UNIVERSITE SAAD DAHLAB DE BLIDA

Faculté de Technologie

MEMOIRE DE MAGISTER

En Electronique

Spécialité : Communication

Application des systèmes dynamiques chaotiques en transmission de données

Présenté par :

CHIKHI Mohamed Lazhar

Devant le jury composé de :

M. BOUNEKHLA	Professeur, Université de Blida	Président
K .BENMANSOUR	Maître de conférences A, Université de Médéa	Examinateur
M. HADJ SADOK	Maître de conférences A, Université de Blida	Examinateur
A. FERDJOUNI	Maître de conférences A, Université de Blida	Promoteur

Blida, Juin 2012

ملخص

في هذا العمل يتم تقديم نظام للإرسال الآمن للمعلومات قائم على اساس التزامن بين نظامين فوضويين. الباعث هو عبارة عن مذبذب من النوع colpitts يتم فيه إدراج الرسالة باستخدام اسلوب الإحتواء. يتم بث فقط حالة واحدة من حالات الباعث إلى المستقبل عن طريق قناة عامة. هذا الأخير هو عبارة عن مراقب يعمل خطوة بخطوة لإعادة بناء جميع حالات الباعث. و نحصل بذلك على تزامن النظامين الفوضويين (باعث – مستقبل) و في نفس الوقت يتم استرجاع الرسالة. يتم عرض نتائج المحاكاة و المحاكاة المشتركة في بيئة Matlab Simulink-Xilinx System Générator كما يتم تنفيذ تطبيق نظام ارسال فوضوي في دارة FPGA مع عرض نتائج التجارب.

Résumé

Dans ce travail, un système de transmission sécurisée d'information basé sur la synchronisation de deux systèmes chaotiques est présenté. L'émetteur est un oscillateur de type Colpitts chaotique dans lequel le message est inséré à l'aide de la méthode dite par inclusion. Seulement un des états de l'émetteur est transmis au récepteur via un canal public. Ce dernier est un observateur à modes glissants fonctionnant étape par étape conçu pour reconstruire tous les états de l'émetteur. Ainsi, la synchronisation des deux systèmes chaotiques (émetteur - récepteur) est obtenue et le message est récupéré. Les résultats de simulation et de co-simulation sous environnement Matlab Simulink-Xilinx SystemGénérator sont présentés et une implémentation de l'ensemble du système de transmission chaotique sur circuit FPGA est réalisée avec une présentation des résultats expérimentaux.

Abstract

In this work, a secure information transmission system based on chaotic systems synchronization is proposed. The transmitter is a chaotic Colpitts oscillator in which the message to be transmitted is inserted using the inclusion method. Only one state of the transmitter is passed on via a public channel to the receiver. This latter is a sliding mode observer running step by step to rebuild all the states of the emitter. The synchronization of the two chaotic systems (transmitter-receiver) is therefore achieved and the message is recovered. Simulation and co-simualtion results obtained using the Matlab/Simulink and the Xilinx System Generator environments are presented and an implementation of the transmission system on FPGA is described along with some experimental results.

REMERCIEMENTS

Je tiens tout d'abord à remercier M. Ferdjouni Abdelaziz de m'avoir encadré. Son expérience et ses conseils ont beaucoup contribué à l'aboutissement de ce travail.

Mes remerciements vont également à MM. Bounekhla M'hamed, Benmansour Khelifa et Hadj Sadok M'hamed qui m'ont fait l'honneur de participer au jury de ma soutenance.

Je remercie aussi mes collègues du laboratoire LABSET et du département d'électronique de l'université de Blida qui m'ont permis de réaliser ce travail dans de très bonnes conditions.

Enfin, je remercie mon épouse et mes enfants pour leur soutien et leurs encouragements tout au long de la préparation de ce mémoire.

Table des matières

LISTE DES ILLUSTRATIONS, GRAPHIQUES ET TABLEAUX

INTRODUCTION

La cryptographie joue un rôle important dans la sécurité et la fiabilité des systèmes de transmission de données, surtout avec le développement des nouvelles techniques de communication. Ainsi, les utilisateurs ont besoin d'authentifier et de protéger des données sensibles dans leurs ordinateurs et de garantir la confidentialité des transactions sur des réseaux publics tels que l'Internet. En général, un crypto-système doit considérer plusieurs aspects tels que l'intégrité des données, l'authentification, l'autorisation, la confidentialité, et bien d'autres.

Les techniques de cryptographie classiques sont basées sur la théorie des nombres et en particulier sur la décomposition d'un entier en éléments simples. Nous pouvons ainsi citer les deux algorithmes bien connus : DES (Data Encryption Standard) et RSA (dont le nom est formé des initiales de ses inventeurs :R. Rivest, A. Shamir et L. Adleman). Néanmoins, avec la révolution de l'informatique, ces algorithmes s'avèrent peu sécurisés.

Depuis quelques années, la théorie des systèmes non linéaires et surtout chaotiques a été appliquée à la cryptographie afin de proposer d'autres méthodes de chiffrement. En 1990, T. Pecora et L. Carroll ont réussi à reproduire de manière exacte un signal électrique en synchronisant deux signaux chaotiques. Cette découverte de la synchronisation des signaux chaotiques a permis d'utiliser le chaos comme moyen de modulation de l'information. En effet, les propriétés des systèmes chaotiques (spectre continu et sensibilité aux conditions initiales) font de ces systèmes de bons outils pour la transmission sécurisée de données. De nombreux schémas sont proposés afin d'appliquer les systèmes chaotiques dans le domaine de la cryptographie.

Il est bien connu que les systèmes de communication traditionnels comportent deux parties appelées émetteur et récepteur. Le signal de sortie de l'émetteur est modulé puis transmis par le canal public au récepteur qui démodule le signal reçu afin de récupérer le signal original.

Pour la cryptographie chaotique, un des concepts les plus importants de la démodulation est la synchronisation, c'est à dire que le récepteur essaie de reconstruire les états de l'émetteur à partir du signal transmis considéré comme la sortie du système à observer, et ensuite de récupérer le message crypté considéré comme une entrée inconnue. Du point de vue automatique, cette technique peut être classifiée dans le domaine de la conception d'observateurs. Différents types d'observateurs sont alors proposés pour les systèmes chaotiques ainsi que pour les systèmes chaotiques à entrée inconnue. Certains de ces observateurs sont destinés uniquement à la reconstruction des états de l'émetteur, et d'autres à la récupération de l'information (entrée inconnue) en plus de la synchronisation des états. Le fonctionnement correct de ces observateurs dépend de plusieurs conditions dont la condition de recouvrement d'observabilité et de l'inversibilité à gauche du système ; ces conditions permettent de retrouver les états chaotiques et l'information noyée dans le système à partir de sa sortie et de ses dérivées.

Dans ce travail, nous avons conçu un système de communication basé sur la synchronisation de systèmes chaotiques à l'aide d'observateurs. L'émetteur chaotique est construit autour de l'oscillateur de Colpitts et le récepteur est constitué d'un observateur à modes glissants afin de reconstruire les états de l'émetteur et de récupérer le message. Le système de transmission chaotique sera ensuite implémenté sur circuit FPGA. Les différents signaux reconstruits au niveau du récepteur et en particulier le message seront visualisés sur oscilloscope numérique et ce grâce à une carte de conversion analogique-numérique (pour l'inclusion du message) et numérique-analogique (pour la visualisation). Une co-simulation hardware sous les environnements Matlab-Simulink et SystemGenerator-Xilinx nous permettra de comparer les signaux obtenus sous simulation et ceux provenant de la carte FPGA et de valider le bon fonctionnement du système de communication.

Ce mémoire est organisé de la façon suivante :

Le chapitre 1 présente des définitions importantes concernant les systèmes non linéaires et les systèmes chaotiques. Ces définitions seront utilisées pour la conception de l'émetteur chaotique.

Dans le chapitre 2, après une présentation des différentes méthodes de transmission d'information à l'aide de signaux chaotiques, la structure de l'émetteur

chaotique construite autour de l'oscillateur de Colpitts est analysée et son comportement en fonction des variations de ses paramètres est étudié. La méthode d'inclusion du message est ensuite présentée.

Le chapitre 3 est consacré aux différentes méthodes de synchronisation chaotique et à la synthèse du récepteur chaotique utilisant un observateur à modes glissants pour la récupération du message.

L'implémentation de l'ensemble émetteur chaotique – récepteur chaotique sur circuit FPGA ainsi que la vérification expérimentale pour la récupération du message sont présentées dans le chapitre 4.

Enfin, la conclusion reprend les principaux points abordés dans ce manuscrit et expose certaines perspectives d'approfondissement et d'élargissement pour notre travail.

CHAPITRE 1

SYSTEMES DYNAMIQUES CHAOTIQUES

1.1 Introduction

Les systèmes dynamiques chaotiques sont depuis longtemps connus dans le domaine des mathématiques, mais c'est seulement au cours des deux dernières décennies que les applications concrètes se sont multipliées. Notre étude se focalise sur l'usage du chaos pour la transmission sécurisée de l'information. Dans cette perspective, ce chapitre est destiné tout d'abord à l'étude des systèmes dynamiques chaotiques. Les résultats fondamentaux qui y sont exposés peuvent être trouvés, parmi les nombreux ouvrages sur les systèmes non linéaires dans [1] [2] [3] et plus particulièrement pour les systèmes chaotiques dans [4].

Après quelques rappels sur les systèmes dynamiques autonomes et non autonome, les différents types de points fixes selon leur stabilité sont définis. Les méthodes directe et indirecte de Lyapunov permettant de tester la stabilité des systèmes dynamiques non linéaires sont exposées. La notion de chaos est ensuite introduite, ainsi que la description des différents types d'attracteurs et des bifurcations qui peuvent apparaitre dans l'évolution de tout système dynamique. Nous terminons ce chapitre par le calcul des exposants de Lyapunov permettant de caractériser le comportement chaotique d'un système et par la présentation de quelques systèmes chaotiques.

1.2 Définitions

Un système dynamique non linéaire est défini par une équation différentielle :

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

où : $x \in U \subseteq \mathbb{R}^n$ est un vecteur de dimension n représentant l'état du système et $u \in V \subseteq \mathbb{R}^p$ représente l'entrée du système. $\mathbb{R}^n$ est appelé l'espace des phases et $\mathbb{R}^p$ l'espace des paramètres. Cette équation est en général associée à une autre équation désignant le vecteur de sortie :

$$y = h(t,x,u) \tag{1.2}$$

Un système dynamique non linéaire est dit autonome lorsqu'il ne dépend pas explicitement du temps. Un système autonome est décrit par les équations suivantes :

$$\begin{cases} \dot{x} = f(x,y) \\ \dot{y} = g(x,y) \end{cases} \tag{1.3}$$

On peut toujours transformer un système autonome en un système non autonome par un changement de variables.

1.2.1 Flot et espaces de phase

On considère le système autonome suivant :

$$\dot{x} = \frac{dx}{dt} = f(x) \ , \ x \in \mathbb{R}^n \ , \ f \in C^r(U) \ , \ U \subseteq \mathbb{R}^n \tag{1.4}$$

Définition 1.1 : Soit $x(x_0,t),\ x_0 \in D$, une solution de (1.4) avec comme conditions initiales $x(0) = x_0$. On appelle flot de (1.4), ou du champ de vecteurs f, l'application $\phi_t : D \to \mathbb{R}^n$ définie par :

$$\phi_t(x_0) = x(x_0,t) \tag{1.5}$$

$\phi_t(x_0)$ possède les propriétés suivantes :

(i) $\phi_t(x_0)$ est de classe C^r

(ii) $\phi_0(x_0) = x_0$

(iii) $\phi_{t+s}(x_0) = \phi_t(\phi_s(x_0))$.

Dans un système dynamique de dimension *n*, l'espace $x_1, x_2, \ldots, x_n$ est appelé espace de phases ou espaces d'états. L'évolution suivant *t* du système se traduit alors par un déplacement du point représentatif dans l'espace de phase, traçant ainsi une trajectoire de phase et $x_1, x_2, \ldots, x_n$ sont les états du système. Par un point de l'espace de phase ne passe qu'une seule trajectoire. Par conséquent, deux trajectoires avec deux conditions initiales différentes ne coïncident jamais au cours du temps.

1.2.2 Point fixe ou point d'équilibre

Définition 1.2 : On appelle point fixe (ou point stationnaire ou point d'équilibre ou point critique) du système (1.1), le point $x*$ de l'espace de phase tel que:

$$f(x*) = 0 \tag{1.6}$$

Par un changement de variable $X = x - x*$, on peut ramener le point fixe $x*$ à l'origine. Les points fixes jouent un rôle très important dans les applications car ils permettent de caractériser les trajectoires voisines.

1.3 Stabilité du point d'équilibre

L'étude qualitative des systèmes dynamique permet d'analyser le comportement des solutions sans avoir à résoudre l'équation différentielle. En particulier, elle permet l'étude locale des solutions autour des points d'équilibre.

1.3.1 Stabilité au sens de Lyapunov

Soit le système autonome : $\dot{x} = f(x)$, où $f : D \to \mathbb{R}^n$ est une projection localement lipschitzienne de $D \subset \mathbb{R}^n$ dans $\mathbb{R}^n$.On suppose que le point $x*$ est le point d'équilibre, c'est-à-dire : $f(x*) = 0$.

Définition 1.3 : Le point d'équilibre $x*$ est dit stable au sens de Lyapunov si $\forall \varepsilon > 0, \exists \alpha > 0$ tel que :

$$\|x(0) - x*\| < \alpha \Rightarrow \|x(t) - x*\| < \varepsilon \ , \quad \forall t \geq 0 \tag{1.7}$$

Autrement dit, le point d'équilibre est stable si toutes les solutions issues des points proches du point d'équilibre restent proches de celui-ci.

Définition 1.4 : Le point $x*$ est instable s'il n'est pas stable au sens de Lyapunov.

Définition 1.5 : Le point d'équilibre $x*$ est asymptotiquement stable s'il est stable et si l'on peut choisir $\delta > 0$ tel que :

$$\|x(0) - x*\| < \delta \Rightarrow \lim_{t \to \infty} x(t) = x*$$

La stabilité asymptotique signifie qu'on peut déterminer un voisinage du point d'équilibre tel que n'importe quelle trajectoire, issue d'un point $x(0)$ appartenant à un voisinage de $x*$ tende vers $x*$ lorsque $t \to \infty$.

Les définitions précédentes sont locales car elles ne concernent que les orbites voisines d'un point d'équilibre. Pour cela, nous présentons les deux méthodes de Lyapunov permettant d'étudier la stabilité d'un système dynamique.

1.3.2 Méthode indirecte de Lyapunov

Par un changement de coordonnées, le point fixe de (1.1) se ramène à l'origine $(f(0) = 0)$ et le développement de f en série de Taylor autour de $x = 0$ donne :

$$f(x) = Df(0)x + \frac{1}{2!} D^2 f(0)(x,x) + \frac{1}{3!} D^3 f(0)(x,x,x) + ... \tag{1.8}$$

où $Df(0)$ est la matrice jacobienne de $f(x)$ au point d'équilibre $x = 0$.

La méthode indirecte de Lyapunov, pour étudier la stabilité autour d'un point d'équilibre, consiste à étudier le système linéaire :

$$\dot{x} = Ax \tag{1.9}$$

avec :

$$A = Df(0) = \begin{pmatrix} \frac{df_1}{dx_1} & \cdots & \frac{df_1}{dx_n} \\ \vdots & \ddots & \vdots \\ \frac{df_n}{dx_1} & \cdots & \frac{df_n}{dx_n} \end{pmatrix}_{x=0} \tag{1.10}$$

A est la matrice jacobienne de $f(x)$ et son déterminant est le jacobien.

Dans le cas où la matrice jacobienne $Df(0)$ possède *n* valeurs propres $\lambda_i,\ i = 1,.2...,n$ distinctes, la solution de (1.9) est :

$$x(t) = \sum_{i=1}^{n} c_i a^{(i)} e^{\lambda_i t} \tag{1.11}$$

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

a) si toutes les valeurs propres λ_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 partie réelle positive, le point fixe est instable.

d*)* si $Df(0)$ n'a pas de valeur propre nulle ou purement imaginaire, le point fixe est un point hyperbolique ; dans le cas contraire, il est non hyperbolique .

e) s'il existe i et j tels que $\Re\lambda_i < 0$ et $\Re\lambda_j > 0$, le point fixe est un point selle.

f) si toutes les valeurs propres de $Df(0)$ sont réelles et de même signe, le point fixe est un nœud. Un nœud stable est un puits. Un nœud instable est une source.

1.3.3 Méthode directe de Lyapunov

La méthode directe de Lyapunov s'appuie sur une observation fondamentale: si l'énergie totale d'un système, linéaire ou non linéaire, est continûment dissipée, alors on peut estimer que le système tende vers un point d'équilibre [4] [5]. Ainsi, l'idée de Lyapunov est d'examiner la variation d'une fonction scalaire pour étudier la stabilité d'un système donné. La méthode directe de Lyapunov permet d'étudier la stabilité d'un système sans avoir besoin de calculer les solutions de celui-ci. Soit le système :

$$\begin{cases} \dot{x} = f(x) \\ x \in \mathbb{R}^n, f(x^*) = 0 \end{cases} \tag{1.12}$$

Théorème 1.1 : S'il existe une fonction $V : U \to \mathbb{R}$, continue sur un voisinage de *U* de x^* et différentiable telle que :

1. $V(x^*) = 0$ et $V(x) > 0$ et $x \neq x^*$
2. $\dot{V}(x) = \sum_{j=1}^{n} \frac{\delta V}{\delta x_j} \dot{x}_j = \sum_{j=1}^{n} \frac{\delta V}{\delta x_j} f_j(x) \leq 0, \forall x \in U$

alors x^* est un point d'équilibre stable pour le système (1.12).

3. Si de plus, la fonction V est telle que :

$$\dot{V}(x) < 0, \forall x \in U \setminus \{x^*\}$$

alors x^* est un point asymptotiquement stable.

Il n'est pas toujours facile de trouver une fonction de Lyapunov pour un système. Cependant, dans les systèmes mécaniques et électriques, l'énergie est souvent un bon candidat.

1.4 Bifurcations

Une bifurcation est un changement qualitatif d'un système telle que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents, lors d'une variation quantitative d'un paramètre du système. Les valeurs des paramètres au

moment du changement sont appelées valeur de bifurcation. Nous nous intéressons à des bifurcations locales, c'est-à-dire ayant lieu au voisinage d'un point d'équilibre.

Soit un système dynamique, dépendant d'un paramètre μ , de la forme :

$$\dot{x}(t) = f(x(t), \mu) \tag{1.13}$$

Si l'ensemble des valeurs de bifurcation est défini par k conditions :

$$C_1(\mu) = C_2(\mu) = ... = C_k(\mu) = 0 \quad \text{avec} \quad 1 \le k \le p$$

la bifurcation est dite de co-dimension *k*. Il existe quatre types de bifurcations de co-dimension un que nous allons décrire par la suite.

1.4.1 Bifurcation nœud col

C'est la bifurcation la plus simple. Lorsque μ franchit 0, un point d'équilibre stable (nœud) et un point d'équilibre instable (col) apparaissent simultanément ; elle est souvent représentée par l'équation :

$$\frac{dx}{dt} = \mu - x^2 \tag{1.14}$$

qui s'appelle équation générique de bifurcation nœud-col. On a alors :

$$f(x, \mu) = \mu - x^2 .$$

- ✓ Si $\mu < 0$, l'équation $f(x, \mu) = 0$ n'admet pas de solution : il n'y a donc pas de points fixes.
- ✓ Si $\mu > 0$, on a :

$$\mu - x^2 = 0 \Leftrightarrow \begin{pmatrix} x = \sqrt{\mu} \\ et \\ x = -\sqrt{\mu} \end{pmatrix}$$

Par conséquent, l'équation (1.14) admet deux points fixes (figure 1.1). On détermine leur stabilité.

$$\frac{df(x,\mu)}{dx} = -2x \Rightarrow \left.\frac{df(x,\mu)}{dx}\right|_{x=\sqrt{\mu}} = -2\sqrt{\mu} < 0 \Rightarrow \text{Le point fixe } x = \sqrt{\mu} \text{ est stable.}$$

$$\frac{df(x,\mu)}{dx} = -2x \Rightarrow \left.\frac{df(x,\mu)}{dx}\right|_{x=-\sqrt{\mu}} = 2\sqrt{\mu} > 0 \Rightarrow \text{Le point fixe } x = -\sqrt{\mu} \text{ est instable.}$$

✓ Si $\mu = 0$,le seul point fixe est $x = 0$.

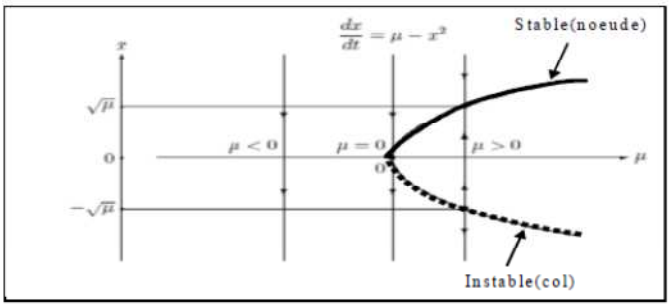


Figure 1.1 - Diagramme de bifurcation nœud-col

1.4.2 Bifurcation transcritique

Elle est caractérisée par un échange de stabilité entre les points fixes (les points stables deviennent instables et vice versa) lorsque μ franchit 0. Elle est souvent représentée par l'équation :

$$\frac{dx}{dt} = \mu x - x^2 \tag{1.15}$$

qui s'appelle équation générique de la bifurcation transcritique. On a alors :

$$f(x,\mu) = \mu x - x^2 = 0 \Leftrightarrow \begin{cases} x = 0 \\ ou \\ x = \mu \end{cases}$$

On a donc deux points fixes (figure 1.2) et on détermine leur stabilité :

$$\left.\frac{df(x,\mu)}{dx}\right|_{x=0} = \mu \text{ et } \left.\frac{df(x,\mu)}{dx}\right|_{x=\mu} = -\mu$$

- ✓ Si $\mu < 0$,le point fixe $x = 0$ est stable, mais $x = \mu$ est instable.
- ✓ Si $\mu > 0$,le point fixe $x = 0$ est instable mais $x = \mu$ est stable

On remarque un échange de stabilité en $\mu = 0$.

- ✓ Si $\mu = 0$,le seul point fixe est $x = 0$ et en intégrant l'équation (1.15) ,on obtient :

$$x(t) = \frac{1}{t + \frac{1}{x_0}}$$

D'où le point $x = 0$ est semi-stable (stable si $x_0 > 0$ et instable si $x_0 < 0$).

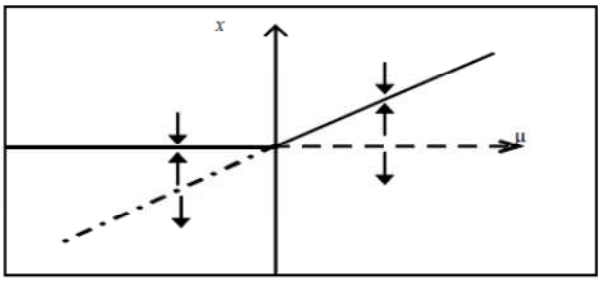


Figure 1.2 - Bifurcation transcritique

1.4.3 Bifurcation fourche (Pitchfork)

Au point de la bifurcation fourche (figure 1.3), la stabilité du point fixe change au profit de la naissance d'une paire de points fixes.

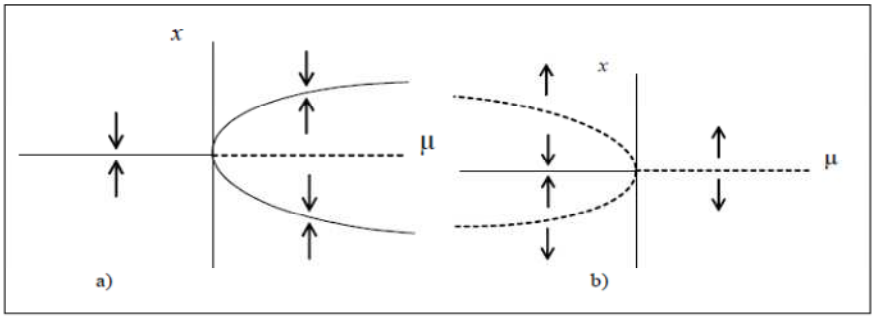


Figure 1.3 - Diagramme de bifurcation fourche a)sur-critique b)sous-critique

L'équation générique d'une bifurcation fourche (sur-critique) est :

$$\frac{dx}{dt} = \mu x - x^3 \tag{1.16}$$

et pour la sous-critique, elle s'écrit :

$$\frac{dx}{dt} = \mu x + x^3 \tag{1.17}$$

Dans le cas d'une bifurcation sur-critique, on a :

$$f(x,\mu) = \mu x - x^3 = 0 \Leftrightarrow \begin{cases} x = 0 \\ ou \\ x^2 = \mu \end{cases}$$

- ✓ Si $\mu < 0$, on a un seul point fixe $x = 0$;
- ✓ Si $\mu > 0$, on a trois points fixes : $\begin{cases} x = 0 \\ x = \sqrt{\mu} \\ x = -\sqrt{\mu} \end{cases}$

On détermine la stabilité de ces points fixes :

$$\left.\frac{df(x,\mu)}{dx}\right|_{x=0} = \mu \quad \text{et} \quad \left.\frac{df(x,\mu)}{dx}\right|_{x=\pm\sqrt{\mu}} = -2\mu$$

- ✓ Si $\mu < 0$, le seul point fixe $x = 0$ est stable.
- ✓ Si $\mu > 0$, le point fixe $x = 0$ est instable, mais $x = \sqrt{\mu}$ et $x = -\sqrt{\mu}$ sont stables.

On remarque un échange dans le nombre de points fixes et dans la stabilité en $\mu = 0$.

1.4.4 Bifurcation de Hop

La bifurcation de Hopf représentée sur la figure 1.4 a lieu lorsque le paramètre

de contrôle μ prend une valeur critique μ_0 pour laquelle la matrice jacobienne du système possède une paire de valeurs propres complexes conjuguées qui traversent l'axe imaginaire et le type de stabilité de l'équilibre existant change avec l'apparition d'un cycle limite.

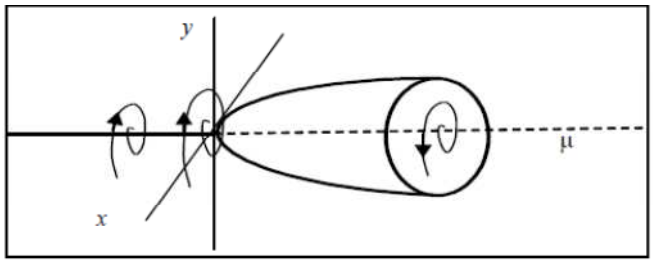


Figure 1.4 - Diagramme de bifurcation Hopf

1.4.5 Bifurcation doublement de période ou Flip

Considérons un système dynamique de la forme (1.13), qui possède un point fixe stable pour $\mu < \mu_0$. Si on augmente μ au-delà de la valeur μ_0, le point d'équilibre se déstabilise et une bifurcation se produit qui donne lieu à un cycle d'ordre 2 stable. Puis, si μ continue d'augmenter, le cycle d'ordre 2 se déstabilise et chacun des deux points du cycle bifurque à son tour. Cette nouvelle bifurcation donne naissance à un cycle d'ordre 4 stable. Si μ augmente toujours, des bifurcations continuent d'apparaitre en doublant la période du cycle à chaque fois, d'où le nom de cette bifurcation, conduisant ainsi à une suite infinie de bifurcations et éventuellement au chaos.

Si on considère comme exemple le système de Rossler qui est un système dynamique continu dont la représentation d'état (b étant le paramètre variable) est donnée par :

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \qquad (1.18)$$

avec : $a = 0.2$; $c = 5.7$

Pour $b > 1.5$, le système possède un point fixe stable. Si b est compris dans l'intervalle $0.8 < \mu < 1.5$, le point fixe se déstabilise et un cycle d'ordre 2 stable apparaît. Puis, si $0.72 < \mu < 0.8$, le cycle d'ordre 2 se déstabilise et un cycle d'ordre 4 stable apparaît et ainsi de suite. La figure 1.5 illustre cette bifurcation doublement de période pour le système de Rossler. Elle a été obtenue en simulant le système (1.18) pour différentes valeurs de b.

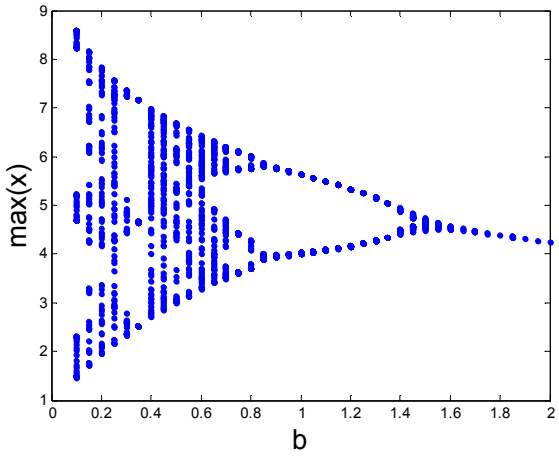


Figure 1.5 - Bifurcation doublement de période

1.5 Attracteurs et bassin d'attraction

Un attracteur Ω d'un système dynamique est un ensemble particulier d'états, sous ensemble de l'espace d'état, qui est le régime permanent du système. Mathématiquement, l'ensemble Ω est un attracteur si :

- Pour tout voisinage U de Ω, il existe un voisinage V de Ω tel que toute solution $x(x_0, t) = \phi_t(x_0)$ restera dans U si $x_0 \in V$.
- $\cap \phi_t(V) = \Omega,\ t \geq 0$.
- Il existe une orbite dense dans Ω.

Lorsque Ω est un attracteur, l'ensemble

$$W = \cup \phi_t(V),\ t < 0$$

est appelé bassin d'attraction de Ω. C'est l'ensemble des points dont les trajectoires asymptotiques convergent vers Ω .

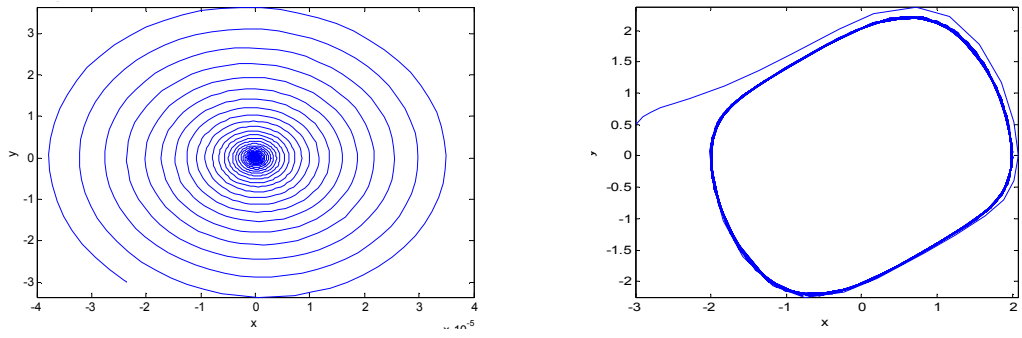
Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques.

1.5.1 Attracteur régulier

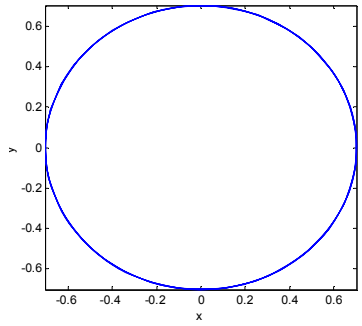
Les attracteurs réguliers caractérisent l'évolution des systèmes non chaotiques et peuvent être de trois sortes :

- **Le point fixe :** c'est l'attracteur le plus simple dans lequel le système évolue vers un état de repos. On remarquera que seuls les puits peuvent être des attracteurs.
- **Le cycle limite périodique :** Il peut arriver que la trajectoire de phase se referme sur elle-même. L'évolution temporelle est alors cyclique, le système présentant des oscillations permanentes. Dans un système dissipatif, cela exige la présence d'un terme de forçage dans les équations pour compenser les pertes par dissipation.
- **Le cycle limite pseudo-périodique :** c'est presque un cas particulier du précédent. Le système présente au moins deux périodes simultanées dont le rapport est irrationnel. La trajectoire de phase ne se referme pas sur elle-même, mais s'enroule sur une variété de dimension 2(par exemple un tore)

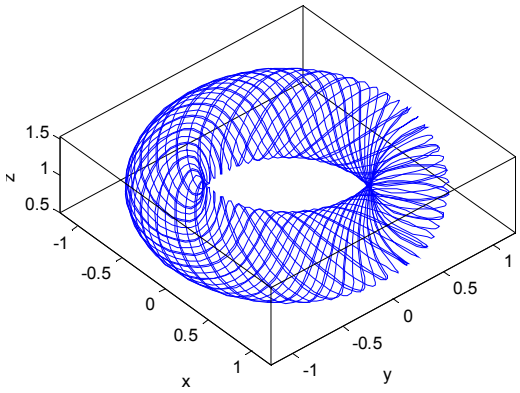
La figure 1.6 représente les différents types d'attracteurs réguliers.



(a) Point fixe (b) Cycle limite



(c) Cercle



(d) Tore(quasi-périodique)

Figure 1.6 - Les différents types d'attracteurs réguliers

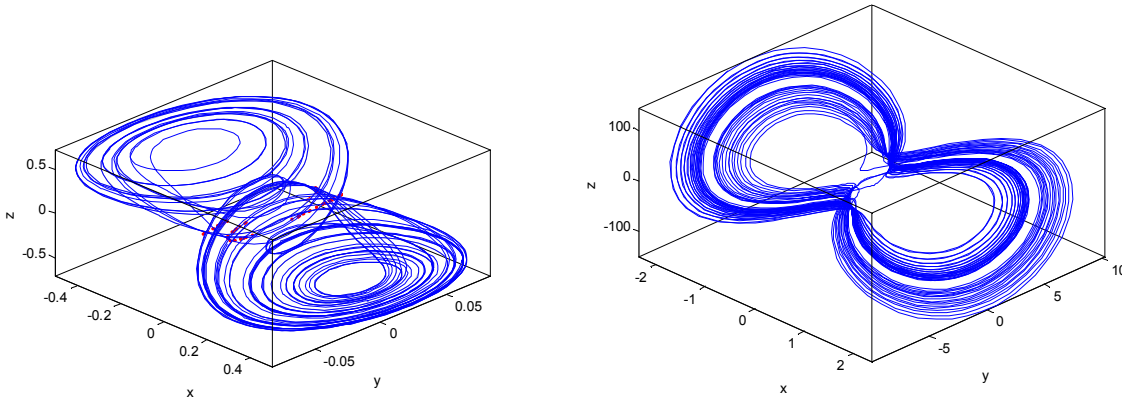
1.5.2 Attracteur étrange

Les attracteurs étranges sont des formes géométriques complexes qui caractérisent l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace de phase et appartenant au bassin d'attraction de l'attracteur donnent des trajectoires qui tendent à former l'attracteur étrange.

L'attracteur étrange se caractérise par :

- La sensibilité aux conditions initiales (deux trajectoires de l'attracteur initialement voisines finissent toujours par s'éloigner l'une de l'autre traduisant ainsi le comportement chaotique du système.
- La dimension d de l'attracteur est fractale (non entière) avec $2 < d < n$ où n est la dimension de l'espace des phases.
- Dans l'espace des phases, l'attracteur est de volume nul.

La figure 1.7 représente deux exemples d'attracteurs étranges correspondants aux systèmes de Chua et de Moore Spiegel.



(a) Oscillateur de Chua (b) Système de Moore Spiegel

Figure 1.7 - Attracteurs étranges

1.6 Section de Poincaré

Pour étudier la stabilité d'un cycle limite, on a souvent recours à la section de Poincaré et l'application du premier retour.

La section de Poincaré est un outil fréquemment utilisé pour étudier les systèmes dynamiques et notamment la stabilité des orbites périodiques.

Soit un système dynamique autonome à temps continu et présentant dans une région de l'espace un comportement asymptotique pour $t \to \infty$.

$$\frac{dx}{dt} = f(x)\ ,\ x \in \mathbb{R}^n \tag{1.19}$$

On définit une hyper surface Σ_p de dimension $n-1$ appelé section de Poincaré. C'est une surface de section acceptable si elle est transversale au champ de vecteurs dans toute la région concerné et si naturellement elle coupe l'ensemble limite que nous voulons étudier [6]. On considère l'ensemble des points $p_0, p_1, p_2, \ldots$ correspondant aux intersections successives de la trajectoire $\varphi_t(x_0)$ avec l'hyper surface Σ_p. L'application du premier retour T est alors définie comme étant l'application qui à un point p_i de Σ_p fait correspondre le point p_{i+1}, prochaine intersection de la trajectoire $\varphi_t(x_0)$ avec Σ_p.

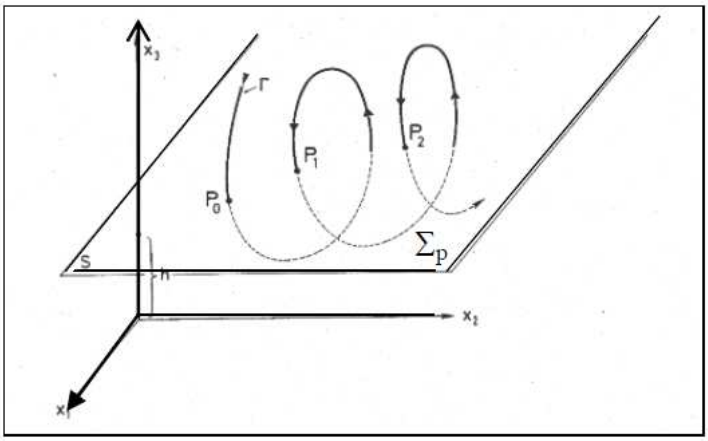


Figure1.8 - Section de Poincaré et application du premier retour

Ainsi, le système dynamique initial (1.18) de dimension n à temps continu est converti en un système de dimension $n-1$ à temps discret :

$$p_{k+1} = T(p_k)\ ,\ k = 0,1,2,... \tag{1.20}$$

Le numéro de l'intersection remplace le temps. Cette conversion se fait sans perte d'information, un point de la section Σ_p définissant une orbite et une seule. Une orbite du système originel est alors transformée en une suite d'intersections p_k, $k = 0,1,2,...$ (figure 1.8) caractérisant le système dynamique et dont les propriétés sont résumées dans le tableau suivant :

Attracteur dans l'espace des phases	Application de Poincaré
Cycle limite	1 point
Cycle limite avec p maxima par période	p points
Attracteur quasi-périodique	Courbe fermée
Attracteur étrange	Courbe(s) ouverte(s)

L'étude de la stabilité d'une orbite périodique peut se faire à travers l'analyse de l'application du premier retour T.

1.7 Le 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 de conditions initiales très proches, vont diverger très rapidement l'une par rapport à l'autre .Cette sensibilité par rapport 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 est impossible.

D'un point de vue mathématique, on dit que f montre une dépendance sensible aux conditions initiales lorsque :

$$\exists \delta > 0, \forall x \in D, \forall \varepsilon > 0, \exists (y, p) \in D : \begin{cases} \|x - y\| < \varepsilon \\ \|f^p(x) - f^p(y)\| > \delta \end{cases} \tag{1.21}$$

1.7.1 Caractéristiques du chaos

Les phénomènes chaotique 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 parmi lesquelles on peut citer [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.

- *L'attracteur étrange*

Dans l'espace de phase, le chaos donne lieu à des trajectoires, appelées attracteur chaotique ou attracteur étrange. Géométriquement, un tel attracteur peut

être décrit comme le résultat d'une opération d'étirement et de repliement d'un cycle de l'espace de phases, répétée un nombre infini de fois. La longueur de l'attracteur est infinie bien qu'i soit contenu dans un espace fini.

On peut alors donner cette définition :

Définition 1.6 : On dit qu'un attracteur A est étrange si :

i) Dans l'espace de phases, l'attracteur est de volume nul et sa dimension d est fractale (non entière) avec $2 < d < n$ où n est la dimension de l'espace de phase .

ii) Deux trajectoires de l'attracteur initialement voisines finissent toujours par s'écarter l'une de l'autre.

- *Le spectre fréquentiel*

Une façon simple de caractériser le chaos consiste à calculer le spectre de Fourier de l'évolution temporelle d'une des variables du système. L'existence de spectres larges est une caractéristique essentielle des mouvements chaotiques d'un système.

1.7.2 Transition vers le chaos

Un système dynamique possède en général un ou plusieurs paramètres dit de contrôle, qui agissent sur les caractéristiques de la fonction de transition. Selon la valeur du paramètre de contrôle, les mêmes conditions initiales mènent à des trajectoires correspondant à des régimes dynamiques qualitativement différents.

Il existe plusieurs scénarios qui décrivent le passage du point fixe au chaos. On peut ainsi citer trois types de transition vers le chaos :

- *L'intermittence vers le chaos :*

Un mouvement périodique stable est entrecoupé par des bouffées de turbulence. Lorsqu'on augmente les paramètres de contrôle, les bouffées de turbulence deviennent de plus en plus fréquentes jusqu'à l'apparition du chaos.

- *Le dédoublement de période :*

Il est caractérisé par une succession de bifurcations de types fourches. A mesure que la contrainte augmente, la période d'un système forcé est multiplié par

deux, puis par quatre, puis par huit, etc. ; ces doublements de période sont de plus en plus rapprochés. Lorsque la période est infinie, le système devient chaotique. La turbulence dans les fluides peut apparaitre suivant ce scénario.

- *La quasi-périodicité :*

Elle intervient quand un deuxième système perturbe un système initialement périodique. Si le rapport des périodes des deux systèmes en présence n'est par rationnel, alors le système est quasi-périodique et peut évoluer vers le chaos.

1.8 Exposants de Lyapunov

Alexandre Lyapunov a introduit l'idée de mesurer la divergence possible entre deux orbites issues de conditions initiales voisines. Lorsque cette divergence croit exponentiellement avec le temps à partir de conditions initiales voisines d'un point donné, on a le phénomène de sensibilité aux conditions initiales, idée à laquelle sont attachés les **exposants de Lyapunov**, qui donnent une mesure quantitative de cette divergence exponentielle locale et mesure en fait le degré de sensibilité d'un système dynamique [4].

1.8.1 Calcul des exposants de Lyapunov

Considérons le système dynamique autonome à temps continu défini par :

$$\begin{cases} \dot{x} = f(x); f : \mathbb{R}^n \to \mathbb{R}^n \\ x(0) = x_0 \end{cases} \tag{1.22}$$

où $\varphi(x_0, t)$ est une trajectoire solution de ce système de condition initiale x_0 et x_p un point de cette trajectoire à $t = t_p$ dans l'espace des phases.

Un champ de vecteurs ou champ vectoriel est une fonction qui associe un vecteur à chaque point d'un espace euclidien ou plus généralement d'une variété différentielle. Les champs de vecteurs sont souvent utilisés en physique, pour modéliser par exemple la vitesse et la direction d'un fluide en mouvement dans l'espace, ou la valeur et la direction d'une force, comme la force magnétique ou gravitationnelle, qui évoluent point par point.

Le calcul des exposants de Lyapunov consiste dans un premier temps à linéariser le vecteur champ au voisinage d'un point de la trajectoire considérée. Soient $\varphi(x_0,t)$ cette trajectoire et x_p un point de la trajectoire ($x_p = \varphi(x_0,t_p)$).

En considérant une petite perturbation $\delta x_p(t)$ appliquée au voisinage de x_p et en développant en série de Taylor du premier ordre le vecteur champ $f(x_p)$, le système linéarisé autour de x_p s'écrit :

$$\frac{d\delta x_p}{dt} = J_f(x_p)\delta x_p \tag{1.23}$$

où $J_f(x_p)$ est la matrice jacobienne de f au point x_p.

Il s'agit ensuite d'intégrer chacune des composantes $x_k(t)$ avec $k = 1,2,.....,n$ de la trajectoire $\varphi(x_0,t)$ à partir de l'équation (1.21). Chacune de ces composantes $x_k(t)$ intégrées est introduite dans l'équation (1.22). La dernière opération consiste à intégrer le système (1.22) lui-même. Au final, nous obtenons une matrice $n \times n$ $\Phi_t(x_p)$ appelée matrice de la solution fondamentale.

Toute perturbation $\delta x_p(t)$, à $t = t_p$, au voisinage $\delta x_p(t)$ d'un point x_p, de la trajectoire pourra s'écrire sous la forme :

$$\delta x_p(t) = \Phi(\delta x_p(t_p)) \tag{1.24}$$

Soient $\mu_k(t)$ les valeurs propres de cette matrice, $k = 1,2,.....,n$.

L'exposant de Lyapunov λ_k du $k^{ième}$ ordre est lié à la valeur propre $\mu_k(t)$ et s'écrit :

$$\lambda_k = \lim_{t\to+\infty} \frac{1}{t} Ln\left|\mu_k(t)\right| \tag{1.25}$$

L'exposant de Lyapunov λ_k existe dans la mesure où la limite existe.

Remarque : Si $\lambda_k > 0$,alors la distance entre les trajectoires augmente de façon exponentielle et finalement un régime chaotique atteint. Par contre, si $\lambda_k < 0$, la

distance entre les trajectoires converge vers zéro lorsque $t \to \infty$ et un mouvement régulier est obtenu.

1.8.2 Comportement du système en fonction des exposants de Lyapunov

En étudiant les exposants de Lyapunov d'un système non linéaire, on peut définir le type d'attracteur (comportement asymptotique) généré par le système :

- $\lambda_n \le ..... \le \lambda_2 \le \lambda_1 \le 0$: des exposants de Lyapunov négatifs montrent l'existence d'un point fixe.
- $\lambda_1 = 0, \lambda_n \le ..... \le \lambda_2 \le 0$: l'attracteur est une orbite fermée.
- $\lambda_1 = \lambda_2 = 0, \lambda_n \le ..... \le \lambda_3 \le 0$: l'attracteur est quasi-périodique (2 fréquences).
- $\lambda_1 = \lambda_2 = ... = \lambda_k = 0, \lambda_n \le ..... \le \lambda_{k+1} \le 0$: l'attracteur est quasi-périodique (k fréquences).
- $\lambda_1 > 0, \sum_{i=1}^{n} \lambda_i < 0$: l'attracteur est chaotique.
- $\lambda_1 > \lambda_2 > ... > \lambda_k > 0, \sum_{i=1}^{n} \lambda_i < 0$: l'attracteur est hyper-chaotique.

1.9 Exemples de systèmes chaotiques

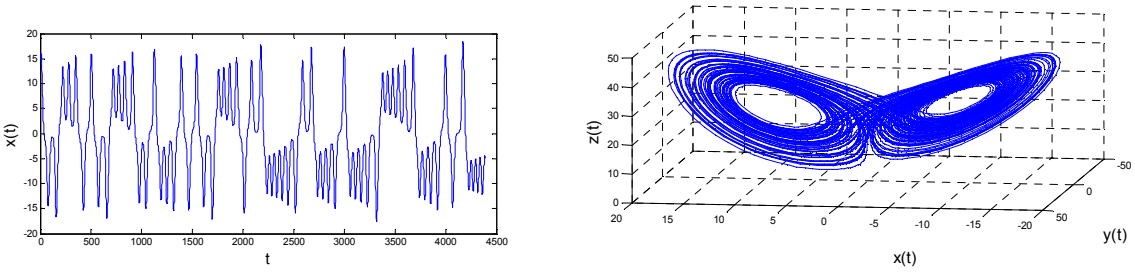
Dans cette section, nous présentons quelques exemples de systèmes chaotiques les plus célèbres.

1.9.1 Système de Lorentz

Le système de Lorentz est un exemple célèbre de système différentiel au comportement chaotique pour certaines valeurs de paramètres. Ce système est défini par les équations suivantes :

$$\begin{cases} \dot{x} = \sigma(y - x) \\ \dot{y} = -rx - y - xz \\ \dot{z} = -bz + xy \end{cases} \tag{1.26}$$

Pour $\sigma = 10,\ r = \frac{8}{3}$ et $b = 28$, on a un comportement chaotique du système. L'espace des phases et la coordonnée *x* sont représentés sur la figure 1.9.



a) Coordonnée *x*(t) b) Attracteur chaotique de Lorenz

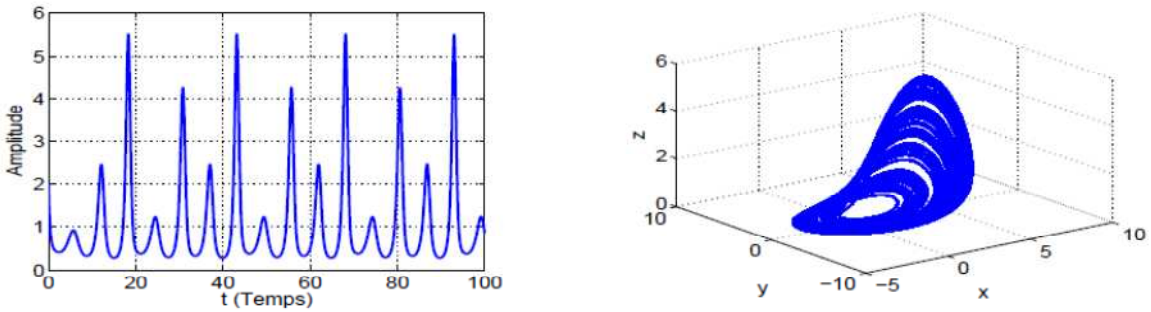
Figure 1.9 - Système chaotique de Lorenz

1.9.2 Système de Rössler

Les équations de ce système sont les suivantes :

$$\begin{cases} \dot{x} = -(y+z) \\ \dot{y} = x + ay \\ \dot{z} = b + z(x-c) \end{cases} \tag{1.27}$$

Ce système, qui a été proposé par l'Allemand Otto Rössler, est lié à l'étude de l'écoulement des fluides. Pour $a = 0,398$, $b = 2$ et $c = 2$, l'attracteur de Rössler et l'évolution dans le temps de la coordonnée z sont représentés sur la figure 1.10.



a) La troisième coordonnée *z* b) L'attracteur chaotique de Rössler

Figure 1.10 - Système chaotique de Rössler

1.10 Conclusion

Dans ce chapitre, nous avons présenté quelques éléments de la théorie des systèmes dynamiques et du chaos : points fixes, linéarisation autour du point fixe, étude de la stabilité, bifurcations, etc. Les principales caractéristiques d'un système chaotique ont étés décrites en mettant en évidence l'intérêt du calcul des exposants de Lyapunov ainsi que les différents scénarios possibles de transition vers le chaos.

Ces notions seront exploitées dans les chapitres suivants, lors de l'étude des différents comportements de l'oscillateur de Colpitts, qui sera utilisé en tant que générateur de signaux chaotiques destinés à chiffrer un message confidentiel.

CHAPITRE 2

TRANSMISSION CHAOTIQUE :

ETUDE DE L'EMETTEUR

2.1 Introduction

La transmission chaotique de données a été à l'origine de la transmission de données et a attiré beaucoup d'attention, particulièrement après le travail exceptionnel de Carroll et de Pecora sur la synchronisation de deux systèmes chaotiques [1]. Bien que l'étude d'appliquer le chaos dans la transmission de données soit plus récente que celle de la transmission traditionnelle, le chaos possède plusieurs propriétés qui sont très intéressantes pour la transmission.

La conception d'un système de communication chaotique peut être décomposée en trois étapes à savoir le choix de l'émetteur, le choix du récepteur et la mise au point de la synchronisation de la transmission chaotique pour la récupération du message crypté (figure 2.1).

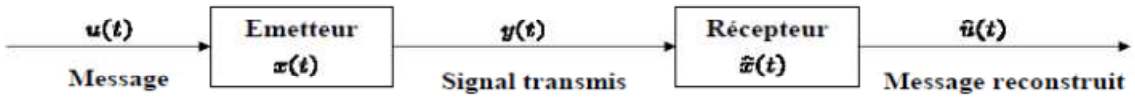


Figure 2.1 - Principe général d'un système de communications

Dans ce chapitre, nous discuterons d'abord des principaux avantages de l'approche par transmission chaotique. Après cela, nous donnerons une vue d'ensemble des principaux schémas de transmission chaotique. Puis, nous présenterons la structure de l'émetteur chaotique construit autour de l'oscillateur Colpitts et ses principales caractéristiques. Nous expliquerons notre approche pour

injecter le message confidentiel dans l'oscillateur chaotique de Colpitts et les conditions à respecter au niveau de l'amplitude et de la fréquence du signal.

L'étude de la synchronisation chaotique et l'analyse du récepteur pour la récupération du message seront présentées dans le chapitre suivant.

2.2 Méthodes de transmission chaotique

L'idée d'utiliser des signaux aléatoires pour la communication sécurisée a été mise en œuvre en 1926 par Vernam [9]. Il proposa dans son article d'utiliser un alphabet binaire et de coder chaque mot à l'aide d'un bit de la clef, choisi de façon arbitraire. Plus tard, dans les années 90, cette idée a été développée dans le contexte des signaux chaotiques [10] [11]. A cause de la nature imprédictible à long terme du chaos, on a cru pendant longtemps que le chaos serait inutilisable et incontrôlable, mais depuis quelques décennies, les chercheurs ont réussi à modéliser le chaos par des équations différentielles et montrer qu'il existe un aspect déterministe dans ce phénomène qui apparait aléatoire à première vue. C'est cette nature semblable au bruit des signaux chaotiques qui a motivé les chercheurs à camoufler un message confidentiel à l'aide d'un signal chaotique, de façon à ne pas pouvoir le distinguer. Ainsi, différentes méthodes ont été proposées afin de masquer le message dans un système chaotique et ensuite de le restaurer. Ces méthodes sont toutes basées sur la synchronisation des systèmes chaotiques et ont été améliorées au fil des années dans le but d'augmenter de plus en plus la sécurité et la rapidité de la transmission de l'information. Ces méthodes sont parfois appelées méthodes de cryptographie chaotique.

En parallèle avec le chiffrage d'informations discrètes ou binaires, des recherches ont été effectuées afin de pouvoir appliquer les méthodes de cryptographie aux informations continues. Grâce aux résultats obtenus en synchronisation des systèmes chaotiques [8] [12], il a été possible d'employer des signaux chaotiques continus comme porteur d'informations. Dans ce cas, le message est codé par l'émetteur et il est décodé et extrait du signal chaotique par le récepteur. Parmi les méthodes de transmission chaotique, on peut citer la méthode par addition, la commutation chaotique, la modulation chaotique, et la méthode par inclusion.

2.2.1 Méthode par addition

Cette méthode est la première chronologiquement à utiliser la synchronisation du chaos ; elle est présentée dans [11]. L'idée repose sur l'observation des signaux chaotiques : *a priori*, ils ressemblent à du bruit, comme le montre la figure 2.2.

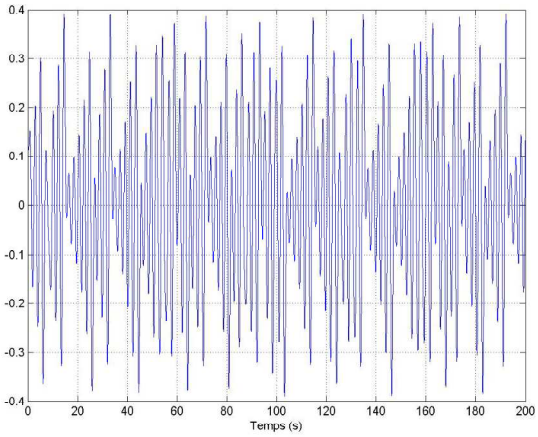


Figure 2.2 - Signal chaotique

Le principe est alors très simple : il suffit d'ajouter le message utile u(t) à une porteuse chaotique, de façon à "noyer" l'information dans du bruit. Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal y(t) (porteuse chaotique +message), et donc ne cherchera pas à appliquer des techniques de décryptage. Au niveau du récepteur autorisé, après synchronisation grâce au signal reçu, on obtient le message original par soustraction (figure 2.3).

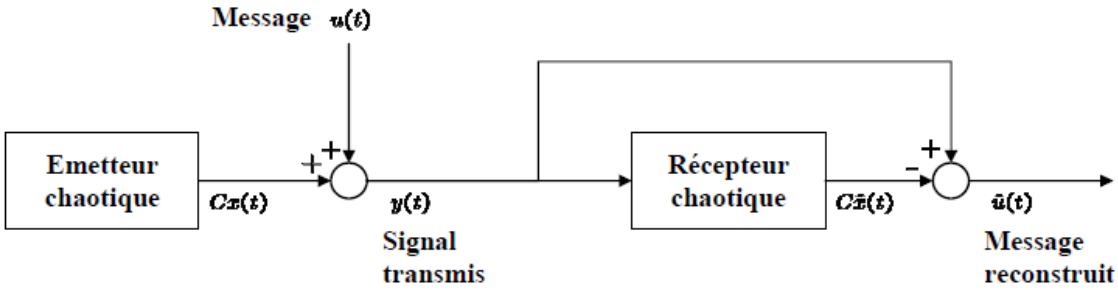


Figure 2.3 - Méthode par addition

Le principal avantage de cette méthode réside dans la simplicité du cryptage. On peut souligner que cette technique peut être appliquée à des messages continus ou discrets. Dans les deux cas, il est impératif que l'amplitude du message original soit significativement plus petite que celle de la porteuse chaotique, d'une part pour ne pas perturber l'établissement de la synchronisation au niveau du récepteur, et d'autre part pour garantir le secret de la transmission. Dans tous les cas, à cause de la présence du message, la synchronisation ne peut être parfaite. En outre, la fréquence du message doit être comprise dans le spectre du signal chaotique. Un autre problème qui se pose naturellement concerne la présence d'un bruit additif au niveau du canal de transmission. Dans ce cas, il faut que l'amplitude du message soit plus grande que celle du bruit. Il y a donc un compromis à trouver entre la sécurité de la transmission, et la robustesse au bruit.

2.2.2 Méthode par commutation chaotique

Cette technique, exposée dans [13] [14], est réservée aux messages prenant un nombre fini de valeurs. Pour plus de simplicité, nous traitons le cas des messages binaires : $u(t) \in \{0,1\}$ .L'émetteur est constitué de deux systèmes chaotiques : ces deux systèmes peuvent avoir le même modèle dynamique, avec des paramètres différents, ou avoir deux modèles dynamiques totalement différents.

La figure 2.4 illustre le principe du cryptage par commutation : selon la valeur de $u(t)$ à l'instant t (c'est-à-dire $u(t) = 1$ ou $u(t) = 0$), l'émetteur est soit le système chaotique $\sum_0$, soit le système $\sum_1$. La sortie $y(t)$ est transmise à deux copies $\sum_0', \sum_1'$ des émetteurs chaotiques, de sorties respectives $\hat{y}_0(t)$ et $\hat{y}_1(t)$. Si $u(t)$ prend la valeur 0, alors $\sum_0'$ se synchronise, et $\sum_1'$ ne se synchronise pas. Ainsi, l'erreur de synchronisation $e_0(t) = \hat{y}_0(t) - \hat{y}(t)$ va tendre vers 0, tandis que l'erreur $e_1(t) = \hat{y}_1(t) - \hat{y}(t)$ sera d'amplitude non nulle. Le processus est symétrique lorsque le message prend la valeur 1.

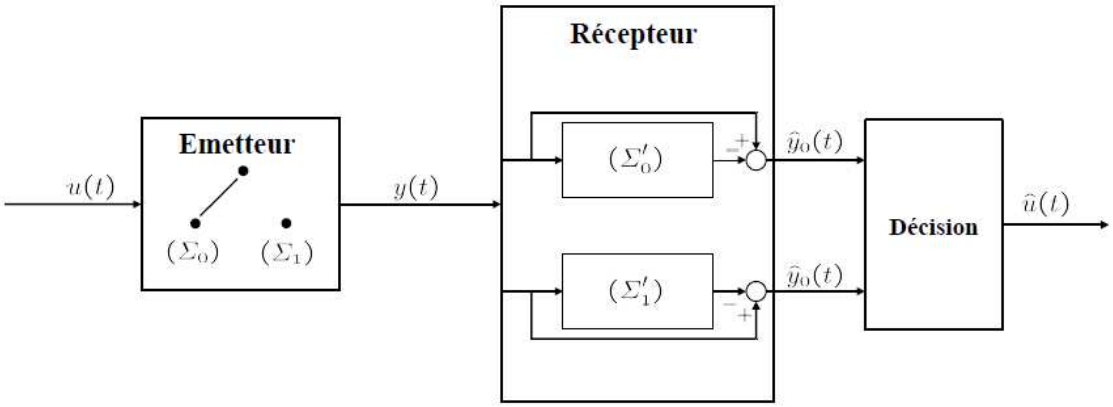


Figure 2.4 - Méthode par commutation chaotique

Par comparaison des valeurs des intégrales des carrés des erreurs $e_0^2(t)$ et $e_1^2(t)$, la valeur du message $u(t)$ est facilement retrouvée pendant l'intervalle de temps entre deux commutations. Notons que cet intervalle doit être suffisamment long pour que la synchronisation puisse s'établir. Cette méthode a l'énorme avantage d'être robuste au bruit : en effet, au niveau du récepteur, on détermine la valeur exacte du message soit en évaluant l'erreur de synchronisation au niveau des deux copies comme précédemment, soit par corrélation entre le signal $y(t)$ reçu et les signaux $\hat{y}_0(t)$ et $\hat{y}_1(t)$. Dans ce dernier cas, il s'agit de déterminer quel signal chaotique généré par les deux copies "ressemble" le plus au signal reçu. La corrélation minimise l'influence du bruit sur l'erreur de synchronisation. En revanche, le taux de transmission du cryptage par commutation est assez bas, car un signal binaire contient moins d'information qu'un signal analogique, et le temps nécessaire à l'établissement de la synchronisation est perdu à chaque fois que le message change de valeur. En outre, la sécurité n'est plus garantie si les deux ensembles de paramètres correspondant à $\sum_0$ et $\sum_1$ sont trop différents, car on peut observer les changements de système chaotique émetteur au niveau du signal transmis : cela est dû aux caractéristiques propres à chaque système chaotique, qui possède des trajectoires bien spécifiques.

2.2.3 Méthode par modulation chaotique

Cette technique, développée dans [15], utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure 2.5.

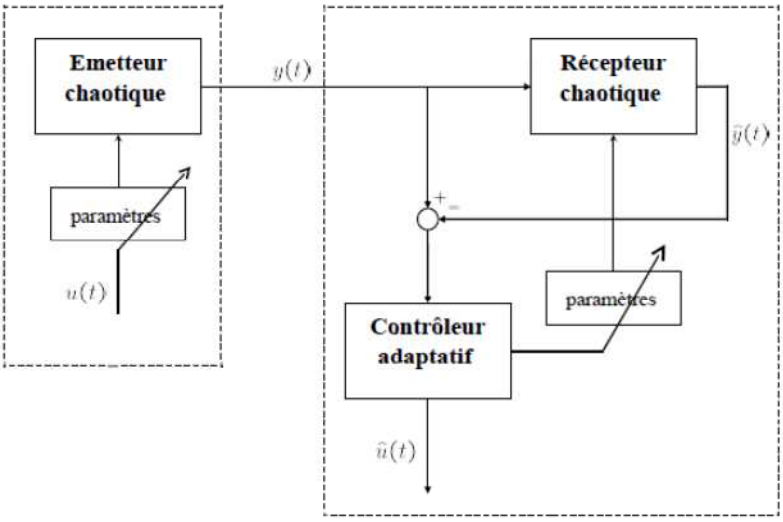


Figure 2.5 - Principe du cryptage par modulation

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

2.2.4 Méthode par inclusion

Cette technique de cryptage consiste à injecter le message dans la dynamique de l'émetteur, sans toutefois réaliser une modulation de paramètre. La restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur.

2.2.4.1 Observateurs à entrées inconnues

Le schéma de la figure 2.6 illustre un problème classique d'estimation d'état non linéaire à entrées inconnues : il faut reconstruire l'état $x(t)$ du système émetteur et également l'entrée inconnue $u(t)$.

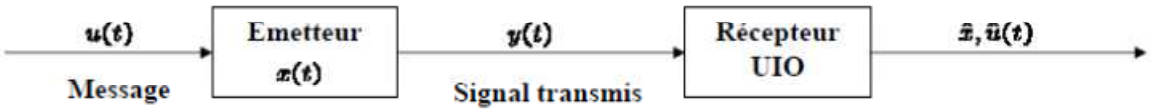


Figure 2.6 - Observateur à entrées inconnues

Différentes techniques de synthèse d'observateurs à entrées inconnues ont été développées dans la littérature, et peuvent être utilisées à des fins de décryptage. Parmi les articles utilisant les observateurs à entrées inconnues pour décrypter l'information, on peut citer [16] [17], qui traitent le cas des systèmes à temps discret, et [16] qui généralise les résultats établis dans [18] [19].

2.2.4.2 Méthode par inversion

L'article [20] présente un processus de décryptage par inversion, i.e. le récepteur est conçu en inversant le modèle de l'émetteur.

Définition 2.1 : (Système inverse). On considère deux systèmes $\sum_1$ et $\sum_2$. Alors $\sum_2$ est un système inverse de $\sum_1$ si :

(i) l'ensemble E des entrées admissibles de $\sum_1$ coïncide avec l'ensemble des sorties de $\sum_2$, et l'ensemble E' des entrées admissibles de $\sum_2$ coïncide avec l'ensemble des sorties de $\sum_1$.

(ii) pour tout signal $u \in E$ et toute condition initiale du système $\sum_1$, il existe une condition initiale du système $\sum_2$, telle que pour tout $t \geq 0, u(t) = \hat{u}(t)$.

(iii) la condition (ii) est vraie en échangeant les rôles de $\sum_1$ et $\sum_2$.

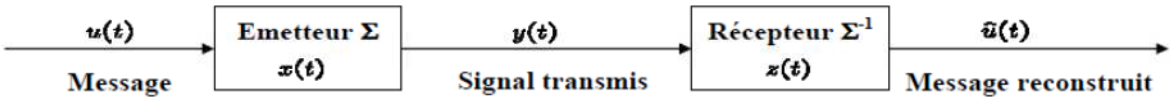


Figure 2.7 - Méthode par inversion

La figure 2.7 présente le principe général de cette approche cryptage par inclusion-décryptage par inversion :

$$\begin{aligned} y &= \sum(u, x) \\ \hat{u} &= \sum^{-1}(y, x) \end{aligned} \tag{2.1}$$

2.3 Choix de la structure de l'émetteur chaotique

De nombreuses variétés d'oscillateurs ont été proposés dans la littérature pour la génération de signaux chaotiques [21] [22]. Ces oscillateurs, qui différent par leur structures et/ou par leurs éléments électriques et/ou par la technologie utilisée, offrent la possibilité de générer des comportements chaotiques des plus basses fréquences aux plus hautes. Le point commun entre tous ces oscillateurs est la présence d'un élément non linéaire et d'un élément qui réinjecte de l'énergie. Généralement, il est possible de les modéliser par des équations différentielles pour lesquels l'analyse explicite ou implicite de leur modèle mathématique est faisable. La caractéristique spécifique du chaos permet de l'utiliser dans plusieurs applications et en particulier dans le domaine des communications pour la sécurisation de l'information.

Pour la génération de signaux chaotiques, nous avons opté pour l'utilisation de l'oscillateur Colpitts. Ce choix peut être expliqué par les points suivants :

- La simplicité de la structure de l'oscillateur de Colpitts qui utilise un seul transistor permettant de générer des signaux chaotiques en modifiant

uniquement les conditions de fonctionnement du transistor, les autres paramètres étant fixés à des valeurs appropriées.

- La possibilité de faire évoluer la fréquence fondamentale de l'oscillateur vers les fréquences élevées. Il suffit pour cela de choisir la technologie adéquate pour le transistor et inclure dans l'étude et la conception de l'oscillateur les effets liés à la montée en fréquence.
- La structure de l'oscillateur de Colpitts possède un non linéarité intrinsèque due à la caractéristique intrinsèque du transistor.
- L'utilisation de l'oscillateur de Colpitts dans les systèmes de communications chaotiques a été démontrée pour la transmission de signaux binaires [23] et continus [24].

La figure 2.8 représente le montage basses fréquences de l'oscillateur de Colpitts. C'est une structure en base commune qui permet d'obtenir un gain plus élevé tout en autorisant une bande passante plus large. Le circuit résonnant L-C est connecté entre le collecteur et la base du transistor et une fraction de la tension du circuit L-C est réinjectée au niveau de l'émetteur. Les tensions d'alimentation V_1 et V_2 permettent de fixer le point de fonctionnement du transistor. Le choix des valeurs du circuit résonnant détermine la fréquence fondamentale de l'oscillateur.

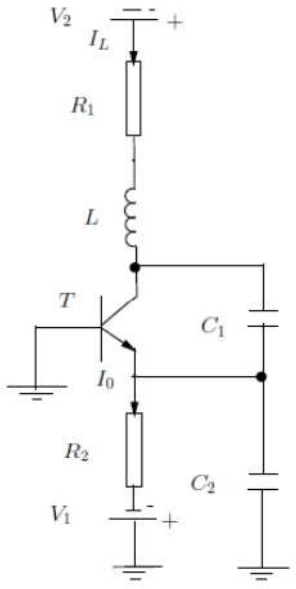


Figure 2.8 - Oscillateur de Colpitts

2.4 Analyse de l'oscillateur de Colpitts chaotique

Tout système oscillant est composé d'un élément passif qui dissipe de l'énergie: le résonateur, et d'un élément actif qui apporte de l'énergie: l'amplificateur. Dans le cas d'un oscillateur électronique, le résonateur est en général un filtre et l'amplificateur est souvent un amplificateur opérationnel ou un transistor.

2.4.1 Le critère d'oscillation de Barkhausen

La figure 2.9 montre la représentation la plus élémentaire d'un oscillateur électronique, l'élément $A(j\omega)$ est la fonction de transfert de l'amplificateur et l'élément $B(j\omega)$ est la fonction de transfert d'un filtre. Supposons que les différentes grandeurs soient sinusoïdales c'est-à-dire : $V_2 = |A| e^{j\phi_A} V_1$ et $V_3 = |B| e^{j\phi_B} V_2$ et donc : $V_3 = |A||B| e^{j(\phi_A+\phi_B)} V_1 = V_1$. Le critère d'oscillation de Barkhausen nécessite donc deux conditions :

$$\begin{cases} |A|.|B| = 1 \\ \phi_A + \phi_B = 0 + 2k\pi \qquad k \in \mathbb{Z} \end{cases} \tag{2.2}$$

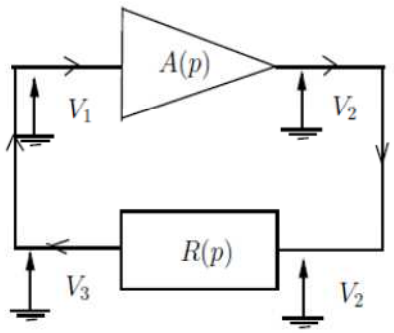


Figure 2.9 - Oscillateur électronique: modèle de Barkhausen

Cependant, dans la pratique, les oscillations prennent naissance à partir de fluctuations qui sont amplifiées, ce qui nécessite comme condition d'oscillation: $|A|.|B| > 1$. Mais les oscillations ne peuvent croitre indéfiniment, elles s'arrêtent sur

une non-linéarité de l'amplificateur .Cela signifie que dans un oscillateur, l'amplificateur possède toujours une caractéristique non linéaire. Une conséquence directe est que tout oscillateur est potentiellement chaotique car tout système chaotique est nécessairement non linéaire.

2.4.2 Conditions d'oscillations de l'oscillateur de Colpitts

La structure générale d'un oscillateur Colpitts est représenté sur la figure 2.10 où la caractéristique non linéaire qui peut être celle d'un amplificateur à base de transistor bipolaires ou à effet de champ est définie par $i_2 = gV_1$, g étant la transconductance du transistor.

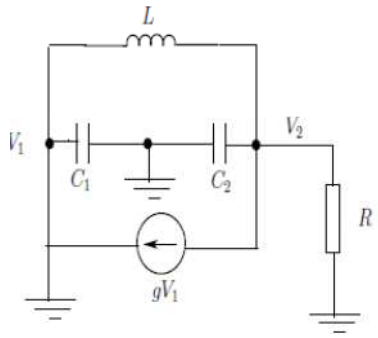


Figure 2.10 - Schéma de principe de l'oscillateur de Colpitts

En utilisant la loi de Kirchoff, nous écrivons les équations aux nœuds aux deux extrémités de l'inductance *L* :

$$\begin{cases} -gV_1 - \frac{V_2}{R} - jC_2\omega V_2 + \frac{V_1 - V_2}{jL\omega} = 0 \\ \frac{V_2 - V_1}{jL\omega} - jC_1\omega V_1 + gV_1 = 0 \end{cases} \tag{2.3}$$

En calculant V_2 dans la deuxième équation et en remplaçant dans la première équation, on obtient l'expression suivante :

$$\left[-g + \frac{1}{jL\omega}\right] - \left[jC_1\omega + \frac{1}{jL\omega}\right]\left[\frac{1}{R} + jC_2\omega + \frac{1}{jL\omega}\right] = 0 \tag{2.4}$$

En annulant la partie imaginaire de (2.4), on obtient :

$$C_1C_2RL\omega^2 - \left(C_1 + C_2\right)R\omega = 0$$

D'où la pulsation d'oscillation de l'oscillateur Colpitts :

$$\omega_0 = \frac{1}{L\dfrac{C_1C_2}{C_1 + C_2}} \tag{2.5}$$

qui correspond à la pulsation d'accord de l'inductance accordée par les deux condensateurs en série.

En annulant la partie réelle de l'équation (2.4), on obtient la relation suivante :

$$-Rg + LC_1\omega_0^2 - 1 = 0 \;\Rightarrow\; R = \frac{LC_1\omega_0^2 - 1}{g} \tag{2.6}$$

qui représente la condition d'oscillation du montage Colpitts. En effet, l'oscillation démarre lorsque la valeur de *R* est supérieure à la valeur obtenue par (2.6). En remplaçant ω_0 dans (2.6), on détermine la condition d'oscillation suivante :

$$gR > \frac{C_1}{C_2} \tag{2.7}$$

2.4.3 Equations d'état de l'oscillateur Colpitts

Pour décrire le modèle mathématique de l'oscillateur de Colpitts, nous écrivons ces équations d'état en considérant les variables d'état V_{C1}, V_{C2} et I_L (figure 2.7). Les équations d'état sont alors données par :

$$\begin{cases} \dfrac{dV_{C1}}{dt} = -\dfrac{1}{C_1} f(-V_{C2}) + \dfrac{1}{C_1} I_L \\ \dfrac{dV_{C2}}{dt} = \dfrac{1}{C_2} I_L - \dfrac{1}{C_2} I_0 \\ \dfrac{dI_L}{dt} = -\dfrac{1}{L} V_{C1} - \dfrac{1}{L} V_{C2} - \dfrac{R}{L} I_L + \dfrac{E_2}{L} \end{cases} \tag{2.8}$$

où $f(-V_{C2})$ est la caractéristique courant-tension du transistor permettant de calculer le courant d'émetteur donnée par :

$$I_E = f(V_{BE}) = f(-V_{C2}) = I_S\left[\exp(\frac{V_{BE}}{V_T}) - 1\right] \simeq I_S\left[\exp(\frac{V_{BE}}{V_T})\right] \simeq I_S\left[\exp(\frac{-V_{C2}}{V_T})\right] \qquad (2.9)$$

où I_S est le courant de saturation inverse de la jonction base-émetteur du transistor et $V_T \simeq 27mV$ à la température ambiante. Dans [25] [26], Maggio et al. ont normalisé le modèle mathématique de l'oscillateur de Colpitts. Pour cela, les tensions, le courant et le temps sont respectivement normalisés par rapport à $V_{ref} = V_T, I_{ref} = I_0$ et $t_{ref} = \frac{1}{\omega_0}$ où ω_0 représente la pulsation d'oscillation. Le point de fonctionnement du système (2.8) est donné par :

$$\begin{cases} V_{C1o} = V_{CC} - \alpha R I_0 + V_T Ln(\alpha \frac{I_0}{I_S}) \\ V_{C2o} = -V_T Ln(\alpha \frac{I_0}{I_S}) \\ I_{Lo} = \alpha I_0 \end{cases} \qquad (2.10)$$

où α est le gain en courant du transistor en base commune. Par la suite, nous considérons $\alpha \simeq 1$, ce qui signifie que l'on néglige le courant de base du transistor. Les trois variables d'état sans dimensions (x_1, x_2, x_3) s'écrivent alors :

$$\begin{cases} x_1(t) = \frac{1}{V_T}\left[V_{C1}(\omega_0 t) - V_{C1o}\right] \\ x_2(t) = \frac{1}{V_T}\left[V_{C2}(\omega_0 t) - V_{C2o}\right] \\ x_3(t) = \frac{1}{I_0}\left[I_L(\omega_0 t) - I_{Lo}\right] \end{cases} \qquad (2.11)$$

En combinant les équations (2.8) et (2.11), nous obtenons le système normalisé ci-dessous :

$$\begin{cases} \dot{x}_1 = \dfrac{g}{Q(1-k)}\left[-n(x_2)+x_3\right] \\ \dot{x}_2 = \dfrac{g}{Qk}x_3 \\ \dot{x}_3 = -\dfrac{Qk(1-k)}{g}\left(x_1+x_2\right)-\dfrac{1}{Q}x_3 \end{cases} \tag{2.12}$$

avec $n(x_2)=\exp(-x_2)-1$ et $k=\dfrac{C_2}{C_1+C_2}$. Le paramètre *g* est le gain de la boucle de réaction lorsque le critère de Barkhausen est satisfait, et $Q=\dfrac{L\omega_0}{R}$ est le facteur de qualité di circuit $L-C$ non chargé. Il y a alors des oscillations sinusoïdales lorsque $g=1$. Dans ce cas une bifurcation de Hopf apparait. Le point d'équilibre situé à l'origine se transforme en un cycle limite. Si l'on considère I_0 comme une source de courant idéale, le paramètre g se calcule par [25] :

$$g=\frac{LI_0}{(C_1+C_2)RV_T}$$

2.5 Comportement chaotique de l'oscillateur de Colpitts

2.5.1 Linéarisation du système non linéaire

Le point d'équilibre du système (2.12) est situé à l'origine (0, 0, 0) après l'application du changement de coordonnées indiquée en (2.11). Il est alors possible de linéariser ce système autour du point d'équilibre en utilisant sa matrice jacobienne. Nous pouvons donc étudier le comportement du système linéarisé $\dot{x}=Ax$.

La matrice jacobienne de (2.12) au point d'équilibre (0, 0, 0) est calculée par :

$$A=\begin{pmatrix} 0 & \frac{g}{Q(1-k)} & \frac{g}{Q(1-k)} \\ 0 & 0 & \frac{g}{Qk} \\ -\frac{Qk(1-k)}{g} & -\frac{Qk(1-k)}{g} & -\frac{1}{Q} \end{pmatrix} \qquad (2.13)$$

D'où, l'équation caractéristique de la matrice A :

$$\lambda^3+\frac{\lambda^2}{Q}+\lambda+\frac{g}{Q}=0$$

Pour $g=1$, les valeurs propres de A sont :

$$\lambda_1=j\ ;\ \lambda_2=-j\ ;\ \lambda_3=-\frac{1}{Q}$$

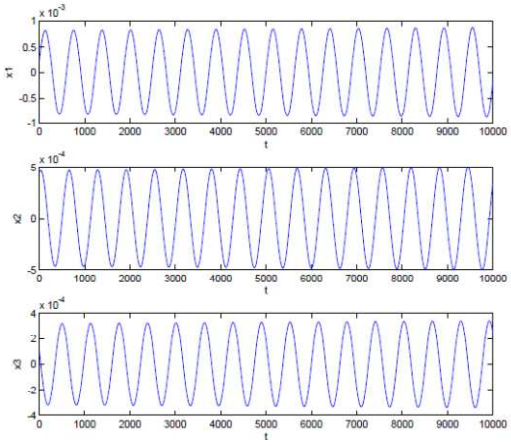
Le point d'équilibre est ainsi caractérisé par des valeurs propres purement imaginaires (λ_1,λ_2), ce qui justifie l'apparition des oscillations sinusoïdales pour $g=1.$

2.5.2 Evolution vers le chaos de l'oscillateur de Colpitts

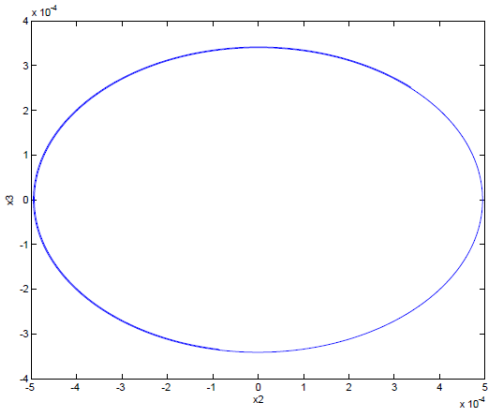
En faisant varier les paramètres g et Q du système (2.12), nous obtenons différents types d'oscillations. Ces comportements montrent la bifurcation des oscillations périodiques par rapport à l'oscillation sinusoïdale qui correspond au cycle limite [25].

Afin d'obtenir par simulation différents comportement pour l'oscillateur de Colpitts, nous fixons *L* = 1mH, C_1 = C_2 = 470nF. La fréquence d'oscillation est alors :

$$f_0=\frac{1}{2\pi\sqrt{L\frac{C_1C_2}{C_1+C_2}}}$$



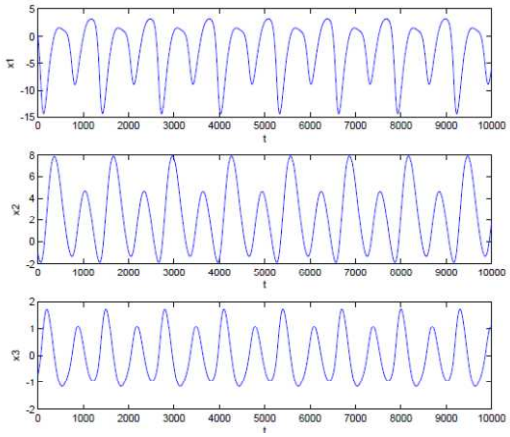
a) Réponses temporelles

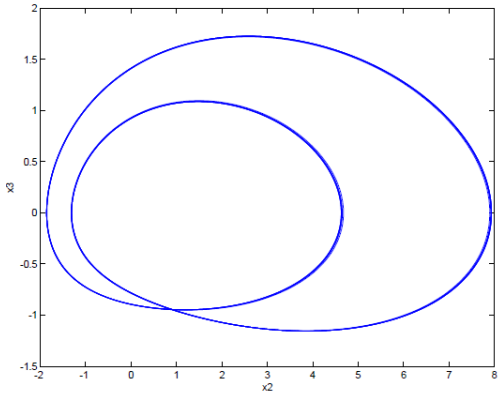


b) Plan de phase

Figure 2.11 - Réponses temporelles et plan de phase pour $g = 1.003$

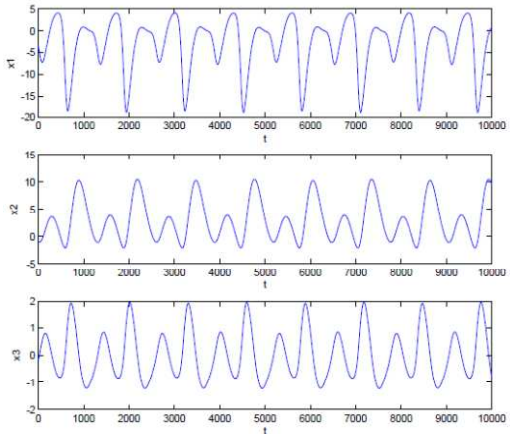
La valeur de Q est obtenue en remplaçant les valeurs ci-dessus dans $Q = \frac{2\pi f_0 L}{R}$. Pour ces valeurs, nous obtenons $Q = 1.38$. Ainsi, nous faisons varier le paramètre *g*, qui lui-même dépend de du courant I_0, soit le terme non linéaire du système d'équations (2.12). Pour démarrer l'oscillation, nous avons fixé la valeur de *g* légèrement supérieur à 1, pour satisfaire la condition de Barkaussen. Les résultats obtenus pour différentes valeurs de g sont donnés par les figures ci-dessous. Pour $g = 1.003$, la condition de Barkaussen est vérifiée, donc le système présente des oscillations sinusoïdales au niveau des réponses temporelles (figure 2.11a) et, par conséquent, un cycle limite dans le plan de phase $x_2 - x_3$ (figure 2.11b). En augmentant la valeur de g à 2.15, le système présente des oscillations sinusoïdales à deux périodes (figure 2.12a) correspondant à 2 cycles limites dans le plan de phase (figure 2.12b). Pour $g = 2.4$, le système oscille avec 4 périodes (figure 2.13a) correspondant à 4 cycles limites dans le plan de phase (figure 2.13b). Mais pour $g = 4.5$, le système présente un comportement chaotique (figure 2.14a) correspondant à un attracteur chaotique étrange dans le plan de phase (figure 2.14b).

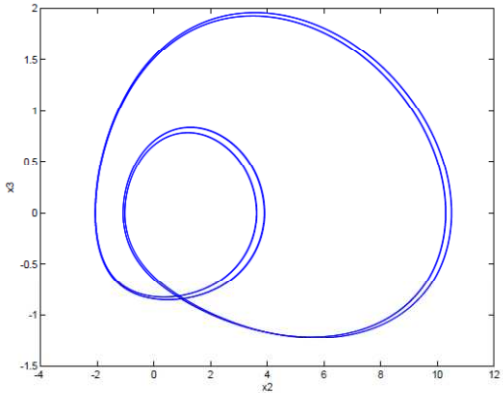




a) Réponses temporelles b) Plan de phase

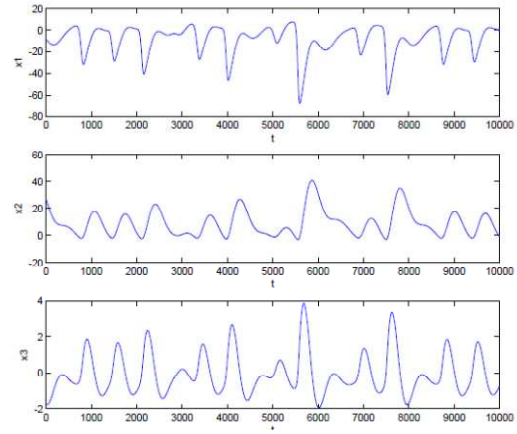
Figure 2.12 - Réponses temporelles et plan de phase pour $g = 2.15$

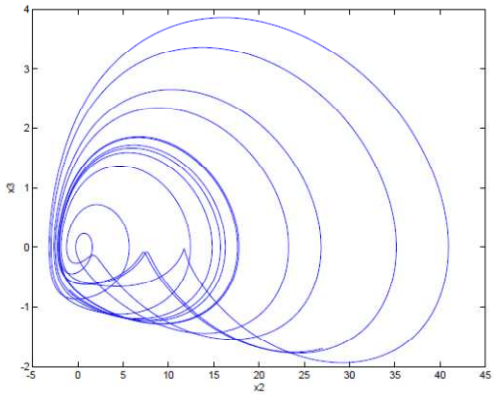




a) Réponses temporelles b) Plan de phase

Figure 2.13 - Réponses temporelles et plan de phase pour $g = 2.4$





a) Réponses temporelles b) Plan de phase

Figure 2.14 - Réponses temporelles et plan de phase pour $g = 4.5$

2.6 Calcul des exposants de Lyapunov

Il existe des algorithmes numériques pour calculer les exposants de Lyapunov d'un système dynamique, à partir de son modèle dynamique. En utilisant un programme de la bibliothèque Matlab appliqué à l'oscillateur chaotique de Colpitts et en introduisant les éléments de la matrice jacobienne, nous obtenons les exposants de Lyapunov.

Pour $Q = 1.38$, nous obtenons : $\lambda_1 = 0,2794$, $\lambda_2 = 0.2705$ et $\lambda_3 = -1.274$. Les deux premiers exposants sont positifs et justifient le comportement hyper-chaotique de l'oscillateur de Colpitts pour les paramètres donnés ci-dessus. Ceci justifie aussi les résultats obtenus par le calcul des valeurs propres de la matrice jacobienne.

2.7 Section de Poincaré pour l'oscillateur de Colpitts

Le point d'équilibre de l'oscillateur Colpitts est situé à l'origine $O(0,0,0)$ et correspond au point d'opération du système. De plus, l'espace des phases se divise en deux régions correspondant aux différents modes d'opération du transistor [26] [27]. Pour $x_2 \leq 1$, le transistor fonctionne dans sa région active et pour $x_2 > 1$,il est dans la région bloquée. Cela peut être vérifié dans la figure 2.15. Dans la région active, les trajectoires sont accélérées par l'énergie fournie par le transistor, alors que dans la région non active, elles évoluent grâce aux oscillations naturelles du circuit $L - C$ non chargé.

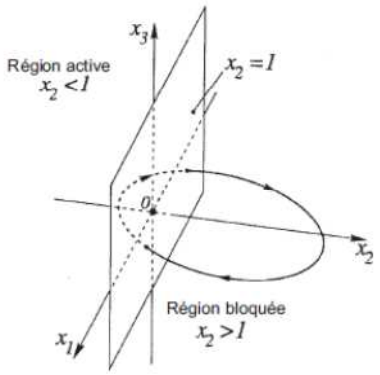


Figure 2.15 - Zones de fonctionnement de l'oscillateur Colpitts

Ainsi, d'après ces définitions, nous pouvons obtenir la section de Poincaré pour les différents comportements de l'oscillateur de Colpitts. Notons que la section de Poincaré est obtenue dans un sens, c'est à dire pour $\dot{x}_2 > 0$. La section de Poincaré pour $g = 4.45$ (comportement chaotique) est représentée sur la figure 2.16.

D'après cette figure la section de Poincaré comprend plusieurs points, contrairement au comportement périodique (cycle limite) qui aurait donné lieu à un seul point.

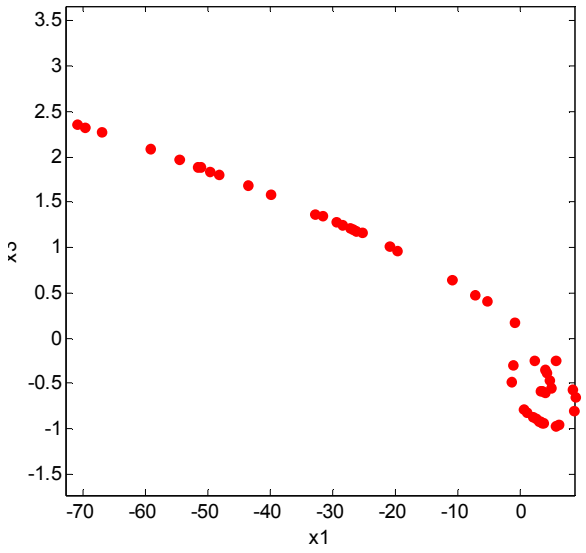


Figure 2.16 - Section de Poincaré de l'oscillateur chaotique de Colpitts

2.8 Diagramme de bifurcation de l'oscillateur de Colpitts

Pour montrer la route vers le chaos (diagramme de bifurcations) de l'oscillateur de Colpitts, nous avons observé son comportement en faisant varier le paramètre Q. Pour cela, nous avons discrétisé ce paramètre dans nos simulations.

Nous avons utilisé un pas de 0.01 afin d'échantillonner Q. Le diagramme de bifurcation de la figure 2.17 est obtenu. Ce diagramme montre la projection des variations de l'état x_3 du système (2.11) en fonction de Q, sur le plan $x_2 = 1$ de la figure 2.13. En fonction des valeurs de Q, différents régimes de fonctionnement sont obtenus pour l'oscillateur de Colpitts.

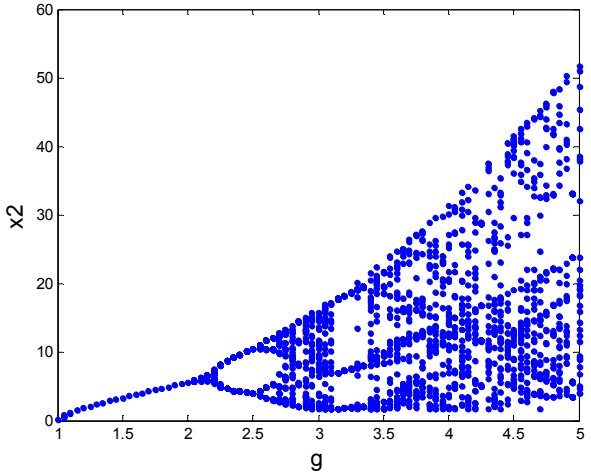


Figure 2.17 - Diagramme de bifurcation de l'oscillateur de Colpitts

2.9 Inclusion du message dans l'émetteur chaotique

Pour inclure le signal du message m dans l'oscillateur de Colpitts, la structure utilisée peut être considérée comme une combinaison des méthodes par addition et par modulation chaotique. Après avoir ajusté les paramètres pour obtenir un comportement chaotique, le signal *m* est ajouté à la dérivée de l'état x_1 du système (2.12). En utilisant cet état, la condition de recouvrement d'observabilité (observability matching condition) est respectée. Cette condition, qui sera expliquée en détail au chapitre suivant, permet de retrouver le message au niveau du récepteur. Ainsi l'état x_1 est modulé en fonction du message m. De ce fait, la méthode ressemble à la modulation d'un état chaotique ; par contre, le signal transmis au récepteur est l'état x_2, ce qui veut dire que l'on ne transmet pas directement l'état modulé au récepteur. Cela fait une différence entre notre approche et la méthode par addition dans laquelle le message est ajouté à la sortie de l'émetteur et la somme est transmise directement au récepteur. Il est important de noter que l'amplitude et la fréquence du message doivent être choisies de telle manière que l'on ne puisse pas détecter de variations visibles relatives au message sur la sortie du système, et aussi que le message ne nous fasse pas sortir du bassin d'attraction de l'attracteur étrange[28]. Le système (2.12) devient alors :

$$\begin{cases} \dot{x}_1 = \dfrac{g}{Q(1-k)}\left[-n(x_2)+x_3\right]+m \\ \dot{x}_2 = \dfrac{g}{Qk}x_3 \\ \dot{x}_3 = -\dfrac{Qk(1-k)}{g}\left[x_1+x_2\right]-\dfrac{1}{Q}x_3 \\ y = x_2 \end{cases} \tag{2.14}$$

Expérimentalement, l'ajout du message à la dérivée de x_1 correspond à l'inclusion d'un courant I_m dans le signal chaotique généré au nœud V_{C1} de l'oscillateur de Colpitts, dont les paramètres sont ajustés afin d'obtenir un régime chaotique.

2.10 Conclusion

Dans ce chapitre, nous avons présenté les principales méthodes de transmission d'information par les signaux chaotiques. Nous avons ensuite expliqué le principe de fonctionnement de l'oscillateur de Colpitts en étudiant les différents comportements de cet oscillateur en fonction de variations de ses paramètres. Ces études ont été mises en évidence à l'aide de simulations. Nous avons ajusté les paramètres de l'oscillateur de Colpitts afin d'obtenir un comportement chaotique. L'oscillateur de Colpitts incluant le message sera par la suite utilisé en tant qu'émetteur de notre système de communication.

CHAPITRE 3

SYNCHRONISATION CHAOTIQUE :

ETUDE DU RECEPTEUR

3.1 Introduction

Depuis quelques années, la théorie des systèmes chaotiques a été appliquée dans le domaine des communications. La synchronisation des systèmes chaotiques semble impossible dans un premier temps, notamment à cause de la sensibilité de ces systèmes aux conditions initiales. De plus, un système chaotique n'est pas asymptotiquement stable, c'est-à-dire que les trajectoires issues des conditions initiales voisines (légèrement différentes) divergent exponentiellement avec le temps. En effet, on peut dire que pour les systèmes réels, il n'est pas facile de produire et de reproduire les mêmes conditions de démarrage. D'après ce point de vue, tout changement de paramètre dans un système chaotique pourrait conduire à une divergence entre ces trajectoires. Pourtant ce raisonnement n'est pas correct. Il peut exister des conditions sous lesquelles les trajectoires de deux systèmes chaotiques différents peuvent converger l'une vers l'autre, si certaines informations (énergie) pertinentes sont échangées. En 1983, Chua a abordé la question de synchronisation en utilisant des circuits électriques linéaires par morceaux [29]. Dans les années 90, Pecora et Caroll ont montré que deux systèmes chaotiques pourraient se synchroniser sous certaines conditions, si l'un deux est piloté par au moins une composante (une ou plusieurs variables d'état) de l'autre [8] [30].

Depuis les années 90, de nombreux ouvrages ont été publiés au sujet de la synchronisation chaotique [31] [32]. Une raison importante de l'attirance des chercheurs vers la synchronisation des systèmes chaotiques est son application à la

communication sécurisée [33] [34]. Les travaux de Pecora et Caroll ont permis de suggérer que les systèmes chaotiques pourraient être utilisés dans la *communication*, où leur nature semblable aux bruits améliorerait la sécurité et le rejet des perturbations. En effet, une fois la synchronisation entre l'émetteur et le récepteur atteinte, il est possible de récupérer un message masqué par l'émetteur chaotique.

Ce chapitre présente les principales méthodes de synchronisation de systèmes chaotiques et en particulier l'utilisation d'observateurs pour reconstruire les états de l'émetteur chaotique et le message. Pour cela, nous vérifions l'observabilité de l'oscillateur de Colpitts chaotique et les conditions de recouvrement d'observabilité et d'inversibilité à gauche de notre émetteur chaotique. Nous utilisons ensuite un observateur à modes glissants que nous avons étudié par simulation et appliqué à notre émetteur. Les résultats de simulations seront présentés et commentés à la fin de ce chapitre.

3.2 Méthodes de synchronisation chaotique

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

En plus du couplage simple (par résistance ou suiveur), d'autres méthodes ont été proposées pour la synchronisation des systèmes chaotiques. Ainsi pour la

synchronisation unidirectionnelle, on peut citer la méthode par décomposition du système [8] [30], la synchronisation impulsive [34], la synchronisation par des méthodes itératives [36] ou la synchronisation par la boucle fermée. Dans la majorité des cas, les deux systèmes doivent avoir des structures identiques, ce qui n'est pas tout à fait réalisable en pratique. Un petit écart entre les valeurs des composants peut entraîner un écart considérable entre les comportements des deux circuits et détruire le phénomène de synchronisation. La synchronisation peut être décrite par la définition suivante :

Définition 3.1 : Considérons les deux systèmes suivants :

$$\begin{cases} \dot{x} = f_1(x) \\ \dot{z} = f_2(z) \end{cases} \tag{3.1}$$

avec $x, z \in \mathbb{R}^n$, f_1 et f_2 sont des fonctions non linéaires définies de $\mathbb{R}^n \to \mathbb{R}^n$. Les deux systèmes sont dits synchronisés si :

$$\lim_{t\to\infty} = \left\| z(t) - x(t) \right\| = 0 \tag{3.2}$$

où $z(t) - x(t)$ représente l'erreur de synchronisation.

3.2.1 Synchronisation par couplage bidirectionnel

Pour expliquer la synchronisation bidirectionnelle (mutuelle) de deux systèmes chaotiques, on considère les deux systèmes donnés ci-dessous :

$$\begin{cases} \dot{x} = f(x) + \lambda(z - x) \\ \dot{z} = g(z) + \mu(x - z) \end{cases} \tag{3.3}$$

où $x, z \in \mathbb{R}^n$ et λ, μ sont des matrices diagonales $n \times n$, $\lambda = diag\left[\lambda_i\right]$, $\mu = diag\left[\mu_i\right]$, $i = 1, 2, ...n.$ On suppose que $f(0) = g(0) = 0$. Du point de vue de l'ingénierie électronique, ce type de synchronisation définit l'évolution temporelle de deux circuits électroniques couplés à l'aide d'une résistance. Le problème de synchronisation consiste alors à trouver λ et μ de telle manière que $\lim_{t\to\infty} = \left\| z(t) - x(t) \right\| = 0$. Cette méthode a été étudiée dans [35] et a été appliquée à

l'oscillateur de Colpitts dans [36] [37]. La figure 3.1 illustre ce type de synchronisation.

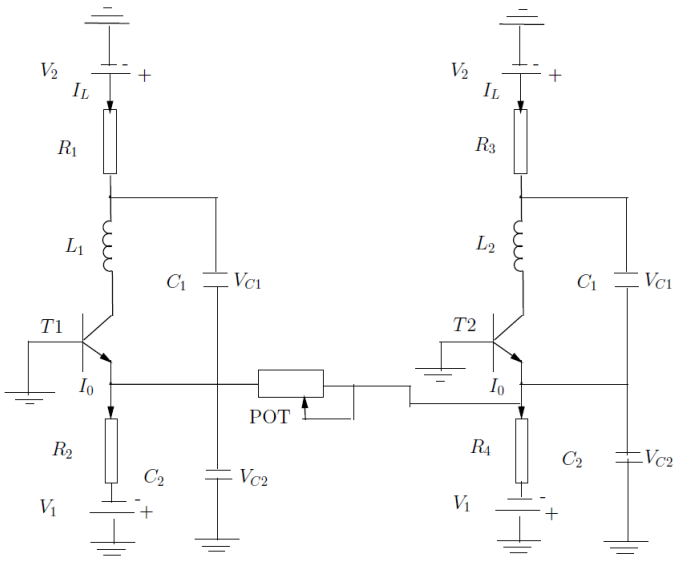


Figure 3.1 - Couplage bidirectionnel de deux oscillateurs de Colpitts

Les résultats obtenus montrent que pour avoir une synchronisation bidirectionnelle, la résistance de couplage POT doit être très faible ($POT = 36\Omega$) pour que l'échange de l'énergie ait lieu dans les deux sens.

Lorsque les deux oscillateurs sont synchronisés, la dimension du système global, constitué des deux oscillateurs couplés, passe de 6 à 3.

3.2.2 Synchronisation par couplage unidirectionnel

La synchronisation unidirectionnelle des systèmes chaotiques est basée sur l'injection d'une partie du signal d'erreur dans le système esclave (celui qui doit se synchroniser avec l'autre). Mathématiquement parlant, on peut considérer les deux systèmes donnés ci-dessous :

$$\begin{cases} \dot{x} = f_1(x) \\ \dot{z} = f_2(z) + \alpha(x - z) \end{cases} \tag{3.4}$$

où $x, z \in \mathbb{R}^n$, $\alpha = diag\left[\alpha_1, \alpha_2, ..., \alpha_n\right]^T$. Le problème de synchronisation consiste alors à trouver α tel que $\lim_{t\to\infty} = \left\|z(t) - x(t)\right\| = 0$. Ce type de synchronisation a été appliqué au circuit de Chua [38] et a été également étudié par Koracev et al. dans [35]. Les conditions de convergence de cette approche sont analysées dans [39].

L'exemple donné ci-après illustre de façon simple la différence entre la synchronisation par couplage unidirectionnel et bidirectionnel.

Exemple 3.1 : Soient deux systèmes chaotiques identiques *a* et *b* de dimension 3, décrits par $\dot{x}_a = f(x_a)$ et $\dot{x}_b = f(x_b)$. Le schéma de couplage des deux systèmes est montré dans les figures 3.2(a) (couplage unidirectionnel) et 3.2(b) (couplage bidirectionnel). Le couplage de ces systèmes peut être exprimé par les équations suivantes :

$$\begin{cases} \dot{x}_{1a} = f_1(x_a) + k_{a1}(x_{1b} - x_{1a}) \\ \dot{x}_{2a} = f_2(x_a) + k_{a2}(x_{1b} - x_{1a}) \\ \dot{x}_{3a} = f_3(x_a) + k_{a3}(x_{1b} - x_{1a}) \end{cases} \tag{3.5}$$

$$\begin{cases} \dot{x}_{1b} = f_1(x_b) + k_{b1}(x_{1a} - x_{1b}) \\ \dot{x}_{2b} = f_2(x_b) + k_{b2}(x_{1a} - x_{1b}) \\ \dot{x}_{3b} = f_3(x_b) + k_{b3}(x_{1a} - x_{1b}) \end{cases} \tag{3.6}$$

où k_{ai}, k_{bj} sont appelés constantes de couplage. Si les coefficients $k_{ai} = 0$ pour $i = 1, 2, 3$, il existe alors un couplage unidirectionnel du système (*a*) au système (*b*), car l'état de (*a*) influence le système (*b*) tandis que le système (*b*) n'a aucune influence sur le système (*a*). Le système (*a*) est alors le maître (ou l'émetteur) et le système (*b*) est l'esclave (ou le récepteur).

Si $k_{ai} \neq 0$ et $k_{bi} \neq 0$ pour au moins une valeur de $i = 1, 2, 3$ et au moins une valeur de $j = 1, 2, 3$, alors un couplage bidirectionnel est établi entre les deux systèmes, c'est à dire que chaque système est influencé par l'autre et vice versa.

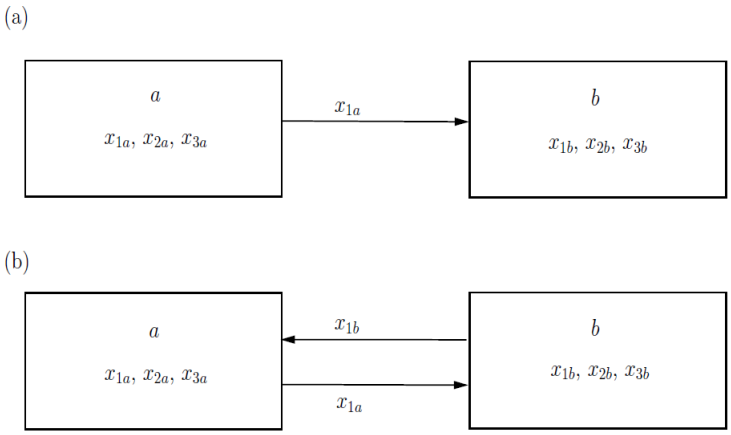


Figure 3.2 - Schéma de couplage : (a) unidirectionnel, (b) bidirectionnel

Lorsque la synchronisation des deux systèmes est atteinte, les termes de couplage contenant les coefficients *k* deviennent nuls. Cela veut dire que $x_a = x_b$ et qu'un comportement commun est obtenu pour les deux systèmes. En effet la dimension du système est réduite de 6 à 3.

3.2.3 Synchronisation par décomposition du système

Cette méthode introduite par Pecora et Carroll suggèrent qu'il est possible de construire un ensemble de systèmes dynamiques chaotiques tels que leurs signaux communs soient synchronisés. Ils considèrent un système de dimension *m* de la forme :

$$w(t) = \begin{pmatrix} x(t) \\ z(t) \end{pmatrix} \tag{3.7}$$

dans lequel $x(t)$ est de dimension m_1 et z est de dimension m_2, tel que $m = m_1 + m_2$. Ainsi, le système w est décomposé en deux sous systèmes x et z . Aussi, le système $\dot{w} = f(w)$ (de dimension m) est supposé chaotique. Les équations des sous-systèmes sont données par :

$$\begin{cases} \dot{x} = G(x,z) \\ \dot{z} = H(x,z) \end{cases} \tag{3.8}$$

d'où :

$$\dot{w} = f(w) = \begin{pmatrix} G(x,z) \\ H(x,z) \end{pmatrix} \tag{3.9}$$

Le système (3.9) est appelé pilote. On considère un système de réponse $\hat{z}$ comme étant une copie du sous-système z. Le système $\hat{z}$, piloté par l'état $x(t)$ du sous-système x, est défini par :

$$\dot{\hat{z}} = H(x,\hat{z}) \tag{3.10}$$

Le schéma de cette méthode est représenté sur la figure 3.3. Le système (3.10) se synchronise alors avec le système (3.9) lorsque :

$$\lim_{t\to\infty} \left\| z(t) - \hat{z}(t) \right\| = 0 \tag{3.11}$$

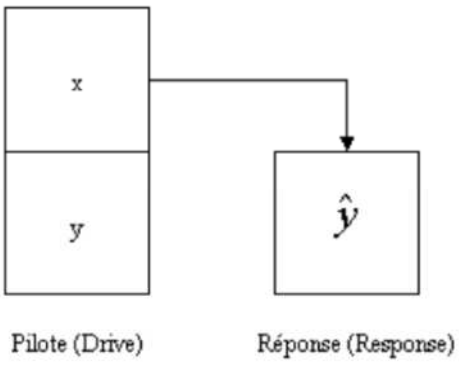


Figure 3.3 - Synchronisation par décomposition du système chaotique

L'approche de la synchronisation par décomposition du système chaotique n'est pas toujours facile et possible à mettre en œuvre. La méthode de Pecora et arroll a été appliquée à plusieurs systèmes comme le circuit de Chua [21], le système de Lorenz et Rossler [40], etc.

3.2.4 Approche utilisant des observateurs

Nijmeijer et Mareels [41] ont montré que la théorie de l'estimation non linéaire peut être naturellement utilisée dans le domaine de la synchronisation des systèmes chaotiques. En effet, le récepteur peut être une copie de l'émetteur, mais ce n'est pas une nécessité : il suffit que le récepteur, à partir du signal transmis, se synchronise avec la dynamique de l'émetteur. Il s'agit donc bien d'un problème d'observation. Cette approche étant celle utilisée dans le cadre de notre projet, elle sera détaillée dans la section suivante.

3.3 Synchronisation chaotique à l'aide d'observateur

L'utilisation des observateurs est proposée pour estimer les états inconnus d'un système qui ne sont pas mesurables directement. Un système dynamique est dit observable si on peut récupérer toutes ses grandeurs (de façon statique ou dynamique) par une combinaison de mesures de ses sorties et de leurs dérivées.

En 1997, Nijmeijer et Mareels ont montré que la synchronisation unidirectionnelle de deux systèmes chaotiques peut être considérée comme un problème d'observateur non linéaire [41] et par conséquent, les théories de l'automatique peuvent être utilisées afin d'analyser ce phénomène. La figure 3.4 illustre ce principe de synchronisation.

Plusieurs types d'observateurs non linéaires ont été rapportés dans la littérature :

- L'observateur de Kalman étendu.
- Les observateurs reposant sur une approche analytique.
- Les observateurs à grands gains.
- Les observateurs à modes glissants.
- Les observateurs adaptatifs.
- Les observateurs algébriques.
- Les observateurs numériques.

Ainsi, l'émetteur et le récepteur se synchronisent si le système $\dot{\hat{x}} = \hat{f}(\hat{x}, u)$ (défini au niveau du récepteur) est un observateur convergent pour le système $\dot{x} = f(x, u)$ (défini au niveau de l'émetteur). Autrement dit, le problème de synchronisation revient à déterminer une fonction $\hat{f}$ telle que :

$$\lim_{t \to \infty} \left\| x(t) - \hat{x}(t) \right\| = 0 \tag{3.12}$$

Les différents observateurs (en temps continu et en temps discret) cités précédemment ont été conçus dans le but de réaliser des systèmes de transmissions sécurisées.

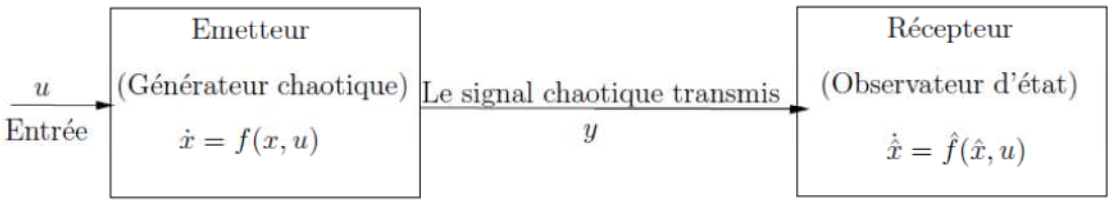


Figure 3.4 - Principe de synchronisation à base d'observateurs

Dans ce qui suit, nous allons rappeler quelques définitions liées à la notion d'observabilité et les conditions de recouvrement d'observabilité des systèmes non linéaires.

3.3.1 Observabilité des systèmes linéaires

Soit un système continu décrit par l'équation d'état déterministe suivante:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) \end{cases} \tag{3.13}$$

où les vecteurs $x(t) \in \mathbb{R}^n, u(t) \in \mathbb{R}^m$ et $y(t) \in \mathbb{R}^p$ représentent respectivement l'état, la commande et la sortie du système. Les matrices A, B et C sont des matrices constantes de dimensions appropriées. L'observabilité du système linéaire (3.13) est garantie si et seulement si :

$$rang(O) = rang\left(\begin{bmatrix} C \\ CA \\ \vdots \\ CA^{n-1} \end{bmatrix}\right) = n \tag{3.14}$$

Par conséquent le système linéaire (3.14) est observable, si le rang de la matrice d'observabilité O est égal à la dimension n de ce système. Dans le cas où le rang de la matrice O est inférieur à *n*, on parle alors d'observabilité partielle.

3.3.2 Observabilité des systèmes non linéaires

Considérons maintenant le système non linéaire :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \tag{3.15}$$

dans lequel $x \in M \subseteq \mathbb{R}^n$ et $y \in \mathbb{R}^p$ représentent respectivement l'état et la sortie du système. Les fonctions f et h sont des vecteurs de fonctions analytiques de dimensions appropriées. Notons que pour tout $x^0 \in M$, il existe une solution pour $\dot{x} = f(x(t))$ telle que $x(0) = x^0$ et $x(t) \in M$ pour tout $t \in \mathbb{R}$. On note U un sous-ensemble ouvert de M. Pour tout $x \in \mathbb{R}^n$, le système (3.15) est supposé avoir des états bornés en temps fini. Le problème d'observabilité consiste à pouvoir récupérer tous les états du système à partir de la sortie et de ses dérivées. Par ailleurs, toutes les définitions d'observabilité sont basées sur la notion d'indiscernabilité entre deux états initiaux.

Pour déterminer la condition de rang d'observabilité, nous définissons tout d'abord la dérivée de Lie qui est une notion largement utilisée dans l'étude d'observabilité des systèmes non linéaires.

Définition 3.2 (Dérivée de Lie) : Considérons h une fonction C^∞ de $\mathbb{R}^n$ dans $\mathbb{R}$. On définit la dérivée de Lie de h dans la direction de f, notée $L_f h$, la dérivée de h le long de la courbe intégrale de f en $t = 0$:

$$L_f h(x) = \sum_{i=1}^{n} f_i(x) \frac{\partial h(x)}{\partial x_i} \tag{3.16}$$

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

Le système (3.15) satisfait la condition du rang d'observabilité si :

$$rang(O) = rang \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} \\ \vdots \\ dL_f^{\infty} h \end{pmatrix}_x = n \tag{3.17}$$

L'écriture de $dL_f^k h$ est donnée par le co-vecteur :

$$dL_f^k h = \left(\frac{\partial L_f^k h}{\partial x_1}, \frac{\partial L_f^k h}{\partial x_2}, \ldots, \frac{\partial L_f^k h}{\partial x_n} \right) \tag{3.18}$$

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

$$rang(O) = rang \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ \vdots \\ dL_f^{n-1} \end{pmatrix}_x = n \tag{3.19}$$

Remarque : Si la condition (3.19) est vérifiée (mais pas la condition (3.18)), cela signifie que les états à observer sont situés dans les termes dérivatifs d'ordre supérieur. Par conséquent, un observateur de dimension n ne suffira pas pour récupérer les états du système. Autrement dit, nous devons tenir compte de la perte d'observabilité lors de la conception de l'observateur. Cette perte d'observabilité peut

être utilisée dans la transmission sécurisée de données afin d'augmenter la robustesse et la confidentialité de la transmission [42].

Exemple 3.2 : Soit le système non linéaire :

$$\begin{cases} \dot{x}_1 = \dfrac{x_1^2}{2} + e^{x_2} + x_2 \\ \dot{x}_2 = x_1^2 \\ y = x_1 \end{cases} \tag{3.20}$$

Dans ce système, $h = \begin{bmatrix} x_1 & 0 \end{bmatrix}$ et $dh = \begin{bmatrix} 1 & 0 \end{bmatrix}$. En appliquant la condition de rang d'observabilité donnée en (3.19), on obtient :

$$O = \begin{pmatrix} dh \\ dL_f h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x_1 & \mathrm{e}^{x_2} + 1 \end{pmatrix} \tag{3.21}$$

On en déduit : $rang(O) = 2 = n.$ Le système est donc observable.

3.3.3 Cas d'un système non linéaire avec injection de sortie

Dans un système non linéaire avec injection de sortie, la non linéarité ne dépend que de la sortie disponible. Sous certaines conditions géométriques, il est aussi possible d'employer une transformation de coordonnées afin de réécrire le système (3.15) sous une telle forme [43]. On peut construire un observateur complet ou réduit pour un tel système [41]. Considérons le système (3.22) :

$$\begin{cases} \dot{x}(t) = Ex(t) + g(Cx(t), t) \\ y = Cx(t) \end{cases} \tag{3.22}$$

Avec :

$$E = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & \ddots & \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

$$C = (1 \;\; 0 \;\; 0 \;\; \dots \;\; 0) \in \mathbb{R}^{(1\times n)}$$

$$g(y,t) = (g_1(y,t) \;\; g_2(y,t) \;\; \dots \;\; g_n(y,t))^T$$

Si la paire de matrices (E, C) est observable, et grâce à la structure particulière du système (3.22), nous pouvons construire l'observateur complet suivant :

$$\begin{cases} \dot{\hat{x}}(t) = E\hat{x}(t) + g(y(t),t) + K(\hat{y}(t) - y(t) \\ y(t) = C\hat{x}(t) \end{cases} \tag{3.23}$$

La dynamique de l'erreur d'estimation $e = x - \hat{x}$ est calculée par :

$$\dot{e}(t) = (E + KC)e(t) \tag{3.24}$$

Il suffit alors de choisir K tel que $E + KC$ soit asymptotiquement stable [41]. Le cas d'un système avec les dynamiques d'erreur linéaires est également discuté dans [41]. Les systèmes avec injection de sortie sont très utiles et simples pour concevoir des observateurs. Cependant, certaines conditions nécessaires et suffisantes sont requises afin de transformer le système (3.15) en un système de la forme (3.22) [43].

3.3.4 Méthode d'inversion à gauche et condition de recouvrement d'observabilité

Dans la transmission de données par synchronisation de systèmes chaotiques, il est important de pouvoir estimer l'entrée inconnue du système en plus de la synchronisation des états. En effet, l'entrée inconnue peut être un défaut, une perturbation, ou dans notre cas, un message confidentiel. La transmission

d'information avec la méthode par inclusion est non seulement un problème d'observabilité mais aussi un problème d'inversion à gauche, c'est à dire reconstruire tous les états ainsi que le message inconnu à partir de la sortie du système et de ses dérivées [44].

Deux types d'observateurs ont été proposés pour les systèmes à entrée inconnue à savoir :

- les observateurs destinés à estimer seulement les états du système (sans tenir compte de l'entrée inconnue) [4].

- les observateurs destinés à l'estimation des états et de l'entrée inconnue [45].

Soit le système :

$$\begin{cases} \dot{x} = f(x,u) \ , x_0 \in D \subseteq \mathbb{R}^n \\ y(t) = h(x,u) \end{cases} \tag{3.25}$$

dans lequel $x \in \mathbb{R}^n$ est l'espace d'états, $u \in \mathbb{R}^m$ est le vecteur d'entrée, et $y \in \mathbb{R}^p$ représente la sortie du système, $t \in T = \left[0, t_f\right]$. Les fonctions $f(x,u), h(x,u)$ et $u(t)$ sont considérées suffisamment dérivables. Le problème d'inversion du système consiste à reconstruire x,u ou une partie de ceux-ci à partir de la sortie *y(t)* du système. Le système (3.25) génère le "mapping" suivant (pour la condition initiale x_0 connue) :

$$\phi(u) : U \subseteq C^N(T, \mathbb{R}^m) \rightarrow C^N(T, \mathbb{R}^p) : u \rightarrow x(t, x_0, u) \rightarrow y(t) = h(x,u)$$

Avant d'introduire les propriétés du système (3.25), on considère un ensemble de fonctions U définies sur le domaine D_α constitué de fonctions et de leurs dérivées d'ordre 1 à α. Alors nous avons : $U = U(D_\alpha)$ où :

$$D_0 = \bigcup_{t \in T} u(t) \ , D_1 = \bigcup_{t \in T} (u(t), \dot{u}(t)), \ldots, D_\alpha = \bigcup_{t \in T} (u(t), \ldots, u(t)^\alpha), D_i \subseteq \mathbb{R}^{(i+m)}$$

Définition 3.3 : Le système (3.25) est inversible dans le domaine $D \times D_\alpha \times T$ si pour tout $x_0 \in D$ et deux entrées différentes $u_1(t), u_2(t) \in D_\alpha$, il existe un instant $t \in T$ tel que $h(\phi(x_0, u_1) \neq h(\phi(x_0, u_2)$.

Nous écrivons maintenant le système (3.17) de la façon suivante :

$$\dot{x} = f(x) + p(x)m \quad , \quad \mathrm{y} = \mathrm{h(x)} \tag{3.26}$$

dans lequel l'entrée inconnue (message) est considérée être bornée, et les champs de vecteurs $f, p : U \subseteq \mathbb{R}^n \to \mathbb{R}^n$ et $h : U \subseteq \mathbb{R}^n \to \mathbb{R}$ sont des réels analytiques. Le vecteur de sortie de ce système est transmis au récepteur qui doit générer un vecteur de sortie qui convergera asymptotiquement vers le vecteur d'entrée de l'émetteur. Ce problème constitue le problème d'inversion à gauche.

Dans le système (3.26), on considère que *m* est continu, ou au moins continu par morceaux. Afin d'étudier l'observabilité de l'oscillateur de Colpitts et la condition de recouvrement d'observabilité de l'émetteur chaotique (oscillateur de Colpitts incluant le message), nous posons les hypothèses suivantes :

i) La perturbation (entrée inconnue $\rightarrow$message) est bornée.

ii) $span\left\{dh, dL_f h, \ldots, dL_f^{n-1} h\right\}$ est de rang *n*

iii) $((dh)^T, (dL_f h)^T, \ldots, (dL_f^{n-1} h)^T)^T \, p\big|_x = (0 \;\; 0 \;\; \cdots \;\; 0 \;\; \theta)^T$

où θ signifie une fonction non nulle presque partout dans $U \subseteq \mathbb{R}^n \to \mathbb{R}$.

La condition donnée dans l'hypothèse *(iii)* est appelée condition de recouvrement d'observabilité (observability matching condition en anglais). Cette condition garantie la propriété d'inversibilité à gauche, c'est à dire la possibilité de récupérer tous les états et le message à partir de y et de ses dérivées [45].

3.4 Etude de l'observabilité de l'émetteur chaotique

Les équations de l'émetteur chaotique à base de l'oscillateur Colpitts présentées dans le chapitre précédent (équation (2.11)) sont :

$$\begin{cases} \dot{x}_1 = \dfrac{g}{Q(1-k)}\left[-n(x_2) + x_3\right] \\ \dot{x}_2 = \dfrac{g}{Qk}x_3 \\ \dot{x}_3 = -\dfrac{Qk(1-k)}{g}\left[x_1 + x_2\right] - \dfrac{1}{Q}x_3 \end{cases} \tag{3.27}$$

C'est un système avec injection de sortie car le terme non linéaire $n(x_2)$ dépend uniquement de la sortie du système, soit $y = x_2$. De plus, les états du système sont bornés. Nous étudions d'abord l'observabilité de l'oscillateur de Colpitts. Pour cela, nous procédons de deux manières différentes pour étudier l'observabilité de ce système.

3.4.1 Etude du système linéarisé

Le point d'équilibre du système (3.27) est situé à l'origine $(0,0,0)$. Il est alors possible de linéariser le système en utilisant sa matrice jacobienne donnée en (2.12).

Afin d'étudier l'observabilité de l'oscillateur de Colpitts, nous étudions l'observabilité du système linéarisé $\dot{x} = Ax\ ;\ y = Cx$ dans lequel $C = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}$. Ainsi, nous calculons la matrice d'observabilité O de la manière suivante :

$$O = \begin{pmatrix} C \\ CA \\ CA^2 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \dfrac{g}{Qk} \\ -(1-k) & -(1-k) & -\dfrac{g}{Q^2 k} \end{pmatrix} \tag{3.28}$$

On en déduit que $rang(O) = 3 = n$ et d'après la condition du rang d'observabilité, le système est observable.

3.4.2 Etude à l'aide de l'algèbre de Lie

Dans cette méthode, nous utilisons l'algèbre de Lie pour vérifier la condition du rang d'observabilité. Nous écrivons alors la matrice O sous la forme suivante :

$$O=\begin{pmatrix} dh \\ dL_f h \\ dL_f^2 h \end{pmatrix}=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \dfrac{g}{Qk} \\ -(1-k) & -(1-k) & -\dfrac{g}{Q^2 k} \end{pmatrix} \tag{3.29}$$

Nous obtenons ainsi la même matrice que la matrice obtenue par la linéarisation du système. En effet, le terme non linéaire $n(x_2)$ intervient dans la troisième dérivée de la sortie. Le rang de O est égal à $n=3$ et le système est donc observable.

3.4.3 Condition de recouvrement d'observabilité de l'émetteur

A ce stade, les hypothèses *(i)* et *(ii)* sont vérifiées pour l'oscillateur de Colpitts. Nous étudions maintenant la condition de recouvrement d'observabilité et l'inversibilité à gauche de l'émetteur chaotique (oscillateur de Colpitts incluant le message inconnu) donné en (2.13), c'est-à-dire la possibilité de retrouver le message injecté dans l'oscillateur. Nous écrivons le système (2.13) sous la forme :

$$\begin{cases} \dot{x}=f(x)+p(x)m \\ y=Cx \end{cases} \tag{3.30}$$

où : $p(x)=\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. On calcule ensuite $O.p(x)$:

$$O.p(x)=\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & \dfrac{g}{Qk} \\ -(1-k) & -(1-k) & -\dfrac{g}{Q^2 k} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ \theta=-(1-k) \end{pmatrix} \tag{3.31}$$

avec $\theta \neq 0$ si $k \neq 1$.

Ainsi, la condition de recouvrement d'observabilité de l'émetteur chaotique est vérifiée. Il est alors possible d'extraire le message *m* à l'aide d'un observateur à modes glissants si l'entrée du système reste bornée.

3.5 Synchronisation chaotique par observateur à modes glissants

Le principe des observateurs à modes glissants consiste à contraindre, à l'aide de fonctions discontinues, les dynamiques d'un système d'ordre n à converger vers une variété S de dimension $n-p$ dite surface de glissement (p étant la dimension du vecteur de mesure). L'attractivité de cette surface est assurée par des conditions appelées conditions de glissement. Si ces conditions sont vérifiées, le système converge vers la surface de glissement et *y* évolue selon une dynamique d'ordre $n-p$.

Dans le cas des observateurs à modes glissants, les dynamiques concernées sont celles des erreurs d'observation $e(t)=x(t)-\hat{x}(t)$. A partir de leurs valeurs initiales $e(0)$, ces erreurs convergent vers les valeurs d'équilibre en deux étapes :

- Dans une première phase, la trajectoire des erreurs d'observation évolue vers la surface de glissement sur laquelle les erreurs entre la sortie de l'observateur et la sortie du système réel (les mesures) $e_y=y-\hat{y}$ sont nulles. Cette étape, qui généralement est très dynamique, est appelée mode d'atteinte.

- Dans la seconde phase, la trajectoire des erreurs d'observation glisse sur la surface de glissement avec des dynamiques imposées de manière à annuler toutes les erreurs d'observation. Ce dernier mode est appelé mode de glissement. Les différentes étapes de synthèse d'un observateur à mode glissant sont connues et clairement identifiées dans [46]. Ces dernières sont rappelées ci-dessous.

Considérons un système d'état non linéaire d'ordre n :

$$\begin{cases} \dot{x}=f(x,u), & x\in R^n \\ y=h(x), & y\in R^p \end{cases} \tag{3.32}$$

L'observateur à modes glissants est défini avec la structure suivante :

$$\begin{cases} \dot{\hat{x}} = f\left(\hat{x},u\right) - K\Gamma_s \\ \hat{y} = h\left(\hat{x}\right) \end{cases} \tag{3.33}$$

où

K est la matrice de gain de dimension (*n*×*p*) .

Γ_s est un vecteur de dimension *p*×1 défini par :

$$\Gamma_s = \left[sign\left(\hat{y}_1 - y_1\right) \ \cdots \ sign\left(\hat{y}_p - y_p\right) \right]^T$$

Nous définissons également les vecteurs relatifs aux erreurs d'observation tel que :

$e = x - \hat{x}$ est le vecteur d'état des erreurs d'observation.

$S = e_y = y - \hat{y}$ est la surface de glissement.

La figure 3.5 représente le schéma fonctionnel d'un observateur à modes glissants.

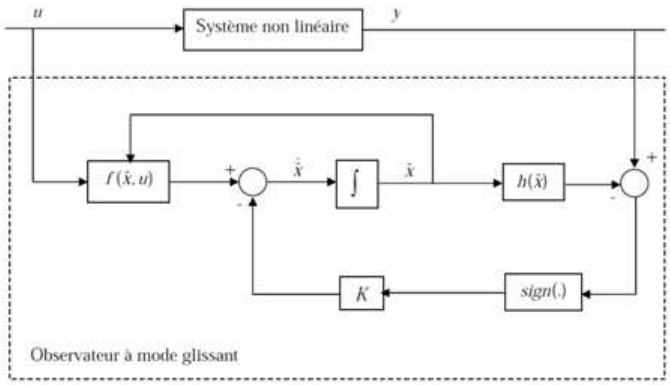


Figure 3.5 - Schéma fonctionnel d'un observateur à modes glissants

Pour que l'état estimé converge vers l'état réel, l'observateur à mode glissant doit respecter deux conditions.

La première concerne le mode d'atteinte et garantie l'attractivité de la surface de glissement $S = 0$ de dimension p, laquelle est attractive si la fonction de Lyapunov $V(x) = S^T \times S$ vérifie la condition : $\dot{V}(x) < 0 \text{ si } S \neq 0$.

La deuxième concerne le mode glissant. Durant cette étape, la matrice des gains correctifs agit de manière à satisfaire la condition d'invariance suivante :

$$\begin{cases} \dot{S} = 0 \\ S = 0 \end{cases} \tag{3.34}$$

Durant ce mode, les dynamiques du système sont réduites et le système d'ordre n devient un système équivalent d'ordre $n - p$. Ces critères permettent la synthèse de l'observateur à mode glissant et déterminent son fonctionnement.

3.5.1 Observateur à mode glissant étape par étape

L'observateur à mode glissant étape par étape a été développé pour des systèmes pouvant se mettre sous la forme, appelée forme triangulaire d'observation, suivante [46]**:**

$$\begin{cases} \dot{x}_1 = x_2 + g_1\left(x_1, u\right) \\ \dot{x}_2 = x_3 + g_2\left(x_1, x_2, u\right) \\ \vdots \\ \dot{x}_{n-1} = x_n + g_{n-1}\left(x_1, x_2, \ldots, x_{n-1}, u\right) \\ \dot{x}_n = f_n\left(x_1, x_2, \ldots, x_n\right) + g_n\left(x_1, x_2, \ldots, x_n, u\right) \\ y = x_1 \end{cases} \tag{3.35}$$

où f_n et g_i pour $i = 1, 2, \ldots, n$ sont des fonctions scalaires, x_i sont les états du système, u est le vecteur d'entrée et y est la sortie. La structure de l'observateur proposé est :

$$\begin{cases} \dot{\hat{x}}_1 = \hat{x}_2 + g_1\left(x_1, u\right) + k_1 sign_1\left(x_1 - \hat{x}_1\right) \\ \dot{\hat{x}}_2 = \hat{x}_3 + g_2\left(x_1, \tilde{x}_2, u\right) + k_2 sign_2\left(\tilde{x}_2 - \hat{x}_2\right) \\ \vdots \\ \dot{\hat{x}}_{n-1} = \hat{x}_n + g_{n-1}\left(x_1, \tilde{x}_2, \ldots, \tilde{x}_{n-1}, u\right) + k_{n-1} sign_{n-1}\left(\tilde{x}_{n-1} - \hat{x}_{n-1}\right) \\ \dot{\hat{x}}_n = f_n\left(x_1, \tilde{x}_2, \ldots, \tilde{x}_n\right) + g_2\left(x_1, \tilde{x}_2, \ldots, \tilde{x}_n, u\right) + k_n sign_n\left(\tilde{x}_n - \hat{x}_n\right) \\ y = x_1 \end{cases} \tag{3.36}$$

où les variables $\tilde{x}_i$ sont données par :

$$\begin{cases} \overline{x}_1 = x_1 \\ \overline{x}_i = \hat{x}_i + k_{i-1} sign_{éq,i-1}\left(\tilde{x}_{i-1} - \hat{x}_{i-1}\right) \text{ pour } i > 1 \end{cases} \tag{3.37}$$

où $sign_{eq}$ désigne la fonction $sign(\ )$ classique filtrée par un filtre passe bas. La fonction $sign_i$ est définie de manière à imposer à ce que le terme correctif ne soit actif que si $\tilde{x}_j - \hat{x}_j = 0$ pour $j = 1,\ldots,i$ c'est-à-dire, s'il existe $j \in \{1,\ldots,i-1\}$ tel que $\tilde{x}_j - \hat{x}_j = 0$ alors la fonction $sign_i$ est mise à zéro sinon elle est égale à la fonction $sign(\ )$ usuelle. La convergence des erreurs d'observation en temps fini n'est assurée que si le système est à entrées bornées et à états bornés (BIBS) pour une durée finie. Si cette condition est vérifiée alors les k_i peuvent être choisis tel que l'état de l'observateur $\hat{x}$ converge en un temps fini vers l'état x réel du système. Cependant cette convergence se fait étape par étape :

Etape 1 : Dans cette étape on assure la convergence de $e_1 = x_1 - \hat{x}_1$ vers zéro dans un temps $t < t_1$. Pour $i > 1$ toutes les fonctions $sign_i$ sont égales à zéro, les dynamiques des erreurs d'observation $e = x - \hat{x}$ sont donc :

$$\begin{cases} \dot{e}_1 = e_2 - k_1 sign\left(x_1 - \hat{x}_1\right) \\ \dot{e}_2 = e_3 + g_2\left(x_1, x_2, u\right) - g_2\left(x_1, \hat{x}_2, u\right) \\ \vdots \\ \dot{e}_{n-1} = e_n + g_{n-1}\left(x_1, x_2, \ldots, x_{n-1}, u\right) - g_{n-1}\left(x_1, \hat{x}_2, \ldots, \hat{x}_{n-1}, u\right) \\ \dot{e}_n = f_n\left(x_1, x_2, \ldots, x_n\right) - f_n\left(x_1, \hat{x}_2, \ldots, \hat{x}_n\right) + g_n\left(x_1, x_2, \ldots, x_n, u\right) - g_n\left(x_1, \hat{x}_2, \ldots, \hat{x}_n, u\right) \end{cases} \tag{3.38}$$

L'entrée *u* et les états sont bornés. Par conséquent, les états du système ne divergent pas et les erreurs d'observation sont aussi bornées. On considère la fonction de Lyapunov $V_1 = \frac{e_1^2}{2}$, alors :

$$\dot{V}_1 = e_1(e_2 - k_1 sign(e_1)) \tag{3.39}$$

En choisissant $k_1 > |e_2|_{\max}$, l'erreur d'observation e_1 converge vers zéro en un temps fini t_1. Après cet instant, e_1 reste égale à zéro et on obtient alors $e_2 = k_1 sign(x_1 - \hat{x}_1)$ ce qui implique $\tilde{x}_2 = x_2$.

Etape 2 : L'objectif dans cette étape est d'atteindre la surface de glissement $e_2 = x_2 - \hat{x}_2$. Pour rester sur la surface $e_1 = 0$, il faut que $k_1 > |e_2|_{\max}$, mais cela est vérifié de part le fait que e_2 est strictement décroissante après t_1. Les dynamiques des erreurs d'observation sont alors :

$$\begin{cases} \dot{e}_1 = e_2 - k_1 sign(x_1 - \hat{x}_1) = 0 \\ \dot{e}_2 = e_3 + g_2(x_1, x_2, u) - g_2(x_1, \hat{x}_2, u) - k_2 sign(x_1 - \hat{x}_1) = e_3 - k_2 sign(e_2) \\ \vdots \\ \dot{e}_{n-1} = e_n + g_{n-1}(x_1, x_2, \ldots, x_{n-1}, u) - g_{n-1}(x_1, \hat{x}_2, \ldots, \hat{x}_{n-1}, u) \\ \dot{e}_n = f_n(x_1, x_2, \ldots, x_n) - f_n(x_1, \hat{x}_2, \ldots, \hat{x}_n) + g_n(x_1, x_2, \ldots, x_n, u) - g_n(x_1, \hat{x}_2, \ldots, \hat{x}_n, u) \end{cases} \quad (3.40)$$

En choisissant la fonction de Lyapunov $V_2 = \frac{e_1^2}{2} + \frac{e_2^2}{2}$, on aura :

$$\dot{V}_2 = e_1(e_2 - k_1 sign(e_1)) + e_2(e_3 - k_1 sign(e_2)) = e_2(e_3 - k_1 sign(e_2)) \quad (3.41)$$

Si $k_3 > |e_3|_{\max}$, alors e_2 converge vers zéro après un temps fini $t_2 > t_1$.L'erreur d'observation est strictement décroissante durant la période $[t_1, t_2]$, ce qui implique que la condition imposée dans la première étape sur k_1 doit être vérifiée aussi après t_1.Enfin après un temps fini t_2 ,on a $\tilde{x}_3 = x_3$.

Ainsi, étape par étape, nous obtenons la convergence de toutes les composantes de l'erreur d'observation vers zéro et celles de $\hat{x}$ vers x pour tous $i < n$ sous conditions, que $k_i > |e_{i+1}|_{\max}$ durant $[t_i, t_{i+1}]$.

Etape n : cette étape commence à l'instant t_{n-1} et à cet instant, on a : $e_j = 0$ pour tous $j < n$.

$$\begin{cases} \dot{e}_1 = e_2 - k_1 sign\left(x_1 - \hat{x}_1\right) = 0 \\ \dot{e}_2 = e_3 - k_2 sign\left(x_2 - \hat{x}_2\right) = 0 \\ \vdots \\ \dot{e}_{n-1} = e_n - k_{n-1} sign\left(x_{n-1} - \hat{x}_{n-1}\right) = 0 \\ \dot{e}_n = f_n\left(x_1, x_2, \ldots, x_n\right) - f_n\left(x_1, \hat{x}_2, \ldots, \hat{x}_n\right) + g_n\left(x_1, x_2, \ldots, x_n, u\right) - g_n\left(x_1, \hat{x}_2, \ldots, \hat{x}_n, u\right) \\ \qquad\qquad - k_n sign_n\left(\tilde{x}_n - \hat{x}_n\right) = -k_n sign_n\left(e_n\right) \end{cases} \tag{3.42}$$

De la même façon, on choisit la fonction de Lyapunov $V_n = \frac{e_1^2}{2} + \frac{e_2^2}{2} + \ldots + \frac{e_n^2}{2}$. On obtient donc : $\dot{V}_n = e_n(-k_n sign(e_n))$.

Ainsi, e_n converge vers zéro en un temps fini $t_n > t_{n-1}$ pour toutes valeurs de $k_n > 0$, si évidement toutes les conditions sur $k_j, j < n$ sont elles aussi vérifiées.

3.5.2 Phénomène de réticence ou chattering

Un mode de glissement idéal ne peut exister en pratique car cela nécessite la présence d'une commande ou d'un correcteur d'erreur d'estimation qui commute à une fréquence infinie. En présence des limitations sur le temps de commutation, la discontinuité produit un comportement dynamique particulier sur la surface de glissement. Ce phénomène représenté sur la figure 3.6 est appelé réticence (ou chattering).

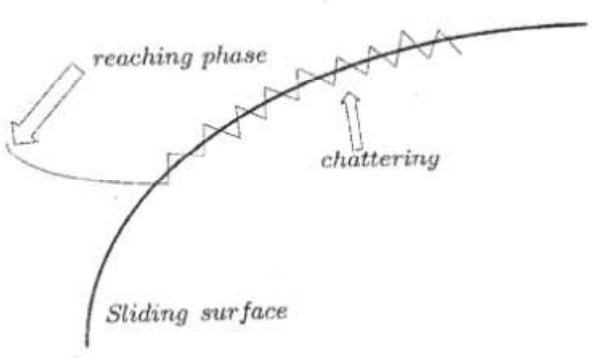


Figure 3.6 - Phénomène de chattering

Le chattering est un inconvénient majeur car même s'il est filtré à la sortie du système, il peut affecter la performance du processus, et peut même conduire à l'instabilité. Des solutions existent pour diminuer le chattering. Une solution est d'utiliser une fonction d'adoucissement en remplaçant la fonction $sign$ par une fonction de saturation qui filtre les hautes fréquences. Cette fonction est montrée dans la figure 3.7 et est exprimée par :

$$\begin{cases} sat(s) = 1 \ \text{ si } \ s > \varepsilon \\ sat(s) = -1 \ \text{ si } \ s < \varepsilon \\ sat(s) = \dfrac{s}{\varepsilon} \ \text{ si } \ |s| \le \varepsilon \end{cases} \tag{3.43}$$

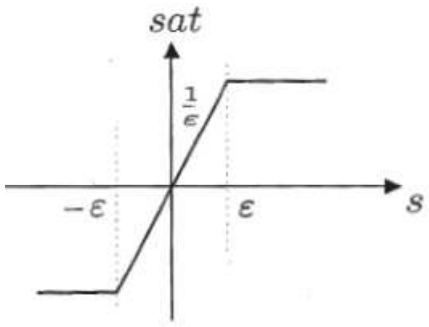


Figure 3.7 - Fonction de saturation pour réduire le chattering

3.6 Récepteur chaotique à base d'observateurs à modes glissants

Dans une section précédente, nous avons vérifié l'observabilité de l'oscillateur de Colpitts et la condition de recouvrement d'observabilité de l'émetteur chaotique donnée en (2.13). De plus, le système possède des états bornés et le message est lui aussi borné. Nous pouvons alors choisir des k_i constants [28] [47]. Nous allons donc pouvoir construire un observateur à modes glissants pour le système (2.13) dans le but de reconstruire tous les états de l'émetteur chaotique et le message à partir de l'état connu x_2, qui est ici la sortie du système (2.13) transmise au récepteur. Les équations de cet observateur sont données par [46] [47] :

$$\begin{cases} \dot{\hat{x}}_1 = \dfrac{g}{Q(1-k)}\left[-n(x_2) + \tilde{x}_3\right] + E_2 k_3 \operatorname{sgn}(\tilde{x}_1 - \hat{x}_1) \\ \dot{\hat{x}}_2 = \dfrac{g}{Qk}\hat{x}_3 + k_1 \operatorname{sgn}(x_2 - \hat{x}_2) \\ \dot{\hat{x}}_3 = -\dfrac{Qk(1-k)}{g}\left[\hat{x}_1 + x_2\right] - \dfrac{1}{Q}\tilde{x}_3 + E_1 k_2 \operatorname{sgn}(\tilde{x}_3 - \hat{x}_3) \end{cases} \quad (3.44)$$

L'observateur à modes glissants donné en (3.44) fonctionne étape par étape : lorsque $\hat{x}_2 = x_2$, alors $E_1 = 1$ sinon $E_1 = 0$. Donc quand $E_1 = 1$, l'observateur reconstruit l'état suivant c'est à dire x_3. De la même manière, lorsque $\hat{x}_3 = \tilde{x}_3$, alors $E_2 = 1$ sinon $E_2 = 0$. Quand $E_2 = 1$, on passe à l'étape suivante, c'est à dire la reconstruction de x_1. Enfin, lorsque $\hat{x}_1 = \tilde{x}_1$ et $E_2 = 1$ alors $E_3 = 1$ et le message est reconstruit par l'observateur. Les états auxiliaires $\tilde{x}_1, \tilde{x}_3$ et l'estimation du message $\tilde{m}$ se calculent comme suit :

$$\begin{cases} \tilde{x}_3 = \hat{x}_3 + E_1 k_1 \dfrac{Qk}{g} \operatorname{sgn}(x_2 - \hat{x}_2) \\ \tilde{x}_1 = \hat{x}_1 - E_2 k_2 \dfrac{g}{Qk(1-k)} \operatorname{sgn}(\tilde{x}_3 - \hat{x}_3) \\ \tilde{m} = E_3 k_3 \dfrac{Q(1-k)}{g} \operatorname{sgn}(\tilde{x}_1 - \hat{x}_1) \end{cases} \quad (3.45)$$

Nous allons montrer la convergence de l'observateur à modes glissants (3.44) en temps fini, c'est-à-dire que l'erreur d'estimation $e_i = x_i - \hat{x}_i$ tend vers zéro au bout d'un temps fini.

Etape 1 : nous considérons maintenant que $E_1 = 0$ (si $E_1 = 1$, on passe directement à l'étape suivante). Les dynamiques de l'erreur d'estimation $e = x - \hat{x}$ sont alors données par :

$$\begin{cases} \dot{e}_2 = \dfrac{g}{Qk} e_3 - k_1 \operatorname{sgn}(e_2) \\ \dot{e}_3 = -\dfrac{Qk(1-k)}{g} e_1 - \dfrac{1}{Q} e_3 \\ \dot{e}_1 = \dfrac{g}{Q(1-k)} e_3 + m \end{cases} \tag{3.46}$$

Grâce à la convergence en temps fini des modes glissants, il existe $t_1 > 0$ tel que $\forall t \geq t_1$, $\hat{x}_2 = x_2$. Nous passons ensuite à l'étape suivante :

Etape 2 : Lorsque $\hat{x}_2 = x_2$, nous avons $e_2 = 0$ et E_1 devient égal à 1, $\forall t \geq t_1, \dot{e}_2 = 0$. Par conséquent, puisque $\tilde{x}_3 = \hat{x}_3$, nous obtenons :

$$\begin{cases} \dot{e}_2 = \dfrac{g}{Qk} e_3 - k_1 \operatorname{sgn}(e_2) = 0 \\ \dot{e}_3 = -\dfrac{Qk(1-k)}{g} e_1 - \dfrac{1}{Q} e_3 - k_2 \operatorname{sgn}(e_3) \\ \dot{e}_1 = \dfrac{g}{Q(1-k)} e_3 + m \end{cases} \tag{3.47}$$

De la même manière, il existe $t_2 > t_1 > 0$ tel que $\hat{x}_3 = \tilde{x}_3 = x_3$ et nous passons à l'étape suivante.

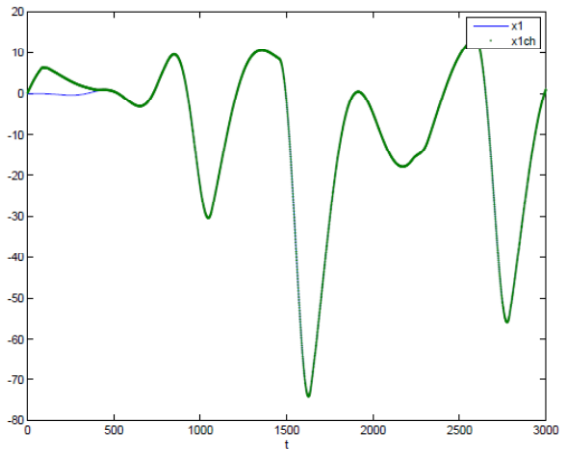
Etape 3 : Lorsque $\left[\hat{x}_3 = x_3 \text{ et } \mathrm{E}_1 = 1\right]$, alors $E_2 = 1$ et comme $e_3 = 0$, $\forall t \geq t_2 \geq t_1$, $\dot{e}_3 = 0$. Par conséquent, puisque $\tilde{x}_1 = x_1$, nous obtenons :

$$\begin{cases} \dot{e}_2 = \dfrac{g}{Qk} e_3 - k_1 \operatorname{sgn}(e_2) = 0 \\ \dot{e}_3 = -\dfrac{Qk(1-k)}{g} e_1 - \dfrac{1}{Q} e_3 - k_2 \operatorname{sgn}(e_3) = 0 \\ \dot{e}_1 = \dfrac{g}{Q(1-k)} e_3 + m - k_3 \operatorname{sgn}(e_1) \end{cases} \tag{3.48}$$

Si $\left[\hat{x}_1 = x_1 \text{ et } \mathrm{E}_2 = 1\right]$ alors $E_3 = 1$ et donc $\dot{e}_1 = 0$. Nous retrouvons le message m dont l'estimation est donnée en (3.45).

3.7 Simulation

Les résultats de simulation de l'observateur à modes glissants donné en (3.44) et utilisé au niveau du récepteur chaotique sont montrés dans la figure 3.8. Dans cette simulation, un message sinusoïdal est inclus dans l'oscillateur de Colpitts chaotique au niveau de l'émetteur. Comme nous pouvons le constater sur la figure 3.9, le message est restitué avec un léger chattering qui peut être supprimé par filtrage. Nous avons fixé les paramètres comme suit : $g = 4.5$ et $Q = 1.38$ dans le modèle normalisé de l'oscillateur de Colpitts donnée en (2.12) afin d'obtenir un comportement chaotique d'après les résultats du chapitre 2, et les coefficients $k_1 = 50, k_2 = 150, k_3 = 150$ dans l'observateur à modes glissants. Nous démarrons la simulation en fixant des conditions initiales différentes au niveau de l'émetteur et du récepteur. De plus, pour diminuer le chattering, nous avons utilisé des fonctions arc-tangente au lieu de la fonction $sign$. Il est important de noter que la construction des états est montrée étape par étape, en commençant par l'état connu et transmis par l'émetteur, soit le signal x_2. Ensuite nous reconstruisons respectivement x_3 et x_1 et enfin le message m est récupéré après la synchronisation de tous les états. La convergence en temps fini de l'observateur à modes glissants est montrée dans la figure 3.10, qui représente les erreurs d'estimation des états.



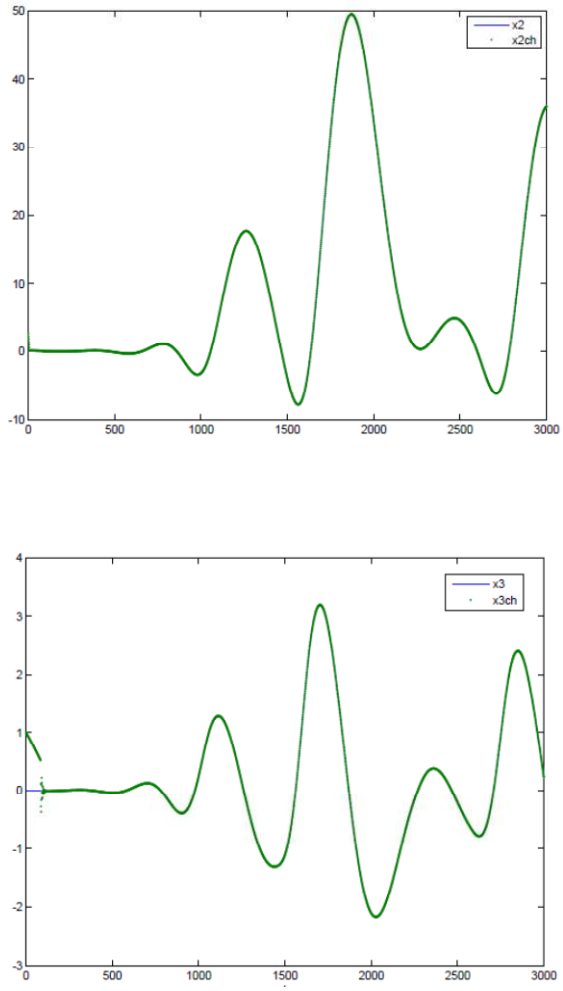


Figure 3.8 - Signaux synchronisés au niveau du récepteur chaotique

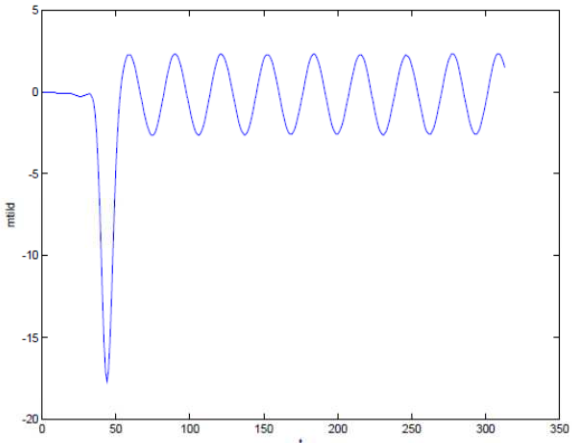


Figure 3.9 - Message récupéré au niveau du récepteur chaotique

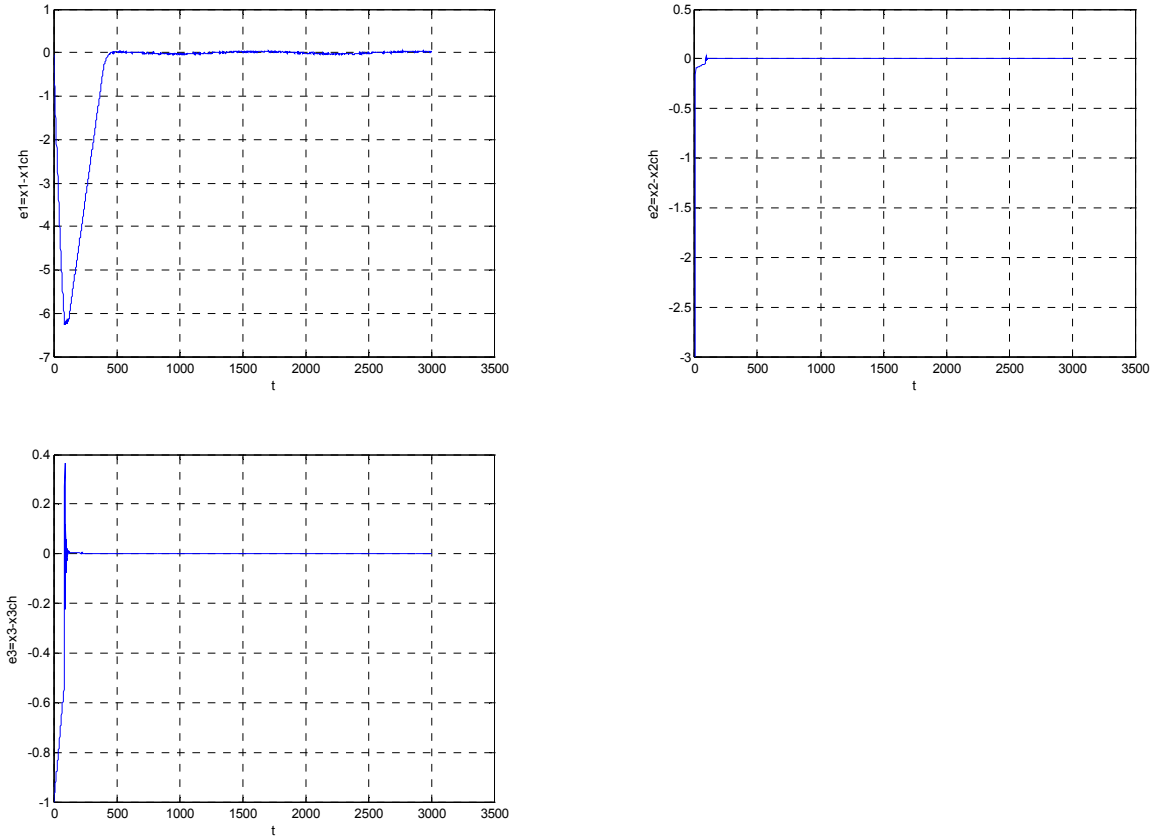


Figure 3.10 - Erreurs d'estimation des états

3.8 Conclusion

Dans ce chapitre, 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. Pour cela, un observateur à modes glissants fonctionnant étape par étape a été proposé et simulé. Nous avons ainsi montré la convergence en temps fini de l'observateur, et ce après avoir vérifié la condition de recouvrement d'observabilité de l'émetteur chaotique. Ces résultats nous seront d'un grand apport lors de l'implémentation de la transmission chaotique (émetteur et récepteur) sur circuit FPGA et qui sera étudiée dans le prochain chapitre.

CHAPITRE 4

IMPLEMENTATION DE LA TRANSMISSION CHAOTIQUE SUR FPGA

4.1 Introduction

Grâce à l'évolution des technologies numériques, il est aujourd'hui possible de concevoir des composants numériques toujours plus rapides et à plus forte densité d'intégration. Dans le cadre de notre projet, la réalisation d'un système de transmission chaotique incluant l'émetteur et le récepteur nécessite des ressources matérielles conséquentes. C'est pourquoi nous avons opté pour une cible numérique de type FPGA qui nous semble particulièrement adaptée pour le développement d'un tel système [48]. Ce type d'implantation numérique sur FPGA nécessite toutefois de mettre en œuvre des outils spécifiques dans le cadre d'une méthodologie de conception adaptée [49].

Dans ce chapitre, après avoir brièvement décrit la technologie FPGA, nous présentons le flot de conception ISE de Xilinx et de Co-simulation sous environnement Matlab Simulink - System Generator Xilinx permettant d'une part l'implantation de la transmission chaotique sur FPGA, et d'autre part la simulation hardware de l'architecture implémentée. La description de la plateforme FPGA SPARTAN 3^E et de la carte de conversion CAN et CNA est également présentée. Nous terminons le chapitre par la présentation de l'ensemble des résultats expérimentaux et de leurs comparaisons aux résultats simulés.

4.2 Description des composants FPGA

Les FPGA sont des composants VLSI (Very Large Scale Integration). Ils sont

programmables par l'utilisateur et essentiellement constitués de trois parties :

- Une matrice de blocs logiques configurables CLB (Configurable Logic Bloc).

- Des blocs d'entrée/sortie configurables.

- Un réseau d'interconnexions programmables.

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

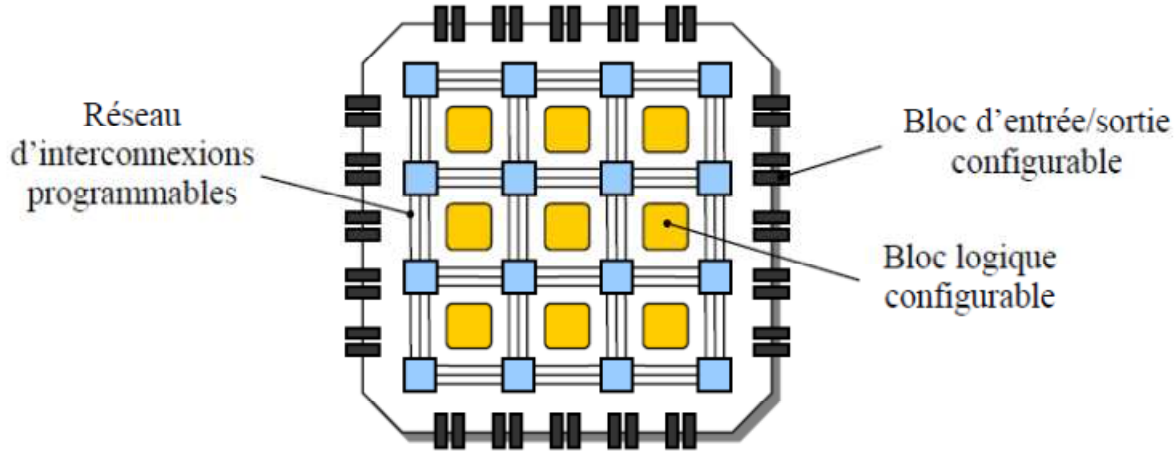


Figure 4.1 - Description de l'architecture générique d'un FPGA

Il existe plusieurs fabricants de composants FPGA tels que Actel, Xilinx et Altera. Ces constructeurs utilisent différentes technologies pour la fabrication des FPGA. Parmi ces technologies, celles qui assurent une reprogrammation des FPGA sont les plus intéressantes puisqu'elles permettent une grande flexibilité de conception. Les différentes technologies reprogrammables des FPGA sont les suivantes :

- La technologie EPROM : cette technologie utilise des mémoires EPROM (Erasable Programmable Read-Only Memory). Son principal inconvénient est l'opération de reconfiguration qui nécessite l'utilisation d'une source ultra violet.

- La technologie EEPROM : cette technologie utilise des mémoires EEPROM (Electrically Erasable Programmable Read-Only Memory). Par rapport à la technologie EPROM, elle présente l'avantage de pouvoir être reprogrammée électriquement.

- La technologie Static Ram (SRAM) : pour cette technologie, les connexions sont réalisées en rendant les transistors passants ce qui permet une reconfiguration rapide du circuit FPGA. Cependant, son principal inconvénient est la surface nécessaire pour la SRAM.

- La technologie FLASH : Cette technologie est limitée en nombre de reconfigurations et possède un temps de reconfiguration plus long par rapport à la technologie SRAM. L'avantage de cette technologie est qu'elle garde sa configuration même si l'alimentation est coupée. Par conséquent, un FPGA à base de technologie Flash déjà programmé est prêt à fonctionner dès sa mise sous tension.

La figure 4.2 présente la structure d'une cellule logique d'un bloc logique configurable CLB de la technologie Xilinx. Cette structure comporte une table LUT (*Look-up Table*) de 4 bits qui permet de réaliser n'importe quelle fonction combinatoire de quatre variables logiques. Cette LUT peut être aussi configurée comme étant une mémoire RAM (16×1) ou un registre à décalage de 16 bits. Elle comporte aussi un multiplexeur et une bascule D avec toutes ses entrées de contrôle (horloge, reset, enable).

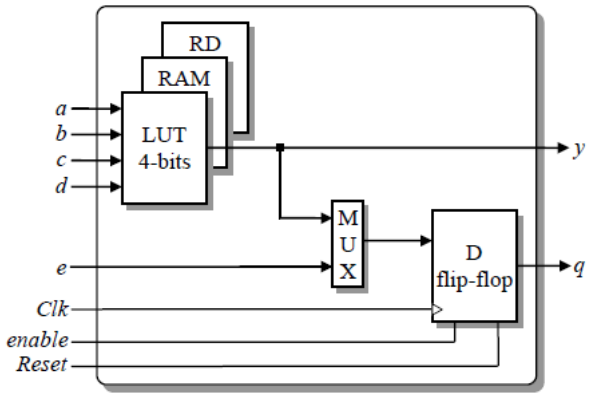


Figure 4.2 - Structure d'une cellule logique

Notons également que les FPGA actuels offrent la possibilité d'utiliser des blocs dédiés tels que les mémoires RAM, les multiplieurs câblés, les interfaces PCI et les cœurs processeurs [50], [51].

4.3 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 [52] (Very high speed integrated Hardware Description Language) et le Verilog [53]. 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 4.3 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.

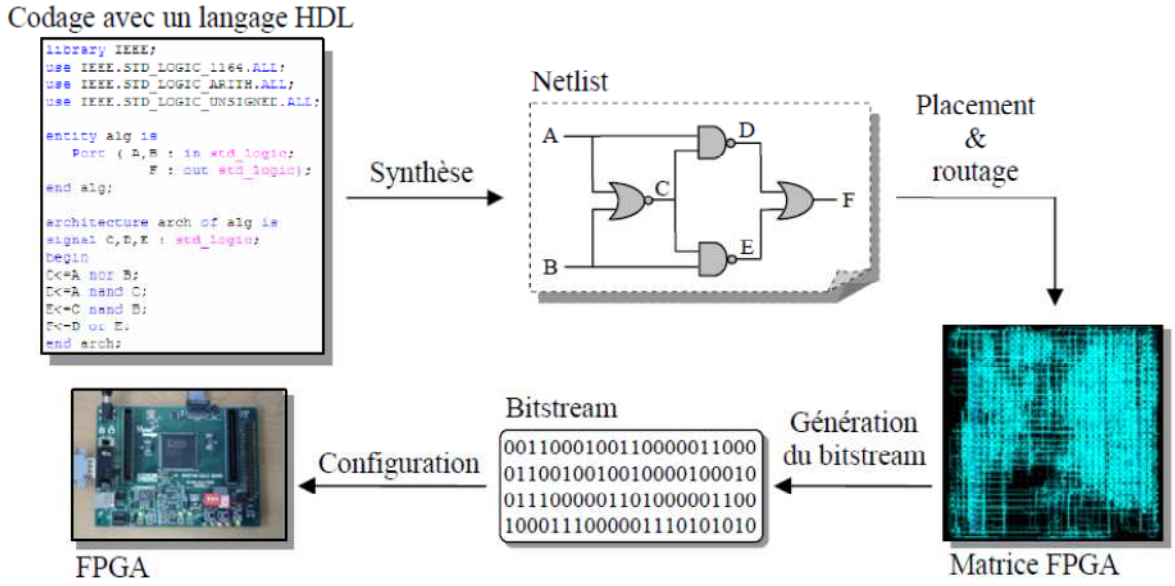


Figure 4.3 - Programmation d'un FPGA

Pour l'élaboration du modèle en vue de son implémentation sur FPGA, nous avons utilisé le logiciel System Generator sur Simulink. Il nous permet de créer un modèle sous Matlab-Simulink et d'effectuer des simulations aboutissant à des résultats comparables à ceux obtenus sous Simulink. Cette approche a été retenue afin de réduire le temps de conception sur le FPGA. Pour ce faire, il suffit de demander au logiciel de créer un fichier de type NGC contenant toutes les informations sur le bloc, en particulier, ses ports d'entrée et de sortie ainsi que la façon dont il sera implémenté sur notre FPGA. Il faudra, par la suite, importer ce fichier dans un autre environnement de travail, l'ISE de Xilinx pour que l'implémentation sur FPGA puisse être effectuée. La plate-forme FPGA utilisée est la carte SPARTAN 3^E construite autour du circuit FPGA XC24C500.

4.3.1 Présentation du logiciel ISE

L'environnement ISE (Integrated Software Environment) Xilinx est un logiciel de programmation des produits Xilinx (CPLD, FPGA Spartan et Virtex…). Il intègre différents outils permettant de passer à travers le flot de conception d'un système numérique à savoir :

- un éditeur de textes, de schémas et de diagrammes d'états.
- un compilateur VHDL et Verilog.
- un simulateur.
- un outil pour la gestion des contraintes temporelles.
- un outil pour la synthèse.
- un outil pour la vérification.
- un outil pour l'implémentation sur FPGA et CPLD.

La figure 4.4 représente le flot de conception du logiciel ISE incluant toutes les étapes pour l'implémentation d'un circuit FPGA. Quatre étapes sont nécessaires pour l'implémentation d'un circuit FPGA :

i) La spécification regroupe les trois modes (schématique, diagrammes d'états ou HDL) de saisie d'un circuit électronique. La spécification HDL est synthétisée pour générer un fichier appelé *NETLIST* qui décrit les interconnexions entre les registres.

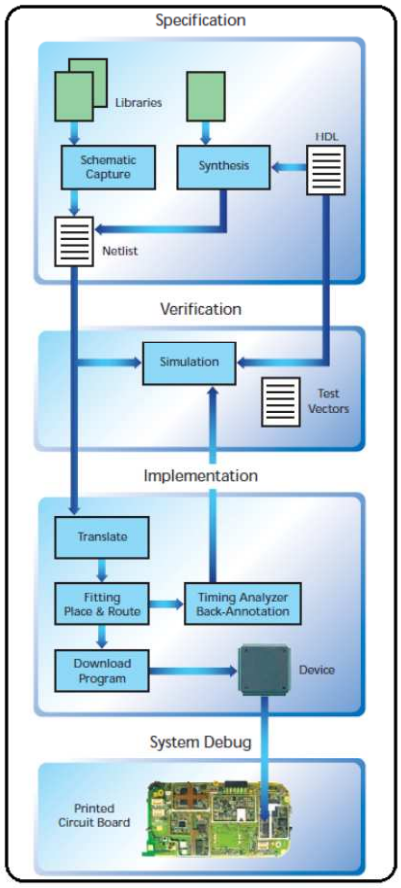


Figure 4.4 - Flot de conception du logiciel ISE Xilinx

ii) La vérification du design est une étape parallèle où le concepteur observe le comportement du code et vérifie s'il se comporte tel qu'il est supposé. Un simulateur simule le circuit à condition de lui fournir les vecteurs de test.

iii) L'implémentation sur le composant en spécifiant les références exactes de celui-ci à savoir : le boîtier, la fréquence de travail et les autres options spécifiques à chaque composant. Cette étape se décompose à son tour en sous-étapes :

- Fitting : c'est le dimensionnement de la conception en fonction des ressources internes du composant cible.
- Place and route : les sous programmes de placement et de routage sont exécutés après compilation du code :
    - ✓ Place : c'est le processus de sélection des modules ou blocs logiques où les portes logiques seront placées.

- ✓ Route : le routage est l'interconnexion physique entre les différents blocs logiques.

- Downloading ou programming : le fichier de programmation généré est ensuite chargé sur le FPGA ciblé par l'application.

iv) Le débogage du système : après chargement des interconnexions sur le FPGA, des tests peuvent être effectués sur le circuit implémenté afin de vérifier le bon fonctionnement de l'implémentation.

La figure 4.5 représente l'interface Project Navigator de ISE 10.1 permettant l'accès à toutes les ressources d'un projet ainsi qu'aux outils de l'implémentation.

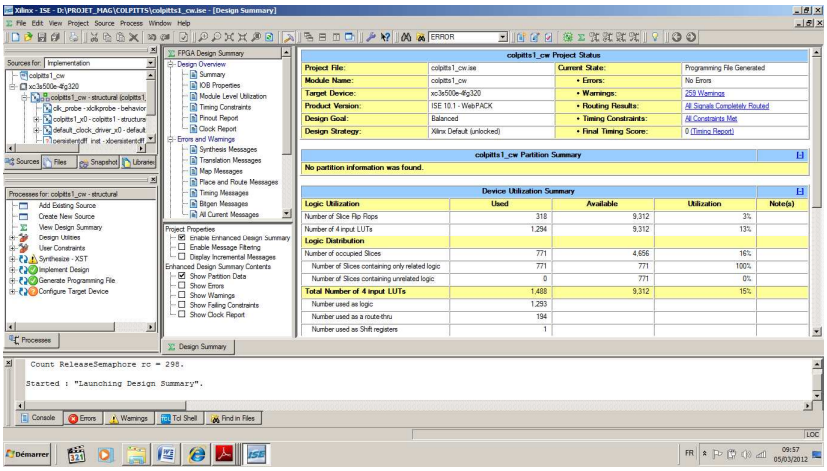


Figure 4.5 - Interface Project Navigator ISE 10.1

4.3.2 System Generator et Co-simulation

System Generator est un outil de design de DSP fourni par XILINX. Il permet d'utiliser l'environnement Matlab-Simulink pour la conception des applications sur circuits FPGA : c'est une interface entre MATLAB-Simulink et ISE -XILINX. Parmi les principales tâches pouvant êtres exécutées dans cet environnement, on peut citer :

- Conception et simulation des systèmes dans un environnement graphique (Simulink).
- Co-simulation logicielle (Simulink) - matérielle (FPGA) par communication JTAG ou USB.
- Génération automatique du code VHDL ou Verilog.

La figure 4.6 résume l'ensemble des fonctionnalités de l'outil System Generator de Xilinx.

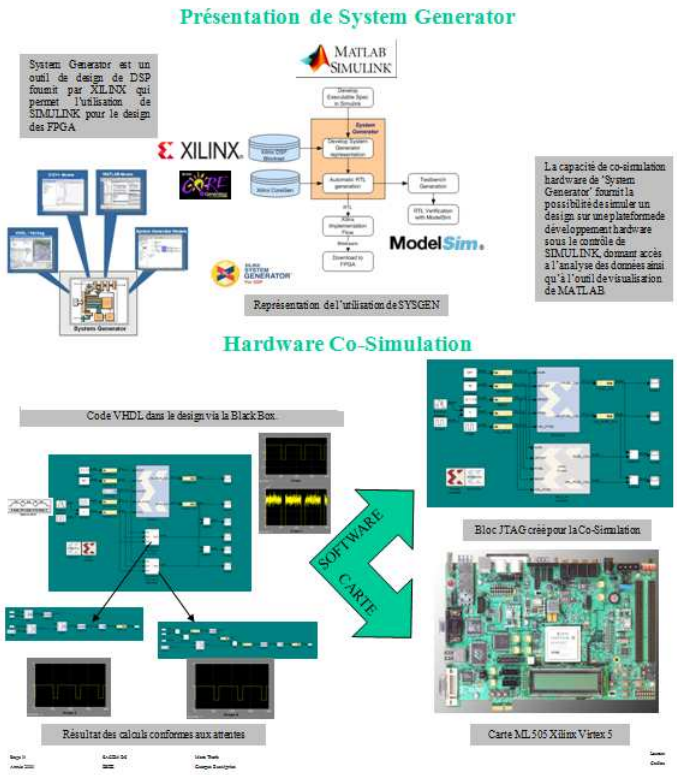


Figure 4.6 - Environnement Simulink-System Generator et co-simulation

4.4 Réalisation expérimentale de l'implémentation

Le schéma synoptique de l'implémentation expérimentale de la transmission chaotique (émetteur et récepteur) est représenté sur la figure 4.7. Il est constitué des éléments suivants :

- Un étage de conversion analogique-numérique 8 bits pour l'inclusion du message à transmettre au niveau de l'émetteur.
- La plate-forme de développement FPGA SPARTAN 3^E pour l'implémentation de la transmission chaotique.
- Un étage de conversion numérique-analogique 12 bits pour la récupération du message au niveau du récepteur et l'affichage des différents signaux mis en jeu au niveau de la transmission sur oscilloscope numérique.

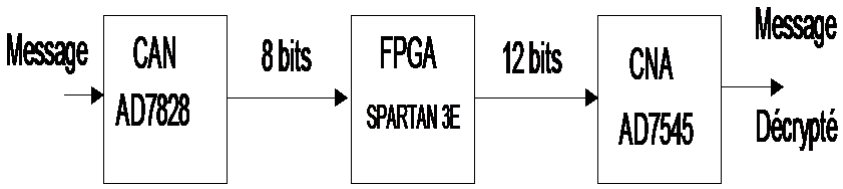


Figure 4.7 - Architecture de l'implémentation de la transmission chaotique

Les photos de la figure 4.8 montrent l'environnement de la réalisation expérimentale où l'on distingue la carte SPARTAN 3^E et la carte de conversion.

Figure 4.8 - Réalisation expérimentale de l'implémentation

4.4.1 Plate-forme de développement SPARTAN 3^E

La plate-forme de développement SPARTAN 3^E (figure 4.9) est une plate-forme de conception et de mise en œuvre de circuits numériques implémentés sur circuit FPGA (xc4vlx25). Elle dispose de ports d'entrées-sorties, de ports de communication, d'un port VGA, de deux ports PS2 (pour connecter un clavier ou une souris), d'un port RS232, d'un port de sortie audio, d'un afficheur LCD deux lignes à 16 caractères, de switches à usage général, des LEDs et des boutons poussoirs. La communication avec cette carte peut être établie via un câble USB ou JTAG. Après chargement du fichier de programmation, l'implémentation permet de tester le bon fonctionnement du circuit ou la détection des bugs ou dysfonctionnements.

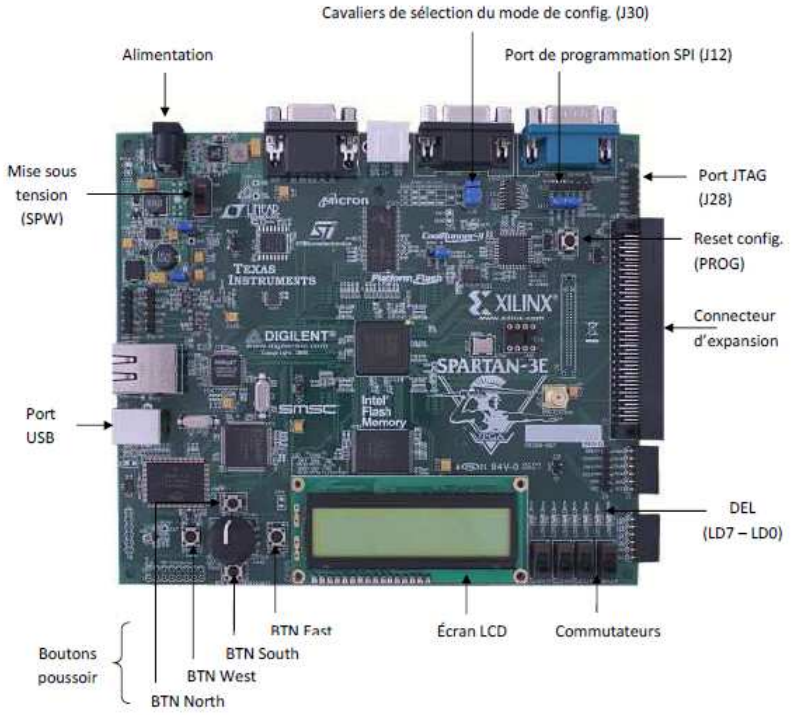


Figure 4.9 - Plate-forme de développement SPARTAN 3^{E}

4.4.2 Conversion analogique numérique

La carte de conversion analogique numérique (CAN) assure la conversion analogique-numérique du message *m* que l'on souhaite crypter à travers la transmission chaotique. Elle est basée sur l'utilisation d'un convertisseur AD7828 de résolution 8 bits (figure 4.10).

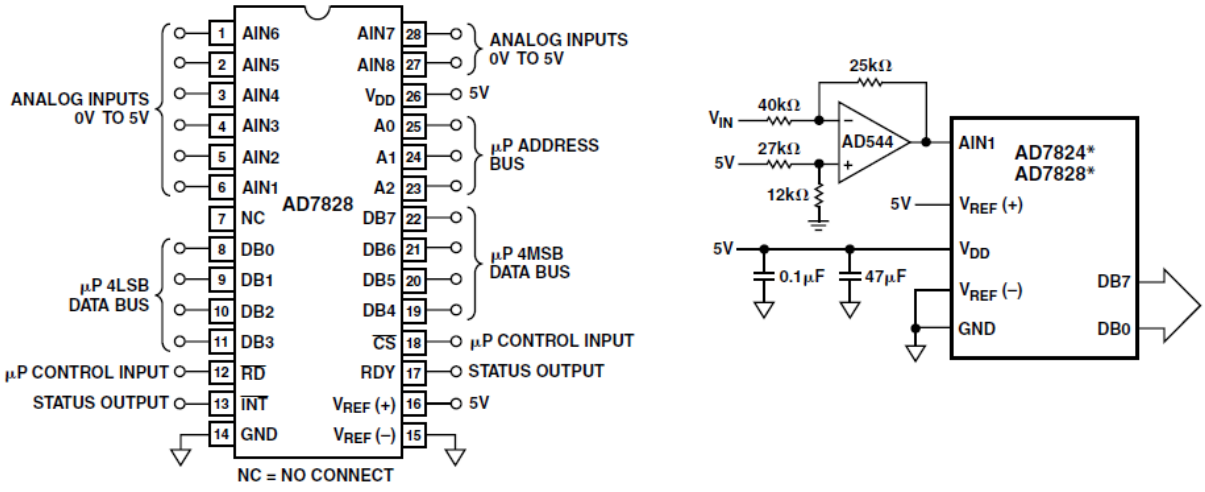


Figure 4.10 - Conversion A/N pour l'acquisition du message

Les différents signaux de contrôle nécessaires au fonctionnement du convertisseur sont gérés par le circuit FPGA. L'amplificateur opérationnel assure une mise en forme pour une conversion bipolaire afin d'obtenir un bit de signe.

4.4.3 Conversion numérique analogique

La carte de conversion numérique-analogique est constituée de trois convertisseurs AD7545 de résolution 12 bits. Les données à convertir sont recueillies à partir de la carte FPGA. Le courant de sortie I_{outA} est proportionnel au code binaire des 12 bits à l'entrée du convertisseur AD7545. Il est donc possible d'avoir une tension analogique V_{analog} image des 12 bits d'entrée du CNA en plaçant une résistance de mesure entre la sortie I_{outA} et la masse. La figure 4.11 présente le montage réalisé pour une conversion analogique numérique.

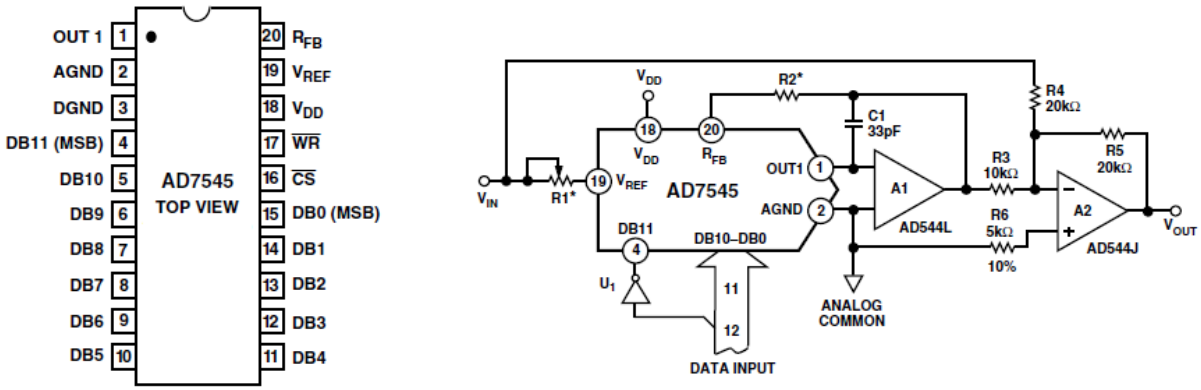


Figure 4.11 - Montage de conversion numérique analogique

4.5 Implémentation de l'émetteur chaotique sur FPGA

Nous rappelons le système normalisé de l'oscillateur chaotique de Colpitts obtenu dans le chapitre 2 (eq. 2.12) :

$$\begin{cases} \dot{x}_1 = \dfrac{g}{Q(1-k)}\left[-n(x_2)+x_3\right]+m \\ \dot{x}_2 = \dfrac{g}{Qk}x_3 \\ \dot{x}_3 = -\dfrac{Qk(1-k)}{g}\left(x_1+x_2\right)-\dfrac{1}{Q}x_3 \end{cases}$$

où $n(x_2) = \exp(-x_2) - 1$ est la fonction non linéaire.

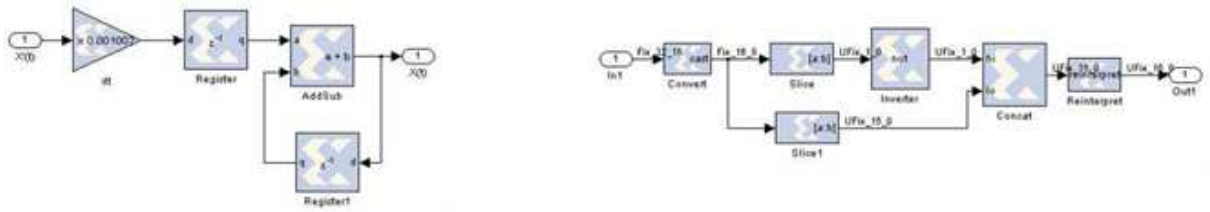
Pour l'implémentation de cette fonction non linéaire, nous avons utilisé une approximation de l'exponentielle par le modèle linéaire par morceaux [54]. Celui-ci permet de mettre en évidence les deux régimes de fonctionnement de l'élément non linéaire du transistor de l'oscillateur de Colpitts.

$$n_{pwl}(x_2) = \begin{cases} -x_2 \ , x_2 \le 1 & \text{(régime actif)} \\ -1 \ \ , x_2 > 1 & \text{(régime bloqué)} \end{cases}$$

Certaines fonctions n'étant pas disponibles dans la bibliothèque de System Generator, nous les avons synthétisées à l'aide des blocs disponibles tel que :

- le bloc intégrateur (figure 4.12a).

- le bloc réduction de résolution et inversion du bit le plus significatif pour la carte de conversion numérique analogique (figure 4.12b).



(a) (b)

Figure 4.12 - Bloc intégrateur (a) et bloc réduction de résolution (b)

Notons aussi que certaines fonctions écrites sous Matlab peuvent être intégrées sous System Generator à l'aide du bloc MCode block.

La figure 4.13 représente l'implémentation de l'émetteur chaotique incluant l'oscillateur chaotique de Colpitts et l'insertion du message à transmettre. Le bloc Resource Estimator permet de déterminer les ressources utilisées lors de l'implémentation.

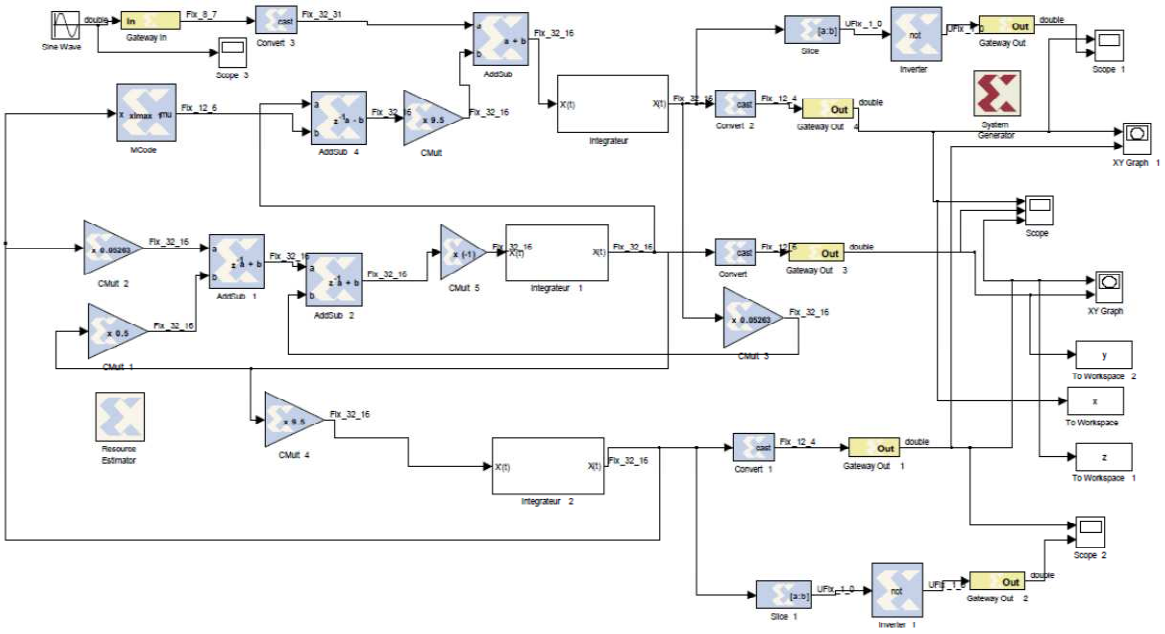
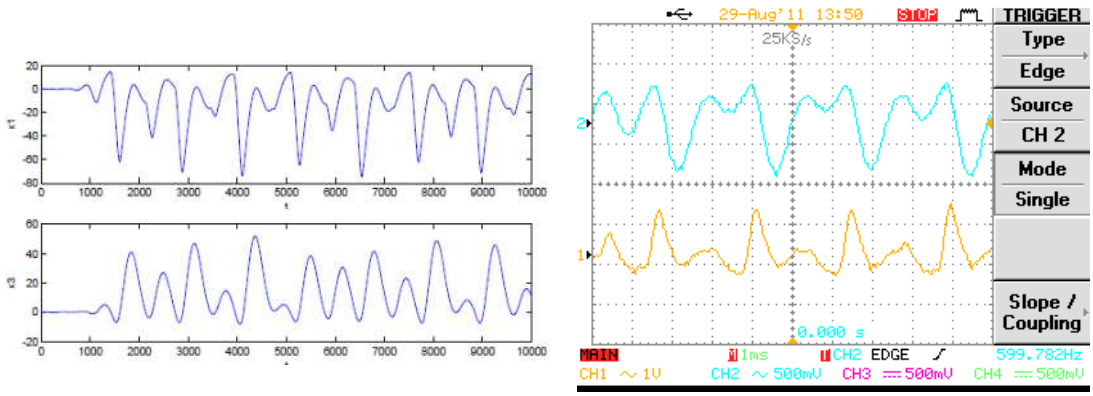


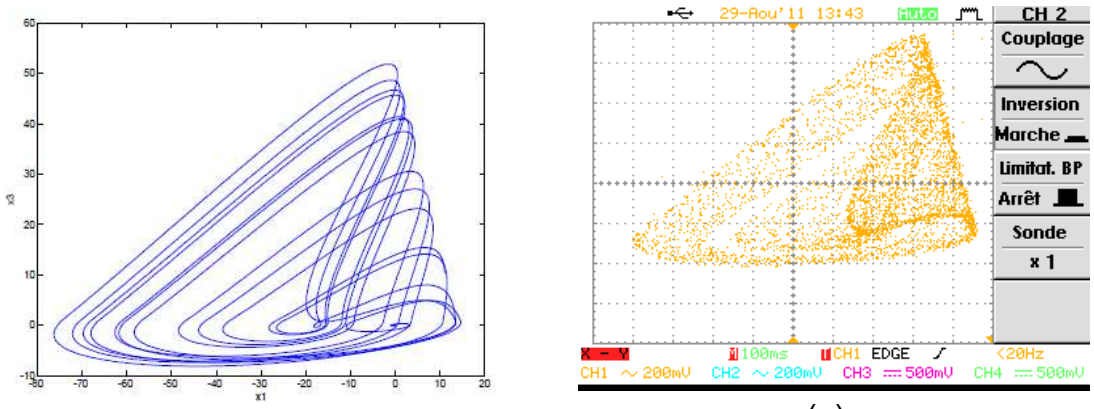
Figure 4.13 - Implémentation de l'émetteur chaotique.

Les signaux simulés sous Simulink-System Generator et relevés au niveau de la carte de conversion numérique-analogique à l'aide d'un oscilloscope numérique sont représentés sur les figures 4.14 et 4.15. Ces figures montrent le bon fonctionnement de l'émetteur chaotique ; on remarque que l'insertion du message n'a pas modifié le comportement chaotique du système. La figure 4.16 représente le signal transmis $x_2(t)$ au niveau de l'émetteur en absence et en présence du message *m*.



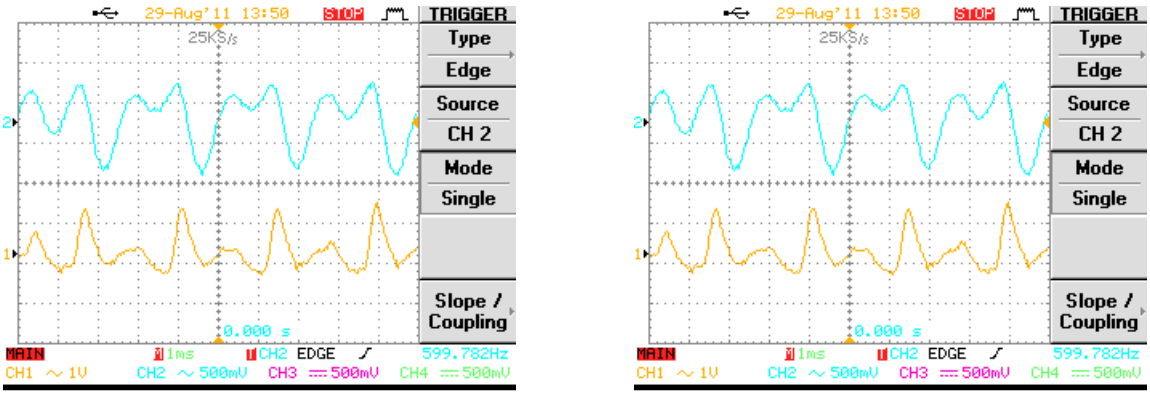
(a) (b)

Figure 4.14 - Signaux $x_1(t)$ et $x_3(t)$ (a) simulés et (b) expérimentaux



(b) (a)

Figure 4.15 - Plan de phase $x_1(t), x_3(t)$ (a) simulé et (b) expérimental



(a) (b)

Figure 4.16 - Signal transmis $x_2(t)$ (a) en absence et (b) en présence du message *m*

4.6 Implémentation de la transmission chaotique sur FPGA

Le système de transmission chaotique constitué de l'émetteur chaotique (oscillateur de Colpitts incluant le message) et du récepteur chaotique (à base d'observateur à modes glissants permettant la récupération du message) a été implanté sur la carte FPGA SPARTAN 3^E associée à une carte de conversion analogique-numérique et numérique-analogique. La figure 4.17 représente l'implémentation de l'émetteur et du récepteur sur FPGA.

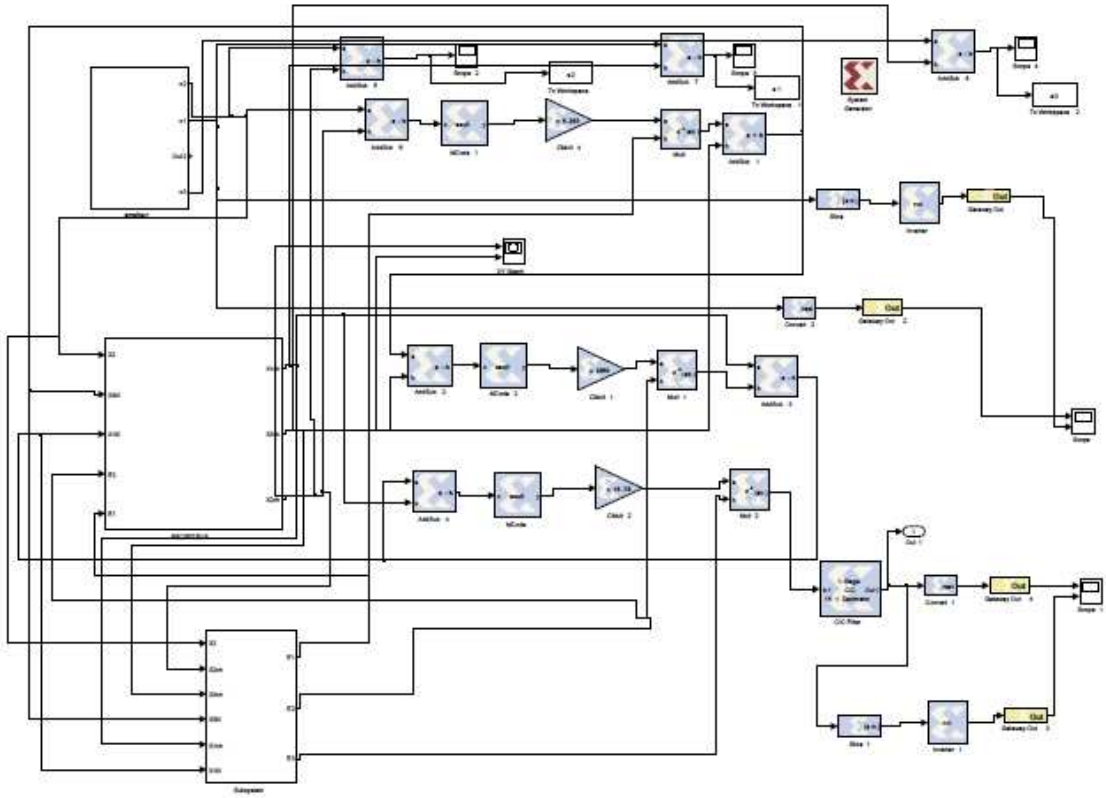


Figure 4.17- Implémentation de l'émetteur et du récepteur sur FPGA

Les figures 4.18 à 4.23 montrent les différents oscillogrammes relevés au niveau de la carte FPGA associée avec la carte de conversion. La visualisation de ces différents signaux nous permet de :

- vérifier la synchronisation de l'émetteur et du récepteur (figures 4.18 ,4.19 et 4.20).
- mesurer l'erreur entre les signaux estimés au niveau du récepteur et les signaux de l'émetteur (figures 4.21 et 4.22).
- montrer le fonctionnement étape par étape de l'observateur à modes glissants en effectuant un zoom des signaux d'erreurs au voisinage de l'origine.
- montrer la récupération du message associé à un léger chattering (figure 4.23).

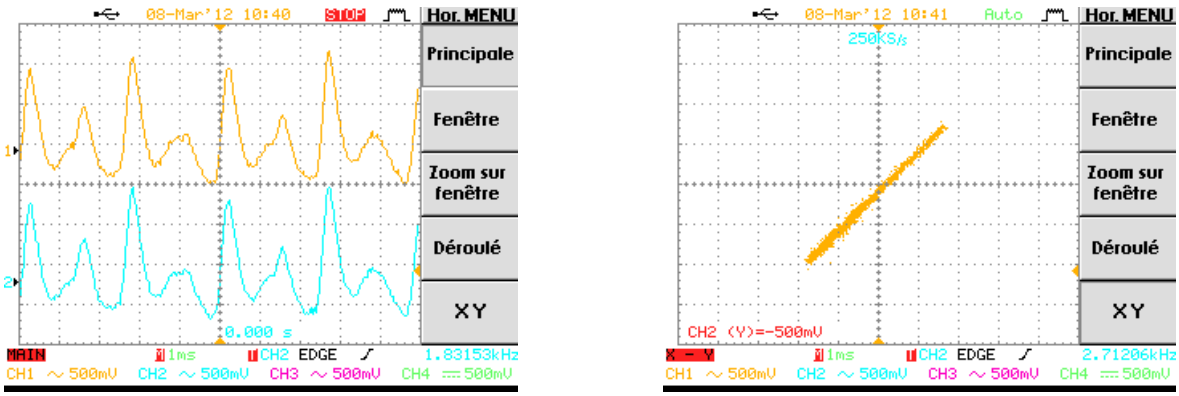


Figure 4.18 - Synchronisation des signaux $x_1(t), \hat{x}_1(t)$

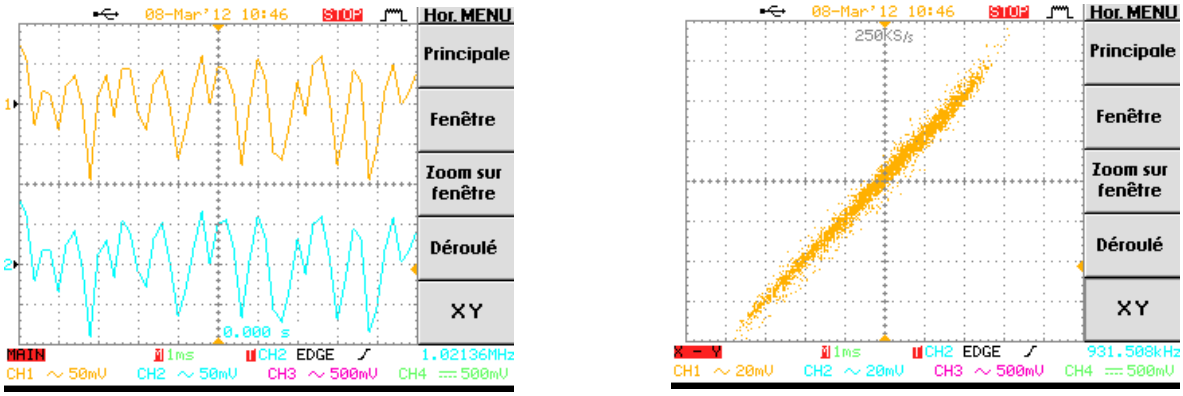


Figure 4.19 - Synchronisation des signaux $x_2(t), \hat{x}_2(t)$

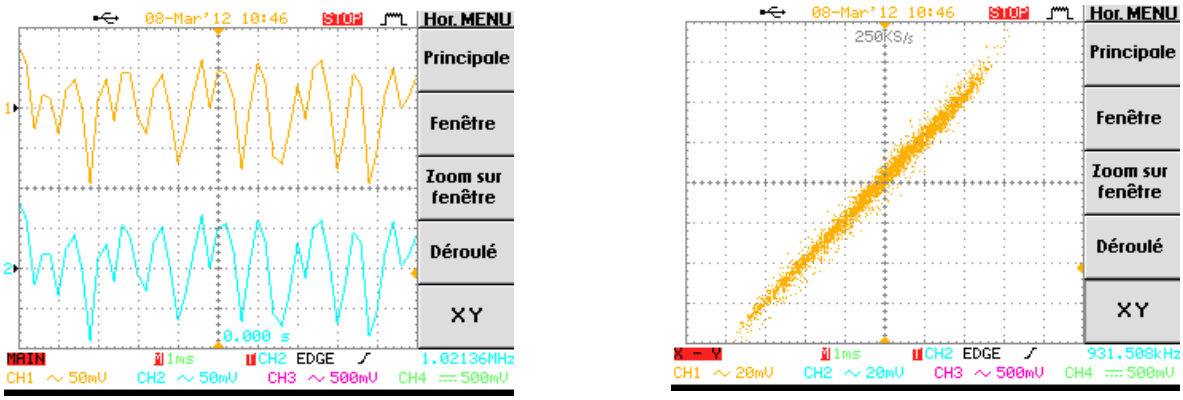


Figure 4.20 - Synchronisation des signaux $x_3(t), \hat{x}_3(t)$

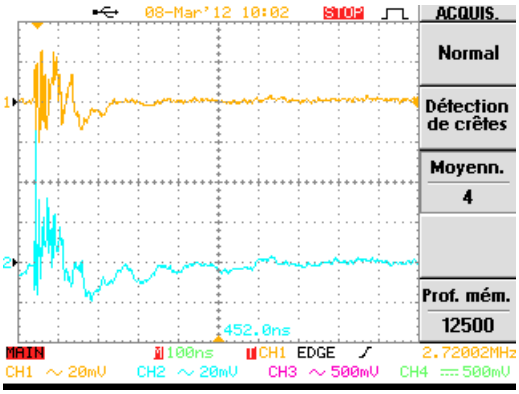


Figure 4.21 - Erreur de synchronisation $e_2(t)$ et $e_3(t)$

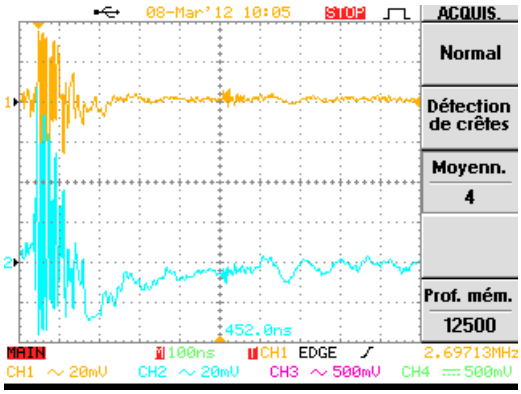


Figure 4.22 - Erreur de synchronisation $e_2(t)$ et $e_1(t)$

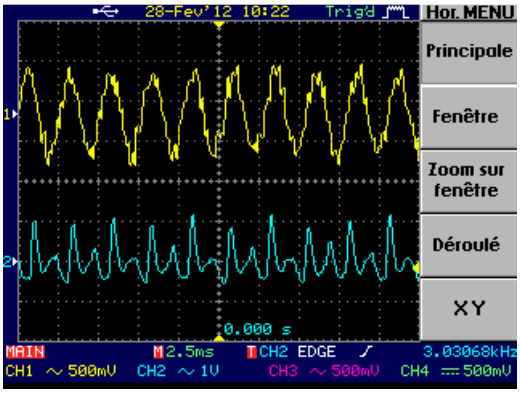
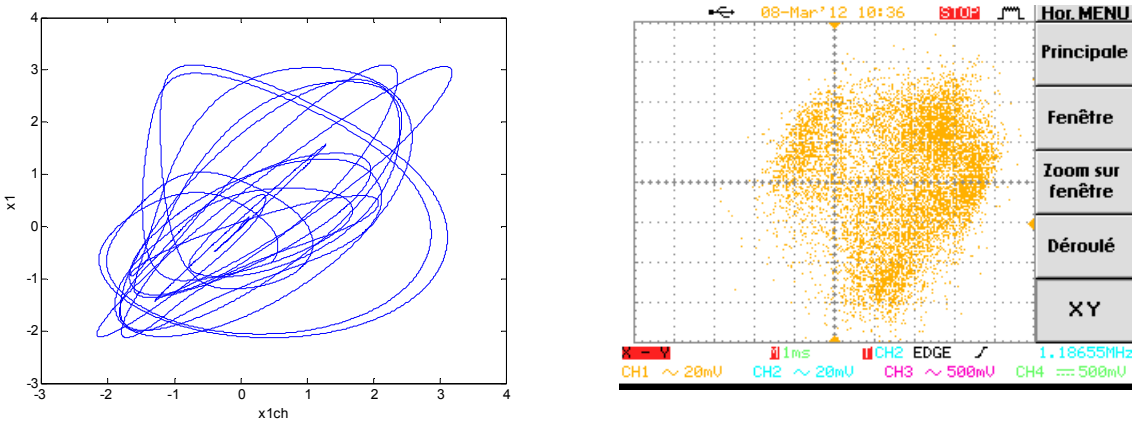


Figure 4.23 - Signal $\tilde{m}(t)$ décrypté

Lorsque l'émetteur et le récepteur ne sont pas synchronisés, la caractéristique $x_i(t) = f(\hat{x}_i(t))$ pour $i = 1, 2$ et 3 n'est plus une droite mais une courbe aléatoire. La figure 4.24 représente par exemple la caractéristique $x_1(t) = f(\hat{x}_1(t))$ obtenue par simulation (figure 4.24a) et expérimentalement (figure 4.24b).



(a) (b)

Figure 4.24 - Désynchronisation entre l'émetteur et le récepteur (a) Simulation (b) Expérimentale

L'environnement ISE fournit un rapport d'implémentation sous forme de tableaux contenant les informations utiles liées au design. Le tableau 4.1 comptabilise toutes les ressources internes utilisées en nombre et en pourcentage.

synchaot_cw Project Status			
Project File:	synchaot_cw.ise	**Current State:**	Programming File Generated
Module Name:	synchaot_cw	• **Errors:**	
Target Device:	xc3s500e-4fg320	• **Warnings:**	
Product Version:	ISE 10.1 - WebPACK	• **Routing Results:**	All Signals Completely Routed
Design Goal:	Balanced	• **Timing Constraints:**	All Constraints Met
Design Strategy:	Xilinx Default (unlocked)	• **Final Timing Score:**	0 (Timing Report)

synchaot_cw Partition Summary
No partition information was found.

Device Utilization Summary				
Logic Utilization	**Used**	**Available**	**Utilization**	**Note(s)**
Number of Slice Flip Flops	619	9,312	6%	
Number of 4 input LUTs	4,836	9,312	51%	
Logic Distribution				
Number of occupied Slices	2,796	4,656	60%	
Number of Slices containing only related logic	2,796	2,796	100%	
Number of Slices containing unrelated logic	0	2,796	0%	
Total Number of 4 input LUTs	5,448	9,312	58%	
Number used as logic	4,795			
Number used as a route-thru	612			
Number used as Shift registers	41			
Number of bonded IOBs	27	232	11%	
Number of BUFGMUXs	1	24	4%	
Number of MULT18X18SIOs	20	20	100%	
Number of RPM macros	28			

Tableau 4.1 - Ressources consommées par l'implémentation

La figure 4.25 est un aperçu du circuit implémenté sur la carte SPARTAN 3^E avec les routages et l'emplacement des ressources utilisées.

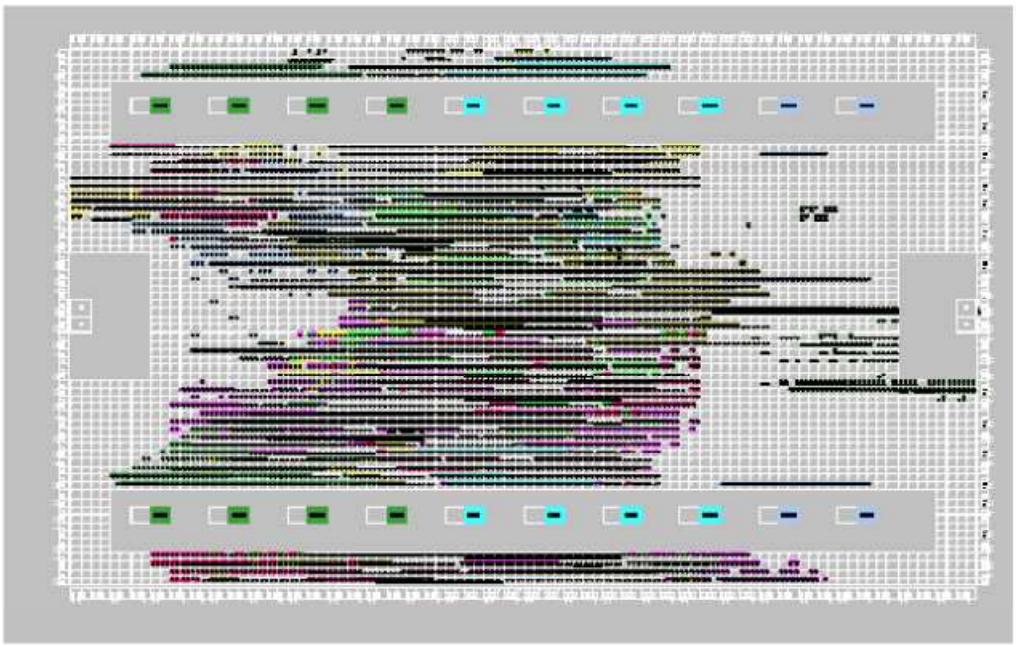


Figure 4.25 - Aperçu du circuit implémenté sur le FPGA SPARTAN 3^E

4.7 Conclusion

L'objectif de ce chapitre a été l'implantation sur cible FPGA d'une transmission chaotique. L'émetteur constitué de l'oscillateur chaotique de Colpitts incluant le message à crypter a été implémenté sur la carte FPGA SPARTAN 3^E et une concordance entre les signaux obtenus par simulation et les signaux relevés au niveau de la carte a été observée. L'implémentation du récepteur a mis en évidence le fonctionnement expérimental étape par étape de l'observateur à modes glissants permettant la récupération du message crypté associé à un léger chattering qui pourra être minimisé par un filtrage adéquat. Enfin, une estimation des ressources utilisées par les différentes implémentations a été faite.

CONCLUSION

Dans ce mémoire, nous avons étudié et réalisé une implémentation sur FPGA d'un système de communication chaotique basé sur la synchronisation à l'aide d'observateur à modes glissants pour la récupération du message crypté.

Le premier chapitre a été consacré à l'étude des systèmes dynamiques chaotiques Leurs principales caractéristiques ont étés décrites en mettant en évidence l'intérêt du calcul des exposants de Lyapunov ainsi que les différents scénarios possibles de transition vers le chaos. Dans le deuxième chapitre, nous avons présenté les principales méthodes de transmission d'information par les signaux chaotiques. Nous avons ensuite expliqué le principe de fonctionnement de l'oscillateur de Colpitts en étudiant les différents comportements de cet oscillateur en fonction des variations de ses paramètres. Ces études ont été mises en évidence à l'aide de simulations. Nous avons ajusté les paramètres de l'oscillateur de Colpitts afin d'obtenir un comportement chaotique. L'oscillateur de Colpitts incluant le message a été par la suite utilisé en tant qu'émetteur de notre système de communication. Dans le chapitre trois, nous avons montré que les systèmes de communication chaotiques sont basés sur la synchronisation entre l'émetteur et le récepteur. En général, le message est considéré comme une entrée inconnue pour l'émetteur. Cette entrée inconnue est récupérée par le récepteur, une fois que celui-ci a été synchronisé avec l'émetteur. Dans le dernier chaptre, une implémentation de l'ensemble émetteur chaotique –récepteur chaotique a été réalisée sur circuit sur circuit FPGA. Les différents signaux reconstruits au niveau du récepteur et en particulier le message ont été visualisés sur oscilloscope numérique.

La contribution principale de ce travail a été l'implémentation de la transmission chaotique sur circuit FPGA et la récupération du message crypté grâce à l'utilisation d'un observateur à modes glissants fonctionnant étape par étape. Nous

avons montré par simulation et par réalisation expérimentale la convergence en temps fini de l'observateur même dans le cas où les caractéristiques de l'émetteur et du récepteur ne sont pas identiques, ce qui est toujours le cas en pratique.

Comme perspectives, nous envisageons une augmentation de la fréquence de fonctionnement du système et étudier les contraintes éventuelles au niveau de l'implantation sur circuit FPGA, l'utilisation d'un observateur à modes glissants d'ordre supérieur afin de diminuer l'effet du chattering, et l'étude de la faisabilité d'un cryptage chaotique multi-entrées multi-sorties.

LISTE DES SYMBOLES ET DES ABREVIATIONS

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

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

$U \subseteq \mathbb{R}^n$: espace d'états.

x : vecteur d'états du système.

u : vecteur d'entrée du système.

y : vecteur de sortie du système.

μ : paramètre de bifurcation.

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

x^* : point d'équilibre.

A : matrice jacobienne de $f(x)$.

λ_i : valeurs propres de la matrice jacobienne ou exposant de Lyapunov.

$m(t)$: message transmis.

α : gain en courant du transistor en base commune.

g : gain de la boucle de réaction.

Q : facteur de qualité.

$diag(\alpha_i)$: matrice diagonale.

k_{ai} : constante de couplage.

$L_f h$: dérivée de Lie de h dans la direction de f.

e : vecteur d'états des erreurs d'observation.

S : surface de glissement.

$V(x)$: fonction de Lyapunov.

$sign$: fonction signe.

k_i : coefficient de gain de l'observateur à modes glissants.

E_i : coefficient conditionnel de l'observateur à modes glissants.

DES : Data Encryption Standard.

FPGA : Field Programmable Gate Array.

VLSI : Very Large Scale Integration.

CAN : Convertisseur Analogique Numérique.

CNA : Convertisseur Numérique Analogique.

LUT : Look-Up Table.

CLB : Configurable Logic Block.

HDL : Hardware Description Langage.

CPLD : Complex Programmable Logic Device.

REFERENCES

1. Nijmeijer, H. and Van Der Schaft, A. J., “Nonlinear dynamical control systems”, Springer, 1990.

2. Slotine, J. J. E. and Li, W., “Applied nonlinear control”, Prentice Hall, New Jersey, 1991.

3. Goncalvès, E., “Introduction aux systèmes dynamiques et chaos”, Institut National Polytechnique de Grenoble, 2004.

4. Dang-Vu, H. and Delcarte, C., “Bifurcations et chaos : Une introduction à la dynamique contemporaine avec des programmes en Pascal, Fortran et Mathematica”, Ellipses, 2000.

5. Strogatz, S. H., “Nonlinear dynamics and chaos”, Perseus Book, 1994.

6. Alligood, K. T., Sauer, T. D. and Yorke, A. J., “Chaos : An introduction to dynamical systems”, Springer-verlag, New York, 1996.

7. Chen, G. and Ueta, T., “Chaos in Circuits and systems”, World Scientific, Singapore, 2002.

8. Pecora, L. M. and Caroll, T. L., “Synchronization in chaotic systems”, Phys. Rev. Lett. 64, p. 821–824, 1990.

9. Vernam, G. S., “Cipher printing telegraph systems for secret wire and telegraphic communications”, J. Amer. Inst. Elec. Eng. 55, p. 109, 1926.

10. Parlitz, U., Kocarev, L., Stojanovski, T. and Preckel, H., “Encoding messages using chaotic synchronization”, Phys. Rev. E 53, p. 4351–4361, 1996.

11. Wu, C. W. and Chua, L. O., “A simple way to synchronize chaotic systems with applications to secure communication systems”, Int. J. Bifurcation and Chaos 3, p. 1619–1627, 1993.

12. Corron, N. and Hahs, D., “A new approch to communication using chaotic signals”, IEEE Transactions on Circuit and Systems, vol. 44, pp. 373–382, 1997.

13. Dedieu, H., Kennedy, M. P. and Hasler, M., “Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua’s circuits”, IEEE Transactions on Circuits and Systems I, vol. 40, no. 10, pages 634–642, 1993.

14. Parlitz, U., Chua, L. O., Kocarev L., Halle, K. S. and Shang, A., “Transmission of digital signals by chaotic synchronization”, International Journal of Bifurcation and Chaos, vol. 2, pages 973–977, 1993.

15. Tang, S., Chen, H. F., Hwang S. K. and Liu, J. M., “Message encoding and decoding through chaos modulation in chaotic optical communications”, IEEE Transactions on Circuits and Systems I, vol. 49, no. 2, pages 163–169, 2002.

16. Inoue, E. and Ushio, T., “Chaos communication using unknown input observers”, Electronics and Communications in Japan, vol. J82-A, no. 12, pages 1801–1807, 2001.

17. Millérioux, G. and Daafouz, J., “Unknown input observers for message-embedded chaos synchronization of discrete-time systems”, International Journal of Bifurcation and Chaos, vol. 14, no. 4, pages 1357–1368, 2004.

18. Boutayeb, M., Darouach, M. and Rafaralahy, H., “Generalized state-space observers for chaotic synchronization and secure communication”, IEEE Transactions on Circuits and Systems I, vol. 49, no. 3, pages 345–349, 2002.

19. Liao, T.-L. and Huang, N.-S., “An observer-based approach for chaotic synchronization with applications to secure communications”, IEEE Transactions on Circuits and Systems I, vol. 46, no. 9, pages 1144–1150, 1999.

20. Feldmann, U., Hasler, M. and Schwarz, W., “Communication by chaotic signals : The inverse system approach”, Int. J. Circuit Theory Appl., vol. 24, pages 551–579, 1996.

21. Ogoraztek, J. M., “Chaos and complexity in nonlinear electronic circuits”, World Scientific, Singapore, Series A, Vol.22, 1997.

22. Hasler, M., “Electrical circuits with chaotic behavior”, Proc. IEEE 75, p. 1009–1021, 1987.

23. Rubezic, V. and Ostojic, R., “Synchronization of chaotic Colpitts oscillators with application to binary communications”, IEEE, 1999.

24. L'Hernault, M., Barbot, J. P. and Ouslimani, A., “Sliding mode observer for a chaotic communication system : experimental results”, 1st IFAC conference on analysis and control of chaotic systems, France, 2006.

25. Maggio, G. M., di Bernardo, M. and Kennedy, M P., “Nonsmooth Bifurcations in Piecewise-Linear Model of the Colpitts Oscillator”, IEEE Transactions on Circuits and Systems-I : Fundamental Theory and Applications 47, p. 1160–1177, 2000.

26. Maggio, G. M. and Feo , O. D., “Nonlinear Analysis of the Colpitts Oscillator and Applications to Design”, IEEE Transactions on circuits and systems-I : Fundamental Theory and Applications 46, 1999.

27. Maggio, G. M. and Kennedy, M. P., “Classification of steady state behavior of the Colpitts oscillator”, in Proceedings of ICECS, p. 811–814, 1999.

28. Boutat-Baddas, L., Barbot, J. P., Boutat; D. and Tauleigne, R., “Sliding Mode Observers and Observability Singularity in Chaotic Synchronization”, in Mathematical problems in engineering, p. 11–31, 2004.

29. Tang, Y. S., Mees, A. I. and Chua, L. O., “Synchronization and chaos”, IEEE Transactions on Circuits and Systems 30, p. 1–2, 1983.

30. Pecora, L. M. and Carroll, T. L., “Synchronized chaotic signal and systems”, Proc. IEEE ICASSP, 1992.

31. Sira-Ramirez, H. and Cruz-Hernandez, C., “Synchronization of chaotic systems : A generalized hamiltonian system approach”, Int. J. Bifurcation and Chaos 11, p. 1381–1395, 2000.

32. Fradkov, A. L. and Pogromsky, A. Y., “Introduction to Control of Oscillations and Chaos”, World Scientific, Singapore, Series A, Vol.35, 1998.

33. Chen, M., Zhou, D. and Shang, Y., “A new observer-based synchronization scheme for private communication”, Chaos, Solitons and Fractales 24, p. 1025–1030, 2005.

34. Yang, T., “A survey of chaotic secure communication systems”, International Journal of Computational Cognition 2 (2004), p. 81–130, 2004.

35. Kocarev, L., Shang, A. and Chua, L. O., “Transitions in dynamical regimes by driving : a unified method of control and synchronization of chaos”, Chaos, Solitons and Fractales 24, p. 1025–1030, 2005.

36. Baziliauskas, A., Tamasevicius, A., Bumeliene, S. and Lindberg, E., “Synchronization of Chaotic Colpitts Oscillators”, Scientific Proceedings of Riga Technical University I, p. 55–58, 2001.

37. Rubezic, V., Lutovac, B. and Ostojic, A., “Linear Generalized Synchronization of Two Chaotic Colpitts Oscillators”, in Proceedings of ICECS, p. 223–225, 2001.

38. Chua, L. O., Kocarev, L., Eckert K. and Itoh, M., “Experimental Chaos Synchronization in Chua's Circuit”, Int. J. Bifurcation and Chaos 2, p. 705–708, 1992.

39. Mykolaitis, G., Tamasevicius, A. and Bumeliene, S., “Experimental demonstration of chaos from Colpitts oscillator in VHF and UHF ranges”, Electronics letters 40, 2004.

40. Caroll, T. and Pecora, L. M., “Synchronizing chaotic circuits”, IEEE Trans. on Circuits and Systems 38, p. 453–456, 1991.

41. Nijmeijer, H. and Mareels, M. Y., “An observer looks at synchronization”, IEEE Transactions on Circuits and Systems 44, p. 882–890, 1997.

42. Boutat-Baddas, L., “Analyse des singularités d'observabilité et de détectabilité : Application à la synchronisation des circuits électroniques chaotiques”, Thèse de doctorat de l’université Cergy-Pontoise, 2002.

43. Krener, A. J. and Isidori, A., “Linearization by output injection and non-linear observers”, Systems and control letters 3, p. 47–52, 1983.

44. Floquet, T. and Barbot, J. P., “A sliding mode approach of unknown input observers for linear systems”, 43rd IEEE CDC, Atlantis, Paradise Island, Bahamas, 2004.

45. Devaney, R. L., “An Introduction to Chaotic Dynamical Systems”, Westview Press, 2003.

46. Barbot, J. P., Djemai, M. and Boukhobza, T., “Sliding mode observers”, in Sliding mode control in engineering, Marcel Dekker, p. 103–130, 2002.

47. L'Hernault, M., “Faisabilité d’un système d’émission-réception analogique pour les communications sécurisées par le chaos”, Thèse de doctorat de l’université Paris 6, 2007.

48. Andina J.R, Moure M.J., Valdes M.D “Features, design tools, and application domains of FPGA” IEEE Transactions on Industrial Electronics, Vol54,n°4, pp11810-1823, 2007.

49. Cofer R.C ,Harding B.F ,“Rapid System prototyping with FPGA” ,Newnes,2006.

50. Maxfield C., “World class designs”, Newnes ,2009.

51. Steve K.,“Advanced FPGA design” ,Wiley,2007.

52. Pedroni V. A. , “ Circuit dessign with VHDL”, MIT Press, 2004.

53. Chu P. P. “FPGA Prototyping by verilog examples”, Wiley, 2008.

54. Li G. H., Zhou S. P.Yang K., “Controlling chaos in Colpitts oscillator”, Chaos, Solitons and Fractal 33, pp 582-587, 2007.