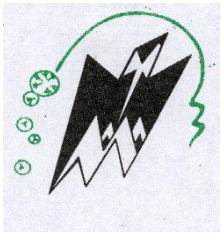
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE



UNIVERSITE MOULOUD MAMMERI TIZI-OUZOU

FACULTE DU GENIE ELECTRIQUE ET INFORMATIQUE

DEPARTEMENT D'AUTOMATIQUE

MEMOIRE DE MAGISTER

Spécialité : Automatique

Option : Automatique des Systèmes Continus et Productique

Thème :

Etude et réalisation d'un système sécurisé à base de systèmes chaotiques

Présenté par :

M^{elle} MEGHERBI OUERDIA

Soutenu le 10/10/2013 devant le jury composé de :

Mr KARA Redouane	UMMTO	Maître de conférences Classe A	Président
Mr DJENNOUNE Said	UMMTO	Professeur	Rapporteur
Mr LAHDIR Mourad	UMMTO	Maître de conférences Classe A	Examinateur
Mr MANSOURI Rachid	UMMTO	Maître de conférences Classe A	Examinateur
Mr HAMICHE Hamid	UMMTO	Maître de conférences Classe B	Examinateur

REMERCIEMENTS

J’exprime mes remerciements les plus sincères à mon encadreur Mr Said Djennoune, professeur à l’université Mouloud Mammeri, sous la direction duquel j’ai eu le plaisir de travailler. Par ses conseils, et sa rigueur scientifique il m’a permis de réaliser ce travail.

Je tiens particulièrement à remercier Mr Hamid Hamiche, Maître de conférences à l’université Mouloud Mammeri, qui par sa persévérance et sa patience, a su me guider dans chacune des étapes lors de mes recherches. Ses conseils, sa disponibilité et ses encouragements m’ont permis de surmonter bien des difficultés et aller de l’avant.

Qu’il accepte ma profonde gratitude.

Je ne peux oublier l’aide permanente et le soutien indéfectible que m’ont apportés mes amis étudiants au sein du laboratoire L2CSP; je les en remercie infiniment.

Mes grands remerciements vont aussi à Mr. Ziani chef du département d’électronique à l’université de Tizi-Ouzou pour son précieux concours logistique en mettant à ma disposition le matériel et l’appareillage de mesure nécessaires pour la réalisation de mon travail.

Je ne manquerai pas de remercier tous les membres du laboratoire L2CSP qui grâce à leurs efforts et leurs expériences, m’ont donné la possibilité de travailler dans un cadre de recherche convivial et riche en connaissances durant ces dernières années.

Je remercie également tous les membres du jury pour m’avoir honorée par leur présence et pour avoir accepté d’évaluer ce travail de mémoire.

Enfin, pour avoir cru en moi et pour m’avoir soutenue toute la durée du mémoire, j’exprime ma profonde gratitude à toute ma famille. Je leur dois en grande partie l’aboutissement de ce travail.

DEDICACE

Je dédie ce travail à la mémoire de ma défunte mère qui en aurait été, j'en suis convaincue, très fière.

SOMMAIRE

TABLE DES FIGURES

INTRODUCTION GENERALE

Depuis l'antiquité, l'homme n'a pas cessé de chercher les différents moyens pour transmettre un message à son correspondant et pouvoir ainsi communiquer avec lui en toute sécurité. Il a fourni, à travers des époques successives, des efforts autant physiques qu'intellectuels pour pouvoir trouver une technique de communication efficace et appropriée.

En effet, les modes de télécommunications sont en évolution continue avec la recherche permanente de meilleurs débits, de facilité d'utilisation, de mobilité améliorée et surtout d'une confidentialité élevée.

La cryptographie a depuis des siècles été une histoire de conflit qui oppose deux camps, un qui cherche à cacher une information et un autre qui essaie de trouver ce qu'on lui cache. Ainsi à chaque fois que le premier trouve un moyen de chiffrer ses messages le second essaie et, avec le temps et les moyens dont il dispose, réussit à trouver la méthode ou « l'astuce » pour le décrypter. La cryptographie ancienne utilisait différents outils pour dissimuler une information ou un texte secret. Certains remplaçaient des mots par des nombres, d'autres mélangeaient, décalaient ou permutaient les lettres, comme dans la substitution alphabétique inverse, pour rendre la lecture du message difficile voire impossible [3].

La cryptographie actuelle cherche à transformer de façon mathématique et algorithmique un message clair pour obtenir un autre chiffré et qui, à première vue, semble aléatoire. Plus l'inversion de la transformation est difficile plus la sécurité est élevée et vice versa. On cherche alors un phénomène d'apparence aléatoire mais qui est déterministe à l'origine pour le masquage d'information.

Il existe plusieurs systèmes présentant ce comportement, ils sont dits chaotiques, ils sont régis par des lois déterministes, dépendent d'un ou de plusieurs paramètres et leur évolution dans le temps est imprévisible. L'étude de tels systèmes est liée à la théorie du chaos qui a connu un grand essor à partir de 1960 grâce aux travaux de plusieurs chercheurs notamment ceux de Lorenz et à la découverte de nouveaux outils de calculs [37].

La cryptographie chaotique est ainsi née par inclusion du chaos dans les télécommunications et systèmes de transmission. L'idée consiste à noyer un message dans un signal chaotique pour faire face aux éventuelles tentatives de piratage.

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

La synchronisation des systèmes chaotiques est une approche intéressante pour résoudre ce problème. Introduite en 1990 par les travaux de Pecora et Caroll [50] [51], cette technique permet de reconstruire les états de l'émetteur à partir du signal transmis. Différentes approches ont été proposées depuis pour améliorer ce processus et réduire l'erreur entre les états de l'émetteur et ceux restaurés au niveau du récepteur [33][41][60].

En 1997, H.Nijmeijer et I.Mareels [45] [46] ont montré que la synchronisation unidirectionnelle des systèmes chaotiques peut être considérée comme un problème de synthèse d'observateur.Différents types d'observateurs sont alors proposés pour les systèmes chaotiques. Ces observateurs peuvent être destinés uniquement à reconstruire les états de l'émetteur ou servir à reconstruire les états de l'émetteur et récupérer l'information. Le fonctionnement correct de ces observateurs dépend de plusieurs conditions : la condition d'observabilité pour retrouver les états du système, la condition de recouvrement de l'observabilité pour retrouver les états du système et l'information noyée dans le système et la condition d'identifiabilité des paramètres qui représentent les clés de codage [15].

Ce travail de mémoire de magister consiste à réaliser un système de transmission sécurisée à base du chaos, il repose d'une part sur la synchronisation chaotique et d'une autre sur le masquage de l'information secrète. Ce système se compose de deux oscillateurs chaotiques liés par un canal de transmission publique, un message sera crypté puis envoyé à partir de l'oscillateur émetteur. L'objectif est de récupérer ce signal utile en utilisant un observateur impulsif de l'oscillateur émetteur.

Ce mémoire est organisé comme suit :

Le premier chapitre sera un rappel sur les systèmes dynamiques en général et chaotiques en particulier.Il énoncera également quelques concepts et définitions introductifs à la théorie du chaos.

Le second chapitre expliquera plus en détails les motivations et techniques de synchronisation des systèmes chaotiques, et l'apport de cette initiative dans le cadre de notre travail. Il cite également les approches envisagées pour inclure le chaos dans la transmission sécurisée.

Le troisième chapitre est consacré à une méthode de synchronisation récente et mentionnée dans le second chapitre : il s'agit de la synchronisation impulsive. Le principe et les raisons du choix de la méthode seront présentés tout au long de cette partie du mémoire.

Le quatrième et dernier chapitre décrit le système de transmission réalisé.Il précisera le fonctionnement et le rôle de chaque module et composante du système.Les étapes de réalisation et les résultats de simulation et d'expérimentation seront énoncés et illustrés à la fin de ce chapitre.

Ce travail sera finalisé par une conclusion et synthèse des différentes phases d'étude et de développement. Elle permettra de qualifier les modèles théoriques mis en œuvre et d'envisager d'autres perspectives plus intéressantes pour améliorer le système présenté et augmenter ses performances.

CHAPITRE 1 : GENERALITES SUR LES SYSTEMES CHAOTIQUES

1.1 INTRODUCTION

Depuis longtemps, le chaos était synonyme de désordre et de confusion. Il s'opposait à l'ordre et devait être évité. La science était caractérisée par le déterminisme, la prévisibilité et la réversibilité. Poincaré fut l'un des premiers à entrevoir la théorie du chaos [8]. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes.

Le terme "chaos" définit un état particulier d'un système dont le comportement ne se répète jamais qui est très sensible aux conditions initiales, et imprédictible à long terme. Des chercheurs d'horizons divers ont alors commencé à s'intéresser à ce comportement. Ils ont cherché à répondre à des questions telles que : Les arythmies cardiaques ou les variations d'une population animale obéissent-elles à des règles? Les mouvements commerciaux ou les marchés financiers peuvent-ils s'expliquer?

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

L'objectif de ce chapitre est de donner quelques notions élémentaires sur les systèmes dynamiques afin de mieux appréhender ce qu'est le chaos : ses apparitions dans un système et la manière de le quantifier.

1.2 LES SYSTEMES DYNAMIQUES

Un système dynamique est une structure qui évolue au cours du temps de façon à la fois :

– Causale, où son avenir ne dépend que de phénomènes du passé ou du présent
– Déterministe, c'est-à-dire qu'à partir d'une « condition initiale » donnée à l'instant « présent» va correspondre à chaque instant ultérieur un et un seul état « futur» possible.

L'évolution déterministe du système dynamique peut alors se modéliser de deux façons distinctes

- Une évolution continue dans le temps, représentée par une équation différentielle ordinaire.
- Une évolution discrète dans le temps, l'étude théorique de ces modèles discrets est fondamentale, car elle permet de mettre en évidence des résultats importants, qui se généralisent souvent aux évolutions dynamiques continues. Elle est représentée par le modèle général des équations aux différences finies

1.2.1 Temps continu

$$\dot{x}(t) = F(x(t), t) \tag{1.1}$$

Où$F : \mathbb{R}^n \times \mathbb{R}^+ \rightarrow \mathbb{R}^n$désigne la dynamique du système
Si on associe à cette dynamique un état initial

$$x_0 = x(t_0)$$

Pour chaque couple choisi, ($\mathbf{x}_0$, t_0) on peut identifier une solution unique :

$\Phi(.; x_0, t_0) : \mathbb{R}^+ \rightarrow \mathbb{R}^n$ telle que :

$$\Phi_F(t_0; x_0, t_0) = x_0 \; et \; \dot{\Phi}_F(t; x_0, t_0) = F(\Phi_F(t; x_0, t_0), t) \tag{1.2}$$

Cette solution appelée souvent trajectoire, fournit les états successifs occupés par le système à chaque instant t.

1.2.2 Temps discret

Un système dynamique dans le cas discret est représenté par une équation aux différences finies sous la forme :

$$x(k+1) = G(x(k), k) \tag{1.3}$$

$G : \mathbb{R}^n \text{ x } \mathbb{Z}^+ \rightarrow \mathbb{R}^n$ Indique la dynamique du système en temps discret.

On peut également identifier pour chaque couple (x_0, k_0) une solution unique

$$\Phi_G(.; x_0, k_0): \mathbb{Z}^+ \rightarrow \mathbb{R}^n$$

telle que :

$$\Phi_G(k_0; x_0, k_0) = x_0 \text{et} \Phi_G(k+1; x_0, k_0) = G(\Phi_G(k; x_0, k_0), k) \tag{1.4}$$

1.3 DEFINITION DU CHAOS

Le chaos tel que le scientifique le comprend ne signifie pas l'absence d'ordre; il se rattache plutôt à une notion d'imprévisibilité, d'impossibilité de prévoir une évolution à long terme du fait que l'état final dépend de manière si sensible de l'état initial

.

On appelle donc un système dynamique chaotique, un système qui dépend de plusieurs paramètres et caractérisés par une extrême sensibilité aux conditions initiales. Ils ne sont pas déterminés ou modélisés par des systèmes d'équations linéaires ni par les lois de la mécanique classique ; pourtant, ils ne sont pas nécessairement aléatoires, relevant du seul calcul des probabilités.

L'exemple suivant illustre les propriétés d'un système chaotique. Soit le modèle chaotique donné par Otto de Rössler.

$$\begin{cases} \dot{x}_1 = -x_2 - x_3 \\ \dot{x}_2 = x_1 + ax_2 + 0.01x_1 \ln(x_3) \\ \dot{x}_3 = c + x_3(x_1 - b) \end{cases} \quad (1.5)$$

Où (x_1, x_2, x_3) est le vecteur d'état et a ,b, c sont les paramètres du système.
Le système de Rössler montre un comportement chaotique pour $a = 0.2$, $b = 5.7$, $c = 0.2$, avec les conditions initiales $x_1(0) = 0.01$, $x_2(0) = 0.01$ et $x_3(0) = 0.01$

Les définitions et propriétés suivantes permettent de comprendre qualitativement les points marquants des systèmes chaotiques.

1.3.1 La non-linéarité

Un système chaotique est un système dynamique non linéaire. Un système linéaire ne peut pas être chaotique.

1.3.2 Le déterminisme

La notion de déterminisme signifie la capacité de « prédire » le futur d'un phénomène à partir d'un évènement passé ou présent. L'évolution irrégulière du comportement d'un système chaotique est due aux non linéarités

Dans les phénomènes aléatoires, il est absolument impossible de prévoir la trajectoire d'une quelconque particule. À l'opposé, un système chaotique a des règles fondamentales déterministes et non probabilistes.

1.3.3 L'aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires. La figure suivante illustre l'aspect aléatoire du système de Rössler.

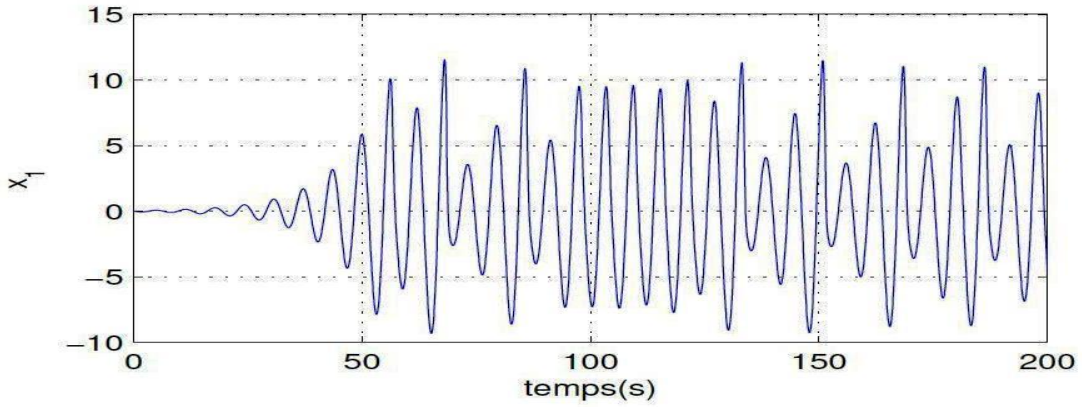


Fig. 1. 1 Etat chaotique $\boldsymbol{x_1}$ du système de Rössler

1.3.4 Sensibilité aux conditions initiales

Certains phénomènes dynamiques non linéaires sont si sensibles aux conditions initiales que, même s'ils sont régis par des lois rigoureuses et parfaitement déterministes, les prédictions exactes sont impossibles. Comme la plupart des phénomènes sont non linéaires, on comprend alors l'importance de la découverte de Lorenz [37].

Une autre propriété des phénomènes chaotiques est qu'ils sont très sensibles aux perturbations. L'un des premiers chercheurs à s'en être aperçu fut Edward Lorenz qui s'intéressait à la météorologie et par conséquent aux mouvements turbulents d'un fluide comme l'atmosphère. Lorenz venait de découvrir que dans des systèmes non linéaires, d'infimes différences dans les conditions initiales engendraient à la longue des trajectoires totalement différentes. Il a illustré ce fait par *l'effet papillon*. Le battement d'ailes d'un papillon aujourd'hui à Pekin engendrerait une tempête le mois prochain à new York [37].

Il est clair que la moindre erreur ou imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction sur l'évolution à long terme du système.

Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant des taux de divergence des trajectoires. Ceci est illustré par la figure 1.2 :

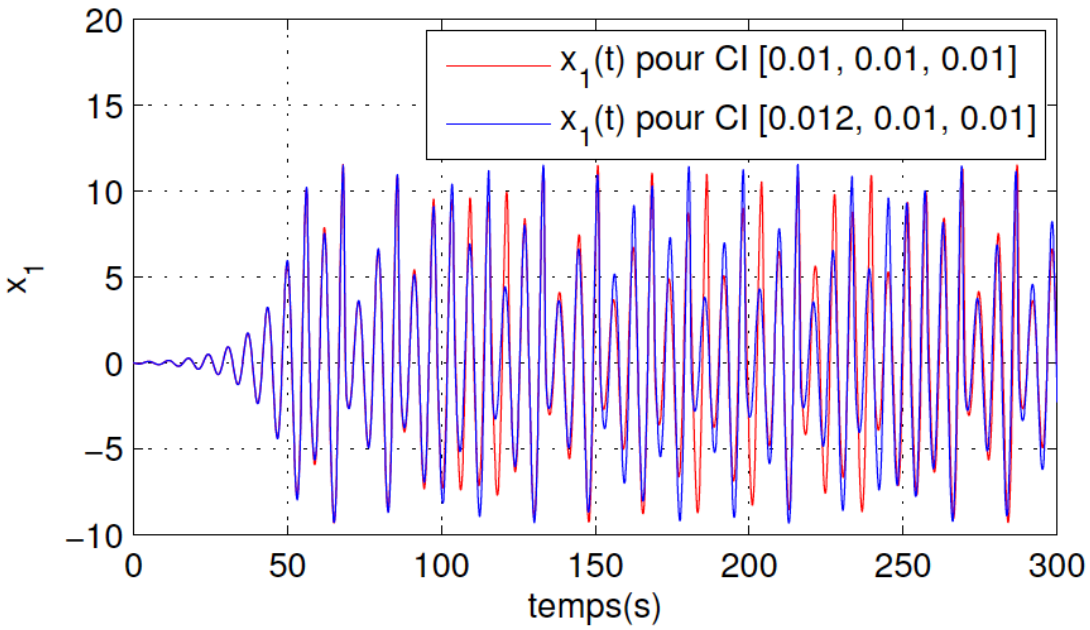


Fig. 1. 2 Illustration de la propriété de sensibilité aux conditions initiales sur l'état $\boldsymbol{x_1}$

1.3.5 Attracteur étrange

Un attracteur est un objet géométrique vers lequel tendent toutes les trajectoires de l'espace des phases, c'est-à-dire, une situation ou un ensemble de situations vers lesquelles évolue un système, quelles que soient ses conditions initiales.

Dans un espace des phases à deux dimensions, les attracteurs sont soit des points, soit des cycles limites.

Pour tous les attracteurs réguliers, c'est-à-dire pour tous les systèmes non chaotiques, des trajectoires qui partent de "points" proches l'un de l'autre dans l'espace de phase restent indéfiniment voisines. On sait donc prévoir l'évolution de ces systèmes, à partir d'une situation connue.

Les systèmes à deux variables ne peuvent pas conduire à des mouvements chaotiques : il suffit de rajouter une troisième variable pour que de tels systèmes, dans certaines conditions, deviennent instables. Sous-adjacent dans le chaos déterministe, cet objet particulier possède une structure fractale.

La figure 1.3 illustre l'attracteur chaotique du système de Rössler.

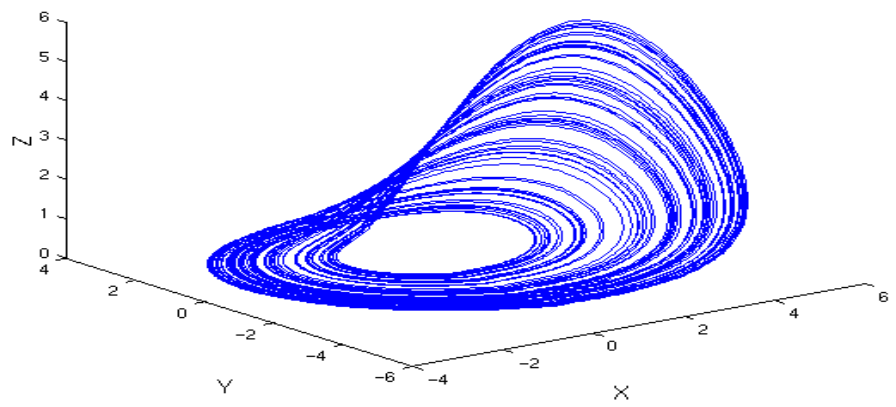


Fig. 1. 3 Attracteur étrange de Rössler

L'attracteur chaotique dit aussi étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. En effet, les trajectoires des points divergent (puisque, par définition deux point ne peuvent avoir la même évolution), mais comme l'attracteur a des dimensions finies, il doit se replier sur lui-même.

Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases. Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges ou chaotiques.

L'objet géométrique observé dans la figure 1.3 est relativement complexe et dégage la richesse d'informations que contient le système. Un attracteur chaotique possède notamment la propriété remarquable suivante : la trajectoire ne repasse jamais par un même état. Ce qui signifie, entre autres, que cette trajectoire passe par une infinité d'états.

Il est à noter que pour observer les trajectoires d'un attracteur, il est parfois intéressant de réduire la dimension *d* de l'espace de phases.

La section de Poincaré est un hyperplan Σ de dimension *d-1* qui transforme la trajectoire continue en une succession de points de passages discontinus à travers la section (figure 1.4).

Cette section peut être considérée comme une transformation du système en temps continu en un système en temps discret.

Le principe consiste à se ramener à une étude dans R^2 par intersection de trajectoire dans $\mathbb{R}^n$.

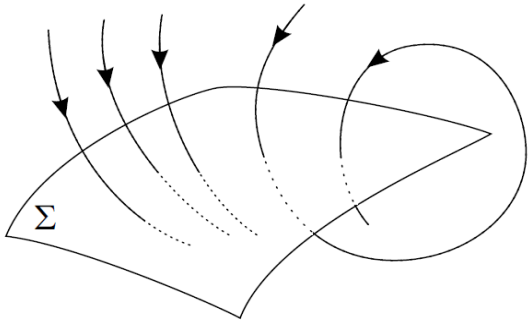


Fig. 1. 4 Section de Poincaré

1.3.6 Les exposants de Lyapunov

L'évolution chaotique est difficile à appréhender car la divergence des trajectoires sur l'attracteur est rapide. Pour cette raison on essaie si c'est possible de mesurer sinon d'estimer la vitesse de divergence ou de convergence. Cette vitesse est donnée par l'exposant de Lyapunov qui caractérise le taux de séparation de deux trajectoires très proches [43] [62].

Soit $f: \mathbb{R} \to \mathbb{R}$ une fonction de classe C^1. Pour chaque point x_0 on définit un exposant de Lyapunov $\lambda(x_0)$ comme suit :

$$\lambda(x_0) = \lim_{n\to\infty} \sup \frac{1}{n} \log(|(f^n)'(x_0)|) = \lim_{n\to\infty} \sup \frac{1}{n} \sum_{j=0}^{n-1} \log(|f'(x_j)|), \qquad (1.6)$$

Avec $x_j = f^j(x_0)$

Donc deux trajectoires dans le plan de phase initialement séparées par un taux Z_1 divergent après un temps $\Delta t = t_2 - t_1$ vers Z_2 tel que :

$$|Z_2| \approx e^{\lambda \Delta t} |Z_1| \qquad (1.7)$$

Où λ est l'exposant de Lyapunov

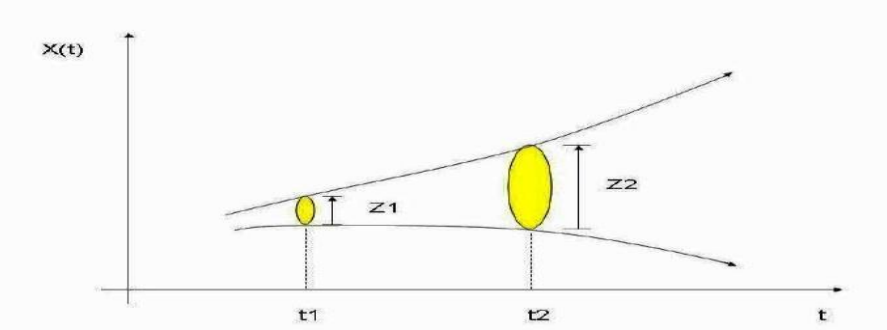


Fig. 1. 5 Divergence de deux trajectoires dans le plan de phase

Les exposants de Lyapunov sont une généralisation des valeurs propres pour le pointfixe et des multiplieurs caractéristiques pour les solutions périodiques.

Pour un attracteur non chaotique, les exposants de Lyapunov sont tous inférieurs ou égaux à zéro et leur somme est négative. Un attracteur étrange possèdera toujours au moins trois exposants de Lyapunov, dont un au moins doit être positif (voir le tableau ci-dessous).

ETAT STABLE	Flot	Dimension de Lyapunov	Exposants de Lyapunov
Point d'équilibre	point	0	$\lambda_n \leq \cdots \leq \lambda_1 \leq 0$
Périodique	cercle	1	$\lambda_1 = 0$ $\lambda_n \leq \cdots \leq \lambda_2 \leq 0$
Période d'ordre 2	tore	2	$\lambda_1 = \lambda_2 = 0$ $\lambda_n \leq \cdots \leq \lambda_3 \leq 0$
Période d'ordre K	K-tores	K	$\lambda_1 = \cdots = \lambda_K = 0$ $\lambda_n \leq \cdots \leq \lambda_{K+1} \leq 0$
Chaotique		Non entier	$\lambda_1 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$
Hyperchaotique		Non entier	$\lambda_1 > 0, \quad \lambda_2 > 0$ $\sum_{i=1}^{n} \lambda_i < 0$

Tab 1.1 Classification des régimes permanents selon les exposants de Lyapunov

1.4 LES DYNAMIQUES CHAOTIQUES

Depuis que l'attracteur de Lorenz est découvert en 1963, la recherche dans le domaine du chaos a attiré l'attention des chercheurs et experts, Plusieurs sortes de systèmes chaotiques et hyper-chaotiques ont été présentés par la suite.

En termes de modèles mathématiques et de leurs propriétés, les systèmes chaotiques peuvent être classés en chaos continu, chaos discret, chaos commuté, chaos retardé, hyperchaos…..etc.

Dans ce qui suit, quelques propriétés de systèmes chaotiques continus et discrets seront présentées.

1.4.1 LE CHAOS CONTINU

Plusieurs systèmes chaotiques continus ont été étudiés dans la littérature. Parmi ces systèmes, on retrouve le système de Lorenz, le système de Rossler, l'attracteur de Chen et la fonction jerk [63].

Prenons comme exemple de systèmes chaotiques continus, le système de Lorenz [37] [44]:

$$\begin{cases} \frac{dx}{dt} = \sigma\,(y - x) \\ \frac{dy}{dt} = x\,(\rho - z) - y \\ \frac{dz}{dt} = xy - bz \end{cases} \tag{1.8}$$

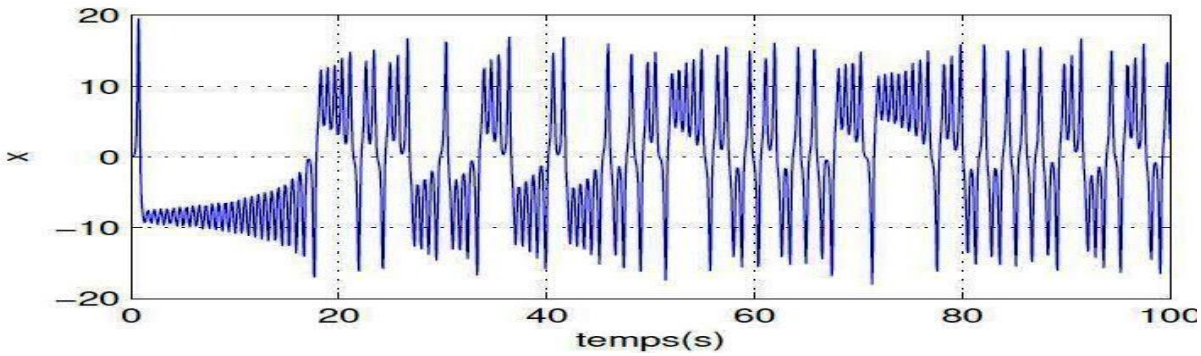
Le système de Lorenz est un système d'équations non linéaires à cause des termes xyetxz. Ce système n'est pas intégrable dans le cas général. La détermination de ce système doit se faire à l'aide des méthodes d'approximation [44].

Lorsque les paramètres réels σ, ρ et b prennent les valeurs suivantes : $\sigma = 10$,$\rho = 28$ et$b = \frac{8}{3}$,avec les conditions initiales $x(0) = y(0) = z(0) = 0.01$, le système (1.8) est chaotique.

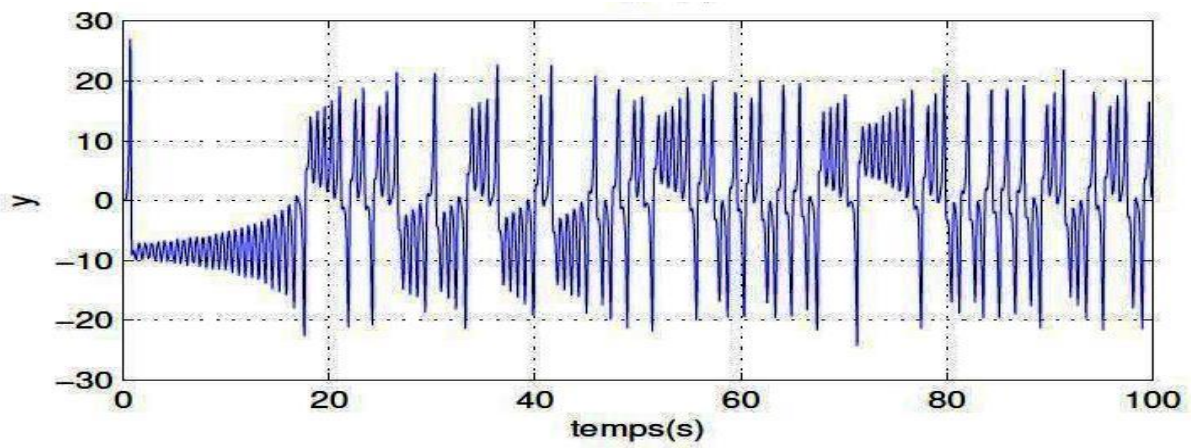
Dans ce qui suit, nous vérifions quelques propriétés du système chaotique (1.8)

- **Aspect aléatoire**

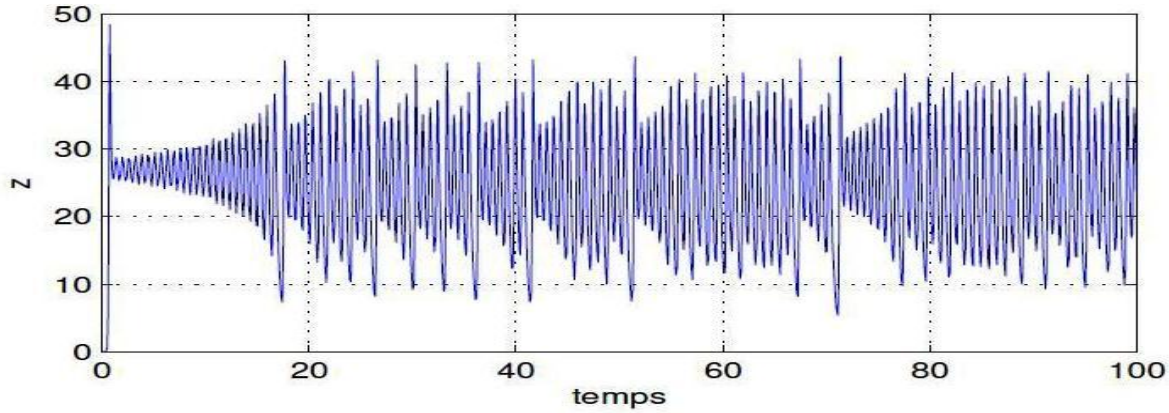
La figure (1.6) illustre l'aspect aléatoire des états du système (1.8)



(a) : état x du système de Lorenz



(b) : état y du système de Lorenz



(c) : état z du système de Lorenz

Fig. 1. 6 Aspects aléatoires des états du système de Lorenz

- **Attracteur étrange**

Le système chaotique (1.8) présente un superbe attracteur étrange en forme d'ailes de papillon, représenté sur la figure (1.7). La trajectoire commençant par s'enrouler sur une aile, puis sautant pour commencer à s'enrouler sur l'autre aile, et ainsi de suite.

On observe que la dynamique du système de Lorenz donné par le système (1.8) est indépendante du temps t, par conséquent ce type de système est qualifié d'être autonome [65].

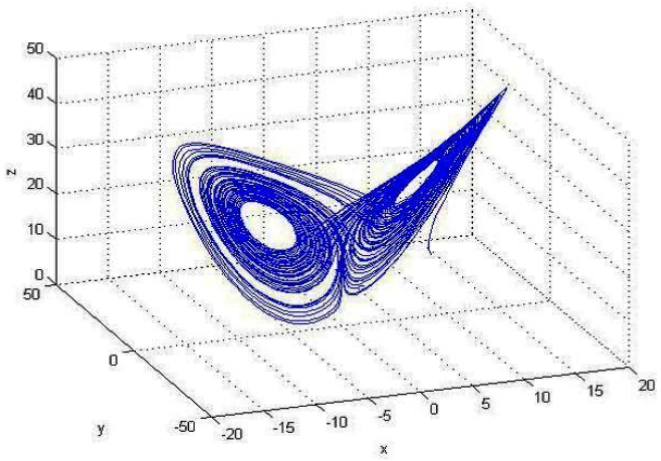


Fig. 1. 7 Attracteur étrange de Lorenz

- **Les exposants de Lyapunov**

Après calcul des exposants de Lyapunov (voir figure 1.8), nous avons obtenu les valeurs suivantes :

$$\lambda_1 = 0.85922,\ \lambda_2 = -0.0015763\ ,\lambda_3 = -145208$$

Nous constatons bien qu'il y a un exposants de Lyapunov, ce qui signifie que le système est chaotique.

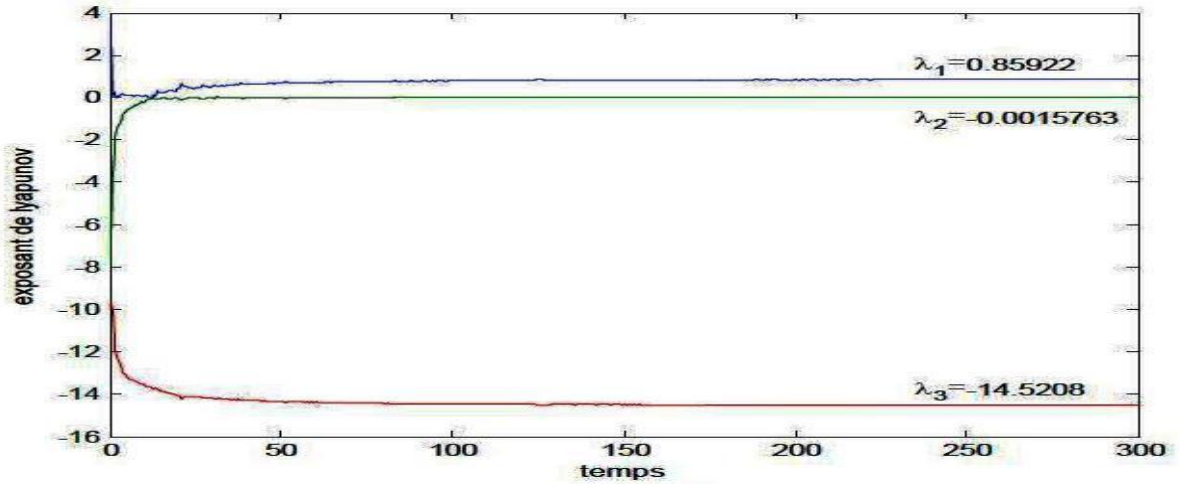


Fig. 1. 8 Exposants de Lyapunov du système chaotique continu de Lorenz

1.4.2 LE CHAOS DISCRET

Le système chaotique discret le plus connu est la fonction logistique qui est l'une des fonctions de Chebyshev, il existe toutefois d'autre systèmes chaotiques discrets comme le système de Henon, la fonction de Tent et la fonction Gaussienne discrète.

La fonction logistique très connue dans la théorie des systèmes non linéaires, est une application non bijective du domaine [0, 1] dans lui-même qui sert de récurrence à la suite [44] :

$$x_{k+1} = f(x_k) = r x_k \, (1 - x_k) \tag{1.9}$$

où$k = 0,1,\ldots\ldots$ dénote le temps discret, x la variable dynamique et r un paramètre réel.

La dynamique de cette application correspond à un comportement très différent ; ainsi selon la valeur du paramètre r, une plus grande variété de régimes permanents seprésente, parmi lesquelles on trouve, par ordre de complexité :

- Pour $0 < r < 3$, le système possède un point fixe attractif, qui devient instablelorsque $r = 3$.
- Pour $3 < r < 3.57\ldots\ldots$, le système évolue périodiquement de période r^n, avec n unentier qui tend vers l'infini lorsque r tend vers $3.57\ldots\ldots$

- Pour r = 4, le système évolue de manière chaotique.

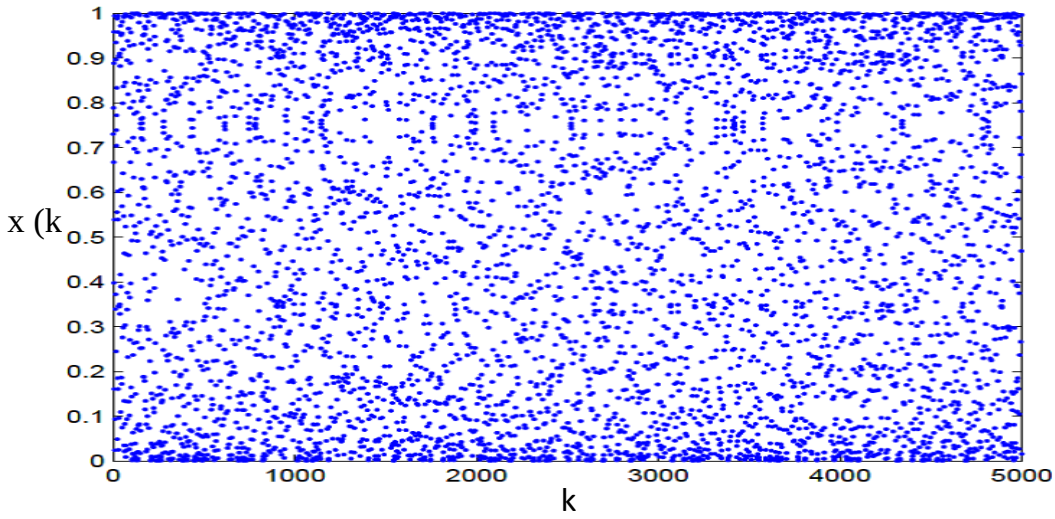


Fig. 1. 9 Trajectoire de la fonction logistique

De même que pour le cas continu, nous présentons dans ce qui suit quelques propriétés du système chaotique discret (1.9).

- **Aspect aléatoire**

La figure suivante illustre l'aspect aléatoire du système (1.9) pour $r = 4$. Il est alors impossible de discerner à l'œil nu cette trajectoire de celle d'une variable aléatoire.

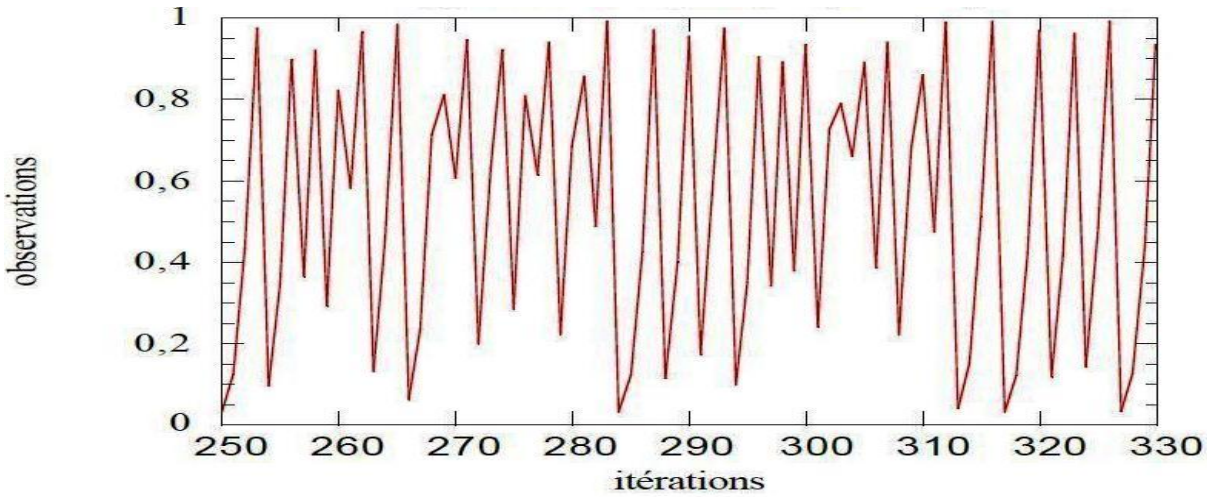


Fig. 1. 10 Application logistique pour r = 4

- **Exposant de Lyapunov**

Comme il a été déjà mentionné la fonction logistique présente un comportement chaotique à partir d'une valeur spécifique du paramètre r soit $r = 4$. Après calcul de l'exposant de Lyapunov de fonction logistique :

$$x_{k+1} = 4x_k\ (1 - x_k) \tag{1.10}$$

Nous avons obtenu la valeur $\lambda = ln2 > 0$, d'où le comportement chaotique.

1.4.3 LE CHAOS A RETARD

Le système de Mackey- Glass est le premier chaos à retard découvert en 1977 à partir d'un modèle physiologique. Il est donné par l'équation suivante [65]:

$$\dot{x}(t) = -x(t) + \frac{2x\ (t-\tau)}{1+x(t-\tau)^{10}} \tag{1.11}$$

Le portrait de phase de ce système est donné par la figure (1.7)

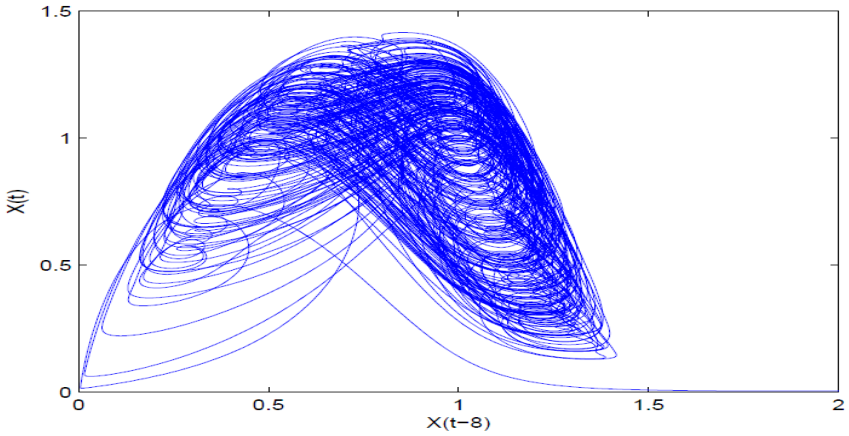


Fig. 1. 11 Portrait de phase du système de Mackey-Glass avec $\boldsymbol{\tau = 8}$

Un autre système chaotique à retard est celui d'Ikeda obtenu comme modèle d'un système optique passif :

$$\dot{x} = -x(t) + \mu \sin\ (x\ (t-\tau)\ ) \tag{1.12}$$

1.5 BIFURCATION ET ROUTES VERS LE CHAOS

La theorie de bifurcation est l'etude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique[65].

Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées *valeurs de bifurcation*.

Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation [44] (figure (1.8)).

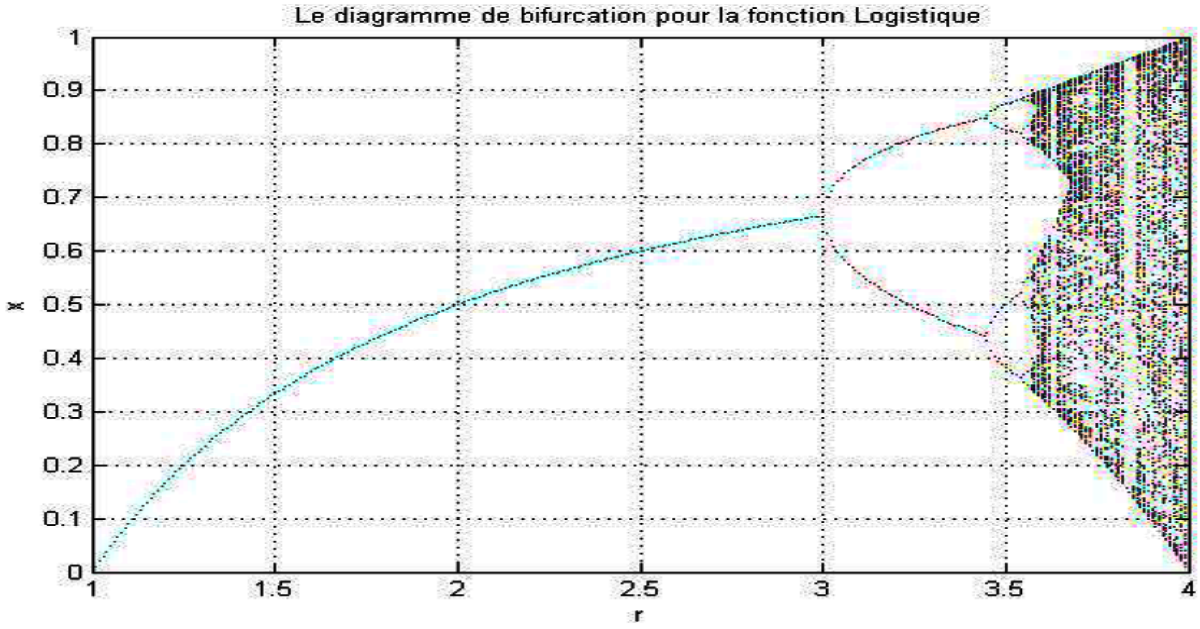


Fig. 1. 12 Diagramme de bifurcation de la fonction logistique

Dans les équations de Lorenz par exemple, la résolution du système n'apporte pas toujours le chaos.Ce régime n'apparaît que pour certaines valeurs des paramètres. Pour caractériser le chaos.

Il peut être intéressant d'étudier l'apparition du chaos (ce qu'on appelle le scénario ou la route vers le chaos).

On distingue trois scénarios théoriques d'évolution vers le chaos. Toutes ces évolutions ont permis de classer certains phénomènes expérimentaux comme chaotiques déterministes.

On obtient l'apparition du chaos en modifiant la valeur d'un paramètre du système que ça soit de manière théorique ou expérimentale.

- ***Le doublement de période***

L'augmentation d'un paramètre provoque, pour un système périodique, l'apparition d'un doublement de période, la période se multiplie ainsi en 4, 8, 16,……

A partir d'une certaine valeur du paramètre, Les doublements étant de plus en plus rapprochés, on tend vers un point auquel on obtiendrait hypothétiquement une fréquence infinie et c'est à ce moment que le chaos apparait.

- ***L'intermittence***

Ce scénario est caractérisé par un mouvement périodique stable entrecoupé par des mouvements chaotiques qui apparaissent de manière irrégulière.
Le système conserve pendant un certain laps de temps un régime périodiqueou pratiquement quasi-périodique, c'est à dire une certaine "régularité", et il sedéstabilise, brutalement, pour donner lieu à un comportement chaotique. Il sestabilise de nouveau, pour donner lieu à une autre « explosion chaotique » plus tard.
La fréquence et la durée des phases chaotiques ont tendance à s'accroître plus on s'éloigne de la valeur critique de la contrainte ayant conduit à leur apparition.

- ***La quasi-périodicité***

Ce troisième scénario fait intervenir pour un système périodique l'apparition d'une autre période dont le rapport avec la première n'est pas rationnel.

1.6 CONCLUSION

Dans le présent chapitre, quelques définitions et notions sur les systèmes chaotiques ont été présentées. Nous allons montrer leur utilisation à des fins de chiffrement de données.

En effet, les systèmes chaotiques possèdent des propriétés proches de celles requisesen cryptographie usuelle.

Le prochain chapitre introduit la notion de la cryptographie et présente lesdifférents schémas de chiffrement basés sur l'utilisation des systèmes dynamiques chaotiques.

En effet, la propriété déterministe du chaos associée à la possibilité de synchroniser le chaos permet d'envisager son utilisation pour réaliser par exemple des fonctions de codagedans les systèmes de télécommunications.

CHAPITRE 2 : SYNCHRONISATION DES SYSTEMES CHAOTIQUES

2.1 INTRODUCTION

L'utilisation du chaos dans les systèmes de télécommunication a été rendue possibledepuis la maîtrise de la synchronisation des systèmes chaotiques. En effet le problème de synchronisation du récepteur dans le but de dupliquer le signal chaotique utilisé au niveau du récepteur se pose directement [19] [50].

La synchronisation des systèmes chaotiques peut paraître énigmatique et ambiguë. En effet la synchronisation de ces systèmes présente plus de contraintes contrairement au cas d'oscillations périodiques où il n'y a pas d'instabilité intrinsèque.

Dans la littérature plusieurs concepts de synchronisation chaotique ont été proposés tout d'abord avec les travaux de Yamada et Fujisaka [59] qui ont utilisé une approche locale de la synchronisation chaotique. Par la suite Afraimovich et al. [1] ont développé les concepts importants liés à la synchronisationchaotique et ultérieurement Pecora et Carroll [50] [51] ont défini la synchronisation chaotique connue sous le nom de synchronisation identique, développée sur la base de circuits chaotiques couplés, avec l'un maître et l'autre esclave ; Ces travaux ont ouvert la voie des applications du chaos aux télécommunications [20].

Dans ce chapitre, nous citerons les différentes approches de synchronisation des systèmes chaotiques. Ensuite, on introduit le concept de synchronisation impulsive de deux systèmes chaotiques identiques.

2.2 COMMUNICATION SECURISEE A BASE DU CHAOS

Comme il a été déjà mentionné dans le premier chapitre, le chaos déterministe peut générer des comportements dynamiques d'apparences aléatoires.Il serait donc intéressant d'utiliser ces derniers comme porteuses d'informations en télécommunication.

En 1990, L.M.Pecora et T.L.Caroll [50] ont introduit la notion de synchronisation de deux systèmes chaotiques identiques. Trois ans plus tard, Cuomo et Oppenheim [10] présentèrent le premier dispositif de communication entre deux systèmes chaotiques de Lorenz identiques. En 1997 Kolumban, Kennedy et Chua [26] [27] réalisèrent des communications numériques à base de deux circuits de Chua identiques. Plus tard, le domaine du chaos attira l'attention de la communauté scientifique et plusieurs systèmes de communications symétriques furent présentés.

Le diagramme principal de la communication sécurisée par le chaos est montré sur la figure (2.1). Le principe est de masquer une information par des signaux chaotiques et de l'envoyer vers le récepteur sur un canal public. L'information cryptée est récupérée au niveau du récepteur.

La clé du système de transmission est l'ensemble des paramètres des deux générateurs chaotiques à l'émission et à la réception qui doivent être synchronisés, c'est à dire $x = y$.

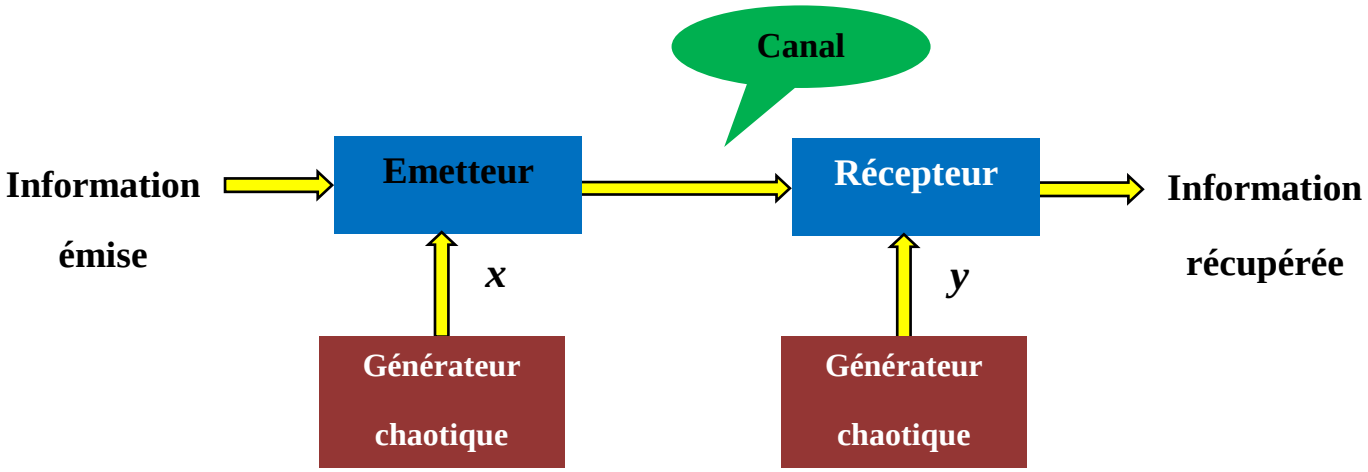


Fig. 2.1 Principe de la communication sécurisée à base du chaos

2.3 CONCEPT ET METHODES DE SYNCHRONISATION

Le concept de synchronisation repose sur le constat qu'un système chaotique est déterministe et possède un ou plusieurs exposants de Lyapunov positifs et qu'il est instable. Il est donc possible de construire une réplique identique à ce système et d'essayer de synchroniser de façon que les deux signaux chaotiques issus des deux exemplaires soient identiques.

Il existe deux classes de synchronisation suivant la manière avec laquelle les deux systèmes chaotiques sont couplés ; on distingue la synchronisation unidirectionnelle et la synchronisation bidirectionnelle.

2.3.1 SYNCHRONISATION UNIDIRECTIONNELLE

Dans le cas d'une synchronisation unidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément fonctionnant dans un seul sens, par exemple l'utilisation d'un circuit électrique suiveur [14].

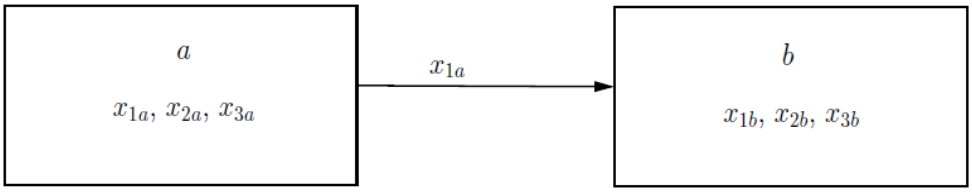


Fig. 2.2 Couplage unidirectionnel

2.3.2 SYNCHRONISATION BIDIRECTIONNELLE

Dans le cas d'une synchronisation bidirectionnelle, le couplage entre deux systèmes identiques a et b est réalisé à l'aide d'un élément permettant l'échange d'énergie dans les deux sens, par exemple l'utilisation d'une simple résistance [14].

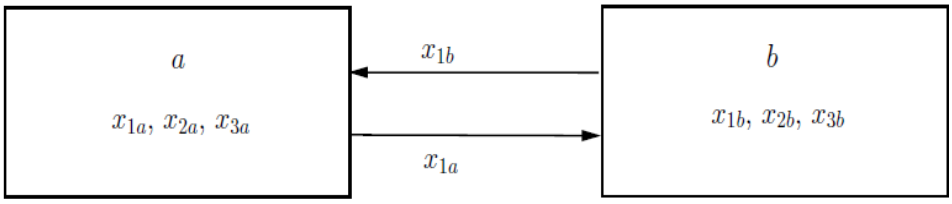


Fig. 2.3 Couplage bidirectionnel

2.4 METHODES DE SYNCHRONISATION

Plusieurs méthodes de synchronisation ont été proposées dans la littérature. Dans ce qui suit nous citerons quelques approches en expliquant leurs principes et avantages [14].

2.4.1 SYNCHRONISATION PAR REPARTITION DU SYSTEME

Pour illustrer la méthode de synchronisation par couplage entre deux systèmes chaotiques, nous avons choisi de présenter la synchronisation identique proposée par Pecora et Carroll [50] [51]. L'avantage de cette approche est de représenter une solution simple et performante.L'objectif est qu'un système esclave reproduise le plus fidèlement possible l'état du maître, après un régime transitoire.

L'idée consiste à diviser le système d'origine en deux sous-systèmes de telle sorte que les variables dynamiques de départ soient réparties de part et d'autre de chacun des sous-systèmes. Il s'agit ensuite de reproduire les sous-systèmes à l'identique et de les mettre en cascade. Le signal issu du système de départ (système maître) sert à piloter (synchroniser) le premier des deux sous-systèmes dupliqués mis en cascade, qui lui-même permet de synchroniser le second sous-système dupliqué [4] [8].

Partant d'un système chaotique défini par la dynamique suivante :

$$\dot{x}(t) = f(x(t)) \tag{2.1}$$

où$x = [x_1, \ldots \ldots x_n]$ désigne le vecteur d'état

On divise le système initial en deux sous-systèmes avec une réorganisation des variables d'état dans un ordre quelconque.

$$\begin{cases} S_1 : \dot{x}^{\{1\}} = F^{\{1\}}(x^{\{1\}}, x^{\{2\}}) \\ S_2 : \dot{x}^{\{2\}} = F^{\{2\}}\left(x^{\{1\}}, x^{\{2\}}\right) \end{cases} \tag{2.2}$$

Avec

$$x^{\{1\}} = [x_1, \ldots \ldots, x_m]^T$$

$$x^{\{2\}} = [x_{m+1}, \ldots \ldots, x_n]^T$$

$$F(x) = \left[F^{\{1\}}(x)\ ;\ F^{\{2\}}(x)\right]$$

Soit un autre système $S_2^{'}$ de dynamique identique $\mathrm{F}^{\{2\}}$ et un vecteur d'état $\hat{x}^{\{2\}}$:

$$S_2^{'} : \dot{\hat{x}}^{\{2\}} = F^{\{2\}}\left(x^{\{1\}}, \hat{x}^{\{2\}}\right) \tag{2.3}$$

Pecora et Caroll ont démontré que le système $S_2^{'}$ est candidat pour se synchroniser avec le système initial à la condition nécessaire et suffisante qu'il soit stable, ceci est équivalent à ce que les exposants de Lyapunov soient négatifs.

Une convergence parfaite des trajectoires est ainsi accomplie.

$$\lim_{t\to\infty}\left\|\hat{x}^{\{2\}}(t) - x^{\{2\}}(t)\right\| = 0 \tag{2.4}$$

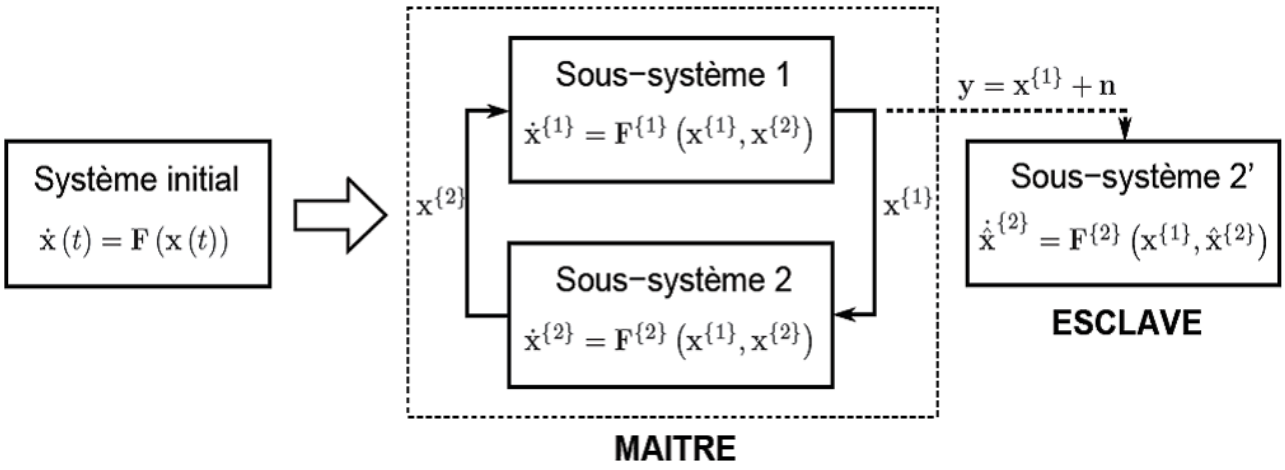


Fig. 2. 4 Synchronisation maître-esclave

2.4.2 SYNCHRONISATION GENERALISEE

Cette méthode est une généralisation du concept de synchronisation identique. Les deux systèmes se synchronisent, au sens généralisé s'il existe une transformation M telle que

$$\lim_{t\to\infty}\left\|x^{'}(t) - M(x(t))\right\| = 0 \tag{2.5}$$

où$x(t)$ est l'état du système émetteur et $x^{'}(t)$ est l'état du système récepteur.

Les conditions initiales ne sont pas tenues en compte dans ce cas.
Si M est inversible, alors $M^{-1}(x^{'})$ fournit une estimation de l'état x ; dans le cas contraire, il serait impossible de fournir une estimation de l'état x. Ceci présente alors un inconvénient majeur pour les techniques de communication utilisant l'état de l'émetteur pour décrypter le message transmis [5] [8].

2.4.3 SYNCHRONISATION RETARDEE

Dans ce mode de synchronisation, l'état du système esclave converge vers l'état décalé dans le temps du système maitre [33].

$$\lim_{t\to\infty} \|x^{'}(t) - x(t-\tau)\| = 0 \qquad (2.6)$$

où$x(t)$ est l'état du système émetteur, $x^{'}(t)$ est l'état du système récepteur et τ est un retard positif.

2.4.4 SYNCHRONISATION PROJECTIVE

Dans cette méthode, l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur. Soit a et τ tels que :

$$\lim_{t\to\infty} \|x^{'}(t) - ax(t-\tau)\| = 0 \qquad (2.7)$$

où a est le facteur d'échelle, $x(t)$ est l'état du système émetteur, $x^{'}(t)$ est l'état du système récepteur et τ est un retard positif.

Cette approche est utilisée pour des systèmes partiellement linéaires et permet de synchroniser à un facteur près les états qui ne peuvent être synchronisés [5] [8] [41].

2.4.5 SYNCHRONISATION PAR BOUCLE FERMEE

La synchronisation des systèmes chaotiques par les méthodes en boucle ouverte implique une sensibilité aux variations paramétriques. Pour y remédier, de nouvelles techniques basées sur un bouclage par contre-réaction ont été proposées.
L'idée est d'appliquer une correction au système en fonction de l'erreur entre le signal transmis par le premier système et le signal régénéré par l'autre.Cette erreur est ainsi injectée en contre-réaction d'où l'appellation de l'approche.

Cette technique permet également la synchronisation entre des paires différentes de systèmes chaotiques.

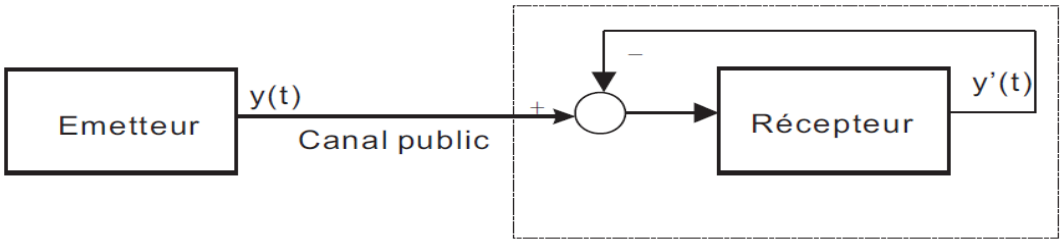


Fig. 2.5 Synchronisation par boucle fermée

2.4.6 SYNCHRONISATION DE PHASES

Pour deux systèmes périodiques de phases Φ_1 et Φ_2, la synchronisation est exprimée par la relation [6] :

$$|n\Phi_1 - m\Phi_2| < c \tag{2.8}$$

Avec m, n des entiers naturels et *c*est une constante positive.

Cette notion de synchronisation a été étendue aux systèmes chaotiques, l'approche analytique est l'une des solutions permettant de définir la phase d'un système chaotiques.

Un signal analytique $\Psi(t)$est une fonction complexe définie comme suit :

$$\Psi(t) = s(t) + j\tilde{s}(t) = A(t)e^{j\Phi(t)} \tag{2.9}$$

Où$\tilde{s}(t)$ est la transformée de Hilbert de la série temporelle $s(t)$, $A(t)$ est l'amplitude de $\Psi(t)$ et $\Phi(t)$ sa phase.

La synchronisation de phase entre deux systèmes chaotiques couplés se produit si

$$|n\Phi_1(t) - m\Phi_2(t)| < c \tag{2.10}$$

Il est à noter que dans ce cas, les amplitudes restent non corrélées.

2.4.7 SYNCHRONISATION IMPULSIVE

Dans un schéma de transmission usuel, un des états du système dynamique est transmis afin de réaliser la synchronisation par le récepteur. Dansle but de réduire la redondance du signal transmis la synchronisation impulsive a été proposée (figure 2.6).

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

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

$$\dot{x}(t) = f(x(t)) \tag{2.11}$$

On définit un signal impulsif qui consiste en une suite d'instants discrets auxquelles un signal y(t) = Cx(t) est envoyé par le système maître au système esclave, dont les variables d'état subissent un saut et un changement d'état.

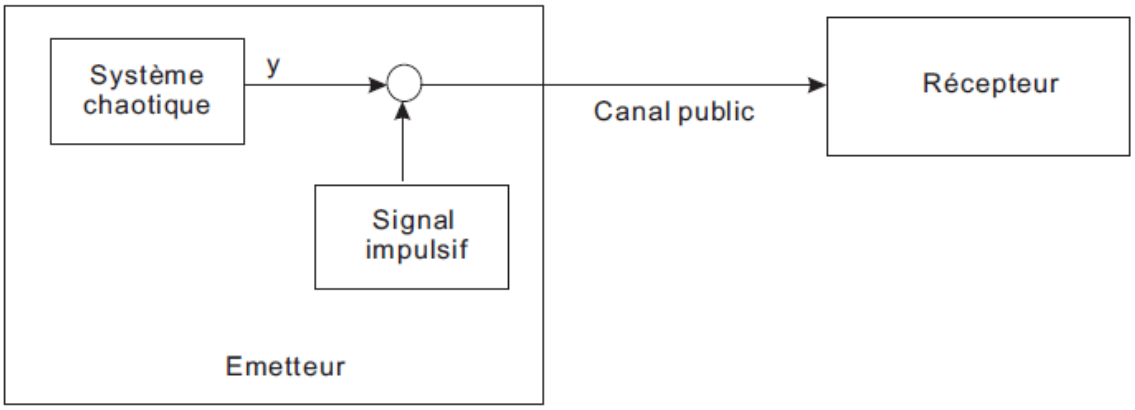


Fig. 2.6 Synchronisation impulsive

Cette méthode sera mieux développée et discutée par la suite pour être appliquée pour la réalisation d'un système de transmission sécurisée.

2.5 PROPRIETES DES SYSTEMES DE COMMUNICATION A BASE DU CHAOS

Dans cette partie, des propriétés des systèmes de communication chaotiques seront étudiées et comparées aux propriétés des systèmes classiques.

2.5.1 Spectre à large bande

Les systèmes chaotiques ont spécifiquement un spectre à large bande. Cette propriété est bénéfique pour les applications qui nécessitent une importante robustesse face aux interférences et une faible probabilité de détection [58].

Ces problèmes ont été pris en compte par les premiers systèmes de transmission en utilisant des spectres larges et des modulations par saut de fréquences. Cependant malgré le recours à ces moyens, la synchronisation entre l'émetteur et le récepteur reste une tâche qui n'est pas toujours triviale. En effet les schémas de transmission qui utilisent un saut de fréquence requièrent une nouvelle synchronisation à chaque changement de fréquence de la porteuse. Donc l'utilisation des systèmes chaotiques permet la transmission des signaux à large bandes, ainsi la synchronisation entre l'émetteur et le récepteur est plus simple.

2.5.2 Signal non périodique

La périodicité, dans la communication sécurisée engendre des pics spectraux indésirables.

Par contre, un signal chaotique est non périodique et son évolution ne peut être prédite sur un long intervalle de temps. Par conséquent, il y a absence des pics spectraux. De plus il est plus difficile de développer un modèle de prévisions pour les dynamiques non périodiques [58].

2.5.3. Implémentation analogique simple

Les systèmes de communication à base du chaos peuvent être implémentés en utilisant des dispositifs électriques ou optiques. Dans les schémas traditionnels par exemple, la transmission par saut de fréquences nécessite la numérisation des données, ceci impliques des circuits indépendants plus complexes [58].

2.6 TECHNIQUES DE CRYPTAGE PAR LE CHAOS

Les schémas de communication exploitant la synchronisation des systèmes chaotiques appartiennent au domaine général de reconstruction d'entrées inconnues [8] [14]. Les systèmes chaotiques constituent une classe particulière de systèmes non linéaires, il est donc possible de leur appliquer toutes les méthodes relatives aux systèmes non linéaires.

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

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

Dans ce mémoire, nous nous intéressons uniquement aux systèmes de communications à porteuse chaotique.

2.6.1 CRYPTAGE PAR ADDITION

Cette méthode est la première chronologiquement à utiliser la synchronisation du chaos [8]. L'idée repose sur l'observation des signaux chaotiques. Le principe est alors très simple : il suffit d'additionner directement le signalInformationnel $u(t)$ au signal chaotique C_x(t) et de le récupérer ensuite par synchronisation chaotique (voire Fig. 2.7). Le même système est utilisé à la fois à l'émetteur et au récepteur, avec la différence que le récepteur est contrôlé par le signal émis pour obtenir la synchronisation.

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

Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal y(t) (porteuse chaotique plus le message), donc il ne cherchera pas à appliquer des techniques de décryptage [3].

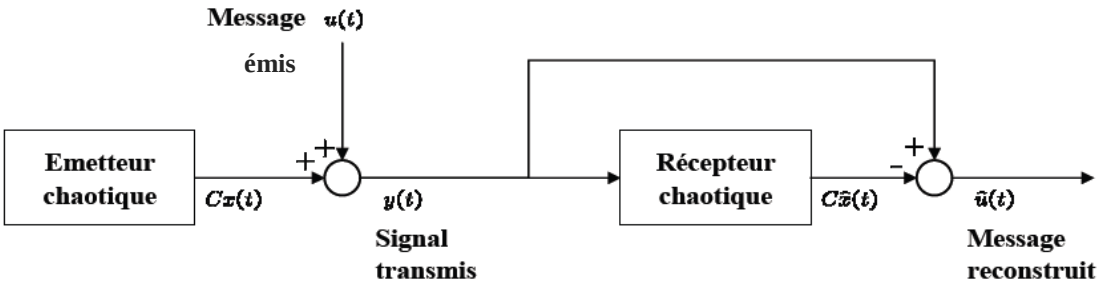


Fig. 2.7 Cryptage par addition

Le principal avantage de cette méthode réside dans la simplicité du cryptage. On peut souligner que cette technique peut être appliquée à des messages continus ou discrets.

L'inconvénient de cette méthode est qu'afin de garantir la synchronisation le message doit être au moins de 20 à 30 dB inférieur à la sortie de l'émetteur [14]. Toutefois, en présence d'un bruit de canal d'une puissance proche de celle du message, il devient difficile de détecter l'information. De plus, cette méthode reste sensible aux attaques extérieures [54], et l'usage du canal de transmission est inefficace du point de vue de l'énergie transmise par rapport à la qualité d'information fournie.

2.6.2 CRYPTAGE PAR COMMUTATION

Cette technique, est réservée aux messages prenant un nombre fini de valeurs.
L'émetteur est constitué de deux ou plusieurs systèmes chaotiques : ces deux systèmes peuvent avoir le même modèle dynamique, avec des paramètres différents, ou avoir deux modèles dynamiques totalement différents [8] [30]. La figure ci-dessous illustre cette méthode de cryptage.

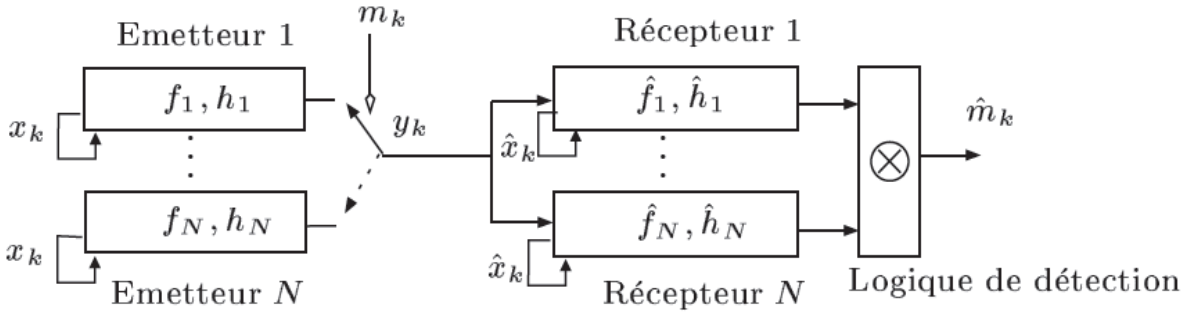


Fig. 2.8 Cryptage par commutation

Du côté de l'émetteur, à chaque symbole m_k de l'information correspond un signal y_k issu d'un système chaotique Σ_k défini par :

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_k = h_i(x_k) \end{cases} \tag{2.12}$$

Avec $i \in \{1, \ldots\ldots, N\}$, $x_k \in \mathbb{R}^n$

Le rôle du récepteur est la détection de l'émetteur du signal de sortie y_k, il est donc composé d'autant de systèmes que l'émetteur

$$\begin{cases} \hat{x}_{k+1} = \hat{f}_i(\hat{x}(k)) \\ \hat{y}_k = \hat{h}_i(\hat{x}_k) \end{cases} \qquad i = 1, \ldots\ldots\ldots, N \tag{2.13}$$

La détection peut être cohérente ou non cohérente.Dans le premier cas, une synchronisation d'un seul système du récepteur est effectuée pour pouvoir reconstruire ensuite l'information m_i associée à l'aide d'une logique de détection. Dans le cas de détection non cohérente, nous utilisons les outils statistiques basés sur la corrélation entre les signaux y_k et $\hat{y}_k$.

2.6.3 CRYPTAGE PAR MODULATION PARAMETRIQUE

L'approche par modulation utilise le message contenant l'information pour moduler un ou plusieurs paramètres θ de l'émetteur chaotique.

Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure (2.9).

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la trajectoire un changement continu d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique "normal". Cependant, la façon d'injecter le message et donc la fonction demodulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur.

Cette technique exploite pleinement les qualités et propriétés des systèmes chaotiques. Elle n'a pas d'équivalent parmi les systèmes de communication "classiques".

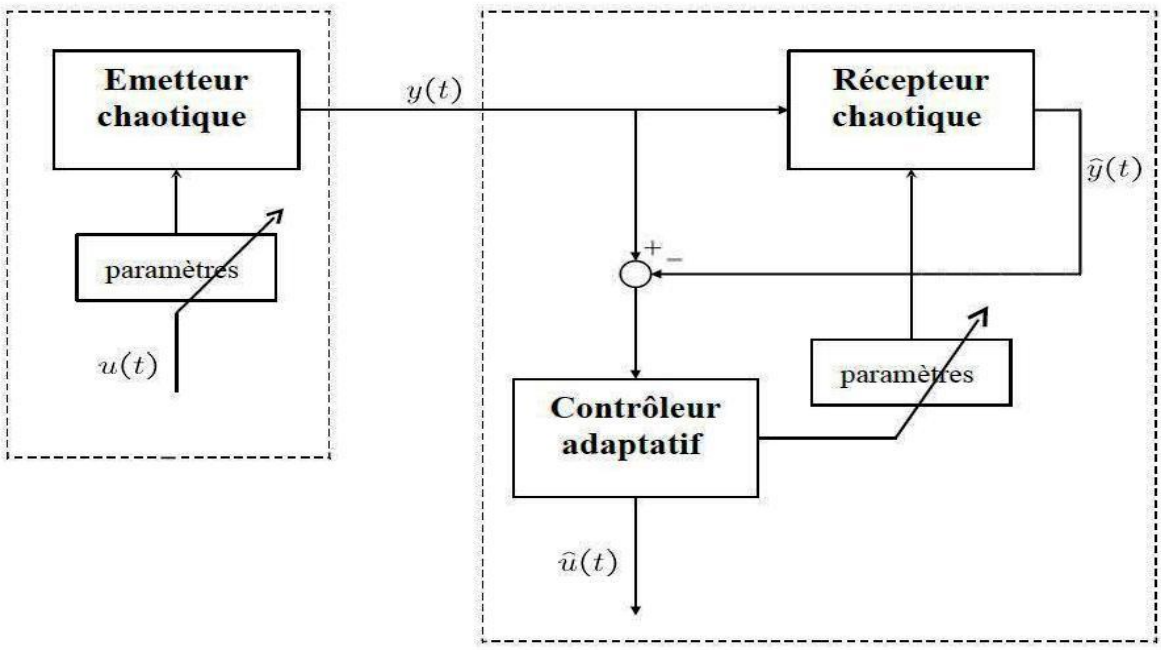


Fig. 2.9 Cryptage par modulation paramétrique

2.6.4CRYPTAGE PAR INCLUSION

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

La restauration de l'information se fait principalement par deux techniques, reposant soit sur les observateurs à entrées inconnues, soit sur l'inversion du système émetteur [14] [6]. Cette méthode présente beaucoup d'avantages et reste très utilisée en pratique [14] [18] [30] [31].

2.6.5 CRYPTAGE MIXTE

Afin de faire face aux problèmes de sécurité des méthodes précédentes, unenouvelle technique combinant les principes de la cryptographie standard et la synchronisation chaotique a été proposée. Le message *u(t)*contenant l'information est crypté grâce à une clé, *c(t)*, générée par l'émetteur chaotique [8].

Le message crypté est alors injecté dans la dynamique du système chaotique, pour la rendre plus complexe. Ensuite, un signal y(t) fonction des variables d'état de l'émetteur est transmis au récepteur, qui établit une synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message. Le principe général de cette méthode est illustré par la figure (2.10).

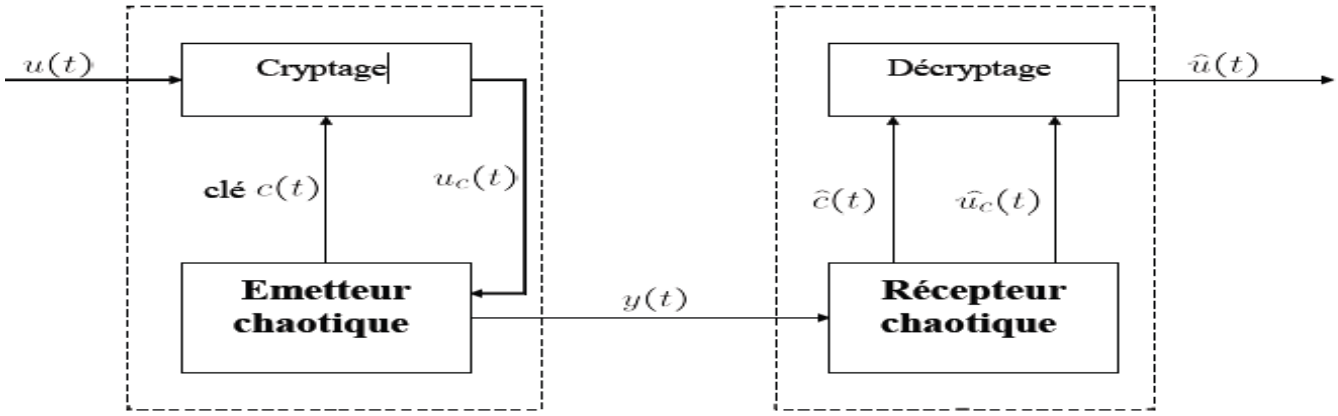


Fig. 2.10 Cryptage mixte

2.6.6 TRANSMISSION PAR DEUX VOIES

Dans ce schéma de communication, l'émetteur envoie deux signaux au récepteur [8] :

- Le premier signal y, est une fonction à valeurs réelles de l'état x du système chaotique émetteur, dont l'unique but est de permettre la synchronisation du récepteur.
- Le secondsignaly_2, envoyé sur un autre canal, est un signal chaotique contenant l'information à transmettre.

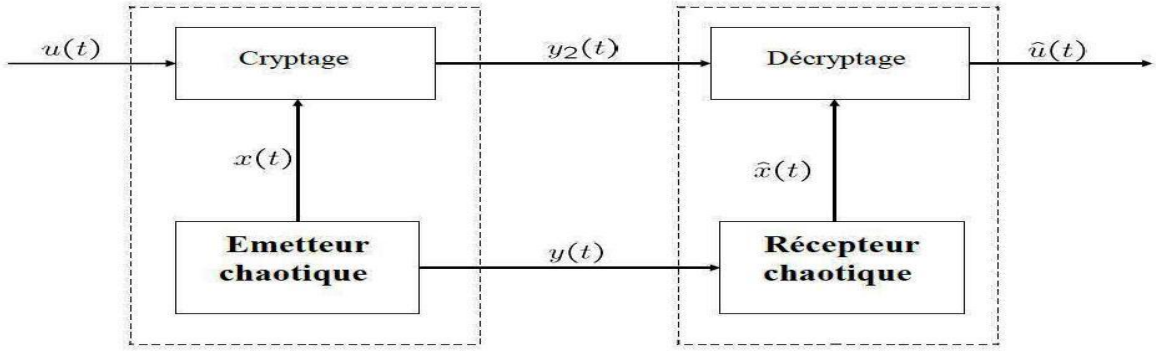


Fig. 2. 11 Transmission par deux voies

Cette méthode présente plusieurs avantages :

- Le signal y ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale.
- Le second signal y_2 contient l'information qui peut être soit cryptée par une fonction non linéaire de l'état x, soit simplement masquée par un signal chaotique généré parl'émetteur, qui sert de porteuse.
- Les deux étapes de synchronisationet de cryptage étant totalement indépendantes, le décryptage n'est pas nécessairement effectué, au niveau du récepteur, en même temps que la synchronisation.

2.7 LA CRYPTANALYSE

La cryptanalyse est l'étude des probabilités de succès des attaques possiblessur les systèmes cryptographiques afin de déterminer leurs éventuelles faiblesses [3]. L'un des principaux objectifs de la cryptanalyse est de tester si un adversaire peut déchiffrer le texte clair ou récupérer la clé secrète. Pour cela, il est nécessaire de se mettre à la place de l'adversaire ou pirate.

La cryptographie et la cryptanalyse sont deux domaines d'études évoluant en parallèle. En effet, de nouveaux systèmes de chiffrement, toujours plus complexes, sont conçus pour remplacer ceux qui ont été éliminés par la cryptanalyse et de nouvelles techniques de cryptanalyse sont inventées pour tester ces nouveaux systèmes. Le problème de la cryptographie est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire à un intrus pour déchiffrer l'information soit supérieure à sa durée de validité.

La réussite pratique d'une attaque dépend d'un certain nombre d'éléments, comme les connaissances nécessaires a priori, l'effort demandé (complexité, temps de calcul), la quantité et la qualité des informations pouvant être déduites de l'attaque.Il existe différentes attaques qui peuvent avoir lieu sur les systèmes cryptographiques. Dans ce qui suit nous citerons les attaques les plus fréquentes [58].

2.7.1 Les attaques qui ne nécessitent pas la recherche de la clé

Dans certains cas, il est possible de briser un système de cryptage sans la recherche de la clé utilisée pour crypter le message. Ces attaques surviennent lorsqu'il existe une dépendance entre les statistiques d'ordre faible (moyenne, moyenne quadratique….) du signal transmis et le message. La transmission de données binaires présente un grand risque dans ce cas, car une simple classification des données transmises en deux groupes permettrait de décoder le message sans connaître la dynamique exacte et ce quel que soit la dimension ou la complexité des systèmes chaotiques utilisés.

Ces attaques peuvent s'effectuer en utilisant le spectrogramme du signal transmis ou bien par calcul d'une fonction de retour du signal transmis.

2.7.2Les attaques qui nécessitent une connaissance partielle des dynamiques chaotiques

Il peut arriver qu'un récepteur non autorisé prenne connaissance de la classe générale des dynamiques, et alors manque seulement de paramètres spécifiques des dynamiques chaotiques. Par exemple, l'intrus peut supposer que les dynamiques secrètes sont celles d'un circuit de Chua, alors il peut réduire l'espace de recherche de la clé.

Ces attaques sont basées sur la modélisation des dynamiques de faibles dimensions et sur la synchronisation généralisée [58].

2.7.3 Les attaques qui nécessitent une reconstruction de la clé sans connaissance à priori des dynamiques

Le récepteur non autorisé peut aussi tenter de reconstruire les dynamiques chaotiques secrètes de l'émetteur sans avoir une connaissance à priori du types dynamiques utilisées.
Ces attaques sont effectuées par moyen de modèles de prévision des dynamiques non linéaires. Dans ce cadre K. M. Short [54] proposa un modèle pour prévoir la valeur moyenne du prochain échantillon du signal porteur d'informations transmises en fonction des échantillons précédents. Ce modèle de prévision a été utilisé pour décrypter l'information dans un système de transmission à base de deux circuits chaotiques de Chua.

2.8 CONCLUSION

Dans ce chapitre, nous avons expliqué le concept de synchronisation des systèmes chaotiques ainsi que les différents modes de synchronisation. Cette démarche nous sera très utile pour notre système de transmission.

La cryptographie chaotique peut s'effectuer sous différents schémas, il s'agit de définir la façon d'introduire le message dans l'émetteur.

Dans le chapitre qui suit nous nous intéresserons à la méthode de synchronisation impulsive. Les concepts de base y seront énoncés et la façon de l'appliquer dans ce travail de mémoire sera développée avec plus de détails.

CHAPITRE 3 : SYNCHRONISATION IMPULSIVE DES SYSTEMES CHAOTIQUES

3.1 INTRODUCTION

Durant les dernières décennies, la synchronisation du chaos a attiré une attention considérable à cause de son application potentielle dans divers champs tels que les réactions chimiques, systèmes biologiques et communication sécurisée….etc. Plusieurs méthodes ont été proposées pour mieux l'exploiter, et envisager des perspectives d'application plus intéressantes.

Récemment une nouvelle méthode de commande est développée, il s'agit de la synchronisation impulsive [60] [62]. Cette technique assure la synchronisation des systèmes chaotiques en utilisant de simples impulsions [19], et elle est appliquée dans plusieurs systèmes de communication basés sur le chaos puisqu'elle garantit une bonne performance pour la condition de synchronisation.

La commande impulsive est très attractive car elle permet la stabilisation d'un système chaotique en utilisant uniquement de petites impulsions, elle offre également la possibilité de moduler un signal numérique par une porteuse chaotique dans les applications à large spectre.

Le signal transmis dans notre cas consiste en une séquence de période T et comprend deux régions : une région de synchronisation qui comporte les impulsions de synchronisation et utilisée pour synchroniser impulsivement les systèmes chaotiques, et une autre qui contient le signal brouillé contenant l'information utile à transmettre.

Dans ce chapitre, nous expliquons de quelle façon deux systèmes chaotiques identiques ou différents peuvent être synchronisés par la méthode de commande impulsive.

3.2 THEORIE DES SYSTEMES IMPULSIFS

La dynamique d'un système impulsif est définie par un ensemble d'équations différentielles ordinaires et d'équations aux différences pour décrire le mouvement du système à l'arrivée des impulsions [29].

Considérons le système non linéaire:

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

Où $f: R_+ \times R^n \to R^n$ est continue

$x \in R^n$est le vecteur d'état

Soit l'ensemble discret $\{\tau_i\}$des instants de temps, tel que

$0 < \tau_1 < \tau_2 < \cdots < \tau_i < \tau_{i+1} < \cdots,$

$$\tau_i \to \infty \text{ quand } i \to \infty$$

On définit le saut $U(i, x)$ dans la variable d'état à un instant τ_i comme suit

$$U(i, x) = \Delta x|_{t=\tau_i} \triangleq x(\tau_i^+) - x(\tau_i^-) \tag{3.2}$$

Un système d'équations différentielles impulsif est alors défini comme suit [60] [61]:

$$\begin{cases} \dot{x} = f(t, x), \ t \neq \tau_i \\ \Delta x = U(i, x) \quad t = \tau_i \\ x(\tau_i^+) = x_0 \ \ t_0 \geq 0, i = 1,2, \ldots \end{cases} \tag{3.3}$$

Avec

$$\Delta x(\tau_i) = x(\tau_i^+) - x(\tau_i^-), \qquad x(\tau_i^+) = \lim_{t \to \tau_i^+} x(t) \ , \qquad x(\tau_i^-) = \lim_{t \to \tau_i^-} x(t)$$

Dans ce mémoire, l'étude est restreinte au cas où les impulsions ont lieu à des intervalles fixes. Les conditions d'existence et d'unicité de solutions pour le système impulsif sont expliquées dans la suite de ce chapitre. Toutefois, il est important d'introduire et définir les classes de fonctions suivantes [19] [20].

Définition 1

Soit $V : \mathbb{R}_+ \times \mathbb{R}^n \to \mathbb{R}_+$

V est dite appartenant à la classe $\nu_0$si :

V est continue dans $(\tau_{i-1}, \tau_i] \times \mathbb{R}^n$et pour chaque $x \in R^n$, i=1,2,…….

1. La limite : $\lim_{(t\,,y)\to(\tau_i^+,x)} V(t,y) = V(\tau_i^+, x)$existe.
2. V est localement lipchitzienne en x.

La classe $\nu_0$représente la classe des fonctions de Lyapunov qui seront utilisées pour étudier la stabilité des systèmes impulsifs [36].

Définition 2

Pour$(t,x) \in (\tau_{i-1}, \tau_i] \times \mathbb{R}^n$tel que $t \neq \tau_i$, $i = 1,2, \ldots \ldots \ldots$

On définit la dérivée à droite de $V(t,x)$

$$D^+V(t,x) \triangleq \lim_{h\to 0} sup \frac{1}{h}[V\big(t+h, x+hf(t,x)\big) - V(t,x)]$$

Si la fonction $V(t,x)$ est différentiable sur$\mathbb{R}^+ \times \mathbb{R}^n$, on se ramène alors à la notion usuelle de dérivée :

$$D^+V(t,x) = \frac{\partial}{\partial t}V(t,x) + \frac{\partial}{\partial x}V(t,x).f(t,x) \tag{3.4}$$

Définition 3 : Système de comparaison

Soit $V \in \nu_0$ et supposons que :

$$\begin{cases} D^+V(t,x) \le g\big(t, V(t,x)\big) & t \neq \tau_i \\ V\big(t, x+I(t,x)\big) \le \psi_i\big(V(t,x)\big) & t = \tau_i \end{cases} \tag{3.5}$$

Avec $g: \mathbb{R}_+ \times \mathbb{R}_+ \to \mathbb{R}$ est continue et $\psi_k : \mathbb{R}_+ \to \mathbb{R}_+$ est non décroissante.

Alors on peut définir un système de comparaison du système impulsif initial [35] tel que :

$$\begin{cases} \dot{w} = g(t,w) & t \neq \tau_i \\ w(\tau_i^+) = \psi_i(w(\tau_i)) \\ w(t_0^+) = w_0 \ge 0 \end{cases} \tag{3.6}$$

Définition 4

L'ensemble S_ρ est défini tel que

$$S_\rho = \{x \in \mathbb{R}^n \,|\, \|x\| < \rho\} \tag{3.7}$$

Avec $\| \, . \, \|$désigne la norme euclidienne sur $\mathbb{R}^n$

Définition 5

Une fonction α est dite appartenant à une classe $\mathcal{K}$ si

$\alpha \in C[\mathbb{R}_+, \mathbb{R}_+],\ \alpha(0) = 0\ et\ \alpha(x)$ est strictement croissante en x

Supposons :

$$f(t,0) = 0\ ,\ \ U(i,0) = 0\ \ \ et\ \ \ g(t,0) = 0\ \ \ \forall i \tag{3.8}$$

Avec les hypothèses ci-dessus, on peut déduire que les solutions triviales des systèmes (3.3) et (3.6) sont identiques pour tout instant sauf aux instants τ_i.

3.3 STABILITE DES SYSTEMES IMPULSIFS

Dans cette partie du mémoire, nous donnerons quelques définitionset théorèmes de stabilité des systèmes impulsifs [23].

Considérons de nouveau le système dynamique (3.1)

Definition 6 (Attractivité d'une boule)

La boule $B_\epsilon = \{x \in \mathbb{R}^n / \|x\| < \epsilon\}$ est attractive sur $B_\rho = \{x \in \mathbb{R}^n / \|x\| < \rho\}$ pour la dynamique (3.1), s'il existe une fonction β de classe $\mathcal{L}^1$ telle que

$\forall\, x(0) \coloneqq x_0 \in B_\rho$ le flux $\Phi(t, x_0)$du système (1) vérifie [23]:

$$\forall t > 0,\ \|\Phi(t, x_0)\|_\epsilon \leq \beta(t) \tag{3.9}$$

Definition 7 (stabilité asymptotique d'une boule)

La boule $B_\epsilon = \{x \in \mathbb{R}^n / \|x\| < \epsilon\}$ est asymptotiquement stable sur $B_\rho = \{x \in \mathbb{R}^n / \|x\| < \rho\}$ pour la dynamique (3.1) si elle est stable et attractive sur B_ρ .

Definition 8 (stabilité asymptotique globale d'une boule)

La boule $B_\epsilon = \{x \in \mathbb{R}^n / \|x\| < \epsilon\}$ est globalement asymptotiquement stable pour la dynamique (3.1) si elle est asymptotiquement stable sur $\mathbb{R}^n$

Dans cette partie du mémoire on considère la classe suivante des dynamiques impulsives [23].

$$\begin{cases} \dot{x}_1(t) = f_1(x_1(t), x_2(t), t) & t \neq t_k \\ \dot{x}_2(t) = f_2(x_1(t), x_2(t), t) & t \neq t_k \\ x_1(t_k^+) = 0 \\ x_2(t_k^+) = x_2(t_k) \end{cases} \tag{3.10}$$

Avec$x_1(t) \in \mathbb{R}^p$, $x_2(t) \in \mathbb{R}^{n-p}$, $f_1 : \mathbb{R}^n \to \mathbb{R}^p$ et $f_2 : \mathbb{R}^n \to \mathbb{R}^{n-p}$

La séquence $T = \{t_k : k \in \mathbb{N}\} \subset \mathbb{R}^+$vérifie qu'il existe τ_{min} et τ_{max} avec

$$0 < \tau_{min} < \tau_{max} \quad tels\ que \quad \forall k > 0 \quad t_{k+1} \geq t_k + \tau_{min} \quad et \qquad t_{k+1} \leq t_k + \tau_{max}$$

On définit $$\theta_k \triangleq t_{k+1} - t_k \tag{3.11}$$

Et on suppose que

$$t_i + \tau_{min} < t_{i+1} \quad et \quad t_i + \tau_{max} > t_{i+1}$$

A partir de la définition de la stabilité asymptotique globale d'une boule, il est possible de présenter des conditions de stabilité suffisantes pour le système (3.10). Pour cela, on doit poser quelques hypothèses.

Hypothèse 1

$f_1$est au moins Lipchitzienne localement où l_1 et l_2 sont les constante de Lipchitz par rapport à x_1 et x_2 .

Hypothèse 2

$$f_2(x_2, x_1, t) = Ax_2 + B(t)x_1 \text{ où } \forall t \geq 0 \; B(t) < M \tag{3.12}$$

Théorème 3 [23]

Si le système (3.10) vérifie les Hypothèses 1 et 2 et s'il existe une fonction définie positive $V_2 : \mathbb{R}^{n-p} \to \mathbb{R}^+ V_2 \in C^1$ telle que

1. $\forall\, x_2 \neq 0 \;\; \left.\frac{\partial V_2}{\partial x_2}\right|_{x_2(.)} Ax_2 < l_v \|x_2\|_2^2$ (3.13)
2. $\left.\frac{\partial V_2}{\partial x_2}\right|_{x_2(.)}$ est Lipchitzienne où k_v est sa constante de Lipchitz

Alors il existe un $\theta_{max} > 0$ tel que pour toute séquence $\theta_k \leq \theta_{max}$, $x_2(t_k)$ converge globalement et asymptotiquement vers 0 pour tout $k \to +\infty$.

Démonstration

On a :

$$\dot{V}_1\big(X_1(t)\big) = \left.\frac{\partial V_2(.)}{\partial x_2}\right|_{x_2(.)} Ax_2 + \left.\frac{\partial V_2(.)}{\partial x_2}\right|_{x_2(.)} B(t)x_1 \tag{3.14}$$

A partir de l'hypothèse 2 et de la condition (2), $\forall\, t \in [\, t_k, t_{k+1}[$ on a

$$\dot{V}_2\big(x_2(t)\big) \leq -l_v \|x_2\|_2^2 + k_v M \|x_1\|_2 \|x_2\|_2 \tag{3.15}$$

Comme x_1 est initialisé à chaque instant impulsif et f_1 est Lipchitzienne pour tout instant $\forall\, t \in [\, t_k, t_{k+1}[$, $x_1(t) < x_{1,max}(k)$

Nous obtenons alors

$$\dot{V}_2\big(x_2(t)\big) \leq -l_v \|x_2\|_2^2 + k_v M \big\|x_{1,\max}(k)\big\|_2 \|x_2\|_2 \tag{3.16}$$

Alors $\dot{V}_2\big(x_2(t)\big) \leq 0$ si

$$\|x_2(t)\|_2 > \frac{k_v M \|x_{1,\max}(k)\|_1}{l_v} := \varsigma(k) \geq \frac{k_v M \|x_{1,\max}(k)\|_2}{l_v} \tag{3.17}$$

On peut conclure alors que la boule$B_\varsigma = \{x_2 \in \mathbb{R}^{n-p} / \|x_2\|_2 \leq \varsigma\}$ est globalement asymptotiquement stable.

Comme ς est fonction de k et comme on le verra plus tard est aussi fonction de $\|x_2(t_k)\|_2$, on doit donc étudier le comportement de ς par rapport à k.

Pour cela, on définit la fonction de Lyapunov $V_1(X_1(t))$ comme

$$V_1\big(x_1(t)\big) = \|x_1(t)\|_1 = \sum_{i=1}^{p} |x_i(t)| \tag{3.18}$$

La dérivée est alors donnée par :

$$\dot{V}_1\big(x_1(t)\big) = \sum_{i=1}^{p} sign\,(x_i(t)) \frac{\partial x_i(t)}{\partial t} \tag{3.19}$$

La dérivée de V_1est une fonction à plusieurs valeurs, plusieurs problèmes peuvent alors survenir pour :

$x_i(t) = 0$ car $sign(0) \in [-1,1]$.

Cependant le pire cas est toujours considéré, pour cette raison $sign\big(x_i(t)\big)\frac{\partial x_i(t)}{\partial t}$ est majoré par $\left|\frac{\partial x_i(t)}{\partial t}\right|$. Par conséquent nous avons :

$$\dot{V}_1\big(x_1(t)\big) \leq \sum_{i=1}^{p} |\dot{x}_i(t)| = \|f_1(x)\|_1 \tag{3.20}$$

D'après l'Hypothèse 1, f_1 est lipchitzienne, il existe alors $l_1 > 0$ (constante de Lipchitz par rapport à x_1) et $l_2 > 0$ (constante de Lipchitz par rapport à x_2), telles que :

$$\begin{aligned} \dot{V}_1\big(x_1(t)\big) &\leq l_1\|x_1(t)\|_1 + l_2\|x_2(t)\|_1 \\ &= l_1 V_1(x_1(t)) + l_2\|x_2(t)\|_1 \end{aligned} \tag{3.21}$$

Ce qui implique comme $V_1(t_k^+) = 0$:

$$\forall t \in [t_k, t_{k+1}[: \quad V_1\big(x_1(t)\big) \leq l_2 \int_{t_k}^{t} e^{l_1(t-\tau)} \|x_2(t)\|_1 \, d\tau \tag{3.22}$$

Ceci implique que $V_1\big(x_1(t_{k+1})\big) \leq \frac{l_2}{l_1}\big(e^{l_1(t_{k+1}-t_k)} - 1\big)\|x_2(t_k)\|_1$

A partir de là, il est possible de calculer $\|x_{1,\max}(k)\|_1$:

$$\|x_{1,\max}(k)\|_1 = \frac{l_2}{l_1}\left(e^{l_1(t_{k+1}-t_k)} - 1\right)\|x_2(t_k)\|_1 \tag{3.23}$$

En utilisant cette dernière inégalité dans (3.17), On obtient l'inégalité suivante :

$$\|x_2(t)\|_2 > \frac{k_v M}{l_v}\frac{l_2}{l_1}\left(e^{l_1(t_{k+1}-t_k)} - 1\right)\|x_2(t_k)\|_1 \tag{3.24}$$

Si $\dot{V}_2 < 0$, alors $\|x_2(t)\|_2 > k_v\|x_2(t_{k+1})\|_2 \; \forall \in [t_k, t_{k+1}]$ et selon la relation entre normes on obtient :

$$\|x_2(t_{k+1})\|_2 > \frac{k_v M}{l_v}\frac{l_2}{l_1}\left(e^{l_1(t_{k+1}-t_k)} - 1\right)\sqrt{n-p}\,\|x_2(t_k)\|_2 \tag{3.25}$$

Dans notre cas, et pour obtenir une séquence contractante, on désire que

$\|x_2(t_{k+1})\|_2 < \|x_2(t_k)\|_2$, ceci nous mène à l'inégalité suivante :

$$\|x_2(t_k)\|_2 > \frac{k_v M}{l_v}\frac{l_2}{l_1}\left(e^{l_1(t_{k+1}-t_k)} - 1\right)\sqrt{n-p}\,\|x_2(t_k)\|_2 \tag{3.26}$$

Ce qui est vérifié si $\frac{k_v M}{l_v}\frac{l_2}{l_1}\left(e^{l_1(t_{k+1}-t_k)} - 1\right)\sqrt{n-p} < 1$

Alors pour tout $t_{k+1} - t_k = \theta_k \leq \theta_{max}$ avec :

$$\theta_{max} = \frac{1}{l_1}\log\frac{l_v l_1}{k_v M l_2\sqrt{n-p}} + 1 \tag{3.27}$$

La séquence $x_2(t_k)$ converge vers zéro quand $k \to \infty$

Corollaire 1

Supposons que les conditions et hypothèses du Théorème sont vérifiées pour le système (3.10) alors :$x_1(t)\ et\ x_2(t)$ convergent vers 0 pour $t \to \infty$.

3.4 OBSERVATEUR IMPULSIF

Considérons la classe des systèmes suivants :

$$\begin{cases} \dot{x}_1(t) = f_1(x_1, x_2, t) \\ \dot{x}_2(t) = f_2(x_1, x_2, t) \\ y(t_k) = x_1(t_k) \end{cases} \tag{3.28}$$

Où $x(t) = (x_1(t)^T,\ x_2(t)^T)^T \in \mathbb{R}^n$est le vecteur d'état, avec $x_1(t) \in \mathbb{R}^p$, $x_2(t) \in \mathbb{R}^{n-p}$ et $y(t_k) \in \mathbb{R}^p$est le vecteur de sortie.

Les fonctions f_1 et f_2 sont continûment différentiables et Lipchitziennes. De plus, les états évoluent dans un espace borné.

L'observateur impulsif du système (3.28) est donné comme suit :

$$\begin{cases} \dot{\hat{x}}_1(t) = f_1(\hat{x}_1, \hat{x}_2, t) \\ \dot{\hat{x}}_2(t) = f_2(\hat{x}_1, \hat{x}_2, t) \\ \hat{x}_1(t_k^+) = x_1(t_k) \end{cases} \tag{3.29}$$

A partir des systèmes (3.28) et (3.29), on obtient le système d'erreurs d'observation :

$$\begin{cases} \dot{e}_1(t) = f_1\big(x_1(t), x_2(t)\big) - f_1\big(\hat{x}_1(t), \hat{x}_2(t)\big) \\ \dot{e}_2(t) = f_2\big(x_1(t), x_2(t)\big) - f_2\big(\hat{x}_1(t), \hat{x}_2(t)\big) \\ e_1(t_k^+) = 0 \end{cases} \tag{3.30}$$

Corollaire 2

Si le système (3.30) vérifie les deux Hypothèses 1 et 2 et les conditions du Théorème, alors il existe un θ_{max} tel que pour chaque séquence impulsive $\theta_k \leq \theta_{max}$, les états de l'observateur (3.29) convergent vers les états du système (3.28).

Ces résultats de stabilité seront utilisés pour synchroniser impulsivement deux oscillateurs chaotiques de Colpitts dans le chapitre qui suit.

3.5 APPLICATION A LATRANSMISSION SECURISEE

Il existe plusieurs methodes proposées qui combine la synchronisation du chaos avec la communication sécurisée.Elles sont souvent basées sur le masquage , la commutation, ou la modulation des signaux chaotiques.

Dans la suite de ce chapitre, nous allons expliquer comment intégrer la théorie des systèmes impulsifs dans les techniques de cryptographie pour concevoir un schéma de transmission sécurisée [20] [21].

Le système de transmission proposé est constitué de deux blocs (voir Fig.3.1):

Un bloc emetteur contient un oscillateur chaotique de Colpitts, un module de cryptage pour masquer l'information utile et un module de composition pour multiplexer deux signaux : le signal de synchronisation et le signal porteur d'information.

Un autre bloc servant de recepteur contient également un oscillateur de Colpitts identique au premier, un bloc de décomposition pour decomposer le sigal transmis en un signal de synchronisation et un signal porteur d'information. Un bloc de decryptage est conçu pour récupérer l'information utile.

L'information (message) est cryptée par l'une des méthodes de cryptage. La clé du cryptage secrète est l'ensemble des paramètres de l'oscillateur Colpitts.

Chaque cycle de durée Tcompte une région de synchronisation de durée d et le reste du cycle est consacré à la transmission du signal d'information [9] [10] (voir figure 3.2).

La région dcomprend des impulsions de synchronisation qui serviront à synchroniser l'emetteur et le recepteur quand à la région T-d, elle contient le signal chaotique porteur de l'information. Après multiplexage des deux signaux, le signal résultant est envoyé au recepteur à travers le canal publique.Le choix des durées doit être effectué tel que le rapport signal utile / signal transmis soit proche de l'unité assurant ainsi une bonne transmission. De plus, la période T est choisie de telle sorte que les deux systèmes chaotiques soient synchronisés.

Au niveau du récepteur, le bloc de décomposition est utilisé pour éxtraire les signaux de synchronisation et d'information séparement. Les impulsions sont alors utilisées pour synchroniser les deux systèmes chaotiques, ce qui permet de retrouver la clé pour decrypter l'information utile [19][20][21].

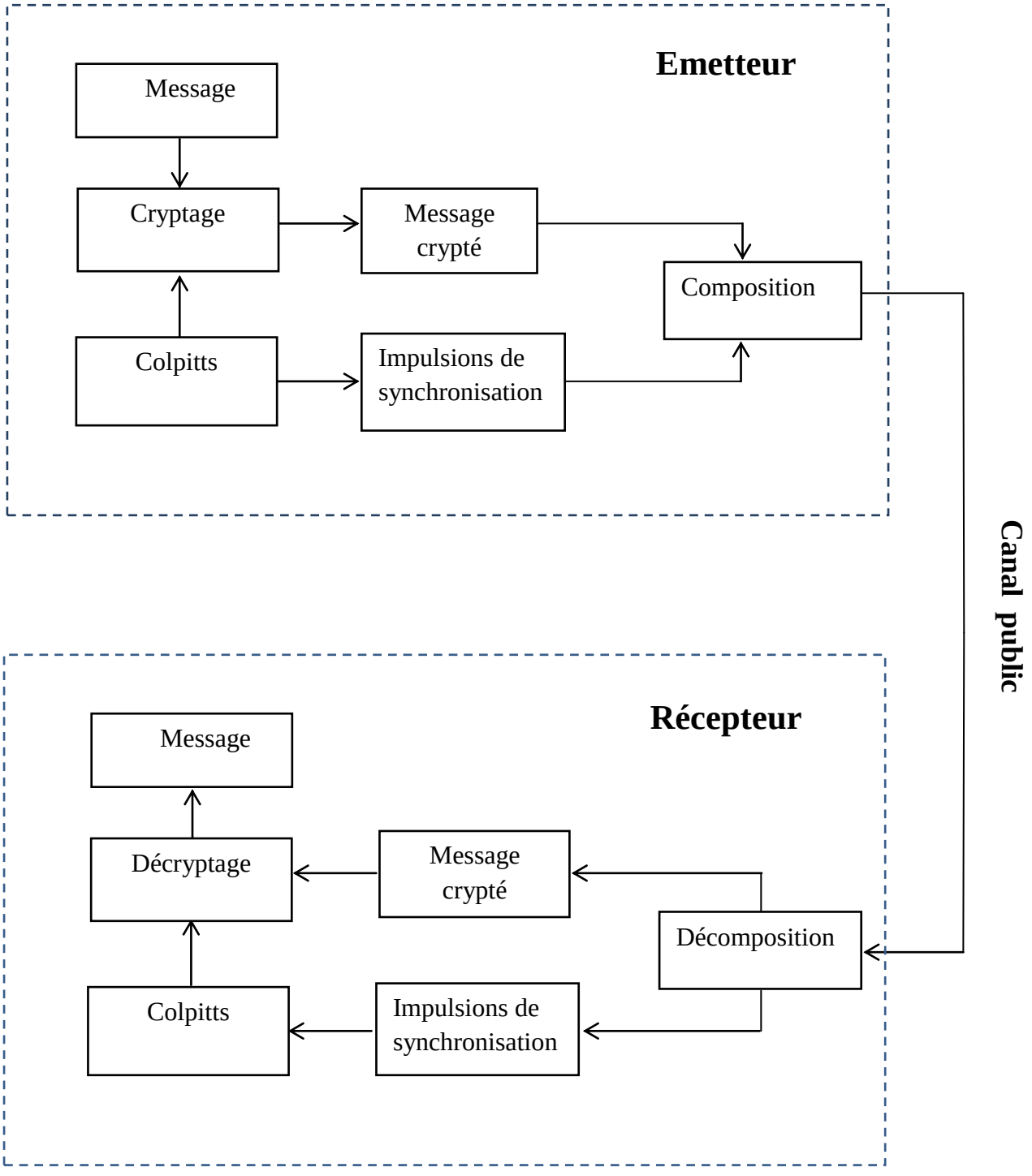


Fig. 3. 1 Diagramme bloc de la synchronisation impulsive

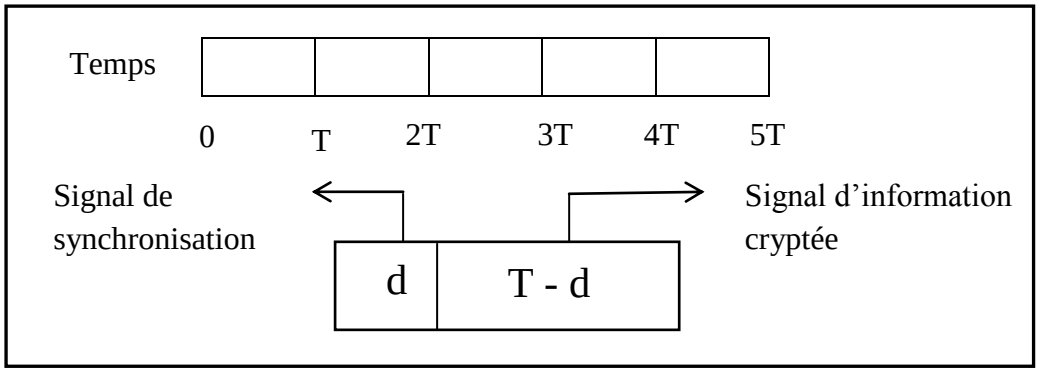


Fig. 3. 2 Cycle de transmission

3.4 CONCLUSION

Dans cette partie du mémoire, des concepts de base sur les systèmes impulsifs sont introduits pour mieux assimiler la notion de synchronisation impulsive.

Les systèmes impulsifs sont définis par deux dynamiques différentes :

- Une dynamique décrite par des équations différentielles ordinaires pour expliquer l'évolution du système avant l'arrivée des impulsions.
- Une dynamique formulée par une équation aux différences pour traduire le changement du comportement du système à l'arrivée des impulsions.

C'est à partir de ça, qu'un schéma de transmission chaotique a été proposé dans ce chapitre. Les impulsions vont servir à « forcer » l'état du système chaotique au niveau récepteur à suivre l'état chaotique de l'émetteur, d'où l'appellation : synchronisation impulsive.

Les résultats d'application de cette méthode seront illustrés à la fin du prochain chapitre.

CHAPITRE 4 : REALISATION DU SYSTEME DE TRANSMISSION

4.1 INTRODUCTION

De nombreux oscillateurs générateurs du chaos ont été proposés dans la littérature. Ces circuits diffèrent par leurs structures, par leurs éléments électriques ainsi que par la technologie utilisée. Ils offrent la possibilité de manifester des comportements chaotiques des plus basses fréquences aux plus hautes.

L'un des oscillateurs les plus utilisés dans la transmission est le circuit du Chua [19] [20] [60], c'est un circuit simple qui dispose d'une résistance négative non linéaire qui lui transporte de l'énergie. La génération du comportement chaotique se fait par un choix adéquat et précis des paramètres électriques du circuit.

L'exemple d'oscillateurs chaotiques choisi pour effectuer ce travail de mémoire est l'oscillateur de Colpitts. Le choix est justifié par la simplicité de la structure de cet oscillateur, il comporte une non linéarité intrinsèque liée à la caractéristique exponentielle du transistor. La modification des conditions de fonctionnement permet de générer un comportement chaotique. De plus, il est possible de faire évoluer la fréquence fondamentale vers des fréquences élevées par un choix de technologie appropriée du transistor.

Dans ce chapitre, nous allons d'abord expliquer en détail le fonctionnement de ce circuit, étudier son comportement en différents régimes puis expliquer l'utilisation des signaux générés par cet oscillateur pour le masquage et la transmission de l'information.

Un signal message sera injecté de deux façons différentes, l'une par addition au signal chaotique généré par l'oscillateur et l'autre par inclusion dans la dynamique de l'oscillateur. Dans le premier cas, des résultats de simulations sous Matlab ainsi que des résultats expérimentaux seront donnés. Par contre dans le second cas, nous présenterons uniquement des résultats de simulation sous Matlab.

4.2 PRESENTATION DE L'OSCILLATEUR COLPITTS

Dans les paragraphes suivants, Une analyse générale de l'oscillateur Colpittssera effectuée pour expliquer les caractéristiques, le fonctionnement et les différents comportements de ce circuit.

4.2.1 CIRCUIT ELECTRONIQUE

Le circuit en basses fréquences de l'oscillateur Colpitts utilisé dans ce mémoire est un montage en base commune. Cette structure permet d'obtenir un gain plus élevé en autorisant une bande passante plus large.

L'oscillateur comporte un transistor bipolaire classique, un circuit résonnant LC connecté entre le collecteur et la base du transistor. Une partie de la tension est retournée à l'émetteur [39] [40].

Le point de fonctionnement du transistor est déterminé par les tensions d'alimentation V_1et V_2.

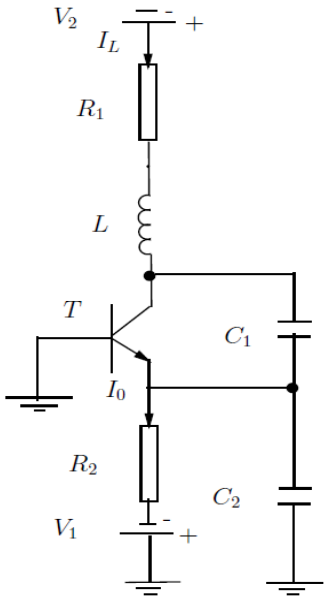


Fig. 4.1 Oscillateur de Colpitts avec $\boldsymbol{R_1 = 47\Omega, R_2 = 1k}$, $\boldsymbol{C_1 = C_2 = 470nF}$, $\boldsymbol{L = 1mH}$, $\boldsymbol{T}$: $\boldsymbol{2N2222}$

4.2.2 CONDITIONS D'OSCILLATION

La figure suivante montre la représentation la plus élémentaire d'un oscillateur électronique, il s'agit d'un amplificateur dans une boucle de réaction [14] [47].

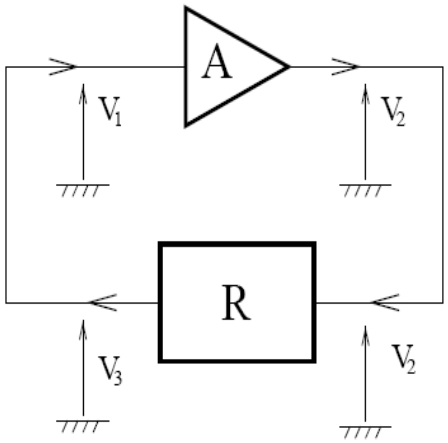


Fig. 4.2 Structure d'un oscillateur de réaction

Supposons que les différentes grandeurs du montage soient sinusoïdales c'est-à-dire :

$$V_2 = |A|.e^{j\,\Phi_A} V_1$$

Et $$V_3 = |R|.e^{j\,\Phi_R} V_2$$

Ceci implique $$V_3 = |R|.e^{j\,\Phi_R} V_2 = |A||R|.e^{j\,(\Phi_R + \Phi_A)}\, V_1 \qquad (4.1)$$

Selon le critère de Barkhausen, le système peut osciller à condition que la phase du gain de la boucle soit nulle, et l'amplitude soit unitaire:

$$\begin{cases} |A|.|R| = 1 \\ \Phi_A + \phi_R = 0 + 2k\pi, \quad k \in \mathbb{Z} \end{cases} \qquad (4.2)$$

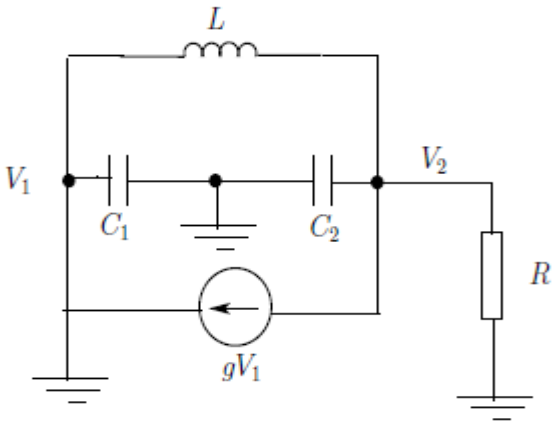


Fig. 4.3 Principe de l'oscillateur de Colpitts

En appliquant la loi de Kirchhoff, les équations du courant aux deux extrémités de l'inductance sont comme suit :

$$\begin{cases} -gV_1 - \frac{V_2}{R} - jC_2\omega V_2 + \frac{V_1 - V_2}{jL\omega} = 0 \\ \frac{V_2 - V_1}{jL\omega} - jC_1\omega V_1 + gV_1 = 0 \end{cases} \tag{4.3}$$

En remplaçant la valeur de V_2 dans la première équation, on obtient :

$$\left[-g + \frac{1}{jL\omega}\right]\frac{1}{jL\omega} - \left[jC_1\omega + \frac{1}{jL\omega}\right]\left[\frac{1}{R} + jC_2\omega + \frac{1}{jL\omega}\right] = 0 \tag{4.4}$$

La valeur de la fréquence d'accord ω est calculée par annulation de la partie imaginaire dans l'équation (4.4)

$$C_1C_2RL\omega^2 - (C_1 + C_2)R\omega = 0 \Longrightarrow \omega = \frac{1}{\sqrt{L\frac{C_1C_2}{C_1+C_2}}} \tag{4.5}$$

En annulant la partie réelle, nous obtenons la condition d'oscillation de l'oscillateur Colpitts :

$$-Rg + LC_1\omega^2 - 1 = 0 \Longrightarrow R = \frac{LC_1\omega^2 - 1}{g} \tag{4.6}$$

L'oscillation démarre lorsque R supérieur à la valeur obtenue par (4.6). En remplaçantω, on trouve la condition d'oscillation suivante :

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

4.2.3 REPRESENTATION D'ETAT

Le circuit se met en équation en utilisant la loi des mailles et la loi des nœuds afin d'obtenir le système suivant [14] [15]:

$$\begin{cases} \frac{dV_{C1}}{dt} = -\frac{1}{C_1} f(-V_{C2}) + \frac{1}{C_1} I_L \\ \frac{dV_{C2}}{dt} = \frac{1}{C_2} I_L - \frac{1}{C_2} I_0 \\ \frac{dI_L}{dt} = -\frac{1}{L_1} V_{C1} - \frac{1}{L_1} V_{C2} - \frac{R_1}{L_1} I_L + \frac{V_2}{L_1} \end{cases} \quad (4.7)$$

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

$$I_E = f(V_{BE}) = f(-V_{C2}) \cong I_S \left[\exp\left(\frac{V_{BE}}{V_T}\right)\right] \cong I_S \left[\exp\left(\frac{-V_{C2}}{V_T}\right)\right] \quad (4.8)$$

Où $V_T = 27mv$

Et I_s désigne le courant de saturation inverse de la jonction base émetteur

Le système (4.7) peut être normalisé comme suit :

$$\begin{cases} z_1(t) = \frac{1}{V_T}\left[V_{C1}(\omega_0 t) - V_{C_{1o}}\right] \\ z_2(t) = \frac{1}{V_T}\left[V_{C2}(\omega_0 t) - V_{C_{2o}}\right] \\ z_3(t) = \frac{1}{I_0}\left[I_L(\omega_0 t) - I_{L_o}\right] \end{cases} \quad (4.9)$$

Les équations d'états de l'oscillateur présenté au début du chapitre sont finalement données sous forme :

$$\begin{cases} \dot{z}_1 = \frac{g}{q(1-k)}(-\eta(z_2) + z_3) \\ \dot{z}_2 = \frac{g}{q_k} z_3 \\ \dot{z}_3 = -\frac{q_k(1-k)}{g}([z_1 + z_2] - \frac{1}{q} z_3) \end{cases} \quad (4.10)$$

Avec : $\eta(z_2) = \exp(-z_2) - 1$ et $k = \frac{C_2}{C_1 + C_2}$

Où q représente le facteur de qualité du circuit résonnant LC :

$$q = \frac{LW_0}{R} \tag{4.11}$$

et g est le gain de la boucle de réaction vérifiant la critère de Barkhausen, il est obtenu par l'équation :

$$g = \frac{LI_0}{(C_1+C_2)R_1V_T} \tag{4.12}$$

I_0 le paramètre de contrôle appelé aussi paramètre de bifurcation comme il a été mentionné dans le premier chapitre du mémoire.

En posant $a_1 = \frac{g}{q(1-k)}$, $a_2 = \frac{g}{qk}$, $a_3 = \frac{qk(1-k)}{g}$, $a_4 = \frac{1}{q}$, $y = z_2$

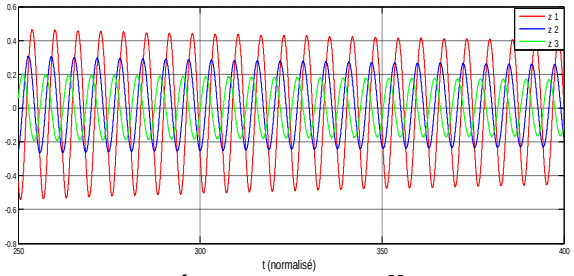
La représentation du système se simplifie :

$$\begin{cases} \dot{z}_1 = a_1(-exp(-z_2) + 1 + z_3) \\ \dot{z}_2 = a_2 z_3 \\ \dot{z}_3 = -a_3(z_1 + z_2) - a_4 z_3) \\ y_1 = z_2 \end{cases} \tag{4.13}$$

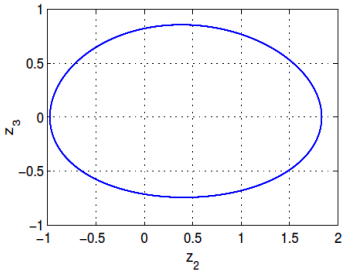
En faisant varier les paramètres g et q du système (4.10), nous obtenons différents types d'oscillations. Pour démarrer l'oscillation, nous avons fixé la valeur de g légèrement supérieure à 1 pour satisfaire la condition de Barkhausen. Les résultats obtenus pour différentes valeurs de g sont donnés par la figure (4.4).

Pour $g = 1.0029$, la condition de Barkhausen et vérifiée ; le système présente des oscillations sinusoïdales et par conséquent un cycle limite dans le plan de phase $z_2 - z_3$. En augmentant la valeur de g à 2.13, le système présente des oscillations sinusoïdales à deux périodes correspondant à deux cycle limites dans le plan de phase (Fig. 4.4.b). Pour $g = 2.4$ le système oscille avec quatre périodes correspondant à 4 cycles limites en plan de phase (Fig. 4.4.c)

Pour $g = 4.46$, le système présente un comportement chaotique correspondant à un attracteur étrange en plan de phase (Fig. 4.4.d).

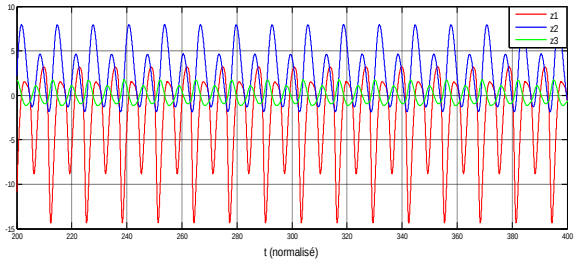


Réponses temporelles

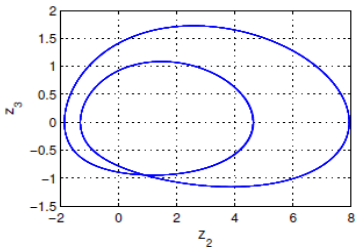


Plan de phase

(a) : g = 1.0029

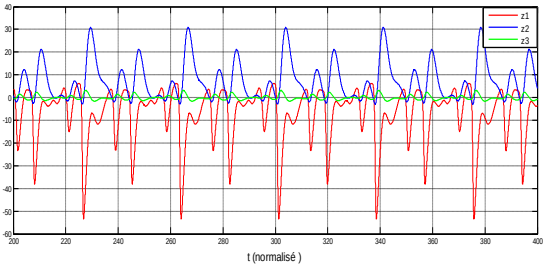


Réponses temporelles

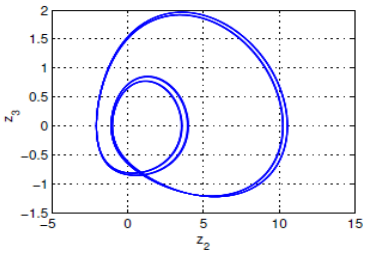


Plan de phase

(b) : g = 2.13

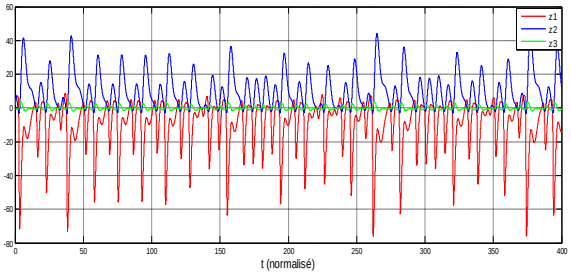


Réponses temporelles

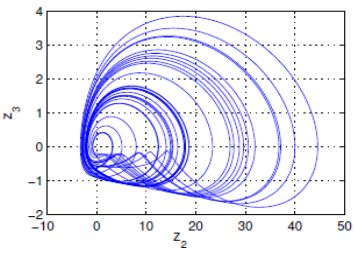


Plan de phase

(c) : g =2.4



Réponses temporelles



Plan de phase

(d) : g = 4.46

Fig. 4.4 Différents régimes de l'oscillateur de Colpitts

4.3 SYNCHRONISATION IMPULSIVEDE DEUX OSCILLATEURS

Dans cette partie, nous proposons un observateur impulsif à l'oscillateur de Colpitts (4.13). Le système Colpitts-Observateur sera utilisé pour la transmission de données

4.3.1 L'OBSERVATEUR IMPULSIF

Dans cette section, un observateur impulsif pour le système Colpitts sera calculé pour servir de récepteur dans le système de transmission final.Pour concevoir un observateur impulsif pour le système (4.13)nous tenons compte des hypothèses citées dans le chapitre précédent.

En choisissant la sortie $y = z_2$, la dynamique de l'observateur est donc définie comme suit :

$$\begin{cases} \dot{\hat{z}}_1 = a_1(-\exp(-\hat{z}_2) + 1 + \hat{z}_3) \\ \dot{\hat{z}}_2 = a_2\hat{z}_3 \\ \dot{\hat{z}}_3 = -a_3(\hat{z}_1 + \hat{z}_2) - a_4\hat{z}_3 \\ \hat{z}_2(t_k^+) = z_2(t_k) \end{cases} \tag{4.14}$$

On définit le vecteur d'erreurs d'observation suivant :

$$E = (e_1, e_2, e_3)^T$$

telles que :

$$e_1 = z_1 - \hat{z}_1\,,\ e_2 = z_2 - \hat{z}_2,\ e_3 = z_3 - \hat{z}_3 \tag{4.15}$$

Le système d'erreurs dynamiques est alors donné sous forme :

$$\begin{cases} \dot{e}_1 = a_1 exp(-z_2)(\exp(e_2) - 1) + a_1 e_3 \\ \dot{e}_2 = a_2 e_3 \\ \dot{e}_3 = -a_3(e_1 + e_2) - a_4 e_3 \\ e_2(t_k^+) = 0 \end{cases} \tag{4.16}$$

En négligeant les termes d'ordre supérieur dans la série de Taylor de l'expression de $\exp(e_2)$ le système devient [14] [23]:

$$\begin{cases} \dot{e}_1 = a_1(-exp(-z_2)e_2 + e_3) \\ \dot{e}_2 = a_2 e_3 \\ \dot{e}_3 = -a_3(e_1 + e_2) - a_4 e_3 \\ e_2(t_k^+) = 0 \end{cases} \tag{4.17}$$

Où : $$f_1(e_1, e_2, e_3) = a_2 e_3 \quad (4.18)$$

$$f_2(e_1, e_2, e_3) = \begin{pmatrix} 0 & a_1 \\ -a_3 & -a_4 \end{pmatrix} \begin{pmatrix} e_1 \\ e_2 \end{pmatrix} + \begin{pmatrix} a_1 \exp(-xz_2(t)) \\ -a_3 \end{pmatrix} e_2 \quad (4.19)$$

Comme les états évoluent dans un espace borné, alors les erreurs sont bornées et par conséquent f_1 est Lipchitzienne.

En posant $E_2 = \begin{pmatrix} e_1 \\ e_3 \end{pmatrix}$, On définit la fonction de Lyapunov V_2 comme suit :

$$V_2(e_1, e_3) = (e_1 e_3) \begin{pmatrix} p_1 & 0 \\ 0 & p_2 \end{pmatrix} \begin{pmatrix} e_1 \\ e_3 \end{pmatrix} \quad (4.20)$$

Avec $p_1, p_2 > 0$

On obtient :

$$\frac{\partial V_2}{\partial E} A E_2 = \begin{pmatrix} e_1 \\ e_3 \end{pmatrix}^T \begin{pmatrix} 0 & a_1 p_1 - a_3 p_2 \\ a_1 p_1 - a_3 p_2 & -2a_4 p_2 \end{pmatrix} \begin{pmatrix} e_1 \\ e_3 \end{pmatrix}$$

$$\leq \lambda_{min} \begin{pmatrix} 0 & a_1 p_1 - a_3 p_2 \\ a_1 p_1 - a_3 p_2 & -2a_4 p_2 \end{pmatrix} \|E_2\|_2^2$$

On peut alors choisir p_1 et p_2 tels que $\lambda_{min} \begin{pmatrix} 0 & a_1 p_1 - a_3 p_2 \\ a_1 p_1 - a_3 p_2 & -2a_4 p_2 \end{pmatrix} < 0$

Les conditions du théorème 1 sont satisfaites et on peut conclure que l'observateur (4.14) converge vers le système de Colpitts (4.13).

En appliquant l'équation (3.27), nous pouvons finalement montrer que $\theta_{max} = 0.4$. Cette valeur correspond à la période maximale de synchronisation.

4.3.2 SCHEMA DE TRANSMISSION

La synchronisation impulsive des deux oscillateurs Colpitts a permis de réaliser un schéma de transmission à porteuse chaotique. Le schéma synoptique de transmission en utilisant le système chaotique de Colpitts est donné par la figure 4.5

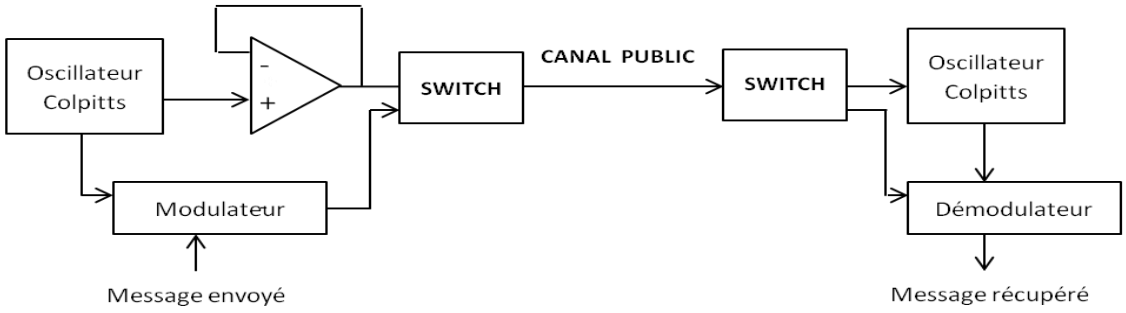


Fig. 4. 5 Modulation à porteuse chaotique

Le circuit de la synchronisation impulsive est constitué de deux circuits de Colpitts identiques, un suiveur de tension pour établir une synchronisation unidirectionnelle et un switch pour faire passer le signal chaotique (voir Fig. 4.6). L'envoi du signal chaotique se fait pendant une durée d à travers un switch. Le cycle se répète à chaque période T (voir Fig. 4.7).

La fréquence du signal impulsif utilisé est de 160Khz et le rapport cyclique est fixé à 10% de la période du signal.

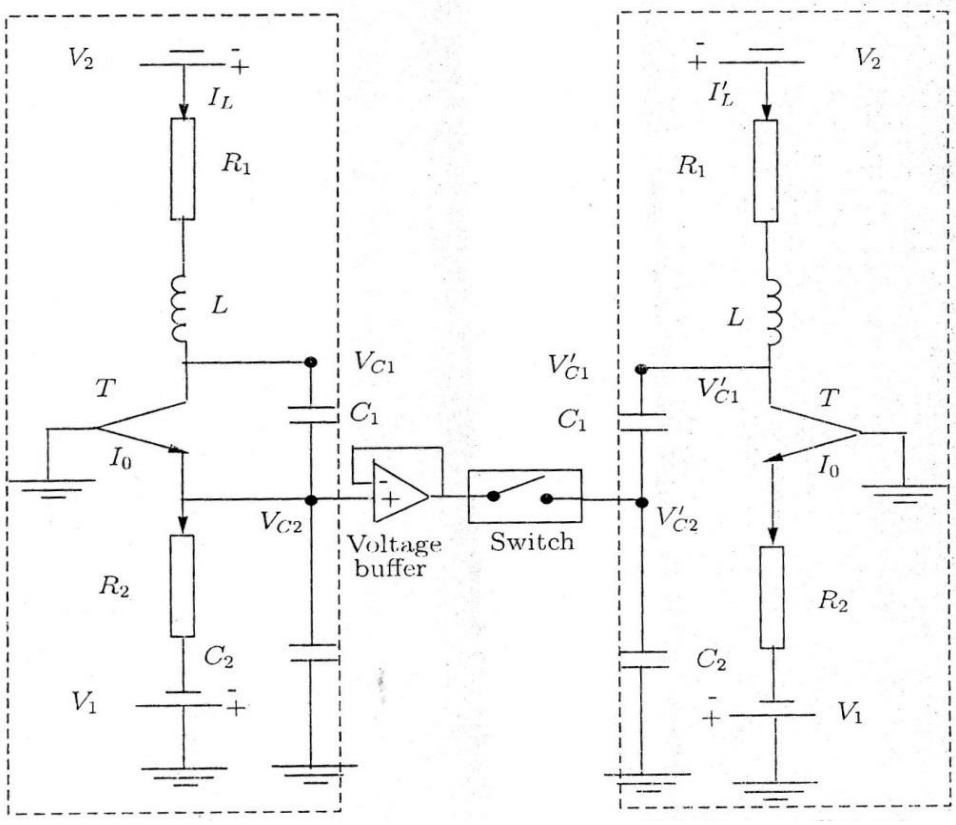


Fig. 4. 6 Circuit de synchronisation de deux oscillateurs de Colpitts

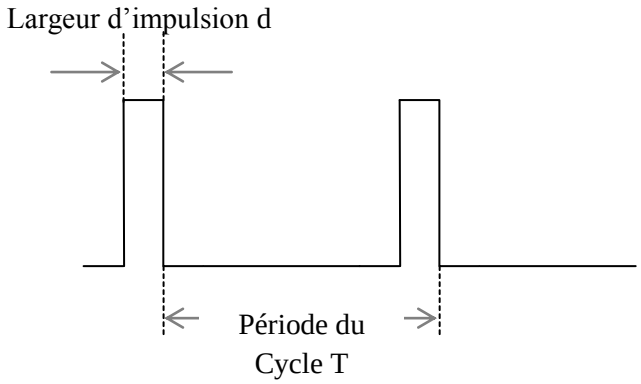


Fig. 4. 7 Chronogramme de transmission

4.4 RESULTATS DE SIMULATION ET EXPERIMENTATION

Cette partie est consacrée à la présentation des résultats de simulation sous Matlab/Simulink et des résultats expérimentaux.

4.4.1 RESULTATS DE SIMULATION

Ici, nous présentons les résultats de simulations numériques obtenus sous Matlab permettant d'illustrer les performances du système de transmission proposé.Il est à noter que les grandeurs temps, tensions et courant sont normalisées.

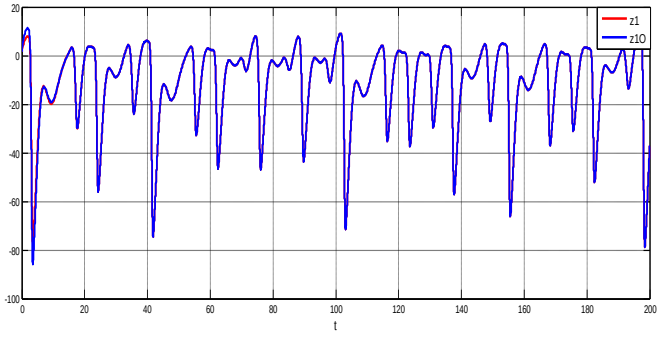
Les simulations sont effectuées en utilisant la méthode numérique Runge -Kutta pour la résolution des équations différentielles avec un temps de calcul égal à 0.0004.

Pour obtenir le régime chaotique, les paramètres du système sont fixés comme suit :

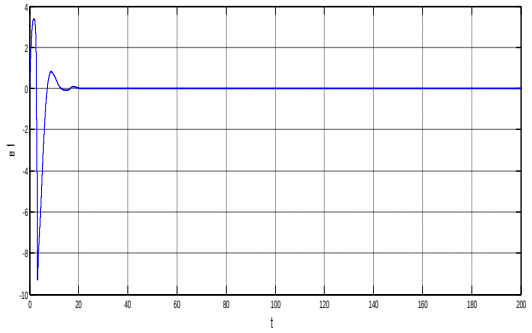
$g = 4.46, q = 1.38, k = 0.5$. Les conditions initialesde l'oscillateur ainsi que de l'observateur sont choisis à l'intérieur du bassin de l'attracteur chaotiques : $z_1(0) = 1.6$, $z_2(0) = 8$, $z_3(0)$=0.1.

La période des impulsions de synchronisation est choisie égale à $\theta_{max} = T = 0.04$, la durée de chaque impulsions est de d=0.04.La figure (4.8) présente les états synchronisés de l'oscillateur et de l'observateur ainsi que les erreurs de synchronisation entre les états synchronisés en utilisant la méthode de la synchronisation impulsive.

En observant les résultats de synchronisation, on peut constater que tous les états sont synchronisés après un instant $t = 12$ (t normalisé).

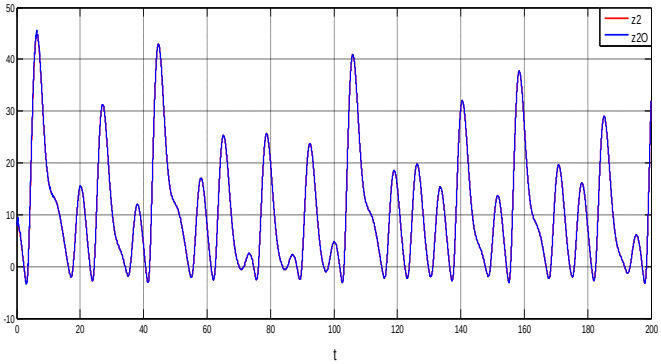


a : Etats z_1 et $\hat{z}_1$

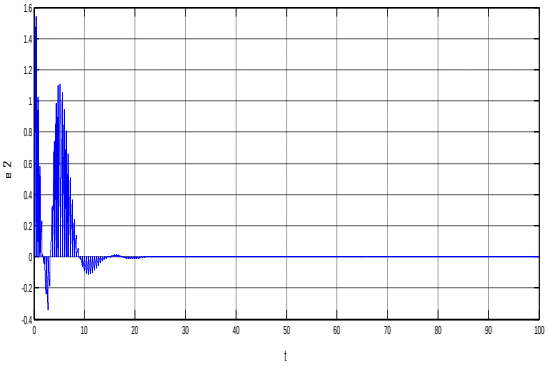


b : Erreur de synchronisation $\boldsymbol{e_1 = z_1 - \hat{z}_1}$

Fig. 4. 8 Résultats de synchronisation des états $\boldsymbol{z_1}$ et $\boldsymbol{\hat{z}_1}$

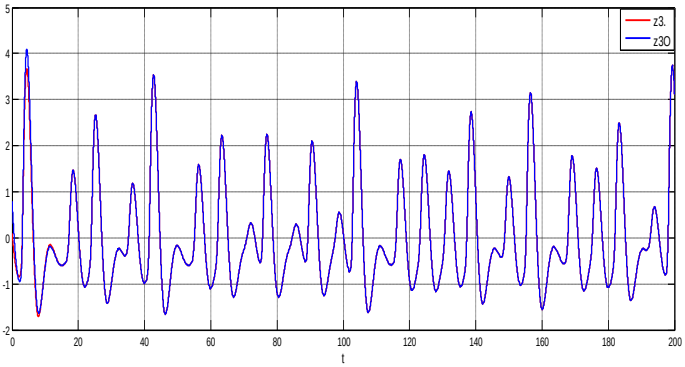


a : Etats z_2 et $\hat{z}_2$

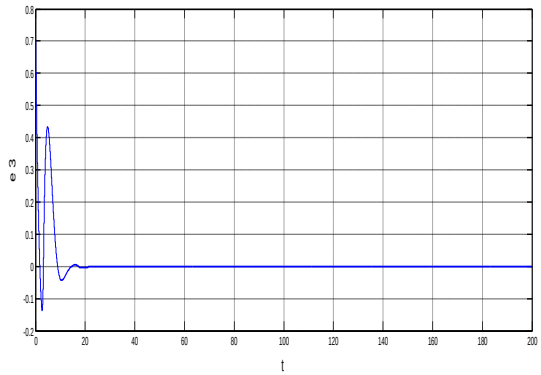


b : Erreur de synchronisation $e_2 = z_2 - \hat{z}_2$

Fig. 4. 9 Résultats de synchronisation des états $\boldsymbol{z_2}$ et $\boldsymbol{\hat{z}_2}$



a : Etats z_3 et $\hat{z}_3$



b : Erreur de synchronisation $e_3 = z_3 - \hat{z}_3$

Fig. 4. 10 Résultats de synchronisation des états $\boldsymbol{z_3}$ et $\boldsymbol{\hat{z}_3}$

Le plan de phase des deux signaux z_2 et $\hat{z}_2$ montre une droite de 45° (figure 4.11). Ceci implique que les deux oscillateurs sont bien synchronisés puisqu'on retrouve le même signal à la sortie du deuxième système.

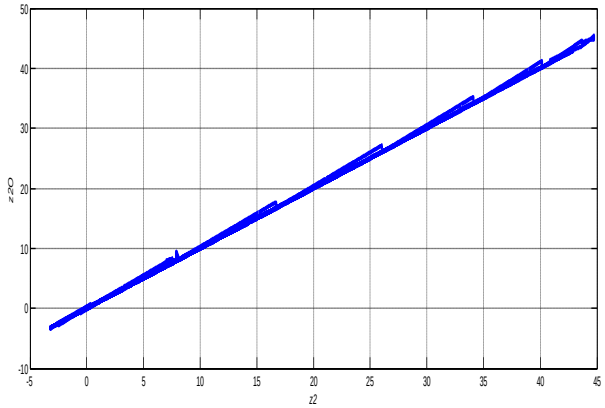
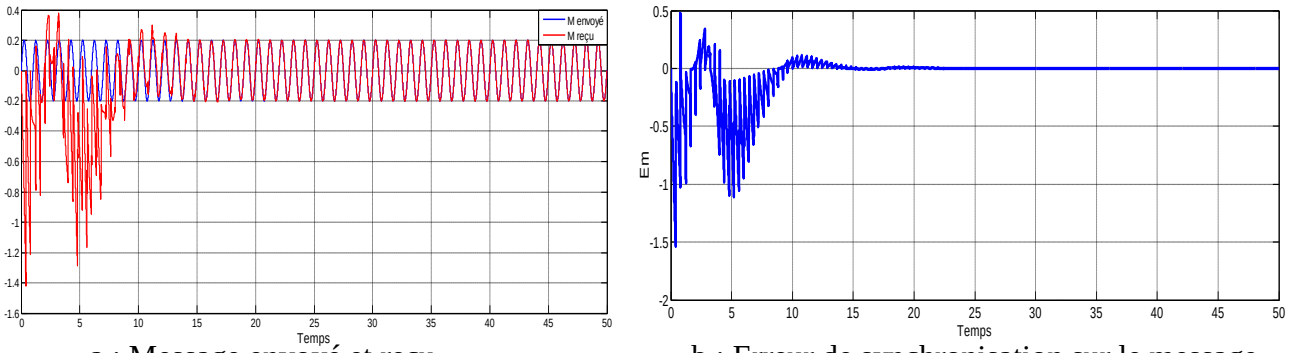


Fig. 4. 11 Plan de phase de deux signaux synchronisés $\boldsymbol{z_2}$ et $\boldsymbol{\hat{z}_2}$

Une fois les états de sorties des deux oscillateurs synchronisés, le message est récupéré au niveau du récepteur.

Deux modes de cryptage différents sont utilisés pour masquer le message. Dans le premier cas Le message M est additionné à l'état z_3 de l'oscillateur chaotique au niveau de l'émetteur. Dans le deuxième cas, le message est inclus dans la dynamique z_1 de l'oscillateur.

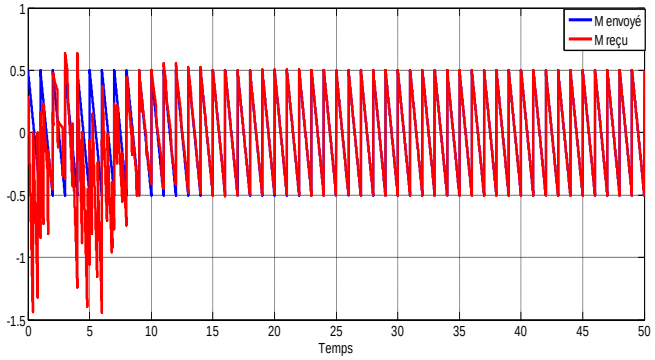
Les figures (4.12), (4.13) et (4.14) illustrent les résultats de récupération du message M dans le cas de cryptage par addition.



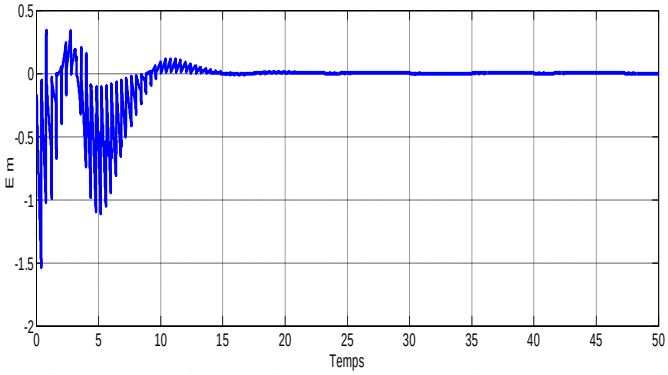
a : Message envoyé et reçu

b : Erreur de synchronisation sur le message.

Fig. 4. 12 Récupération d'un signal sinusoïdal par cryptage additif

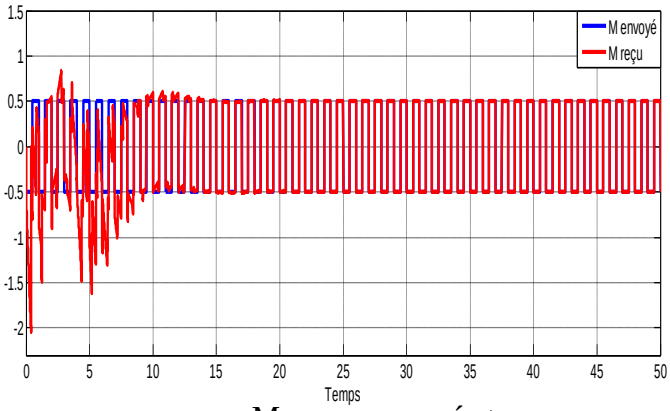


a : Message envoyé et reçu

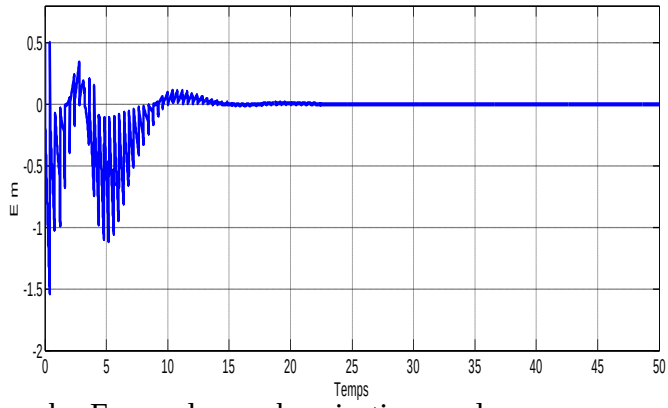


b : Erreur de synchronisation sur le message

Fig. 4. 13 Récupération d'un signal message triangulaire par cryptage additif



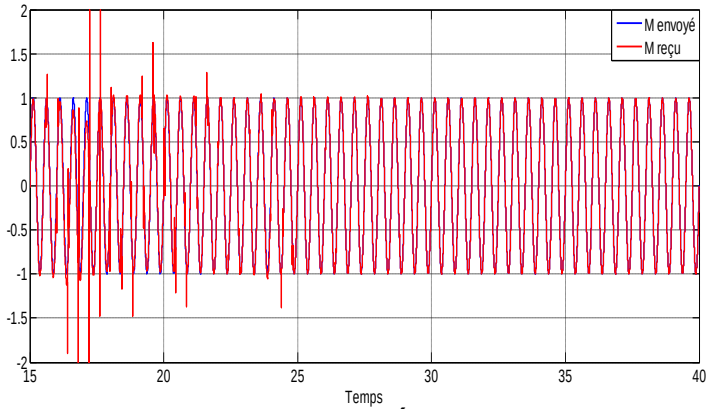
a : Message envoyé et reçu



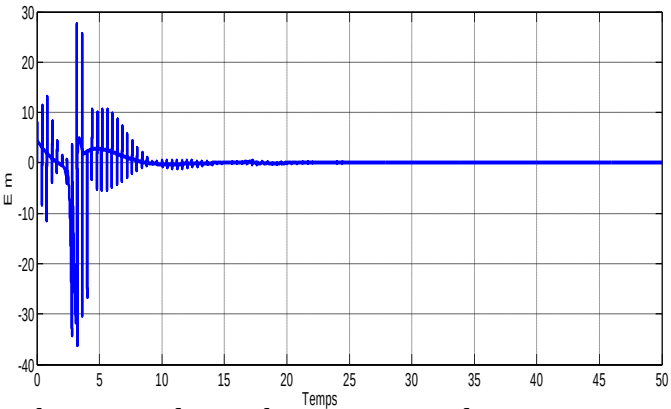
b : Erreur de synchronisation sur le message

Fig. 4. 14 Récupération d'un signal carré par cryptage additif

Les figures (4.15) et (4.16) illustrent les résultats de récupération du message M dans le cas de cryptage par la méthode d'inclusion.

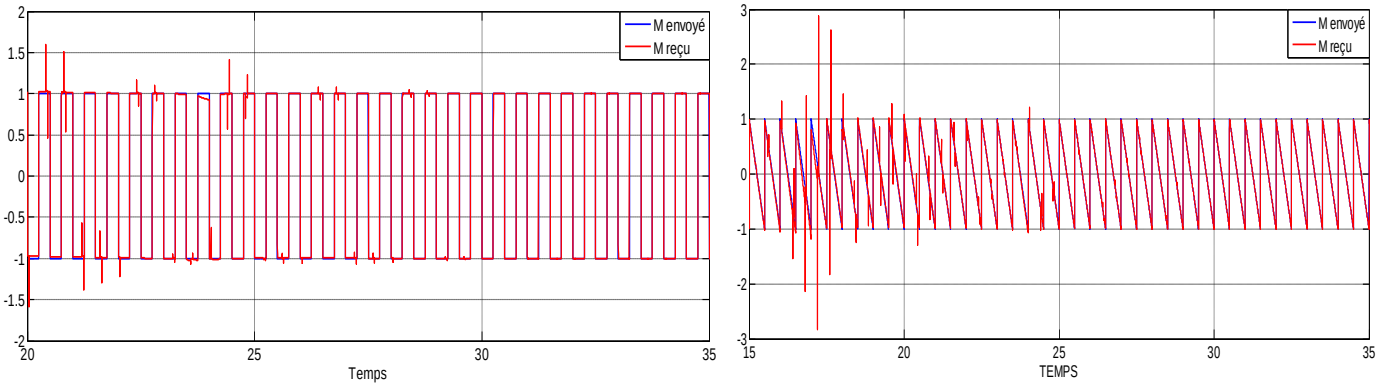


a : Message envoyé et reçu



b : Erreur de synchronisation sur le message

Fig. 4. 15 Récupération d'un signal sinusoïdal par la méthode d'inclusion



a : Message carré b : Message triangulaire

Fig. 4. 16 Récupération des messages carré et triangulaire par la méthode d'inclusion

A travers ces résultats, nous constatons bien qu'une fois les synchronisations des états sont assurées, les messages envoyés sont parfaitement récupérés. Ceci illustre les performances de la méthode de synchronisation impulsive.

4.4.2 REALISATION ET RESULTATS EXPERIMENTAUX

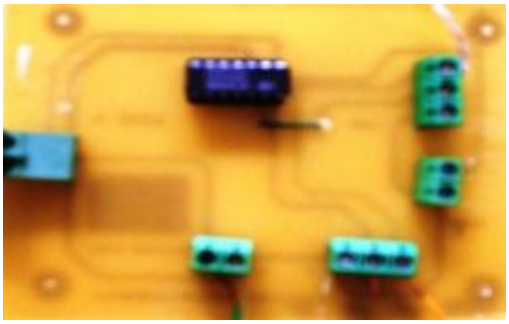
Les deux circuits de Colpitts qui servent d'émetteur et du récepteur dans notre système de transmission sont réalisés expérimentalement (voir Fig. 4.17).Ici nous avons réalisé le système de transmission par addition car il est simple à implémenter. Les mesures temporelles des signaux VC_2 et I_L issus du système (4.7) sont visualisés sur un oscilloscope numérique de Type HAMEG HM407-2.

La figure4.18 montre les comportements obtenus pour chaque circuit, en fixant la tension V_2 à 18V et en jouant sur la tension base-émetteur V_1.

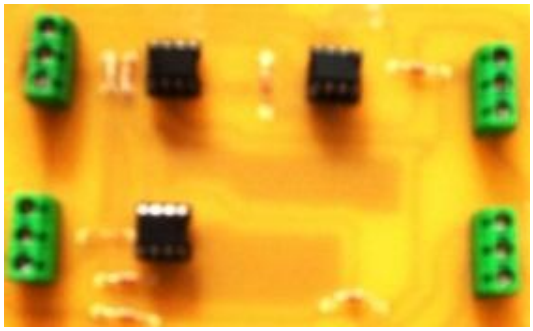
Le début d'oscillation a lieu lorsque $V_1 = 4.4\,V$, le plan de phase des deux signaux indique un cycle limite, un doublement de période apparait à $V_1 = 5\,V$, le nombre de périodes augmente encore à 4 puis à 8 lorsque la tension V_1 atteint les valeurs $12\ V$ et $16V$ respectivement.

Un comportement chaotique est observé pour une valeur de V_1 égale à $18\ V$, le plan de phase présente une forme particulière, c'est l'attracteur chaotique étrange. C'est cette valeur qui sera utilisé pour la transmission d'informations.

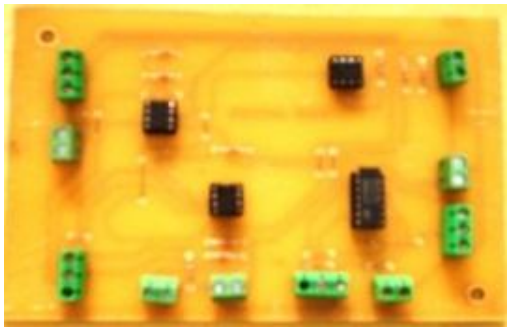
a : Oscillateur de Colpitts utilisé au niveau de l'émetteur et du récepteur



b : Module de composition des signaux

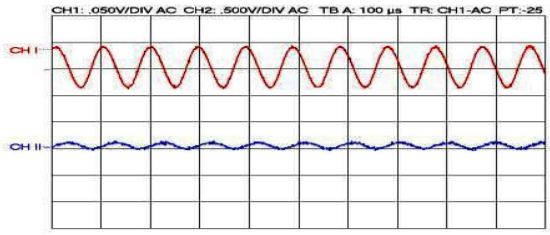


c : Module de cryptage

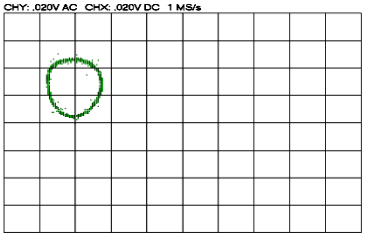


d : module de décomposition et du décryptage

Fig. 4. 17 Circuit de transmission réalisé

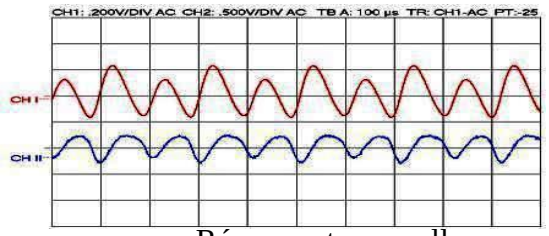


Réponses temporelles

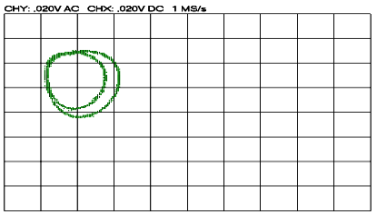


plan de phase

a : V_1= 4.4 V

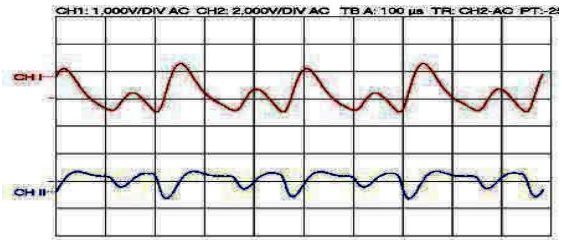


Réponses temporelles

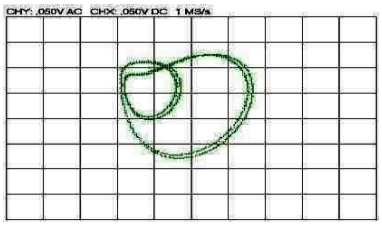


Plan de phase

b : V_1 = 5 V

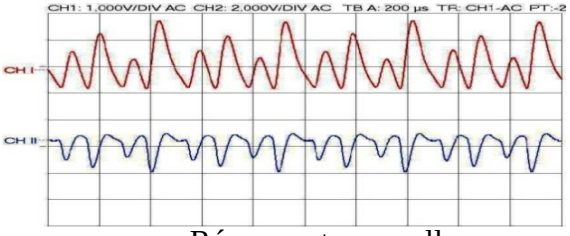


Réponses temporelles

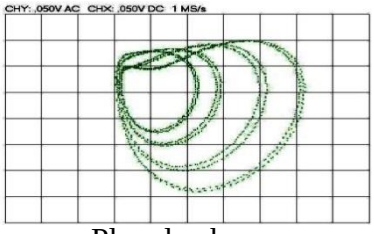


Plan de phase

c : V_1 = 12 V

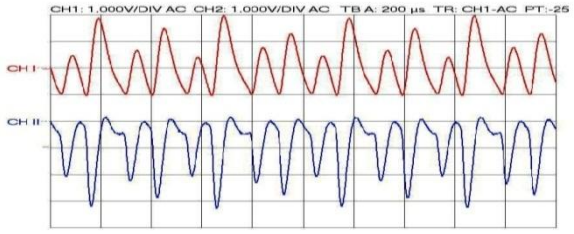


Réponses temporelles

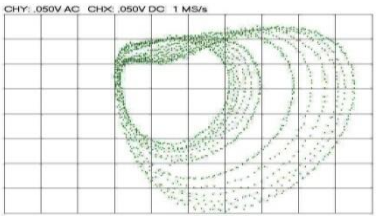


Plan de phase

d : V_1 = 16 V



Réponses temporelles



Plan de phase

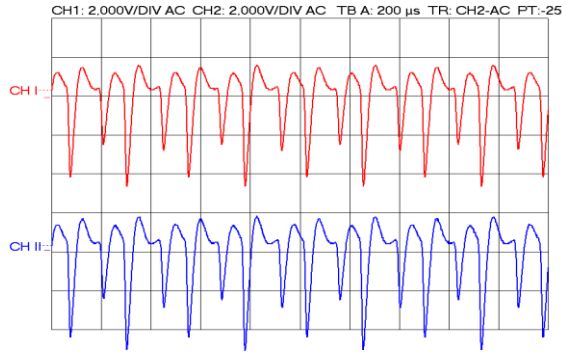
e : V_1 = 18 V

Fig. 4. 18 Différents régimes de l'oscillateur de Colpitts visualisés sur l'oscilloscope

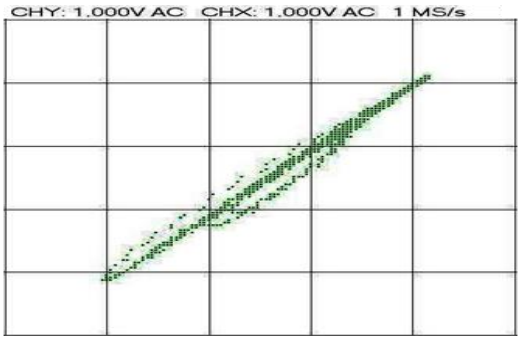
Le module de synchronisation réalisé est composé d'un suiveur et d'un switch. Le suiveur a pour rôle d'assurer un couplage dans une seule direction et par conséquent une synchronisation unidirectionnelle. Le switch sert à la commutation entre le signal de synchronisation échantillonné $y = V_{C2}$ et le signal porteur d'information, le circuit utilisé est le CD 4066 BP.

Les figures (4.19), (4.20) et (4.21) montrent les signaux de sortie des oscillateurs du côté de l'émetteur (V_{C1},V_{C2},I_L) et du côté du récepteur ($V_{C1}o$,$V_{C2}o$, I_Lo) On peut conclure que les deux oscillateurs sont bien synchronisés. La droite apparaissant sur les plans de phase des signaux V_{C2} et $V_{C2}o$ des signaux V_{C1} et $V_{C1}o$ et des signaux I_L et I_{L0} confirment les résultats obtenus par simulation.

Le signal message envoyé est un signal d'amplitude 0.5 V crête à crête et de fréquence 1Khz. La figure (4.22) illustre l'envoi et la réception d'un message sinusoïdal.

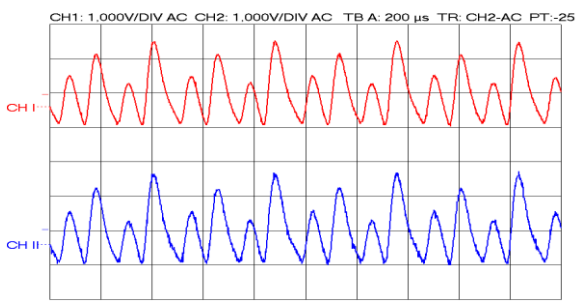


a : Les états V_{c1}(CH I) et $V_{c1}o$(CH II)

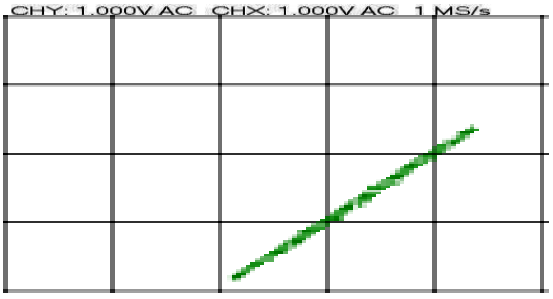


b : Plan de phase $V_{c1} - V_{c1}o$

Fig. 4. 19 Résultats de synchronisation des états V_{c1} et $V_{c1}o$

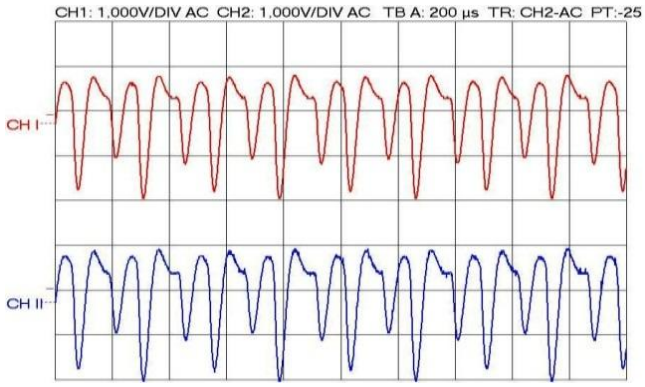


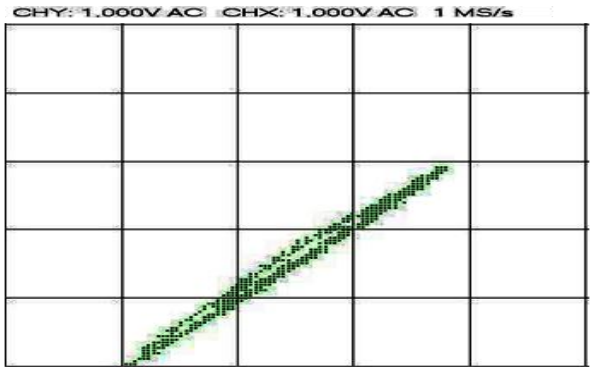
a : Les états V_{c2} (CH I) et $V_{c2}o$(CH II)



b : Plan de phase $V_{c2} - V_{c2}o$

Fig. 4. 20 Résultats de synchronisation des états $\boldsymbol{V_{c2}}$ et $\boldsymbol{V_{c2}o}$

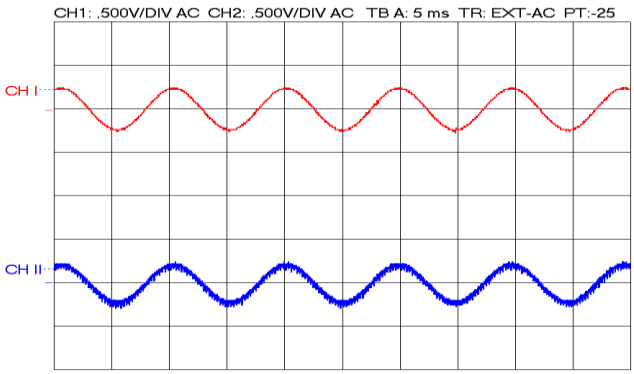


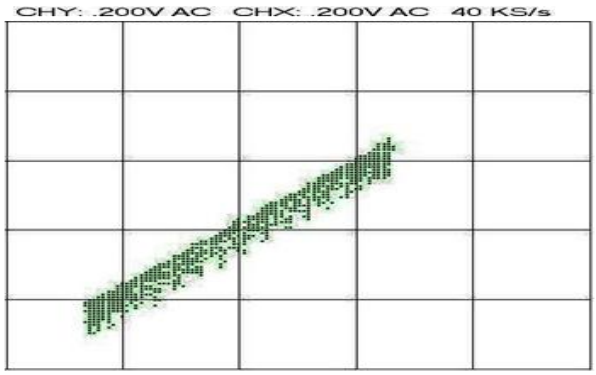


a : Les états I_L (CH I) et $I_L o$ (CH II)

b : Plan de phase $I_L - I_L o$

Fig. 4. 21 Résultats de synchronisation des états $\boldsymbol{I_L}$ et $\boldsymbol{I_L o}$





a : Message envoyé et reçu

b : Plan de phase des messages envoyé et reçu

Fig. 4.22 Résultats de synchronisation du message sinusoïdal

Il est à noter le signal message est bien caché dans le signal chaotiqueI_L. Ceci est illustré par la figure ci-dessous.

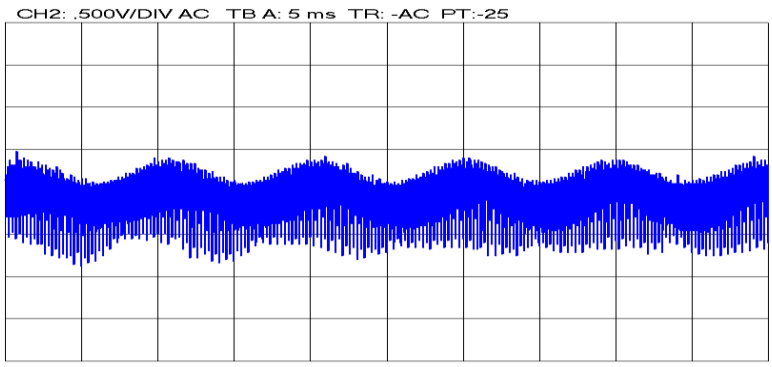
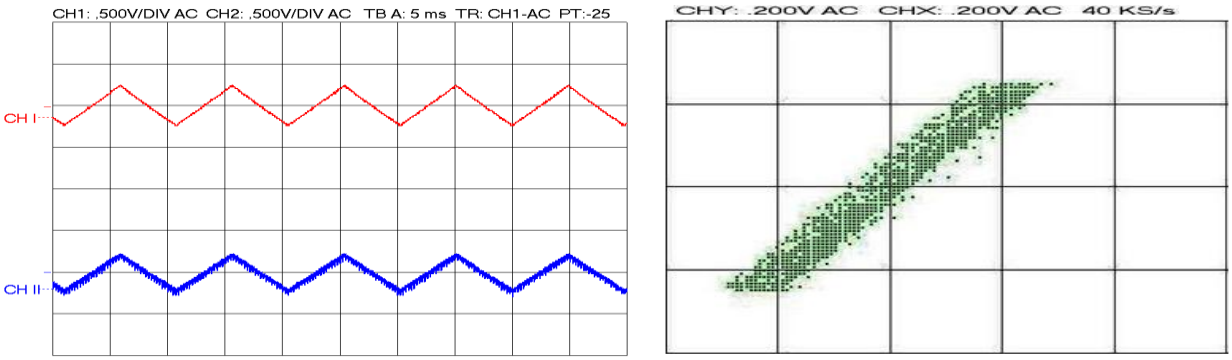


Fig. 4. 23 Signal porteur du message sinusoïdal

La figure (4.24) montre les signaux visualisés à l'oscilloscope dans le cas où nous envoyons un signal triangulaire d'amplitude 0.5 V crête à crête et de fréquence 1Khz. Les résultats obtenus montrent bien que les deux messages sont synchronisés



a : Message envoyé et reçu b : Plan de phase des messages envoyé et reçu

Fig. 4. 24 Résultats de synchronisation du message triangulaire

De même que pour le message sinusoïdal, le message triangulaire est bien masqué par le signal I_L comme nous pouvons le constater sur la figure (4.25)

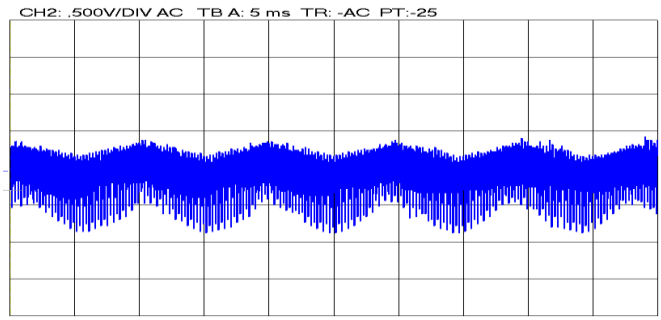


Fig. 4. 25 Signal porteur du message triangulaire

4.5 CONCLUSION

Dans ce dernier chapitre, des résultats de simulations et expérimentaux sont donnés pour illustrer les performances du système de transmission basé sur la synchronisation impulsive de deux oscillateurs de Colpitts.

Les résultats de simulations ont montré que la synchronisation impulsive des deux oscillateurs de Colpitts est réussie. Ceci a permis la récupération du message en utilisant les méthodes de cryptage par addition et par inclusion.

Les résultats expérimentaux obtenus après la réalisation du système de transmission en utilisant le cryptage par addition confirment ceux obtenus par simulation et nous motivent à envisager une amélioration du système réalisé en tenant compte des bruits du canal et des variations des paramètres des oscillateurs de Colpitts. De plus, il est intéressant de réaliser pratiquement le même système en utilisant cette fois la méthode de cryptage par inclusion qui est plus complexe et plus robuste.

CONCLUSION GENERALE

Ce mémoire consiste à réaliser un système de transmission de données basé sur la synchronisation impulsive de deux oscillateurs chaotiques de Colpitts. Ce système résulte de l'inclusion de la théorie du chaos dans les télécommunications.

Dans le premier chapitre de ce mémoire, nous avons évoqué d'abord quelques notions sur les systèmes dynamiques qu'ils soient en temps continu ou en temps discret. Par la suite, nous nous sommes intéressés à une classe particulière de systèmes non linéaires qui sont dits chaotiques.

Ces systèmes présentent plusieurs caractéristiques dont l'exploitation serait intéressante pour la transmission de données. Parmi ces caractéristiques que nous avons développées avec plus de détails, nous pouvons citer le déterminisme qui signifie que ces systèmes sont régis par des règles fondamentales non probabilistes. Il est alors possible de reproduire le comportement chaotique.Une autre propriété intéressante de ces systèmes, est la sensibilité aux conditions initiales. En effet, un moindre écart ou imprécision dans les conditions initiales engendre des évolutions totalement différentes. Ceci implique l'impossibilité de prédiction à long terme du comportement du système chaotique. Nous avons également cité les différentes classes des systèmes chaotiques, et pour chaque catégorie nous avons donné des exemples de systèmes chaotiques utilisés par la communauté scientifique.

Un des points intéressants par lequel nous avons clos le premier chapitre est la transition vers le régime chaotique. En effet le chaos peut se manifester par intermittence, par quasi-périodicité ou par doublements de périodes dûs au changement des paramètres du système comme nous l'avons d'ailleurs constaté pour l'oscillateur de Colpitts.

Dans le deuxième chapitre du mémoire, nous avons donné le schéma général de la transmission sécurisée à base du chaos. Le principe est de noyer l'information utile dans un signal ou dans une combinaison de signaux chaotiques puis l'envoyer sur un canal public vers le récepteur qui récupère l'information par décryptage.

Pour récupérer le message, les signaux chaotiques utilisés pour le masquage doivent être présents au niveau de l'émetteur et du récepteur. A ce stade, la synchronisation de l'émetteur et du récepteur s'impose pour obtenir une « copie » identique du système chaotique de l'émetteur à la réception. Nous avons alors introduit le concept de synchronisation des systèmes chaotiques et rappelé les différentes techniques de synchronisation proposées dans la littérature. Dans la deuxième partie de ce chapitre, nous avons présenté les différents systèmes de transmission possibles à partir de la synchronisation de l'émetteur et du récepteur, parmi lesquelles nous avons choisi, pour la suite de notre travail, deux méthodes : La première méthode est le cryptage additif, où l'information est cryptée par une simple addition à l'un des signaux de sortie du générateur chaotique. Cette méthode a été d'abord appliquée en simulations puis en pratique lors de la réalisation expérimentale du système de transmission. La deuxième méthode, utilisée uniquement en simulation pour vérifier sa faisabilité et ses performances, est la méthode d'inclusion. Elle consiste à inclure l'information utile dans la dynamique du système chaotique de l'émetteur.Un système de transmission robuste doit faire face aux éventuelles attaques. Comme nous l'avons mentionné à la fin du deuxième chapitre, un système de transmission à base des systèmes chaotiques peut être sujet à plusieurs types d'attaques. Ces dernières peuvent exiger une connaissance complète ou partielle des systèmes chaotiques utilisés, certaines autres attaques peuvent se passer de ces informations pour déchiffrer le message.

La méthode de synchronisation choisie dans notre cas et appliquée dans le système de transmission réalisé est la synchronisation impulsive. C'est une approche récente qui utilise de courtes impulsions de commande pour synchroniser les états ou signaux de deus systèmes chaotiques.Pour cette raison, nous lui avons consacré le troisième chapitre pour expliquer son principe et son application sur les systèmes chaotiques. Nous avons également donné la dynamique d'un observateur impulsif pour estimer les états chaotiques.

La méthode de la synchronisation a été appliquée pour synchroniser deux oscillateurs de Colpitts. Une fois synchronisés, ces deux oscillateurs sont exploités pour la transmission de données. Le choix du Colpitts est justifié par la simplicité de sa structure et de son fonctionnement. En effet, la modification des conditions de fonctionnement du transistor permet de générer le comportement chaotique. Un observateur impulsif a été proposé par la

suite pour estimer les signaux chaotiques de l'oscillateur en tenant compte des définitions, théorèmes et corollaires énoncés dans le second chapitre.

Nous avons finalisé notre travail par des résultats de simulation numérique sous Matlab puis par des résultats expérimentaux obtenus après la réalisation du système de transmission. Les résultats de simulation illustrent les performances du système de transmission proposé que ça soit par cryptage additif ou par la méthode d'inclusion. La synchronisation des deux oscillateurs a eu lieu dans les deux cas et les différents signaux ont été récupérés au niveau du récepteur. En pratique, le système de transmission a été réalisé en utilisant un cryptage additif du signal message sur la sortie I_L de l'oscillateur de Colpitts au niveau de l'émetteur. La synchronisation impulsive a été établie entre les deux oscillateurs, le signal de synchronisation est la tension V_{C2} de l'oscillateur. Pour une bonne transmission, la chronologie d'envoi des deux signaux doit assurer un rapport signal utile sur signal transmis proche de l'unité. Sur les derniers résultats expérimentaux, nous pouvons constater que les différents signaux messages envoyés de l'émetteur ont été bien récupérés au niveau du récepteur.

Tout ce travail peut être amélioré par l'étude de la robustesse du système de transmission conçu vis-à-vis des bruits de canal de transmission, et aussi par l'étude de la robustesse par rapport aux variations des paramètres de l'oscillateur de Colpitts. En outre nous pouvons améliorer le système de chiffrage par le choix de fonctions de cryptage plus complexes, par conséquent plus difficiles à déchiffrer lors d'une éventuelle attaque. Une autre amélioration à notre travail consiste à réaliser expérimentalement le schéma proposé du cryptage par inclusion, car il est plus robuste face aux attaques et aux bruits de canaux. Enfin nous envisageons de réaliser le schéma de transmission proposé à l'aide de circuits programmables.

ANNEXE A : RAPPELS SUR LES AMPLIFICATEURS OPERATIONNELS

Les amplificateurs opérationnels sont originalement conçus pour exécuter des opérations mathématiques telles l'addition, la soustraction, la multiplication, la division, le changement de signe, la dérivation et l'intégration dans les calculs et simulations analogiques.

Malgré qu'ils soient toujours utilisés pour effectuer ces fonctions, ils sont également utilisés dans un large domaine d'applications.

Les ampli-op sont produits en package de circuits intégrés. Les connexions aux circuiteries internes sont faites via des broches de connexion dual-in-line (DIL). La forme la plus simple est le package DIL a 8 broches comme illustré sur la figure suivante :

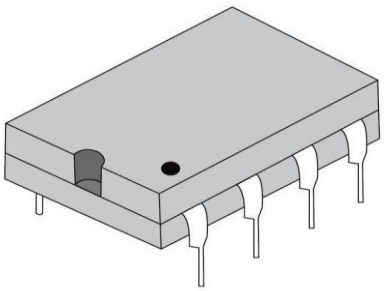


Figure A. 1 Package DIL à 8 broches

L'un des plus connus et plus anciens amplificateurs opérationnels est le 741. Il est produit dans un package DIL à 8 broches et reste largement utilisé. Comme tous les amplificateurs opérationnels fonctionnent de manière similaire, nous nous focaliserons dans cet annexe de mémoire sur les caractéristiques et fonctions de l'amplificateur 741.

A.1 CARACTERISTIQUES DE BASE D'UN AMPLIFICATEUR OPERATIONNEL

Un amplificateur opérationnel est un amplificateur différentiel linéaire à gain élevé couplé directement ; le terme différentiel fait référence au fait qu'il amplifie effectivement la différence des tensions appliquées à ces deux entrées. Le symbole d'un amplificateur opérationnel est illustré sur la figure A.2.

Le signe (-) dans le symbole triangulaire général indique l'entrée inverseuse. L'entrée non inverseuse est identifiée par le signe (+).

Comme tout autre amplificateur, l'amplificateur opérationnel requiert une alimentation continue et souvent symétrique ($-V_S$, 0 V, $+V_S$)pour fonctionner.

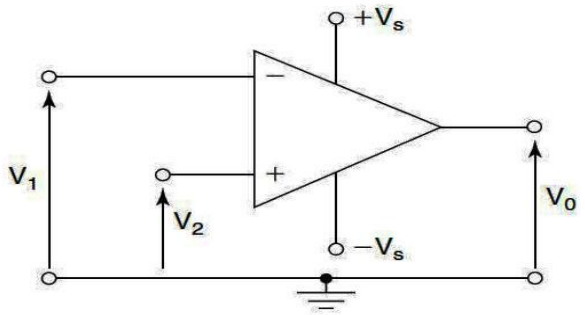


Figure A. 2 Symbole de l'amplificateur opérationnel

Les caractéristiques idéales pour un amplificateur opérationnel et les valeurs typiques actuelles pour l'amplificateur 741 sont donnés par la Table suivante :

Caractéristique	Idéale	Typique (741)
Gain de tension en Boucle ouverte	Infinie	200000
Résistance d'entrée	Infinie	1 MΩ
Résistance de sortie	Nulle	75 Ω
Largeur de bande	Infinie	Supérieure à 1MHz
Taux de rejection en mode commun	Infinie	30000 (90 dB)
Vitesse de balayage	Infinie	0.5 V/µS

TAB A.1 Caractéristiques des amplificateurs opérationnels

A.2 MONTAGES A BASE D'AMPLIFICATEURS OPERATIONNELS

Dans cette partie, nous présenterons quelques circuits de base réalisés à l'aide d'amplificateurs opérationnels et qui sont utilisés pour la réalisation du système de transmission

A.2.1 MONTAGE SUIVEUR

Cette Configuration est montrée sur la figure A.3. Dans ce montage, le gain est presque unitaire et comme l'entrée non inverseuse est utilisée, la tension de sortie sera égale à la tension d'entrée. Si la tension d'entrée varie, alors la sortie suivra exactement les mêmes variations.

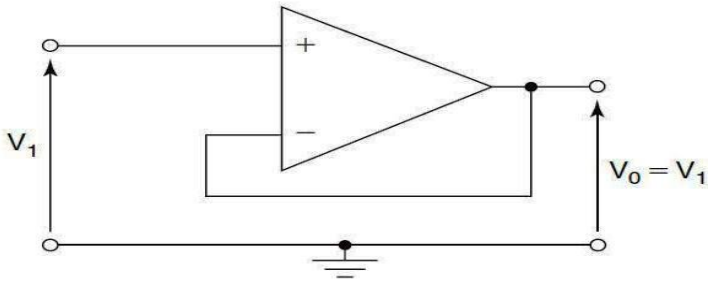


Figure A. 3 Montage suiveur

A.2.2 MONTAGE AMPLIFICATEUR INVERSEUR

Le circuit d'un amplificateur inverseur est montré sur la figure A.4 Dans cette application, l'entrée non inverseuse est connectée à la masse. Le point B du circuit est alors à 0V. Due au gain élevé en boucle ouverte, une entrée de quelques microvolts pourrait causer la saturation ; Ainsi la différence de potentiel entre les points A et B est virtuellement nulle. Ceci signifie que A est un point de masse virtuel.

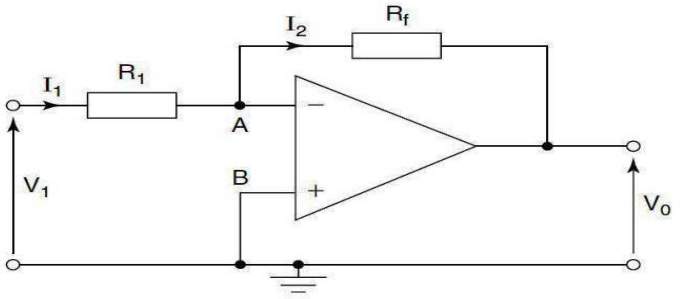


Figure A. 4 Montage amplificateur inverseur

En utilisant la notion de masse virtuelle, nous pouvons affirmer que la tension V_1 est appliquée via la résistanceR_1traversée par un courant négligeable dû à la résistance d'entrée importante de l'amplificateur. Nous avons alors $I_1 = I_2$.

La résistance R_f est une résistance de réaction liant la sortie et l'entrée. En tenant toujours compte de la masse virtuelle A, V_0 est connectée à travers R_f. La relation entre la tension de sortie V_0 et la tension d'entrée V_1 est déterminée comme suit :

$$I_1 = \frac{V_1}{R_1} \text{et } I_2 = \frac{-V_0}{R_f}$$

Toutefois $I_1 = I_2$ alors $\frac{V_1}{R_1} = \frac{-V_0}{R_f} \text{et} \frac{V_0}{V_1} = A_v = -\frac{R_f}{R_1}$

A partir de ces équations, nous pouvons constater que le gain en boucle fermée dépend seulement du rapport R_f/R_1. Dans ce cas il est possible de varier le gain par le choix de différentes valeurs de ces deux résistances.

A.2.3 MONTAGE AMPLIFICATEUR NON INVERSEUR

.

Dans ce montage, l'entrée est appliquée à l'entrée non inverseuse mais la résistance d'entrée R_1 et la résistance R_f sont connectées à l'entrée inverseuse (voir figure A.5).

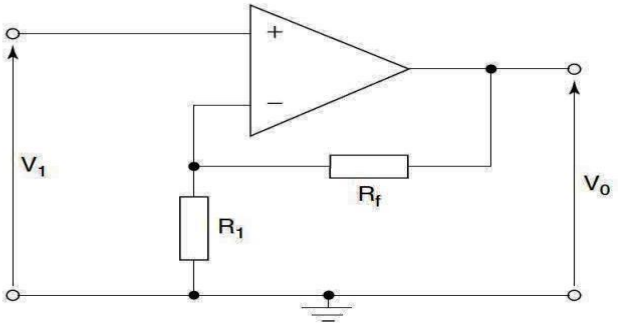


Figure A. 5 Montage amplificateur non inverseur

Les résistances R_f et R_1 forment un diviseur potentiel entre la sortie et le point 0V. la différence de potentiel entre les bornes de R_1 sera une proportion deV_0. Ainsi

$$\frac{V_0}{V_1} = A_v = \frac{R_1 + R_f}{R_1}$$

$$A_v = 1 + \frac{R_f}{R_1}$$

A.2.4 MONTAGE SOMMATEUR

Le montage sommateur à base d'amplificateurs opérationnel est donné par la figure (A.6)

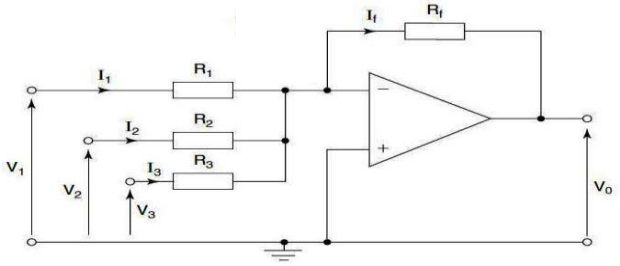


Figure A. 6 Montage sommateur

$I_1 = \frac{V_1}{R_1}; I_2 = \frac{V_2}{R_2}; I_3 = \frac{V_3}{R_3}$; et $I_f = -\frac{V_0}{R_f}$

En appliquant les lois de Kirchhoff on obtient

$$I_f = I_1 + I_2 + I_3$$

Alors $-\frac{V_0}{R_f} = \frac{V_1}{R_1} + \frac{V_2}{R_2} + \frac{V_3}{R_3} \Rightarrow V_0 = -[\frac{R_f}{R_1}V_1 + \frac{R_f}{R_2}V_2 + \frac{R_f}{R_3}V_3]$

En choisissant $R_f = R_1 = R_2 = R_3$ on aura

$$V_0 = -(V_1 + V_2 + V_3)$$

La sortie est ainsi la somme inversée des tensions d'entrée.

A.2.5 MONTAGE SOUSTRACTEUR

Dans ce montage, des tensions sont appliquées à chacune des bornes d'entrée comme illustré sur la figure A.7.

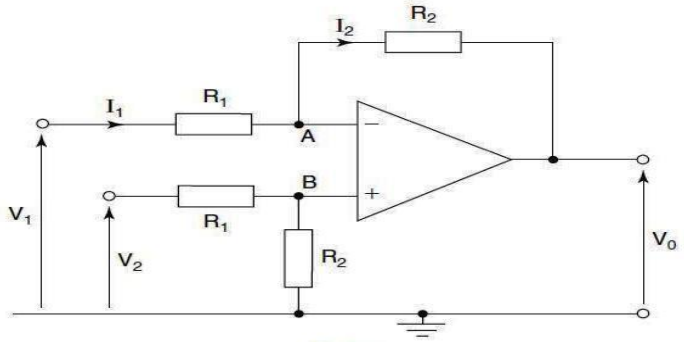


Figure A. 7 Montage soustracteur

La tension de sortie est donnée par:

$$V_0 = \frac{R_2}{R_1}(V_2 - V_1)$$

Si on choisit $R_1 = R_2$, Alors $V_0 = V_2 - V_1$

A.2.6 LE MONTAGE INTEGRATEUR

Le circuit électronique d'un intégrateur à base d'un amplificateur opérationnel est montré sur la figure A.8. Dans ce cas, la résistance de réaction est remplacée par une capacité

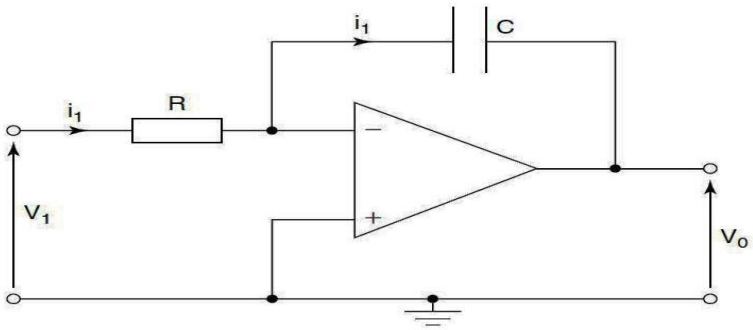


Figure A. 8 Montage intégrateur

La tension de sortie est ainsi donnée par :

$$V_0 = -\int \frac{1}{CR} V_1 \, dt$$

A.2.7 LE MONTAGE DERIVATEUR

Dans cette application la résistance et la capacité du circuit précédent sont placés inversement (figure A.9)

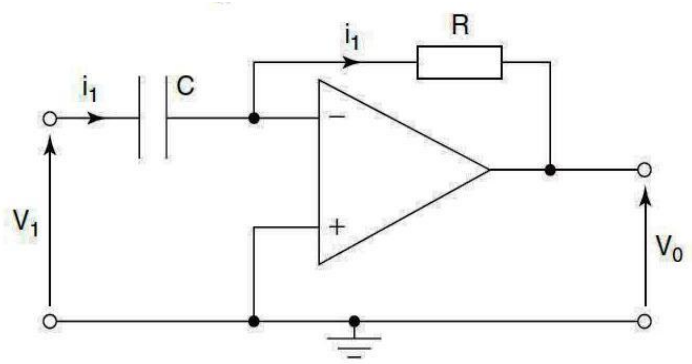


Figure A. 9 Montage dérivateur

La tension de sortie résultante du circuit sera la dérivée de la tension d'entrée. Par exemple si $v_1 = V_m \sin \omega t$, alors :

$$V_0 = -CR \frac{d}{dt}(V_m \sin \omega t) = -CR\text{x } \omega V_m \cos \omega t$$

$$V_0 = -\omega CRV_m \cos \omega t \text{ où } \omega CRV_m \sin \left(\omega t + \frac{\pi}{2}\right)$$

A.2.8 LE MONTAGE COMPARATEUR

Comme son nom l'indique, Ce montage compare les valeurs relatives de deux tensions appliquées à ses entrées. Le montage comme on peut le voir sur la figure A.10 ne contient pas de réaction et opère donc en boucle ouverte.De ce fait, son grand gain en boucle ouverte conduit à la saturation soit positive soit négative de la tension de sortie dès que la différence des tensions d'entrée n'est pas strictement nulle. On obtient donc avec le circuit de la figure A.10.

$$V_s = +E \;\; si \;\; V_{e1} > V_{e2}$$

$$V_s = -E \;\; si \;\; V_{e1} < V_{e2}$$

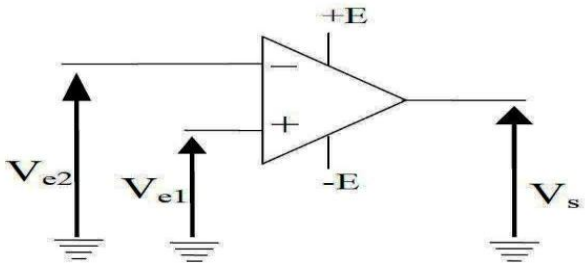


Figure A. 10 Montage comparateur

ANNEXE B : CIRCUITS EXPERIMENTAUX

Dans cette seconde annexe, nous illustrerons les circuits imprimés des principaux modules du système de transmission réalisé.

La figure B.1 présente la face cuivre du circuit de Colpitts utilisé en émission et en réception. Des connecteurs sont prévus pour observer les signaux de sortie V_{c1} , V_{C2} et I_L.

Les connecteurs de sortie sont représentés par les points x_1, x_2 et x_3 correspondant respectivement à V_{c1} , V_{c2} et I_L.

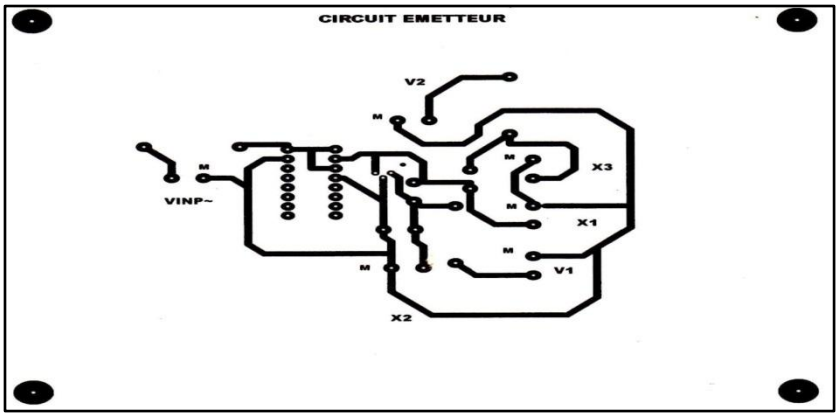


Figure B. 1 Circuit imprimé de l'oscillateur de Colpitts

La figure B.2 illustre le circuit sommateur utilisé pour additionner le message envoyé à la sortie I_L du circuit de Colpitts de l'émetteur.

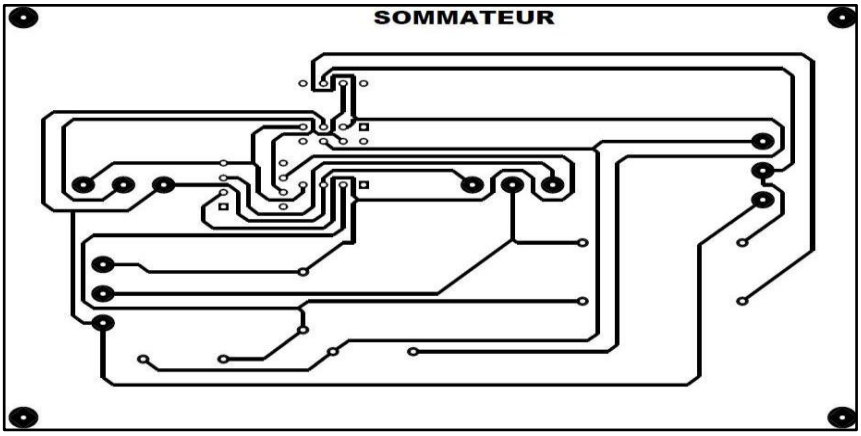


Figure B. 2 Circuit imprimé du sommateur utilisé

Comme il a été mentionné dans ce mémoire. La commutation entre le signal de synchronisation et le signal porteur de l'information est effectuée en utilisant un circuit CD 4066BP. La figure B. 3 montre le brochage approprié pour assurer le multiplexage des deux signaux.

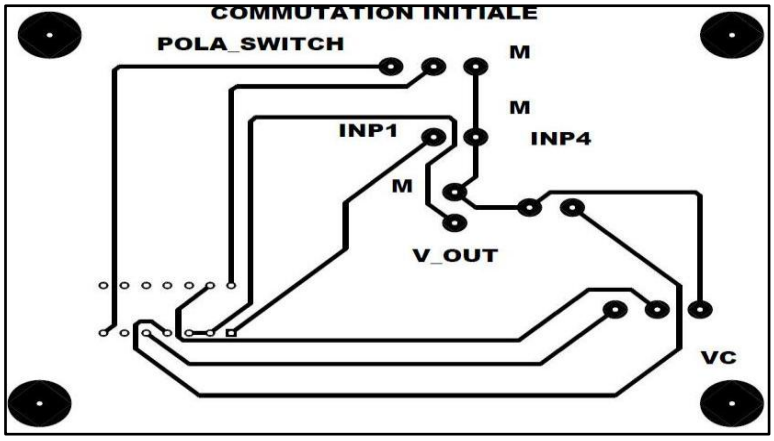


Figure B. 3 Circuit de commutation utilisé

BIBLIOGRAPHIE

[1]V.S. Afraimovich, N.N. Verichev, M.N. Rabinovich. "Stochastic synchronization of oscillations in dissipative systems." *Radiophys. and Quantum Electronics*, 1986: 747-751.

[2] J.M. Amigo."Chaos-Based Cryptography." *Intelligent Computing Based on Chaos*, 2009: 291-313.

[3] F. Anstett.*Les systèmes dynamiques chaotiques pour le chiffrement synthèse et cryptanalyse.*2006.

[4] M.A. Aziz-Alaoui "Synchronization of chaos." *Encyclopedia of Mathematical*, 2006: 213-226.

[5] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares , C.S. Zhou. "The synchronization of chaotic systems." *Physics Reports*, 2002: 1-101.

[6] J.Y. Chen, K.W.Wong, L.M.Cheng. "A secure communication scheme based on the phase synchronization of chaotic systems." *Chaos*, 2003: 508-514.

[7] M. Cheng, H.Hu. "A Novel Chaotic Synchronization Scheme Based on Impulsive Stability Theory." *Journal of Computers*, March 2012: 755-761.

[8] E. Cherrier. *Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires.*Thèse de doctorat, 2006.

[9] Y.H. Chu. "Dynamical cryptography based on synchronised chaotic systems." *Electronics Letters*, Jun 10, 1999: 974-975.

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

[11] H. Dedieu, M.P.Kennedy, M.Hasler. "Chaos shift keying: modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits." *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, October 1993: 634-642.

[12] D. Goumidi. *Fonction logistique et standard chaotique pour le chiffrement des images satellitaires.*Mémoire de Magister, Université Mentouri de Constantine, 2010.

[13] K.S. Halle, C.W. Wu, M. Itoh, L.O. Chua. "Spread Spectrum Communication Through Modulation of Chaos." *International Journal of Bifurcation and Chaos*, 1993: 469.477.

[14] H. Hamiche.*Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques, Applications à la Transmission Sécurisée de Données.* Thèse de Doctorat, Universite Mouloud Mammeri de Tizi-Ouzou, 2011.

[15] H. Hamiche, M. Ghanes, J.P. Barbot, S.Djennoune. "Secure digital communication based on hybrid dynamical systems." *IEEE, IET International Symposium on Communication Systems, Networksand Digital Signal Processing*, 2010: 244-249.

[16] D.He."Hyper Chaos Synchronization Shift Keying (HCSSK) Modulation and Démodulation in Wireless Communication." *IEEE International Conference on Neural Networks and Signal Processing* , Nanjing, Chine,June 7-11, 2008: 250- 254.

[17] M. Itoh, T.Yang.L.O.Chua. "Experimental Study of Impulsive Synchronization of Chaotic and Hyperchaotic Circuits." *International Journal of Bifurcation and Chaos*, july 1999: 1393-1424.

[18] M.P. Kennedy. "Chaos in the Colpitts oscillator." *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Nov 1994: 771-774.

[19] A. Khadra.*Impulsive Control and Synchronization of Chaos-Generating-Systems with Applications to Secure Communication.*Thèse de Doctorat, Université de Waterloo, Ontario, Canada,2004.

[20] A.Khadra, X.Liu, X.Shen. "Robust impulsive synchronization and application to communication security ." *Dynamics of Continuous Discrete and Impulsive Systems–Series B: Applications & Algorithms*, 2003: 403-417.

[21] A. Khadra, X.Liu,X.Shen. "Application of impulsive synchronization to communication security." *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, March 2003: 341-351.

[22] A. Khadra, X.Z. Liu, X. Shen. "Impulsively synchronizing chaotic systems with delay and applications to secure communication." *Automatica*, 2005: 1491-1502.

[23] Y. Khaled, D.Benmerzouk, J-P. Barbot,K.Busawon,M.Ghanes. "Strange attractor identification and state observation." *2nd International Symposium on Environment Friendly Energies and Applications (EFEA)*, Newcastle, 25-27July, 2012.

[24] Y. Khaled, J.P.Barbot, D.Benmerzouk, K.Busawon. "A new type of impulsive observer for hyperchaotic system." *IFAC Conference on analysis and control of chaotic systems*, June 20-22, 2012.

[25] L. Kocarev, K.S. Halle, K.Eckert, L.O.Chua, U.Parlitz. "Experimental Demonstration of Secure Communications Via Chaotic Synchronization." *International Journal of Bifurcation and Chaos*, September 1992: 709–713.

[26] G. Kolumbán, M.P. Kennedy, L.O.Chua."The role of synchronization in digital communications using chaos - part I : Fundamentals of digital communications." *IEEE Transactions on Circuits and Systems I*, 1997: 927-936.

[27] G. Kolumbán, M. P. Kennedy, L. O. Chua. "The role of synchronization in digital communications using chaos - part II : chaotic modulation and chaotic synchronization." *IEEE Transactions on Circuits and Systems I*, 1998: 1129–1140.

[28] G. Kolumbán, M.P.Kennedy, L.O.Chua. "The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization." *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Nov 1998: 1129-1140.

[29] V. Lakshmikantham, D.D. Bainov, P.S.Simeonov. *Theory of Impulsive Differential Equations.* Singapore: World Scientific Publishing Company, 1989.

[30] M. L'Hernault, J.P. Barbot, A.Ouslimani. "Feasibility of Analog Realization of a Sliding-Mode Observer: Application to Data Transmission." *IEEE Transactions on Circuits and Systems I: Regular Papers*, March 2008: 614- 624.

[31] M. L'Hernault. *Faisabilité d'un Système d'Emission-Réception Analogique pour les Communications Sécurisées par le Chaos.* Thèse de Doctorat, Université Pierre et Marie Curie, France, 2007.

[32] M. L'Hernault, J. De Leon, J.P. Barbot, A. Ouslimani. *Comparaison d'un observateur à modes glissants et un observateur adaptatif pour la synchronisation de systèmes chaotiques.*

[33] C. Li, X. Liao K.W. Wong. "Chaotic lag synchronization of coupled time-delayed systems and its application in secure communication." *Systems & Control Letters*, 1986: 133-142.

[34] Y. Li, X.Liu, X.Shen. "Chaos Synchronization Using Impulsive Driving and Application to Scure Communication." *Dynamics of Continuous, Discrete and Impulsive Systems Series B: Applications & Algorithms 10* , 2003: 899-913.

[35] Z. Li, Y. Soh, W. Xie. "The stabilization and synchronization of Chua's oscillators via impulsive control." *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Nov 2001: 1351- 1355.

[36] Z. Li, Y.Soh, C.Wen. "Switched and Impulsive Systems : Analysis, Design and Applications." *Lecture Notes in Control and Information Sciences*, vol.313, 2005.

[37] N, Lorenz. E. *The Essence of Chaos.* University of Washington Press, 1993.

[38] M.B. Luca. *Apports du chaos et des estimateurs d'états pour la transmission sécurisée de l'information.* l'Université de Bretagne Occidentale: Thèse de Doctorat, Université de Bretagne Occidentale, 2006.

[39] G.M. Maggio M.P. Kennedy. "Experimental manifestations of chaos in the Colpitts Oscillator." *Proceedings of ICECS*, 1997: 194-204.

[40] G.M.Maggio, O.De Feo, M.P.Kennedy. "Nonlinear analysis of the Colpitts oscillator and applications to design." *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, Sep 1999: 1118-1130.

[41] R. Mainieri, J. Rehacek. "Projective synchronization in three-dimensional chaotic." *Physical Review Letters*, 1999: 3042–3045.

[42] P. Manneville. *Dynamique non linéaire et chaos.* Séminaire E2PHY, 2005.

[43] A.J. Michaels. "Digital Chaotic Communications." Thèse de Doctorat, Georgia Institute of Technology, 2009.

[44] Y. Moussa. "Elaboration d'Algorithmes de Masquage pour Les Systèmes de Communication Chaotique." Thèse de Doctorat, Université Mentouri - Constantine, 2012.

[45] H. Nijmeijer. «On Synchronization of Chaotic Systems.» *IEEE 36 th Conférence on Decision and Control CDC'97*, 1997.

[46] H. Nijmeijer, M. Y. Ivan. Mareels. «An observerLooks at Synchronization.» *IEEE transaction on circuits and Systems: Fundamantal Theory and Applications*, vol.44 1997:882-890.

[47] J. Oden. "Le chaos dans les systèmes dynamiques." cours,http://www.hypo-theses.com/docs/user101_Le_chaos_dans_les_systemes_dynamiques.pdf,2007.

[48] M.J. Ogorzalek. "Taming chaos. I. Synchronization." *IEEE Transactions on Circuits and Systems I Fundamental Theory and Applications*, Nov 1993: 693-699.

[49] A.I Panas, T. Yang, L.O. Chua. "Experimental results of impulsive synchronization between two Chua's circuits." *International Journal of Bifurcations and Chaos*, 1998: 639-644.

[50] L.M. Pecora, T.L.Caroll. "Synchronization in chaotic systems." *PHYSICAL REVIEW LETTERS*, February 19, 1990: 821-825.

[51] L.M. Pecora, T.L.Caroll. "Synchronizing nonautonomous chaotic circuits." *IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing*, Oct 1993: 646-650.

[52] S. Penaud. "Etude des potentialités du chaos pour les systèmes de télécommunications : Evaluation des performances de systèmes à accès multiples à répartition par les codes (CDMA) utilisant des séquences d'étalement chaotiques." Thèse de Doctorat, Université de Limoges, 2001.

[53] C. Robilliard, E.H. Huntington, M. R. Frater. "Digital transmission for improved synchronization of analog chaos generators in communications systems." *Chaos 17*, 2007.

[54] K.M. Short. "Steps Toward Unmasking Secure Communications." *International Journal of Bifurcation and Chaos*, 1994:959-977.

[55] C.P. Silva, A.M.Young. "Introduction to chaos-based communications and signal processing." *IEEE Aerospace Conference Proceedings*, 2001: 279-299.

[56] P. Stavroulakis. "Chaos Applications In Telecommunications." *Taylor & Francis Group*, 2006.

[57] J. Suykens, M.Yalçın, J.Vandewalle. "Chaotic Systems Synchronization." *Chaos Control Lecture Notes in Control and Information Science*, 2003: 117-135.

[58] R. Tenny. "Symmetric and Asymmetric Secure Communication Schemes." Thèse de Doctorat, University of California, San Diego, 2003.

[59] T. Yamada, H. Fujisaka. "Stability theory of synchronized motion in coupledoscillator." *Progress of Theoretical Physics*, 1983: 32-47.

[60] T. Yang, L.O. Chua. "Impulsive stabilization for control and synchronization of chaotic systems: theory and application to secure communication." *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, oct 1997: 976-988.

[61] T. Yang, L.O. Chua, C.W. Wu. "Cryptography based on chaotic systems." *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, May 1997: 469-472.

[62] T. Yang. «Impulsive Control theory.» *Springer Verlag, Lecture Notes in Control and Information sciences*, 2001.

[63] T. Yang. *Impulsive systems and Control : Theory and Applications.*Huntington, NY: Nova Science Publishers, 2001.

[64] A. Zemouche. "*Sur l'observation de l'état des systèmes dynamiques non linéaires.*" Thèse de Doctorat, Université Louis Pasteur Strasbourg I, 2007.

[65] H. Zhang. *Chaos Synchronization and Its Application to Secure Communication.*Thèse de Doctorat, Université de Waterloo, Ontario, Canada, 2010.

[66] H. Zhang, T.D.Ma,W.Yu. "A practical approach to robust impulsive lag synchronization between different chaotic systems." *Chinese Physics B*, 2008.

[67] G. Zheng. *"Formes Normales d'Observabilité Paramétrées par les Sorties : Applications au Cryptage par Synchronisation de Systèmes Chaotiques."* Thèse de doctorat,Université de Cergy-Pontoise, France,2006

TRAVAUX PERSONNELS

O. Megherbi H. Hamiche et S. Djennoune, Réalisation d'un système de transmission sécurisée de données à base de deux systèmes chaotiques de Colpitts, 3 rd International CONFERENCE ON SYSTEMS AND PROCESSING INFORMATION. - 2013. Communication acceptée pour une présentation Poster.

O. Megherbi H.Hamiche et S.Djennoune, Transmission sécurisée de données à base de deux systèmes chaotiques de Colpitts . Communication présentée pour la 8 ème conférence sur le Génie Electrique (CGE'08).Bordj el Bahri, Alger, Algérie - 2013.