République Algérienne Démocratique Et Populaire
Ministère de l'Enseignement Supérieur Et De La Recherche Scientifique

Université Mentouri Constantine 1

Faculté des Sciences Exactes

Département de Mathématiques

N°d'ordre : 219/DS/2018
Série :11/Math/2018

THESE DE DOCTORAT

EN Mathématique

Présenté par : Berguellah Nour Elhouda

Intitulé

SYSTÈMES DYNAMIQUES CHAOTIQUES ET CRYPTOGRAPHIE : APPLICATION À LA SÉCURITÉ DES COMMUNICATIONS

Soutenue le :22/11/2018

Devant jury

Mr Bessila khaled	M.A	Univ. Mentouri. Constantine 1	Président
Mr Hamri Nasr eddine	Prof	Centre Universities de Mila	Rapporteur
Mr Zeraoulia Elhaj	Prof	Univ.de Tebessa	Examinateur
Mr Berkene Abdelhak	M.A	Univ. Mentouri. Constantine 1	Examinateur
Mr Hmieda Ali	M.A	Univ. Mentouri. Constantine 1	Examinateur
Mr Abdelwaheb Med saleh	M.A	Centre Universities de Mila	Examinateur

Remerciements

Je remercie avant tout DIEU Allah tout puissant pour la volonté, la santé et la patience qu'il m'a donnée afin de réaliser ce modeste travail.

J'exprime ma plus grande reconnaissance et mon respect à mon encadreur Pr HAMRI NASR EDDINE pour avoir accepté de diriger ce travail, de m'avoir guidé et soutenu avec patience et indulgence, pour ces lectures enrichissantes de ma thèse et pour les précieux conseils qu'il n'a cessé de me prodiguer.

J'exprime également mes remerciements aux membres du jury, qui ont accepté d'évaluer mon travail de thèse. Merci à Monsieur BSSILA KHALED d'avoir accepté d'être le président du jury de cette thèse, à Messieurs HMIEDA, BERKEN, ZRAOULIA, et Mr *M-S ABD ELWAHAB* pour avoir accepté d'examiner ce manuscrit et de faire partie de mon jury de thèse.

Mes sincères remerciements s'adressent aussi à tous mes enseignants à l'université de Constantine 1 depuis licence jusqu'à maintenant.

Il s'agit de mes parents qui ont tout fait que je sois ce que je suis, je remercie particulièrement ma mère dont le fait de penser à elle me redonne la confiance et me rassure, également à mon père pour ces plusieurs conseils et son soutient.

Toute ma gratitude et mes chaleureux remerciements vont à toute la famille et à la belle famille.

Enfin, je ne remercierai sans doute jamais assez mon cher époux, qui a su faire preuve d'une grande patience, de compréhension et m'a accompagné et soutenu de façon permanente dans les moments difficiles et mes chère enfants BARAE,ABDERAHMANE et LOKMANE.

Je n'omettrai pas de remercier mes collègues de l'école supérieure de comptabilité et de finance chacun avec son nom pour leurs soutien et conseils.

Chaotic dynamical systems and cryptography : application on communication security

Abstract

In this work we present two chaotic models used for secure transmission of a functional message which is the function sin ωt, without forgetting the role of synchronization mechanisms of chaotic systems to the success of these transmissions.

Key words :

Chaos; Synchronization; Cryptography; CSK modulator; CSK demodulator.

Systèmes dynamiques chaotiques et cryptographie : Application à la sécurité des communications

Résumé :

Dans ce travail nous présentons deux modèles chaotiques utilisés pour transmission sécurisé d'un message fonctionnel qui est la fonction sin ωt, en soulignant le rôle des mécanismes de synchronisation des systèmes chaotiques dans la réussite de ces transmissions.

Mots clés :

Chaos ; Synchronisation ; Cryptographie ; Modulateur CSK; Démodulateur CSK.

الانظمة الديناميكية الفوضوية و التشفير تطبيق حول تامين الاتصالات

ملخص

في هذا العمل نقدم نوعين من النماذج الفوضوية المستخدمة في عملية النقل الآمن للرسالة الدالية وهي الدالة $\sin\omega t$,دون ان ننسى دور آليات التزامن لإنجاح هذه الإرساليات

الكلمات المفتاحية

المغير CSK , المنضم CSK , التشفير, التزامن , الفوضى

Table des matières

Chapitre 1

Introduction générale

L'échange de données (paroles, images, signes, signal etc....) pour l'homme est une nécessité. La sécurité de cette opération devient parfois plus qu'une exigence. Ainsi depuis César à l'ère de l'informatique, le chiffrement de certains messages a toujours été un besoin afin de les cacher à tout intrus non autorisé de façon à s'abriter d'un éventuel usage malveillant. De nos jours, l'ensemble de ces méthodes a été regroupé dans une branche appelée la cryptographie. Parallèlement, une autre branche ennemie à la cryptographie appelée la cryptanalyse a été développée, qui est l'art de révéler les textes en clair qui ont été l'objet d'un chiffrement sans connaître la clé de déchiffrement.

Ces 20 dernières années ont été marquées par une révolution de la technologie de l'information avec l'avènement de l'Internet [17] [22], la miniaturisation des moyens de communication, comme le téléphone et l'ordinateur portables et la prolifération des réseaux sans fil. Cette banalisation d'échange d'informations à n'importe quels lieu et moment et de n'importe quelle manière, a causé l'engouement du grand public et même les organismes de pouvoir culturel, financier, politique, militaire et scientifique pour les nouvelles technologies de l'information. Entraînant la circulation d'un flux grandissant de données, à travers des canaux généralement qui ont un aspect public. La valeur de la donnée transmise est intrinsèque à son contenu qui peut être

une simple lettre de bonjours, ou un signal de commande d'un réacteur nucléaire à tel point qu'il est souvent nécessaire de le protéger. D'où vient l'importance spéciale assumée par la cryptographie. En conséquence la cryptographie est devenue aujourd'hui pour tous un moyen quotidien de protection des données qui doivent être communiquées ou stockées à longue période et de protéger des transferts de fonds électroniques et des communications classifiées [5] [21].

Les premiers principes de base de la cryptographie moderne reviennent à Auguste Kerkhoffs, énoncés dans son article intitulé "La cryptographie militaire" publié en 1883 et dont l'idée la plus importante est que la sécurité du chiffre ne doit pas dépendre de ce qui ne peut être facilement changé. En d'autres termes, aucun secret ne doit résider dans l'algorithme de cryptage mais plutôt dans la clé.

Ces principes ont été reformulés par Claude Shannon en posant également le problème de sécurité des cryptosystèmes avec l'introduction de la notion de sécurité parfaite, qui est une approche irréalisable en pratique. D'où sont fondés les algorithmes de cryptage utilisés actuellement, en profitant astucieusement de la puissance des mathématiques et en utilisant adéquatement des techniques de substitutions, de permutations et d'itérations.

Bien que l'efficacité de ces algorithmes soit reconnue, leur temps de calcul est long, ce qui entraîne une diminution du débit des messages transmis [15]. Il y à aussi la question de réduction du niveau de confidentialité dans ces algorithmes avec le développement sans cesse des techniques de cryptanalyses, causées par la puissance croissante des calculateurs disponibles. Ces failles ont poussé les recherches vers le développement de nouveaux systèmes. L'usage du chaos a été une des alternatives proposées [9].

Les systèmes dynamiques chaotiques sont des systèmes déterministes non linéaires qui montrent souvent un comportement non divergent, apériodique et éventuellement borné. Les signaux qui évoluent dans ces systèmes sont en général, à large bande, ce qui fait apparaître leur trajectoire comme du bruit pseudo aléatoire. En

raison de ces propriétés et à cause de la fragilité des cryptosystèmes classiques, les signaux chaotiques fournissent potentiellement une classe importante des signaux qui peuvent être utilisés pour masquer les informations dans une transmission sécurisée [15], il suffit donc de les mélanger de manières appropriées au messages en clair qu'on souhaite transmettre confidentiellement [22] [8].

La difficulté dans l'utilisation de cette procédure réside dans la restitution du message original. Ainsi ce n'est qu'à partir de 1990 après la découverte de Carroll et Pécora de la synchronisation du chaos [12], que la communication sécurisée chaotiquement a fait l'objet d'un intérêt croissant dans la littérature.

Dans ce travail on a présenté des approches qui proposent l'usage du chaos pour sécuriser la transmission des données. Ainsi il est organisé comme suit :

Dans le premier chapitre on fait une introduction générale de la cryptographie, dans lequel on analyse ses limites où on expose les motivations, qui poussent à chercher des techniques alternatives.

Le deuxième chapitre est une présentation théorique des systèmes dynamiques chaotiques.

Le troisième chapitre est consacré au concept de la synchronisation entre les systèmes chaotiques, des résultats de simulations sont aussi présentés.

Le quatrième chapitre sera consacré à la cryptographie chaotique, l'utilisation la plus souhaitée du signal chaotique. On commence d'abord par une classification des cryptosystèmes ainsi que leurs relations avec le chaos. Enfin on donne un état de l'art sur les différentes techniques de cryptage en utilisant le chaos.

Le cinquième chapitre présente les résultats obtenus en simulant deux modèles de cryptosystèmes chaotiques accompagnés par des interprétations et des analyses des performances.

Enfin, la conclusion présente le bilan du travail réalisé et les perspectives envisagées

.

Chapitre 2

Système Dynamique

2.1 Définition

Dans ce chapitre nous étudions des systèmes d'équations différentielles dans le cas continu de la forme :

$$\frac{dx}{dt} = \dot{x} = f(x, t, v), \quad x \in U \subseteq \mathbb{R}^n, \quad v \in V \subseteq \mathbb{R}^p \tag{2.1}$$

Le système (2.1) est appelé système dynamique, $\mathbb{R}^n$ est l'espace des phases et $\mathbb{R}^p$ est l'espace des paramètres.

Exemple 1. *: L'oscilateur de Duffing*

$$\begin{cases} \frac{dx}{dt} = y \\ \frac{dy}{dt} = x - x^3 - \delta y + \gamma \cos \omega t \end{cases} \tag{2.2}$$

Où δ, α, ω, γ sont des paramètres physiques réels, $\mathbb{R}^2$ est l'espace des phases et $\mathbb{R}^3$ est l'espace des paramètres.

2.2 Système autonome et non autonome

Considérons un système d'équations différentielles du premier ordre :

$$\frac{dx}{dt} = f(x,t) \tag{2.3}$$

où $x = (x_1, x_2, \ldots, x_n)^t$ et $f = (f_1, f_2, \ldots, f)^t$ sont champs de vecteurs (pour simplifier l'écriture) ; nous ne montions pas les paramètres qui se trouvent dans les f_i, nous supposons que les f_i sont de classe $C^r (r \geqslant 1)$ en x et t. Dans ce cas les fonctions $x_i(t)$ sont aussi de classe C^r. Alors on peut transformer les équations différentielles d'ordre $n (n > 1)$ en un système de n équations du premier ordre avec un changement de variable approprié, par exemple :

$$\frac{d^n x}{d^n t} = f(x, \frac{dx}{dt}, \frac{dx^2}{d^2 t}, \ldots, \frac{dx^{n-1}}{d^{n-1} t}, t) \tag{2.4}$$

Peut s'écrire sous forme :

$$\begin{cases} \frac{dx_1}{dt} & = & x_2 \\ \frac{dx_2}{dt} & = & x_3 \\ \vdots & & \\ \frac{dx_{n-1}}{dt} & = & x_n \\ \frac{dx_n}{dt} & = & f(x_1, x_2, \ldots, x_n, t) \end{cases} \tag{2.5}$$

Où l'on a posé $x_1 = x$ (à noter que cette transformation n'est pas unique). La solution de (2.3) pour condition initial $x(t_0) = x_0$ sera notée $x(x_0, t)$. Elle décrit dans l'espace des phases $x = (x_1, x_2, \ldots, x_n)$ une courbe intégrale appelée trajectoire ou orbite. Lorsque le champ de vecteurs f dépend explicitement du temps le système est dit non autonome, dans le cas contraire on dit que le système est autonome. Dans un système autonome, la trajectoire $x(x_0, t)$ ne dépend pas de la condition initiale t_0.

Exemple 2.

$$\begin{cases} \frac{dx}{dt} & = & y \\ \frac{dy}{dt} & = & -x \\ x(t_0) & = & 1 \quad et \quad y(t_0) = 0 \end{cases} \tag{2.6}$$

$$\begin{cases} \frac{dx}{dt} & = & y \\ \frac{dy}{dt} & = & -x+t \\ x(t_0) & = & 1 \quad et \quad y(t_0)=0 \end{cases} \tag{2.7}$$

La solution du système autonome (2.6) est :

$$x(t)=\cos(t-t_0), \quad y(t)=-\sin(t-t_0)$$

La trajectoire est un cercle passant par le point $(1,0)$ *et d'équation* $x^2+y^2=1$. *Par contre, la trajectoire du système non autonome (2.7) dépend de la condition initiale* t_0, *ainsi :*

1. *Si* $t_0=\frac{\pi}{2}$ *la solution est* $x(t)=\cos(t)+(1-\frac{\pi}{2})\sin(t)+t \quad et \quad y(t)=-\sin(t)+(1-\frac{\pi}{2})\cos(t)+1$
2. *Si* $t_0=\pi$ *la solution est*
   $x(t)=(\pi-1)cos(t)+\sin(t)+t \quad et \quad y(t)=-(\pi-1)\sin(t)+\cos(t)+1$
3. *Si* $t_0=2\pi$ *la solution est*
   $x(t)=(1-2\pi)\cos(t)-\sin(t)+t \quad et \quad y(t)=-(1-2\pi)\sin(t)-\cos(t)+1$

Les trajectoires de ces deux cas au voisinage du point $(1,0)$ *sont représentées sur la figure (2.1).*

2.3 Flot et point fixes

2.3.1 Flot d'un Champ de vecteurs

Considérons le système autonome :

$$\frac{dx}{dt}=f(x), \quad \forall x\in\mathbb{R}^n \tag{2.8}$$

Définition 1. *Soit* $x(x_0,t)$, $x\in D$ *une solution de (2.8) comme condition initial* $x(0)=x_0$, *on appelle flot de (2.8) ou champ de vecteurs* f, *l'application*

$$\begin{array}{rcl} \phi_t : D & \longrightarrow & \mathbb{R}^n \\ x_0 & \longmapsto & \phi_t(x_0)=x(x_0,t) \end{array}$$

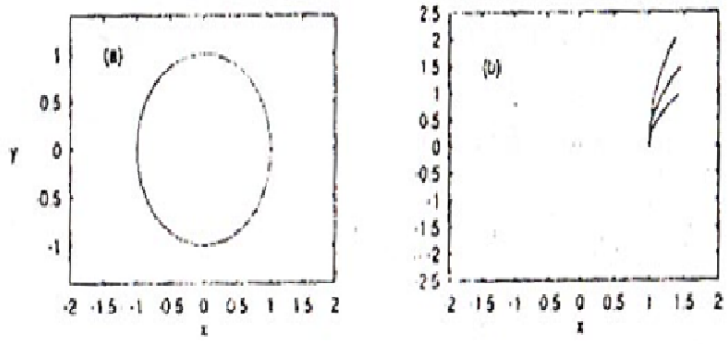


FIGURE 2.1 – Système autonome à droite et Système non-autonome à gauche

ϕ_t Possède les propiétés suivantes :

1. *$\phi_t(x_0)$ est de classe C^r.*
2. *$\phi_t(x_0) = x_0$*
3. *$\phi_{t+s}(x_0) = \phi_t(\phi_s(x_0))$*

Exemple 3. *: Considérons le système linéaire*

$$\frac{dx}{dt} = Ax, \quad A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \tag{2.9}$$

où $x(0) = x_0$, la solution est $x(x_0, t) = e^{At}x_0$ avec $e^{At} = \begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$

$\phi_t = e^{At}$ est le flot de (2.9).

La famille d'application ϕ_t est appelée semi groupe.

Un point $a \in U$ est le point limite ω d'une trajectoire $x(x_0, t)$ s'il existe une séquent $t_n \longrightarrow +\infty$ telle que $\lim_{n\longrightarrow\infty} \phi_{t_n} = a$.

De même un point $b \in U$ est le point limite α d'une trajectoire $x(x_0, t)$ s'il existe une séquent $t_n \longrightarrow -\infty$ telle que $\lim_{n\longrightarrow\infty} \phi_{t_n} = b$.

L'ensemble des points limites α (resp limite ω) de $x(x_0, t)$ est désigné par $\alpha(x)$ (resp

$\omega(x)$ *).*

L'ensemble $\alpha(x) \cup \omega(x)$ *est appelé l'ensemble limite de* $x(x_0, t)$.

Un cycle limite α *(resp* ω *) est une orbite fermé* Γ *tel que* $\Gamma \subset \alpha(x)$ *(resp* $\Gamma \subset \omega(x)$*).*

Définition 2. *On appelle point fixe (ou point d'équilibre) de (2.8) le point* $\overline{x}$ *de l'espace des phases obtenue en annulant le second membre de (2.8) :*

$$f(\overline{x}) = 0 \tag{2.10}$$

Par changement de variable $\varepsilon = x - \overline{x}$*, on peut ramener le point* $\overline{x}$ *à l'origine.*

2.3.2 Stabilité des points fixes

Nous illustrons les concepts des points fixes stables, instables, et asymptotiquements stables par l'exemple du pendule amorti.

Exemple 4. *L'équation du mouvement du pendule est :*

$$\frac{d\theta^2}{dt^2} + \gamma \frac{d\theta}{dt} + k \sin\theta = 0 \tag{2.11}$$

où : $\gamma = \frac{c}{ml}$, $k = \frac{g}{l}$, *et* $\theta(t)$ *est l'angle que fait à l'instant* t, l *est le fil avec la verticale* (OR), g *est l'accélération de la pesanteur,* $c > 0$ *est le coefficient d'amortissement de l'air. La force d'amortissement* $c\frac{d\theta}{dt}$ *s'oppose toujour à la direction du mouvement.*

Pour simplifier le problème on suppose que $k = 1$*, (2.11) s'écrit alors en posant :* $x = \theta, \quad y = \frac{d\theta}{dt}$ *:*

$$\begin{cases} \frac{dx}{dt} &= y \\ \frac{dy}{dt} &= -\sin x - \gamma y \end{cases} \tag{2.12}$$

Les points fixes du système (2.12) sont donnés par : $\overline{y} = 0$ *et* $\overline{x} = \pm n\pi$ *et* $n = 0, 1, \ldots$

Ces points fixes correspondants à deux positions d'équilibres physiques :

Le point d'équilibre $R(\theta = 0)$ *est stable, et le point d'équilibre* $R'(\theta = \pi)$ *est instable.*

En présence du frottement de l'air $\gamma \neq 0$*, la masse va osciller autour de* R *avec une amplitude de plus en plus petit et tend vers* R *lorsque* $t \longrightarrow \infty$*, dans ce cas on dit*

que le point R est asymptotiquement stable.
En l'absence du frottement de l'air $\gamma = 0$, la masse va osciller indéfiniment autour de R avec une amplitude constante, le point R alors est un point d'équilibre stable.

Définition 3. *Un point fixe $\overline{x} \in \mathbb{R}^n$ est stable si et seulement si :*

$$\forall \varepsilon > 0, \exists \delta > 0 : \| x(0) - \overline{x} \| < \delta \Longrightarrow \| x(t) - \overline{x} \| < \varepsilon$$

Si de plus

$$\exists \delta_0 > 0, avec : 0 < \delta_0 < \delta \quad , \| x(0) - \overline{x} \| < \delta_0 \Longrightarrow \lim_{t \longrightarrow \infty} x(t) = \overline{x}$$

$\overline{x}$ est asymptotiquement. S'il n'est pas stable alors il est instable $(x(0) = x_0)$.

2.3.3 Système linéarisé et valeurs propres

Supposons que, par changement de coordonnées, le point fixe été ramené à l'origine $f(0) = 0$, le developement de Taylor en $x = 0$ s'écrit :

$$f(x) = Df(0)x + \frac{1}{2!}D^2 f(0)(x,x) + \frac{1}{3!}D^3 f(0)(x,x,x) + \ldots \tag{2.13}$$

où, l'on a posé $f = (f_1, f_2, \ldots, f_n)^t$ et $x = (x_1, x_2, \ldots, x_n)^t$ alors :

$$\begin{array}{lcl} Df(x)(x) & = & \sum_j (\frac{\partial f(x)}{\partial x_j}) x_j \\ D^2 f(x)(x,x) & = & \sum_{i,j} (\frac{\partial f^2(x)}{\partial x_i x_j}) x_i x_j \\ D^3 f(x)(x,x,x) & = & \sum_{i,j,k} (\frac{\partial f^3(x)}{\partial x_i x_j x_k}) x_i x_j x_k ... \end{array} \tag{2.14}$$

La matrice $Df(x) = (\frac{\partial f_i(x)}{\partial x_j})$ s'appelle la matrice jacobienne de $f(x)$(son déterminant est le jacobien) pour x petit, (2.13) montre que le comportement du système au voisinage de 0 est celui du système linéarisé

$$\dot{x} = Df(0)x \tag{2.15}$$

Dans le cas où la matrice $Df(x)$ posséde n valeurs propres $\lambda_i, \quad i = 1, n$ distinctes, la solution de (2.15) est :

$$x = \sum_{i=1,n} c_i a^{(i)} \exp \lambda_i t$$

où $a^{(i)}$ sont les vecteurs propres correspondant à la valeur propre λ_i et les c_i sont des constantes (déterminées par les conditions initiales). On en deduit que :

1. Si toutes les valeurs propres λ_i ont leurs parties réelles négatives le point fixe est asymbtotiquement stable.
2. S'il y a au moins une valeur propre à d'imaginaire pure et les autres valeurs propres ayant leurs parties réelles négatives, le point fixe est un centre ou un point elliptique (stable mais pas asymptotiquement stable).
3. Si une des valeurs propres à sa partie réelle positive le point fixe est instable.
4. Si $Df(0)$ n'a pas de valeurs propres nulles ou purement imaginaire le point fixe est un point hyperbolique, dans le cas contraire il est non hyperbolique.
5. S'il existe i et j tel que $Re\lambda_i < 0$ et $Re\lambda_j > 0$, le point fixe est un point selle.
6. Si toutes les valeurs propres de $Df(0)$ sont réelles et de même signe, le point fixe est un noeud ; un noeud stable est un puits, et un noeud instable est une source.

Exemple 5. *Dans l'espace des phases $\mathbb{R}$, l'équation (2.15) s'écrit :*

$$\dot{x} = Ax \tag{2.16}$$

avec $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$*, les valeurs propres de la matrice A sont les solutions de l'équation $\lambda^2 - p\lambda + q = 0$ avec $p = a + d$ et $q = ad - bc$, on suppose que la matrice A soit diagonalisable, les solutions de (2.16) sont alors :*

$$x(t) = (c_1 a^{(1)} \exp \lambda_1 t + c_2 a^{(2)}) \exp(\lambda_2 t), \quad si \ \ \Delta = p^2 - 4q \neq 0, \quad \lambda_{1,2} = \frac{p \pm \sqrt{\Delta}}{2}$$

$$x(t) = (c_1 a^{(1)} + t c_2 a^{(2)}) \exp(\frac{pt}{2}), \quad si \ \ \Delta = p^2 - 4q = 0$$

où a^1, a^2 sont des vecteurs propres de A, et c_1, c_2 des constantes d'intégrations.
On en deduit la classification des points fixes :

1. *Si* $\Delta = p^2 - 4q < 0, \quad p \neq 0$, *le point fixe est asymptotiquement stable si* $p < 0$ *et instable si* $p > 0$. *Les trajectoires au voisinage de 0 sont des spirales ; le point fixe s'appelle un foyer.*

2. *Si* $\Delta = p^2 - 4q < 0, \quad p = 0$ *le point fixe est un centre ou un point elliptique. Les trajectoires au voisinage de* 0 *sont des ellipses ; l'origine est un point fixe stable mais pas asymptotiquement stable.*

3. *Si* $\Delta = p^2 - 4q = 0, \quad p \neq 0$ *le point fixe est un noeud stable si* $p > 0$, *asymptotiquement stable si* $p < 0$.

4. *Si* $\Delta = p^2 - 4q > 0, \quad q > 0$ *le point fixe est un noeud impropre instable si* $p > 0$, *asymptotiquement stable si* $p < 0$.

5. *Si* $\Delta = p^2 - 4q > 0, \quad q < 0$ *le point fixe est un point selle.*

Les différents points fixes sont indiqués sur la figure (2.2).

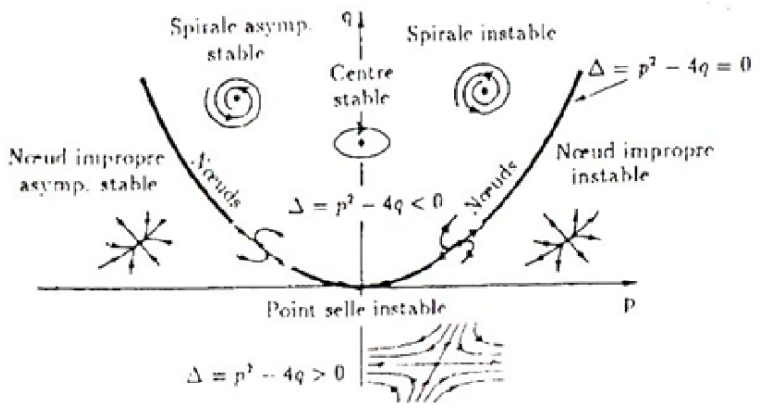


FIGURE 2.2 – Le diagramme de stabilité

2.4 Théorème de Poincaré-Bendixson

Dans un espace des phases à deux dimensions, il est souvent possible de démontrer que les orbites d'un système non linéaire spiralent vers une courbe fermée ou

cycle limite même si l'on ne sait pas résoudre ce système, ceci grâce au théorème suivant :

Théorème Supposons q'une orbite $x(x_0, t)$ du système de deux équations :

$$\frac{dx}{dt} = f(x), \quad x = (x_1, x_2)^t, \quad f = (f_1, f_2)^t \tag{2.17}$$

reste dans un domaine compact $D \subset \mathbb{R}^2$, alors :

1. $x(x_0, t)$ est une solution périodique de (2.17)
2. ou bien $x(x_0, t)$ tend vers une solution périodique de (2.17)
3. ou bien $x(x_0, t)$ tend vers un point fixe de (2.17)

Exemple 6. *Considerons l'équation différentielle du second ordre :*

$$\ddot{x} + (x^2 + 2\dot{x} - 1)\dot{x} + x = 0 \tag{2.18}$$

ou sous forme de système

$$\begin{cases} \frac{dx}{dt} &= y \\ \frac{dy}{dt} &= -x + (1 - x^2 - 2y^2)y \end{cases} \tag{2.19}$$

on a alors : $\frac{d}{dt}(\frac{x^2+y^2}{2}) = y^2(1 - x^2 - 2y^2)$

Observons que $(1 - x^2 - 2y^2)$ *est positif pour* $x^2 + y^2 < \frac{1}{2}$*, et négatif pour* $x^2 + y^2 > \frac{1}{2}$.

Donc $x^2(t) + y^2(t)$ *est croissante pour* $x^2 + y^2 < \frac{1}{2}$ *et décroissante pour* $x^2 + y^2 > \frac{1}{2}$. *Ceci implique que toute orbite* $x(t)$ *et* $y(t)$ *de (2.19) avec le point initial* $t = t_0$ *est dans l'anneau* $\frac{1}{2} < x^2 + y^2 < 1$ *restera dans cet anneau pour* $t > t_0$*. Comme cet anneau ne contient pas des points fixes de (2.19), alors par le théorème de Poincaré-Bendixson, il existe une solution périodique de (2.19) contenue dans cet anneau.*

Remarque 1. *Si D est le domaine simplement connexe (c'est à dire il n'y pas des trous dans D), alors on a le théorème :*

Critère de Bendixon *Si dans un domaine simplement connexe $D \subset \mathbb{R}^2$, l'expression :*

$$divf = \sum_{i=1}^{2} \frac{\partial f_i}{\partial x_i}$$

n'est pas identiquement nulle et ne change pas de signe, alors le système (2.19) n'a pas d'orbite périodique contenue dans D.

Exemple 7. *Considerons l'oscilateur de Duffing non forcé :*

$$\ddot{x} - x + x^3 + (\delta - x^2)\dot{x} = 0 \quad (\delta > 0) \tag{2.20}$$

ou sous forme de système :

$$\begin{cases} \frac{dx}{dt} &= y \\ \frac{dy}{dt} &= x - x^3 - \delta y + x^2 y \end{cases} \tag{2.21}$$

le système (2.21) admet trois points fixes.
D'autre part :

$$Divf = x^2 - \delta \tag{2.22}$$

le second membre de (2.22) s'annule sur les droites $x = \pm\sqrt{\delta}$. Ces deux droites divisent le plan en trois région $\mathbf{R}_1, \mathbf{R}_2, \mathbf{R}_3$ (figure 2.3). D'aprés le Critère de Bendixson, le système (2.21) ne peut avoir une orbite périodique contenue entièrement dans une des trois région $\mathbf{R}_1, \mathbf{R}_2, \mathbf{R}_3$, cependant le Critère de Bendixson n'empéche pas l'existence d'orbite périodique qui sont à cheval sur deux ou trois régions (figure 2.3).

2.5 La fonction de Lyapunov

Soit $\bar{x}$ un poit fixe de (2.8) et soit $V : W \longrightarrow \mathbb{R}$ une fonction différentiable définie sur un voisinage de $\bar{x}$ tel que : $V(\bar{x}) = 0$ et $V(x) > 0$, si $x \neq \bar{x}$ posons que :

$$\dot{V} = \sum_{j=1}^{n} \frac{\partial V}{\partial x_j}\dot{x}_j = \sum_{j=1}^{n} \frac{\partial V}{\partial x_j} f_j(x)$$

Alors on a le théorème suivant :

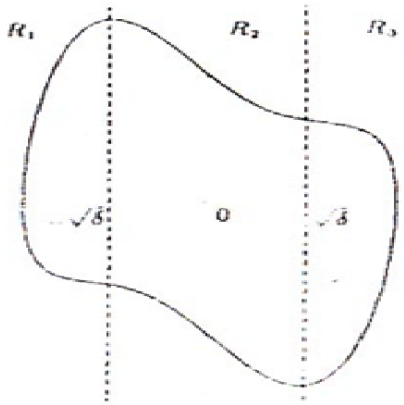


FIGURE 2.3 – Les régions R_1, R_2, R_3

Théorème de Lyapunov

1. Si $\dot{V}(x) \leqslant 0$ dans $W - \{\bar{x}\} \Longrightarrow \bar{x}$ est un point fixe stable.
2. Si $\dot{V}(x) < 0$ dans $W - \{\bar{x}\} \Longrightarrow \bar{x}$ est un point fixe asymptotiquement stable.
3. Si $\dot{V}(x) > 0$ dans $W - \{\bar{x}\} \Longrightarrow \bar{x}$ est un point fixe instable.

Il n'y a pas de régle générale pour trouver une fonction de Lyapunov, cependant dans des problèmes de mécanique, l'énergie est souvent un bon candidat.

Exemple 8. *Soit l'équation*

$$m\ddot{x} + k(x + x^3) = 0$$

en posant : $\dot{x} = y$ *alors :*

$$\begin{cases} \dot{x} &= y \\ \dot{y} &= \frac{-k}{m}(x + x^3) \end{cases} \tag{2.23}$$

étudions la stabilité du système (2.23) au point $(x, y) = (0, 0)$.
L'énergie totale du système est :

$$E(x, y) = \frac{my^2}{2} + k(\frac{x^2}{2} + \frac{x^4}{4})$$

$E(x,y)$ est aussi une fonction de Lyapunov pour (2.23) car :
$E(0,0) = 0$ *et* $E(x,y) > 0$ *pour* $E(0,0) \neq 0$, *et*

$$\dot{E}(x,y) = my\dot{y} + k(x+x^3)\dot{x} = -ky(x+x^3) + k(x+x^3)y = 0$$

le point fixe alors $(x,y) = (0,0)$ *est stable d'après le Théorème de Lyapunov.*

2.6 Attracteur et Attracteur étrange

2.6.1 Attracteur

Soit A un ensemble compact, et fermé de l'espace des phases, on suppose que A est un ensemble invariant (c'est-à-dire $\phi_t(A) = A$). On dit que A est stable si : Pour tout voisinage U de A, $\exists$ un voisinage V de A tel que tout solution $x(x_0,t) = \phi_t(x_0)$ restera dans U, si de plus :

$$\bigcap_{t \geqslant 0} \phi_t(V) = A$$

et s'il existe une orbite dense dans A, alors A est un attracteur.
Lorsque A est un attracteur, l'ensemble $W = \bigcup_{t<0} \phi_t(V)$ est appelé bassin d'attraction de A, c'est l'ensemble des points dont les trajectoires asymptotiques convergent vers A. L'attracteur le plus simple est un point fixe. Un deuxième type d'attracteur pour un champ de vecteur est le cycle limite ω, c'est une trajectoire fermée qui attire toute les orbites proches.

Exemple 9. *Soit le système*

$$\begin{cases} \frac{dx}{dt} &= -y + x(1-x^2-y^2) \\ \frac{dy}{dt} &= x + y(1-x^2-y^2) \end{cases} \tag{2.24}$$

En coordonnées polaires $x = r\cos\theta$ *et* $y = r\sin\theta$, *le système (2.24) devient :*

$$\begin{cases} \frac{dr}{dt} &= r(1-r^2) \\ \frac{d\theta}{dt} &= 1 \end{cases} \tag{2.25}$$

La solution générale de (2.25) est :

$$\begin{cases} r(t) &= \frac{r_0}{[r_0^2+(1-r_0^2)e^{-2r}]^{\frac{1}{2}}} \\ \theta &= t+\theta_0 \end{cases} \tag{2.26}$$

où : $r_0 = r(0)$ *et* $\theta_0 = \theta(0)$ *D'où :*

$$\begin{cases} x(t) &= \frac{r_0}{[r_0^2+(1-r_0^2)e^{-2r}]^{\frac{1}{2}}}\cos(t+\theta_0) \\ y(t) &= \frac{r_0}{[r_0^2+(1-r_0^2)e^{-2r}]^{\frac{1}{2}}}\sin(t+\theta_0) \end{cases} \tag{2.27}$$

On remarquera que :

1. $x = 0$, $y = 0$ *est le seul point fixe de (2.24)*
2. *La solution correspondant à* $r_0 = 1$ *:*

   $$x(t) = \cos(t+\theta_0), \quad y(t) = \sin(t+\theta_0)$$

   est périodique de période 2π *; son orbite est le cercle unite* $x^2 + y^2 = 1$.
3. *D'aprés (2.26), toutes les orbites de (2.24) à l'exception de l'origine, spiralent vers le cercle unité qui est le cycle limite et le bassin d'attraction du cycle limite est* $\mathbb{R}^2 - (0,0)$. *La situation est décrit sur la figure (2.4).*

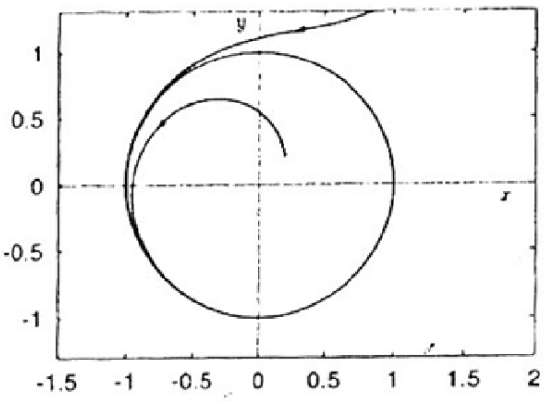


FIGURE 2.4 – Le cycle limite de l'exemple 9

2.6.2 L'attracteur étrange

Un autre type d'attracteur intéressant est l'attracteur étrange. Cet attracteur a été introduit par Ruelle et Takens. Les caractéristique d'un attracteur étrange sont :

1. Dans l'espace des phases, l'attracteur est de volume nul.
2. La dimension d de l'attracteur est fractale (non entière) avec $2 < d < n$, où n est la dimension de l'espace des phases.
3. Sensibilités aux conditions initiales : deux trajectoires de l'attracteur initialement voisines finissent toujours par s'écater l'une de l'autre.

Théorème 1. *Soient ϕ_t le flot (2.8), V un volume de l'espace des phases au temps $t = 0$, $V(t) = \phi_t(V)$ l'image de V par ϕ_t. On a :*

$$\frac{dV(t)}{dt}|_{t=0} = \int_V Divf dx_1 \dots dx_n, \quad Divf \equiv \sum_{i=1}^{n} \frac{\partial f_t}{\partial x_t} \tag{2.28}$$

Exemple 10. *Nous présentons dans cet exemple le prototype de l'attracteur étrange : attracteur de Lorenz. Considerons le système suivant :*

$$\begin{cases} \frac{dx}{dt} &= -\sigma x + \sigma y \\ \frac{dy}{dt} &= -xz + rx - y \\ \frac{dz}{dt} &= xy - bz \end{cases} \tag{2.29}$$

avec $\sigma = 10$ et $b = \frac{8}{3}$. Ce système est un modéle simplifié du phénomène de conservation naturelle entre deux plaques planes horizontales, infinies. La plaque supérieure étant à la température T et la plaque inferieure à la température $T + \Delta T$. Le paramètre r est lié à ΔT et donc au nombre de Rayleigh ; x est proportionnel à la vitesse du fluide, y caractérise la différence de température entre le fluide montant et le fluide descendant, z est proportionnel à la déviation du profil vertical au température par rapport à sa valeur d'équilibre. Ce modèle n'est valable que dans le voisinage immédiat de la transition conduction/convection car les coefficients de Fourier retenus par Lorenz décrivent de simples rouleaux.

L'origine est un point fixe. La matrice jacobienne à l'origine est :

$$\begin{pmatrix} -\sigma & \sigma & 0 \\ r & -1 & 0 \\ 0 & 0 & -b \end{pmatrix} \tag{2.30}$$

Son équation caractéristique,

$$(\lambda + b)[(\lambda^2 + (\sigma + 1)\lambda + \sigma(1 - r))] = 0 \tag{2.31}$$

Pour racines,

$$\lambda_{1,2} = \frac{-(1+\sigma) \pm \sqrt{(1+\sigma)^2 - 4\sigma(1-r)}}{2}, \quad \lambda_3 = -b \tag{2.32}$$

Tant que $0 < r < 1$ toutes les valeurs propres sont négatives : le point fixe est stable. Quand $r = 1$, les valeurs propres sont :

$$\lambda_1 = 0, \quad \lambda_2 = -(\sigma + 1), \quad \lambda_3 = -b \tag{2.33}$$

Pour $r > 1$, on a $\lambda_1 > 0, \lambda_2 < 0, \lambda_3 < 0$, l'origine est devenue instable. Mais l'orsque $r < 1$, deux nouveaux points fixes apparaissent que nous désignons par C et $\grave{C}$, et dont les coordonnées sont :

$$\dot{x} = \dot{y} = \pm\sqrt{b(r-1)}, \quad \dot{z} = r - 1 \tag{2.34}$$

La matrice jacobienne correspondant à ces points fixes s'écrit :

$$\begin{pmatrix} -\sigma & \sigma & 0 \\ 1 & -1 & -\dot{x} \\ \dot{y} & \dot{x} & -b \end{pmatrix} \tag{2.35}$$

Ses valeurs propres sont les racines du polynome caractéristique :

$$P(\lambda) = \lambda^3 + (\sigma + b + 1)\lambda^2 + b(\sigma + r)\lambda + 2b\sigma(r - 1) = 0 \tag{2.36}$$

Les relations entre les racines et les coefficients de $P(\lambda)$ s'écrivent :

$$\begin{cases} \lambda_1 + \lambda_2 + \lambda_3 & = & -(\sigma + b + 1) \\ \lambda_1\lambda_2 + \lambda_2\lambda_3 + \lambda_3\lambda_1 & = & b(\sigma + r) \\ \lambda_1\lambda_2\lambda_3 & = & -2\sigma b(r - 1) \end{cases} \tag{2.37}$$

Pour $r > 1$, les coefficients de (2.36) sont tous positifs. On en deduit qu'une racine de (2.36) est réelle négative ; notons λ_3 cette racine. Les deux autre racines sont réelles si :

$$q^2 + \frac{4p^3}{27} \leqslant 0$$

où p et q sont les coefficients de l'équation réduite :

$$u^3 + pu + q = 0$$

avec :

$$\begin{cases} u &= \lambda + \frac{1}{3}(\sigma + b + 1) \\ p &= b(r + \sigma) - \frac{1}{3}(\sigma + b + 1)^2 \\ q &= \frac{2}{27}(\sigma + b + 1)^3 - \frac{1}{3}b(r + \sigma)(\sigma + b + 1) + 2\sigma b(r - 1) \end{cases}$$

Pour les valeurs des paramètres $\sigma = 10$ et $b = \frac{8}{3}$, la relation $q^2 + \frac{4}{27}p = 0$ est obtenue pour $r = r_1 = 1,34561...$ les trois racines de (2.36) sont donc réelles si $r < r_1$ et elle sont toutes négatives.

Si r est légérement plus grand que r_1, il y a une racine réelle négative λ_3 et deux racines complexe conjuguées. Écrivons le polynome caractéristique (2.36) sous la forme :

$$P(\lambda) = (\lambda - \lambda_3)(\lambda - \lambda_r - i\lambda_t)(\lambda - \lambda_r + i\lambda_t) \ \ avec : \lambda_{1,2} = \lambda_r = \pm\lambda_t$$

(2.37) s'écrit alors :

$$\begin{cases} \lambda_3 + 2\lambda_r &= -(\sigma + b + 1) \\ \lambda_r^2 + \lambda_t^2 + 2\lambda_3\lambda_r &= b(\sigma + r) \\ \lambda_3(\lambda_r^2\lambda_t^2) &= -2\sigma b(r - 1) \end{cases} \tag{2.38}$$

Pour $r > r_1$ et proche de r_1, λ_t rest négatif et les points fixes C, C' sont restés stables. Si r continue à croitre, on obtient $\lambda_r = 0$ lorsque :

$$r = r_c = \frac{\sigma(\sigma + b + 3)}{\sigma - b - 1} \tag{2.39}$$

(c'est-à-dire $r_c \approx 24,7368...$ pour $\sigma = 10$, et $b = \frac{8}{3}$). Les valeurs propres sont alors :

$$\lambda_{1,2} = \pm iu_0, \quad \lambda_3 = -(\sigma + b + 1) \tag{2.40}$$

avec :

$$u_0^2 = b(r_c + \sigma) = \frac{2\sigma b(\sigma + 1)}{\sigma - b - 1}$$

Si r croit encore, pour $r > r_c$ les points fixes C, C' deviennent instables à leur tour car λ_r est devenue positive et on obtient un attracteur chaotique (trouver par Lorenz à $r = 28$).

La divergence du champ de vecteurs f est partout négative :

$$Div f = -\sigma - 1 - b = -\frac{41}{3}$$

Donc les éléments de volume se contractent. Au bout d'une unité de temps cette contraction réduit un volume donné V_0 d'un facteur :

$$\exp(-\sigma + b + 1) = \exp(-\frac{41}{3})$$

C'est donc d'un système très dissipatif. La figure (2.5) montre une vue de l'attracteur de Lorenz pour $r = 28$

2.7 Système Hamiltonien

2.7.1 Définition

Un système hamiltonien à n degrés de liberté est un système d'équations du mouvement de la forme :

$$\frac{dq_i}{dt} = \frac{\partial H}{\partial p_i}, \quad \frac{dp_i}{dt} = -\frac{\partial H}{\partial q_i}, \quad i = 1, 2, ..., n \tag{2.41}$$

où : $H = H(q, p, t)$ est le hamiltonien. L'espace des phases du système (2.41) est $\mathbb{R}^{2n}$. On déduit de (2.41) :

$$\begin{aligned} \frac{dH}{dt} &= \frac{\partial H}{\partial t} + \Sigma_{i=1}^n \frac{\partial H}{\partial p_i}\frac{dp_i}{dt} + \Sigma_{i=1}^n \frac{\partial H}{\partial q_i}\frac{dq_i}{dt} \\ &= -\Sigma_{i=1}^n \frac{\partial H}{\partial p_i}\frac{H}{\partial q_i} + \Sigma_{i=1}^n \frac{\partial H}{\partial q_i}\frac{\partial H}{\partial p_i} + \frac{\partial H}{\partial t} \\ &= \frac{\partial H}{\partial t} \end{aligned} \tag{2.42}$$

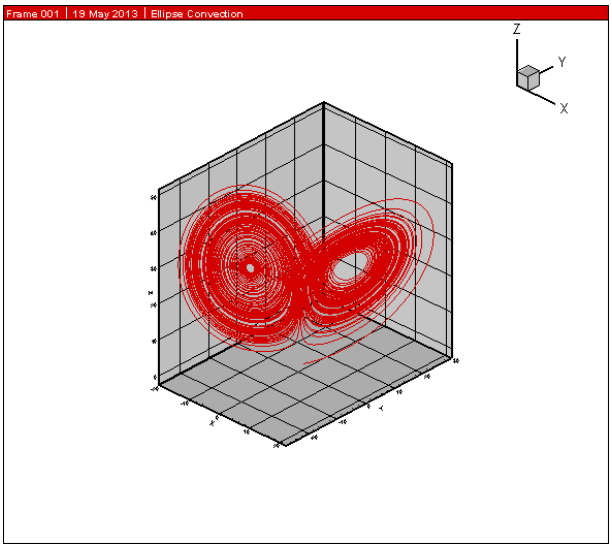


FIGURE 2.5 – Une vue de l'attracteur de Lorenz

En conséquence, si le hamiltonien H ne dépend pas explicitement du temps, il sera conservé au cours du temps $H(q,p) = E$ constante.

Exemple 11. *Considerons l'équation du mouvement de l'oscilateur harmonique :*

$$\ddot{q} + \omega_0^2 q = 0 \tag{2.43}$$

est équivalent à :

$$\begin{cases} \dot{q} &= \frac{\partial H}{\partial p} = p \\ \dot{p} &= -\frac{\partial H}{\partial q} = -\omega_0^2 q \end{cases} \tag{2.44}$$

avec :

$$H = \frac{1}{2}(p^2 + \omega_0^2 q^2) \tag{2.45}$$

L'oscillateur harmonique est donc un système hamiltonien à un degré de liberté.

2.7.2 Transformation canonique

Définition 4. *Un changement de variable :*

$$\begin{cases} q_i &= q_i(Q_j, P_j) \\ p_i &= p_i(Q_j, P_j), \quad i,j = 1,2,...,n \end{cases} \tag{2.46}$$

est dit canonique s'il préserve la forme hamiltonienne des équations d'évolution :

$$\begin{cases} \dot{Q}_i &= \frac{\partial H(Q,P)}{\partial P_i} \\ \dot{P}_i &= -\frac{\partial H(Q,P)}{\partial Q_i}, \quad i = 1,2,...,n \end{cases} \tag{2.47}$$

où $H(Q,P)$ est l'hamiltonien transformé.

Cherchons maintenant les conditions pour que (2.46) soit une transformation canonique.

Théorème 2. *Pour que (2.46) soit une transformation canonique, il faut et il suffit que :*

$$\begin{cases} \{Q_k, Q_l\} &= \{P_k, P_l\} = 0 \\ \{Q_k, P_l\} &= -\{P_k, Q_l\} = \delta_{kl} \end{cases} \tag{2.48}$$

où $\{\alpha, \beta\}$ est le crochet de Lagrange :

$$\{\alpha, \beta\} = \Sigma_{i=1}^{n} (\frac{\partial q_i}{\partial \alpha}\frac{\partial p_i}{\partial \beta} - \frac{\partial p_i}{\partial \alpha}\frac{\partial q_i}{\partial \beta})$$

Exemple 12. *Considerons l'oscilateur harmonique de l'exemple. Les équations hamiltonienne sont (2.46). La transformation suivante :*

$$\begin{cases} q(P,Q) &= \sqrt{\frac{2P}{\omega_0}} \sin Q \\ p(P,Q) &= \sqrt{2\omega_0 P} \cos Q \end{cases} \tag{2.49}$$

est canonique car :

$$dq \wedge dp = (\frac{1}{\sqrt{2\omega_0 P}} \sin Q dP + \sqrt{\frac{2P}{\omega_0}} \cos Q dQ) \wedge (\frac{\omega_0}{\sqrt{2P}} \cos Q dP - \sqrt{2\omega_0 P} \sin Q dQ) = dQ \wedge dP$$

les nouvelles équations du mouvement sont :

$$\begin{cases} \dot{Q} &= \omega_0 \\ \dot{P} &= 0 \end{cases} \tag{2.50}$$

et le nouveau hamiltonien est :

$$H = H(P) = \omega_0 P \tag{2.51}$$

Nous verrons plus loin que Q et P sont des variables d'action et angulaires de l'oscilateur harmonique.

2.7.3 Système integrable-Variables d'action et angulaires

Dans le cas où le hamiltonien ne dépend pas explicitement du temps, nous avons vu que l'énergie $E = H(p, q)$ est une constante. Plus généralement, une fonction $f(p, q)$ est une constante du mouvement si $f(p, q) = constante$ quand $p(t)$ et $q(t)$ évoluent selon (2.41). On a donc, si $H = H(p, q)$:

$$\dot{f} = \dot{p}\frac{\partial f}{\partial p} + \dot{q}\frac{\partial f}{\partial q} = \frac{\partial H}{\partial p}\frac{\partial f}{\partial q} - \frac{\partial H}{\partial q}\frac{\partial f}{\partial p} = 0$$

Cette dernière expression est appelée un crochet de Poisson de f et de H, et est notée $[f, H]$ où :

$$[f, f] \equiv \frac{\partial f_1}{\partial q}\frac{\partial f_2}{\partial p} - \frac{\partial f_1}{\partial p}\frac{\partial f_2}{\partial q}$$

Ainsi la condition pour que f soit une constante du mouvement (pour un hamiltonien indépendant du temps) est :

$$[f, H] = 0$$

En particulier, le hamiltonien H est une constante du mouvement car : $[H, H] = 0$

Définition 5. *Un hamiltonien $H(p, q)$, à n degrés de liberté, est dit integrable s'il existe n constantes du mouvement, linéairement indépendantes.*

$$f_1(q, p) = H(q, p) = h_1, \quad f_2(q, p) = h_2, \cdots, f_n(q, p) = h_n$$

avec

$$[f_1, f_2] = 0 \quad \forall i, j$$

Les constantes $h_i, i = 1, 2, ..., n$, sont appelées intégrales premières.

Exemple 13. *Considerons le hamiltonien du problème de Toda :*

$$H_T = \frac{1}{2}(p_x^2 + p_y^2) + \frac{1}{24}(e^{2x-2y\sqrt{3}} + e^{2x+2y\sqrt{3}} + e^{-4x}) - \frac{1}{8} \tag{2.52}$$

Les équations hamiltoniennes s'écrivent :

$$\begin{cases} \dot{x} &= \frac{\partial H_T}{\partial p_x} = p_x \\ \dot{y} &= \frac{\partial H_T}{\partial p_y} = p_y \\ \dot{p}_x &= \frac{\partial H_T}{\partial x} = \frac{1}{6}(e^{-4x} - e^{2x}\cosh(2y\sqrt{3})) \\ \dot{p}_y &= -\frac{\partial H_T}{\partial y} = -\frac{e^{2x}}{2\sqrt{3}}\sinh(2y\sqrt{3})) \end{cases}$$

H_T est une constante du mouvement. Une deuxième integrale du mouvement est trouvé par Hénon :

$$I = 8\dot{y}(\dot{y}^2 - 3\dot{x}^2) + (\dot{y} + \dot{x}\sqrt{3})e^{2x-2y\sqrt{3}} + (\dot{y} - \dot{x}\sqrt{3})e^{2x+2y\sqrt{3}} - 2\dot{y}e^{-4x}$$

Le hamiltonien (2.52) est donc integrable.

2.8 Variétés centrales

2.8.1 Théorème de la variété centrale

Soit $\bar{x}$ un point fixe de :

$$\frac{dx}{dt} = f(x), \quad x \in \mathbb{R}^n, \quad f \in C^r(D) \tag{2.53}$$

La linéarisation de (2.53) autour de $\bar{x}$ s'écrit :

$$\frac{d\xi}{dt} = J\xi \tag{2.54}$$

où : $\xi = x - \bar{x}$ et J est la matrice jacobienne.

$$J \equiv Df(\bar{x}) = \|\frac{\partial f_i}{\partial x_j}\|_{x=\bar{x}}$$

On substitue $\xi = ue^{\lambda t}, \quad u \in \mathbb{R}^n$, dans (2.54) et on obtient les équations aux vecteurs propres :

$$(J - \lambda I)u = 0 \tag{2.55}$$

$$|J - \lambda I| = 0 \tag{2.56}$$

soient $u_1, ...u_s$ les vecteurs propres de J correspondant aux valeurs propres λ dont la partie réelle est négative, $v_1, ..., v_u$ les vecteurs propres de J correspondant aux valeurs propres λ dont la partie réelle est positive, $w_1, ..., w_c$ les vecteurs propres de J correspondant aux valeurs propres λ dont la partie réelle nulle, avec $s+u+c = n$ et soient E^s le sous espace vectoriel engendré par $\{u_1, ...u_s\}$, E^u le sous espace vectoriel engendré par $\{v_1, ...v_u\}$, E^c le sous espace vectoriel engendré par $\{w_1, ...w_c\}$, avec $\mathbb{R}^n = E^s \oplus E^u \oplus E^c$. On a le Théorème suivant :

Théorème 3. *Il existe des variétés de classe C^r stable W^s et instable W^u et centrale W^c, tangentes respectivement à E^s, E^u et E^c en x. Ces variétés sont invariantes par rapport au flot ϕ_t de (2.53). W^s et W^u sont unique mais W^c ne l'est pas nécessairement. La situation au voisinage de x, est illustrée sur la figure (2.6).*

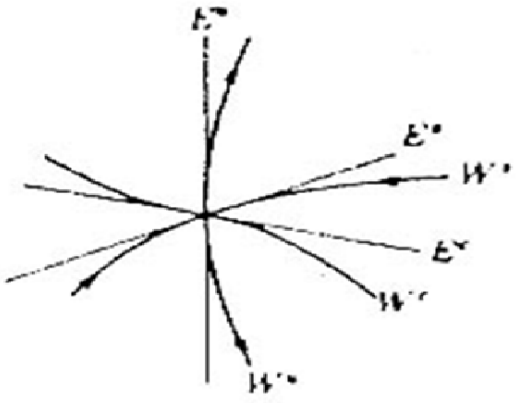


FIGURE 2.6 – Variété stable, instable, et centrale

On a $\phi_t(W^s) \subset W^s$, $\phi_t(W^u) \subset W^u$, $\phi_t(W^c) \subset W^c$ *et :*

$$\lim_{t \longrightarrow +\infty} \phi_t(x) = \dot{x}, \quad pour x \in W^s \tag{2.57}$$

$$\lim_{t \longrightarrow -\infty} \phi_t(x) = \dot{x}, \quad pour x \in W^u \tag{2.58}$$

Noter que x *est la limite* ω*(resp. la limite* α*) de toute trajectoire* $\phi_t(x)$ *appartenant à* W^s*(resp. appartenant à* W^u *).*

De plus, on ne peut attribuer de directions au flot de W^c *sans connaitre les premiers termes du dévelopement limité de* f *au voisinage de* $\bar{x}$*. Si* $E^c = \phi$*, le point* $\bar{x}$ *est un point fixe hyperbolique (ou non-dégénéré).*

Exemple 14. *Soit le système non-linéaire suivant :*

$$\begin{cases} \frac{dx}{dt} &= -x \\ \frac{dy}{dt} &= -y + x^2 \\ \frac{dz}{dt} &= z + x^2 \end{cases} \tag{2.59}$$

Le seul point fixe du système (2.59) est l'origine et la matrice :

$$J = Df(0) = \|\frac{\partial f_i(0)}{\partial x_j}\| = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

est déja diagonale ; par conséquent les sous espaces E^s *et* E^u *sont respectivement le plan* x*,* y *et l'axe* z*. Après avoir résolu la première équation* $\frac{dx}{dt} = -x$*, le système non-linéaire se réduit à deux équations différentielles linéaires qui peuvent etre résolues facilement et on obtient :*

$$\begin{cases} x(t) &= x_0 e^{-t} \\ y(t) &= y_0 e^{-t} + x_0^2(e^{-t} - e^{-2t}) \\ z(t) &= z_0 e^{-t} + \frac{x_0^2}{3}(e^{t} - e^{-2t}) \end{cases}$$

où : $(x_0, y_0, z_0) = (x(0), y(0), z(0))$*. Par conséquent,* $\lim_{t \longrightarrow +\infty} \phi_t(x_0, y_0, z_0) = (0, 0, 0)$ *si et seulement si* $z_0 + \frac{x_0^2}{3} = 0$ *; d'où :*

$$W^s = \{(x_0, y_0, z_0) \in \mathbb{R}^3, \;\; z_0 = -\frac{x_0^2}{3}\}$$

De même $\lim_{t\longrightarrow-\infty}\phi_t(x_0,y_0,z_0)=(0,0,0)$ *si et seulement si* $x_0=y_0=0$*, d'où :*

$$W^u=\{(x_0,y_0,z_0)\in\mathbb{R}^3,\ \ x_0=y_0=0\}$$

W^s *est tangente à* E^s *et* $W^u=E^u=$ *l'axe des z.*

2.8.2 Etude locale de la variété centrale

Supposons que, par changement de coordonnées, le point fixe $\overline{x}$ ait été ramené à l'origine et les équations du système dynamique mises sous la forme :

$$\begin{cases}\dot{x} &= Ax+f(x,y)\\ \dot{y} &= By+g(x,y)\end{cases} \tag{2.60}$$

où x et f sont des n-vecteurs et A est une matrice $n\times n$ dont les valeurs propres ont leur partie réelle nulle. De même, y et g sont des m-vecteurs et B une matrice $m\times m$ dont les valeurs propres ont leur partie réelle négative (pour simplifier, nous avons supposé que le système linéairisé n'a pas de valeurs propres avec partie réelle positive). Dans la pratique, lorsque la matrice jacobienne est diagonalisable, on peut ramener le système dynamique à la forme (2.60) en utilisant la base des vecteurs propres. Localement la variété centrale peut être représentée au voisinage de $\bar{x}=0$ par :

$$W^c(0)=\{(x,y)\in\mathbb{R}^n\times\mathbb{R}^m,\quad y=h(x),|x|<\delta,h(0)=0,Dh(0)=0\} \tag{2.61}$$

pour δ suffisament petit. Les conditions $h(0)=0$ et $Dh(0)=0$ impliquent que $W^c(0)$ est tangente à $E^c\equiv(y=0)$ au point $(x,y)=(0,0)$.
Portant $y=h(x)$ avec $h(0)=Dh(0)=0$, on obtient :

$$\dot{x}=Ax+f(x,h(x)),\quad x\in\mathbb{R}^n,\quad h:\mathbb{R}^n\to\mathbb{R}^m \tag{2.62}$$

Le théorème suivant permet de lier la dynamique de (2.60) à celle de (2.62).

Théorème 4. *Si l'origine* $x=0$ *de* (2.62) *est localement asymptotiquement stable (resp instable), alors l'origine de* (2.60) *est aussi localement asymptotiquement stable (resp instable).*

Exemple 15. *Soit le système :*

$$\begin{cases} \dot{x} &= x^2y - x^5 \\ \dot{y} &= -y + x^2 \end{cases} \tag{2.63}$$

L'origine est, bien entendu, le point fixe et la matrice jacobienne à l'origine est :

$$J = \begin{pmatrix} 0 & 0 \\ 0 & -1 \end{pmatrix} \tag{2.64}$$

Les valeurs propres de (2.64) *sont* 0 *et* -1*, il existe donc une variété centrale pour* (2.63) *représentée par* (2.61) *:*

$$W^c(0) = \{(x,y) \in \mathbb{R}^2, \quad y = h(x), |x| < \delta, h(0) = 0, h'(0) = 0\} \tag{2.65}$$

Portant $y = h(x)$ *et* $\dot{y} = h'(x)$ *on obtient :*

$$(xh - x)h' = -h + x^2 \tag{2.66}$$

écrivons $h(x)$ *sous la forme d'un développement limité*

$$h(x) = ax^2 + bx^3 + O(x^4) \tag{2.67}$$

où l'on a tenu compte des conditions $h(0) = h'(0) = 0$*. portons (2.67) dans (2.66) et égalisons les coefficients des puissances de* x*, nous obtenons* $a = 1$ *et* $b = 0$ *; d'où*

$$y = h(x) = x^3 + O(x^4) \tag{2.68}$$

d'où $\dot{x} > 0$ *La variété centrale est donc une parabole, au voisinage de l'origine. Portant (2.68) dans (2.63), on obtient :*

$$\dot{x} = x^4 + O(x^5) \tag{2.69}$$

d'où $\dot{x} > 0$*, et* $x = 0$ *est donc un point instable de (2.69). D'où par le théorème* $(x,y) = (0,0)$ *est un point d'équilibre instable de (2.63). La géométrie du flot prés de* $(x,y) = (0,0)$ *est illustré par la figure (2.7).*

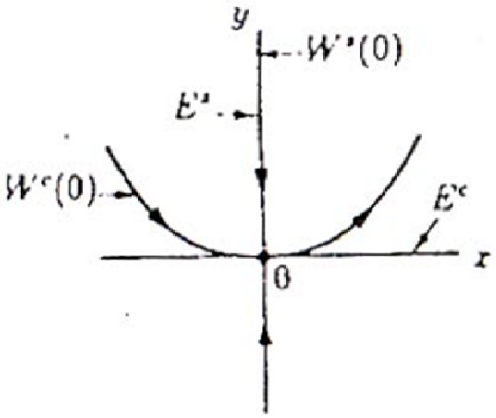


FIGURE 2.7 – Un point fixe instable et sa variété centrale.

2.8.3 Variété centrale dépendant d'un paramètre

Dans ce cas où (2.53) dépend d'un paramètre vectoriel $\theta \in \mathbb{R}^p$, on considère θ comme une nouvelle variable (vectorielle) dépendante et on remplace (2.60) par le système suivant :

$$\begin{cases} \dot{x} &= Ax + f(x, y, \theta) \\ \dot{y} &= By + g(x, y, \theta) \\ \dot{\theta} &= 0 \end{cases} \tag{2.70}$$

avec $(x, y, \theta) \in \mathbb{R}^n \times \mathbb{R}^m \times \mathbb{R}^p$. L'équation de la variété centrale s'écrit alors :

$$y = h(x, \theta)$$

(la dimension de la variété centrale est $n + p$). Le système d'équation aux dérivées partielles satisfait par $h(x, \theta)$ est encore :

$$Dh(x, \theta)[Ax + f(x, h(x, \theta), \theta) - Bh(x, \theta) - g(x, h(x, \theta), \theta) = 0 \tag{2.71}$$

Cependant, le développement de Taylor de $h(x,\theta)$ au voisinage de $(x,\theta)=(0,0)$ est maintenant :

$$h(x,\theta)=\sum_{k,l=1}^{p} b_{1kl}\theta_k\theta_l+\sum_{i=1}^{n}\sum_{i=1}^{p} b_{2ik}x_i\theta_k+\sum_{i,j=1}^{n} a_{2ij}x_ix_j+\sum_{i,j,k=1}^{n} a_{3ijk}x_ix_jx_k+\cdots \tag{2.72}$$

Exemple 16. *Considerons l'équation de Duffing quadratique :*

$$\begin{cases} \dot{u} &= v \\ \dot{v} &= \beta u-u^2-\delta u, \delta>0 \end{cases} \tag{2.73}$$

où β est le paramètre de bifurcation. La matrice jacobienne au point fixe $(u,v)=(0,0)$ et à $\beta=0$ est

$$D(0,0)=\begin{pmatrix} 0 & 1 \\ 0 & -\delta \end{pmatrix} \tag{2.74}$$

Ses valeurs propres et ses vecteurs propres sont $0,-\delta$ et $(1,0)^T,(1,-\delta)^T$ respectivement. Nous passons ensuite à la base des vecteurs propres en utilisant les transformations :

$$\begin{aligned} \begin{pmatrix} u \\ v \end{pmatrix} &= \begin{pmatrix} 1 & 1 \\ 0 & -\delta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \\ \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} 1 & \frac{1}{\delta} \\ 0 & \frac{-1}{\delta} \end{pmatrix}\begin{pmatrix} u \\ v \end{pmatrix} \end{aligned}$$

(2.73) s'écrit alors :

$$\begin{aligned} \begin{pmatrix} x \\ y \end{pmatrix} &= [\begin{pmatrix} 0 & 0 \\ 0 & -\delta \end{pmatrix}+\tfrac{\beta}{\delta}\begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix}]\begin{pmatrix} x \\ y \end{pmatrix}+\tfrac{1}{\delta}\begin{pmatrix} -(x+y)^2 \\ (x+y)^2 \end{pmatrix} \\ \dot{\beta} &= 0 \end{aligned}$$

ou :

$$\begin{cases} \dot{x} &= \frac{\beta}{\delta}(x+y)-\frac{1}{\delta}(x+y)^2 \\ \dot{y} &= -\delta y-\frac{\beta}{\delta}(x+y)+\frac{1}{\delta}(x+y)^2 \\ \dot{\beta} &= 0 \end{cases} \tag{2.75}$$

Nous cherchons une variété centrale de la forme :

$$y = h(x, \beta) = ax^2 + bx\beta + c\beta^2 + O(3) \tag{2.76}$$

où $O(3)$ *désigne les termes d'ordre* $x^3,\ x^2\beta,\ x\beta^2$ *et* β^3*. L'équation (2.71) s'écrit :*

$$\frac{\partial h}{\partial x}(\frac{\beta}{\delta}(x+h) - \frac{1}{\delta}(x+h)^2) + \delta h + \frac{\beta}{\delta}(x+h) - \frac{1}{\delta}(x+h)^2 = 0$$

Portant (2.76) dans cette dernière équation, nous obtenons :

$$(2ax+b\beta+\cdots)(\frac{\beta}{\delta}(x+\cdots)-\cdots)+\delta(ax^2+bx\beta+c\beta^2)+\frac{\beta}{\delta}(x+ax^2+bx\beta+c\beta^2)-(\frac{1}{\delta}(x+\cdots))^2 = 0$$

Egalisant les coefficients de $x^2,\ x\beta$ *et* β^2 *à zéro, on obtient :*

$$a = \frac{1}{\delta},\ \ b = -\frac{1}{\delta^2},\ \ c = 0$$

on en deduit :

$$y = \frac{1}{\delta^2}(x^2 - \beta x) + O(3) \tag{2.77}$$

portant (2.77) dans (2.75), on obtient :

$$\begin{cases} \dot{x} &= \frac{1}{\delta}(\beta x - x^2) + O(3) = q(x) \\ \dot{\beta} &= 0 \end{cases} \tag{2.78}$$

Les points fixes de (2.78) sont $x = 0$ *et* $x = \beta$*, avec :*

- *Pour* $\beta < 0$ *:* $q_x(0) < 0$ *,* $q_x(\beta) > 0$*.*
- *Pour* $\beta > 0$ *:* $q_x(0) > 0$ *,* $q_x(\beta) < 0$*.*

Il y a donc échange de stabilité. La figure (2.8) donne le diagramme de bifurcation au voisinage de l'origine.

2.9 Formes normales

Pour compléter la théorie de la variété centrale nous exposons dans cette partie la théorie de la forme normale permettant, par des transformations de coordonées sur la variété centrale, de deduire le système (2.10) à une forme plus simple, ne contenant

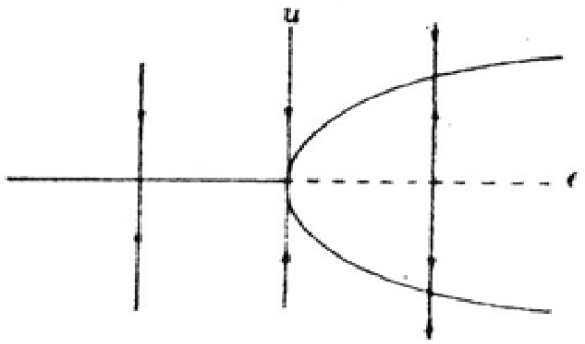


FIGURE 2.8 – Système de Lorenz : Bifurcation fourche à $r = 1$

que des termes résonants, appelée forme normale. Pour simplifier la notation, nous ne mentionnons par explicitement les paramètres qui se trouvent au second membre de (2.10)

2.9.1 Théorème de la forme normale

Eccrivons (2.10) sous la forme

$$\dot{x} = Ax + F(x), avec \;\; F(x) = f(x, h(x)), \;\; x \in \mathbb{R}^n \tag{2.79}$$

Soit H_k l'espace vectoriel engendré par les vecteurs

$$x^k \theta_i \equiv (x_1^{k_1} x_2^{k_2} \cdots x_n^{k_n})\theta_i, \quad 1 \leqslant i \leqslant n, \quad k_1 + k_2 + \cdots + k_n = k \tag{2.80}$$

Où $\{\theta_1, \theta_2, \cdots, \theta\_n\}$ est la base du système de coordonées $(x_1, x_2, \cdots, x_n)$. Ecrivons maintenant (2.79) sous la forme d'un développement de Taylor à n variables autour de l'origine :

$$\dot{x} = Ax + F^{(2)}(x) + F^{(3)}(x) + \cdots + F^{(k)}(x) + O(\mid x \mid^{k+1}) \tag{2.81}$$

Explicitement $F^{(k)}(x)$ est de la forme :

$$F^{(k)}(x) = (F_1^{(k)}, F_2^{(k)} \cdots, F_n^{(k)})^T \tag{2.82}$$

où $F_1^{(k)}, F_2^{(k)} \cdots, F_n^{(k)}$ sont des polynomes homogènes de degré k en x. Posons $L = Ax$, alors L induit un endomorphisme, $adL : H_k \to H_k$ défini par :

$$adL(Y) = [Y, L] = (DL)Y - (DY)L, \quad \forall Y(x) \in H_k \tag{2.83}$$

où, par définition $DL = A.[A, B] = AB - BA$ est le crochet de Lie. Dans le système de coordonnées $(x_1, x_2, \cdots x_n)$, (2.83) s'écrira :

$$[Y, L] = \sum_{j=1}^{n} (\frac{\partial L_i}{\partial x_j} Y_j - \frac{\partial Y_i}{\partial x_j} L_j) \tag{2.84}$$

avec $L_i = \sum_{j=1}^{n} A_{ij} x_j$. Soit G_k le sous espace vectoriel supplémentaire de $adL(H_k)$ dans H_k(c'est à dire : $H_k = adL(H_k) \oplus G_k$), alors on a le théorème suivant :

Théorème 5. *Il existe une suite de changement de coordonnées de la forme :*

$$x = y + P(y), \quad P(y) \in H_r, \quad r = 2, 3, \cdots, k \tag{2.85}$$

qui transforme le système (1.81) en la forme normale :

$$\dot{y} = Ay + g^2(y) + g^3(y) + \cdots + g^k(y) + O(|y|^{k+1}) \tag{2.86}$$

où $g^{(i)} \in G_i, \quad 2 \leqslant i \leqslant k$

Ce théorème s'appelle aussi théorème de Poincaré Dulac. Explicitement $P(y)$ est de la forme :

$$P(y) = (P_1, P_2, \cdots, P_n)^T \tag{2.87}$$

où $P_1, P_2, \cdots, P_n$ sont des polynomes homogènes de degré r en y

Exemple 17. *Considerons le système différentiel*

$$\begin{pmatrix} \dot{x} \\ \dot{y} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} F_1^{(2)}(x, y) \\ F_1^{(2)}(x, y) \end{pmatrix} + O(3) \tag{2.88}$$

avec :

$$\begin{aligned} F_1^2(x, y) &= c_{120}x^2 + c_{111}xy + c_{102}y^2 \\ F_2^2(x, y) &= c_{220}x^2 + c_{211}xy + c_{202}y^2 \end{aligned}$$

dans la base canonique $e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ *et* $e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ *La matrice*

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \tag{2.89}$$

a pour valeurs propres $\lambda_1 = \lambda_2 = 0$. *On deduit une base de* H_2 *:*

$$\{\begin{pmatrix} x^2 \\ 0 \end{pmatrix}, \begin{pmatrix} xy \\ 0 \end{pmatrix}, \begin{pmatrix} y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ x^2 \end{pmatrix}, \begin{pmatrix} 0 \\ xy \end{pmatrix}, \begin{pmatrix} 0 \\ y^2 \end{pmatrix}\}$$

Pour calculer $adL(H_2)$, *on calcule l'action de* adL *sur chaque valeur de base* H_2. *D'où, d'après (2.83), avec :*

$$L = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ 0 \end{pmatrix}$$

on a

$$\begin{aligned}
adL \begin{pmatrix} x^2 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x^2 \\ 0 \end{pmatrix} - \begin{pmatrix} 2x & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y \\ 0 \end{pmatrix} = -2 \begin{pmatrix} xy \\ 0 \end{pmatrix} \\
adL \begin{pmatrix} xy \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} xy \\ 0 \end{pmatrix} - \begin{pmatrix} y & x \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y \\ 0 \end{pmatrix} = - \begin{pmatrix} y^2 \\ 0 \end{pmatrix} \\
adL \begin{pmatrix} y^2 \\ 0 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y^2 \\ 0 \end{pmatrix} - \begin{pmatrix} 2y & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} y \\ 0 \end{pmatrix} = -2 \begin{pmatrix} 0 \\ 0 \end{pmatrix} \\
adL \begin{pmatrix} 0 \\ x^2 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ x^2 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 2x & 0 \end{pmatrix} \begin{pmatrix} y \\ 0 \end{pmatrix} = \begin{pmatrix} x^2 \\ -2xy \end{pmatrix} \\
adL \begin{pmatrix} 0 \\ xy \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ xy \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ y & x \end{pmatrix} \begin{pmatrix} y \\ 0 \end{pmatrix} = \begin{pmatrix} xy \\ -y^2 \end{pmatrix} \\
adL \begin{pmatrix} 0 \\ y^2 \end{pmatrix} &= \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ y^2 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & 2y \end{pmatrix} \begin{pmatrix} y \\ 0 \end{pmatrix} = \begin{pmatrix} y^2 \\ 0 \end{pmatrix}
\end{aligned}$$

On deduit une base de $adL(H_2)$ *:*

$$\{\begin{pmatrix} xy \\ 0 \end{pmatrix}, \begin{pmatrix} y^2 \\ 0 \end{pmatrix}, \begin{pmatrix} x^2 \\ -2xy \end{pmatrix}, \begin{pmatrix} xy \\ -y^2 \end{pmatrix}, \}$$

d'où dim ad $L(H_2) = 4$. *Comme dim* $H_2 = 6$ *et* $H_2 = ad\ L(H_2) \oplus G_2$, *on deduit que* $dimG_2 = 2$. *Cependant le choix d'une base de* G_2 *n'est pas unique.*

2.9.2 Orbites homocline et hétérocline

Soit $\bar{x}$ un point fixe, $W^s(\bar{x}) \cap W^u(\bar{x})$ est l'ensemble des trajectoires qui tendent vers $\bar{x}$ à la fois pour $t \longrightarrow +\infty$ et pour $t \longrightarrow -\infty$. Une trajectoire qui appartient à $W^s(\bar{x}) \cap W^u(\bar{x})$ est appelée orbite homocline (figure 2.9 à gauche). Soient $\bar{x}_1$, $\bar{x}_2$ deux points fixes instables. Une trajectoire qui appartient à $W^s(\bar{x}_1) \cap W^u(\bar{x}_2)$ ou $W^u(\bar{x}_2) \cap W^s(\bar{x}_1)$ est appelée orbite hétérocline (figure 2.9 à droite).

FIGURE 2.9 – Orbite homocline à gauche Orbite hétérocline à droite

a/ Orbite homoclines et hétérocline dans un espace des phases à deux dimensions

On déduit du théorème de Poincaré-Bendixson que, dans un espace des phases à deux dimensions, les seuls attracteurs possibles sont :

1. les points fixes
2. les cycles limites

3. les orbites hétéroclines (trajectoire reliant deux points selles) ou homoclines (trajectoire reliant un point selle à lui même)

Exemple 18. *Dans l'exemple du pendule libre, les points selles ($x = \pm n\pi, \quad y = 0$, n impair) correspondent à $E(x, y) = 2$. L'orbite correspondante est une orbite hétérocline (ou homocline si l'on suppose que tous les points $x = n\pi$ sont confondus).*

b/ Orbite homocline dans un espace des phase à trois dimensions

Exemple 19. *Considérons le système de Lorenz :*

$$\begin{cases} \frac{dx}{dt} &= -\sigma x + \sigma y \\ \frac{dy}{dt} &= -xz + rx - y \\ \frac{dz}{dt} &= xy - bz, \quad \sigma = 10, \quad b = \frac{8}{3} \end{cases} \tag{2.90}$$

Nous avons vu que pour $r > 1$ et $r < \frac{\sigma(\sigma+b+3)}{\sigma-b-1}$ l'origine est un point fixe instable car les valeurs propres de la matrice jacobienne à l'origine possède deux valeurs propres négatives et une valeur propre positive. Par contre, les points fixes C et C' sont stables. La variété stable à l'origine $W^s(O)$ est une surface séparatrice séparant les bassins d'attraction des points fixe C et C'. La variété instable à l'origine $W^u(O)$, qui est une courbe présente l'aspect de la figure (2.9). Pour $r < r' \approx 13.926\ldots$, sa branche de droite tens vers C, sa branche de gauche tend vers C'. Pour $r > r'$, c'est le contraire qui se produit (figure a et b). Pour $r = r'$, les deux branches retournent à l'origine. La variété instable $W^u(O)$ est alors une courbe homocline contenue dans $W^s(O)$(figure 9). Cette courbe homocline a été découverte en 1979 *par Kaplan et Yorke. Quant à la variété stable à l'origine $W^s(O)$, on ne connait pas sa forme globale, on sait seulement qu'elle contient l'axe OZ et qu'au voisinage de l'origine elle a la forme d'une double héliee du coté z positif et aplatie du coté z négatif (figure 2.10).*

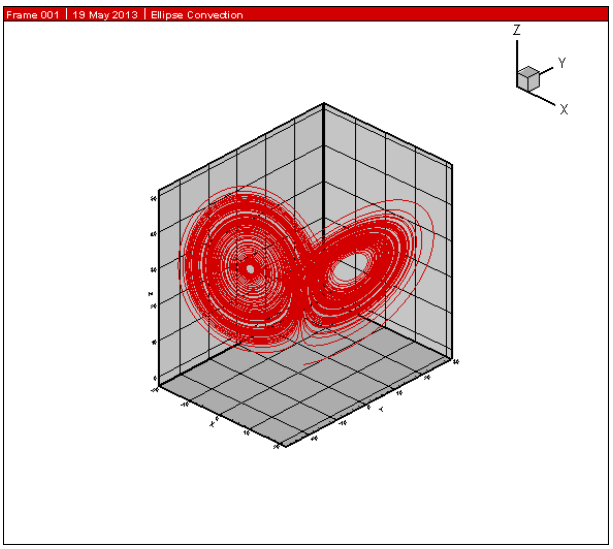


FIGURE 2.10 – L'attracteur de Lorenz

Chapitre 3

La synchronisation des systèmes dynamiques chaotiques

3.1 Introduction

L'usage du chaos pour la sécurisation de la télécommunication pose directement le problème de synchronisation du récepteur afin de suivre le signal chaotique employé à l'émetteur. Alors c'est quoi la synchronisation ? Le mot "synchronisation" vient du grec (syn) qui veut dire "ensemble " et (chronos) qui veut dire "temps. " De plus le dictionnaire la définit en tant qu'action de faire se produire ou s'accomplir simultanément (plusieurs faits, plusieurs actions appartenant à des séries différentes). Dans les relations humaines se synchroniser est l'une des premières choses que nous avons appris, car un bébé qui répond au sourire de sa mère, ne fait rien d'autre que de se synchroniser sur les expressions du visage de sa mère. L'histoire de la synchronisation revient au 17^{eme} siècle quand le célèbre scientifique hollandais Christian Huygens a rapporté son observation, que deux horloges à pendule supportées par une même planche en bois, finissaient par avoir les mêmes oscillations périodiques (même phase et même fréquence). En outre, il a remarqué que si l'oscillation d'une des pendules était perturbée par une force externe, elle reviendrait à son état initial.

C'était la première découverte de la synchronisation. La conclusion de Huygens sur la cause de cette synchronisation est le mouvement de la planche en bois ,malgré qu'il soit à peine perceptible. Ce mouvement représente donc un faible accouplement des deux horloges. Par conséquent, dans le contexte classique la synchronisation n'est réservée qu'aux mouvements périodiques. Par ailleurs le concept moderne couvre également les systèmes chaotiques. En résumé la synchronisation est le changement du rythme des oscillateurs (périodique ou non) dûs aux interactions faibles. Selon Pikovsky, il y a trois conditions qui doivent être rassemblées pour qu'un phénomène soit considéré synchrone :

1. Les systèmes oscillent indépendamment.

2. Le changement du comportement est dû à un accouplement faible.

3. Le changement du comportement se produit dans une certaine gamme de disparité. Si un oscillateur change lentement, le second devrait suivre cette variation.

L'aspect pseudo aléatoire du chaos nous amène à penser qu'il est impossible de le synchroniser. Cette hypothèse a été proposée par Fujisaka et al en 1983. Ce n'est qu'en 1990 que les deux chercheurs Pecora et Carroll [12] ont montré, que deux systèmes chaotiques identiques peuvent se synchroniser. Cette découverte a ouvert la voie pour des applications du chaos aux télécommunications et encore d'autres méthodes pour synchroniser le chaos. Ainsi, après la méthode de Pecora et Carroll d'autres propositions pour synchroniser le chaos ont été proposées, comme la méthode de synchronisation généralisée dont Rulkov et al ont posé les bases. Dans ce chapitre nous présentons une étude sur quelque méthodes principales de la synchronisation.

3.2 Synchronisation identique

3.2.1 Synchronisation de Pecora et Carroll

Comme il a été dit précédemment, les systèmes chaotiques sont des systèmes dynamiques qui définent la synchronisation à cause de leur sensibilité aux conditions initiales. L'évolution de deux systèmes chaotiques identiques, qui commencent presque aux mêmes points initiaux, devient non corrélative au cours du temps. D'où l'impossibilité pratique de construire des systèmes chaotiques identiques, synchronisés dans le laboratoire. En 1990 Pecora et Carroll ont exposé, dans un article [12], leur découverte que deux systèmes chaotiques identiques se synchronisent sous certaines conditions. Alors ils ont considéré un système chaotique autonome de dimension n :

$$\dot{x} = f(x) \tag{3.1}$$

En 1990 Caroll et Pecora ont montré que : si on substitue une variable d'un système chaotique par la décomposition de ce système, alors on peut le synchroniser avec un autre système identique. Supposons qu'on a deux systèmes dynamiques chaotiques identique de dimension n présentés par :

$$\dot{X} = f(X) \tag{3.2}$$

$$\dot{Y} = f(Y) \tag{3.3}$$

L'un des deux systèmes est le maître et l'autre est l'ésclave, l'idée de cette méthode est de décomposer le système maitre en deux sous systèmes comme suit :

$$\dot{X}_1 = F_1(X_1, X_2) \tag{3.4}$$

$$\dot{X}_2 = F_2(X_1, X_2) \tag{3.5}$$

et on va considérer l'un des deux systèmes comme un signal transmetteur et il sera injecter dans le système esclave, alors on obtient le système suivant :

$$\dot{Y} = F_2(X_1, Y) \tag{3.6}$$

Comme système esclave ou recepteur, et X_1 est signal transmetteur. Le schéma suivant représent la synchronisation de Caroll et Pecora. Dans cette méthode, la synchronisation complète est définie comme l'identité entre les trajectoire des système esclave et de système maître pour le même signal chaotique transméteur. L'existence de la synchronisation complète implique que le système esclave est asymptotiquement stable : $e(t) \to 0$ lorsque $t \to \infty$

evec $e(t)$ est représente le système erreur de la synchronisation définie par :

$$e(t) = Y - X_2$$

Théorème 6. *Les systèmes maître et esclave sont synchronisés si et seulement si tous les exposants de Lyapunov du système esclave, appelés les exposants de Lyapunov conditionnels, sont négatifs.*

Exemple 20. *Pour clarifier ce concept et illustrer la technique de Pecora-Carroll on reprend un exemple sur la synchronisation identique du système de Lorenz donné dans la référence [12]. Le modèle mathématique de ce système est :*

$$\begin{cases} \dot{x} = a(x - y) \\ \dot{y} = -xz + rx - y \\ \dot{z} = xy - bz \end{cases} \tag{3.7}$$

où : $a = 16, b = 4, r = 45,92$

Pour le choix du sous-système esclave trois configurations de deux variables sont possibles :

$$\begin{cases} \dot{x}_1 = a(x_1 - y_1) \\ \dot{y}_1 = -x_1 z + r x_1 - y_1 \end{cases} \tag{3.8}$$

$$\begin{cases} \dot{x}_1 = a(x_1 - y) \\ \dot{z}_1 = -x_1 z_1 + r x_1 - y \end{cases} \tag{3.9}$$

$$\begin{cases} \dot{y}_1 = a(x - y_1) \\ \dot{z}_1 = -x z_1 + r x - y_1 \end{cases} \tag{3.10}$$

Suivant le théorème 6, la synchronisation identique nécessite la recherche d'une configuration du sous-système esclave qui donne des exposants de Lyapunov conditionnels négatifs. En utilisant l'algorithme de A.Wolf et al [1], on a obtenu le tableau (1) qui donne les valeurs approximatives des exposants de Lyapunov conditionnels pour les configurations précédentes.

système de Lorenz	Signal maître	Configuration du sous système esclave	Exposants de Lyapunov
a=16 ; r = 45,92 ; b = 4	x	(y,z)	0,0002 ;-17,0036
	y	(x,z)	-4,0007 ;-16,0033
	z	(x,y)	-2.4125 ;-2.5885)

Tableau 1 Les exposants de Lyapunov conditionnels pour les différentes configurations du sous- système esclave du système (3.7)

Dans les figures (3.1),(3.2) et (3.3) [2] montre graphiquement que la garantie de la synchronisation maître esclave est donnée par les valeurs négatives des exposants de Lyapunov associées au système esclave. Ainsi on remarque, dans les figures (3.2) et (3.3), que les états du système esclave convergent asymptotiquement vers les états correspondant au système maître, alors que la figure (3.1) représente une divergence d'états. En conclusion, le choix d'un sous système esclave candidat pour la synchronisation est limité par les conditions du théorème 6. En plus pour un éventuel usage de cette méthode pour la sécurisation de la communication entre émetteur et récepteur, la réalisation du sous-système esclave , dans le récepteur, dupliqué d'un sous système du système maître de l'émetteur ne semble pas très facile à mettre en pratique a cause des disparités des paramètres. Ces contraintes ont poussé les chercheurs à trouver d'autres méthodes de synchronisation qui cassent relativement les limites posées dans le cas de la synchronisation identique.

3.2.2 Synchronisation par la méthode de controle continue

Le principe de cette methode est : Supposons qu'on a deux systèmes chaotiques identiques définit par :

$$\dot{X} = AX + \phi(X) \tag{3.11}$$

$$\dot{Y} = AY + \phi(Y) + M_{n\times n}(Y - X) \tag{3.12}$$

les deux systèmes sont liés par un accouplement unidirectionnel, avec X et Y sont des variables des système maitre et esclave respectivement, et $M_{n\times n}$ une matrice carrrée diagonale d'ordre n définie par :

$$M_{n\times n} = \begin{pmatrix} P_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & p_n \end{pmatrix}$$

A est une matrice constante carrée d'ordre n, et ϕ une fonction continue qui représente la partie non linéaire de chaque système vérifiée la condition de Lipschitz suivante :

$$\|\phi(X) - \phi(Y)\| \leqslant \rho\|X - Y\| \tag{3.13}$$

ρ est appelé la constante de Lipschitz, et $\|.\|$ la norme euclidienne, alors on a le théorème suivant :

Théorème 7. *Soit E la matrice unitaire d'ordre n, et λ_i sont les valeurs propres de la matrice symétrique*

$$\frac{(A + M_{n\times n}) + (A + M_{n\times n})^T}{2} + \rho E$$

Si $max(\lambda_i) < 0$, alors le système maitre et le système esclave sont synchronisés dans le sense que le système erreur tend vers zero exponentiellement.

Exemple 21. *Considérons l'attracteur de Four-scroll suivant :*

$$\begin{cases} \dot{x} = ax - yz \\ \dot{y} = -by + xz \\ \dot{z} = -cz + xy \end{cases} \tag{3.14}$$

où : a, b and c sont des paramètres positives. Ce système est un attracteur chaotique présenté dans la figure (3.4), avec les valeurs $a = 0.4, b = 12, c = 5$.

Pour trouver la synchronisation de l'attracteur de Four-scroll, on a deux systèmes de Four-scroll, le premier est appelé système maitre et l'autre est système esclave définies par :

Système maître

$$\begin{cases} \dot{x}_1 = ax_1 + y_1 z_1 \\ \dot{y}_1 = -by_1 + x_1 z_1 \\ \dot{z}_1 = -cz_1 + x_1 y_1 \end{cases} \tag{3.15}$$

Système esclave

$$\begin{cases} \dot{x}_2 = ax_2 + y_2 z_2 + u \\ \dot{y}_2 = -by_2 + x_2 z_2 \\ \dot{z}_2 = -cz_2 + x_2 y_2 \end{cases} \tag{3.16}$$

où : u est le contrôle d'accoupelement choisiser par :

$$u = -y_1 z_1 + y_2 z_2 - (a+1)(x_2 - x_1)$$

Avec les paramètres donnés dans la référence [14], à l'instant $t = 5s$ *, on a trouvé que l'erreur de la synchronisation entre les systèmes* (3.15) *et* (3.16) *tendant vers* 0. *les graphes de la synchronisation sont donnés par :*

3.3 Synchronisation généralisée

Dans le concept de la synchronisation identique sous l'effet d'accouplement unidirectionnel il a été indiqué que le système maitre et esclave sont identiques ou presque identiques. Cependant, on va imaginer que le système maitre et esclave sont différent. En général, quand il y une différence entre les systèmes couplés on peut pas affirmer que les systèmes chaotiques non identiques peuvent être synchronisés, mais plusieurs travaux ont démontré que ce type de synchronisation chaotique existe, ce phénomène est appelé Synchronisation généralisé.
Pour définir ce type de synchronisation on va travailler sur des systèmes non linéaire composé d'un système maitre autonome avec des variables dynamiques x dans un espace de phase X, couplé avec un système esclave avec des variables dynamiques y dans l'espace d'état Y. La dynamique des ces deux systèmes est données par :

$$\dot{x} = F(x(t)) \tag{3.17}$$

$$\dot{y} = G(y(t), g, x(t)) \tag{3.18}$$

où g est une constante qui caractérise la force d'accouplement unidirectionnel.

Définition 6. *Lorsque $g \neq 0$, on dit que les deux systèmes chaotiques maitre et esclave sont synchronisés au sens généralisé s'il y a une transformation $\phi : X \rightarrow Y$ qui prend les trajectoires de l'attracteur de l'espace X dans les trajectoires de l'attracteur de l'espace Y, pour que $y(t) = \phi(x(t))$, et si cette transformation ne dépend pas des conditions initiales du système esclave $y(0)$ dans le bassin d'attraction de l'attracteur synchronisé.*

Remarque 2. *On remarque que dans cette définition de la synchronisation généralisée l'existence de la transformation ϕ est exigée seulement pour les trajectoires sur l'attracteur mais n'exigée pas pour les trajectoires passagère.*

Plusieurs méthodes ont été proposées pour étudier la synchronisation généralisée, on va proposer une des ces méthodes qui est "la synchronisation par l'auxiliaire approché".

3.3.1 Synchronisation par la méthode du système auxiliaire approché

Le principe de cette méthode est basé sur le fait que si le même système maître $X(t)$ conduit deux système esclaves identiques $Y(t)$ et $Z(t)$ qui commencentpar des conditions initiales différentes dans un bassin d'attraction, alors l'analyse de stabilité de la synchronisation dans un espace des phases $X \oplus Y$, qui peut en générale avoire une forme très compliquée $y(t) = \phi(x(t))$, peut être remplacée par l'analyse de la stabilité tout à fait simple $z(t) = y(t)$ dans l'espace $Z \oplus Y$ A cet effet on va supposer le système auxiliaire suivant :

$$\dot{z} = G(z(t), g, x(t)) \tag{3.19}$$

Qui est identique au système maître (3.18). Clairement, quand le système recepteur (ou esclave)(3.18) et son auxiliaire (3.19) ont le même signal émetteur $x(t)$, alors les champs (domaines) vectoriels dans les espaces de phase du recepteur et son auxiliaire sont identique et peuvent se développer sur des attracteurs identiques. Il est facile de montrer que la stabilité linéaire du collecteur $z(t) = y(t)$ est équivalente à la stabilité linéaire du collecteur des mouvements synchronisés dans $X \oplus Y$, qui est déterminer par $\phi(.)$. Les équations linéarisées qui dirigent l'évolution des quantités

$$\zeta_y(t) = y(t) - \phi(x(t))$$

et

$$\zeta_z(t) = z(t) - \phi(x(t))$$

sont :

$$\dot{\zeta}_y(t) = DG(\phi(x(t), g, x(t)).\zeta_y(t) \tag{3.20}$$

$$\dot{\zeta}_z(t) = DG(\phi(x(t), g, x(t)).\zeta_z(t) \tag{3.21}$$

avec :

$$DG(w, h_u(t)) = \frac{\partial G(w, h_u(t))}{\partial w} \tag{3.22}$$

Puis que les équations linéarisées pour $\zeta_y(t)$ et $\zeta_z(t)$ sont identiques, les équations linéarisées pour $\zeta_z(t) - \zeta_y(t) = z(t) - y(t)$ ont la même matrice jacobienne $DG(., g, x(t))$ que dans l'équation précédente. Donc, si le collecteur des mouvements synchronisés dans $X \oplus Y \oplus Z$ est linéairement stable pour $z(t) - y(t)$, alors il est linéairement stable pour $\zeta_y(t) = y(t) - \phi(x(t))$ et vice versa. Notons que l'équation linéarisée pour $z(t) - y(t)$ est identique à l'équation qui est définit les exposants de Lyapunov conditionnels pour le système récepteur. Ainsi, quand le collecteur $z = y$ est linéairement stable, les exposants de Lyapunov conditionnels pour le système émetteur, conditionnés sur la valeur du système récepteur $x(t)$, sont tous négatifs.

Exemple 22.

On va prendre comme un exemple deux systèmes chaotiques couplés unidirectionnellement, système de Chen et l'autre est celuit de $L\ddot{u}$. Pour cela on va supposer le système émetteur de Chen suivant :

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = (c - a)x_1 + cy_1 - x_1 z_1 \\ \dot{z}_1 = x_1 y_1 - bz_1 \end{cases} \tag{3.23}$$

Avec a, b et c sont des constantes qui caractérisent le système et on suppose le système de $L\ddot{u}$ comme système récepteur :

$$\begin{cases} \dot{x}_2 = a(y_2 + x_2) - g(x_2 - x_1) \\ \dot{y}_2 = by_2 - x_2 z_2 \\ \dot{z}_2 = -cz_2 + x_2 y_2 \end{cases} \tag{3.24}$$

dans le système émetteur on a $a = 35$, $b = 3$ et $c = 28$ par contre dans le système récepteur on a $a = 23$, $b = 20$ et $c = 3$. Le système émeteur est couplé avec système

récepteur seulement par le scalaire $x(t)$, avec g un entier qui caractérise la force d'accouplement unidirectionnel. on va montrer que ces deux systèmes peuvent être synchronisés dans le sens général, et pour cela on va suppose un système auxiliaire, qui est identique au système récepteur qui est représenté par l'équation (3.24)

$$\begin{cases} \dot{x}_3 = a(y_3 + x_3) - g(x_3 - x_3) \\ \dot{y}_3 = by_3 - x_3 z_3 \\ \dot{z}_3 = -cz_3 + x_3 y_3 \end{cases} \tag{3.25}$$

Pour $e_x = x_3 - x_2$, $e_y = y_3 - y_2$ et $e_z = z_3 - z_2$ on trouve le système suivant :

$$\begin{cases} \dot{e}_x = a(e_y - e_x) - ge_x \\ \dot{e}_y = be_y - z_3 e_x - x_2 e_z \\ \dot{e}_z = -ce_z + x_3 e_z - y_2 e_x \end{cases} \tag{3.26}$$

on va choisir la fonction de Lyapunov suivante :

$$V_g(t) = \frac{1}{2}(e_x^2 + e_y^2 + e_z^2) \tag{3.27}$$

Il est clair que cette fonction est toujour positive, alors pour que le système (3.26) soit stable il suffit que sa dérivée soit négative, et pour cela il suffit que le paramètre g vérifier cette relation :

$$g > -\alpha - \frac{\beta e_y^2 + \sigma e_z^2}{e_x^2} \tag{3.28}$$

Dans cette partie on a essayé de donner au phénomène de la synchronisation généralisée une compréhension pratique en appliquant la méthode sur les systèmes chaotiques de Chen et *Lü*.

3.4 Synchronisation de phase

Un cas fréquemment étudié dans la littérature est quand une force périodique externe faible est appliquée à un système chaotique autonôme, cette situation peut être décrite par un système d'équation différentielles d'ordre n suivant :

$$\dot{x}(t) = f(x) + p(t) \tag{3.29}$$

avec $p(t) = A_1 \cos(wt + \delta_1), A_2 \cos(wt + \delta_2), ..., A_n \cos(wt + \delta_n)$ représente la force périodique appliquée de fréquence ω dans l'intensité est mesurée par l'amplitude $A_i, i = 1, 2, ...n$. Dans ces circonstances il est possible d'observer le phénomène connu comme la synchronisation de phase. Cela signifiée que le système reste chaotique mais sa dynamique est modifiée de telle facon que la phase de l'attracteur chaotique rencontre celui de la force appliquée. La présence de la synchronisation de phase d'un système chaotique à une force agissante de la fréquence w est représentée par la relation suivante :

$$\psi(t) = \phi(t) \pm \frac{m}{n} wt \tag{3.30}$$

avec m et n deux entiers, comme le cas où il y a deux nombres réels ε_1 et ε_2 qui vérifient $\varepsilon_1 < \varepsilon_2$ et $\varepsilon_2 - \varepsilon < 2\pi$ tel que $\varepsilon_1 < \psi < \varepsilon_2$ pour tout t, $\phi(t)$ représente la phase de l'oscillateur chaotique et ψ est la différence entre la phase de l'oscilateur chaotique et celle de la force agissante. Cette condition peut être réécrite, comme :

$$|n\Omega - mw| = 0 \tag{3.31}$$

Pour que la synchronisation de phase signifié que la phase de l'oscilateur reste toujours assez près de la phase de la force $m = n = 1$, ou à une de ses harmonique $m > n$ ou bien la fréquence de l'oscilateur, ω est près d'une harmonie de la fréquence de la force $m < n$. La synchronisation de phase peut être obtenue ou non, selon les propriétés de la force appliquée : sa fréquence , w amplitude A_i et les angles $\delta_i, i = 1, 2, ...n$ à cause des approches différentes à la phase de l'oscilateur présenté dans la subdivision précédentela synchronisation de phase peut être contrôlée de plusieurs facons.

3.5 Synchronisation retardée

Après la synchronisation complète et généralisée, les chercheurs ont découvert que deux systèmes dynamiques chaotique non identiques peuvent exposer un phénomène de synchronisation dans lequel les variables dynamiques des deux systèmes deviennent synchronisées mais en retard, ils ont applé ce phénomène la synchronisation retardée. A cet effet, considerons deux systèmes chaotiques légèrement différents $\dot{x_1} = F_1(x_1)$ et $\dot{x_2} = F_2(x_2)$, acrochés par un accouplement unidirectionnel définit par la force d'accouplement ε, donc on s'attend que $x_1(t)$ soit synchronisée avec $x_2(t+\tau)$ dans une gamme de valeurs de ε où $\tau \neq 0$ est le retard de temps qui dépend beaucoup plus de ε que du paramètre caractérisant la différence entre les deux oscilateurs.

Pour évaluer quantitativement la synchronisation retardée, nous utilisons la fonction de similitude suivante définie en ce qui concerne une variable dynamique, disons x, des oscilateurs chaotiques :

$$s(\tau) = \sqrt{\frac{\langle (x_2(t-\tau) - x_1(t))^2 \rangle}{(\langle x_1^2(t) \rangle \langle x_2^2(t) \rangle)^{\frac{1}{2}}}} \tag{3.32}$$

où τ est le temps de retard. Soit s_{min} la valeur minimale de $s(\tau)$ et soit τ_{min} la quantité de retard où s_{min} est réalisé. On désigne par $\langle . \rangle$ le produit scalaire définit sur l'espace de phases.

La synchronisation retardée entre les deux oscilateurs est caractériser par les conditions :

$$s_{min} = 0 \ \ et \ \ \tau \neq 0 \tag{3.33}$$

Tandis que la synchronisation complète est caractérisée par les conditions :

$$s_{min} = 0 \ \ et \ \ \tau = 0 \tag{3.34}$$

Pour mettre en application un système de sécurisation de la communication par synchronisation du chaos trois problèmes techniques critiques devraient être d'abord résolus. Le premier est la disparité des paramètres entre l'émetteur et le récepteur

chaotiques, le deuxième est la non linéarité et le bruit additif au niveau du canal de liaison et le troisième est la robustesse du système. Ainsi ce chapitre a été consacré pour la présentation par ordre d'évolution des trois méthodes de synchronisation en critiquant leurs limites. Actuellement il n'existe évidemment pas de méthodes sans inconvénients. Cependant la synchronisation identique présente des qualités plus avantageuses par rapport aux autres méthodes, surtout concernant les limites dues aux disparités des paramètres.

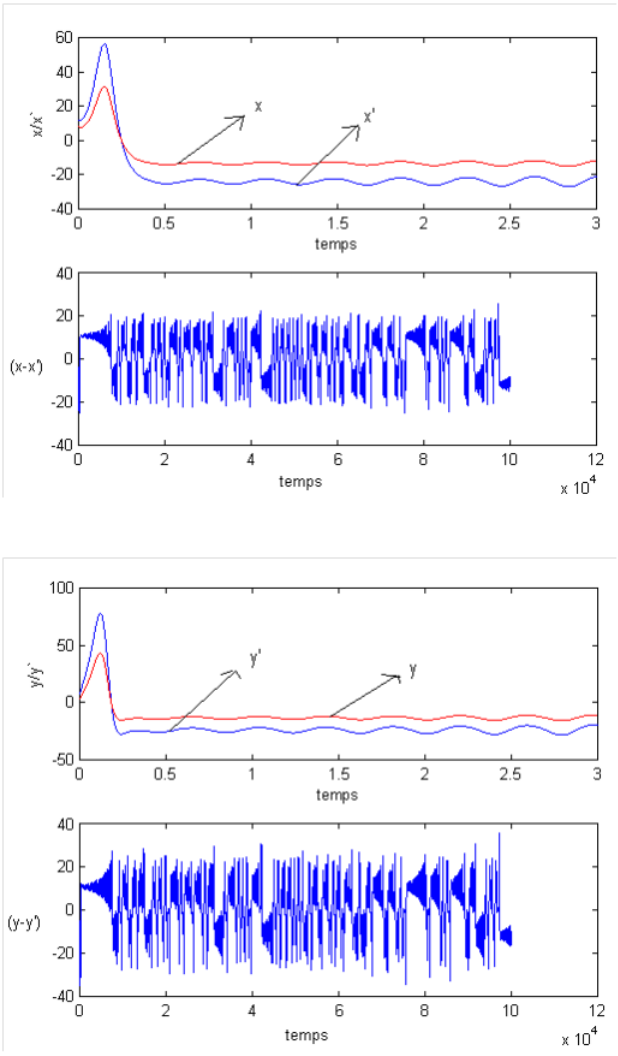


FIGURE 3.1 – Test de la synchronisation pour un sous- système esclave (x, y)

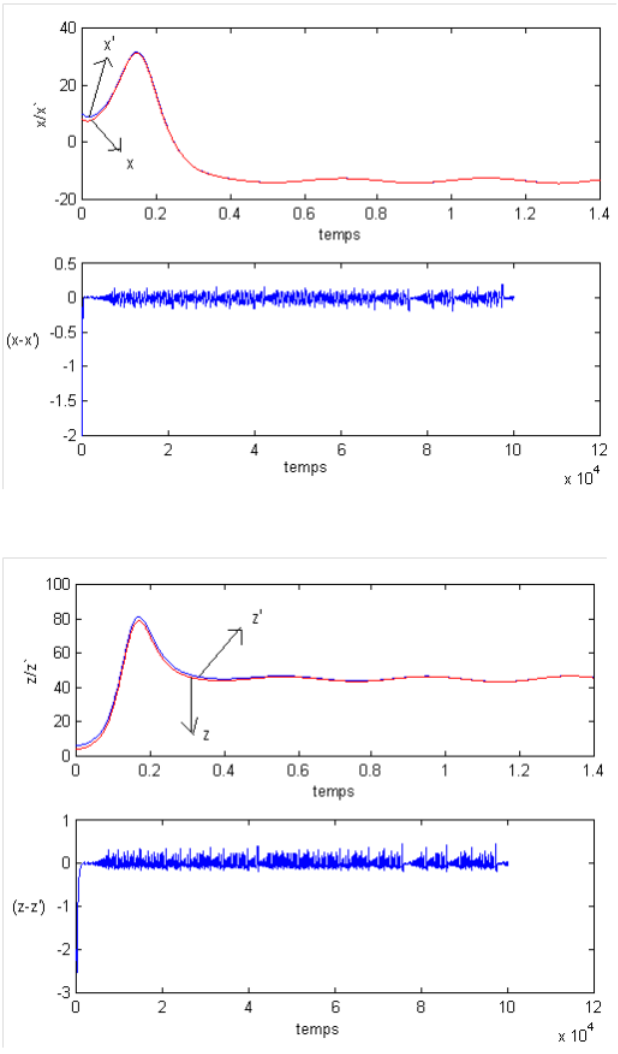


FIGURE 3.2 – Test de la synchronisation pour un sous- système esclave (x, z)

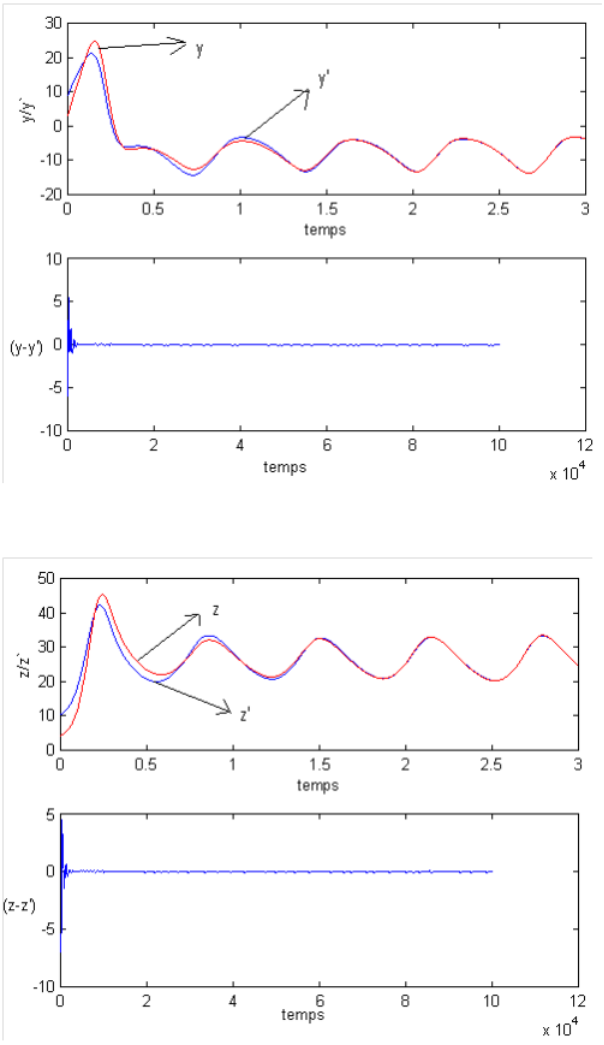


FIGURE 3.3 – Test de la synchronisation pour un sous- système esclave (y, z)

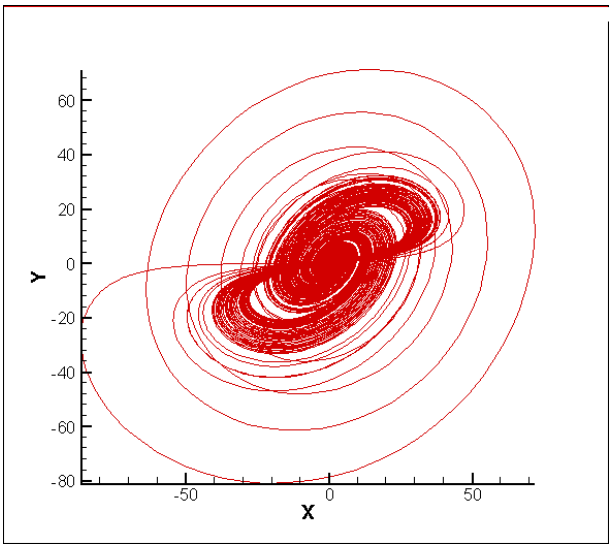


FIGURE 3.4 – L'attreacteur de Four-scroll

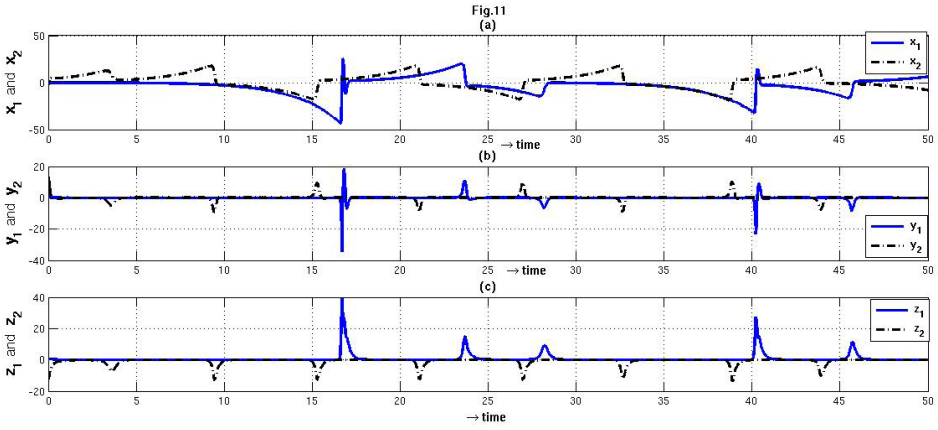


FIGURE 3.5 – présentation de la solution d'un couple attracteurs systèmes de Four-scroll avec control active desactivaté.

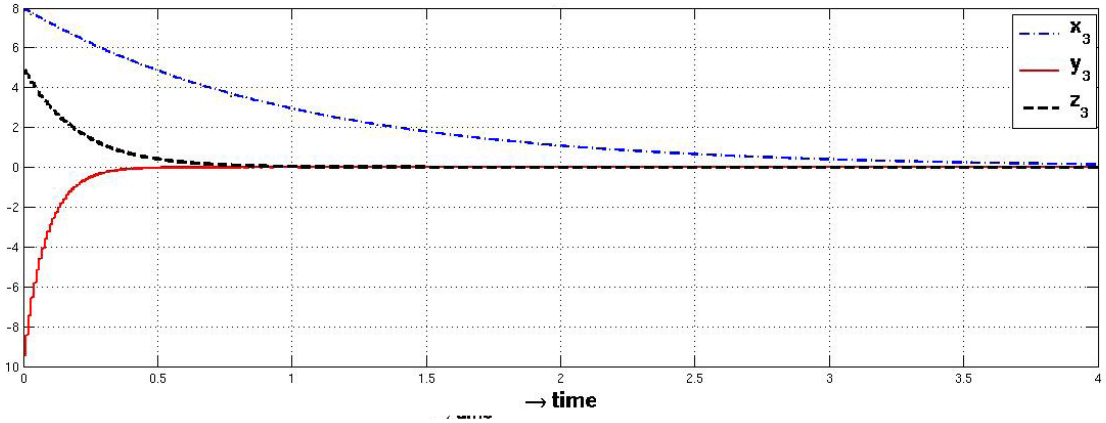


FIGURE 3.6 – présentation de different signals $e_1, e_2 et e_3$ lorsque le control active est activé.

Chapitre 4

La cryptographie chaotique et la securité des communications

4.1 Introduction et historique

Cacher des informations particulières à certaines personnes a toujours été un des intérêts principaux de l'homme. On a ainsi cherché à établir des techniques dites de « cryptage » afin de rendre ces informations incompréhensibles à ceux qui n'ont pas accès à une « clé » secrète. Ces techniques intéressent des personnes de divers domaines que ce soit le militaire, le commercial ou tout simplement personnel.

Au cours de l'Histoire diverses techniques cryptographiques ont été développées, les premières datant de l'antiquité comme la scytale ou le codage de César. Ces techniques primitives ont évoluées vers l'apparition des techniques de masquage, puis vers l'utilisation des machines automatisées et actuellement à l'utilisation des ordinateurs. En effet ceux-ci apportent une puissance de calcul remarquable qui a donné naissance à des techniques complexes.

Depuis les années 1990, le chaos est utilisé au coeur des systèmes de trans-

missions sécurisées, ou crypto-systèmes. Bien que purement déterministe, un signal chaotique présente une forte ressemblance avec un bruit. Par conséquent, les techniques de cryptage chaotique consistent à cacher, à noyer l'information dans un signal porteur chaotique. Cette révolution dans l'étude du chaos a été rendue possible grâce à la découverte de la capacité de synchronisation des systèmes chaotiques, qui semblait a priori impossible.

Dans un premier temps, plusieurs montages électroniques simulant la synchronisation des systèmes de Lorenz ou Rössler ont été réalisés. Ils ont été suivis par de nombreuses configurations pour permettre la transmission de signaux « sécurisés », les plus notables étant ceux de Cuomo en 1992 [8] [9] qui utilisaient une transmission par masquage et étalement de spectre. Dans la décennie qui a suivie il y a eu de nombreuses autres configurations et des améliorations de celles déjà existantes. Dans notre rapport on étudiera en détail la transmission par masquage mais les configurations utilisées pourront être appliquées à d'autres techniques de communication.

Cependant, les difficultés issues de la synchronisation en temps continu ont mené certains chercheurs à mettre au point d'autre techniques de « synchronisation » comme le Chaos Shift Keying(CSK) [5], proposé par Kolomban et Kennedy, qui est utile pour la transmission en temps continu.

Dans ce chapitre on va présenter quelque techniques de cryptage chaotique.

4.2 Les crypto-systèmes

Un crypto-système a pour but de chiffrer un message clair en un message codé (Cryptogramme) suivant des techniques complexes, incompréhensible par toute personne curieuse (Cryptanalyse ou décrypteur) différente du destinataire légitime.

4.2.1 Classification des crypto-systèmes

Les crypto-systèmes peuvent être classés conformément aux différentes caractéristiques. Ainsi, selon les types des clefs utilisées, on a la catégorie suivante des crypto-systèmes :

Systèmes symétriques, systèmes asymétriques et systèmes hybrides.
Une autre catégorie des crypto-systèmes est basée sur les techniques de chiffrement :

Chiffrement par bloc ou chiffrement par flot.

La notion de sécurité est une autre caractéristique qui peut être utilisée pour classes les crypto-systèmes. Ainsi, on a les systèmes à sécurité parfaite ou inconditionnelle, les systèmes à sécurité sémantique et les systèmes à sécurité calculatoire liée à la quantité de ressources informatiques.

4.2.2 Relation entre le chaos et les crypto-systèmes

Tout d'abord, nous notons qu'il y a une forte ressemblance entre les systèmes chaotiques et les crypto-systèmes symétriques à chiffrement par bloc. Pour commencer, un crypto-système est dit bon, s'il satisfera les trois caractéristiques suivantes :

1. Transformation aléatoire des données nettes aux données chiffrées sans garder aucune information sur les données nettes.
2. Soit fortement sensible aux données nettes de telle sorte qu'un plus petit changement dans les données nettes engendre des données chiffrées complètement différentes.
3. Soit aussi fortement sensible à la clef de telle sorte qu'un plus petit changement dans la clef donne une naissance à des nouvelles données chiffrées complètement différentes. Une autre caractéristique importante des crypto-systèmes

symétriques et qu'ils utilisent quelques fonctions de chiffrage en mode itératif qui est une condition pratique pour certains crypto-systèmes populaires.

En ce qui concerne les caractéristiques particulières des systèmes chaotiques, notons qu'un système chaotique est constitué de quelques fonctions de base f qu'ils sont itérées sur un ensemble X. Le fonctionnement d'un tel système consiste à remplir les conditions suivantes :

1. Soit un mélangeur, ceci signifie que l'ensemble X devrait être aléatoirement mélangé par la répétition de l'action de f.
2. Soit sensible à l'état initial de telle sorte qu'une légère modification dans les états initiaux engendra des états complètement différents.
3. Soit sensible aux certains paramètres de contrôle et un léger changement dans ces paramètres causera un changement dans les propriétés de la carte chaotique.

En comparant entres les particularités d'un crypto-système et les caractéristiques d'un système chaotique, il est évident que le chiffrage et le chaos montrent des similarités remarquables, si nous considérons que les données nettes correspond à un état initial, la clef correspond à l'ensemble des paramètres, et la fonction de chiffrage correspond à la fonction de base f.

Cependant, il y a une différence importante entre ces deux concepts. En fait, le cryptosystème travaille sur des ensembles finis (discrets), alors que le système chaotique est conçu pour travailler sur des ensembles infinis (continus). C'est probablement la raison principale pour laquelle la relation entre le chaos et le chiffrage a été restée inaperçue.

4.3 Transmission à porteuse chaotique

Les signaux chaotiques peuvent être utilisés pour la transmission de l'information, principalement dans deux objectifs : Le premier est de protéger l'information

transmise. Dans ce cas, les applications réalisées sont en compétition avec les méthodes de cryptographie classiques. Un deuxième objectif est d'étaler le signal informationnel avec tous les avantages des techniques à étalement de spectre. Dans ce deuxième cas, les méthodes développées doivent être comparées aux systèmes classiques à étalement de spectre.

Si on regarde du point de vue de la structure d'un tel système de transmission, on peut définir deux approches : La première, est représentée dans la figure (4.1)[15]. Elle remplace le signal porteur sinusoïdal par un modulateur chaotique contrôlé d'une manière quelconque par le signal informationnel. Cette solution a l'avantage d'être très simple à implémenter mais par contre nécessite un système chaotique avec des contraintes fortes sur les paramètres intrinsèques. En plus, celui-ci doit travailler à des hautes fréquences.

En pratique, il est difficile de trouver des circuits permettant un tel fonctionnement et donc, pour le moment, cette solution est surtout considérée dans un cadre théorique.

Une deuxième solution est de moduler le signal informationnel par celui chaotique en bande de base, et après d'appliquer une transposition en haute-fréquence par l'intermédiaire d'une porteuse sinusoïdale. Ce schéma est présenté dans la figure (4.2)[15]. Son avantage principal consiste dans une simplification importante du modulateur chaotique, mais avec une complexité générale du système plus importante.

Exemple 23. *Cet exemple exploite les dynamiques chaotiques produites par des lasers à semi-conducteurs pour réaliser des communications optiques sécurisées. Ce type de cryptographie est intéressant pour des utilisations commerciales et militaires. Pour pouvoir être déployées à grande échelle, il est nécessaire que les communications chaotiques apportent un niveau de sécurité plus élevé, soient capables de véhiculer de très grands débits de données et, enfin, qu'elles soient compatibles avec l'infrastruc-*

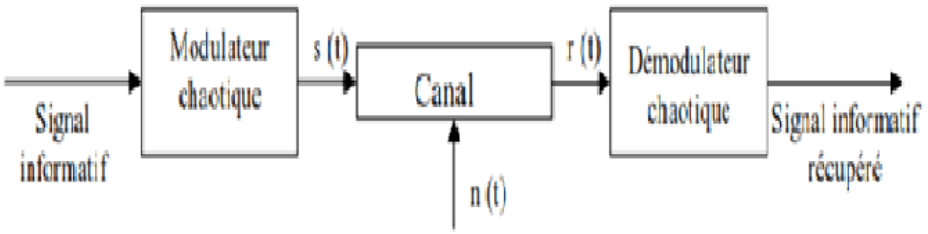


FIGURE 4.1 – Modulation directe du signal informationnel par une porteuse haute fréquence chaotique

ture existante des télécommunications optiques.

Actuellement, les principes utilisés dans les télécommunications classiques ont recours à la théorie linéaire. En particulier, des efforts considérables sont déployés pour faire en sorte que les émetteurs et les récepteurs conventionnels opèrent dans un régime linéaire. Au lieu d'essayer d'éviter les non-linéarités, nous proposons d'exploiter les dynamiques complexes qui sont produites naturellement par des systèmes dynamiques optiques non-linéaires. Ces dynamiques complexes, qui ont longtemps été considérées comme nuisibles, peuvent aussi être une source d'améliorations dans les systèmes de télécommunications. En effet, les dynamiques complexes et imprévisibles peuvent être exploitées pour masquer physiquement un message [7].

Alice encrypte des données en utilisant la dynamique chaotique d'un laser, les

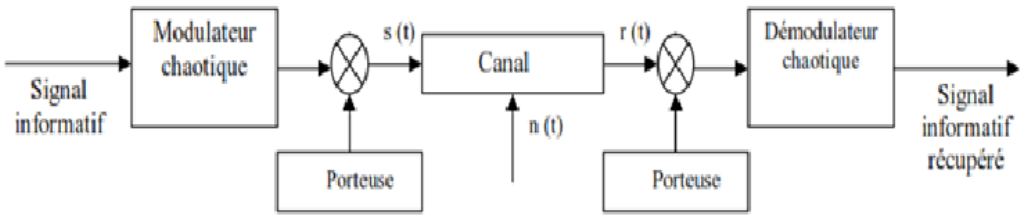


FIGURE 4.2 – Modulation en bande de base du signal informationnel par le signal chaotique, combinée avec une mise sur porteuse classique.

informations sont transmises à Bob qui les décrypte par synchronisation. Une espionne, Eve, peut pirater la ligne et décrypter les informations si elle parvient à identifier le laser d'Alice.

Les systèmes dynamiques non-linéaires peuvent aussi présenter une grande efficacité, étant donné qu'ils réagissent fortement à de faibles perturbations, et peuvent donc être contrôlés et produire des signaux en réponse à une faible énergie de commande. Ils présentent aussi une grande capacité de transport d'information, car la variété d'états complexes produits offre de nombreuses possibilités d'encodage compact de l'information. Enfin, comme les communications optiques non-linéaires ne doivent pas se conformer à la division classique du spectre en bandes de fréquences, le nombre de canaux utilisables pourrait être plus grand que dans le cas de systèmes linéaires. Le nombre de canaux disponibles est en effet uniquement limité par la ca-

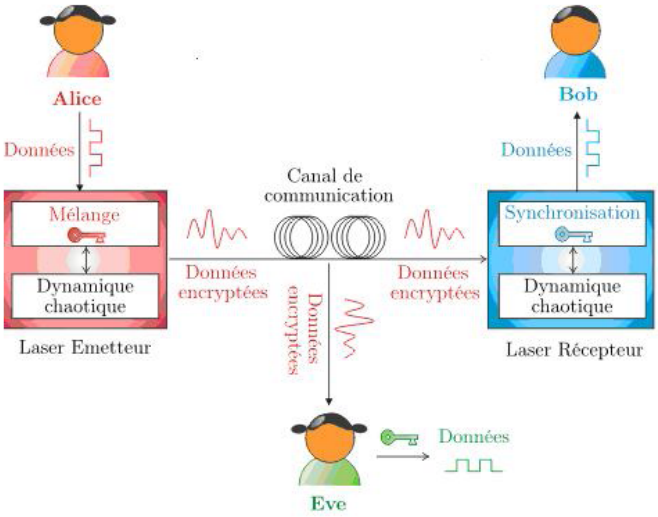


FIGURE 4.3 – Description d'un système de communication par chaos.

pacité des récepteurs à distinguer des états chaotiques différents.

Des crypto-systèmes optiques peuvent être construits en utilisant des lasers à semiconducteurs soumis à une rétroaction optique ou à l'injection optique d'un autre laser. Ce type de système possède un riche comportement dynamique. Dans certaines conditions opératoires, l'intensité optique du laser peut fluctuer de façon chaotique. Ces fluctuations chaotiques peuvent être utilisées pour masquer ou encoder physiquement un message utile en temps réel.

Le décryptage du message est possible en utilisant comme récepteur une copie de l'émetteur, qui se synchronise avec l'émetteur et permet d'extraire le message utile [9] .

4.4 Masquage par addition

4.4.1 Présentation de la technique

Cette technique est considérée comme la première proposition d'utiliser le chaos pour sécuriser la communication [18][15] . Elle est présentée dans les références [9][21][2]. Son principe est de brouiller le signal message $m(t)$ dans un signal chaotique $c(t)$, par une opération d'addition direct avant de le transmettre, afin d'avoir un signal crypté $s(t)$. Pour récupérer le signal message au niveau du récepteur autorisé, le même système générateur du chaos est utilisé à la fois à l'émission et à la réception, avec la différence que dans le récepteur, ce système est contrôlé par le signal reçu $r(t)$ (égal au signal $s(t)$ affecté par les perturbations dans le canal) pour obtenir la synchronisation. L'ordre de grandeur du signal message, doit être impérativement très faible par rapport à celui du signal chaotique $c(t)$, pour ne donner aucun espoir de le récupérer par les intrus, sans savoir le signal $c(t)$ exact et pour avoir une bonne synchronisation au niveau du récepteur autorisé. La clef de cryptage et de décryptage est égale aux valeurs des paramètres d'accouplement entre l'émetteur et le récepteur et des paramètres caractérisant les systèmes chaotiques utilisés. Alors le signal message est reconstitué par la différence entre le signal recu $r(t)$ et le signal $c(t)$ proche de $c(t)$ résultat de la synchronisation, voir la figure (4.4).

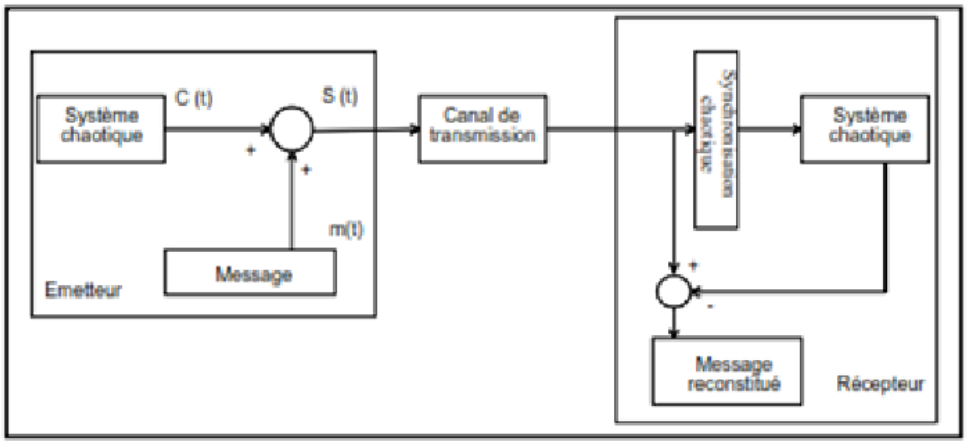


FIGURE 4.4 – Schéma du masquage chaotique par addition

L'exemple de simulation suivant illustre ce principe :

Exemple 24. *Ainsi dans cette simulation, on utilise la synchronisation identique entre deux systèmes de Rossler [15]. De cette façon on prend le système (4.1) comme générateur d'un signal chaotique (on a choisi* $c(t) = x_8(t)$ *une variable d'état du système (4.1) dans l'émetteur). Au niveau du récepteur la synchronisation est faite en utilisant le système (4.2) avec les mêmes conditions initiales que celles données dans l'exemple précédent, mais contrôlé par le signal* $r(t)$ *reçu. On aura alors le système suivant :*

$$\begin{cases} \dot{y}_1 = -(y_2 + y_3) - g(y_1 - r(t)) \\ \dot{y}_2 = y_1 + 0.2.y_2 \\ \dot{y}_3 = 0.2 + y_3(y_1 - 5.7) \end{cases} \tag{4.1}$$

Si on suppose que les perturbations dues au canal sont négligeables et que la trans-

mission ne nécessite pas de modulation on aura alors :

$$r(t) = s(t) = c(t) + m(t) \tag{4.2}$$

Avec $m(t)$ *le signal message et* g *de valeur* 0.2 *le paramètre d'accouplement.*
La clé de cryptage et de décryptage est le paramètre d'accouplement g *et les paramètres du système émetteur. Si on choisit pour* $m(t)$ *un signal carré d'amplitude égale a* 0.0001 *et de fréquence égale* $1Hz$*, comme le montre la figure (4.5).*

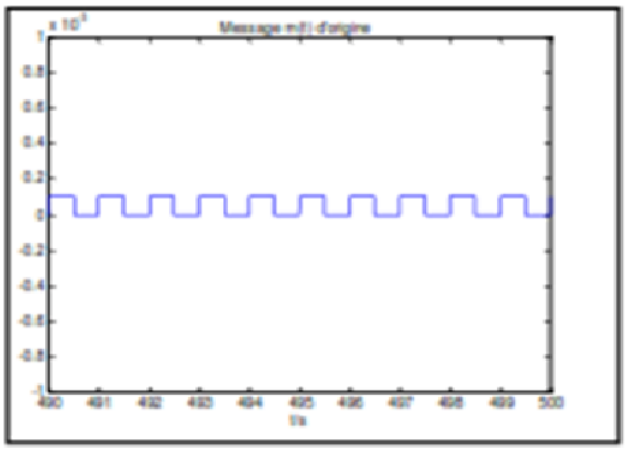
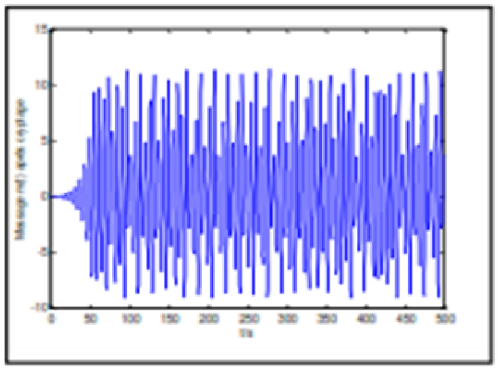


FIGURE 4.5 – Message $m(t)$ d'origine

Au niveau de l'émetteur on aura alors le message crypté représenté sur la figure (4.6) à droite, et on aura alors le message reconstitué à la sortie du récepteur à gauche.

Pour vérifier la qualité du résultat on diminue l'échelle de l'axe des ordonnées de la représentation du signal reconstitué on aura alors la figure (4.7) suivante :



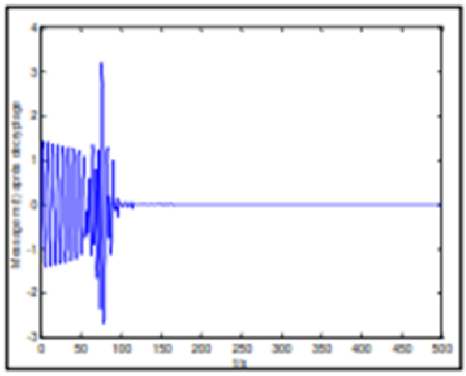


FIGURE 4.6 – Message $m(t)$ après cryptage à droite et Message reconstitué apès cryptage et décryptage par la méthode du masquage par addition à gauche

Si on visualise notre signal entre les deux points d'abscisses respectivement $490s$ *et* $500s$*, alors on aura la figure (4.8) suivante :*

On constate dans la figure (4.8) qu'on a une forme similaire à notre signal message $m(t)$ *d'origine (amplitude* 0.0001 *et période de* $1s$*).*

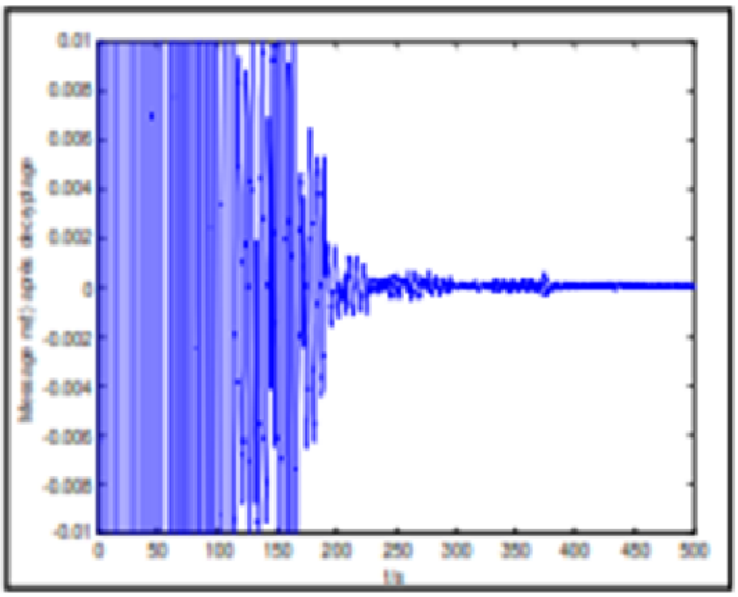


FIGURE 4.7 – Message reconstitué après cryptage et décryptage par la méthode du masquage par addition après diminution de l'échelle de la représentation

4.4.2 Discussion des résultats

Les avantages du masquage chaotique par addition résident dans sa simplicité de réalisation et la possibilité de l'utiliser pour masquer l'analogique ou le numérique avec des canaux à fort SNR, comme c'est le cas des fibres optiques [15]. Inversement on souligne des inconvénients qui limitent l'application de cette technique en pratique tels que :

1. La synchronisation non parfaite au niveau du récepteur, même avec une amplitude très faible du signal message devant le signal chaotique, ce qui implique la sensibilité au bruit du canal.
2. Sensibilité à la disparité des paramètres, entre les systèmes chaotiques dans l'émetteur et le récepteur.
3. Le faible degré de sécurité démontré, en testant cette technique par des mé-

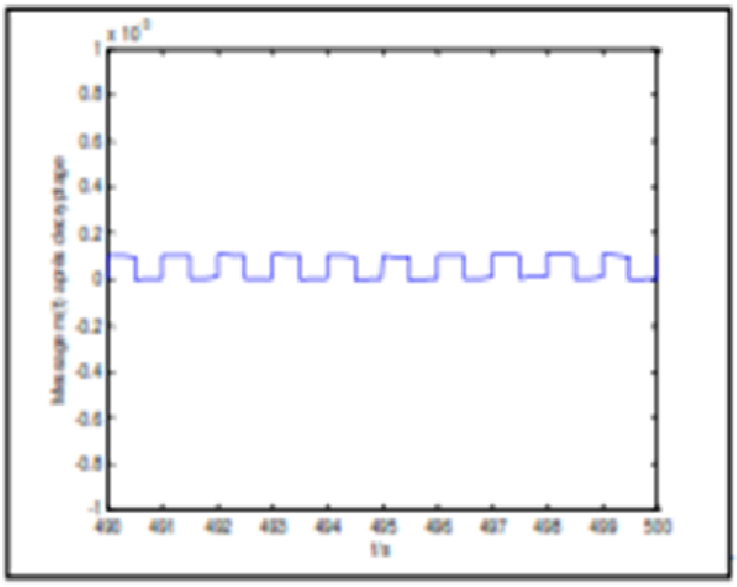


FIGURE 4.8 – Visualisation du message décrypté entre deux points d'abscisses $490s$ et $500s$

thodes de cryptanalyse exposées dans les articles [3] [8] [21] .

4.5 Masquage par décalage chaotique

4.5.1 Présentation de la technique

L'apparition de cette technique, est considérée comme une conséquence des problèmes d'application pratique du masquage par addition. Elle a été proposée pour la première fois par le groupe de Kocarev [5] [21], et sa dénomination actuelle connue par " Chaos shift keying : CSK" revient à l'article du groupe de Dedieu [5].
La CSK définie comme une modulation numérique est inspirée des techniques de modulation classique telle que la FSK (frequency shift keying) la ASK (amplitude shift keying) et la PSK (phase shift keying). Alors le système de masquage par CSK

est constitué par un modulateur CSK au niveau de l'émetteur et d'un démodulateur CSK au niveau du récepteur raccordés par un canal routeur du signal comme il est représenté sur la figure (4.9)[5].

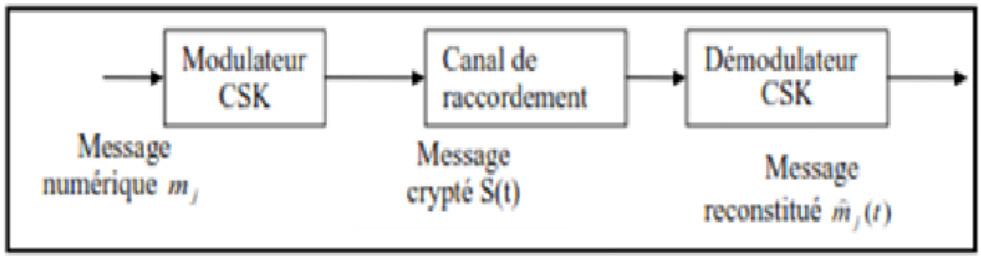


FIGURE 4.9 – Schéma de principe simplifié d'un système de cryptage CSK.

4.5.2 Le modulateur CSK

Son idée de base est la même que celle de la modulation numérique classique, c'est-à-dire associer à chaque symbole du message à transmettre non pas une porteuse sinusoïdale, mais une porteuse chaotique différente [18] [2], en se déplaçant dans une période de durée T. Ainsi en utilisant la notation la plus générale introduite dans [4], les éléments de l'ensemble d'un signal message numérique incluent dans un espace de symboles à M niveaux modulé par CSK sont définis par :

$$S(t) = \sum_{j=1}^{N} mjg_i(t) \tag{4.3}$$

Où m_j sont les éléments du vecteur signal message et $g_i(t)$ i sont les porteurs chaotiques. Avec $j = 1, 2.....N; i = 1, 2.....M; N \leqslant M$ et $m_j = 1$ si $i = j$ et $m_j = 0$ si $i \neq j$

Le signal $S(t)$ peut être généré comme il est représenté dans la figure(4.10) [4].

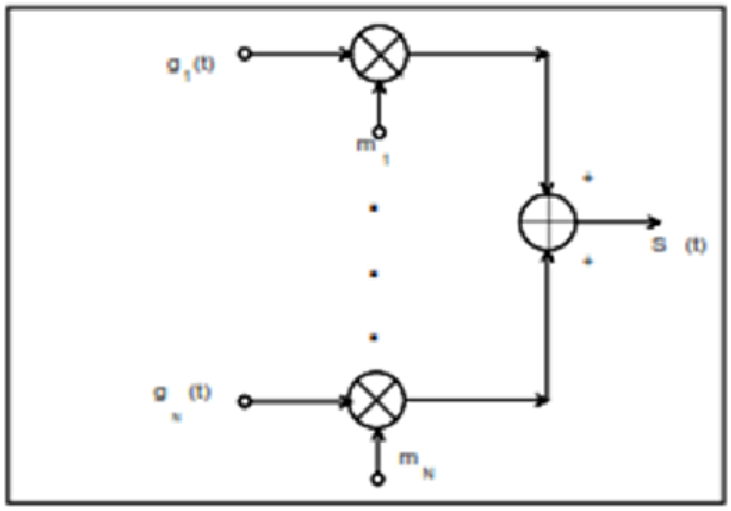


FIGURE 4.10 – Principe de la modulation par CSK

4.5.3 Le Démodulateur CSK

Du côté du récepteur autorisé si on suppose que le signal est reçu par bande de base, on peut citer deux types de schémas qui ont été proposés [19] :

1. Démodulation basée sur la synchronisation et le calcul d'erreur : à ce niveau les porteurs chaotiques g_i , utilisés pour la modulation, seront reconstruits en utilisant des unités de synchronisation chaotiques. Le nombre de ces unités est égal au nombre des porteurs chaotiques g_i, figure (4.11)[4]. Ainsi dans cette configuration, le signal reçu va essayer de synchroniser toutes les unités de

synchronisation. Alors si on suppose que le signal transmis $S(t) = g_i(t)$, on n'aura donc la synchronisation qu'avec la $i - me$ unité. De cette façon on va avoir une convergence de $g_i(t)$ vers la sortie de l'unité $\hat{g}_i(t)$ et une divergence pour les autres unités. L'estimation des symboles m_j du message sera faite après le calcul des erreurs de synchronisation dans le bloc de décision. Les paramètres des unités de synchronisation et le temps symbole peuvent être considérés comme la clé de décryptage.

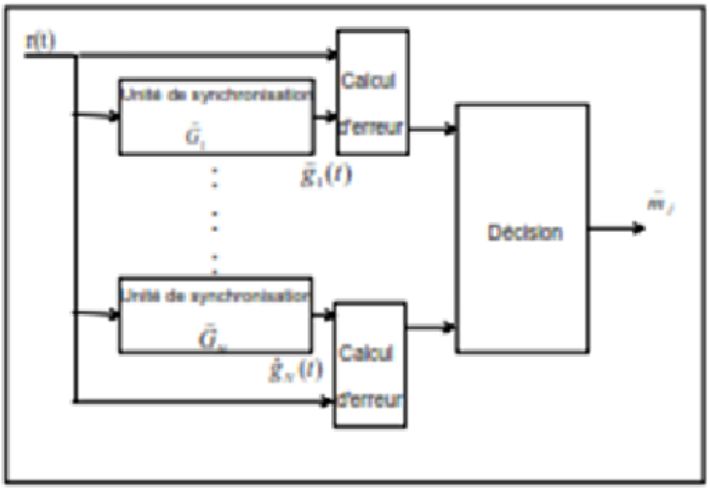


FIGURE 4.11 – Démodulation basée sur la synchronisation et le calcule d'erreur

2. Démodulation basée sur la synchronisation et la corrélation : Dans ce modèle, la reconstitution des porteurs chaotiques $g_i(t)$ est aussi nécessaire, ainsi elle se fait de la même manière que pour le modèle précèdent. Comme la corrélation est un processus générique dans les systèmes de communication qui est employé pour évaluer la similarité entre deux signaux, alors la différence de ce système par rapport au précédent est que chaque unité de synchronisation chaotique est cascadée par un bloc corrélateur. De cette manière, si les porteurs chaotiques

$\hat{g}_i(t)$ reconstitués par synchronisation pendant un temps Ts convergent vers $g_i(t)$, le symbole transmis peut être identifié en évaluant la corrélation entre $g_i(t)$ et $\hat{g}_i(t)$. La prise de décision sera faite en comparant les éléments du vecteur de décision $Z = (z, z, ..., z)$ sorties des corrélateurs. Alors l'affirmation de la convergence de $g_i(t)$ vers $\hat{g}_i(t)$ sur un intervalle $[T_s, T]$, va nous donner une observation $z_i > z_k, k = 1, ...M, i \neq k$. La figure (4.12)[4] illustre ce principe. Les paramètres des unités de synchronisation et le temps symbole peuvent être considérés comme la clé de décryptage.

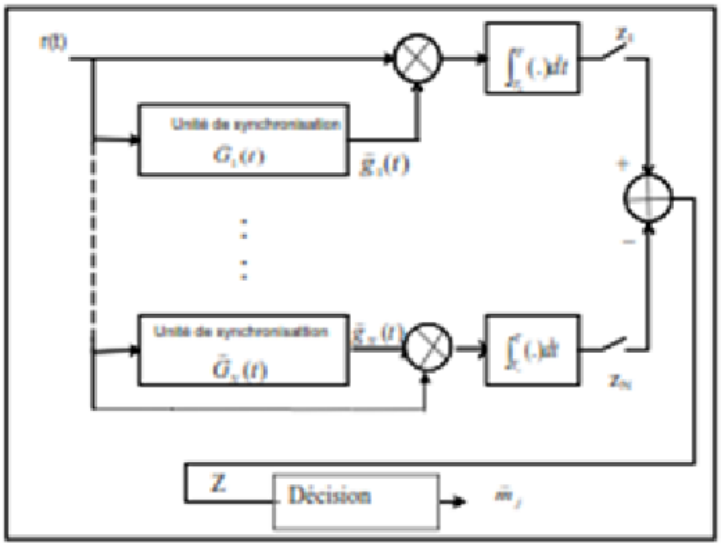


FIGURE 4.12 – Démodulation basée sur la synchronisation et la corrélation

Remarque 3. *Il est à noter que ces propositions sont basées sur la démodulation cohérente, c'est-à-dire le récepteur est capable de reproduire la même porteuse chaotique que celle émise par l'émetteur, afin que le message d'origine soit décrypté. L'inconvénient le plus important pour ces deux techniques est que la synchronisation se perd,*

lorsque le symbole du signal message change. Ainsi le temps de transmission d'un seul symbole doit être supérieur ou égal à la somme du temps de synchronisation, plus le temps de décision, ce qui limite le débit de transmission du message. Des modifications de la méthode CSK pour la démodulation non cohérente, qui n'exigent pas la reproduction de la même porteuse chaotique de l'émission, ont été également proposées [2] .

Alors que la synchronisation étant un élément clé dans l'étude des communications sécurisées par le chaos, ainsi dans notre étude de la CSK, on va choisissez de simuler un système à récepteur cohérent, dont la démodulation est basée sur la synchronisation et le calcul d'erreur et on va choisissez comme signal un message fonctionnel.

Chapitre 5

Application de la cryptographie chaotique sur deux modèles chaotiques

5.1 Introduction

Au siècle passé, plusieurs chercheurs se sont intéressées aux comportements inhabituels des systèmes dynamiques chaotiques et on a découvert que certains systèmes présentaient des instabilités de nature très étranges. Ce fût la découverte des signaux chaotiques qui ont un comportement complètement déterministe mais qui font penser à des allures pseudo-aléatoires. Une définition universelle du chaos n'existe pas vraiment, les mathématiciens qui étudient les systèmes chaotiques utilisent certaines caractéristiques de la stabilité du système (les exposants de Lyapunov) pour définir un comportement chaotique.

En 1990, Pecora et Carroll ont publié un article [12] dans lequel ils présentent la démonstration théorique et expérimentale de la possibilité de synchroniser deux systèmes chaotiques. Ici, la synchronisation signifie que deux systèmes chaotiques ayant la même structure mais forcement des conditions initiales différentes sont amenés

à reproduire le même signal chaotique. Ce phénomène qui semblait être impossible pour les systèmes chaotiques (ceux-ci étant très sensibles à des perturbations sur leurs trajectoires) fut une révolution dans la communauté scientifique. C'est ainsi que l'utilisation du chaos dans la cryptographie à vue le jour.

Dans un premier temps, plusieurs montages électroniques simulant la synchronisation des systèmes de Lorenz ou Rössler ont été réalisés. Ils ont été suivis par de nombreuses configurations pour permettre la transmission de signaux « sécurisés », les plus notables étant ceux de Cuomo en 1992 qui utilisaient une transmission par masquage et étalement de spectre [8] [9]. Dans la décennie qui a suivie il y a eu de nombreuses autres configurations et des améliorations de celles déjà existantes. Dans notre rapport on étudiera en détail l'utilisation de deux modèles chaotiques pour sécuriser un message fonctionel qui est la fonction $\sin \omega t$.

5.2 Caractérisation des systèmes chaotiques

Définition 7. *Un système dynamique est un triplet* (T, M, ϕ) *où :*
T *est un monoïde.*
M *est l'espace des phases.*
ϕ *est une fonction définie :* $\Phi : T \subset T \times M \longrightarrow M$ *Avec :*

$$\phi(t_1, \phi(t_2, x)) = \phi(t_1 + t_2, x)$$

$\phi(x, t)$ *est appelée la fonction d'évolution du système dynamique.*
x *représente l'état initial du système dynamique.*

Définition 8. *Un système dynamique chaotique est un système dynamique non linéaire qui vérifié :*

- *La sensibilité au condition initial.*
- *Il a une dimension fractal.*
- *Déterminisme.*
- *Il a un attracteur étrange.*

5.2.1 Système de Four-scroll

Considèrons le modèle de Four-scroll [10] :

$$\begin{cases} \dot{x}_1 = ax_1 + y_1 z_1 \\ \dot{y}_1 = -by_1 + x_1 z_1 \\ \dot{z}_1 = -cz_1 + x_1 y_1 \end{cases} \tag{5.1}$$

x, y et z étant des variables d'états et a, b et c des paramètres réels constants et positifs. Pour les données numériques suivantes : $a = 0,4,\ b = 12\ et\ c = 5$, le système de four-scroll (5.1) constitue l'attracteur chaotique de la figure (5.1).

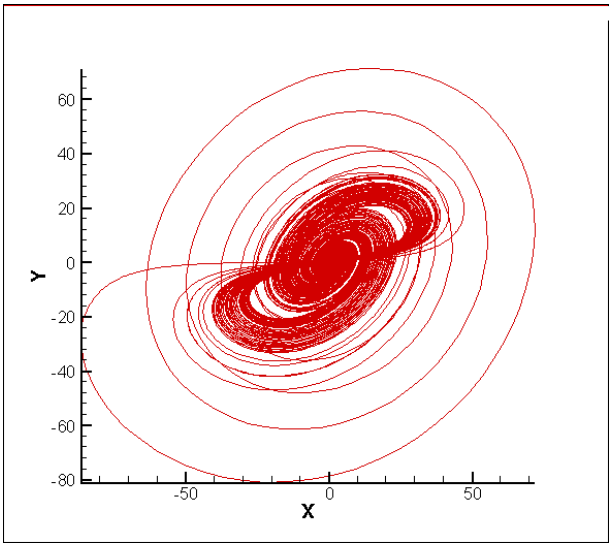


FIGURE 5.1 – L'attracteur de Four-scroll

5.2.2 Système de Lorenz

Considèrons le modèle de Lorenz [20] :

$$\begin{cases} \dot{x}_1 = a(y_1 - x_1) \\ \dot{y}_1 = bx_1 - x_1 z_1 - y_1 \\ \dot{z}_1 = x_1 y_1 - cz_1 \end{cases} \tag{5.2}$$

x, y et z étant des variables d'états et a, b et c des paramètres réels constants et positifs. Pour les données numériques suivantes : $a = 10$, $b = \frac{8}{3}$ et $c = 28$, le système de Lorenz (5.2) constitue l'attracteur chaotique de la figure (5.2).

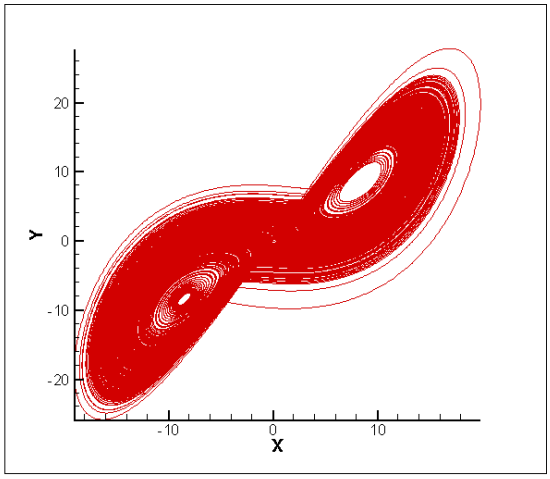


FIGURE 5.2 – L'attracteur de Lorenz

5.3 Utilisation du chaos pour la sécurisation des communications

L'idée de base est de brouiller un message adéquatement avec le chaos au niveau de l'émetteur, afin de le dissimuler des intrus, avant de le transmettre à sa destination

qui sera la seule capable de le déchiffrer. Ainsi dans ce travail on va crypté un message fonctionel utilisant le système chaotique de fours-croll par la méthode de CSK.

5.3.1 Le modulateur CSK

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

$$S(t) = \sum_{j=1}^{n} m_j g_i(t) \tag{5.3}$$

Où m_j sont les éléments du vecteur signal message et $g_i(t)$ sont les porteuse chaotiques. Avec $j = 1, 2.....N$; $i = 1, 2.....M$ et $N \leq M$ et

$$m_j = \sin \omega t \tag{5.4}$$

Puisque le débit du signal message à masquer est limité par le temps de synchronisation Ts des oscillateurs chaotiques ($5s$ dans notre cas), on a choisi dans notre simulation d'utiliser la fonction $\sin \omega t$, avec $\omega = \frac{\pi}{2}$ qui génère des séquences 1 et -1, et on a réglé son débit T égale à $15s$ supérieur au temps de synchronisation Ts, pour la probabilité d'apparition des 1 et des -1. La figure (5.3) représente l'allure du signal message mj avant la modulation.

Modulateur CSK en utilisant le modèle de Four-scroll

Il a été vérifié dans la référence [14] que le système (5.1), qui est considéré comme système maître, se synchronise identiquement avec un système esclave dont

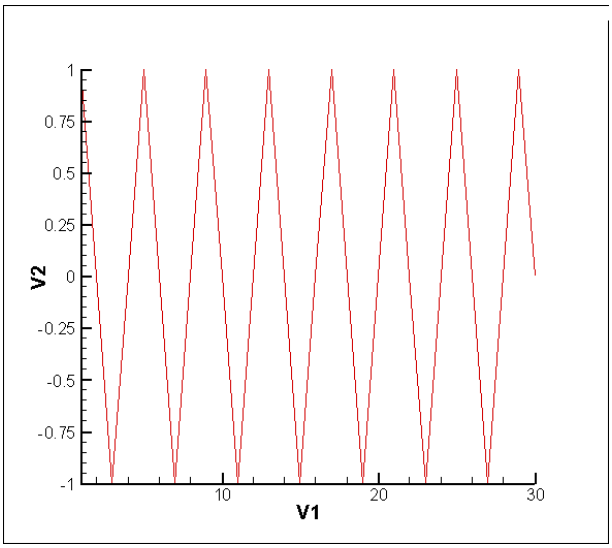


FIGURE 5.3 – L'allure du signal message avant cryptage (le signal message a crypté)

les équations d'états sont données par :

$$\begin{cases} \dot{x}_2 = ax_2 + y_2z_2 + u \\ \dot{y}_2 = -by_2 + x_2z_2 \\ \dot{z}_2 = -cz_2 + x_2y_2 \end{cases} \tag{5.5}$$

où : u est le contrôle d'accouplement choisisser par :

$$u = -y_1z_1 + y_2z_2 - (a+1)(x_2 - x_1)$$

Avec les paramètres donnés dans la référence [14], à l'instant $t = 5s$, on a trouvé que l'erreur de synchronisation entre les systèmes (5.1) et (5.5) tendant vers 0. Ainsi on va considérer par la suite que le temps de synchronisation Ts est aux environs de $15s$.

Dans notre simulation, on a utilisé deux oscillateurs chaotiques $G1$ (système maître) et $G2$ (système esclave) pour coder le 1 et le -1 du signal message. Ils sont similaires mais statistiquement différents. Concernant leurs paramètres on a choisi respectivement :

1. pour le système $G1$: $x_1(0) = 0,\ \ y_1(0) = 1,\ \ z_1(0) = 1$
2. pour le système $G2$: $x_2(0) = -5,6,\ \ y_2(0) = 13,6,\ \ z_2(0) = -12,5$

Au niveau de la réception, les blocs de synchronisation $G1$ et $G2$ dont les équations d'états sont celles du système (5.1) et (5.5) respectivement, les paramètres sont identiques aux systèmes $G1$ et $G2$. À la sortie du modulateur CSK, le signal $S(t)$ est représenté sur la figure (5.4).

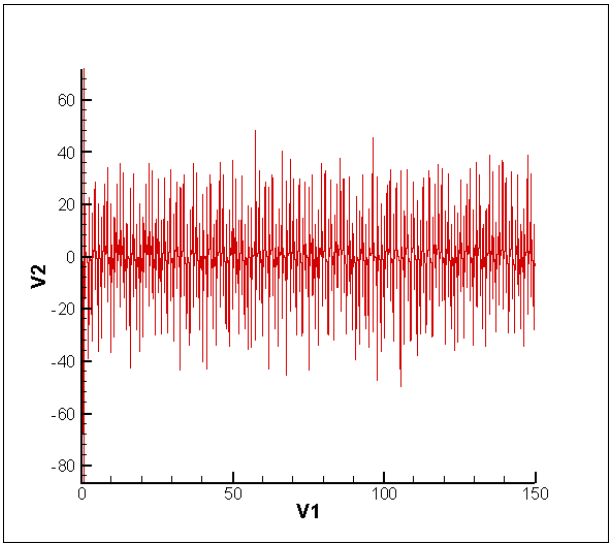


FIGURE 5.4 – L'allure du signal message après cryptage par CSK en utilisant le modèle de Four-scroll (le signal message crypté par CSK)

Modulateur CSK en utilisant le modèle de Lorenz

Par la même idée du modulateur CSK, le signal message sera chiffré. Dans ce cas, le temps de synchronisation sera réglé en continu à 15 secondes de plus que le temps de synchronisation (4 secondes dans notre cas [23]) pour la probabilité d'apparition de 1 et -1, car la vitesse du signal message (Que nous allons le masquer) est limité par le moment de la synchronisation. Il a été vérifié [23] que le système (5.2), considéré comme système maître, se synchronise identiquement avec un système esclave dont

les équations d'état sont données par :

$$\begin{cases} \dot{x}_2 = a(y_2 - x_2) + C_1 \\ \dot{y}_2 = bx_2 - x_2 z_2 - y_2 + C_2 \\ \dot{z}_2 = x_2 y_1 - cz_2 + C_3 \end{cases} \tag{5.6}$$

Où : C_1, C_2 et C_3 sont trois fonctions du contrôle d'accouplements. Avec le choix approprié de C_1, C_2 et C_3 et avec les paramètres donnés dans la référence [23] , au temps $t = 4s$ seconde, on a constaté que l'erreur de synchronisation entre les systèmes (5.2) et (5.6) tendant vers 0 seconde. Nous allons donc considérer le temps de synchronisation T second environ de 15 seconde.

Dans notre simulation, nous avons utilisé deux oscillateurs chaotiques $G1$ (système maître) et $G2$ (système esclave) à codez le signal message $\sin \omega t$. Elles sont similaire mais statistiquement différent. Concernant leurs paramètres ont été choisis respectivement :

1. Système $G1 : x_1(0) = 1,\ \ y_1(0) = 1,\ \ z_1(0) = 0$
2. Système $G2 : x_2(0) = 0,2,\ \ y_2(0) = 0,3,\ \ z_2(0) = 0,1$

À la réception, les blocs de synchronisation G1 et G2 dont les équations d'état sont celles des systèmes (5.2) et (5.6) respectivement, les paramètres sont identiques aux systèmes G1 et G2. À la sortie du modulateur CSK, le signal S (t) est représenté sur la Figure (5.5).

5.3.2 Le démodulateur CSK

Démodulator CSK en utilisant le modèle de Four-scroll

Si on suppose que le signal message crypté $S(t)$ est reçu par le récepteur autorisé, représenté sur la figure (5.4), sans perturbation.

À ce niveau il y'aura alors synchronisation respectivement des deux oscillateurs $G1$ ou $G2$ avec le signal $S(t)$ reçu, selon que la valeur du signal message mj est égale à

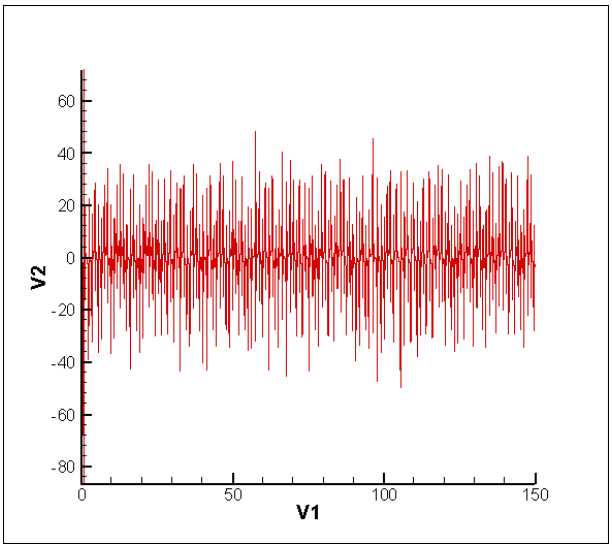


FIGURE 5.5 – L'allure du signal message après cryptage en utilsant le modèle de Lorenz (le signal message crypté par CSK)

1 ou -1 . Ce résultat est identifié par l'annulation de signal erreur de synchronisation e_1, comme il est représenté sur la figure (5.6).

À partir de cette erreur de synchronisation, la prise de décision pour récupérer le signal message sera alors faite dans le bloc de décision.

La procédure de traitement au niveau de ce bloc peut être résumée comme suit :

1. Quelque soit le signe de l'erreur de la synchronisation identique entre deux signaux chaotiques, la règle de base est qu'une erreur nulle implique la synchronisation. La figure (5.6) représente la détection des zones de synchronisation de $G1$ et $G1$, et les signaux de la fonction $\sin \omega t$ enveloppant des porteuses chaotiques. Pour détecter ces enveloppes, on a procédé comme pour la démodulation classique, par écrêtage de notre signal dans l'intervalle $[-10, 10]$, par l'étage limiteur. On aura ainsi le signal représenté sur la figure (5.7).
2. Ensuite ces signaux seront filtrés par des filtres passe bas, pour atténuer les porteuses chaotiques et maintenir les enveloppes de $\sin \omega t$. On a choisi pour

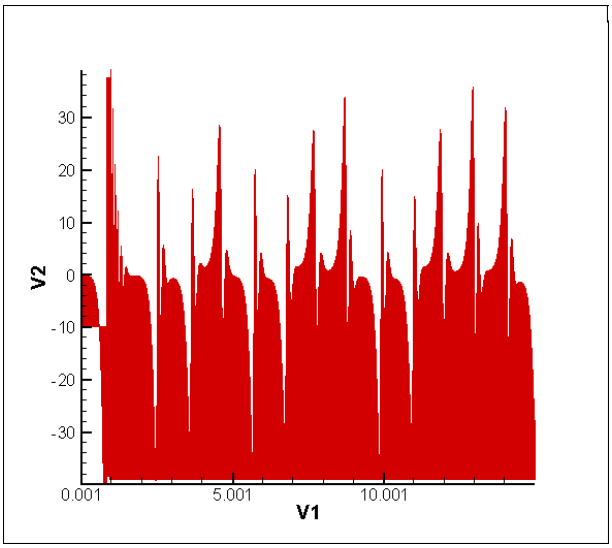


FIGURE 5.6 – Détection des zones de synchronisation de $G1$ et $G1$ pour le modèle de Four-scroll.

cela des filtres passe bas. Le signal filtré est représenté sur la figure (5.8).

3. Les signaux de la fonction $\sin \omega t$ résultants de signal erreur, seront tirés de signal représenté sur la figure (5.9), par seuillage et comparaison. On a utilisé pour cela l'étage comparateur réalisant l'opération suivante :

$$\begin{cases} 1 \Rightarrow signal \geq 0 \\ -1 \Rightarrow signal < 0 \end{cases} \tag{5.7}$$

On aura alors le signal représenté sur la figure (5.9)

4. Pour reconstituer le signal original, on a procédé par la détection des fronts montants de signal erreur représenté sur la figure (5.10) par l'étages détecteurs des fronts montants. Ce signal devient comme représenté sur la figure (5.10).

5. En comparant le signal représenté sur la figure (5.10) avec le signal message mj d'origine, représenté sur la figure (5.3), on a remarqué que ce signal décalé un peut avec le signal de la fonction $\sin \omega t$ issu de signal erreur. Alors pour

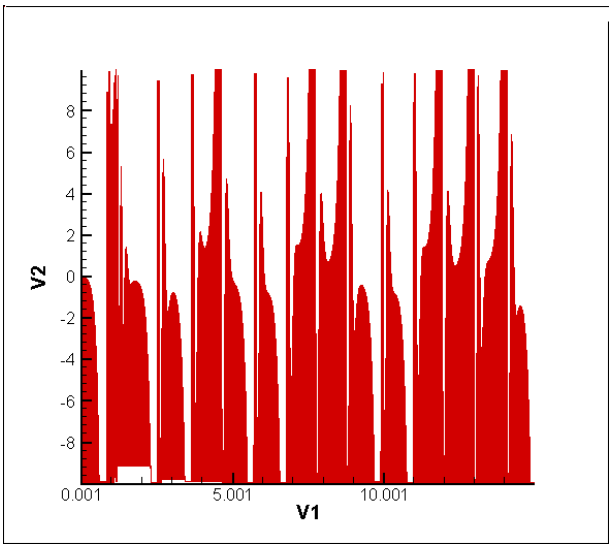


FIGURE 5.7 – Valeurs limitées de signal erreur de synchronisation pour le modèle de Four-scroll.

récupérer le signal message d'origine, ce signal sera injecté dans une bascule T.

Les figures (5.11) représentent le signal reconstruit par l'opération de décryptage en utilisant le modèle de Four-scroll et le signal original respectivement. Ils sont donc identiques.

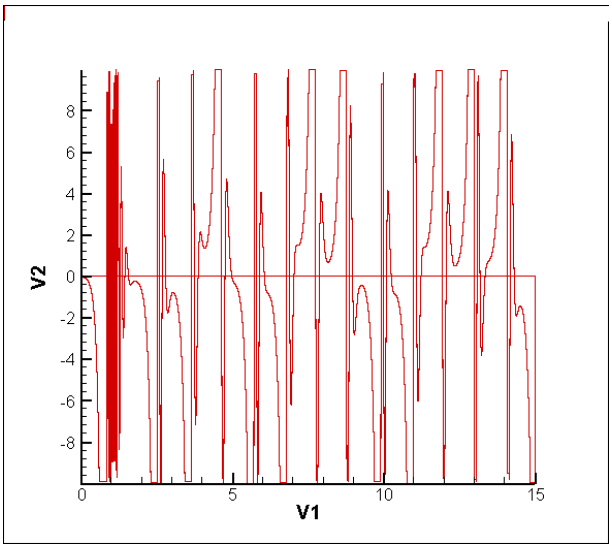


FIGURE 5.8 – Filtrage du signal erreur pour le modèle de Four-scroll.

Démodulator CSK en utilisant le modèle de Lorenz

Maintenant, nous décrypterons le même signal message que nous avons masqué en utilisant le modèle de Lorenz selon les mêmes étapes du démodulateur CSK. Tout d'abord, quel que soit le signe d'erreur de la synchronisation identique entre les deux signaux chaotiques, la règle de base est l'erreur zéro implique la synchronisation. La figure (5.12) Représente la détection des zones de synchronisation de $G1$ et $G2$, et les signaux de la fonction $\sin \omega t$ qui enveloppent les porteuse chaotiques. Pour détecter ces enveloppes, nous procédons comme dans la démodulation classique, en coupant notre signal dans l'intervalle $[-10, 10]$ par la phase limite comme nous l'avons fait sur le modèle de Four-scroll. Cela fournira le signal représenté sur la Figure (5.12).

Ensuite, ces signaux sont filtrés par des filtres passe-bas, pour atténuer les porteuse chaotiques et garder les enveloppes de $\sin \omega t$. Les signaux de la fonction $\sin \omega t$ résultats du signal erreur, seront montrés dans la Figure (5.13) par filtrage, seuillage et comparaison. Nous le faisons comme nous l'avons fait dans le modèle de Four-scroll.

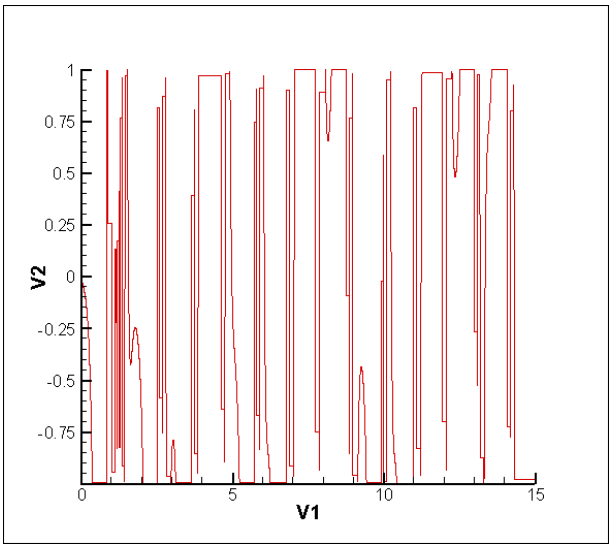


FIGURE 5.9 – Seuillage et comparaison de signal erreur pour le modèle de Four-scroll.

Nous aurons le signal représenté sur la Figure (5.13).

Pour reconstruire le signal d'origine, nous avons effectué la détection des front montant du signal erreur comme indiqué sur la figure (5.14) par l'étage des front montant. Ce signal devient tel qu'illustré à la Figure (5.14).

En comparant le signal représenté sur la Figure (5.14) avec le signal message original mj présenté dans la Figure (5.3), nous avons noté qu'il y avait une petite différence entre eux. Donc, pour récupérer le signal message original, nous l'aurons injecté dans une bascule T. Les figures (5.15) représentent le signal reconstruit par l'opération de décryptage en utilisant le modèle de Lorenz et le signal original respectivement. Ils sont donc identiques.

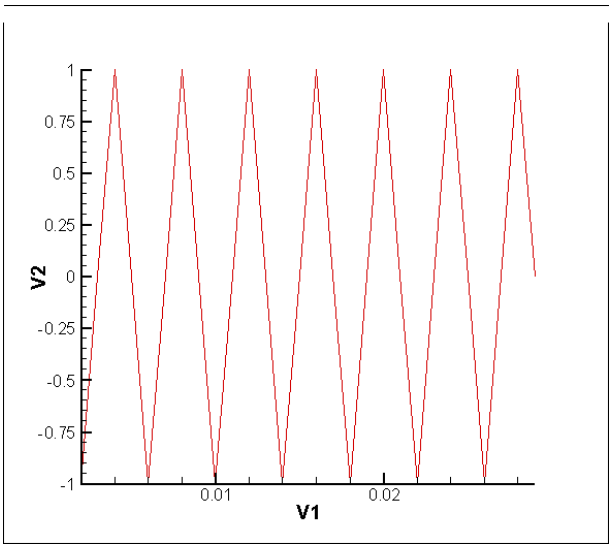


FIGURE 5.10 – Detection des front montant pour le modèle de Four-scroll.

5.4 Discussion des résultats

Grâce à cette étude analytique du cryptosystème chaotique de la fonction $\sin \omega t$ en utilisant la méthode CSK pour deux systèmes séparément, le système de Lorenz et le système de Four-scroll, on a trouvé que nous pouvons chiffrer le message fonctionel en utilisant les deux systèmes. Pour le cryptage, nous avons obtenu presque les mêmes résultats, mais pour le décryptage, il dépendait de la vitesse de la synchronisation de chaque système. De même que la vitesse du décryptage dans le système de Lorenz était légèrement plus rapide que la vitesse de décryptage dans le système de Four-scroll. Sur cette base, nous concluons que le système de cryptage et de décryptage dépendait de la vitesse de synchronisation. Cependant, dans notre étude analytique, le processus de cryptage et de décryptage utilisant la méthode CSK dans les deux cas a été complètement réussi et nous avons obtenu de très bons résultats.

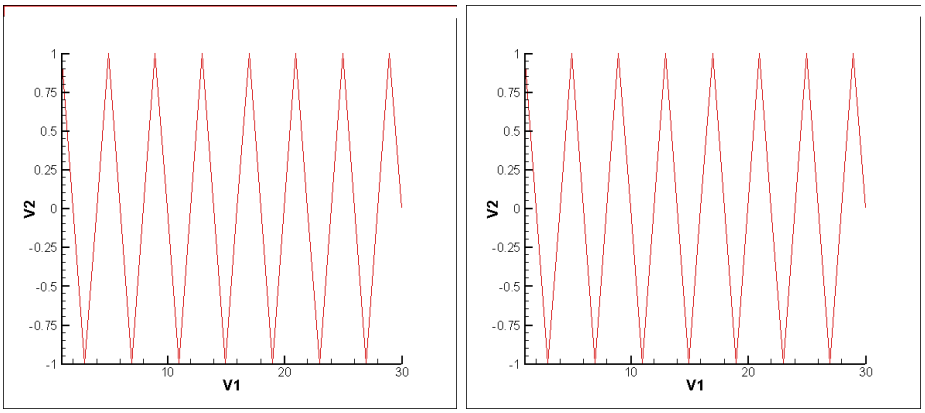


FIGURE 5.11 – Message après décryptage pour le mdèle de Four-scroll à gauche et message original à droite.

5.5 Conclusion

Nous avons situé tout d'abord les problèmes rencontrés dans les crypto systèmes utilisés actuellement. Une accentuation a été faite sur les limites de sécurité de cet cryptos systèmes. Nous avons remarqué à travers notre recherche bibliographique sur les cryptosystèmes les plus utilisés actuellement, et que cette sécurité est calculatoire, car elle est fondée sur les calculs algébriques. C'est l'une des raisons qui ont déclenché la nécessité de chercher d'alternatif, dont l'usage du chaos sujet de notre travail, est l'une des solutions proposées.

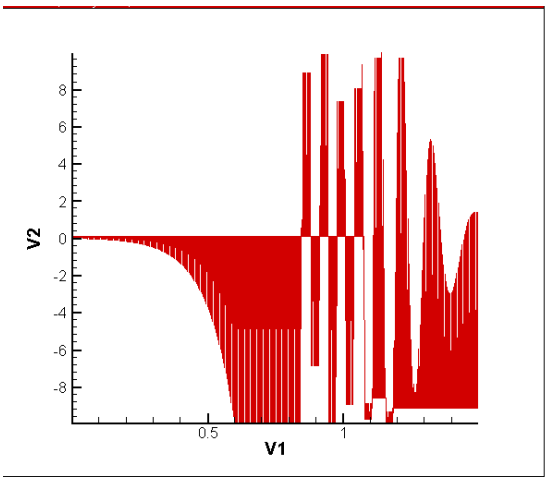


FIGURE 5.12 – Détection et valeurs limité des zones de synchronisation de $G1$ et $G2$ pour le modèle de Lorenz.

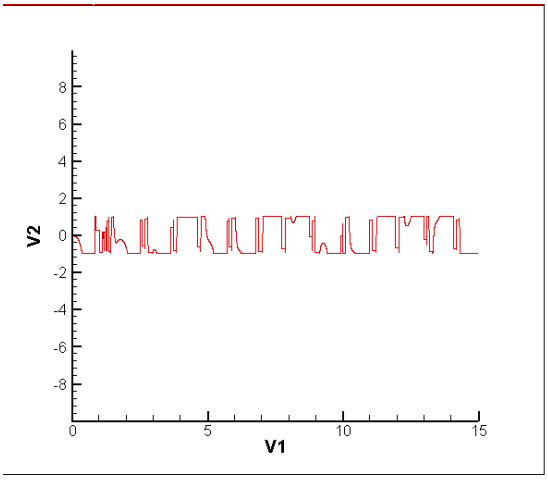


FIGURE 5.13 – Filtrage, seuillage et comparison de signal erreur pour le modèle de Lorenz.

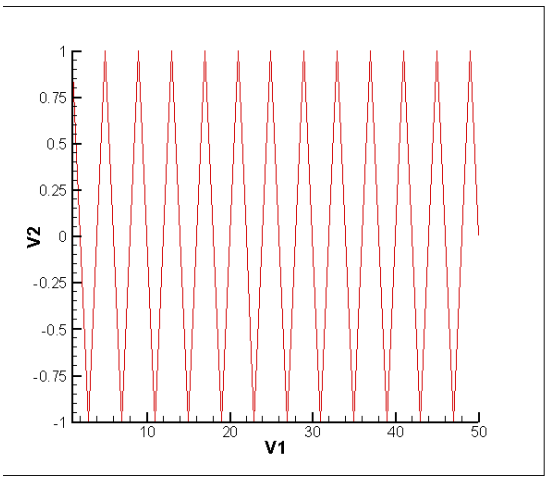


FIGURE 5.14 – Detection des front montant pour le modèle de Lorenz.

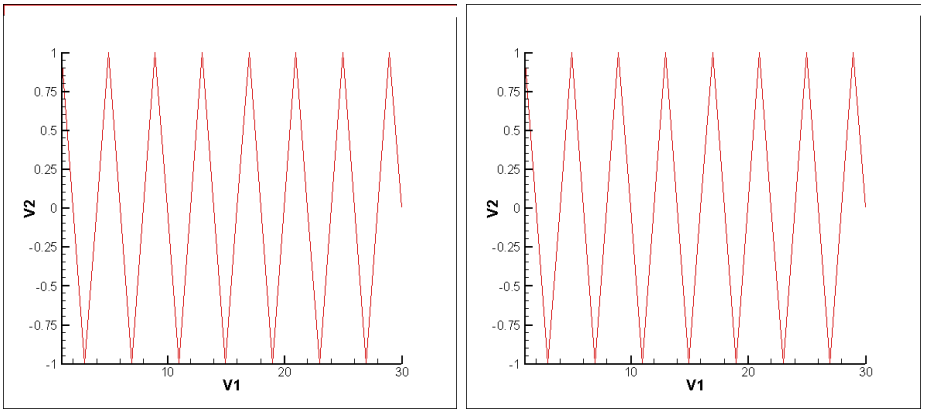


FIGURE 5.15 – Message après décryptage pour le modèle de Lorenz à droite et le message original à gauche.

Chapitre 6

Conclusion Générale

Nous avons situé tout d'abord les problèmes rencontrés dans les crypto systèmes utilisés actuellement. Une accentuation a été faite sur les limites de sécurité de ces cryptos systèmes. Nous avons remarqué à travers notre recherche bibliographique sur les cryptosystèmes les plus utilisés actuellement tels que le AES, DES et le RAS, que cette sécurité est calculatoire, car elle est fondée sur les calculs algébriques. C'est l'une des raisons qui ont déclenché, la nécessité de chercher d'alternatif, dont l'usage du chaos sujet de notre travail, est l'une des solutions proposées.

A ce niveau, notre travail a été débuté par l'exploration du phénomène chaotique en le simulant par ordinateur. Nous avons ainsi vérifié la sensibilité des systèmes chaotiques même aux faibles variations des conditions initiales, dépisté la route vers le chaos d'un système dynamique en traçant son diagramme de bifurcation, identifié le chaos dans un système dynamique par le calcul de ses exposants de Lyapunov et représenté graphiquement le comportement de quelques systèmes chaotiques célèbres dans le domaine temporel et l'espace des phases.

La découverte en 1990 de Pecora et Carroll sur la synchronisation du chaos a été un déclic, pour la possibilité de l'utiliser dans la sécurisation de la communica-

tion. D'où vient l'objectif de la deuxième phase de notre travail. Dans des conditions idéales (en négligeant la disparité des paramètres et perturbation d'accouplement entre le système maître et le système esclave) de bons résultats ont été obtenus par le test de la synchronisation du chaos en utilisant trois techniques (l'approche de Pécorra et Carroll, synchronisation généralisée et la synchronisation retardé). On note que la robustesse de ces techniques vis-à-vis de la disparité des paramètres et les perturbations d'accouplement est limitée.

La troisième est la dernière phase de notre travail consiste dans l'étude de l'usage du chaos pour sécuriser les données. Deux techniques ont été simulées et analysées :
1.Le masquage par addition est la première méthode étudiée. Les résultats obtenus dans cette méthode montrent une mauvaise reconstitution du signal message à la réception même avec des conditions idéales de fonctionnement.
2.Le masquage par décalage chaotique est la deuxième méthode étudiée. On note dans cette méthode, une similarité parfaite entre le signal message d'origine et le signal reconstitué au niveau de la réception dans un fonctionnement idéal. En revanche, cette similarité diminue avec un temps symbole inférieur au temps de synchronisation, la disparité des paramètres et l'augmentation du bruit du canal. Concernant la sécurité de cette technique, elle peut être augmentée par mixage avec les techniques de cryptographie classiques.
Plusieurs perspectives peuvent être envisagées à la suite de ce travail ,à savoir :

1. Etude et estimation de toutes les techniques de synchronisation du chaos et la poursuite de la recherche dans ce domaine.
2. Etude et estimation de toutes les techniques de cryptage par chaos et la poursuite de la recherche dans ce domaine.
3. Usage du chaos pour sécuriser la transmission par ondes radios.

Bibliographie

[1] A. Wolf, J. B. Swift, H. L. Swinney, et J. A. Vastano. "Determining lyapunov exponents from a time series" Physica D, vol .16 ,pp .285 ?317, 1985 .

[2] E. Cherrier . Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires .Thèse de doctorat , institut national polytechnique de Lorraine , 2006 .

[3] G. Alvarez, L. Hernández, J. Muñoz, F. Montoya et S. Li. "Security analysis of communication system based on the synchronization of different order chaotic systems" Physics Letters A, vol. 345, pp. 245-250, 2005.

[4] G. Kolumban, M. P. Kennedy and L. O. Chua. "The role of synchronization in digital communications using chaos - part III Performance Bounds for Correlation Receivers "IEEE Transactions on Circuits and Systems I : Fundamental theory and application, vol. 47, pp.1673-1683 , 2000.

[5] H. Dedieu, M.P. Kennedy et M. Hasler. "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, pp .634-642, 1993.

[6] H. D. I. Abarbanel, N.F. Rulkov, et Mikhail M. Sushchik "Generalized synchronization of chaos : The auxiliary system approach "Physical review E, vol. 53 ,pp.4528-4535, 1995.

[7] "http/ : www.umi2958.eu/spip.php ?article132 et lang=fr"

[8] K.M. Cuomo, A.V. Oppenheim et S.H. Isabelle " Spread spectrum modulation and Signal masking using synchronized chaotic systems" MIT Tech. Rep, vol. 570, 1992.

[9] K.M. Cuomo, A.V. Oppenheim et S.H. Strogatz. "Synchronization of Lorenz based chaotic circuits with applications to communications" IEEE Transactions on Circuits and Systems II, vol. 40, pp. 626-633, 1993.

[10] Lü J, Chen G, Chen D Z (2004). "A new chaotic system and beyond : The generalized Lorenz-like system", Internat. J. Bifur. Chaos 14 (5) : 1507-1537.

[11] Lorenz E "Deterministic nonperiodic flow". J. Atmos. Sci., 20, 130-141.

[12] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems", Physical Review Letters, vol. 64, 1990.

[13] Liu W, Chen G (2004). "Can a Three-Dimensional Smooth Autonomous Quadratic Chaotic System Generate a Single Four-Scroll Attractor ?", Inte. J. Bifur. Chaos 14 (4) : 1395-1403.

[14] Mohammad Ali Khan "Synchronization of different 3D chaotic systems by generalized active control", ISSN 1746-7659, England, UK Journal of Information and Computing Science Vol. 7, No. 4, 2012, pp. 272-283.

[15] Mihai Bogdan Luca. « Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information ». Thèse doctorat 2006.

[16] N.F. Rulkov, M.M.Sushchik, L.S.Tsimring et H.D.I. Abarbanel "Generalized synchronization of chaos in directionally coupled chaotic systems " Physical Review E, vol. 51, pp 980-994, 1995.

[17] R. Dumont .Introduction a la cryptographie et a la sécurité informatique. Note de cours, université de Liége, 2006-2007.

[18] S. Boccaletti ,J. Kurths, G. Osipovd et D.L. Valladares, C.S. Zhou " The synchronization of chaotic systems" Physics Reports,vol. 366, pp.1-101,2002.

[19] Serge Dos Santos,"Synchronisation des systèmes : application aux fluctuations de base fréquence des oscilateurs ultra-stable", Thèse de doctorat.

[20] Tigan. GH "A note on chaos synchronization between two differential three-dimensional systems",Differential Geometry - Dynamical Systems, Vol.7, 2005, pp. 105-110.

[21] T. Yang, L.B. Yang et C.-M. Yang. "Cryptanalyzing chaotic secure communications using return maps" Physics Letters A, vol. 245, pp. 495-510, 1998.

[22] X. Bavard. Numérisation du chaos et applications aux systèmes de communication sécurisés par chaos en longueur d'onde. Thèse de doctorat, Université de Franche -Comté, 2004.

[23] Z. L. Zhu, S. Li et H. Yu " A new approach to generalized chaos synchronization based on the stability of the error System " Kybernetika, Vol. 44. No. 4, pp .492-500, 2008 .