الجمهورية الجزائرية الديمقراطية الشعبية
République Algérienne démocratique et populaire

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

جامعة سعد دحلب البليدة
Université SAAD DAHLAB de BLIDA

كلية التكنولوجيا
Faculté de Technologie

قسم الإلكترونيك
Département d'Électronique

Mémoire de Master

Filière : Électronique

Spécialité : Electronique des systèmes Embarqué

Présenté par

Chabane Abdeldjalil

&

Fechit Abdelhak

Implémentation d'un système de transmission sécurisée des données à base de chaos sur carte Arduino

Proposé par : Mr. Ferdjouni Abdelaziz

Année universitaire 2020-2021

Remercîments

Je tiens à remercier tout d’abord Dieu tout puissant, qui ma donnée durant toutes ces années la santé, le courage et la fois en moi-même pour en arrive là.

Je remercier vivement mes parents pour leur soutien et conseil.

Je tiens surtout à exprimer ma gratitude à mon promoteur Mr.Ferdjouni Abdelaziz pour l’intéressante documentation qu’il a mis à ma disposition, et pour ses conseil précieux.

En particulier je tiens à remercier Mr.Lazhar Chikhi pour leur disponibilité et conseils avisé.

Mes remercîments s’adressent également aux membres de jury pour leur temp et l’attention qu’ils accordent au présent mémoire.

ملخص: تتميز الأنظمة الفوضوية بعدد من الخصائص بما في ذلك الحساسية للظروف الأولية وعدم القدرة على التنبؤ، مما يجعل الأنظمة الفوضوية مهمة للغاية في تشفير البيانات، وقد أتاح لنا العمل الذي قمنا به مكننا من الوصول لمجال صعب للغاية وهو الفوضى، لقد تمكنا من دراسته وانجزنا نظام نقل البيانات بشكل آمن عن طريق الفوضى. لقد قدمنا جميع النقاط الأساسية المتعلقة بهذه الأنظمة، مثل تعريفها وخصائصها، واستنتجنا أنه على الرغم من تعقيد هذه الأنظمة، إلا أن دراستها و توضيفها ليس بالأمر المستحيل.

كلمات المفتاحية: الفوضى، فوضوي، انتقال، التزامن، التشفير.

Résumé : Les systèmes chaotiques sont caractérisés par un certain nombre de propriétés dont la sensibilité aux conditions initiales et l'imprévisibilité, ce qui rend les systèmes chaotiques très intéressants dans le cryptage des données, le travail que nous avons réalisé, nous a permis de toucher à un domaine très difficile qui est le chaos, nous avons étudié et réalisé une transmission de données sécurisé par le chaos. Nous avons présenté tous les points essentiels concernant ces systèmes, tel que leur définition et leur caractéristique, on a conclu que malgré la complexité de ces systèmes, que son étude et sa réalisation n'est pas impossible

Mots clés : chaos, chaotique, Rössler, Hénon-Hieles, Hénon modifier, Transmission, Synchronisation, Cryptage.

Abstract: : Chaotic systems are characterized by a number of properties including sensitivity to initial conditions and unpredictability, which makes chaotic systems very interesting in data encryption, the work we have done has allowed us to touch a very difficult area which is chaos, we have studied and achieved a secure data transmission by chaos. We have presented all the essential points concerning these systems, such as their definition and their characteristic, it was concluded that despite the complexity of these systems, that its study and its realization is not impossible.

Keywords : chaos, chaotic, Rössler, Hénon-Hieles, modified Henon, Transmission, Synchronisation, Encryption

Listes des acronymes et abréviations

UART Universal Asynchronous Receiver Transmitter

ASCII American Standard Code for Information Interchange

Table des matières

Liste des figures

Liste des tableaux

Introduction générale

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

Au cours des dernière années, la synchronisation des systèmes chaotiques a attiré beaucoup d'attention en raison de ses larges applications dans divers domaines de nombreux types de synchronisation ont été proposés dans les systèmes chaotiques la plupart des travaux en synchronisation du chaos ont été soumis au système chaotique continue plutôt que le système discret.

Dans la pratique le système dynamique chaotique au temp discret joue un rôle plus important que leur parties continue.il est important de considérer la synchronisation des systèmes dynamique chaotique hyper-chaotique discret. Récemment de plus en plus d'attention ont été accordée à la synchronisation du chaos (hyper-chaotique) dans le système dynamique discret en raison de ses applications dans la télécommunication, la transmission sécurisée de l'information et la cryptographie.

Un système de communication numérique comporte toute les action visant à transmettre des donnée d'un émetteur a un récepteur à travers un support physique qu'on appelle canal de transmission avec le développement des systèmes de communication et l'arrivée des réseaux de communication moderne la sécurité de transmission est devenu une obligation et une précaution qu'il faudra prendre, en vue de réduire le risque des intrusion malveillante et de protéger les donnée contre l'interception la modification ou le vol et garantir la fiabilité la confidentialité, l'authenticité ainsi que l'intégrité des donnée transmise la cryptographie est une technique permettant d'assurer la sécurité de transmission des données.

L'idée d'utiliser le chaos dans le système de transmission est survenu lors des travaux de Pérora et Carroll en 1990 qui ont démontré que deux systèmes chaotique un maitre et un esclave peuvent synchroniser sous certaine condition. Cette synchronisation est utilisée pour pouvoir récupérer l'information, le cryptage chaotique s'effectue au niveau de l'émetteur par nombreuse technique permettant d'insérer le message crypter le résultat sera ensuite transférer à travers le biais d'un canal de transmission au récepteur. Ce dernier connait les caractéristiques de générateur du chaos, il va décrypter à son tour le signal reçu pour restituer le message.

- Le premier chapitre a été consacré à la présentation des généralités sur les systèmes chaotiques, les caractéristiques d'un système chaotique et à l'étude de système de Rössler en utilisant différents outils d'analyse.
- Le deuxième chapitre présente les différentes méthodes de synchronisation de deux systèmes chaotiques en s'intéressant beaucoup plus à la méthode choisie, synchronisation à l'aide d'un observateur, pour récupérer l'information émise.

- Le troisième chapitre porte sur un schéma de transmission de données à base de la synchronisation de deux systèmes chaotiques. En décrivant la chaine de transmission, puis le principe de la méthode suivie (choix de l'émetteur, du récepteur et mise au point du processus de transmission de l'information). Enfin, les résultats de simulation sont présentés sous le logiciel Matlab.
- Le quatrième chapitre est destiné à la réalisation d'un système de transmission sur 2 cartes Arduino Méga suivant le schéma de transmission adopté. Pour enfin effectuer des différents tests et illustre les résultats d'expérimentation.

1. Le chaos dans le Système dynamique de Rössler

I.1 Introduction

Durant des années, le chaos était considéré comme incontrôlable et même inutilisable, malgré la mise en équation de certains phénomènes et la démonstration du déterminisme dans des aspects d'apparence aléatoire.

L'étude de la stabilité en comparant les trajectoires suivies par un des deux corps à partir de deux positions initiales très proches, ou on a conclu que les trajectoires étaient presque identiques à court terme, mais à long terme il y'avait une nette différence, donc on ne peut jamais prédire complètement l'évolution d'un système chaotique, cette signification a été avancée en 1908 par Pierre Duhem [1].

La première visualisation de phénomène du chaos déterministe a été observée par coïncidence par Edward Lorenz en 1961, à la suite d'une série de calculs qui avaient pour but de prévoir des phénomènes météorologiques. Ce dernier se servait de son ordinateur (royal McBean lgp-300) pour calculer ses prévisions, en obtenant ses résultats finaux, il voulait les refaire une deuxième fois pour s'assurer, pour gagner du temps il a pris en compte que trois chiffres après la virgule aux lieux de six en croyant qu'il aurait une petite variation dans les résultats, mais il a été stupéfait par ces résultats qui était totalement différents des premiers A partir de là, on a découvert le comportement chaotique d'un système non linéaire, une métaphore a contribué à l'essor de la théorie de Lorenz : « le simple battement d'aile du papillon au Brésil pourrait déclencher une tornade au Texas »[2].

I.2 Définition du chaos

La théorie du chaos étudie le comportement des systèmes dynamiques très sensibles aux conditions initiales, un phénomène généralement illustré par l'effet papillon. Pour de tels systèmes, des différences infimes dans les conditions initiales entraînent des résultats totalement différents, rendant en général toute prédiction impossible à long terme. Cela concerne même les systèmes purement déterministes (ceux dont le comportement futur est entièrement déterminé par les conditions initiales, sans aucune intervention du hasard) : leur nature déterministe ne les rend pas prévisibles car on ne peut pas connaître les conditions initiales avec une précision infinie. Ce comportement paradoxal est connu sous le nom de chaos déterministe, ou tout simplement de chaos [1].

Le comportement chaotique est à la base de nombreux systèmes naturels, tels que la météo ou le climat. Ce comportement peut être étudié grâce à l'analyse par des modèles mathématiques chaotiques, ou par des techniques analytiques de récurrence et des applications de Poincaré. La théorie du chaos a des applications en météorologie, sociologie, physique, informatique, ingénierie, économie, biologie et philosophie [2].

I.3 Les Système chaotique

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

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

Dans ce qui suit, prenons l'exemple du système de Rössler quelque propriété de systèmes chaotique seront présenté.

I.4 Système de Rössler

Un système de trois équations différentielles non linéaires. Ces équations différentielles définissent un système dynamique continu et tridimensionnel qui présente des caractéristiques chaotiques. L'ensemble des trajectoires à long terme de ce système définissent un attracteur étrange aux propriétés fractales [3].

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \quad (1.1)$$

Ce système est minimal pour un chaos continu pour au moins trois raisons :

1) Son espace de phase a la dimension minimale trois.
2) La non-linéarité est minimale car il y a un seul terme quadratique, et il génère un attracteur chaotique avec une seule orbite, contrairement à l'attracteur de Lorrenz qui a deux lobes.
3) (x, y, z) Sont les trois variables qui évoluent dans le temps continu t et (a, b, c) sont trois paramètres.
4) Les termes linéaires des deux premières équations créent des oscillations dans les variables x et y. Ces oscillations peuvent être amplifiées si $a > 0$, ce qui se traduit par un mouvement en spirale. Le mouvement en x et y est alors couplé à la variable z régie par la troisième équation, qui contient le terme non linéaire et qui induit la réinjection à le début du mouvement en spirale.

   Ce système présente des attracteurs stationnaires, périodiques, quasi-périodiques et chaotiques en fonction de la valeur des paramètres (a, b, c).

L'étude du système de Rössler se fait pour des valeur $a = 0.2, b = 0.2, c = 5.7$

I.4.1 Point d'équilibre

Le système possède deux points d'équilibre :

1) Le premier autour de l'origine $x = y = z = 0$, dans laquelle le mouvement tourne en spirale.
2) Le deuxième à une certaine distance de l'origine en raison de la non-linéarité quadratique.

$$\begin{cases} \dot{x} = 0 \rightarrow -y = z \\ \dot{y} = 0 \rightarrow x = -ay \\ \dot{z} = ay^2 + cy + b = 0 \end{cases}$$

$$\begin{cases} x = -\dfrac{c \pm \sqrt{(c^2 - 4ab)}}{2} \\ y = -\dfrac{c \pm \sqrt{(c^2 - 4ab)}}{2a} \\ z = \dfrac{c \pm \sqrt{(c^2 - 4ab)}}{2a} \end{cases} \tag{1.2}$$

Donc on a deux points d'équilibre :

$$\begin{pmatrix} e_1\left(\dfrac{c + \sqrt{(c^2 - 4ab)}}{2}; -\dfrac{c - \sqrt{(c^2 - 4ab}}{2a}; \dfrac{c + \sqrt{(c^2 - 4ab}}{2a}\right) \\ e_2\left(\dfrac{c - \sqrt{(c^2 - 4ab)}}{2}; -\dfrac{c + \sqrt{(c^2 - 4ab}}{2a}; \dfrac{c - \sqrt{(c^2 - 4ab}}{2a}\right) \end{pmatrix} \tag{1.3}$$

$$e_1\{5.69, -28.46, 28.46\}$$

$$e_2\{0.007, -0.35, 0.35\}$$

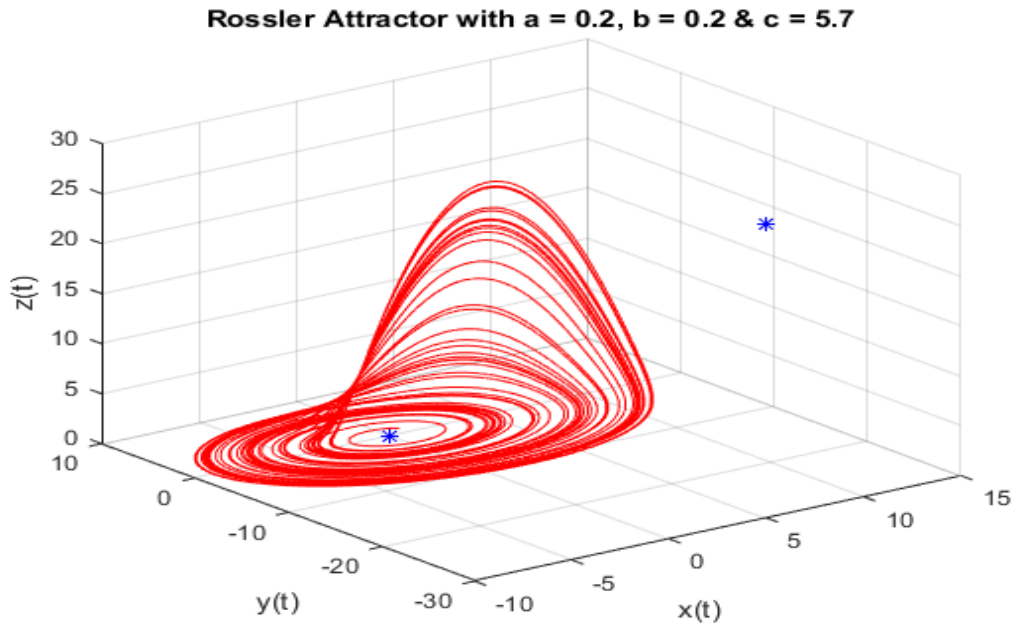


Figure 1-1-1:Attracteur de Rössler pour a=0.2, b=0.2, c=5.7

La nature des points d'équilibre dépend des 3 paramètre (a, b, c) et

Le nombre de solutions dépendra donc du signe du déterminant $D = (c/a)^2 - 4b/a$.

$$Cr = 2 * \sqrt{ab}$$

Tableau 1.1-1:point d'équilibre en fonction des paramètres de système

a<0					
b<0					
c<-Cr<0	C=-Cr	c>Cr	0<c<Cr	c=Cr	c>Cr
Zi=$0.5(-1+(-1)^i\left[\frac{c^2-Cr^2}{a^2}\right]^{\frac{1}{2}})$	Zi=-0.5	Critique	Critique	Zi=-0.5	Zi=$0.5(-1+(-1)^i\left[\frac{c^2-Cr^2}{a^2}\right]^{\frac{1}{2}})$
Y=-zi	Y=0.5			Y=0.5	Y=-Zi
X=a zi	X=$-a/2$			X=$-a/2$	X=a Zi
2 points	1 point			1 point	2 points

a=0		a>0			
b≠0	b=0	b=0			b>0
c≠0		c<0	c=0	c>0	Pour tout c
Z=b/c	Z=0	Z=0 et z=c/a	Z=0	Z=0 et z=c/a	Zi=$0.5(-1+(-1)^i\left[\frac{c^2+Cr^2}{a^2}\right]^{\frac{1}{2}})$
Y=$-b/c$	Y=0	Y=0 et Y=-c/a	Y=0	Y=0 et y=-c/a	Y=-Zi
X=0	X=0	X=0 et x=-c	X=0	X=0 et x=-c	X=a Zi
1 point	1 point	2 points	1 point	2 points	2 points i=1,2

I.4.2 L'aspect aléatoire

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

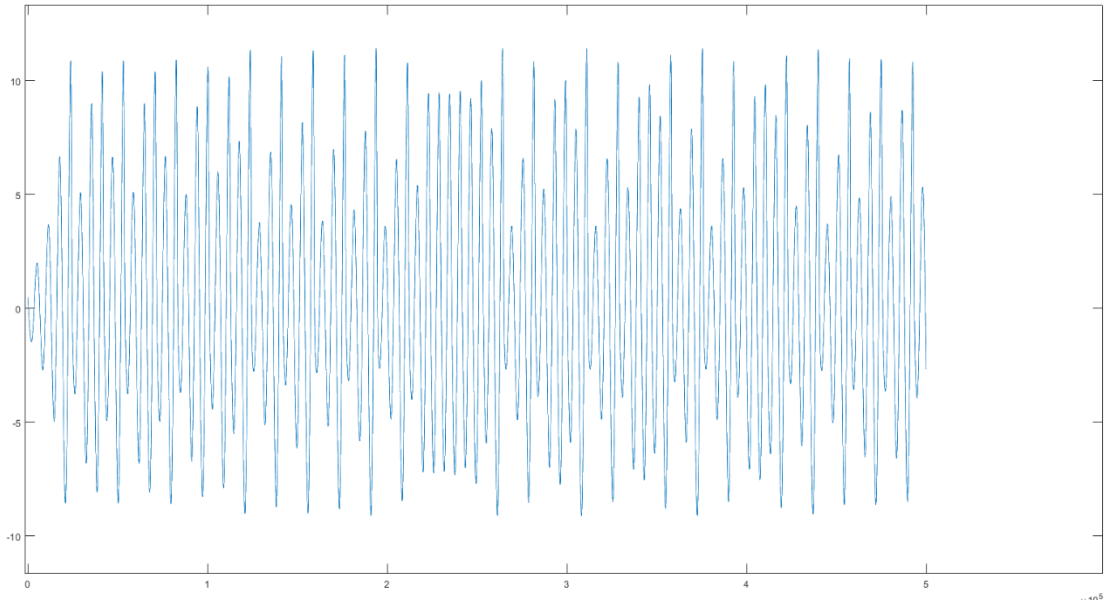


Figure 1-2: l'état $x(t)$

I.4.3 Stabilité des points d'équilibre

Méthode indirecte de Lyapunov

Lyapunov et autres ont remarqué par l'étude des trajectoires des courbes intégrales au voisinage de l'équilibre que, dans la majorité des cas, les point d'équilibres des systèmes non linéaires. Donc l'étude d'un système linéaire est aisée puisqu'elle se résout dans un critère purement algébrique. Dans ce fait, la méthode la plus classique pour la détermination de la stabilité non linéaire du point d'équilibre se réduit à la linéarisation du système en ce point [4].

Linéarisation des équations de système

La linéarité du système au points $(\dot{x}, \dot{y}, \dot{z})$ s'appelle la matrice jacobienne de $f(x, y, z)$

Soit x^* le point d'équilibre (ainsi $f_1(x^*) = f_2(x^*) = f_3(x^*) = 0$)

De (1.3) :

$$jac = \begin{bmatrix} \frac{df_1(x^*)}{dx} & \frac{df_1(x^*)}{dy} & \frac{df_1(x^*)}{dz} \\ \frac{df_2(x^*)}{dx} & \frac{df_2(x^*)}{dy} & \frac{df_2(x^*)}{dz} \\ \frac{df_3(x^*)}{dx} & \frac{df_3(x^*)}{dy} & \frac{df_3(x^*)}{dz} \end{bmatrix} = \begin{pmatrix} 0 & -1 & -1 \\ 1 & a & 0 \\ z & 0 & x-c \end{pmatrix} \quad (1.4)$$

La méthode indirecte de lyapunov, pour étudier la stabilité autour d'un point d'équilibre x^*, consiste à étudier les valeur propre λ_i,ou $i = 1, \ldots\ldots, n$ sont des constantes déterminer par les Conditions initiales.

Théorème :

- *Si toutes les valeurs propre λ_i ont leur partie réelle négative le point fixe est asymptotiquement stable.*
- *Si une ou plusieurs valeurs propres sont des imaginaires pures, les autres valeurs ayant leur partie réelle négative, le point fixe est un point centre ou un point elliptique (stable mais pas asymptotiquement stable).*
- *Si une des valeurs propres à sa partie réelle positive le point fixe est instable*

Etude de la stabilité pour le système de Rössler

L'étude revient à étudier le signe des valeurs propres de la jacobienne de ce système au niveau des points d'équilibre.

$$|\lambda I - jac| = \begin{bmatrix} \lambda & -1 & -1 \\ 1 & \lambda - a & 0 \\ z & 0 & \lambda - x + c \end{bmatrix} \quad (1.5)$$

Après calcul du déterminant de la jacobienne, on obtient un polynôme du troisième degré.

- Pour $e_1(5.69, -28.46,\ 28.46)$

$$det_{|\lambda I - Jac|} = \lambda^3 - 0.19\lambda^2 - 27.462\lambda + 0.01$$

$$\begin{cases} \lambda_1 = 0.0971028 + 0.995786i \\ \lambda_2 = 0.0971028 - 0.995786i \\ \lambda_3 = -5.68718 \end{cases}$$

➢ Le point d'équilibre est instable

- Pour $e_1(0.007, -0.35,\ 0.35)$

$$det_{|\lambda I - Jac|} = \lambda^3 + 5.493\lambda^2 - 0.488\lambda + 7.685$$

$$\begin{cases} \lambda_1 = -0.0000046 + 5.4280259i \\ \lambda_2 = -0.0000046 - 5.4280259i \\ \lambda_3 = 0.192983 \end{cases}$$

➢ Le point d'équilibre n'est pas stable

I.4.4 Bifurcation

La théorie de bifurcation est l'étude mathématique des changements qualitatifs ou topologiques de la structure d'un système dynamique. Une bifurcation survient lorsqu'une variation quantitative d'un paramètre du système engendre un changement qualitatif des propriétés d'un système telles que la stabilité, le nombre de points d'équilibre ou la nature des régimes permanents. Les valeurs des paramètres au moment du changement sont appelées valeurs de bifurcation. Dans les systèmes dynamiques, un diagramme de bifurcation montre les comportements possibles d'un système, à long terme, en fonction des paramètres de bifurcation [5][6].

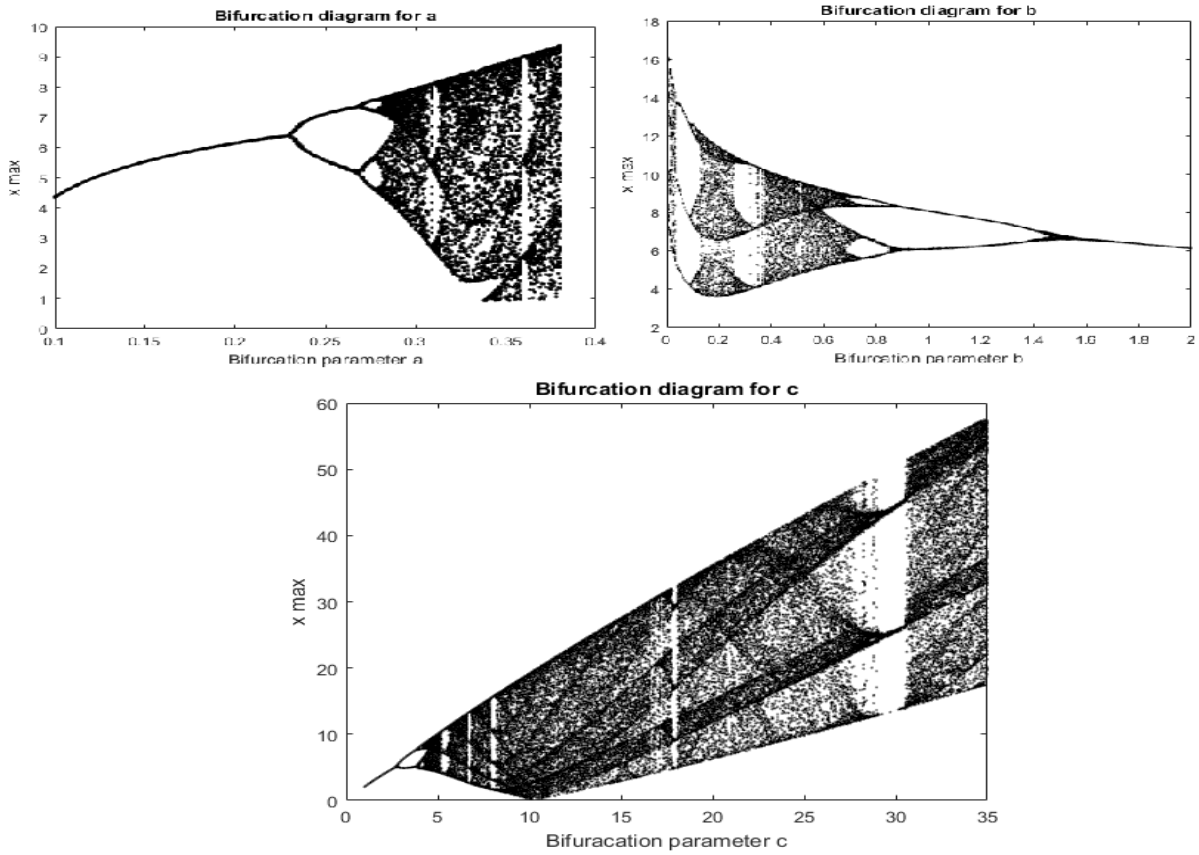


Figure 1-3: Diagrammes de bifurcation pour les 3 paramètres

Dans les équations de Rössler par exemple, la résolution du système n'apporte pas toujours le chaos. Ce régime n'apparaît que pour certaines valeurs des paramètres. Pour caractériser le chaos. Il peut être intéressant d'étudier l'apparition du chaos (ce qu'on appelle le scénario ou la route vers le chaos). On distingue trois scénarios théoriques d'évolution vers le chaos. Toutes ces évolutions ont permis de classer certains phénomènes expérimentaux comme chaotiques déterministes.

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

Le doublement de période *:* L'augmentation d'un paramètre provoque, pour un système périodique, l'apparition d'un doublement de période, la période se multiplie ainsi en 4, 8, 16, … A partir d'une certaine valeur du paramètre, Les doublements étant de plus en plus

rapprochés, on tend vers un point auquel on obtiendrait hypothétiquement une fréquence infinie et c'est à ce moment que le chaos apparait.

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

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

I.4.5 Sensibilité aux conditions initiales

Certains phénomènes dynamiques non linéaires sont si sensibles aux conditions initiales que, même s'ils sont régis par des lois rigoureuses et parfaitement déterministes, les prédictions exactes sont impossibles. Comme la plupart des phénomènes sont non linéaires, on comprend alors l'importance de la découverte de Lorrenz [7]. Une autre propriété des phénomènes chaotiques est qu'ils sont très sensibles aux perturbations. L'un des premiers chercheurs à s'en être aperçu fut Edward Lorenz qui s'intéressait à la météorologie et par conséquent aux mouvements turbulents d'un fluide comme l'atmosphère. Lorenz venait de découvrir que dans des systèmes non linéaires, d'infimes différences dans les conditions initiales engendraient à la longue des trajectoires totalement différentes. Il a illustré ce fait par **l'effet papillon**. Le battement d'ailes d'un papillon aujourd'hui à Pékin engendrerait une tempête le mois prochain à new York [7]. Il est clair que la moindre erreur ou imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction sur l'évolution à long terme du système. Une des propriétés essentielles du chaos est donc bien cette sensibilité aux conditions initiales que l'on peut caractériser en mesurant des taux de divergence des trajectoires. Ceci est illustré par la figure

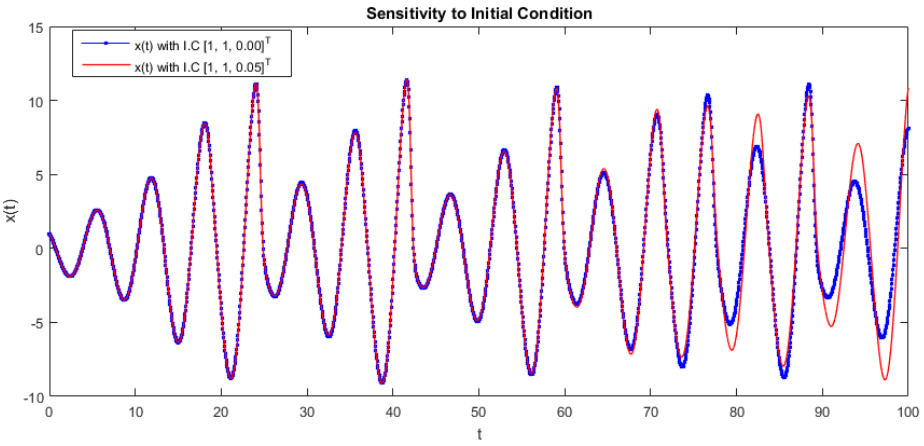


Figure 1-4:illustration de la propriété de sensibilité aux condition initiale sur l'état x(t)

I.4.6 Section de Poincaré

La technique dite des sections de Poincaré facilite l'étude des systèmes dynamiques considères en ramenant l'analyse d'un système différentiel (temps continu) à celle d'une application (temps discret). Par le biais de cette méthode, la dimension *d* du problème initial sous forme de système différentiel est réduite d'une unité avec l'application en dimension *d* – 1[4].

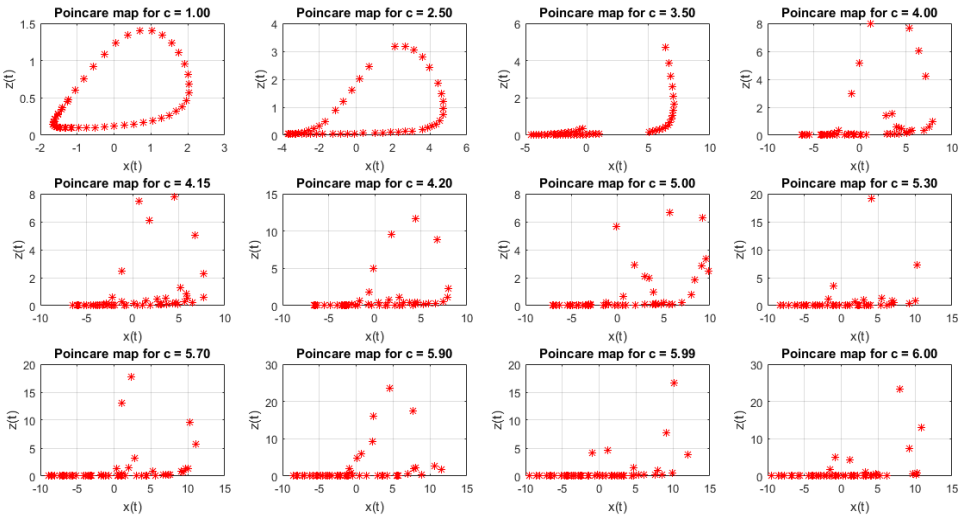


Figure 1-5: Plan de Poincaré pour différent valeur de c

I.5 Systèmes chaotique discrets

Dans la pratique, les systèmes chaotiques discrets (SCD) jouent un rôle plus important que leurs parties continues. En fait, de nombreux modèles mathématiques des processus physiques, des phénomènes biologiques, des réactions chimiques et des systèmes économiques étaient définis en utilisant des systèmes chaotiques discrets. Certains systèmes chaotiques et hyper-chaotiques discrets intéressants ont été présentés dans les deux dernières décennies.

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

$$\{x_{n+1} = G\big(x(k), u(k)\big) y(k) = h\big(x(k), u(k)\big) \tag{1.8}$$

Ou G :$\mathbb{R}^n \to \mathbb{R}^n \times \mathbb{Z}^+ \to \mathbb{R}^n$ désigne la dynamique du système en temps discret.

Parmi les systèmes chaotiques discret nous pouvons citer les systèmes suivants :

I.5.1 Système de Henon

Système de Henon [4], est un dynamique discret de 2 dimensions dont la représentation d'état est le suivant :

$$\begin{cases} x_1(k+1) = a - x_1^2(k) + bx_2(k) \\ x_2(k+1) = x_1(k) \end{cases} \tag{1.9}$$

Pour les valeurs a=1.4 et b=0.3, cet attracteur présente un comportement chaotique comme l'illustre la figure

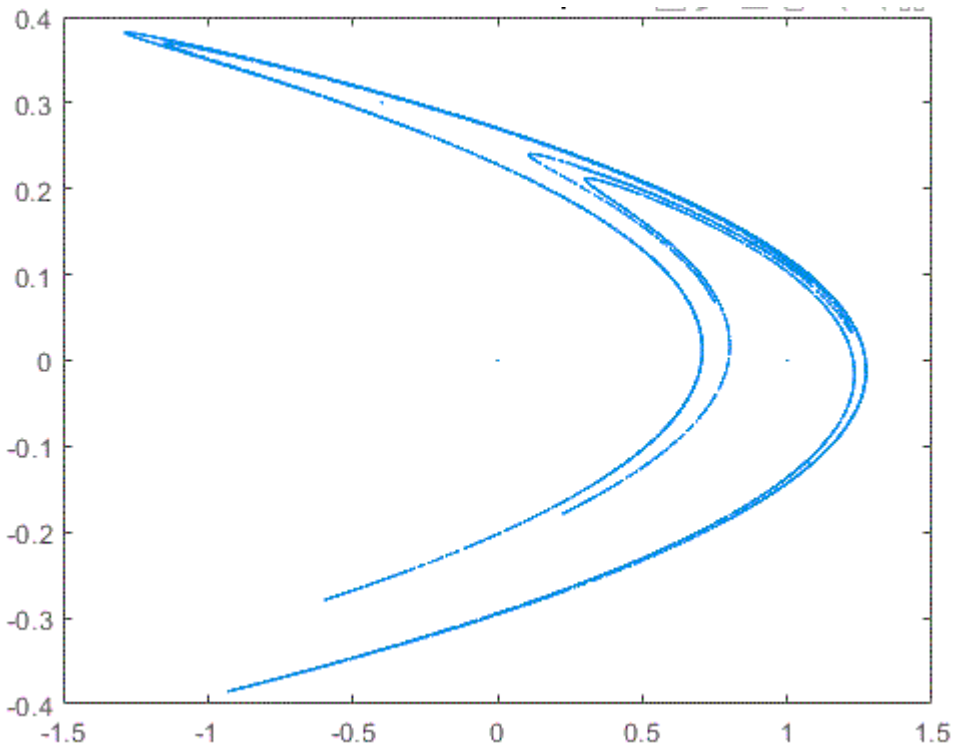


Figure 1-6:Attracteur de Hénon

I.5.2 Oscillateur de Lozi

René Lozi [], propose l'application suivante :

$$\begin{cases} x_1(k+1) = -a|x_1(k)| + x_2(k) + 1 \\ x_2(k+1) = bx_1(k) \end{cases} \tag{1.10}$$

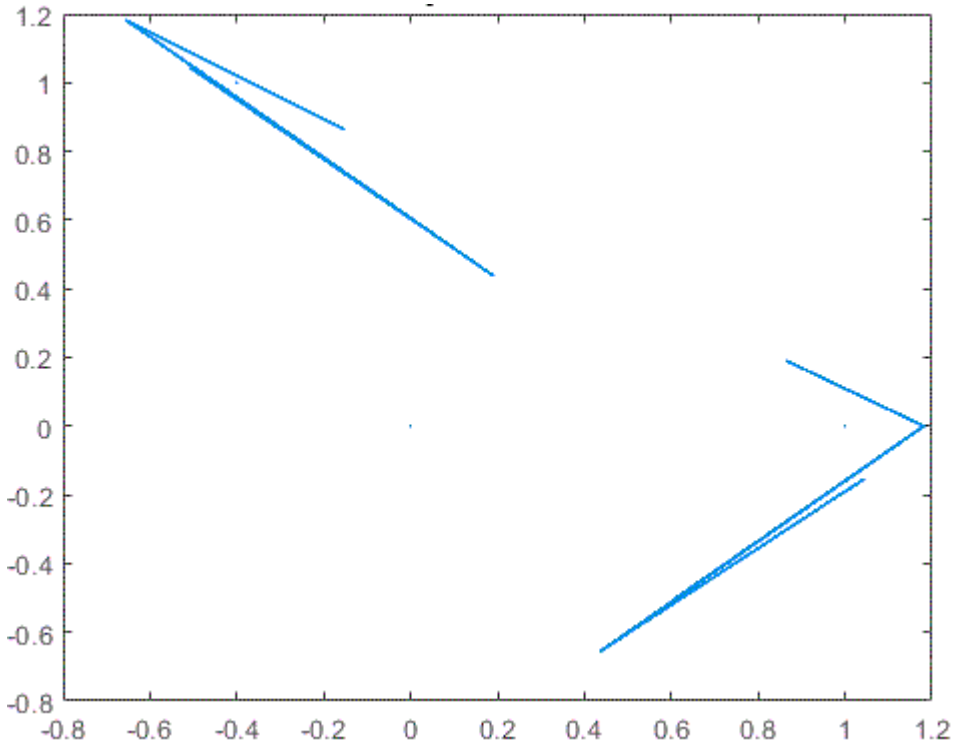


Figure 1-7:Attracteur de Lozi

I.5.3 Système de Rössler discret dans l'espace

Le système discret de Rössler discret tels que $a = 3.8, \beta = 0.05, \gamma = 3.35, \delta = 3.78, \varsigma = 0.2, \eta = 0.1$ et $\theta = 1.9$, est représenter par :

$$\begin{cases} x_1(k+1) = ax_1(k)\big(1 - x_1(k)\big) - \beta\big(x_3(k) + \gamma\big)\big(1 - 2x_2(k)\big) \\ x_2(k+1) = \delta x_2(k)\big(1 - x_2(k)\big) + \varsigma x_3(k) \\ x_3(k+1) = \eta\big(1 - \theta x_1(k)\big)\big[\big(x_3(k) + \gamma\big)\big(1 - 2x_2(k)\big) - 1\big] \end{cases} \quad (1.11)$$

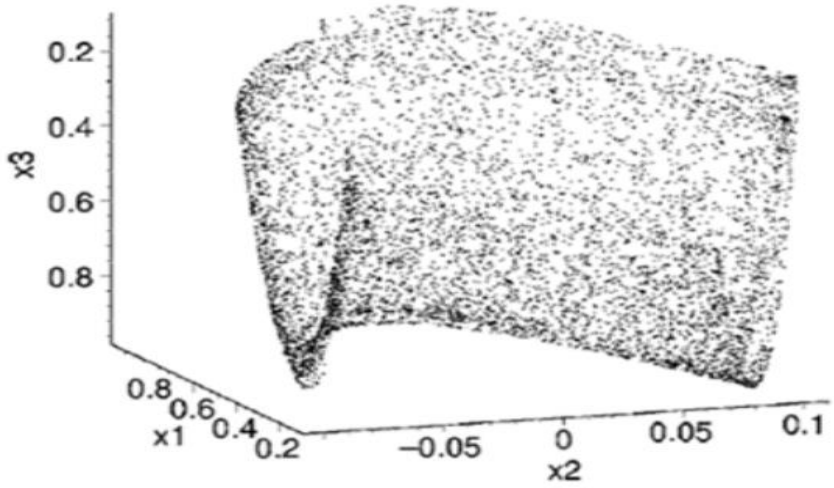


Figure 1-8: L'attracteur hyper-chaotique du système discret de Rössler

I.6 Conclusion

Ce chapitre, comporte quelques définitions qui présente les systèmes chaotiques. Ensuite Le système de Rössler a été pris comme un modèle d'étude, cette étude a fait ressortir les notions et les propriétés de ce système. Ainsi que ses caractéristiques ont été déduit.

Enfin de ce chapitre les systèmes chaotiques discrets ont été abordée. Ces systèmes seront exploités dans le chapitre qui vont suivre ou nous allons abordée la synchronisation et le cryptage des systèmes chaotique.

II. Synchronisation des systèmes chaotique

II.1 Introduction

La synchronisation est une caractéristique omniprésente dans beaucoup de systèmes naturels et dans les sciences non linéaires, signifie avoir le même comportement au même moment.

La synchronisation de deux systèmes dynamiques signifie donc généralement que l'un des systèmes copie le mouvement de l'autre. Lorsque le comportement de plusieurs systèmes se synchronisent, ces systèmes sont dits synchrones. On sait que beaucoup d'oscillateurs couplés, grâce à de faibles interactions, font apparaître un phénomène de synchronisation.

II.2 Synchronisation des systèmes chaotique

À première vue, la synchronisation de systèmes chaotiques peut paraître surprenante, car intuitivement, la sensibilité aux conditions initiales devrait empêcher toute synchronisation. En effet, il est difficile d'imaginer que deux systèmes chaotiques puissent produire le même signal chaotique, à moins qu'ils ne soient initialisés exactement au même point, ce qui est physiquement généralement impossible.

Cependant, aujourd'hui, la synchronisation des oscillateurs chaotiques couplés est un phénomène bien établi expérimentalement et raisonnablement bien compris théoriquement, et durant les trois dernières décennies, de nombreuses études sur la synchronisation se sont tournées vers les systèmes chaotiques.

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

II.2.1 Les types de synchronisation

Il existe deux types de synchronisation suivant la manière avec laquelle les deux systèmes chaotiques sont couplés ; on distingue la synchronisation :

a) 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

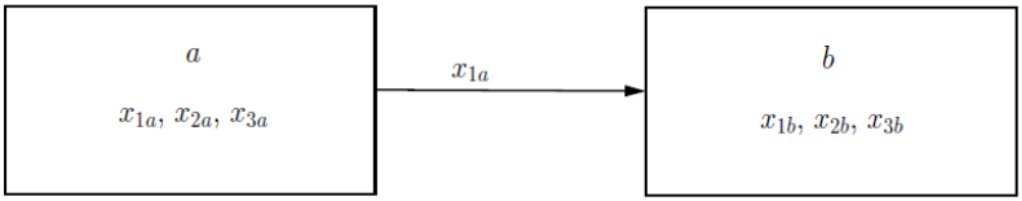


Figure II-1:Synchronisation unidirectionnelle

b) 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 dans les deux sens, par exemple l'utilisation d'une simple résistance.

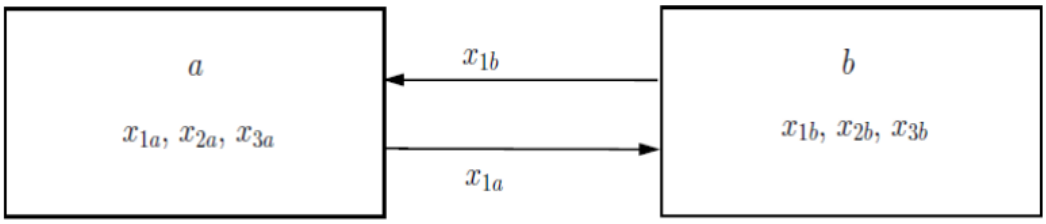


Figure II-2:Synchronisation bidirectionnelle

II.3 Méthode de synchronisation

Il existe plusieurs types de synchronisation :

II.3.1 Synchronisation par boucle fermée

Le principe de cette méthode consiste à injecter l'erreur d'estimation dans le récepteur en contre réaction pour corriger l'évolution du récepteur et afin de réaliser la synchronisation, cette méthode peut être applique pour les systèmes non identiques [8].

Soient les deux systèmes suivants :

Emetteur :

$$\begin{cases} \dot{x} = f(x) \\ \dot{y} = h(x) \end{cases} \tag{2.1}$$

Récepteur :

$$\begin{cases} \dot{x} = f(\hat{x}) + g(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \tag{2.2}$$

Avec g fonction de l'erreur entre y et $\hat{y}$, g est choisie de telle sorte à garantir la synchronisation.

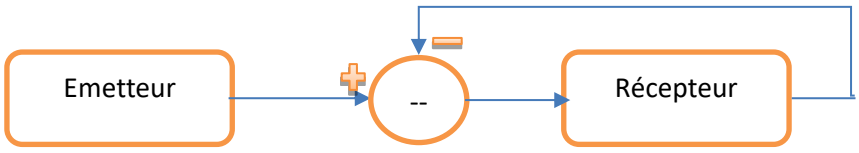


Figure II-3:Principe de synchronisation en boucle fermée

L'utilisation de la synchronisation en boucle ouvert provoque une sensibilité aux variations des paramètre, afin d'éviter cet inconvénient, la synchronisation par boucle fermée a été proposée.

II.3.2 Synchronisation par décomposition de systèmes

Certains systèmes chaotiques peuvent se décomposer en deux sous-systèmes, l'un maitre et l'autre esclave, ces derniers peuvent se synchroniser en les couplant avec un signal commun [1], l'avantage de cette méthode réside dans le fait que celle-ci présente une solution simple et performante, le but de cette méthode est qu'après un régime transitoire, le système esclave doit reproduire l'état du maitre.

Considérons le système chaotique suivant :

$$\begin{cases} \dot{x} = f(x) \\ y = h(x) \end{cases} \tag{2.3}$$

Ou $x = [x_1, \dots \dots, x_n]^T$ est le vecteur d'état.

On divisera le système initial en deux sous systèmes (S_1, S_2) :

$$\begin{cases} S_1 = \dot{X}_1 = \dot{F_1}(x_1, x_2) \\ S_2 = \dot{X}_2 = F_2(x_1, x_2) \end{cases} \tag{2.4}$$

Ensuite nous allons concevoir un nouveau sous système S'_2 qui présente une même dynamique que S'_2 et dont l'entrée est x_1

$$S'_2 = \hat{\dot{x}}_2 = F_2(x_1, \hat{x}_2) \tag{2.5}$$

Le sous système S'_2 est un candidat qui peut se synchroniser avec la dynamique avec la dynamique complète initiale, une synchronisation parfaite peut s'accomplir si ce dernier est stable, ce qui veut dire que l'ensemble des coefficients de Lyapunov du sous-système S'_2 sont négatifs.

On appellera le système (S_1, S_2) maitre et le sous-système (S'_2)esclave.

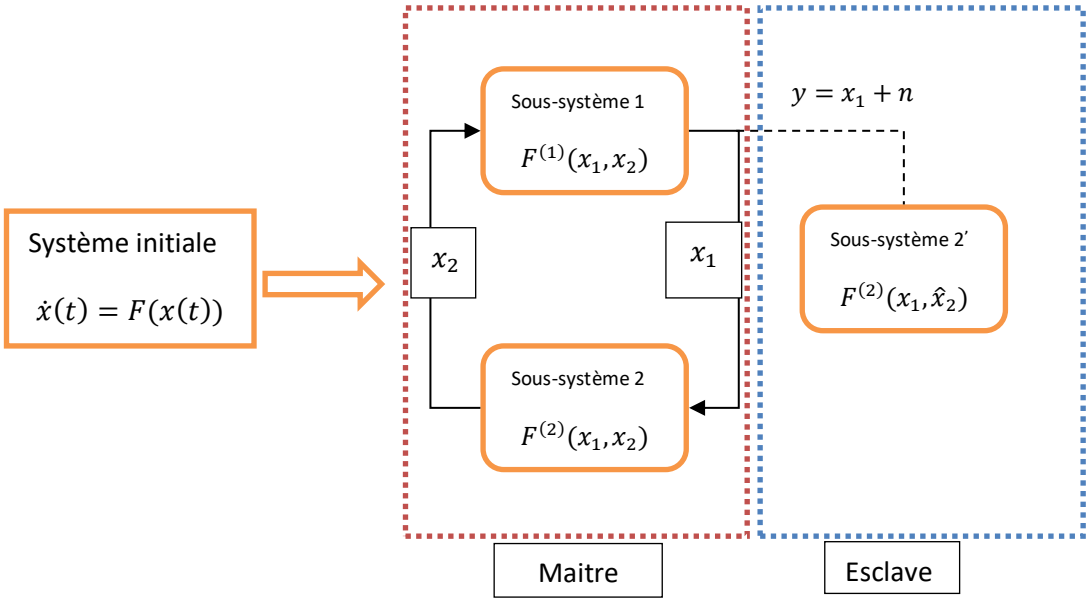


Figure II-4:Principe de la synchronisation identique

II.3.3 Synchronisation à l'aide d'observateur

La connaissance des entrées, des sorties et du modèle d'un système dynamique permet la reconstruction d'un ou plusieurs états du système qui ne peuvent être mesurés directement, soit à cause de leur inaccessibilité ou par économie [8].

La synchronisation par observateur consiste à construire un système esclave qui soit un observateur du système maitre, et qui va permettre d'avoir une évolution identique.

Dans le cas non linéaire, le problème de la conception d'un observateur est défini comme suit :

$$\begin{cases} S_1 = \dot{x} = f(x) \\ S_2 = \dot{\hat{x}} = \hat{f}(\hat{x}) \end{cases} \tag{2.6}$$

Si les systèmes S_1 et S_2 sont synchronisé on aura :

$$\lim_{t \to \infty} |x(t) - \hat{x}(t)| = 0 \tag{2.7}$$

Tels que :

$x(t)$: Etat du système.

$\hat{x}(t)$: Etat estimé.

Le principe de la synchronisation par observateur a illustré pas la figure suivante :

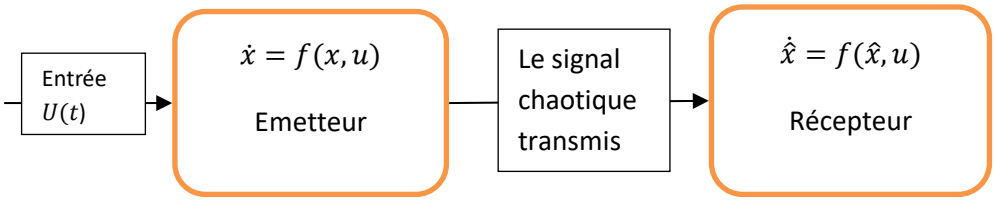


Figure II-5:Principe de la synchronisation à l'aide d'observateur

L'étude d'observabilité :

Soit un système :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + Du(t) \\ x(t_0) = x_0 \end{cases} \tag{2.8}$$

Ou $x \in \mathbb{R}^n, y \in \mathbb{R}^m, A, B, C\ et\ D$ des matrices de dimension appropriées.

Le système est dit complétement observable s'il existe un temps fini $t_1 > t_0$, tel que la connaissance de l'entrée $u(t)$ et de la sortie $y(t)$ pour $t \in [t_0, t_1]$ permet de reconstruire l'état $x(t)$.

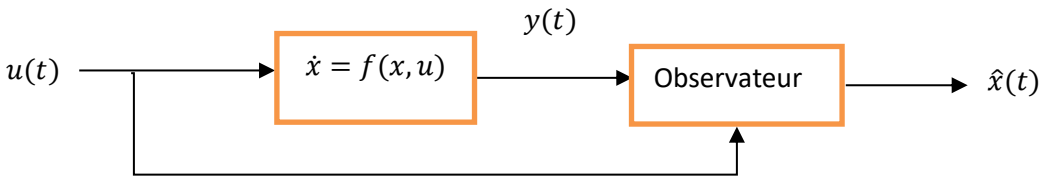


Figure II-6:synthèse d'observateur

Observabilité des système non linéaires :

Cas continue :

Soit le système non linéaire suivant [9] :

$$\begin{cases} \dot{x}(t) = f(x) + g(x)u(t) \\ y(t) = h(x) \end{cases} \tag{2.9}$$

La dérivée de lie est utilisée pour définir l'observabilité d'un système non linéaire, elle est définie comme suit :

$$Lfh(x) = \sum_{i=1}^{n} \frac{\partial h(x)}{\partial x_i} f_i(x) = \frac{\partial h(x)}{\partial x_1} f_1(x) + \frac{\partial h(x)}{\partial x_2} f_2(x) + \cdots \frac{\partial h(x)}{\partial x_n} f_n(x) \tag{2.10}$$

Avec : $$f(x) = \begin{vmatrix} f_1(x) \\ f_2(x) \\ . \\ . \\ . \\ f_n(x) \end{vmatrix}$$

Le système doit satisfaire la condition du rang d'observabilité $rang(M) = n$ avec :

$$M = [dh; dL_f h; \dots\dots, dL^{n-1}{}_f h]$$

$$rang(M) = rang \begin{vmatrix} dh \\ dL_f h \\ . \\ . \\ . \\ dL_f^{n-1} h \end{vmatrix} \quad (2.11)$$

Ou n est la dimension du système.

Cas discret :

Soit le système non linéaire a temp discret suivant :

$$\begin{cases} x_{k+1} = f(x_k, u_k) \\ y_k = h(x_k) \end{cases} \quad (2.12)$$

Ou $x_k \in \mathbb{R}^n, y_k \in \mathbb{R}^p, u_k = (u_k, \dots\dots, u_{mk})^T \in \mathbb{R}^m$.

Comme pour le cas continu, l'observabilité des systèmes en temps discret se vérifie par le rang d'observabilité.

$$\dim\big(doh(x_0)\big) = n$$

Ceci peut être reformulé comme suit :

$$rang[span\{dh, d(foh), \dots., d(f^{n-1}oh)\}] = n$$

Avec n dimension du système.

Observateur de Luenberger [10] :

Soit le système suivant :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y = Cx(t) \end{cases} \quad (2.13)$$

Et on a l'observateur dynamique de cette forme :

$$\begin{cases} \dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + L\big(y(t) - \hat{y}(t)\big) \\ \hat{y} = C\hat{x}(t) \end{cases} \quad (2.14)$$

L'évolution de l'état est corrigée grâce au modèle en fonction de l'écart entre la sortie mesurée et la sortie reconstruite par l'observateur $(y(t) - \hat{y}(t))$.

$$\begin{cases} \dot{\hat{x}} = A\hat{x} + Bu(t) + L\big(y(t) - C\hat{x}(t)\big) \\ \dot{\hat{x}}(t) = (A - LC)\hat{x}(t) + Bu(t) + Ly(t) \end{cases} \tag{2.15}$$

L'état x en fonction de la commande u et des mesures y est reconstruit par l'observateur, et la matrice de gain L est choisie de manière à ce que l'erreur converge exponentiellement vers 0.

$$\lim_{t\to\infty} e(t) = \lim_{t\to\infty}\big(x(t) - \hat{x}(t)\big) = 0 \tag{2.16}$$

Pour que le système soit stable, et en utilisant la technique de placement de pôles, on choisit le gain L de l'observateur de telle sorte que les valeurs propres de la matrice$(A - LC)$ soient dans le demi-plan complexe gauche (à partie réel négative), de ce fait on choisit une dynamique d'erreur plus rapide que celle de processus.

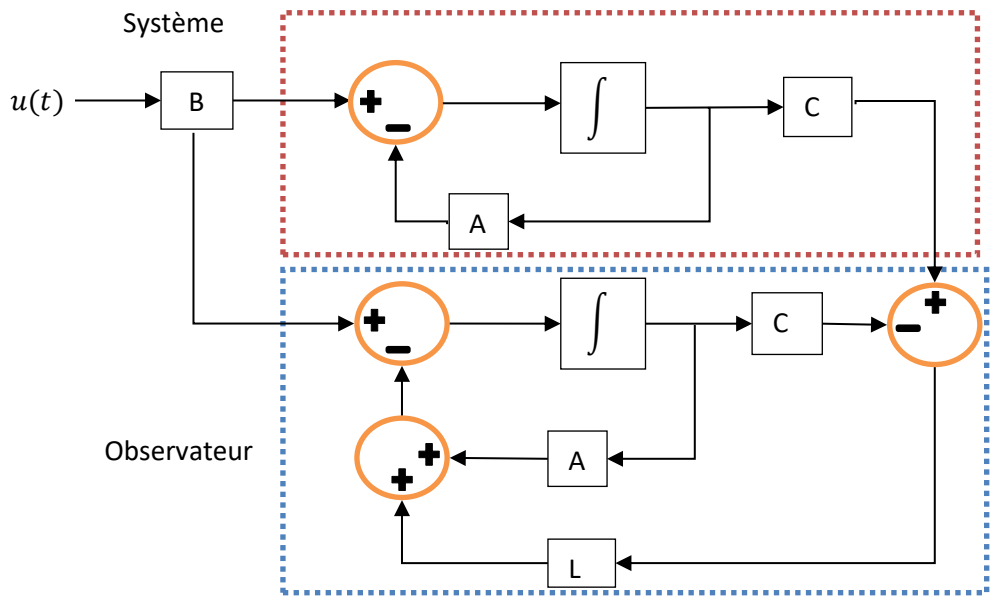


Figure II-7: Schéma de l'observateur de Luenberger

Observateur a modes glissants [11] :

Un observateur a modes glissants est un observateur dont le terme correcteur est une fonction sgn, Il s'agit de contraindre, a l'aide des fonctions discontinues, les dynamiques du système a convergé sur une « surface de glissement ».

Soit le système :

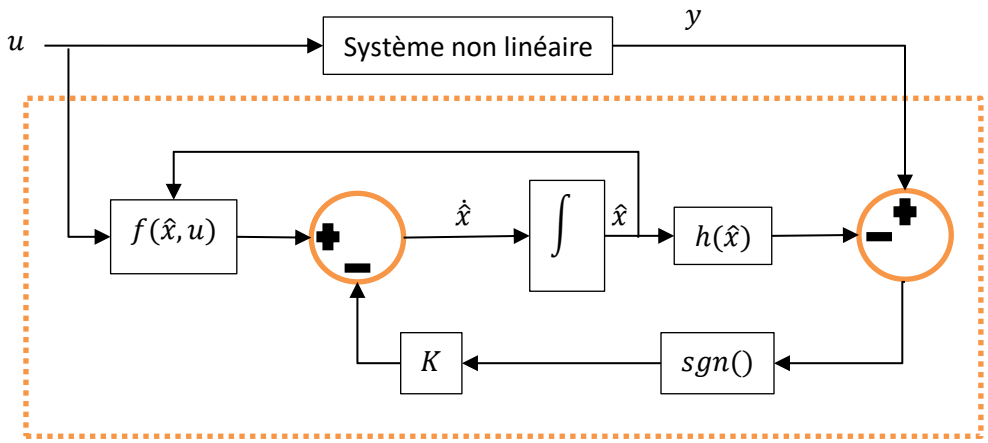
$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases} \tag{2.17}$$

L'observateur a modes glissants pour ce système s'écrit de la façon suivante :

$$\begin{cases} \dot{\hat{x}} = f(\hat{x}) + g(\hat{x})u + Ksgn(y - \hat{y}) \\ \hat{y} = h(\hat{x}) \end{cases} \quad (2.18)$$

Ou K est une matrice de gain de dimension $n * p$ dans ce cas, on impose l'évolution des dynamiques du système sur une variété s, sur laquelle l'erreur d'estimation de la sortie $e = (y - \hat{y})$ est nulle ainsi cette erreur converge vers 0 au bout d'un temps fini, et la dynamique du système se réduit de n a $n - p$.

La figure (**2.8**) illustre le principe d'observateur on mode glissant



Observateur en mode glissant

Figure II-8:Schéma d'observateur en mode glissant

Observateur impulsif :

Considérons le système suivant :

$$\begin{cases} \dot{x}_1(t) = f_1(x_1, x_2, t) \\ \dot{x}_2(t) = f_2(x_1, x_2, t) \\ y(t_k) = x_1(t_k) \end{cases} \quad (2.19)$$

Ou $x_1 \in \mathbb{R}^n, et\ x_2 \in \mathbb{R}^{n-p}$ sont les états du système,$y(t_k) \in \mathbb{R}^n$ est le vecteur de sortie.

Le principe consiste à contraindre l'observateur à suivre l'évolution du système original a des instant (t_k), un état du système est transmis sous forme d'impulsion pour réduire les redondances du signal, l'observateur prend la forme mathématique suivante [11] :

$$\begin{cases} \dot{\hat{x}}_1(t) = f_1(\hat{x}_1, \hat{x}_2, t) \\ \dot{\hat{x}}_2(t) = f_2(\hat{x}_1, \hat{x}_2, t) \\ \hat{x}_1(t_k) = x_1(t_k) \end{cases} \quad (2.20)$$

Le système d'erreur d'observation est donné comme suit :

$$\begin{cases} \dot{e}_1(t) = f_1(x_1, x_2, t) - f_1(\hat{x}_1, \hat{x}_2, t) \\ \dot{e}_1(t) = f_2(x_1, x_2, t) - f_2(\hat{x}_1, \hat{x}_2, t) \\ e_1(t_k) = 0 \end{cases} \quad (2.21)$$

Avec t_k instant ou l'impulsion est appliqué.

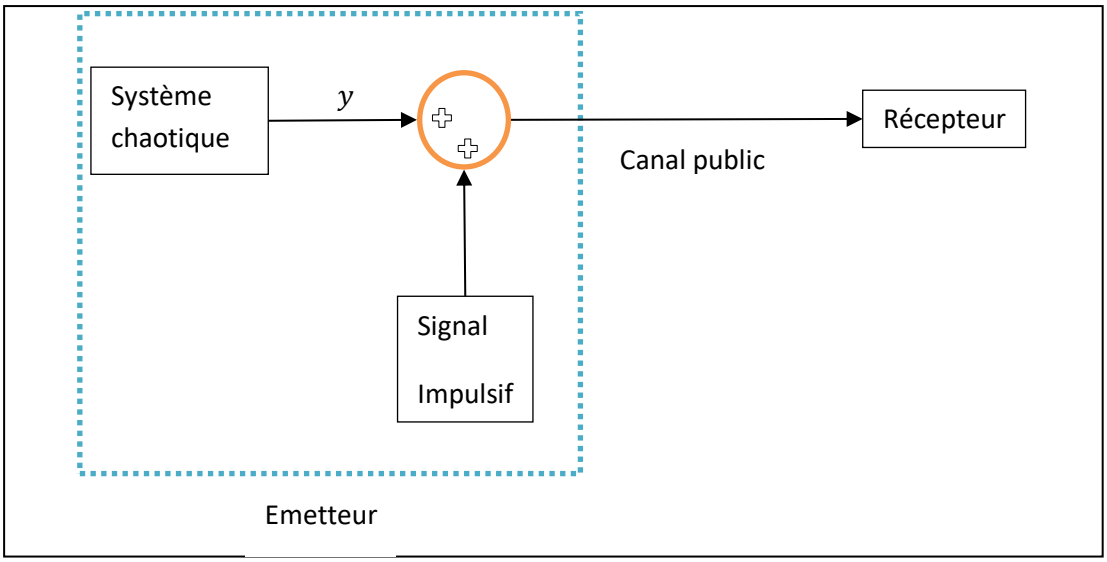


Figure II-9:Synchronisation impulsif

II.4 Transmission sécurisée par le chaos

Dans cette section, on s'intéresse aux techniques de transmission sécurisée d'information qui reposent sur le principe de synchronisation chaotique. La majorité des techniques de cryptage chaotique utilisent la configuration maitre-esclave pour laquelle on dispose d'un émetteur (système maitre) qui génère le signal du texte chiffré transmis vers un système récepteur (système esclave) qui a pour l'objectif de synchroniser avec le système maitre et de restaurer le signal d'information. Parmi la méthode de transmission chaotique on peut citer :

II.4.1 Cryptage par addition (masquage chaotique)

Dans cette technique [14], l'émetteur est un système chaotique $x(t)$ dont le signal de sortie $y(t)$ est ajouté au signal du message. La somme de deux signaux est transmise au récepteur. Le récepteur est constitué d'un système chaotique identique à l'émetteur. Ainsi, après la synchronisation des deux systèmes chaotiques le message est extrait à l'aide d'une opération de soustraction. La figure (2-10) illustre le principe de base de cette technique :

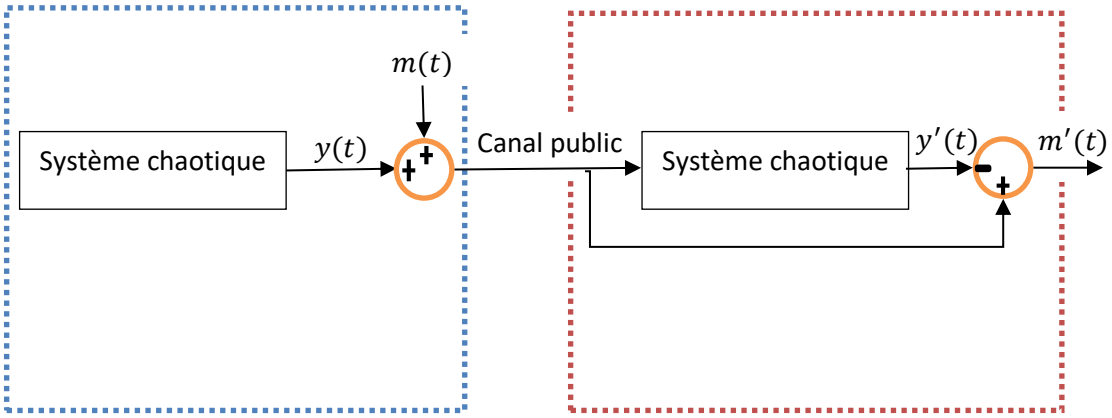


Figure II-10:Schéma de la méthode de cryptage par addition

Cette technique peut être appliqué pour la transmission de messages continue ou discrets.

Afin de garantir le secret et pour un cryptage efficace, il faut que l'amplitude du signal $m(t)$ soit inferieur a celle du signal porteur chaotique [14].

II.4.2 Cryptage par commutation

Dans cette méthode [15], l'émetteur est composé de deux systèmes chaotiques et le message $M(t)$ (de type binaire : 0 ou 1) est utilisé pour commuter entre $A(t)$ encodant le bit 1 et $B(t)$ encodant le bit 0. Le signal résultant est transmis travers le canal de transmission vers le système récepteur constitué de deux systèmes chaotiques esclaves identique à ceux de l'émetteur le premier système esclave synchronise exclusivement avec le premier oscillateur (correspondant au signal chaotique $A(t)$ de telle façon que le bit 1 est détecté par la convergence de l'erreur de synchronisation vers zéro et par conséquent le signal d'information peut être enfin restauré à la fin de processus de détection. Le schéma représentant par la figure (2.11).

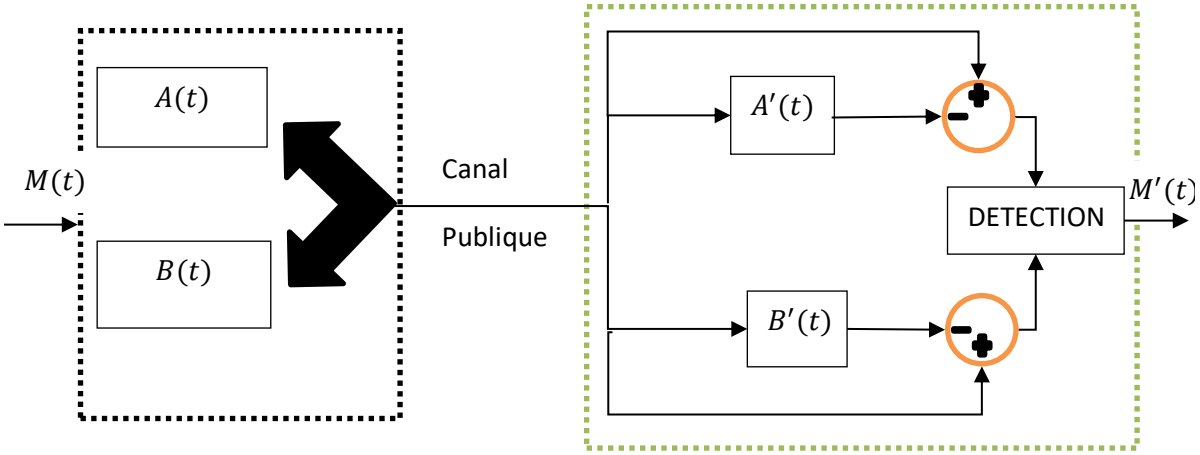


Figure II-11:Schéma de la méthode de cryptage par commutation.

II.4.3 Cryptage par modulation

Le principe de la modulation paramétrique [15], consiste à utiliser le message $M(t)$ pour moduler l'un des paramètres du système chaotique émetteur $X(t)$. Le système récepteur $Z(t)$ synchrone d'une manière adaptive avec l'émetteur chaotique et le message $M(t)$ est restauré par l'intermédiaire d'une loi d'adaptation. La figure (2.12) représente le schéma d'un système de communication utilisant cette technique.

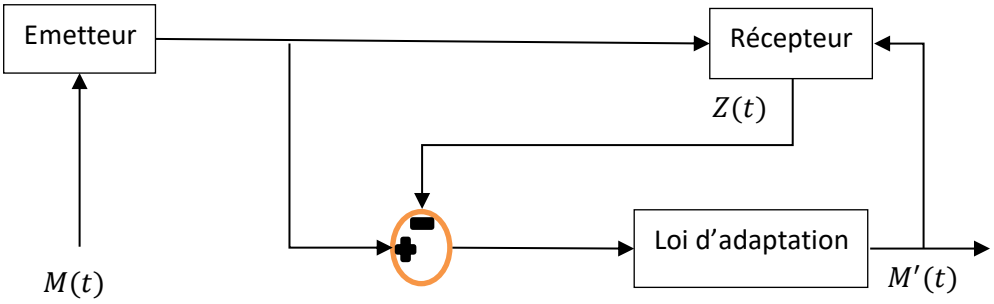


Figure II-12:schéma de la méthode de cryptage par modulation

II.4.4 Cryptage par inclusion

Le principe de cette méthode repose sur le fait d'inclure le message utile $U(t)$ dans la structure du système chaotique l'organe émetteur, la récupération du message se fait par observateur a entrées inconnues, ou l'inversion du système émetteur, cette méthode présente beaucoup d'avantage et nécessite un seul canal de transmission [16].

La figure (2.13) illustre la méthode de cryptage par inclusion

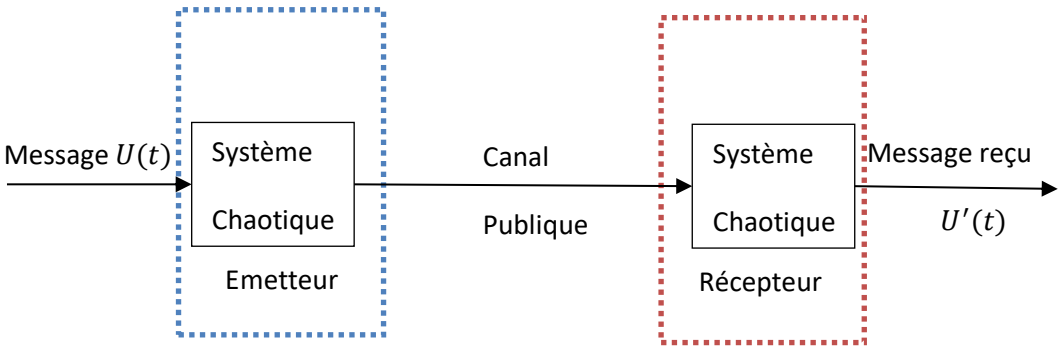


Figure II-13:Schéma de la méthode de cryptage par inclusion.

II.5 La cryptanalyse

La cryptanalyse est l'étude des probabilités de succès des attaques possible sur les systèmes cryptographiques afin de déterminer leur éventuelle faiblesse [16], l'un des principaux objectifs de la cryptanalyse est de tester si un adversaire peut déchiffrer le texte clair ou récupérer la clé secrète. Pour cela, il est nécessaire de se mettre à la place de l'adversaire ou pirate.

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

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

II.6 Conclusion

Dans la première partie de ce chapitre nous avons introduit la synchronisation des systèmes chaotique. Ensuite nous avons concentré sur les différents types et les diverses méthodes de synchronisation les plus performante.

Dans la deuxième partie les différents modèles de cryptographie avec les avantages et inconvénients de chaque modèle été présenté. Ainsi que les conditions appropriées pour l'implémentation.

Enfin, un domaine d'étude très important parallèle à la cryptographie été introduit il s'agit de la cryptanalyse constatons son importance face aux attaque et piratage.

Depuis que Pecora et Carrol ont démontré que deux système chaotique identique peut se synchronisent à des condition parfaits l'objectif est devenu la réalisation d'un lien entre la dynamique chaotique et le domaine de télécommunication. Dans le prochain chapitre un nouveau schéma de transmission de donnée à base de synchronisation de deux systèmes chaotiques sera traité.

III. Simulation du système de transmission à base de Synchronisation des deux oscillateur Henon-Hieles

III.1 Introduction

Les perspectives d'utilisation du chaos dans diverses application, notamment en télécommunication, et plus particulièrement dans les communications chaotiques. Grace a son grand potentiel dans les applications technologiques, la génération de l'hyper chaos est récemment devenu un thème central de recherche. Il faut savoir que la plupart des travaux sur la synchronisation des systèmes chaotique s'est consacré aux systèmes dynamiques a temp continu. Mais récemment, plusieurs études ont adressé la synchronisation des systèmes a temp discret pour leur divers avantage dans le domaine des communications privées, les clés d'un système de cryptage chaotique sont souvent les paramètre du système chaotique. La possibilité d'identifier les paramètres du système chaotique. Par conséquent, un système de cryptage chaotique sur doit être conçu de façon à ce que ses paramètres ne soient pas identifiable. Dans ce chapitre, quelques solutions sont apportées afin de sécuriser la transmission d'information basée sur la synchronisation chaotique. Notre schéma de transmission étudié est constitué de système dynamique chaotique a temps discret. L'émetteur est composé d'un système chaotique a temp discret dit Henon modifié, la synchronisation est faite par deux méthodes différentes. Dans chaque synchronisation une méthode de cryptage différent est introduite.

III.2 Etude d'observabilité du système

III.2.1 Caractéristique du système de Henon-Hieles

Notre étude se porte sur le système de Hénon-Hiles qui est un oscillateur chaotique, il est défini pas les équations d'état suivant :

$$\begin{cases} x(k+1) = a - y^2(k) - bz(k) \\ y(k+1) = x(k) \\ z(k+1) = y(k) \end{cases} \quad (3.1)$$

Ou a et b sont des constant positives.

On remarque qu'il y a une variable d'état de plus z que le système de Henon régulier (**voir chapitre 1)**. Notant que les deux systèmes sont linéaires pour $a = 0$.

III.2.2 Simulation de système Henon-Hieles sur Simulink

Le comportement chaotique du système est obtenu avec les valeurs des paramètre $a = 1.76$ et $b = 0.1$.

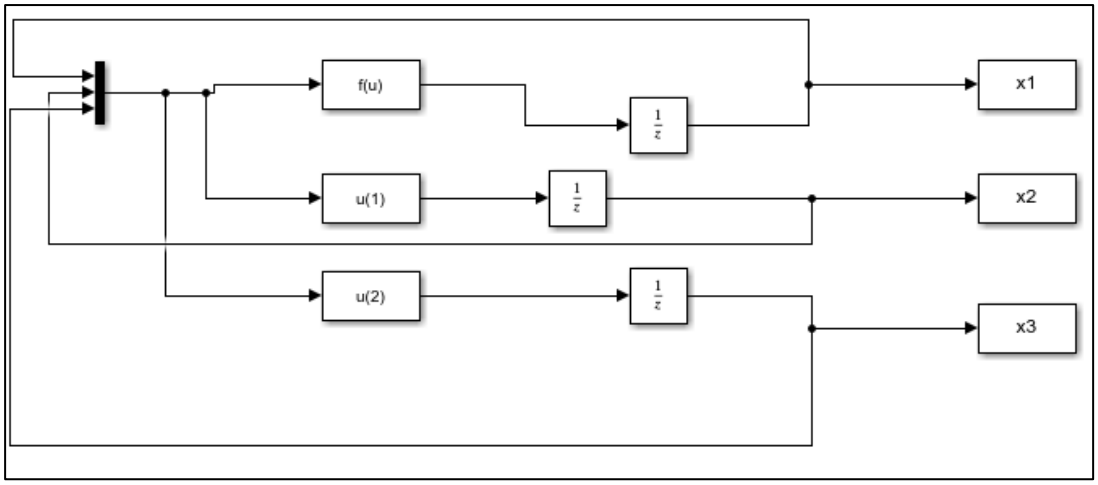


Figure III-1:schéma Simulink du système de Henon-Hieles

- **Visualisation des états :**
  a) $x(k)$

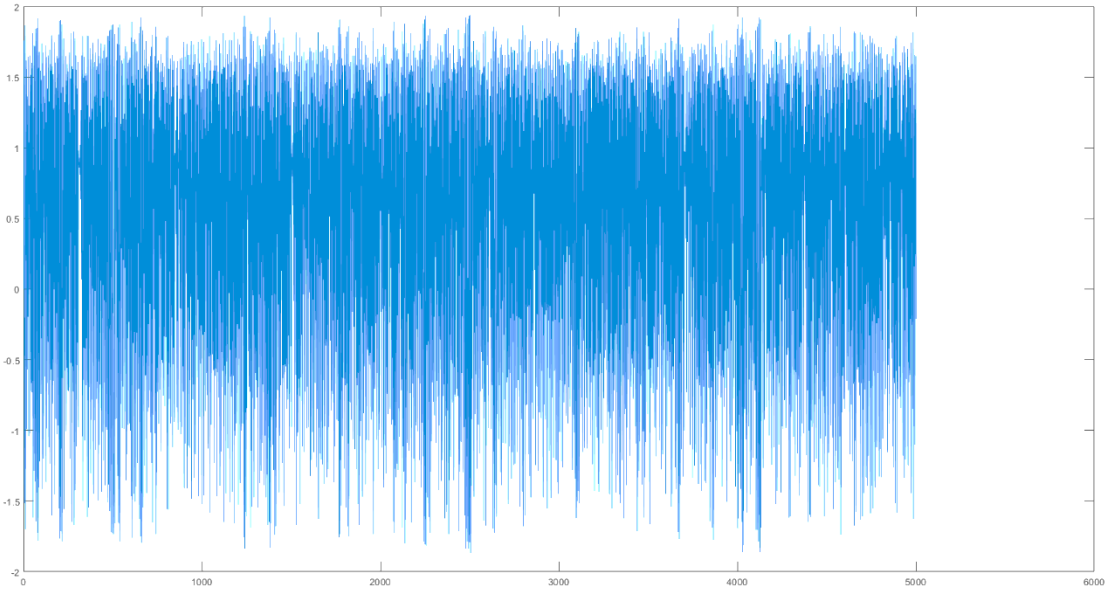


Figure III-2:graphe de l'état x(k)

b) $y(k)$

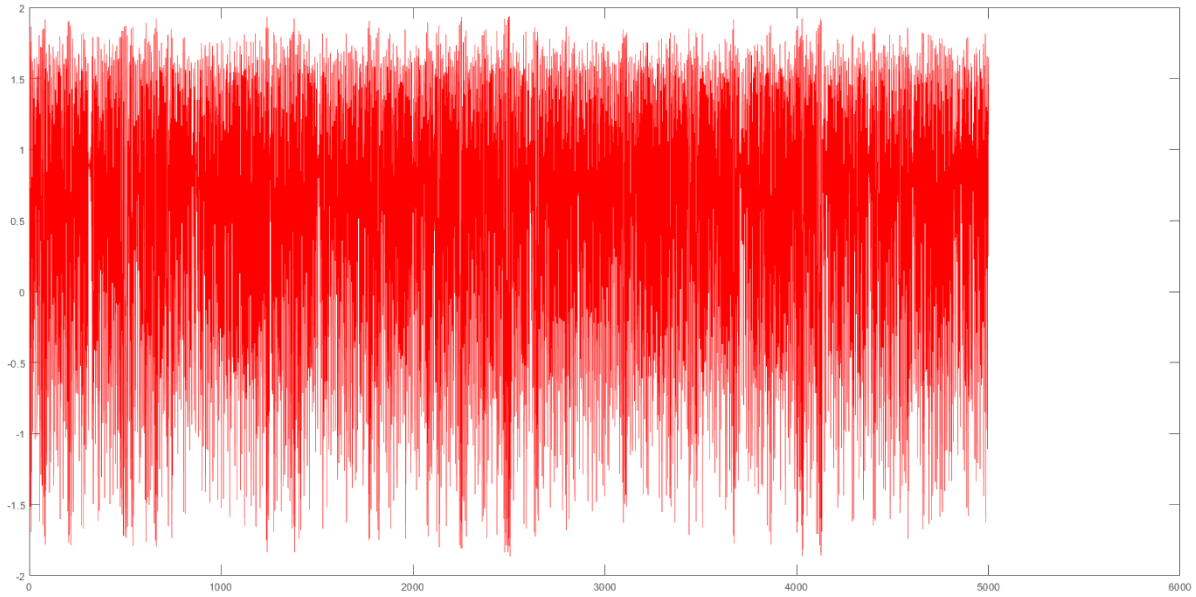


Figure III-3:graphe de l'état y(k)

c) $z(k)$

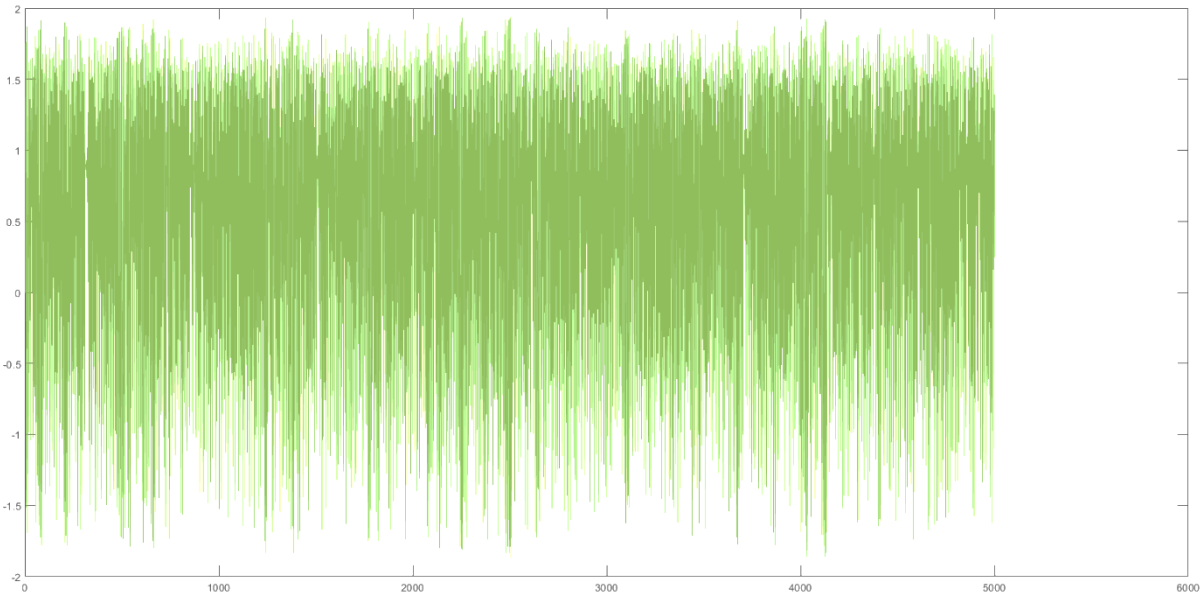


Figure III-4:graphe de l'état y(k)

Observation : les signaux $x(k), y(k), z(k)$ ont des oscillations apériodiques et irrégulières ce qui indique leurs natures chaotiques.

- **Visualisation de l'attracteur**

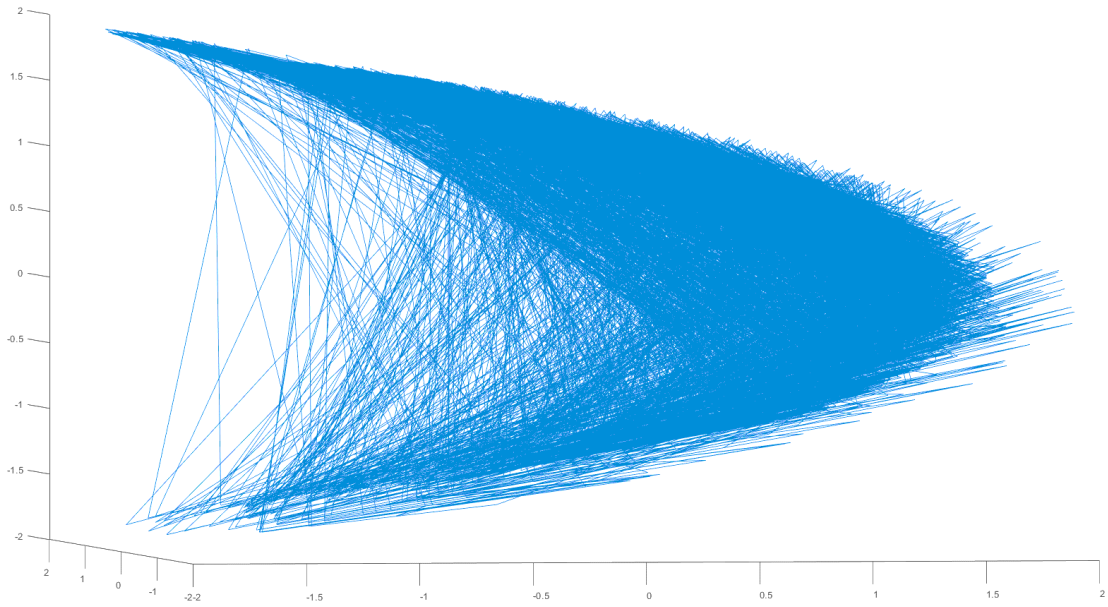


Figure III-5:attracteur Henon modifier

Comme on a vue dans le premier chapitre l'un des propriétés des dynamique chaotique est la sensibilité aux conditions initiales. Une valeur différente de $x(0)$ conduit à une tout autre suite qui après une courte phase, dessine la même image.

III.2.3 Vérification d'observabilité du système de Henon-Hieles

Dans cette partie. On a choisi la variable d'état $y(k)$ comme une sortie de système (3.1).

$$\begin{cases} x(k+1) = a - y^2(k) - bz(k) \\ y(k+1) = x(k) \\ z(k+1) = y(k) \\ s(k) = y(k) \end{cases} \tag{3.2}$$

Condition d'observabilité :

On étudie l'observabilité d'un système non linéaire en étudiant le rang de la matrice d'observabilité. On dit qu'un système est localement observable si et seulement si sa matrice d'observabilité est de rang plein par les colonnes.

On considère le système non linéaire suivant :

$$\begin{cases} x(k+1) = f\big(x(k)\big) + p\big(x(k)\big)w(k) \\ s(k) = h\big(x(k)\big) \end{cases} \tag{3.3}$$

Ou $w(k)$ représente une entrée inconnue, qui peut être une perturbation, une erreur ou un message.

Les champs des vecteur p: $f, p: \mathbb{R}^n \to \mathbb{R}$ et $h: U \subset \mathbb{R}^n \to \mathbb{R}$ sont supposé réels, le message doit être discret.la sortie du system est transmise au récepteur, ce qui devrait générer un vecteur de sortie qui converge asymptotiquement vers le vecteur d'entrée de l'émetteur. Ceci

constitue le problème l'inversion à gauche.il est possible de concevoir un observateur discret pour le système. Pour cela il est nécessaire de vérifier certaines conditions qui sont :

1. Les états ainsi que la perturbation inconnue sont bornés.
2. L'espace vectoriel $span\{dh, d(f \circ h), \dots, d(f^{n-1} \circ h)\} est\ de\ rang\ n.$
3. $O.p = ((dh)^T, (d(f \circ h)^T)^T.p = (0, \dots\dots, \theta)^T$ Ou θ est une fonction différente de 0 presque partout dans $u \subset \mathbb{R}^n \to \mathbb{R}$

- La troisième condition est appelée condition d'observabilité, elle garantit la propriété d'inversion a gauche.la possibilité de récupérer tous l'état, et le message $w(k)$ à partir de sortie $s(k)$ et ses itérations.

Vérification d'Observabilité :

Dans ce qui On considère le système qui peut être réécrit sous la forme du premier système. Dans ce qui suit nous vérifions les trois hypothèses.

a) Tous les états du système sont bornés. Ceci nous assure que l'hypothèse 1 est vérifiée.

b) On étudie la faible observabilité locale du système. On calcule la matrice d'observabilité dans le voisinage du point d'équilibre $(0,0,0)$ du système ci-dessous :

On a $h = [0\ y\ 0]$ et dh= [0 1 0] ensuite :

$$O = \begin{pmatrix} dh \\ d(f \circ h) \\ d(f^2 \circ h) \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & -2x_2 & -b \end{pmatrix} \quad (3.4)$$

Avec ces valeurs on trouve que le $rang\ (O) = 3 = n$, donc le système est localement observable l'hypothèse 2 est vérifiée. Par conséquent, l'observateur donné ci-dessous permet de reconstituer tous les états du système. Ceci explique le choix de la sortie s.

c) Pour la troisième condition, on a

$$p = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

On calcule maintenant $O.p$:

$$O.p = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & -2x_2 & -b \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ -b \end{pmatrix} \quad (3.5)$$

On note que la valeur de $\theta \neq 0$. Ainsi, la condition d'observabilité donnée dans l'hypothèse 3 est vérifier. Par conséquent le système Henon-Hieles est complétement observable.

III.3 Synchronisation à l'aide d'un observateur :

L'observateur est choisi afin de récupérer les états ainsi que le message du système de Hénon-Hieles. Dans ce qui suit, nous étudions le choix du signal de sortie dans le but de garantir l'observabilité du système.

La troisième condition d'observabilité garantit la propriété d'inversion à gauche [17] (la possibilité de récupérer tous les états, et le message $m(k)$ à partir de la sortie $s(k)$ et ses itérations. Par conséquent, l'observateur donné ci-dessous permet de reconstituer le message transmis du premier système

Détermination des paramètres d'observateur par placement des pôles

$$\begin{cases} \hat{x}(k+1) = a - y^2(k) - b\hat{z}(k) + g_1\big(\hat{y}(k) - y(k)\big) \\ \hat{y}(k+1) = \hat{x}(k) + g_2\big(\hat{y}(k) - y(k)\big) \\ \hat{z}(k+1) = y(k) + g_3\big(\hat{y}(k) - y(k)\big) \end{cases} \tag{3.6}$$

L'état corrigée grâce au modèle en fonction de l'écart entre la sortie mesurée et la sortie reconstruite par l'observateur $(y(t) - \hat{y}(t))$ .g_1, g_2, g_3 Sont respectivement les gains de l'observateur.

A partir des système émetteur(3.2) et récepteur (3.6) on obtient l'erreur d'observation :

$$\begin{cases} e_1(k+1) = -b\big(\hat{z}(k) - z(k)\big) + g_1 e_2(k) \\ e_2(k+1) = e_1(k) + g_2 e_2(k) \\ e_3(k+1) = (\hat{y}(k) - y(k) + (g_3 e_2(k) \end{cases}$$

$$\begin{cases} e_1(k+1) = -be_3(k) + g_1 e_2(k) \\ e_2(k+1) = e_1(k) + g_2 e_2(k) \\ e_3(k+1) = e_2(k) + g_3 e_2(k) \end{cases} \tag{3.7}$$

Par placement des pôles

$$\begin{pmatrix} e_1(k+1) \\ e_2(k+1) \\ e_3(k+1) \end{pmatrix} = \begin{vmatrix} 0 & g_1 & -b \\ 1 & g_2 & 0 \\ 0 & g_3 + 1 & 0 \end{vmatrix} \begin{pmatrix} e_1(k) \\ e_2(k) \\ e_3(k) \end{pmatrix} \tag{3.8}$$

$$G = \begin{vmatrix} 0 & g_1 & -b \\ 1 & g_2 & 0 \\ 0 & g_3 + 1 & 0 \end{vmatrix}$$

$$|ZI - G| = \begin{vmatrix} z & -g_1 & b \\ -1 & z - g_2 & 0 \\ 0 & -1 - g_3 & z \end{vmatrix} \tag{3.9}$$

$$det_{|ZI-G|} = z^3 - g_2 z^2 - z g_1 + b g_3 + b \tag{3.10}$$

Soit z_1, z_2, z_3 les trois racines du polynôme (3.10) on a :

$$\begin{aligned} det_{|ZI-G|} &= (z - z_1)(z - z_2)(z - z_3) \\ &= (z - z_1)(z^2 + z(z_2 + z_3) + z_2 z_3 \\ &= z^3 - z^2(z_2 + z_3 + z_1) + z(z_1 z_2 + z_2 z_3 + z_1 z_3) - z_1 z_2 z_3 \end{aligned} \tag{3.11}$$

Par identification entre $(3.10)\ et\ (3.11)$, on obtient :

$$\begin{cases} g_1 = -(z_1 z_2 + z_2 z_3 + z_1 z_3) \\ g_2 = z_1 + z_2 + z_3 \\ g_3 = \dfrac{z_1 z_2 z_3 + b}{b} \end{cases} \tag{3.12}$$

Prenons $z_1 = z_2 = z_3 = 0$ on obtient $(\boldsymbol{g_1 = 0}\ ; \boldsymbol{g_2 = 0}; \boldsymbol{g_3 = 1}\ )$

Pour $z_1 = 0.4, z_2 = 0.3, z_3 = 0.1$ on obtient $(\boldsymbol{g_1 = 0.9}\ ; \boldsymbol{g_2 = 0.6}; \boldsymbol{g_3 = 1.4})$

III.3.1 Simulation de la Synchronisation en Simulink

La simulation se fait sous Matlab Simulink, on transmet $y(k)$ dont on a étudié l'observabilité, le signal est injecté dans le système récepteur.

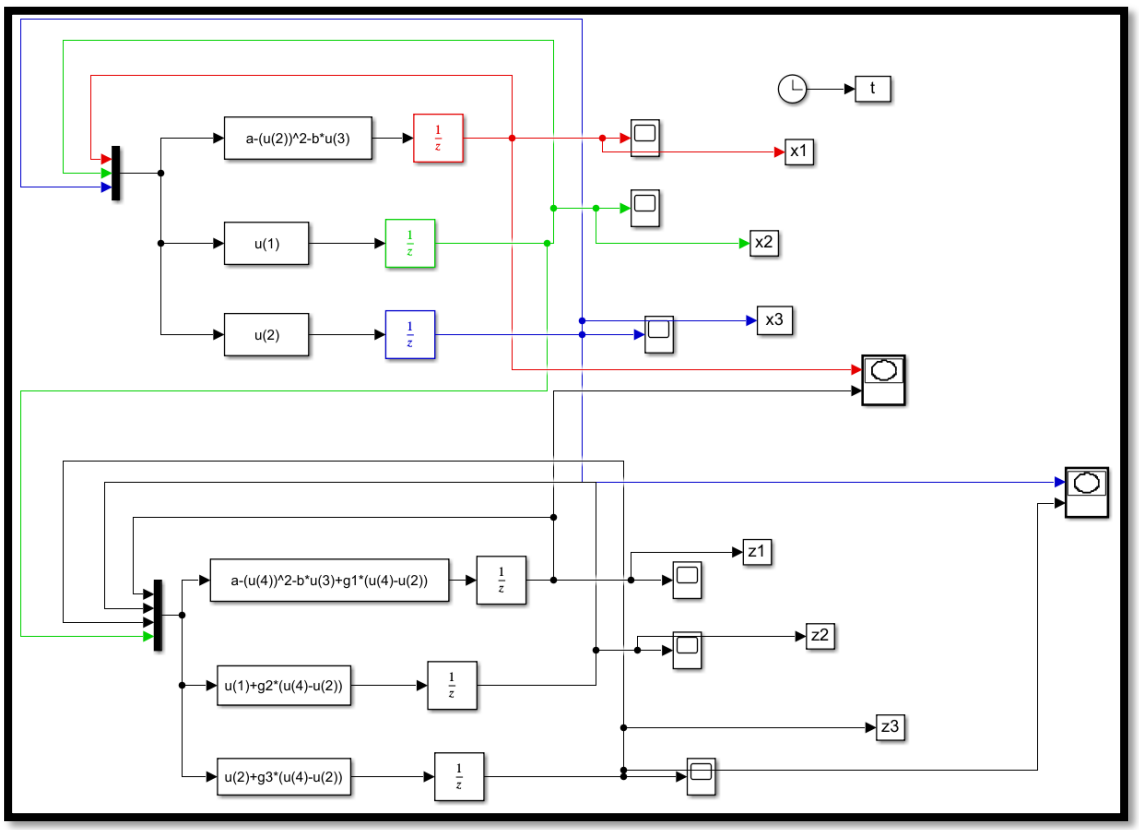


Figure III-6:Schéma Simulink de la synchronisation pour système Henon-Hieles

Pour des valeurs différentes de gain on a une synchronisation plus ou moins satisfaisante.

Si on prend $\boldsymbol{g_1 = 0.9, g_2 = 0.6, g_3 = 1.4}$, on obtient les résultats suivants :

a) $x(k)$ *et* $\hat{x}(k)$

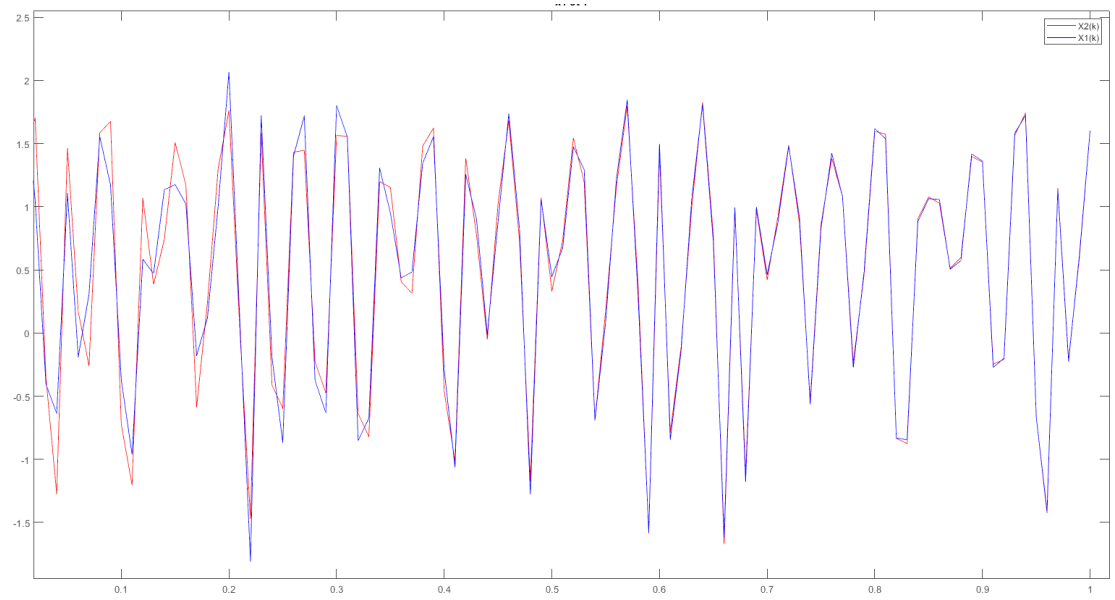


Figure III-7:graphe x(k) et x̂(k)

b) $y(k)$ *et* $\hat{y}(k)$

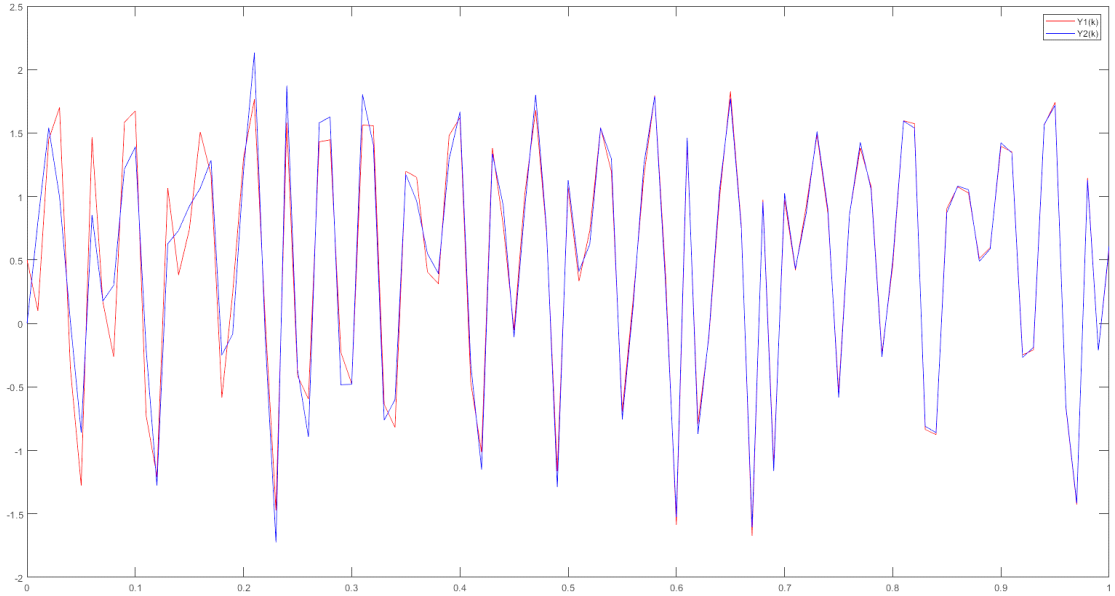


Figure III-8: : graphe y(k) et ŷ(k)

c) $z(k)$ *et* $\hat{z}(k)$

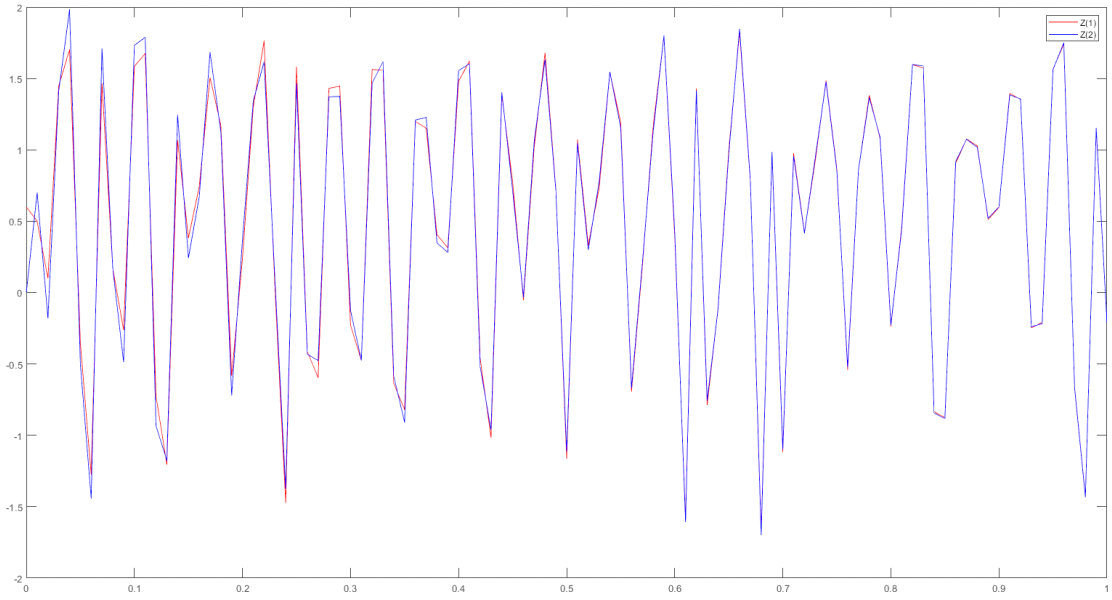


Figure III-9 : graphe z(k) et ẑ(k)

d) **Plan de phase** $x, \hat{x}$

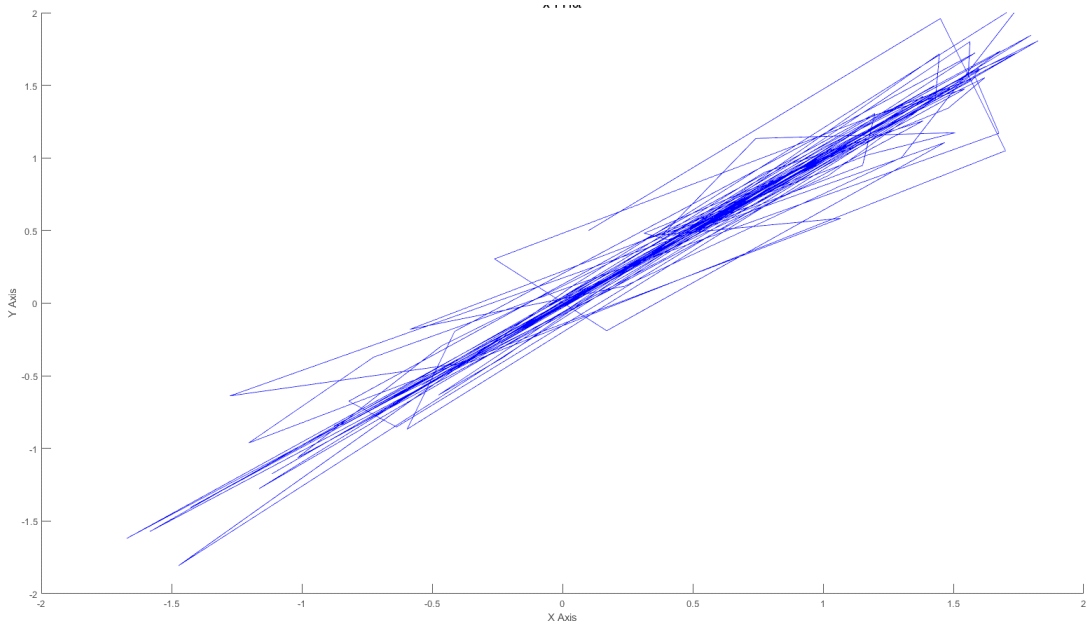


Figure III-10:Plan de phase (x, x̂)

Analyse des résultats : On remarque que la synchronisation prend une durée de temp importante 0.9s et la synchronisation n'est pas parfaite ce qui n'est pas idéal pour un dispositif de communication.

On change les paramètres de gain $g_1 = 0, g_2 = 0, g_3 = 1$, on obtient :

a) $x(k)$ *et* $\hat{x}(k)$

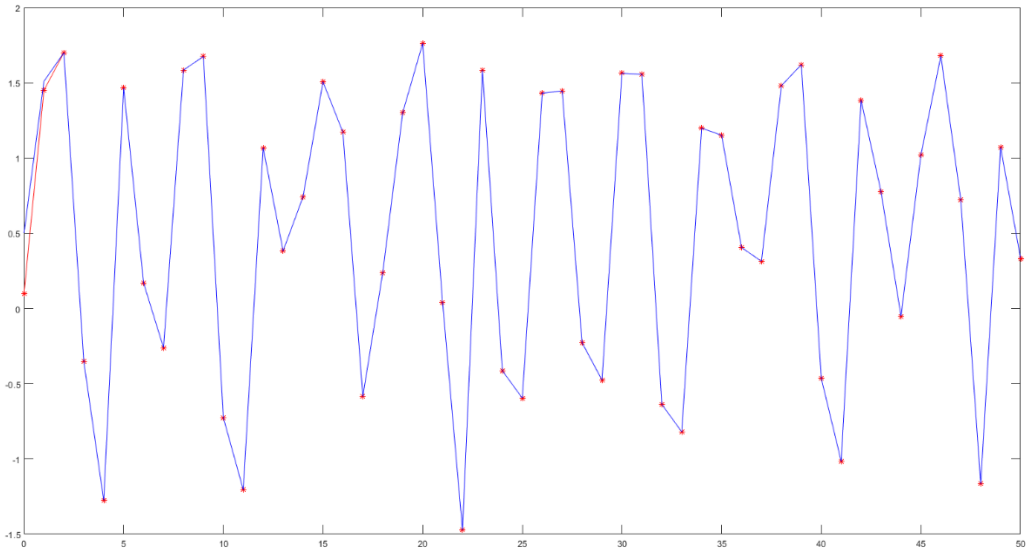


Figure III-11:graphe x(k) et x^(k)

b) $y(k)$ *et* $\hat{y}(k)$

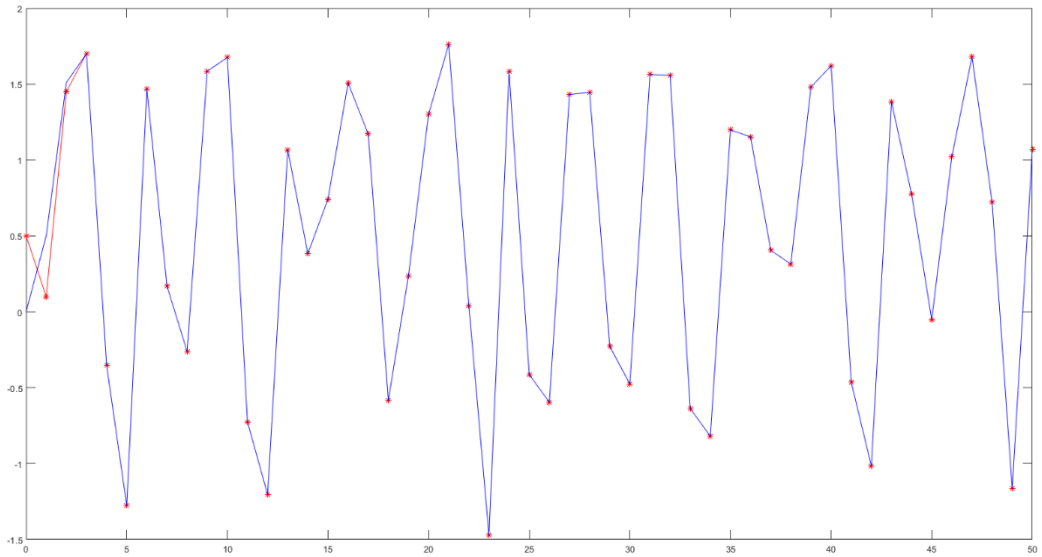


Figure III-12:graphe y(k) et y^(k)

a) $z(k)$ *et* $\hat{z}(k)$

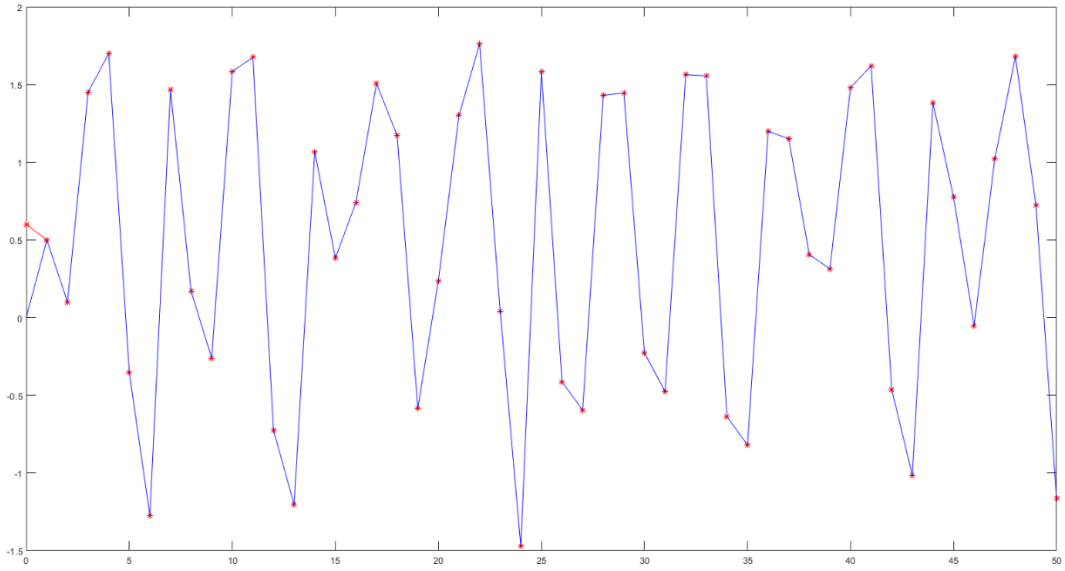


Figure III-14 : graphe z(k) et ẑ(k)

b) Plan de phase $x, \hat{x}$

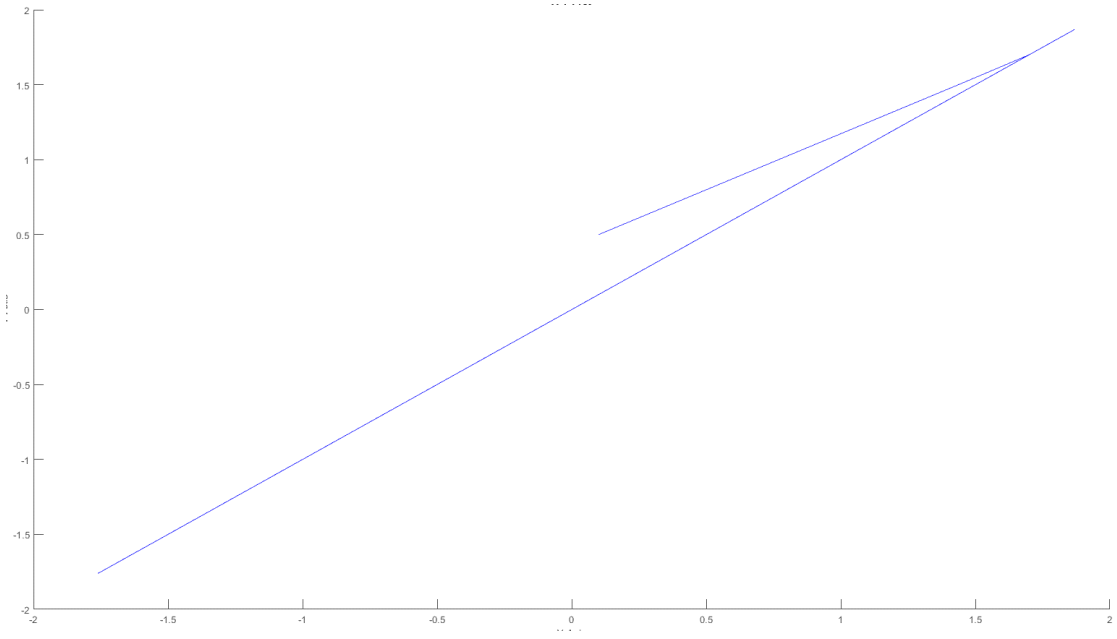


Figure III-13:Plan de phase (x, x̂)

Analyse des résultats : On note que les états des deux systèmes confondent très rapidement, et les deux systèmes se synchronisent parfaitement. Par conséquent ce choix de paramètre de gain permet de synchroniser les deux systèmes.

III.3.2 Insertion de message

On note que la condition d'observabilité donnée dans l'hypothèse 3 est vérifiée. Ce qui implique que la meilleure option est d'insérer le message dans la troisième dynamique du système. Dans l'intention de garder le comportement chaotique

Notre approche pour inclure le signal de message est la méthode par addition (Voir chapitre 2), on ajoute le message à l'état $z(k)$ de l'émetteur, de coté de récepteur on soustrait le message du signal de l'entrée.

On prend l'exemple d'un signal sinusoïdale numérique. Le signal doit être bornée et préserver

Le comportement chaotique du système. On prend l'exemple d'un signal sinusoïdale numérique avec une amplitude de 0.2 et une fréquence de 1hz :

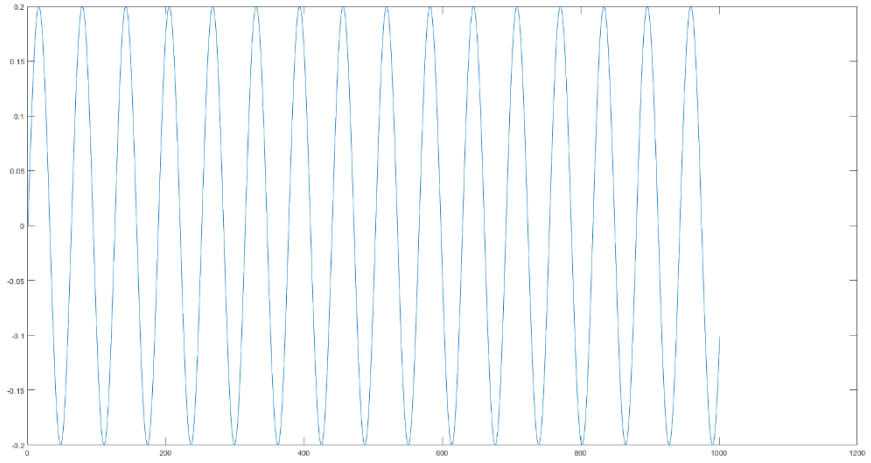


Figure III-14::Message a ajoutée (signal sinusoïdal)

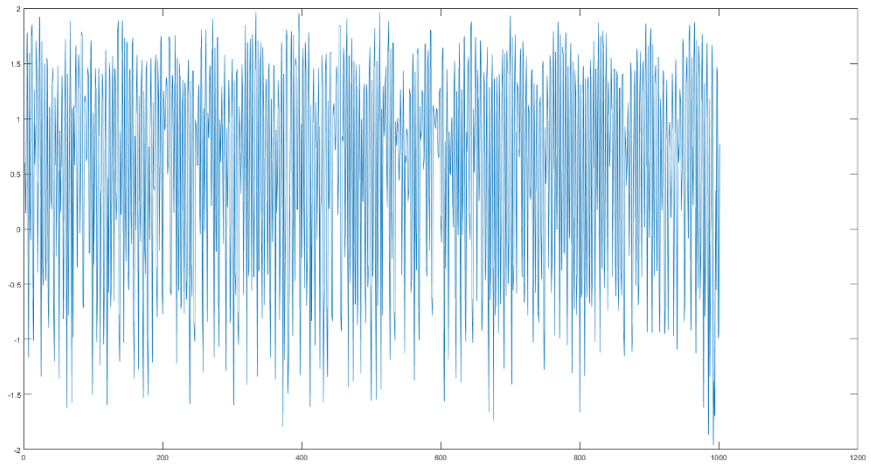


Figure III-15:Message aprés le cryptage par addition

III.3.3 Récupération du message

De coté de récepteur on soustrait le message du signal de l'entrée

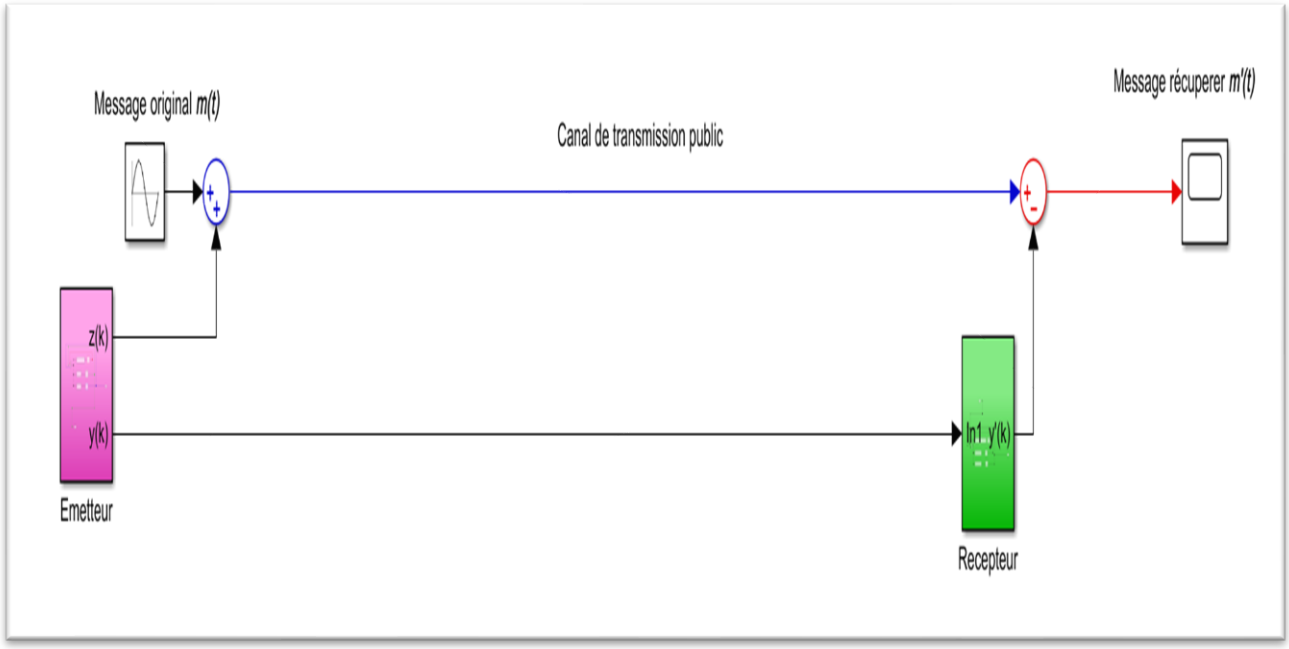


Figure III-16:schéma Simulink de récuperation de message

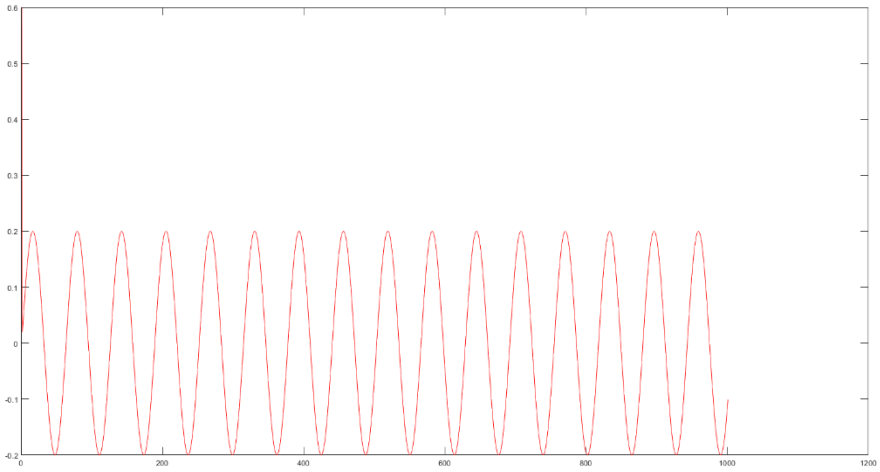


Figure III-17:Message récupérer

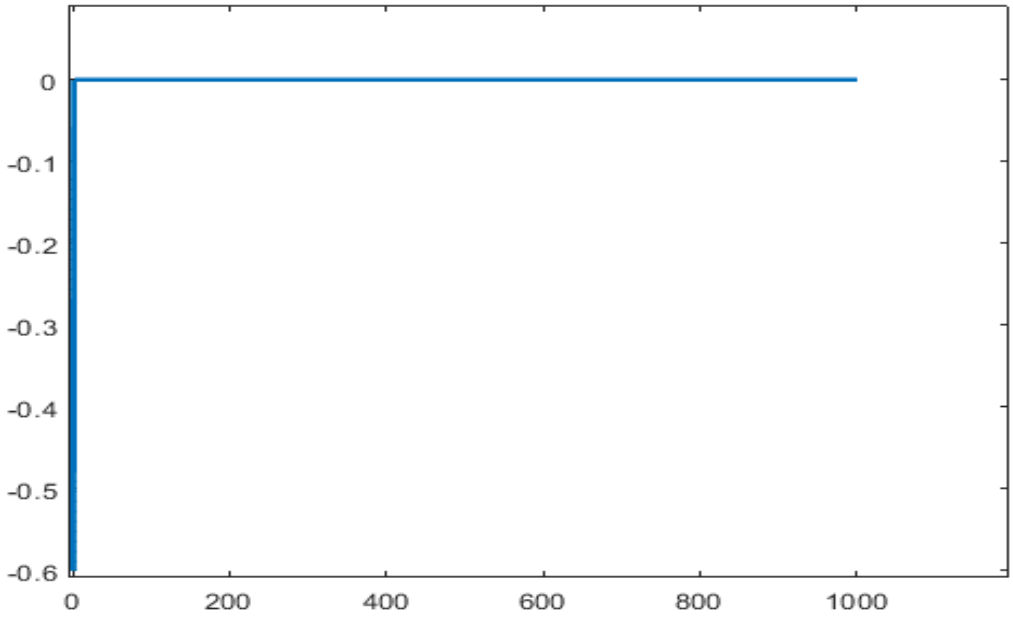


Figure III-18:Erreur de synchronisation

Analyse des résultats :

- La figure (3.18) montre que l'erreur de synchronisation tend vers 0 au bout d'$1ms$, et Le signal $m(k)$ est reconstitué.

III.4 Synchronisation à l'aide d'un observateur retardé

III.4.1 Cryptage et inclusion de message

Pour améliorer la sécurité de système le message est crypté par inclusion comme montré sur la Figure 19*:*

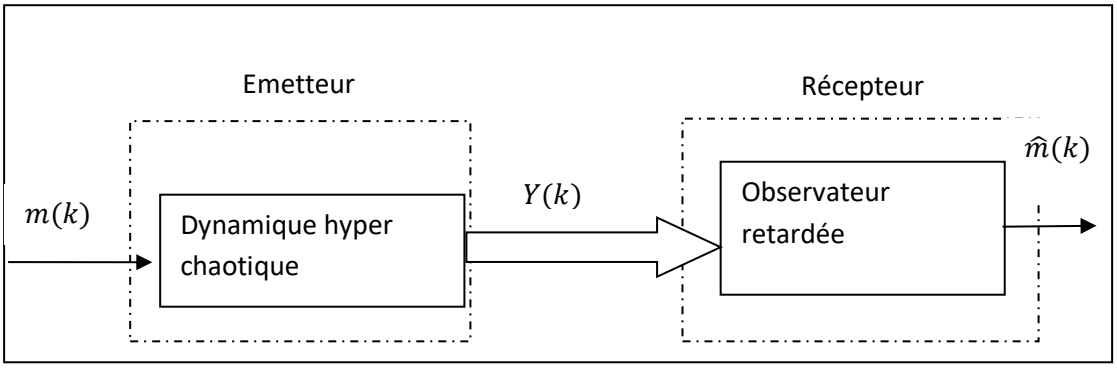


Figure III-19:Chaîne de transmission

Afin de préserver le comportement chaotique, Le message crypté est introduit dans la Troisième dynamique du système. On obtient :

$$\begin{cases} x(k+1) = a - y^2(k) - bz(k) \\ y(k+1) = x(k) \\ z(k+1) = y(k) + m(k) \\ s(k) = y(k) \end{cases} \quad (3.13)$$

III.4.2 Présentation de l'observateur

Dans cette partie on présente l'observateur retardé

Nous allons concevoir l'observateur étape par étape qui fonctionne avec un pas d'échantillonnage T.

- La première étape consiste à appliquer un pas de retard (n-1) sur la sortie et ainsi reconstruire le premier état du système de départ.
- La seconde étape on applique deux pas de retard (n-2) sur la sortie et un pas de retard (n-1) sur l'état venant d'être reconstruit afin de reconstruire le second état.
- L'application du retard est faite sur tous les états jusqu'à la dernière information contenant l'entrée du système de départ. Chaque état reconstruit a itération n contribue à la reconstruction du prochain état a l'itération n-1[20].

Reconstruction de l'état $\hat{x}$:

De (3.13) on a :

$$\hat{y}(k+1) = \hat{x}(k)$$

En appliquons un retard d'un pas sur la sortie, on obtient l'état $\hat{x}$ comme suit :

$$\hat{x}(k-1) = s(k) = x(k-1) \quad (3.14)$$

Reconstruction de l'état $\hat{z}$:

De la première équation de système (3.14) on a :

$$\hat{z}(k) = \frac{a - \hat{x}(k+1) - y^2(k)}{b}$$

En appliquons un retard de deux pas on obtient l'état $\hat{z}$ comme suit :

$$\hat{z}(k-2) = \frac{a - s(k) - y^2(k-2)}{b} \quad (3.15)$$

Reconstitution de message $\hat{m}(k)$:

A partir du système (3.13) ,on a :

$$\hat{m}(k-3) = \hat{z}(k+1) - \hat{y}(k)$$

En utilisant les équations (3.14), (3.15) et en appliquant trois pas de retard, on obtient :

$$\hat{m}(k-3) = \frac{a - s(k) - s^2(k-2)}{b} - s(k-3) \qquad (3.16)$$

Par conséquence les équations de l'observateur sont données par les équations (3.14) (3.15), (3.16)

$$\begin{cases} \hat{x}(k-1) = s(k) \\ \hat{z}(k-2) = \dfrac{a - s(k) - y^2(k-2)}{b} \\ \hat{m}(k-3) = \dfrac{a - s(k) - s^2(k-2)}{b} - s(k-3) \end{cases} \qquad (3.17)$$

III.4.3 Simulation de la Synchronisation en Simulink

La simulation se fait sous Matlab Simulink, on transmet $y(k)$ et en appliquons un retard de 3 pas pour le récepteur.

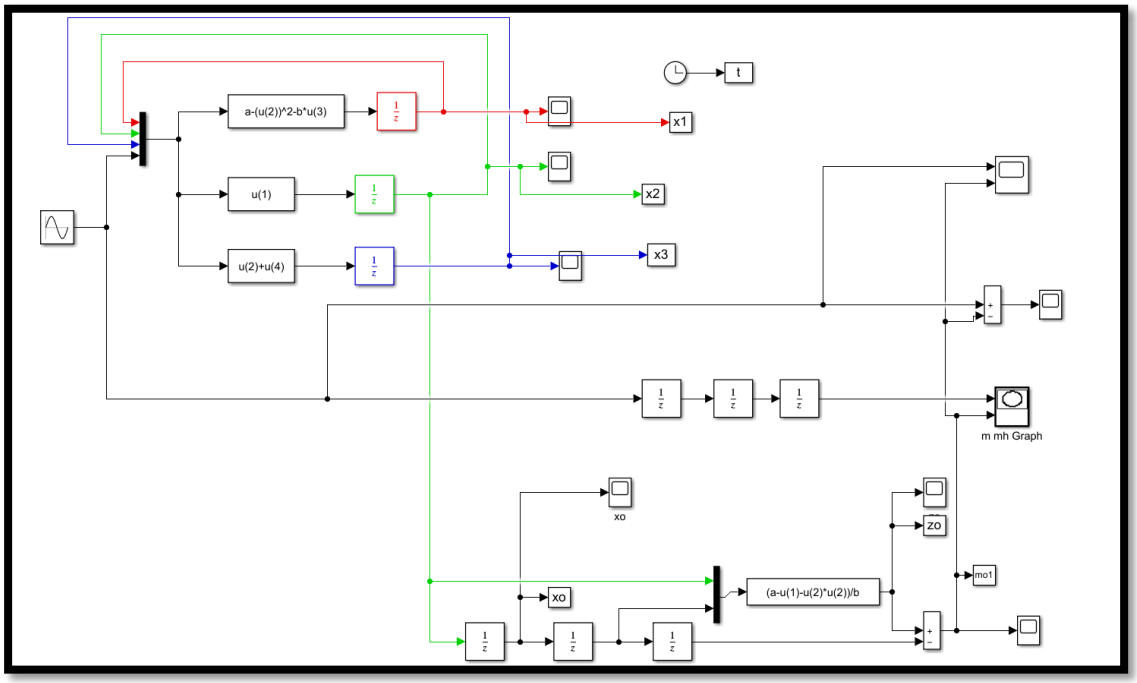


Figure III-20:schéma Simulink pour la synchronisation retardée

On a choisi $m(k)$ un signal sinusoïdal d'amplitude 1 et de fréquence 10Hz, La période T dans notre simulation $T = \frac{1}{f} = 0.1s$. Prenons Le paramètre $a = 1.7$

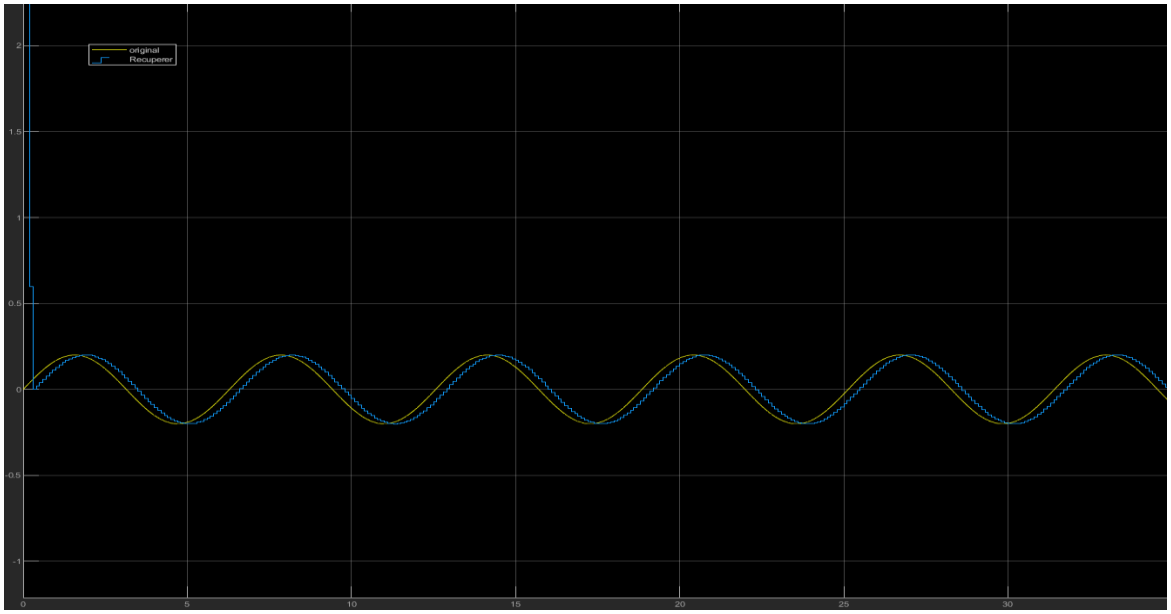


Figure III-21: $\boldsymbol{m(k)\ et\ \widehat{m}(k)}$

.

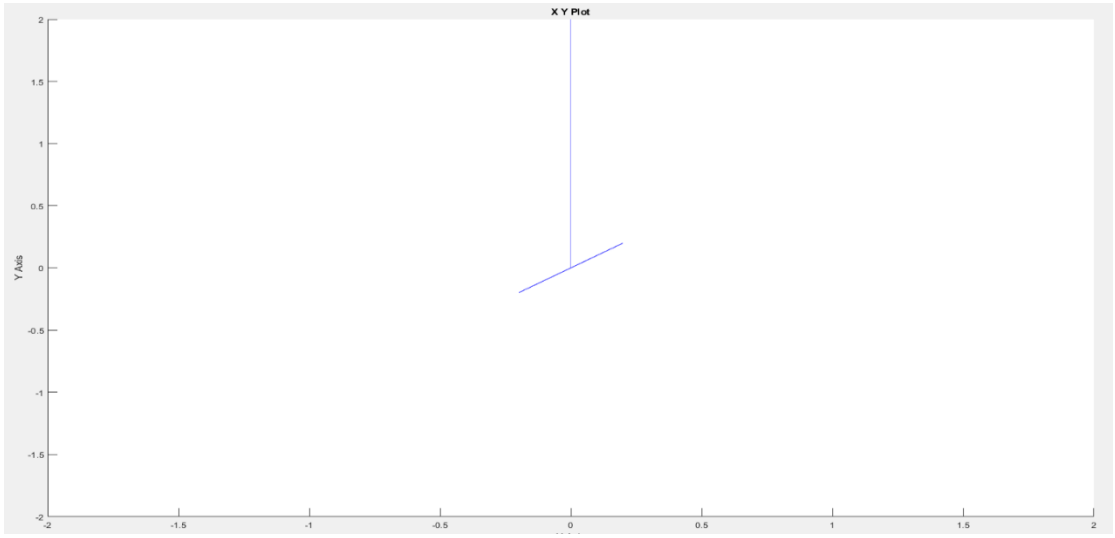


Figure III-22:plan de phase

Observation :

On remarque que le message $m(k)$ est reconstitué après la synchronisation, l'erreur du message $e_m(k) = m(k) - \widehat{m}(k)$ disparait au bout de $3T = 0.3s$, ce qui correspond à un retard de trois pas d'après l'équation (3.16).

III.5 Conclusion

Dans ce chapitre on a étudié l'observation du système, afin de choisir un observateur, Puis on a fait la synchronisation des deux système émetteur et récepteur par deux types de synchronisation, par la suite nous avons insérer le message on utilise la méthode de cryptage par addition et la méthode par inclusion. Enfin le message a été récupérer du récepteur avec sucée.

Dans le chapitre suivant nous allons réaliser un dispositif de transmission sécurisée de données sur des cartes Arduino.

IV. Implémentation du système de transmission sur carte Arduino

IV.1 Introduction

Les premières expérimentations de communication basées sur le chaos ont été réalisée sur des circuits électroniques analogique [18], mais la sensibilité des systèmes a la déviation des composant a longtemps posé problème dans les systèmes de communication. En effet, les systèmes chaotiques sont très sensibles aux perturbations et le signal issu de deux systèmes très proches divergent très rapidement.

En revanche, les systèmes numériques programmable (µController, Processeur, FPGA) permettant de générer aisément et de maniéré reproductible des signaux issus de discrétisation d'équation chaotique.

Dans notre étude, nous avons choisi d'utiliser deux carte Arduino Méga. L'intérêt de son utilisation se justifie par sa disponibilité son efficacité et ses fonctionnalités. On abordera la manière de programmation de la carte avec Matlab Simulink.et nous présentons par la suite les schémas synoptiques de transmission adopté par la suite on montre les résultats obtenus des différents tests.

IV.2 Présentation de système de transmission

IV.2.1 Emetteur

L'émetteur est constitué d'une carte Arduino Méga contenant les équations du système Hénon-Heiles, sert au cryptage du message et la génération du signal crypter et la clé.

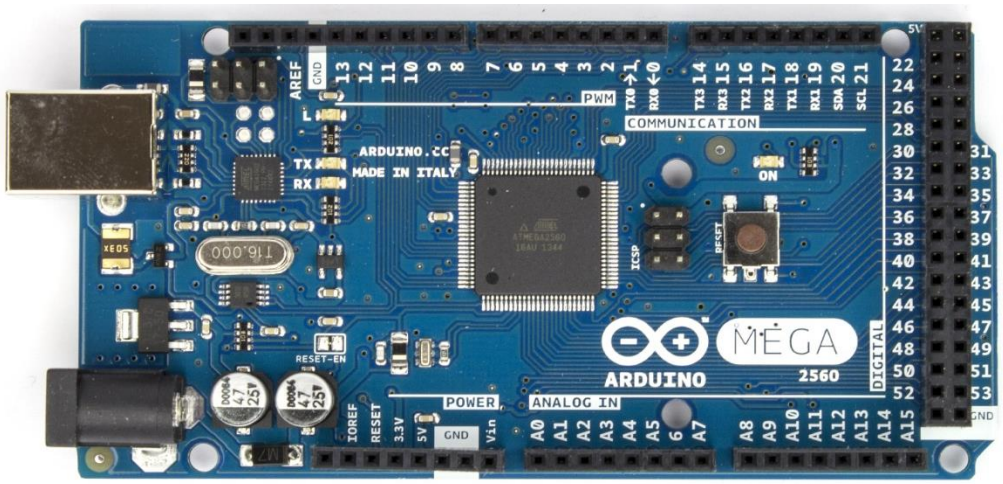


Figure IV-1:Carte Arduino Méga

IV.2.2 Récepteur

Est un autre carte Arduino Méga contenant un Observateur du système émetteur il a pour tâche le décryptage du message reçu.

IV.2.3 Manipulation de la carte Arduino avec Simulink

Pour cela il faut utiliser la bibliothèque **support Package for Arduino Hardware**, la bibliothèque génère automatiquement le code à partir du modèle Simulink qui va fonctionner alors sur la carte Arduino de façon autonome.

La bibliothèque Simulink **support Package for Arduino Hardware** offre une variation des bloque spécifique à la carte Arduino en plus des milliers des block et des fonctions mathématique, d'ingénierie et de traçage intégrer dans Simulink pour analyser et visualiser les données collectées à partir de la carte Arduino.sa permet d'écrire et lire des données de la carte Arduino et voir immédiatement les résultats dans Matlab sans compiler de code.

4444

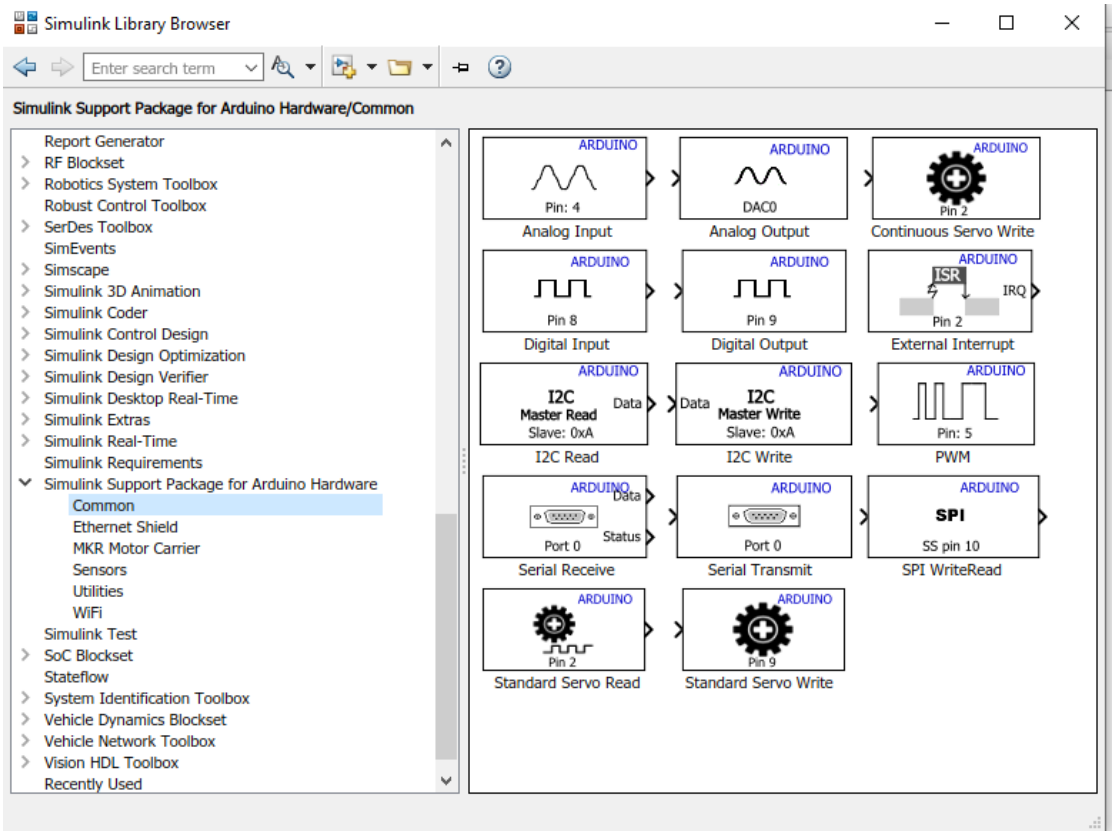


Figure IV-2:Bibliothéque Arduino Hardware support package

IV.2.4 Communication série Arduino

La communication série sur les broches **TX/RX** utilise des niveaux logiques TTL (5V ou 3,3V selon la carte). La voie série est émulée à travers l'USB c'est une liaison virtuelle de l'RS232, l'émulation est gérée par un circuit intégré.

Serial est utilisé pour la communication entre la carte Arduino et un ordinateur ou d'autres appareils. Toutes les cartes Arduino ont au moins un port série (également appelé UART ou USART) : Serial. Il communique sur les broches numériques 0 (RX) et 1 (TX) ainsi qu'avec l'ordinateur via USB. Ainsi, l'utilisation de ces fonctions, interrompre les broches 0 et 1 pour l'entrée ou la sortie numérique.

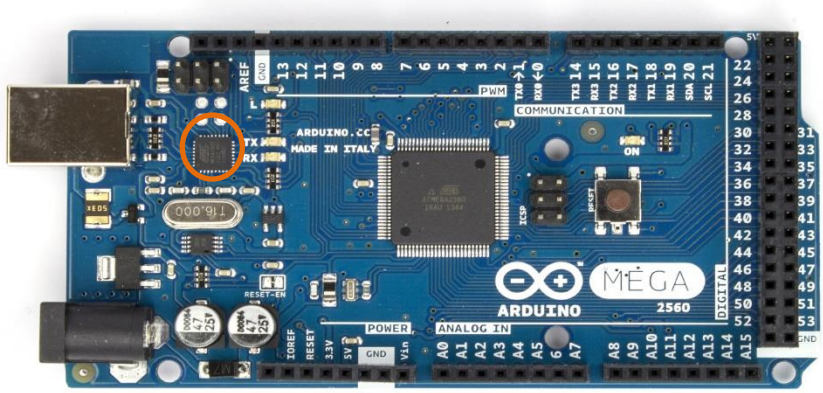


Figure IV-3:Circuit emulateur de port série

L'Arduino Méga dispose de trois ports série supplémentaires : Serial1 sur les broches 19 (RX) et 18 (TX), Serial2 sur les broches 17 (RX) et 16 (TX), Serial3 sur les broches 15 (RX) et 14 (TX). Pour utiliser ces broches pour communiquer avec un ordinateur personnel, il faut utiliser un adaptateur USB-série supplémentaire, car ils ne sont pas connectés à l'adaptateur USB-série du Méga. Pour les utiliser pour communiquer avec un périphérique série TTL externe, il faut connecter la broche TX à la broche RX de l'appareil, le RX à la broche TX de l'appareil et La GND de l'Arduino Méga à la GND de l'appareil.

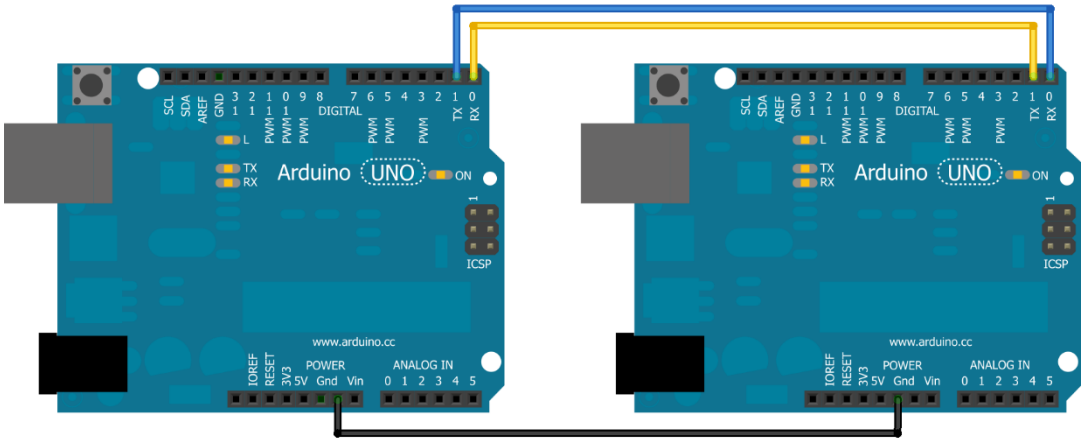


Figure IV-4:Communication série entre 2 Arduino

IV.2.5 Transmission des données

Les données qui transitent par la voie série sont transmises sous une forme binaire codée sur 8 bits selon la table ASCII. C'est à dire avec des niveaux logiques 0 et 1. La donnée commence avec un bit Start et se termine avec un bit stop comme illustré dans la figure suivante :

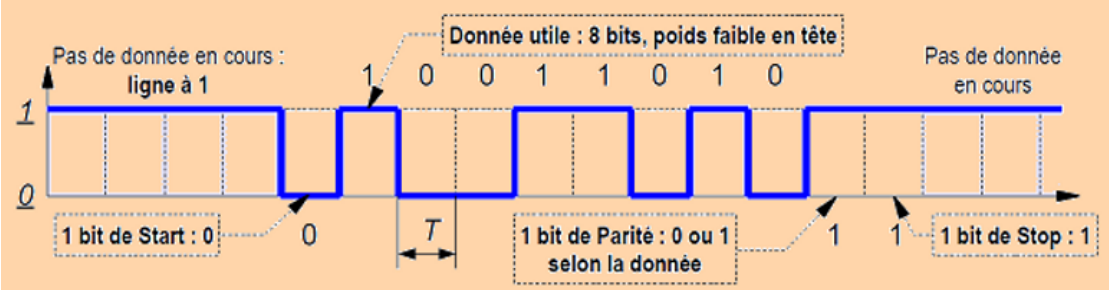


Figure IV-5:Transmission d'un octet avec le Protocol UART

IV.2.6 Vitesse de transmission

La norme définit la vitesse à laquelle sont envoyées les données. Elles sont exprimées en bit par seconde (bit/s). Elle préconise des vitesses inférieures à 20 000 bits/s. Sauf qu'on pratique, il est très courant d'utiliser des débits supérieurs pouvant atteindre les 115 200 bits/s. Quand on va utiliser la voie série, on va définir la vitesse à laquelle sont transférées les données. Cette vitesse dépend de plusieurs contraintes qui sont : la longueur du câble utilisé reliant les deux interlocuteurs et la vitesse à laquelle les deux interlocuteurs peuvent se comprendre.

Tableau 2:Vitesse de transmission en communication serial

Bauds	Bit/s	Durée de bit (µs)	Vitesse (bytes/s)
50	50	20000000	6.25
200	200	5000000	25
1200	1200	833	150
2400	2400	416	300
4800	4800	208	600
9600	9600	104	1200
19200	19200	52	2400
38400	38400	26	4800
57600	57600	17	7200
115200	115200	8	14400

IV.3 Implémentation du système

La méthode de cryptage par addition est adoptée et le message choisit est un signal carré.

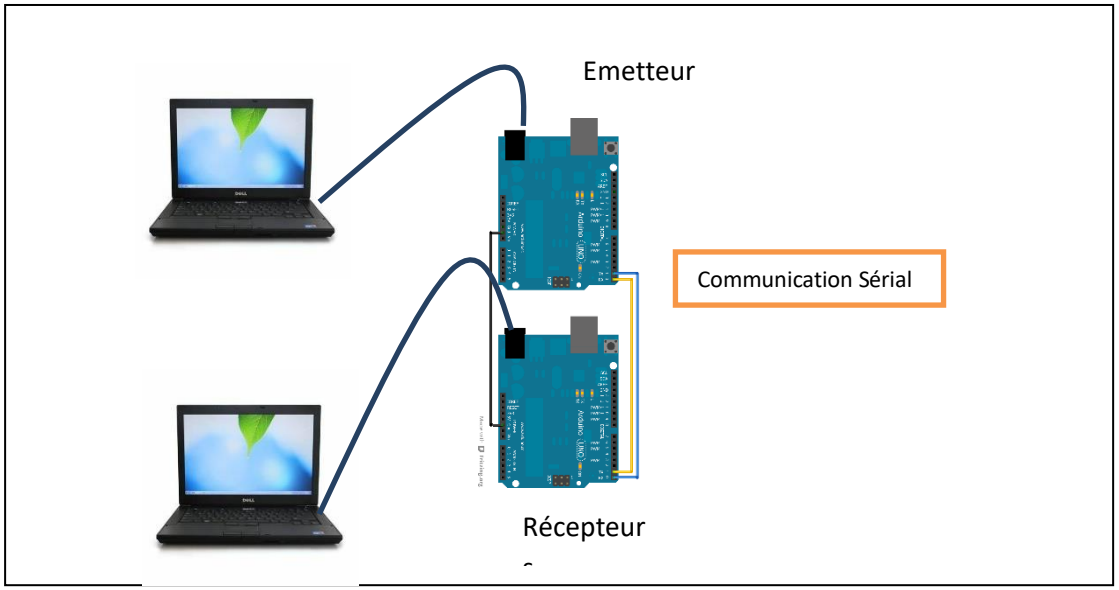


Figure IV-6: montage du système de transsmission

IV.3.1 Emetteur

Le programme émetteur est compilé vers la carte Arduino 1 via la liaison RS232 (port 0)

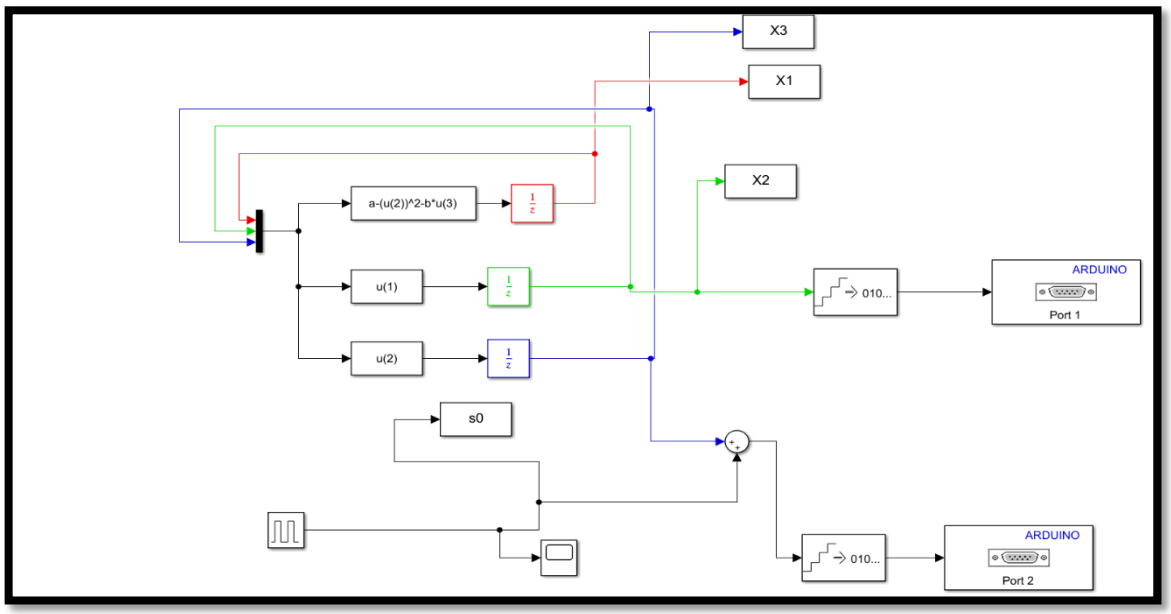


Figure IV-7:Schémas Simulink de l'emetteur

Les port serial Transmitter (TX1, TX2) ont utiliser pour envoyer les données de Arduino émetteur ver Arduino récepteur

- Port TX1 : contient le message crypter
- Port TX2 : contient la clé de décryptions

IV.3.2 Récepteur

Les port serial Reciever (RX1, RX2) sont utiliser pour la réception des données du broche (TX1 TX2) de l'émetteur dans cet ordre

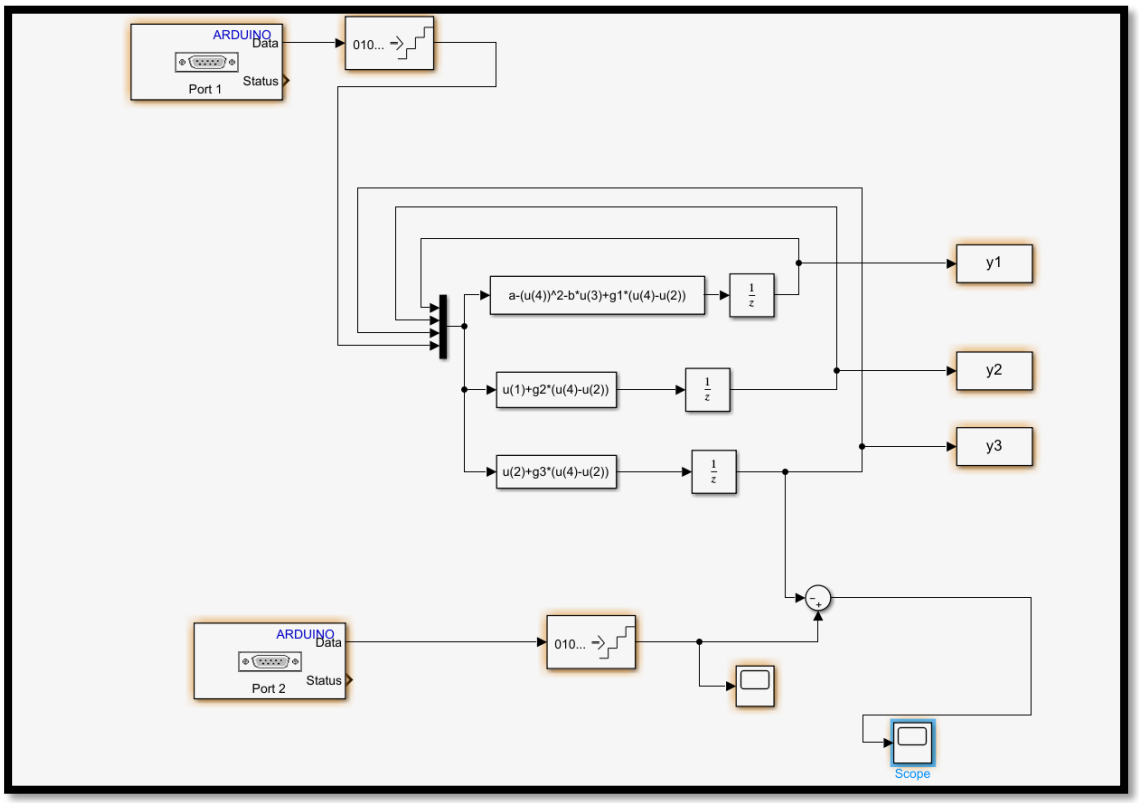


Figure IV-8:Schémas Simulink de récepteur

IV.4 Visualisation des signaux

IV.4.1 Message originale (signal carré)

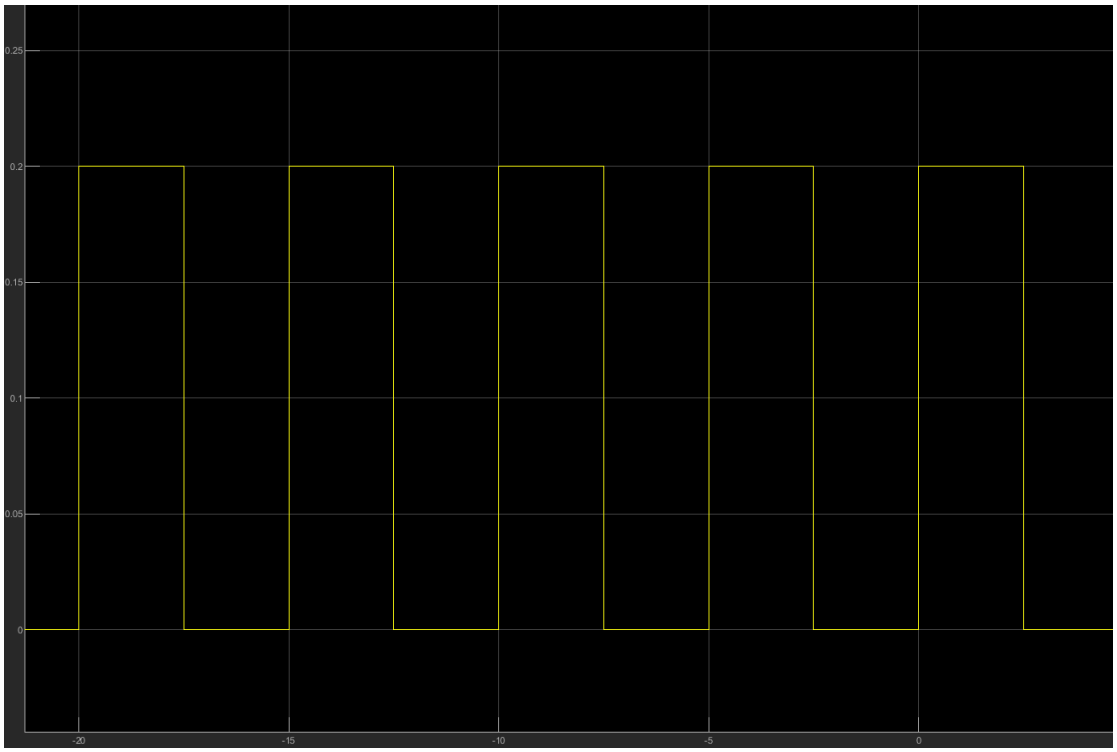


Figure IV-9:Message originale

IV.4.2 Clé de décryptage

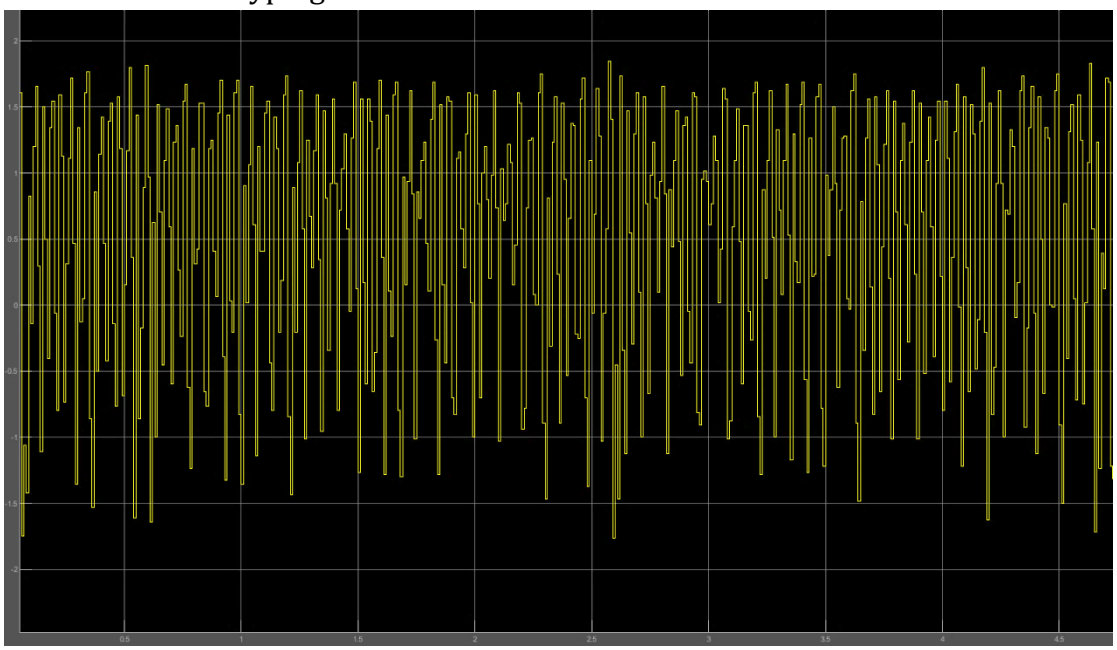


Figure IV-10:Clé de décryptage $y(k)$

IV.4.3 Message crypté

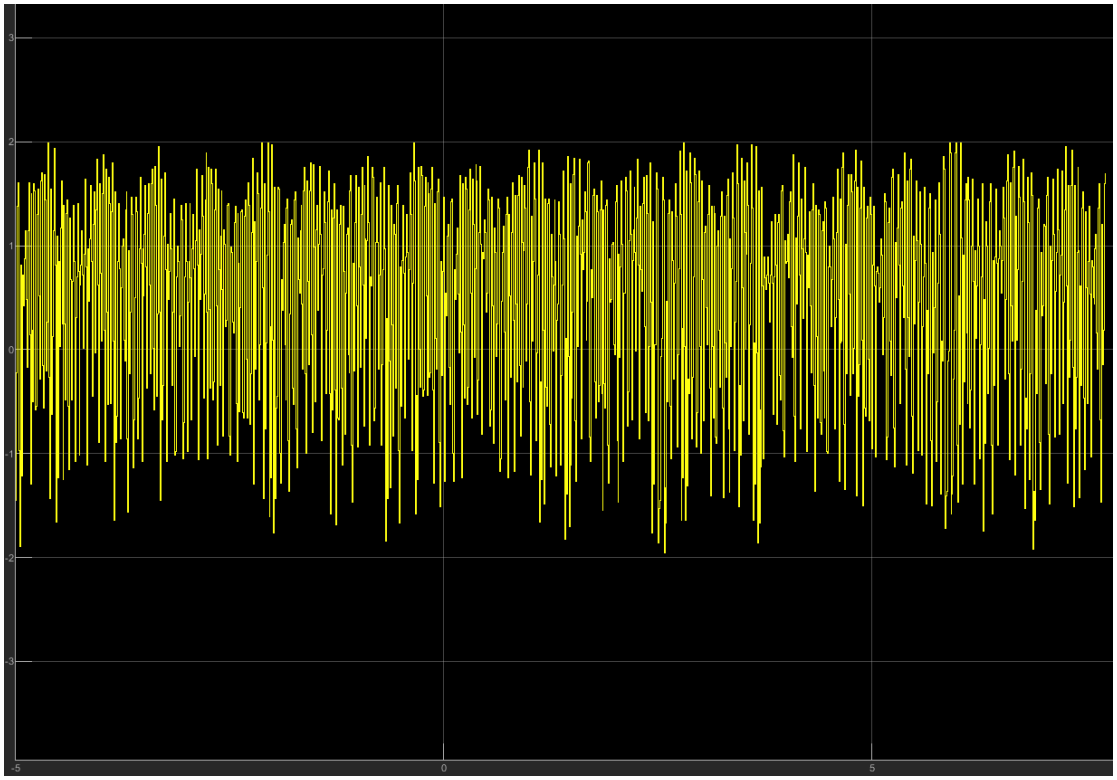


Figure IV-11:Message crypter

IV.4.4 Message récupérer

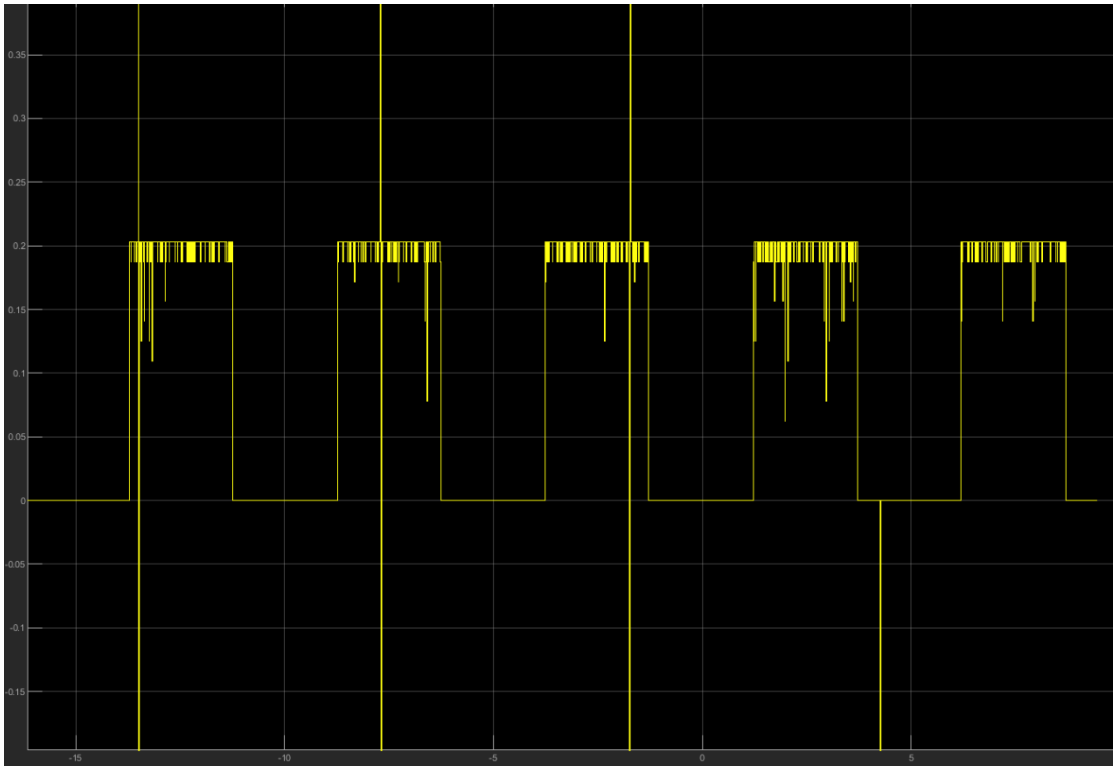


Figure IV-12:Message récupérer

IV.4.5 Message original (signal sinusoïdal)

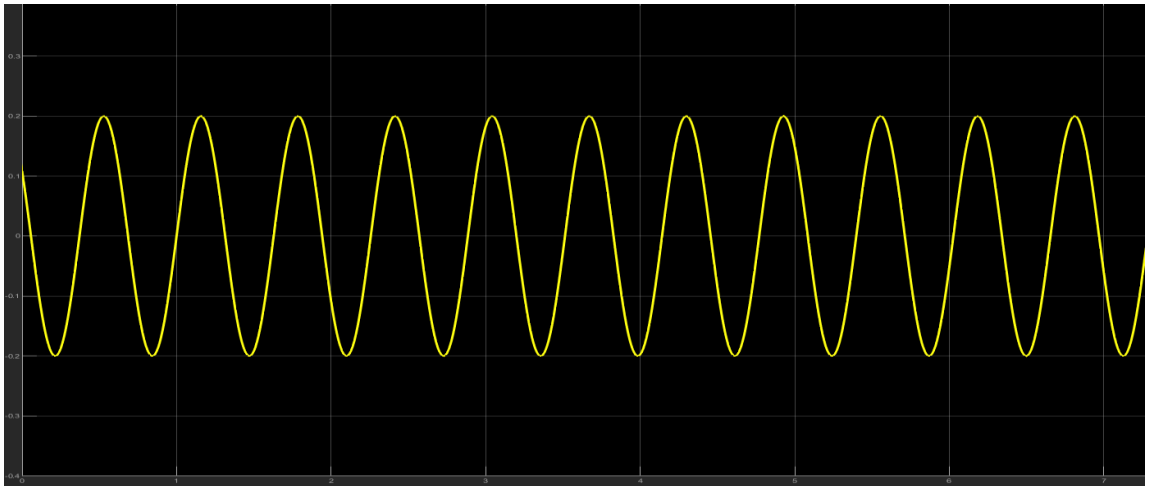


Figure IV-13:Message original

IV.4.6 Message récupérer

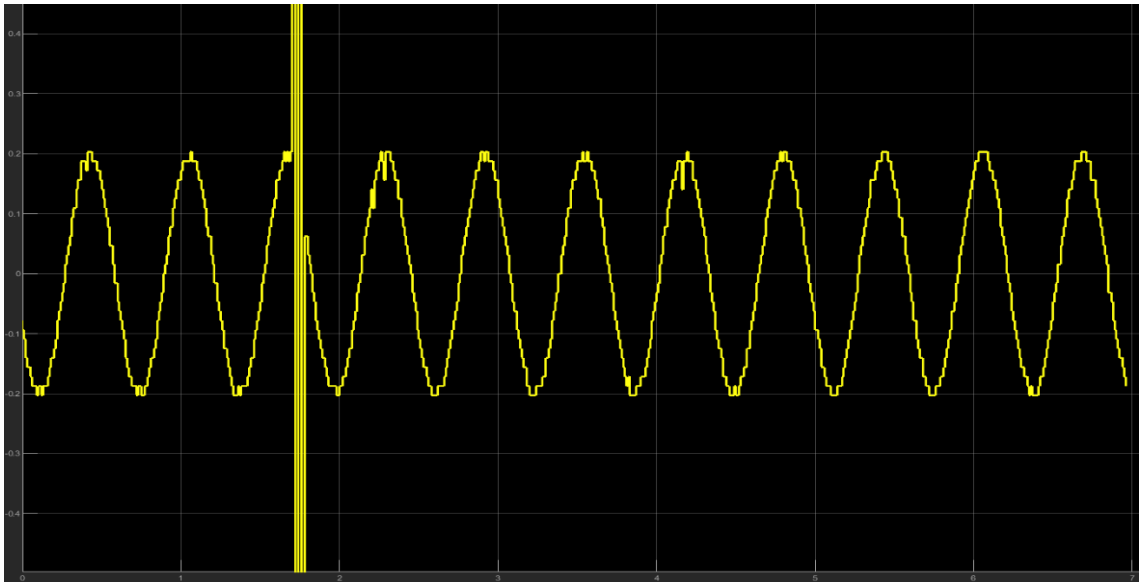


Figure IV-14:Message recuperer

IV.4.7 L'erreur $m(k) - \hat{m}(k)$

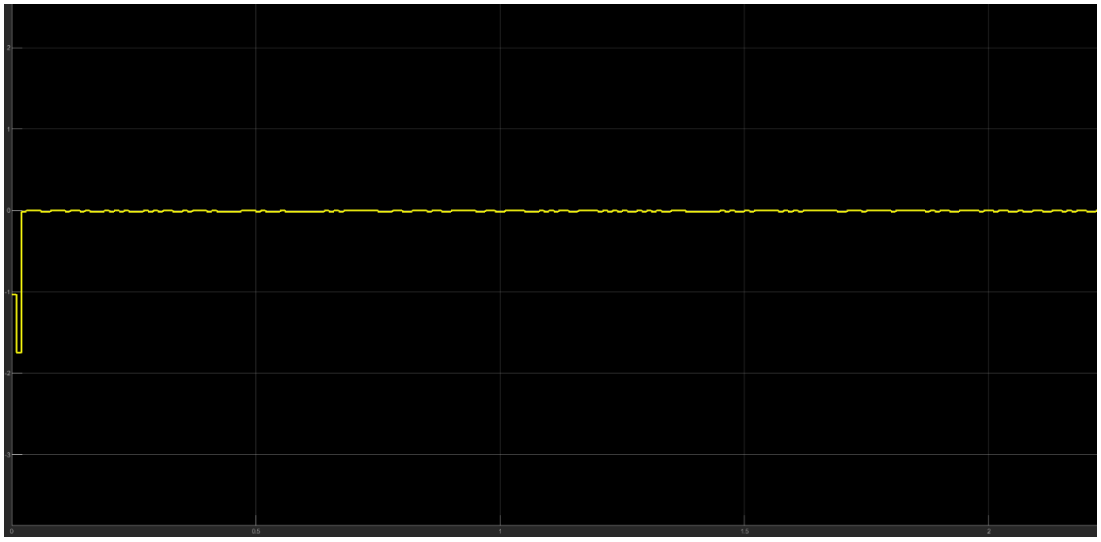


Figure IV-15:l'erreur m(k)-m'(k)

Observation : d'après les **figures 13** et **14** on a constaté que le message envoyer a bien était récupérer cela montre que la synchronisation qu'on a étudiée et réaliser à bien fonctionner.

IV.5 Implémentation de système de synchronisation retardée

IV.5.1 Emetteur :

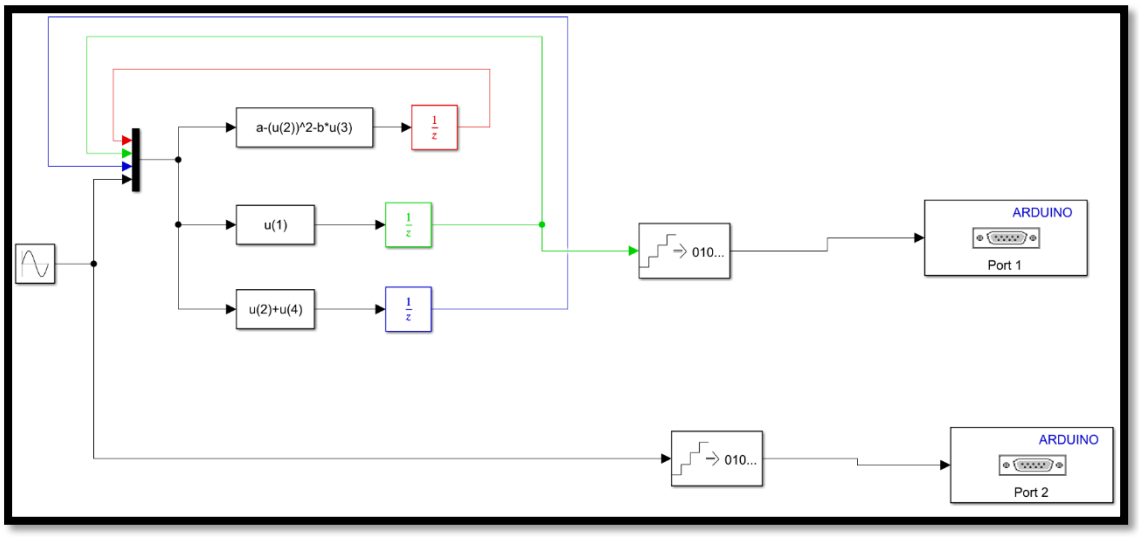


Figure IV-16:schéma Simulink d'emetteur

On va prendre le message un signal sinusoïdal de période 10hz et une amplitude de 1.

IV.5.2 Récepteur :

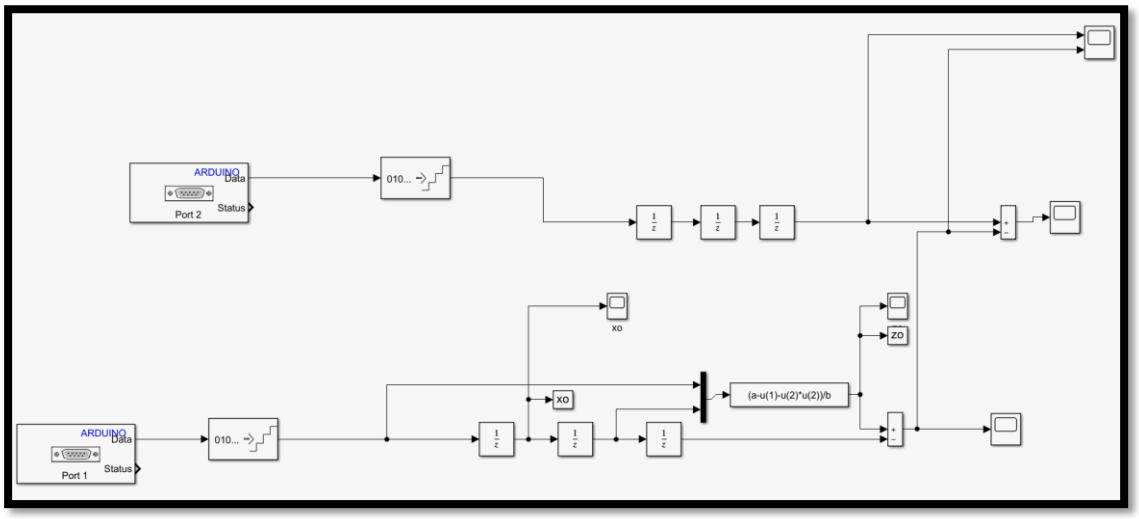


Figure IV-17:schéma Simulink de récepteur

IV.5.3 Visualisation des signaux

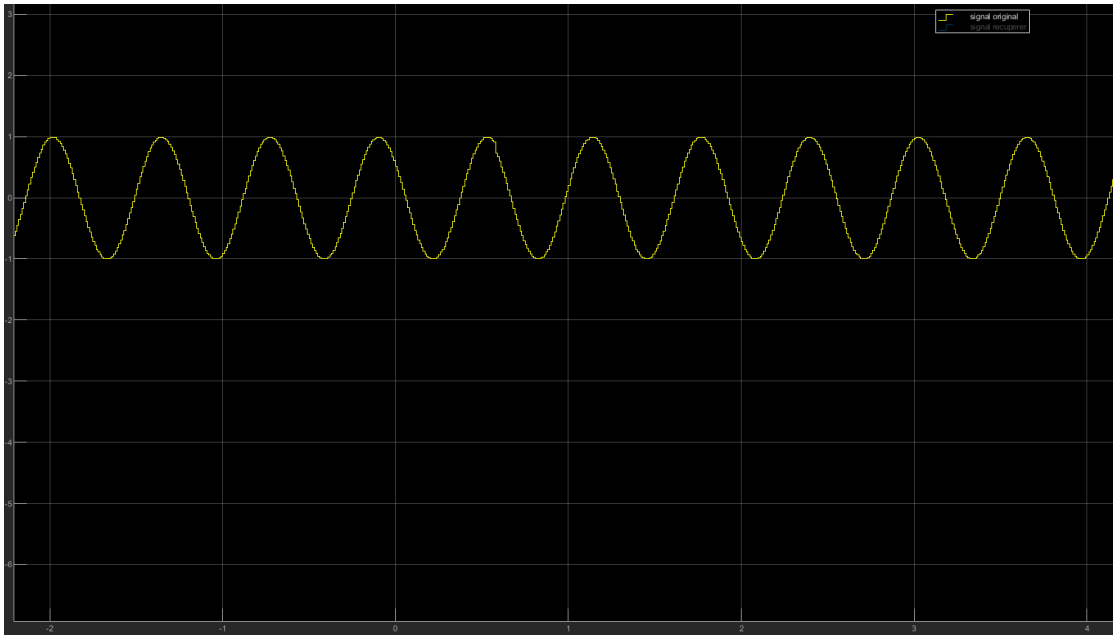


Figure IV-18:Signal original

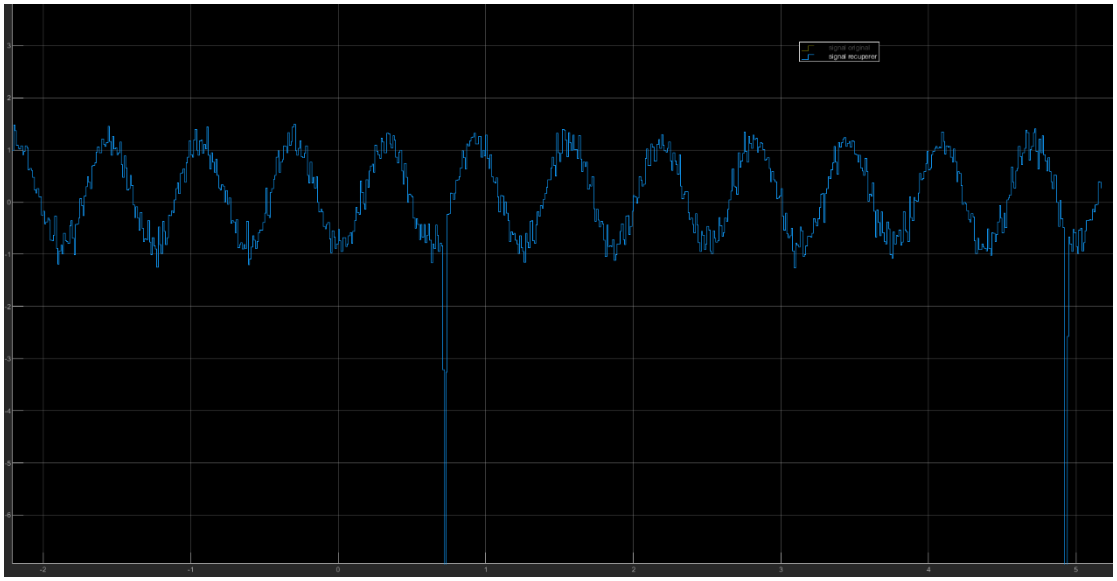


Figure IV-19:Signal récupérer

IV.5.4 Comparaison du signal récupérer et le signal original

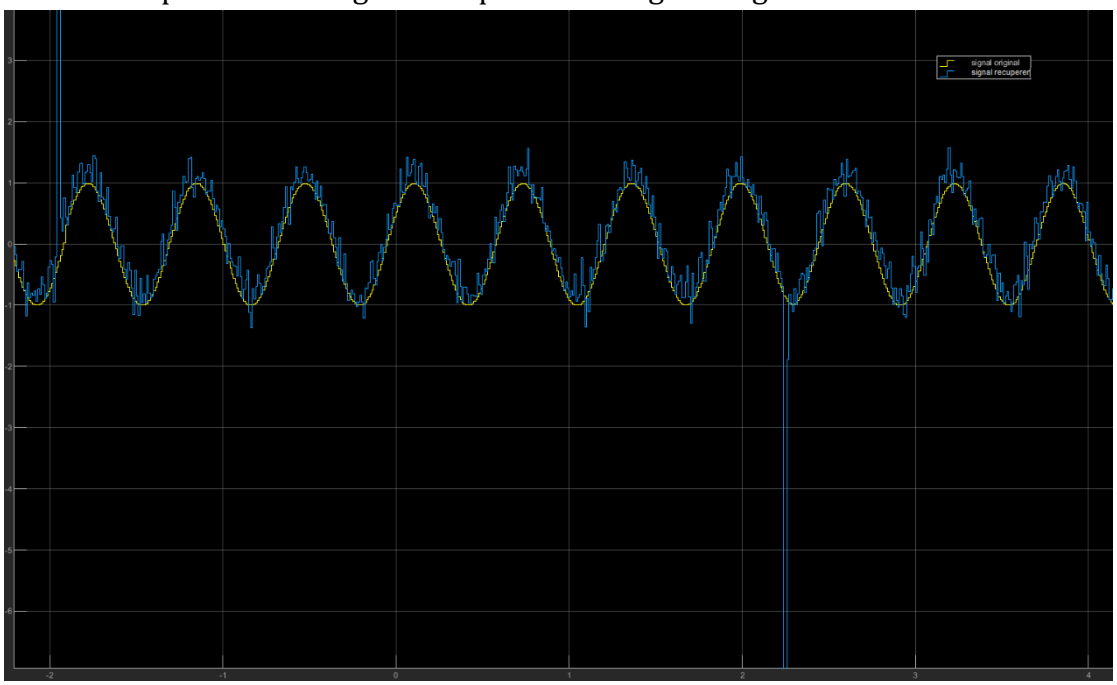


Figure IV-20:comparaison des signaux

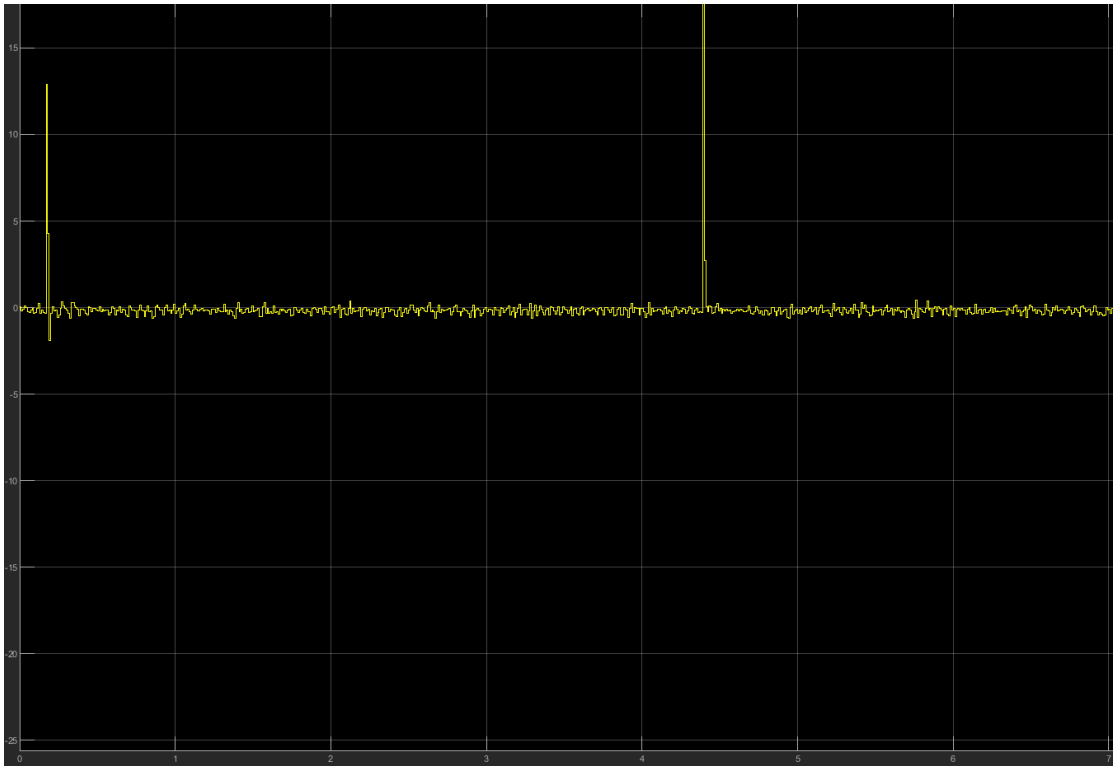


Figure IV-21:Erreur de synchroniation

Observation : d'après les **Figures IV-22** ***et IV-23*** on constaté que le message envoyé a bien était récupére cela montre que la synchronisation retardé qu'on étudié et réaliser a bien fonctionné.

IV.6 Conclusion

En début de ce chapitre les étapes d'installation et la mise en fonction des carte Arduino à l'aide de logiciel Matlab Simulink ont été expliquer.la programmation des deux cartes Arduino au tant qu'émetteur et récepteur hyper chaotique a été fait.et nous avons visualiser les résultats. Les résultats ont montré que le message est bien récupéré. Enfin on a pu créer un système de transmission base de chaos réaliser pratiquement sur des cartes Arduino.

V. Conclusion générale

Ce mémoire nous a conduit à étudier les systèmes dynamiques chaotique, et mettre en pratique ces notions en programmant un système de transmission hyper chaotique sur des carte Arduino-Méga.

Notre travail présente quelques notions sur le chaos, ainsi que quelques définitions importantes, les deux classes de systèmes chaotiques et leurs propriétés sont présentées à l'aide d'exemples simulés sous logiciel Matlab Simulink.

Une brève explication des différents scénarios vers le chaos est donnée à la fin du premier chapitre. En expliquant l'intermittence, la quasi-périodicité et le doublement de périodes. Toutes ces notions sont exploitées lorsque le phénomène de synchronisation des systèmes chaotique est abordé. Nous avons introduit la notion de communication sécurisée a base du chaos, les différentes méthodes de synchronisation et schémas de principe, ainsi que les techniques de transmission sécurisée d'information qui repose sur le principe de synchronisation chaotique. Nous avons aussi passé en revue les techniques de cryptage a base du chaos.

Nous avons, ensuite, introduit un nouveau schéma de transmission de données basé sur la synchronisation de deux systèmes chaotiques, celui-ci est simulé sous logiciel Simulink. Le choix de l'émetteur s'est porté sur le système hyper chaotique a temps discret de Hénon-Hieles, tandis que le récepteur n'est autre qu'un observateur discret retardé qui est choisi afin de récupérer les états ainsi que le message du système Hénon modifiée. Le choix de l'observateur s'est fixé après vérification de trois conditions qui permettent la conception de celui-ci.

Le principe de la méthode de transmission est d'inclure le signal du message à envoyer par addition dans le modèle de Hénon modifié. Ceci consiste en l'ajout du message dans l'une des dynamiques de l'émetteur. Des figures illustrant la synchronisation ainsi que les erreurs de synchronisation de tous les états et du message ont été données avec illustration des résultats de simulation. Les résultats de simulation montrent les performances du système de transmission proposé. La synchronisation de deux systèmes s'est produite, et les différents signaux ont été récupérés au niveau de récepteur.

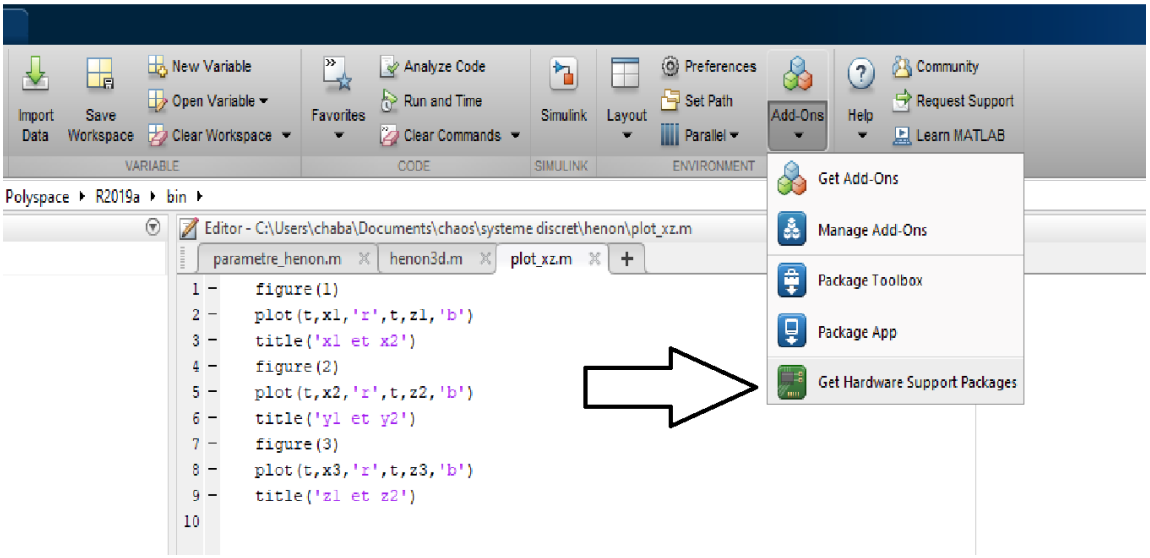
Enfin dans ce travaille la réalisation pratique exposée dans le chapitre 4, s'est faite par des carte Arduino, on a réussi à obtenir des résultats satisfaisants. Nos résultats prouvent que la transmission sécurisée par le chaos étudié par la simulation, fonctionnent en pratique. Ces résultats ouvrent une possibilité de développement de ces méthodes dans le futur.

Annexe

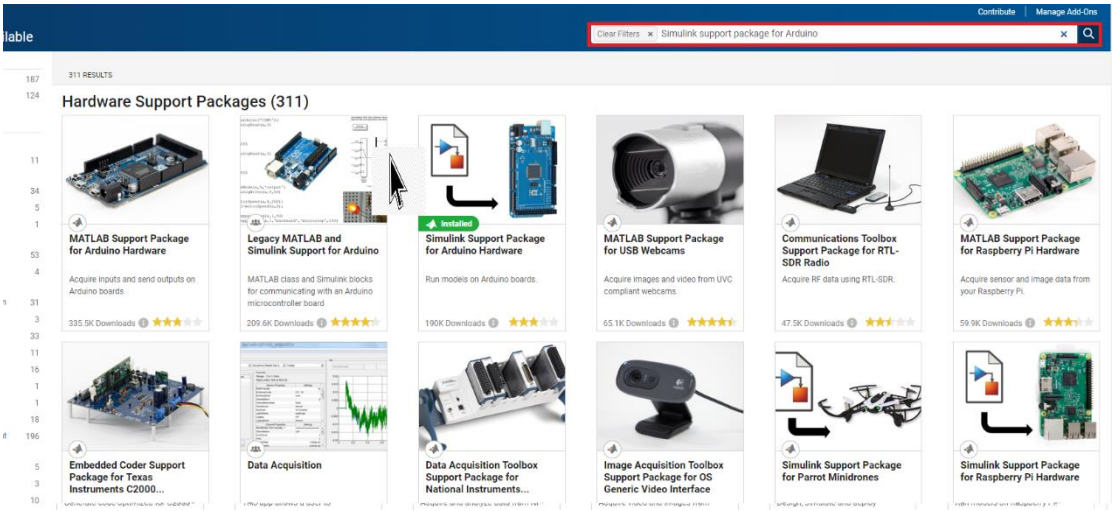
a) L'installation de support Package for Arduino Hardware

L'installation est relativement simple sur les dernières versions de Matlab on prend l'exemple de la version Matlab 2019a :

1) Après le démarrage de Matlab en tant qu'administrateur sur le droit dans l'angle **Add-ons** on sélectionne **Get Hardware Support Package.**



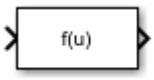
2) Après une page de magasin des extension Matlab s'ouvre, on tape **Simulink Support Package for Arduino Hardware** dans la barre de recherche et on click **search**



3) Après sélectionné Simulink support package est click sur installé.

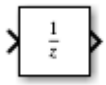
b) Liste des blocs Simulink utilisé

1) Block Simulink standard



Fcn : ce block applique l'expression mathématique spécifiée a son entrée. L'expression peut inclure une ou plusieurs de ses composant :

- **U –** l'entrée du block. Si u est un vecteur, **u(i)** représente l'élément d'ordre i du vecteur ; **u (1)** représente le seul premier élément
- Les constant numérique.
- Les opérateurs numériques.
- Les opérateurs arithmétiques ($\pm * /^{x}$).
- Les opérateur rationnels ($== \rightarrow \leftarrow <> \neq \geq \leq$), l'expression renvoie 1 si la relation est vraie ; sinon elle retourne 0.
- Les opérateur logique (! && ||) l'expression renvoie 1 si la relation est vraie ; sinon elle retourne 0.
- Parenthèses
- Les fonctions mathématiques et **tanh.**



Unit Delay : Ce block retarde l'entrée durant une période spécifiez. Ce bloc est équivalent au z^{-1} opérateur a temps discret. Chaque signal peut être un scalaire ou un vecteur. Si l'entrée est un vecteur. Le bloc retarde tous les éléments du vecteur durant la même période.

Mux : Le bloc multiplexeur combine en une sortie unique plusieurs entrés. Une entrée peut être un signal scalaire ou vectoriel, toutes les entrées doivent être du même type de données numérique.

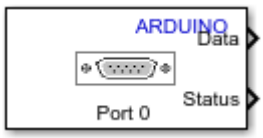
Sum : Le bloc **Sum** effectue une addition ou une soustraction sur ses entrées. Ce bloc peut sommer ou soustraire des scalaire, vecteur, ou les éléments de matrice. Il peut aussi inverser les éléments d'un signal.

Pulse Generator : ce bloc génère des impulsions carrées a intervalles réguliers. Les paramètres de forme d'onde du bloc. **Amplitude, Largeur d'impulsion, période, et retard de phase,** permettant de déterminer la forme d'onde de sortie. Le schéma suivant montre comment chaque paramétré affecte la forme d'onde.

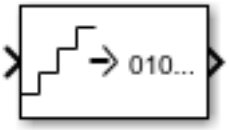
Sin Wave : : ce bloc génère un signal sinusoïdal avec une période fixé. Les paramètres de forme d'onde du bloc. **Amplitude, période, et retard de phase,** permettant de déterminer la forme d'onde de sortie.

2) Block Arduino support package

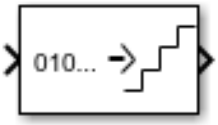
Arduino Serial Transmit TX : Envoyer des données mises en mémoire tampon sur le port série spécifié, le bloc accepte des données sous forme de vecteur ou scalaires **uint8**.



Arduino Serial Receive RX : reçois un octet de données par période de la mémoire tampon du port série spécifié, le bloc dispose de deux sorties Data et Statu, la sortie Statu se met a 1 lorsqu'une donnée et disponible sur la sortie Data.



Uniforme encoder : Ce bloc effectue les deux opérations suivantes sur chaque échantillon d'entrée ou matrice, quantifie la valeur avec la même précision et encode la valeur à virgule flottante quantifié à une valeur entière.



Uniforme decoder : fait l'opération inverse de Uniform Encoder et reconstruit, quantifiés les valeurs à virgule flottante à partir de l'entrée entière codé, Les entrées peuvent être des valeurs réelles ou complexes, les types de données traiter **(uint8, uint16, uint32, int8, int16, ou int32).**

Bibliographie

- [1] Megherbi Ouerdia, réalisation d'un système sécurisé à base de systèmes chaotique, mémoire de Magister en automatique, Université Mouloud Mammeri Tizi-Ouzou, Algérie,2013
- [2] David Ruelle, Chaos, imprédictibilité et hasard, conférence de vulgarisation donnée en 2000 par l'auteur à l'Université de tous les savoirs, puis publiée dans : Qu'est-ce que l'Univers ? (Éd. Y. Michaud), Odile Jacob (2000), 647-656.
- [3] O. E. Rössler, « An Equation for Continuous Chaos », Physics Letters, vol. 57A, no 5, 1976, p. 397–398.
- [4] Ouahabi Rabiaa, Système dynamique et chaos : diffèrent méthodes de contrôle et synchronisation, thèse de Doctorat en science, Université frères Mentouri - Constantine 1,2018
- [5] Dang-Vu, H and Delcarte, C, "Bifurcations et chaos : une introduction à la dynamique contemporaine avec des programmes en Pascal, Fortran et Mathematica, *« Markéting*, Paris : Ellipses Ed, 2000. 24, 27, 53
- [6] Berger, P and Pomeau, Yves and Vidal, Charles, "L'ordre dans le Chaos : Vers une Approche Déterministe de la Turbulence, *« Paris : Hermann*, 1984. 27
- [7] N, Lorenz. E. The Essence of Chaos. University of Washington Press, 1993.
- [8] R. A. Essedik, *observateur à mode glissant d'ordre suppérieur et inversion à gauche,* Université de Tlemcen, 19 mai 2013.
- [9] L. Larger, *Cryptographie par chaos à l'aide des dynamiques non linéaires à retard,* FrancheComté .
- [10] S.Allouache, N.Hamma, Conception d'un système de transmission de données à base de système chaotiques. Mémoire de Master automatique option commande des systèmes, Université Mouloud Mammeri de Tizi-Ouzou, Algerie,2015.
- [11]T.Nessrine, H.imene, Transmission sécurisée par synchronisation d'un système chaotique Hyperjerk, Mémoire de Master Instrumentation, Université Saad Dahleb Blida, Algerie,2020.
- [12] N. S. Boukhalfa, *Synthése d'observateurs non linéaires.*
- *[13]* **Oppenheim, A.V., Cuomo, K.M., Strogatz, S.H.** (1993), "Synchronization of lorenz-based chaotic circuits with applications to communications," IEEE Trans. on Circ. Syst. II, Vol.40(10), pp. 626–633.
- *[14]* **Kevin, M.S., Cuomo, Oppenheim, A.V.** (1993), "Circuit implementation of synchronized
  chaos with applications to communications," Phys. Rev. Lett., Vol. 71.
- *[15]* **Kevin, M.S.** (1996), "Unmasking a modulated chaotic communications scheme," Int. J.Bifurcation Chaos, Vol. 6, pp. 367-375.
- *[16]* F. Anstett.Les systèmes dynamiques chaotiques pour le chiffrement synthèse et cryptanalyse.2006.
- [17]H.Hamiche, K.Hannoun, S.Guermah, R.Saddaoui, M.Laghrouche, Analysis and implementation of a novel robust transmission scheme for private digital communications,
- [18] L.M. Pecora and T.L. Carrol, «Synchronization in Chaotic systems», Phys, Rev. Lett, vol. 64, pp. 973977,1992.

- [19] Djemaï, M., Barbot, J.P., Belmouhoub, I.: Discrete-time normal form for left invertibility problem. Eur. J. Control 15, 194–204 (2009)
- [20] I. Belmouhoub, M. Djemai et J.P. Barbot, “Observability quadratic Normal Form for Discrete-Time systems”. IEEE Transactions on Automatic Control, vol. 50, Juilliet 2005.