MINISTÈRE DE L'ENSEIGNEMENT SUPÉRIEURE ET DE LA RECHERCHE SCIENTIFIQUE
UNIVERSITÉ MOULOUD MAMMERI DE TIZI-OUZOU
FACULTÉ DE GÉNIE ÉLECTRIQUE ET INFORMATIQUE
DÉPARTEMENT AUTOMATIQUE

THÈSE DE DOCTORAT

Spécialité : AUTOMATIQUE

Présentée et soutenue publiquement par :

Hamid HAMICHE

Ingénieur en Electronique, UMMTO

Magister en Automatique, UMMTO

Thème

Inversion à Gauche des Systèmes Dynamiques Hybrides Chaotiques. Application à la Transmission Sécurisée de Données

*Thèse soutenue le **/**/2011 devant le jury composé de MM :*

Moussa DIAF	*Professeur, Université de Tizi-Ouzou*	Président
Saïd DJENNOUNE	*Professeur, Université de Tizi-Ouzou*	Rapporteur
Jean-Pierre BARBOT	*Professeur, ENSEA, Cergy-Pontoise, France*	Co-Rapporeur
Mohammed Seghir BOUCHERIT	*Professeur, Ecole Nationale Polytechnique d'Alger*	Examinateur
Djamila BENMERZOUK	*Professeur, Université de Tlemcen*	Examinatrice
Salah HADDAB	*Maître de Conférences A, Université de Tizi-Ouzou*	Examinateur
Malek GHANES	*Maître de Conférences, ENSEA, Cergy-Pontoise, France*	Invité

Avant propos

Je tiens à exprimer ma profonde gratitude et mes remerciements les plus sincères à M. Saïd Djennoune, Professeur à l'université Mouloud Mammeri de Tizi-Ouzou, sous la direction duquel j'ai eu le plaisir de travailler. Ses conseils, ses critiques et sa rigueur scientifique m'ont permis de mener ce travail à son terme.

Je tiens particulièrement à remercier mon co-encadreur de thèse, M. Jean-Pierre Barbot, Professeur des universités, et directeur du laboratoire ECS-Lab à l'Ecole Nationale Supérieure de l'Electronique et ses Applications de Cergy-Pontoise pour avoir accepté de m'accueillir dans son équipe ECS-Lab. Par sa compétence, ses conseils, ses critiques et sa entière disponibilité, il a joué un rôle déterminant dans le développement de mes recherches. Ce travail est le résultat de notre collaboration qui a toujours été agréable et enrichissante. Qu'il trouve ici l'expression de ma profonde reconnaissance.

Mes grands remerciements vont également à M. Malek Ghanes, Maître de Conférences à l'Ecole Nationale Supérieure de l'Electronique et ses Applications de Cergy-Pontoise, et membre de l'ECS-Lab, pour avoir co-encadré avec Jean-Pierre Barbot mes travaux de recherche et pour ses conseils judicieux et nos discussions fructueuses, ainsi que pour sa disponibilité et son soutien permanent.

J'exprime mes sincères remerciements à M. Moussa Diaf, Professeur à l'université Mouloud Mammeri de Tizi-Ouzou, qui m'a fait l'honneur de présider le Jury de cette thèse.

Je suis honoré de la présence dans ce Jury de M. Mohammed Seghir Boucherit, Professeur à l'Ecole Nationale Polytechnique d'Alger, de Djamila Benmerzouk, Professeur à l'université Abou-Bakr Belkaïd de Tlemcen, de Salah Haddab, Maître de Conférences A à

l'université Mouloud Mammeri de Tizi-Ouzou, et de l'intérêt qu'ils ont porté à ce travail. Qu'ils trouvent ici l'expression de mon profond respect.

J'adresse mes vifs remerciements à mon ami Karim Kemih, Maître de Conférences A à l'université de Djidjel pour son soutien, son aide précieuse et surtout de sa compétence.

Je remercie sincèrement mes collègues de la Faculté du Génie Electrique et Informatique en particulier : M. Ahmed Maïdi, M. Kamal Bennamane, M. Redouane Kara, M. Kamal Hammouche, M. Mourad Lahdir M. Rabah Mellah ainsi que tous mes collègues du laboratoire L2CSP pour leur soutien permanent et leurs encouragements.

Mes sincères remerciements vont aussi aux membres de l'Equipe Commande des Systèmes de l'E.N.S.E.A en particulier : Achour Ouslimani, Mohammed Djemaï, Sid Ahmed Raka et François Caudron sans oublier l'ingénieur du Laboratoire Jean-Pierre Bennoiton pour leur soutien et leurs encouragements.

Je remercie tous ceux qui de près ou de loin ont contribué à la réalisation de cette thèse.

Enfin pour avoir cru en moi, j'exprime ma profonde gratitude à ma femme Naïma, à toute ma famille et à tous mes amis(es) ; ce modeste travail leur est dédié.

Table des matières

Table des figures

Notations

Ensembles

- $\mathbb{R}$ (resp. $\mathbb{R}^+$) : ensemble des nombres réels (resp. réels positifs ou nuls).
- $\mathbb{R}^n$: espace vectoriel de dimension n construit sur le corps des réels.
- $L_f^i h$: ième dérivée de Lie de h dans la direction de f.
- $dL_f^i h$: le différentiel de $L_f^i h$.
- $\mathbb{N}$: ensemmble des nombres entiers naturels.
- $\mathbb{N}^*$: ensemmble des nombres entiers naturels non nuls.
- $C^k(\mathbb{R}^n, \mathbb{R}^m)$: ensemble des fonctions k fois continûment différentielles de $\mathbb{R}^n$ dans $\mathbb{R}^m$.
- $L_f \lambda(x) = \sum_{j=1}^{n} \frac{\partial \lambda}{\partial x_i} f_i(x)$: la dérivée de λ long de f.

Matrices et normes

- $M > 0$ ($M \geq 0$) : Matrice M symétrique définie (resp. semi-définie) positive.
- $M < 0$ ($M \leq 0$) : Matrice M symétrique définie (resp. semi-définie) négative.
- I_s (I) : Matrice identité de dimension $s \times s$ (resp. appropriée).
- M^T : Transposée de la matrice M.
- M^{-1} : Inverse de la matrice M.
- $\lambda_{min}(M)$ (resp. $\lambda_{max}(M)$) : Valeur propre minimale (resp. maximale) de M.
- $||x||$: Norme euclidienne du vecteur x.

Acronymes

DES : Data Encryption Standard

RSA : Rivest Shamir Adleman

Introduction générale

La théorie de l'estimation tient une place de plus en plus importante en Automatique [30], [6]. La connaissance de l'état du système étudié est nécessaire dans de nombreuses stratégies, notamment de détection de défauts, de diagnostic, de commande. Lorsqu'il n'est pas possible de mesurer directement l'état, et ce pour des raisons physiques ou économiques, on a recours à un système dynamique auxiliaire, appelé observateur, qui est chargé d'estimer l'état du système. La construction d'un observateur en temps continu ou en temps discret se décompose en deux phases, à savoir une phase de synthèse, ou de conception, qui consiste à choisir la dynamique de l'observateur, et une phase d'analyse de la convergence de l'état de l'observateur vers l'état du système. La synthèse de l'observateur exploite les informations disponibles, à savoir le modèle dynamique du système étudié, ses entrées et ses sorties mesurées. Lorsqu'une partie (ou la totalité) des entrées n'est pas disponible, l'observateur est dit à entrées inconnues. Le problème à résoudre devient alors plus complexe, puisqu'il s'agit soit d'estimer l'état du système, malgré la présence d'entrées qui interviennent effectivement dans la dynamique du système mais que l'on ne peut pas inclure dans la dynamique de l'observateur, soit d'estimer l'état et les entrées inconnues également. Tous ces observateurs dépend de plusieurs conditions : la condition d'observabilité pour retrouver les états du système ; la condition de recouvrement de l'observabilité ("observability matching condition") pour retrouver les états du système et l'information noyée dans le système (inversibilité à gauche du système). Les observateurs à entrées inconnues interviennent dans le domaine du diagnostic, pour la détection de défauts et la transmission sécurisée de données.

Mais, ces dernières années, des efforts particuliers de recherches se sont intéressés à l'étude des systèmes hybrides. Ces recherches sont motivées non seulement parce que beaucoup de systèmes réels s'avèrent exhiber des comportements hybrides, mais également parce que la commande de beaucoup de systèmes complexes est seulement possible

par l'intermédiaire de combinaison des lois de commande continues classiques avec une logique de surveillance discrète. De ce fait, les systèmes hybrides sont un concept rigoureux pour modéliser les systèmes complexes. Ils sont notamment employés dans le but de fournir des modèles reflétant mieux la nature des problèmes de commande. Leurs propriétés théoriques sont toujours le sujet de recherches intenses. Parmi les problèmes à traiter, celui de l'observation est particulièrement important pour le contrôle. En effet, de nombreuses méthodes de commande des processus sont élaborées à partir de la connaissance de l'état du système. En général, seules les variables d'entrée et de sortie sont connues. Il est alors nécessaire, à partir de ces informations de reconstruire l'état du modèle choisi afin d'élaborer la commande. Bien que la théorie de l'observation d'état ait atteint une certaine maturité dans les domaines des systèmes continus et des systèmes à événements discrets, beaucoup de points méritent d'être approfondie sur le concept de l'observabilité et de la synthèse d'observateurs hybrides : l'identifiabilité et l'inversion à gauche appliquée en particulier à la transmission sécurisée de données.

En effet, la cryptographie joue un rôle important dans la sécurité et la fiabilité des systèmes de transmission de données. Avec le développement du commerce électronique, les utilisateurs ont besoin d'authentifier et protéger des données sensibles dans leurs ordinateurs et de garantir la confidentialité des transactions sur des réseaux publics tels que l'Internet. En général, un "crypto" système ou cryptosystème doit considérer plusieurs aspects, tels que l'intégrité des données, l'authentification, l'autorisation et la confidentialité. Les techniques de cryptographie classiques sont basées sur la théorie des nombres, et en particulier sur la décomposition d'un entier en éléments simples, en utilisant l'algorithme symétrique *DES* [5] et l'algorithme asymétrique *RSA* [11]. L'algorithme *DES* est particulièrement utilisé dans le domaine des transactions bancaires : il est employé pour crypter les opérations sur un compte bancaire et les codes de cartes dans les guichets automatiques.

Le *DES* est un algorithme de cryptage extrêmement sûr : il est particulièrement difficile, voire impossible, de trouver la clé à partir de textes cryptés (même en disposant du texte en clair correspondant). On peut noter que la sécurité réside dans la clé et pas dans la fonction de cryptage. Par conséquent, le problème principal est l'échange de clés : l'émetteur doit transmettre l'unique clé au récepteur sans qu'elle soit interceptée, sinon le cryptage n'a plus aucun intérêt.

L'algorithme le plus répandu est l'algorithme *RSA*. Il a été inventé en 1978 par R. Rivest, A. Shamir et L. Adleman. Il est fondé sur les propriétés des nombres premiers. Le principe est simple : on choisit deux nombres premiers p et q au hasard. On calcule $n = pq$ et $z = (p-1)(q-1)$. On choisit un nombre d premier avec z, et on cherche e tel que $ed \equiv 1[n]$. Le couple (e, n) constitue la clé publique, (d, n) la clé privée. La fonction de cryptage est la multiplication par e modulo n, la fonction de décryptage est la multiplication par d modulo n. La connaissance de n donne théoriquement accès à p et q qui sont par définition les facteurs premiers de n. La force de la technique *RSA* repose sur l'extrême difficulté à factoriser de grands nombres. Mais le développement de la puissance de calcul des ordinateurs et l'utilisation du parallélisme améliorent sans cesse les temps de factorisation. Le choix d'une longueur de clé (la taille de n) est directement lié au niveau de confidentialité recherché. En contrepartie, l'algorithme *RSA* est très lent, ce qui n'est guère pratique pour les fichiers volumineux : plus la clé est grande, plus les processus de cryptage et de décryptage sont longs. Cette technique est donc réservée aux messages courts.

Pour ces raisons, plusieurs chercheurs ont essayé de mettre en oeuvre d'autres cryptosystèmes. Ainsi, au cours de ces dernières décennies, la théorie des systèmes non linéaires chaotiques a été appliquée à la cryptographie afin d'augmenter le degré de sécurité. Les systèmes chaotiques constituent une classe de systèmes non linéaires au comportement très complexe restés méconnus jusqu'au 20 ième siècle. Henri Poincaré [5] fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème d'interactions de trois corps célestes. Plus tard, en 1960, les travaux de Edward Lorenz [30], passionné de météorologie, ont changé le cours de cette branche des mathématiques. Il a mis en évidence une propriété de certains systèmes non linéaires : d'infimes différences dans les conditions initiales finissent par engendrer des comportements très éloignés. Comme la plupart des systèmes physiques sont non linéaires, la découverte de Lorenz est d'une importance cruciale : certains phénomènes non linéaires sont si sensibles aux conditions initiales, bien qu'étant régis par des lois rigoureuses et parfaitement déterministes, que toute prévision de leur comportement est impossible. Ce phénomène, qui traduit cette sensibilité aux conditions initiales, est connu sous le nom d'effet papillon. Le battement d'ailes d'un papillon, aujourd'hui à Pekin, engendrerait une tempête, le mois prochain à New York.

Grâce aux propriétés naturelles des systèmes chaotiques, telles que leur sensibilité aux conditions initiales et le fait qu'ils évoluent dans une large bande de fréquence, les systèmes chaotiques sont devenus de bons candidats pour la cryptographie.

L'idée d'utilisation du chaos dans les systèmes de communication a été inspirée de la découverte de Pecora-Carroll en 1990 [126]. Ils ont montré que deux systèmes chaotiques identiques avec des conditions initiales différentes peuvent éventuellement se synchroniser s'ils sont couplés d'une certaine manière convenable, c'est à dire sous certaines conditions. Le développement des systèmes de communication utilisant le chaos a commencé donc avec des schémas de synchronisation très simples de circuits électroniques, visant pour le cryptage et la reconstruction simultanés d'un signal d'information. Par la suite, de nombreuses techniques de cryptage par addition, par commutation, par modulation, etc, ont été mises au point pour inclure le message clair dans un signal porteur chaotique, voire dans la dynamique même de l'émetteur. Par un processus de synchronisation, le récepteur est capable d'estimer l'état de l'émetteur, puis d'effectuer le décryptage du message crypté.

Il est bien connu que les systèmes de communication traditionnels comportent deux parties, respectivement appelées émetteur et récepteur. Le signal de sortie de l'émetteur est modulé et transmis par le canal public au récepteur qui démodule le signal reçu afin de récupérer le signal original. La récupération du message est soumise à une condition essentielle. Cette condition se traduit par le rapport signal utile sur signal transmis qui doit être le plus proche possible de l'unité.

Il existe deux types de récupération de signal : la démodulation cohérente et la démodulation non cohérente. La récupération de message par une démodulation non cohérente emploie des attributs statistiques du signal transmis pour reconstruire le message. Ainsi, la récupération de ce dernier n'est pas directement en fonction du système chaotique.

Pour la cryptographie chaotique, un des concepts les plus importants de démodulation cohérente est la synchronisation, c'est à dire que le récepteur essaie de reconstruire les états de l'émetteur à partir du signal transmis considéré comme la sortie du système à observer et ensuite de récupérer le message crypté considéré comme une entrée inconnue. Du point de vue de l'automatique, cette technique peut être classée dans le domaine de la conception d'observateurs [115].

Même si les techniques de cryptage par le chaos sont en plein essor, des attaques

spécifiques ont été développées en parallèle, ouvrant ainsi une nouvelle voie dans la cryptanalyse, qui s'oppose à la cryptographie, et qui désigne l'art de déchiffrer un message sans la clé de cryptage. Par conséquent, la proposition d'une nouvelle façon de transmettre un message, en exploitant la synchronisation et les propriétés des systèmes chaotiques, doit s'accompagner d'une réflexion sur la sécurité du processus.

Les travaux que nous avons réalisés dans cette thèse s'inscrivent dans ce contexte particulier. Notre objectif est de proposer un nouveau système de transmission sécurisé robuste. L'émetteur est composé principalement d'un système chaotique en temps continu dit oscillateur de Colpitts et d'un système chaotique en temps discret dit de Hénon modifié. Dans le but de rendre la structure de l'émetteur plus complexe (ce qui est favorable dans le cas d'une transmission sécurisée), des états du système en temps continu sont introduits dans la dynamique du système en temps discret. Ainsi, le nouveau système obtenu est hybride. Le récepteur est composé d'un observateur en temps continu et d'un observateur en temps discret. De la même façon, pour avoir un observateur hybride, des états échantillonnés de l'observateur en temps continu sont introduits dans la dynamique de l'observateur en temps discret. Ceci constitue notre première contribution dans cette thèse, car l'identifiabilité et la conception d'observateurs pour ces systèmes sont difficiles et restent des problèmes ouverts (toujours d'actualité). La sortie transmise au récepteur est composée d'un signal de synchronisation issu du système continu et d'un signal utile qui contient le message issu du système hybride. La reconstitution des états, ainsi que le message de l'observateur hybride, passe par la synchronisation des deux systèmes chaotiques en temps continu (émetteur et récepteur) avant la synchronisation des deux systèmes hybrides. Pour reconstruire les états du système en continu, nous allons utiliser la synchronisation impulsive. Cette méthode de synchronisation a montré une grande efficacité dans les applications de communication par le chaos, car elle maintient la synchronisation par des impulsions de petite taille. Par conséquent, elle permet d'économiser la capacité du canal de communication pour la transmission des messages secrets. En outre, puisque ces impulsions sont à temps discret, la redondance des informations de synchronisation dans le canal sera réduite, ce qui augmente la sécurité du système de communication. Ensuite, nous effectuons une étude sur la cryptanalyse du système de transmission. Dans ce travail de thèse, nous montrons que les paramètres du système hybride obtenu peuvent être identifiés lorsque les textes clairs sont connus. Dans le but d'augmenter la difficulté

d'identification des paramètres du système de transmission afin, de rendre le système de transmission robuste, des états du système en temps continu de l'émetteur sont d'abord retardés, ensuite échantillonnés avant d'être introduits dans la dynamique du système hybride. Ceci constitue notre deuxième contribution dans ce travail de thèse, car les systèmes retardés en temps continu sont de dimension infinie, contrairement aux systèmes à temps discrets. Avec cette stratégie, ces retards qui jouent le rôle de clés secrètes supplémentaires augmentent la complexité d'identifier, d'observer et de contrôler cette classe de systèmes [134]. Plusieurs valeurs sur les retards des états du système en temps continu impliqueraient autant de système en temps discret. Enfin, nous montrons que la méthode proposée présente l'avantage que les deux systèmes en temps continu peuvent se resynchroniser en cas de perte de synchronisation.

Cette thèse est organisée de la façon suivante :

Le chapitre 1 est consacré à la théorie de la synchronisation des systèmes chaotiques. Dans cette partie, quelques méthodes de synchronisations chaotiques sont présentées. Ensuite, nous appliquons deux méthodes de synchronisation sur un nouveau système chaotique.

Dans le chapitre 2, nous proposons une nouvelle méthode adaptée à la transmission sécurisée de données. Ici, nous commençons par la présentation de l'émetteur qui est constitué principalement d'un système chaotique en temps continu et d'un système chaotique hybride.

Dans le chapitre 3, nous présentons le récepteur du système de transmission sécurisé. Dans cette partie, nous présentons deux observateurs dont le premier a pour rôle de récupérer les états du système chaotique en temps continu et le second de récupérer les états ainsi que le message du système chaotique hybride.

Le chapitre 4 est dédié à la présentation des résultats de simulation. Ce chapitre est subdivisé en deux parties : La première concerne la présentation des simulations numériques dans le cas de l'application de la méthode pour la transmission sécurisée d'un signal et la seconde pour la transmission d'une image.

Le chapitre 5 est consacré à l'étude de la cryptanalyse et de l'identifiabilité du système de transmission proposé. Dans ce chapitre, nous effectuons le test de robustesse du système de transmission proposé.

La thèse se termine par une conclusion et quelques perspectives.

Chapitre 1
Synchronisation des systèmes chaotiques

Chapitre 1

Synchronisation des systèmes chaotiques

1.1 Introduction

Le phénomène de synchronisation a été étudié depuis longtemps. Au 17 ième siècle, Huygens (1629-1695) remarqua ce phénomène en étudiant deux horloges de fréquences légèrement différentes. Il constata qu'en les reliant l'une à l'autre avec un morceau de bois, elles affichaient toutes les deux la même heure : elles se synchronisaient. Des exemples de synchronisation existent dans la nature, dans le domaine de la science de la vie et de la terre, ainsi que dans les domaines techniques. En neurobiologie, la notion de synchronisation apparaît pour expliquer le fonctionnement du cerveau : chaque activité est produite par un ensemble de neurones dont les signaux électriques oscillent de manière synchrone [59].

Dans le domaine des communications, les procédés utilisés pour transmettre l'information sous forme numérique exigent, en général, un synchronisme précis entre certaines fonctions du récepteur et les fonctions correspondantes de l'émetteur. Par "synchronisme", on entend que les générateurs rythmant les deux fonctions associées doivent avoir la même fréquence nominale et présenter un déphasage constant et bien déterminé.

Si, par exemple, on utilise une transmission synchrone en bande de base [73], le récepteur identifiera chacune des données binaires en échantillonnant le signal transmis, à un instant bien déterminé de l'intervalle de temps attribué à cette donnée. Le générateur commandant l'échantillonnage doit être synchrone de l'horloge "bit" qui, dans l'émetteur,

commande la sortie des données. Dans le cas où l'information est organisée en mots, dont le rythme d'émission est fixé par une horloge particulière, il faudra disposer également, dans le récepteur, d'un générateur synchrone de cette horloge "mot".

Lorsque la transmission fait appel à une modulation [73], un autre type de synchronisme peut être nécessaire. Il existe en effet des procédés de démodulation, dits "synchrones", exigeant un signal de référence synchrone de la porteuse utilisée pour la transmission.

Exceptionnellement, un synchronisme de très courte durée peut être obtenu en faisant démarrer le générateur localisé dans le récepteur, avec une phase initiale et une fréquence correcte. C'est le cas du dispositif d'identification des bits en transmission asynchrone [73], dans lequel le synchronisme ne doit être assuré que pendant la durée du traitement de chaque mot. Même si les générateurs de l'émetteur et du récepteur possèdent la même fréquence nominale et présentent initialement le déphasage désiré, les fluctuations de phase dues au bruit détruisent peu à peu le synchronisme. On fait alors appel à un asservissement permettant de synchroniser automatiquement le générateur du récepteur sur un signal de référence provenant de l'émetteur. Ces asservissements sont appelés *les boucles à verrouillage de phase* (en anglais Phase Locked Loop, PLL) où ils sont omniprésents dans les appareillages de communications numériques [73].

Depuis quelques années, la théorie des systèmes chaotiques a été appliquée dans le domaine des communications. La synchronisation des systèmes chaotiques semble impossible dans un premier temps, notamment à cause de la sensibilité de ces systèmes aux conditions initiales. De plus, un système chaotique n'est pas asymptotiquement stable, c'est-à-dire que les trajectoires issues des conditions initiales voisines (légèrement différentes) divergent exponentiellement avec le temps. En effet, on peut dire que pour les systèmes réels, il n'est pas facile de produire et de reproduire les mêmes conditions de démarrage. D'après ce point de vue, tout changement de paramètre dans un système chaotique pourrait conduire à une divergence entre ces trajectoires. Pourtant ce raisonnement n'est pas correct. Il peut exister des conditions sous lesquelles les trajectoires de deux systèmes chaotiques différents peuvent converger l'une vers l'autre, si certaines informations (énergie) pertinentes sont échangées. En 1983, Chua a abordé la question de synchronisation en utilisant des circuits électriques linéaires par morceaux [147]. Dans les années 90, Pecora et Caroll ont montré que deux systèmes chaotiques pourraient se synchroniser

sous certaines conditions, si l'un deux est piloté par au moins une composante (une ou plusieurs variables d'état) de l'autre [126], [127], etc. Depuis les années 90, de nombreux ouvrages ont été publiés au sujet de la synchronisation chaotique [52], [120], etc.
Une raison importante de l'attirance des chercheurs vers la synchronisation des systèmes chaotiques est son application à la communication sécurisée [27], [53], etc. Les travaux de Pecora et Caroll ont permis de suggérer que les systèmes chaotiques pourraient être utilisés dans la communication, où leur nature semblable aux bruits améliorerait la sécurité et le rejet des perturbations. En effet, une fois la synchronisation entre l'émetteur et le récepteur atteinte, il est possible de récupérer un message masqué par l'émetteur chaotique. C'est ainsi qu'en 1990, Parlitz proposa le couplage de deux attracteurs étranges identiques, dans le but de camoufler un message confidentiel en le superposant à un signal chaotique, et en le restaurant à la réception. Ce n'est donc qu'en 1992 que les ingénieurs ont réalisé des systèmes de communication chaotique sécurisée [37], [36]. Dans [119], Oppenheim *et al.* ont proposé des méthodes qu'ils ont appelées commutation chaotique ou modulation et masquage chaotique. Koracev *et al.* dans [87] proposent de noyer le message dans le système chaotique et d'utiliser le concept de synchronisation afin d'augmenter la sécurité de la communication.
Dans la première section de ce chapitre, nous allons présenter quelques brèves notions sur le chaos et ses avantages dans les transmissions sécurisées. La section 1.3 est consacrée aux principales méthodes de synchronisation des systèmes chaotiques. Dans la section 1.4, nous allons présenter le principe de la synchronisation des systèmes chaotiques par les observateurs dans les deux cas continus et discrets. Dans la section 1.5, nous allons appliquer les deux méthodes de synchronisation passive et impulsive sur deux systèmes chaotiques identiques de Qi. La section 1.6 présente d'une manière générale la transmission sécurisée d'informations en détaillant l'idée d'utiliser les signaux chaotiques pour la transmission de données. Nous présenterons certaines méthodes de transmission à l'aide de signaux chaotiques. Enfin, dans la dernière section, nous donnerons des notions de base sur les systèmes hybrides qui seront exploités dans la synthèse des observateurs.

1.2 Quelques notions sur le chaos

1.2.1 Caractérisation du chaos

L'étude théorique approfondie du chaos est loin d'être l'objectif de ce travail de thèse. Dans cette section, nous nous limitons à définir brièvement le phénomène chaotique apparaissant dans un système non linéaire dynamique déterministe. Des détails sur la description du chaos et ses caractéristiques seront donnés en Annexe A.

Quelques systèmes physiques se comportent de manière chaotique. Parmi ces systèmes, on peut citer l'atmosphère, un robinet qui goutte, un pendule excité dans un champ magnétique, etc. Ces quelques systèmes se démarquent par leurs dimensions et l'origine de leurs mouvements. Il existe plusieurs définitions possibles du chaos. Ces définitions ne sont pas toutes équivalentes, mais elles convergent vers certains points communs caractérisant ainsi le chaos. Ci-dessous, nous présentons d'une manière succincte quelques caractéristiques qui permettent de comprendre les points marquants d'un système chaotique.

– Sensibilité aux conditions initiales

  Les systèmes chaotiques sont extrêmement sensibles aux perturbations. On peut illustrer ce fait par l'effet papillon, popularisé par le météorologue Edward Lorenz. L'évolution d'un système dynamique chaotique est imprédictible en ce sens qu'elle est sensible aux conditions initiales. Ainsi, deux trajectoires de phases initialement voisines s'écartent toujours l'une de l'autre, et ceci quelle que soit leur proximité initiale. Il est en particulier clair que la moindre erreur ou simple imprécision sur la condition initiale interdit de décider à tout temps quelle sera la trajectoire effectivement suivie et, en conséquence, de faire une prédiction autre que statistique sur le devenir à long terme du système. Ainsi, bien que l'on traite de systèmes déterministes, il est impossible de prévoir à long terme leurs comportements.

– Attracteur étrange

  Un attracteur est la zone de l'espace des phases qui attire les trajectoires d'un système dynamique quelconque. L'attracteur le plus simple est un point, c'est l'attracteur d'un système qui évolue à taux constant, d'autres attracteurs peuvent inclure des cycles qui se répètent au cours du temps. Dans le premier cas, le mouvement atteint un état stationnaire ; dans le deuxième cas, le mouvement se reproduit continûment. Dans le cas d'un système chaotique, la trajectoire converge vers une région

particulière de l'espace appelée attracteur étrange qui est une signature du chaos, c'est ce qui différencie un signal chaotique d'un signal aléatoire En effet, si le mouvement est aléatoire les points de la trajectoire remplissent l'espace de phase de manière aléatoire.

– Exposants de Lyapunov

Les exposants de Lyapunov sont des coefficients qui permettent de mesurer la sensibilité aux conditions initiales d'une série temporelle. Par définition, un exposant de Lyapunov est le taux exponentiel moyen de divergence ou de convergence de trajectoires voisines de l'espace des phases. Il mesure le taux local d'expansion de l'espace dans lequel l'expansion est maximale, c'est-à-dire en général vers l'attracteur. Un attracteur étrange est un attracteur dont l'un au moins de ses exposants de Lyapunov est positif. Autrement dit, le plus grand exposant est positif pour le système chaotique et négatif pour les autres systèmes.

1.2.2 Avantages du chaos

En première approche, les systèmes chaotiques sont des systèmes dynamiques qui évoluent dans une région bornée, qui possèdent une infinité de trajectoires non périodiques denses. Ils sont très sensibles aux conditions initiales [1], [28], [29] : deux conditions initiales très proches conduisent à deux trajectoires qui s'éloignent rapidement l'une de l'autre [74], [113]. Les propriétés nous permettent théoriquement de générer un nombre infini de signaux chaotiques non corrélés d'un même système en utilisant différentes valeurs initiales. Ceci peut être employé pour générer des séries de nombres pseudo-aléatoires. Cette série est très utile dans certains cryptosystèmes traditionnels ou dans le protocole de TCP/IP [15]. Une autre application de cette propriété est de produire des séquences chaotiques [69] pour remplacer les séquences étalées conventionnelles [130] utilisées dans les systèmes de spectre étalé par séquence directe. Ensuite, il est à noter qu'en raison de leur propriété aléatoire, les signaux chaotiques ont des fonctions d'autocorrélation très étroites et des spectres de puissance à large bande proche du bruit blanc. Ainsi, la corrélation croisée de signaux chaotiques a une valeur très petite. Puisque le système chaotique a une trajectoire non périodique et est sensible aux conditions et aux paramètres initiaux, logiquement il peut aussi être employé pour crypter des messages.

Dans les systèmes de transmission conventionnels, des signaux sinusoïdaux sont em-

ployés comme signaux porteurs, ce qui offrent une efficacité excellente dans une large bande. Cependant, la puissance transmise est concentrée dans une bande étroite, entraînant une densité spectrale de puissance élevée. Les problèmes principaux avec cette caractéristique sont : l'atténuation élevée dans une bande de fréquence étroite ce qui peut mener à la perte de synchronisation, des niveaux élevés d'interférence avec d'autres utilisateurs du réseau, les possibilités élevées d'interception, etc. Au contraire, les signaux chaotiques sont habituellement identifiés comme du bruit et ont des bandes larges, ainsi ils peuvent être utilisés pour étaler l'information originale à bande étroite. Ainsi, en utilisant les signaux chaotiques pour crypter l'information, les signaux résultants sont des signaux de spectre écarté ayant une bande plus grande et des densités spectrales de puissance inférieures à des solutions usuelles [100].

1.2.3 Technique de démodulation

Du point de vue de la transmission, il existe la technique de démodulation cohérente et la technique de démodulation non cohérente pour récupérer le signal transmis [83]. Dans une démodulation non cohérente, le récepteur ne connaît pas (et n'essaie pas d'estimer) la forme d'onde transmise. Au lieu de cela, il emploie des attributs statistiques du signal transmis afin de décider des propriétés du signal émis, par exemple, la variance, l'espérance et beaucoup d'autres propriétés statistiques. L'avantage principal d'employer des méthodes non cohérentes est que le récepteur n'a pas à être synchronisé avec l'émetteur. De plus, les récepteurs non cohérents sont souvent plus simples que leurs homologues cohérents. L'inconvénient en employant la démodulation non cohérente est que certaines propriétés statistiques du signal transmis peuvent permettre à un récepteur non autorisé de décoder le message sans aucune connaissance de la dynamique secrète de l'émetteur. Par conséquent les schémas de transmission chaotique de données qui permettent la démodulation non cohérente ne sont pas très sûrs d'un point de vue du chiffrage. Mais ils sont très utiles dans un environnement où la synchronisation entre l'émetteur et le récepteur est difficile.

La démodulation cohérente implique que la forme d'onde transmise est connue par ce récepteur mais il peut aussi être corrélé par du bruit, pour maximiser le rapport signal sur bruit (en anglais Signal to Noise Ratio, SNR). Pour le signal transmis qui est modulé, la démodulation cohérente exige la récupération de l'amplitude et de la phase du signal.

Ceci peut être fait en employant une PLL qui récupère la phase du signal, et un Contrôle automatique de gain (en anglais Automatic Gain Control, AGC) qui normalise l'amplitude du signal reçu. Dans le cas de la transmission chaotique, la connaissance de l'état de l'émetteur implique la connaissance de la forme d'onde transmise. Par conséquent, la synchronisation entre l'émetteur et le récepteur permet au récepteur de reconstruire la forme d'onde transmise et d'employer des techniques de détections cohérentes.

1.3 Méthodes de synchronisation

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

En plus du couplage simple (par résistance ou suiveur), d'autres méthodes ont été proposées pour la synchronisation des systèmes chaotiques. Ainsi pour la synchronisation unidirectionnelle, on peut citer la méthode par décomposition du système [89], la synchronisation impulsive [122], la synchronisation par des méthodes itératives [27] ou la synchronisation par la boucle fermée. Dans la majorité des cas, les deux systèmes doivent avoir des structures identiques, ce qui n'est pas tout à fait réalisable en pratique. Un petit écart entre les valeurs des composants peut entraîner un écart considérable entre les comportements des deux circuits et détruire le phénomène de synchronisation. La synchronisation peut être décrite par la définition suivante :

Définition 1 *[115] Considérons les deux systèmes suivants :*

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

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

$$\lim_{t \longrightarrow \infty} \|z(t) - x(t)\| = 0$$

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

1.3.1 Synchronisation par couplage bidirectionnel

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

$$\begin{cases} \dot{x} = f(x) + \lambda(z - x) \\ \dot{z} = g(z) + \mu(x - z) \end{cases} \tag{1.1}$$

où $x, z \in \mathbb{R}^n$ et λ, μ sont des matrices diagonales $n \times n$;$\lambda = diag[\lambda_i]$, $\mu = diag[\mu_i]$, $i = 1, ...n$. On suppose que $f(0) = g(0) = 0$. Du point de vue de l'ingénierie électronique, ce type de synchronisation définit l'évolution temporelle de deux circuits électroniques couplés à l'aide d'une résistance. Le problème de synchronisation consiste alors à trouver λ et μ à coefficients arbitraires de telle manière que $\lim_{t \longrightarrow \infty} \|z(t) - x(t)\| = 0$. Cette méthode a été étudiée dans [90] et a été appliquée à l'oscillateur de Colpitts dans [12]. La figure 1.1 illustre ce type de synchronisation.

Ce travail a été détaillé dans [71]. Les résultats obtenus montrent que pour avoir une synchronisation bidirectionnelle, la résistance de couplage (potentiomètre : POT) doit être très faible ($POT = 36\Omega$) pour que l'échange de l'énergie ait lieu dans les deux sens. Lorsque les deux oscillateurs sont synchronisés, la dimension du système global, constitué des deux oscillateurs couplés, passe de 6 à 3.

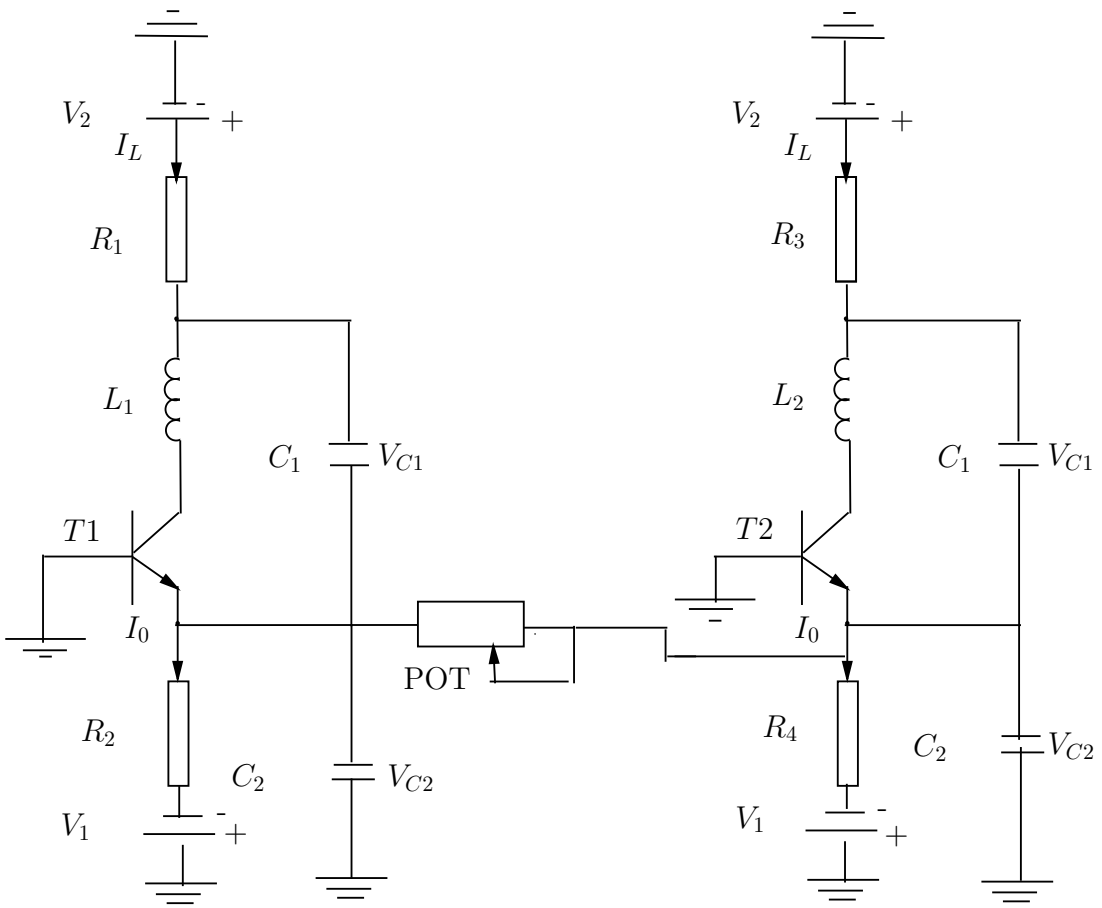


FIG. 1.1: Couplage bidirectionnel de deux oscillateurs de Colpitts

1.3.2 Synchronisation par couplage unidirectionnel

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

$$\begin{cases} \dot{x} = f_1(x) \\ \dot{z} = f_2(z) + \alpha(x - z) \end{cases} \tag{1.2}$$

où $x, z \in \mathbb{R}^n$, $\alpha = diag[\alpha_1, ..., \alpha_n]^T$. Le problème de synchronisation consiste alors à trouver α tel que $\lim_{t \longrightarrow \infty} \|z(t) - x(t)\| = 0$. Ce type de synchronisation a été appliquée au circuit de Chua [32] et a été aussi étudié par Koracev *et al.* dans [90]. Les conditions de convergence de cette approche sont étudiées dans [118].

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

Exemple 1 *Soient deux systèmes chaotiques* ***identiques*** *a et b de dimension 3, décrits par* $\dot{x_a} = f(x_a)$ *et* $\dot{x_b} = f(x_b)$*. Le schéma de couplage des deux systèmes est montré dans les figures 1.2(a) (couplage unidirectionnel) et 1.2(b)(couplage bidirectionnel). Le couplage de ces systèmes peut être exprimé par les équations suivantes.*

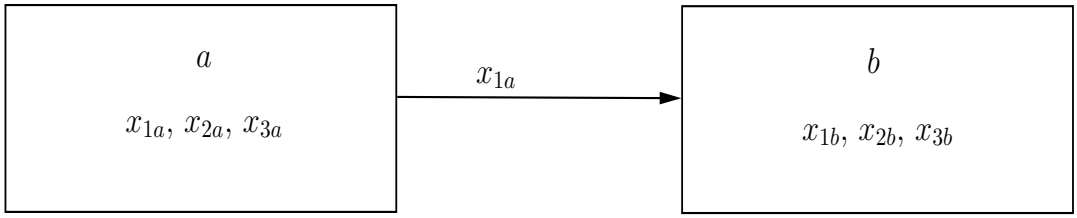
$$\begin{cases} \dot{x}_{1a} = f_1(x_a) + k_{a1}(x_{1b} - x_{1a}) \\ \dot{x}_{2a} = f_2(x_a) + k_{a2}(x_{1b} - x_{1a}) \\ \dot{x}_{3a} = f_3(x_a) + k_{a3}(x_{1b} - x_{1a}) \end{cases}$$

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

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

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

(a)



(b)

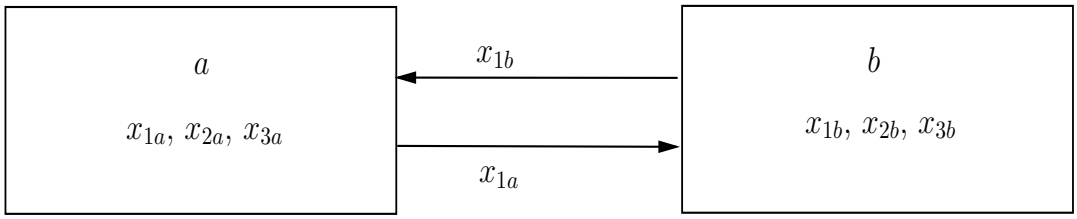


FIG. *1.2: Schémas de couplage : (a) unidirectionnel, (b) bidirectionnel*

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

Dans le contexte du système de l'exemple 1, on considère le vecteur de dimension 6 :

$$z(t) = \begin{pmatrix} x_a(t) \\ x_b(t) \end{pmatrix}$$

On suppose que les deux systèmes sont synchronisés, c'est à dire que $x_a(t) = x_b(t)$. Imaginons maintenant que z soit légèrement perturbé. Si la synchronisation des deux systèmes est stable, alors z revient à sa position initiale et les deux systèmes restent synchronisés. Pour étudier ce problème, on considère $x_a - x_b = \Delta$ et on soustrait les équations du système b de celle du système a. Ensuite, on linéairise le système obtenu par rapport à la perturbation Δ. On obtient alors :

$$\dot{\Delta} = Df(x)\Delta - k\Delta_1 \tag{1.3}$$

dans lequel $Df(x)$ est la matrice jacobienne de $f(x)$, $x(t) = x_a(t) = x_b(t)$ représente la

situation de synchronisation chaotique vérifiant $\dot{x} = f(x)$ et $k = [k_{a1} + k_{b1}, k_{a2} + k_{b2}, k_{a3} + k_{b3}]^T$ et $f(x)$ une fonction qui doit être au moins de classe C^1.

Si pour $|x_a(0) - x_b(0)| < \epsilon$ (avec $\epsilon > 0$ et petit), nous obtenons $|x_a(t) - x_b(t)| \to 0$ pour $t \to \infty$, on dit alors que la synchronisation est stable. La synchronisation chaotique sera **globalement** stable si pour toute trajectoire $x(t)$ sur l'attracteur chaotique du système synchronisé $\dot{x} = f(x)$(comportement commun), les exposants de Lyapunov sont négatifs lorsque le système est soumis à une légère perturbation Δ_0. Plus de détails sont donnés dans [120] à ce sujet.

Les méthodes de synchronisation chaotique expliquées jusqu'ici sont basées sur l'utilisation de systèmes identiques, même si il existe une légère différence entre leurs paramètres. On se demande maintenant ce qui se passerait si les systèmes n'étaient pas du tout identiques, et même de structure différentes ?

Dans [136], deux systèmes chaotiques couplés de façon unidirectionnelle (que l'on note aussi "synchronisation") sont considérés avec les équations de la forme :

$$\begin{cases} \dot{x} = f(x) \\ \dot{z} = g(z, h(x)) \end{cases} \tag{1.4}$$

où x et z sont respectivement de dimension n et m. le système z est piloté par une fonction de x, c'est à dire $h(x)$. D'après [136], il existe une synchronisation entre les deux systèmes si l'état de z est déterminé uniquement par x, une fois son attracteur chaotique est atteint, c'est à dire :

$$z = \Phi(x)$$

dans lequel Φ ne dépend pas des conditions initiales de z. Ce type de synchronisation est appelé "synchronisation globale". Une autre définition pour la synchronisation globale des systèmes chaotiques est donnée dans [91]. D'après cette définition, la synchronisation globale apparaît si pour toute condition initiale x_0 du système pilote x, le système de réponse z est asymptotiquement stable, c'est à dire qu'il existe une région B de l'espace de z telle que pour deux points initiaux z_{10} et $z_{20} \in B$:

$$\lim_{t \longrightarrow \infty} \|z(t, x_0, z_{10}) - z(t, x_0, z_{20})\| = 0$$

où $z(t, x_0, z_{10})$, $z(t, x_0, z_{20})$ sont des trajectoires dans B (pour t suffisamment grand) générées à partir de (x_0, z_{10}) et (x_0, z_{20}). Suivant les propriétés de Φ, la synchronisation globale est appelée "forte" ou "faible" [131]. La synchronisation globale faible correspond à une fonction $\Phi \in C^0$ et non lisse, tandis que la synchronisation globale forte est associée à une fonction $\Phi \in C^1$ ou plus.

Dans ce qui suit, nous allons donner les méthodes classiques de synchronisation des systèmes chaotiques.

1.3.3 Synchronisation par décomposition du système

Certains systèmes chaotiques possèdent la propriété d'auto synchronisation, c'est à dire qu'on peut les décomposer en deux sous-systèmes, l'un *maître*, l'autre *esclave*. Ces derniers peuvent se synchroniser sous l'effet d'un couplage avec un signal commun. Dans le schéma de synchronisation proposé par Pecora et Carroll [126], un système chaotique

$$\dot{x} = f(x) \tag{1.5}$$

avec une sortie $y = h(x)$ est décomposé en deux sous-systèmes dont les états sont x_1 et x_2 respectivement :

$$\dot{x_1} = f_1(x_1, x_2) \tag{1.6}$$

$$\dot{x_2} = f_2(x_2, y) \tag{1.7}$$

où

$$x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

Le système est partitionné de façon à ce que les Exposants de Lyapunov Conditionnels (ELCs)[126] du sous-système (1.7) soient negatifs.

Qualitativement, les ELCs caractérisent la stabilité de (1.7). Si tous les ELCs sont négatifs, alors la trajectoire $x_2(t)$ est asymptotiquement stable [126]. Ceci signifie que les états de plusieurs copies du sous-système (1.7) se synchroniseront à l'aide du même signal

$y(t)$.

En particulier, on considère le système décrit par :

$$\dot{\hat{x}}_2 = f_2(\hat{x}_2, y) \tag{1.8}$$

Si les ELCs de ce système sont tous négatifs et $\hat{x}_2(0)$ est suffisamment proche de $x_2(0)$, alors l'état $\hat{x}_2$ converge asymptotiquement vers x_2, c'est à dire :

$$\lim_{t \longrightarrow \infty} \|x_2 - \hat{x}_2\| = 0$$

En gros, le problème dans le principe de Pecora Carroll est de trouver une décomposition (1.6)-(1.7) convenable, c'est à dire telle que les ELCs de (1.7) soient négatifs.

Ce principe, qui a été initié par Pecora et Carroll [126] en 1990 et ensuite repris dans beaucoup de travaux tels que [25] et [86], peut être résumé par la figure 5.

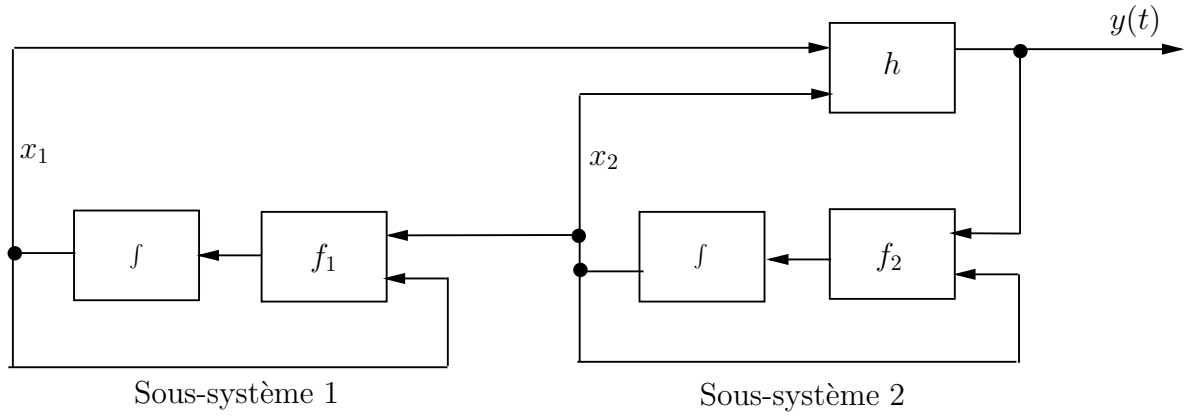


FIG. 1.3: Principe de Pecora-Caroll

1.3.4 Synchronisation par la contre-réaction

La technique de synchronisation présentée par Pecora et Caroll souffre d'une forte sensibilité aux variations de paramètres, ainsi qu'en présence des bruits à l'entrée du système. La raison fondamentale de la sensibilité de cette méthode est que la synchronisation est faite boucle ouverte [86]. Les nouvelles techniques sont basées sur un bouclage par contre réaction et ont été développées pour récupérer les signaux d'entrées [129]. Ces techniques utilisent une réplique du système original et le signal transmis $x_s(t)$ est comparé au signal régénéré localement $\tilde{x}_s(t)$ pour produire un signal d'erreur $\varepsilon(t)$ qui est appliqué par

contre-réaction dans le système à travers une fonction de correction $c(.)$ comme montré par la figure 1.4. L'équation du récepteur peut être écrite comme suit :

$$\dot{\tilde{x}} = f(x) + c(\varepsilon(t)) = f(x) + c(x_s(t) - \tilde{x}_s(t))$$

Par un bon choix de la fonction de correction, on peut montrer [115] que sous certaines conditions que la stabilité globale peut être maintenue. De plus, cette approche est récemment utilisée pour synchroniser deux paires différentes de systèmes chaotiques [103].

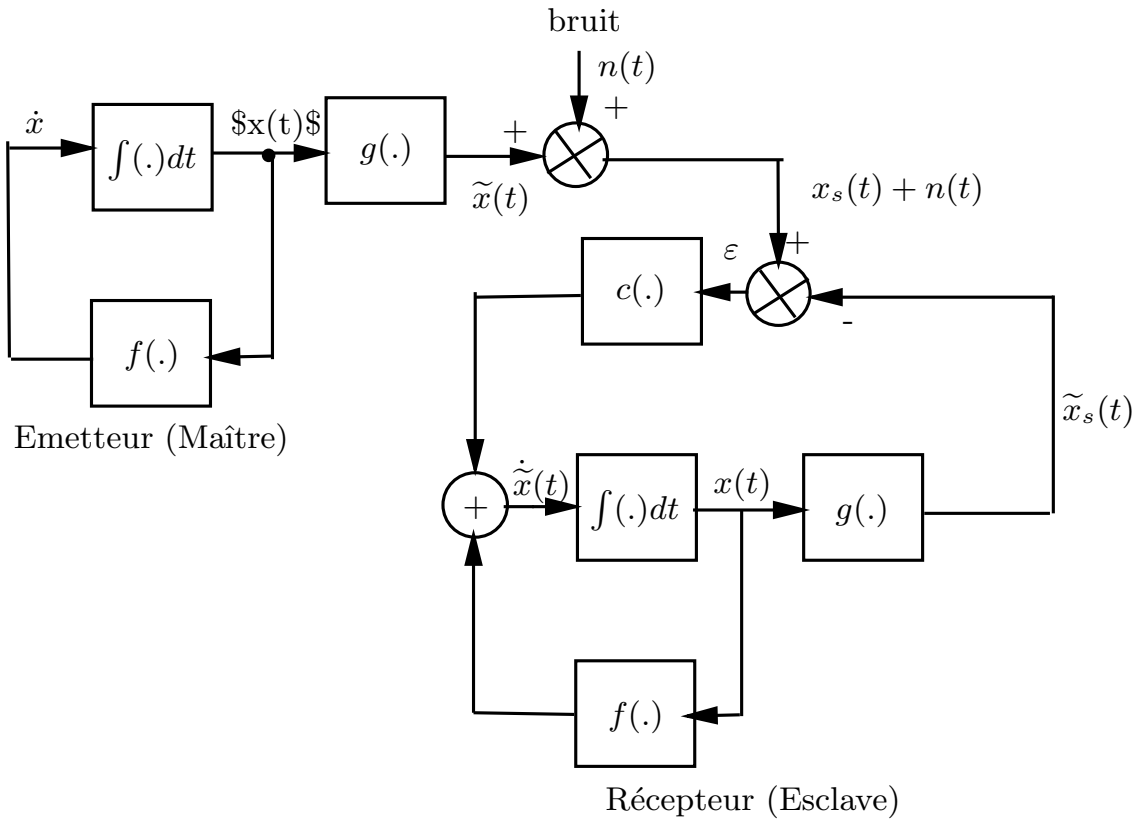


FIG. 1.4: Architecture d'une synchronisation chaotique par contre-réaction

1.3.5 Synchronisation par l'approche du système inverse

Le troisième type de synchronisation des systèmes est utilisé pour les systèmes non autonomes. Une définition formelle pour les systèmes inverses est donnée en [129], [68]. Un exemple pour ce type de système est donnée par la figure 1.5. La diode est bien connue pour sa génération d'un signal chaotique sous certaines conditions de fréquence et d'am-

plitude du générateur d'entrée. Le courant chaotique est donc transformé en une tension de sortie à travers l'amplificateur opérationnel montré par la figure 1.5. En revanche, le circuit résonnant réalisé avec la diode au niveau du récepteur est alimenté par le courant issu de l'émetteur. Aussi pour assurer un courant nul à l'entrée du second amplificateur opérationnel, la sortie $r(t)$ du récepteur doit correspondre au signal d'entrée $e(t)$.

Lorsque le signal d'entrée est modulé, le signal issu du récepteur portera la même information de modulation lorsque la synchronisation est assurée.

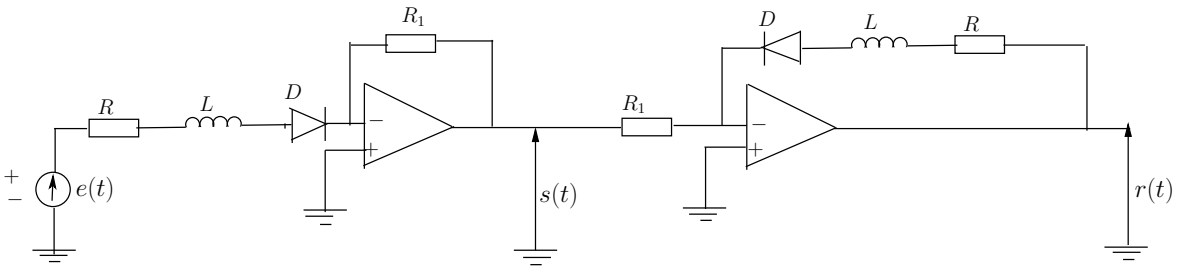


FIG. 1.5: Synchronisation d'un système non autonome basée sur le système inverse

1.4 Méthode de couplage unidirectionnel choisie : l'approche par observateur

L'utilisation des observateurs est proposée pour estimer les états inconnus d'un système qui ne sont pas mesurables directement. Un système dynamique est dit observable si on peut récupérer toutes ses grandeurs (de façon statique ou dynamique) par une combinaison de mesures de ses sorties et de leurs dérivées. En se basant sur l'idée de contrôlabilité et d'observabilité, dans les années 1960, Kalman a établi des théorèmes pour les systèmes linéaires [79]. Les systèmes non linéaires n'ont été traités sur ce sujet que vers le début des années 70, lorsque Bonnard [18], Sussman-Jurdjevic [145] et Hermann-Krener [70] ont posé les bases de la contrôlabilité (et ensuite de l'observabilité) non linéaire à l'aide de l'algèbre de Lie. Ainsi, des observateurs ont été conçus pour différents types de systèmes. Dans [49], un observateur a été proposé pour un système discret. La méthode est basée sur l'algèbre différentielle et suggère qu'en connaissant seulement un nombre fini d'échantillons d'entrées et de sorties précédentes, on peut reconstruire exactement l'état actuel

du système. Une reconstruction exacte des états d'un système chaotique discret est proposée par Sira-Ramirez dans [142]. De plus, Parker et Chua ont proposé un reconstructeur d'attracteur basé sur les échantillons d'une seule variable d'état provenant d'un système continu [125]. Aussi, différentes formes de systèmes ont été traitées et des observateurs appropriés ont été proposés. [143], [143], [23], etc.

En 1997, Nijmeijer et Mareels ont montré que la synchronisation unidirectionnelle de deux systèmes chaotiques peut être considérée comme un problème d'observateur non linéaire [115] et par conséquent, les théories de l'automatique peuvent être utilisées afin d'analyser ce phénomène (voir par exemple [93]). La figure 2.7 illustre ce principe de synchronisation.

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

-L'observateur de Kalman étendu [79].

- Les observateurs reposant sur une approche analytique [56], etc.

- Les observateurs à grands gains [19].

- Les observateurs à modes glissants [7].

- Les observateurs adaptatifs [92].

- Les observateurs algébriques [9].

- Les observateurs numériques [44].

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

$$\lim_{t \longrightarrow \infty} \|x(t) - \hat{x}(t)\| = 0.$$

Les différents observateurs (en temps continu et en temps discret) cités précédemment ont

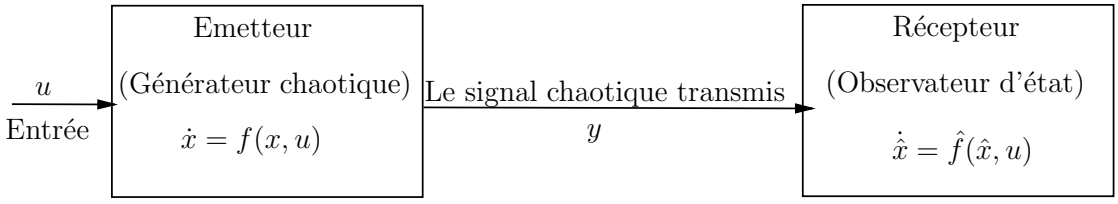


FIG. 1.6: Principe de synchronisation à base d'observateurs

été conçus dans le but de réaliser des systèmes de transmissions sécurisées. Récemment, la théorie des systèmes hybrides a été introduite dans le but d'augmenter la robustesse des systèmes de transmission. Dans la littérature, peu de travaux ont été faits en utilisant les systèmes hybrides pour la conception des systèmes de transmissions sécurisées. Parmi ces travaux, on peut citer [111], [39], [60].

Dans ce travail de thèse, notre objectif consiste à concevoir un système de transmission sécurisée en utilisant les systèmes hybrides. L'émetteur est composé d'une combinaison d'un système chaotique en temps continu et d'un système chaotique en temps discret. Le système chaotique obtenu est hybride (voir les détails au chapitre 2). Au niveau de la réception, des observateurs en temps continu et en temps discret seront utilisés (voir les détails au chapitre 3).

Dans ce qui suit, nous allons rappeler quelques définitions liées à la notion d'observabilité et les conditions de recouvrement d'observabilité des systèmes non linéaires (en temps continu et discret) et les deux types d'observateurs utilisés.

1.4.1 Cas continu

1.4.1.1 Observabilité des systèmes non linéaire

Considérons le système non linéaire donné par la forme suivante :

$$\begin{cases} \dot{x}(t) = f(x) \\ y(t) = h(x) \end{cases} \tag{1.9}$$

dans lequel $x \in M \subseteq \mathbb{R}^n$ et $y \in \mathbb{R}^p$ représentent respectivement l'état et la sortie du système. Les fonctions f, h sont des vecteurs de fonctions analytiques de dimensions appropriées. Notons que pour tout $x^0 \in M$, il existe une solution pour $\dot{x}(t) = f(x(t))$ telle que $x(0) = x^0$ et $x(t) \in M$ pour tout $t \in \mathbb{R}$. On note U un sous ensemble ouvert de M. Pour tout $x \in \mathbb{R}^n$, le système (1.9) est supposé avoir des états bornés en temps fini.

Le problème d'observabilité consiste à pouvoir reconstruire tous les états du système à partir de la sortie et de ses dérivées. Par ailleurs, toutes les définitions d'observabilité sont basées sur la notion d'"indiscernabilité" entre deux états initiaux. Quelques définitions liées à l'observabilité des systèmes non linéaires sont reportées dans l'annexe.

1.4.1.2 Condition du rang d'observabilité

Définition 2 . *Considérons le système dynamique de la forme (1.9). On dit que la paire* (f, h) *est observable au sens du rang si la condition donnée par (1.10) est satisfaite.*

$$rang(O) = rang \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{pmatrix} = n \tag{1.10}$$

où

$$O = \begin{pmatrix} dh \\ dL_f h \\ \vdots \\ dL_f^{n-1} h \end{pmatrix} \tag{1.11}$$

$L_f h$ *désigne la dérivée de Lie de* h *dans la direction de* f *(voir définition en annexe).*

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

$$dL_f^k h = (\tfrac{\partial L_f^k h}{\partial x_1}, \tfrac{\partial L_f^k h}{\partial x_2}, ..., \tfrac{\partial L_f^k h}{\partial x_n}) \tag{1.12}$$

Exemple 2 *Soit le système non linéaire :*

$$\begin{cases} \dot{x}_1 = \frac{x_1^2}{2} + \exp(x_2) + x_2 \\ \dot{x}_2 = x_1^2 \\ y = x_1 \end{cases}$$

Dans ce système, $h = [x_1 \;\; 0]$ *et* $dh = [1 \;\; 0]$*. Appliquons la condition du rang d'observabilité donnée en (1.10) :*

D'après (1.11), on a :

$$O = \begin{pmatrix} dh \\ dL_f h \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ x_1 & \exp(x_2) + 1 \end{pmatrix}$$

Alors rang(O)=2=n. Le système est donc localement faiblement observable.

1.4.1 3 Méthode d'inversion à gauche et condition de recouvrement d'observabilité

Dans la transmission de données (analogiques ou numériques) par synchronisation de systèmes chaotiques (en temps continu ou en temps discrets), il est important de pouvoir estimer l'entrée inconnue du système en plus de la synchronisation des états. En effet, l'entrée inconnue peut être un défaut, une perturbation ou dans notre travail, un message confidentiel. La transmission d'informations avec la méthode par inclusion est non seulement un problème d'observabilité mais aussi un problème d'inversion à gauche, c'est à dire reconstruire tous les états ainsi que le message inconnu à partir de la sortie du système et ses dérivées [71].

Deux types d'observateurs continus ont été proposés pour les systèmes à entrées inconnues. Des observateurs destinés à estimer seulement les états du système (sans tenir compte de l'entrée inconnue) [38], [40], et des observateurs destinés à l'estimation des états et de l'entrée inconnue [33].

Soit le système :

$$\begin{cases} \dot{x}(t) = f(x,u), x_0 \in D \subseteq \mathbb{R}^n \\ y(t) = h(x,u) \end{cases} \tag{1.13}$$

dans lequel $x \in \mathbb{R}^n$ est l'espace d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée, et $y \in \mathbb{R}^k$ représente le vecteur de sortie du système, $t \in T = [0, t_f]$. Les fonctions $f(x,u), h(x,u), u(t)$ sont considérées suffisamment dérivables. Le problème de l'inversion du système consiste à reconstruire x et u ou une partie de ceux-ci à partir de la sortie $y(.)$ du système et de ses dérivées. Le système (1.13) génère le "mapping" suivant (pour la condition initiale x_0 connue) :

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

Avant d'introduire les propriétés du système (1.13), on considère un ensemble de fonctions U définies sur le domaine D_α constitué de fonctions et de leurs dérivées d'ordre 1 à α. Alors, nous avons : $U = U(D_\alpha)$ où :

$$D_0 = \bigcup_{t \in T} u(t), D_1 = \bigcup_{t \in T} (u(t), \dot{u}(t)), ..., D_\alpha = \bigcup_{t \in T} (u(t), ..., u(t)^{(\alpha)}), D_i \subseteq \mathbb{R}^{(i+1)m}$$

Définition 3 *Le système (1.13) est inversible dans le domaine $D \times D_\alpha \times T$ si pour tout $x_0 \in D$ et deux entrées différentes $u_1(t)$, $u_2(t) \in D_\alpha$, il existe un instant $t \in T$ tel que $h(\Phi(x_0, u_1)) \neq h(\Phi(x_0, u_2))$.*

Nous écrivons maintenant le système (1.13) de la façon suivante :

$$\begin{cases} \dot{x} = f(x) + p(x)w \\ y = h(x) \end{cases} \tag{1.14}$$

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

Dans le système (1.14), on considère que w est continu, ou au moins continu par morceaux. La conception d'un observateur à entrées inconnues est réalisable localement au voisinage de x_0 si les conditions données par les hypothèses suivantes sont vérifiées :

Hypothèse 1 *La perturbation (entrée inconnue) est bornée.*

Hypothèse 2 *span $\{dh, dL_f h, ..., dL_f^{n-1} h\}$ est de rang n.*

Hypothèse 3 $((dh)^T, (dL_f h)^T, ..., (dL_f^{n-1} h)^T)^T = (0...0, \theta)^T$.

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

La condition donnée dans l'hypothèse 3 est appelée condition de recouvrement d'observabilité (en anglais Observabilité Matching Condition) pour les systèmes continus. Cette condition garantie la propriété d'inversibilité à gauche, c'est à dire la possibilité de retrouver tous les états et le message à partir de la sortie y et de ses dérivées (voir [10] pour plus de détails).

Exemple 3 *Soit le système non linéaire :*

$$\begin{cases} \dot{x}_1 = x_2^2 + x_3 + w \\ \dot{x}_2 = 2x_3 \\ \dot{x}_3 = 2(x_1 + x_2) \\ y = x_2 \end{cases}$$

On veut tester la condition de recouvrement d'observabilité de ce système où w est son entrée inconnue.

Tout d'abord, on va tester la condition d'observabilité de ce système.

On a $h = [0 \quad x_2 \quad 0]$ et $dh = [0 \quad 1 \quad 0]$. Appliquons la condition du rang d'observabilité donnée en (1.10) : D'après (1.11), on a :

$$O = \begin{pmatrix} dh \\ dL_f h \\ dL_f^2 h \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 4 & 4 & 0 \end{pmatrix}$$

Alors rang(O)=3=n. Le système est donc localement faiblement observable. Nous étudions maintenant la condition de recouvrement d'observabilité et l'inversibilité à gauche du système donnée par l'hypothèse 3.

Nous écrivons le système d'abord sous la forme analytique donnée par 1.14.

où $P(x) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. *Calculons maintenant :*

$$OP(x) = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 2 \\ 4 & 4 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \theta = 4 \end{pmatrix}$$

avec $\theta = 4 \neq 0$. Ainsi, la condition de recouvrement d'observabilité donnée par l'hypothèse 3 est vérifiée, il est alors possible d'extraire l'entrée inconnue à l'aide d'un observateur.

Dans notre travail, nous avons utilisé un observateur impulsif. Quelques notions théoriques sur ce type d'observateurs sont données par la section suivante.

1.4.1.4 Approche de la synchronisation par observateur impulsif

Un observateur impulsif ([80], [103], [156]) est approprié pour les schémas de synchronisations impulsives chaotiques lorsque la sortie est discrète. En utilisant la sortie d'un système (émetteur) à des instants de temps discrets, l'observateur permet de reconstruire tous les états.

Concepts de base sur la commande impulsive

Considérons le système non linéaire donné comme suit :

$$\dot{x} = f(t, x) \tag{1.15}$$

où $x \in \mathbb{R}^n$ est le vecteur d'état, t est la variable temps, et $f : \mathbb{R}^n \to \mathbb{R}^n$. Les sauts dans les variables d'état se produisent à des instants discrets $t = \tau_i$ où $x(\tau_i^-) = x(\tau_i)$.

Posons $\delta^+ x(t = \tau_i) = x(\tau_i^+) - x(\tau_i^-) = U(i, x)$ avec $i = 1, 2, ...$, et $0 < \tau_1 < \tau_2 < ...\tau_i < \tau_{i+1} < ...$ et $\lim\limits_{i \longrightarrow \infty} \tau_i = \infty$. Alors, ce système impulsif est décrit par :

$$\begin{cases} \dot{x} & = & f(t, x), \quad t \neq \tau_i \\ \delta^+ x(t = \tau_i) & = & x(\tau_i^+) - x(\tau_i^-), \quad t = \tau_i, \quad i = 1, 2, ... \\ x(t_0^+) = x_0, \quad t_0 \geq 0 \end{cases} \tag{1.16}$$

L'équation (1.16) est appelée aussi une équation différentielle impulsive [94]. Pour étudier la stabilité du système d'équations différentielles impulsives (1.16), nous utilisons les théorèmes et les définitions suivants :

Définition 4 *[94] Une fonction $V : (\tau_{i-1}, \tau_i] \times \mathbb{R}^n \to \mathbb{R}^+$ est dite appartenir à la classe ν^0 si*

a) V est continu dans $(\tau_{i-1}, \tau_i] \times \mathbb{R}^n \to \mathbb{R}^+$ et pour chaque $x \in \mathbb{R}^n$

$$\lim_{(t,y) \longrightarrow (\tau_i^+, x)} V(t, y) = V(\tau_i^+, x), i = 1, 2, ... \tag{1.17}$$

existe.

b) V est localement Lipschitzienne en x

Définition 5 *[94] Pour $(t, x) \in (\tau_{i-1}, \tau_i] \times \mathbb{R}^n$, nous définissons*

$$D^+ V(t, x) = \lim_{h \longrightarrow 0} sup \frac{1}{h} [V[t + h, x + hf(t, x)] - V(t, x)] \tag{1.18}$$

Définition 6 *[94] Système de comparaison : Soit $V \in \nu_0$ et supposons que*

$$\begin{cases} D^+ V(t, x) \leq g[t, V(t, x)], \quad t \neq \tau_i \\ V[t, x + U(i, x)] \leq \Psi_i[V(t, x)], \quad t = \tau_i \end{cases} \tag{1.19}$$

où $g : \mathbb{R}^+ \times \mathbb{R}^+ \to \mathbb{R}$ est continu et $\Psi_i : \mathbb{R}^+ \to \mathbb{R}^+$ non décroissante. Alors, le système

donné ci-dessous est appelé le système de comparaison du système (1.16).

$$\begin{cases} \dot{w} = g(t,w), \quad t \neq \tau_i \\ w(\tau_i^+) = \Psi_i[w(\tau_i] \\ w(t_0^+) = w_0 \geq 0 \end{cases} \tag{1.20}$$

Définition 7 *[94]* $S_\rho = x \in \mathbb{R}^n \mid \|x\| < \rho$
où $\|.\|$ *désigne la norme euclidienne sur* $\mathbb{R}^n$

Définition 8 *[94] Une fonction* α *est dit appartenir à la classe* κ *si* $\alpha \in C[\mathbb{R}^+, \mathbb{R}^+]$, $\alpha(0) = 0$ *et* $\alpha(x)$ *est strictement croissante en* x*.*

Hypothèse 4 $f(t,0) = 0$, $U(i,0) = 0$ *et* $g(t,0) = 0$ *pour tout* i*. Avec ces hypothèses, les solutions triviales de (1.16) et (1.20) sont identiques pour tous les temps, sauf à l'ensemble des valeurs discrètes* τ_i*.*

Théorème 1 *[94] Supposons que les trois conditions suivantes sont vérifiées.*

a) $V : \mathbb{R}^+ \times S_\rho \to \mathbb{R}^+, \rho > 0, V \in \nu_0, D^+V(t,x) \leq g[t, V(t,x)], \quad t \neq \tau_i$

b) Il existe ρ_0 *tel que* $x \in S_{\rho_0}$ *implique que* $x + U(i,x) \in S_{\rho_0}$ *pour tout* i *et* $V[t, x + U(i,x)] \leq \Psi_i[V(t,x)], t = \tau_i, x \in S_{\rho_0}$.

c) $\beta(\|x\|) \leq V(t,x) \leq \alpha(\|x\|)$ *sur* $\mathbb{R}^+ \times S_\rho$*, où* $\alpha(.), \beta(.) \in \kappa$.

Alors les propriétés de stabilité de la solution triviale du système de comparaison (1.20) implique les propriétés de stabilité correspondantes de la solution triviale (1.16).

Théorème 2 *[94] Soit* $g(t,w) = \dot{\lambda}(t)w, \lambda \in C^1[\mathbb{R}^+, \mathbb{R}^+], \Psi_i(w) = d_i w$ *et* $d_i \geq 0$ *pour tout* i*. Alors l'origine du système (1.16) est asymptotiquement stable si les conditions*

$$\lambda(\tau_{i+1}) + \ln(\gamma d_i) \leq \lambda(\tau_i) \quad pour \quad tout \quad i, \quad \gamma > 1 \tag{1.21}$$

et

$$\dot{\lambda}(t) \geq 0 \tag{1.22}$$

sont satisfaites.

Le but recherché est de concevoir un observateur pour la première équation donnée par (1.16). Pour cela, il faut tenir compte de l'hypothèse suivante :

Hypothèse 5 *a) En raison du comportement chaotique, le vecteur d'état du système (1.16) est dans un domaine ouvert borné* $D \subset \mathbb{R}^n$.

b) $\Phi(x)$ *est globalement Lipschitz dans le domaine* D *et* L *sa constante de Lipschitz.*

c) Toutes les iso Lyapunov (surface de la fonction de Lyapunov d'équation $v(x) = c$ *où* c *est une constante) sont inclus dans le domaine* D.

où $v(x)$ *est une fonction de Lyapunov définie positive.*

Tout d'abord, on écrit la première équation donnée par (1.16) sous la forme suivante :

$$\dot{Z} = AZ + \Phi(Z) \tag{1.23}$$

alors les équations de l'observateur impulsif correspondant au système (1.23) sont données comme suit :

$$\begin{cases} \dot{\hat{Z}} & = & A\hat{Z} + \Phi(\hat{Z}), \quad t \neq \tau_i \\ \delta^+\hat{Z} & = & -BE, \quad t = \tau_i, \quad i = 1, 2, ... \\ \hat{Z}(t_0^+) = Z_0, \quad t_0 \geq 0 \end{cases} \tag{1.24}$$

où E désigne le vecteur des erreurs d'état entre les deux systèmes (1.23) et (3.9) et B une matrice de dimension appropriée.

Alors, le système d'erreur de synchronisation impulsive est donné comme suit :

$$\begin{cases} \dot{E} = AE + \Psi(Z, \hat{Z}), \quad t \neq \tau_i \\ \delta^+E = BE, \quad t = \tau_i, \quad i = 1, 2, ... \end{cases} \tag{1.25}$$

où $\Psi(Z, \hat{Z}) = \Phi(Z) - \Phi(\hat{Z})$

Dans ce qui suit, nous présentons quelques notions sur l'observabilité des systèmes non linéaires en temps discret ainsi que le type d'observateur en temps discret utilisé dans notre travail.

1.4.2 Cas discret

1.4.2.1 Observabilité des systèmes non linéaire

Soit le système non linéaire à temps discret décrit par la forme suivante :

$$\begin{cases} x_{k+1} = f(x_k, u_k) \\ y_k = h(x_k) \end{cases} \tag{1.26}$$

où $x_k \in \mathbb{R}^n$, $u_k = (u_{1k}, ..., u_{mk})^T \in \mathbb{R}^m$ et $y_k \in \mathbb{R}^p$. Pour toute entrée $u_k \in \mathbb{R}^m$ constante, $f_{uk}(x_k) = f(x_k, u_k)$ est un champ de vecteur C^∞ sur $\mathbb{R}^n$ et les h_i pour $i = 1, ..., p$, les composantes de h qui sont des fonctions définies de C^∞ de $\mathbb{R}^n$ sur $\mathbb{R}$.

De même que pour le cas continu, le problème d'observabilité consiste à pouvoir reconstruire tous les états du système à partir de la sortie et de ses itérées. Toutes les définitions d'observabilité sont basées sur la notion d'"indiscernabilité" entre deux états initiaux. Quelques définitions liées à l'observabilité des systèmes non linéaires à temps discret sont reportées dans l'Annexe B.

1.4.2.2 Condition de rang d'observabilité

L'observabilié du système (1.26) peut être aussi vérifiée par la condition de rang d'observabilité.

Définition 9 ***(observabilité au sens du rang)*** *Le système (1.26) est dit observable au sens du rang en $x_0 \in \mathbb{R}^n$ si :*

$$dim(dOh(x_0)) = n \tag{1.27}$$

où l'espace d'observation $O(h)(x_k)$ est défini par :

$$O(h)(x_k) = span(h_i(x_k), h_i \circ f_{u_{1k}}(x_k), ..., h_i \circ f_{u_{1k}} \circ ... \circ f_{u_{lk}}(x_k)) \tag{1.28}$$

tel que : $1 \leq i \leq p$, $u_{1k}, ..., u_{lk} \in \mathbb{R}^n$ et $x_k \in \mathbb{R}^n$.

Cette définition peut être reformulée comme suit :

Définition 10 ***(observabilité au sens du rang)*** *Le système (1.26) est dit observable au sens du rang en $x_0 \in \mathbb{R}^n$ si :*

$$span\{dh, d(f \circ h), ..., d(f^{n-1} \circ h)\} \tag{1.29}$$

est de rang n.

Exemple 4

$$\begin{cases} x_1(n+1) = a - x_2^2(n) - bx_3(n) \\ x_2(n+1) = x_1(n) \\ x_3(n+1) = x_2(n) \\ y = h(x) = x_3 \end{cases} \tag{1.30}$$

où : a, b les paramètres du système et $h(x)$ sa sortie.

Appliquons la condition du rang d'observabilité donnée en (1.29) :

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

Alors $rang(O) = 3 = n$ $\forall x$. Le système est donc globalement faiblement observable.

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

De même que pour le cas continu, dans la transmission de données numériques par synchronisation de systèmes chaotiques discrets, il est important de pouvoir estimer l'entrée inconnue du système en plus de la synchronisation des états. Pour cela, plusieurs types d'observateurs ont été proposés pour les systèmes discrets à entrées inconnues. Parmi ces méthodes, on peut citer l'observateur en temps discret retardé étape par étape [14], [43].

Soit le système donné par (1.26), le problème de l'inversion du système consiste à reconstruire x et u ou une partie de ceux-ci à partir de la sortie $y(.)$ du système et de ses itérés.

De même que pour le cas continu, nous écrivons le système (1.26) de la façon suivante :

$$\begin{cases} x_{k+1} = f(x_k) + g(x_k)u_k \\ y_k = h(x_k) \end{cases} \tag{1.31}$$

dans lequel l'entrée inconnue (perturbation) u_k est considérée être bornée, et les champs de vecteurs $f, g : \mathbb{R}^n \to \mathbb{R}^n$ et $h : U \subset \mathbb{R}^n \to R^m$ sont des champs de vecteurs analytiques. La conception d'un observateur à entrées inconnues est réalisable localement au voisinage de x_0 si les conditions données par les hypothèses suivantes sont vérifiées :

Hypothèse 6 *La perturbation (entrée inconnue) est bornée.*

Hypothèse 7 *span* $\{dh, df \circ h, ..., df^{n-1} \circ h\}$ *est de rang* n *en* x_0.

Hypothèse 8 $O.g = ((dh)^T, (d(f \circ h))^T, ..., (d(f^{n-1} \circ h))^T)^T g = (0, ..., \theta)^T$.

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

La condition donnée dans l'hypothèse 8 est appelée condition de recouvrement d'observabilité pour les systèmes discrets. Cette condition garantie la propriété d'inversibilité à gauche, c'est à dire la possibilité de retrouver tous les états et le message à partir de la sortie y et de ses itérés (voir [43] pour plus de détails).

Exemple 5 *Considérons le système donné par l'exemple 4 où* $u(n)$ *est l'entrée inconnue du système.*

$$\begin{cases} x_1(n+1) = a - x_2^2(n) - bx_3(n) + u(n) \\ x_2(n+1) = x_1(n) \\ x_3(n+1) = x_2(n) \end{cases} \tag{1.32}$$

On veut tester la condition de recouvrement d'observabilité de ce système. La première étape consiste alors à tester sa condition d'observabilité. Dans cet exemple, nous avons montré que le système est localement faiblement observable (voir exemple 4). Nous étudions maintenant la condition de recouvrement d'observabilité et l'inversibilité à gauche du système donnée par l'hypothèse 8.

Nous écrivons d'abord le système sous la forme analytique donnée par (1.31).

où $g(x) = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$. *Calculons maintenant :*

$$Og(x) = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \theta = 1 \end{pmatrix}$$

avec $\theta = 1 \neq 0$. *Ainsi, la condition de recouvrement d'observabilité donnée par l'hypothèse 8 est vérifiée, il est alors possible d'extraire l'entrée inconnue à l'aide d'un observateur discret.*

1.4.2.4 Etude de l'observateur chaotique discret retardé étape par étape

L'observateur discret retardé étape par étape consiste à la reconstruction de tous les états et le message du système original à partir de la sortie transmis et de ses itérés. Ceci est possible si les deux hypothèses (7 et 8) citées précédemment sont vérifiées. Ici, la reconstruction sera faite étape par étape. La première étape consiste à appliquer un retard sur la sortie (itération $n-1$) et ensuite, reconstruire le premier état du système original. La seconde étape consiste à appliquer deux retards sur la sortie (itération $n-2$) et un retard (itération $n-1$) sur l'état reconstruit précédemment afin de reconstruire le second état. Cette opération sera appliquée sur tous les états jusqu'à la dernière information, qui contient l'entrée du système original. En résumé, on peut dire donc, que chaque état reconstruit à l'itération de n intervient dans la reconstruction du prochain état à l'itération $n-1$. (voir les travaux [14], [43]).

La section suivante est consacrée à l'application de deux méthodes de synchronisation, l'une de type passif et l'autre de type impulsif afin de synchroniser deux systèmes chaotiques de Qi.

1.5 Synchronisation passive et impulsive du système de Qi

Quelques rappels sur la synchronisation impulsive ont été présentés dans la section précédente. Dans le but d'illustrer le principe de la synchronisation passive, quelques notions de base sur les systèmes passifs sont données ci-dessous.

La passivité est une propriété qui est liée à la fois à la notion de stabilité interne (c'est à dire au sens Lyapunov) et à la notion de stabilité entrée-sortie.
Considérons le système non linéaire donné comme suit :

$$\begin{cases} \dot{x} = f(x) + g(x)u \\ y = h(x) \end{cases} \tag{1.33}$$

dans lequel $x \in \mathbb{R}^n$ est l'espace d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée, et $y \in \mathbb{R}^m$ représente le vecteur de sortie du système. Les fonctions $f(x)$, $g(x)$ et $h(x)$ sont des champs de vecteurs. Nous supposons que le champ de vecteur f a au moins un point équilibre. Sans perte de généralités, nous supposons également que ce point d'équilibre est à l'origine c'est à dire $x = 0$. Si le point d'équilibre n'est pas à l'origine, nous pouvons par une transformation de coordonnées le ramener à l'origine.

Définition 11 *(Système à minimum de phase) [163] Le système donné par (1.33) est à minimum de phase si la jacobienne $L_g h(0)$ est non singulière et $x = 0$ est l'un des points d'équilibre asymptotiquement stable du champ de vecteur f.*

Définition 12 *(Passivité) [160] Le système donné par (1.33) est passif si il existe une constante réelle β, telle que pour tout $t \geq 0$,*

$$\int_0^t u^T(\tau) y(\tau) d\tau \geq \beta, \tag{1.34}$$

ou bien, il existe une constante $\rho > 0$ et une constante réelle β, telle que pour tout $t \geq 0$,

$$\int_0^t u^T(\tau) y(\tau) d\tau + \beta \geq \rho \int_0^t y^T(\tau) y(\tau) d\tau. \tag{1.35}$$

Soit $z = \varphi(x)$ une transformation de coordonnées, le système (1.33) peut être représenté par la forme normale suivante :

$$\begin{cases} \dot{z} = f(z) + g(z, y)y \\ \dot{y} = l(z, y) + k(z, y)u \end{cases} \tag{1.36}$$

où $k(z, y)$ est non singulière pour tout (z, y).

Le système non linéaire (1.36) peut être rendu passif par une commande en boucle

fermée de la forme suivante [160] :

$$u = \gamma(z, y) + \theta(z, y)\upsilon \tag{1.37}$$

où υ est un signal de référence extérieur.

Dans ce qui suit, nous allons appliquer les deux méthodes de synchronisation sur deux systèmes chaotiques de Qi.

1.5.1 Présentation du système chaotique de Qi

Dans cette partie, nous allons présenter le système dit de Qi. Ce dernier est très utilisé dans le domaine des transmissions sécurisées de données, car il présente l'avantage d'être hyperchaotique en raison de ses 2 exposants de Lyapunov positifs (voir Annexe A). Il est donné dans les cas autonome et non autonome.

Le système chaotique à quatre dimension dit de Qi est donné comme suit [132] :

$$\begin{cases} \dot{x_1} = a(x_2 - x_1) + x_2x_3x_4 \\ \dot{x_2} = b(x_1 + x_2) - x_1x_3x_4 \\ \dot{x_3} = -cx_3 + x_1x_2x_4 \\ \dot{x_4} = -dx_4 + x_1x_2x_3 \end{cases} \tag{1.38}$$

où $c = c_1 + c_2 \sin(t)$, et a, b, c_1, c_2, d sont tous paramètres constants positifs. Pour avoir un comportement chaotique, les paramètres du système de Qi (1.38) sont donnés comme suit :

- Cas autonome

  $a = 35, b = 10, c_1 = 1, c_2 = 0, d = 10.$
- Cas non autonome

  $a = 30, b = 10, c_1 = 95, c_2 = 10, d = 10.$

Les figures 1.7 et 1.8 montrent les attracteurs chaotiques du système (1.38) dans les deux cas autonome et non autonome.

1.5.2 Synchronisation passive du système chaotique de Qi

La synchronisation passive de deux systèmes chaotiques identiques de Qi est étudiée ci-dessous.

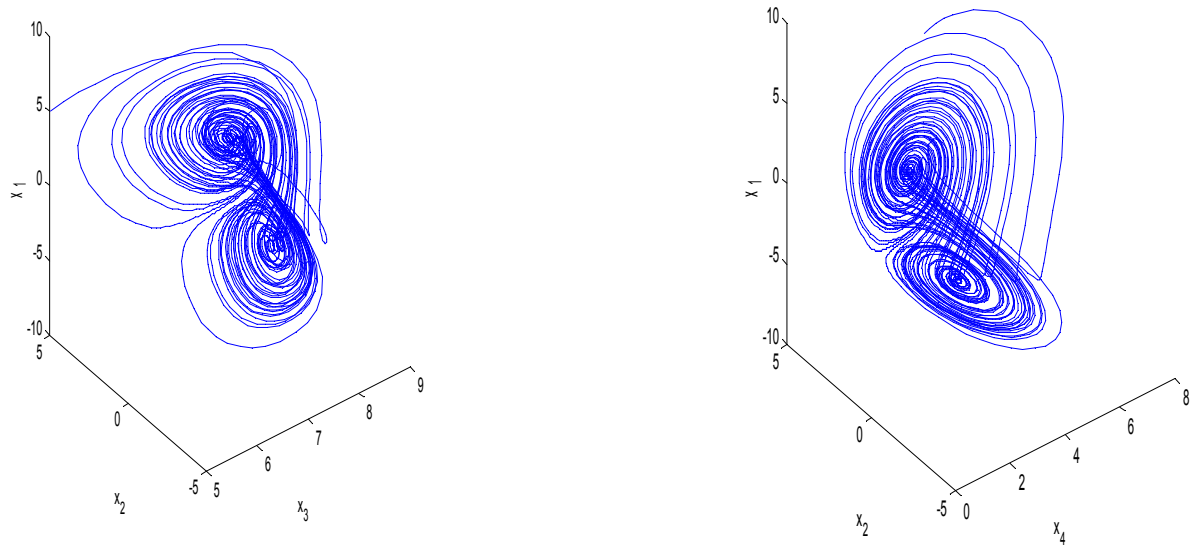


FIG. 1.7: Attracteurs chaotiques du système de Qi : cas autonome

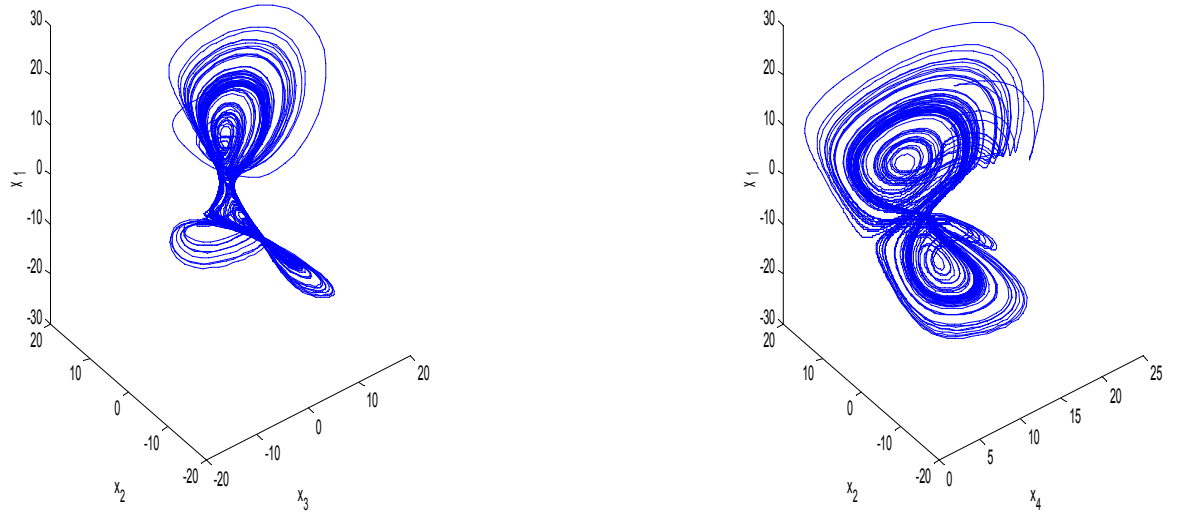


FIG. 1.8: Attracteurs chaotiques du système de Qi : cas non autonome

Supposons que les équations de l'émetteur sont données par (1.38) et les équations du

récepteur sont :

$$\begin{cases} \dot{y_1} = a(y_2 - y_1) + y_2 y_3 y_4 \\ \dot{y_2} = b(y_1 + y_2) - y_1 y_3 y_4 + u \\ \dot{y_3} = -cy_3 + y_1 y_2 y_4 \\ \dot{y_4} = -dy_4 + y_1 y_2 y_3 \end{cases} \tag{1.39}$$

où u est une loi de commande. Soient : $e_1 = y_1 - x_1$, $e_2 = y_2 - x_2$, $e_3 = y_3 - x_3$ et $e_4 = y_4 - x_4$ les erreurs sur les états des systèmes (1.38) et (1.39). Le système d'erreurs dynamiques est donnée comme suit :

$$\begin{cases} \dot{e_1} = a(e_2 - e_1) + y_2 y_3 y_4 - x_2 x_3 x_4 \\ \dot{e_2} = b(e_1 + e_2) - y_1 y_3 y_4 + x_1 x_3 x_4 + u \\ \dot{e_3} = -ce_3 + y_1 y_2 y_4 - x_1 x_2 x_4 \\ \dot{e_4} = -de_4 + y_1 y_2 y_3 - x_1 x_2 x_3 \end{cases} \tag{1.40}$$

Le système (1.40) est bien sous la forme normale donnée par (1.36), où : $z_1 = e_1$, $z_2 = e_3$, $z_3 = e_4$, $y = e_2$ et $z = [z_1, z_2, z_3]^T$,

$$f(z) = [-az_1 + y_2 y_3 y_4 - x_2 x_3 x_4, -cz_2 + y_1 y_2 y_4 - x_1 x_2 x_4, -dz_3 + y_1 y_2 y_3 - x_1 x_2 x_3]^T,$$

$$g(z, y) = [a, 0, 0]^T, \quad l(z, y) = bz_1 + by - y_1 y_3 y_4 + x_1 x_3 x_4, \quad k(z, y) = 1 \tag{1.41}$$

Notre objectif consiste à concevoir une loi de commande donnée par (1.37) afin de rendre le système en boucle fermée (1.40) passif. Pour cela, il faut d'abord satisfaire la condition qui est donnée par la définition 11. Les deux théorèmes suivants découlent des résultats établis dans [81].

Théorème 3 *Le système d'erreurs donné par (1.40) est à minimum de phase.*

Preuve.

Choisissons la fonction de stockage suivante :

$$V(z, y) = W(z) + \frac{1}{2} y^2 \tag{1.42}$$

où $W(z)$ est une fonction de Lyapunov de $f(z)$ avec $W(0) = 0$,

$$W(z) = \frac{1}{2}(z_1^2 + z_2^2 + z_3^2) \tag{1.43}$$

La dynamique des zéros du système (1.40) décrit ces dynamiques internes qui sont conformées à la contrainte externe $y = 0$, c'est à dire,

$$\dot{z} = f(z) \tag{1.44}$$

Considérons le système (40) :

$$\frac{d}{dt}W(z) = \frac{\partial W(z)}{\partial z}f(z) = [z_1 \quad z_2 \quad z_3]f(z)$$

$$\begin{aligned} &= (-az_1 + y_2y_3y_4 - x_2x_3x_4)z_1 + (-cz_2 + y_1y_2y_4 - x_1x_2x_4)z_2 \\ &+ (-dz_3 + y_1y_2y_3 - x_1x_2x_3)z_3 \leq 0 \end{aligned} \tag{1.45}$$

Donc, $f(z)$ est globalement asymptotiquement stable au point d'équilibre $(0, 0, 0, 0)$. Au même temps, $L_gh(0) = 1$ est non singulière. Alors le système d'erreurs (1.40) est à minimum de phase et il peut être équivalent à un système passif par un retour d'état appropié. □

Le retour d'état permettant de rendre le système (1.40) passif est donné par le théorème suivant :

Théorème 4 *Le système d'erreurs (1.40) peut être équivalent à un système passif et globalement asymptotiquement stabilisé par le retour d'état suivant :*

$$\begin{aligned} u &= k^{-1}(z, y)[-l^T(z, y) - \frac{\partial W}{\partial z}g(z, y) - \gamma y + \upsilon] \\ &= -(a + b)z_1 - (b + \gamma)y + y_1y_2y_3 - x_1x_2x_3 + \upsilon \end{aligned} \tag{1.46}$$

où γ est une constante positive dans notre cas.

Preuve.

La dérivée de $V(z,y)$ le long de la trajectoire du système d'erreurs (1.40) est :

$$\begin{aligned}\frac{d}{dt}V(z,y) &= \frac{\partial}{\partial z}W(z)\dot{z} + y\dot{y} \\ &= \frac{\partial}{\partial z}W(z)f(z) + \frac{\partial}{\partial z}W(z)g(z,y)y + l(z,y)y + k(z,y)uy\end{aligned} \tag{1.47}$$

Du théorème 3, le système donné par (1.40) est à minimum de phase.

$$\frac{\partial W(z)}{\partial z}f(z) \leq 0, \tag{1.48}$$

alors l'équation (42) devient :

$$\frac{d}{dt}V(z,y) \leq \frac{\partial}{\partial z}W(z)g(z,y)y + (l(z,y) + k(z,y)u)y \tag{1.49}$$

En substituant l'équation (42) dans (44), nous obtenons :

$$\frac{d}{dt}V(z,y) \leq -\gamma y^T y + \upsilon^T y \tag{1.50}$$

En intégrant les 2 membres de l'inégalité (1.50)

$$V(z,y) - V(z_0,y_0) \leq \int_0^t -\gamma y^T(\tau)y(\tau)d\tau + \int_0^t \upsilon^T(\tau)y(\tau)d\tau \tag{1.51}$$

Soit $\rho = V(z_0,y_0)$ et nous avons $V(z,y) \geq 0$, alors :

$$\int_0^t \upsilon^T(\tau)y(\tau)d\tau + \rho \geq V(z,y) + \int_0^t -\gamma y^T(\tau)y(\tau)d\tau \geq \int_0^t -\gamma y^T(\tau)y(\tau)d\tau \tag{1.52}$$

Nous constatons bien que l'équation (48) vérifie la définition 12. Donc, le retour d'état donné par (42) peut rendre le système (1.40) passif. □

1.5.3 Synchronisation impulsive du système chaotique de Qi

Maintenant, considérons le système d'erreurs donné par (1.40) avec un retour d'état nul ($u = 0$). Ce système peut être décomposé en une partie linéaire et non linéaire donné comme suit :

$$\dot{e} = Ae + \Phi(e) \tag{1.53}$$

où :

$$e = (e_1, e_2, e_3)^T, \quad A = \begin{bmatrix} -a & a & 0 & 0 \\ b & b & 0 & 0 \\ 0 & 0 & -c & 0 \\ 0 & 0 & 0 & -d \end{bmatrix},$$

et

$$\Phi(e) = \begin{bmatrix} y_2y_3y_4 - x_2x_3x_4 \\ -y_1y_3y_4 + x_1x_3x_4 \\ y_1y_2y_4 - x_1x_2x_4 \\ y_1y_2y_3 - x_1x_2x_3 \end{bmatrix}. \tag{1.54}$$

Donc, le système (1.53) peut être écrit sous la forme donnée par (1.25).

Dans ce qui suit, on définit les notation suivantes :

$$\lambda'(A) = \frac{1}{2}\lambda_{max}(A + A^T) \tag{1.55}$$

$$\beta_i = \lambda_{max}[(I + B_i)^T(I + B_i)] \tag{1.56}$$

où I est une matrice identité de dimension $n \times n$, $\lambda'(A)$ est la valeur propre maximale de la matrice $A + A^T$ et β_i la valeur propre maximale de la matrice $[(I + B_i)^T(I + B_i)]$. Le théorème suivant découle des résultats établis dans [80].

Théorème 5 *1. Si $2\lambda'(A) = \lambda < 0$ (λ est une constante) et s'il existe une constante $0 \leq \alpha < -\lambda$, telle que :*

$$\ln \beta_i - \alpha(\tau_i - \tau_{i-1}) \leq 0, k = 1, 2, ... \tag{1.57}$$

Alors, la solution du système (1.25) est globalement exponentiellement stable.

2. Si $2\lambda'(A) = \lambda \geq 0$ (λ est une constante) et il existe une constante $\alpha \geq 1$, telle que :

$$\ln(\alpha\beta_i) + \lambda(\tau_{i+1} - \tau_i) \leq 0, k = 1, 2, ... \tag{1.58}$$

Alors $\alpha = 1$ implique que la solution du système (1.25) est stable et $\alpha > 1$ implique que la solution triviale du système (1.25) est globalement asymptotiquement stable.

Preuve.

Considérons la fonction de Lyapunov donnée par la forme : $V(e) = e^T e$. Pour $t \neq \tau_i$, nous avons :

$$\begin{aligned} D^+V(t,e) &= \dot{e}^T e + e^T \dot{e} = (Ae + \Phi)^T e + e^T(Ae + \Phi) \\ &= e^T(A^T + A)e + \Phi^T e + e^T \Phi \\ &\leq 2\lambda'(A)v(e(t)), t \in (\tau_{i-1}, \tau_i], i = 1, 2, ... \end{aligned} \tag{1.59}$$

Ce qui implique que :

$$V(e(t)) \leq V(e(\tau_{i-1}^+)) \exp(2\lambda'(A)(t - \tau_{i-1})), t \in (\tau_{i-1}, \tau_i], i = 1, 2, ... \tag{1.60}$$

A partir de l'équation (1.25), on a :

$$\begin{aligned} V(\tau_i^+) &= ([I + B_i)e(\tau_i)]^T (I + B_i)e(\tau_i) \\ &\leq \beta_i V(e(\tau_i)), i = 1, 2, ... \end{aligned} \tag{1.61}$$

A partir des équations (1.60) et (1.61) et pour $t \in (\tau_0, \tau_1]$, on a :

$$V(e(t)) \leq V(e(t_0^+)) \exp(2\lambda'(A)(\tau_1 - \tau_0)) \tag{1.62}$$

ceci correspond à :

$$V(e(\tau_1)) \leq V(e(\tau_0^+)) \exp(2\lambda'(A)(\tau_1 - \tau_0)) \tag{1.63}$$

$$V(\tau_1^+) \leq \beta_1 V(e(\tau_1))$$

$$et : \leq \beta_1 V(e(\tau_0^+)) \exp(2\lambda'(A)(\tau_1 - \tau_0)) \tag{1.64}$$

Par conséquent, pour $t \in (\tau_1, \tau_2]$

$$\begin{aligned} V(e(t)) &\leq V(e(\tau_1^+)) \exp(2\lambda'(A)(t - \tau_1)) \\ &\leq \beta_1 V(e(\tau_0)) \exp(2\lambda'(A)(t - \tau_0)) \end{aligned} \tag{1.65}$$

En général, pour $t \in (\tau_i, \tau_{i+1}]$

$$V(e(t)) \leq V(e(\tau_0^+))\beta_1\beta_2...\beta_i \exp(2\lambda'(A)(t-\tau_0)) \tag{1.66}$$

1. Lorsque $2\lambda'(A) = \lambda < 0$, et à partir des équations (1.25) et (1.66), avec $t \in (\tau_i, \tau_{i+1}]$

$$\begin{aligned} &V(e(\tau_0^+))\beta_1\beta_2...\beta_i \exp(2\lambda'(A)(t-\tau_0)) \\ &= V(e(\tau_0^+))\beta_1\beta_2...\beta_i \exp(\lambda(t-\tau_0)) \\ &= V(e(\tau_0^+))\beta_1\beta_2...\beta_i \exp(-\alpha(t-\tau_0)) \exp((\alpha+\lambda)(t-\tau_0)) \end{aligned}$$

   Alors :

$$\begin{aligned} V(e(t)) &\leq V(e(\tau_0^+))\beta_1\beta_2...\beta_i \exp(-\alpha(\tau_i - t_0)) \exp((\alpha+\lambda)(t-\tau_0)) \\ &\leq V(e(\tau_0^+)) \exp((\alpha+\lambda)(t-\tau_0)) \end{aligned} \tag{1.67}$$

   Ce qui implique que la solution du système (1.25) est globalement asymptotiquement stable.

2. Lorsque $2\lambda'(A) = \lambda \geq 0$, et à partir des systèmes (1.59) et (1.66), avec $t \in (\tau_i, \tau_{i+1}]$, on a :

$$\begin{aligned} V(e(t)) &\leq V(e(\tau_0^+))\beta_1\beta_2...\beta_i \exp(2\lambda'(A)(t-\tau_0)) \\ &\leq V(e(\tau_0^+))\beta_1\beta_2...\beta_i \exp(\lambda(\tau_{i+1}-\tau_0)) \\ &\leq V(e(\tau_0^+))\beta_1 \exp(\lambda(\tau_1-\tau_0))\beta_2 \exp(\lambda(\tau_3-\tau_2))... \\ &\quad \beta_i \exp(\lambda(\tau_{i+1}-\tau_i)) \exp(\lambda(\tau_1-\tau_0)) \\ &\leq V(e(\tau_0^+))\frac{1}{\alpha^i} \exp(\lambda(\tau_1-\tau_0)) \end{aligned} \tag{1.68}$$

□

Il est à noter qu'en pratique, les matrices B_i sont choisies de telles manières que leurs gains soient constants et les distances impulsives $\Delta = \tau_i - \tau_{i-1}$ $(i = 1, 2, ...)$ soient positives

et constantes. Nous avons le corollaire suivant :

Corollary 1 *Supposons que* $\tau_i = \tau > 0$ *et les matrices* $B_i = B$, $(i = 1, 2, ...)$

1. *Si* $2\lambda'(A) = \lambda < 0$ *(*λ *est une constante) et il existe une constante* $0 \leq \alpha < -\lambda$, *telle que* $\ln \beta_i - \alpha\tau \leq 0$, *alors la solution du système (1.25) est globalement exponentiellement stable.*

2. *Si* $2\lambda'(A) = \lambda \geq 0$ *et il existe une constante* $\alpha \geq 1$, *telle que* $\ln(\alpha\beta_i) + \lambda\alpha\tau \leq 0$, *lors la solution triviale du système (1.25) est globalement asymptotiquement stable.*

Les résultats des synchronisations impulsive et passive appliquées aux deux systèmes de Qi sont donnés ci-dessous.

1.5.4 Résultats de simulation

Dans cette section, des résultats de simulation effectués sous Matlab seront présentés afin d'illustrer les performances des deux méthodes proposées. Dans toutes les simulations, nous avons appliqué la méthode de Runge-Kutta d'ordre quatre avec un pas de 0.01s pour résoudre les équations différentielles. Les valeurs initiales choisies des états de l'émetteur (1.38) sont $x_1(0) = 1$, $x_2(0) = 1$, $x_3(0) = 1$, $x_4(0) = 1$ et celles du récepteur (1.39) sont $y_1(0) = -1$, $y_2(0) = -5$, $y_3(0) = 1$, $y_4(0) = 1$.

Pour la synchronisation passive, nous avons appliqué la commande par retour d'état (42) en choisissant la valeur de $\gamma = 11$ et $\upsilon = 0$.

Les figures 1.9 et 1.10 montrent les réponses des états ainsi que les erreurs de synchronisation de l'émetteur (1.38) et de son récepteur (1.39) dans les deux cas autonome et non autonome. Ici, les états de l'émetteur sont représentés par des lignes continues et ceux du récepteur en lignes discontinues. Ces figures montrent bien que les erreurs de synchronisation des systèmes (1.38) et (1.39) convergent vers zéro.

Pour la synchronisation impulsive, nous avons $A + A^T = \begin{pmatrix} 70 & 45 & 0 & 0 \\ 45 & 20 & 0 & 0 \\ 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & -20 \end{pmatrix}$

Les valeurs propres de $A + A^T$ sont : $\lambda_1 = -20.00$, $\lambda_2 = -6.48$, $\lambda_3 = -2.00$ et $\lambda_4 = 96.48$. Donc, $2\lambda'(A) = \lambda = 96.48 > 0$.

Les matrices $B_i, (i = 1, 2, ...)$ sont choisies comme une matrice constante notée B, telle que : $B = \begin{bmatrix} -0.3 & 0 & 0 & 0 \\ 0 & -0.4 & 0 & 0 \\ 0 & 0 & -0.5 & 0 \\ 0 & 0 & 0 & -0.6 \end{bmatrix}$.

En utilisant l'équation (1.56), il est alors facile de constater que : $\beta_i = 0.49$. Donc, les instants d'application de la commande impulsive afin de synchroniser les deux systèmes (34) et (35) sont donnés par $0 \leq \tau \leq \frac{\ln \alpha + \ln(0.49)}{96.48}$. En choisissant $\alpha = 1.1$, alors $0 \leq \tau \leq 0.0064$.

Les figures 1.11 et 1.12 montrent les réponses des états ainsi que les erreurs de synchronisation de l'émetteur (1.38) et de son récepteur (1.39) dans les deux cas autonome et non autonome avec $\tau = 0.001s$. Ici, les états de l'émetteur sont représentés par des lignes continues et ceux du récepteur en lignes discontinues. Ces figures montrent bien que les erreurs de synchronisation des systèmes (1.38) et (1.39) convergent aussi vers zéro.

1.6 Transmission basée sur la synchronisation de systèmes chaotiques

En transmission sécurisée d'information binaire, le message appelé "texte" est transformé de manière à le rendre incompréhensible. Ce processus est appelé "chiffrement" ou "cryptage". Par ailleurs, le destinataire doit engager un processus, appelé "déchiffrement" ou "décryptage", pour reconstruire le message à partir du texte chiffré. Pour cela, des algorithmes sont utilisées, qui sont en effet des fonctions mathématiques destinées au chiffrement et déchiffrement du message. Afin de transmettre le message d'une manière sûre, un élément appelé "clé" de cryptage est introduit, qui est utilisé par l'expéditeur et le destinataire. Cette clé peut prendre des valeurs parmi un grand nombre de valeurs possibles. Certains algorithmes utilisent des clés différentes pour le chiffrement et le déchiffrement. Avec ces algorithmes, toute la sécurité réside dans la (les) clé(s) et non pas dans l'algorithme. Alors un espion, même s'il connaît l'algorithme, ne peut pas détecter le message s'il ne connaît pas la clé.

On distingue deux types de clés : clé "secrète" et clé "publique". Dans un algorithme à clé secrète, la clé de chiffrement est calculée à partir de la clé de déchiffrement et vice-

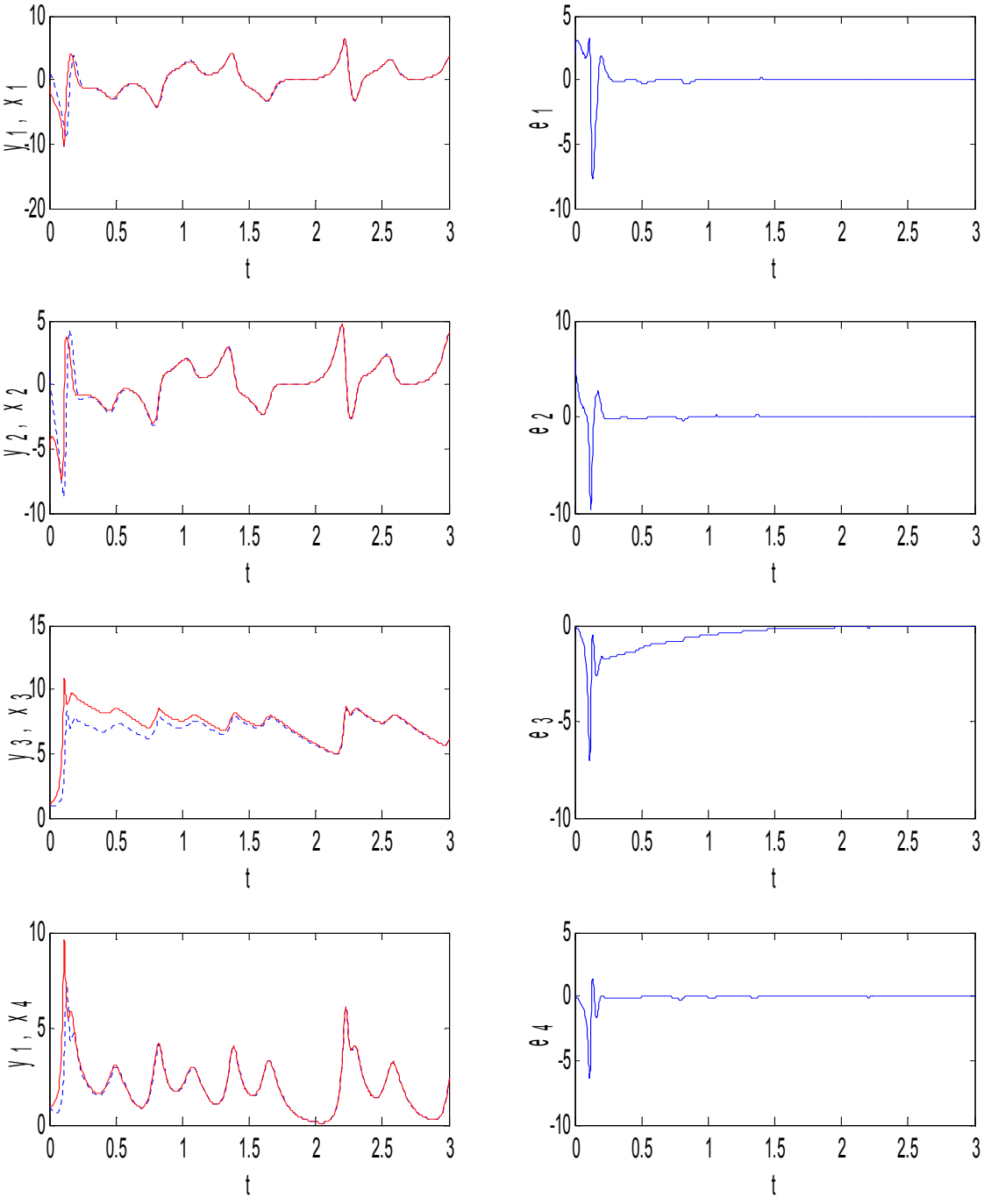


FIG. 1.9: Synchronisation passive du système chaotique de Qi : cas autonome

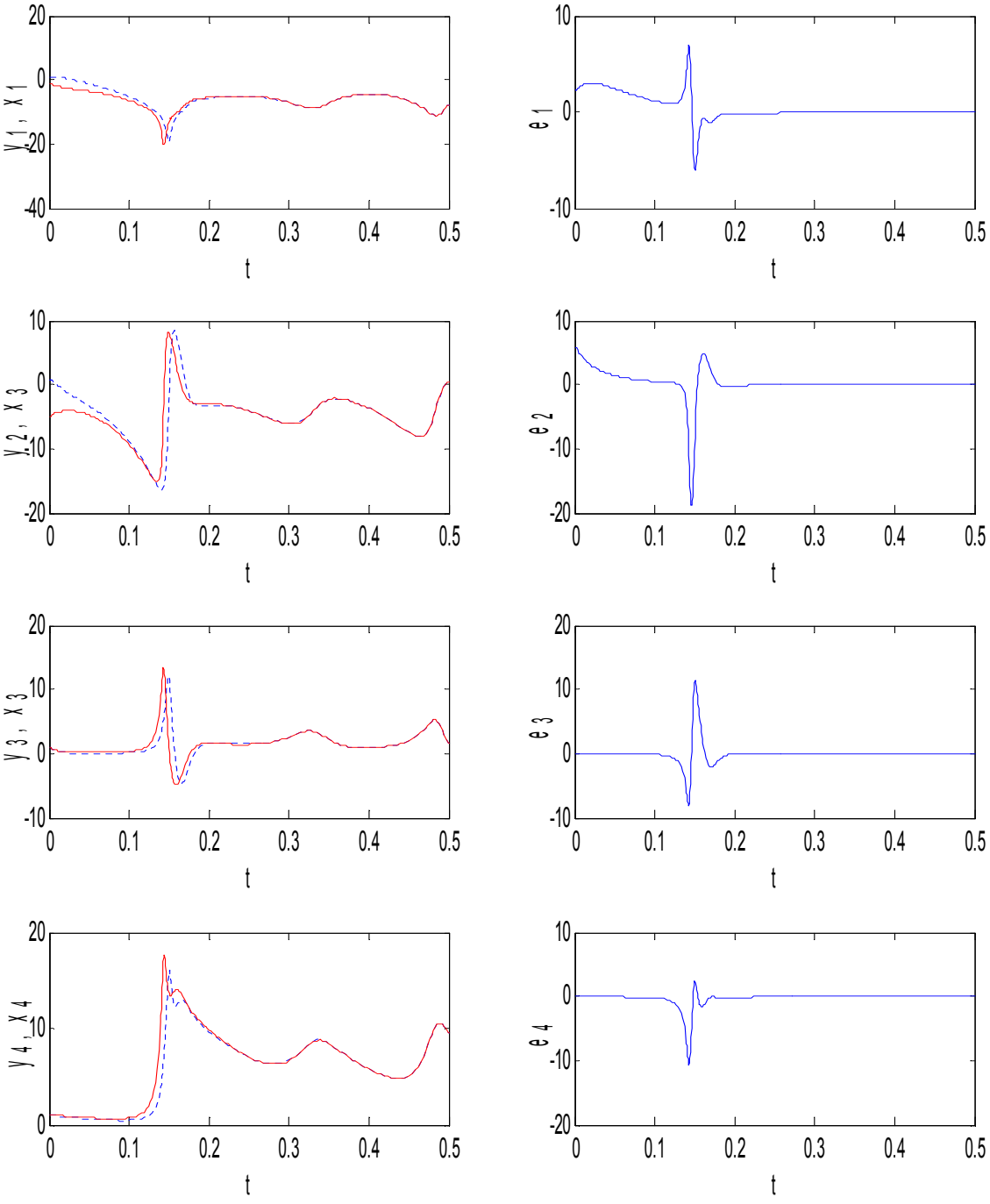


FIG. 1.10: Synchronisation passive du système chaotique de Qi : cas non autonome

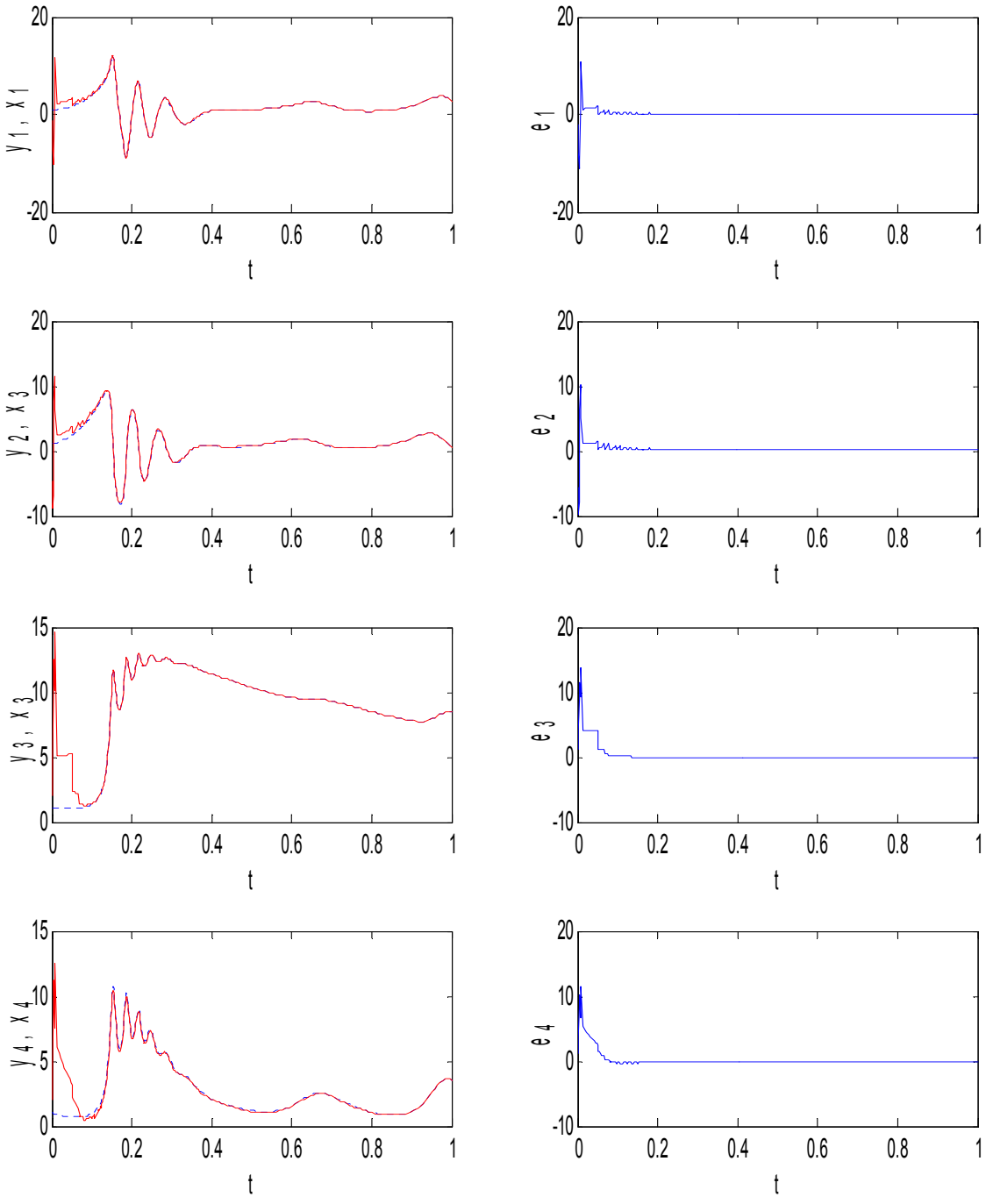


FIG. 1.11: Synchronisation impulsive du système chaotique de Qi : cas autonome

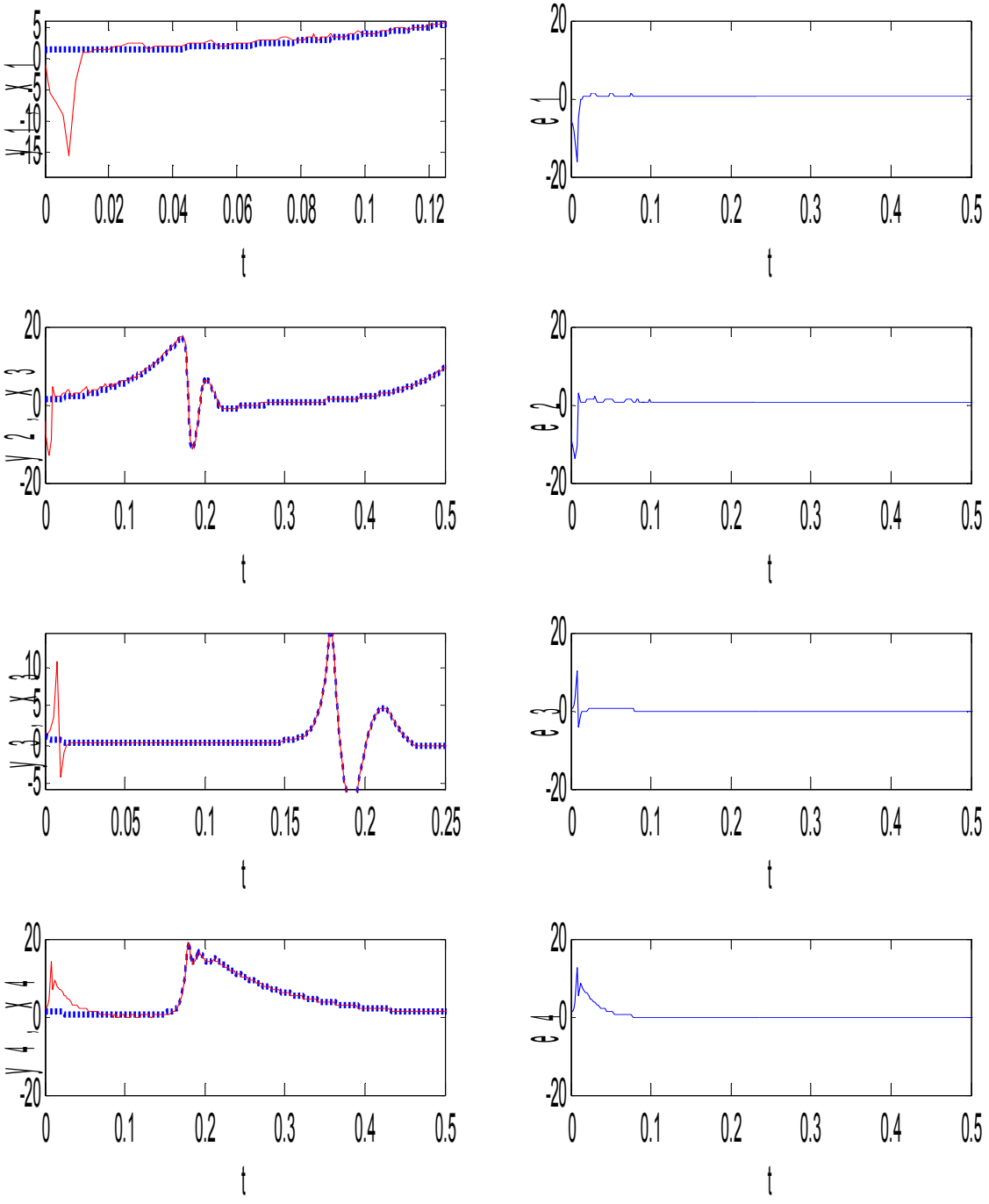


FIG. 1.12: Synchronisation impulsive du système chaotique de Qi : cas non autonome

versa. Dans la plupart des cas, les deux clés sont identiques, l'expéditeur et le destinataire se mettent d'accord sur une clé avant d'échanger des messages. Ainsi, si cette clé secrète est dévoilée, n'importe qui peut lire le message.

Un algorithme à clé publique utilise des clés différentes au niveau du chiffrement et du déchiffrement. De plus, ces clés ne peuvent pas être calculées l'une à partir de l'autre. Ainsi, la clé de chiffrement peut être rendue publique, mais seul celui qui possède la clé de déchiffrement peut lire le message. La clé de déchiffrement est alors appelée clé "privée".

L'idée d'utiliser les signaux aléatoires pour la communication sécurisée a été mise en oeuvre en 1926 par Vernam [148]. Il proposa dans son article d'utiliser un alphabet binaire et coder chaque bit à l'aide d'un bit de la clé, choisi de façon arbitraire. Plus tard, dans les années 90, cette idée a été développée dans le contexte des signaux chaotiques [123], [124] [153]. A cause de la nature imprédictible à long terme du chaos (voir Annexe A), on a cru pendant longtemps que le chaos serait inutilisable et incontrôlable, mais depuis quelques années, les chercheurs ont réussi à modéliser le chaos par des équations différentielles et montré qu'il existe un coté déterministe dans ce phénomène qui apparaît aléatoire à première vue. C'est cette nature semblable aux signaux aléatoires qui a motivé les chercheurs d'essayer de camoufler un message confidentiel à l'aide d'un signal chaotique, de façon à ne pas pouvoir le distinguer. Ainsi différentes méthodes ont été proposées afin de masquer le message dans un système chaotique et ensuite le restaurer. Ces méthodes sont toutes basées sur la synchronisation des systèmes chaotiques et ont été améliorées au fil des années dans le but d'augmenter de plus en plus la sécurité et la rapidité de transmission de l'information. Ces méthodes sont parfois appelées méthodes de cryptographie chaotique.

En parallèle avec le chiffrage d'informations discrètes ou binaires, des recherches ont été effectuées afin de pouvoir appliquer les méthodes de cryptographie aux informations continues. Grâce aux résultats obtenus en synchronisation des systèmes chaotiques [128], il a été possible d'employer des signaux chaotiques continus comme porteur d'informations. Dans ce cas, le message est codé par l'émetteur et il est décodé et extrait du signal chaotique par le récepteur. Parmi les méthodes de transmission chaotiques, on peut citer le cryptage par addition, le cryptage par commutation, le cryptage par modulation, le cryptage par inclusion.

1.6.1 Cryptage par addition

Dans cette méthode appelée, masquage chaotique, l'émetteur est un système chaotique autonome dont le signal de sortie $y(t)$ est ajouté au signal du message $m(t)$. La somme de deux signaux est transmise au récepteur à travers le canal de transmission, qui est un canal public. Le récepteur est constitué d'un système chaotique identique à l'émetteur et un simple soustracteur. Ainsi, après la synchronisation des deux systèmes chaotiques (émetteur et récepteur), le message est extrait à l'aide d'une opération de soustraction [37], [87]. Notons que dans cette méthode, l'attracteur étrange du système chaotique n'est pas modifié par le message. L'inconvénient de cette méthode est qu'afin de garantir la synchronisation, le message doit être au moins de 20 à 30 dB inférieur à la sortie de l'émetteur. Or, en présence d'un bruit de canal d'une puissance proche de celle du message, il devient difficile de détecter l'information. De plus, cette méthode reste sensible aux attaques extérieures [140] et l'usage du canal de transmission est inefficace du point de vue de l'énergie transmise par rapport à la qualité d'information fournie [155]. Le schéma représentant cette méthode est donné par la figure 1.13.

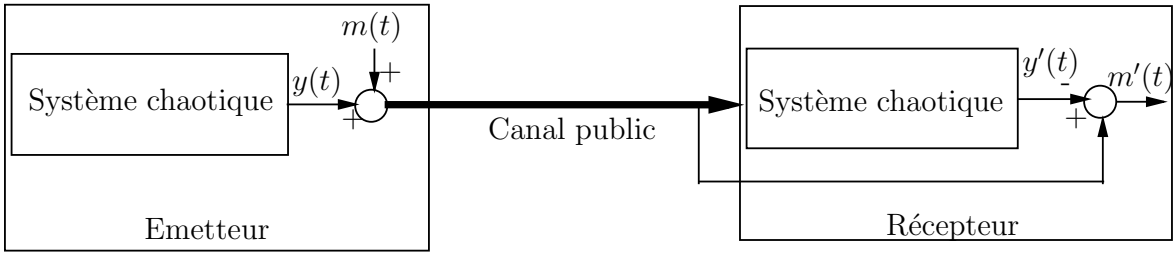


FIG. 1.13: Méthode par addition

1.6.2 Cryptage par commutation

Cette méthode (en anglais Chaos Shift Keying, CSK) est utilisée pour transmettre un message binaire (voir figure 1.14). L'émetteur est composé de deux systèmes chaotiques et pour chaque niveau de message $m(t)$ (0 ou 1), l'un des systèmes envoie sa sortie sur la ligne de transmission. Ainsi, le signal transmis commute entre deux attracteurs étranges. Le récepteur est constitué de deux systèmes chaotiques identiques à ceux de l'émetteur. Pour chaque valeur du message, l'un des deux systèmes se synchronise avec l'émetteur et un bloc de comparaison permet de relever la valeur du message notée $m'(t)$ [34], [41]. Il est à noter que cette méthode reste sensible aux attaques détaillées dans [50].

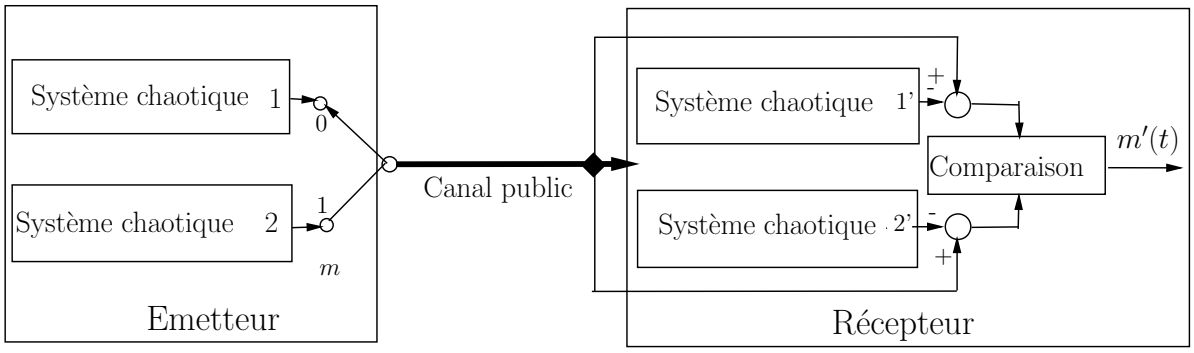


FIG. 1.14: Principe de cryptage par commutation

1.6.3 Cryptage par modulation

Cette technique, développée dans [7], [20], [95], utilise le message contenant l'information pour moduler un paramètre de l'émetteur chaotique. Un contrôleur adaptatif est chargé de maintenir la synchronisation au niveau du récepteur, tout en suivant les changements du paramètre modulé. Le schéma correspondant est présenté à la figure 1.15. Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la

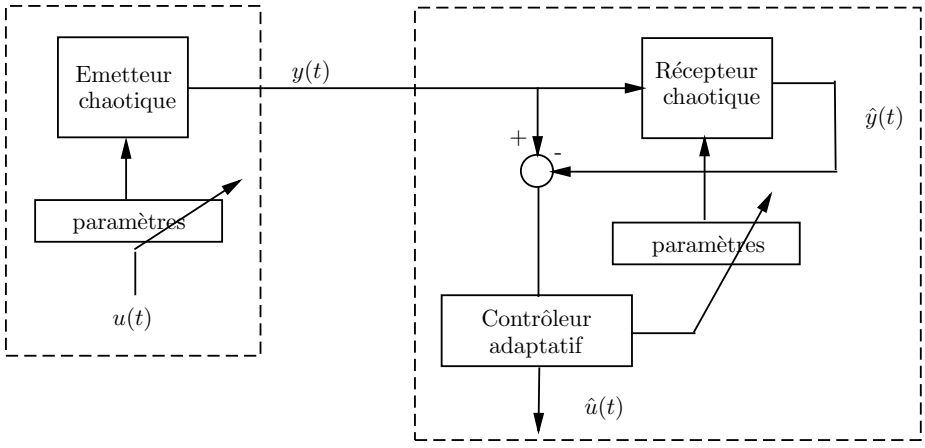


FIG. 1.15: Principe de cryptage par modulation

trajectoire de changer continûment d'attracteur, et de ce fait, le signal transmis est plus complexe qu'un signal chaotique "normal". Cependant, la façon d'injecter le message et donc la fonction de modulation des paramètres ne doivent pas supprimer le caractère chaotique du signal envoyé au récepteur. Il est important de souligner que cette technique exploite pleinement les qualités des systèmes chaotiques. Elle n'a pas d'équivalent parmi les systèmes de communication "classique". Cependant, le cryptage par modulation s'est

avéré sensible à certaines attaques détaillées dans les références [141], [159].

1.6.4 Cryptage par inclusion

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

1.6.4.1 Observateurs à entrées inconnues

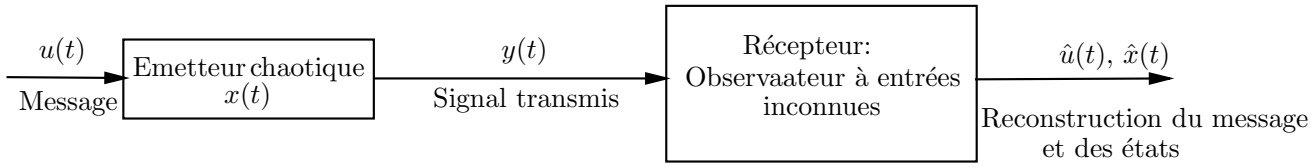


FIG. 1.16: Observateurs à entrées inconnues

Le schéma de la figure 1.16 illustre un problème classique d'estimation d'état non linéaire à entrées inconnues : il faut reconstruire l'état $x(t)$ du système émetteur et également l'entrée inconnue $u(t)$. Différentes techniques de synthèse d'observateurs à entrées inconnues ont été utilisées dans la littérature, et peuvent être utilisées à des fins de décryptage. Parmi les articles utilisant ces types d'observateurs pour décrypter l'information, on peut citer [21], [112].

1.6.4.2 Décryptage par inversion

L'article [48] présente un processus de décryptage par inversion c'est à dire, le récepteur est conçu en inversant le modèle de l'émetteur. La figure 1.17 présente le principe général de cette approche. Dans ce qui suit, quelques notions sur les systèmes dynamiques hybrides

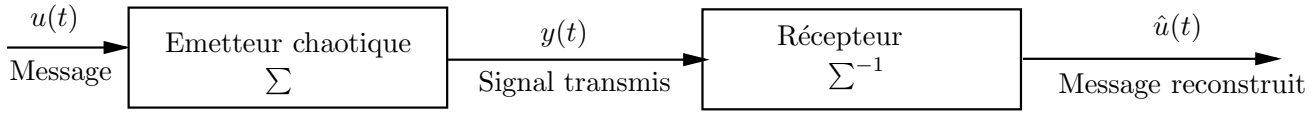


FIG. 1.17: Principe du cryptage par inversion

sont rappelés.

1.7 Rappels sur les systèmes dynamiques hybrides

1.7.1 Définition d'un système dynamique hybride

Les systèmes dynamiques hybrides [98], [137], [161] peuvent être définis comme des systèmes faisant intervenir explicitement et simultanément des phénomènes ou des modèles de type dynamique continu et événementiel, ce terme hybride se réfère au couplage essentiel des phénomènes continus et discrets au sein d'un système dont l'évolution au cours du temps est décrite par un ensemble de lois mathématiques qui peuvent être de natures continues au sens classique d'équations différentielles ou équations aux différences soumis au éléments décisionnels discrets ou événementiels.

La première formulation unitaire des concepts concernant les systèmes hybrides a été proposée par M. S. Branicky [22]. Ces travaux ont permis d'établir une classification de ces systèmes.

1.7.2 Classification des systèmes hybrides

Nous présentons dans ce paragraphe la classification de Branicky des systèmes dynamiques hybrides.

Phénomènes hybrides

Soit $x(t)$ la trajectoire d'un état continu du système hybride avec une valeur initiale fixée et arbitraire $x(t_0) \in X$ et $\dot{x}(t)$ la vitesse de l'état continu pour le même système hybride.

Avant d'étudier comment se produisent les interactions entre les deux parties qui forment le système hybride, nous allons d'abord présenter les actions discrètes qui peuvent intervenir lors de l'évolution d'un système continu décrit par une équation différentielle de la forme :

$$\dot{x} = f(x,t) \quad pour \quad t \geq 0 \tag{1.69}$$

où f est le champ de vecteurs.

On note τ l'instant où intervient une action discrète dont nous verrons ultérieurement comment elle peut être déclenchée. L'ensemble action et déclenchement est appelé phénomène hybride.

Action des phénomènes hybrides

Les action des phénomènes hybrides sur le système continu sont de deux types :

- Les phénomènes hybrides agissent sur la dynamique du système continu, modifiant ainsi cette dynamique. Le système hybride se situe alors pour $t \geq \tau$ dans un autre mode de fonctionnement. On appelle ce phénomène commutation de modèle et τ instant de commutation. Un exemple simple de modèle formel avec deux modes de fonctionnement est le suivant :

$$\dot{x} = f_1(x,t) \quad pour \quad t < \tau,$$

$$\dot{x} = f_2(x,t) \quad pour \quad t \geq \tau$$

- Les phénomènes hybrides agissent également sur le vecteur d'état du système, le faisant évoluer de manière différente pour $t = \tau$. C'est à dire qu'à l'instant τ, l'état saute de $x(\tau^-)$ à $x(\tau^+)$ sans changement de modèle $x(\tau^-) \neq x(\tau^+)$. On appelle ce phénomène saut de l'état. Un exemple de modèle formel est représenté par les équations suivantes :

$$\dot{x} = f(x,t) pour \quad t \geq 0 \quad et \quad t \neq \tau,$$

$$x(\tau^+) = x(\tau^-) + g \quad pour \quad g \neq 0$$

Les deux actions peuvent être couplées. En effet, on peut considérer qu'a l'instant τ, on a une commutation de modèle et saut du vecteur d'état. Un exemple de modèle formel est le suivant :

$$\dot{x} = f_1(x,t) \quad pour \quad t < \tau,$$

$$x(\tau^+) = x(\tau^-) + g \quad pour \quad g \neq 0$$

$$\dot{x} = f_2(x,t) \quad pour \quad t > \tau.$$

L'état continu du système est alors ré-initialisé de $x(\tau^-)$ à $x(\tau^+)$. Notons que τ^- et τ^+ correspondent respectivement aux limites à gauche et à droite de τ, et g la constante provoquant une discontinuité à l'instant τ.

Déclenchement des phénomènes hybrides

L'action du phénomène hybride, comme le passage d'un mode de fonctionnement à un autre est déclenchée par un événement. Ces événements sont alors classés en deux types :

- Les événements déctenchés lorsque le vecteur d'état continu atteint certaines valeurs, provoquant ainsi un phénomène hybride dit autonome.
- Les événements déclenchés par une commande discrète externe, provoquant un phénomène hybride dit contrôlé.

Branicky a proposé la classification suivante :

- Systèmes hybrides à commutation autonome.
- Systèmes hybrides à saut autonome.
- Systèmes hybrides à commutation contrôlée.
- Systèmes hybrides à saut contrôlé.

Dans les paragraphes suivants, des brefs rappels sur les différentes catégories sont présentés :

- Systèmes hybrides à commutation autonome

  Ces systèmes sont représentés par des équations différentielles définies par morceaux, l'espace d'état X est un sous ensemble fermé de $\mathbb{R}^n$. X est découpé en sous domaines $\{X_q, q \in Q\}$, fermé, d'intérieur non vide et deux à deux disjoints, et tel que :

  $$\bigcup_{q \in Q} X_q = X$$

  Sur chaque domaine X_q, on définit un champ de vecteurs f_q.

  D'un autre point de vu, c'est un système qui est caractérisé par un changement discontinu du champ de vecteur $f(x(t), u(t))$ lorsque l'état atteint certains seuils. Ceci peut être illustré par la figure suivante :

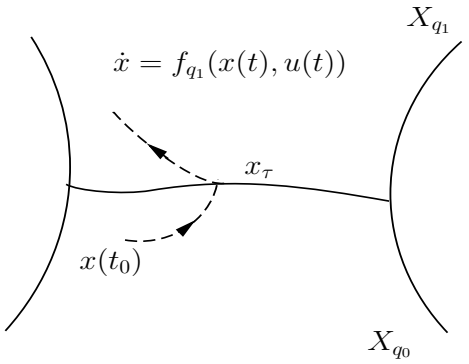


FIG. 1.18: Trajectoire du système dynamique à commutation autonome

La trajectoire du système dynamique à commutation autonome, se construit de la manière décrite par la figure 1.18. Si $x(t_0)$ appartient à l'intérieur du domaine X_{q_0}, alors $x(t)$ est solution de l'équation différentielle associée au champs de vecteurs $f_{q_0}(x(t), u(t))$ jusqu'à l'instant τ où $x(t)$ atteint la frontière séparant le domaine X_{q_0} du domaine X_{q_1}, $x(t)$ devient alors solution de l'équation différentielle associée au champs de vecteurs $f_{q_1}(x(t), u(t))$.

– Systèmes hybrides à saut autonome

  Dans ce cas, lorsque l'état atteint une certaine région de l'espace d'état, il effectue un saut, c'est à dire qu'il passe de façon discontinue de sa valeur courante à une autre.

  Généralement, dans le cas des systèmes à saut autonome, le système possède un seul mode de fonctionnement et une seule transition autorisant la réinitialisation de la variable continue.

– Systèmes hybrides à commutations contrôlées

  Un système dynamique à commutations contrôlées ou switched system est un système hybride où la variable discrète $q(t)$ n'est pas vue comme une variable d'état mais comme une variable de contrôle. Ainsi, l'évolution de $q(t)$ n'est pas contrainte par un système de gardes mais donnée par un individu extérieur (commande).

– Système hybride à saut contrôlé

  Dans ce cas, la valeur de l'état change de façon discontinue, en réponse à une commande. Ce type de comportement est présent dans les systèmes électrotechniques, avec des entrées de type impulsionnels.

1.8 Conclusion

Dans la première partie de ce chapitre, nous avons souligné le rôle que peut jouer un signal chaotique dans une transmission sécurisée. Nous avons expliqué ces propriétés qui ont motivé les chercheurs d'essayer de camoufler un message confidentiel à l'aide d'un signal chaotique. Ainsi, les systèmes chaotiques sont devenus très utilisés dans le domaine de la transmission sécurisée d'informations.

Ensuite, nous avons abordé le phénomène de synchronisation et présenté par la suite les principales méthodes utilisées pour la synchronisation des systèmes chaotiques à savoir la synchronisation unidirectionnelle et la synchronisation bidirectionnelle. La différence entre les deux types a été expliquée à travers un exemple choisi. Dans la synchronisation unidirectionnelle, nous avons signalé que le transfert d'énergie se fait dans un seul sens c'est à dire d'un système vers un autre. En pratique, par exemple, un simple schéma électrique à base d'amplificateurs monté en suiveur réalise cette tache. Par contre, pour la synchronisation bidirectionnelle, le transfert d'énergie s'effectue dans les deux sens. L'utilisation d'une simple résistance en pratique permet d'assurer ce type de couplage.

Dans ce chapitre, nous avons expliqué le principe de la synchronisation unidirectionnelle par l'approche observateur. Ici, nous avons souligné que, le récepteur de la chaîne de transmission n'est rien d'autre qu'un simple observateur. Pour cela, nous avons jugé utile de donner dans les deux cas (continu et discret) quelques notions sur l'observabilité et la condition de recouvrement d'observabilité (condition pour récupérer le message) ainsi quelques rappels sur les observateurs utilisés dans notre travail.

Ensuite, nous avons traité le problème de synchronisation de deux systèmes chaotiques identiques de Qi. Ici, deux méthodes de synchronisation ont été utilisées. La première est la commande passive, elle est basée sur la théorie de stabilité de Lyapunov. L'autre est basée sur les techniques de commandes impulsives. Pour assurer la synchronisation entre les deux systèmes, nous avons donné des conditions suffisantes pour chaque méthode. Les résultats de simulation montrent bien que, malgré l'extrême sensibilité aux conditions initiales des systèmes chaotiques, les deux systèmes se synchronisent. En conséquence, ces résultats illustrent bien les performances des deux méthodes proposées.

Les principales méthodes de transmission basée sur la synchronisation de systèmes chaotiques ont fait également l'objet de ce chapitre. Dans la méthode de cryptage par addition, nous avons signalé ses principaux inconvénients qui sont sa sensibilité aux attaques

extérieures ainsi que la difficulté pour détecter le message utile en cas de présence de bruit de canal de transmission. La méthode de cryptage par inclusion reste moins sensible aux perturbations extérieures ainsi qu'au bruit de canal d'où son choix dans notre thèse pour réaliser notre schéma de transmission sécurisée (voir chapitre2).

Enfin, nous avons jugé utile de donner quelques notions sur les systèmes dynamiques hybrides car, ils seront utilisés dans le prochain chapitre qui sera consacré à l'étude de l'émetteur du schéma de transmission sécurisé proposé.

Chapitre 2

Etude de l'émetteur

Chapitre 2

Etude de l'émetteur

2.1 Introduction

Ces dernières années, différents types d'observateurs sont proposés pour les systèmes chaotiques (observateurs destinés uniquement à reconstruire les états de l'émetteur) [54] et aussi pour les systèmes chaotiques à entrées inconnues (observateurs destinés à reconstruire les états de l'émetteur et récupérer l'information) [7]. Le fonctionnement correct de ces observateurs dépend de plusieurs conditions : la condition d'observabilité pour retrouver les états du système ; la condition de recouvrement de l'observabilité pour retrouver les états du système et l'information noyée dans le système (inversibilité à gauche du système) ; la condition d'identifiabilité des paramètres qui représente les clés de codage. Dans ce travail, notre objectif consiste à concevoir un système de chiffrement sûr. Ici, nous nous sommes intéressés à l'étude d'un schéma de transmission constitué de systèmes dynamiques hybrides. L'émetteur est composé d'un système chaotique en temps continu dit de Colpitts et d'un système chaotique en temps discret dit de Hénon modifié. Le récepteur est composé d'un observateur en temps continu et d'un observateur en temps discret. Dans le but de rendre la structure de l'émetteur plus complexe, les états du système en temps continu seront introduits dans la dynamique du système en temps discret. La sortie transmise au récepteur est composée d'un signal dit de synchronisation issu du système en temps continu et d'un signal utile qui contient le message (ajouté par la méthode d'inclusion) issu du système en temps discret. La récupération du message au niveau du récepteur passe d'abord par la synchronisation des deux systèmes en temps continu (de l'émetteur et du récepteur). Il est à noter que pour les intrus, le temps

de la synchronisation des deux systèmes en temps continu est inconnu. Ceci-ci joue un rôle important dans l'identification de tous les paramètres du système dynamique hybride (système qui constitue les clés de codage). Néanmoins avec cette stratégie, nous allons montrer le schéma de transmission proposé n'est pas robuste contre une attaque à textes clairs connus (voir chapitre 5) et que les clés secrètes sont identifiables. Pour résoudre ce problème, nous allons proposer d'introduire des retards (clés secrètes supplémentaires) sur les états continus [165] En conséquence, les paramètres du système dynamique hybride ne sont pas identifiables contre une attaque à textes clairs connus.

Ce chapitre est organisé comme suit. Dans la section 2.2, un rappel sur les systèmes de communications chaotique sera présenté. La section 2.3 sera consacrée à la présentation détaillée de l'émetteur. Enfin, nous terminons ce chapitre par une conclusion.

2.2 Systèmes de communications chaotiques

2.2.1 Introduction

Dans le domaine de la cryptographie, d'intenses recherches sont menées pour mettre au point de nouvelles techniques de cryptage. Des systèmes pseudo-chaotiques discrets sont ainsi utilisés depuis longtemps pour générer des clés chiffrées. Les systèmes chaotiques représentent donc un fort potentiel d'applications dans les systèmes de communications sécurisées. Depuis les années 1990, les manifestations du chaos ne représentent plus des phénomènes nuisibles. En effet, la théorie OGY [121] a démontré qu'il est possible de contrôler les systèmes chaotiques. Par la suite, l'intérêt pour ces systèmes ne s'est jamais démenti, de nombreuses recherches leurs sont consacrées. Il est ainsi apparu qu'il existe des analogies entre les propriétés intrinsèques des systèmes chaotiques et les propriétés des cryptosystèmes classiques [2].

- L'ergodicité des systèmes chaotiques (une orbite est ergodique si l'ensemble de ses éléments est dense dans l'attracteur) correspond à la propriété de confusion : la trajectoire chaotique a la même distribution quelque soit le message à crypter.
- La sensibilité aux conditions initiales, (voir annexe A), ainsi que la sensibilité aux variations des paramètres du système, et la propriété de *mixage* correspond à la propriété de *diffusion* : Un petit changement dans le message ou dans la clé induit un grand changement dans le signal crypté.

- Le déterminisme des systèmes chaotiques est à mettre en parallèle avec le déterminisme des générateurs pseudo-aléatoires.
- La complexité de la structure chaotique et la complexité d'un algorithme de cryptage classique résultent d'un processus très simple.

Dans un premier temps, on a supposé qu'un signal chaotique pouvait servir de porteuse dans un système de communications sécurisées. Les propriétés des systèmes chaotiques (voir Annexe A) les font ressembler, à première vue seulement, aux signaux pseudo-aléatoires traditionnellement utilisés pour masquer l'information dans certains cryptosystèmes classiques. Par ailleurs, pour pouvoir être utilisé comme porteuse en cryptographie classique, un signal pseudo-aléatoire doit posséder un spectre infiniment large, plat et une densité spectrale de puissance beaucoup plus grande que celle de l'information à camoufler. Ces conditions, une fois remplies, doivent permettre de noyer totalement le message dans le "bruit" tant au niveau temporel qu'au niveau spectral. Malheureusement, ces conditions sont loin d'être vérifiées dans le cas des signaux chaotiques. D'autres propriétés intrinsèques des systèmes chaotiques représentent également des arguments importants qui plaident en faveur de leur utilisation dans un système de communications sécurisées. Parmi ces propriétés, on peut mentionner la sensibilité dans les paramètres qui représente une prévention contre les attaques. En effet, si l'émetteur et le récepteur doivent partager les mêmes valeurs de paramètres, on peut considérer dans une première approche que tous ces paramètres constituent les clés du système de communications. En réalité, cela, n'est pas suffisant pour garantir un bon niveau de sécurité : le cryptosystème chaotique doit posséder une clé plus forte. Ce point sera abordé dans le dernier chapitre. Une autre propriété fondamentale des systèmes chaotiques réside dans leur comportement asymptotique apériodique, contrairement aux générateurs pseudo-aléatoires qui peuvent être périodiques.

La différence fondamentale entre les émetteurs chaotiques et les générateurs de nombres pseudo-aléatoires réside dans la propriété de synchronisation. Ces deux classes de systèmes permettant de générer des signaux apparemment aléatoires sont déterministes : dans les deux cas, si on connaît les paramètres et les conditions initiales, on sait reproduire le signal transmis. Or, la capacité de synchronisation des systèmes chaotiques implique que le récepteur peut se passer de la connaissance de l'état initial de l'émetteur. La synchronisation, étudiée au chapitre précèdent, est donc un processus fondamental des techniques

de cryptage à base de systèmes chaotiques.

2.2.2 Inconvénients des méthodes de transmission chaotiques

Dans cette section, les inconvénients des méthodes de transmission chaotiques cités au chapitre précédent seront passé en revue.

- Dans le principe de cryptage par addition décrit au paragraphe 1.6.1, le message étant ajouté à la porteuse chaotique. La synchronisation ne peut pas être parfaite car, au niveau du récepteur, le message apparaît comme une perturbation, même sous l'hypothèse d'une amplitude du message très faible devant celle de la porteuse. C'est la première limitation de cette méthode. Par ailleurs, au niveau spectral, le message doit être caché dans la partie basses fréquences du spectre de la porteuse chaotique : la largeur de cette partie "utile" de la densité spectrale varie selon le système chaotique, mais cette condition limite le choix de messages pouvant être transmis.
- La technique de cryptage par commutation décrite au paragraphe 1.6.2 présentent des limitations. D'une part, elle ne concerne que les messages prenant un nombre fini de valeurs, alors que nous voulons transmettre des messages à valeurs réelles. D'autres part, le signal transmis est constitué de séquences générées alternativement par les différents systèmes chaotiques constituant l'émetteur. A chaque changement de système chaotique au niveau de l'émetteur, la synchronisation est rompue, et il faut que le récepteur se synchronise de nouveau (seul le système chaotique récepteur correspondant au système chaotique émetteur se synchronise). Le temps nécessaire à la transmission est donc plus long que pour la technique précédente, puisqu'il faut ajouter le temps nécessaire à l'établissement d'une nouvelle synchronisation à chaque fois que le message change de valeur. Cette technique a été démontée par des cryptanalystes : par exemple, l'article de Yang et *al*, [158] exploite une méthode de détection de changement des paramètres de l'émetteur, tandis que Zhou et *al*, [167] utilise des applications de premier retour et une fonction d'autocorrélation pour reconstruire le message .
- Les techniques de cryptage par modulation ne semble pas résister à des attaques spécifiques, exploitant la signature intrinsèque de chaque attracteur chaotique. En effet, l'article de Short1 [141] montre que l'injection du message dans la dynamique

de l'émetteur provoque une petite distorsion dans l'espace de phase du système chaotique original. Or, cet espace des phases peut être reproduit, par des techniques de reconstruction (par plongement, par retard, etc), plus ou moins facilement selon la complexité du chaos considéré.

– Le cryptage par inclusion s'apparente aux méthodes de cryptage classiques. L'inconvénient majeur réside dans le principe même de l'injection du message dans la dynamique de l'émetteur : comment garantir en effet que le système ainsi modifié conserve un comportement chaotique ? Le problème s'avère d'autant plus délicat que le message peut prendre des formes très différentes. Les détails sur les inconvénients de cette méthode sont donnés dans la thèse de Cherrier [30]. Malgré ces inconvénients, cette méthode reste toujours applicable dans les communications chaotiques sécurisées.

Après avoir présenté les inconvénients des méthodes de cryptage chaotique précédentes, la technique de cryptage par inclusion sera utilisé pour la conception de notre nouvelle méthode transmission sécurisée.

2.3 Principe de la méthode proposée

La conception d'un système de communication peut être décomposée en trois étapes, à savoir le choix de l'émetteur, le choix du récepteur, et la mise au point du processus de transmission de l'information.

La première étape consiste à choisir un émetteur chaotique. Le choix de l'émetteur a un impact direct sur la sécurité du cryptosystème et ce à deux niveaux. L'impact sur la sécurité du cryptage lui-même fera l'objet du chapitre 5. En ce qui concerne la sécurité du processus de synchronisation, on peut noter qu'il existe des attaques exploitant principalement des techniques de reconstruction à retard, dont le principe est étudié dans les travaux de Pecora dans [126]. Ces attaques tentent de reconstituer la géométrie de l'attracteur chaotique correspondant à l'émetteur exploitant uniquement les informations contenues dans une série temporelle du signal transmis. Pour appliquer ces techniques, il faut disposer d'un nombre suffisamment important de données, nombre qui augmente avec la complexité du chaos. Une mesure possible pour augmenter cette complexité, et pour augmenter par conséquent la sécurité d'un cryptosystème, consiste à prendre comme

émetteur un système à structure très complexe. C'est la raison pour laquelle, nous avons opté pour un système chaotique hybride. Ce dernier est composé principalement d'un système chaotique en temps continu et d'un système chaotique en temps discret. Dans le but de rendre la structure de l'émetteur beaucoup plus complexe et par conséquent augmenter la sécurité du cryptosystème, des états du système en temps continu retardés et échantillonnés seront introduits dans la dynamique du système en temps discret. (les détails sur cette partie feront l'objet de ce chapitre).

La deuxième étape consiste à concevoir un récepteur qui se synchronise avec l'émetteur choisi. Il sera présenté dans le prochain chapitre.

La troisième étape consiste à mettre au point une technique de transmission des signaux chaotiques incluant le message et à garantir un certain niveau de sécurité. Cette partie ne sera pas développée, on suppose uniquement que le canal est idéal.

Dans ce travail de thèse, nous nous sommes intéressés à la conception d'un nouveau système de communication basé sur la synchronisation des systèmes chaotiques à l'aide d'observateurs [62], [63], [64]. Le schéma global de notre système pour les communications privées est montré par la figure 2.1.

2.3.1 Etude de l'émetteur

L'émetteur est constitué de quatre blocs : un système chaotique en temps continu, un système chaotique en temps discret, un conformateurs d'impulsions et un bloc de multiplexage (voir figure 2.1). Ces blocs sont détaillés de la manière suivante :

2.3.1.1 Etude du système chaotique en temps continu

Le système en temps continu est un oscillateur de Colpitts permettant la génération de signaux chaotiques. Ce choix peut être expliqué par les points suivants :

- La structure de l'oscillateur illustré par le schéma de la figure 2.2 est simple. Elle utilise un seul transistor et permet, comme nous allons le montrer dans les paragraphes suivants, de générer des comportements chaotiques en modifiant uniquement les conditions de fonctionnement du transistor. Les autres paramètres électriques de l'oscillateur sont fixés à des valeurs appropriées.
- La possibilité de faire évoluer la fréquence fondamentale de l'oscillateur vers les fréquences élevées [152]. Il suffit pour cela, de choisir la technologie adéquate pour

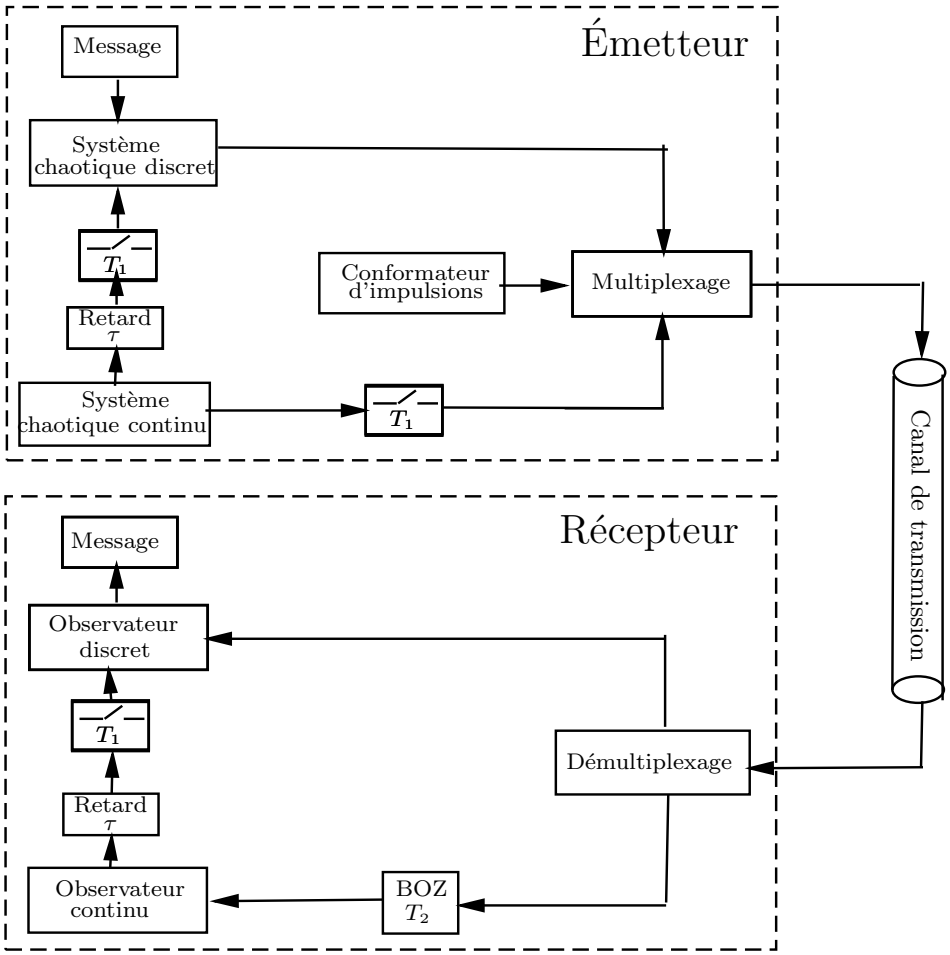


FIG. 2.1: Chaîne de transmission basée sur un système dynamique hybride

le transistor et d'inclure dans l'étude et la conception de l'oscillateur les effets liés à la montée en fréquence.

- La structure de l'oscillateur de Colpitts possède une non linéarité intrinsèque due à la caractéristique exponentielle du transistor.
- La simplicité d'utilisation de l'oscillateur de Colpitts dans des systèmes de communications chaotiques. Il a été largement appliquée pour la transmission de signaux binaires [135] et continus [71], [72], etc.

La figure 2.2 montre le montage de basses fréquences de l'oscillateur de Colpitts. Le transistor utilisé est un transistor bipolaire classique (BJT). Le circuit résonnant LC est connecté entre le collecteur et la base du transistor et une fraction de la tension du circuit LC est retournée à l'émetteur. Les tensions d'alimentation V_1 et V_2 permettent de fixer le point de fonctionnement du transistor. Le choix des valeurs du circuit résonnant détermine

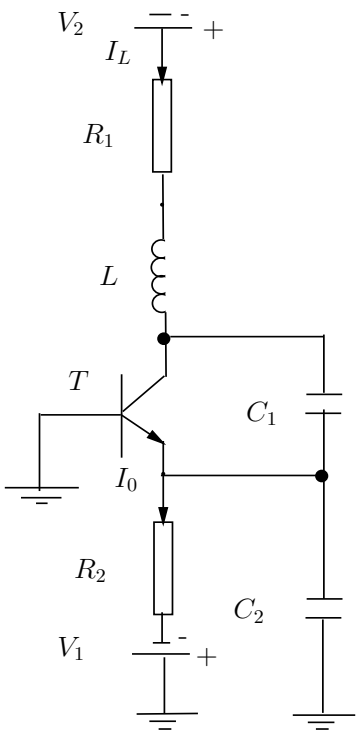


FIG. 2.2: Oscillateur électronique de Colpitts

la fréquence fondamentale de l'oscillateur. Avant de présenter l'oscillateur de Colpitts utilisé, il est nécessaire de donner quelques notions sur les oscillateurs électroniques.

2.3.1.1.1 Les oscillateurs

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

2.3.1.1.2 Le critère d'oscillation de Barkhausen

La figure 2.3 montre la représentation la plus élémentaire d'un oscillateur électronique, l'élément $A(p)$ est la fonction de transfert de l'amplificateur et l'élément $R(p)$ est la fonction de transfert d'un filtre. Supposons que les différentes grandeurs du montage soient sinusoïdales c'est à dire : $V_2 = |A| \exp(j\phi_A)V_1$ et $V_3 = |R| \exp(j\phi_R)V_2$ et donc : $V_3 = |A||R| \exp(j(\phi_A + \phi_R))$. Le critère de Barkhausen impose que V_3 soit l'unité, ce qui nécessite deux conditions :

$$\begin{cases} |A|.|R| = 1 \\ \phi_A + \phi_R = 0 + 2k\Pi, \quad k \in \mathbb{Z} \end{cases} \tag{2.1}$$

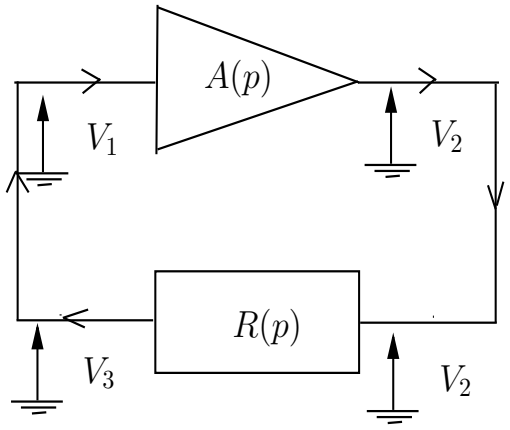


FIG. 2.3: Oscillateur électronique : modèle de Barkhausen.

Cependant, dans la pratique, les oscillations prennent naissance à partir de fluctuations qui sont amplifiées, ce qui nécessite un gain plus grand que l'unité. Mais les oscillations ne peuvent croître indéfiniment, elles s'arrêtent sur une "non-linéarité" de l'amplificateur. Cela signifie que dans un oscillateur, l'amplificateur possède toujours une caractéristique non linéaire. Une conséquence directe est que tout oscillateur électronique est potentiellement chaotique, en effet, tout système chaotique est nécessairement non linéaire.

2.3.1.1.3 L'oscillateur de Colpitts

Dans ce qui suit, on s'intéresse à l'oscillateur de Colpitts décrit par la figure 2.2. Ses conditions d'oscillations et ses équations d'état seront données.

Détermination des conditions d'oscillation

Pour étudier le fonctionnement de l'oscillateur de Colpitts, considérons la figure 2.4. La caractéristique non linéaire du transistor est définie par $i_2 = gV_1$ En utilisant la loi de

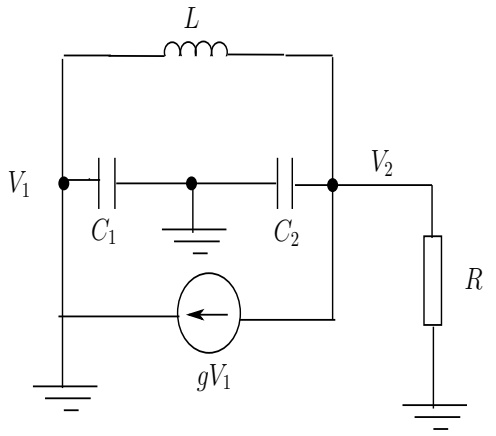


FIG. 2.4: Schéma de pricipe de l'oscillateur de Colpitts

Kirchoff, nous écrivons les équations du courant aux deux extrémités de l'inductance L :

$$\begin{cases} -gV_1 - \frac{V_2}{R} - jC_2wV_2 + \frac{V_1-V_2}{jLw} = 0 \\ \frac{V_2-V_1}{jLw} - jC_1wV_1 + gV_1 = 0 \end{cases}$$

En résolvant la deuxième équation pour V_2 et en remplaçant le résultat dans la première équation, on obtient :

$$[-g + \frac{1}{jLw}] - [jC_1w + \frac{1}{jLw}][\frac{1}{R} + jC_2w + \frac{1}{jLw}] = 0 \tag{2.2}$$

En annulant la partie imaginaire de (2.2), on obtient :

$$C_1C_2RLw^2 - (C_1 + C_2)Rw = 0 \tag{2.3}$$

et donc la pulsation d'oscillation est calculée par :

$$w = \frac{1}{L\frac{C_1C_2}{C_1+C_2}} \tag{2.4}$$

qui est la fréquence d'accord de l'inductance accordée par les deux condensateurs en série. En annulant la partie réelle de 2.2, on obtient la relation suivante :

$$-Rg + LC_1w^2 - 1 = 0 \Rightarrow R = \frac{LC_1w^2-1}{g} \tag{2.5}$$

qui représente la condition d'oscillation du Colpitts. En effet l'oscillation démarre lorsque la valeur de R est supérieure à la valeur obtenue par (2.5). Si l'on remplace ω dans (2.5), on trouve la condition d'oscillation comme suit :

$$gR > \frac{C_1}{C_2} \tag{2.6}$$

Détermination des équations d'état

Pour décrire le modèle mathématique de l'oscillateur de Colpitts, nous écrivons ces équations d'état en considérant les variables d'état V_{c1}, V_{c2} et I_L (voir figure2.2). Les

équations d'état sont alors données par :

$$\begin{cases} \frac{dV_{C1}}{dt} = -\frac{1}{C_1} f(-V_{C2}) + \frac{1}{C_1} I_L \\ \frac{dV_{C2}}{dt} = \frac{1}{C_2} I_L - \frac{1}{C_2} I_0 \\ \frac{dI_L}{dt} = -\frac{1}{L_1} V_{C1} - \frac{1}{L_1} V_{C2} - \frac{R_1}{L_1} I_L + \frac{V_2}{L_1} \end{cases} \tag{2.7}$$

où $f(.)$ est la caractéristique courant-tension du transistor. Cette fonction est en effet le courant de l'émetteur qui peut être exprimé par :

$$I_E = f(V_{BE}) = f(-V_{C2}) \simeq I_S[\exp(\frac{V_{BE}}{V_T})] \simeq [\exp(\frac{-V_{C2}}{V_T})] \tag{2.8}$$

où I_s est le courant de saturation inverse de la jonction base-émetteur (BE) du transistor et $V_T \simeq 27mv$. Dans [105], [109], Maggio *et al* ont normalisé le modèle mathématique de l'oscillateur de Colpitts. Pour cela, les tensions, le courant et le temps sont respectivement normalisés par rapport à $V_{ref} = V_T$, $I_{ref} = I_0$ et $t_{ref} = \frac{1}{w_0}$. w_0 représente la pulsation centrale d'oscillation. Le point d'opération du système (2.7) est donné par [109] :

$$O : \begin{cases} VC_{1o} = V_{CC} - \alpha R I_0 + V_T \ln(\alpha \frac{I_0}{I_S}) \\ VC_{2o} = -V_T \ln(\alpha \frac{I_0}{I_S}) \\ I_{Lo} = \alpha I_0 \end{cases} \tag{2.9}$$

Par la suite, nous considérons $\alpha = 1$, ce qui veut dire qu'on néglige le courant de la base du transistor, Les trois variables d'état sans dimensions (z_1, z_2, z_3), s'écrivent alors :

$$\begin{cases} z_1(t) = \frac{1}{V_T}[V_{C1}(w_0 t) - V_{C1o}] \\ z_2(t) = \frac{1}{V_T}[V_{C2}(w_0 t) - V_{C2o}] \\ z_3(t) = \frac{1}{I_o}[I_L(w_0 t) - I_{Lo}] \end{cases} \tag{2.10}$$

En combinant les équations (2.7), (2.9) et (2.10), nous obtenons le système normalisé ci-dessous :

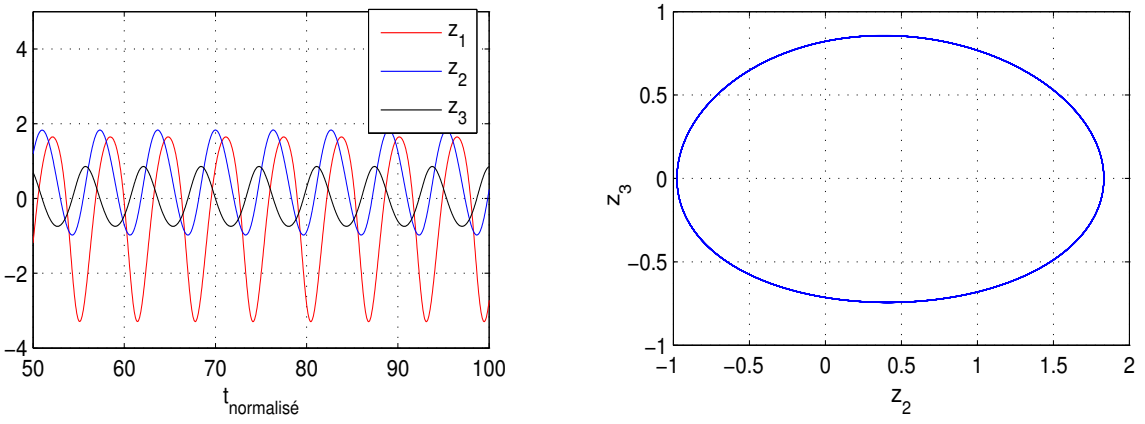
$$\begin{cases} \dot{z_1} = \frac{g}{Q(1-k)}(-\eta(z_2) + z_3) \\ \dot{z_2} = \frac{g}{Qk} z_3 \\ \dot{z_3} = -\frac{Qk(1-k)}{g}([z_1 + z_2] - \frac{1}{Q} z_3) \end{cases} \tag{2.11}$$

avec $\eta(z_2) = \exp(-z_2) - 1$ et $k = \frac{C_2}{C_1+C_2}$. Le paramètre g est le gain de la boucle de la réaction lorsque le critère de Barkaussen [105] est satisfait, et $Q = \frac{LW_0}{R}$ est le facteur de qualité du circuit LC non chargé. Il y a alors des oscillations sinusoïdales lorsque $g = 1$. Il est à noter que pour avoir un comportement chaotique, les paramètres du système (2.11) sont donnés comme suit : $g = 4.46$; $Q = 1.38$ et $k = 0.5$. $z_1(0) = 1.6$; $z_2(0) = 8$ et $z_3(0) = 0.1$, les conditions initiales du système qui sont choisies à l'intérieur du bassin d'attraction étrange. Si on considère I_0 comme une source de courant idéale, le paramètre g se calcule par [109] :

$$g = \frac{LI_0}{(C_1+C_2)R_1V_T} \tag{2.12}$$

En faisant varier les paramètres g et Q du système (2.11), nous obtenons différents types d'oscillations. Ces comportements montrent la bifurcation des oscillations périodiques, par rapport à l'oscillation sinusoïdale qui correspond au cycle limite (voir Annexe A) [105].

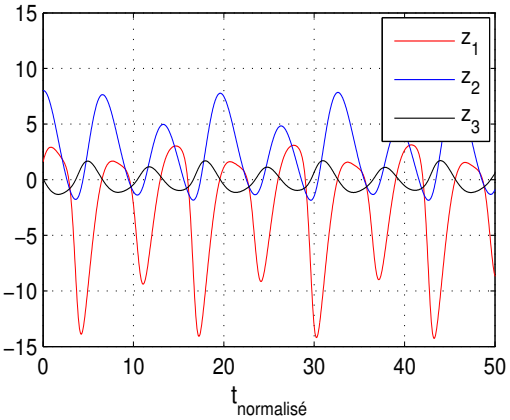
Afin d'obtenir par simulation différents comportement pour l'oscillateur de Colpitts, nous fixons $L = 1mH$, $C_1 = C_2 = 470nF$. La fréquence d'oscillation est alors $f_0 = \frac{1}{2\Pi\sqrt{L\frac{C_1C_2}{C_1+C_2}}} = 10.38KHz$. La valeur de Q est obtenue en remplaçant les valeurs ci-dessus dans $Q = \frac{2\Pi f_0 L}{R_1}$. Pour ces valeurs, nous obtenons $Q = 1.38$. Ainsi, nous faisons varier le paramètre g, qui lui-même dépend de I_0 d'après (2.12), soit le terme non linéaire du système d'équations (2.11). Pour démarrer l'oscillation, nous avons fixé la valeur de g légèrement supérieur à 1, pour satisfaire la condition de Barkaussen (2.1). Les résultats obtenus pour différentes valeurs de g sont donnés par les figures ci-dessous. Pour $g =$



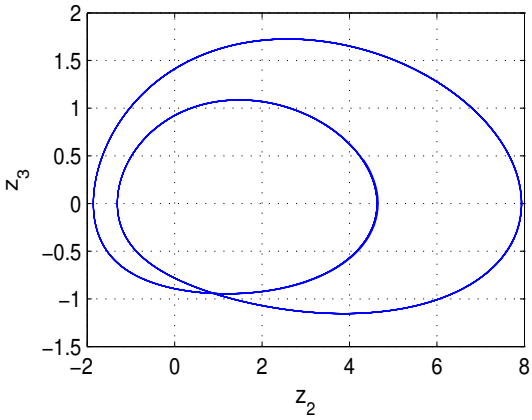
(a) Réponses temporelles

(b) Plan de phase

FIG. 2.5: Oscillateur de Colpitts : $g = 1.0029$.

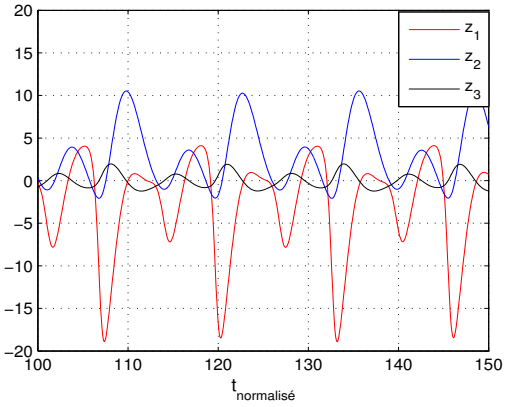


(a) Réponses temporelles

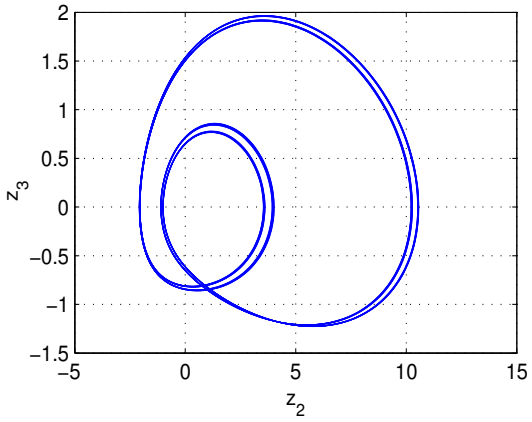


(b) Plan de phase

FIG. 2.6: Oscillateur de Colpitts : $g = 2.13$.

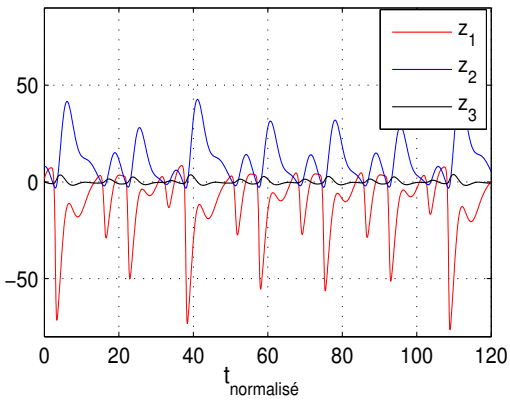


(a) Réponses temporelles

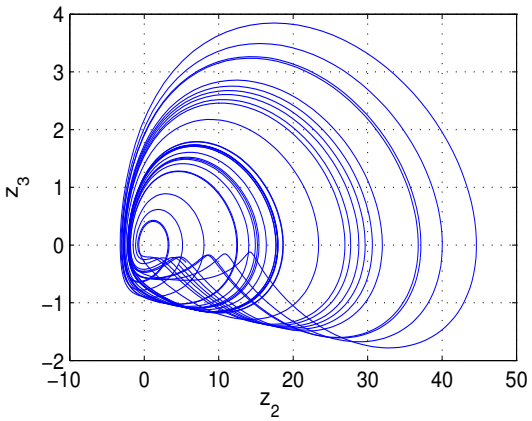


(b) Plan de phase

FIG. 2.7: Oscillateur de Colpitts : $g = 2.4$.



(a) Réponses temporelles



(b) Plan de phase

FIG. 2.8: Oscillateur de Colpitts : $g = 4.46$.

1.0029, la condition de Barkaussen est vérifiée, donc le système présente des oscillations sinusoïdales au niveau des réponses temporelles (voir figure 2a) et, par conséquent, un

cycle limite dans le plan de phase $z_2 - z_3$ (voir figure 2b). En augmentant la valeur de g à 2.13, le système présente des oscillations sinusoïdales à deux périodes (voir figure 5a) correspondant à 2 cycles limites dans le plan de phase (voir figure 5b). Pour $g = 2.4$, le système oscille avec 4 périodes (voir figure 2.7a) correspondant à 4 cycles limites dans le plan de phase (voir figure 2.7b). Mais, pour $g = 4.46$, le système présente un comportement chaotique (voir figure 2.8a) correspondant à un attracteur chaotique étrange dans le plan de phase.

Dans ce qui suit, nous utilisons le modèle simplifié du système (2.11) donné par :

$$\begin{cases} \dot{z_1} = a_1(-exp(-z_2) + 1 + z_3) \\ \dot{z_2} = a_2 z_3 \\ \dot{z_3} = -a_3(z_1 + z_2) - a_4 z_3 \\ y_1 = z_2 \end{cases} \tag{2.13}$$

avec $a_1 = \frac{g}{q(1-k)}$, $a_2 = \frac{g}{qk}$, $a_3 = \frac{qk(1-k)}{g}$, $a_4 = \frac{1}{q}$ et $y_1 = z_2$ la sortie de (2.13). Le système en temps discret est décrit par la section suivante.

2.3.1.2 Etude du système chaotique en temps discret

Le système chaotique en temps discret utilisé est dit système de Hénon modifié. Ce système a été largement étudié dans la littérature, on peut citer par exemple les travaux de Dmitriev [46] et de Vesely [149]. Il est donné par les équations suivantes :

$$\begin{cases} x_1(k+1) = a - x_2^2(k) - bx_3(k) \\ x_2(k+1) = x_1(k) \\ x_3(k+1) = x_2(k) \\ y_2(k) = x_2(k) \end{cases} \tag{2.14}$$

Pour avoir un comportement chaotique, les paramètres du système (2.14) sont donnés comme suit : $a = 1.76$ et $b = 0.1$. $x_1(0) = 0.1$ $x_2(0) = 0.1$ et $x_3(0) = 0.1$, les conditions initiales du système (2.14) qui sont choisies à l'intérieur du bassin d'attraction étrange. $y_2(k) = x_2(k)$ est la sortie du système (2.14). Le comportement chaotique du système (2.14) est illustré par les figures suivantes : Notre approche pour inclure le signal du message m dans le modèle de Hénon modifié est la méthode par inclusion (décrite au

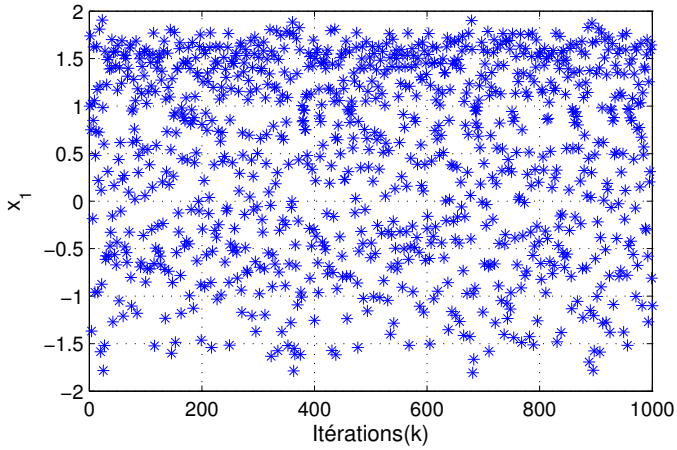


FIG. 2.9: L'état discret $x_1(k)$

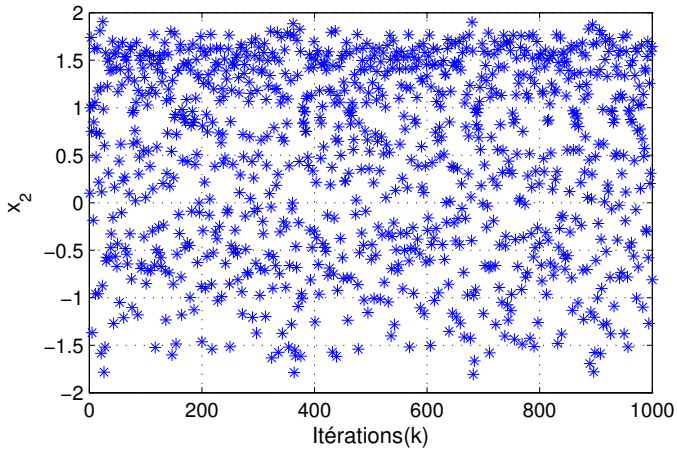


FIG. 2.10: L'état discret $x_2(k)$

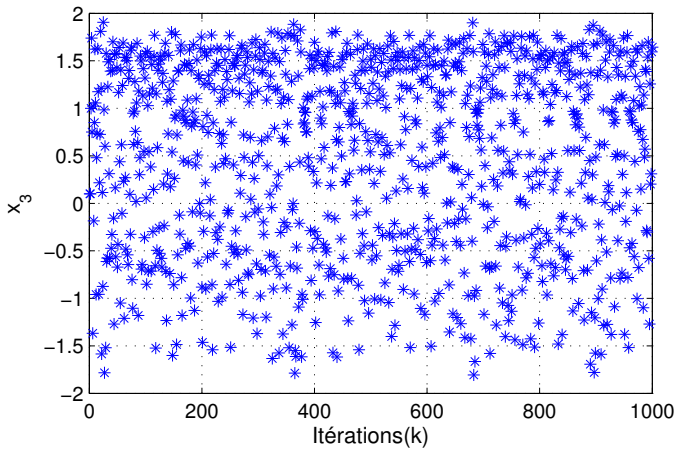


FIG. 2.11: L'état discret $x_3(k)$

chapitre1). Cette dernière consiste à ajouter le message dans l'une des dynamiques du système. Après avoir ajusté les paramètres pour obtenir un comportement chaotique, le

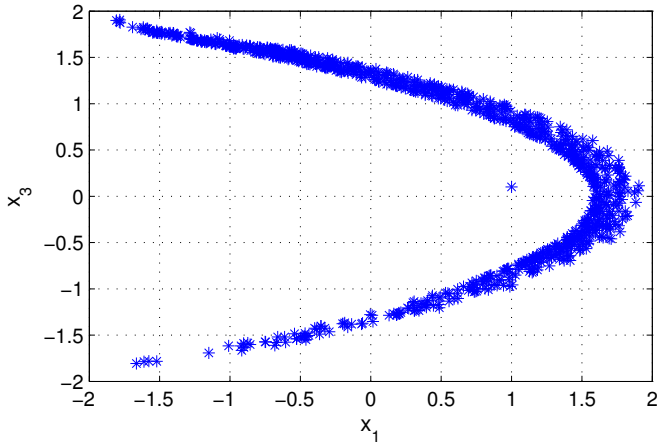


FIG. 2.12: Plan de phase $x_1(k) - x_3(k)$

signal m est ajouté à la l'itéré de l'état $x_1(n)$ du système (2.14). Ainsi, l'état $x_1(n)$ est modulé en fonction du message m. Par contre, le signal transmis au récepteur est l'état x_2, ce qui veut dire que l'on ne transmet pas directement l'état modulé au récepteur. Cela fait une différence substantielle entre notre approche et la méthode par addition dans laquelle le message m est ajoutée à la sortie de l'émetteur et la somme est transmise directement au récepteur. Il est important de noter que l'amplitude et la fréquence du message doivent être choisies de telle manière que l'on ne puisse pas détecter de variations visibles relatives au message sur la sortie du système. De plus, nous assumons que le message est borné et assez petit afin préserver le comportement chaotique, c'est à dire rester dans l'attracteur étrange [149]. Dans les communications privées, le but recherché est d'augmenter la sécurité du système de transmission. Dans notre travail, nous nous sommes intéressés à rendre la structure du système (2.14) plus complexe. Pour cela, nous avons introduits les états z_i $(i = 1, 3)$ échantillonnés du système en temps continu (2.13) et le message m dans la troisième dynamique du système en temps discret (2.14). La période d'échantillonnage T_1 des états z_1 et z_3 (dont la valeur est donnée en simulation) est choisie pour assurer la synchronisation entre l'émetteur et le récepteur des deux systèmes en temps continu. Le

nouveau système obtenu est donné comme suit :

$$\begin{cases} x_1(k+1) & = & a - x_2^2(k) - bx_3(k) \\ x_2(k+1) & = & x_1(k) \\ x_3(k+1) & = & x_2(k) + A_1 z_1(nT_1) \\ & + & A_2 z_3(nT_1) + cm(k) \\ y_2(k) = x_2(k) & & \end{cases} \tag{2.15}$$

avec : A, B and c les nouveaux coefficients du système (2.15).

Le système en temps discret (2.15) reçoit les informations z_1 et z_3 délivrées par le système en temps continu (2.13). Nous désignons alors (2.15) par un système à dynamique hybride.

Pour préserver le comportement chaotique du système défini par (2.15), ces paramètres sont choisis avec beaucoup de précaution. Dans notre cas, il faut satisfaire les valeurs suivantes : $A_1 \leq 0.01$, $A_2 \leq 0.01$ and $c \leq 1$.

Pour augmenter d'avantage la sécurité du système (2.15), les deux états z_i $(i = 1, 3)$ sont retardés par des retards τ_j $(j = 1, 2)$ avant d'être échantillonné (une analyse approfondie sera donnée dans le chapitre 5). Le nouveau système hybride obtenu est donné comme suit :

$$\begin{cases} x_1(k+1) & = & a - x_2^2(k) - bx_3(k) \\ x_2(k+1) & = & x_1(k) \\ x_3(k+1) & = & x_2(k) + A_1 z_1(nT_1 - \tau_1) \\ & + & A_2 z_3(nT_1 - \tau_2) + cm(k) \\ y_2(k) = x_2(k) & & \end{cases} \tag{2.16}$$

2.3.1.3 Etude du bloc conformateur d'impulsions

Le bloc conformateur d'impulsions est un compteur ayant pour rôle la génération d'impulsions. Ces derniers seront utilisés pour contrôler l'envoi des deux signaux issus des systèmes en temps continu et hybride. Dans notre travail, nous avons choisi d'envoyer le signal $y_1 = z_2$ qui joue le rôle de signal de synchronisation sur une période T_1 et le signal $y_2 = x_2$ qui représente le signal utile (porteur d'informations) sur une période $9T1$ (voir paragraphe suivant). Donc, le signal de contôle issu du bloc conformateur d'impulsions

est un signal périodique de période $T_2 = 10T_1$.

2.3.1.4 Etude du bloc de multiplexage

Le bloc de multiplexage a pour rôle d'envoyer dans le canal suivant la règle définie précédemment les deux sorties y_1 et y_2. Ce bloc est piloté par le signal d'horloge issu de la sortie du conformateur d'impulsions. Le signal y_1 est d'abord échantillonné avec un pas d'échantillonnage T_2 mais bloqué uniquement durant la période T_1 qui doit vérifier le théorème de Shannon. Ensuite, il sera introduit dans le bloc multiplexage pour être envoyé dans le canal pendant une durée T_1. Quant au signal $y_2 = x_2$ qui n'est pas itéré pendant l'envoi du signal y_1, il sera envoyé pendant 9 durées T_1. Le choix de cette durée est fait dans le but d'assurer une bonne transmission, c'est à dire, un rapport signal utile (donné sur $9T_1$) sur signal de transmission (donné sur $T_2 = 10T_1$) le plus possible proche de un. Le cycle de transmission des deux signaux y_1 et y_2 est résumé par le schéma suivant :

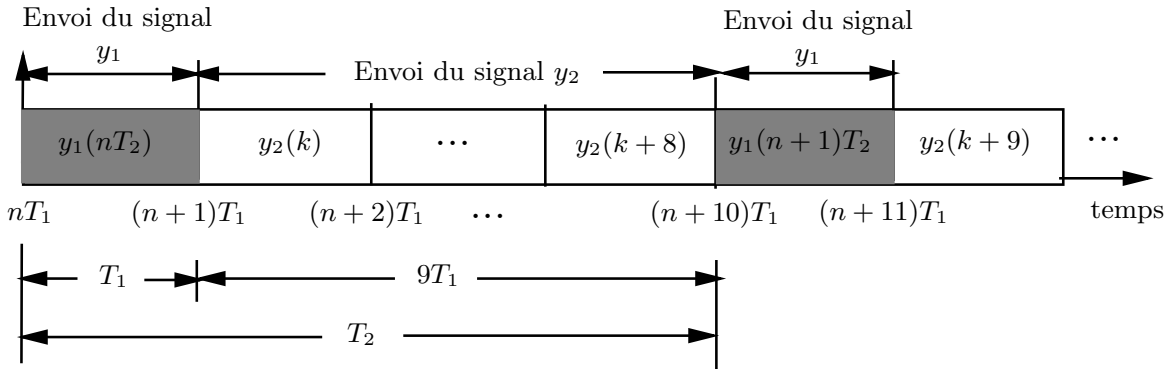


FIG. 2.13: Cycles de transmission des signaux y_1 et y_2

2.4 Conclusion

Dans ce chapitre, nous avons présenté l'émetteur du nouveau schéma de transmission proposé. L'émetteur est constitué principalement d'un système d'un système en temps continu et d'un système hybride. Dans un premier temps, nous avons procédé à l'étude du système en temps continu. D'abord, nous avons expliqué le choix et le principe de fonctionnement de l'oscillateur de Colpitts en étudiant ses différents comportements en fonction de variation de ses paramètres. Dans cette partie, nous avons ajusté les paramètres de l'oscillateur de Colpitts afin d'obtenir un comportement chaotique. Ces études

ont été mises en évidence à l'aide de simulations. Ensuite, nous sommes passés à la présentation du système hybride. De même, dans cette partie, nous avons donné les paramètres de ce système qui nous permettent d'avoir un comportement chaotique. Pour rendre le système de transmission robuste, nous avons jugé utile de rendre la structure d'émetteur plus complexe. Pour ce faire, nous avons introduit les états du système en temps continu dans la dynamique du système en temps discret pour avoir une dynamique hybride. Néanmoins, ce schéma n'est pas robuste contre une attaque à textes clairs connus (voir les détails au chapitre 5). La solution proposée consiste alors à retarder les états du système en temps continu avant leurs échantillonnages. Dans le chapitre qui suit, nous allons passer à la description et à l'étude du récepteur.

Chapitre 3

Etude du récepteur

3.1 Introduction

La recherche sur la synchronisation des systèmes chaotiques est un domaine en plein essor. Nous nous contenterons donc de citer quelques schémas de synchronisation utilisant les différentes techniques d'observation non linéaires présentées dans la littérature. La majorité des articles sur la synchronisation chaotique concerne des travaux utilisant des observateurs de type "grand gain", exploitant le fait que la plupart des systèmes chaotiques utilisés possèdent des non linéarités lipschitziennes. Parmi les nombreuses références disponibles dans la littérature, on peut citer les travaux de Liao *et al.* [96] qui proposent un schéma de communications sécurisées utilisant la synchronisation chaotique, appliqué aux systèmes de Lorenz et Rössler. Les auteurs construisent un observateur qui garantit une convergence exponentielle de l'erreur de synchronisation vers zéro. Ces travaux ont été généralisés à une plus grande classe de systèmes non linéaires par Boutayeb *et al.* [21]. Dans l'article [3], Alvarez *et al.* détaillent la construction d'un observateur pour une classe de systèmes, dont le gain peut être formulé explicitement en fonction de la vitesse de convergence désirée. Jiang *et al.* [76] ont mis au point un critère de synchronisation utilisant une commande par retour d'état linéaire, appliquée au circuit de Chua. Ce critère est étendu à une classe de systèmes chaotiques dans [77]. Dans l'article [47], Feki propose un observateur réduit permettant la synchronisation exponentielle de l'émetteur et du récepteur. Les travaux de Celikovsky *et al.* [26] traitent le problème de la synchronisation des systèmes chaotiques par la théorie de la commande, et détaillent un processus de synchronisation globale exponentielle. La théorie des modes glissants est à

l'origine du schéma de synchronisation présenté par Chen *et al.* dans [27] et par L'Hernault dans [72]. Une comparaison de différentes techniques de synchronisation, appliquées à des systèmes chaotiques connus, est détaillée dans [61]. Le fonctionnement correct de tous ces observateurs dépend de plusieurs conditions : la condition d'observabilité pour retrouver les états du système ; la condition de recouvrement de l'observabilité ("observability matching condition") pour retrouver les états du système et l'information noyée dans le système (inversibilité à gauche du système) ; la condition d'identifiabilité des paramètres qui représente les clés de codage.

Ce chapitre est consacré à l'étude du récepteur de la méthode de transmission sécurisée décrite au chapitre 2. Le rôle de ce récepteur est d'assurer la synchronisation entre l'émetteur et le récepteur. Il est constitué de deux types d'observateurs. Le premier observateur est de type impulsif, il consiste à récupérer tous les états du système en temps continu de l'émetteur. La synchronisation impulsive expliquée au chapitre 1 sera utilisée pour récupérer les états du système en temps continu. Cette méthode de synchronisation a montré une grande efficacité dans les applications de communication utilisant le chaos car elle maintient la synchronisation par des impulsions de petite taille. Dans la synchronisation impulsive, la transmission se fait à des instants temps discret. Cela permettra d'économiser la capacité du canal de communication pour la transmission des messages. En outre, du fait que ces impulsions sont discrètes, la redondance de l'information de synchronisation dans le canal sera réduite et donc la sécurité du système de communication va augmenter. Le second observateur est de type hybride, simple à concevoir ayant pour rôle la récupération de tous les états ainsi que l'information discrète cachée du système hybride.

Ce chapitre est organisé comme suit. La section 3.2.1 est consacrée à l'étude de l'observateur en temps continu déstiné à reconstruire les états du système en temps continu. Ici, nous allons montrer que l'utilisation d'un observateur impulsif classique donné par Yang *et al.* dans [157] n'est pas possible. A cet effet, un nouvel observateur impulsif sera proposé. Dans la section 3.2.2, deux observateurs hybrides seront présentés. Le premier consiste à récupérer les états ainsi que le message du système hybride sans retard et le second a pour rôle, la récupération des états ainsi que le message du système hybride avec retard. La section 3.2.3 sera consacrée à la présentation du bloc de démultiplexage. Enfin, nous terminons le chapitre par une conclusion.

3.2 Etude du récepteur

Le récepteur est constitué de trois blocs (voir Figure 2.1) : un observateur en temps continu, un observateur hybride et un bloc de démultiplexage. Les clés privées (quelques paramètres du système chaotique en temps continu et du système hybride et des valeurs du retard) décrites dans la section 2.3.1 pour l'émetteur sont utilisées pour récupérer le message.

Dans ce qui suit, nous allons nous intéresser à la synchronisation entre l'émetteur et le récepteur du schéma de transmission proposé. Nous allons présenter deux observateurs, l'un en temps continu ayant pour rôle, la récupération des états du système en temps continu (2.13) et l'autre en temps discret ayant pour rôle la récupération des états du système sans retard (2.15) et du système avec retard (2.16). Comme expliqué au chapitre 2, l'ajout de ces retards dans le système chaotique en temps discret (2.14) permet d'augmenter la difficulté d'identification des paramètres du système (2.16) (voir rôle de ces retards au chapitre 5). Les blocs du récepteur sont détaillés de la manière suivante :

3.2.1 Etude de l'observateur en temps continu

Cette partie est consacrée à la conception d'un observateur impulsif classique pour récupérer les états du système (2.13). Pour ce faire, nous utilisons les travaux de Yang *et al* [157].

3.2.1.1 Observateur impulsif classique

Le principe de la conception de cet observateur est illustré par l'exemple qui suit [157] :

Exemple 6 *Dans cet exemple, nous étudions la synchronisation impulsive du système de Chua.*

Le système de Chua est modélisé par les équations suivantes [32] :

$$\begin{cases} \dot{x_1} = \alpha[x_2 - x_1 - f(x_1)] \\ \dot{x_2} = x_1 - x_2 + x_3 \\ \dot{x_3} = -\beta x_2 - \gamma x_3 \end{cases} \tag{3.1}$$

où $f(x)$ est une fonction non linéaire par morceaux qui traduit la caractéristique de la diode de Chua, elle est donnée par :

$$f(x_1) = bx_1 + \frac{1}{2}(a-b)(|x_1+1| - |x_1-1|) \tag{3.2}$$

où $a < b < 0$ sont deux constantes. Les états du système (3.1) sont tous mesurables.

Soit $X = (x_1, x_2, x_3)^T$, alors le système (3.1) peut être représenté par :

$$\dot{X} = AX + \Phi(X) \tag{3.3}$$

où :

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix}, \quad \Phi(X) = \begin{pmatrix} -\alpha f(x_1) & 0 & 0 \end{pmatrix}^T.$$

Posons $\delta^+ x(t=\tau_i) = x(\tau_i^+) - x(\tau_i^-) = U(i,x)$ avec $i = 1, 2, ...,$ et $0 < \tau_1 < \tau_2 < ...\tau_i < \tau_{i+1} < ...$ et $\lim\limits_{i \longrightarrow \infty} \tau_i = \infty$.

Il est facile de vérifier que les hypothèses données par 5 sont vérifiées. En appliquant les concepts de base de la commande impulsive décrits dans la section 5 du chapitre 1, l'observateur impulsif proposé pour (3.3) est donné comme suit :

$$\begin{cases} \dot{\hat{X}} & = & A\hat{X} + \Phi(\hat{X}), \quad t \neq \tau_i \\ \delta^+ \hat{X} & = & -BE, \quad t = \tau_i, \quad i = 1, 2, ... \\ \hat{X}(t_0^+) & = & X_0, \quad t_0 \geq 0 \end{cases} \tag{3.4}$$

où $E = (e_1 \;\; e_2 \;\; e_3)^T = (x_1 - \hat{x}_1 \;\; x_2 - \hat{x}_2 \;\; x_3 - \hat{x}_3)^T$, est le vecteur d'état sur les erreurs de synchronisation entre les deux systèmes (3.3) et (3.4) et B une matrice symétrique.

Il est à noter qu'aux instants de temps discrets $t = \tau_i$, tous les états de l'émetteur donné par (3.3) sont transmis au récepteur (3.4).

Le système d'erreur de synchronisation impulsive est donné par :

$$\begin{cases} \dot{E} & = & AE + \Psi(X, \hat{X}), \quad t \neq \tau_i \\ \delta^+ E & = & BE, \quad t = \tau_i, \quad i = 1, 2, ... \end{cases} \tag{3.5}$$

où $\Psi(X,\hat{X}) = \Phi(X) - \Phi(\hat{X}) = (-\alpha f(x_1) + \alpha f(\hat{x}_1) \;\; 0 \;\; 0)^T$. *Le théorème suivant garantit la stabilité asymptotique du système (3.5).*

Théorème 6 *[157] Supposons que* d *est la plus grande valeur propre de* $(I + B^T)(I + B)$, *où* I *est une matrice identité de dimension* 3×3. *Nous supposons également que le rayon spectral* ρ *de* $I + B$ *satisfait* $\rho(I + B) \leq 1$. *Soit* q *la plus grande valeur propre de* $(A + A^T)$ *et supposons que les impulsions sont équidistants et séparées par un intervalle* Δ. *Si*

$$0 \leq q + 2|\alpha a|a \leq -\frac{1}{\Delta}\ln(\epsilon d) \tag{3.6}$$

où $\epsilon > 1$, *alors la synchronisation impulsive du système (3.5) est asymptotiquement stable.*

La démonstration de ce théorème est donné par Yang et al *dans [156].*

Dans ce qui suit, nous présentons des résultats de simulation. Les valeurs numériques des paramètres du système (3.1) sont donnés comme suit : $\alpha = 15$, $\beta = 20$, $\gamma = 0.5$, $a = \frac{-120}{7}$, $b = \frac{-75}{7}$. *Les conditions initiales du système (3.1) sont* $(x_1(0), x_2(0), x_3(0)) = (-2.121304, -0.066170, 2.881090)$ *et* $(\hat{x}_1(0), \hat{x}_2(0), \hat{x}_3(0)) = (0, 0, 0)$ *La matrice* B *est choisie comme suit :*

$$B = \begin{pmatrix} -1.5 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \tag{3.7}$$

En considérant les matrices A *et* B *respectivement, on trouve que :* $q = 20.162$ *et* $d = 0.25$. *En choisissant* $\epsilon = 1.1$, *la synchronisation impulsive du système (3.5) est asymptotiquement stable que si* $0 \leq \Delta \leq 0.0021s$.

Les résultats sur les erreurs de synchronisation impulsive des états sont donnés par la figure 3.1. La figure 3.1a montre bien pour $\Delta = 0.002s$ *(la condition donnée par (3.6) est satisfaite), la synchronisation impulsive est asymptotiquement stable. Par contre, la figure 3.1b montre que pour* $\Delta = 5s$ *(la condition donnée par (3.6) est insatisfaite), la synchronisation impulsive est asymptotiquement instable.*

Dans ce qui suit, la même démarche sera utilisée afin de concevoir un observateur impulsif pour le système (2.13).

Maintenant, considérons le système (2.13) dont $y_1 = z_2$, la seule sortie transmise à des instants en temps discret. Les impulsions sont séparées par un intervalle de temps

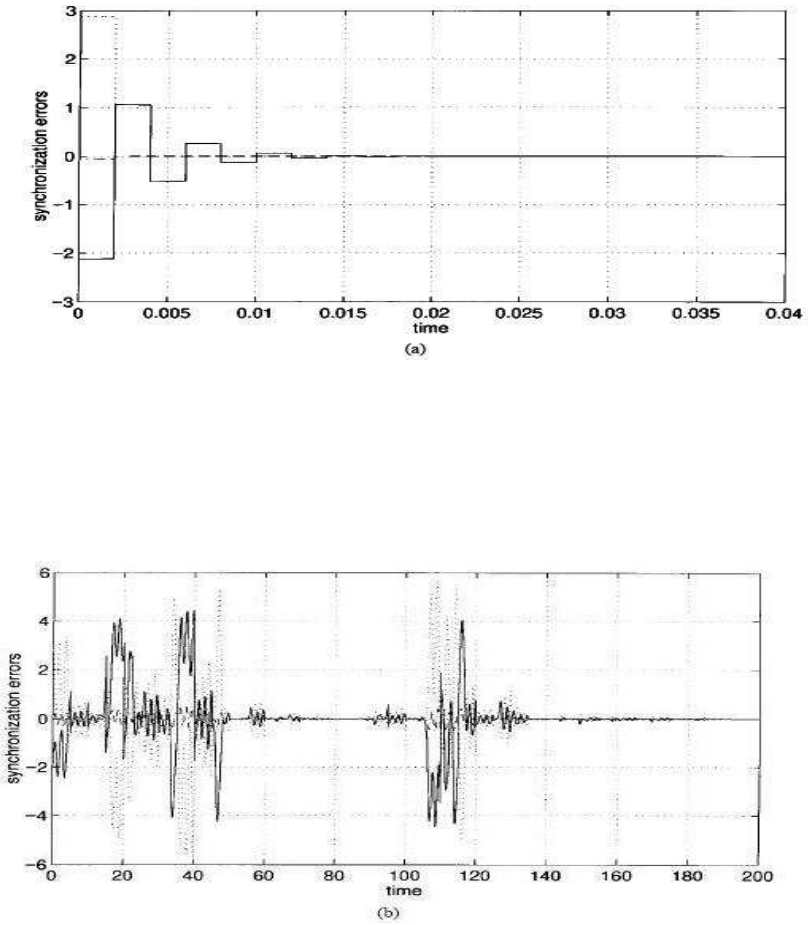


FIG. 3.1: Erreur de synchronisation sur les états : (a) $\Delta = 0.002s$ et (b) $\Delta = 5s$

$T_2 = \tau_{i+1} - \tau_i$ (voir Figure 2.13).

Soit $Z = (z_1, z_2, z_3)^T$, alors, ce système peut être représenté par :

$$\dot{Z} = AZ + \Phi(Z), \tag{3.8}$$

où :

$$A = \begin{pmatrix} 0 & 0 & a_1 \\ 0 & 0 & a_2 \\ -a_3 & -a_3 & -a_4 \end{pmatrix}, \quad \Phi(Z) = \begin{bmatrix} a_1(1 - \exp(-z_2)) & 0 & 0 \end{bmatrix}^T.$$

Il est facile de vérifier que les hypothèses 5 sont vérifiées où $n = 3$.

De même que l'exemple précèdent, l'observateur impulsif proposé pour (3.8) est donné comme suit :

$$\begin{cases} \dot{\hat{Z}} & = A\hat{Z} + \Phi(\hat{Z}), \quad t \neq \tau_i \\ \delta^+\hat{Z} & = -BE, \quad t = \tau_i, \quad i = 1, 2, ... \\ \hat{Z}(t_0^+) & = Z_0, \quad t_0 \geq 0 \end{cases} \tag{3.9}$$

où $E = (e_1 \;\; e_2 \;\; e_3)^T = (z_1 - \hat{z_1} \;\; z_2 - \hat{z_2} \;\; z_3 - \hat{z_3})^T$ est le vecteur d'état sur les erreurs de synchronisation entre les deux systèmes (3.8) et (3.9) et B une matrice symétrique. Le système d'erreur de synchronisation impulsive est donné par :

$$\begin{cases} \dot{E} & = AE + \Psi(Z, \hat{Z}), \quad t \neq \tau_i \\ \delta^+E & = BE, \quad t = \tau_i, \quad i = 1, 2, ... \end{cases} \tag{3.10}$$

où $\Psi(Z, \hat{Z}) = \Phi(Z) - \Phi[\hat{Z}) = (a_1(\exp(-\hat{z_2}) - \exp(-z_2)] \;\; 0 \;\; 0)^T$. Le théorème suivant garantit la stabilité asymptotique du système (3.10). Ce théorème découle du résultat établi dans [157] pour le circuit de Chua.

Théorème 7 *Supposons que les hypothèses données par 5 sont vérifiées et supposons que d est la plus grande valeur propre de $(I + B^T)(I + B)$, où I est une matrice identité de dimension 3×3. Nous supposons également que le rayon spectral ρ de $I + B$ satisfait $\rho(I + B) \leq 1$. Soit q la plus grande valeur propre de $(A + A^T)$ et supposons que les impulsions sont équidistants et séparées par un intervalle T_2. Si*

$$0 \leq q + 2L \leq -\frac{1}{T_2}\ln(\epsilon d) \tag{3.11}$$

où $\epsilon > 1$, alors la synchronisation impulsive du système (3.10) est asymptotiquement stable.

Preuve.

Considérons la fonction de Lyapunov $V(t,E) = E^T E$. Pour $t \neq \tau_i$, nous avons :

$$\begin{aligned} D^+V(t,E) &= E^T AE + E^T A^T E + E^T \Psi(E) + \Psi^T(E)E \\ &\leq qE^T E + 2|\Phi(Z) - \Phi(\hat{Z})|e_{z_1} \\ &\leq qE^T E + 2Le_{z_1}^2 \\ &\leq (q+2L)E^T E \\ &\leq (q+2L)V(t,E) \end{aligned}$$

Donc, la condition 1 du Théorème 5 décrite au chapitre 1 est satisfaite avec $g(t,w) = (q+2L)w$.

La matrice B est symétrique, $I+B$ l'est aussi. En utilisant la norme euclidienne, nous avons :

$$\rho(I+B) = \|I+B\|.$$

En donnant n'importe quelle valeur $\rho_E > 0$ et $E \in S_{\rho_E}$ où $S_{\rho_E} = \{E \in \mathbb{R}^3 \mid \|E\| < \rho_E\}$, nous avons :

$$\|E+BE\| \leq \|I+B\|\|E\| = \rho(I+B)\|E\| \leq \|E\|$$

Cette dernière inégalité provient de l'expression $\rho(I+B) \leq 1$. En conséquence, $E+BE \in S_{\rho_E}$.

Pour $t = \tau_i$, nous avons :

$$\begin{aligned} V(\tau_i, E+BE) &= (E+BE)^T(E+BE) \\ &= E^T(I+B^T)(I+B)E \\ &\leq dV(\tau_i,E) \end{aligned}$$

Donc, la condition 2 du Théorème 5 est satisfaite avec $\Psi_i(w) = dw$. Nous pouvons également constater que la condition 3 du Théorème 5 est aussi satisfaite. Toutes les conditions du thèorème 5 sont satisfaites, alors la stabilité asymptotique du système (3.10) est equi-

valente à la stabilité asymptotique du système de comparaison donné comme suit :

$$\begin{cases} \dot{w} = (q + 2L)w, \quad t \neq \tau_i \\ w(\tau_i) = dw(\tau_i) \\ w(t_0) = w_0 \geq 0 \end{cases} \tag{3.12}$$

A partir du Théorème 2, nous posons $\dot{\lambda} = q + 2L \geq 0$. La synchronisation impulsive du système (3.10) est asymptotiquement stable que si la condition donnée par (3.11) est satisfaite. □

Néanmoins, nous constatons que la condition (3.11) n'est jamais satisfaite car $y_1 = z_2$ est la seule sortie transmise au récepteur. Contrairement à l'exemple précèdent où la condition (3.6) peut être satisfaite parce que tous ses états sont mesurables. En conséquence, l'observateur donné par (3.9) ne peut pas être utilisé pour assurer la synchronisation impulsive. A cet effet, un nouvel observateur impulsif est présenté ci-dessous.

3.2.1.2 Observateur impulsif proposé

Considérons le système (2.13) en tenant compte des hypothèses données par 5. En considérant uniquement la seule sortie mesurable $y_1 = z_2$, l'observateur proposé pour le système (3.8) s'écrit :

$$\begin{cases} \dot{\hat{z}}_1 & = & a_1(-\exp(-\hat{z}_2) + 1 + \hat{z}_3) \\ \dot{\hat{z}}_2 & = & a_2\hat{z}_3 \\ \dot{\hat{z}}_3 & = & -a_3(\hat{z}_1 + \hat{z}_2) - a_4\hat{z}_3 \\ \hat{z}_2(\tau_i^+) & = & z_2(\tau_i) \end{cases} \tag{3.13}$$

Définissons les erreurs d'observation :

$$e_1 = z_1 - \hat{z}_1, \quad e_2 = z_2 - \hat{z}_2, \quad e_3 = z_3 - \hat{z}_3 \tag{3.14}$$

A partir de (3.8), (3.13) et (3.14), les erreurs dynamiques de (3.14) sont :

$$\begin{cases} \dot{e_1} & = & a_1 \exp(-z_2)(\exp(e_2) - 1) + a_1 e_3 \\ \dot{e_2} & = & a_2 e_3 \\ \dot{e_3} & = & -a_3(e_1 + e_2) - a_4 e_3 \\ e_2(\tau_i) & = & 0 \end{cases} \tag{3.15}$$

En negligeant les termes d'ordre supérieurs dans la série de Taylor de l'expression $\exp(e_2)$, le système (3.15) devient :

$$\begin{cases} \dot{e_1} & = & a_1(\exp(-z_2)e_2 + e_3) \\ \dot{e_2} & = & a_2 e_3 \\ \dot{e_3} & = & -a_3(e_1 + e_2) - a_4 e_3 \\ e_2(\tau_i) & = & 0 \end{cases} \tag{3.16}$$

qui peut être réécrit sous la forme compacte :

$$\dot{E} = A'(t)E \tag{3.17}$$

où

$$A'(t) = \begin{pmatrix} 0 & a_1 \exp(-z_2(t)) & a_1 \\ 0 & 0 & a_2 \\ -a_3 & -a_3 & -a_4 \end{pmatrix} \tag{3.18}$$

et $E = (e_1 \;\; e_2 \;\; e_3)^T$.

Pour avoir une approximation du système en temps discret (3.17) homogène ainsi que dans le but de déterminer la limite de T_2 pour lequel l'observateur est valide, il est nécessaire de considérer l'approximation de $z_2(t)$ donnée par :

$$z_2(t) = z_2(0) + \dot{z_2}(0)t + O(t^2) \tag{3.19}$$

Considérons la série de Taylor de premier ordre de $\exp(-z_2(t))$. Alors l'approximation

homogène de $\exp(-z_2(t))$ est donnée par :

$$\exp(-z_2(t)) = \exp(-z_2(0)) - \exp(-z_2(0))\dot{z_2}(t)t + O(t^2) \tag{3.20}$$

Par conséquence, la solution de $\int_0^{T_2} \exp(-z_2(t))dt$ devient :

$$\int_0^{T_2} \exp(-z_2(t))dt = \exp(-z_2(0))T_2 - \dot{z_2}(0)\exp(-z_2(0))\frac{T_2^2}{2} + O(T_2^3) \tag{3.21}$$

Il est bien connu que la solution (3.17) est donnée par :

$$E(t) = E(0)\exp(\int_0^{T_2} \exp(A'(t))dt) \tag{3.22}$$

Il découle de (3.18), (3.21) et (3.22) que :

$$E[(k+1)T_2] = \exp(\tilde{A})E(kT_2) \tag{3.23}$$

avec

$$\tilde{A} = \begin{pmatrix} 0 & a_1[\exp(-z_2(0))T_2 - \dot{z_2}(0)\exp(-z_2(0))\frac{T_2^2}{2}] & a_1T_2 \\ 0 & 0 & a_2T_2 \\ -a_3T_2 & -a_3T_2 & -a_4T_2 \end{pmatrix} \tag{3.24}$$

Afin de garantir la convergence du système (3.23), une condition suffisante est établie par le Théorème qui suit :

Théorème 8 *[64] Le système (3.23) est asymptotiquement stable si et seulement si pour toute matrice $Q = Q^T > 0$, il existe une matrice unique $P = P^T > 0$ telle que l'égalité suivante :*

$$M\exp(\tilde{A})M^TPM\exp(\tilde{A})M^T - P = -Q \tag{3.25}$$

est satisfaite.

où P est une matrice de dimension 2×2 et M une matrice de dimension 2×3 égale à :

$$M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Etant donné que $e_2(k)$ est initialisée à chaque instant $t = \tau_i$, seule la dynamique des erreurs $e_1(k+1)$ et $e_3(k+1)$ sera étudiée. A cet effet, l'ajout de la matrice M permet de construire $e_1(k+1)$ et $e_3(k+1)$.

Preuve.

Pour $t = \tau_i$, on considére la fonction de Lyapunov candidate en temps discret k :

$$V(kT_2) = E(kT_2)^T M^T P M E(kT_2)$$

$$\Delta V(kT_2) = V[(k+1)T_2] - V(kT_2)$$

Il en résulte

$$\Delta V(kT_2) = E[(k+1)T_2]^T M^T P M E[(k+1)T_2] - E(kT_2)^T M^T P M E(kT_2)$$

$$\begin{aligned} \Delta V(kT_2) &= E(kT_2)^T M^T [M \exp(\tilde{A}) M^T P M \exp(\tilde{A}) M^T - P] M E(kT_2) \\ &= E(kT_2)^T M^T (-Q) M E(kT_2) \end{aligned}$$

□

Maintenant, nous utilisons le résultat du Théorème 8 pour déterminer la période des impulsions T_2 permettant d'assurer la stabilité asymptotique du système (3.23). La détermination de cet intervalle de manière analytique étant difficile, le calcul se fera numériquement en faisant plusieurs tests. Le premier test consiste à prendre une valeur de T_2 faible de l'ordre $0.001s$, ensuite de faire augmenter cette valeur graduellement jusqu'à la perte de la stabilité asymptotique du système (3.23).

Alors, nous trouvons que le système (3.23) est asymptotiquement stable que si (3.26) est satisfaite.

$$0 \leq T_2 \leq 0.4s. \tag{3.26}$$

3.2.2 Etude de l'observateur hybride

Dans cette partie, un observateur hybride étape par étape [14], [43] est choisi afin de récupérer les états ainsi que le message du système hybride sans retard (2.15) et du système hybride avec retard (2.16). La conception de cet observateur est illustrée par l'exemple suivant :

Exemple 7 *Considérons le système donné par (1.32). La méthode de cryptage par inclusion est utilisée pour camoufler le message $u(n)$ avec $y(n) = x_2(n)$ sa sortie correspondante. Le pas de discrétisation considéré dans ce système est $T = 1s$.*

Dans cet exemple, les deux hypothèses 7 et 8 sont vérifiées, il est alors possible de concevoir un observateur hybride retardé étape par étape.

- Reconstruction de l'état $\hat{x}_3$:

A partir de la dernière équation de (1.32), on a :

$$\hat{x}_3(n+1) = y(n)$$

En appliquant un retard sur la sortie, on déduit l'état $\hat{x}_3$ comme suit :

$$\hat{x}_3(n) = y(n-1) \tag{3.27}$$

- Reconstruction de l'état $\hat{x}_1$:

De la deuxième équation de (1.32), on a également :

$$\hat{x}_2(n+1) = \hat{x}_1(n)$$

En appliquant deux retards sur la sortie et en utilisant l'équation (3.27), on obtient l'état $\hat{x}_1$:

$$\hat{x}_1(n-2) = y(n-1) \tag{3.28}$$

- Reconstruction du message $\hat{u}$:

A partir de la première équation de (1.32), on a :

$$\hat{u}(n) = \hat{x}_1(n+1) + \hat{x}_2^2(n) + b\hat{x}_3(n) - a$$

En appliquant trois retards sur la sortie et en utilisant les équations (3.27) et (3.28), on aura :

$$\hat{u}(n-3) = y(n-1) + y^2(n-3) + by(n-4) - a \tag{3.29}$$

Les résultats de simulation sur les erreurs de reconstruction des états ainsi que celle du message sont donnés par les figures 3.2, 3.3 et 3.4.

Les figures 3.2, 3.3 respectivement montrent bien que les erreurs de synchronisation des états x_3 et x_1 s'annulent après un pas $T = 1s$ et deux pas $T = 2s$. Quant à la figure 3.4, elle montre que l'erreur de synchronisation du message u s'annule après trois pas $T = 3s$. Donc, l'observateur conçu permet de reconstruire tous les états ainsi que le message.

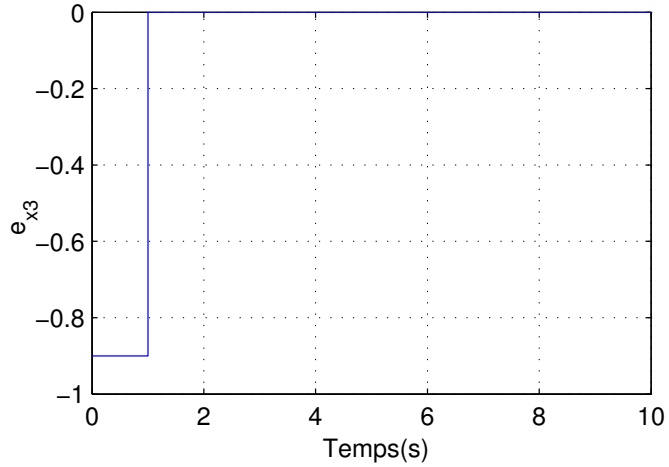


FIG. 3.2: Erreur de synchronisation de l'état x_3

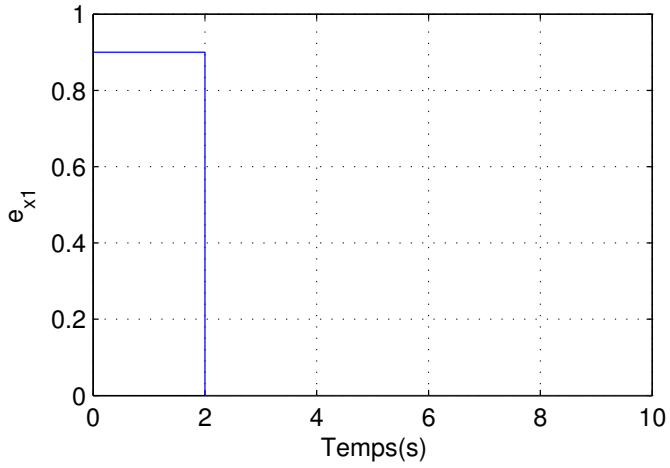


FIG. 3.3: Erreur de synchronisation de l'état x_1

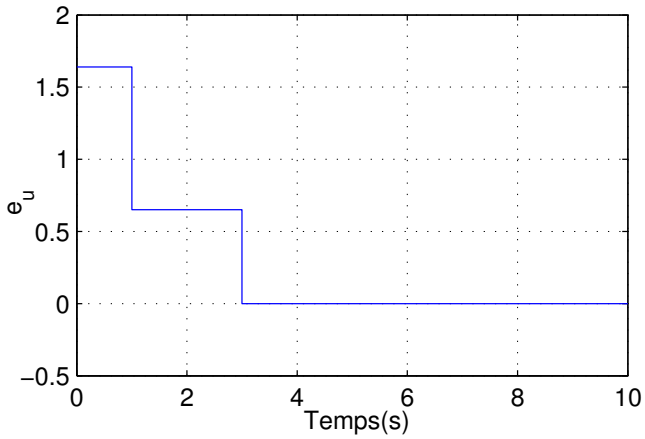


FIG. 3.4: Erreur de synchronisation du message u

A travers cet exemple, nous avons montré la démarche à suivre afin de concevoir un observateur hybride qui nous permet de reconstruire tous les états ainsi que le message. Dans ce qui suit, la même procédure sera utilisée afin de concevoir deux observateurs hybrides. Le premier correspond au système hybride sans retard (2.15) et le second au système hybride avec retard (2.16).

– **Cas sans retard**

Considérons le système (2.15), nous allons concevoir un observateur hybride, fonctionnant à la période T_1, de la façon suivante :

- Reconstruction de l'état $\hat{x}_1$:

A partir du système (2.15), on a :

$$\hat{x}_2(k+1) = \hat{x}_1(k)$$

En appliquant un retard sur la sortie, on déduit l'état $\hat{x}_1$ comme suit :

$$\hat{x}_1(k-1) = y_2(k) \tag{3.30}$$

- Reconstruction de l'état $\hat{x}_3$:

Du système (2.15), on a également :

$$\hat{x}_3(k) = \frac{a - \hat{x}_1(k+1) - \hat{x}_2^2(k)}{b}$$

En appliquant deux retards sur la sortie et en utilisant l'équation (3.30), on obtient

l'état $\hat{x}_3$:

$$\hat{x}_3(k-2) = \frac{a - y_2(k) - y_2^2(k-2)}{b} \tag{3.31}$$

- Reconstruction du message $\hat{m}$:

Du système (2.15), on a :

$$\hat{m}(k) = \frac{\hat{x}_3(k+1) - \hat{x}_2(k) - A\hat{z}_1(nT_1) - B\hat{z}_3(nT_1))}{c}$$

En appliquant trois retards sur la sortie et en utilisant l'équation (3.31), on aura :

$$\begin{aligned} \hat{m}(k-3) &= \frac{a - y_2(k) - y_2^2(k-2)}{bc} \\ &- \frac{y_2(k-3) + A\hat{z}_1(nT_1 - 3T_1) + B\hat{z}_3(nT_1 - 3T_1)}{c} \end{aligned} \tag{3.32}$$

Donc, les équations de l'observateur sont :

$$\begin{cases} \hat{x}_1(k-1) = y_2(k) \\ \hat{x}_3(k-2) = \frac{a - y_2(k) - y_2^2(k-2)}{b} \\ \hat{m}(k-3) = \frac{a - y_2(k) - y_2^2(k-2)}{bc} \\ \qquad - \frac{y_2(k-3) + A\hat{z}_1(nT_1 - 3T_1) + B\hat{z}_3(nT_1 - 3T_1)}{c} \end{cases} \tag{3.33}$$

L'équation (3.32) permet de reconstituer le message mais ceci uniquement après synchronisation des deux systèmes en temps continu (2.13) et (3.13).

– **Cas avec retard**

Le même calcul qu'auparavant sera fait dans ce cas.

Considérons le système (2.16).

- Reconstruction de l'état $\hat{x}_1$:

A partir du système (2.16), on a :

$$\hat{x}_2(k+1) = \hat{x}_1(k)$$

En appliquant un retard sur la sortie, on déduit l'état $\hat{x}_1$ comme suit :

$$\hat{x}_1(k-1) = y_2(k) \tag{3.34}$$

- Reconstruction de l'état $\hat{x}_3$:

Du système (2.16), on a également :

$$\hat{x}_3(k) = \frac{a - \hat{x}_1(k+1) - \hat{x}_2^2(k)}{b}$$

En appliquant deux retards sur la sortie et en utilisant l'équation (3.34), on obtient l'état $\hat{x}_3$:

$$\hat{x}_3(k-2) = \frac{a - y_2(k) - y_2^2(k-2)}{b} \tag{3.35}$$

- Reconstruction du message $\hat{m}$:

Du système (2.16), on a :

$$\hat{m}(k) = \frac{\hat{x}_3(k+1) - \hat{x}_2(k) - A\hat{z}_1(nT_1 - \tau_1) - B\hat{z}_3(nT_1 - \tau_2)}{c}$$

En appliquant trois retards sur la sortie et en utilisant l'équation (3.35), on aura :

$$\begin{aligned} \hat{m}(k-3) &= \frac{a - y_2(k) - y_2^2(k-2)}{bc} \\ &- \frac{y_2(k-3) + A\hat{z}_1(nT_1 - \tau_1 - 3T_1) + B\hat{z}_3(nT_1 - \tau_2 - 3T_1)}{c}. \end{aligned} \tag{3.36}$$

Donc, les équations de l'observateur sont :

$$\begin{cases} \hat{x}_1(k-1) = y_2(k) \\ \hat{x}_3(k-2) = \frac{a - y_2(k) - y_2^2(k-2)}{b} \\ \hat{m}(k-3) = \frac{a - y_2(k) - y_2^2(k-2)}{bc} \\ \qquad - \frac{y_2(k-3) + A\hat{z}_1(nT_1 - \tau_1 - 3T_1) + B\hat{z}_3(nT_1 - \tau_2 - 3T_1)}{c} \end{cases} \tag{3.37}$$

Si les deux systèmes (2.13) et (3.13) sont synchronisés, l'équation (3.36) permet de reconstuire le message m.

3.2.3 Etude du bloc de démultiplexage

A la réception, le signal reçu sera d'abord démultiplexé en deux signaux y_1 et y_2. Le signal y_1 qui n'est accessible que durant la période T_1 est maintenant mémorisé sur une

période $T_2 = 10T_1$ (voir figure 2.13). Ensuite, il est introduit dans l'observateur en temps continu. L'autre signal y_2 est accessible pendant 9 cycles et change tous les cycles. Il est introduit dans l'observateur hybride.

3.3 Conclusion

Dans ce chapitre, deux types d'observateurs ont été proposés. Le premier est de type impulsif et a pour rôle de récupérer tous les états du système en temps continu et l'autre pour récupérer les états du système hybride. Le choix de l'observateur impulsif s'explique par les avantages qu'ils présentent. Parmi ses avantages, nous avons : l'augmentation la sécurité du système de communication chaotique car, la redondance de l'information de synchronisation dans le canal est réduite. Le second observateur utilisé dans notre travail est de type hybride étape par étape. Son choix s'explique par sa facilité de conception.

Dans ce travail, nous avons montré que la récupération du message passe d'abord par la synchronisation des états des systèmes en temps continu où le signal y_1 joue le rôle de signal de synchronisation. Pour un pirate, le temps de synchronisation des deux systèmes en temps continu est inconnu et par conséquence, il joue un rôle important pour l'identification de tous les paramètres du système hybride de l'émetteur. Le chapitre suivant sera consacré à la présentation des résultats de simulation.

Chapitre 4

Résultats de simulation

Chapitre 4

Résultats de simulation

4.1 Introduction

Dans ce chapitre, les performances de la méthode proposée seront évaluées à l'aide du logiciel Matlab. Ce chapitre est subdivisé comme suit : La section 4.2 est consacrée à la présentation des résultats de simulation appropriés à une transmission sécurisé d'un signal numérique, en considérant deux cas : le cas où $T_2 = 0.4s$ qui satisfait la condition (3.26) et le cas où $T_2 = 0.5s$ qui ne satisfait pas cette condition. Dans chaque cas, des résultats de simulation seront aussi donnés et commentés en absence et en présence des retards. Dans ce dernier, nous introduisons uniquement à chaque période T_1 dans l'état continu échantillonné $z_1(nT_2)$ des retards différents notés τ_{1i} (pour $i = 1, ..., 9$) (voir chapitre 5). Dans la section 4.3, des résultats de simulation seront présentés et commentés dans le cas de l'application de la méthode sur une transmission sécurisée d'une image. Dans la section 4.4, nous allons présenter quelques résultats de simulation sur la synchronisation des états des systèmes en temps continu dans le cas où il y a une perte du signal de synchronisation. La section 4.5 consiste à étudier l'impact de la présence de bruit de transmission ainsi que les variations des paramètres des systèmes chaotiques sur la restauration de message. Enfin, ce chapitre sera clôturé par une conclusion.

4.2 Transmission d'un signal numérique

Dans cette section, nous présentons les résultats de simulation dans le cas d'une transmission d'un signal numérique. Nous allons d'abord présenter les résultats de la synchro-

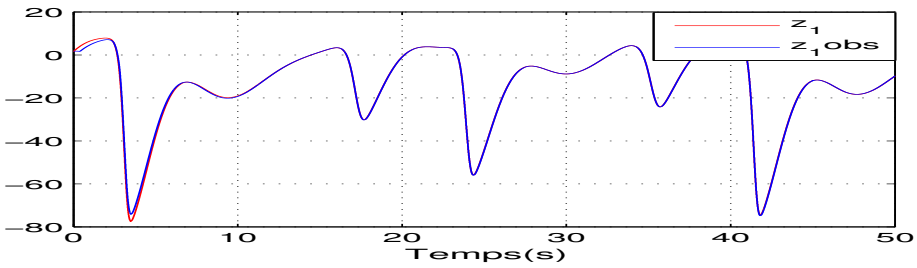


FIG. 4.1: Les états z_1 et $\hat{z}_1$

nisation des deux systèmes en temps continu, ensuite, ceux des deux systèmes dynamiques hybrides. Dans cette section, nous considérons que le canal est idéal, sans retard dans la transmission et non bruité.

Dans ce qui suit, deux cas seront traités :

- T_2 satisfait l'inégalité (3.26) : $T_2 = 0.4s$
- T_2 ne satisfait pas l'inégalité (3.26) : $T_2 = 0.5s$

4.2.1 Cas où $T_2 = 0.4s$

4.2.1.1 Résultats de la synchronisation des deux systèmes en temps continu sans retards

Les conditions initiales choisies d'observateur (3.13) sont : $\hat{z}_1(0) = 1.8$, $\hat{z}_3(0) = 0$ et la condition initiale de $\hat{z}_2(0)$ est donnée par la sortie y_1 du système (3.13). Les conditions initiales du système en temps continu (2.13) sont données dans le paragraphe 2.3.1.1. Les états des systèmes en temps continu (2.13) et (3.13) sont échantillonnés avec un pas d'échantillonnage $T_1 = 0.04s$.

Les figures 4.1, 4.3, 4.5 et 4.2, 4.4, 4.6 montrent respectivement les états et leurs erreurs de synchronisation. A travers ces figures, nous constatons bien que toutes les erreurs de synchronisation (e_1, e_2 et e_3) convergent vers zéro à partir de l'instant $t = 9s$, grâce au bon choix de la période T_2 qui satisfait la condition (3.26).

4.2.1.2 Résultats de la synchronisation des deux systèmes dynamiques hybrides sans retards

Dans cette partie, les résultats de simulation pour la synchronisation des deux systèmes (2.15) et (3.33) sont présentés. Les nouveaux paramètres A_1, A_2 et c choisis du système

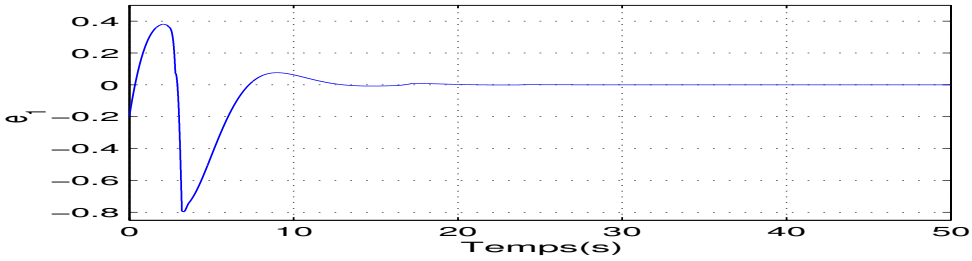


FIG. 4.2: Erreur de synchronisation de l'état z_1

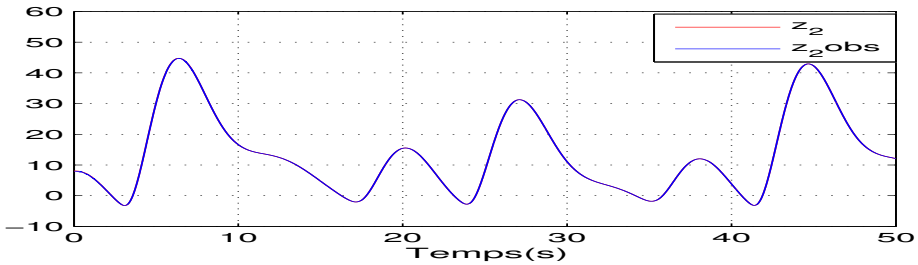


FIG. 4.3: Les états z_2 et $\hat{z}_2$

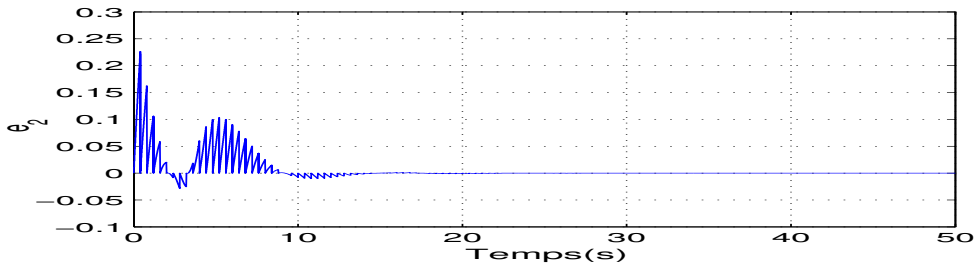


FIG. 4.4: Erreur de synchronisation de l'état z_2

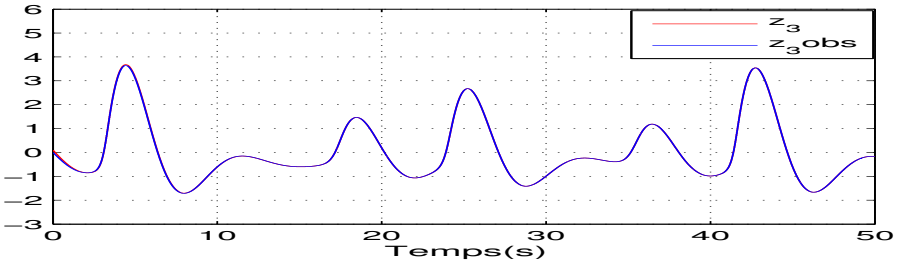


FIG. 4.5: Les états z_3 et $\hat{z}_3$

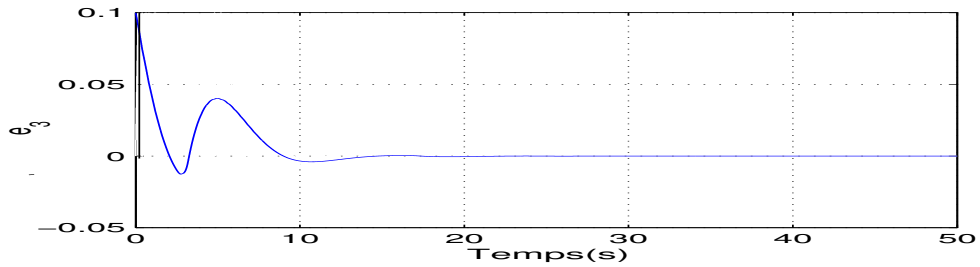


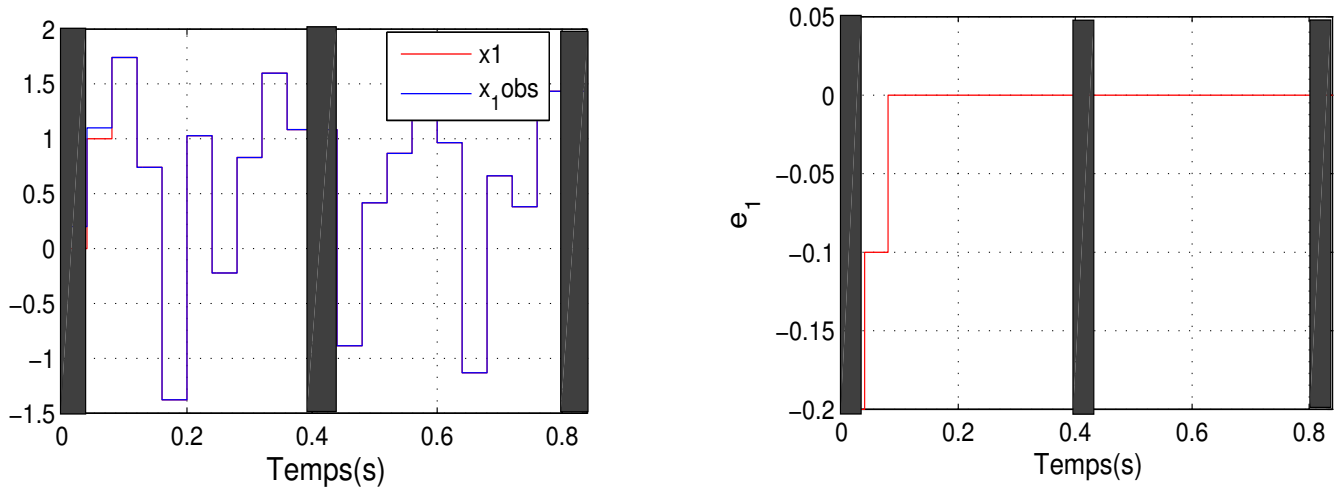
FIG. 4.6: Erreur de synchronisation de l'état z_3

(2.15) vérifiant les conditions données dans le paragraphe 2.3.1.2 sont : $A_1 = 0.001$, $A_2 = 0.001$ et $c = 1$. Le message à masquer est un signal carré d'amplitude 0.1 et de période égale à 0.8s. Il est à noter que les deux sorties à transmettre (y_1 et y_2) sont envoyées sur le canal à chaque période $T_2 = 10T_1$ (voir figure 2.13).

Les résultats de synchronisation des états ainsi que leurs erreurs de synchronisation sont donnés respectivement par les figures (4.7a, 4.8a) et (4.7b, 4.8b). Il est à noter que les états reconstruits x_1 et x_3 du système (3.33) ne dépendent pas des états z_1, z_2 et z_3 du système (2.13). Cela permet d'établir que l'erreur $e_1 = x_1 - \hat{x}_1$ s'annule après $T_1 = 0.04s$ qui correspond à un retard d'un pas qui est en accord avec l'équation (3.30). L'erreur e_3 s'annule après $2T_1 = 0.08s$ qui correspond à un retard de deux pas qui est en accord avec l'équation (3.31). En revanche, la reconstruction du message m (voir équation (3.32)) dépend de la la synchronisation des états des deux système en temps continu (2.13) et (3.13). Donc, la récupération du message m (voir figures 4.9a et 4.9b) est obtenue à partir de l'instant $t = 9s$ qui correspond au temps de synchronisation des deux systèmes (2.13) et (3.13). Il est important de noter durant l'envoi du signal de synchronisation y_1 correspondant à la période T_1, les états en temps discret ainsi que le message sont préservés à leurs anciennes valeurs. Autrement dit, ils ne sont pas itérés. Ceci est montré par les cycles colorés en gris sur les figures.

4.2.1.3 Résultats de la synchronisation des deux systèmes en temps continu avec retards

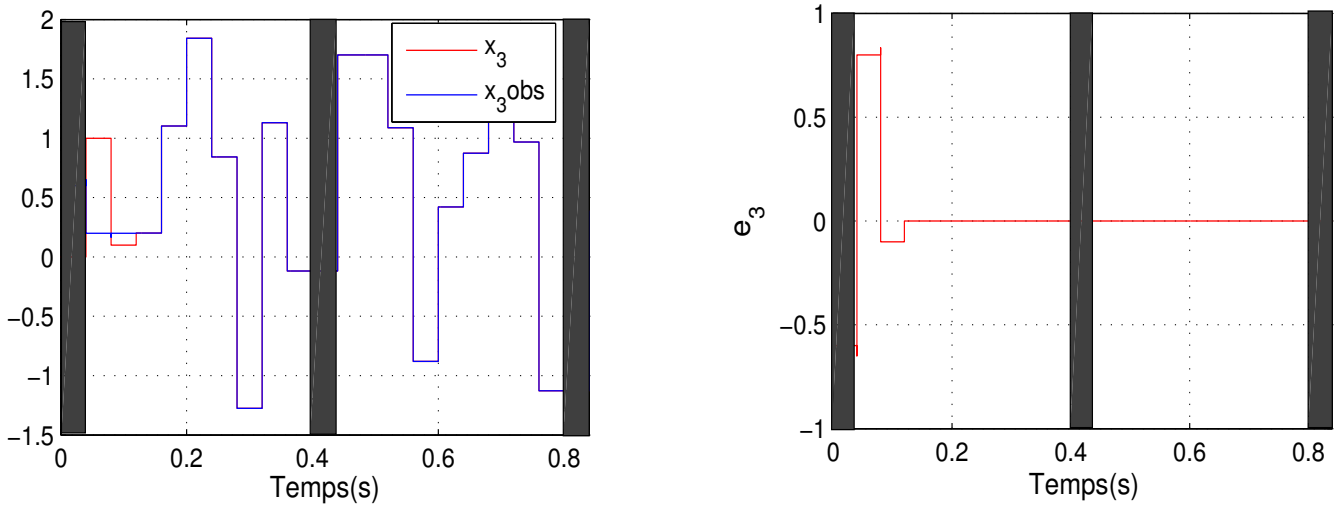
Dans cette partie, les mêmes paramètres de simulation sont considérés.
Les figures 4.10, 4.12, 4.14 et 4.11, 4.13, 4.15 montrent respectivement les états et leurs erreurs de synchronisation. De même, que le cas sans retard, nous constatons bien que les erreurs de synchronisation (e_1, e_2 et e_3) convergent vers zéro à partir de $t = 9s$. Ce



(a) (x_1 et $\hat{x}_1$)

(b) Erreur de synchronisation de l'état x_1

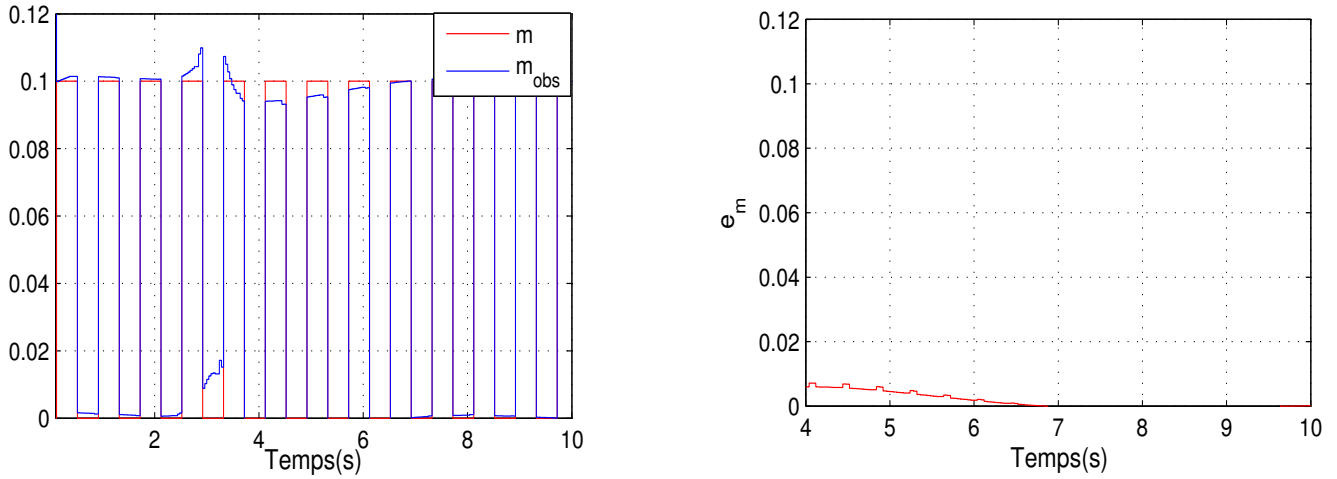
FIG. 4.7: Résultats de simulation sur la synchronisation des états x_1 et $\hat{x}_1$



(a) (x_3 et $\hat{x}_3$)

(b) Erreur de synchronisation de l'état x_3

FIG. 4.8: Résultats de simulation sur la synchronisation des états x_3 et $\hat{x}_3$



(a) Messages: m et $\hat{m}$

(b) Zoom sur l'erreur de synchronisation du message m

FIG. 4.9: Résultats de simulation sur la synchronisation des messages m et $\hat{m}$

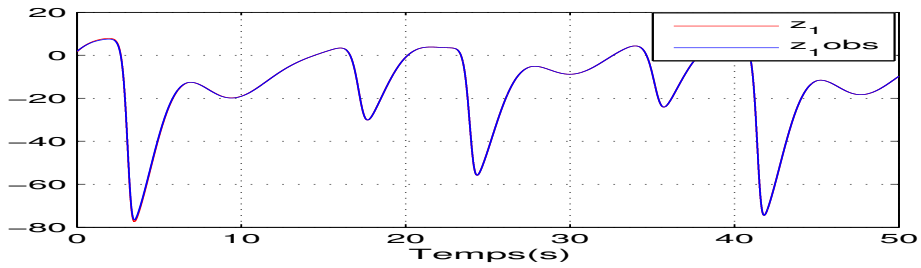


FIG. 4.10: Les états z_1 et $\hat{z}_1$

résultat est prévisible à cause du bon choix de la période T_2.

4.2.1.4 Résultats de la synchronisation des deux systèmes dynamiques hybrides avec retards

Dans cette partie, nous introduisons les retards τ_{1i} (pour $i = 1, ..., 9$) qui sont les nouveaux paramètres du système (2.16). Pour les simulations, nous avons choisi les valeurs numériques suivantes : $\tau_{11} = \tau_{12} = \tau_{13} = \tau_{14} = 0.01s$, $\tau_{15} = \tau_{16} = \tau_{17} = \tau_{18} = 0.02s$ et $\tau_{19} = 0.03s$. Il est à noter que ces valeurs peuvent être changées à chaque période T_2. Dans notre cas, nous gardons les mêmes valeurs des retards durant tout le temps de la simulation. Les résultats de synchronisation des états ainsi que leurs erreurs de synchronisation sont donnés respectivement par les figures (4.16a, 4.17a) et (4.16b, 4.17b). A travers ces figures, nous constatons que l'erreur e_1 s'annule après un pas $T_1 = 0.04s$ et l'erreur e_3 s'annule après deux pas $2T_1 = 0.08s$. De même qu'auparavant, la récupération

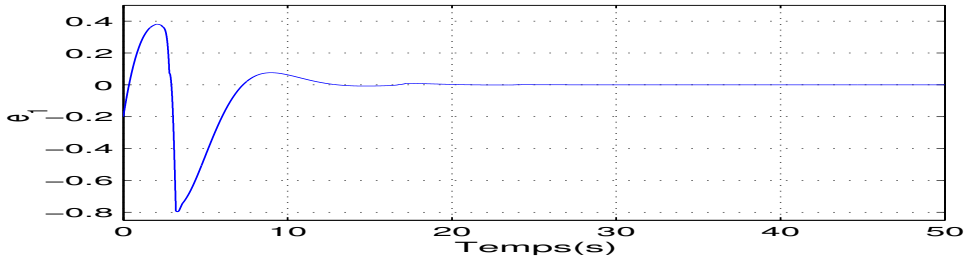


FIG. 4.11: Erreur de synchronisation de l'état z_1

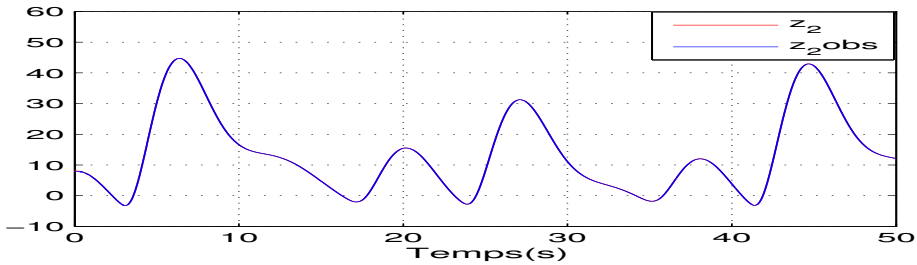


FIG. 4.12: Les états z_2 et $\hat{z}_2$

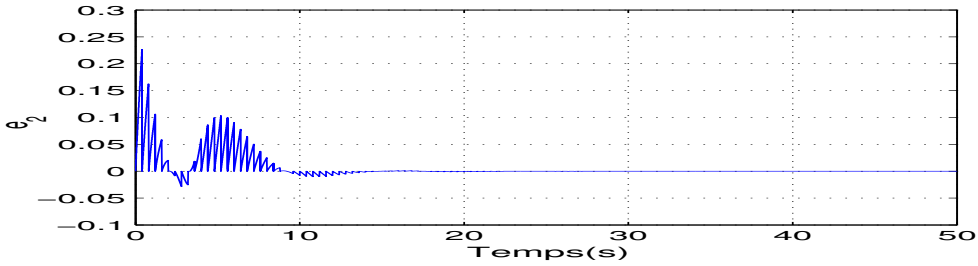


FIG. 4.13: Erreur de synchronisation de l'état z_2

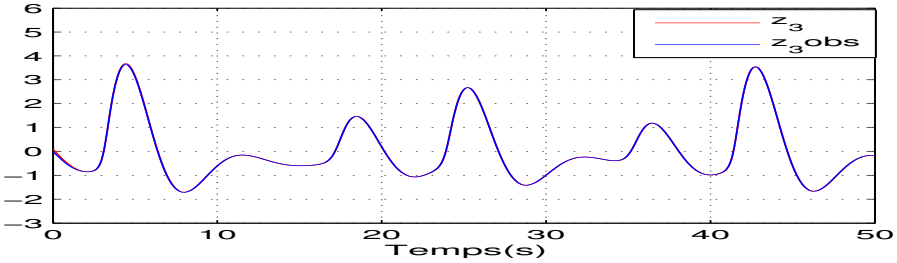


FIG. 4.14: Les états z_3 et $\hat{z}_3$

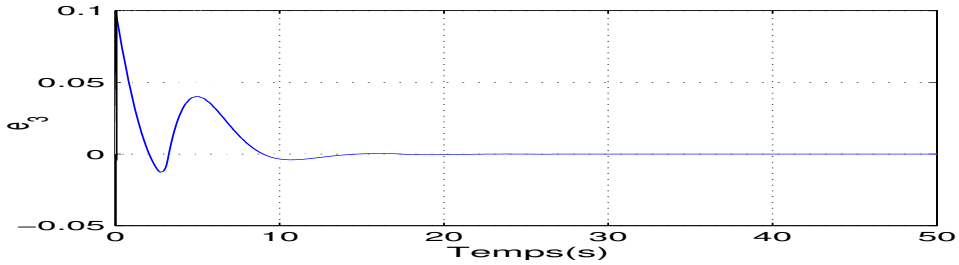
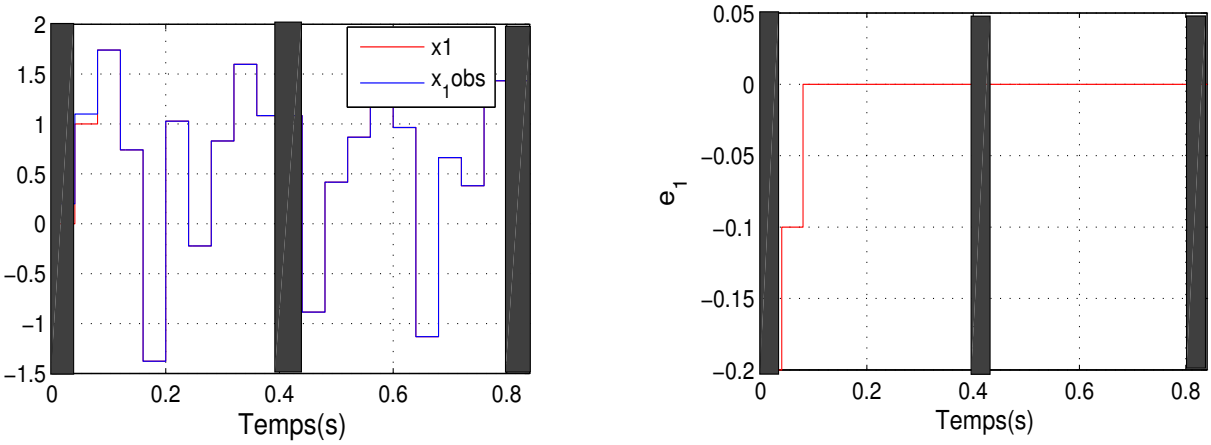


FIG. 4.15: Erreur de synchronisation de l'état z_3



(a) (x_1 et $\hat{x}_1$)

(b) Erreur de synchronisation de l'état x_1

FIG. 4.16: Résultats de simulation sur la synchronisation des états x_1 et $\hat{x}_1$

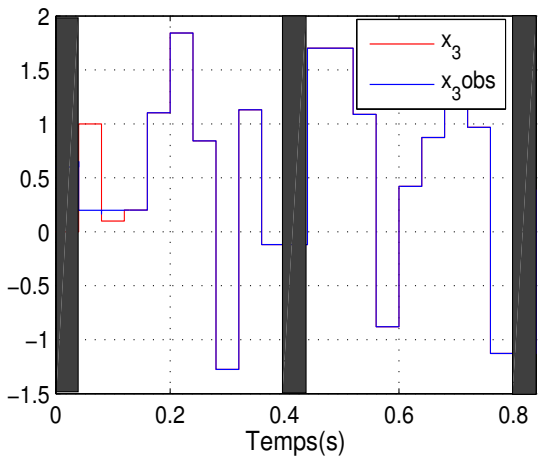
du message m (voir figures 4.18a et 4.18b) est obtenue à partir de l'instant $t = 9s$ qui correspond au temps de synchronisation des deux systèmes (2.13) et (3.13).

4.2.2 Cas où $T_2 = 0.5s$

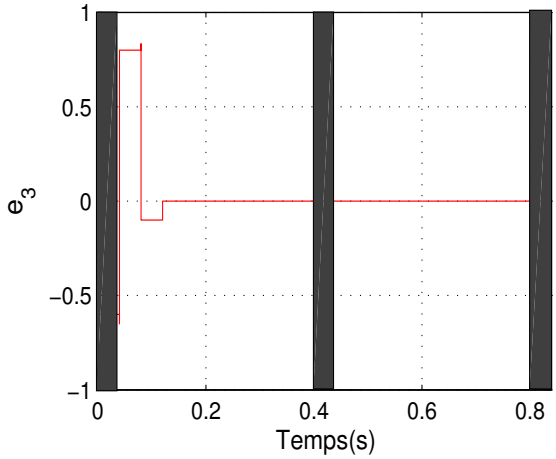
4.2.2.1 Résultats de la synchronisation des deux systèmes en temps continu avec retards

Dans cette partie, nous gardons les mêmes paramètres de simulation que ceux donnés dans le cas précédent en considérant uniquement le cas avec retards.

Les états et leurs erreurs de synchronisation sont représentés respectivement par les figures 4.19, 4.21, 4.23 et 4.20, 4.22, 4.24. D'après ces figures, nous constatons bien que tous les états e_1, e_2 et e_3 ne convergent pas vers zéro. Autrement dit, les deux systèmes en temps continu sont désynchronisés. Ceci est expliqué par le fait que la valeur de T_2 ne satisfait pas la condition (3.26).

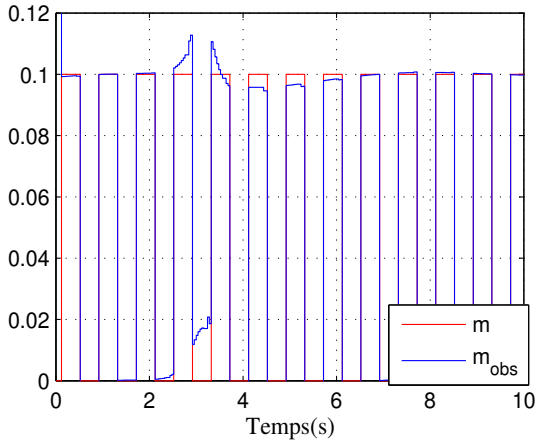


(a) (x_3 et $\hat{x}_3$)

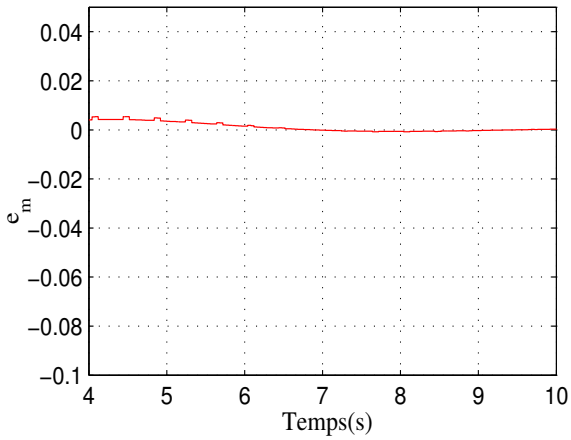


(b) Erreur de synchronisation de l'état x_3

FIG. 4.17: Résultats de simulation sur la synchronisation des états x_3 et $\hat{x}_3$



(a) Messages: m et $\hat{m}$



(b) Zoom sur l'erreur de synchronisation du message m

FIG. 4.18: Résultats de simulation sur la synchronisation des messages m et $\hat{m}$

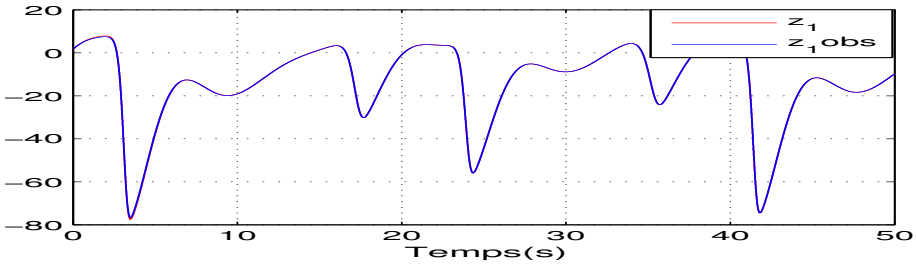


FIG. 4.19: Les états z_1 et $\hat{z}_1$

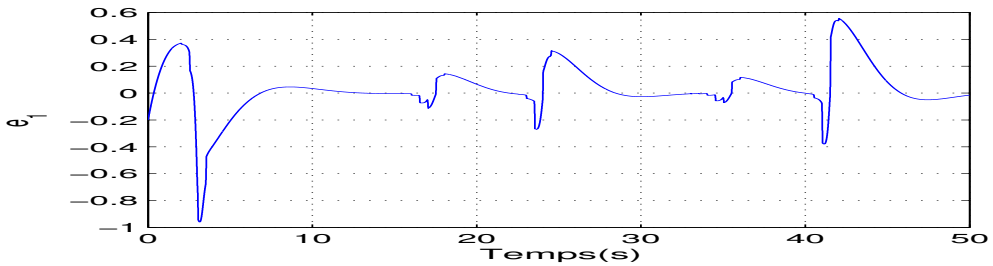


FIG. 4.20: Erreur de synchronisation de l'état z_1

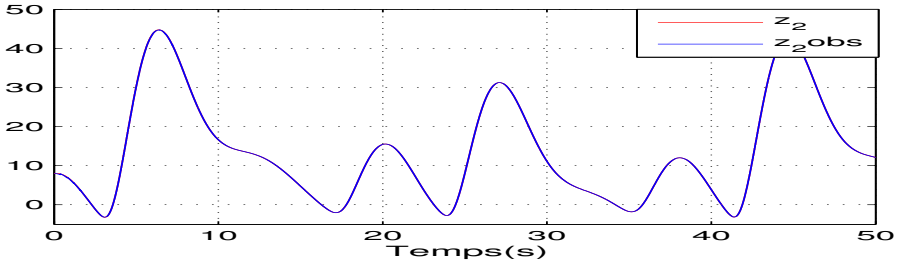


FIG. 4.21: Les états z_2 et $\hat{z}_2$

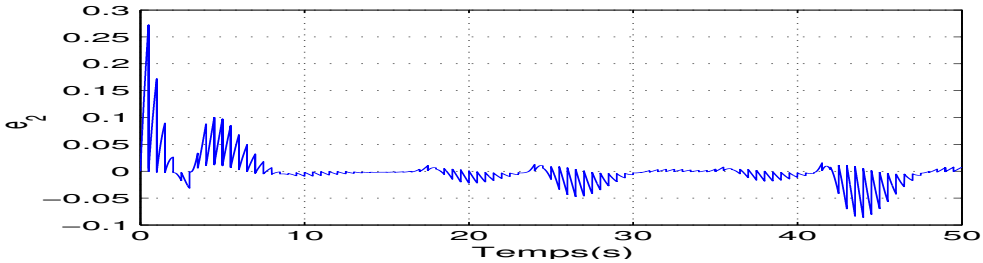


FIG. 4.22: Erreur de synchronisation de l'état z_2

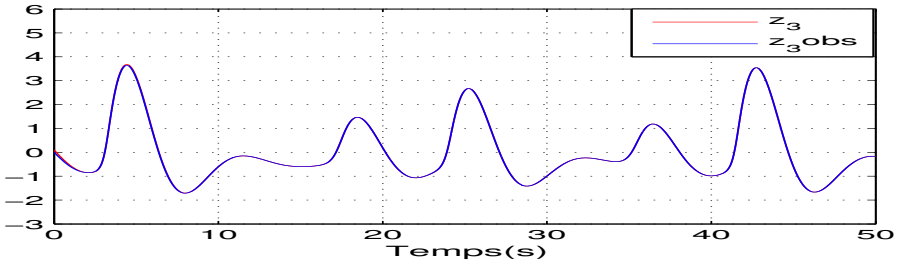


FIG. 4.23: Les états z_3 et $\hat{z}_3$

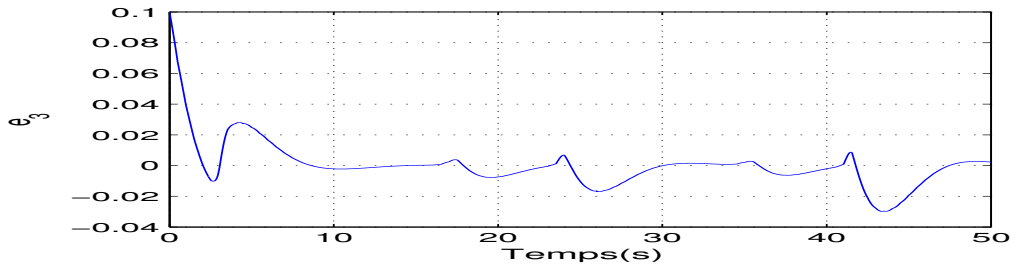
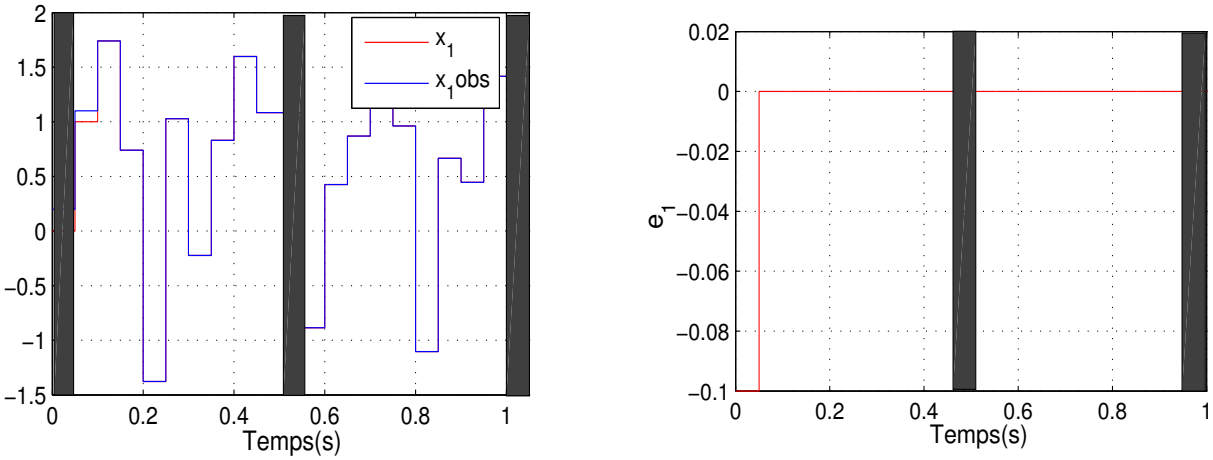


FIG. 4.24: Erreur de synchronisation de l'état z_3



(a) (x_1 et $\hat{x}_1$)

(b) Erreur de synchronisation de l'état x_1

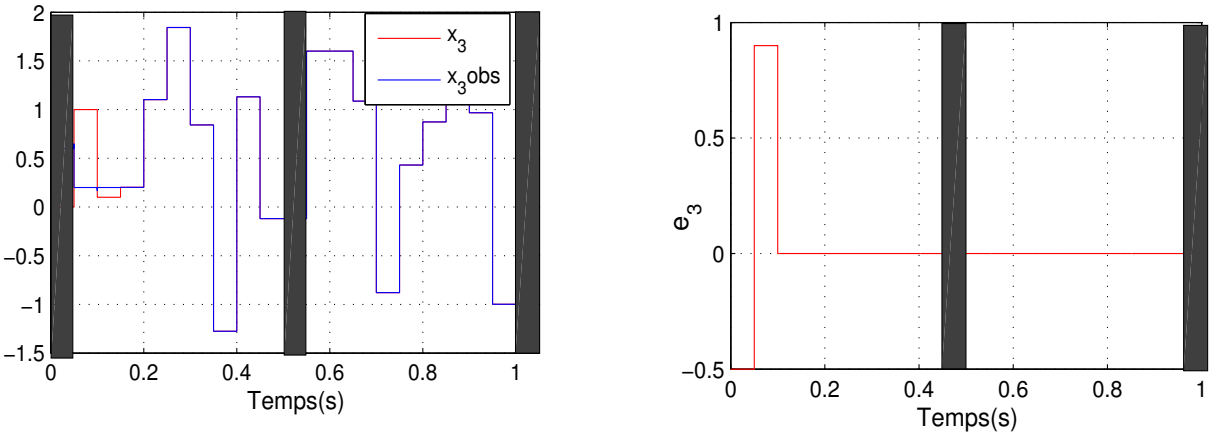
FIG. 4.25: Résultats de simulation sur la synchronisation des états x_1 et $\hat{x}_1$

4.2.2.2 Résultats de synchronisation des deux systèmes dynamiques hybrides avec retards

Les états des deux systèmes hybrides sont représentés respectivement par les figures 4.25a et 4.26a tandis que les erreurs de synchronisation sont montrées par les figures 4.25b and 4.26b. L'erreur e_1 s'annule après un pas $T_1 = 0.05s$ et l'erreur e_3 après deux pas $2T_1 = 0.1s$. D'après les figures précédentes (figures 4.19, 4.21, 4.23 et 4.20, 4.22, 4.24), les deux systèmes en temps continu (2.13) et (3.13) ne sont pas synchronisés. En conséquence, le message m n'est pas reconstitué comme montré par les figures 4.27a et 4.27b.

4.3 Transmission d'une image

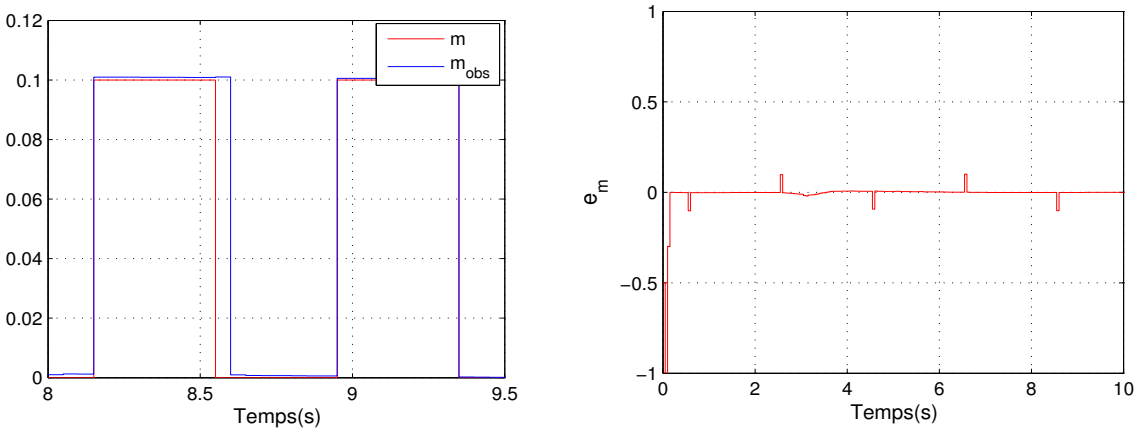
Dans cette section, nous gardons les mêmes paramètres de simulation que ceux donnés à la section précédente. Comme exemple, nous prenons l'image originale de Lena en noir et blanc donnée par la figure 4.28. Elle est définie comme une matrice de 256 lignes et 256



(a) (x_3 et $\hat{x}_3$)

(b) Erreur de synchronisation de l'état x_3

FIG. 4.26: Résultats de simulation sur la synchronisation des états x_3 et $\hat{x}_3$



(a) Messages: m et $\hat{m}$

(b) Zoom sur l'erreur de synchronisation du message m

FIG. 4.27: Résultats de simulation sur la synchronisation des messages m et $\hat{m}$

FIG. 4.28: Image originale

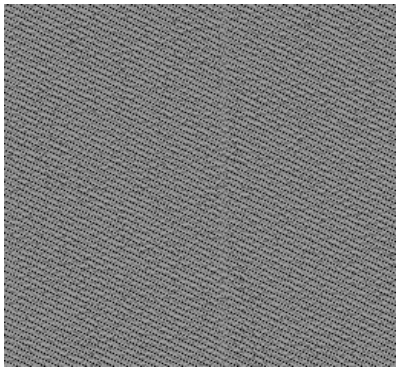
colonnes, qui sera convertie en un vecteur de 65535 pixels. A partir de cette image, nous générons un signal à une dimension. De même que la section précédente, des résultats de simulation obtenus sous Matlab seront donnés uniquement avec retards dans les deux cas : $T_2 = 0.4s$ et $T_2 = 0.5s$.

4.3.1 Cas où $T_2 = 0.4s$

La figure 4.29a montre l'image cryptée correspondant au signal transmis au récepteur, et la figure 4.29b montre l'image décryptée. Nous constatons bien que cette image reconstruite au niveau du récepteur est identique à celle de l'image originale transmise au niveau de l'émetteur. Elle présente seulement quelques pixels incorrects dans les premiers points (en haut) de l'image. Ces résultats sont expliqués par le bon choix de la période T_2 qui satisfait la condition (3.26). Ainsi, ils permettent d'affirmer la performance de la méthode proposée.

4.3.2 Cas où $T_2 = 0.5s$

La figure 4.30a est le résultat du cryptage de l'image originale donnée par la figure 4.28. L'image reconstruite est donnée par la figure 4.30b. D'après cette figure, nous constatons que l'image n'est pas totalement reconstruite au niveau du récepteur. Ceci en raison du mauvais choix de la période T_2 qui ne satisfait pas la condition (3.26). Si on augmente

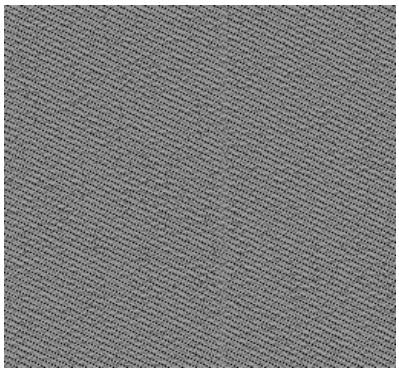


(a) Image cryptée

(b) Image décryptée

FIG. 4.29: Reconstruction de l'image

d'avantage la valeur de la période T_2, c'est à dire on s'éloigne plus de la condition (3.26), l'image reconstruite sera encore plus dégradée.



(a) Image cryptée

(b) Image décryptée

FIG. 4.30: Reconstruction de l'image

4.4 Résultats de la synchronisation : Cas de perte du signal de synchronisation

Dans cette section, nous gardons les mêmes paramètres de simulation que ceux donnés dans le paragraphe 4.2.1. Nous supposons qu'il y a perte du signal de synchronisation entre les instants $t_1 = 15s$ et $t_2 = 25s$ comme montré par la figure 4.31.

Les états et les erreurs de synchronisation des deux systèmes en temps continu sont

représentés respectivement par les figures 4.32, 4.34, 4.36 et 4.33, 4.35, 4.37. Ces figures montrent bien que malgré la perte du signal de synchronisation entre les instants $t_1 = 15s$ et $t_2 = 25s$, les états des deux systèmes en temps continu se resynchronisent une seconde fois à partir de l'instant $t = 35s$.

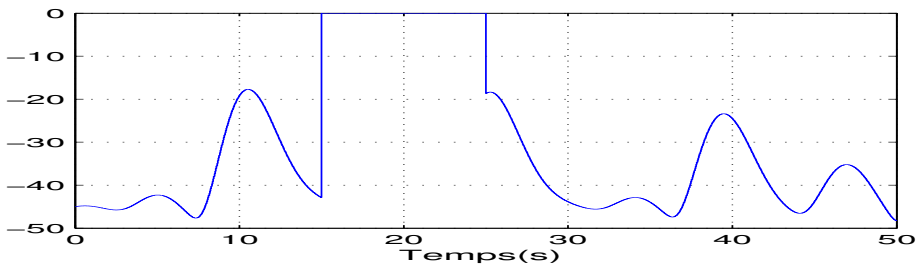


FIG. 4.31: Le signal de synchronisation $y_1 = z_2$

4.5 Robustesses aux bruits de transmission et aux variations des paramètres

La dernière partie de ce chapitre aborde la question de la robustesse du système de communication proposé. Deux tests seront alors présentés. La première concerne la robustesse du système aux bruits de transmission et la seconde concerne la robustesse du système de communication aux variations des paramètres des systèmes chaotiques.

4.5.1 Robustesse aux bruits de transmission

La robustesse aux bruits se pose pour tout système de communication analogique ou numérique : l'émetteur est relié au récepteur par un canal, élément physique qui permet

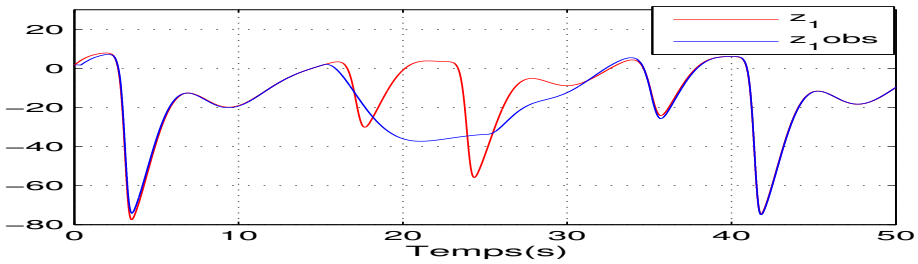


FIG. 4.32: Les états z_1 et $\hat{z}_1$

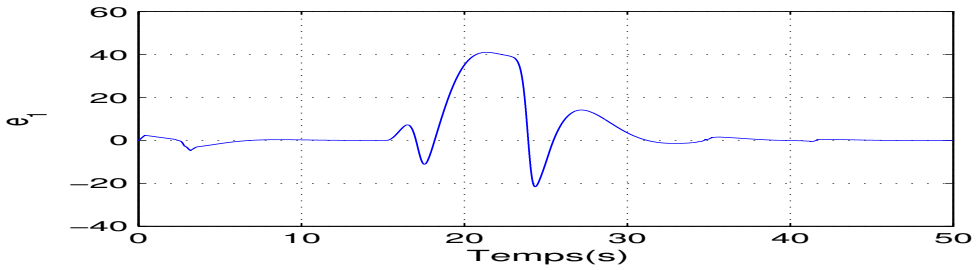


FIG. 4.33: Erreur de synchronisation de l'état z_1

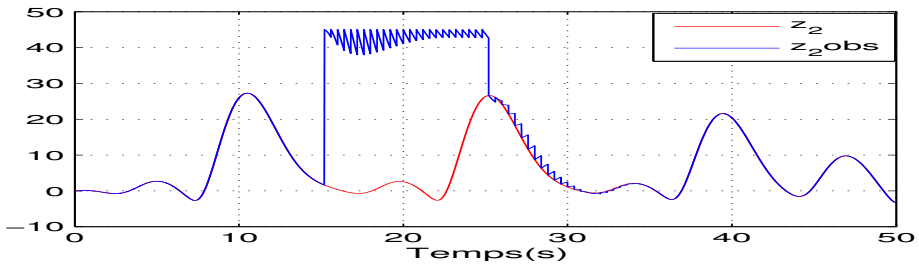


FIG. 4.34: Les états z_2 et $\hat{z}_2$

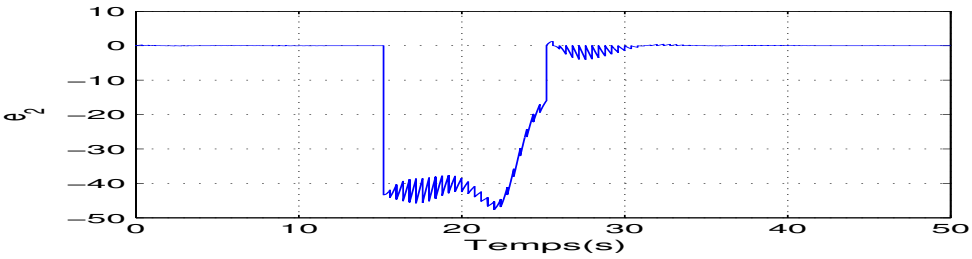


FIG. 4.35: Erreur de synchronisation de l'état z_2

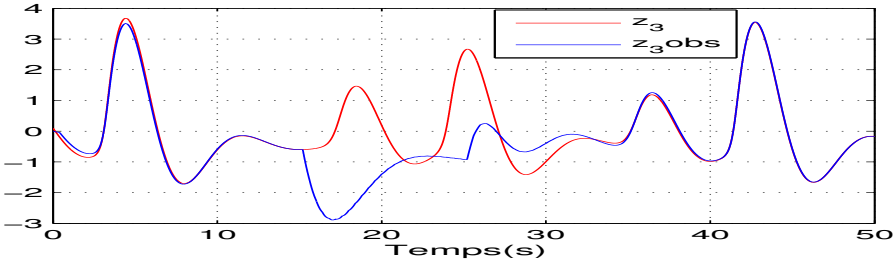


FIG. 4.36: Les états z_3 et $\hat{z}_3$

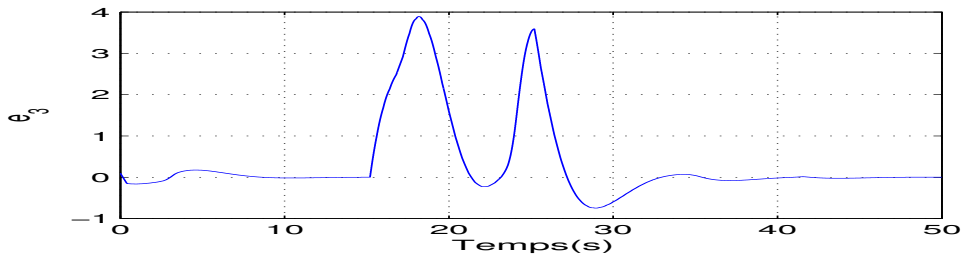


FIG. 4.37: Erreur de synchronisation de l'état z_3

de transmettre les informations. Selon la nature du canal, les signaux sont de nature différente :

- atmosphère : ondes électromagnétiques ou ondes Hertziennes.
- câble coaxial : signaux électriques (tensions, courants).
- fibre optique : ondes électromagnétiques optiques (lumière visible, infrarouge).

Quelque soit le canal utilisé, le bruit perturbe le signal en lui ajoutant une grandeur qui peut rendre le message plus ou moins compréhensible par le récepteur.

Dans ce paragraphe, nous étudions l'impact, sur la qualité de restauration du message (image de Lena), du bruit affectant le signal dévolu à la synchronisation. Cette hypothèse sur la présence de bruit sur le signal transmis y_1 et y_2 permet d'appliquer les résultats théoriques décrits au chapitre précèdent.

Dans ce qui suit, on considère un bruit additif $b(t)$ gaussien, normal centré perturbant les signal transmis. Pour quantifier le rapport entre l'amplitude du signal et celle du bruit qui l'affecte, on rappelle la définition du rapport signal sur bruit (SNR), exprimé en décibels :

$$SNR(y,b) = 20\log_{10}\frac{||y(t)||}{||b(t)||} \tag{4.1}$$

Plus ce rapport est grand, moins le bruit perturbe le signal original. Les figures 4.38a et 4.38b respectivement montrent les images reconstruites pour deux différents SNR ($(SNR = 50dB)$ et $(SNR = 60dB)$) qui correspondent à un niveau de bruit important. La présence du bruit sur le signal transmis, comme nous venons de le voir apporte des erreurs dans l'estimation des états de l'émetteur (système en temps continu (2.11) et système hybride (2.15)). Par conséquence, l'image n'est pas reconstruite. Par contre, la figure 4.38c représente l'image décryptée, lorsqu'on considère la présence de bruit sur le signal transmis. Avec un $SNR = 75dB$ qui correspond à un faible niveau de bruit, la

restauration reste donc correcte.

4.5.2 Sensibilité aux variations de paramètres

Dans ce paragraphe, nous testons la robustesse et la capacité d'adaptation du système de communication proposé face à un pirate possédant des paramètres proches des valeurs réels du système. Dans le système (2.15), nous avons considéré uniquement une variation de $\pm 0.5\%$ sur le retard τ_1. Tous les autres paramètres sont gardés constants. Dans ce paragraphe, nous considérons le cas d'une transmission d'un signal carré identique à celui utilisé précédemment. Notons que $\tau_1 = 0.03s$ et que $T_2 = 0.4s$ satisfait la condition (3.26).

Les résultats obtenus sont montrés par la figure 4.39.

Il est à noter que le message est très affecté par cette variation. Par cette façon, nous avons augmenté la difficulté pour l'identification des paramètres du système (2.15) dans le sens que juste pour une variation de $\pm 0.5\%$ sur le retard considéré, nous avons plus de 200 paramètres possibles pour identifier la clé secrète.

4.6 Conclusion

Dans ce chapitre, nous avons présenté des simulations sous le logiciel Matlab, dans le but de valoriser les résultats théoriques donnés au chapitre précédent. Les résultats de simulation de la transmission sécurisée d'un message ont été subdivisés en deux parties. La première partie a été consacrée à la transmission sécurisée d'un signal numérique, et la seconde à la transmission sécurisée d'une image. Dans la première partie, nous avons présenté les résultats de simulation dans les deux cas possibles à savoir que T_2 satisfait ou non la condition (3.26). En effet, dans le premier cas, nous avons donné les résultats en absence et en présence des retards, par contre, dans le deuxième cas, nous avons juste présenté les résultats de simulation avec retards. Le rôle joué par ces retards n'a pas été expliqué à travers les résultats de simulation, car, il sera détaillé au chapitre suivant.

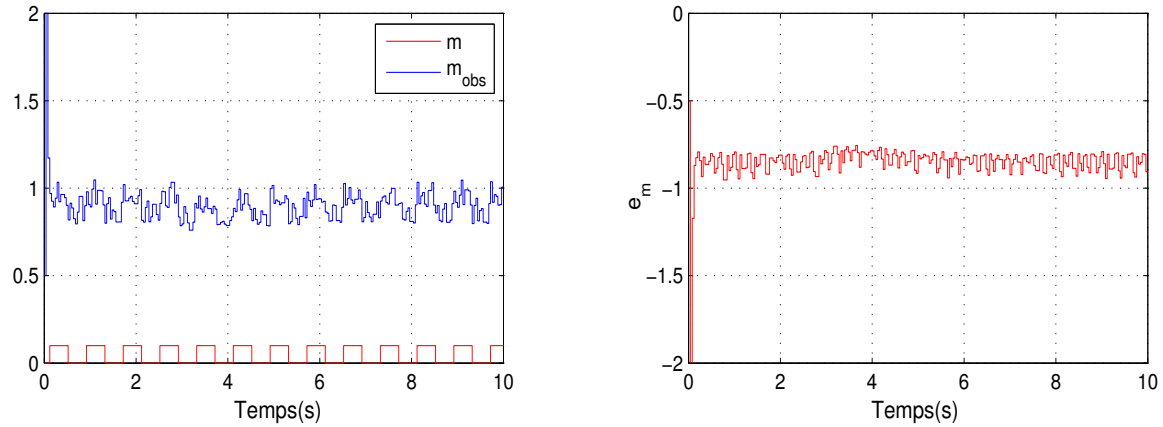
Les résultats de simulation obtenus ont montré que la reconstruction de l'information masquée dépend de la synchronisation des deux systèmes en temps continu. Le message secret a été bien reconstitué dans le cas où $T_2 = 0.4s$ qui satisfait la condition (3.26), car les deux systèmes en temps continu sont synchronisés après un instant $t = 9s$. Par contre dans le cas contraire, c'est à dire $T_2 = 0.5s$, le message secret n'a pas été récupéré car la

(a) $SNR = 50 \ \ dB$

(b) $SNR = 60 \ \ dB$

(c) $SNR = 75 \ \ dB$

FIG. 4.38: Images décryptées en présence de bruits, pour différents SNR



(a) Les messages: m et $\hat{m}$

(b) Erreur sur le message m

FIG. 4.39: Résultats de simulation sur la synchronisation des messages m et $\hat{m}$

synchronisation des deux systèmes en temps continu n'est pas assurée. Il est à noter que le temps de récupération du message correspond bien à ce temps de synchronisation. Ce dernier joue un rôle important pour améliorer la robustesse du système de communications sécurisées. Dans la deuxième partie, les résultats théoriques ont été appliqués sur une transmission sécurisée d'une image. Les résultats obtenus ont montré qu'en respectant le choix de la période T_2, l'image secrète est bien reconstruite et vice-versa. Ensuite, nous avons traité le où il y a perte temporaire du signal de synchronisation. Ici, nous avons montré à travers les résultats de simulation que les deux systèmes en temps continu peuvent se resynchroniser malgré cette défaillance. Ceci reste un grand avantage de la méthode de transmission proposée. Enfin, il est à signaler que dans les deux cas, la restauration de l'information masquée se révèle excellente, sous l'hypothèse de conditions parfaites (ni bruit, ni retard dans la transmission). A la fin de ce chapitre, nous avons envisagé le cas où le cryptosystème proposé est perturbé par la présence de bruit de transmission et par la variation des paramètres de ces systèmes chaotiques. L'observateur détaillé au chapitre 3, choisi comme récepteur, permet d'atténuer l'influence d'un bruit additif sur la synchronisation des états et par conséquent sur la récupération du message confidentiel. Les simulations, pour différents niveaux de bruit, montrent que la restauration du message est meilleure à partir d'un $SNR = 75dB$. Au contraire, lorsque le SNR est faible (par exemple $SNR = 50dB$), la restauration du message n'est pas possible.

Ensuite, nous avons testé la sensibilité du schéma de communication face à la variation de ces clés secrètes. Nous avons montré que le message reconstruit est affecté uniquement

par une légère variation de l'ordre $\pm 0.5\%$ sur le retard τ_1. Dans le prochain chapitre, une étude détaillée sur la robustesse du système de communications sera donnée.

Chapitre 5

Cryptanalyse et identifiabilité

Chapitre 5

Cryptanalyse et identifiabilité

5.1 Introduction

Une étape essentielle de la validation d'un schéma de transmission est la cryptanalyse. La cryptanalyse est l'étude des attaques possibles sur les cryptosystèmes afin de déceler leurs éventuelles faiblesses. Cependant, la cryptanalyse est effectuée sous un certain nombre d'hypothèses. Une hypothèse fondamentale est que l'adversaire connaît complètement l'algorithme de chiffrement, à l'exception de la clé secrète qui est inconnue. Dans ce cas, la sécurité du cryptosystème repose entièrement sur la clé secrète. Ainsi, la question qui se pose alors est : à partir de la connaissance de la structure du système et du signal transitant sur le canal non sécurisé, est-il possible de reconstruire les paramètres du système chaotique, supposés jouer le rôle de clé secrète ?

Pour répondre à cette question, nous considérons dans ce travail une attaque particulière, appelé attaque à texte clair connu (en anglais known plaintext attack). Dans cette attaque, on suppose que l'adversaire connaît une séquence du texte clair et la séquence correspondante du texte chiffré.

La reconstruction des valeurs des paramètres du système chaotique est directement liée au concept d'identifiabilité. Parmi les travaux de recherches effectués dans le domaine de l'identifiabilité, on peut citer les articles de Anstett [6].

Par ailleurs, il existe différentes méthodes dans la littérature pour tester l'identifiabilité paramétrique des systèmes à temps continu ou à temps discret, comme l'approche basée sur la relation entrée-sortie ou celle basé sur l'égalité des sorties. La première approche est dédiée aux systèmes polynomiaux, qui correspond bien à notre cas de figure, elle sera

développée dans ce chapitre.

Ce chapitre est organisé comme suit. Dans la section 5.2, un rappel sur la cryptographie sera présenté. Dans cette section, nous avons jugé utile de donner quelques définitions telles que, la cryptanalyse, la présentation des différentes attaques possibles rencontrées en littérature, l'identifiabilité des systèmes en temps continu et en temps discret, etc. La section 5.3 sera consacrée à l'étude de la cryptanalyse et de l'identifiabilité du schéma de transmission proposé. Enfin, nous clôturons ce chapitre par une conclusion.

5.2 Introduction générale à la cryptographie

La cryptographie est l'étude de techniques mathématiques liées à la sécurité d'information. Par sécurité de l'information, on entend confidentialité des données, intégrité des données, authentification des données et des communicants, et non répudiation des données. La confidentialité consiste à garder des données secrètes pour tous ce qui ne sont pas autorisés à les connaître. L'intégrité des données a pour but de préserver les données de toute altération non autorisée. L'authentification des données consiste à faire le lien entre les données et leur expéditeur. L'authentification des entités consiste à s'assurer de leur identité. La non répudiation consiste à éviter que, par la suite, les communicants nient leurs actions : l'émetteur nie avoir envoyé un message et le récepteur nie avoir reçu un message. La cryptographie consiste notamment en l'élaboration de schémas de chiffrement-déchiffrement ou *cryptosystèmes*. Le chiffrement (en anglais encryption) est l'opération qui consiste à masquer un message appelé "texte" afin d'en cacher le sens à tous ceux qui ne sont pas autorisés à le connaître. Le déchiffrement (en anglais decryption) est l'opération inverse du chiffrement, il a pour but de récupérer l'information masquée. Un cryptosystème est l'ensemble des deux méthodes de chiffrement et de déchiffrement. En cryptographie, l'information à masquer est également appelée message ou *texte clair* (en anglais plaintext). Le résultat du chiffrement d'un texte clair est appelé *texte chiffré* (en anglais ciphertext). Le texte chiffré est le résultat d'une transformation dépendant du message et d'une clé.

Lorsqu'un cryptosystème est synthétisé, il faut s'assurer qu'il est effectivement robuste face à des attaques pirates. Cette étape de validation est appelée la cryptanalyse. Elle consiste à tester les cryptosystèmes afin de déceler leurs éventuelles faiblesses. Dans ce qui

suit, nous allons présenter une introduction à la cryptanalyse ainsi que quelques attaques possibles dans le domaine de piratage.

5.2.1 Cryptanalyse

Considérons un système de communication représenté sur la figure 5.1. Alice et Bob essayent de communiquer de façon sécurisée. Un adversaire, Charlie, tente de faire échouer la communication secrète entre Alice et Bob. Il peut, par exemple, intercepter le signal transitant sur le canal dans le but de récupérer le texte clair, il peut modifier le signal transitant sur le canal, ou encore, il peut se faire passer pour l'une des entités Alice ou Bob. Toutes ces tentatives, et il en existe de nombreuses autres, sont des attaques sur le cryptosystème.

La cryptanalyse est l'étude des probabilités de succès des attaques possibles sur les cryptosystèmes afin de déceler leurs éventuelles faiblesses [42]. 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, la cryptanalyse se met à la place de l'adversaire. La cryptographie

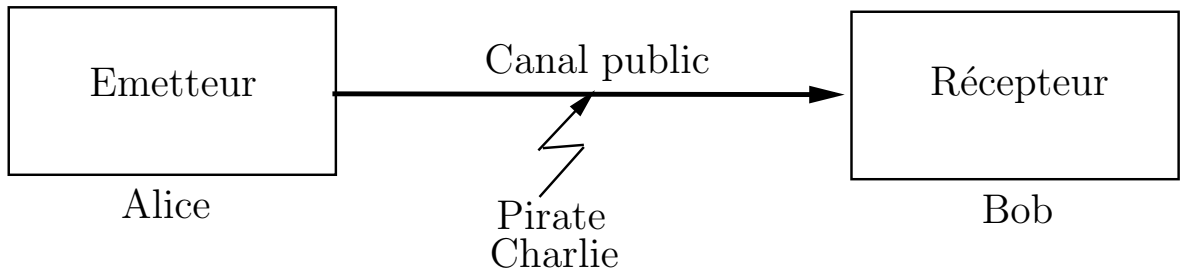


FIG. 5.1: Schéma de communication

et la cryptanalyse [42] sont deux domaines d'études évoluant constamment et en parallèle. En effet, de nouveaux cryptosystèmes, toujours plus complexes, sont développés pour remplacer ceux qui ont été "cassés" par la cryptanalyse et de nouvelles techniques de cryptanalyse sont inventées pour tester ces nouveaux cryptosystèmes. Le problème de la cryptographie est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire pour "casser" un cryptosystème soit supérieure à sa durée de validité. La tendance actuelle est de chercher à prouver la sécurité d'un système sur la base d'hypothèses sur la puissance de calcul requise ou sur la quantité de texte clair ou choisi connue.

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 (déchiffrement de la clé secrète, algorithme de chiffrement découvert sans connaître la clé secrète, informations sur le texte clair, etc).

La complexité de l'attaque se caractérise par le temps en nombre d'opérations effectuées (addition, ou exclusif, etc), par la mémoire nécessaire et par la quantité de données (texte clair et texte chiffré) requises.

A travers les années, de nombreuses attaques possibles contre les cryptosystèmes ont été identifiées, de telle sorte qu'il est difficile d'en établir une liste exhaustive. En revanche, on distingue deux classes d'attaques : les attaques actives et les attaques passives.

Dans les attaques actives, l'adversaire agit sur l'information. Il altère l'intégrité des données, l'authentification et la confidentialité. Il peut chercher à altérer la transmission du message sur le canal, par exemple, en modifiant le message (suppression, ajout, modification des séquences du message), en retardant (ou empêchant) sa transmission, en répétant son envoi, etc.

Dans les attaques passives, l'adversaire observe des informations qui transitent sur le canal sans les modifier. Il cherche à récupérer des informations sur le cryptosystème sans l'altérer, telles que le message, la clé secrète, etc. Dans ce cas, l'adversaire touche à la confidentialité des données.

5.2.1.1 Hypothèse de Kerchoff

La cryptanalyse des schémas de cryptage peut être effectuée sous un certain nombre d'hypothèses. Une hypothèse fondamentale connue sous le non de principe de Kerchoff [84], [11], est que l'adversaire connaît complètement l'algorithme de cryptage, à l'exception de la clé secrète qui est inconnue. Dans ce cas, la sécurité du cryptosystème repose entièrement sur la clé secrète. Cette hypothèse signifie que la sécurité d'un schéma de cryptage ne doit pas reposer sur la confidentialité du schéma, c'est à dire la fonction de chiffrement employée, mais sur la confidentialité de la clé.

Le but de l'adversaire est alors de retrouver le texte clair ou une quelconque information sur le texte clair, ce qui, dans la plupart des cas, nécessite la connaissance de la clé secrète. D'autres hypothèses peuvent alors être formulées. Elles ne concernent que des attaques passives et sont décrites dans [110]. L'objectif commun de ces attaques est de retrouver

systématiquement le texte clair à partir du texte chiffré ou de déduire la clé secrète. Ces attaques sont rappelées ci-dessous, elles sont classées de la plus réaliste à la plus hypothétique.

-*Attaque à texte chiffré uniquement* (en anglais ciphertext only attak) : l'adversaire tente de déduire la clé secrète ou le texte clair en observant seulement le texte chiffré.

-*Attaque à texte clair connu* (en anglais known plaintext attak) : l'adversaire connaît une séquence du texte clair et la séquence correspondante du texte chiffré.

-*Attaque à texte clair choisi* (en anglais chosen plaintext attak) : l'adversaire choisit une séquence du texte clair et analyse la séquence correspondante du texte chiffré.

-*Attaque adaptative à texte clair choisi* (en anglais adaptive chosen plaintext attak) : cette attaque est une attaque à texte clair choisi où le choix du texte clair peut dépendre du texte chiffré reçu précédemment.

-*Attaque à texte chiffré choisi* (en anglais chosen ciphertext attak) : l'adversaire choisit une séquence du texte chiffré et connaît la séquence du texte clair correspondant.

-*Attaque adaptative à texte chiffré choisi* (en anglais adaptive chosen ciphertext attak) : cette attaque est une attaque à texte chiffré choisi où le choix du texte chiffré peut dépendre du texte clair reçu précédemment.

5.2.1.2 Attaque brute

L'attaque la plus élémentaire est appelée attaque brute ou recherche exhaustive. Elle consiste à essayer de façon exhaustive toutes les valeurs possibles de la clé secrète. Pour décider si la clé secrète est correcte, il faut connaître le texte chiffré et une information sur le texte clair (par exemple, savoir si le texte clair est une image, un texte dans une langue donnée, etc). En effet, pour la clé correspondante à celle recherchée, le déchiffrement du texte chiffré produira le texte clair attendu (par exemple, un texte cohérent dans une langue donnée, une image, etc).

Cette attaque est la plus coûteuse en terme de calcul et en mémoire à cause de la recherche exhaustive. Une manière de définir un cryptosystème comme sécurisé est qu'il n'existe aucune autre méthode moins coûteuse (temps de calcul, mémoire, etc) que la recherche exhaustive [139].

La réussite de cette attaque dépend du nombre de possibilités pour la clé recherchée. Plus il y aura de possibilités à tester, plus la probabilité de trouver la clé sera faible et

l'attaque coûteuse.

5.2.1.3 Attaque algébrique

Dans une attaque algébrique, le système de chiffrement est représenté par un système d'équations algébriques multivariables dépendant de l'information, de la clé secrète et du texte de chiffrement. Le principe de cette attaque est de tenir compte de la structure algébrique du système et de résoudre le système d'équations afin de récupérer la clé secrète qui est donnée par la solution de ce système d'équations. Dans la suite, nous nous intéressons au chiffrement par inclusion. On rappelle que dans un schéma de transmission, l'émetteur peut admettre la représentation d'état en temps continu donnée par :

$$\begin{cases} \dot{x}(t) = f_\theta(x(t), m(t)) \\ y(t) = h_\theta(x(t), m(t)) \end{cases} \tag{5.1}$$

ou en temps discret :

$$\begin{cases} x(k+1) = f_\theta(x(k), m(k)) \\ y(k) = h_\theta(x(k), m(k)) \end{cases} \tag{5.2}$$

où $x(t)$ (respectivement $x(k)$) $\in \mathbb{R}^n$ est le vecteur d'état, $y(t)$ (resp. $y(k)$)$\in \mathbb{R}^p$ la sortie, $m(t)$ (resp.$m(k)$)$\in \mathbb{R}$, l'information à masquer, et $\theta = [\theta_1, ..., \theta_l] \in \Theta \subset \mathbb{R}^l$ les paramètres du système chaotique, supposés jouer le rôle de clé secrète, f_θ est une fonction non linéaire et h_θ une fonction éventuellement non linéaire, toutes les deux paramétrées par θ.

Le problème est de tester l'identifiabilité c'est à dire la capacité de déterminer tous les paramètres du vecteur θ donné dans les deux types de systèmes (5.1) et (5.2). Dans cette partie, nous ne considérons que le cas simple où le système (5.1) ou (5.2) est mono-entrée mono-sortie, mais les résultats présentés pourront être étendus à des multi-entrées multi-sorties. Seul le signal de sortie $y(t)$ ou $y(k)$ est transmis au récepteur par l'intermédiaire d'un canal de transmission qui n'est pas sécurisé. Nous nous attacherons au cas où le système (5.1) ou (5.2) présente des non linéarités de type polynomial. Ce type de non linéarité se trouve dans un grand nombre de systèmes chaotiques (récurrence, logistique, Hénon, etc).

Nous allons effectuer la cryptanalyse des deux schémas (correspondant aux deux systèmes (5.1) et (5.2)) à travers des attaques particulières, de type passif, qui s'attachent au problème de récupération des paramètres θ supposés jouer le rôle de la clé secrète. On

se place sous l'hypothèse de Kerchoff. Dans ce cas, la sécurité du cryptosystème repose entièrement sur la clé secrète et non sur la méconnaissance du schéma de chiffrement. On se met alors à la place d'un adversaire qui connaît la structure du système (5.1) ou (5.2) ainsi que le signal $y(t)$ ou $y(k)$ transitant sur le canal. La question qui se pose alors est : à partir de ces connaissances, est t-il possible de retrouver les paramètres ?

Pour répondre à cette question, on considère une attaque brute ou recherche exhaustive. Dans ce contexte, on admet que l'adversaire n'a pas d'autre stratégie que d'essayer exhaustivement toutes les valeurs possibles pour le vecteur de paramètres θ. On considère que l'ensemble des paramètres Θ est un ensemble fini. Dans un contexte de recherche exhaustive, la situation la plus défavorable pour un adversaire, qui est la plus favorable pour la sécurité du système, est qu'il existe une unique valeur de chaque paramètre. En effet dans ce cas, l'adversaire doit essayer toutes les valeurs possibles pour retrouver chaque paramètre et la probabilité de trouver le bon candidat est la plus faible. Le problème de l'unicité de la valeur des paramètres est lié au concept d'identifiabilité.

Il existe de nombreuses définitions de l'identifiabilité dans la littérature. Dans la section suivante, nous effectuons la synthèse de ces définitions, pour le système en temps continu et les systèmes à temps discret.

5.2.2 Définitions de l'identifiabilité

Par "*système identifiable*", on entend unicité de la valeur des paramètres, c'est à dire qu'un comportement entrée-sortie donné, lui correspond une unique valeur des paramètres. Un système sera dit identifiable si tous ces paramètres le sont.

Parmi les différentes définitions de l'identifiabilité existantes dans la littérature, on distingue des définitions analytiques et des définitions algébriques. On distinguera également les définitions de l'identifiabilité locales de celles de l'identifiabilité globale, l'identifiabilité locale est une condition nécessaire pour l'identifiabilité globale. La propriété d'identifiabilité locale est vraie pour $\theta \in v(\theta) \subset \Theta$ où $v(\theta)$ est un voisinage de θ et la propriété d'identifiabilité globale est vraie pour $\theta \subset \Theta$. Quelques définitions sont répertoriées dans [116] et seront rappelées ci-dessous.

5.2.2.1 Définitions analytiques

Dans cette partie, nous allons donner les définitions dans les deux cas : continu et discret.

– **Cas de système à temps continu**

Considérons le système à temps continu donné par (5.1). Les deux définitions suivantes sont des définitions structurelles de l'identifiabilité. Une propriété est dite *structurelle* si elle est vraie pour toutes les valeurs des paramètres sauf pour un ensemble de mesure nulle (ensemble de valeurs atypiques des paramètres). Cet ensemble de mesure nulle conduit à des singularités où aucune conclusion sur l'identifiabilité n'est possible.

Définition 13 *[151] Le système (5.1) est* structurellement localement identifiable *si, pour tout $\theta \in \Theta$, il existe un voisinage $v(\theta)$ de θ, tel que :*

$$\hat{\theta} \in v(\theta), y(m(t), \theta) = y(m(t), \hat{\theta}) \Rightarrow \hat{\theta}_i = \theta_i \quad pour \quad tout \quad i = 1, ..., l. \tag{5.3}$$

Définition 14 *[151] Le système (5.1) est* structurellement globalement identifiable *si, pour presque tout $\theta \in \Theta$:*

$$y(m(t), \theta) = y(m(t), \hat{\theta}) \Rightarrow \hat{\theta}_i = \theta_i \quad pour \quad tout \quad i = 1, ..., l. \tag{5.4}$$

D'autres définitions de l'identifiabilité ont été proposées dans [101]. Ces définitions sont énoncées pour une condition initiale $x(0)$ et un ensemble d'entrées fixés. Cependant, l'ensemble des entrées considérées est restreint par rapport aux définitions précédentes.

– **Cas de système à temps discret**

Considérons le système à temps discret admettant la représentation d'état (5.2)

Définition 15 *[45] Une séquence d'entrée sur un horizon d'itérations $[0, T]$, notée $\{m(k)\}_0^T$, est appelée entrée admissible sur $[0, T]$ si le système (5.2) admet une unique solution locale.*

Définition 16 *[117] Le système (5.2) est localement fortement x_0-identifiable en θ pour la séquence d'entrées admissibles $\{m(k)\}_0^T$, s'il existe un voisinage ouvert de θ,*

$\upsilon(\theta) \subset \Theta$, tel que pour tout $\hat{\theta} \in \upsilon(\theta)$ et pour tout $\theta \in \upsilon(\theta)$:

$$\hat{\theta} \neq \theta \Rightarrow \{y(k)(x_0, m(k), \hat{\theta})\}_0^T \neq \{y(k)(x_0, m(k), \theta)\}_0^T \tag{5.5}$$

La Définition 16 n'est pas structurelle puisqu'elle est valable uniquement pour la valeur particulière θ.

Définition 17 *[117] Le système (5.2) est structurellement identifiable s'il existe $T > 0$, un sous-ensemble ouvert $\chi_0 \subset \chi$ des sous ensembles denses (voir Annexe C) et $M_0^T \subset M$, tels que, quels que soient $x_0 \in \chi_0$, $\theta \in v(\theta)$ et $\{m_k\}_0^T \in M_0^T$, le système (5.2) est localement fortement x_0-identifiable en θ pour la séquence d'entrées admissibles $\{m_k\}_0^T$.*

5.2.2.2 Définitions algébriques

Pour les définitions algébriques, nous supposons que les fonctions f_θ et h_θ des systèmes à temps continu (5.1) et à temps discret (5.2) respectivement, sont polynomiales (en x, en θ et en m). Comme expliqué dans [102], cette restriction n'est pas une contrainte sévère. Par exemple, la restriction $x(t) = \sin(y(t))$ peut aussi s'écrire $(\dot{x}(t))^2 = (\dot{y}(t))^2(1 - x(t))^2$.

Il est à noter que dans les définitions algébriques, les conditions initiales ne sont pas prises en compte.

– **Cas de système à temps continu**

Définition 18 *[45] Le système (5.1) est globalement identifiable si et seulement s'il peut être réécrit sous forme de régression linéaire telle que, pour $i = 1, ..., l$:*

$$P_i(y(t), \dot{y}(t), ..., m(t), \dot{m}(t), ...,)\theta_i - Q_i(y(t), \dot{y}(t), ..., m(t), \dot{m}(t), ...,) = 0 \tag{5.6}$$

où P_i et Q_i sont des polynômes dépendants uniquement de $y(t)$, de $m(t)$ et de leurs dérivées.

– **Cas de système à temps discret**

Définition 19 *[117] Le système (5.2) est globalement identifiable si et seulement s'il peut être réécrit sous forme de régression linéaire telle que, pour $i = 1, ..., l$:*

$$\begin{aligned} &P_i(y(k), ..., y(k+N), m(k), ..., m(k+N))\theta_i \\ &-Q_i(y(k), ..., y(k+N), m(k), ..., m(k+N)) = 0 \end{aligned} \tag{5.7}$$

où P_i et Q_i sont des polynômes dépendants uniquement de $y(k)$, de $m(k)$ et de leurs itérés et $N = s + l - 1$ (s est l'indice d'observabilité qui sera définie ci-dessous).

Dans ce qui suit, nous allons présenter deux approches qui permettent de tester l'identifiabilité des paramètres uniquement des systèmes à temps discret qui fera l'objet de notre étude dans la section suivante. La première basée sur la relation entrée-sortie et dédiée aux systèmes polynomiaux (en y, en x et en θ), permet de tester l'identifiabilité au sens de la définition algébrique. Cette approche est constructive dans le sens où elle permet non seulement de conclure quant à l'identifiabilité des paramètres mais aussi de reconstruire les paramètres dans un contexte d'attaque à texte connu. La seconde, basée sur l'égalité des sorties permet de tester l'identifiabilité au sens de la définition analytique. Elle sera présentée en Annexe C.

5.2.3 Approche basée sur la relation entrée-sortie

Cette approche permet de tester l'identifiabilité au sens de la définition algébrique (19). On considère que les fonctions f_θ et h_θ sont polynomiales.

5.2.3.1 Principe de l'approche

Si la définition 19 est vérifiée, chaque paramètre θ_i peut se réécrire sous la forme suivante :

$$\theta_i = \frac{Q_i(y(k),...,y(k+N),m(k),...,m(k+N))}{P_i(y(k),...,y(k+N),m(k),...,m(k+N))} \tag{5.8}$$

avec $P_i \neq 0$. Cette condition est appelée *condition d'excitation persistante*. L'ensemble des valeurs de $y(k)$ et de $m(k)$ correspondant à $P_i = 0$ est l'ensemble des mesures nulles, en général.

Pour obtenir la relation (5.7), nous devons éliminer les états internes $x(k)$ et leurs itérés dans le système (5.2), considérés comme indéterminés. Cela conduit à une relation dépendant uniquement du vecteur de paramètres θ, de la sortie $y(k)$, de l'entrée $m(k)$ et de leurs itérés. Cette relation est appelée *relation entrée-sortie* et est de la forme :

$$\Gamma_1(\theta, y_k, ..., y_{k+s}, m_k, ..., m_{k+s}) = 0 \tag{5.9}$$

où s est l'indice d'observabilité du système (5.2), défini comme suit :

Soit f_θ^i la ième composition de la fonction f_θ, $f_\theta^i(x_k) \triangleq f_\theta(f_\theta^{i-1}(x_k))\ \forall i \geq 1$ et $f_\theta^0(x_k) \triangleq x_k$. L'indice d'observabilité s est un entier positif tel que $\forall x_k \in v(x_k)$ où $v(x_k)$ est un voisinage de x_k, nous avons :

$$rang(\frac{\partial(h_\theta(x_k),(h_\theta \circ f_\theta)(x_k),...,(h_\theta \circ f_\theta^{s-1})(x_k))}{\partial x_k}) = s \tag{5.10}$$

et

$$rang(\frac{\partial(h_\theta(x_k),(h_\theta \circ f_\theta)(x_k),...,(h_\theta \circ f_\theta^{s-1}),(h_\theta \circ f_\theta^{s})(x_k)}{\partial x_k}) = s \tag{5.11}$$

Nous considérons trois approches d'élimination de variables dédiées aux systèmes polynomiaux, c'est à dire l'obtention de la relation entrée-sortie : L'approche basée sur les bases de Gröbner, l'approche basée sur l'ensemble caractéristique et celle basée sur le résultant de deux polynômes. Dans ce qui suit, nous allons étudier uniquement l'approche basée sur les bases de Gröbner. Elle sera présentée ci-dessous. Les deux autres approches seront présentées en Annexe C.

Définition 20 *[5] Un ordre lexicographique des variables $x_1(k), ..., x_n(k)$, noté $<$, est un ordre total portant sur le nom des variables et de leurs itérés, tel que, $\forall i = 1, ..., n$, $\forall j = 1, ..., n$:*

$$\begin{aligned} &-x_i(k) < x_i(k+l), \forall \ \ l \in \mathbb{N} \\ &-x_i(k) < x_j(l) \Rightarrow x_i(k+t) < x_j(l+t), \forall \ \ l \in \mathbb{N}, \forall \ \ t \in \mathbb{N} \\ &-x_i(k) < x_j(k) \Rightarrow x_i^\alpha(k) < x_j^\beta(k), \forall \ \ \alpha \in \mathbb{N}, \forall \ \ \beta \in \mathbb{N} \end{aligned} \tag{5.12}$$

5.2.3.2 Bases de Gröbner

Le principe de l'approche est le suivant. Pour un ordre lexicographique fixé, il suffit alors de chercher une base dont une expression ne contient plus les variables à éliminer $x(k)$, mais contient seulement $y(k)$, $m(k)$, leurs itérés et le vecteur de paramètre θ. Cette expression de la base est de la forme recherchée (5.9). Une telle base est appelée base de Gröbner (voir Annexe C pour une définition plus formelle).

L'exemple suivant illustre le principe de l'étude de l'identifiabilité d'un système en

utilisant les bases de Gröbner.

Exemple 8 *Considérons le cryptosystème chaotique où l'information $m(k)$ est injectée dans la récurrence de Hénon :*

$$\begin{cases} x_1(k+1) = \theta_1 x_1^2(k) + \theta_2 x_2(k) + m(k) \\ x_2(k+1) = \theta_3 x_1(k) + \theta_4 m(k) \\ y(k) = x_1(k) \end{cases} \tag{5.13}$$

Le système (5.13) est de la forme (5.2) avec :

$$f_\theta(x(k), m(k)) = \begin{cases} \theta_1 x_1^2(k) + \theta_2 x_2(k) + m(k) \\ \theta_3 x_1(k) + \theta_4 m(k) \end{cases}, \quad h_\theta(x(k), m(k)) = x_1(k) \tag{5.14}$$

Dans cet exemple, l'identifiabilité du vecteur de paramètres $[\theta_1 \ \ \theta_2 \ \ \theta_3 \ \ \theta_4]^T$ ($l = 4$) est testée avec l'approche basée sur la relation entrée-sortie. L'élimination du vecteur d'état est effectuée avec l'approche basée sur les bases de Gröbner.

Comme $x_2(k)$ n'est pas directement transmis, il est choisi comme étant le plus grand et l'ordre lexicographique correspondant est :

$$x_1(k) < x_2(k) \tag{5.15}$$

L'indice d'observabilité du système (5.13) est égal à la dimension du système $n = 2$. En effet, on a :

$$rang \begin{bmatrix} \frac{\partial h_\theta(x(k))}{\partial x_1(k)} & \frac{\partial h_\theta(x(k))}{\partial x_2(k)} \\ \frac{\partial (h_\theta \circ f_\theta)(x(k))}{\partial x_1(k)} & \frac{\partial (h_\theta \circ f_\theta)(x(k))}{\partial x_2(k)} \end{bmatrix} = rang \begin{bmatrix} 1 & 0 \\ 2\theta_1 x_1(k) & \theta_2 \end{bmatrix} = 2,$$

$$rang \begin{bmatrix} \frac{\partial h_\theta(x(k))}{\partial x_1(k)} & \frac{\partial h_\theta(x(k))}{\partial x_2(k)} \\ \frac{\partial (h_\theta \circ f_\theta)(x(k))}{\partial x_1(k)} & \frac{\partial (h_\theta \circ f_\theta)(x(k))}{\partial x_2(k)} \\ \frac{\partial (h_\theta \circ f_\theta^2)(x(k))}{\partial x_1(k)} & \frac{\partial (h_\theta \circ f_\theta^2)(x(k))}{\partial x_2(k)} \end{bmatrix} =$$

$$rang \begin{bmatrix} 1 & 0 \\ 2\theta_1 x_1(k) & \theta_2 \\ 4(\theta_1^2 x_1(k)(\theta_1(x_1^2(k) + m(k) + \theta_2 x_2(k) + \theta_2\theta_3 & 2\theta_1\theta_2(\theta_2 x_2(k) + m(k) + \theta_1 x_1^2(k)) \end{bmatrix} = 2$$

Pour obtenir la relation entrée-sortie donnée par (5.9) ($\Gamma_1 = 0$), le système (5.13) est itéré une fois :

$$\begin{cases} x_1(k+1) - \theta_1 x_1^2(k) - \theta_2 x_2(k) - m(k) = 0 \\ x_1(k+2) - \theta_1 x_1^2(k+1) - \theta_2 x_2(k+1) - m(k+1) = 0 \\ x_2(k+1) - \theta_3 x_1(k) - \theta_4 m(k) = 0 \\ x_2(k+2) - \theta_3 x_1(k+1) - \theta_4 m(k+1) = 0 \\ y(k) - x_1(k) = 0 \\ y(k+1) - x_1(k+1) = 0 \\ y(k+2) - x_1(k+2) = 0 \end{cases} \tag{5.16}$$

Le logiciel de calcul symbolique Maxima, disponible en ligne à http : //maxima.sourceforge.net, permet de calculer, avec la fonction ploy − buchberger, la base de Gröbner de l'idéal associé du système (5.13), avec l'ordre lexicographique (5.15). Une des expressions de la base de Gröbner est la relation entrée-sortie recherchée (5.9) :

$$\theta_1 y^2(k+1) + \theta_2\theta_3 y(k) - y(k+2) + m(k+1) + \theta_2\theta_4 m(k) = 0 \tag{5.17}$$

Les autres expressions de la base ne présentent pas d'intérêt pour notre étude car elles contiennent le vecteur d'état interne. La relation entrée-sortie (5.17) est itérée $l - 1 = 3$ fois, ce qui conduit à $\Gamma_2 = 0$, $\Gamma_3 = 0$ et $\Gamma_4 = 0$, respectivement :

$$\begin{cases} \theta_1 y^2(k+2) + \theta_2\theta_3 y(k+1) - y(k+3) + m(k+2) + \theta_2\theta_4 m(k+1) = 0 \\ \theta_1 y^2(k+3) + \theta_2\theta_3 y(k+2) - y(k+4) + m(k+3) + \theta_2\theta_4 m(k+2) = 0 \\ \theta_1 y^2(k+4) + \theta_2\theta_3 y(k+3) - y(k+5) + m(k+4) + \theta_2\theta_4 m(k+3) = 0 \end{cases} \tag{5.18}$$

L'ensemble d'équations (5.17) et (5.18) ne peut pas être réécrit sous la forme (5.7), excepté pour le paramètre θ_1 :

$$\begin{aligned} &P_1(y(k), ..., y(k+5), m(k), ..., m(k+5))\theta_1 \\ &-Q_1(y(k), ..., y(k+5), m(k), ..., m(k+5)) = 0 \end{aligned} \tag{5.19}$$

avec :

$$
\begin{aligned}
&P_1(y(k),...,y(k+5),m(k),...,m(k+5)) = \\
&-m(k)y(k+1)y^2(k+3)+m(k+1)y(k)y^2(k+3)+m(k)y^3(k+2)-m(k) \\
&+2y(k)y^2(k+2)-m(k+1)y^2(k+1)y(k+2)+m(k+2)y^3(k+1) \\
&Q_1(y(k),...,y(k+5),m(k),...,m(k+5)) = \\
&-(y(k+1)(m(k)(y(k+4)-m(k+3))+m(k+1)m(k+2))+(y(k)(m(k+1)(m(k+3) \\
&-y(k+4))+m(k+2)y(k+3)-m^2(k+2)) \\
&(y(k+2)(m(k)(m(k+2)-y(k+3))-m(k+2)y(k+1))-m^2(k+1))+m(k+1)y^2(k+2))
\end{aligned}
\tag{5.20}
$$

Les relations (5.8) sont uniquement satisfaites pour θ_1 et seul θ_1 est identifiable. Dans le contexte d'une attaque brute, il pourrait jouer le rôle d'une de clé secrète, contrairement aux autres paramètres θ_2, θ_3 et θ_4 pour lesquels plusieurs paires (θ_2, θ_3) ou (θ_2, θ_4) vérifient les relations (5.17) et (5.18) .

En revanche, selon (5.7) et ici (5.19), il est clair qu'en effectuant une attaque à texte clair connu, le paramètre θ_1 peut facilement être reconstruit avec P_1 et Q_1 (5.20). Par conséquent θ_1 ne peut finalement pas jouer le rôle de clé secrète.

5.3 Cryptanalyse et identifiabilité

Afin d'étudier la robustesse du système de transmission proposé, une étude de la cryptanalyse et de l'identifiabilité sera donnée. Dans cette section, nous considérons les cryptosystèmes chaotiques à temps discret, de la forme (5.2) et présentant des non linéarités polynomiales. On suppose que l'adversaire connaît la structure du système ainsi que le signal de sortie y_k qui transite sur le canal, d'après l'hypothèse de Kerchoff. Dans ce qui suit, deux cas seront traités. Le premier cas consiste à tester l'identifiabilité du système dynamique hybride sans retard (2.15) et le second au système dynamique hybride avec retard (2.16). Dans notre étude, nous allons uniquement considérer l'attaque à texte clair connu.

5.3.1 Etude sans retards

Ce système est composé des états continus échantillonnés (z_1 et z_3) et d'une partie discrète. Dans ce qui suit, nous étudions l'identifiabilité du système global (2.15).

Le système (2.13) peut être réécrit comme suit :

$$\begin{cases} \dot{z_1} = \frac{g}{Q(1-k)}[-exp(-z_2) + 1 + z_3] \\ \dot{z_2} = \frac{g}{Qk} z_3 \\ \dot{z_3} = -\frac{Qk(1-k)}{g}[(z_1 + z_2) - \frac{1}{q} z_3] \\ y_1 = z_2 \end{cases} \tag{5.21}$$

où g, Q et k les paramètres du système.

En appliquant le schéma de discrétisation d'Euler pour le système (5.21), nous obtenons le système suivant :

$$\begin{cases} z_1(n+1) = z_1(n) + T\frac{g}{Q(1-k)}[-exp(-z_2(n)) + 1 + z_3(n)] \\ z_2(n+1) = z_2(n) + T\frac{g}{Qk} z_3(n) \\ z_3(n+1) = z_3(n) + T(\frac{-Qk(1-k)}{g})[z_1(n) + z_2(n)) - \frac{1}{q} z_3(n)] \\ y_1(n) = z_2(n) \end{cases} \tag{5.22}$$

où T est le pas d'échantillonnage.

Le système (5.22) peut être réécrit sous la forme donnée dans [6].

$$\begin{cases} z(n+1) = f_1(\theta_1, z(n)) \\ y_1(n) = h_1(z) = z_2(n) \end{cases} \tag{5.23}$$

où $z(n) = (z_1(n) \quad z_2(n) \quad z_3(n))^T$ les états du système (5.23) et $\theta_1 = (g \quad Q \quad k)^T$ ses paramètres à identifier.

Ici, dans cette étude, nous supposons que tous les paramètres de θ_1 sont identifiables, ce qui est favorable à un piratage.

Le système (2.15) peut être réécrit comme suit : [6] :

$$\begin{cases} x(k+1) = f_2(\theta_2, x(k), z_1(nT_2), z_3(nT_2), m(k)) \\ y_2(k) = h_2(\theta_2, x(k), z_1(nT_2), z_3(nT_2), m(k)) = x_2(k) \end{cases} \tag{5.24}$$

avec :

$$f_2(\theta_2, x(k), z_1(nT_2), z_3(nT_2), m(k)) = \begin{cases} a - x_2^2(k) - bx_3(k) \\ x_1(k) \\ x_2(k) + A_1 z_1(nT_1) + A_2 z_3(nT_1) + cm(k) \end{cases} \tag{5.25}$$

où $x(k) \in \mathbb{R}^3$, les états du système (2.14), $z_1(nT_2)$ et $z_3(nT_2)$ les deux états continus ajoutés au système (2.14) après échantillonnage, $y_2(k) \in \mathbb{R}$ la sortie et $m(k) \in \mathbb{R}$ le message à masquer. $\theta_2 = [a, b, c, A_1, A_2]^T \in \Theta \subset \mathbb{R}^5$ est le vecteur de paramètres (clés secrètes) du système dynamique hybride (2.15). Les fonctions f_2 et h_2 sont non linéaires. La période $9T_1$ correspond à la durée d'envoi du signal $y_2(k)$ comme montrée par la figure 2.13.

Le test de l'identifiabilité (au sens de la définition algébrique) du système (2.15) par l'approche entrée-sortie étant difficile. L'identifiabilité sera étudiée comme suit :

Considérons la première sortie du système (5.23) à l'instant nT_2 ce qui correspond à l'envoi du signal y_1 et les sorties du système (5.2) à des instants différents $k, ..., k+8$ qui correspondent à l'envoi des signaux y_2 (voir figure 5).

$$\begin{cases} y_1(nT_2) & = & z_2(nT_2) \\ y_2(k) & = & h_2(\theta_2, x(k), z_1(nT_2), z_3(nT_2), m(k)) \\ y_2(k+1) & = & h_2 \circ f_2(\theta_2, x(k), z_1(nT_2), z_3(nT_2), m(k)) \\ \vdots & \vdots & \vdots \\ y_2(k+8) & = & h_2\circ, \cdots, \circ f_2(\theta_2, x(k), z_1(nT_2), z_3(nT_2), m(k))\} \end{cases} \tag{5.26}$$

Dans le système (5.26), nous considérons le cas d'une attaque en texte clair connu c'est à dire, le message $m(k)$ et les sorties y_1 et y_2 sont connus.

Ici, nous considérons deux cas :

- Cas où les deux systèmes en temps continu ne sont pas synchronisés.

  Dans ce cas, les états z_1 et z_3 ne sont pas encore connus. Alors, nous avons 10 inconnus ($x_1(k)$, $x_2(k)$, $x_3(k)$, a, b, A_1, A_2, c, $z_1(nT_2)$, $z_3(nT_2)$) dans le système (5.26) avec 9 équations. Ainsi, pour retrouver tous ces inconnus, y compris les clés secrètes θ_2, il est nécessaire d'avoir au moins les équations de y_1 et y_2 sur 2 cycles T_2. Alors, nous avons 20 équations à 10 inconnues dont tous les paramètres de θ_2 sont identifiables. Par conséquent, le système de transmission de données n'est pas robuste contre les attaques à textes clairs connus
- Cas où les deux systèmes en temps continu sont synchronisés.

  Dans ce cas, les états $z_1(nT_2)$ et $z_3(nT_2)$ sont connus. Alors, nous avons 8 inconnus avec 9 équations, les paramètres de θ_2 sont identifiables. En conséquence, même

dans ce cas, le schéma de transmission n'est pas robuste contre les attaques à textes clairs connus.

5.3.2 Etude avec retards

La question est de savoir comment obtenir une relation entrée-sortie où tous les paramètres de θ_2 ne sont pas identifiables, au moins avec les méthodes habituelles et à l'égard de définitions classiques. Dans le but d'avoir plus d'inconnus que de nombre d'équations indépendantes dans le système (5.26), il est proposé ici d'introduire des retards (qui sont aussi des clés secrètes) avant d'échantillonner les états continus z_1 et z_3. L'ajout de ces retards augmente le nombre de paramètres inconnus du système (5.26) et par conséquent résout notre problème.

Soient τ_1, τ_2 respectivement les retards appliqués à z_1 et z_3 et posons $\tau_1 z_1(nT_2) = z_1(nT_2 - \tau_1)$ et $\tau_2 z_3(nT_2) = z_3(nT_2 - \tau_2)$.

En introduisant des retards, le système (5.26) devient :

$$\begin{cases} y_1(nT_2) & = & z_2(nT2) \\ y_2(k) & = & h_2(\theta_2, x(k), z_1(nT_2 - \tau_1), z_3(nT_2 - \tau_2), m(k)) \\ y_2(k+1) & = & h_2 \circ f(\theta, x(k), z_1(nT_2 - \tau_1), z_3(nT_2 - \tau_2), m(k)) \\ \vdots & \vdots & \vdots \\ y_2(k+8) & = & h_2\circ, \cdots, \circ f_2(\theta, x(k), z_1(nT_2 - \tau_1), z_3(nT_2 - \tau_2), m(k)) \end{cases} \tag{5.27}$$

Pour rendre le système (5.26) non identifiable, des retards variables notés τ_{1i} ($i = 1, ..., 9$) sont introduits sur l'état $z_1(nT_2)$ pour chaque période T_1. Le choix de l'état z_1 s'explique par sa variation rapide durant la période T_2 par rapport à l'état z_3. Par conséquent, la difficulté pour les pirates de connaître z_1 est augmentée. Ce système est donné par (2.16), qui est robuste par rapport aux attaques à textes clairs connus. Il est à noter que ces retards ne sont pas des multiples de T_1 car, si c'est le cas (multiples de T_1), ils seront traités comme des itérations et, par conséquent, ils ne jouent pas le rôle de clés secrètes dans le système (2.16).

Le système (2.16) peut être réécrit comme suit :

$$\begin{cases} y_1(nT_2) &= z_2(nT_2) \\ y_2(k) &= h_2(\theta_2, x(k), z_1(nT_2 - \tau_{11}), z_3(nT_2), m(k)) \\ y_2(k+1) &= h_2 \circ f_2(\theta_2, x(k), z_1(nT_2 - \tau_{12}), z_3(nT_2), m(k)) \\ \vdots & \vdots \\ y_2(k+8) &= h_2\circ, \cdots, \circ f_2(\theta_2, x(k), z_1(nT_2 - \tau_{19}), z_3(nT_2), m(k)) \end{cases} \tag{5.28}$$

Supposons que les deux systèmes en temps continu sont synchronisés. Nous allons tester la possibilité d'identifier les retards τ_{1i} dans le système (5.28).

Dans la première période $n = 1$, nous avons 17 (8+9) inconnus avec 9 équations. Dans la seconde période T_2, nous avons 26 (17+9) inconnus avec 18 (9+9) équations, etc. Ici, nous constatons que le nombre d'équations et le nombre d'inconnus augmentent du même nombre et que le nombre d'inconnus est toujours supérieur au nombre d'équations. Ceci rend le système (2.16) non identifiable. Par conséquent, ce système de transmission de données est robuste contre les attaques à textes clairs connus.

5.4 Conclusion

Dans la première partie de ce chapitre, nous avons présenté quelques notions sur la cryptographie. Ici, nous avons jugé utile de donner quelques définitions de l'identifiabilité algébrique et analytique et que soit dans le cas continu ou dans le cas discret. Dans la seconde partie de ce chapitre, nous avons étudié la robustesse de la méthode de transmission proposée contre les attaques à textes clairs connus. Ici, nous avons considéré les deux cas de figure : cas de transmission sans retards et cas de transmission avec retards. Nous avons montré que dans le premier cas, le système chaotique hybride présenté au niveau de l'émetteur peut être cassé. Par conséquent, le système de transmission n'est pas robuste contre des attaques à textes clairs connus car le nombre d'équations est supérieur au nombre d'inconnus. Par contre dans le second cas, l'ajout des retards permet d'avoir constamment un nombre d'équations toujours inférieur au nombre d'inconnus. Alors, la récupération des clés secrètes est impossible à réaliser. Par conséquent, le système de transmission est robuste contre des attaques à textes clairs connus.

Conclusion générale

Les objectifs de ce travail étaient d'appliquer la méthode d'inversion à gauche sur un système dynamique hybride. Comme application à ce travail, nous avons traité la transmission sécurisée de données en exploitant les propriétés des systèmes chaotiques. Deux approches ont été alors proposées.

La première, qui est décrite dans le chapitre 1, traite le problème de synchronisation de deux systèmes chaotiques identiques de Qi. Deux méthodes de synchronisation ont été ainsi utilisées. La première est la commande passive, elle est basée sur la théorie de stabilité de Lyapunov. L'autre est basée sur les techniques de commandes impulsives. Pour assurer la synchronisation entre les deux systèmes, nous avons donné des conditions suffisantes pour chaque méthode. Les résultats de simulation montrent bien que, malgré l'extrême sensibilité aux conditions initiales des systèmes chaotiques, les deux systèmes se synchronisent.

Dans la deuxième approche, nous avons élaboré un nouveau système hybride de transmission pour les communications privées (chapitre 2). Ensuite, nous avons souligné l'intérêt d'utiliser ce type de système dans les transmissions sécurisées. Ce système est constitué de deux parties, l'émetteur et le récepteur. L'émetteur est composé d'un système chaotique en temps continu (Colpitts) et d'un système chaotique en temps discret (Hénon modifié). Dans le but de rendre la structure du système en temps discret plus complexe et par conséquent complexifier la structure de l'émetteur, nous avons introduit après échantillonnage quelques états du système en temps continu dans les dynamiques du système en temps discret. Afin de renforcer la robustesse du système de transmission contre les attaques à textes clairs connus, une solution a été proposée. Elle consiste à ajouter des retards dans les états échantillonnés introduits au système chaotique discret. Ces retards constituent des clés supplémentaires qui renforcent la sécurité du système. Le récepteur présenté en détail dans le chapitre 3 est constitué de deux types d'observateurs, le pre-

mier est de type impulsif, permet de récupérer tous les états du système en temps continu. Quant au second, il a pour rôle de récupérer tous les états ainsi que le message camouflé du système en temps discret. Les choix de ces deux types d'observateurs ont été justifiés dans ce chapitre.

Nous avons testé notre nouveau schéma de transmission sécurisé pour envoyer des messages confidentiels qui sont dans notre application un signal carré et une image. Les résultats de simulation obtenus montrent que la récupération du message confidentiel passe d'abord par la synchronisation des deux systèmes en temps continu et que cette synchronisation est possible que si la période T_2 satisfait la condition expliquée au chapitre 4. Parmi les avantages de cette méthode proposée est que même en cas de perte de paquets d'informations due à une désynchronisation, les deux systèmes en temps continu peuvent se resynchroniser.

La robustesse de notre nouveau schéma de transmission a été également abordée d'une manière détaillée. Ainsi, dans un premier temps, nous avons rappelé quelques notions théoriques essentielles sur la cryptographie. Ensuite, nous sommes passés à l'étude de la robustesse de la nouvelle méthode de transmission proposée contre les attaques à textes clairs connus. Ici, nous avons pris en considération les deux cas : cas de transmission sans retards et cas de transmission avec retards. Dans cette étude, nous avons montré que dans le premier cas, les paramètres de l'émetteur peuvent être facilement identifiés. Par conséquent, le système de transmission n'est pas robuste contre des attaques à textes clairs connus. Par contre dans le second cas, l'ajout des retards permet de rendre le système de transmission ainsi proposé robuste, car les paramètres de l'émetteur ne sont pas identifiables.

Les problèmes traités dans cette thèse laissent entrevoir quelques perspectives et élargissements, tant sur le plan théorique que pratique.

D'un point de vue pratique, une expérimentation du cryptosystème chaotique proposé constituerait un prolongement intéressant de cette thèse. Comme cela a déjà été réalisé pour le circuit de Colpitts notamment, il faudrait construire les autres blocs en utilisant des micro-controlleurs. Comme pour tout système physique, on peut supposer que les valeurs des paramètres des différents composants électroniques possèdent une marge d'incertitude. Cela ouvre la voie à une réflexion sur la synchronisation des systèmes chaotiques incertains.

Dans notre étude, nous avons proposé un oscillateur de Colpitts qui travaille à une

fréquence de $10Khz$. Il sera très intéressant de monter en fréquence afin d'élargir le spectre de fréquence de l'oscillateur.

Dans les systèmes des transmissions sécurisées, en particulier les systèmes chaotiques, les documents numériques quels qu'ils soient sont soumis au problème de piratage. Une solution pour empêcher la copie des documents numériques est d'ajouter une signature. Le watermarking chaotique (traduction française : filigrane chaotique), appelé tatouage chaotique, permet d'insérer dans un document numérique une signature non perceptible qui peut résoudre les problèmes des droits d'auteurs ou augmenter la fonctionnalité du document. Une des extensions de notre travail est de concevoir un algorithme pour l'insertion d'une signature sur les donnés numériques à transmettre. A cet effet, une étude sur la robustesse de l'image tatouée contre différents traitements possibles de l'image (compression JPEG, lissages d'images, etc) doit être menée.

La taille brute des images numériques étant souvent très importante, il serait aussi intéressant d'étudier la cas de la compression d'images par ce nouveau schéma de transmission.

Nous nous sommes attachés dans cette thèse à synchroniser deux systèmes chaotiques en temps continu, il serait utile d'étudier les synchronisations de plusieurs systèmes chaotiques. Pour résoudre ce problème, nous envisageons utiliser soit, les réseaux de neurones ou bien les systèmes à événements discrets.

Annexe A

Généralités sur systèmes chaotiques

Annexe A : Généralités sur systèmes chaotiques

.1 Définitions

Définition 21 *(Système dynamique non linéaire) Un système dynamique en temps continu est décrit par un système d'équations différentielles, alors qu'en temps discret, on parle d'un système d'équations aux différences finies.*

– *temps continu*

$$\dot{x} = f(t, x, u) y = h(t, x, u) \tag{29}$$

où : $x \in U \subseteq \mathbb{R}^n$ est un vecteur de dimension n, $f : \mathbb{R}^n \to \mathbb{R}^n$ est une fonction non linéaire désignant le champs de vecteurs, $h : \mathbb{R}^n \to \mathbb{R}$ une fonction éventuellement non linéaire qui désigne le vecteur de sortie et $u \in V \subseteq \mathbb{R}^p$ représente l'entrée du système.

Si le système (30) ne dépend pas de l'entrée, on aura alors :

$$\dot{x} = f(t, x) \tag{30}$$

Le système (30) est un système dynamique car, à partir de n'importe quelle condition initiale x_0, on peut résoudre les équations et obtenir l'état futur $x(t)$ pour $t > 0$.

– temps discret

Comme il a été déjà précisé le système dynamique est dans ce cas représenté par des équations aux différences finies, avec le modèle général suivant :

$$x(k+1) = G(k, x(k), u(k)) y(k) = h(k, x(k), u(k)) \tag{31}$$

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

En temps discret, on définit aussi le système autonome comme une dynamique qui ne dépend pas de l'instant k :

$$x(k+1) = G(x(k), u(k)) y(k) = h(x(k), u(k)) \tag{32}$$

Dans ce qui, nous allons donner uniquement quelques notions sur les systèmes continus. Pour le cas discret, les définitions restent les mêmes.

Définition 22 *(Système autonome) Un système dynamique non linéaire est dit autonome lorsqu'il ne dépend pas explicitement du temps. Un système autonome est donné ci-dessous :*

$$\dot{x} = f(x) \tag{33}$$

où $x \in \mathbb{R}^n$. Un système autonome est indépendant du temps initial, alors qu'un système non autonome ne l'est pas. Dans un système autonome, tout instant peut être considéré comme instant initial, et tout état $x(t)$ du système peut être considéré comme un état initial.

Définition 23 *(Flot) Toute solution $\varphi_t(x)$ du système autonome (33), considérée comme un ensemble de trajectoires avec différentes conditions initiales, est appelée flot.*

Définition 24 *(Espace des phases) Dans un système dynamique de dimension n, l'espace $x_1, x_2, ...x_n$ est appelé espace des phases ou espace d'états. Ainsi le chemin parcouru par le système est appelé "trajectoire", et $x_1, x_2, ...x_n$ sont les "états" du système.*

Définition 25 *(Point fixe ou point d'équilibre) On appelle point fixe ou point d'équilibre du système (33), le point x^* tel que :*

$$f(x^*) = 0$$

Remarque 1 *Par un changement de variables $\xi = x - x^*$ on peut ramener le point x^* à l'origine.*

Exemple 9 *Considérons un simple pendule montré dans la figure 2, où l est la longueur de la corde considérée comme rigide et sans masse, et m représente la masse en mouvement. On note θ l'angle que la corde fait avec la verticale. Afin d'écrire les équations du mouvement, on identifie les forces agissants sur la masse. Ainsi, il y a la force gravitationnelle donnée par $F_g = mg$ où g est l'accélération de la gravité. On suppose aussi que la masse est soumise à une force de résistance de friction proportionnelle à la vitesse de la masse et de coefficient de friction k.*

D'après la seconde loi de mouvement de Newton, on obtient alors l'équation du mouvement :

$$ml\ddot{\theta} = -mgsin(\theta) - kl\dot{\theta}$$

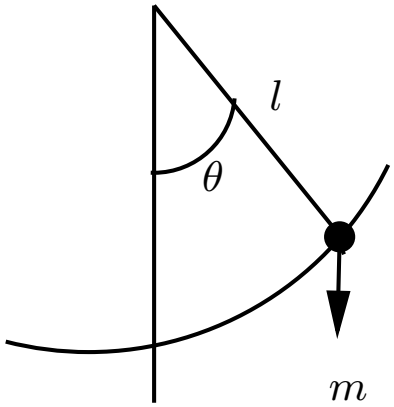


FIG. 2: Pendule simple

On décrit alors le modèle dans l'espace d'état non linéaire en choisissant $x_1 = \theta$ *et* $x_2 = \dot{\theta}$.

$$\begin{cases} \dot{x}_1 = x_2 \\ \dot{x}_2 = -\frac{g}{l} sin(x_1) - \frac{k}{m} x_2 \end{cases}$$

Afin de trouver les points d'équilibre, on pose : $\dot{x}_1 = \dot{x}_2 = 0$

$$\begin{cases} 0 = x_2 \\ 0 = -\frac{g}{l} sin(x_1) - \frac{k}{m} x_2 \end{cases}$$

Les points d'équilibre sont alors situés au $(n\Pi, 0)$ *pour* $n = 0, \pm 1, \pm 2, ...$ *Physiquement, cela correspond à l'existence de deux points d'équilibre* $(0, 0)$ *et* $(\Pi, 0)$. *Mais le pendule peut rester au point* $(0, 0)$, *alors qu'il ne pourra pas maintenir sa position d'équilibre en* $(\Pi, 0)$. *Ainsi, on dit que le point* $(0, 0)$ *est un point d'équilibre stable tandis que le point* $(\Pi, 0)$ *est un point d'équilibre instable.*

Définition 26 *(Cycle limite) Un système non linéaire peut être un siège d'oscillations, caractérisés par leurs amplitudes et leurs fréquences, indépendantes de la condition initiale* x_0, *et sans excitation extérieure. Ce siège est appelé cycle limite.*

Définition 27 *(Comportement chaotique) Un système non linéaire peut avoir un com-*

portement en régime permanent plus complexe que comportements habituels : oscillations périodiques, quasi-périodiques, etc. Dans ce cas, la sortie du système est extrêmement sensible aux conditions initiales, d'où la "non prévisibilité" de la sortie à long terme. On dit alors que le système a un comportement chaotique.

L'exemple suivant illustre le caractère chaotique de tels systèmes.

Soit le modèle chaotique donné par Otto de Rössler :

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

avec (x_1, x_2, x_3) le vecteur d'état et a, b et c les paramètres du système.

Le système de Rössler montre un comportement chaotique pour $a = 0.2$, $b = 5.7$, $c = 0.2$ avec les conditions initiales $x_1(0) = 0.01$, $x_2(0) = 0.01$ et $x_3(0) = 0.01$.

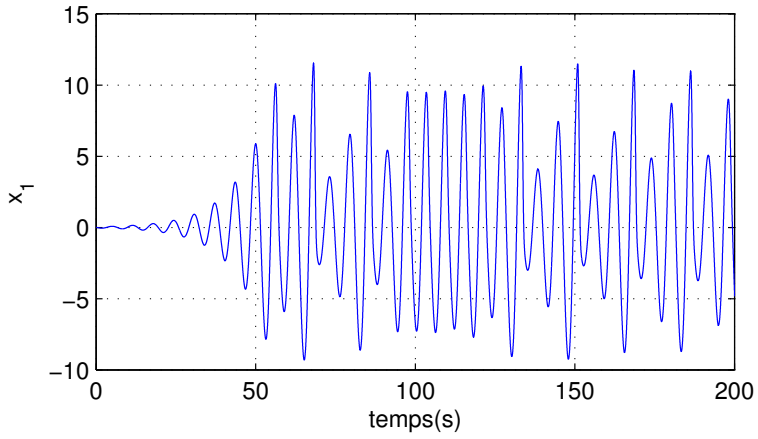


FIG. 3: Etat chaotique x_1 du système de Rössler

Remarque 2 *Pour un système autonome en temps continu, au moins trois variables d'état sont nécessaires pour générer le chaos. Dans le cas d'un système non-autonome, il faut au moins deux variables d'état et une entrée indépendante.*

En étudiant l'évolution temporelle des variables d'état, on peut facilement identifier une solution de type fixe (ou point d'équilibre) ou une solution périodique. En revanche, il n'est pas facile de dire si le système est chaotique ou pas. Pour réssoudre ce problème, nous étudions l'espace des phases ou l'espace d'états. Une trajectoire quasi-périodique

converge vers une forme (un attracteur), tandis qu'une trajectoire chaotique montre un comportement plus compliqué.

.2 Sensibilité aux conditions initiales

La sensibilité aux conditions initiales a été découverte en 1963 par Edward Lorenz lors de ses travaux en météorologie. C'est une explication scientifique de l'effet papillon (un battement d'ailes de papillon à un endroit du monde peut être la cause d'une tempête à un autre endroit), démontrant que, dans un système non linéaire, une modification infime des conditions initiales peut entraîner des résultats imprévisibles à long terme Dans ce qui suit, cette sensibilité aux conditions initiales sera illustrée à travers le système de rössler présenté précédemment.

Les conditions initiales sont choisies comme suit : $x_1(0) = 0.01$, $x_2(0) = 0.01$, $x_3(0) = 0.01$ et $x_1'(0) = 0.012$, $x_2'(0) = 0.01$ et $x_3'(0) = 0.01$.

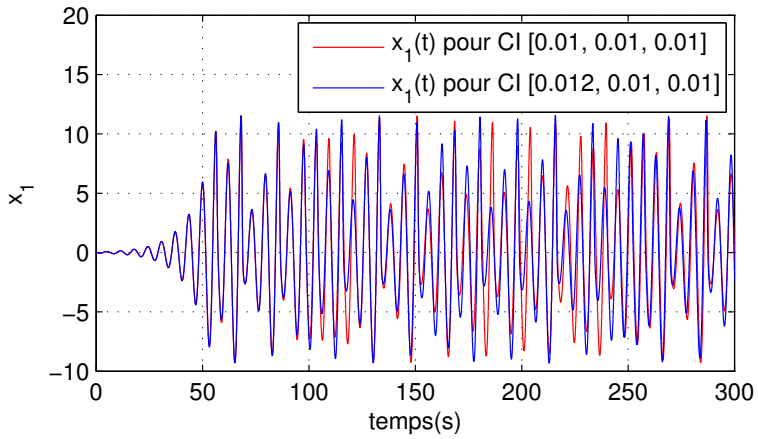


FIG. 4: Illustration de la propriété de sensibilité aux conditions initiales sur l'état x_1

Les systèmes chaotiques montrent une sensibilité exponentielle aux conditions initiales, c'est à dire qu'un petit écart entre deux conditions initiales conduit à une divergence rapide des trajectoires au cours du temps. C'est dans ce contexte qu'on définit les exposants de Lyapunov, expliqués au paragraphe suivant.

.3 Exposants de Lyapunov

Les exposants de Lyapunov, présentés par Oseledec pour la première fois en 1968 [72], jouent un rôle important dans l'étude des systèmes non linéaires, notamment les

systèmes chaotiques. Ils qualifient le degré de divergence des trajectoires d'un système dynamique non linéaire soumis à des conditions initiales différentes. Cette divergence est exprimée par les exposants de Lyapunov. Les exposants de Lyapunov caractérisent ainsi le comportement du système non linéaire et notamment son caractère chaotique ou hyperchaotique [72]. Par exemple, la positivité du plus grand exposant de Lyapunov d'un système dynamique non linéaire affirme l'existence d'un régime chaotique.

Des méthodes très variées existent pour calculer les exposants de Lyapunov [30]. A titre d'exemple, le paragraphe suivant explique les principes de calcul des exposants de Lyapunov pour les systèmes non linéaires de dimension 1 et de dimension supérieure à 1.

.3.1 Cas d'une équation différentielle simple

Bien qu'en général, les exposants de Lyapunov soient utilisés pour déterminer le degré de divergence des trajectoires d'un attracteur (dimension >1), ils peuvent aussi être employés pour caractériser la divergence des trajectoires d'une équation différentielle simple (dimension 1). Considérons l'équation différentielle donnée par :

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

avec : $\dot{x}_a = f(x_a)$ première trajectoire $\dot{x}_b = f(x_b)$ seconde trajectoire $d = x_b - x_a$ la différence. Nous avons donc :

$$\dot{d} = \dot{x}_b - \dot{x}_a = f(x_b) - f(x_a) \approx f'(x_a)d \tag{34}$$

On suppose que la distance d est petite et on développe $f(x_b) = f(x_a + d)$ en série de Taylor :

$$f(x_a + d) = f(x_a) + f'(x_a)(x_b - x_a) = f(x_a) + f'(x_a)d$$

On considère aussi que $f'(x_a)$ est constante (ou elle varie très lentement), c'est à dire $f'(x_a) \approx \lambda$. Le flot associé à l'équation (34), appelé $D(t)$ est donné par :

$$D(t) = d_0 e^{\lambda(t-t_0)} \tag{35}$$

où d_0 est la distance initiale entre les trajectoires et t_0 représente l'instant initial.

D'après (35), il est évident que le signe de λ détermine la convergence ou la divergence des trajectoires. La valeur de λ est calculée d'après la relation suivante :

$$\lambda = \frac{1}{t - t_0} ln \frac{D(t)}{d_0} \tag{36}$$

Pour les systèmes non linéaires réels, la condition $f'(x_a) \approx \lambda$ n'est pas vérifiée dans la plupart des cas. Cependant, il est possible de trouver la divergence finale des trajectoires à long terme, c'est-à-dire la limite de (36) lorsque t tend vers l'infini :

$$\lambda = \lim_{t \longrightarrow \infty} \frac{1}{t - t_0} ln \frac{D(t)}{d_0} \tag{37}$$

Cette limite est appelée "exposant de Lyapunov"

Remarque 3 *Si $\lambda > 0$ alors la distance entre les trajectoires augment de façon exponentielle et finalement à un régime chaotique est atteint. En revanche, si $\lambda < 0$, la distance entre les trajectoires converge vers zéro lorsque $t \rightarrow \infty$ et un mouvement régulier est obtenu. Dans un système d'ordre supérieur à un, il suffit que le plus grand exposant de Lyapunov soit positif pour pouvoir qualifier le système de "chaotique".*

.3.2 Cas d'un système d'équations non linéaires

Nous allons maintenant expliquer le principe de calcul des exposants de Lyapunov pour un système d'équations non linéaires. pour cela, on considère le système :

$$\dot{x} = f(x, p) \tag{38}$$

Dans lequel x est le vecteur des variables d'état et $f = [f_1(x,p), f_1(x,p), ..., f_d(x,p)]$ représente le vecteur de fonctions non linéaires, qui dépendent de l'ensemble de paramètres $p = p_1, p_2, etc.$ Pour calculer les exposants de Lyapunov, il est considéré que pour une condition initiale $x(0)$, l'orbite fermée $x(t) + \eta_x(t)$ démarrée à $x(o) + \eta_x(0)$ vérifient les équations linéairisées données par :

$$\dot{\eta} = A(t)\eta; A(t) = \frac{\partial f(x_i(t))}{\partial x_j} \tag{39}$$

où $A(t)$ est la matrice jacobienne du système calculée au long de la trajectoire $x(t)$. Si f est continue et suffisamment différentiable, les exposants de Lyapunov sont calculés comme les états du système (39). Afin de calculer le spectre des exposants de Lyapunov, il faut résoudre simultanément les systèmes (38) et (39) en partant des conditions initiales $x(0)$ et un ensemble de vecteurs orthogonaux et normalisés $\eta_{x_1}(0), \eta_{x_2}(0), ..., \eta_{x_d}(0)$. Les calculs sont effectués sur un intervalle fini de temps T au bout duquel les vecteurs $\eta_{x_1}(T), \eta_{x_2}(T), ..., \eta_{x_d}(T)$ sont obtenus. Les exposants de Lyapunov sont ensuite calculés comme suit :

$$\lambda_i = \frac{1}{NT} \sum_{k=1}^{N} ln\eta_{x_i}^{(k)}, i = 1, 2, ...d \tag{40}$$

où N est le nombre d'itérations de l'algorithme et d représente la dimension du système [72].

.3.3 Comportement du système en fonction des exposants de Lyapunov

En étudiant les exposants de Lyapunov d'un système non linéaire, on peut définir le type d'attracteur (comportement asymptotique) généré par le système (sous l'hypothèse que les trajectoires évoluent dans une région bornée) :

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

.4 Stabilité d'un point d'équilibre

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

Définition 28 *(Stabilité au sens de Lyapunov) Le point d'équilibre x^* est dit stable si $\forall \epsilon > 0, \exists \alpha > 0$ tel que :*

$$\|x(0) - x^*\| < \alpha \Longrightarrow \|x(t) - x^*\| < \epsilon, \forall t \geq 0$$

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

Si l'on suppose que le point d'équilibre est ramené à l'origine par un changement de coordonnées, la stabilité du point d'équilibre $x^* = 0$ est étudiée de la façon suivante : $\forall \epsilon > 0, \exists \alpha > 0$ tel que :

$$\|x(0)\| < \alpha \Longrightarrow \|x(t)\| < \epsilon, \forall t \geq 0$$

Définition 29 *(Instabilité) Le point d'équilibre x^* est dit instable s'il n'est pas stable au sens de Lyapunov.*

Définition 30 *(Stabilité asymptotique) Le point d'équilibre x^* est asymptotiquement stable s'il est stable et si l'on peut choisir $\delta > 0$ tel que :*

$$\|x(0) - x^*\| < \delta \Longrightarrow \lim_{t \longrightarrow \infty} x(t) = x^*$$

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

Définition 31 *(Stabilité exponentielle) Le point d'équilibre x^* est exponentiellement stable si $\alpha > 0$ et $\lambda > 0$ tels que :*

$$\forall t > 0, \exists B_r(x^*, r), \forall x(0) \in B_r, \|x(t) - x^*\| < \alpha \|x(0) - x^*\| e^{-\lambda t}$$

dans lequel $B_r = \{x \in \mathbb{R}^n / \|x(t)\| \leq r\}$, et $\| \bullet \|$ est une norme sur $\mathbb{R}^n$. Dans ce cas λ est appelé "taux de convergence".

Définition 32 *(Stabilité globale) Si le système est asymptotiquement (exponentiellement) stable quelle que soit $x(0)$, le point d'équilibre est dit globalement (exponentiellement) stable.*

.4.1 Etude de la stabilité à l'aide du système linéairisé

Pour étudier la stabilité du point d'équilibre, on peut aussi étudier les valeurs propres de la matrice jacobienne A du système au point d'équilibre. Différents cas sont possibles :

- Si toutes les valeurs propres de A possèdent des parties réelles négatives, alors le point d'équilibre x^* est asymptotiquement stable appelé "puit" (en anglais sink) car toutes les trajectoires voisines convergent vers ce point. et est appelé
- Si l'une des valeurs propres de A possède une partie réelle positive, le point d'équilibre est instable. Aussi, si toutes les valeurs propres ont des parties réelles positives, le point d'équilibre est appelé "source". Un point d'équilibre ayant des valeurs propres stables et instables est un point appelé "selle".
- Le point d'équilibre est dit "hyperbolique" si toutes les valeurs propres de A ont des parties réelles non nulles. Tous les points d'équilibre hyperboliques sont instables asymptotiquement stables.

Il est à noter que dans les définitions ci-dessus, on tient compte de la partie réelle des valeurs propres. Le cas des valeurs propres purement imaginaires est étudié dans [72].

.4.2 Méthode directe de Lyapunov

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

$$\dot{x} = f(x) \tag{41}$$

où $x \in \mathbb{R}^n$ et $f(x^*) = 0$.

Théorème 9 *S'il existe une fonction $V : U \to \mathbb{R}$, continue sur un voisinage U de x^* et différentiable telle que :*

1. *$V(x^* = 0$ et $V(x) > 0$ si $x \neq x^*$,*
2. *$\dot{V} = \sum_{j=1}^{n} \frac{\partial V}{\partial x_j} \dot{x}_j = \sum_{j=1}^{n} \frac{\partial V}{\partial x_j} f_j \leq 0, \forall x \in U$ alors x^* est un point d'équilibre stable pour le système (41)*
3. *Si de plus, la fonction V est telle que :*

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

alors x^* est un point d'équilibre asymptotiquement stable.

Exemple 10 *Soit le système :*

$$\dot{x} = y + ax(x^2 + y^2) \dot{y} = -x + ay(x^2 + y^2) \tag{42}$$

Ce système a un point d'équilibre unique $(0, 0)$. On pose $V = x^2 + y^2$, alors :

$$\dot{V} = 2(x\dot{x} + y\dot{y}) = 2a(x^2 + y^2)^2 \tag{43}$$

D'après le théorème de Lyapunov, si $a < 0$, le point fixe est asymptotiquement stable ; si $a = 0$, le point est au moins stable au sens de Lyapunov, et si $a > 0$, le système est instable au sens de Lyapunov.

Exemple 11 *Considérons à nouveau l'équation du pendule de l'exemple 9. On considère la fonction de Lyapunov :*

$$\dot{V}(x) = \frac{g}{l}(1 - cosx_1) + \frac{1}{2}x_2^2$$

$\dot{V}(x)$ est calculée alors par :

$$\dot{V}(x) = \frac{g}{l}\dot{x}_1 + x_2\dot{x}_2 = -\frac{k}{m}x_2^2$$

$\dot{V}(x) \leq 0$ quelque soit x_1, ce qui montre que le point d'équilibre $(0, 0)$ est stable. Cependant, nous savons que l'origine est asymptotiquement stable mais la fonction de Lyapunov

choisie ne prouve pas cette propriété. Il faut alors chercher une autre fonction de Lyapunov ou d'autres théorèmes de stabilité, comme par exemple le théorème de LaSalle [72].

.5 Bifurcation

Soit le système :

$$\dot{x} = f(x, \mu), x \in \mathbb{R}^n, \mu \in \mathbb{R}^p \tag{44}$$

Où f est une fonction $C^r(r > 1)$ sur un ouvert dans $R_n x R^p$. De plus, on considère que le système possède un point d'équilibre en $(x, \mu) = (x_0, \mu_0)$, c'est-à-dire $f(x_0, \mu_0) = 0$.

Le comportement du système (44) dépend de l'ensemble des paramètres μ. A chaque fois que, pour une valeur donnée d'un paramètre- dite valeur critique- la solution du système d'équation change qualitativement, on dit qu'il y a une bifurcation. La bifurcation est en effet associée au changement topologique de la trajectoire d'un système dynamique lorsqu'un ou plusieurs de ces paramètres varient. Ainsi, le paramètre μ dans l'équation (44) est appelée "paramètre de bifurcation", et la valeur de μ pour laquelle, on paut observer une bifurcation est appelé "point de bifurcation". La représentation d'une propriété caractéristique d'une solution, en fonction du paramètre de bifurcation constitue un "diagramme de bifurcation".

L'exemple le plus connu d'un système non linéaire pour lequel il est possible de tracer un diagramme de bifurcation est l'équation logistique [1]. Il est facile de tracer le diagramme de bifurcation de ce système car μ est un scalaire.

Lorsque le système possède p paramètres, il faut fixer $p - 1$ paramètres et faire varier le paramètre restant pour tracer le diagramme de bifurcation et étudier le comportement du système.

Exemple 12 *Soit le système :*

$$x = \mu - x^2$$

avec $x \in \mathbb{R}$ l'état et $\mu \in \mathbb{R}$ le paramètre. Les points d'équilibre sont les solutions de $\dot{x} = 0$:

$$x_e = \pm\sqrt{\mu}$$

Ces solutions n'existent que pour $\mu \geq 0$. Un changement qualitatif dans la dynamique apparaît lorsque $\mu = 0$. Pour $\mu \geq 0$. Le pont d'équilibre $x_e = -\sqrt{\mu}$ est instable, alors que

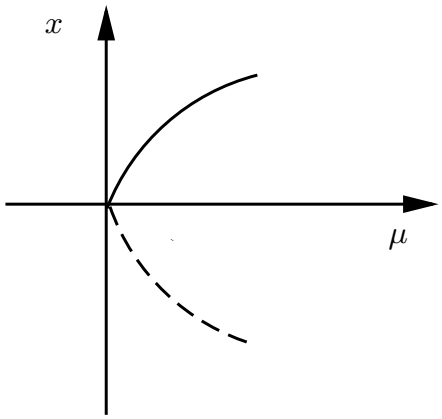


FIG. 5: Diagramme de bifurcation du pendule simple

le point d'équilibre $x_e = \sqrt{\mu}$ est stable. Les deux états (stable et instable) se coïncident alors en $\mu = 0$. Cette bifurcation est montrée dans la figure 5.

Définition 33 *Bifurcation de Hopf) Soit le système $\dot{x} = f(x, \mu)$ avec $x \in \mathbb{R}^2$. On appelle bifurcation de Hopf le phénomène d'apparition d'un cercle autour du pont d'équilibre lors de passage par $\mu = 0$. Ce cercle possède une propriété d'attractivité duale à celle du point d'équilibre.*

La bifurcation de Hopf correspond à une situation où le paramètre μ varie jusqu'à dépasser le paramètre critique μ_0, et déplace une paire de valeurs propres complexes et conjuguées du plan gauche vers le plan droit en traversant l'axe imaginaire. Dans ce cas, les autres valeurs propres restent stables. Au moment de traverser l'axe imaginaire, la partie réelle des valeurs propres conjuguées devient nulle et ceci donne naissance à un cycle limite.

Théorème 10 *(Poincaré-Andronov-Hopf) Supposons le système $\dot{x} = f(x, \mu)$ de dimension 2, avec le point d'équilibre $(0, 0)$. On suppose aussi que les valeurs propres (complexes conjuguées) de la matrice jacobienne du système sont purement imaginaire lorsque $\mu = \mu_0$. On note ces valeurs propres λ_μ et $\overline{\lambda}_\mu$. Si la partie réelle des valeurs propres vérifie :*

$$\frac{d\mathbf{R}}{\lambda_\mu} d\mu | \mu = \mu_0 > 0$$

alors :

- *$\mu = \mu_0$ est un point de bifurcation du système ;*

- *Pour des valeurs de μ suffisamment proches de μ_0 avec $\mu < \mu_0$, le point d'équilibre est asymptotiquement stable ;*

- *Pour des valeurs de μ suffisamment proches de μ_0 avec $\mu > \mu_0$, le point d'équilibre est instable ;*

- *Pour ces valeurs de μ suffisamment proches de μ_0 avec $\mu \neq \mu_0$, le point d'équilibre est entouré d'un cycle limite d'amplitude $O(\sqrt{|\mu|})$.*

La bifurcation de Hopf est appelée "sur critique" si le point d'équilibre passe d'un état stable à un état instable. De la même manière, la bifurcation de Hopf est dite "sous critique" si le point d'équilibre passe d'un état instable à un état stable.

.6 Section de Poincaré

En mathématiques, dans la théorie des systèmes dynamiques, *la section de Poincaré* est l'intersection d'une trajectoire (périodique, quasi-périodique ou chaotique) dans l'espace d'au moins trois dimension, avec un hyperplan d'une dimension inférieure. Ainsi, nous observons le retour de la trajectoire vers l'hyperplan qui commence à un certain point de celle-ci l'ensemble des points marqués par la trajectoire sur l'hyperplan est appelé plan de Poincaré [1].

Considérons $x(x_0, t_0, t \equiv \varphi_t(x_0)$ une solution d'un système autonome $\dot{x} = f(x)$. On définit localement un hyperplan $\sum \subset \mathbb{R}^n$ de dimension $n-1$, transversal au champs de vecteurs f en x_0. On suppose maintenant un point x au voisinage $V \subseteq \sum$ de x_0. L'application de Poincaré $P : V \to \sum$ est alors définie par :

$$x_1 = P(x) = \varphi_\tau(x) \tag{45}$$

où $\tau = \tau(x)$ est le temps après lequel la trajectoire retourne et intersecte $\sum$ pour la première fois.

L'hyperplan $\sum$ s'appelle alors "section de Poincaré". La section de Poincaré remplace le système dynamique en temps continu par un système en temps discret. C'est une visualisation par échantillonnage du système avec une paramétrisation qui doit être choisie convenablement pour accéder au maximum d'informations.

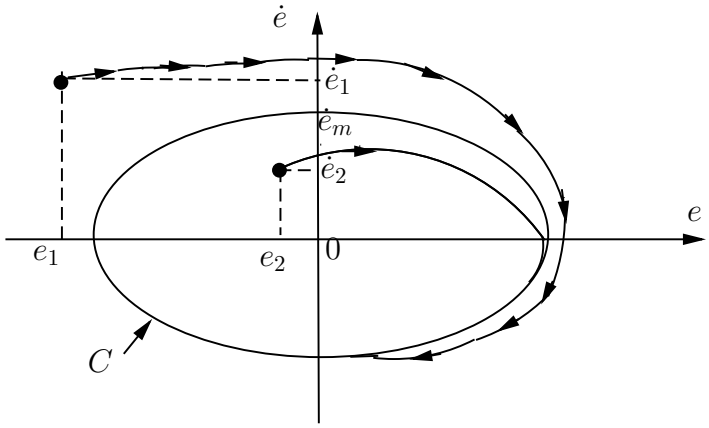


FIG. 6: Plan de Phase d'un pendule entretenu

.7 Notion d'attracteur

Les systèmes dynamiques ont tendance a être dissipatifs : en l'absence de force, le mouvement cesse. L'énergie fournie et la dissipation se combinent afin d'éliminer les transitions et de conduire le système à son comportement caractéristique.

Prenons un exemple simple qui est celui du pendule oscillant entretenu : l'énergie fournie au pendule depuis l'extérieur permet de compenser les divers pertes de ce dernier et est donc dissipé par le système. Lorsque l'énergie fournie et celle dissipée par le pendule sont égales, un état permanent est atteint. Le régime est alors périodique : l'amplitude des oscillations est constante et la trajectoire représentative dans l'espace des phases est un cycle limite. La figure 6 explique ce phénomène pour le pendule dont les équations sont données en figure (30). Dans cette figure, le cycle limite est présenté par C.

Pour vérifier le caractère attracteur, il suffit d'écarter le système de son état permanent. Par exemple, on perturbe le pendule par un choc l'amenant à une amplitude et une vitesse supérieures au maximum du cycle. Au bout d'un certain temps, la dissipation fait converger la trajectoire correspondante vers le cycle limite.

De la même manière, un freinage temporaire du pendule entretenu peut réduire à un instant l'amplitude et la vitesse, mais l'évolution dans le temps ramène la trajectoire vers le cycle limite. En fait, toute trajectoire de l'espace des phases qui débute d'un point dans un certain voisinage du cycle limite, sera attiré vers l'attracteur C.

Définition 34 *L'ensemble invariant A (c'est-à-dire $\Phi_t(A) = A$) est un attracteur si pour tout voisinage U de A, il existe un voisinage V de A tel que :*

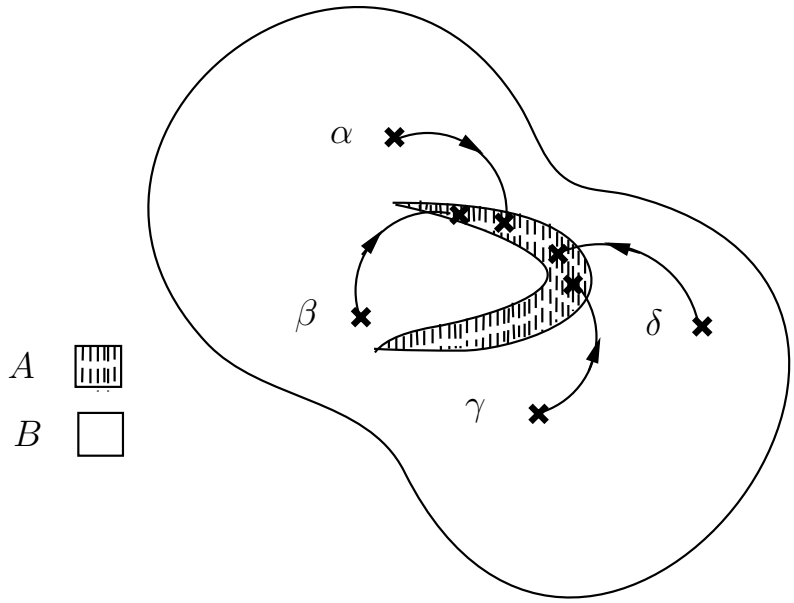


FIG. 7: A : Attracteur, B : Bassin d'attraction

- $x(x_0(t)) \equiv \Phi_t(x_0)$ *reste dans* U *si* $x_0 \in V$,
- $\bigcap_{t\geq 0} \Phi_t(V) = A$

Remarque 4 *L'attracteur le plus simple est le point fixe. Un deuxième type d'attracteur pour un champ de vecteurs est le cycle limite : c'est une trajectoire fermée qui attire toute les trajectoires proches.*

Définition 35 *(Bassin d'attraction) Le bassin d'attraction est l'ensemble des points de l'espace des phases qui sont sous l'effet de l'attracteur. C'est à dire que toutes les trajectoires qui commencent à ces points tendent vers l'attracteur après un temps fini.*

Autrement dit, l'attracteur A n'est pas autre chose que la limite asymptotique des solutions partant de toute condition initiale située dans son bassin d'attraction (figure7). Ainsi, l'ensemble $W = \bigcup_{t<0} \Phi_t(V)$ est le bassin d'attraction de A.

Pour un système défini par les équations différentielles, le bassin d'attraction est reformulé pour une solution asymptotiquement stable $x^*(t)$, c'est à dire l'ensemble des points initiaux x_0 pour lesquels les solutions $x(x_0, t)$ satisfont :

$$\lim_{t\longrightarrow\infty} \|x(x_0, t) - x^*(t)\| = 0 \tag{46}$$

est le bassin d'attraction de la solution $x_0(t)$ (pour plus d'exemples voir [72]).

.7.1 Attracteur étrange

Le terme attracteur étrange a été utilisé pour la première fois par David Ruelle et Floris Takens en 1971, afin de décrire l'attracteur obtenu par une série de bifurcations d'un système modélisant le courant d'un liquide [30]. En fait, avant l'article de Ruelle et Takens, les attracteurs avaient déjà fait l'objet de publications mais ils sont restés ignorés. Cette appellation d'attracteur étrange fait appel à leur propriété peu commune, qui est leur dimension fractale. En effet la structure géométrique des trajectoires générées par un système chaotique est extrêmement complexe à cause des étirements, repliements et contractions s'opérant dans une région bornée de l'espace d'état. La section de Poincaré d'une trajectoire chaotique est constituée d'une infinité de couches fines, ce qui suppose que les trajectoires tendent à remplir un espace de dimension non entière, c'est à dire fractale.

La dimension d'un ensemble est le nombre de paramètres indépendants nécessaires pour décrire un point dans l'ensemble. Par exemple, un point dans un plan cartésien est défini par deux paramètres, qui sont ses coordonnées. La dimension du plan est donc égale à 2.

Revenons maintenant à l'exemple du pendule. Au départ, en dehors du cycle limite, deux coordonnées $\dot{\theta}_i$, θ_i sont nécessaires pour caractériser le système. L'espace des phases possède alors deux dimensions. Une fois atteinte l'asymptote, une seule trajectoire subsiste : la ligne C qui est suffisante pour repérer un point. La dimension de l'attracteur est donc inférieure à celle de l'espace des phases, soit le nombre de degré de liberté du système. De plus, une fois que les trajectoires ont atteint l'attracteur, tout volume représentatif d'un ensemble de conditions initiales devient nul. Ce qui revient à dire que le volume de l'attracteur est nul dans $\mathbb{R}^n$.

Définition 36 *(Dimension de Hausdorff) [30] La dimension de Hausdorff est un nombre réel achevé et non négatif, c'est à dire un nombre appartenant à l'intervalle infini* $[0, \infty$*, associé à un espace métrique quelconque.*

Un attracteur étrange est reconnu par sa dimension de Hausdorff fractale. Un ensemble A est fractale si sa dimension n'est pas entière [1]. la dimension fractale satisfait les propriétés

suivantes :

1. si $A \subset B$, alors $d(A) \leq B$
2. si $A = \emptyset$, alors $d(A) = 0$
3. $d(A \times B)$=$d(A) + d(B)$
4. si f est une application différentielle sur A, alors $d(f(A))$=$d(A)$

Les caractéristiques de l'attracteur étrange sont alors :

- Dans l'espace des phases, est de volume nul,
- La dimension d de l'attracteur est fractale avec $2 < d < n$, où n est la dimension de l'espace des phases,
- Sensibilité aux conditions initiales : deux trajectoires de l'attracteur initialement voisines finissent par s'écarter l'une de l'autre.

Dans ce qui suit, nous allons présenter deux exemple d'attracteurs. Le premier est un attracteur d'un système non linéaire en temps continu et l'autre d'un système non linéaire en temps discret.

.7.2 Attracteur de Lorenz

L'attracteur de Lorenz fut introduit par Edward Lorenz en 1963. Il s'agit d'un système dynamique non linéaire en temps continu de dimension 3, obtenu des équations de transfert de la chaleur dans un liquide. Le système de Lorenz est défini par :

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = x(b - z) - y \\ dotz = xy - cz \end{cases} \tag{47}$$

avec (x, y, z) le vecteur d'état et a, b et c les paramètres du système.

Le système de Lorenz montre un comportement chaotique et génère un attracteur étrange pour $a = 10$, $b = 28$, $c = 8/3$. La dimension de Hausdorff de l'attracteur de Lorenz est estimée entre 2 et 3. La figure 11 montre l'attracteur de Lorenz en partant des conditions initiales $x_0 = y_0 = z_0 = 0.01$ avec un pas de simulation de 0.01. Si l'on regarde l'attracteur de plus près, nous constatons que la trajectoire mêle deux comportements différents : Le premier est un comportement apparemment régulier, c'est à dire dans plusieurs régions de l'espace d'état, elle forme des boucles semblables à celles de

trajectoires périodiques. Le deuxième comportement semble aléatoire, c'est à dire que le nombre de boucles décrites dans une région avant de rejoindre brusquement une autre région est imprévisible. Aussi, les instants auxquels ces changements de région apparaissent sont imprévisibles.

.7.3 Attracteur de Hénon

Le modèle de Hénon est donné comme suit :

$$\begin{cases} x(n+1) = a - x^2(n) + by(n) \\ y(n+1) = x(n) \end{cases} \tag{48}$$

avec (x, y) le vecteur d'état et a, b les paramètres du système.

Le système de Hénon montre un comportement chaotique et génère un attracteur étrange pour $a = 1.4$, $b = 0.3$ avec $x(0) = 0$ et $y(0) = 0$ les conditions initiales du système.

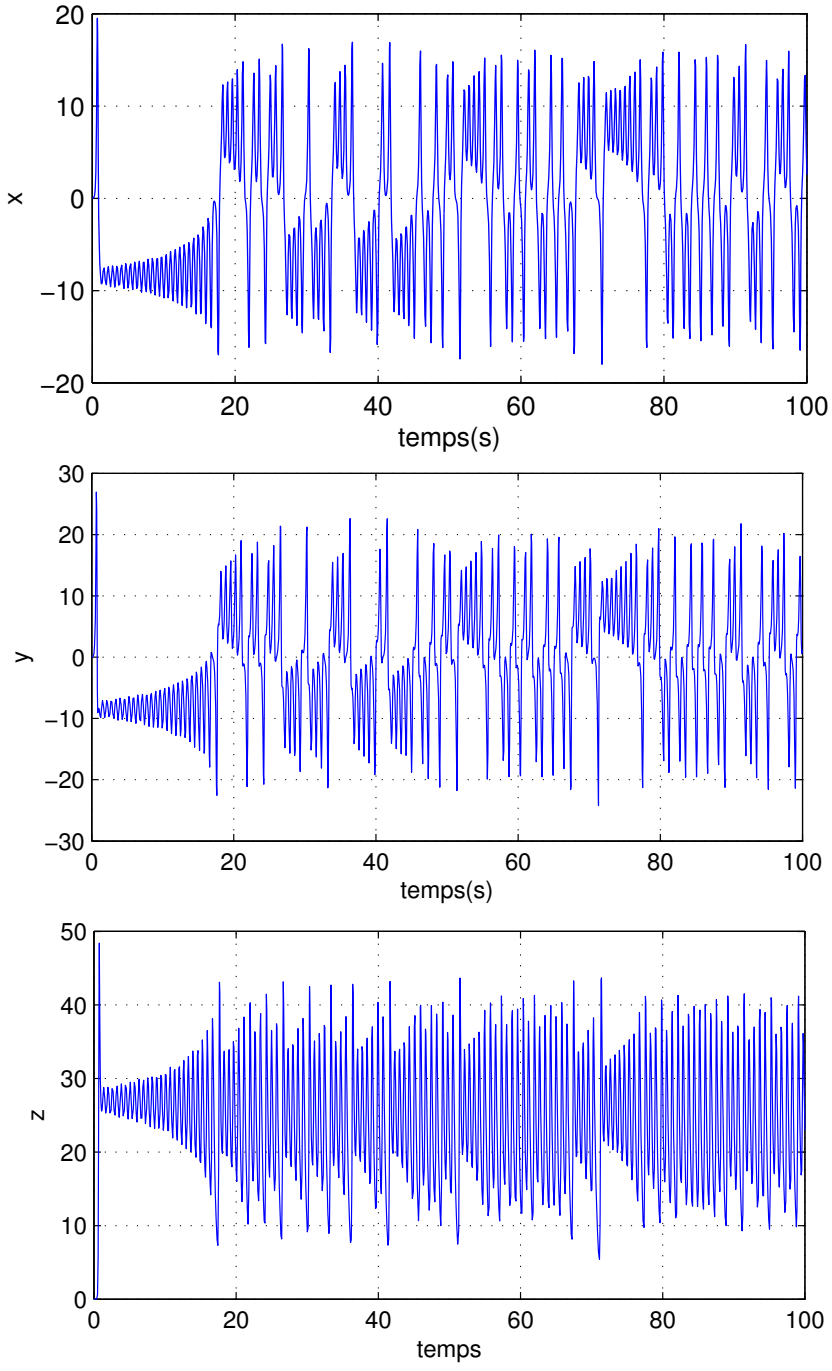


FIG. 8: Etats chaotiques du système de Lorenz

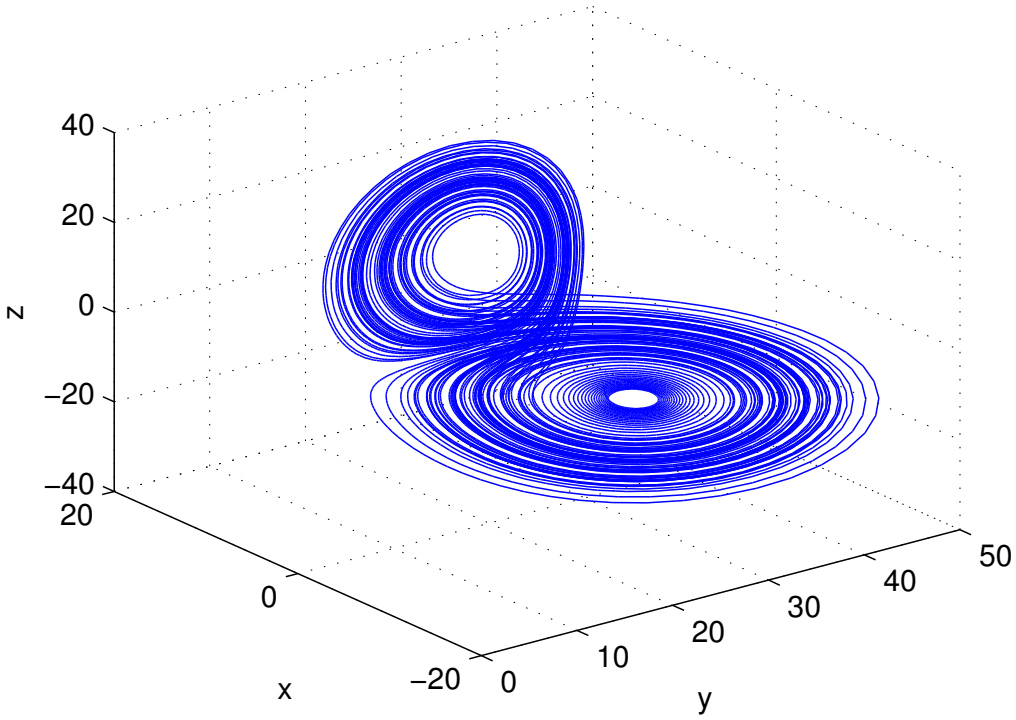


FIG. 9: Attracteur de Lorenz

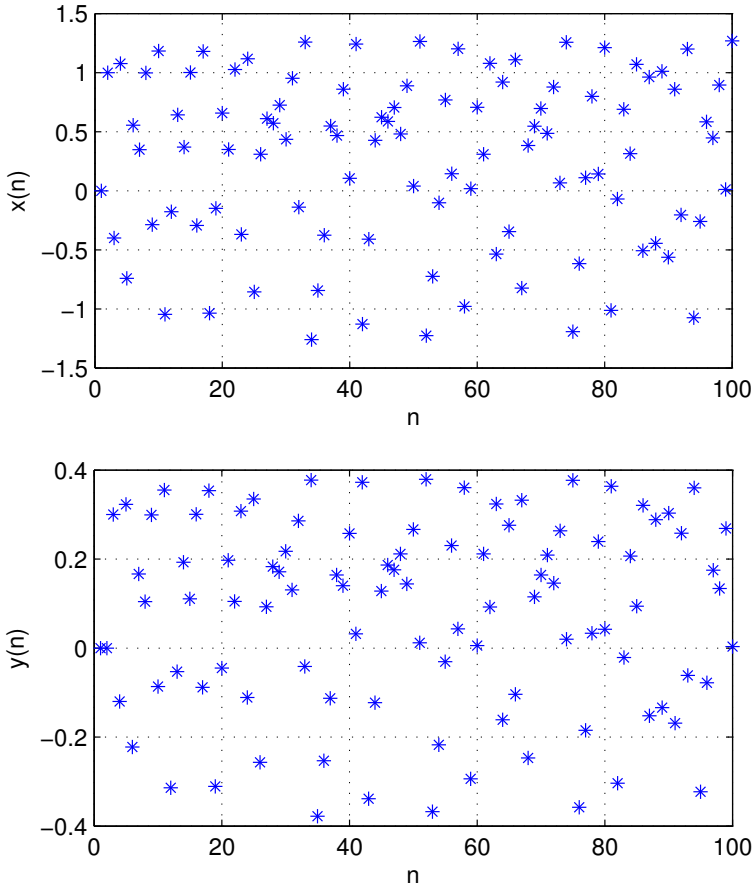


FIG. 10: Etats chaotiques du système de Hénon

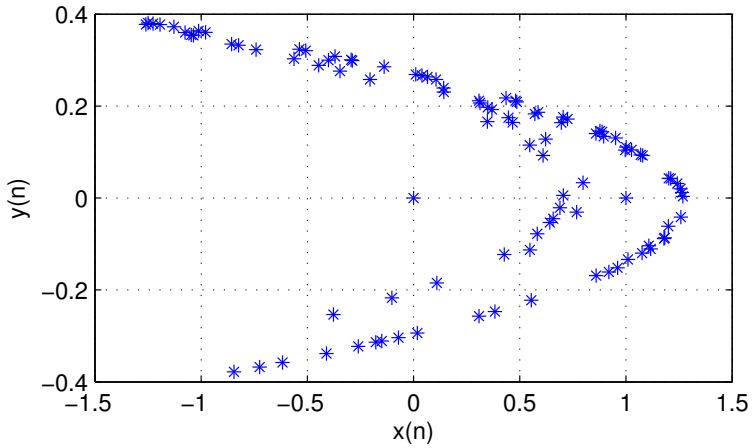


FIG. 11: Attracteur de Hénon

Annexe B
Rappels sur l'observabilité des systèmes et l'algèbre de Lie

Annexe B : Rappels sur l'observabilité et l'algèbre de Lie

.8 Observabilité des systèmes non linéaire

.8.1 Observabilité des systèmes non linéaire en temps continu

Considérons le système non linéaire donné par la forme suivante :

$$\sum \begin{cases} \dot{x}(t) = f(x) \\ y(t) = h(x) \end{cases} \tag{49}$$

Définition 37 ***(Indiscernabilité)*** *Une paire de points initiaux x^0 et x^1 est dite U-indisernable si les deux solutions $x^0(t)$ et $x^1(t)$ vérifient $x^i(0)=x^i$, $x^i(t) \in U$, et $\forall\ t \in [0,T]$:*

$$h(x^0(t)) = h(x^1(t))$$

Autrement dit, les deux états initiaux x^0 et x^1 sont U-indiscernables si les deux conditions initiales correspondantes y^0 et y^1 sont identiques. Tous les points $x^1 \in U$ qui sont U-indiscernables de x^0 sont montrés par $I(x^0, U)$.

Définition 38 ***(Observabilité)*** *Le système (49) est observable en $x^0 \in M$ si $I(x^0, M) = x^0$.*

La définition donnée ci-dessus est un concept global ; il est donc parfois nécessaire de parcourir une distance considérable pendant longtemps afin de pouvoir distinguer deux points initiaux dans M. Le concept local est alors utilisé, qui garantit que pour discerner deux points de $U \subset M$, on est pas obligé de sortir de U. Ceci pose donc une limite à l'intervalle de temps à parcourir pour distinguer deux points initiaux.

Définition 39 ***(Observabilité locale)*** *Le système (49) est localement observable en x^0 si pout tout voisinage ouvert et suffisamment petit U de x^0, $I(x^0, U) = \{x^0\}$.*

Il est clair qu'on peut poser $U = M$. Les deux définitions données ci-dessus montrent qu'un point $x^0 \in M$ peut être discerné en tout autre point dans M.

On peut affaiblir les conditions d'observabilité, en distinguant l'état x^0 seulement des points proches de celui-ci.

Définition 40 ***(Observabilité faible)*** *Le système (49) est faiblement observable en x^0, s'il existe un voisinage ouvert V de x^0 tel que $I(x^0, M) \cap V = \{x^0\}$.*

Dans un système faiblement observable, tout point x^0 peut être distingué de ses points voisins mais encore une fois cela peut prendre un intervalle de temps important. C'est pour cela qu'un concept local d'observabilité faible est défini.

Définition 41 ***(Observabilité faible locale)*** *Le système (49) est localement faiblement observable en x^0 s'il existe un voisinage ouvert V de x^0 tel que pour tout voisinage ouvert U de x^0 contenu dans V, $I(x^0, U) \cap V = \{x^0\}$. Autrement dit, le système (49)est localement faiblement observable si l'on ne peut distinguer instantanément chaque point de ses voisins.*

.8.2 Observabilité des systèmes non linéaire en temps discret

Considérons le système non linéaire donné par la forme suivante : Soit le système non linéaire à temps-discret décrit par la forme suivante :

$$\begin{cases} x_{k+1} = f(x_k, u_k) \\ y_k = h(x_k) \end{cases} \tag{50}$$

où $x_k \in \mathbb{R}^n$, $u_k = (u_{1k}, ..., u_{mk})^T \in \mathbb{R}^m$ et $y_k \in \mathbb{R}^p$. Pour toute entrée $u_k \in \mathbb{R}^m$ constante, $f_{uk}(x_k) = f(x_k, u_k)$ est un champ de vecteur C^∞ sur $\mathbb{R}^n$ et les h_i pour $i = 1, ..., p$, les composantes de h qui sont des fonctions définies de C^∞ de $\mathbb{R}^n$ sur $\mathbb{R}$. On définit la séquence de commande sur un horizon de taille N.

$$U_{[k,k+N-1]} = \begin{pmatrix} u_k \\ u_{k+1} \\ \vdots \\ u_{k+N-1} \end{pmatrix} \in \mathbb{R} \times \mathbb{N} \tag{51}$$

Soit $\chi_{U_{[0,k-1]}}(k, 0, x_0)$ la solution à l'instant $k \geq 0$ du système (50) soumis à la commande $U_{[0,k-1]}$ et issue de la condition initiale x_0 à l'instant $k = 0$.

Définition 42 ***(Discernabilité)*** *Deux états initiaux distincts x_0 et $\bar{x}_0 \in \mathbb{R}^n$ sont dits U discernables si, pour tout $k \in \mathbb{N}$ et toute séquence d'entrées admissibles $U_{[0,k-1]}$, les trajectoires $h(\chi_{U_{[0,k-1]}}(k,0,x_0))$ et $h(\chi_{U_{[0,k-1]}}(k,0,\bar{x}_0))$ sont différentes sur leur domaine de définition commun. Dans ce cas, on dit que $U_{[0,k-1]}$ distingue les points x_0 et $\bar{x}_0$. Le système non linéaire (50) est dit observable en $x_0 \in \mathbb{R}^n$, si l'ensemble des états indiscernables de x_0 ne contient que x_0.*

Nous remarquons que la définition précédente requiert un test infini qui est irréalisable en pratique. Il semble alors intéressant d'introduire le concept N-observabilité forte.

Définition 43 ***(N-observabilité forte)*** *Le système non linéaire (50) est dit N-fortement observable ou N-observable en temps fini en $x_0 \in \mathbb{R}^n$ si, pour tout $k = 0, ..., N$ et toute séquence d'entrées admissibles $U_{[0,k-1]}, h(\chi_{U_{[0,k-1]}}(k,0,x_0)) = h(\chi_{U_{[0,k-1]}}(k,0,\bar{x}_0))$, $\bar{x}_0 \in \mathbb{R}^n$, implique $x_0 = \bar{x}_0$. Dans ce cas, on dit que $U_{[0,k-1]}$ est une entrée universelle pour (50) sur $[0, N-1]$.*

Le système non linéaire (50) est dit N-localement fortement observable en $x_0 \in \mathbb{R}^n$ s'il existe un voisinage ν_{x_0} de x_0 tel que pour tout $\bar{x}_0 \in \nu_{x_0}$, pour tout $k = 0, ..., N$ et toute séquence d'entrées admissibles $U_{[0,k-1]}, h(\chi_{U_{[0,k-1]}}(k,0,x_0)) = h(\chi_{U_{[0,k-1]}}(k,0,\bar{x}_0))$, implique $x_0 = \bar{x}_0$.

Si ces propriérés sont vraies pour tout $x_0 \in \mathbb{R}^n$, le système (50) est dit (N-localement)N-fortement observable.

Une condition d'observabilité plus forte, la N-observabilité en temps fini peut être également définie.

Définition 44 ***(Observabilité uniforme)*** *Le système non linéaire (50) est dit N-uniformément observable en $x_0 \in \mathbb{R}^n$ si, pour tout $\bar{x}_0 \in \mathbb{R}^n$, pour tout $k = 0, ..., N$ et toute séquence d'entrées admissibles $U_{[0,k-1]}$, il existe un entier $N \in [n-1, \infty[$ et une fonction $\alpha : \mathbb{R}^+ \to \mathbb{R}^+$ tels que :*

$$\sum_{k=0}^{N} \|h(\chi_{U_{[0,k]}}(k,0,x_0)) - h(\chi_{U_{[0,k]}}(k,0,\bar{x}_0))\| \geq \alpha(\|x_0 - \bar{x}_0\|)$$

où la fonction α est continue, croissante avec $\alpha(0) = 0$.

Le système (50) est dit N-uniformément observable s'il est pour tout $x_k \in \mathbb{R}^n$.

.9 Algèbre de Lie

Définition 45 *(Dérivée de Lie) Considérons h une fonction C^∞ de $\mathbb{R}^n$ dans R. On définit la dérivée de Lie de h dans la direction de f, notée $L_f h$, la dérivée de h le long de la courbe intégrale de f en $t = 0$:*

$$L_f h(x) = \sum_{i=1}^{n} f_i(x) \frac{\partial h}{\partial x_i(x)} \tag{52}$$

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

Définition 46 *(Crochet de Lie) On appelle crochet de Lie de deux champs de vecteurs f et g, le produit $[f, g]$ dont l'expression, dans les nouvelles coordonnées locales, est donnée par les n vecteurs suivants :*

$$\begin{aligned}[f,g](x) &= \begin{bmatrix} \frac{\partial g_1}{\partial x_1} & \cdots & \frac{\partial g_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial g_n}{\partial x_1} & \cdots & \frac{\partial g_n}{\partial x_n} \end{bmatrix} \begin{bmatrix} f_1 \\ \vdots \\ f_n \end{bmatrix} - \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \vdots & & \vdots \\ \frac{\partial f_n}{\partial x_1} & \cdots & \frac{\partial f_n}{\partial x_n} \end{bmatrix} \begin{bmatrix} g_1 \\ \vdots \\ g_n \end{bmatrix} \\ &= \frac{\partial g}{\partial x} f - \frac{\partial f}{\partial x} g \end{aligned} \tag{53}$$

On peut répéter le crochet de Lie autant de fois qu'on veut, d'où l'opérateur suivant :

$$[f, [f, \ldots\ldots, [f, g]]] = ad_f^k g(x) = [f, ad_f^{k-1} g](x) \quad pour k \geq 1.$$

pour $k = 0$, on a : $ad_f^0 g(x) = g(x)$

Définition 47 *(Série exponentielle de Lie) On définit la notion de série exponentielle de Lie associée à tout champs de vecteurs analytique $f(.)$ comme suit :*

$$e^{L_f} = \sum_{p \geq 0} \frac{1}{p!} = 1 + L_f + \frac{1}{2!} L_f^2 +, \ldots, + \frac{1}{p!} L_f^p +, ..., \tag{54}$$

où : L_f^p représente l'itéré p fois de l'opérateur L_f

Annexe C

Rappels d'algèbre

Annexe C : Rappels d'algèbre

Cette partie contient les définitions d'algèbre nécessaire pour décrire les approches d'élimination de variables utilisées dans le chapitre 5. L'approche par les bases de Gröbner, l'approche basée sur l'ensemble caractéristique et celle basée sur le résultant de deux polynômes.

.10 Bases de Gröbner

Définition 48 *Un anneau est un triplet $\mathbb{A}, +, \times$ tel que :*

- *$\mathbb{A}$ est un ensemble.*
- *$+$ est une loi de composition interne associative qui admet un élément neutre et un inverse ($(\mathbb{A}, +)$ est un groupe commutatif).*
- *$\times$ est une loi de composition interne associative et distributive par rapport à $+$.*

Définition 49 *Un idéal de polynômes est un sous ensemble I de $\mathbb{A}$, tel que :*

- *$\forall r \in I$, $\forall q \in I$, $r + q \in I$,*
- *$\forall r \in I$, $\forall q \in \mathbb{A}$, $r \times q \in I$,*

Définition 50 *Un ordre lexicographique des variables $x_1(k)$,...,$x_n(k)$, noté $<$, est un ordre total portant sur le non des variables et de leurs itérés, tel que $\forall i = 1, ..., n$, $\forall j = 1, ..., n$:*

$$-x_i(k) < x_i(k+l), \forall \;\; l \in \mathbb{N} - x_i(k) < x_j(l) \Rightarrow x_i(k+t) < x_j(l+t), \forall \;\; l \in \mathbb{N}, \forall \;\; t \in \mathbb{N} - x_i(k) < x_j(k)$$

Il existe plusieurs ordres lexicographiques différents. En fait, il existe un différent pour chaque permutation de variables dans l'ordre.

Définition 51 *Soient $p, q \in \mathbb{A}$. Notons $\alpha = [\alpha_1, ..., \alpha_n]$ le degré algébrique maximum de la variable $x(k) = [x_1(k), ..., x_n(k)]^T$ du polynôme p, $\beta = [\beta_1, ..., \beta_n]$ le degré algébrique maximum de la variable $x(k)$ du polynôme q et $\gamma = \min(\alpha, \beta)$. Le S-polynôme de p et q, noté $S(p, q)$, est défini par :*

$$S(p, q) = lc(q)(x(k))^{\beta-\gamma} p - lc(p)(x(k))^{\alpha-\gamma} q \tag{56}$$

où $lc(p)$ et $lc(q)$ représentent les coefficients des termes de tête de p et q respectivement.

Définition 52 *soit un ordre fixé. Soient G un ensemble de polynômes de $\mathbb{A}$ et I l'idéal que G engendre les conditions suivantes sont équivalentes :*

1. *Tout polynôme de A admet une unique forme normale par G.*
2. *Tout polynôme de I admet zéro pour forme normale par G.*
3. *Tout S-polynôme $S(p,q)$ $(\forall p \in G, \ \forall q \in G)$ admet zéro pour forme normale par G.*
4. *L'ensemble g est une base de Gröbner de I.*

La définition précédente signifie qu'une base de Gröbner G d'un idéal I est un système de réécriture qui permet de réécrire tout polynôme de $\mathbb{A}$ en un unique polynôme et qui permet de réécrire tout polynôme de I en zéro.

.11 Ensemble caractéristique

Définition 53 *Un polynôme q_i est dit réduit par rapport au polynôme q_j si q_i ne contient ni le terme de tête de q_j avec un degré algébrique plus grand ou égal que celui du terme de tête de q_j, ni ces itérés. Un ensemble de polynômes $q = \{q_1, ..., q_i\}$ qui sont tous réduits les uns par rapport aux autres, est appelé ensemble autoréduit.*

Définition 54 *Deux ensembles autoréduits $q = \{q_1, ..., q_i\}$ et $r = \{r_1, ..., r_o\}$ sont dits ordonnés en ordre croissant par rapport à leurs termes de tête, tels que $q_1 < q_2 < ...q_i$ et $r_1 < r_2 < ...r_o$, s'ils vérifient les conditions suivantes :*

- *S'il existe un entier l, $l \leq \min(i, o)$, tel que ordre(q_j)=ordre(r_j), $j = 1, ..., l-1$, ordre(q_l)<ordre(r_l), alors l'ensemble q est d'ordre inférieur à l'ensemble r.*
- *Si $i < o$ et ordre(q_j)=ordre(r_j), $j = 1, ..., i$, alors q est aussi d'ordre inférieur à l'ensemble r.*

Exemple 13 *Considérons les ensembles de polynômes $q = q_1, q_2$ et $r = r_1, r_2, r_3$, avec respectivement :*

$$\begin{cases} q_1 = x_1(k+2) - \theta_1(1 - x_1(k+1))x_1(k) = 0 \\ q_2 = x_1(k) - x_2(k) = 0 \end{cases} \tag{57}$$

$$\begin{cases} r_1 = x_1(k+2) - \theta_2(x_1(k+1))^2 - x_1(k) = 0 \\ r_2 = x_1(k) - (x_2(k))^2 = 0 \\ r_3 = x_1(k+1) - \theta_3(x_1(k))^2 - x_3(k) = 0 \end{cases} \tag{58}$$

Considérons l'ordre lexicographique $x_1(k) < x_2(k) < x_3(k)$. Le terme de tête de q_1 est $x_1(k+1)$ et celui de q_2 est $x_2(k)$. Ces termes de tête ont tous deux un ordre algébrique de 1. Le terme de tête de q_1 n'apparaît pas dans q_2 avec un degré égal ou supérieur. Par conséquent, q_1, est réduit par rapport à q_2. D'autre part, le terme de tête de q_2 n'apparaît pas dans q_1. Par conséquent, q_2, est réduit par rapport à q_1. L'ensemble q est autoréduit.

Le terme de tête de r_1 est $x_1(k+2)$, celui de r_2 est $(x_2(k))^2$ et celui de r_3 est $x_3(k)$. Aucun des trois termes de tête n'apparaît avec un degré égal ou supérieur dans r_1, r_2 et r_3. Par conséquent, les trois polynômes sont réduits les uns par rapport aux autres et l'ensemble r est dit autoréduit.

q_1 et r_1 ont le même terme de tête. Par conséquent, ordre*(q_1)=*ordre*(r_1). Par ailleurs, d'après l'ordre lexicographique choisi, le terme de tête de r_2 a un plus grand ordre que celui de q_2. En effet, $x_2(k)$ a un ordre algébrique égal à 1, alors $(x_2(k))^2$ a un ordre algébrique de 2. Par conséquent, ordre (q_2)=ordre (r_2). D'après la définition 54, la relation d'ordre entre les paramètres q et r est ordre $(q)<$ ordre (r)*

Définition 55 *Un ensemble de polynômes autoréduit d'ordre inférieur est appelé ensemble caractéristique*

.12 Résultant de deux polynômes

Pour expliquer le principe de l'élimination basée sur le résultant de polynômes, quelques définitions s'avèrent nécessaires et sont détaillés dans [5].

Définition 56 *Le déterminant de la matrice de Sylvester M de deux polynômes p et q est appelé le résultant de p et q, et sera noté $R(p,q)$.*

Théorème 11 *Soient deux polynômes $p = a_0 + a_1x(k) + a_2x_2(k)^2 + ...a_mx_(k)^m$ et $q = b_0 + b_1x(k) + b_2x_2(k)^2 + ...b_nx_(k)^n$. Le résultant $R(p,q)$ de p et q est nul si et seulement si les polynômes ont un zéro commun ou si $a_0 = b_0 = 0$.*

Considérons deux polynômes p et q, dépendant tous les deux de $x_1(k)$ et $x_2(k)$. Supposons que l'on souhaite éliminer la variable $x_2(k)$. Les polynômes p et q peuvent être vus comme des polynômes dépendant uniquement de la variable $x_2(k)$ et dont les coefficients sont des fonctions de $x_1(k)$, le résultant sera un polynôme dépendant uniquement de $x_1(k)$ et la

variable $x_2(k)$ sera ainsi éliminée. D'après le théorème 11, pour que les deux polynômes aient un zéro commun, le résultant doit être nul. Par conséquent, poser le résultant égal à zéro donne une équation uniquement en $x_1(k)$.

Cette approche peut être étendue à des polynômes multivariables. Dans ce cas, les variables sont éliminées les unes après les autres, selon, l'ordre lexicographique fixé, en calculant successivement les résultants.

.13 Approche basée sur l'égalité des sorties

Considérons les deux systèmes suivants :

$$\begin{cases} x(k+1) = f_\theta(x(k), m(k)) \\ y(k) = h_\theta(x(k), m(k)) \end{cases} \tag{59}$$

$$\begin{cases} x(k+1) = f_{\hat{\theta}}(x(k), m(k)) \\ y(k) = h_{\hat{\theta}}(x(k), m(k)) \end{cases} \tag{60}$$

L'approche basée sur l'égalité des sorties est directement dérivée de la Définition 17. Les trajectoires $y(k)(x(0), m(k), \theta)$ contiennent des informations sur le vecteur de paramètre θ. L'approche consiste à tester si l'égalité des trajectoires de sortie des systèmes (59) et (60) sur l'intervalle $[0 - T]$, implique l'égalité des vecteurs de paramètres θ et $\hat{\theta}$. Le théorème énonce une condition suffisante de l'identifiabilité structurelle du système (59). La condition initiale $x(0)$ et l'entrée $m(k)$ sont spécifiées dans les Définitions 15 et 16.

Théorème 12 *Le système (59) est structurellement identifiable pour presque tout $\theta \in \Theta$ si, quels que soient $x(0)$, $m(k)$, il existe $T > 0$, tel que :*

$$\{y(k)(x(0), m(k), \theta)\}_0^T = \{y(k)(x(0), m(k), \hat{\theta})\}_0^T \Rightarrow \hat{\theta} = \theta \tag{61}$$

Ce théorème porte sur l'identifiabilité globale du système. Si l'on restreint à l'identifiabilité locale, seule la considération d'un voisinage θ permet de conserver la propriété d'unicité de la solution. Par exemple, le paramètre θ_2 est localement identifiable pour $\theta \in \Theta$ et globalement identifiable dans un voisinage de θ. En effet, il existe une unique valeur pour ce paramètre, qui est $-\theta$ dans un voisinage $v_1(\theta)$ et qui est $+\theta$ dans un voisinage $v_2(\theta)$.

T est un entier positif et représente le nombre d'itérations requis pour prouver le Théorème 12. Si T tend vers l'infini, cela signifie que la relation précédente ne peut pas être prouvée. Dans ce cas, aucune conclusion sur l'identifiabilité structurelle ne peut être donnée. Comme T est inconnu a priori, Le Théorème 12 est seulement une condition suffisante d'identifiabilité structurelle.

Remarque 5 *Dans le cas des systèmes à temps continu, cette approche est fortement connectée à celle basée sur le développement en série de Taylor de la trajectoire de sortie. Pour tester leur égalité, les trajectoires de sortie $y(t)$ sont approximées par leur développement en série de Taylor. Les coefficients du développement en série de Taylor sont uniques et contiennent des informations sur les paramètres. Le principe est alors de tester si l'égalité de ces coefficients implique l'égalité des vecteurs de paramètres θ et $\hat{\theta}$.*

Définition 57 *Soient F et X deux ensembles. F est dense dans X si F est inclus dans X et si pour tout point $x \in X$, chaque voisinage de x contient au moins un point de F.*

Bibliographie

Bibliographie

[1] K. T. Alligood, T. D. Sauer and A. J. Yorke, Chaos : An introduction to dynamical systems, *Springer-verlag*, New York, 1996.

[2] G. Alvarez and S. Li, Some basic cryptographic requirements for chaos-based cryptosystems, *International Journal of Bifurcations and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[3] J. Alvarez-Ramirez, H. Puebla and I. Cervantes, Convergence rate of observer-based approach for chaotic synchronization, *Physics Letters A*, vol. 289, pp. 193–198, 2001.

[4] M. Anguelova and B. Wennberga. State elimination and identiability of the delay parameter for nonlinear time delay systems, *Automatica*, vol. 44, no. 5, pp. 1373–1378, 2008.

[5] F. Anstett, *Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse*, Thèse, Université de Henri Poincaré, Nancy1, 2006.

[6] F. Anstett, G. Millerioux and G. Bloch, Chaotic Cryptosystems : Cryptanalysis and Identifiability, *IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications*, vol. 53, December 2006.

[7] J.P. Barbot, I. Belmouhoub and L.Boutat-Baddas, Observability Bifurcations : Application to Cryptography, *In Chaos in Automatic Control, Taylor and Francis*, 2005.

[8] J.P. Barbot, I. Belmouhoub and L. Boutat-baddas, Estimation des dérivées d'un signal multidimensionnel avec applications aux images et aux vidéos, *20ème colloque sur le traitement du signal et de l'image*, GRETSI, Belgique, 2005.

[9] J.P. Barbot, M. Fliess and T. Floquet, An algebraic framework for the design of nonlinear observers with unknown input, *46 th IEEE Conference on Decision and Control CDC'07*, New Orleans, USA, 2007.

[10] J.P. Barbot, M. Djemai and T. Boukhobza, Sliding mode observers, *In sliding mode control in engineering, Maercel Dekker*, pp. 103–130, 2002.

[11] P. Barthélemy, R. Rolland and P. Véron, *Cryptographie*, Edition Hermès-Lavoisier, 2005.

[12] A. Basiliauskas, A.Tamasevicius, S. Bumeliene and E. Lindberg, Synchronization of Chaotic Colpitts Oscillator, *Scientific proceeding of Riga Technical university*, pp. 55–58, 2001.

[13] G. Bastin, M. Gevers, Stable adaptive observers for nollinear time varying systems, *IEEE Transactions on Automatic Control*, vol. 37, pp. 650–658, 1988.

[14] I. Belmouhoub, M. Djemaï and J.P. Barbot, Observability quadtatic Normal Form for Discrete-Time systems, *IEEE Transactions on Automatic Control*,vol. 50, July 2005.

[15] F. Beritelli, E. D. Cola and L. Fortuna, Multilayer chaotic encryption for secure communications in pachet switching networks, *IEEE Transactions on communication*, vol. 30, no. 4, pp. 1575–1582, 2000.

[16] G. Besançon, Remarks on nonlinear adaptive observer design, *Systems and Control Letters*, vol. 41, pp. 271–280, 2000.

[17] F. Bohme and W. Schwarz, The Chaotizer-Dechaotizer Channel, *IEEE Transactions on Circuit and Systems*, vol. 43, pp. 596–599, 1996.

[18] B. Bonnard, Controllabilité des systèmes non linéaires, *SIAM Journal Control*, vol. 8, 1970.

[19] B. Bonnard and H. Hammouri, A high gain observer for a class of uniformaly observable systems, *30 th IEEE Conference on Decision and Control CDC'91*, Brighton , UK, 1991.

[20] L. Boutat-baddas, *Analyse des singularités d'observabilité et de détectabilité : Application à la synchronisation des circuits électroniques chaotiques*, Thèse, Université de Cergy-Pontoise, 2002.

[21] M. Boutayeb, M. Darouach and H. Raparalahy, Generalized state-space observers for chaotic synchronization and secure communications, *IEEE Transactions on Circuits and Systems :Fundamantal Theory and Applications*, vol. 49, no. 3, pp. 345–349, 2002.

[22] M.S. Branicky,*Study in hybrid systems*, Ph.D. dissertation, Dept. Elec. Eng and Computer Sci., Massachusetts Inst.Technol., Cambridge, June, 1995.

[23] K. Busawon, R. W. Jones and M. D. Thom, An observer for linear time delay systems, *Proceeding Modelling Identification and Control*, pp. 34–39,2004.

[24] R.L. Carol and D.P. Lindorff, An adaptive observer for single-input single-output linear systems, *IEEE Transactions on Automatic Control*, vol. 38, pp. 428–435, 1973.

[25] T.L. Carroll and L.M. Pecora, Synchronizing chaotic circuits, *IEEE Transactions on Circuit and Systems*, vol. 38, pp. 453–456, 1991.

[26] S. Celikovsky and G. Chen, Secure synchronization of a class of chaotic systems from a nonlinear observer approach, *IEEE Transactions on Automatic Control*, vol. 50, no. 1, pp. 76–82, 2005.

[27] M. Chen, D. Zhou and Y. Shang, A new observer-based synchronization scheme for private communication, *Chaos, Solitons and Fractales*, 30, pp. 1025–1030, 2005.

[28] G. Chen and X. Dong, From chaos to order : methodologies, perspectives and applications, *World Scientific*, Singapore, 1998.

[29] G. Chen and T. Ueta, Chaos in Circuits and systems, *World Scientific, Singapore*, 2002.

[30] E. Cherrier, *Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires*, Thèse, Institut National Polytechnique de Lorraine, 2006.

[31] Y.M. Cho and R. Rajmani, A systematic approach to adaptive observer synthesis for nonlinear systems, *IEEE Transactions on Automatic Control*, vol. 42, pp. 534–537, 1997.

[32] L.O. Chua, l. Koracev, K. Eckert and M. Itoh, Experimental chaos synchronization in Chua's circuit, *International Journal of Bifurcations and Chaos*, vol. 2, pp. 705–708, 1992.

[33] J.T. Corless, State and input estimation for a class of uncertain systems, *Automatica*, vol. 37, 1998.

[34] N. Corron, D. Hahs, A new approch to communication using chaotic signals, *IEEE Transactions on Circuit and Systems*, vol. 44, pp. 373–382, 1997.

[35] K.M. Cuomo and A. V. Oppenheim, Circuit implementation of synchronized chaos with application to communications, *Physics, review and Letters*, vol. 71, pp. 65–68, 1993.

[36] K.M. Cuomo, A. V. Oppenheim and S. H. Strogatz, Synchronization of Lorenz based chaotic circuits with appllication to communications, *Physics, review and Letters*, vol. 71, pp. 65–68, 1993.

[37] K. M. Cuomo and A. V. Oppenheim, Circuit implementation of synchronized chaos with application to communications, *IEEE Transactions on Circuit and Systems*, vol. 40, pp. 626–633, 1993.

[38] M. Darouach, On the nouvel approach to the design of unknown input observers, *IEEE Transactions on Automatic Control*, vol.39, pp. 698–699, 1994.

[39] J. Daafouz and G. Millérioux, Poly-quadratic stability and global chaos synchronization of discrete time hybrid systems, Special Issue of Mathematics and Computers in Simulation, vol. 58, pp. 295–307, 2002.

[40] M. Darouach, m. Zasadzinski, S. J. Xu, Full-order observers for linear systems with unknown inputs, *IEEE Transactions on Automatic Control*, vol.39, pp. 606–609, 1994.

[41] H. Dedieu H, M.P. Kennedy and M. Hasler, Newblock Chaos shift keying : modulation and demodulation of a chaoticcarrier using self-synchronizing Chua's circuits, *IEEE Transactions on Circuits and Systems, Circuits and Systems II : Analog and Digital Signal Processing*, vol. 40, pp. 634–642, 1993.

[42] H. Delfs and H. Knebl, *Introduction to cryptography*, Springer verlag, Berlin, 2002.

[43] M. Djemaï, J.P. Barbot and I. Belmouhoub, Discrete-Time Normal Form for Left Invertibility Problem, *European Journal of Control*, vol. 15, pp. 194–204, 2009.

[44] S. Diop, J. W. Grizzle, P. E. Normal and S. Ibrir, On numerical observers : application to a simple academic adaptive control example, *Procedding European Control conference*, 1997.

[45] S. Diop and M. Fliess, Nonlinear observability, identifiability and persistent trajectory, *Procedding of 30th Conference on Decision and Control*, pp. 714–718, 1991.

[46] A.S Dmitriev, G.A Kassian and A.D Khilinsky, Chaotic synchronization of henon mappings : The information approach, *Technical Physics Letters*, vol. 51, May 2002.

[47] M. Feki, Observer-based chaotic synchronization in the presence of unknown inputs, *Chaos, Solitons and Fractals*, vol. 15, pp. 831–840, 2003.

[48] U. Feldmann, M. Hasler and W. Shwarz, Communications par chaotic signals : the inverse system approach, *International Journal of Circuit : Theory ans Applications*, vol. 24, pp. 551–579, 1996.

[49] M. Fliess, Quelques remarques sur les observateurs non linéaires,*11ème colloque sur le traitement du signal et de l'image*, GRETSI,Nice, 1987.

[50] M. Fliess, C. Join, M. Mboup and A. Sedoglavic, Estimation des dérivées d'un signal multidimensionnel avec applications aux images et aux vidéos, *20ème colloque sur le traitement du signal et de l'image*, GRETSI, Belgique, 2005.

[51] T. Floquet and J.P. Barbot, A sliding mode approach of unknown input observers for linear systems, *43 th IEEE Conference on Decision and Control, CDC' 04*, Atlantis, Paradis, Island, Bahamas, 2004.

[52] A. Fradkov, A.Y. Pogromsky, Introduction to control of oscillations and chaos, *World scientific, Singapore, Series A*, vol. 35, 1998.

[53] A. Fradkov, H. Nijmeijer and A. Markov, Adaptive observer-based synchronization for communication, *International Journal of Bifurcations and Chaos*, pp. 2807–2813, 2000.

[54] G.C. Freeland and T.S Durrani, Nonlinear state observers for chaotic systems and their application to communications signal process, *Exploiting Chaos in Signal Processing, IEE Colloquium on*, 1994.

[55] E. Fridman, Stability of systems with uncertain delays : a new 'complete' lyapunov-krasovskii functional, *IEEE Transactions on Automatic Control*, vol. 51, pp. 885–890, 2006.

[56] J.P. Gauthier, H. Hammouri and S. Othman, A simple observer for nonlinear systems : application to bioreactors, *IEEE Transactions on Automatic Control*, vol. 37, pp. 875–880, 2001.

[57] M.Ghanes, G. Zheng and J. De Leon, On simultaneous parameter identification and state estimation for cascade state affine systems, *American Control Conference ACC' 08*, Seattle, Washington, USA, pp. 11-13 June, 2008.

[58] M. Ghanes, J.DeLeon, A. Glumineau and J.P. Barbot, A robust output feedback controller of the induction motor drives : new design and experimental validation, *IEEE International Journal of control*, vol. 83, pp. 484–497, 2010.

[59] J.M. Gonzalez-Miranda, Synchronization and control of chaos : An introduction for scientist and engineers, *Imperial college Press*, 2004.

[60] Z.H. Guan, D.J. Hill, X. Shen and X. YU, Synchronization of chaotic systems via hybrid impulsive and switching control, *5 th Control Conference*, China, 2005.

[61] M. Haeri and B. Khademian, Comparison between different synchronization methods of identical chaotic systems, *Chaos, Solitons and Fractals*, vol. 29, no. 4, pp. 1002–1022, 2006.

[62] H.Hamiche, M. Ghanes, J.P Barbot and S. Djennoune, Systèmes dynamiques hybrides pour les communications privées, *Conférence Internationale de Francofonie en Automatique, CIFA'10*, Nancy, France, 2010.

[63] H. Hamiche, M. Ghanes, J.P Barbot and S. Djennoune, Secure Digital Communication based on Hybrid Dynamical Systems, *Communication systems, Networks and Digital Processing, CSNDSP'10*, Newcastle, U.K, 2010.

[64] H. Hamiche, M. Ghanes, J.P Barbot and S. Djennoune, Secure Digital Communication based on Hybrid Dynamical Systems, *Nonlinear Analysis : Hybrid Systems* (révision).

[65] H. Hamiche, K. Kemih, M. Ghanes, G. Zhang and S. Djennoune, Passive and impulsive synchronization of a new four-dimensional chaotic system, *Nonlinear Analysis : Theory, Methods, Applications*, vol. 74, no. 4 pp. 1146–1154, 2011.

[66] H. Hamiche, M. Ghanes, J-P Barbot and S. Djennoune, Transmission sécurisée à base de la dynamique chaotique hybride, *Conférence sur le Génie Electrique, CGE'07*, Alger, Algérie, 2011.

[67] H. Hamiche, F. Almansba, S. Guermah, S. Djennoune and M. Bettayeb, Commande par retour d'état adaptatif : application au circuit de Chua, *Conférence sur le Génie Electrique, CGE'05*, Alger, Algérie, 2007.

[68] M. Hasler, Synchronization of chaotic systems and transmission of information, *International Journal of Bifurcations and Chaos*, vol. 8, pp. 657–659, 1998.

[69] G. Heidari-Bateni and C. C. McGillem, A chaotic direct-sequence spread-spectrum communication system, *IEEE Transactions on communication*, vol. 42, pp. 1524-1527, 1994.

[70] R. Hermann and A. Krener, Nonlinear controllability and observability, *IEEE Transactions on Automatic Control*, vol. 22, pp. 728–740, 1977.

[71] M. L'Hernault, J.P. Barbot and A. Ouslimani, Feasability of Analogue Realization of Sliding Mode Observer : Application to Data Transmission, *IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications*, vol. 55, March 2008.

[72] M. L'Hernault, *Feasabilité d'un système d'émission-réception analogique pour les communications sécurisées par le chaos*, Thèse, Université de Cergy Pontoise, 2007.

[73] J. Hervé, *Electronique pour les transmissions numériques*, Edition ellipses, 1993.

[74] R. C. Hilborn, *Chaos and nonlinear dynamics : An introduction for scientists and engineers*, Oxford University Press, New York, 2000.

[75] N.H. Huijberts, H. Nijmeijer and R. Willems, System identification in communication with chaotic system, *IEEE Transactions on Circuits and Systems-I*, vol. 47, pp. 800–808, 2000.

[76] G.P. Jiang, G. Chen and W.K.S. Tang, A new criterion for chaos synchronization using linear state feeback control, *International Journal of Bifurcation and Chaos*, vol. 13, no.8, pp. 2343–2351, 2003.

[77] G.P. Jiang and W.X. Zheng, An LMI criterion for linear-state-feeback based chaos synchronization of a class of chaotic systems, *Chaos, Solitons and Fractals*, vol. 26, pp. 437–443, 2005.

[78] J.K. John and R.E. Amritkor, Synchronization of feedback and adaptive control, *International Journal of Bifurcations and Chaos*, vol. 4, pp. 1687–1695, 1994.

[79] R.E. Kalman, A new approach to linear filtering and prediction problems, *Transactions. ASME, Journal Basic Engineering*, vol. 82, pp. 34–35, 1960.

[80] K. Kemih, A. Kemiha and M. Ghanes, Chaotic attitude control of satellite using impulsive control, *Chaos, Solitons and Fractals*, vol. 42, no. 2, pp. 735–734, 2009.

[81] K. Kemih, Passivity-based control of chaotic Lü system, *International Journal of Innovative Computing, Information and Control*, vol. 2, no. 2, pp.331–337, 2006.

[82] K. Kemih, M. Benselama, S. Filali, W. Y. Lü and , H. Baudrand, Synchronization of Chen System Based on Passivity Technique for CDMA Underwater Communication, *International Journal of Innovative Computing, Information And Control*, vol. 3, no. 5, pp. 1301–1308, 2007.

[83] M. P. Kennedy, R. Rovati and G. Setti, Chaotic electronics in telecommunications, *CRC Press*, 2000.

[84] A. Kerchoff, La cryptographie militaire, *Journal des sciences militaires*, pp. 5–83, 1883.

[85] A. Khadra, X.Z. Liu and X. Chen, Analysing robustness of impulsive synchronization coupled by delayed impulses, *IEEE Transactions on Automatic and control*, vol. 54, no. 4, pp. 923–928, 2009.

[86] G. Kolumban, M.P. Kennedy and L.O. Chua, The role of synchronization in digital communication using chaos.PartII :chaotic modulation and chaotic synchronization, *IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications*, vol. 11, pp. 1129–1140, 1998.

[87] L. Koracev, Chaos-based cryptography : a brief overview, *IEEE Transactions on Circuits and Systems*, pp. 6–21, July 2001.

[88] L. Koracev, K. S. Halle, K. Eckert, L. O. Chua and U. Parlitz, Experimental demonstration of secure communication via chaotic synchronization, *International Journal of Bifurcations and Chaos*, vol. 2, pp. 709–713, July 1992.

[89] L. Koracev and U. Parlitz, General approach for chaotic synchronization with application to communication, *Physics, Review and Letters*, vol. 76, July 1996.

[90] L. Koracev, A. Shang and L.O. Chua, Transitions in dynamical regimes by driving : a unified method of control and synchronization of chaos, *International Journal of Bifurcations and Chaos*, vol. 2, pp. 479–483, 1993.

[91] L. Koracev and U. Parlitz, Generalized synchronization, predictability and equivalence of unidirectionnaly coupled dynamical systems, *Physics, Review and Letters*, vol. 76, 1996.

[92] G. Kreisselmeier, Adaptive observer with exponential rate of convergence, *IEEE Transactions on Automatic and Control*, vol. 22,pp. 2–8, 1977.

[93] A.J. Krener and A. Isidori, Linearisation by output injection and nonlinear observers, *Systems and Control Letters*, vol. 3, pp. 47–52, 1983.

[94] V. Lakshmikantham, D.D. bainov and P.S. Simeonov, Theory of impulsive diffrential equations, *World Scientific*, Singapore, 1989.

[95] A. Leuciuc, Information transmission using chatic discrete-time filter, *IEEE Transactions on Circuit and Systems*, vol. 47, pp. 82–88, 2000.

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

[97] T. L. Liao, Adaptive synchronization of two Lorenz systems, *Chaos, Solitons and Fractals*, vol. 9, no. 9, pp. 1555–1561, 1998.

[98] D. Liberzon, *Switching in Systems and Control*, Systems and Control : Foundations and Applications, A Birkhauser, 2003.

[99] X.Z. Liu, Impulsive synchronization of chaotic systems subject to time delay, *Nonlinear Analysis : Theory, Methods and Applications*, vol. 11, no. 72, pp. 1320–1327, 2009.

[100] W. Liu and G. Chen, A new chaotic system and its generation, *International Journal of Bifurcation and Chaos*, vol. 13, no. 1, pp. 261–267, 2003.

[101] L. Ljung, System identification : *Theory for the user-Cased*, Prentice Hall, 2nd edition, 1999.

[102] L. Ljung and L. Glad, On global identifiability for arbitrary model parametrizations, *IEEE Automatica*, vol. 30, no. 2, pp. 265–276, 2004.

[103] Y. Liu and P. Davis, Dual synchronization of chaos, *Pysics Review E*, vol. 61, pp. 2176–2179, 2000.

[104] R. Loxton, Teo, K.L., V. Rehbock, An optimization approach to state-delay identification, *IEEE Transactions on Automatic Control*, Vol. 55, N. 9, 2010.

[105] G.M. Maggio and O.D. Feo, Nonlinear Analysis of the Colpitts Oscillator and Application to Design, *IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications*, vol. 49, September 1999.

[106] J. Lü and G. Chen, A new chaotic attractor coined, *International Journal of Bifurcation and Chaos*, vol. 12, no. 3, pp. 659–661, 2002.

[107] J. Lü, G. Chen, D. Cheng and S. Celikovsky, Bridge the gap between the lorenz system and the chen system, *International Journal of Bifurcation and Chaos*, vol. 12, no. 12, pp. 2917–2926, 2003.

[108] J. Lü and J. Lu, Controlling incertain Lü system using linear feedback, *Chaos, Solitons and Fractals*, vol. 17, pp. 127–133, 2003.

[109] G.M Maggio and M.P. Kennedy, Experimental manifestations of chaos in the Colpitts oscillator, Proceeding of ICECS, Seville, spain, pp. 194–204, 1997.

[110] A. Menezes, P. V. Oorschot and S. Vanstone,*Handbook of applied cryptography*, CRC Press, 1996.

[111] G. Millérioux and J. Daafouz, An observer-based approach for input independent global chaos synchronization of discrete-time switched systems, *IEEE Transactions on Circuits and Systems I : Fundamental Theory and Applications*, vol. 10, 2003.

[112] G. Millérioux and J. Daafouz, Unknown input observers for message-embedded chaos synchronization of discrete-time systems, *International Journal of Bifurcations and Chaos*, vol. 14, no. 4 pp. 1357–1368, 2004.

[113] T. Mullin, *The nature of chaos*, Oxford University Press, New York, 1993.

[114] H. Nijmeijer, On Synchronization of Chaotic Systems, *IEEE 36th Conference on Decision and Control CDC' 97*, San Diego, California USA, December 1997.

[115] H. Nijmeijer and Iven M.Y Mareels, An observer Looks at Synchronization, *IEEE Transactions on Circuits and Systems : Fundamantal Theory and Applications*, vol. 44, October 1997.

[116] C. Noiret, *Utilisation du calcul formel pour l'identifiablité de modèles paramètriques et nouveaux algorithmes en estimation des paramètres*, Thèse de doctorat, Université de Technologie de Compiègne, 2000.

[117] S. Nomm and Iven C. H Moog, Identifiability of discrete-time nonlinear systems, *Proceeding of the 6 th IFAC Symposium on Nonlinear Control Systems*, pp. 477–489, Stuttgart, Germany, 2004.

[118] J.M. Ogoraztex, Chaos and complexity in nonlinear electronic circuit, *World Scientific*, Singapore, Series A, vol. 22, 1997.

[119] A. V. Oppenheim, G. W. Wornelli, S. H. Isabelle and K. M. Cuomo, Signal processing in the context of chaotic signals, *IEEE This paper appears in : International*

Conference of Acoustics, Speech, and Signal Processing ICASSP' 92, San Francisco, USA, pp. 117–120, 1992.

[120] E. Ott, T. Sauer and J. A. Yorke, *Coping with chaos : Analysis of chaotic data and exploitation of chaotic systems*, Wiley-Interscience, NY, 1994.

[121] E. Ott, C. Grebogi and J. A. Yorke, Controlling chaos, *Physical Review Letters*, vol. 64, pp. 1196–1199, 1990.

[122] A.I. Panas, T. Yang and L. O. Chua, Experimental results of impulsive synchronization between two chua's circuits, *International Journal of Bifurcations and Chaos*, vol. 8, pp. 639–644, 1998.

[123] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle and A. Shang, Transmission of digital signals by chaotic synchronization, *International Journal of Bifurcations and Chaos*, vol. 3, pp. 973–977, 1993.

[124] U. Parlitz, L. Kocarev, T. Stojanovski and H. Prekel, Encoding message using chaotic synchronization, *Physics, review and Letters*, vol. 53, pp. 4351–4361, 1992.

[125] T.S. Parker and L. O. Chua, Chaos : A tutorial for engineers, *Proceeding IEEE*, vol. 75, pp. 982–4361, 1008, 1987.

[126] L.M. Pecora and T.L. Carroll, Synchronization in Chaotic Systems, *Physicals Review and Letters*, pp. 821–824, 1990.

[127] L.M. Pecora and T.L. Carroll, Synchronized Chaotic signal and systems, *Proceeding IEEE Internatioanl conference of Acoustics, Speech, and Signal ICASSP' 92*, Minneapolis, MN, USA, pp. 137–140, 1992.

[128] L.M. Pecora and T.L. Carroll, Synchronizing chaotique circuits, *IEEE Transactions on Circuit and Systems*, vol. 38, pp. 453–456, 1991.

[129] W. Perruquetti and J.P. Barbot, *Chaos in a Automatic Control*, Taylor and Francis, 2005.

[130] R. L. Peterson, R. E. Ziemer and D. F. Borth, Introduction to spread spectrum communications, *Prentice Hall*, Englewood Cliffs, 1995.

[131] K. Pyragas, Weak and strong synchronization of chaos, *Physicals Review and Letters*, vol. 54, pp. 4508–4511, 1996.

[132] G. Qi, S. Du, G. Chen, Z. Chen and Z. Yuan, On a four-dimensional chaotic system, *Chaos, Solitons and Fractals*, Vol. 23, pp. 1671–1682, 2005.

[133] G. Qi and G. Chen, Analysis and circuit implementation of a new 4D chaotic system, *Physics Letters A*, vol. 352, no. 4-5, pp. 386–397, 2006.

[134] J.P. Richard, Time-delay systems : an overview of some recent advances and open problems, *Automatica*, vol. 39, no. 10, pp. 1667–1694, 2003.

[135] V. Rubezic and R. Ostojic, Synchronization of Colpitts oscillator with application to binary communications, *IEEE Transactions on Circuit and Systems*, 1999.

[136] N.F. Rulkov, M. M. Sushchic, L. S. Tsimring and H. D. I. Abarbanel, Generalized Synchronization of Chaos in directinally coupled chaotic systems, *Physicals Review and Letters*, vol. 51, 1995.

[137] S. S. Sastry, *Nonlinear systems : Analysis, Stability and Control*, Spriger-Verlag, New York, 1999.

[138] Y. Shimizu, M. Miyazaki and H.H. Lee, Chaos synchronization based on fuzzy model using sliding mode control, *International Journal of Innovative Computing Information and Control*, vol. 1, no. 3, pp.563–579, 2005.

[139] B Schneier, *Applied cryptography*, John Wiley and Sons, 1996.

[140] K.M. Short, Steps toward unmasking secure communications, *International Journal of Bifurcations and Chaos*, vol. 4, pp. 955–977, 1994.

[141] K.M. Short, Unmasking a modulated chaotic communications scheme, *International Journal of Bifurcations and Chaos*, vol. 6, pp. 367–375, 1996.

[142] H. Sira-Ramirez, C.A. Ibanez and M. Suarez-Castanon, Exact state reconstructors in the recovery of messages encrypted by the states of nonlinear discrete-time chaotic systems, *International Journal of Bifurcations and Chaos*, vol. 12, pp. 169–177, 2002.

[143] I. Souleiman, A. Glumineau and G. Schreier, Direct transformation of nonlinear systems into state affine MISO form and nonlinear observer design, *IEEE Transactions on Automatic and Control*, vol. 48, pp. 2191–2196, 2003.

[144] S.H. Storgatz, Nonlinear dynamics ans chaos, *Addison-Wesley*, 1995.

[145] H.G. Sussman and V.J. Jurdjevic, Controllability of nonlinear systems, *Journal Differential Equations*, vol. 12, pp. 95–116, 1972.

[146] X.H. Tan, J.Y. Zhang and Y.R. Yang, Synchronization chaotic systems using backstepping design, *Chaos, Solitons and Fractals*, vol. 16, no. 1, pp. 37–45, 2003.

[147] Y.S. Tang, A.I. Mess and L.O. Chua, Synchronization and chaos, *IEEE Transactions on Circuit and Systems*, vol. 30, pp. 1–2, 1983.

[148] G. S. Vernam, Cipher printing telegraph systems for secret wire and telegraphic communications, *Journal of the American Institute of Electrical Engineers*, vol. 55, pp. 109–115, 1926.

[149] K. Vesely and J. Podolsky, Chaos in a modified Henon- Heiles system describing geodesics in gravitational waves, *Technical Physics Letters A*, vol. 271, pp 368–371, July 2000.

[150] U.E. Vincent, Synchronization of identical and non-identical 4-D chaotic systems using active control, *Chaos, Solitons and Fractals*, vol. 37, no. 4, pp. 1065–1075, 2008.

[151] E. Walter and L. Pronzato, Identification of parametric models for experimental data, *Springer-Verlag*, 1997.

[152] C. Wegener and M. Kennedy, RF chaotic colpitts oscillator, *Proceeding of NDES*, pp. 255–258, July 1995.

[153] C.W. Wu and L.O. Chua, Simple way to synchronize chaotic systems with applications to secure communications systems, *International Journal of Bifurcations and Chaos*, vol. 3, pp. 1619–1627, 1993.

[154] J. Yan and C. Li, Generalized projective synchronization of a unified chaotic system, *Chaos, Solitons and Fractals*, vol. 26, pp. 1119–1124 2005.

[155] T. Yang, A survy of chaotic secure communications systems, *International Journal of Computational cognition*, vol. 2, pp. 81–130, 2004.

[156] T. Yang, L.B. Yang and C.M. Yang, Breaking chaotic switching using generalized synchronization : Examples, *IEEE Transactions on Circuits and Systems-I : Fundamenatal Theory and Applications*, vol. 45, no. 10, pp. 1062–1067, 1998.

[157] T. Yang and L.O. Chua, Impulsive stabilization for control and synchronization of chaotic systems : theory and application to secure communication, *IEEE Transactions on Circuits and Systems-I : Fundamenatal Theory and Applications*, vol. 44, n°10, pp. 976–978, 1997.

[158] T. Yang, Recovery of digital signals from chaotic switching, *International Journal of Circuit Theory and applications*, vol. 2, pp. 611–615, 1995.

[159] T. Yang, L.B. Yang and C.M. Yang, Cryptanalysing chaotic secure communications using return maps, *Physics letters A*, vol. 245, pp. 495–510, 1998.

[160] W. Yu, Passive equivalence of chaos in Lorenz system, *IEEE Transaction on Circuits and Systems-1 :Fundamental Theory and Applications*, vol. 46, no. 7, pp. 876–878, 1999.

[161] J. Zayton,*Systèmes dynamiques hybrides*, Edition Hermés, Paris, 2001.

[162] G. Zhang , S.J. Li and D.X. Zhang, Chaos synchronization based on Phase-Locked Loops, *2th International Conference on Future Generation Communication and Networking*, pp. 283–287, 2008.

[163] Q. J. Zhang and J. A. Lu, Passive control and synchronization of hyperchaotic Chen system, *Chinese Physics B*, vol. 17, no. 2, 2008.

[164] J. Zhang, X. Xia, and C.H. Moog, Parameter identifiability of nonlinear systems with time-delay, *IEEE Transactions on Automatic Control*, vol. 47, pp. 371–375, 2006.

[165] G. Zheng, D. Boutat, T. Floquet and J.P. Barbot, Secure data transmission based on multi-input multi-output delayed chaotic system, *International Journal of Bifurcations and Chaos*, vol. 18, 2007.

[166] G. Zheng, J P Barbot, D. Boutat, T. Floquet, J P Richard, Causal observability of nonlinear time- delay systems with unknown inputs, *49th IEEE Conference on Decision and Control CDC'10*, 2010.

[167] C.S. Zhou and T.L, Chen, Extracting information masked by chaos and contaminated with noise : some considerations on the security of communication approaches using chaos, Physics Letters A, no. 234, vol. 429–435, 1997.

Résumé : Dans ce travail, la méthode d'inversion à gauche des systèmes dynamiques hybrides sera étudiée et appliquée sur un système de transmission sécurisée de données . Ici, un système de transmission à base des dynamiques chaotiques hybrides retardées pour des communications privées est proposé. L'émetteur est composé d'un système chaotique à temps continu et d'un système chaotique à temps discret dans lequel le message est inséré par la méthode d'inclusion. Dans le but de complexifier la structure de cet émetteur, ce qui est souhaitable dans le cas de la cryptographie, un couplage entre les deux types de systèmes est réalisé. Le système dynamique obtenu est alors de nature hybride, en raison de l'introduction des états échantillonnés du système à temps continu dans la dynamique du système à temps discret. Le récepteur est composé d'un observateur à temps continu et d'un observateur à temps discret. Le principe de la méthode hybride proposée est de montrer que la reconstruction des états discrets ainsi que le message du récepteur passe d'abord par la synchronisation des deux systèmes chaotiques à temps continu. Pour augmenter la robustesse de la transmission sécurisée de données contre les attaques à textes clairs connus, des retards sont introduits comme un second pare-feu. Ainsi, les paramètres utilisés comme des clés secrètes du système à temps discret ne sont pas identifiables par techniques usuelles. Les résultats de simulation sont présentés pour illustrer les performances de la méthode proposée.

Mots-clés: Chaos, Systèmes dynamiques hybrides, Retards, Observateurs, Inversion à gauche, Communications privées.

Abstract: In this work, the left invertibility method of hybrid systems will be studied and applied for secure data transmission. Here, a transmission scheme based on the chaotic hybrid delayed dynamics for private communications is proposed. The transmitter is composed of a chaotic continuous-time system and a chaotic discrete-time system in which the message is inserted by inclusion. The states of the continuous system are also included, after sampling, in the discrete system. The receiver is composed of a continuous-time observer and a discrete-time observer. The principle of the proposed hybrid method is to show that the discrete states reconstruction including the message of the receiver passes at first by a synchronization of the two continuous-time chaotic systems. To increase the robustness of secure data transmission against known plain-text attacks, delays are introduced as a second firewall. By this way, the parameters used as secret keys of the discrete-time system are not identifiable by usual technical. Simulation results are presented to highlight the performances of the proposed method.

Keywords: Chaos, Hybrid dynamical systems, Delays, Observer, Left invertibility, Private communications.