Université ABBES LAGHROUR Khenchela

Faculté des Sciences et de la Technologi

Département de Génie Industriel

جامـــعة عبـــاس لـــــغرور خـنـشـلة

كليـــة العلـــوم والتكنـــولـــوجيـا

قسـم الهنـدسة الصنـاعية

N° Série :.....

Mémoire de fin d'étude

Présenté pour l'obtention du diplôme de Master

Filière : Télécommunications

Spécialité : Systèmes des Télécommunications

THEME

Synchronisation des oscillateurs chaotiques de Sprott

Réalisé par :

CHEKHAB RAYAN

BELHANI CHAHRAZED

Devant Le Jury :

Président: ***Dr. BOURAS Moustafa***

Examinateur : ***Dr. BEDIAF Abdelaziz***

Encadreuse : ***Dr.MAAMRI Fouzia***

Promotion 2021/2022

Remerciements

En premier lieu, nous tenons à remercier notre DIEU, notre créateur pour nous avoir donné force pour accomplir ce travail.

Nous désirons exprimer notre profonde et vive reconnaissance à notre encadreur, Mme Maamri Fouzia qui a mis toute sa compétence à notre disposition, pour ces directives et conseils judicieux et pour son suivi Régulier à l'élaboration de ce modeste travail.

Nous remercions également tous les membres du jury pour nous avoir honoré par leur présence et pour avoir accepté d'évaluer ce travail de mémoire.

Nous tenons à exprimer nos vifs remerciements à tous nos professeurs qui ont contribués à notre formation.

Nous remercions nos très chers parents pour leur soutien moral et financier qui nous a permis de réussir et de terminer nos études.

En fin, Nous remercions toute personne qui a participé de près ou de loin à l'accomplissement de ce mémoire.

Dédicaces

En guise de reconnaissance envers mon DIEU le tout puissant je dédie ce modeste travail à la communauté scientifique espérant qu'il lui sera utile, à tous ce que qui m'ont appris une lettre depuis le début de mon parcours en quête de connaissance jusqu'à mon arrivée en ce moment.. Ainsi je dédie ce travail à mes chers parents pour leur amour inestimable, leur confiance, leur soutien, leurs sacrifices et toutes les valeurs qu'ils ont su m'inculquer, ma mère HALIMA et mon père ALI, à mes chers frères LAKHDER et ABDELKARIM, ma chère sœur LAYLA à tous mes belles amies sans exception et surtout RAYAN et KENZA à tous mes collègues de spécialité system de télécommunication

CHAHRAZED

Dédicaces

Merci « Allah» Dieu le tout puissant qui m'a donné le courage, la force et la patience pour réaliser ce travail

Je dédie ce modeste travail en signe de respect et de reconnaissance

A Ma chère maman, merci pour toute sa tendresse, son amour, son soutien, et sacrifices et de précieux conseils, merci pour toute son aide et sa présence dans ma.vie. Mon cher père, je lui dois, il lui a consacré sa vie mon éducation A mes sœurs Ilham et Rahma et mes frères et tous ma famille

'' A mon binôme et mon amie ''chahrazed Mon fidèle amie Kenza et tous mes amis

À tous ceux qui ont une place dans mon cœur, et tous ceux qui m'ont aidé de près ou

.de loin. ET tous ceux que j'ai omis de citer

Rayan

Résumé:

Dans ce mémoire nous avons étudiéles systèmes chaotiques, qui sont déterministes, non linéaire, apériodique et très sensibles aux conditions initiales. Depuis la découverte de Pecorra et Carroll que deux systèmes chaotiques peuvent se synchroniser, un intérêt significatif a été accordé à l'usage de ces systèmes pour sécuriser les transmissions et pu être utilisé pour créer des clés pour la cryptographie. Ce travail implique l'utilisation de signaux chaotiques de Sprott pour crypter les signaux d'information. Dans un premier temps, nous avant étudié les émetteurs chaotiques qui insèrent des messages. Nous synchronisons ensuite les deux systèmes émetteur-récepteur en utilisant une méthode de synchronisation. Nous effectuons notre travail en simulant le système Sprott par le logiciel MATLAB.

Mots clés : Système non linéaire ; Chaos ; oscillateur de Sprott ; Synchronisation ; Cryptographie.

Abstract

In this thesis we have studied chaotic systems, which are deterministic, nonlinear, aperiodic and very sensitive to initial conditions. Since the discovery of Pecorra and Carroll, that two chaotic systems can synchronize significant interest has been given to the use of these systems to secure transmissions. This work involves the use of chaotic Sprott signals to encrypt information signals. First, we studied chaotic transmitters that insert messages. and then we synchronize the two transmitter-receiver systems using a synchronization method. We perform our work by simulating the Sprott system using MATLAB software.

Keywords: Nonlinear system; Chaos; Sprott oscillator; synchronization; Cryptography.

ملخص:

قدمنا في هذه المذكرة الأنظمة الفوضوية، وهي غير خطية وغير دورية وحساسة للغاية للظروف الأولية.

منذ اكتشاف Pecorra و Carroll أن نظامين فوضويين يمكنهما المزامنة، ظهر اهتمام كبير باستخدام هذه الأنظمة لتأمين عمليات الإرسال ويمكن استخدامها لإنشاء مفاتيح للتشفير.هذا العمل ينطوي استخدام إشارات sprott الفوضوية لتشفير إشارات المعلومات. في الأول درسنا أجهزة الإرسال الفوضويةالتَّي تدخل الرسائل، ثم نقوم بمزامنة نظامً الإرسال والاستقبال باستخدام طرٌقة التزامن، نقوم بعملنا من خلال محاكاة نظام sprott بواسطة برنامج.MATLAB

الكلمات المفتاحية: نظام غٌر خطي، فوضى، مذبذبsprott،التزامن، التشفٌير.

Sommaire

Sommaire

Liste des figures

Liste des tableaux

Symboles mathématique

x_0,y_0, z_0Conditions **I**nitiales **D**'un **S**ystème d'équations différentielles

x, y, z Les variables d'états d'un système d'équations différentielles

a,b,c Paramètres du système de Hénon ,lorenz ,Rössler

Somme algébrique

$\boldsymbol{\tau}$ Retard positif.

$\dot{X}$ Dérivée du vecteur d'état X

R L'ensemble des nombres réels

$\mathbf{R^P}$Espace vectorielles de dimension **P**

$\mathbf{R^n}$Espace vectorielles de dimension **n**

R résistance

R paramètre de bifurcation

Lim Limite

***v*1,*v*2**i_l sont respectivement la tension

E ensemble non vide d'appelé espace de vide

Vvecteur du paramètre

f champ de vecteur

$(t) et \hat{x}(t)$l'état de système récepteur

Q_1àQ_7Paramètre du système de sprott.

Liste des abbreviations

A

AES Advanced **E**ncryptions **S**tandard

C

CSK chaos shift keying

D

DES Data **E**ncryptions **S**tandard

R

RSA Système **D**e **C**ryptage **A**symétrique (**R**ivest**S**hamir**A**dleman)

m(t) message informatif

x(t)signal chaotique

s(t) signal crypté

Introduction générale

Introduction générale:

Depuis les temps anciens, l'homme n'a pas manqué de rechercher des moyens multiples et variés pour transmettre son message et ses informations aux autres ainsi que pour communiquer avec eux. Cela a conduit à l'effort de développer des méthodes de communication et ceci afin de rechercher leurs meilleurs moyens et les meilleurs voies pour une meilleurs mobilité et tout cela dans un secret complet de communication.

La théorie du chaos montre la nécessité de combiner les méthodes physiques des phénomènes mathématiques. En fait, la théorie du chaos vise à proposer des méthodes ou des moyens pour modéliser le comportement de systèmes dynamiques chaotiques à l'aide d'équations afin d'améliorer leur prévisibilité. La dynamique du chaos peut être identifiée par ses propriétés, telles que le spectre de puissance continu qui est parfois confondu avec le bruit. Dans le domaine temporel, des signaux chaotiques apparaissent de manière aléatoire. Les systèmes chaotiques sont également connus pour leur sensibilité aux conditions initiales : une petite perturbation peut provoquer un changement important dans l'état du système.

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 **[31].**

En effet, le cryptage joue un rôle très important dans la sécurité et la fiabilité des systèmes de transmission. Ce mémoire consiste à réaliser un système basé sur l'oscillateur chaotique dit de Sprott. Il repose d'une part sur la synchronisation chaotique et d'autre part sur le masquage de l'information secrète. Pour cela, nous avons organisé notre mémoire de la manière suivante :

Le premier chapitre : présent un rappel sur le système non linéaire et système dynamique en général et les systèmes chaotiques en particulier. Il énoncera quelques concepts sur la théorie du chaos.

Le deuxième chapitre : étudie principalement des éléments sur la cryptographie et les différentes méthodes de cryptage et décryptage des systèmes chaotiques et nous avons aussi parlé sur le principe de la synchronisation et des différentes méthodes de la synchronisation et aussi leurs types.

Le troisième chapitre, présente spécifiquement la simulation du système chaotique sélectionné sous MATLAB, le circuit Sprott l'occurrence ainsi que la méthode choisie pour sa synchronisation.

Enfin, nous concluons ce travail par une conclusion générale résumant nos principaux résultats.

Chapitre I:

Etude des systèmes non linéaires chaotiques

Chapitre I:Etude des systèmes non linéaires chaotiques

I.1 Introduction :

Le chaos est définit généralement comme un comportement particulier de système dynamique déterministe non linéaire, la notion de déterminisme provenant du fait que le système considéré complètement caractérisé par son état initial et sa dynamique. Les systèmes dynamiques chaotiques sont inclus dans les applications effectives depuis la dernière décade malgré qu'elles soient connues depuis longtemps dans le domaine mathématique. Dans ce chapitre nous rappelons sur quelque notion de système chaotique qui apparaît dans les systèmes dynamiques déterministes. Nous commencerons par définition de système dynamique en général et donnons une brève quantitative sur le chaos. Définition de chaos, quelque outil mathématique de quantification de chaos et aussi appelons sur le système non linéaire (définition, Principe de superposition et son classes), et différent route vers le chaos.

I.2. Système non linéaire :

I.2.1Définition :

Un système non linéaire est un système qui ne satisfait pas le principe de superposition, ou un système dont la sortie n'est pas proportionnelle à son entrée.

1.2.2. Principe de superposition :

Soit les signaux d'entrée u_1 et u_2 génèrent deux signaux de sortie y_1 et y_2, alors la réponse à la somme de l'entrée $u = u_1 + u_2$ est la somme des réponses individuelles, donc $y = y_1 + y_2$. Un système avec une entrée u et une sortie y qui obéit au principe de superposition est un système linéaire. Par conséquent, tout système qui n'obéit plus au principe de superposition est un système non linéaire.

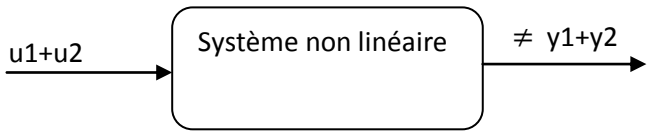


Figure I.1 *Schéma bloc d'un système non linéaire*

Les problèmes non linéaires sont d'intérêt pour les automaticiens, physiciens et mathématiciens, car la plupart des systèmes physiques sont intrinsèquement non linéaire dans la nature.

I.1.3 Classe de systèmes non linéaires :

Soit (I. 1) un système non linéaire mono-entrée mono-sortie (SISO) donné par:

$$\dot{x}_1 = x_2$$

$$x_2 = x_3 \qquad \textbf{(I.1)}$$

$$\dot{x}_n = f(x1, \ldots . \dot{x}n) + \mathrm{g}x1, \ldots . \dot{x}n).u$$

$$y = x_1$$

Où : $x = [x1, x2 \ldots x]^{\mathrm{T}} \epsilon \ \mathrm{R}^n$

Est le vecteur d'état, et u, y sont respectivement l'entrée et la sortie. Le système (I.1) est dit dans sa forme canonique compagne en a variable de phase. On peut alors facilement vérifier que :

$$y^n = f(x) + g(x).u = f(y, \ldots, y^{n-1}) + g(y, .. y^{n-1}).u \textbf{(I.2)}$$

I.3. Système dynamique :

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 phénomène du passé ou de la présente.
- Déterministe : c'est-à-dire qu'à partir d'une «condition initiale » donnée à l'instant.

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 dynamique continues. Elle est représentée par le modèle général des équations aux différences finies **[2].**

De point de vue mathématique, les systèmes dynamiques sont classés en deux catégories Système dynamique continue et Système dynamique discrets.

I.3.1.Systèmes dynamiques continus :

L'évolution d'un système dynamique continue est décrit t par l'équation différentielle ordinaire suivante :

$$\dot{x} = f(x, t, v) \quad \textbf{(I.3)}$$

Où, $x \epsilon E$(E un ensemble non vide de$\mathbb{R}^n$ appelé espace de phase) est le vecteur d'état, $v \epsilon \mathbb{R}^p$ est un vecteur des paramètres et$f: E \times \mathbb{R}_+ \times \mathbb{R}^p$ est le champ de vecteur, qui représente la dynamique du système (I.3) **[3].**

I.3.2.Systèmes dynamiques discrets :

Une modélisation discrète du temps peut être imposée soit par la même nature duprocessus soit par le besoin de ''discrétiser '' un modèle au temps continu pour le traiter numériquement. L'évolution du système est observée en choisissant certains moments du temps que nous allons supposer équidistants. Dans tous les cas le choix de l'unité de temps représente une partie importante de modélisation de système. Dans le modèle, le temps sera donc noté par une variable n qui prend les valeurs entières, dans ce cas, un système dynamique peut se présenter par une fonction itérative **[3]** :

$x_{n+1} = f(x_n, \mathrm{v}), \mathrm{n} \epsilon \mathrm{N}$**(I.4)**

1.3.3. Système autonomes ou non autonomes :

Un système (I.3) est dit autonome lorsque le champ vectoriel f n'est pas explicitement dépendant du temps. Sinon, il est dit non autonome. Un système non autonome peut facilement être converti en n + 1 en utilisant les changements de variables appropriés.

I.4.Etude de système de chaos

1.4.1. Définition de chaos :

Il existe différentes définitions du chaos, dont nous mentionnons les suivantes **[4]** :

- Mouvement irrégulier d'un système dynamique, qui est déterministe, sensible aux conditions initiales, et impossible à prédire à long terme par représentation infinitive et parfaite des valeurs analogiques.

•Le chaos est une évolution à long terme stable et désordonnée qui satisfait certains critères mathématiques spéciaux et se produit dans des systèmes déterministes non linéaires.

- Caractériser les propriétés d'un système dynamique, dont la plupart des orbites présentent des dépendances sensibles

1.4.2. Système dynamique chaotique:

Un système dynamique chaotique est un système qui dépend de multiples paramètres et qui est extrêmement sensible aux conditions initiales, ils ne sont pas déterminés ou modélisés par un système d'équations linéaires ou les lois de la mécanique classique, ils ne sont pas forcément aléatoires, basés sur des calculs basés sur probabilité seule.

1.4.3. Historique de chaos :

1890	Le Roi Oscar II de Suède octroie un prix au premier chercheur qu i pourrait déterminer et résoudre le problème des n-corps des orbites des corps célestes et ainsi prouver la stabilité du système solaire.
1890	Henri Poincaré gagne le premier prix du Roi Oscar II. Etant le plus proche à résoudre le problème de n-corps, il a découvert quel'orbite de trois corps célestes agissantes l'une sur l'autre peut engendrer un comportement instable et imprévisible. Ainsi, le chaos est naît.
1963	Edward lorenz découvre le premier systéme chaotique dans la météo ou encore appelé affracteurétrange.
1975	Tien_Yien et James A. York ont présenté pour la premiére fois le terme ''chaos' dans un article intitule ''Periodthreeimplieschaos''.
1978	Mitchell Feigenbaum introduit un nombreuniversel associé au chaos.

1990	Edward Ott, CelsoGrebogi et James A. Yorke. Introduisent la notion de contrôle duchaos
1990	Lou Pecora. Synchronisation des systémeschaotiques

Tableau I.*1Historique du chaos* ***[5]***

I.4.4. Classe des systèmes chaotiques :

Il existe plusieurs systèmes chaotiques utilisés pour générer des signaux chaotiques. Dans ce paragraphe, nous allons introduire deux catégories : les systèmes chaotiques continus et les systèmes chaotiques à temps discret.

a. Systèmes chaotiques continus :

Un système chaotique à temps continu est décrit par un système d'équation différentielle de forme **[6] :**

$$X = f(t, x, u), Y = (t, x, u) \quad \textbf{(I.5)}$$

Où :X le vecteur d'état de dimension n, f, R^n; R^nest une fonction non linéaire désignant le champ de vecteur, h : R n R une fonction éventuellement non linéaire qui désigne le vecteur de sortie et u∈V⊆R P représente l'entrée du système. Si ce système ne dépend pas de l'entrée, on aura alors.

$$X = f(t, x) \quad \textbf{(I.6)}$$

Il existe plusieurs systèmes chaotiques continus. Parmi eux, on peut citer les systèmes de Lorenz, Rössler, Bogdanov, le circuit de Chua,…etc.

- **Système de Lorenz :**

Le système de Lorenz est généré par le système d'équations suivant **[7]** :

$$X = a(y - x)$$

$$Y = x(b - z) - y \quad \textbf{(I.7)}$$

$$Z = xy - cz$$

Cet exemple a été publié en 1963 dans un journal météorologique.Les variables$x$, y et z représentent les états du système à chaque instant. a, b, c sont lesparamètres du systèmes.

Le système présente un comportement chaotique pour a=12, b=26, c=9 et présente un attracteur étrange en forme d'ailes de papillon **[8].**

❖ **Système de Rössler :**

Le système de Rössler est donné par les équations suivantes travaux en cinétique chimique**[8].**

$$\begin{cases} \dot{x} = -y + z \\ \dot{y} = x + Ay \\ \dot{z} = Bx + xz - cz \end{cases} \quad \textbf{(I.8)}$$

x, y et z sont les variables d'états du système .a, b, c sont les paramètres réels. Les paramètres et les conditions initiales de cette équation ont été choisis de la manière suivante :a=b=0.1, c=12, (xo, yo, zo) = (0.01, 0.01, 0.01). L'ensemble des trajectoires de ce système définissent un attracteur étrange aux propriétés fractales sur le long terme **[8].**

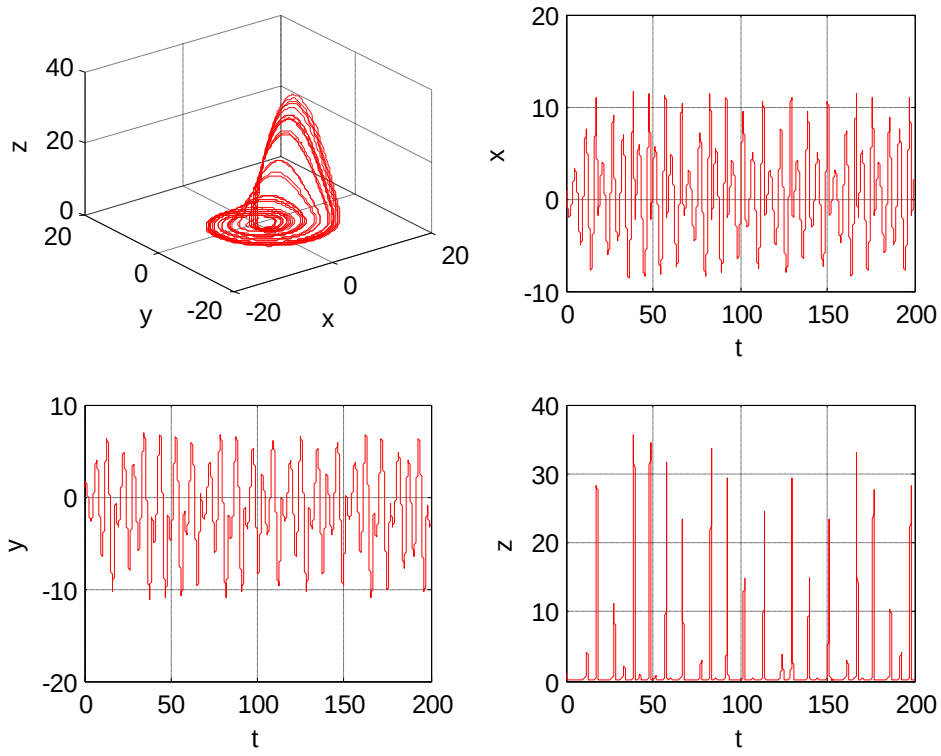


Figure I.2 : Attracteur de Rössler**[8]**

b. Systèmes Chaotiques discrets :

Un système chaotique à temps discret est décrit par un système d'équations aux différences finies, dont le modèle général est le suivant :

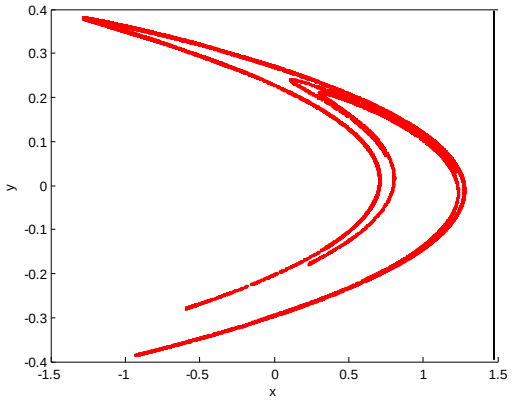
$$X(k+1) = G(x(k), u(k), y(k)) = h(x(k), u(k)) \quad \textbf{(I.9)}$$

La dynamique du système en temps discret. Parmi les systèmes chaotiques discrets, nous pouvons citer les systèmes de Hénon, Hénon modifié, Lozi, la fonction logistique, etc… **[8]**

❖ **Système de Hénon :**

Un autre modèle discret très connu, mais à 2 dimensions, est celui de l'astrophysicien M. Hénon.

$$\begin{cases} x_{n+1} = -1.4x_n^2 + y_n + 1 \\ y_{n+1} = 0.3x_n \end{cases} \quad \textbf{(I.10)}$$



FigureI.3. *Attracteur chaotique de Hénon* **[8]**

Pour les valeurs a=1.4 et b=0.3 le système présente un comportement .chaotique Les conditions initiales prises sont $x_0 = 0.1, y_0 = 0$. Pour d'autres valeurs de a et b, il peut être chaotique, intermittent ou converger vers une orbite périodique. Ainsi la figure(I.3) représente l'attracteur de Hénon.

I.4.5. Propriétés de systèmes chaotiques :

Bien qu'il n'y ait pas de définition mathématique universellement acceptée du chaos, une définition couramment utilisée pour classer un système dynamique comme chaotique doit avoir les propriétés suivantes :

- Aspect aléatoire
- Sensibilité aux conditions initiales
- Notion d'attracteur
- Fonction d'auto corrélation et spectre de puissance
- Bifurcation.

I.4.6. Caractéristiques des systèmes chaotiques :

Les définitions et les propriétés suivantes nous servent une meilleure compréhension des systèmes chaotiques **[9]:**

I.4.6.1. La non-linéarité :

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

I.4.6.2. Le déterminisme

La capacité de «prédire» le futur d'un phénomène à partir d'un évènement passe ou présent est la signification de la notion de déterminisme. La non-linéarité entraine l'évolution irrégulière du comportement d'un système chaotique. Donc un système déterministe est un système dont l'état présent est complètement déterminé par les conditions initiales. Ainsi le système chaotique a des règles fondamentales déterministes et non probabiliste

I.4.6.3. Aspect aléatoire

Tous les états d'un système chaotique présentent des aspects aléatoires. La figure (I.4) illustre l'état chaotique $x1$ du système de Rössler:

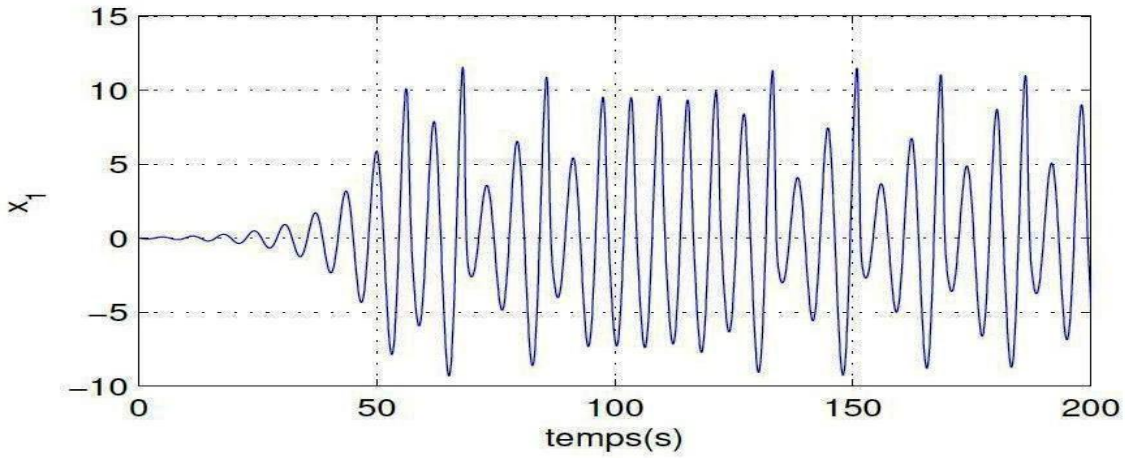


Figure I.4 : *Etat chaotique x_1 du système de Rössler***[9]**

I.4.6.5. Sensibilité aux conditions initiales :

La sensibilité aux conditions initiales signifie que chaque point d'un système chaotique est arbitrairement approximé par un autre point comme un chemin ou une trajectoire avec un futur fondamental. L'évolution à long terme du système ne peut pas être prédite car la moindre erreur ou même le moindre changement dans les conditions initiales peut conduire à de mauvaises décisions sur la trajectoire réellement suivie tout le temps. Par conséquent, la sensibilité aux conditions initiales est l'une des propriétés fondamentales du chaos. On peut la caractérise par le mesure des taux de divergences des trajectoires.

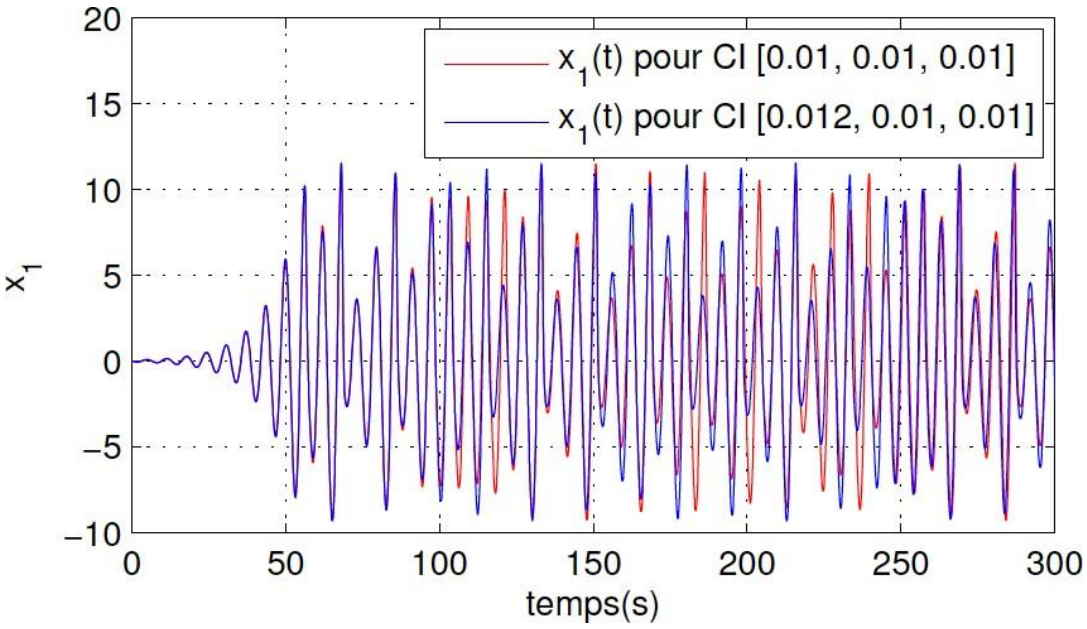


Figure.I .5 *Illustration de la propriété de sensibilité aux conditions initiales sur l'état* x_1 **[9]**

I.5. L'espace de phase :

Les systèmes dynamiques sont caractérisés par un certain nombre de variables d'état qui ont des propriétés qui définissent complètement l'état du système à un instant donné. Par conséquent, le comportement dynamique du système est lié à l'évolution de chacune de ces variables d'état. Cet espace est appelé l'espace des phases, où chaque point définit un état et les points associés à cet état décrivent une trajectoire, également appelée orbite.

I.6. Notion d'attracteur :

L'attracteur est la région de l'espace des phases où converge la trajectoire du système dynamique dissipatif. Un attracteur est une forme géométrique qui caractérise l'évolution à long terme d'un système dynamique. Il en existe quatre types différents:

- **L'attracteur point fixe :** les trajectoires tendent vers un point dans l'espace des phases, nous avons donc une solution stationnaire constante (fréquence nulle).

- **L'attracteur cycle limite :** les trajectoires ont tendance à être des trajectoires fermées dans l'espace des phases, nous avons donc une solution périodique (fréquence unique).

- **L'attracteur « tore » :** Correspond à un état quasi-périodique avec un nombre fini de fréquences.

- **L'attracteur étrange:** Cet attracteur est lié au comportement chaotique, et c'est l'attracteur qui nous intéresse.

I.6.1. Attracteur étrange :

C'est un attracteur associé à un comportement chaotique; le terme attracteur étrange a été utilisé pour la première fois par David Ruelle et Floris en 1971, le nom attracteur étrange fait référence à ses propriétés (pas une courbe ou une surface, ni continue). Par exemple, il existe plusieurs attracteurs étranges (attracteur étrange de Lorenz, attracteur étrange de Rosler,… etc.).

I.6.1.1. Attracteur étrange de Lorenz :

Le météorologue Edward Lorenz a fait un système dynamique continu qui résume l'ensemble des prévisions météorologue en trois équations différentielles qui sont : Un célèbre système chaotique est celui de Lorenz, qui a prouvé que la difficulté de la prédiction de la météorologie réside dans l'existence du chaos dans les équations climatique :

$$\begin{cases} \dot{x} = \sigma(-x + y) \\ \dot{y} = rx - y - xz \\ \dot{z} = xy - bz \end{cases} \quad \textbf{(1.11)}$$

Lorenz a étudié ces équations dans son article en1963 **[10]** et il a observé l'existence d'un attracteur étrange pour les paramètres σ = 10, r = 28, b = 8/3 .L'illustration de l'espace de phase est donnée par la figure suivante :

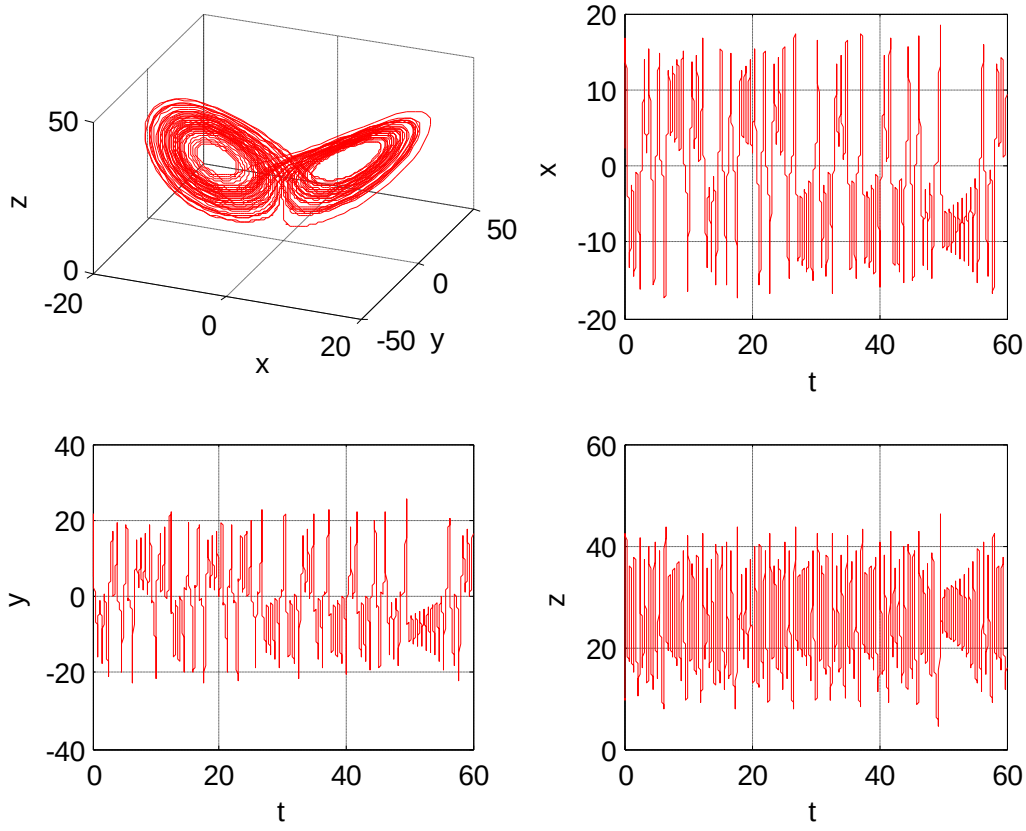


Figure I.6. *Attracteur étrange de Lorenz***[10]**

I.6.2. Dimension de Hausdorff:

La dimension de Hausdorff d'un espace métrique est un nombre réel positif ou nul, c'est-à-dire appartient à l'intervalle [0, ∞], introduit par le mathématicien Felix Hausdorff. En 1918. Un attracteur étrange occupe un volume nul dans l'espace des phases et sa dimension est fractale (d non entier), $2<d<n$, où n est la dimension de l'espace des phases.

I.7. Les exposants de Lyapunov :

L'évolution des flux chaotiques est difficile à appréhender car les trajectoires sur les attracteurs divergent très vite, c'est pourquoi on cherche à estimer voire mesurer la vitesse de divergence ou de convergence, que l'on appelle exponentielle de Lyapunov. L'exposant de Lyapunov est utilisé pour mesurer la stabilité du système et quantifier la sensibilité aux conditions initiales du système chaotique. Le nombre d'exposants de Lyapunov est égal à la dimension de l'espace des phases, et ils sont généralement indexés du plus grand au plus petit.

L'apparition du chaos exige que les exposants de Lyapunov doivent remplir trois conditions:

- Au moins l'un d'eux est positif pour expliquer la divergence des trajectoires.
- Au moins l'un d'eux est négatif pour justifier le repliement des trajectoires.
- Aa somme de tous les exposants est négative pour expliquer qu'un système chaotique est dissipatif, c'est-à-dire qu'il perd de l'énergie. La valeur du plus grand exposant de Lyapunov quantifie le degré de chaos du système, mais le fait que les trois conditions énoncées ci- dessus soient réunies ne suffit pas à conclure qu'un système est chaotique**[11].**

Le tableau suivant résume les différentes configurations d'exposants de Lyapunov évoquées précédemment **[12]:**

Régime permanent	Attracteur	Spectre	Exposants de Lyapunov
point d'équilibre	Point	composante continue	$\lambda_n \leq \lambda_{n-1} \leq \ldots\ldots \leq \lambda_1 < 0$
Périodique	courbe fermée	Fréquence fondamentale+ harmoniques entières	$\lambda_n \leq \lambda_{n-1} \leq \ldots\ldots \lambda_2 < \lambda_1 = 0$
quasi-périodique	Tore	composantes fréquentielles en rapport irrationnel	$\lambda_1 = \ldots = \lambda_i = 0$ $\lambda n \leq \lambda n-1 \leq . \leq \lambda_{i+1} < 0$
Chaotique	Fractale	spectre large	$\lambda_1 > 0$ $\lambda_n \leq \lambda_{n-1} \leq \ldots\ldots \leq \lambda_2 < 0$

Tableau I.2 : *Classification des systèmes dynamiques selon leurs exposants de Lyapunov*

I.8. Application du chaos :

Le chaos peut s'appliquer dans des diverses applications, on peut mentionner les applications suivantes:

- Contrôle: la première application du chaos est le contrôle du comportement irrégulier dans les circuits et les systèmes.
- Synchronisation: communication sécurisé, cryptage, radio.
- Traitement d'information: codage, décodage et le stockage d'information dans des systèmes chaotiques tel que les éléments de et les circuits. mémoires Reconnaissance de forme.
- Prédiction à court terme: les maladies contagieuses, température, économie **[13].**

I.9. Domaines d'application du chaos :

Parmi les nombreux domaines d'application du chaos, on cite les suivants **[14]:**

- Engineering: contrôle de vibration, stabilisation des circuits, réactions chimiques, turbines, étages de puissance, lasers…
- Ordinateurs: communications des paquets dans des réseaux informatiques. Cryptage, contrôle du chaos dans les systèmes robotique.
- Communications: compression et stockage d'image, conception et management des réseaux d'ordinateurs.
- Médecine et biologie: cardiologie, analyse et rythme du cœur(EEG), prédiction et contrôle d'activité irrégulière du cœur.
- Management et finance: prévision économiques, analyses financières, et prévision des marché.

I.10. Bifurcation :

I.10.1. Définition :

Soit le système dynamique non-linéaire suivant **[15]:**

$$x\,(k+1) = ((k),\, \alpha) \qquad \textbf{(I.14)}$$

D'où :

$x(\mathrm{k})\epsilon\mathbb{R}^{\mathrm{n}}, \alpha\epsilon\mathbb{R}^{\mathrm{m}}, \mathrm{k}\epsilon\boldsymbol{N}\ et\ F; \mathbb{R}^{n} \times \mathbb{R}^{m} \times \boldsymbol{N} \rightarrow \mathbb{R}^{\boldsymbol{n}}$

Définition1: Une bifurcation est un changement qualitatif de la solution xf du système (1.14) lorsqu'on modifie le paramètre de contrôle ; c'est à dire la disparition ou le changement de stabilité et l'apparition de nouvelles solutions.

Définition2 : Un diagramme de bifurcation est une portion de l'espace des paramètres sur laquelle sont représentés tous les points de bifurcation.

I.10.2. Types de bifurcations :

Il existe plusieurs types de bifurcations, selon la nature de la dérivée seconde d'une

famille de fonctions $((k), \alpha)$. Chacune de ces bifurcations est caractérisée par un paradigme, qui est l'équation générale typique pour de telles bifurcations. Parmi les différents types de bifurcations, pour les systèmes dynamiques discrets, on trouve :

1-Bifurcation de type nœud-col (ou tangente, ou pli) : cette bifurcation se produit lorsque l'une des deux valeurs propres de $((k), \alpha)$ est égale à +1: Sur le diagramme des bifurcations on observe, dans ce cas, une courbe de points fixes continue tangente à la ligne droite verticale. Deux points d'équilibres existent (un stable et un instable) avant la bifurcation. Après la bifurcation, plus aucun équilibre n'existe **[16].**

1- Bifurcation transcritque : sur le diagramme de bifurcations cela se traduit par deux branches différentes de points fixes qui se croisent en un point et par le changement de stabilité des deux branches au passage par le point d'intersection **[16].**

2- Bifurcation de doublement de période (ou flip) : cette bifurcation a lieu lorsque l'une des deux valeurs propres de DF (x(k);) est égales à 1. Un point fixe stable d'ordre 1, devient instable en même temps que l'apparition d'un cycle d'ordre 2 stable **[16].**

3- Bifurcation de Neimark-Sacker : cette bifurcation se produit lorsque DF (x(k)) possède deux valeurs propres complexe égale à : $e^{\pm \mathrm{i}}$**[16].**

I.11. Route vers le chaos :

Un système dynamique possède en général un ou plusieurs paramètres dit " paramètre de contrôle", qui agissent sur les caractéristiques de la fonction de transition. Selon la valeur du paramètre de contrôle, les mêmes conditions initiales mènent à des trajectoires correspondant à des régimes dynamiques qualitativement déférents. La modification continue du paramètre de contrôle conduit dans bien des cas à une complexification progressive du régime dynamique développé par le système. En général les trois scénarios de transition vers le chaos sont les suivants **[15]** :

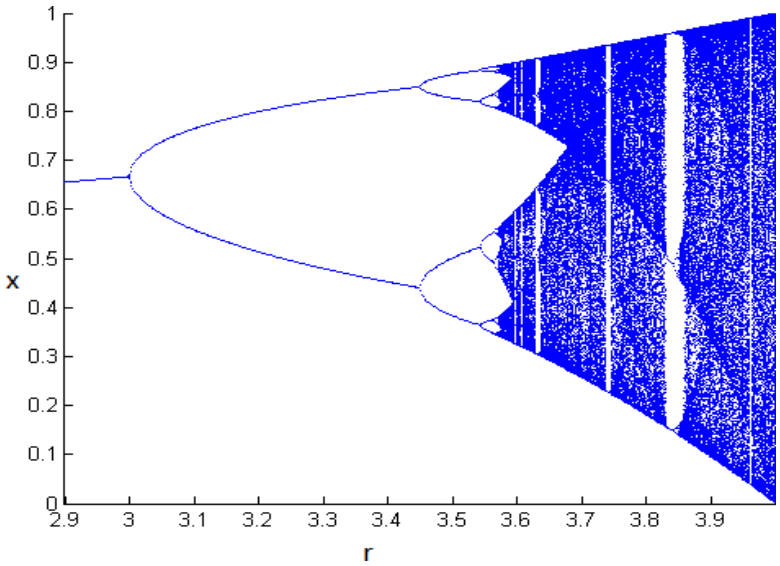


Figure I.7*Diagramme de bifurcations de l'application logistique***[15]**

a. Doublement de période :

Par l'augmentation progressive de la valeur de bifurcation, la période d'un système forcé est multipliée par deux, puis par quatre, par huit, etc..., ces doublements de période étant de plus en plus rapprochés, lorsque la période est infinie, le système devient chaotique (Voire Figure (I.10).

b. Quasi périodicité :

Le troisième scénario de transition vers le chaos est la quasi périodicité, qui intervient quand un deuxième système perturbe un système initialement périodique. Si le rapport des périodes des deux systèmes en présence n'est pas rationnel, alors le système est dit quasi périodique. Ce régime peut, à son tour, perdre la stabilité et devenir alors soit directement chaotique, soit par la survenance d'une troisième fréquence.

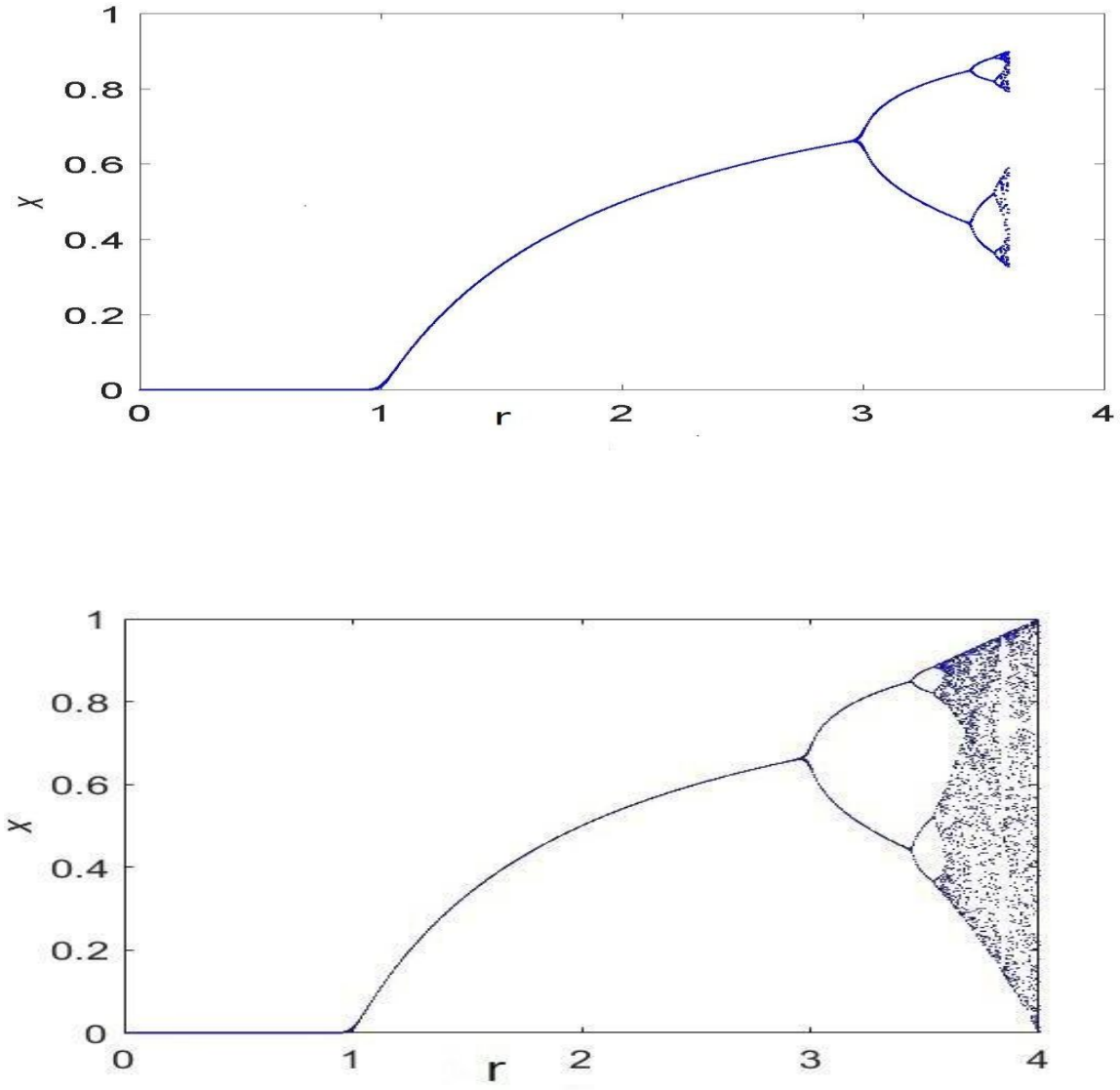


Figure I.8*Transition vers le chaos par doublement de période de l'application logistique***[15]**.

I.12. Conclusion:

Le but de ce chapitre est de présenter les concepts de base système dynamique chaotiques et définitions simple. Il faut se rappeler que l'essence du système chaotique est complexe, irrégulière et aléatoire, son comportement par rapport aux conditions initiales. Les propriétés du chaos sont d'un grand intérêt dans le domaine de la sécurité information, l'intérêt est d'ajouter l'information à transmettre au signal confusion, cette information sera déchiffrée au niveau du récepteur synchroniser. Le prochain chapitre introduit la notion de la cryptographie et présente les différents schémas de chiffrement basés sur l'utilisation des systèmes dynamiques chaotiques, et nous allons présenter la synchronisation des systèmes chaotique.

Chapitre II:

Etude de cryptage chaotique

Chapitre II:Etude de cryptage chaotique

II.1 INTRODUCTION

Les besoins réels en matière de sécurité ne cessent d'augmenter. Pour cette raison, de nombreuses personnes ont développé des systèmes cryptographie, plusieurs explications surgissent. En général, la cryptographie est principalement considérée comme une chimie noire, utilisée uniquement par les états et les gouvernements, reflétant la complexité et la difficulté, parfois uniquement déchiffrable par des mathématiciens superficiels. la cryptographie peut être utilisée pour obtenir la flexibilité, la conformité et la confidentialité des donnée requis par les systèmes actuel.

Dans ce chapitre nous allons introduire les concepts de base liée à la cryptographie tels que le chiffrement et ces différents types, et à la fin nous expliquons la synchronisation chaotique.

II.2. Terminologies:

- **Texte en clair :** est le message à protéger.
- **Texte chiffré :** est le résultat du chiffrement du texte en clair.
- **Chiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte en clair en texte chiffré.
- **Déchiffrement :** est la méthode ou l'algorithme utilisé pour transformer un texte chiffré en texte en clair.
- **Clé :** est le secret partagé utilisé pour chiffrer le texte en clair en texte chiffré et pour déchiffrer le texte chiffré en texte en clair. On peut parfaitement concevoir un algorithme qui n'utilise pas de clé, dans ce cas c'est l'algorithme lui-même qui constitue la clé, et son principe ne doit donc en aucun cas être dévoilé.
- **Cryptographie :** cette branche regroupe l'ensemble des méthodes qui permettent de chiffrer et de déchiffrer un texte en clair afin de le rendre incompréhensible pour qui conque n'est pas en possession de la clé à utiliser pour le déchiffrer. **Cryptanalyse :** c'est l'art de révéler les textes en clair qui ont fait l'objet d'un chiffrement sans connaître la clé utilisée pour chiffrer le texte en clair.

- **Cryptologie :** il s'agit de la science qui étudie les communications secrètes. Elle est composée de deux domaines d'étude complémentaires, la cryptographie et la cryptanalyse **[17].**

II.3. Technique de cryptage par le chaos:

Les schémas de communication utilisant la synchronisation de systèmes chaotiques appartiennent au domaine général de la reconstruction d'entrées inconnues. Les systèmes chaotiques constituent une classe spéciale de systèmes non linéaires, de sorte que toutes les méthodes liées aux systèmes non linéaires peuvent leur être appliquées. Les systèmes de communication utilisant le chaos représentent une application prometteuse pour l'estimation non linéaire de l'état du système. A partir du message contenant les informations, l'expéditeur génère un signal, qui est envoyé sur un canal au récepteur. Le récepteur reconstruit ensuite le message d'origine. Grâce à une "clé" partagée avec l'émetteur. Dans cet article, nous ne nous intéressons qu'aux systèmes chaotiques de communication porteuse.

II.3.1. Type de cryptage:

Il existe différents types de cryptage sur Internet. Mais bien qu'il s'agisse d'un système largement utilisé pour les applications fréquemment utilisées aujourd'hui, les utilisateurs ne savent souvent pas ce qu'ils sont et ne comprennent pas toujours comment ils fonctionnent. Par conséquent, il est important de comprendre les types de cryptage ou de cryptage des données actuellement utilisés et de discerner quel type d'accès Internet est utilisé ou utilisé à de telles fins en fonction de ses caractéristiques ou avantages. Les types de chiffrement de données sont principalement classés selon leur clé et la tâche à effectuer. C’est-à-dire en en cryptographie symétrique et en cryptographie asymétrique Ensuite, nous expliquons leur composition.

II.3.1.1 Cryptage symétrique:

Fondamentalement, il s'agit d'un système de sécurité qui utilise la même clé pour chiffrer et déchiffrer les messages; où l'expéditeur et le destinataire doivent être connus au préalable. Ainsi, un exemple clair de clé symétrique est la machine Enigma de l'armée allemande, où de nouvelles configurations de clé sont créées chaque jour. Par conséquent, le cryptage symétrique souligne que tout le cryptage ne doit pas être effectué par des programmes informatiques. En d'autres termes, chaque utilisateur peut créer un code pour lui-même.

Vous pouvez également obtenir les nombres d'origine en remplaçant les lettres et les chiffres par leurs homologues codés en utilisant les bases suivantes "a=1, b=2, z=3".

✓ **Avantages du cryptage symétrique :**

-La rapidité d'exécution (une seule clé utilisée)

-La simplicité d'implémentation (gestion d'une seule clé).

- Permet de concevoir différents mécanismes cryptographiques (fonctions de hachage, etc...)

- Clés relativement courtes.

✓ **Inconvénients du cryptage symétrique :**

- La complexité de fonctionnement : une obligation d'avoir le nombre de clés privées égal au nombre de destinataires.

- La sécurisation de la chaîne de transmission de la clé.

- Impossibilité de garantir la propriété de non-répudiation dans les schémas de signature électronique**. [18]**

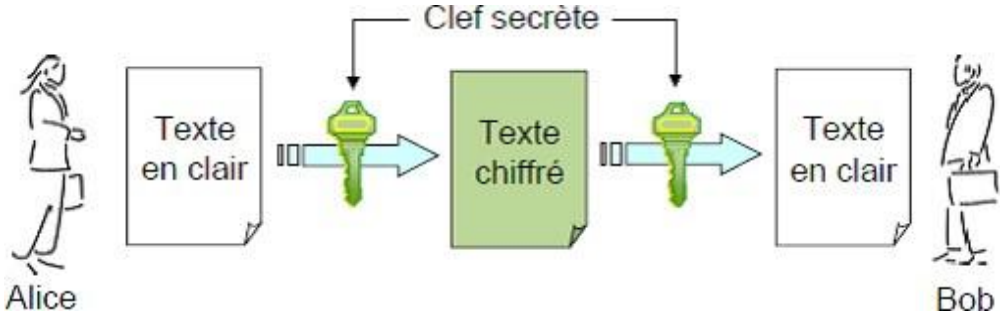


Figure II.1.Principe de cryptage symétrique

II.3.1.2 Cryptage asymétrique

Il est considéré comme une méthode simple et sécurisée et est souvent utilisé pour crypter les données que vous recevrez. C'est pourquoi il est fait électroniquement et basé sur l'utilisation de deux clés, contrairement au cryptage symétrique. Ces clés sont :

- Une clé publique qui peut être distribuée à quiconque veut vous envoyer n'importe quel type d'information cryptée

- Une clé privée, comme son nom l'indique, ne doit être révélée à personne. Il s'agit donc d'un mot de passe qu'une seule personne peut gérer. Pour cette raison, même si un

utilisateur peut chiffrer des données avec la clé publique, elles ne peuvent être lues que par quelqu'un qui possède la clé privée.

Cela signifie que le destinataire sera le seul à avoir accès à la clé de déchiffrement, ce qui permet de visualiser et de lire le message. De plus, des algorithmes complexes sont utilisés pour générer les deux clés, elles sont donc très résistantes aux attaques des cybercriminels.

✓ **Avantages du cryptage asymétrique :**

- l'élimination de la problématique de la transmission de clé

- la possibilité d'utiliser la signature électronique

- l'impossibilité de décrypter le message dans le cas de son interception par une personne non autorisé.

-Une paire de clés (publique/secrète) peut être utilisée plus longtemps qu'une clé Symétrie.

✓ **Inconvénients du cryptage asymétrique :**

- Un temps d'exécution plus lent que le cryptage symétrique

- le danger des attaques par substitution des clés (d'où la nécessité de valider les émetteurs des clés)

-Taille des clés, plus grand que celle des systèmes symétriques**. [18]**

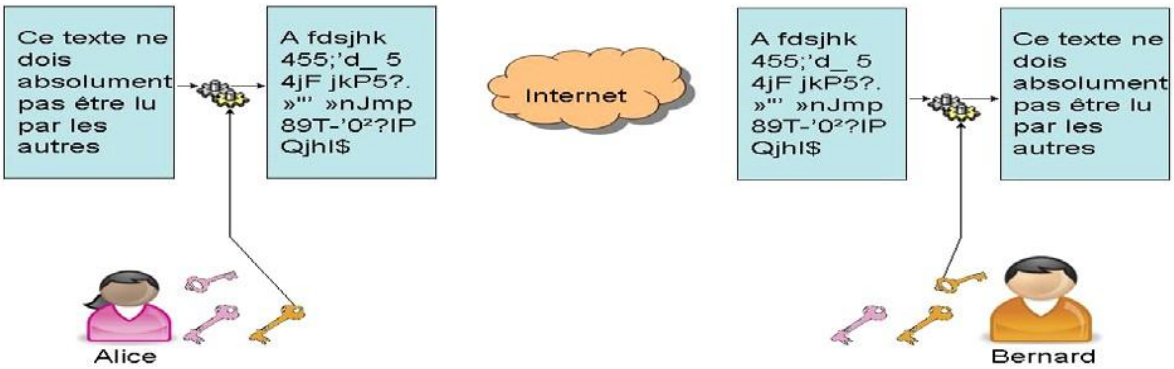


Figure II.2.*Principe de cryptage Asymétrique*

II.3.2. Différences clés entre le chiffrement symétrique et asymétrique:

La différence fondamentale qui distingue le cryptage symétrique et asymétrique est que le cryptage symétrique permet le cryptage et le décryptage du message avec la même clé.

Tandis que, le cryptage asymétrique utilise la clé publique pour le chiffrement et une clé privée pour le déchiffrement.La différence fondamentale qui distingue le cryptage symétrique et asymétrique est que le cryptage symétrique permet le cryptage et le décryptage du message avec la même clé.Tandis que, le cryptage asymétrique utilise la clé publique pour le chiffrement et une clé privée pour le déchiffrement **[19].**

Table de comparaison:

	Cryptagesymétrique	Cryptageasymétrique
Définition	Le cryptage symétrique utilise une seule clé pour le cryptage et le déchiffrement.	Le cryptage asymétrique utilise une clé différente pourle cryptage et le décryptage
Performance	Le cryptage symétrique est rapide en exécution	Le cryptage asymétrique estlent à l'exécution en raison de la charge de calcul élevée.
Algorithmes	AES, DES, 3DES et RC4	Diffie-Heliman, RS4.
Objectif	Le cryptage symétrique est utilisé pour la transmission de donnée en masse.	Cryptage asymétrique est souvent utilisé pour l'échange de clé secrétes

Tableau II.1 *Différences clés entre le chiffrement symétrique et asymétrique*

Le chiffrement symétrique utilise toujours une clé unique pour le chiffrement et le déchiffrement des messages. Cependant dans le chiffrement et utilise la clé publique pour le chiffrement. Par rapport aux algorithmes de chiffrement symétrique , les algorithmes de chiffrement asymétriques sont plus lents à exécuter .En effet , les algorithmes de chiffrement asymétriques sont plus complexes et gourmands en calculs, L'algorithmes de chiffrement symétrique le plus couramment utilisé est DES, 3DES, AES, et RC4.Alors que Diffie_helliman et RSA représente les algorithmes les plus couramment utilisés pour le

chiffrement asymétrique est souvent utilisé pour échanger des clés, tandis que le chiffrement symétrique est utilisé pour échanger des données en masse**[19].**

II.4. Cryptographie:

II.4.1. Définition :

Du grec cryptos (cacher) et graphie (écrire). La cryptographie est la science qui utilise les mathématiques pour chiffrer et déchiffrer des données. Par conséquent, il peu stocker des informations confidentielles ou les transmettre sur un réseau non sécurisé tel qu'Internet, de sorte que personne d'autre que le destinataire ne puisse les lire. Alors que la cryptographie inclut la protection des données, la cryptanalyse est l'étude des informations cryptées pour découvrir leurs secrets. La cryptanalyse classique implique une combinaison intéressante de raisonnement analytique, d'application d'outils mathématiques, de découverte de modèles, de patience, de détermination et de chance. Ces cryptanalyses sont également connus sous le nom de hackers.

II.4.2. Principe :

Tous les algorithmes évoqués jusqu'à présent sont symétriques en ce sens que la même clef est utilisée pour le chiffrement et le déchiffrement. Le problème essentiel de la cryptographie symétrique est la distribution des clefs : pour que n personnes puissent communiquer de manière confidentielle il faut n (n-1)/2 clefs.

L'idée de base des crypto-systèmes à clefs publiques a été proposée dans un article fondamental de Diffie et Hellman en 1976. Le principe fondamental est d'utiliser des clefs de chiffrement et déchiffrement différentes, non reconstructibles l'une à partie de l'autre:

- Une clef publique pour le chiffrement. --Une clef secrète pour le déchiffrement.

Ce système est basé sur une fonction à sens unique, soit une fonction facile à calculer dans un sens mais très difficile à inverser sans la clef privé

Pour faire une explication imagée, la clef publique joue le rôle d'un cadenas. Imaginons que seul Bob possède la clef (clef secrète), Alice enferme son message dans une boîte à l'aide du cadenas et l'envoie à Bob. Personne n'est en mesure de lire le message puisque seul Bob possède la clef du cadenas **[20].**

II.5. Propriété de cryptographie :

II.5.1. La confidentialité :

Consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées.

II.5.2. L'intégrité :

Permet de vérifier qu'une donnée reçue par le récepteur n'a pas été modifiée par une entité tierce (accidentellement ou intentionnellement).

II.5.3. L'authentification :

Permet de vérifier l'identité revendiquée par une entité, ou l'origine d'un message, ou d'une donnée.

II.5.4. La non-répudiation :

Permettant de garantir qu'une transaction ne peut être niée. Autrement dit, la non-répudiation de l'origine prouve que les données ont été envoyées, et la non-répudiation de l'arrivée prouve qu'elles ont été reçues **[21].**

II.6. Principe du cryptage par chaos:

Le chiffrement chaotique des messages est obtenu en superposant un signal chaotique au message initial. Ensuite, nous envoyons le message Chaos Flood au récepteur qui connaît les propriétés du générateur de chaos. Le destinataire soustrait simplement l'encombrement de son message pour trouver l'information.

II.7. Méthode de cryptage:

II.7.1. Cryptage par addition (additive chaos masking scheme):

La première et la plus simple des méthodes de cryptage, illustrée dans l'igue développe en 1993. Elle consiste en deux systèmes chaotiques identiques, l'émetteur et le récepteur. Le signal chaotique c(t) est l'une des variables d'état du système dans l'émetteur. Le message d'information (le signal utile qui doit être crypte) m(t), qui est typiquement très faible devant c(t), est ajoute au signal c(t) et donne le signal transmis s(t). Comme c(t) est très complexe et m(t) est beaucoup plus petit que c(t), alors il est décile de séparer m(t) du signal s(t) sans connaitre c(t).Le même système est utilisea la fois a l'émetteur et au récepteur, avec la différence que le récepteur est contrôle 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.**[5]**

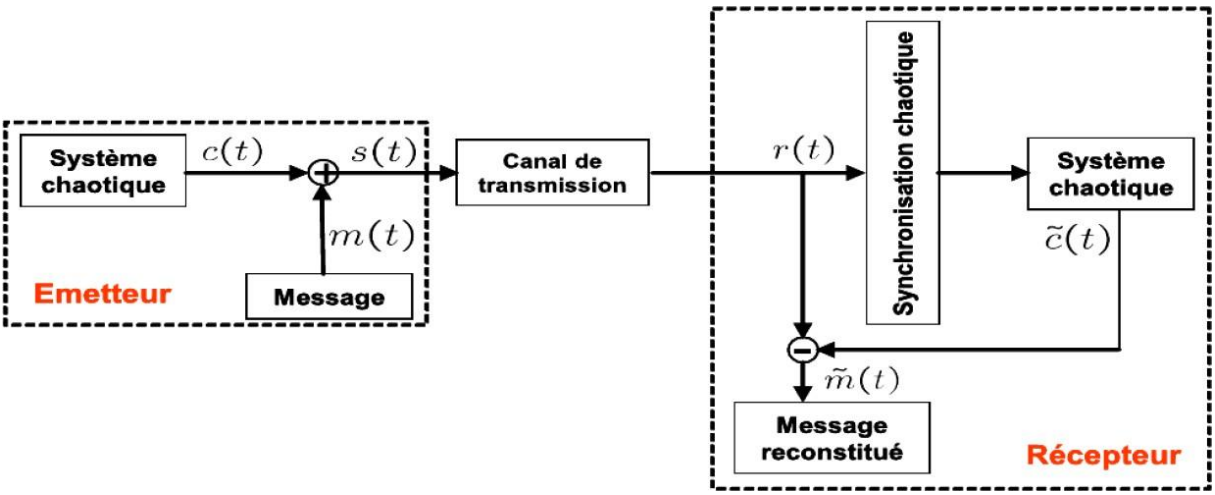


Figure II.3 *Cryptage par addition*

II.7.2. cryptage par commutation:

Cette méthode (Chaos Shift Keying en anglais, CSK) est utilisée pour transmettre des messages binaires (voir Figure II.3). L'émetteur est constitué de deux systèmes chaotiques dont l'un envoie sa sortie sur la ligne de transmission pour chaque niveau de message m(t) (0 ou 1). Ainsi, le signal transmis bascule entre deux attracteurs étranges. Le récepteur est constitué de deux systèmes chaotiques identiques à l'émetteur, et un bloc de comparaison augmente la valeur du message noté m'(t) **[3].**

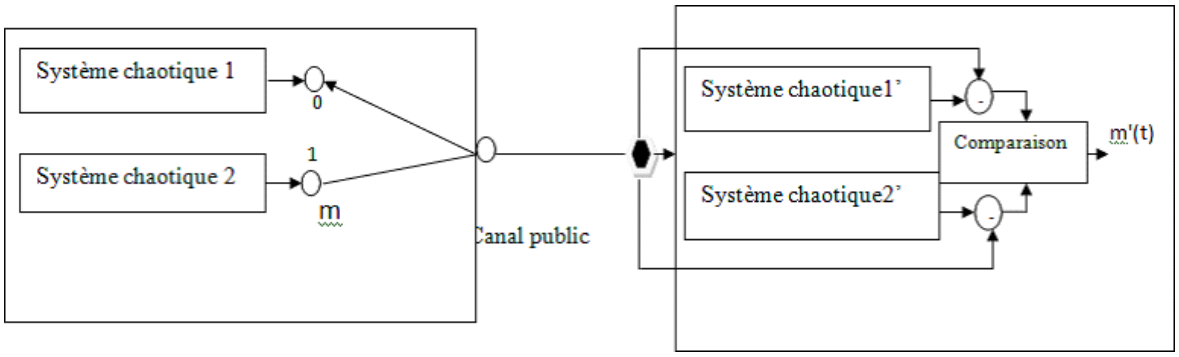


Figure II.4 : *Principe du chiffrement chaotique par commutation*

II.7.3. Cryptage par modulation:

La technique utilise des messages contenant des informations pour moduler les paramètres d'un émetteur chaotique. Le contrôleur adaptatif est responsable du maintien de la synchronisation au niveau du récepteur tout en suivant les modifications des paramètres de

modulation. Le schéma correspondant est illustré à la Fig. Au niveau de l'émetteur, le fait qu'un (ou plusieurs) paramètres soient modulés oblige la trajectoire à changer constamment d'attracteur et, par conséquent, le signal émis est plus complexe que le signal chaotique

normal. Cependant, la manière dont le message est injectée, et donc la fonction de modulation paramétrique, ne peut éliminer le caractère chaotique du signal envoyé au récepteur. Il convient de souligner que cette technique tire pleinement parti des propriétés des systèmes chaotiques. Cependant, le cryptage par modulation s'est avéré sensibles à certaines attaques.**[3]**

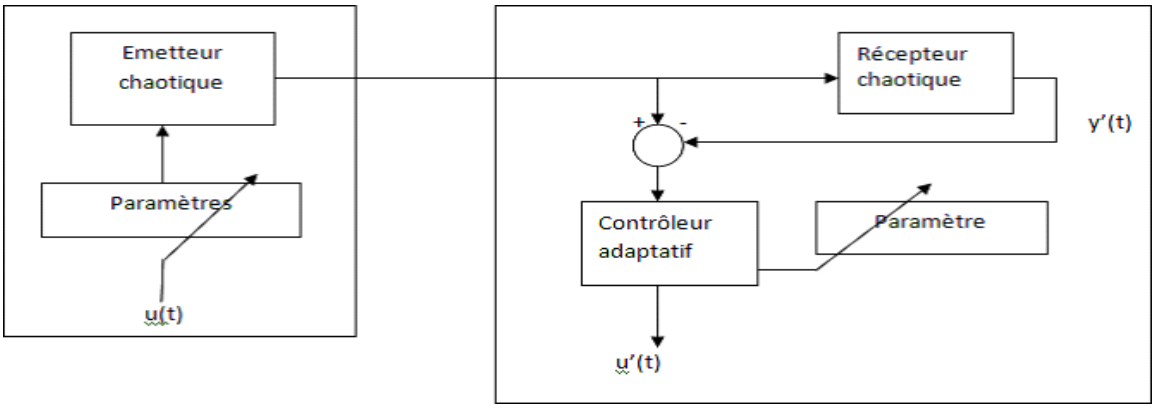


Figure II.5 : *Principe du chiffrement chaotique par modulation*

II.7.4. Cryptage Mixte:

Afin de résoudre les problèmes de sécurité des procédés ci-dessus, une nouvelle technologie qui combine le principe de cryptographie standard avec le principe de synchronisation du chaos est proposée. Le message u(t) contenant l'information est chiffré avec une clé c(t) générée par l'expéditeur chaotique : le message crypté est ensuite injecté dans la dynamique du système chaotique pour le rendre plus complexe. Ensuite, un signal y(t) qui dépend de la variable d'état de l'émetteur est envoyé au récepteur, qui établit une synchronisation avec l'émetteur. C'est alors au récepteur de reconstituer la clé et enfin le

message peut être décodé. Le principe général de cette approche est illustré par la figure **2.6**

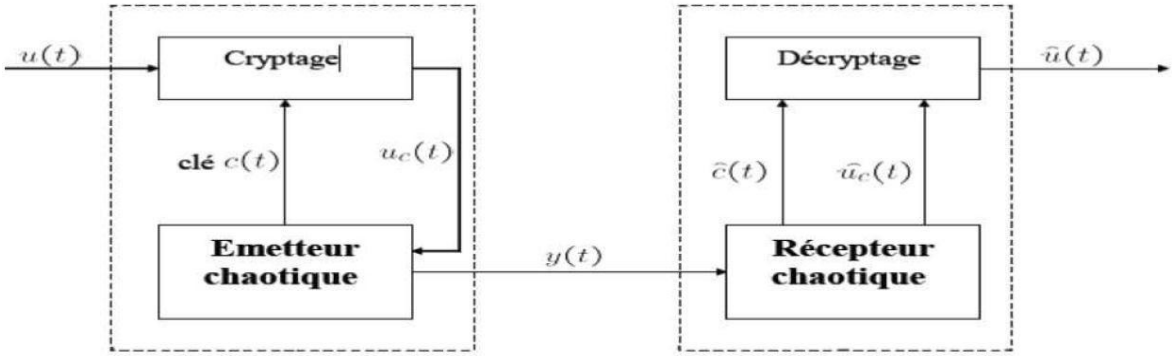


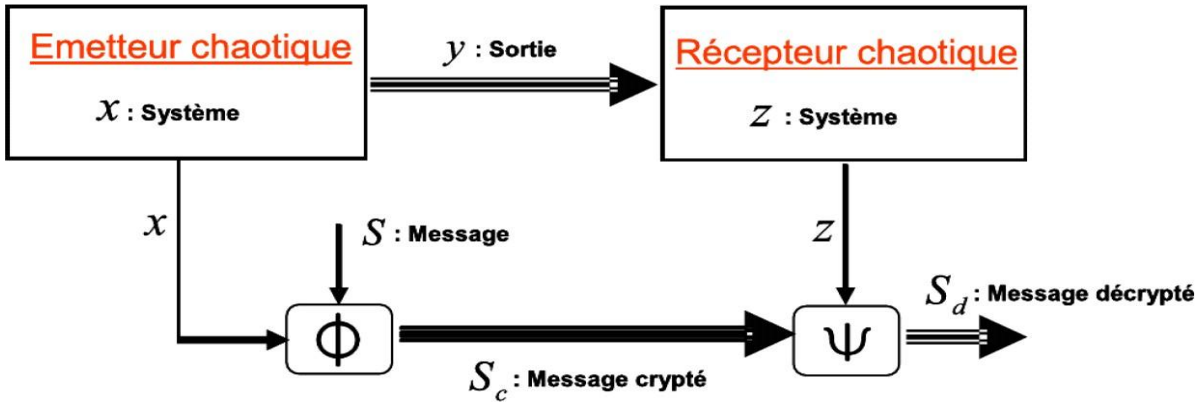
Figure II .6 *Cryptage mixte*

II.7.5 Transmission par deux voix:

Pour cette technique, les deux étapes de synchronisation et de chiffrement sont indépendantes. En fait, deux lignes de transmission sont utilisées. Première est utilisé pour synchroniser l'émetteur et le récepteur, tandis que le second est pour le cryptage Fondamentalement, ce nouveau schéma de communication se compose de trois étapes :

- cryptage
- Synchronisation
- décryptage

Dans la première étape, le message confidentiel s(t) et l'état chaotique x(t) sont chiffrés simultanément à l'aide d'une fonction non linéaire forte Φ. Le signal cryptés c(t) est alors envoyé au récepteur à travers le canal de transmission. Dans la deuxième étape, le signal chaotique y = h(x) est transmis à travers un deuxième canal de transmission séparé du premier canal de transmission. Ce signal n'est utilisé que pour la synchronisation et ne contient aucune information sur le message s(t). Dans la troisième et dernière étape, l'estimé z(t) de l'état x(t) généré par le récepteur chaotique (construit par le processus de synchronisation) et la fonction de déchiffrement Ψ sont utilisés pour reproduire le message confidentiel s(t). La description du système de ce processus est illustrée par la igue . Exemple pour les fonctions Φ et Ψ. **[5]**



FigureII.7. *Communication a deux lignes de transmission*

II.7.6. Cryptage par inclusion:

Cette technique de cryptage consiste à injecter des messages dans la dynamique de l'émetteur, mais n'effectue pas de modulation paramétrique. La récupération des informations est principalement réalisée par deux techniques, s'appuyant sur un observateur avec une entrée inconnue, ou s'appuyant sur l'inversion du système émetteur.

II.8. La cryptanalyse:

La cryptanalyse ou l'attaque d'un crypto-système est une étape importante, mais Parfois ignorée, elle évalue le niveau de sécurité apporté par la méthode proposée. Ainsi, après avoir recherché une méthode chaotique de synchronisation et de chiffrement, Toutes les méthodes d'attaque applicables doivent être explorées dans différents scénarios. Parce que souvent, les failles de sécurité ne sont découvertes qu'après la catastrophe. Ainsi, Ironiquement, le constructeur (ou l'utilisateur) du crypto-système doit être le premier avenant.

En fait, casser le cryptage équivaut à extraire le message source sans Connaissance préalable du schéma récepteur, ou au moins connaissance partie de ce dernier. En général, un intrus doit avoir au moins deux versions (cryptée et texte brut) pour lancer l'attaque. Et les statistiques La linguistique sont souvent utilisées pour associer des symboles en clair à leurs versions chiffrement. C'est ce qui a suscité l'intérêt pour le chiffrement des systèmes chaotiques. Efficace, Les signaux cryptographiques chaotiques associés à des symboles clairs à un instant donné coïncident rarement Les mêmes symboles sont utilisés à d'autres moments. Ici aussi, les méthodes d'identification du chaos ont un grand potentiel. Car Le fait que les transmissions cryptées chaotiques puissent être détectées (ou distinguées) est Établi une base importante pour différentes critiques et comparaisons méthode de cryptage. Ce potentiel sera exploré dans des travaux futurs. Chaos vs Cryptographie.

II.9. Comparaison entre chaos et cryptographie:

La technologie cryptographie de chiffrement basée sur le chaos offre une bonne combinaison de vitesse, de haute sécurité, de complexité, de temps de calcul raisonnable et de puissance de calcul. Plusieurs propriétés font des systèmes chaotiques des candidats attractifs pour la sécurité des communications. On peut citer un des spectre spectres large bande, des trajectoires qui ne reviennent jamais au même état, un des aspect aspects pseudo-aléatoire aléatoires (e.g. comme le bruit), une des implémentation implémentations relativement simple simples d'un de système systèmes chaotique chaotiques. De plus, certains chercheurs ont remarqué une relation intéressante entre le chaos et la cryptographie depuis les années 90. En en fait effet, plusieurs propriétés des systèmes chaotiques ont des correspondances similaires ou presque avec similaires les aux crypto- systèmes traditionnels. Le tableau suivant illustre parfaitement cette correspondance.

II.10. Synchronisation :

II.10.1. Définition de synchronisation :

Définition 1: (de Larousse) Synchronisation est un mot grec décomposé en deux parties : Syn veut dire ensemble et Chrono veut dire temps. C'est l'action de mettre en phase pour créer une simultanéité entre plusieurs opérations, en fonction du temps.

Définition 2: (générale) La synchronisation est une manière de faire l'entretien d'un mouvement périodique (ou chaotique). La synchronisation de deux systèmes dynamiques signifie que chaque système évolue en suivant le comportement de l'autre système. **[22]**

Définition de synchronisation en mathématique :

Après plusieurs tentatives pour dé.nir un mouvement synchronisé, Brown et Kocarev ont récemment fourni une définition mathématique de la synchronisation. Pour construire la définition, ils supposent qu'un système dynamique, global, de dimensionfinie et déterministe est divisible en deux sous-systèmes :

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

$$\dot{y} = f\big(y(t)\big) \textbf{(II.1)}$$

Où, $x(t) \epsilon \mathbb{R}^n$ et $y(t) \epsilon \mathbb{R}^m$ sont des vecteurs qui peuvent avoir des dimensions différentes.

II.10.2. Principe de synchronisation des systèmes chaotiques:

En 1996, Thomas Carol et Louis Peccora ont découvert la synchronisation chaotique du signal. La synchronisation est un phénomène qui se produit lorsque deux systèmes dynamiques identiques évoluent dans le temps. Il s'agit de synchroniser et de rapprocher les trajectoires des deux systèmes jusqu'à ce qu'elles deviennent chaotiques.

La synchronisation suivie à la configuration de synchronisation la plus populaire, cette dernière consiste à forcer un système dynamique appelé l'esclave à se synchroniser avec un deuxième système dynamique appelé le maître (suivant la même trajectoire).

II.11. Type de synchronisation des systèmes chaotique :

Suite à cette découverte de Pecora et Carroll, plusieurs types de synchronisation ont été introduits, souvent basés sur le même principe utilisant le même circuit. Supposons que deux systèmes chaotiques identiques oscillent de manière complètement indépendante. S'ils sont autorisés à échanger de l'énergie d'une manière ou d'une autre, c'est ce qu'on appelle le "couplage"; les deux systèmes finiront par céder la place à un comportement commun, c'est la synchronisation.

On trouve deux types de synchronisation classés selon la direction de l'énergie échangée entre les deux systèmes chaotiques : La synchronisation par couplage unidirectionnelle et synchronisation par couplage bidirectionnelle.

Dans ce qui suit nous allons définir et donner le principe des deux types de synchronisation.

II.11.1. 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 **[23].**

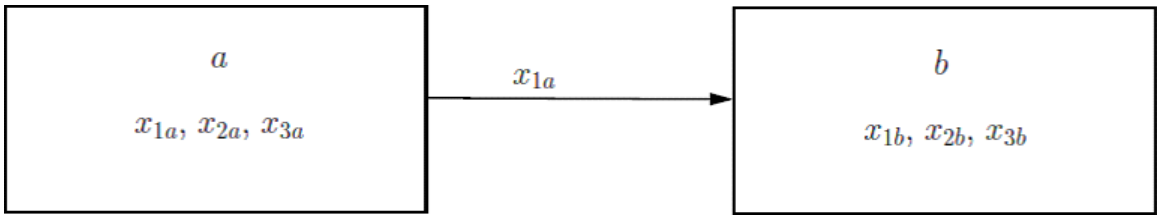


Figure. II.8. *Couplage unidirectionnel*

II.11.2. 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 **[24].**

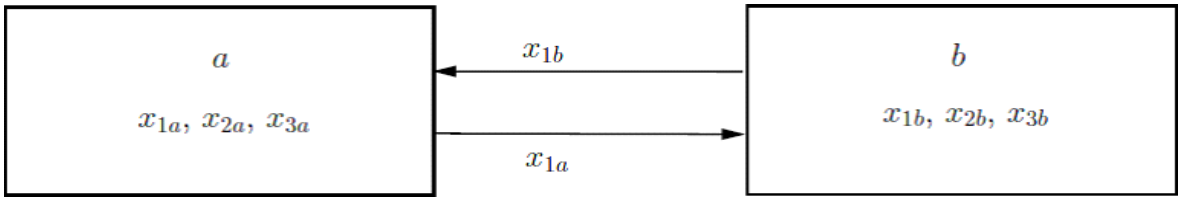


Figure. II.9. *Couplage bidirectionnel*

II.12. Méthode de synchronisation :

Cette section est consacrée à la présentation de diverses méthodes de synchronisation les plus performantes et les plus rencontrées.

II.12.1. Synchronisation par boucle fermée :

L'idée de la synchronisation en boucle fermée est de corriger le comportement du système récepteur en fonction de l'erreur injectée dans ce dernier due à l'erreur entre le signal émis par le premier système et le signal régénéré par l'autre système. La figure ci-dessous est un schéma simplifié de synchronisation en boucle fermée**.**

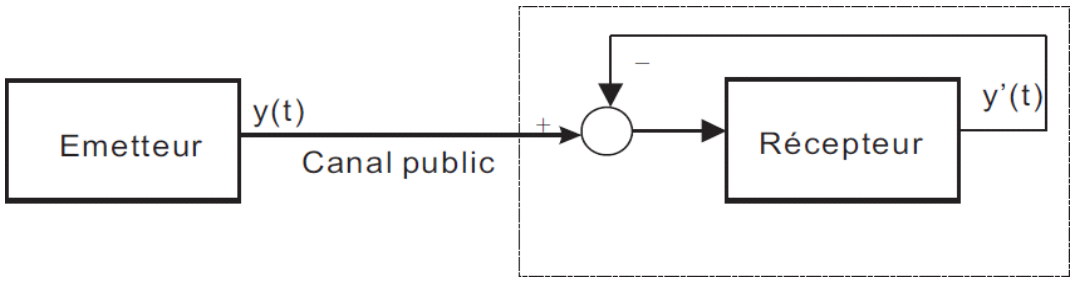


Figure. II.10. *Synchronisation par boucle fermée*

II.12.2. Synchronisation impulsive:

Dans un schéma de transmission commun, l'un des états du système dynamique est transmis pour synchronisation par le récepteur. Pour réduire la redondance du signal transmis, une synchronisation des impulsions a été proposée (Figure II.11). Le contrôle impulsif du système signifie qu'à des moments sélectionnés, l'état du système change soudainement. Dans

ce diagramme de synchronisation, on considère le système maître sous la forme générale suivante :

$$\dot{x}(t) = f\big(x(t)\big) \textbf{(II.3)}$$

On définit un signal impulsionnel, qui est constitué d'une suite d'instants discrets auxquels le signal $y(t) = Cx(t)$ est envoyé par le système maître vers le système esclave, dont les variables d'état subissent un saut et un changement d'état. D'état. La figure représente le schéma synoptique de la synchronisation impulsive.

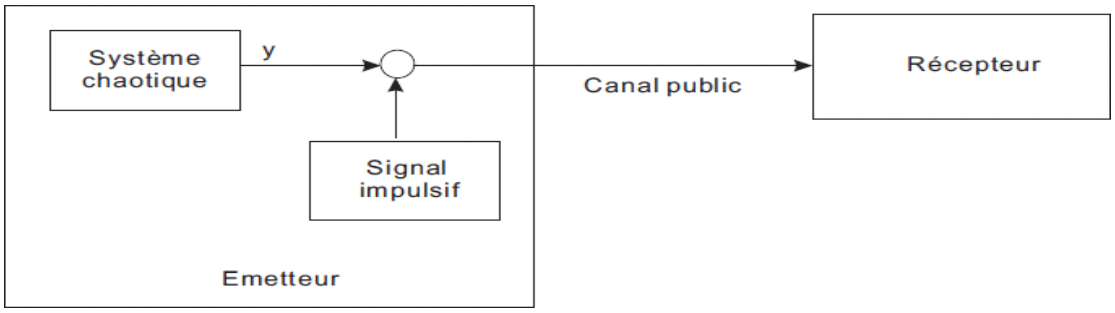


Figure. II.11. *Synchronisation impulsive*

II.12.3. Synchronisation à l'aide d'observateur

La synchronisation peut également être effectuée à l'aide d'observateurs. Un observateur est un système dynamique qui peut estimer des états inconnus du système qui ne peuvent pas être mesurés directement (pour des raisons techniques ou économiques). Un système dynamique est dit observable si toutes ses quantités peuvent être récupérées (soit statiquement, soit dynamiquement) par une combinaison de mesures de sa sortie et de ses dérivées **[25].** La synthèse d'observateurs pour les systèmes linéaires a fait l'objet de nombreux travaux **[26**], en fait le premier travail sur les observateurs, publié vers les années 60 par Kalman et Luenberger, le premier s'intéresse aux systèmes linéaires variant dans le temps, le second s'intéresse au temps- variables - systèmes linéaires invariants. Dans la synchronisation d'observateur, le système maître est un système chaotique arbitraire et le système esclave est l'observateur d'état correspondant. La Figure (II.12) illustre ce principe de synchronisation.

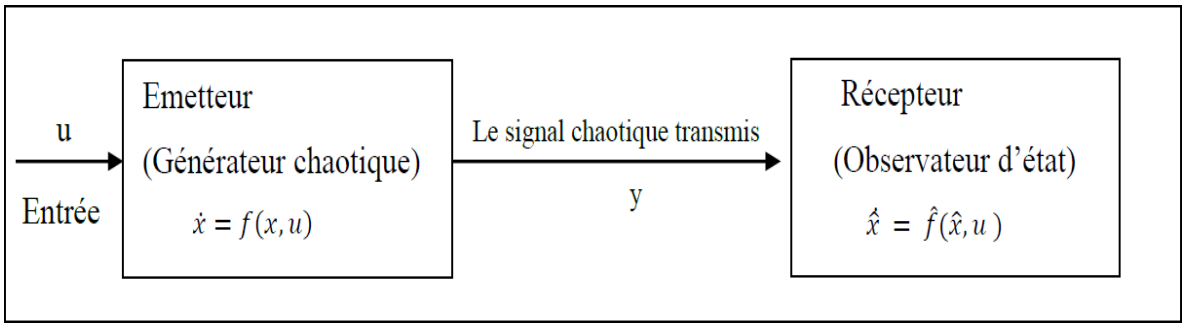


Figure II.12 : *Principe de synchronisation à l'aide d'observateur.*

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

$\lim_{t\to\infty} \|x(t) - \hat{x}(t)\| = 0$**(II.4)**

Des différents types d'observateur (en temps continue et en temps discret) dans différent buts ont été proposés :

- L'observateur de Kalman étendu. Les observateurs à grand gain. Les observateurs à modes glissants sont basés sur la théorie des systèmes à structures variable.
- L'observateur adaptatif, pour l'évaluation des états et les paramètres du système dynamique.
- L'observateur dead-beat pour les systèmes en temps discret.

II.12.4. Synchronisation projective:

Dans cette méthode, l'état du système récepteur est synchronisé avec un multiple de l'état du système émetteur, il y a doncα et τ.

$\lim_{n\to t} \|\hat{x}_1(t) - \alpha x(t-\tau)\| = 0$**(II.5)**

Ce type de synchronisation est utilisé pour des systèmes partiellement linéaires et permet de synchroniser à un facteur prés les états qui ne peuvent être synchronisée **[5].**

2.12.5. Synchronisation identique:

Ou la synchronisation complète, qui est la synchronisation la plus ancienne et la plus simple des systèmes couplés chaotiques et donne une solution simple mais puissante. Le principe est de reproduire l'état du système maître à partir du système **[24]**.

Considérons deux systèmes dynamiques:

$\dot{x}_m(t) = f(x_m(t))$ **(II.6)**

Et

$\dot{x}_s(t) = f(x_s(t))$ **(II.7)**

Où $\dot{x}_m, \dot{x}_s \epsilon R$n sont des vecteurs d'état de dimension n.

Alors (II.6) et (II.7) sont identiquement synchronisés si, quelles que soient leurs conditions initial:

$\lim_{t\to\infty} |x_s(t) - x_m(t) = 0$**(II.8)**

II.12.6. Synchronisation retardée:

En synchronisation retardée, l'état du système esclave tend vers l'état décalé dans le temps du système maître, soit **[25]:**

$\lim_{t\to\infty} \|\hat{x}_1(t) - x(t-\tau)\|$ **(II.9)**

Ou $x(t)$est l'état du système émetteur, $\hat{x}(t)$l'état du système récepteur, et r est un retard positif **[25].**

2.12.7. Synchronisation généraliste :

Cette méthode est une généralisation du même concept de synchronisation. Les deux systèmes sont synchronisés au sens large, s'il existe une transformation M telle que :

$\lim_{n\to\infty} y(t) - M\big(x(t)\big) = 0$ **(II.10)**

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

Dans ce cas Les conditions initiales ne sont prises en compte. Si M est inversible, alors

M^{-1} (y) fournit une estimation de l'état x. Ceci est une impossible de fournir une estimation inconvénient majeur pour les techniques de communication qui utilisent l'état de l'expéditeur pour déchiffrer le message transmis.

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

$\lim_{n\to\infty} \|y(t) - x(t-\tau) = 0$**(II.11)**

Où $x(t)$est l'état du système émetteur, $y(t)$est l'état du système récepteur et r est un retard positif **[26].**

II.13. Propriétés des systèmes de communication à base de chaos:

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

II.13.1 Spectre à large bande

Les systèmes chaotiques en particulier ont un spectre large bande. Cette propriété est bénéfique pour les applications qui nécessitent une grande robustesse contre les interférences et une faible probabilité de détection **[27]**.

Ces problématiques ont été prises en compte par les premiers systèmes de transmission utilisant une modulation à large spectre et à saut de fréquence. Cependant, malgré l'utilisation de ces moyens, la synchronisation entre émetteurs et récepteurs reste une tâche qui n'est pas toujours triviale. En pratique, les schémas de transmission par saut de fréquence nécessitent une nouvelle synchronisation à chaque changement de fréquence porteuse. L'utilisation d'un système chaotique permet ainsi la transmission de signaux large bande et donc une synchronisation plus simple entre émetteur et récepteur.

II.13.2. Signal non périodique

La périodicité des communications de sécurité peut produire des pics spectraux indésirables. D'autre part, les signaux chaotiques sont apériodiques et leur évolution ne peut pas être prédite sur de longs intervalles de temps. Il n'y a donc pas de pics spectraux. De plus, il est plus difficile de développer des modèles prédictifs avec une dynamique apériodique **[27].**

II.13.3. Implémentation analogique simple

Les systèmes de communication basés sur le chaos peuvent être mis en œuvre à l'aide de dispositifs électriques ou optiques. Dans les schémas traditionnels, tels que la transmission par sauts de fréquence, la numérisation des données est nécessaire, ce qui implique des circuits séparés plus complexes **[27].**

II.14. Conclusion :

Le but de ce chapitre était de présenter la cryptographie par chaos avec son principe et son objectif et nous venons de voir le principe de synchronisation des systèmes chaotique et les déférentes méthodes utilisées pour la synchronisation.

La cryptographie fournit une «couche » de sécurité supplémentaire (en plus d'un système désordonné plus ou moins difficile à casser) pour empêcher que le signal transmis soit lu et déchiffré par toute personne/organisation autre que la destination du message chiffré.

Ce travail est très important pour le chapitre suivant, qui effectueront des simulations informatiques et réaliseront ensuite la synchronisation de la communication chaotique.

Chapitre III:

Simulation

III.1. Introduction

Le chaos est l'une des dynamiques les plus complexes que les systèmes non linéaires,euvent présenté. Pour cette raison, des systèmes chaotiques ont été utilisés pour protéger les communications. Les signaux générés par les systèmes chaotique bien que déterministes on des propriétés statistique proche de l'aléatoire .Par conséquent, les systèmes chaotiques ont été utilisés pour communication sécurisée, et plusieurs systèmes de cryptage chaotiques ont été proposés pour masquer les informations.

Dans la plupart des schémas de communication nous trouvons deux parties :un générateur de chaos appelé émetteur, et un système de réponse appelé récepteur.

Dans ce chapitre, on ca étaler les différents résultats sous MATLAB en utilisant l'algorithme d'intégration numérique de Runge – kutta d'ordre4.

III.2.Transmission basée sur la synchronisation de systèmes chaotique:

Dans cette partie du chapitre, on s'intéresse aux techniques de transmission sécurisé d'informations qui reposent sur le principe de synchronisation chaotique. Constaté dans la majorité des techniques développées dans la littérature est l'utilisation de Configuration maître-esclave pour laquelle on dispose d'un émetteur chaotique (systèmeMaître) qui génère un signal porteur du message transmis dans le canal de communication vers un système récepteur (système esclave) qui a pour objectif de se synchroniser avec leSystème maître dans l'objectif de restaurer le signal d'information **[28],[29].**

Les signaux chaotiques peuvent être utilisés pour la transmission de l'information principalement dans deux objectifs : Le premier objectif est de protéger l'information transmise et dans ce cas, les applications réalisées sont en compétition avec les méthodes cryptographie classiques. Un deuxième objectif est d'étaler le signal informationnel avec des avantages des techniques à étalement de spectre. Dans ce deuxième cas, les méthodes développées doivent être comparées aux systèmes classiques à étalement de spectre **[29].**

Si on regarde du point de vue de la structure d'un tel système de transmission, on peut définir deux approches. La première, remplace le signal porteur sinusoïdal par un modulateur chaotique contrôle, d'une manière quelconque par le signal informationnel. Cette solution a l'avantage d'être très simple à implémenter, mais par contre nécessite un système chaotique avec des contraintes fortes sur les paramètres intrinsèques. En plus, celui-ci doit travailler à des hautes fréquences. En pratique, il est difficile de trouver de Circuits permettant un tel

fonctionnement. Pour le moment, cette solution est surtout Considérée dans un cadre théorique **[29].**

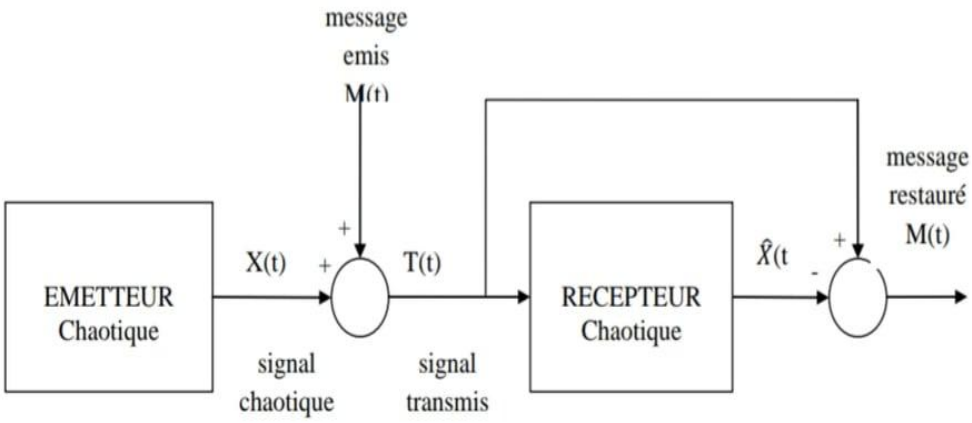


Figure III .1.*Schéma présentatif de la technique de masquage chaotique [30]*

Le system de transmission propose est constitué de deux module:

III.2.1. Bloc émetteur:

Ce module contient un oscillateur chaotique un signal à temps discret et un module de cryptage qui utilise un cryptage additif pour masquer le signal sélectionné.

III.2.2. Bloc récepteur:

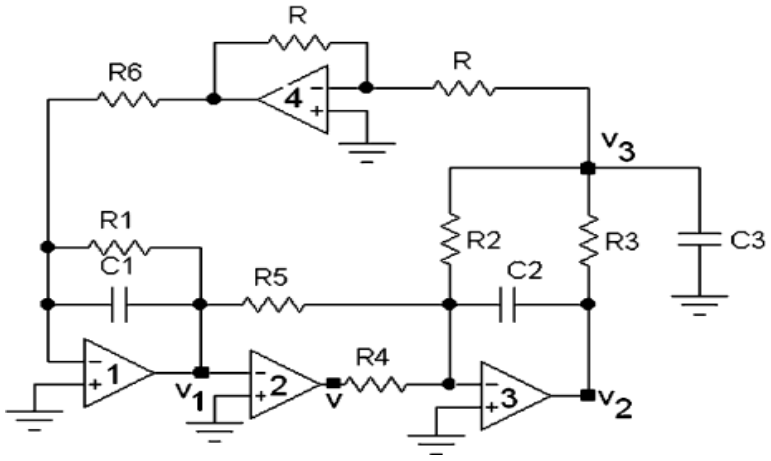
Le bloc continent un observateur pour estimer d'états du system et un bloc de déchiffrement compose de soustracteurs.

III.3.Circuit de Sportt:

III.3.1. oscillateur chaotique de Sprott:

Un circuit Sprott est un circuit électronique qui présente le chaos et de nombreux phénomènes de bifurcation connus.

III.3.2 Présentation du circuit de Sprott:



FigureIII.2 *Le circuit électrique de l'oscillateur de Sprott[31]*

La figure (III.2) représentant notre oscillateur de Sprott comporte des résistances, condensateurs et des amplificateurs opérationnels.

L'oscillateur est un système dynamique du troisième ordre. La dynamique de l'oscillateur est donnée par les trois équations différentielles suivantes :

$$\frac{dv_1}{dt'} = -\frac{1}{R_1C_1}V_1 + \frac{1}{R_6C_1}V_3$$

$$\frac{dV_2}{dt'} = -\frac{1}{R_5C_2}V_1 - \frac{1}{R_2C_2}V_3 + \frac{1}{R_4C_2}V_{cc}\,sign(V_1) \textbf{(III.2)}$$

$$\frac{dV_3}{dt'} = \frac{1}{R_3C_3}V_2 - \left(\frac{1}{RC_3} + \frac{1}{R_2C_3} + \frac{1}{R_3C_3}\right)V_3$$

La fonction signe est définie par:

$$\text{sign } (x) \begin{cases} = -1 & six < 0 \\ = 0 & six = 0 \\ = 1 & six > 0 \end{cases} \quad \textbf{(III.3)}$$

On précède ensuite les changements de variable suivants:

$$X = \frac{V_1}{V_{cc}}, Y = \frac{V_2}{V_{cc}}, Z = \frac{V_3}{V_{cc}}, t = W_0 t', Q_1 = \frac{1}{R_1C_1W_0}, Q_2 = \frac{1}{R_6C_1W_0},$$

$$Q_3 = \frac{1}{R_5C_2W_0}, Q_4 = \frac{1}{R_2C_2W_0}, \quad Q_5 = \frac{1}{R_4C_2W_0}, Q_6 = \frac{1}{R_3C_3w_0}, \textbf{(III.4)}$$

$$Q_7 = \left(\frac{1}{R_3C_3W_0} + \frac{1}{R_2C_3W_0} + \frac{1}{RC_3W_0}\right), W_0 = \frac{1}{\sqrt{R_2R_3C_2C_3}}$$

Le changement de variable sert à rendre les grandeurs adimensionnelles. On obtient le système d'équations différentielles suivant**[32]:**

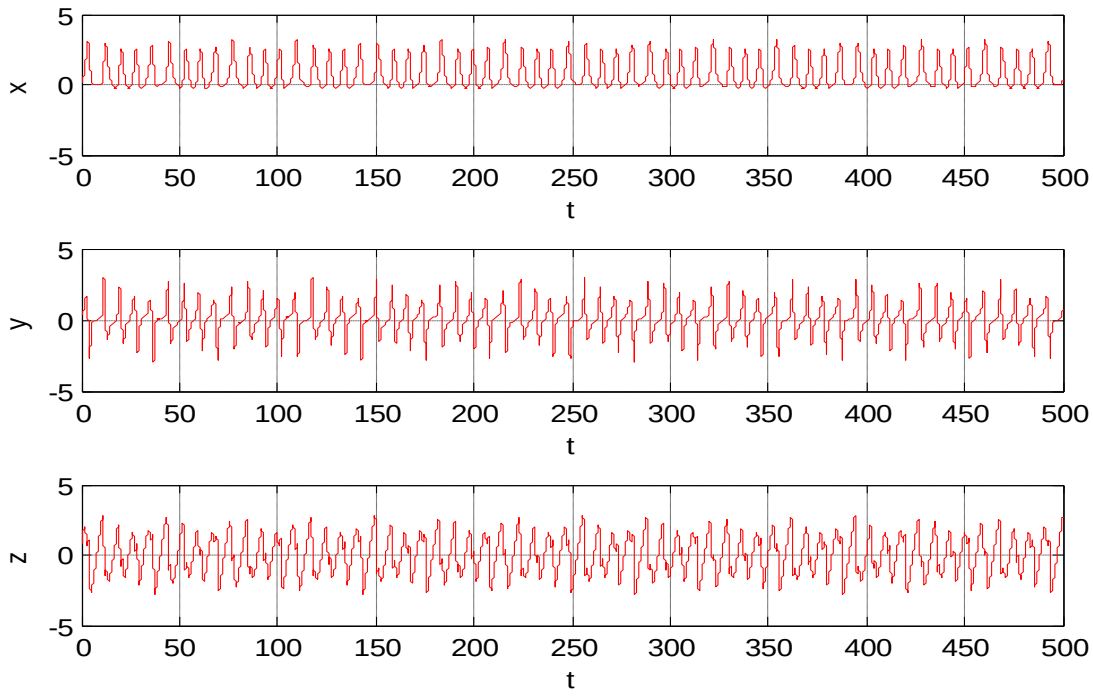
$$\dot{x} = -Q_1x + Q_2z$$

$$\dot{y} = Q3\ x - Q4z + Q5\ (x) \qquad \textbf{(III.5)}$$

$$\dot{z} = Q_6y - Q_7$$

III.3.3.Aspect aléatoire:

Les courbes suivantes montrent l'aspect chaotique de l'oscillateur de Sprott pour les conditions initiales suivantes ($x_0 = 0.1, y_0 = 0.3, z_0 = 0.8$)



FigureIII.3:*Etats (x, y et z) du système de Sprott.*

III.3.4.Palan de phase :

Le système non linéaire de Sprott présente un comportement chaotique. Les figures (III.4), (III.5), (III.6) et la figure (III.7) présentent un exemple d'une trajectoire chaotique de ce circuit.

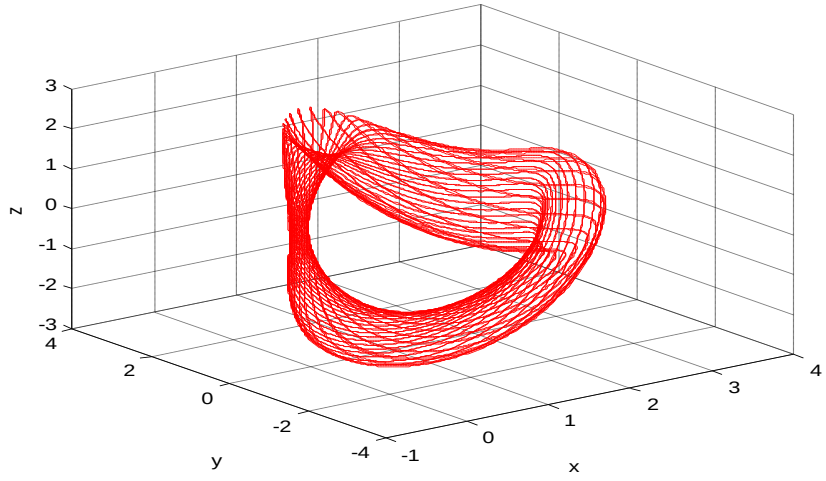
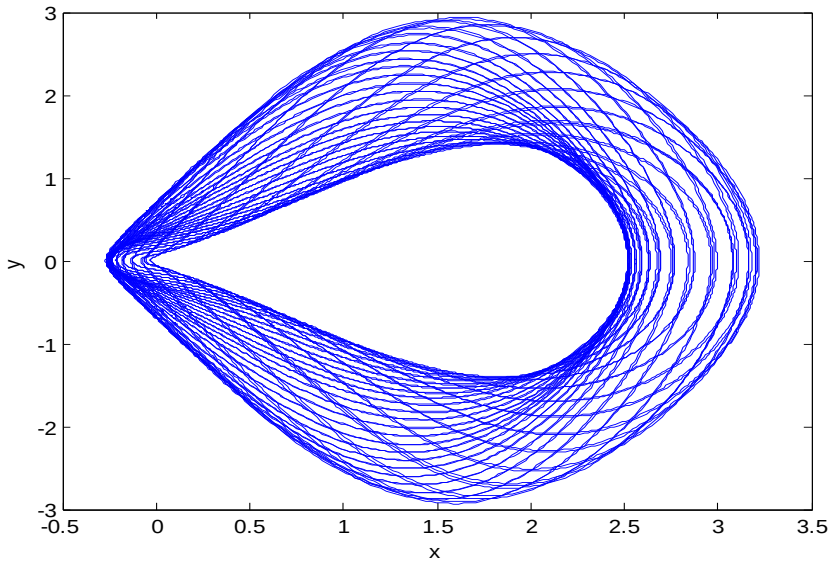


Figure III.4:l'attracteur de l'oscillateur de Sprott

Cette figure présente l'allure de la trajectoire du système de Sprott et illustre l'aspect chaotique de ce système en fonction de X,Y et Z.



FigureIII.5.Plan de phase(X,Y) de l'oscillateur de Sprott

La figure (III.5) présente le comportement chaotique du système dans le plan X,Y.

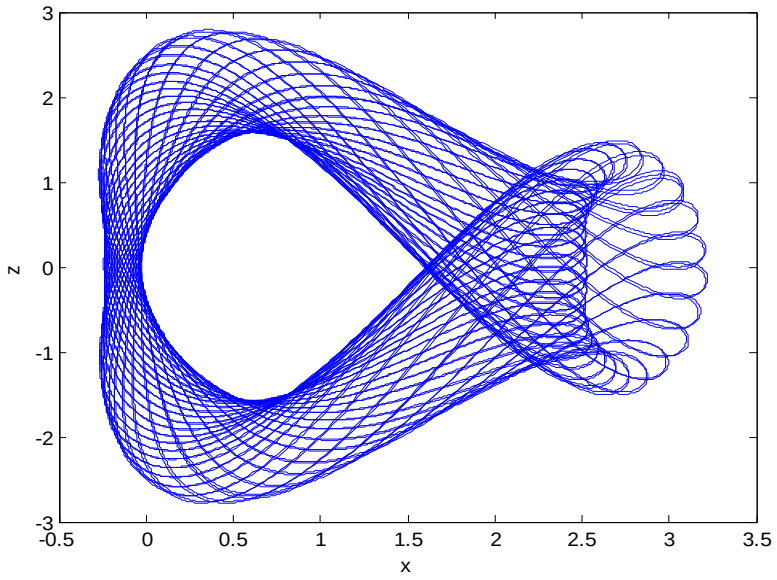
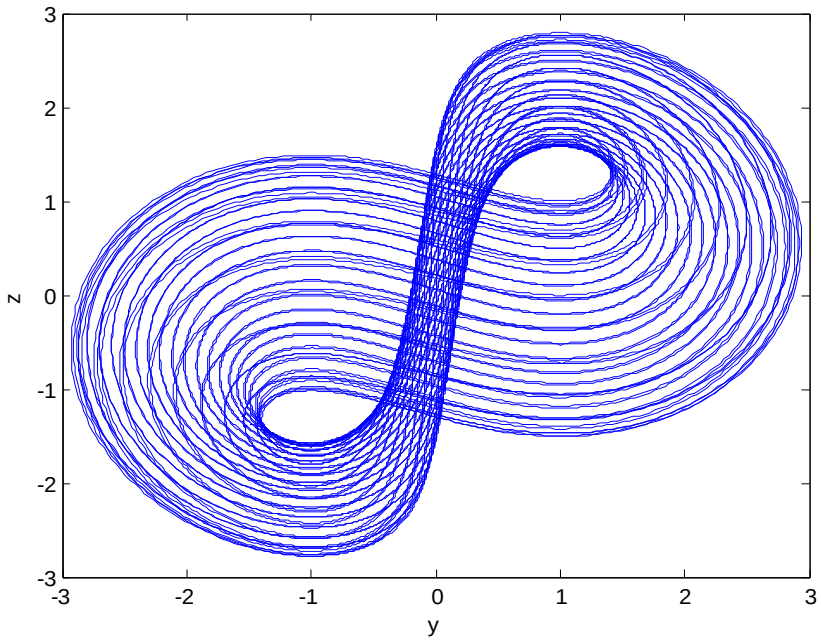


Figure III.6.*Plan de phase (x,z) de l'oscillateur de Sprott*

La figure (III.6) présente le comportement chaotique du système dans le plan X,Z.



***FigureIII.7: Plan** de phase (y,z) de l'oscillateur de Sprott.*

La figure (III.7) présente le comportement chaotique du système dans le plan Y.Z.

III.4.Simulation sous Matlab:

III.4.1.présentation de méthode de Runge-Kutta d'ordre 4:

Est techniques de Runge-Kutta sont des schémas numériques à un pas qui permettent de résoudre les équations différentielles ordinaires.

Elles font parties des méthodes les populaires de par leur facilité de mise en œuvre et leur précision. C'est Carle Runge et Martin Kutta ,qui au début du XXe siècle, ont inventé ces méthode.

Nous décrivons ici deux algorithmes assez utilisés: de Runge-Kutta d'ordre 4**:[33]**

$$\begin{cases} k1 = h.\ f\ (tn, yn\ ) \\ k2 = h.\ f\ (tn + h\ 2\ , yn + k1\ 2\ ) \\ k3 = h.\ f\ (tn + h\ 2, yn + k2\ 2\ ) \\ k4 = h.\ f\ (tn + h,\ yn + k3) \end{cases} \quad \textbf{(III.6)}$$

III.5.Résultats des simulations:

Cette simulation va permettre de comprendre le comportement dynamique de ce circuit Sprott Nous avons utilisé le programme Matlab pour simuler le comportement d'un circuit.

III.5.1.Signal chaotique du circuit de sprott:

Le système Sprott non linéaire a montré un comportement chaotique Les figures (III.8) et (III.9) sont un exemple du trajet chaotique de ce circuit.

III.5.2.Cryptage par chaos:

Après la simulation du système « Emetteur _ Récepteur » sous MATLAB, on visualise les signaux suivants**:[30]**

Le signal émis m (t).

Le signal chaotique x (t).

Le signal crypté s(t) = m(t) +x(t).

Le Principe de synchronisation

Considérons les deux systèmes suivants :

$\dot{x} = f1(x,u)$**(III.7)**

$\widehat{\dot{x}} = f2(\hat{x},u)$

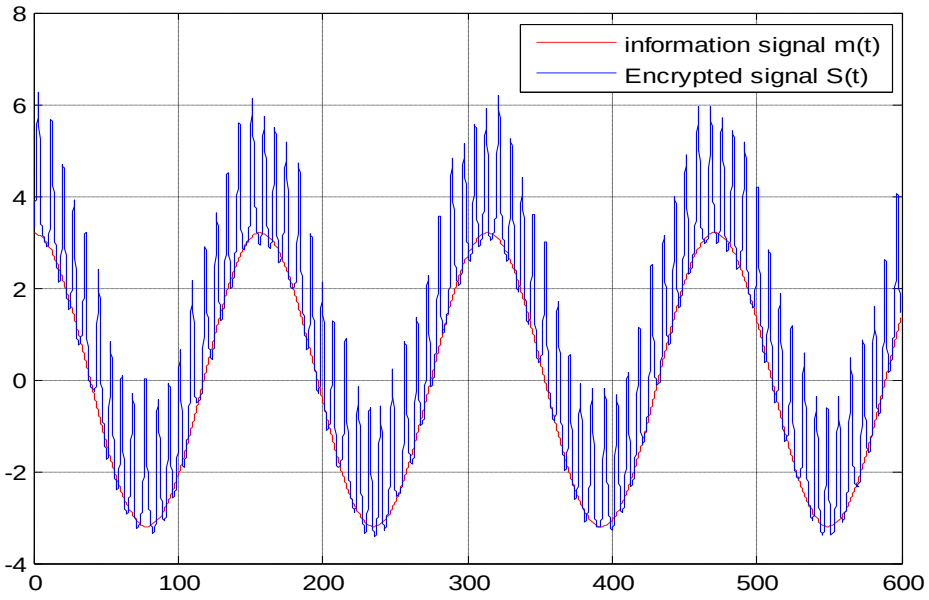
La récupération de l'information est généralement basée sur la synchronisation des états $x$del'émetteur et des états $\hat{x}$ du récepteur.

A cause de la sensibilité aux conditions initiales des signaux chaotiques, les deux oscillateurs de l'émetteur et du récepteur n'auront jamais leurs états identiques dans n'importe quelle valeur de temps.

Les deux systèmes sont dits synchronisés si l'erreur de synchronisation**:**[**30**]

$e = |\hat{x}(t) - x(t)| \rightarrow 0\ quandt \rightarrow \infty$ **(III.8)**

III.5.2.1.Démonstration de la technique utilisée:



FigureIII.8. *L'allure du signal original m(t) et le signal après cryptage s(t)*

La figure (III.10) montre clairement que le signal sinusoïdal est devenu un signal crypté, et il est très difficile de le déchiffrer sans connaitre la clé cryptage. Pour décoder correctement l'information initiale, il est nécessaire de connaitre les caractéristiques du signal chaotique. Le destinataire trouve des informations hors du fouillis de son message.

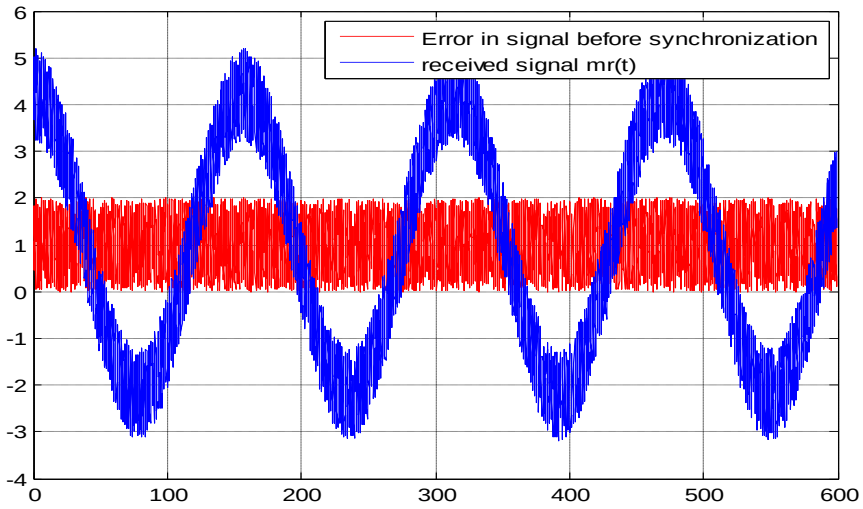


Figure III.9.*L'allure de signal récupère m(t)et l'errer de signal sans synchronisation*

Sur la figure (III.9), on remarque l'erreur de synchronisation entre les deux signaux chaotiques.

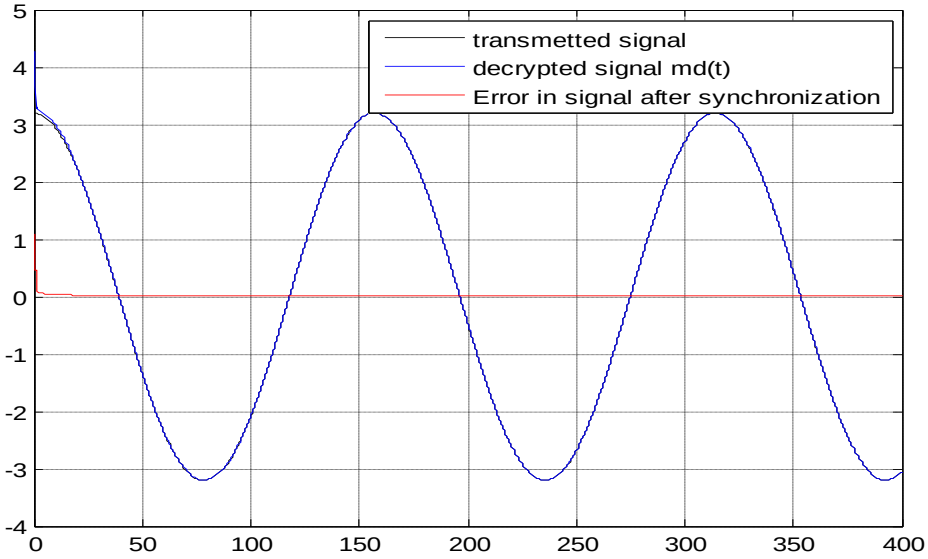
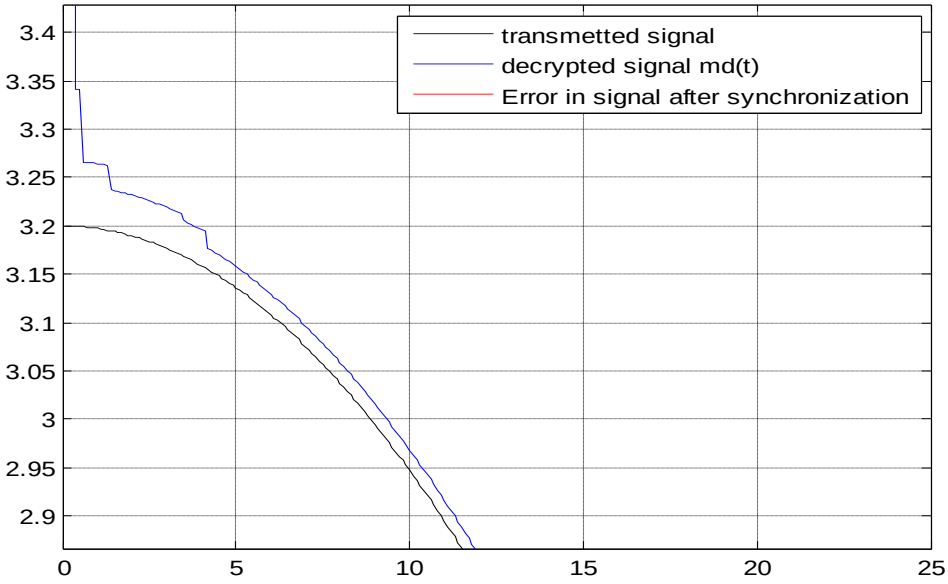


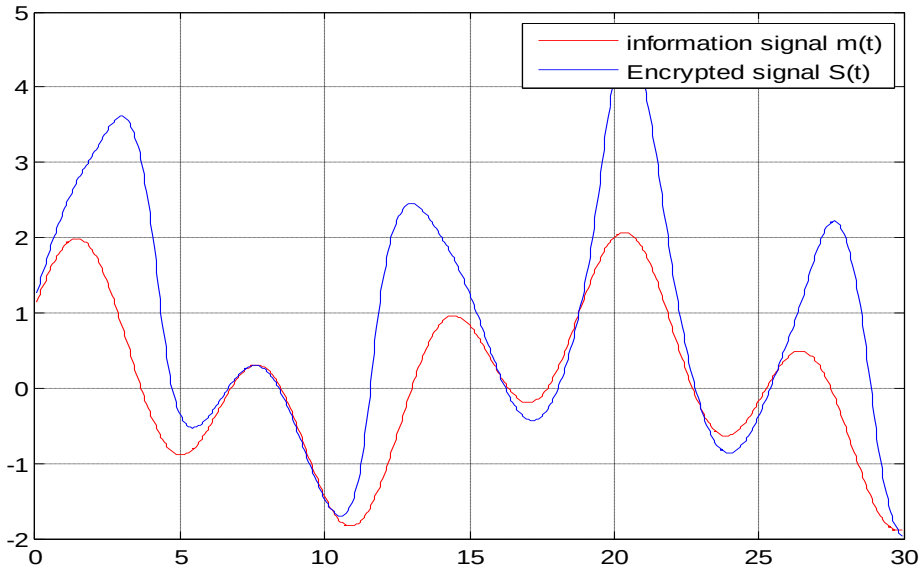
Figure III.10.L'allure de signal décrypter m(t) et l'error de signal après synchronisation

Sur la figure (III.10), nous voyons les erreurs de synchronisation lorsqu'elles approchent de 0.



FigureIII.11.*Le résultat de synchronisation*

Exemple 2 : pour avoir l'efficacité du système de synchronisation, on va simuler un autre exemple. Les résultats de simulation sont présentés dans les figures suivantes.



FigureIII.12*. l'allure du signal original m(t) et le signal après cryptage s(t)*

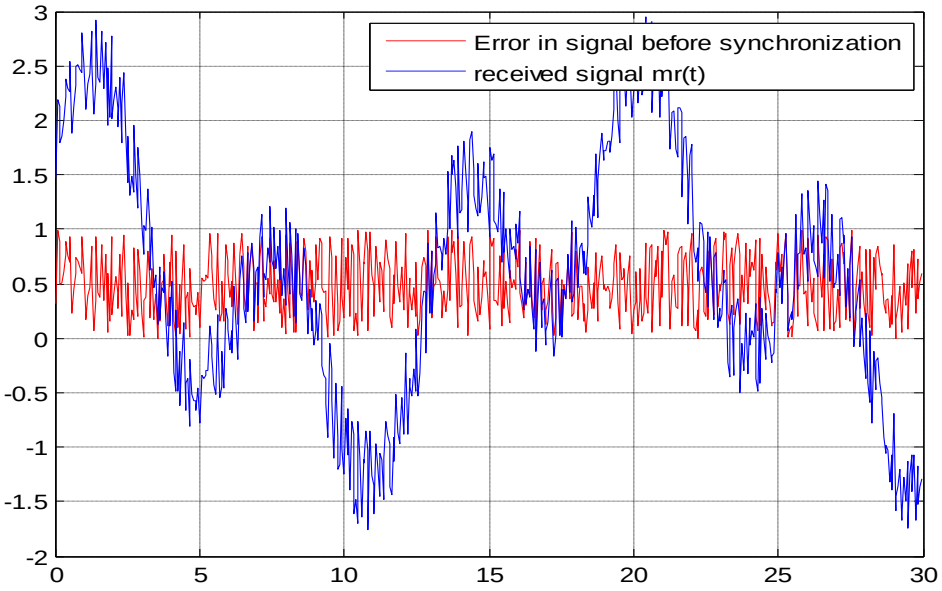


Figure III.13.*L'allure de signal récupère m(t)et l'errer de signal sans synchronisation*

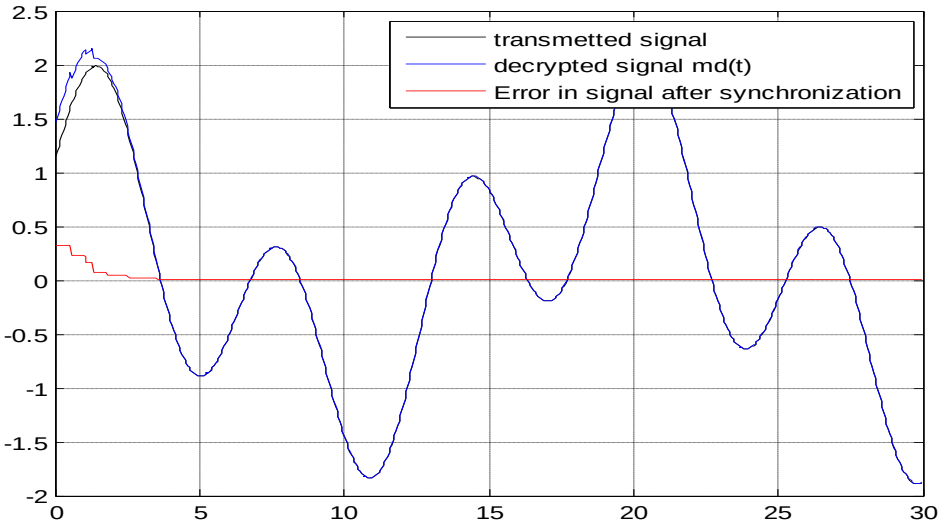


Figure III.14.*L'allure de signal décrypter m(t) et l'error de signal après synchronisation*

Une fois la synchronisation des états sont assurées, en observant les résultats obtenus, nous déduisons que le message est bien noyé dans le signal chaotique et que le message envoyé a été récupéré. Ce qui montre l'efficacité de la méthode de synchronisation.

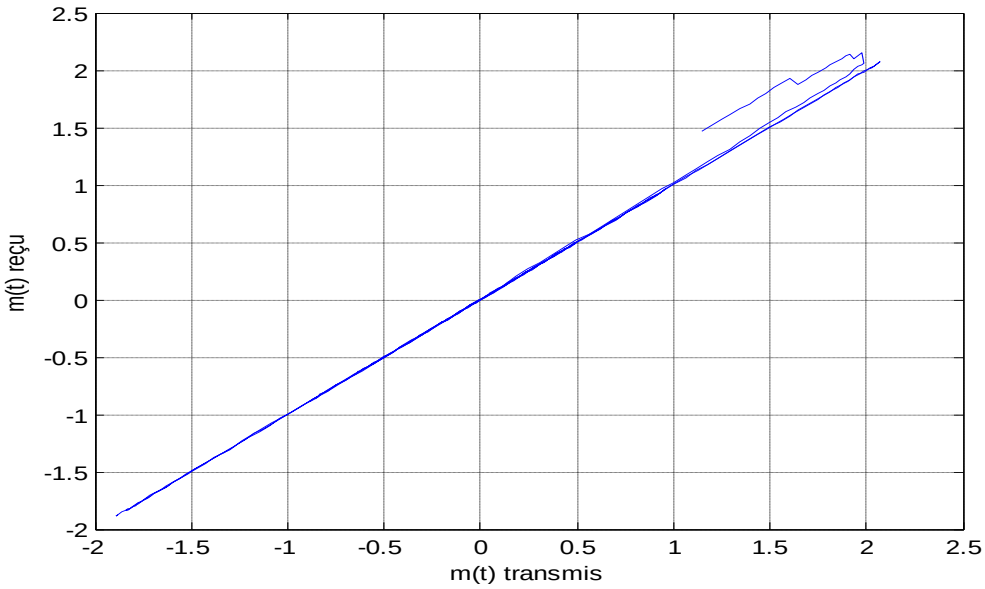


Figure III.15. *Synchronisation des deux circuits.*

Cette figure montre la synchronisation des deux circuits après un temps transitoire.

A Travers le résultat obtenu, nous pouvons confirmer que le message a été récupéré au niveau de l'appareil récepteur, ce qui prouve l'efficacité de la méthode de synchronisation.

III.6.Conclusion:

Dans ce chapitre, nous avons vu ce qu'est un circuit de Sprottet nous avons définis ces circuits dans cette étude, qui permettent la génération de signaux chaotique déterministes à large spectre. Ce signal permet de chiffrer des informations avec une clé déterministe et nous avons montré l'efficacité de la synchronisation. Nous avons étudié également la possibilité d'utiliser le chaos et son comportement pour chiffrer l'information pour une transmission sécurisée à travers ces différentes propriétés. Dans le cas d'un chiffrement chaotique, les paramètres de l'expéditeur et du dentinaire sont les mêmeset les paramètres système jouent le rôle de clés de chiffrement.

Les résultats obtenus one montré l'efficacité des signaux chaotique pour crypter l'information.

Conclusion générale

Conclusion générale

Un système chaotique est un système dynamique qui se développe dans une région finie avec un nombre infini de chemins denses et apériodiques. Il se caractérise par un comportement instable et non linéaire, défini par des équations mathématiques. Le comportement chaotique provient de la grande sensibilité du système dans son état initial. Les signaux chaotiques ont été largement utilisés dans divers domaines de recherche tels que la modulation du signal et le cryptage chaotique des données de communication.

Dans ce mémoire nous avons utilisé les caractéristiques des systèmes chaotiques pour faire l'étude de la synchronisation de deux générateurs de signaux chaotiques pour le chiffrement des transmissions de données.

Dans le premier chapitre de ce mémoire, nous avons présenté quelques généralités sur les systèmes chaotiques. , nous avons ainsi défini les systèmes chaotiques en donnant leurs propriétés les plus connues et les plus intéressantes pour notre système comme l'aspect aléatoire d'un signal chaotique, le déterminisme et la sensibilité aux conditions initiales.

Par la suite nous avons ainsi introduit quelques exemples des systèmes chaotiques, comme le système de Lorenz, de Rössler et de Hénon. Nous avons aussi présenté la bifurcation par la fonction logistique et les domaines d'application d'un système chaotique.

Dans le deuxième chapitre, nous avons introduit les types de cryptage et les concepts de base d'un schéma de cryptage. Nous avons expliqué le cryptage par le chaos et les différentes manières de masquer l'information utile à transmettre par un signal chaotique.

Dans la deuxième partie de ce chapitre, nous avons abordé la synchronisation chaotique, une étape essentielle dans un système de transmission à base du chaos. Nous avons aussi présenté les propriétés des systèmes chaotiques appliqués au cryptage d'une transmission des données.

Dans le dernier chapitre de ce mémoire l'oscillateur chaotique Sprott a été étudié. Nous avons testé par simulation sur Matlab un système de transmission sécurisé de données basé sur les systèmes chaotiques et la synchronisation.

Conclusion générale

Pour la synchronisation de deux systèmes (émetteur et récepteur), on injecte un signal généré par l'émetteur et l'envoyé au récepteur afin que ce dernier se synchronise avec l'émetteur.

Des résultats de simulation sont donnés pour illustrer l'efficacité de la méthode de synchronisation et a permis la récupération du message transmis.

Ce travail est un thème qui ouvre la recherche sur plusieurs axes. Les futurs travaux se concentreront sur l'avantage des oscillateurs chaotiques pour les problèmes de télécommunications, tels que le cryptage pour d'autres applications en télécommunication ainsi que l'application des algorithmes pour la synchronisation.

Bibliographies

Bibliographies

Bibliographie

[1] M.FOURAR SADDEK," commande synergétique est floue des systèmes non linéaire", Mémoire de fin d'études, université FRHAT ABBES, SETIF, ALGERIE, juin 2012.

[2] MegherbiOuerdia, "étude et réalisation d'un système sécurisé à base de système chaotique", Mémoire de magister, université Mouloud Mammeri, Tizi-Ouzou, Algerie, 2013.

[3] BENHABIB CHOUAIB, "étude d'un système chaotique pour la sécurisation descommunications optiques", Mémoire de fin d'étude, université ABDOU BEKER BELKAID, TLEMCEN, Algerie, juin 2014.

[4] M.-a. JAMEEL, The numerical solution of fractional differential chaotic system, Université de Mutah,2009.

[5] M.HAMICHE, Hamid, "Étude et réalisation d'un systéme chaotique basé sur le circuit de CHUA", mémoire de fin d'etude, université MOULOUD MAMMERI, TIZI- OUZOU , Algerie,2014.

[6] G. Kaddoum, "Contributions à l'amélioration des systèmes de communication multi utilisateurs par Chaos : synchronisation et analyse des performances", thèses de Doctorat de l'Université de Toulouse, 2008.

[7] G.Zaibi « Sécurisation par dynamiques des réseaux locaux sans fil au niveau de la couche MAC », thèse de Doctorat de l'université de Toulouse, 2012.

[8] E. Goncalvès « introduction au système dynamiques et Chaos ». Cours de l'institut National Polytechnique de Grenoble, 2004.

[9] M.AIT HAMMI, Abdelfateh, "Étude et réalisation d'un système chaotique basé sur le circuit de chua", Mémoire de fin d'étude, université MOULOUD MAMMERI, TIZI-OUZOU,Algerie, juin 2014

[10] A. R. KIHAL, Système chaotique pour la transmission sécurisée de donnée, Mémoire de magister, Université Mohammed Khider, Biskra, 2013.

[11] T.Hamzia, " Système dynamique et chaos 'application à l'optimisation à l'aide d'algorithme chaotique" , thèse de doctorat, université de Mentouri, Constantine, 2007.

[12] A. BERKANE, "transmission sécurisée à base de la synchronisation impulsive de deux système chaotique discrets", Mémoire de master Professional. Université Mouloud Mammri de Tizi-Ouzo.

[13] A. BOUKABOU, Méthodes de contrôle des systèmes chaotiques d'ordre élevé et leur application pour la synchronisation: Contribution à l'élaboration de nouvelles approches, Thèse doctorat, Université de Constantine, 2006.

[14] H.Benayache, "compression de l'information à l'aide de système chaotique", Mémoire de fin d'étude, université Mohamed Seddik Ben Yahia, Jijel, Algerie,2019.

[15] Ch.Bouchelaghem, "Nouveau schéma de communication sécurisé à base de chaos", Mémoire de master, université AbdElhafidBoussouf, Mila, Algerie, 2019.

[16] http://ram-0000.developpez.com/tutoriels/cryptographie/?page=page_2#L2.

[17] http://ram-0000-developpery.com/ tutowels / cryptographie 12 Page - page 2 L2. <viste le: 02/03/2022>.

[18] http://www.bart-Konieczny.com /fr/ blog / scounde-des- replication-web/ couplage symetique-et asymetrique. Visité le: <2/03/2022>.

[19] https://waytolearnx.com/2018/07/difference-entre-le-cryptage-symetrique-et-asymetrique.html

[20] Jonathan BlANC.Enseignant:Sandrine JULIA .Adrien DE GEORGES. Année universitaire 2003/2004.Licence Informatique. TECHNIQUES .DE.CRYPTOGRAPHIE

[21] Non répudiation- Wikipedia, https://fr. Wikepedia.org / Wiki/Non-repudiation /

[22] Brown, Ret Kocave, L (2000), A. unifying dention of Synchronization for dynamical Systems. Chao: An interdisciplinary Journal of Nonlinear Science, 10(2), 344-369.

[23] H. Kenouni, "Syncranisation des systèmes hyper - chaotiques à retard sous l'effet des perturbations; application au chiffrement d'information, Mémoire de fin d'études université de Jijel, Algérie. 2016.

[24] S. Kassim, "contribution à la transmission numérique sécurise de donner à base de générateur de séquences chaotique d'ordre man entier, Thèse de doctorat, Université Mouloud Menneri, Tizi- Ouzou, Alger, 2018.

[25] H-Hamich, "inverstion à gauche des systèmes dynamiques hybrides chacliques Applications à la transmission Sécurisée de données", Thèse de doctorat, universite Mouloud Menmeri, Tizi-Ouzou, Algerie, 2014.

[26] N.Mezar,S.Sebtu."etude d'un système de transmission de données robuste à base de la synchronisation impulsive chaotique", Mémoire de fin d'étude de Master, 24/09/2017.

[27] R. Tenny, "Symetric and Asymmetric secure communication Schemes" Thèse de doctorat university of california, Sandiaga, 2003.

[28] H. Nijmeijet and I.Mareels. « Synchronisation des systèmes Chaotiquespar observateurs et applications à la transmission d'informations », Thèse de Doctorat de l'Université de Paris Sud 11.2012.

[29] H. Nijmeijet and I. Mareels. «An observer looks at synchronization» IEEE Trans. On CircSyst.I: FundamentalThery and Applications, 44(10): 882-890, 1997.

[30] R.KHELIFI and S.BOUPRIMA. « COMMUNICATION SECURISEE

PAR SYNCHRONISATION CHAOTIQUE»,Thèse de Master de l'université de Abbes Laghrour-Khenchela2020.

[31] B.Nana, P.Woafo, S.Domngang: " Chaotic synchronization with experimental application to secure communications", J. Commun Nonlinear Sci. Numer

Simulate, Vol.14, pp2266-2276, 2009.

[32]M. DJENOURI and M. CHIKHI« communication sécurisée par chaos: Etude et mplementation sur carte FPGA», Thése de Master 2014

[33] (PDF) Méthodes d'Euler et de Runge-Kutta d'ordre 4 pour des...

341165012_Meth... ‹ publication ‹ www.researchgate.net