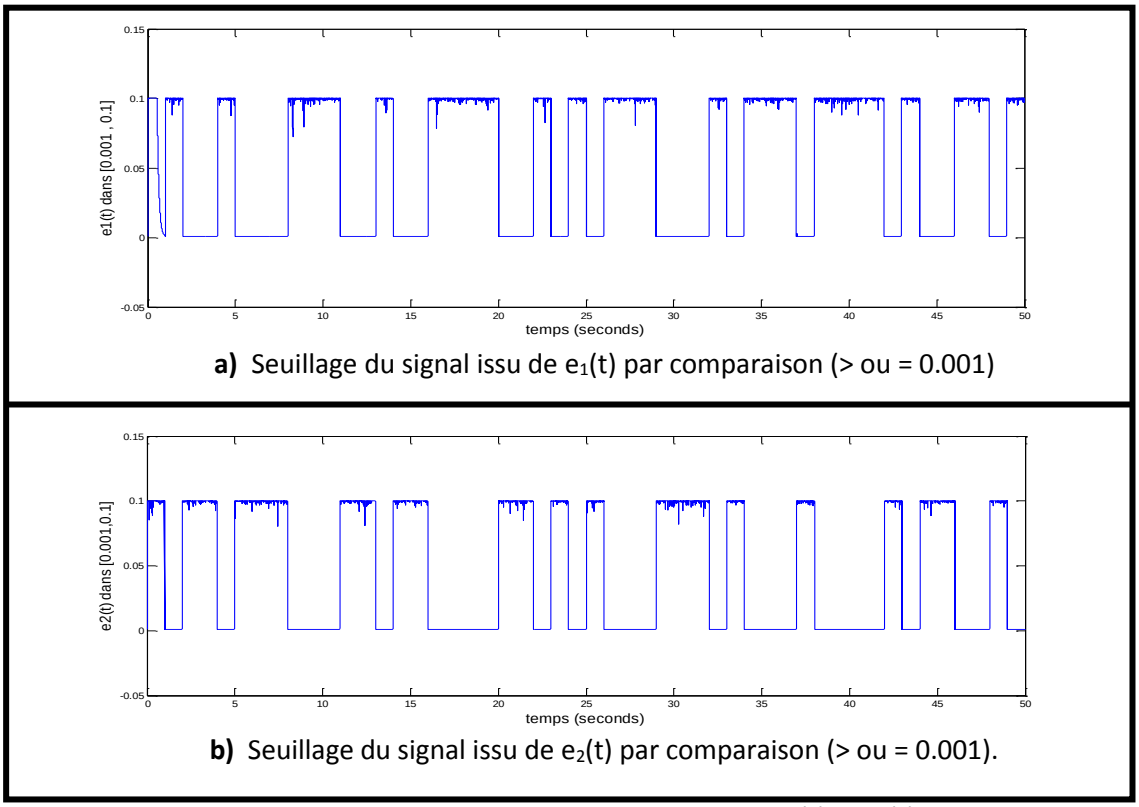



**a)** Filtrage du signal issu de $e_1(t)$.

**b)** Filtrage du signal issu de $e_2(t)$.

**Figure 3.30** : Filtrage des signaux issus de $e_1(t)$ et $e_2(t)$.

La figure 3.31 représente le seuillage des signaux issus de $e_1(t)$ et $e_2(t)$ :

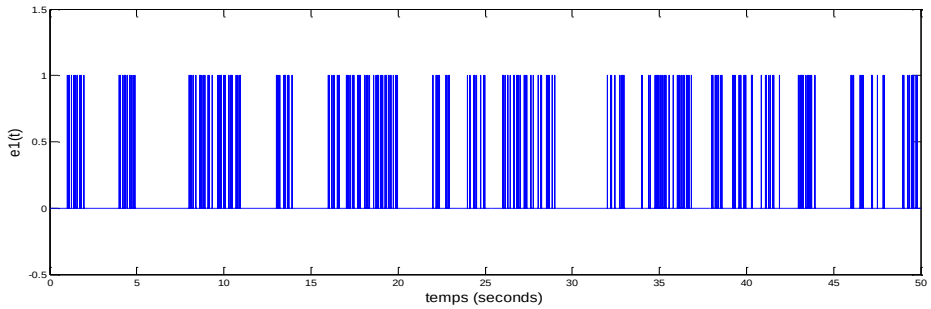



**a)** Seuillage du signal issu de $e_1(t)$ par comparaison (> ou = 0.001)

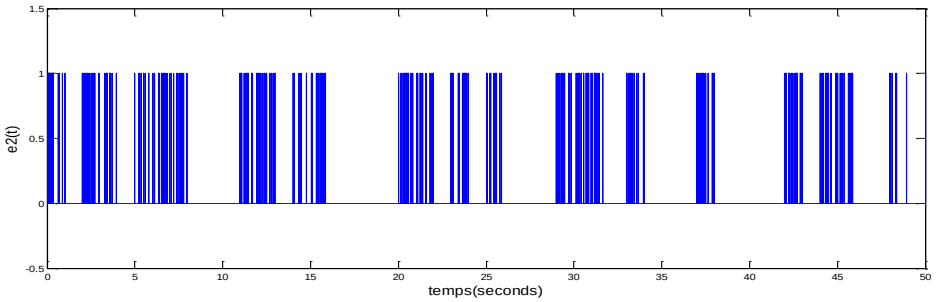
**b)** Seuillage du signal issu de $e_2(t)$ par comparaison (> ou = 0.001).

**Figure 3.31 :** Seuillage des signaux issus de $e_1(t)$ et $e_2(t)$.

La figure 3.32 représente les fronts montants des signaux issus de $e_1(t)$ et $e_2(t)$ :



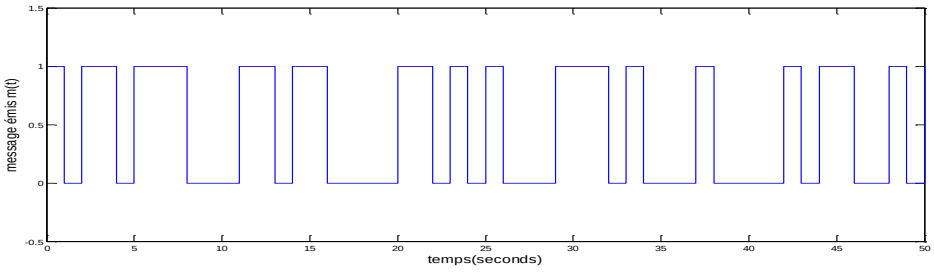

**a)** Détection du front montant du signal issu de $e_1(t)$.



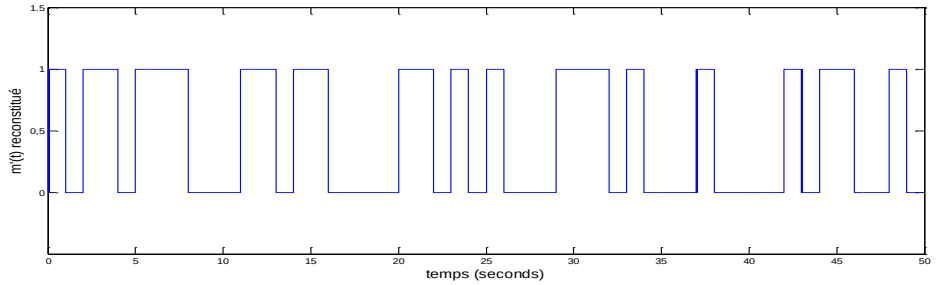

**b)** Détection du front montant du signal issu de $e_2(t)$.

**Figure 3.32:** Détection des fronts montants des signaux issus de $e_1(t)$ et $e_2(t)$.

La figure 3.33 représente le message informatif émis m(t) et le message décrypté m'(t) :




**a)** Le message informatif émis m(t).




**b)** Le message décrypté m'(t).

**Figure 3.33:** Message informatif émis m(t) et message décrypté m'(t).

La figure 3.34 représente la différence entre les deux messages émis m(t) et décrypté m'(t) :

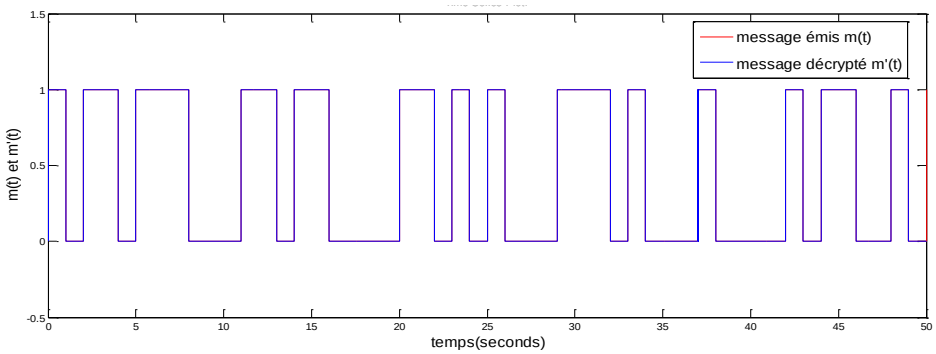



**Figure 3.34 :** Comparaison du message décrypté avec le message émis.

## 3.7 Transmission d'une image:

L'analyse du crypto système hyper chaotique de Qi étudié, sera faite sur sa fiabilité de cryptage et de décryptage d'une image binaire.

Les images numériques sont des tableaux des nombres c'est à dire représentées logiquement par des matrices. Les valeurs des nombres stockés dans les éléments du tableau se situent dans une gamme spécifique, généralement limitée à l'intervalle [0-255]. La valeur 0 indique le manque de la couleur associée (rouge, vert ou bleu), et la valeur 255 est le niveau le plus lumineux auquel cette couleur est affichée [11].

### 3.7.1 L'image utilisée pour l'analyse :

Le choix a été fait sur une image noir et blanc qui contient (90x90) pixels. Elle peut être représentée par une matrice (90x90) contenant des entiers en base 2, représentant le degré de luminosité des pixels constituant l'image .Afin de réaliser le processus de transmission de cette image par l'intermédiaire du crypto système ci-dessous, la transformation suivante est nécessaire:

- La matrice de nombres binaires, sera transformée en un seul vecteur par succession de ces colonnes pour générer le signal binaire à transmettre.

La figure suivante représente le prétraitement de l'image avant sa transmission :

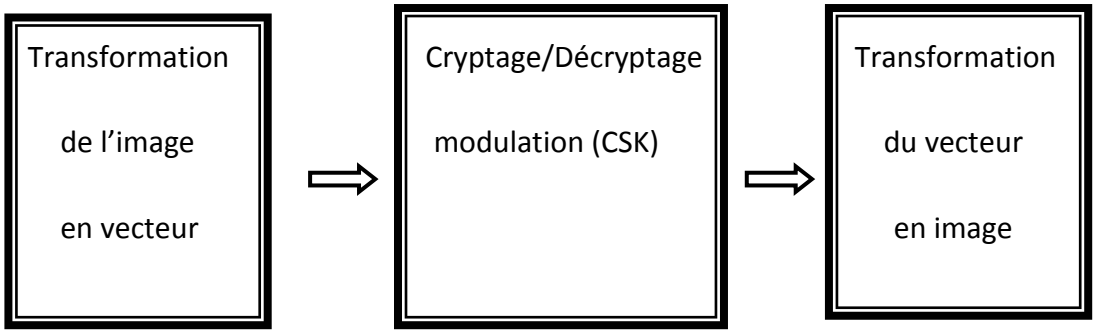



**Figure 3.35 :** Principe de transmission sécurisée d'une image en utilisant la modulation (CSK).

La figure 3.36 représente le schéma complet de la transmission sécurisée d'une image par modulation CSK en utilisant le système hyper chaotique de Qi :

- **Bloc 1 :** Transformation de l'image en vecteur.
- **Bloc 2 :** Cryptage & Décryptage.
- **Bloc 3 :** Transformation du vecteur en image.

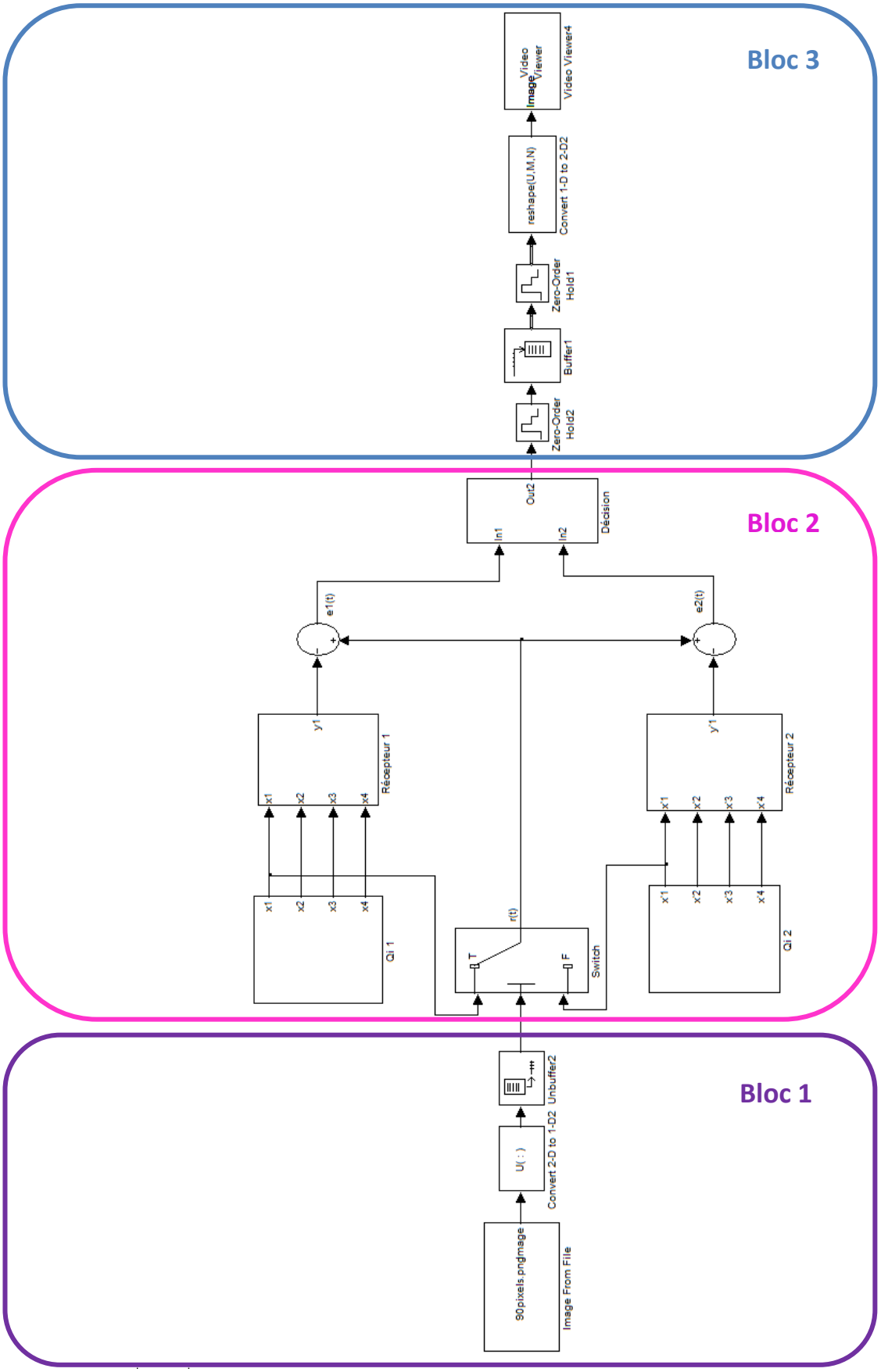
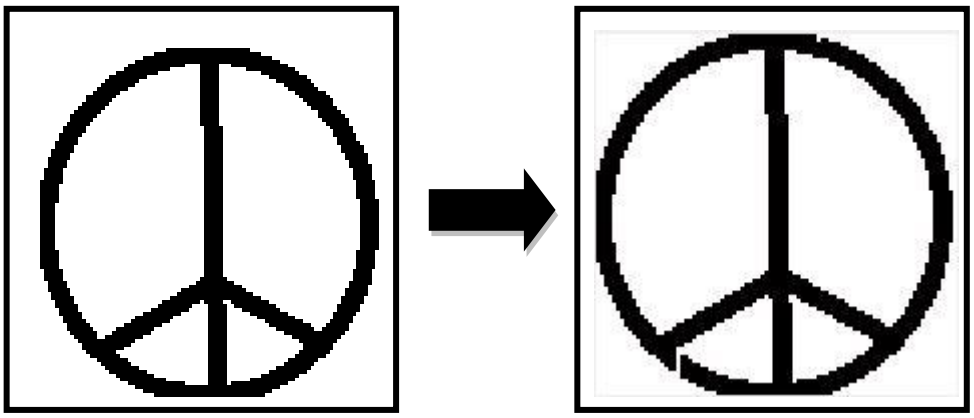


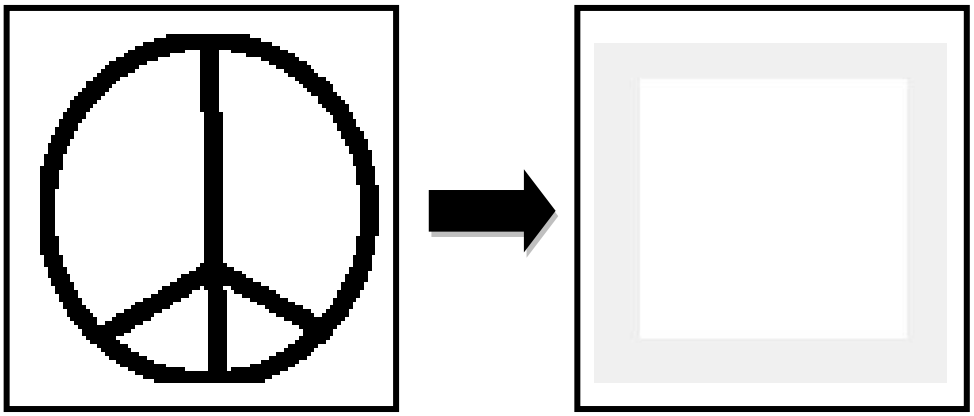

**Figure 3.36 :** Transmission sécurisée d'une image par modulation CSK**.**

Les figures 3.37 et 3.38 représentent respectivement l'image décryptée dans le cas de synchronisation et l'image décryptée dans le cas de non synchronisation.



**a)** image émise **b)** image décryptée

**Figure 3.37 :** Image émise et décryptée dans le cas de synchronisation.



**a)** image émise **b)** image décryptée

**Figure 3.38 :** Image émise et décryptée dans le cas de non synchronisation.

## 3.8 Conclusion :

Dans ce chapitre, nous avons présenté les différentes techniques de cryptage par le chaos, ainsi que les différents types de couplages (unidirectionnels et bidirectionnels) et les méthodes de synchronisation. Ensuite, on a étudié l'émetteur hyper-chaotique de Qi avec l'insertion du message binaire par modulation CSK , et le récepteur hyper-chaotique de Qi avec l'approche utilisée pour la synchronisation en utilisant la méthode par boucle fermée. La condition de synchronisation a été analysée en

calculant les valeurs du coefficient de couplage $K$. Les résultats de simulation de la transmission chaotique permettant de retrouver les états de l'émetteur chaotique et la récupération du message ont été vérifiés. Dans le chapitre suivant, une implémentation sur circuit FPGA de l'émetteur étudié basé sur le système hyper chaotique de Qi sera effectuée.

# Chapitre 4 Implémentation sur circuit FPGA

## 4.1 Introduction :

Les circuits FPGA sont les circuits qui ont permis de pousser encore plus loin le progrès technologique en électronique. En effet, le degré de développement des FPGAs fait d'eux aujourd'hui une solution pour remplacer les ASICs (Circuits intégrés à application spécifique) et les processeurs personnalisés dans des applications de contrôle et de traitement des signaux [10].

Dans le cadre de notre projet nous avons opté pour la technologie FPGA pour la réalisation de notre système hyper chaotique de Qi. En effet l'avantage de cette technique est de se passer d'une réalisation couteuse qui consisterait en la réalisation d'un émetteur en éléments analogiques discrets [9].

## 4.2 Présentation des circuits FPGA :

Un FPGA est un circuit logique reprogrammable. À l'aide de blocs logiques préconstruits et de ressources de routage programmables, c'est un circuit configurable afin de mettre en œuvre des fonctionnalités matérielles personnalisées, sans avoir jamais besoin d'utiliser une maquette ou un fer à souder. Il suffit de développer des tâches de traitement numérique par logiciel et de les compiler sous forme de fichier de configuration ou de flux de bits (bitstream) contenant des informations sur la manière dont les composants doivent être reliés. En outre, les FPGAs sont totalement reconfigurables et peuvent adopter instantanément une nouvelle circuiterie si une nouvelle configuration du circuit est recompilée [10].

### 4.2.1 Description des composants FPGA :

Les circuits FPGA sont constitués d'une matrice de blocs logiques programmables

entourés de blocs d'entrée/sortie programmable IOB. L'ensemble est relié par un réseau d'interconnexions programmable [17].

La figure 4.1 présente l'architecture générique d'un circuit FPGA.

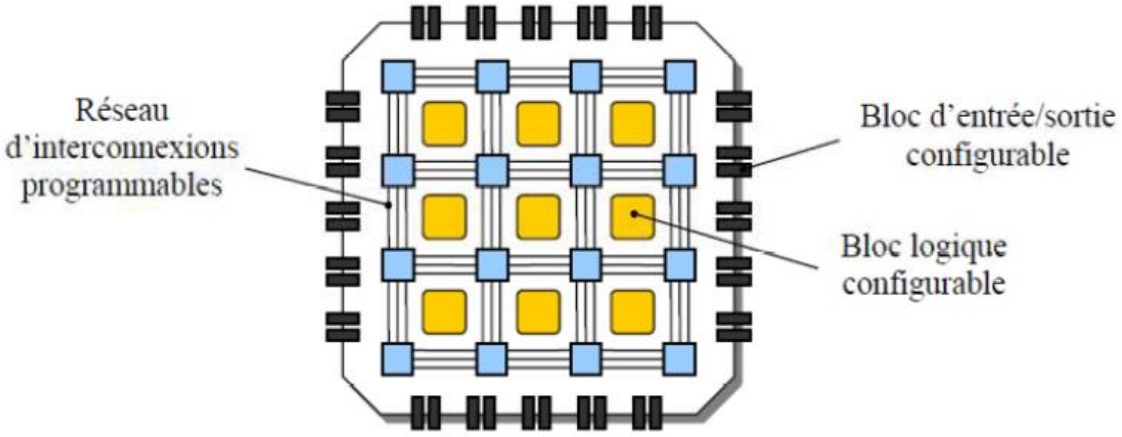



**Figure 4.1 :** Description de l'architecture générique d'un FPGA [5].

### 4.2.2 Technologies des FPGAs :

Il existe plusieurs fabricants de composants FPGA tels que Actel, Xilinx et Altera. Ces constructeurs utilisent différentes technologies pour la fabrication des FPGAs. Parmi ces technologies reprogrammables, on peut citer :

- SRAM - (StaticRandom Access Memory) : pour cette technologie, les connexions sont réalisées en rendant les transistors passants ce qui permet une reconfiguration rapide du circuit FPGA.
- EPROM (UVPROM) - (Erasable Programmable Read-Only Memory): peuvent être effacés (et reprogrammés) par exposition aux rayons ultra-violets.
- EEPROM - (Electrically Erasable Programmable Read-Only Memory): peuvent être effacés et reprogrammés à volonté par source électrique.
- Flash - (Flash-erase EPROM) : mêmes propriétés qu'EEPROM avec une densité supérieure (donc avec un coût inférieur pour une complexité donnée).
- Fusible : programmables une seule fois. Technologie bipolaire.
- Anti-fusible : ne sont programmables qu'une seule fois.

Le tableau 4.1 montre les différents avantages et inconvénients de chaque technologie [8] :

| Technologie | Avantages | Inconvénients |
|---|---|---|
| SRAM | Reprogrammation rapide | Nécessite d'une grande surface |
| EPROM | Reprogrammable à volonté | Nécessite d'une grande surface UV pour la programmation |
| EEPROM | Reprogrammable à volonté électriquement | - |
| Flash | Sauvegarde le programme en cas de coupure de l'alimentation | Nombre de reconfigurations limité |
| Fusible | / | Reprogrammable une seule fois |
| Anti-fusible | Reprogrammable à volonté | - |

**Tableau 4.1 :** Avantages et inconvénients des technologies FPGA.

## 4.3 Plate- forme de développement Virtex-5 :

### 4.3.1 Caractéristiques et périphériques :

La carte FPGA Virtex-5 a plusieurs caractéristiques et périphériques à savoir :

- Référence : Virtex-5 FPGA XC5VLX50-1FFG676.
- Puce de générateur d'horloge programmable du système.
- Horloge de fréquence 100 MHz.
- Commutateurs DIP à usage général, voyants et boutons poussoirs.
- Codec audio stéréo AC97 avec line- in, line-out, 50mW casque, entrée microphone, et SPDIF prises audio numérique.
- Port série RS-232.
- Ecran LCD 2 lignes x 16 caractères.
- Connecteur vidéo DVI (VGA pris en charge avec l'adaptateur fourni).
- Connecteurs de souris et claviers PS/2.

- Contrôleur de configuration système AC™ avec CompactFlash Type I CompactFlash connecteur.
- SRAM synchrone ZBT, 9 Mb sur le bus de données 32 bits avec quatre bits de parité
- Intel P30 StrataFlash ® linéaires puces de mémoires flash (32Mo)
- Serial peripheral interface ™ (SPI) Flash (2Mo)
- Connecteur RJ45 Ethernet.
- Puce d'interface USB avec ports hôtes et périphériques [9].

### 4.3.2 Stéréo AC97 audio codec :

La carte FPGA contient un codec AC97 (U16) qui permet le traitement audio. Un dispositif AD1981 Codec audio prend en charge l'audio stéréo 20 bits avec jusqu'à 48 kHz échantillonnage. Le taux d'échantillonnage pour l'enregistrement et la lecture peut être différent.

Des prises Jacks audio séparées sont prévues pour Microphone, Line In, Line Out et casque. Toutes les prises Jacks audio sont stéréo, sauf le microphone. La prise jack audio du casque est contrôlée par le code audio d'amplificateur interne de 50mW. Une prise SPDIF fournit la sortie audio numérique du codec.

Remarque : La remise à zéro pour le codec AC97 est partagée avec le signal de remise à zéro pour les puces de mémoire flash et est conçu pour être actif à la mise sous tension ou à la réinitialisation du système [9].

Les figures 4.2 et 4.3 présentent la plateforme de développement Virtex-5 [16] :


**Figure 4.2 :** Plateforme de développement Virtex-5 (vu de haut).


**Figure 4.3 :** Plateforme de développement Virtex-5 (vu de bas).

## 4.4 Processus d'implémentation:

La conception des architectures de commande s'effectue en utilisant les outils de Conception Assistée par Ordinateur (CAO).La saisie est effectuée graphiquement ou via un langage de description matériel de haut niveau, nommé également langage HDL (Hardware Description Language). Deux langages HDL sont les plus couramment utilisés, à savoir le VHDL (Very high speed integrated Hardware Description Language) et le Verilog. Ces deux langages sont standardisés et offrent au concepteur différents niveaux de description, et surtout l'avantage d'être portables et compatibles avec toutes les technologies FPGA précédemment introduites. La figure 4.4 résume les différentes étapes de programmation d'un FPGA.

Le synthétiseur des outils CAO génère dans un premier temps une Netlist qui décrit la connectivité de l'architecture. Puis l'outil de placement-routage place de façon optimale tous les composants et effectue le routage entre les différentes cellules logiques. Ces deux étapes permettent de générer un fichier de configuration à télécharger dans la mémoire de configuration du FPGA. Ce fichier est appelé Bitstream et peut être directement chargé sur FPGA à partir d'un ordinateur hôte [9].

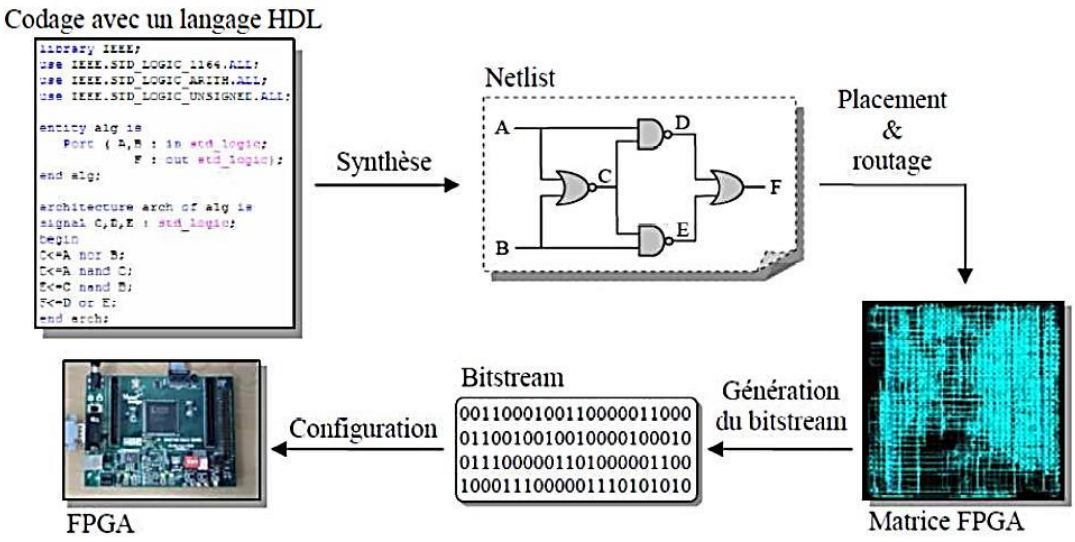



**Figure 4.4** : Programmation d'un FPGA [9].

### 4.4.1 Présentation du logiciel ISE :

Le logiciel Xilinx ISE est un logiciel de description, de simulation et de programmation de circuits et systèmes numériques sur des composants programmables. Le logiciel ISE permet :

- La description de circuits numériques sous forme de schémas logiques, de machines à état finis ou en langages de description matérielle (VHDL, Verilog, ABEL) ;
- La compilation, la simulation comportementale ;
- La synthèse, le placement routage et l'implémentation ;
- La simulation temporelle et l'analyse de timing ;
- La programmation sur les circuits programmables de Xilinx (CPLD et FPGA)[8].

La figure 4.5 représente l'interface Project Navigator de l'ISE 14.2 permettant l'accès à toutes les ressources d'un projet ainsi qu'aux outils de l'implémentation.

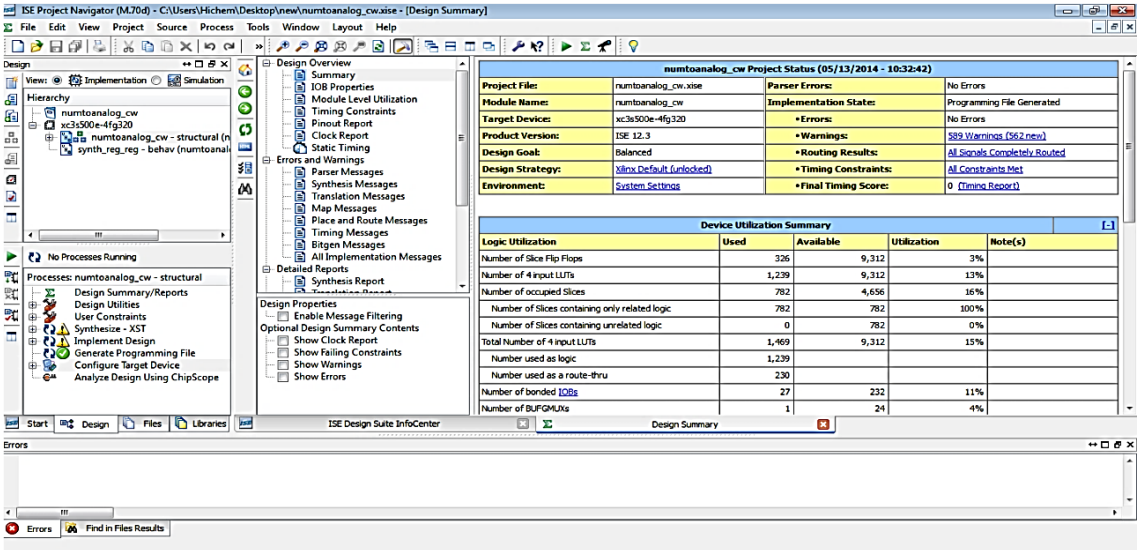



**Figure 4.5 :** L'interface Project Navigator de l'ISE 14.2.

### 4.4.2 Présentation du logiciel de simulation ModelSim:

ModelSim est un logiciel de simulation pour les langages HDL tel que le VHDL, développé par Mentor Graphique. C'est un outil informatique permettant de compiler

un code VHDL et en introduisant les TestBenchs, il permet de simuler le code et de le debugger en cas de dysfonctionnement.

La figure 4.6 illustre l'interface graphique de ModelSim. C'est une interface qui permet de visualiser les simulations dans une fenêtre appelée WAVE. Le programme permet aussi l'exportation des formes d'ondes pour visualisation indépendamment du programme ou sur un support papier [10].

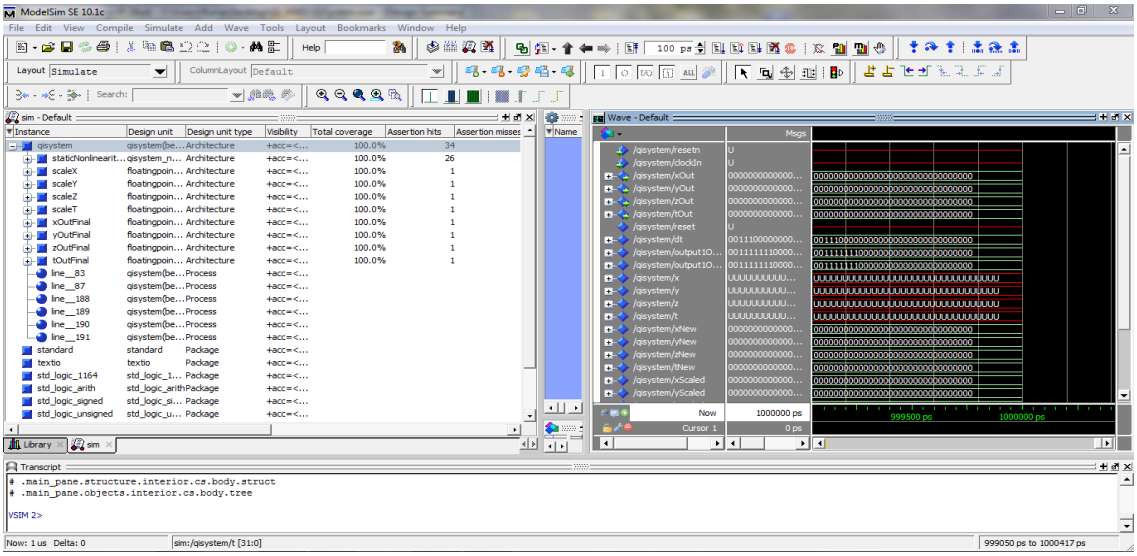


**Figure 4.6 :** Interface graphique du logiciel ModelSim de Mentor Graphics.

## 4.5 Réalisation expérimentale de l'implémentation :

Afin de réaliser l'implémentation expérimentale de notre système hyper chaotique de Qi, nous avons suivis les étapes suivantes :

- **Etape 1 :** la création du programme VHDL sur logiciel ISE.
  - ✓ effectuer une opération de synthèse pour vérifier le bon fonctionnement du montage.
  - ✓ générer le Bitstream en cliquant sur Generate Programming File.
- **Etape 2 :** La simulation avec logiciel ModelSim en introduisant le TestBench.
- **Etape 3 :** Implémentation de l'émetteur hyper chaotique de Qi sur carte FPGA **virtex-5.**

Les photos de la figure 4.7 montrent l'environnement de la réalisation expérimentale de l'implémentation sur carte FPGA **virtex-5** :

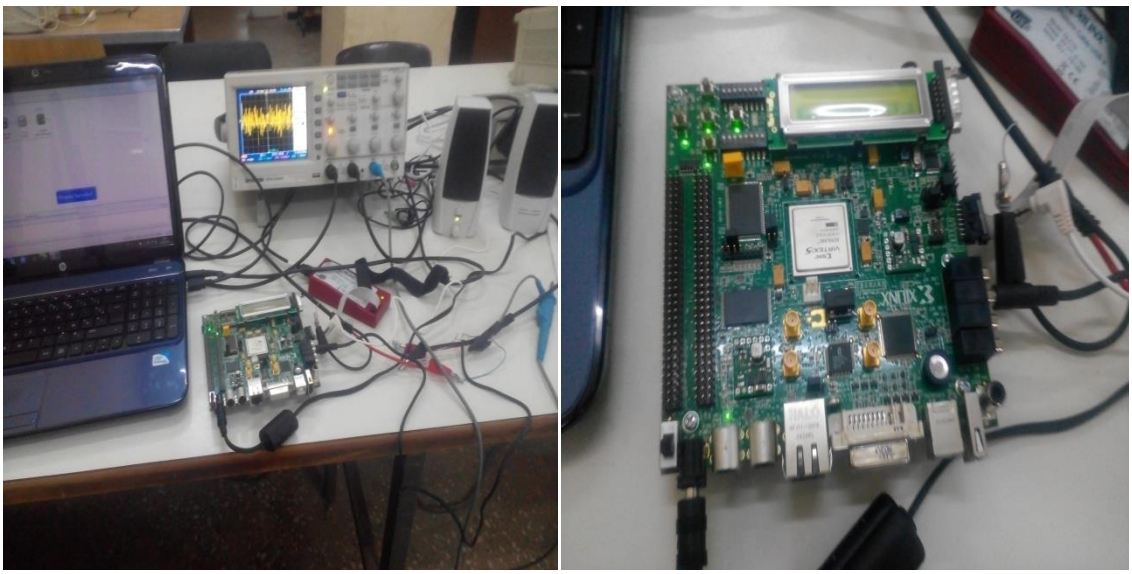


**Figure 4.7 :** Réalisation expérimentale de l'implémentation.

### 4.5.1 Programmation en VHDL :

Dans cette étape, nous avons écrit le programme VHDL en utilisant les blocs IP(CORE Generator & Architecture Wizard ) en particulier les blocs Math Functions Figure 4.8 pour écrire les équations de système hyper chaotique de Qi. L'implémentation a été faite en virgule flottante.

Nous rappelons les équations de l'émetteur hyper chaotique de Qi obtenues dans le chapitre 2 :

$$\begin{cases} \frac{dx_1}{dt} = \mathbf{a}(x_2 - x_1) + x_2 x_3 \\ \frac{dx_2}{dt} = \mathbf{b}(x_1 + x_2) - x_1 x_3 \\ \frac{dx_3}{dt} = -\mathbf{c}x_3 - \mathbf{e}x_4 + x_1 x_2 \\ \frac{dx_4}{dt} = -\mathbf{d}x_4 + \mathbf{f}x_3 + x_1 x_2 \end{cases} \quad (4.1)$$

Où $x_1$ , $x_2$ , $x_3$ , $x_4$ sont des variables d'état, et $\mathbf{a}$, $\mathbf{b}$ , $\mathbf{c}$ , $\mathbf{d}$ , $\mathbf{e}$ , $\mathbf{f}$ sont des paramètres positifs du système.

Lors de la création des équations de notre émetteur hyper chaotique de Qi, on a utilisé l'approximation d'Euleur pour la fonction d'intégration :

$$\frac{dx}{dt} = f'(x) = \frac{\Delta x}{\Delta t} = \dot{x} = \frac{x_{n+1} - x_n}{\Delta t} \quad (4.2)$$

$$x_{n+1} = \Delta t\, f'(x) + x_n \quad (4.3)$$

Où $\Delta t$: représente le pas d'intégration.

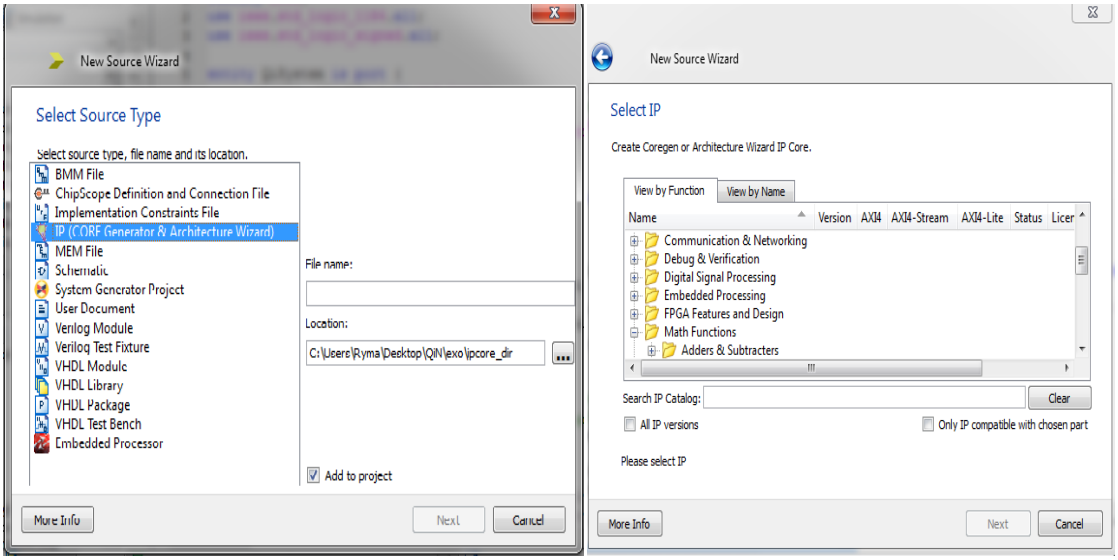



**Figure 4.8:** Interface IP(CORE Generator & Architecture Wizard).

La figure 4.9 représente l'exemple d'un bloc d'addition.

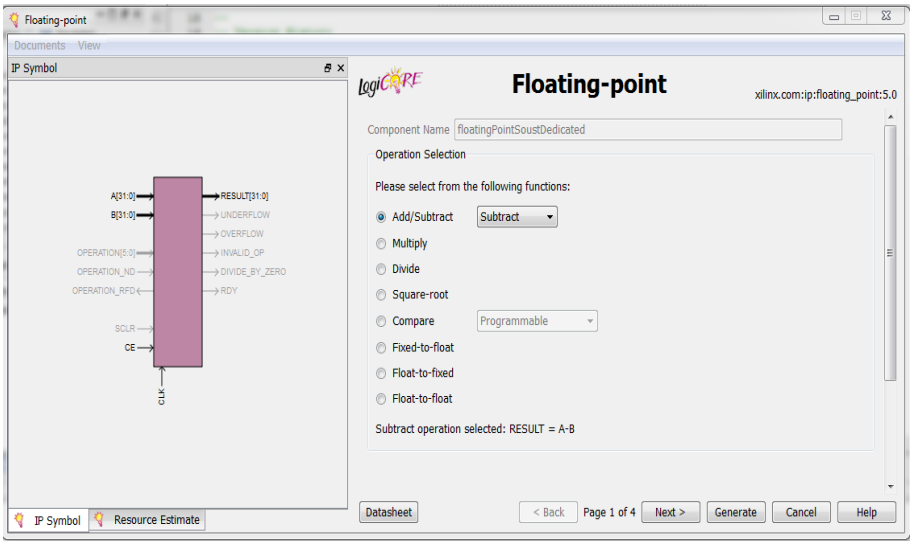



**Figure 4.9 :** Exemple d'un bloc d'addition.

- **Le convertisseur**

Le convertisseur utilisé dans notre projet est le convertisseur du codec AC97 de résolution 20 bits interne sur la carte FPGA **Virtex-5**.La conversion se fera comme suit :

Les données à convertir sont recueillies à partir de la carte FPGA. Les signaux de sorties du système réalisé ( $x_1, x_2, x_3, x_4$ ) de format 20 bits vont subir une conversion numérique analogique.

Après la création du programme VHDL sous le logiciel ISE, on effectue une opération de synthèse pour vérifier le bon fonctionnement du montage et on génère le « Bitstream » en cliquant sur « Generate Programming File ».

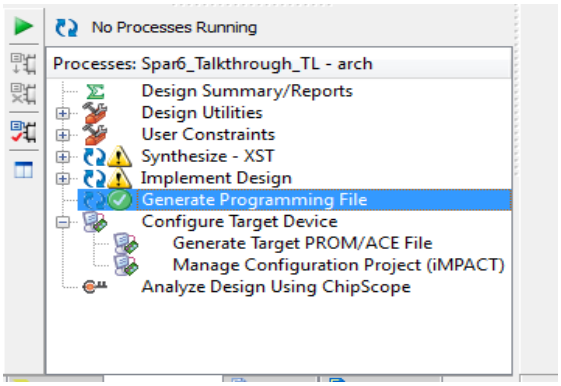



**Figure 4.10 :** La fenêtre pour la synthèse.

### 4.5.2 Simulation avec le logiciel ModelSim :

Dans cette deuxième étape, on a généré un fichier TestBench qui permet de simuler le code VHDL et de le debugger en cas de dysfonctionnement.

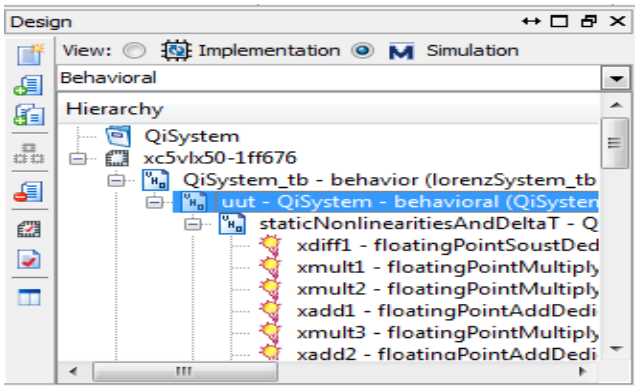



**Figure 4.11 :** La fenêtre pour le TestBench.

Après la simulation du système de Qi sous ModelSim, on a pu visualiser dans une fenêtre appelée WAVE les signaux du système de Qi Figure 4.12:

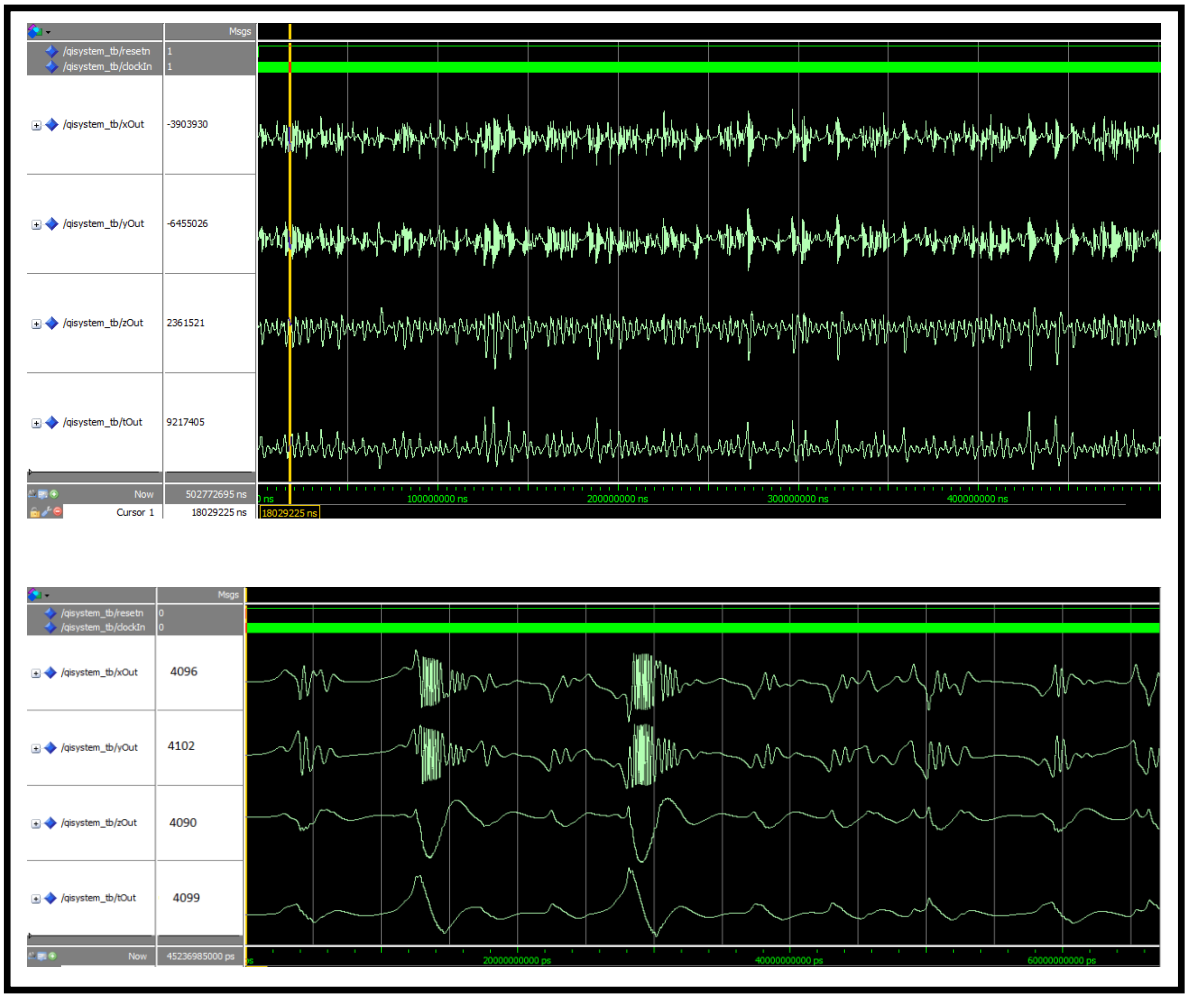



**Figure 4.12 :** La représentation graphique des signaux du système de Qi.

### 4.5.3 Implémentation du système hyper chaotique de Qi :

Après avoir synthétisé et généré notre projet, on a réussi à visualiser les signaux de sortie ( $x_1, x_2, x_3, x_4$ ) grâce au logiciel ModelSim ce qui implique le bon déroulement de l'implémention. On va implémenter notre système dans la carte FPGA **Virtex-5** ; pour cela nous allons connecter cette dernière par câble USB, Ensuite on clique sur « configure Target Device ». Une fenêtre s'ouvre permettant d'implémenter notre projet dans la carte FPGA **virtex-5** : on clique sur bouton droit « initialize chain »puis sur « program » Figure 4.13.

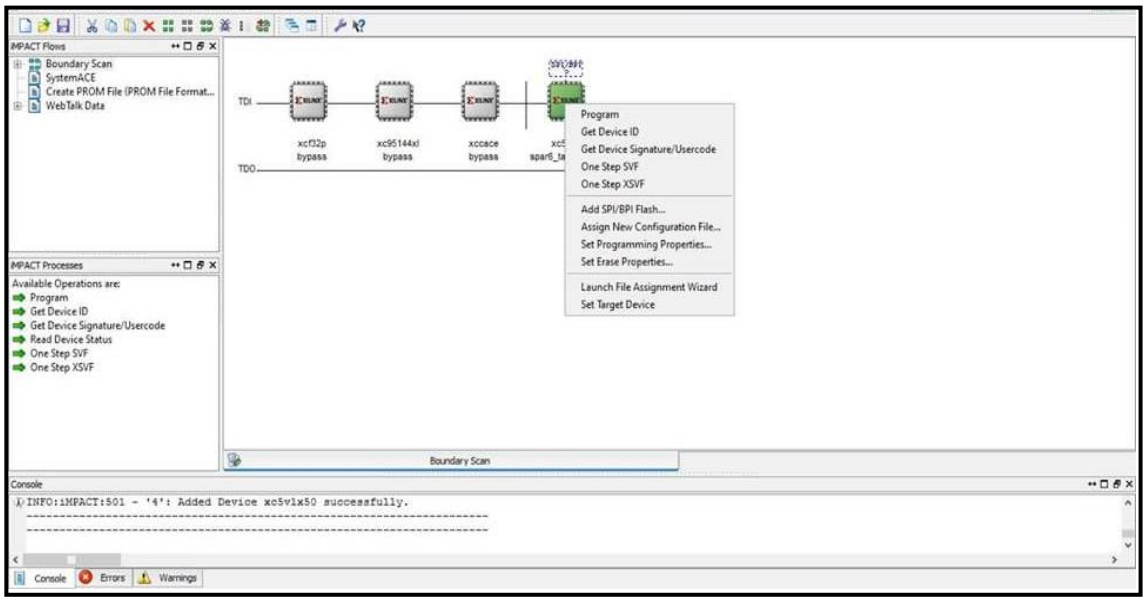



**Figure 4.13 :** Interface permettant la programmation du FPGA.

### 4.5.4 Visualisation des signaux :

Les figures de 4.14 à 4.23 montrent les différents oscillogrammes relevés au niveau de la carte FPGA et les signaux obtenus par la simulation.

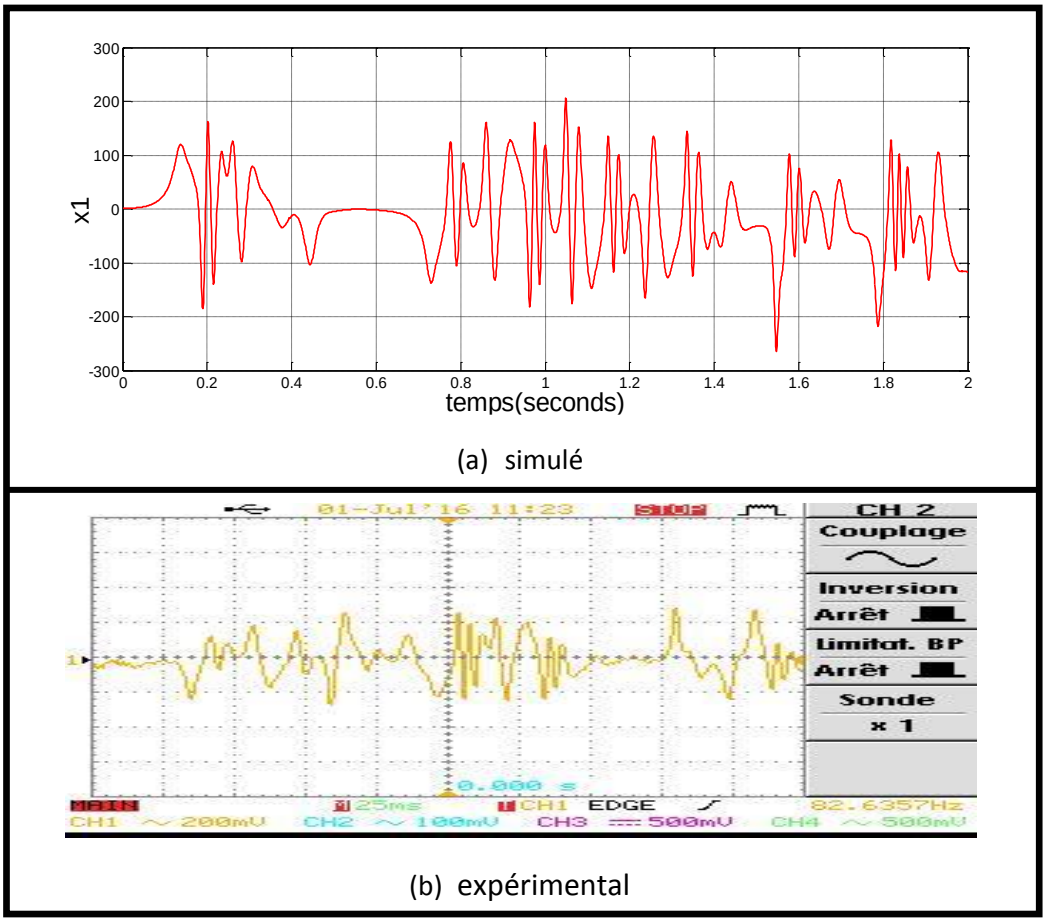
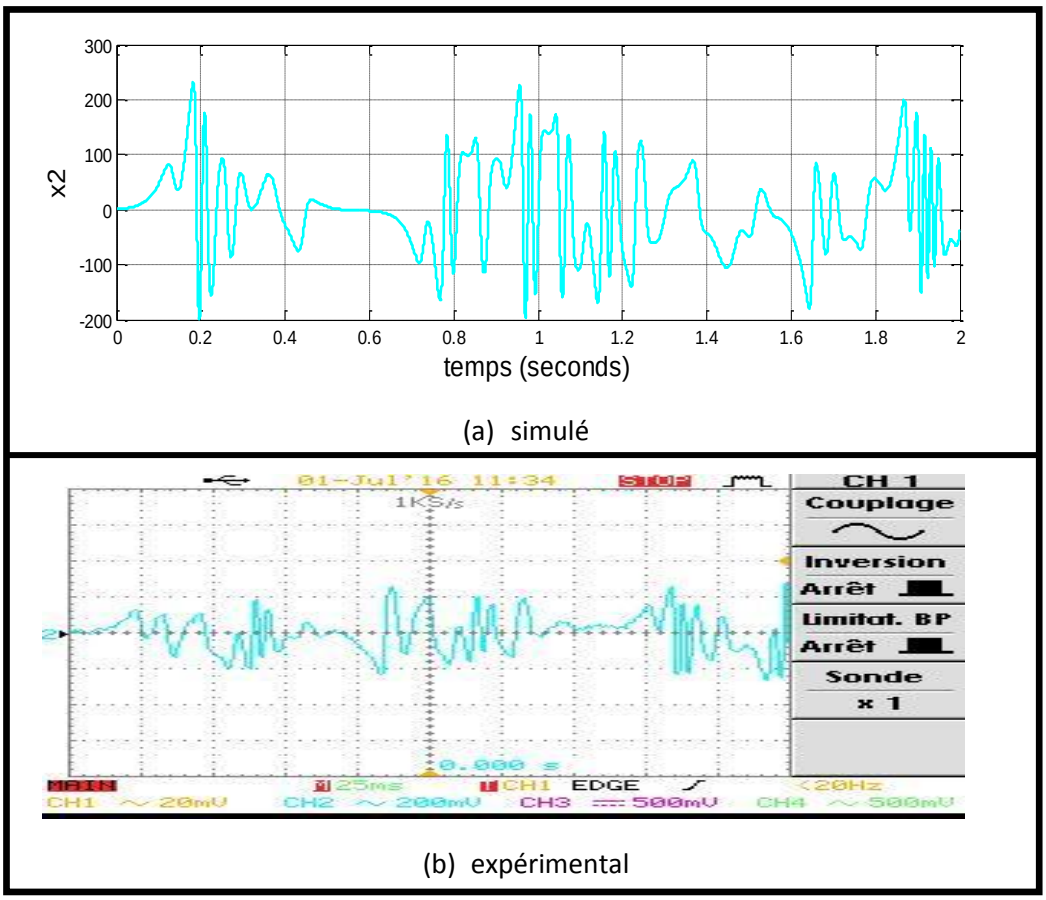


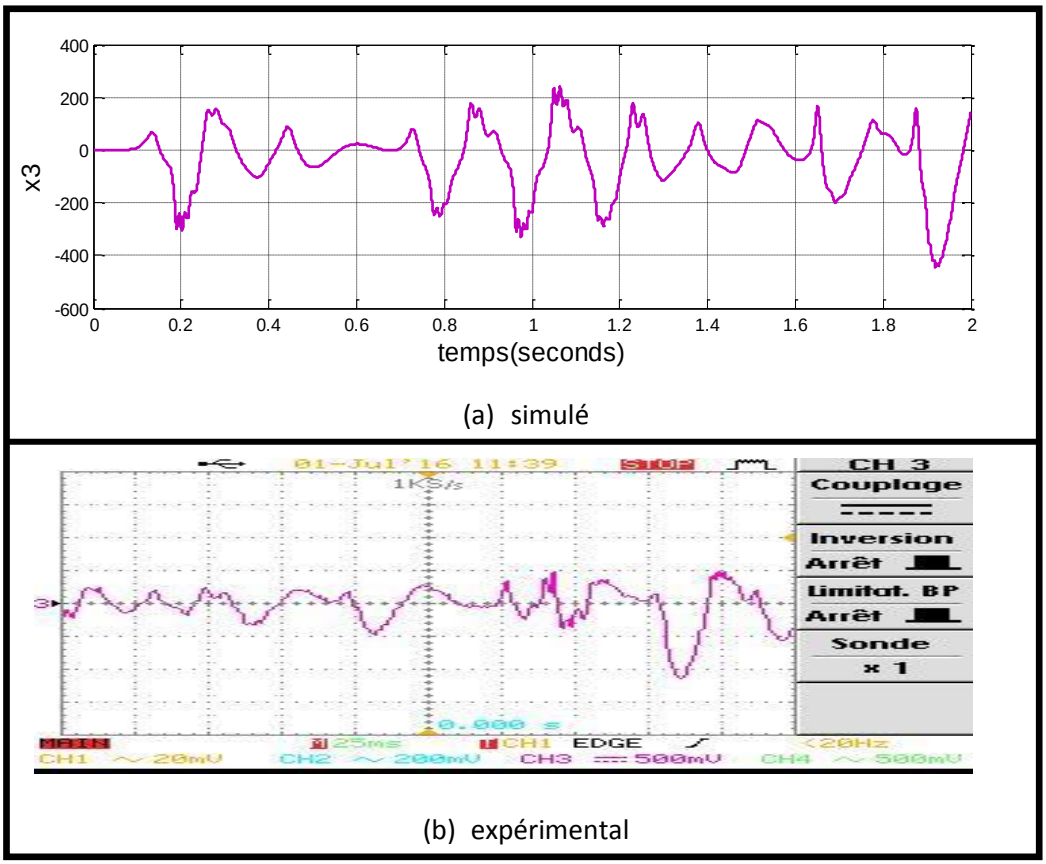

**Figure 4.14 :** L'état $x_1$ en fonction du temps (a) simulé (b) expérimental.




(a) simulé

(b) expérimental

**Figure 4.15 :** L'état $x_2$ en fonction du temps (a) simulé (b) expérimental.




(a) simulé

(b) expérimental

**Figure 4.16 :** L'état $x_3$ en fonction du temps (a) simulé (b) expérimental.

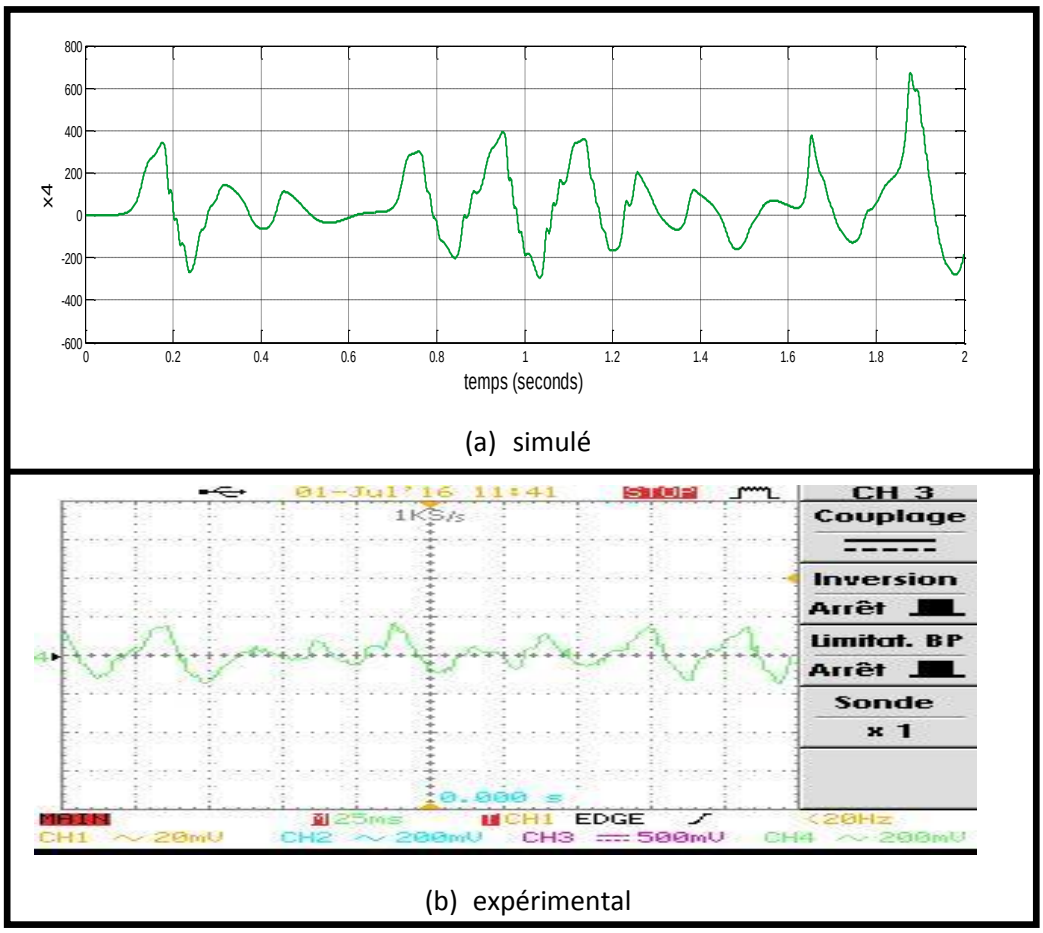
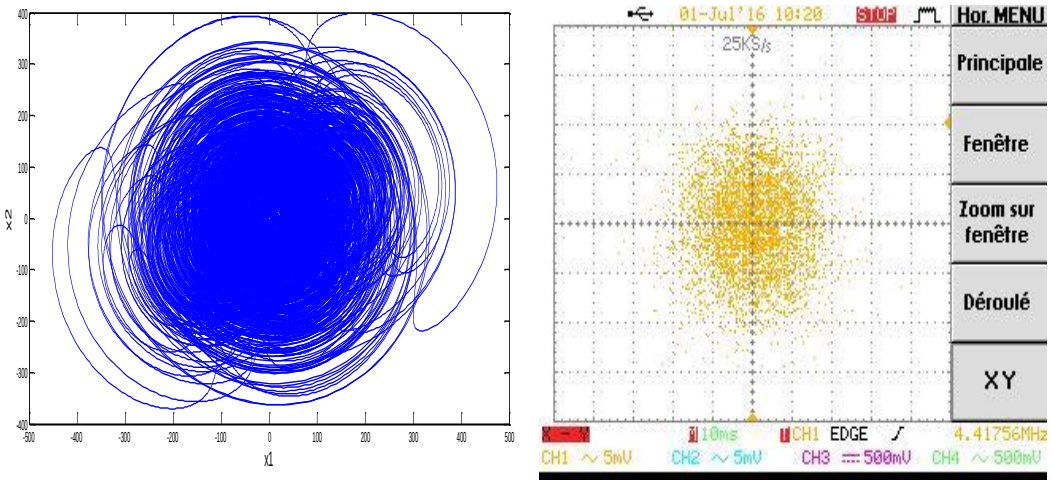
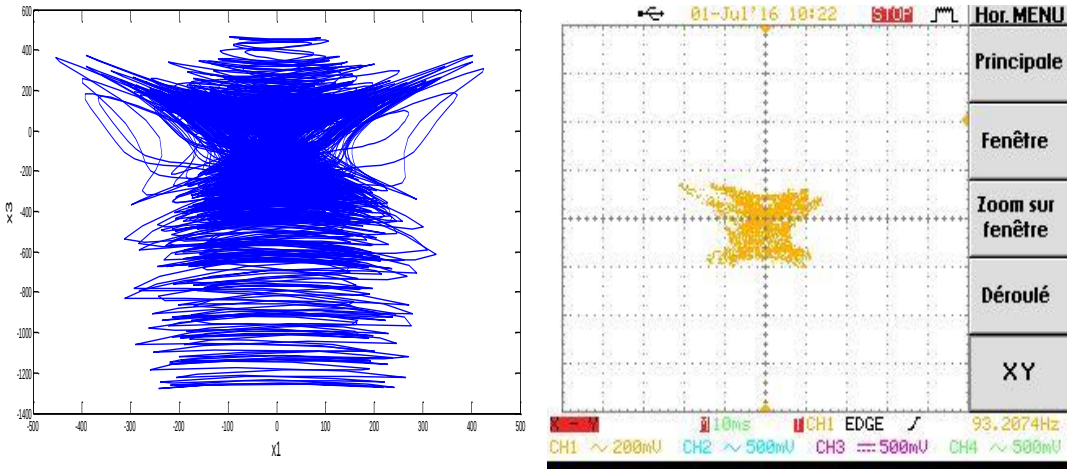



**Figure 4.17 :** L'état $x_4$ en fonction du temps (a) simulé (b) expérimental.



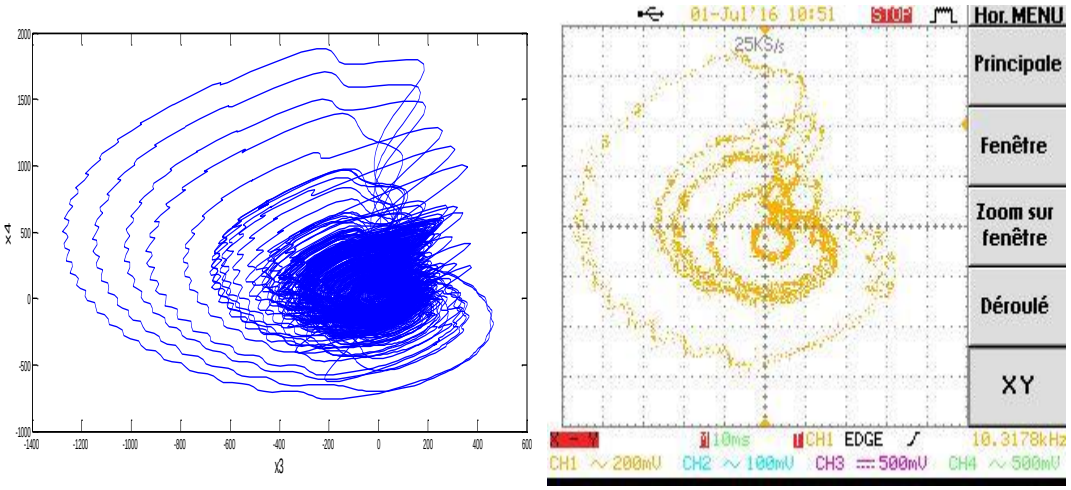

(a) (b)

**Figure 4.18 :** Plan de phase $x_2$ en fonction de $x_1$ (a ) simulé (b) expérimental.



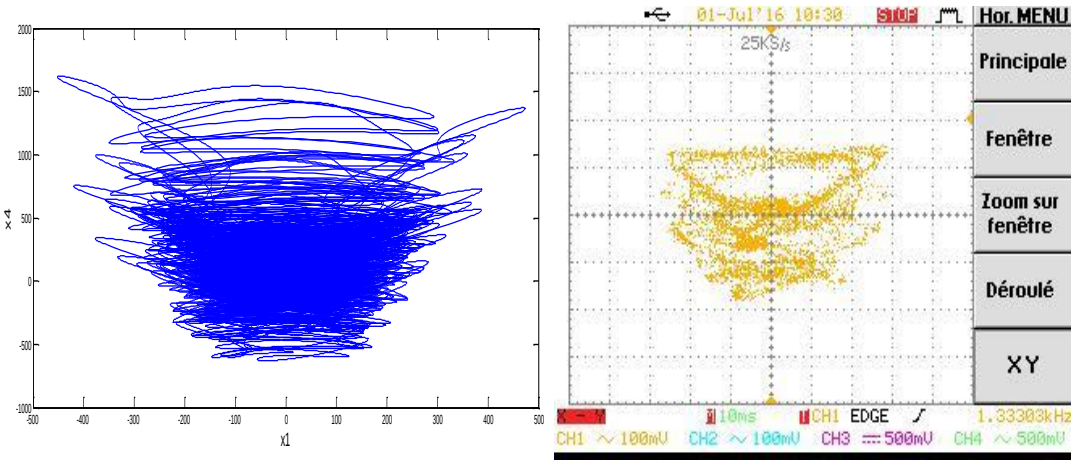

(a) (b)

**Figure 4.19 :** Plan de phase $x_3$ en fonction de $x_1$ (a) simulé (b) expérimental.



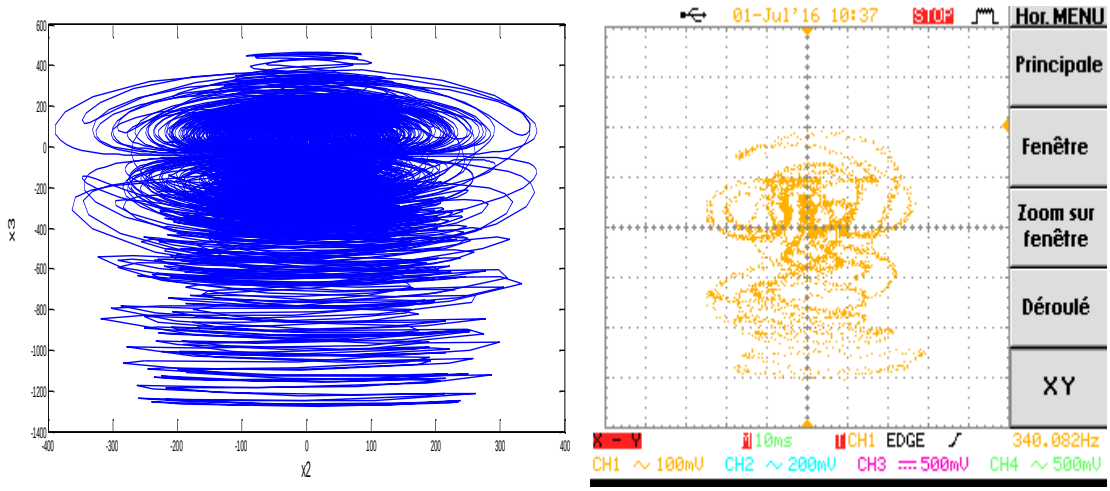

(a) (b)

**Figure 4.20 :** Plan de phase $x_4$ en fonction de $x_3$ (a) simulé (b) expérimental.



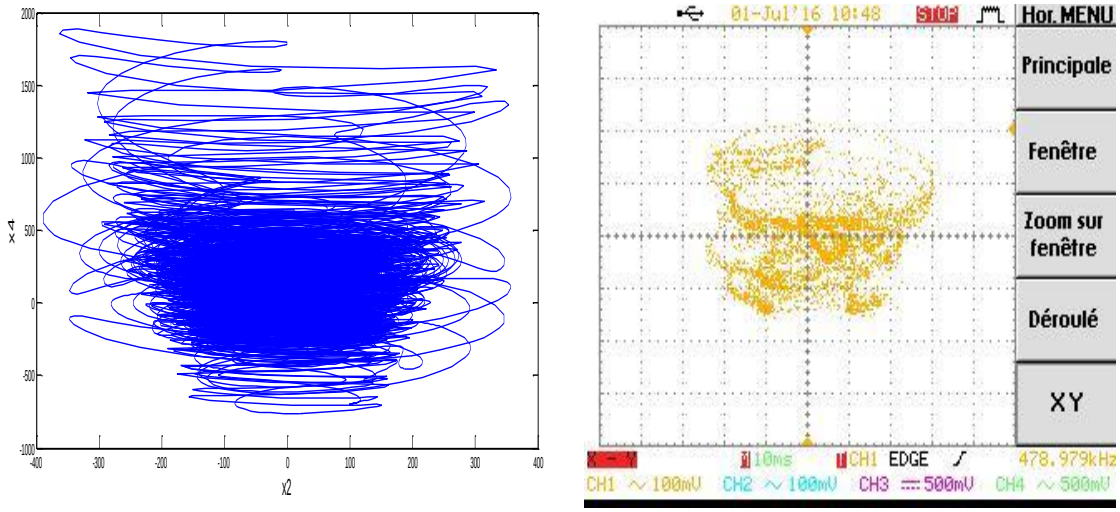

(a) (b)

**Figure 4.21 :** Plan de phase $x_4$ en fonction de $x_1$ (a) simulé (b) expérimental.




(a) (b)

**Figure 4.22 :** Plan de phase $x_3$ en fonction de $x_2$ (a) simulé (b) expérimental.




(a) (b)

**Figure 4.23 :** Plan de phase $x_4$ en fonction de $x_2$ (a) simulé (b) expérimental.

L'environnement ISE fournit un rapport d'implémentation sous forme de tableaux contenant les informations utiles liées au design. Le tableau 4.2 comptabilise toutes les ressources internes utilisées en nombre et en pourcentage.

| Spar6_Talkthrough_TL Project Status | | | |
|---|---|---|---|
| **Project File:** | AC_97Qi.xise | **Parser Errors:** | No Errors |
| **Module Name:** | Spar6_Talkthrough_TL | **Implementation State:** | Programming File Generated |
| **Target Device:** | xc5vlx50-1ff676 | **• Errors:** | |
| **Product Version:** | ISE 14.2 | **• Warnings:** | |
| **Design Goal:** | Balanced | **• Routing Results:** | All Signals Completely Routed |
| **Design Strategy:** | Xilinx Default (unlocked) | **• Timing Constraints:** | All Constraints Met |
| **Environment:** | System Settings | **• Final Timing Score:** | 0 (Timing Report) |

| Device Utilization Summary [-] | | | | |
|---|---|---|---|---|
| **Slice Logic Utilization** | **Used** | **Available** | **Utilization** | **Note(s)** |
| Number of Slice Registers | 17,597 | 28,800 | 61% | |
| Number used as Flip Flops | 17,597 | | | |
| Number of Slice LUTs | 15,200 | 28,800 | 52% | |
| Number used as logic | 13,936 | 28,800 | 48% | |
| Number using O6 output only | 8,480 | | | |
| Number using O5 output only | 2,010 | | | |
| Number using O5 and O6 | 3,446 | | | |
| Number used as Memory | 1,182 | 7,680 | 15% | |
| Number used as Shift Register | 1,182 | | | |
| Number using O6 output only | 1,182 | | | |

**Tableau 4.2 :** Ressources consommées par l'implémentation.

La figure 4.24 est un aperçu du circuit implémenté sur la carte FPGA **virtex-5** avec les routages et l'emplacement des ressources utilisées.

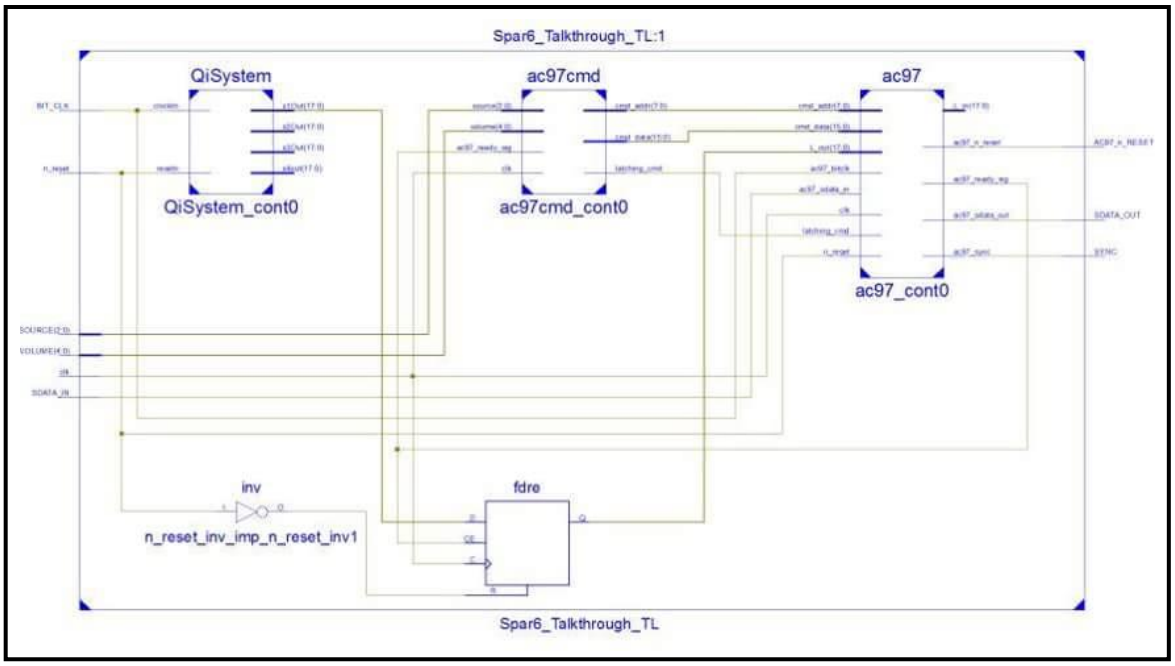



**Figure 4.24 :** Aperçu du circuit implémenté sur le FPGA virtex-5.

## 4.6 Conclusion :

L'objectif de ce chapitre a été l'implémentation sur carte FPGA de l'émetteur chaotique constitué de l'oscillateur hyper chaotique de Qi. Ainsi la simulation à l'aide de logiciel ModelSim nous a permis de visualiser les différents signaux du système. Une bonne concordance entre les signaux obtenus par simulation sous Simulink et ModelSim et les signaux expérimentaux relevés sur oscilloscope numériques au niveau de la carte FPGA virtex-5 a été observée.

# Conclusion générale

Dans ce mémoire, nous avons étudié un système de transmission chaotique basé sur le cryptage par modulation CSK. L'émetteur est construit autour de l'oscillateur de Qi qui présente des caractéristiques très intéressantes. Au niveau du récepteur, la démodulation est basée sur la synchronisation par boucle fermée pour la récupération du message.

Dans le premier chapitre, nous avons présenté un aperçu sur les systèmes dynamiques à temps continu et discret, leurs principales caractéristiques à savoir les différents types de bifurcation, la section de Poincaré, les exposants Lyapunov.etc…

Dans le deuxième chapitre nous avons étudié l'oscillateur de Qi et ses propriétés tels que sa stabilité et le calcul des points fixes. Nous avons utilisé MATLAB Simulink pour visualiser les différents signaux, le plan de phase et les attracteurs étranges de l'oscillateur.

Dans le troisième chapitre, l'insertion du message par modulation CSK a été développée .La démodulation chaotique au niveau du récepteur se fait par la synchronisation chaotique par boucle fermée pour la récupération du message. La simulation sous Matlab Simulink a été concluante sur deux types de messages : un message binaire (générateur de Bernoulli) et une image binaire. Récupérer le message émis crypté et de le décrypté au niveau de la réception**.**

Dans le quatrième chapitre, une implémentation de l'oscillateur chaotique de Qi sur circuit FPGA a été réalisée et les différents signaux obtenus sur oscilloscope numérique

sont en parfaite concordance avec ceux obtenus par simulation sous Matlab Simulink ou sous ModelSim. Sa reprogrammation quasi-instantanée offre la possibilité de régler en temps réel les paramètres d'un processus de transmission afin d'obtenir un schéma fonctionnel avant leur implémentation en circuit final.

Plusieurs perspectives peuvent être envisagées à la suite de ce travail, à savoir :

- Etude comparative par rapport à d'autres techniques de synchronisation chaotique.

- Evaluation du taux BER (Bit Error Rate) de notre transmission sécurisée par modulation CSK (Chaos Shift Keying).

# Bibliographie :


[1] Benhabib. Chouaib : " Etude d'un système chaotique pour la sécurisation des communications optiques ",Thèse de magister, Université Abou bekrbelkaid de Tlemcen, Algérie, juin 2014.

[2]J.Oden :" Le chaos dans les systèmes dynamiques", Rapport Université Paris XI, France, 2007.

[3] M$^{me}$Azib née Benzemam Djamila :" Systèmes chaotiques et hyperchaotiques pour la transmission sécurisée de données", Thèse de magister,Université Abou bekrbelkaid de Tlemcen, Algérie,

2009-2010.

[4] H. Dang-Vu, C.Delcarte : "Bifurcations et chaos : Introduction à la dynamique contemporaine avec des programmes en Pascal, Fortran et Mathématica", Ed. Ellipses, Paru en Septembre 2000.

[5] M. L. Chikhi : " Application des systèmes dynamiques chaotiques en transmission de données ", Thèse de Magister, Université Saad Dahlab, Blida, Algérie, 2012.

[6] A. Ali-Pacha[1]& N. Hadj-Said[1]&A. M'hamed[2]&A.Belghoraf[1] : "Chaos Crypto-Système basé sur l'Attracteur de Hénon-Lozi", Rapport ,Université des Sciences et de la Technologie d'Oran[1],Algérie, Institut National des Télécommunications[2], Evry France

[7] O. Megherbi : " Etude et réalisation d'un système sécurisé à base de systèmes chaotiques", Thèse de magister**,** Université Mouloud Mammeri Tizi-Ouzou, Algérie, 2013.

[8] M. A. Djenouri& M. H. Chikhi : "Communication sécurisée par chaos : Etude et implémentation sur carte FPGA", Thèse de Master 2, Université Saad Dahlab, Blida, Algérie, 2013-2014.

[ 9]S.A.Amine.Arous & A.Abeb : "Modulation chaotique appliquée en communications sécurisées **",**Thèse de Master 2 , Université Saad Dahlab, Blida, Algérie, 2014-2015.

[10] Toufik Nachef : "Implémentation d'une instrumentation sur un FPGA" **,** Thèse de Magister, Université Mouloud Mammeri, Tizi-Ouzou, Algérie,21 novembre 2011.

[11] D.Eddine Goumidi **:** "Fonction logistique et standard chaotique

pour le chiffrement des images satellitaires**",** Thèse de Magister, Université Mentouri de Constantine (UMC), Algérie, 2010.

[12] HOET Thomas & LORENZI Baptiste & SAHIN Serdar : "La cryptographie chaotique" **,** institut national des sciences appliquées de toulouse (INSA),France , 16 janvier 2012.

[13] A.Ridha Kihal: "Systèmes chaotiques pour la transmission sécurisée de données **",** Thèse de Magister, Université Mohamed Khider de Biskra, Algérie, 26 novembre 2013.

[14]http://chaos.pagesperso-orange.fr/lexique.htm.

[15]http://just.loic.free.fr/index.php?page=elem.

[16] http://www.ebay.com/itm/XILINX-Evaluation-Platform-VIRTEX-5- FPGA-ML501-/291478080894?_ul=BR.

[17] Dennis Luke Owuor[1] & Guoyuan Qi[2] : " Secure Communication Based On Qi Hyper-Chaos **"**, Article, Université de Technologie Tshwane de 0001 Pretoria, sud d'Afrique.