Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires

Estelle Pawlowski Cherrier

Institut National
Polytechnique de Lorraine

Centre de Recherche
en Automatique de Nancy

École doctorale IAEM Lorraine
Département de Formation Doctorale en Automatique

Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires

THÈSE

présentée et soutenue publiquement le 26 octobre 2006

pour l'obtention du

Doctorat de l'Institut National Polytechnique de Lorraine

(spécialité automatique et traitement du signal)

par

Estelle Cherrier

Composition du jury

Président :	Fabrice HEITZ	Professeur à l'Université Louis Pasteur, Strasbourg
Rapporteurs :	Geneviève DAUPHIN-TANGUY	Professeur à l'École Centrale de Lille
	Mohammed M'SAAD	Professeur à l'ENSICAEN
Examinateurs :	Mohamed BOUTAYEB	Professeur à l'Université Louis Pasteur de Strasbourg
	Gilles MILLERIOUX	Professeur à l'Université Henri Poincaré, Nancy
	José RAGOT	Professeur à l'INPL
Invité :	M.A. AZIZ-ALAOUI	Professeur à l'Université du Havre

Centre de Recherche en Automatique de Nancy – UMR 7039 - CNRS - UHP - INPL
2, Avenue de la Forêt de Haye 54516 Vandœuvre-Lès-Nancy
Tél.+33 (0)3 83 59 59 59 Fax +33 (0)3 83 59 56 44

Mis en page avec la classe thloria.

A Fabrice, Lucas et Mathias

Remerciements

Je tiens à remercier en premier lieu les membres du jury, notamment Geneviève Dauphin-Tanguy et Mohammed M'Saad, qui ont accepté le lourd et minutieux travail dévolu aux rapporteurs. Merci également à Fabrice Heitz et Gilles Millérioux qui ont bien voulu examiner mon travail. Un merci tout particulier à M.A. Aziz-Alaoui pour son enthousiasme et ses conseils précieux en matière de chaos.
Toute ma reconnaissance va à mon directeur de thèse, José Ragot. Il a prouvé qu'il est possible d'être à la fois loin et très présent, très disponible. Quel enthousiasme ! Je profite donc de cette occasion pour le remercier très chaleureusement : *danke schön*.
Je remercie également mon co-directeur de thèse, Mohamed Boutayeb. Sans lui, je n'aurais pas découvert cette thématique passionnante qui associe l'automatique et les mathématiques.
En vrac, et dans le désordre, merci à Benjamin, merci à ceux qui ont fait le déplacement jusqu'à Nancy, Adlane, Ali, Samia et Florent. Merci à tous les membres de l'équipe AVR. Merci à Marjorie pour son aide logistique précieuse.
Merci à ceux qui m'ont fait l'amitié (et la surprise) de venir me soutenir : Karine, Raïd et Rozat, Aude, Alex, Mme. Ragot.
Pour finir, mes remerciements les plus profonds vont à ma famille. Merci à mes grands-parents, leur présence à ma soutenance représente beaucoup pour moi. Merci à ma sœur, ma complice de toujours... Je termine par mes parents, qui m'ont offert la possibilité de terminer (enfin !) mes études dans la sérénité. Merci pour tout !
Et merci surtout à toi, Fabrice. Tu sais à quel point, sans toi, je n'aurais pu mener cette thèse à son terme. Ces quatre années nous ont surtout permis de fonder notre propre famille. Lucas m'a accompagnée pendant les neuf premiers mois (magiques) de ma thèse. Mathias est né juste avant que je mette le point final. Merci à vous, mes Loulous, pour tous ces moments de bonheur (les nuits blanches sont déjà oubliées...)

Table des matières

Table des figures

Notations

Matrices et vecteurs

$M > 0$ ($M \geqslant 0$)	Matrice M symétrique, définie positive (resp. symétrique, positive)
$M < 0$ ($M \leqslant 0$)	Matrice M symétrique, définie négative (resp. symétrique, négative)
I_n (I)	Matrice identité de dimension n (resp. de dimension appropriée)
M^T	Transposée de la matrice M
M^{-1}	Inverse de la matrice M
$\begin{pmatrix} M_{11} & M_{12} \\ (\star) & M_{22} \end{pmatrix}$	Matrice symétrique, le symbole $(\star)$ représente M_{12}^T
$\lambda(M)$	Ensemble des valeurs propres de M
$\lambda_m(M)$ ($\lambda_M(M)$)	Valeur propre minimale (resp. maximale) de M
$\sigma(M)$	Ensemble des valeurs singulières de M
$\|M\|$	Norme euclidienne de la matrice M
$\|x\|$	Norme euclidienne du vecteur x

Ensembles

$\mathbb{R}$	Ensemble des nombres réels
$\mathbb{R}_+$	Ensemble des nombres réels positifs
$\mathbb{R}^n$	Espace réel euclidien de dimension n
$\mathcal{L}_2$	Espace de Lebesgue à temps continu *i.e.* espace des signaux continus de carré intégrable sur $\mathbb{R}^+$

Notations supplémentaires

$x_\tau(t)$	Désigne le vecteur retardé $x(t-\tau)$
k_f	Constante de Lipschitz de la fonction f
F, $\hat{F}$, $\tilde{F}$	Abréviations désignant resp. $F(x(t))$, $F(\hat{x}(t))$, $F(x(t)) - F(\hat{x}(t))$
H, $\hat{H}$, $\tilde{H}$	Abréviations désignant resp. $H(x(t-\tau))$, $H(\hat{x}(t-\tau))$, $H(x(t-\tau)) - H(\hat{x}(t-\tau))$

Acronymes

LMI	Inégalité matricielle linéaire (Linear Matrix Inequality)
BMI	Inégalité matricielle bilinéaire (Bilinear Matrix Inequality)
LTI	Linéaire à Temps Invariant
UIO	Observateur à entrées inconnues (Unknown Input Observer)
OOR	Observateur d'Ordre Réduit
SCI	Sensibilité aux Conditions Initiales
SISO	Entrée simple sortie simple (Single Input Single Output)
MIMO	Entrée multiple sortie multiple (Multiple Input Multiple Output)
SCTH	Système Chaotique à Tangente Hyperbolique (défini page 46)
SNR	Rapport signal sur bruit (Signal to Noise Ratio)
ssi	Si et Seulement Si

Références personnelles

Revue internationale avec comité de lecture

– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Observers based synchronization and input recovery for a class of nonlinear systems*. IEEE Transactions on Circuits and Systems I, vol. 53, no. 9, pages 1977–1988, 2006.

Revue nationale avec comité de lecture

– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Evaluation des bornes d'un système incertain. Approche par intervalles*. JESA, Journal Européen des Systèmes Automatisés, numéro spécial : "Application des outils de calculs ensemblistes", vol. 37, no. 9, pages 1181–1192, 2003.

Conférences internationales avec comité de lecture

– Estelle Cherrier, Mohamed Boutayeb, *Observer-based approach for synchronization of modified Chua's circuit*. In Proceedings of NOLCOS, IFAC Symposium on Nonlinear Control Systems, Stuttgart, Germany, 2004.
– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Observer-based approach for synchronization of a time-delayed Chua's circuit*. In Proceedings of ISCAS, IEEE International Symposium on Circuit and Systems, Kobe, Japan, 2005.
– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Observers based synchronization and input recovery for a class of chaotic models*. In Proceedings of the joint 44nd IEEE Conference on Decision and Control and European Control Conference, Seville, Spain, 2005.

– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Observateurs non linéaires de multimodèles. Application à la synchronisation et aux communications*. In Proceedings of CIFA, IEEE Conférence Internationale Francophone d'Automatique, Bordeaux, France, 2006.

Conférences nationales avec comité de lecture

– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *State estimation of uncertain parameter systems. Approach by intervals.* In 17th IAR, Annual Meeting, Grenoble, France, 2002.
– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Estimation des bornes de l'état d'un système incertain. Approche par intervalles.* In JDA'03 "Journées Doctorales d'Automatique", Valenciennes, France, 2003.
– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Observer-based approach for a time-delay system. Application to synchronization of modified Chua's circuit.* In 3rd Workshop on Advanced Control and Diagnosis, Karlsruhe, Germany, 2004.
– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Synchronisation basée observateur d'un système chaotique comportant un retard : Application à un circuit de Chua modifié.* In JDMACS, Lyon, France, 2005.
– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Observers based synchronization and input recovery for a class of nonlinear systems. Application to image transmission*. In 5th Workshop on Physics in Signal and Image Processing, Mulhouse, France, 2006. (Accepté)

Travaux en cours de soumission

– Estelle Cherrier, Mohamed Boutayeb, José Ragot *Exponential observer-based synchronization of time-delay chaotic system. Application to cryptosystems*. International Journal of Modelling, Identification and Control , numéro spécial sur les observateurs non linéaires, 2007. (Soumis)
– Estelle Cherrier, Mohamed Boutayeb, José Ragot, M.A. Aziz-Alaoui *Chaotic multimodels : application to observer-based synchronization*. IEEE Transactions on Circuit and Systems II. (Soumis)
– Estelle Cherrier, Mohamed Boutayeb, José Ragot, *Robust observer design for a class of nonlinear delayed systems. Application to experimental synchronization*. In Proceedings of the 26th American Control Conference, New York City, USA, 2006. (Soumis)
– Estelle Cherrier, José Ragot, Mohamed Boutayeb, M.A. Aziz-Alaoui *Observer-based exponential synchronization of chaotic multimodels*. In Proceedings of the European Control Conference, Kos, Greece, 2006. (Soumis)

Introduction générale

« Une cause très petite, et qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard. »

Henri Poincaré, 1908

La théorie de l'estimation tient une place de plus en plus importante en Automatique. 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 financières, on a recours à un système dynamique auxiliaire, appelé *observateur*, qui est chargé d'estimer l'état du système. La construction d'un observateur 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. Les observateurs à entrées inconnues interviennent dans le domaine du diagnostic, pour la détection de défauts (qui sont considérés comme des entrées inconnues), la surveillance de capteurs, l'estimation de perturbations affectant le système.

Le problème de l'estimation de l'état des systèmes linéaires a été entièrement résolu dans les années $1960-1970$. Le cas des systèmes non linéaires, qui concerne la plupart des systèmes physiques, reste un sujet de recherche largement ouvert, et très actif. Les problèmes d'estimation d'état ont été étendus aux systèmes incertains, puis chaotiques. Les systèmes chaotiques constituent une classe de systèmes non linéaires au comportement très complexe, méconnus jusqu'au XX^{ème} siècle. Les travaux du savant américain Edward Lorenz, passionné de météorologie, ont changé le cours 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. Par conséquent, l'apparition de phénomènes chaotiques était synonyme de nuisance et de perte de contrôle. Jusqu'en 1990, les systèmes chaotiques se réduisaient à des objets mathématiques étranges, caractérisés par les propriétés suivantes : un système chaotique est un système déterministe, possédant une sensibilité extrême aux conditions initiales (cette propriété correspond au fameux *effet papillon*) et un comportement asymptotique apériodique. Envisager la synchronisation des systèmes chaotiques semble donc impossible, puisque la notion de synchronisation était réservée jusque-là aux systèmes périodiques, pour désigner deux systèmes dont l'un suit le mouvement de l'autre. Pourtant en 1990, Pecora et Caroll ont mis en évidence la capacité de synchronisation des systèmes chaotiques. Cette découverte est une conséquence de la théorie générale de contrôle du chaos, élaborée la même année. Par la suite, le problème de la synchronisation des systèmes chaotiques a été relié au problème standard d'estimation d'état non linéaire, ce qui a ouvert la voie à des recherches intensives, motivées par les applications potentielles.

Parmi celles-ci, les cryptosystèmes (ou systèmes de transmission sécurisée d'information) chaotiques exploitent les propriétés fondamentales des systèmes chaotiques et leur capacité de synchronisation. L'aspect aléatoire des signaux chaotiques est mis à profit pour noyer l'information à transmettre : diverses techniques de cryptage par addition, par commutation, par modulation... 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. L'étape de synchronisation est fondamentale : elle permet au récepteur d'estimer les signaux utiles pour la restauration du message, en l'occurrence les états de l'émetteur, sans aucune connaissance sur l'état initial de l'émetteur. Les cryptosystèmes utilisant des générateurs de nombres pseudo-aléatoires ne possèdent pas cette propriété, puisque le récepteur doit connaître la condition initiale, ou graine, de l'émetteur pour reproduire la séquence de nombres qui a servi à crypter l'information. Même si les techniques de cryptage par le chaos sont en plein essor, des attaques spécifiques ont été développées en parallèle, ouvrant 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.

Dans ce mémoire, nous développons un système cryptographique chaotique reposant d'une part sur la synchronisation à base d'observateurs, et d'autre part sur une technique de masquage du message par modulation de phase. Le cryptosystème proposé s'inspire du principe de transmission à deux voies, qui découple totalement les phases de synchronisation et de cryptage. Ces deux phases nécessitent chacune une étude de sécurité. L'analyse de sécurité du cryptage doit respecter le principe énoncé par Kerckhoff au XIX^{ème} siècle, qui est à la base de la cryptanalyse : tout système cryptographique fiable doit posséder une clé, et la sécurité doit être analysée en supposant que l'intrus connaît tout le système, sauf la clé. Cette règle nous a incités à analyser soigneusement l'impact, sur la restauration du message, de petites erreurs commises sur la valeur de la clé par le récepteur. La vérification des propriétés de confusion et diffusion permet de quantifier le niveau de sécurité. Ces propriétés ont été identifiées par Shannon en 1949 : le but de la confusion est de rendre la relation entre la clé et le message crypté la plus complexe possible ; le but de la diffusion est de répartir les effets du message clair et de la clé sur la plus grande longueur possible de message crypté. Si ces deux conditions sont remplies, la cryptanalyse s'avère difficile. Il existe également des attaques spécifiques contre les techniques de cryptage par le chaos, reposant notamment sur l'analyse spectrale. Au niveau du processus de synchronisation, les attaques exploitent principalement les techniques de reconstruction dites « à retard ». Il s'agit d'exploiter les informations contenues dans le signal (ou les signaux) transmis au récepteur pour reconstituer la géométrie de l'attracteur correspondant à l'émetteur. L'attracteur d'un système est l'ensemble vers lequel un système évolue de façon irréversible en l'absence de perturbations. Contrairement au caractère prétendument aléatoire des systèmes chaotiques, les attracteurs correspondants possèdent des propriétés géométriques intrinsèques reconnaissables. Ces attaques par reconstruction sont nettement moins efficaces lorsque le chaos généré par l'émetteur est très complexe. C'est en particulier le cas lorsque la dynamique du système chaotique comporte un retard, qui confère une dimension infinie à l'attracteur. La sécurité du processus de synchronisation dépend donc du choix de l'émetteur.

On peut envisager le système de communications proposé sous l'angle de la restauration d'entrées inconnues : l'information à transmettre correspond à une entrée de l'émetteur, la conception du récepteur à la synthèse d'un observateur de l'émetteur chaotique, la synchronisation à l'estimation de l'état de l'émetteur, et le décryptage à l'estimation de l'entrée, inconnue au niveau du récepteur.

Avant de concevoir des observateurs spécifiques pour établir la synchronisation avec la classe de systèmes chaotiques considérés et de proposer une nouvelle technique de cryptage, il nous semble primordial de présenter un état de l'art pour situer et motiver nos travaux. Ainsi le **premier chapitre** est-il divisé en quatre parties. Les deux premières sont consacrées aux différentes techniques d'estimation d'état, respectivement sans puis avec entrées inconnues. La troisième

établit le lien entre les observateurs et la synchronisation d'une classe particulière de systèmes non linéaires, à savoir les systèmes chaotiques. Enfin les principaux systèmes de communications chaotiques à base de synchronisation sont détaillés dans la quatrième partie.

Le **deuxième chapitre** est dédié à la synchronisation à base d'observateurs. Les modèles des émetteurs intervenant dans ce mémoire y sont décrits : ils appartiennent à une classe de systèmes non linéaires comportant un retard, exhibant un comportement chaotique. Différentes techniques d'estimation d'état sont alors appliquées à cette classe de systèmes et aboutissent à la conception d'observateurs spécifiques, d'ordre plein et d'ordre réduit. L'analyse de la stabilité (asymptotique ou exponentielle) de l'erreur d'estimation fait appel à la théorie de la stabilité de Lyapunov-Krasovskii dédiée aux systèmes à retard, et aboutit à des conditions suffisantes de synchronisation, qui sont exprimées sous forme de BMI (inégalités matricielles bilinéaires) et de LMI (inégalités matricielles linéaires). L'efficacité des observateurs proposés est testée à l'aide de simulations numériques. La fin de ce chapitre présente la synthèse d'un observateur robuste au bruit, dont l'analyse fait appel à la théorie $\mathcal{H}_\infty$.

Les travaux présentés dans le **troisième chapitre** concernent les systèmes de communications à base de synchronisation chaotique. Une rapide présentation des techniques de cryptage élaborées depuis le XVI^{ème} siècle avant J.-C. et des techniques de cryptage employées actuellement permet d'introduire les systèmes de cryptage par le chaos proposés dans la littérature. La méthode que nous proposons est d'abord présentée de façon intuitive, puis détaillée analytiquement. Les résultats obtenus sont illustrés par des simulation numériques, afin de tester la transmission de différents messages (son, image, texte) puis leur restauration. La fin de ce chapitre est consacrée à une analyse de la sécurité du procédé de masquage chaotique proposé. Le compromis entre la robustesse et la sécurité apparaît au cours de l'étude du cas où la transmission est bruitée.

Le **quatrième et dernier chapitre** est consacré à la définition d'une nouvelle classe de systèmes chaotiques, dans le but de renforcer la sécurité du processus de synchronisation. Après quelques rappels sur la stabilité des multimodèles standard, nous proposons des observateurs dont la structure est adaptée aux multimodèles, afin d'intégrer ces systèmes, en tant qu'émetteurs, dans le système de communications chaotiques détaillé au chapitre précédent.

CHAPITRE

1

Etat de l'art

Sommaire

Ce chapitre illustre la progression des recherches menées pendant cette thèse, et présente un état de l'art divisé en quatre parties. La première partie, assez générale, est consacrée aux différentes techniques d'estimation de l'état des systèmes non linéaires, systèmes auxquels ce mémoire est consacré. Nous essayons de dégager les principales approches développées dans ce domaine depuis les années 1970 environ, domaine qui reste malgré tout très ouvert, notamment à cause de la multiplicité et de la diversité des systèmes non linéaires. La deuxième partie concerne un problème connexe à la théorie de l'estimation. Il s'agit de reconstruire, non seulement l'état d'un système, mais aussi les entrées inconnues qui interviennent dans la dynamique du système. Dans une troisième partie, nous abordons la synchronisation des systèmes chaotiques, à travers la définition des différents régimes de synchronisation. Le lien avec l'estimation d'état non linéaire est direct. En effet, d'une part les systèmes chaotiques forment une classe de systèmes non linéaires possédant quelques propriétés remarquables. Et d'autre part, après un tour d'horizon des différentes approches de synchronisation, on constate qu'il s'agit en définitive de reconstruire l'état d'un système non linéaire. La quatrième partie de cet état de l'art est dévolue aux systèmes de communications sécurisées, qui exploitent les propriétés du chaos et qui nécessitent une étape de synchronisation pour permettre la reconstruction d'une information, ou entrée inconnue.

1.1 Observateurs non linéaires

Cette section pose le problème de l'estimation d'état des systèmes non linéaires. Nous rappelons tout d'abord les concepts d'observateurs d'ordre plein et d'ordre réduit, puis nous présentons une liste non exhaustive de techniques existantes d'estimation d'état non linéaire.

1.1.1 Introduction

Le domaine de l'estimation d'état des systèmes non linéaires est encore largement ouvert. Même si, comme nous allons le voir, de nombreuses méthodes ont été développées pour concevoir des observateurs non linéaires, le problème reste sans solution dans un grand nombre de cas. C'est un domaine de recherche actif, car la connaissance de l'état d'un système est nécessaire dans de multiples applications, à savoir la commande de procédés, la surveillance de systèmes, le diagnostic et la détection de défauts... En pratique, l'état d'un système peut correspondre à une grandeur physique que l'on ne sait pas mesurer directement ; l'évolution de l'état d'un système peut également permettre, par redondance, de déterminer une défaillance de capteur ou plus généralement de composants du système ; l'élaboration d'une loi de commande passe souvent par l'accès à la valeur d'un ou plusieurs état(s) du système.
La plupart des systèmes physiques sont non linéaires. Parfois une approximation par linéarisation permet de trouver une solution satisfaisante au problème d'estimation d'état. Cependant cette méthode ne peut pas toujours être appliquée, la classe de systèmes non linéaires concernés est assez réduite. Il faut donc concevoir des solutions spécifiques pour les systèmes non linéaires : les premiers résultats sur les observateurs non linéaires datent des années 1970. Contrairement

aux systèmes linéaires dont la représentation d'état est déterminée de la même façon pour tous les systèmes linéaires, par quatre matrices (d'état, de commande...), les systèmes non linéaires ont des représentations d'état très variées, qui exploitent la structure et les propriétés de la fonction non linéaire qui intervient. Il semble donc difficile *a priori*, étant donné l'état des travaux actuels, de trouver une théorie générale sur l'estimation d'état non linéaire, qui unifierait les approches déjà établies.
Revenons au sujet qui sous-tend toutes nos recherches : l'observation des systèmes non linéaires. De manière générale, un observateur est un système dynamique qui permet la reconstruction (asymptotique ou exponentielle) de l'état d'un système, à partir de ses entrées, de ses sorties, et de la connaissance de son modèle dynamique, qui sont les seules informations disponibles.
Ce principe est illustré par la figure 1.1.

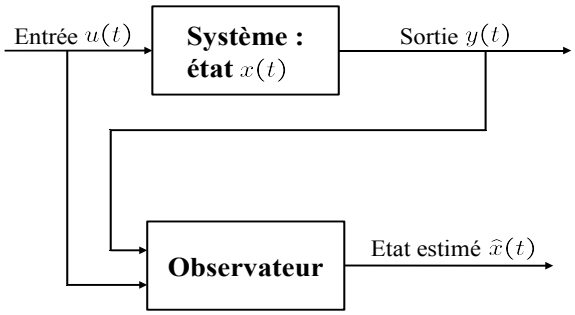


FIG. 1.1 - *Principe de l'observateur*

Théoriquement, le problème de la conception d'un observateur pour un système (non linéaire) donné est posé comme suit.
Soit le système non linéaire :

$$\begin{cases} \dot{x}(t) = f(x(t), u(t)) \\ y(t) = h(x(t), u(t)) \end{cases} \tag{1.1}$$

avec $t \geqslant 0$.
$x \in \mathbb{R}^n$ est le vecteur d'état, $u \in \mathbb{R}^m$ est le vecteur d'entrée, $y \in \mathbb{R}^p$ est le vecteur de sortie, et les conditions initiales sont données par $x_0 = x(0)$.

Définition 1.1.1 (Observateur)**.** On considère le système dynamique :

$$\begin{cases} \dot{z}(t) = \Phi(z(t), u(t), y(t)) \\ \hat{x}(t) = \Psi(z(t), u(t), y(t)) \end{cases} \tag{1.2}$$

où $z \in \mathbb{R}^q$, $q \leqslant n$ avec les conditions initiales $z_0 = z(0)$. Les entrées de ce système sont u et y, et la sortie est l'état estimé $\hat{x} \in \mathbb{R}^n$.
Si les hypothèses suivantes sont vérifiées :

(i) $\hat{x}(t_0) = x(t_0) \quad \Rightarrow \quad \hat{x}(t) = x(t), \quad \forall t \geqslant t_0$,
(ii) l'erreur d'estimation $e(t) = x(t) - \hat{x}(t)$ tend asymptotiquement (respectivement exponentiellement) vers zéro,
alors le système (1.2) est un observateur (respectivement un observateur exponentiel) du système (1.1), d'ordre plein si $q = n$, d'ordre réduit si $q < n$. ♦

Le problème de la synthèse d'un observateur consiste donc à trouver des fonctions Φ et Ψ qui assurent la convergence de l'état estimé $\hat{x}$ vers l'état réel x du système, et ce, indépendamment de x_0, z_0, $u(t)$. Pour étudier la convergence de l'observateur d'un système, des outils concernant la stabilité des systèmes dynamiques sont utilisés, et notamment la théorie élaborée par Lyapunov (voir l'annexe A).
Nous allons maintenant détailler les principales techniques d'estimation non linéaires mises en œuvre dans la littérature. Cette liste ne se prétend pas exhaustive, et le classement des différentes méthodes est un choix qui n'est pas unique, car certaines de ces méthodes font appel à plusieurs approches.
Le problème de l'estimation d'état a d'abord été entièrement résolu dans le cas des systèmes linéaires. Après un rappel succinct des résultats obtenus par Luenberger [Luenberger 71] et Kalman [Kalman 60], nous recenserons les approches développées pour l'estimation de l'état des systèmes non linéaires, dont la plupart trouvent une inspiration certaine dans les techniques établies pour les systèmes linéaires.

1.1.2 Observateurs de systèmes linéaires

Une solution simple et optimale au problème de l'estimation de l'état des systèmes linéaires a été proposée par Luenberger [Luenberger 71] dans le cadre déterministe, et par Kalman [Kalman 60] dans le cadre stochastique.
Dans les deux cas, on considère le modèle dynamique d'un système linéaire défini comme suit :

$$\left\{ \begin{array}{rcl} \dot{x}(t) & = & Ax(t) + Bu(t) + Lw(t) \\ y(t) & = & Cx(t) + v(t) \end{array} \right. \tag{1.3}$$

où $t \geqslant 0$, $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, $y(t) \in \mathbb{R}^p$. $w(t) \in \mathbb{R}^r$ et $v(t) \in \mathbb{R}^p$ sont deux bruits blancs gaussiens d'espérance nulle, de covariances respectives Q et R. Ces bruits sont supposés non corrélés. Les matrices du système sont de dimensions appropriées, et les conditions initiales sont définies par $x(0) = x_0$.

Observateur de Luenberger

La théorie de l'observation de Luenberger repose essentiellement sur des techniques de placement de pôles. On se place dans le cas déterministe, *i.e.* les bruits w et v sont nuls, et Luenberger

propose l'observateur suivant pour le système (1.3) :

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + K\left(y(t) - C\hat{x}(t)\right) \tag{1.4}$$

La dynamique de l'erreur d'estimation $e(t) = x(t) - \hat{x}(t)$ a pour expression :

$$\dot{e}(t) = (A - KC)e(t) \tag{1.5}$$

En utilisant une technique de placement de pôles, il suffit alors de choisir le gain K de l'observateur de telle sorte que les valeurs propres de la matrice $A - KC$ soient dans le demi-plan complexe gauche.

Remarque 1.1.1. En présence de bruits w, v, la dynamique de l'erreur est régie par l'équation :

$$\dot{e}(t) = (A - KC)e(t) + Lw(t) - Kv(t) \tag{1.6}$$

Cette erreur est donc sensible aux bruits par l'intermédiaire des deux fonctions de transfert $(sI - A + KC)^{-1}L$ et $(sI - A + KC)^{-1}K$. L'étude du gain fréquentiel permet de quantifier l'influence des bruits sur e.

Filtre de Kalman

La théorie de l'observation de Kalman nécessite, quant à elle, la résolution d'une équation de Riccati. Kalman utilise les propriétés statistiques des bruits w et v et propose la structure d'observateur suivante :

$$\dot{\hat{x}}(t) = A\hat{x}(t) + Bu(t) + K(t)\left(y(t) - C\hat{x}(t)\right) \tag{1.7}$$

En minimisant la matrice de covariance de l'erreur d'estimation $P(t) = E\left[e(t)e(t)^T\right]$, on obtient l'expression du gain de l'observateur :

$$K(t) = P(t)C^T R^{-1} \tag{1.8}$$

où $P(t)$ est solution de l'équation de Riccati :

$$\dot{P}(t) = AP(t) + P(t)A^T - P(t)C^T R^{-1} CP(t) + LQL^T \tag{1.9}$$

Sous certaines conditions (rappelées dans [Aubry 99]), on peut montrer que la matrice $P(t)$ tend vers une limite et que le filtre est stable, ce qui permet éventuellement de conserver pour K sa valeur en régime permanent.
Le problème de l'observation des systèmes linéaires est donc entièrement résolu. C'est loin d'être le cas lorsqu'il s'agit de systèmes non linéaires. Nous allons voir que la plupart des techniques élaborées dans la littérature s'inspirent des méthodes linéaires et tentent de les généraliser, au prix d'hypothèses très fortes sur la structure des nonlinéarités. De nombreuses références

peuvent être trouvées dans [Misawa 89], [Walcott 87a], ou plus récemment dans [Primbs 96].

1.1.3 Approches stochastiques

Dans ce paragraphe, on considère le système non linéaire (1.1) modifié de la manière suivante :

$$\begin{cases} \dot{x}(t) = f(x(t), u(t)) + Lw(t) \\ y(t) = h(x(t), u(t)) + v(t) \end{cases} \tag{1.10}$$

$w(t) \in \mathbb{R}^r$ et $v(t) \in \mathbb{R}^p$ sont deux bruits blancs gaussiens d'espérance nulle, de covariances respectives Q et R, non corrélés.

Filtre de Kalman étendu

Le filtre de Kalman étendu est une méthode assez répandue pour estimer l'état d'un système non linéaire. Sa conception [Jazwinski 70], [Chen 93], [Reif 98] repose sur la généralisation du filtre de Kalman linéaire (1.7) en utilisant des techniques classiques de linéarisation de la dynamique non linéaire. Ainsi les matrices A et C sont-elles remplacées par les matrices jacobiennes de f et h, évaluées en $\hat{x}(t)$. Le système étudié est linéarisé à chaque instant le long de trajectoires estimées.
On note :

$$A(t) = \frac{\partial f}{\partial x}(\hat{x}(t), u(t)) \tag{1.11}$$

$$C(t) = \frac{\partial h}{\partial x}(\hat{x}(t), u(t)) \tag{1.12}$$

La dynamique du filtre de Kalman étendu se met sous la forme :

$$\dot{\hat{x}}(t) = f(\hat{x}(t), u(t)) + K(t)\left(y(t) - h(\hat{x}(t), u(t))\right) \tag{1.13}$$

L'expression (1.8) du gain $K(t)$ devient :

$$K(t) = P(t)C^T(t)R^{-1} \tag{1.14}$$

et l'équation de Riccati (1.9) est elle aussi modifiée :

$$\dot{P}(t) = A(t)P(t) + P(t)A^T(t) - P(t)C^T(t)R^{-1}C(t)P(t) + LQL^T \tag{1.15}$$

On peut souligner qu'il s'agit seulement de résultats locaux, à savoir qu'une convergence globale ne peut être garantie sans hypothèses supplémentaires. Par ailleurs, la synthèse de ce filtre utilise une approximation de Taylor au premier ordre, par conséquent les fonctions f et h doivent être dérivables, ce qui n'est pas le cas pour tous les systèmes non linéaires. D'un autre côté, on peut supposer qu'en utilisant des termes d'ordre supérieur du développement de Taylor, les

performances sont améliorées. Ainsi [Reif 98] propose un filtre de Kalman étendu légèrement modifié en supposant que les nonlinéarités sont de classe $\mathcal{C}^1$, et que les termes d'ordre deux du développement de Taylor sont bornés, tandis que [Jazwinski 70] propose un filtre du second ordre. De manière générale, toutes ces techniques utilisent des calculs très lourds, pour résoudre l'équation de Riccati (1.15) notamment. Concernant le cas des systèmes à temps discret, on peut se reporter à [Aubry 99] et à ses nombreuses références.

Linéarisation statistique

Cette technique ne fait pas appel à la linéarisation des nonlinéarités à partir du développement de Taylor, mais utilise des approximations non linéaires plus simples que les fonctions initiales. Par exemple, dans [Nørgaard 00] les fonctions f et h sont remplacées par des polynômes en x, choisis par minimisation de l'erreur d'approximation, ce qui donne une formule d'interpolation multi-dimensionnelle. L'inconvénient majeur de cette technique réside dans l'hypothèse faite sur la densité de probabilité de l'erreur, qui n'est pas connue *a priori*, et qui est supposée gaussienne par défaut. En outre, la complexité et le volume de calcul sont souvent plus importants que dans le cas du filtre de Kalman étendu.

1.1.4 Approches nécessitant une transformation

Dans cette partie, le but est toujours de se rapprocher du cas linéaire, que l'on sait traiter. Ces approches font appel à des transformations non linéaires de l'état d'un système afin de rendre la dynamique de l'erreur d'estimation linéaire. Ainsi l'erreur d'estimation converge linéairement ou quasi linéairement dans un espace d'état qui est une transformation non linéaire du système de coordonnées original. On utilise alors des techniques linéaires pour construire un observateur linéaire, puis on applique la transformation inverse pour obtenir un observateur non linéaire pour le système de départ. L'application de ces transformations met le système initial sous la forme canonique d'observabilité généralisée : cela généralise la forme canonique d'observabilité définie dans le cas linéaire. On distingue trois principales approches : les techniques de linéarisation exacte, rigoureuses mais peu utilisables en pratique ; des techniques de linéarisation étendue, qui s'appliquent à une plus grande classe de systèmes ; enfin les techniques de plongement, qui utilisent une classe plus large de transformations.

Techniques de linéarisation exacte

Les techniques de linéarisation exacte de l'erreur d'estimation reposent sur l'existence d'un changement de coordonnées (c'est-à-dire un difféomorphisme, application bijective différentiable et dont la réciproque est différentiable) qui transforme le système non linéaire initial en un système linéaire auxiliaire.
Nous ne détaillons pas cette procédure dans ce mémoire, cependant nous donnons un bref aperçu des étapes de la transformation du système, et de la synthèse de l'observateur. La procé-

dure a été détaillée pour la première fois dans [Bestle 83].
On considère le système non linéaire suivant :

$$\begin{cases} \dot{x}(t) &= f(x(t), u(t)) \\ y(t) &= h(x(t)) \end{cases} \tag{1.16}$$

Nous donnons un résumé de l'algorithme mis en oeuvre pour construire un observateur du système (1.16) par linéarisation.
Étape 1) Étant donné un état initial $x_0 \in \mathbb{R}^n$, le problème de la linéarisation exacte de l'erreur d'estimation consiste à rechercher un difféomorphisme T défini sur un voisinage de x_0 tel que :

$$z(t) = T(x(t)) \tag{1.17}$$

ce qui revient à :

$$x(t) = T^{-1}(z(t)) \tag{1.18}$$

Le difféomorphisme est choisi de telle sorte que le modèle dynamique du système (1.16) se mette, dans le nouveau système de coordonnées, sous la forme canonique observable généralisée :

$$\begin{cases} \dot{z} &= Az + g(y, u) \\ y &= Cz \end{cases} \tag{1.19}$$

Étape 2) Comme la nonlinéarité g ne dépend que des entrées et des mesures, qui sont connues, par injection on linéarise simplement l'erreur d'estimation. En effet, on choisit comme observateur :

$$\dot{\hat{z}}(t) = A\hat{z}(t) + g(y(t), u(t)) + K(y(t) - C\hat{z}(t)) \tag{1.20}$$

Étape 3) La dynamique de l'erreur d'estimation $e(t) = z(t) - \hat{z}(t)$ s'écrit :

$$\dot{e}(t) = (A - KC)e(t) \tag{1.21}$$

Étape 4) On est donc ramené à un problème linéaire, que l'on sait résoudre, par une technique de placement de pôles. Le gain K est choisi de telle sorte que la matrice $A - KC$ soit stable.
Étape 5) Finalement, pour obtenir une estimation de l'état x du système non linéaire initial, il suffit d'appliquer le difféomorphisme inverse :

$$\hat{x} = T^{-1}(\hat{z}) \tag{1.22}$$

La difficulté majeure de cette méthode de linéarisation exacte réside dans l'obtention du difféomorphisme T (1.17). De nombreux articles ont tenté de donner des conditions théoriques garantissant l'existence d'une forme canonique d'observabilité généralisée pour les systèmes non

linéaires. [Krener 83] a donné les conditions nécessaires et suffisantes (utilisant l'algèbre de Lie) pour pouvoir mettre un système non linéaire sous la forme canonique d'observabilité généralisée. Cet article traite le cas SISO, et suppose que la fonction h est linéaire. La classe de systèmes auxquels cette théorie s'applique a été élargie dans [Kazantzis 98], qui s'intéresse aux systèmes non linéaires dont la sortie est une fonction non linéaire de l'état, à valeurs réelles. Le cas de systèmes à plusieurs sorties est traité dans les références [Krener 85], [Xia 89]. Parallèlement, l'article [Bestle 83] introduit la forme canonique d'observabilité non linéaire pour les systèmes dont la nonlinéarité ne dépend que de la sortie et des entrées. Il détaille une transformation implicite sous la forme canonique : cet article propose la synthèse d'un observateur dans le système de coordonnées initial. Ensuite, le gain de l'observateur est choisi de telle sorte que l'erreur dans le nouveau système de coordonnées soit quasi linéaire. L'article [Keller 87] propose une généralisation utilisant la théorie des EDP (Equations aux Dérivées Partielles). Il conçoit un observateur non linéaire qui dépend des n premières dérivées de l'entrée. Plus récemment, [Jo 00] a mis au point une technique de linéarisation entrée-sortie.
On peut souligner également que ces techniques sont des solutions locales, valables dans un voisinage de la condition initiale choisie x_0. On peut légitimement se poser la question de la validité de ces formules lorsqu'on sort de ce voisinage.

Techniques de plongement

Certains systèmes ne remplissent pas les conditions nécessaires pour être mis sous forme canonique d'observabilité généralisée. Pour pallier les hypothèses trop restrictives des précédentes techniques, certains articles [Levine 86], [Rapaport 00] proposent d'utiliser une immersion dans un état de dimension supérieure à celle de l'espace d'état initial, à la place d'un difféomorphisme. Il s'agit donc de trouver une transformation injective (tandis que le difféomorphisme est bijectif), qui concerne une classe plus grande de systèmes non linéaires.

Remarque 1.1.2. On peut souligner que ces techniques sont soit des solutions globales dont les conditions d'application sont très restrictives, soit des solutions locales, valables uniquement dans le domaine de validité de la transformation.

1.1.5 Observateurs à grand gain

Les techniques dites "à grand gain" peuvent être appliquées sans transformation du système initial : dans ce cas, la conception de l'observateur se fait directement à partir de la structure du système.
Les deux articles [Thau 73] et [Kou 75] sont à l'origine de ces techniques qui utilisent la théorie de la stabilité de Lyapunov (voir l'annexe A) pour adapter les techniques développées dans le cas linéaire. La méthode présentée dans [Thau 73] donne des conditions suffisantes de convergence de l'état estimé vers l'état réel du système, pour la classe des systèmes non linéaires décrits par

le modèle suivant :

$$\begin{cases} \dot{x}(t) = Ax(t) + f(x(t), u(t)) \\ y(t) = Cx(t) \end{cases} \tag{1.23}$$

La dynamique de l'état comporte une partie linéaire non commandée et une partie non linéaire commandée, vérifiant en général la condition de Lipschitz par rapport à x (au moins localement) :

Définition 1.1.2 (Condition de Lipschitz)**.** Une fonction $f : \mathbb{R}^n \to \mathbb{R}^m$ est dite k-Lipschitzienne s'il existe $k > 0$ tel que pour tout $(x, y) \in (\mathbb{R}^n)^2$:

$$\|f(x) - f(y)\| \leqslant k\|x - y\| \tag{1.24}$$

♦

L'observateur "à grand gain" possède la structure suivante :

$$\dot{\hat{x}} = A\hat{x} + f(\hat{x}, u) + L(y - C\hat{x}) \tag{1.25}$$

L'appellation "grand gain" provient de la structure de l'observateur : lorsque la fonction non linéaire f possède une grande constante de Lipschitz, la moindre erreur entre l'état réel et l'état estimé va se répercuter et croître. Par conséquent, le gain L de l'observateur (1.25) doit être important pour compenser cette amplification de l'erreur.
La dynamique de l'erreur d'estimation $e = x - \hat{x}$ se déduit de (1.23) et (1.25) :

$$\dot{e}(t) = (A - LC)e(t) + f(x(t), u(t)) - f(\hat{x}(t), u(t)) \tag{1.26}$$

Le résultat présenté dans [Thau 73] est le suivant :

Théorème 1.1.1 (Thau)**.** *Si le gain L vérifie*

$$k < \frac{\lambda_{min}(Q)}{2\lambda_{max}(P)} \tag{1.27}$$

où k est la constante de Lipschitz de $f(.)$, et P, Q sont deux matrices respectivement symétrique définie positive et définie positive, solutions de l'équation de Riccati :

$$(A - LC)^T P + P(A - LC) = -Q \tag{1.28}$$

alors (1.25) *est un observateur asymptotique du système non linéaire* (1.23). ■

La méthode de Thau n'est pas constructive, elle ne donne aucune indication sur le choix d'un gain satisfaisant la condition (1.27). Il s'agit d'une technique de vérification, qui garantit la convergence asymptotique de l'état estimé $\hat{x}$ vers l'état réel x, lorsque le gain L a déjà été choisi. L'article [Kou 75] a étendu les résultats de Thau dans le cadre déterministe. On peut citer

également parmi les techniques dites "à grand gain" les articles [Gauthier 92], [Ciccarella 93], et plus récemment [Kreisselmeier 03], qui proposent de compenser la nonlinéarité, au niveau de la dynamique de l'erreur d'estimation, par un gain suffisamment grand (comparé à la constante de Lipschitz). Une extension de ces résultats aux observateurs exponentiels est détaillée dans [Deza 93].
[Raghavan 94] est à l'origine d'une série d'articles décrivant des méthodes constructives du gain L de l'observateur (1.25). En effet, il propose l'algorithme suivant :

Proposition 1.1.2 ([Raghavan 94])**.** *S'il existe un petit $\varepsilon > 0$ tel que l'équation de Riccati :*

$$AP + PA^T + P\left(k^2 I - \frac{1}{\varepsilon} C^T C\right) P + I + \varepsilon I = 0 \tag{1.29}$$

admette une solution symétrique définie positive P, alors il suffit de choisir

$$L = \frac{1}{2\varepsilon} P C^T \tag{1.30}$$

pour assurer la convergence asymptotique de l'observateur (1.25). ▲

Ce résultat ne donne cependant pas d'indication quant aux conditions que doit remplir la matrice $(A - LC)$: par exemple, il ne suffit pas toujours de choisir des valeurs propres de $(A - LC)$ "loin" dans le demi-plan complexe gauche.

Plus récemment la référence [Rajamani 98] a établi des conditions suffisantes sur la matrice $(A - LC)$ pour que le système dynamique (1.25) soit un observateur du système (1.23) :

Proposition 1.1.3 ([Rajamani 98])**.** *Le système* (1.25) *est un observateur du système* (1.23) *si les conditions suivantes sont vérifiées :*
(i) la paire (A, C) est observable ;
(ii) le gain L est choisi de telle sorte que $(A - LC)$ soit stable et

$$min_{\omega \in \mathbb{R}_+} \sigma_{min}(A - LC - j\omega I) > k \tag{1.31}$$

▲

[Zhu 02] a étendu les résultats précédents aux observateurs réduits : cet article montre que les conditions de la Proposition 1.1.3 garantissent également l'existence d'un observateur réduit asymptotiquement convergent pour le système non linéaire (1.23).

D'autres techniques sont utilisées parallèlement aux techniques à grand gain. Ainsi le cas adaptatif est-il traité dans [Besançon 04], qui propose un observateur à grand gain adaptatif pour les systèmes non linéaires dépendant linéairement de paramètres inconnus. La théorie de la stabilité entrée-état est utilisée dans [Alessandri 04] pour étudier la robustesse aux incertitudes. L'article

[Farza 04] détaille la conception d'un observateur à grand gain pour une classe de systèmes non linéaires MIMO. L'expression du gain est donnée explicitement, sans résolution d'équation.

Remarque 1.1.3. Ces techniques dites "à grand gain" sont très utilisées dans la littérature. Il s'agit principalement de techniques de vérification, qui permettent d'établir des conditions suffisantes de convergence de l'état estimé vers l'état réel. La structure de l'observateur non linéaire est une structure de Luenberger étendue au cas non linéaire. La majoration de l'erreur (1.26) utilise la condition de Lipschitz, majoration qui n'est guère optimale. Aussi ces conditions sont-elles le plus souvent conservatives.

1.1.6 Observateurs à structure variable

Les observateurs à structure variable constituent une autre famille d'observateurs. Dans toutes les méthodes vues précédemment, le modèle dynamique du système étudié était supposé parfaitement connu. Ici, il s'agit de développer une certaine robustesse vis-à-vis d'incertitudes paramétriques. La méthode employée pour construire ces observateurs s'appuie sur la théorie des modes glissants [Walcott 87b], [Slotine 87]. La classe des systèmes étudiés est décrite par :

$$\begin{cases} \dot{x}(t) = Ax(t) + f(x(t), u(t)) \\ y(t) = Cx(t) \end{cases} \tag{1.32}$$

La fonction f représente les nonlinéarités et les incertitudes du système.
On fait les hypothèses suivantes sur le système (1.32) :

(i) la paire (C, A) est détectable, donc il existe une matrice K telle que la matrice $(A - KC)$ soit stable ;

(ii) la fonction f est de la forme

$$f(x(t), u(t)) = P^{-1}C^T h(x(t), u(t)) \tag{1.33}$$

où P est une matrice symétrique définie positive, solution de l'équation de Lyapunov (P existe d'après l'hypothèse (i)) :

$$(A - KC)^T P + P(A - KC) = -Q < 0 \tag{1.34}$$

et la fonction h est inconnue mais bornée :

$$\|h(x(t), u(t))\| \leqslant \rho(u(t)) \tag{1.35}$$

On peut souligner que la nonlinéarité n'intervient pas dans la structure de l'observateur proposé par [Walcott 87b] :

$$\dot{\hat{x}}(t) = A\hat{x}(t) + K(y(t) - C\hat{x}(t)) + \kappa(\hat{x}(t), u(t), y(t)) \tag{1.36}$$

avec

$$\kappa(\hat{x}(t), u(t), y(t)) = \begin{cases} \frac{P^{-1}C^T(y(t)-C\hat{x}(t))}{\|(y(t)-C\hat{x}(t))\|}\rho(u(t)) & \text{si } (x(t)-\hat{x}(t)) \neq 0 \\ 0 & \text{si } (x(t)-\hat{x}(t)) = 0 \end{cases} \tag{1.37}$$

Le terme $\kappa(\hat{x}(t), u(t), y(t))$ dans (1.36) peut être considéré comme un gain variable, qui devient infini lorsque l'erreur d'estimation est petite. Il est démontré dans [Walcott 87b] que l'observateur (1.36) est un observateur exponentiel du système (1.32).
On notera que la connaissance exacte du système n'est pas nécessaire, il suffit de connaître une majoration $\rho(u)$ sur les nonlinéarités ou incertitudes. En revanche, l'hypothèse (ii) impose une contrainte structurelle sur f, qui peut être difficile à vérifier en présence d'incertitudes de modèle. [Slotine 87] propose un observateur légèrement différent, qui n'utilise pas cette condition, mais en contrepartie la convergence globale n'est plus garantie.
La discontinuité de la fonction κ (1.37) est un autre inconvénient de cette méthode : un régime oscillatoire à hautes fréquences peut apparaître dans la dynamique de l'erreur d'estimation. Pour pallier ce problème, [Dawson 92] propose un autre choix pour la fonction κ.

1.2 Observateurs à entrées inconnues

1.2.1 Introduction

Dans la partie précédente, nous avons passé en revue quelques techniques classiques d'estimation d'état pour les systèmes linéaires et non linéaires. Pour les observateurs standard, dans tous les cas, la reconstruction de l'état se fait à partir des entrées éventuelles et des sorties du système. Ces méthodes ne peuvent plus s'appliquer lorsque la dynamique du système est soumise à l'influence d'entrées inconnues. Classiquement, ces entrées inconnues proviennent d'erreurs de modélisation, de défauts de capteurs, ou encore de perturbations, de bruits (sur l'état ou la sortie du système). Dans le cas où le système est influencé par des entrées inconnues, des techniques ont été mises au point pour estimer soit l'état seul, soit l'état et également les entrées inconnues. Ces dernières techniques peuvent en particulier être utilisées pour reconstruire un message contenant des informations à transmettre, message considéré comme une entrée inconnue par le récepteur, ce qui sera l'objet du paragraphe 1.4. Nous proposons un état de l'art succinct concernant les observateurs à entrées inconnues, ou *UIO* (*Unknown Input Observer* en anglais).

1.2.2 Présentation des différentes techniques

Des approches très diverses ont été développées depuis les années 1970 pour estimer l'état et les entrées inconnues d'un système dynamique. Comme dans la section précédente, nous nous

intéressons d'abord au cas des systèmes linéaires. Ensuite nous présentons le problème du point de vue du diagnostic, pour terminer par quelques résultats sur les systèmes non linéaires, dont une partie sera reprise ultérieurement dans ce mémoire.

Systèmes linéaires

Les premiers résultats sur l'estimation d'état linéaire datent des années 1970. Une première solution a été envisagée par [Johnson 71] et [Hostetter 73] lorsque la dynamique des entrées inconnues est connue : ces articles détaillent la construction d'un système dynamique augmenté, dont l'état est constitué de l'état du système initial et des entrées inconnues. L'observateur est alors chargé d'estimer ce vecteur d'état augmenté.

A contrario, les autres techniques de synthèse d'UIO ne nécessitent aucune connaissance sur la dynamique des entrées inconnues. Les travaux de [Wang 75] proposent un UIO d'ordre réduit pour les systèmes linéaires comportant des entrées connues et inconnues. [Kudva 80] donne les conditions d'existence de cet observateur sous forme de contraintes de rang. La méthode proposée est constructive et utilise les inverses généralisées de matrices. [Bhattacharyya 78] utilise une approche géométrique.
La plupart des procédures reposent sur le même principe : le vecteur d'état est divisé en deux parties par une transformation linéaire. La première partie est influencée directement par les entrées inconnues : elle doit donc être mesurée totalement. La seconde partie, libre de toute perturbation inconnue, est estimée par l'UIO d'ordre réduit. Ainsi [Kobayashi 87] met-il au point un algorithme d'inversion, repris par [Liu 02] qui propose un observateur exponentiel. Le système linéaire étudié dans cet article est de la forme suivante :

$$\begin{array}{rcl} \dot{x}(t) & = & Ax(t) + \Gamma(u(t), y(t)) + Bd(t) \\ y(t) & = & Cx(t) \end{array} \tag{1.38}$$

où $x \in \mathbb{R}^n$ est l'état du système, $y \in \mathbb{R}^{n_y}$ la sortie, $u \in \mathbb{R}^{n_u}$ l'entrée, $\Gamma(u, y)$ est une fonction non linéaire connue et $d \in \mathbb{R}^{n_d}$ est l'entrée inconnue. L'observateur proposé dans [Liu 02] est :

$$\dot{\hat{x}}(t) = A\hat{x}(t) + \Gamma(u(t), y(t)) + Bd(t) + K(y(t) - C\hat{x}(t)) \tag{1.39}$$

La perturbation $d(t)$ peut être estimée à partir des signaux disponibles :

$$\hat{d}(t) = F_1 y(t) + F_2 \dot{y}(t) + G_1 \hat{x}(t) + G_2 \dot{\hat{x}}(t) + G_3 \Gamma(u(t), y(t)) \tag{1.40}$$

les gains F_i et G_j, $i = 1, 2$, $j = 1, 3$ étant de dimensions appropriées.

Proposition 1.2.1 ([Liu 02])**.** *Si les conditions suivantes sont vérifiées :*

(i) il existe une matrice F_2 telle que $F_2CB - I_{n_d \times n_d} = 0$
(ii) il existe une matrice K telle que la matrice $A - B(F_1C + F_2CA) - KC$ soit stable (au sens de Hurwitz)
alors en posant $G_1 = -F_1C + F_2CA$, $G_2 = 0$ et $G_3 = -F_2C$, $\hat{x}(t)$ et $\hat{d}(t)$ convergent exponentiellement vers $x(t)$ et vers $d(t)$, respectivement. ▲

Si les hypothèses précédentes ne sont pas vérifiées, un autre observateur est proposé dans le même article, que nous ne détaillons pas ici.
La décomposition en valeurs singulières est utilisée dans [Fairman 84] qui propose une solution constructive au problème de synthèse d'UIO de systèmes linéaires.

Par ailleurs, les approches algébriques ont été largement développées : [Hou 92] propose un UIO d'ordre réduit, [Yang 88] traite le cas d'un UIO d'ordre plein, qui est analysé dans [Darouach 94] :

Théorème 1.2.2 ([Darouach 94])**.** *On considère le système LTI :*

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) + Dv(t) \\ y(t) = Cx(t) \end{cases} \tag{1.41}$$

$x \in \mathbb{R}^n$ est l'état du système, $u \in \mathbb{R}^k$ le vecteur des entrées connues, $v \in \mathbb{R}^m$ le vecteur des entrées inconnues, $y \in \mathbb{R}^p$ le vecteur des sorties.
Le système dynamique suivant :

$$\begin{cases} \dot{z}(t) = Nz(t) + Ly(t) + Gu(t) \\ \hat{x}(t) = z(t) - Ey(t) \end{cases} \tag{1.42}$$

est un observateur du système (1.41) *si et seulement si :*

(i) rang (CD) = rang (D)
(ii) rang $\begin{pmatrix} sP - PA \\ C \end{pmatrix} = n, \forall s \in \mathbb{C}, \mathcal{R}e(s) \geqslant 0$*, où* $P = I_n + EC$.

■

D'autres techniques ont été développées spécialement pour les systèmes singuliers. Par exemple la résolution d'une équation de Sylvester généralisée avec contraintes est détaillée dans [Darouach 96]. Cet article traite le cas des UIO d'ordre réduit en procédant à des transformations matricielles.
[Koenig 02] propose un nouvel observateur à entrées inconnues, de type proportionnel-intégral (PI), également pour les systèmes singuliers linéaires. Cet article généralise les résultats de l'article [Darouach 95] en utilisant les mêmes changements de coordonnées et autres substitutions.
Il considère un système du type :

$$\begin{aligned} E\dot{x}(t) &= Ax(t) + Bu(t) + Nf(t) \\ y(t) &= Cx(t) \end{aligned} \tag{1.43}$$

où $x \in \mathbb{R}^n$ est l'état du système, $u \in \mathbb{R}^{n_u}$ le vecteur des entrées connues, $f \in \mathbb{R}^{n_f}$ le vecteur des entrées inconnues, $y \in \mathbb{R}^m$ le vecteur des sorties et $E \in \mathbb{R}^{e \times n}$, les autres matrices étant de dimensions appropriées.
Les hypothèses structurelles sont moins restrictives que dans [Hou 92] et [Darouach 94] : on suppose simplement que $r = rang(E) \leqslant \min\{e, n\}$, rang $(N) = n_f$ et rang $(C) = m$.
On définit alors le système singulier augmenté :

$$\begin{array}{l} \begin{pmatrix} E & 0 \\ 0 & I \end{pmatrix} \begin{pmatrix} \dot{x}(t) \\ \dot{f}(t) \end{pmatrix} = \begin{pmatrix} A & N \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x(t) \\ f(t) \end{pmatrix} + \begin{pmatrix} B \\ 0 \end{pmatrix} u(t) \\ y(t) = \begin{pmatrix} C & 0 \end{pmatrix} \begin{pmatrix} x(t) \\ f(t) \end{pmatrix} \end{array} \tag{1.44}$$

Si le rang de $\begin{pmatrix} sE^T - A^T & C^T \end{pmatrix}^T$ est égal à n pour tout $s \in \mathbb{C}$, tel que $Re(s) \geqslant 0$ et si

$$rang \begin{pmatrix} E & A \\ 0 & E \\ 0 & C \end{pmatrix} = n + rang(E) \tag{1.45}$$

on peut définir l'observateur suivant :

$$\begin{array}{l} \dot{z}(t) = Fz(t) + L_1 y(t) + L_2 y(t) + Ju(t) + T_1 N \hat{f}(t) \\ \dot{\hat{f}}(t) = L_3(y(t) - \hat{y}(t)) \\ \hat{x}(t) = M_1 z(t) + T_2 y(t) \\ \hat{y}(t) = C\hat{x}(t) \end{array} \tag{1.46}$$

Le théorème suivant présente des conditions suffisantes de stabilité de l'erreur d'estimation de l'état et des entrées inconnues.

Théorème 1.2.3 ([Koenig 02])**.** *Si les conditions suivantes sont vérifiées :*

$$rang \begin{pmatrix} E \\ C \end{pmatrix} = n \tag{1.47}$$

$$rang \begin{pmatrix} sE - A & -N \\ 0 & sI_{n_f} \\ C & 0 \end{pmatrix} = n + n_f, \quad \forall s \in \mathbb{C}, \quad Re(s) \geqslant 0 \tag{1.48}$$

alors le système (1.46) *est un observateur asymptotique de* (1.44). ■

[Koenig 02] propose également un UIO d'ordre réduit. [Corless 98] s'intéresse à l'estimation de l'état et des entrées pour une classe de systèmes incertains. Plus récemment [Daafouz 06] propose une approche intrinsèque des UIO. Cet article établit des conditions nécessaires et suffisantes d'existence d'observateurs à entrées inconnues, en utilisant la théorie des modules.

Observateurs à entrées inconnues appliqués au diagnostic

Une autre catégorie d'articles traite le problème des UIO pour le diagnostic. En effet, les processus physiques subissent la plupart du temps des perturbations aussi diverses que des défauts de capteurs, des bruits, des incertitudes de mesures ou de modélisation. L'utilisation d'observateurs à entrées inconnues (ici, les entrées inconnues sont justement ces perturbations) permet d'estimer les perturbations, ou de les éliminer et ainsi de minimiser leur impact sur le système. Par exemple, [Wünnenberg 90] propose des UIO pour les systèmes affines en la commande et les mesures. Dans [Seliger 91], les entrées inconnues représentent les perturbations et les incertitudes de modélisation. En effet, le système étudié est le suivant :

$$\begin{aligned} \dot{x}(t) &= A(x(t),u(t)) + K(x(t),u(t))f(t) + E(x(t))d(t) \\ y(t) &= Cx(t) \end{aligned} \tag{1.49}$$

f matérialise les défauts de composants et d représente les perturbations et les erreurs de modélisation. Le but est de construire un observateur qui élimine totalement l'influence de d, tout en restant sensible aux défauts f, puisqu'il s'agit justement de détecter les défaillances des composants du système. On cherche alors une transformation linéaire de l'état $z = T(x)$ pour que le système résultant ne soit plus influencé par les incertitudes d. Dans ce cas, le modèle transformé a pour dynamique :

$$\dot{T}(x(t)) = \frac{\partial T}{\partial x}(x(t)).\left(A(x(t),u(t)) + K(x(t),u(t))f(t) + E(x(t))d(t)\right) \tag{1.50}$$

Il faut donc imposer :

$$\frac{\partial T}{\partial x}(x(t)).E(x(t)) = 0 \tag{1.51}$$

Le modèle transformé (1.50) se réduit alors à :

$$\dot{T}(x) = \frac{\partial T}{\partial x}(x(t)).\left(A(x,u) + K(x,u)f\right) \tag{1.52}$$

Ce modèle est dit à perturbations séparées, puisqu'il ne dépend plus des entrées inconnues d. [Seliger 91] utilise ensuite le théorème de Frobenius pour établir des conditions nécessaires et suffisantes pour l'existence d'une transformation T satisfaisant (1.51).
D'autres articles proposent également des solutions pour concevoir des UIO appliqués à la détection de défauts ou à la génération de résidus : [Gaddouna 94] pour les systèmes linéaires, [Hammouri 99] pour les systèmes non linéaires...

Observateurs à entrées inconnues de systèmes non linéaires

Quelques articles traitent le cas des UIO pour les systèmes non linéaires. Ainsi l'article [Boutayeb 95] propose-t-il une approche qui consiste à transformer le système non linéaire initial (satisfaisant la condition de Lipschitz) en système singulier dans la dynamique duquel les entrées inconnues

n'interviennent pas. L'article propose ensuite une méthode constructive de synthèse d'observateurs d'ordre plein et d'ordre réduit. Cette technique, qui fait appel à la théorie de Lyapunov et aux transformations matricielles, sera utilisée au chapitre suivant pour la construction d'un observateur réduit (voir le paragraphe 2.4). Voici le principal résultat concernant l'observateur d'ordre plein pour les systèmes singuliers.
Étant donné le système singulier :

$$\begin{array}{l} E\dot{x}(t) = f(x(t)) \\ y(t) = h(x(t)) \end{array} \tag{1.53}$$

on définit l'observateur suivant :

$$\begin{array}{l} \dot{z}(t) = g(z(t), y(t)) \\ \hat{x}(t) = z(t) + Qy(t) \end{array} \tag{1.54}$$

Théorème 1.2.4 ([Boutayeb 95])**.** *Si les hyptohèses suivantes sont vérifiées :*
(i) rang $\begin{pmatrix} E \\ H \end{pmatrix} = n$*, où* $H = \dfrac{\partial h}{\partial x}(0)$*;*
(ii) la paire (PF, H) *est détectable ;*
alors il existe une matrice non singulière $\begin{pmatrix} P & Q \\ a & b \end{pmatrix}$ *telle que :*

$$\begin{pmatrix} P & Q \\ a & b \end{pmatrix} \begin{pmatrix} E \\ H \end{pmatrix} = \begin{pmatrix} I \\ 0 \end{pmatrix} \tag{1.55}$$

et l'observateur (1.54) *garantit que* $\hat{x} \to x$ *avec :*

$$g(z(t), y(t)) = Pf(\hat{x}(t)) + L(\hat{x}(t), y(t)) \tag{1.56}$$

et $L(\hat{x}(t), h(\hat{x}(t))) = 0$*,* $F = \dfrac{\partial f}{\partial x}(0)$*.* ■

[Sharma 04] propose une extension de l'article [Koenig 02] aux systèmes non linéaires affectés par des perturbations sur l'entrée et la sortie. L'idée repose à nouveau sur une séparation entre les perturbations et le reste du système par une série de transformations sur les équations d'état et de sortie. Lorsque cette séparation est achevée, un observateur est synthétisé pour la partie sans perturbation. [Pertew 05] traite le problème des UIO pour les systèmes non linéaires lipschitziens et utilise des techniques d'optimisation $\mathcal{H}_\infty$ pour la synthèse de l'observateur.

Les systèmes de communications exploitant le chaos représentent une application importante et plutôt nouvelle des UIO non linéaires. Ainsi plusieurs articles proposent de reconstruire le message contenant l'information tout en établissant la synchronisation entre l'émetteur et le récepteur : [Inoue 01] traite le cas des systèmes à temps discret, [Boutayeb 02] et [Ha 04] le

cas des systèmes à temps continu... Nous verrons au paragraphe 1.4 comment les techniques de synthèse d'UIO s'intègrent parmi les méthodes de cryptage chaotique.

1.3 Vers la synchronisation à base d'observateurs

Après un état de l'art (non exhaustif) des différentes techniques d'estimation d'état non linéaires, puis un tour d'horizon rapide des différents observateurs à entrées inconnues, nous abordons dans cette partie la notion de synchronisation.

Le terme "synchronisation" vient du grec "$\sigma\upsilon\gamma$" (syn) qui signifie "avec", et "$\chi\rho o\nu o\varsigma$" (chronos), qui signifie "temps". On peut donc donner une première définition de la synchronisation, à savoir : la synchronisation est un phénomène qui caractérise deux systèmes se comportant de la même façon en même temps. En fait, les manifestations de la synchronisation sont observées depuis le XVII^{ème} siècle. Le mathématicien hollandais Huygens a notamment remarqué que deux horloges à balancier placées contre un mur finissaient par avoir des mouvements identiques. D'où la définition de la synchronisation : deux signaux périodiques sont synchronisés s'ils ont des périodes identiques. Par conséquent, la synchronisation semble à première vue réservée aux mouvements périodiques. Par ailleurs, l'une des propriétés qui caractérise le chaos est justement l'absence de périodicité, ou *apériodicité* (voir l'annexe B) du comportement asymptotique. *A priori* il peut sembler totalement inconcevable de relier les deux phénomènes : synchronisation et chaos. Et pourtant, cette idée reçue a volé en éclats tout d'abord en 1983 [Yamada 83], et surtout en 1990, lorsque les deux chercheurs Pecora et Carroll ont montré [Pecora 90] que deux systèmes chaotiques peuvent se synchroniser. Leurs travaux novateurs ont totalement changé la façon d'appréhender les manifestations du chaos. En effet, jusque-là, l'apparition de phénomènes chaotiques dans l'évolution de systèmes dynamiques était redoutée car incontrôlable, et donc évitée à tout prix. La théorie du contrôle du chaos [Ott 90], puis les articles [Pecora 90], [Carroll 91] ont ainsi ouvert la voie à une recherche foisonnante sur les applications du chaos. Ensuite, le phénomène de synchronisation a rapidement été relié au problème plus général de l'estimation non linéaire [Morgül 96], [Nijmeijer 97], [Millérioux 97]. Après une présentation de ces approches, nous définirons les différents régimes de synchronisation, et nous terminerons par un aperçu des schémas de synchronisation développés dans la littérature. De nombreuses références à ce sujet peuvent être consultées dans [Pecora 97], [Boccaletti 02], [Aziz-Alaoui 06], [Millérioux 06]. On peut noter qu'il existe différents types de synchronisation, selon la nature de la connexion entre le système émetteur et le système récepteur (unidirectionnelle, bidirectionnelle). Dans ce mémoire, nous n'abordons que la synchronisation unidirectionnelle, de l'émetteur vers le récepteur. Ceci, afin d'insérer ce processus au sein d'un système de communications, dans lequel il joue un rôle central (ce sera l'objet de la section 1.4).

1.3.1 Position du problème

Les systèmes chaotiques sont caractérisés par un comportement imprévisible à long terme : ceci est dû à une extrême sensibilité aux conditions initiales (voir l'annexe B pour plus de détails), plus connue dans le langage courant sous l'appellation « effet papillon ». D'où la question suivante, longtemps restée sans objet : peut-on forcer deux systèmes chaotiques à suivre la même trajectoire ? La réponse est oui, même si cela pouvait sembler improbable avant 1990. En effet, même si un système chaotique génère un attracteur remarquable dans l'espace d'état, l'incertitude sur la position exacte du système, à un instant donné, sur l'attracteur, croît de façon exponentielle avec le temps. Ainsi une très petite incertitude sur les conditions initiales se propage et s'amplifie. Les exposants de Lyapunov, définis dans l'annexe B quantifient la vitesse à laquelle cette incertitude augmente. Malgré cette caractéristique qui pourrait sembler incompatible avec la définition même de synchronisation, Pecora et Carroll ont démontré dans leur article fondateur [Pecora 90] que les systèmes chaotiques ont, sous certaines conditions, la propriété de se synchroniser. Par la suite, [Morgül 96], [Nijmeijer 97] et [Millérioux 97] ont montré que le problème de la synchronisation des systèmes chaotiques s'intègre dans le contexte plus général d'estimation d'état non linéaire. Une étude générale du phénomène de synchronisation des systèmes chaotiques se trouve dans [Parlitz 99a], [Parlitz 99b] par exemple.

L'approche de Pecora et Carroll

L'article [Pecora 90] fait référence dans le domaine de la synchronisation des systèmes chaotiques. En effet, c'est le premier article à mentionner et à prouver l'existence d'un tel phénomène. Le principe de synchronisation proposé est appelé principe *maître-esclave* (*master-slave*, ou encore *drive-response*) en référence à la construction du schéma émetteur-signal transmis-récepteur.
On considère un système chaotique décrit par le modèle dynamique suivant :

$$\dot{x}(t) = f(x(t)) \tag{1.57}$$

Le vecteur d'état x est décomposé de la manière suivante :

$$(\Sigma) \quad x(t) = \begin{pmatrix} x_1(t) \\ x_2(t) \end{pmatrix}$$

ce qui donne la décomposition du système (1.57) en deux sous-systèmes :

$$\begin{array}{lrcl} (\Sigma_1) & \dot{x}_1(t) & = & f_1(x_1(t), x_2(t)) \\ (\Sigma_2) & \dot{x}_2(t) & = & f_2(x_1(t), x_2(t)) \end{array} \tag{1.58}$$

Ensuite, on crée un nouveau sous-système (Σ_2') identique au sous-système (Σ_2), dont l'entrée est x_1 :

$$(\Sigma_2') \quad \dot{x}_2'(t) = f_2(x_1(t), x_2'(t)) \tag{1.59}$$

Le système (Σ_1, Σ_2) est appelé système *maître*, et le sous-système (Σ_2') est appelé système *esclave*. On définit alors les notions suivantes :

Définition 1.3.1 (Synchronisation)**.** Si $\lim_{t\to\infty} \|x_2'(t) - x_2(t)\| = 0$, alors on dit que les systèmes (1.58) et (1.59) sont synchronisés. ♦

Définition 1.3.2 (Exposants de Lyapunov conditionnels)**.** Les exposants de Lyapunov du système esclave (1.59) dont l'entrée est une trajectoire particulière $x_1(t)$ sont appelés exposants de Lyapunov conditionnels. ♦

Pecora et Carroll ont établi le résultat suivant :

Théorème 1.3.1 ([Pecora 90])**.** *Les systèmes* (1.58) *et* (1.59) *sont synchronisés si et seulement si tous les exposants de Lyapunov conditionnels de* (1.59) *sont négatifs.* ■

Cette méthode a été appliquée par exemple à un circuit électronique dans les articles [Carroll 91] et [Carroll 92], à deux systèmes de Lorenz dans [Oppenheim 92], à deux circuits de Chua dans [Ogorzalek 93], ou encore à des systèmes de Lur'e comportant des retards dans [Yalcine 01].
On notera que, par construction, on ne peut choisir qu'un nombre fini de décompositions du vecteur d'état x sous la forme (x_1/x_2), et pour certaines de ces décompositions, les hypothèses du Théorème 1.3.1 ne sont pas remplies. Pour garantir la synchronisation en utilisant la méthode de Pecora et Carroll, il faut trouver une décomposition qui donne des exposants de Lyapunov conditionnels négatifs. Cette méthode ne donne pas de procédure systématique pour construire un récepteur à partir de l'émetteur et en outre, le critère des exposants de Lyapunov conditionnels ne semble pas très facile à mettre en pratique.

La décomposition active-passive

Une généralisation du schéma de synchronisation maître-esclave est proposée par [Kocarev 95], et dénommée décomposition *active-passive*. Cette technique considère un système chaotique autonome :

$$\dot{z}(t) = F(z(t)) \tag{1.60}$$

et le réécrit sous la forme d'un système non autonome, que l'on choisit comme émetteur :

$$\dot{x}(t) = f(x(t), s(t)) \tag{1.61}$$

avec $s(t) = h(x(t))$ ou $\dot{s}(t) = h(x(t), s(t))$.
Le récepteur est alors une copie du système non autonome (1.61), le signal $s(t)$ étant le signal transmis par l'émetteur :

$$\dot{y}(t) = f(y(t), s(t)) \tag{1.62}$$

La synchronisation entre l'émetteur et le récepteur est possible si les exposants de Lyapunov du système (1.61) sont négatifs. Dans ce cas, le système (1.61) est un système passif qui tend naturellement vers un point fixe en l'absence de commande. D'où le nom de décomposition active-passive, qui désigne la décomposition donnée par h et f.

Contrairement au principe de Pecora et Carroll qui propose un nombre fini de décompositions possibles, la méthode de décomposition active-passive laisse une totale latitude quant au choix de la fonction h.

Approche utilisant des observateurs

[Morgül 96], [Nijmeijer 97] et [Millérioux 97] ont montré que la théorie de l'estimation non linéaire peut être naturellement utilisée dans le domaine de la synchronisation des systèmes chaotiques. En effet, le récepteur peut être une copie de l'émetteur, mais ce n'est pas une nécessité : il suffit que le récepteur, à partir du signal transmis, se synchronise avec la dynamique de l'émetteur. Il s'agit donc bien d'un problème d'observation. La partie précédente 1.1 propose de nombreux outils pour résoudre de façon variée le problème de la synchronisation des systèmes chaotiques. C'est pourquoi nous ne détaillons pas plus cette approche.

1.3.2 Différents régimes de synchronisation

Plusieurs régimes de synchronisation ont été proposés dans la littérature, parmi lesquels on peut retenir quelques notions de base. On pourra se reporter aux articles de références [Boccaletti 02] et [Aziz-Alaoui 06] par exemple pour plus de détails.On distingue les régimes de :

– *synchronisation identique, ou complète [Pecora 90], [Boccaletti 02], [Ahan 03] :* l'état du récepteur converge asymptotiquement vers l'état de l'émetteur. On considère deux systèmes dynamiques

$$\dot{x}(t) = f(x)(t) \tag{1.63}$$

et

$$\dot{x}'(t) = f'(x'(t)) \tag{1.64}$$

Alors (1.63) et (1.64) sont identiquement synchronisés si, quelles que soient leurs conditions initiales :

$$\lim_{t\to\infty} \|x'(t) - x(t)\| = 0 \tag{1.65}$$

– *synchronisation généralisée [Rulkov 95], [Ahan 03] :* cela correspond à une généralisation du concept de synchronisation identique. Les systèmes (1.63) et (1.64) se synchronisent, au sens

généralisé, s'il existe une transformation M telle que :

$$\lim_{t\to\infty} \|x'(t) - M(x(t))\| = 0 \tag{1.66}$$

et ce, indépendamment des conditions initiales. Si la fonction M est inversible, alors $M^{-1}(x')$ fournit une estimation de l'état x. Mais si cette transformation n'est pas inversible, on ne peut pas estimer x. Cela représente un inconvénient majeur pour certaines techniques de communication, qui utilisent l'état de l'émetteur pour décrypter le message transmis.

– *synchronisation de phase [Chen 03] :* Pour deux systèmes périodiques de phases ϕ_1 et ϕ_2, la synchronisation est exprimée par la relation $|n\phi_1 - m\phi_2| < c$, où m, n sont des entiers naturels et c est une constante positive. Cette notion classique de synchronisation a été étendue aux systèmes chaotiques. Parmi les approches proposées dans [Rosenblum 96] pour définir la phase d'un système chaotique, on peut mentionner l'approche analytique. Un signal analytique $\psi(t)$ est une fonction complexe définie par :

$$\psi(t) = s(t) + j\tilde{s}(t) = A(t)e^{j\phi(t))} \tag{1.67}$$

où $\tilde{s}(t)$ est la transformée de Hilbert de la série temporelle $s(t)$ (V.P. signifie la valeur principale de Cauchy de l'intégrale) :

$$\tilde{s}(t) = \frac{1}{\pi} V.P. \int_{-\infty}^{\infty} \frac{s(\tau)}{t-\tau} d\tau \tag{1.68}$$

Par analogie avec les systèmes périodiques, dans l'expression (1.67), $A(t)$ est l'amplitude du signal $\psi(t)$ et $\phi(t)$ sa phase.
On dit alors qu'il se produit une synchronisation de phase entre deux systèmes chaotiques couplés si $|n\phi_1(t) - m\phi_2(t)| < c$. Dans ce cas, les amplitudes de ces systèmes restent non corrélées.

– *synchronisation retardée [Li 86] :* l'état du système esclave converge vers l'état décalé dans le temps du système maître, c'est-à-dire :

$$\lim_{t\to\infty} \|x'(t) - x(t-\tau)\| = 0 \tag{1.69}$$

– *synchronisation par impulsions [Yang 97a] :* on considère un système maître de la forme

(1.63). On définit une suite d'instants discrets $\{\tau_i, i = 1, 2, \ldots\}$. A chaque instant τ_i, $i = 1, 2, \ldots$, le signal $y(t) = Cx(t)$ est envoyé par le système maître au système esclave, dont les variables d'état subissent un saut. Le système esclave est défini par le système différentiel impulsionnel suivant sachant que le système maître a pour modèle dynamique (1.63) :

$$\begin{cases} \dot{x}'(t) = f(x'(t)), \quad t \neq \tau_i \\ \Delta x' \mid_{t=\tau_i} = -PC(x(\tau_i) - x'(\tau_i)), \quad i = 1, 2, \ldots \end{cases} \tag{1.70}$$

où P est le gain de contrôle.

– *synchronisation projective [Mainieri 99] :* l'état du système récepteur se synchronise avec un multiple de l'état du système émetteur. Il existe donc a et τ tels que :

$$\lim_{t \to \infty} \|x'(t) - ax(t - \tau)\| = 0 \tag{1.71}$$

Ce type de synchronisation est utilisé pour les systèmes "partiellement linéaires" (voir [Mainieri 99] pour plus de détails), et permet de synchroniser, à un facteur près, les états qui ne peuvent être synchronisés.

1.3.3 Quelques schémas de synchronisation

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 au paragraphe 1.1. On peut distinguer plusieurs courants dans la conception de ces schémas de synchronisation.
La majorité des articles sur la synchronisation chaotique concerne des travaux utilisant des observateurs de type "grand gain" (définis au paragraphe 1.1.5), exploitant le fait que la plupart des systèmes chaotiques utilisés possèdent des nonlinéarités lipschitziennes. Parmi les nombreuses références disponibles dans la littérature, on peut citer [Liao 99] qui propose un schéma de communications sécurisées utilisant la synchronisation chaotique, appliqué aux systèmes de Lorenz et Rössler. Il construit un observateur qui garantit une convergence exponentielle de l'erreur de synchronisation vers zéro. [Boutayeb 02] propose une généralisation à une plus grande classe de systèmes non linéaires. [Alvarez-Ramirez 01] détaille 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. Le phénomène de synchronisation est présenté sous la forme d'un problème de suppression de chaos dans [Femat 01]. [Jiang 03] a mis au point un critère de synchronisation utilisant une commande par retour d'état linéaire, appliquée au circuit de Chua. Ce critère est étendu dans [Jiang 05]. [Feki 03] propose un observateur réduit permettant la synchronisation exponentielle de l'émetteur et du récepteur. Dernièrement, [Celikovsk$\acute{y}$ 05] traite le problème de la synchronisation des systèmes chaotiques par la théorie de la commande, et dé-

taille un processus de synchronisation globale exponentielle. La théorie des modes glissants est à l'origine du schéma de synchronisation présenté dans [Chen 05]. Une comparaison de différentes techniques de synchronisation, appliquées à des systèmes chaotiques connus, est détaillée dans [Haeri 06].
Dans ce mémoire, le problème de la synchronisation des systèmes chaotiques est uniquement considéré du point de vue de l'estimation d'état. Dans la suite, nous utiliserons donc indifféremment l'expression « estimation d'état » et le terme « synchronisation ».

1.4 Systèmes de communication

Désormais, nous savons qu'il est possible d'estimer l'état des systèmes chaotiques, qui constituent une classe particulière de systèmes non linéaires. Cette capacité de synchronisation, dérivant de la théorie plus générale du contrôle du chaos (dont les bases ont été posées dans [Ott 90]), a ouvert la voie à de nombreuses applications, parmi lesquelles nous avons retenu les systèmes de communications sécurisées.

1.4.1 Introduction

Les schémas de communication exploitant la synchronisation des systèmes chaotiques appartiennent au domaine général de reconstruction d'entrées inconnues. Les systèmes chaotiques constituent une classe particulière de systèmes non linéaires, il est donc possible de leur appliquer tous les résultats vus précédemment. Un système de communications utilisant le chaos représente une application prometteuse de l'estimation d'état des systèmes non linéaires. Un schéma général de communications est représenté à la figure 1.2. A partir d'un message contenant l'information $u(t)$, l'émetteur génère un signal qui est transmis au récepteur par l'intermédiaire d'un canal (air, câble électrique...) Le récepteur reconstruit alors le message original, grâce à une "clé" partagée avec l'émetteur.
Dans ce mémoire, nous nous intéressons uniquement aux systèmes de communications à por-

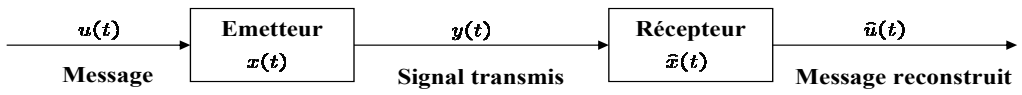


FIG. 1.2 - *Principe général d'un système de communications*

teuse chaotique : l'émetteur du schéma 1.2 est un système chaotique, et le signal transmis $y(t)$ est donc un signal chaotique. La série d'articles [Kolumbán 97], [Kolumbán 98] présente le lien entre ces nouvelles techniques utilisant le chaos et les techniques "classiques" de cryptage numérique, qui ne seront pas abordées ici. Par ailleurs, nous nous limiterons au cas des systèmes continus, pour envoyer tout type de message, aussi bien continu que discret.

1.4.2 Cryptage par addition

Cette méthode est la première chronologiquement à utiliser la synchronisation du chaos. Elle est présentée dans les références [Kocarev 92], [Cuomo 93], [Morgül 99]. L'idée repose sur l'observation des signaux chaotiques : *a priori*, ils ressemblent à du bruit, comme le montre la figure 1.3.

Le principe est alors très simple : il suffit d'ajouter le message utile $u(t)$ à une porteuse chaotique, de façon à "noyer" l'information dans du bruit. Par conséquent, un intrus ne soupçonnera pas qu'un message est transmis, même s'il intercepte le signal $y(t)$ (porteuse chaotique + message), et donc ne cherchera pas à appliquer des techniques de décryptage. Au niveau du récepteur autorisé, après synchronisation grâce au signal reçu, on obtient le message original par soustraction, voir le schéma de la Figure 1.4.

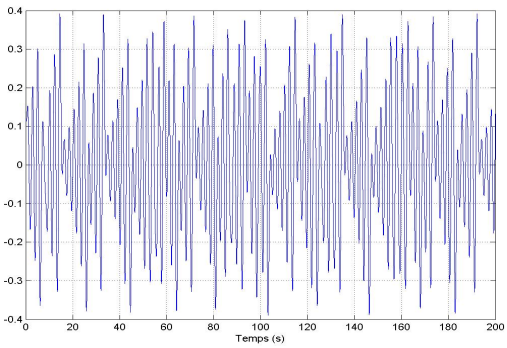


FIG. 1.3 - *Signal chaotique (trajectoire du deuxième état du circuit de Chua, voir Annexe B)*

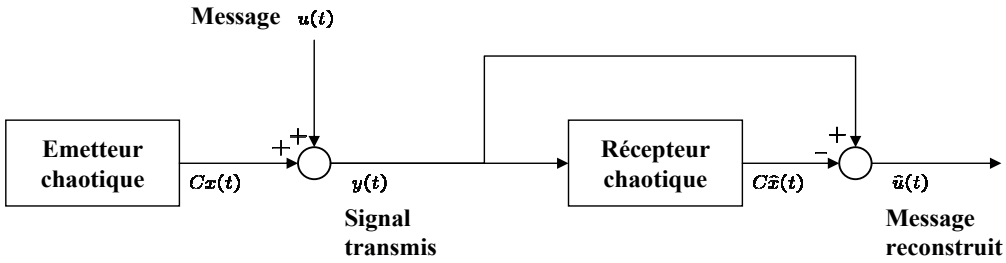


FIG. 1.4 - *Principe du cryptage par addition*

Le principal avantage de cette méthode réside dans la simplicité du cryptage. On peut souligner que cette technique peut être appliquée à des messages continus ou discrets. Dans les deux cas, il est impératif que l'amplitude du message original soit significativement plus petite que celle de la porteuse chaotique, d'une part pour ne pas perturber l'établissement de la synchronisation au niveau du récepteur, et d'autre part pour garantir le secret de la transmission. Dans tous les

cas, à cause de la présence du message, la synchronisation ne peut être parfaite. En outre, la fréquence du message doit être comprise dans le spectre du signal chaotique. Un autre problème qui se pose naturellement concerne la présence d'un bruit additif au niveau du canal de transmission. Dans ce cas, il faut que l'amplitude du message soit plus grande que celle du bruit. Il y a donc un compromis à trouver entre la sécurité de la transmission, et la robustesse au bruit. Ce compromis va s'exprimer dans toutes les techniques que nous présentons dans ce mémoire.

1.4.3 Cryptage par commutation

Cette technique, exposée dans [Dedieu 93], [Parlitz 93], est réservée aux messages prenant un nombre fini de valeurs. Pour plus de simplicité, nous traitons le cas des messages binaires : $u(t) \in \{0, 1\}$. L'émetteur est constitué de deux systèmes chaotiques : ces deux systèmes peuvent avoir le même modèle dynamique, avec des paramètres différents, ou avoir deux modèles dynamiques totalement différents.

La figure 1.5 illustre le principe du cryptage par commutation : selon la valeur de $u(t)$ à l'ins-

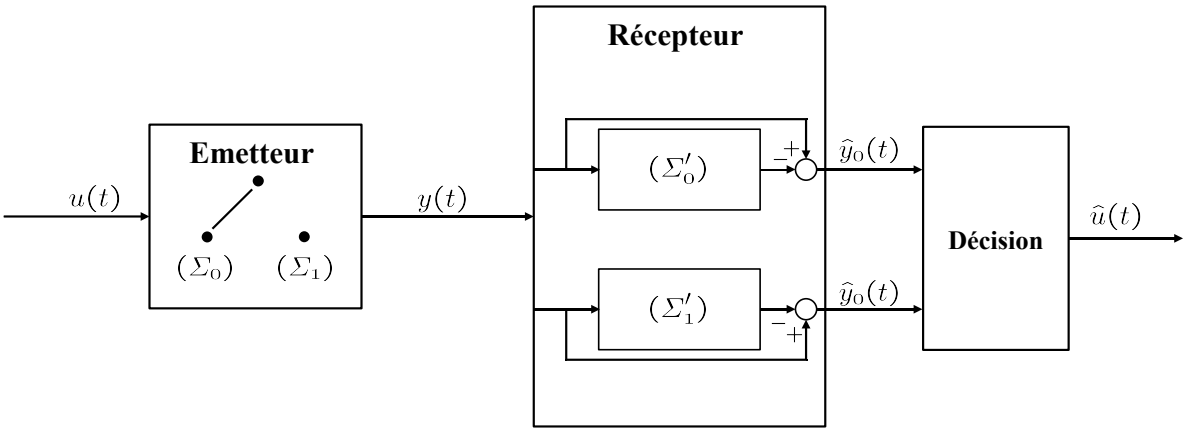


FIG. 1.5 - *Principe du cryptage par commutation*

tant t (c'est-à-dire $u(t) = 0$ ou $u(t) = 1$), l'émetteur est soit le système chaotique Σ_0, soit le système Σ_1. La sortie $y(t)$ est transmise à deux copies Σ'_0, Σ'_1 des émetteurs chaotiques, de sorties respectives $\hat{y}_0(t)$ et $\hat{y}_1(t)$. Si $u(t)$ prend la valeur 0, alors Σ'_0 se synchronise, et Σ'_1 ne se synchronise pas. Ainsi, l'erreur de synchronisation $e_0(t) = \hat{y}_0(t) - y(t)$ va tendre vers 0, tandis que l'erreur $e_1(t) = \hat{y}_1(t) - y(t)$ sera d'amplitude non nulle. Le processus est symétrique lorsque le message prend la valeur 1. Par comparaison des valeurs des intégrales des carrés des erreurs $e_0^2(t)$ et $e_1^2(t)$, la valeur du message $u(t)$ est facilement retrouvée pendant l'intervalle de temps entre deux commutations. Notons que cet intervalle doit être suffisamment long pour que la synchronisation puisse s'établir. Cette méthode a l'énorme avantage d'être robuste au bruit : en effet, au niveau du récepteur, on détermine la valeur exacte du message soit en évaluant l'erreur de synchronisation au niveau des deux copies comme précédemment, soit par corrélation entre

le signal $y(t)$ reçu et les signaux $\hat{y}_0(t)$ et $\hat{y}_1(t)$. Dans ce dernier cas, il s'agit de déterminer quel signal chaotique généré par les deux copies "ressemble" le plus au signal reçu. La corrélation minimise l'influence du bruit sur l'erreur de synchronisation. En revanche, le taux de transmission du cryptage par commutation est assez bas, car un signal binaire contient moins d'information qu'un signal analogique, et le temps nécessaire à l'établissement de la synchronisation est perdu à chaque fois que le message change de valeur. En outre, la sécurité n'est plus garantie si les deux ensembles de paramètres correspondant à Σ_0 et Σ_1 sont trop différents, car on peut observer les changements de système chaotique émetteur au niveau du signal transmis : cela est dû aux caractéristiques propres à chaque système chaotique, qui possède des trajectoires bien spécifiques. On peut constater la différence entre les trajectoires des systèmes chaotiques présentés dans l'annexe B par exemple.

1.4.4 Cryptage par modulation

Cette technique, développée dans [Halle 93], [Cuomo 93], [Yang 96], [Tang 02], 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 1.6.

Au niveau de l'émetteur, le fait de moduler un (ou plusieurs) paramètre(s) impose à la tra-

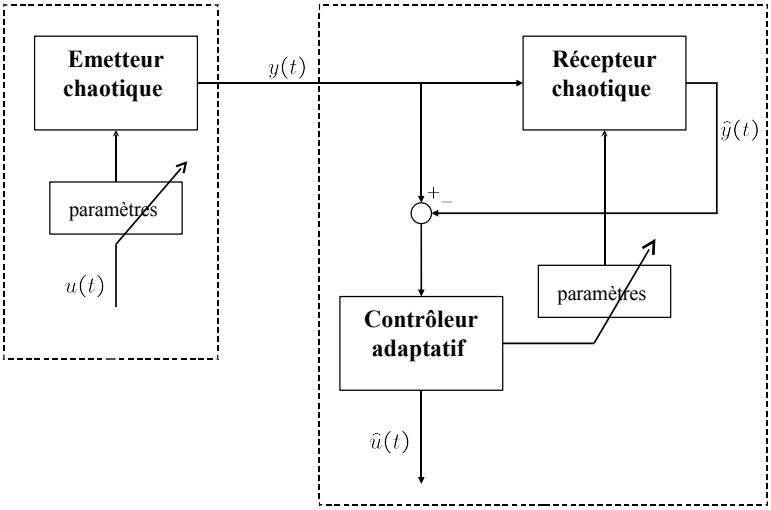


FIG. 1.6 - *Principe du cryptage par modulation*

jectoire 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 "classiques". Cependant, le cryptage par modulation s'est avéré sensible à certaines attaques détaillées dans

les références [Short 96], [Yang 98b].

1.4.5 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.

1.4.5.1 Observateurs à entrées inconnues

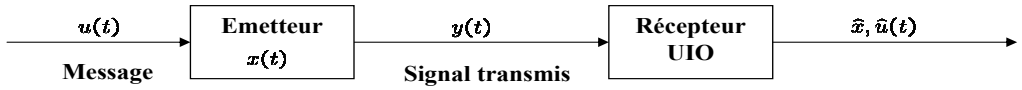


FIG. 1.7 - *Observateur à entrées inconnues*

Le schéma de la figure 1.7 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 présentées dans la section 1.2, et peuvent être utilisées à des fins de décryptage. Parmi les articles utilisant les UIO pour décrypter l'information, on peut citer [Inoue 01], [Millérioux 04] qui traitent le cas des systèmes à temps discret, et [Ha 04] qui généralise les résultats établis dans [Liao 99], [Boutayeb 02].

1.4.5.2 Décryptage par inversion

L'article [Feldmann 96] présente un processus de décryptage par inversion, *i.e.* le récepteur est conçu en inversant le modèle de l'émetteur.

Définition 1.4.1 (Système inverse)**.** On considère deux systèmes, Σ_1 et Σ_2. Alors Σ_2 est un système inverse de Σ_1 si :

(i) l'ensemble E des entrées admissibles de Σ_1 coïncide avec l'ensemble des sorties de Σ_2, et l'ensemble E' des entrées admissibles de Σ_2 coïncide avec l'ensemble des sorties de Σ_1 ;

(ii) pour tout signal $u \in E$ et toute condition initiale du système Σ_1, il existe une condition initiale du système Σ_2, telle que pour tout $t \geqslant 0$, $u(t) = \hat{u}(t)$;

(iii) la condition (ii) est vraie en échangeant les rôles de Σ_1 et Σ_2.

♦

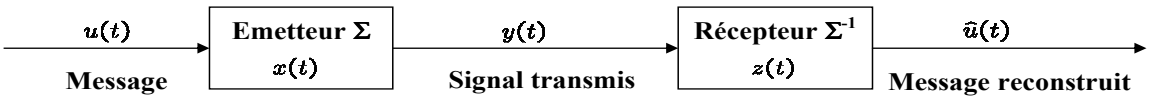


FIG. 1.8 - *Principe du cryptage par inversion*

La figure 1.8 présente le principe général de cette approche cryptage par inclusion-décryptage par inversion :

$$\begin{aligned} y &= \Sigma(u, x) \\ \hat{u} &= \Sigma^{-1}(y, z) \end{aligned} \tag{1.72}$$

1.4.6 Cryptage mixte

Pour pallier les problèmes de sécurité des méthodes précédentes, [Yang 97b] a proposé une nouvelle technique qui combine les principes de la cryptographie standard et la synchronisation chaotique. Le message $u(t)$ contenant l'information est crypté grâce à une clé, $c(t)$, générée par l'émetteur chaotique. Le message crypté $u_c(t)$ est alors injecté dans la dynamique du système chaotique, pour la rendre plus complexe. Ensuite, un signal $y(t)$ fonction des variables d'état de l'émetteur est transmis au récepteur, qui établit une synchronisation avec l'émetteur. La clé est alors reconstruite par le récepteur, qui peut finalement décoder le message. Le principe général de cette méthode est illustré à la figure 1.9.

Effectivement, grâce à la complexité du processus de cryptage, cette nouvelle génération de

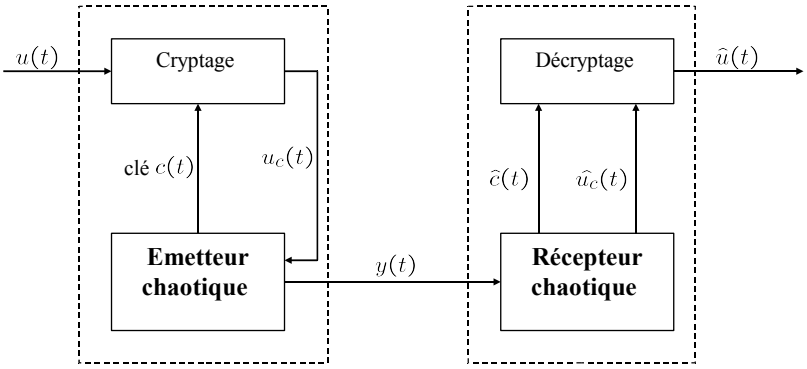


FIG. 1.9 - *Cryptage mixte*

cryptosystèmes s'est révélée jusqu'ici plus robuste aux attaques classiques.

1.4.7 Transmission à deux voies

Dans le schéma présenté à la figure 1.10, l'émetteur envoie deux signaux au récepteur. Le premier, y, est une fonction à valeurs réelles de l'état x du système chaotique émetteur, dont l'unique

but est de permettre la synchronisation du récepteur. Le second, y_2 - envoyé éventuellement sur un autre canal - est un signal chaotique qui contient l'information à transmettre. Le principe a

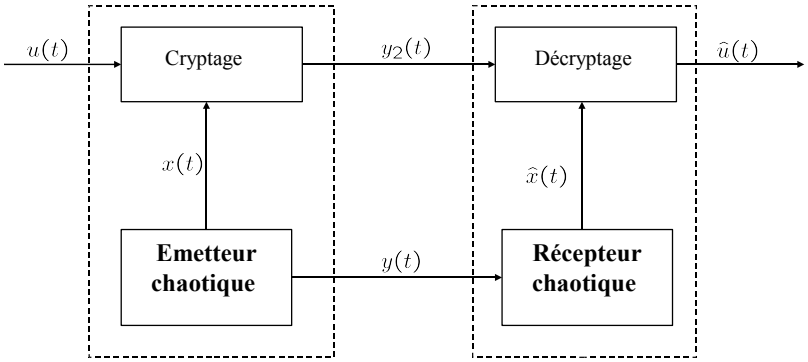


FIG. 1.10 - *Transmission à deux voies*

été utilisé dans les articles [Millérioux 98] et [Jiang 02]. Parmi les avantages de cette méthode, on peut souligner d'une part que le signal y ne contient aucune information, par conséquent la synchronisation peut s'établir de façon optimale. D'un autre côté, le second signal y_2 contient l'information qui peut être soit cryptée par une fonction non linéaire de l'état x comme proposé dans la référence [Jiang 02], soit simplement masquée par un signal chaotique généré par l'émetteur, qui sert de porteuse. On peut noter également que les deux étapes de synchronisation et de cryptage étant totalement indépendantes, le décryptage n'est pas nécessairement effectué, au niveau du récepteur, en même temps que la synchronisation.

1.5 Conclusion

Ce premier chapitre a présenté les notions fondamentales abordées dans ce mémoire. En tenant compte du rôle central joué par les observateurs non linéaires dans nos travaux de recherche, nous avons tout d'abord passé en revue différentes techniques d'estimation d'état. A ce titre, après un bref rappel du problème dans le cadre des systèmes linéaires, nous avons présenté successivement les approches stochastiques, les approches nécessitant une transformation (ou techniques de linéarisation de l'erreur d'estimation), les observateurs à grand gain, pour terminer par les observateurs à structure variable. Cette liste est loin d'être exhaustive, mais présente les principales approches que l'on peut trouver dans la littérature. Nos travaux ne se sont pas penchés uniquement sur l'estimation de l'état d'un système, ils ont également porté sur la restauration d'entrées inconnues. Ainsi, dans un deuxième temps, avons-nous fait un tour d'horizon des différents observateurs à entrées inconnues existants. Ces bases sur l'estimation de l'état et des entrées inconnues étant posées, nous avons pu considérer une application de ces techniques, à savoir la synchronisation des systèmes chaotiques, qui forment une classe particulière de systèmes non linéaires. Dans la troisième partie de cet état de l'art, nous avons défini la notion de synchronisation appliquée aux systèmes chaotiques ainsi que ses différents régimes, et nous

avons retenu la synchronisation identique (ou complète). Dans la suite, lorsqu'il n'y aura pas de confusion possible, nous omettrons le qualificatif "complète", et nous parlerons simplement de synchronisation. La recherche dans ce domaine a commencé dans les années 1990 avec l'article de Pecora et Carroll [Pecora 90] qui fait référence aujourd'hui. En 1997, plusieurs articles [Morgül 96], [Nijmeijer 97] et [Millérioux 97] ont jeté un regard nouveau sur ce problème, et ont montré que des techniques d'estimation d'état permettent de le résoudre. La quatrième partie de cet état de l'art a été consacrée aux systèmes de communications sécurisées reposant sur la synchronisation à base d'observateurs, et appartenant au domaine de la reconstruction d'entrées inconnues. Nous avons présenté le principe des techniques de cryptage exploitant le chaos, à savoir le cryptage par addition, par commutation, par modulation, par inversion, le cryptage mixte, pour terminer par la technique de transmission à deux voies.
Dans le chapitre 2, nous appliquons des techniques d'estimation d'état (il s'agit principalement de techniques "à grand gain") pour établir la synchronisation de systèmes chaotiques possédant une structure particulière. La conception des observateurs est suivie par une analyse détaillée de la convergence asymptotique ou exponentielle de l'état estimé vers l'état réel du système chaotique. Cette analyse fait appel notamment à la théorie de la stabilité de Lyapunov, pour les systèmes dynamiques classiques, et de Lyapunov-Krasovskii, pour les systèmes à retard. Les résultats énoncent des conditions suffisantes de synchronisation (asymptotique ou exponentielle), sous la forme d'inégalités linéaires ou bilinéaires matricielles (LMI ou BMI), pour la résolution desquelles on dispose d'algorithmes numériques puissants d'optimisation convexe (modulo un éventuel changement de variable pour les BMI). Ces différents outils utilisés tout au long de ce deuxième chapitre sont regroupés dans les annexes A et C. A la fin de ce chapitre, nous proposons la synthèse d'un observateur robuste au bruit, qui constitue un problème important dans le domaine de l'estimation d'état. Les observateurs que nous avons conçus sont intégrés dans un système de communications utilisant le chaos que nous présentons au chapitre 3. Notre méthode repose sur le principe de transmission à deux voies. L'étape de synchronisation est ainsi réalisée grâce à l'un des observateurs conçus au chapitre 2. La seconde étape, qui correspond à la transmission sécurisée de l'information, est mise en oeuvre selon un nouveau procédé que nous avons mis au point, qui permet le cryptage, puis la restauration de l'entrée inconnue, après la synchronisation de l'observateur.

CHAPITRE

2 Synchronisation utilisant des observateurs

Sommaire

2.1 Introduction

Ce chapitre est consacré à l'étude des différents schémas de synchronisation que nous avons élaborés, à partir de résultats classiques de la théorie de l'estimation non linéaire. On rappelle que le principe est illustré par le schéma de la figure 1.1. Dans la suite de ce mémoire, la terminologie employée est légèrement différente de celle utilisée dans le domaine de l'estimation d'état standard. Ainsi, le système dont l'état $x(t)$ est à estimer sera désigné comme étant l'*émetteur* ; le système dynamique chargé d'estimer l'état $x(t)$ sera appelé *observateur* ou *récepteur*, et ce, de façon équivalente. Cette dénomination trouvera son explication au chapitre suivant, lorsque les techniques d'estimation d'état que nous allons détailler seront intégrées dans des schémas de communication. La phase de synchronisation se décompose en trois étapes principales, à savoir : le choix de l'émetteur, la conception du récepteur et l'analyse de la synchronisation. Le problème à résoudre est sensiblement plus vaste qu'un problème standard d'estimation d'état. Bien sûr, le cœur du problème de synchronisation reste la reconstruction de l'état du système émetteur, et l'analyse de la convergence de l'observateur. Cependant, le système émetteur, qui est un système non linéaire particulier, n'a pas une forme générale commune à tous les systèmes chaotiques. L'étape du choix de l'émetteur vient donc s'ajouter au problème standard d'estimation d'état. Ce choix est crucial, car sur lui repose toute la sécurité du système de communications du chapitre 3, à travers la définition de la clé secrète. Il est donc important de définir précisément ce choix de l'émetteur. Les deux émetteurs que nous avons retenus dans ce mémoire sont des systèmes chaotiques comportant un retard : il s'agit d'un circuit de Chua modifié, défini dans la littérature, et d'un second système que nous avons conçu en conservant la même structure, mais dont la partie non linéaire est une fonction tangente hyperbolique. Concernant la conception du récepteur, nos différentes approches ont en commun la synthèse d'observateurs, d'ordre plein ou d'ordre réduit. La théorie de la stabilité de Lyapunov (et plus particulièrement ici de Lyapunov-Krasovskii, puisqu'il s'agit de systèmes à retard), définie dans l'annexe A, est ensuite utilisée pour analyser la synchronisation, asymptotique ou exponentielle, des récepteurs avec les émetteurs correspondants. Les résultats présentés énoncent des conditions suffisantes de synchronisation, exprimées sous forme de BMI (voir l'annexe C). Les différents schémas de synchronisation proposés sont testés sur des simulations. La fin de ce chapitre est consacrée à la conception d'un observateur robuste au bruit. Ce problème classique en automatique est résolu en appliquant les principes de la théorie $\mathcal{H}_\infty$.

2.2 Description des émetteurs

Les systèmes chaotiques forment une classe particulière de systèmes non linéaires, dont les principales propriétés sont énoncées dans l'annexe B. Les systèmes de communications à base de systèmes chaotiques permettent de reconstruire des entrées inconnues, et exploitent tout particulièrement l'aspect aléatoire des signaux chaotiques transmis, ainsi que la très grande

sensibilité aux conditions initiales et aux paramètres de l'émetteur, sensibilité caractéristique des systèmes chaotiques. Ainsi, la sécurité de la plupart des systèmes de communication repose-t-elle sur la parfaite connaissance des paramètres du système, connaissance partagée par l'émetteur et le récepteur, ainsi que sur la complexité du signal chaotique transmis. En effet, la grande sensibilité des systèmes chaotiques implique que la moindre imprécision sur l'un des paramètres du système émetteur empêche tout intrus d'établir une synchronisation, et donc potentiellement de reconstruire le message transmis.
Il est donc tout à fait souhaitable que cette sensibilité soit la pus grande possible, et que le signal transmis soit le plus complexe possible.
Par ailleurs, les systèmes à retards ont fait l'objet de nombreuses études destinées à comprendre le rôle fondamental du retard dans de nombreux processus. Un condensé des différentes techniques inhérentes aux systèmes à retards se trouve dans les articles de synthèse [Kharitonov 99], [Richard 03]. Concernant plus particulièrement les systèmes chaotiques à retard, l'article [Farmer 82] a notamment prouvé que le nombre d'exposants de Lyapunov positifs augmente avec le retard, ce qui signifie que la sensibilité d'un système chaotique à retard est plus importante que celle d'un système chaotique classique, sans retard. En outre, en augmentant la valeur du retard, un système chaotique peut devenir hyperchaotique, c'est-à-dire qu'il possède plusieurs exposants de Lyapunov positifs, et son comportement devient beaucoup plus complexe. Les systèmes chaotiques à retard semblent donc particulièrement indiqués pour élaborer des schémas de communications sécurisées.

2.2.1 Circuit de Chua modifié

L'idée d'utiliser des systèmes chaotiques comportant un retard nous est venue à la lecture de la référence [Wang 01]. Cet article considère le circuit de Chua standard (voir l'annexe B) et montre que le fait d'ajouter un terme non linéaire avec retard dans la dynamique du système augmente la complexité du chaos généré. Cette conséquence remarquable de la présence d'un retour d'état avec retard est analysée plus largement dans l'article [Wang 00] : il s'agit de la théorie de l'*anti-contrôle* du chaos, dénommée ainsi par opposition à la théorie du contrôle du chaos [Ott 90], qui vise à supprimer le chaos en ajoutant un terme perturbateur de faible amplitude. Au contraire, la référence [Zhou 04] démontre que la présence d'un retour d'état retardé peut soit rendre chaotique un système non linéaire qui ne l'était pas, soit augmenter la complexité d'un système chaotique. Les travaux de [Wang 01] appliquent cette théorie d'anti-contrôle du chaos, et détaillent le circuit de Chua modifié suivant (voir l'annexe B pour la signification physique des différents paramètres) :

$$\left\{\begin{array}{lcl} \dfrac{dv_1}{dt}(t) & = & \dfrac{1}{C_1}(G(v_2(t)-v_1(t))+f(v_1(t))) \\ \dfrac{dv_2}{dt}(t) & = & \dfrac{1}{C_2}(i_3(t)-G(v_2(t)-v_1(t))) \\ \dfrac{di_3}{dt}(t) & = & -\dfrac{1}{L}(v_2(t)+R_0 i_3(t)+w(v_1(t-\tau))) \end{array}\right. \tag{2.1}$$

où f est la caractéristique non linéaire de la diode de Chua :

$$f(v_1(t)) = G_b v_1(t) + \frac{1}{2}(G_a - G_b)\left(|v_1(t) + E| - |v_1(t) - E|\right) \tag{2.2}$$

et la fonction comportant le retard est donnée par :

$$w(v_1(t-\tau)) = \varepsilon \sin(\sigma v_1(t-\tau))) \tag{2.3}$$

ε et σ sont deux constantes positives, et $\tau > 0$ est le retard.
Le modèle (2.1) peut se mettre sous la forme plus compacte :

$$\dot{x}(t) = Ax(t) + F(x(t)) + H(x(t-\tau)) \tag{2.4}$$

avec

$$x = \begin{pmatrix} v_1 \\ v_2 \\ i_3 \end{pmatrix} \tag{2.5}$$

$$A = \begin{pmatrix} -\frac{G}{C_1} & \frac{G}{C_1} & 0 \\ \frac{G}{C_2} & -\frac{G}{C_2} & \frac{1}{C_2} \\ 0 & -\frac{1}{L} & -\frac{R_0}{L} \end{pmatrix} \tag{2.6}$$

$$F(x(t)) = \begin{pmatrix} -\frac{1}{C_1} f(v_1(t)) \\ 0 \\ 0 \end{pmatrix} \tag{2.7}$$

$$H(x(t-\tau)) = \begin{pmatrix} 0 \\ 0 \\ -\frac{1}{L} w(v_1(t-\tau)) \end{pmatrix} \tag{2.8}$$

Notons que les deux fonctions non linéaires F et H sont Lipschitziennes (voir la définition (1.24)), de constantes respectives

$$k_F = \frac{1}{C_1} \max\{|G_a|, |G_b|\} \tag{2.9}$$

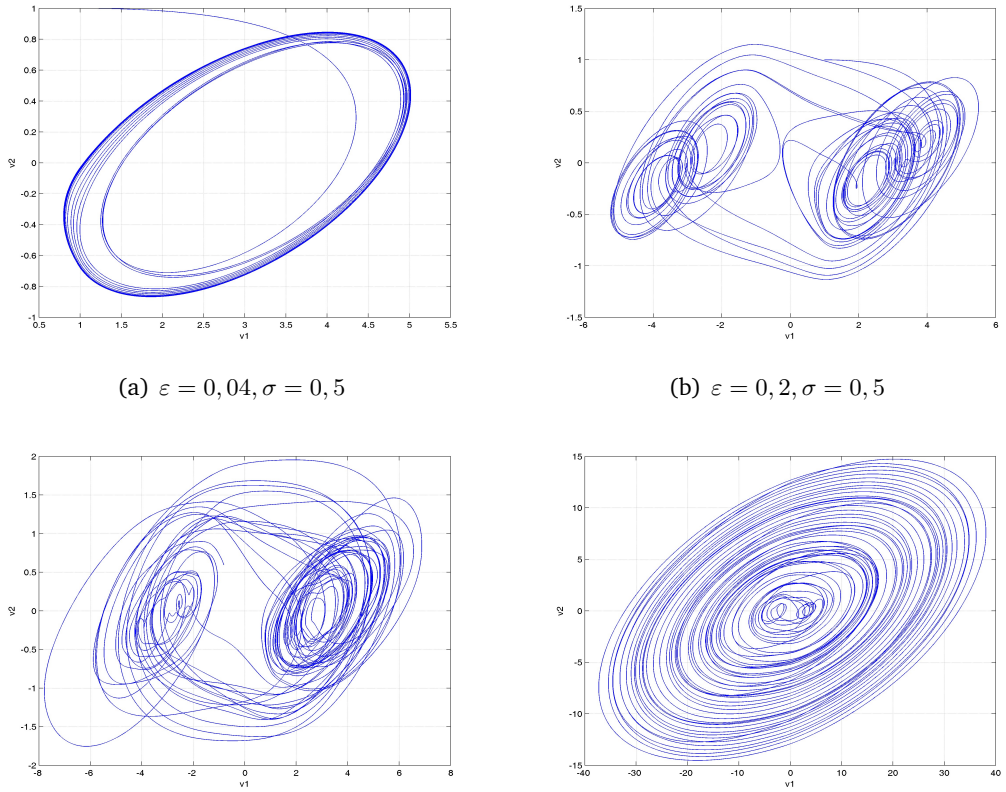
$$k_H = \frac{\varepsilon\sigma}{L} \tag{2.10}$$

[Wang 01] démontre que le système (2.1) est chaotique et génère des attracteurs variés, pour les valeurs de paramètres données dans le tableau 2.1, et pour différentes valeurs de ε et σ,

$R = 1/G$	C_1	C_2	L	R_0	G_a	G_b	E	τ
1910Ω	10nF	100nF	$18,68$mH	16Ω	$-0,75$ms	$-0,41$ms	1V	0.001s

TAB. 2.1 - *Paramètres du circuit de Chua modifié*

comme illustré à la figure 2.1.



(a) $\varepsilon = 0,04, \sigma = 0,5$ (b) $\varepsilon = 0,2, \sigma = 0,5$

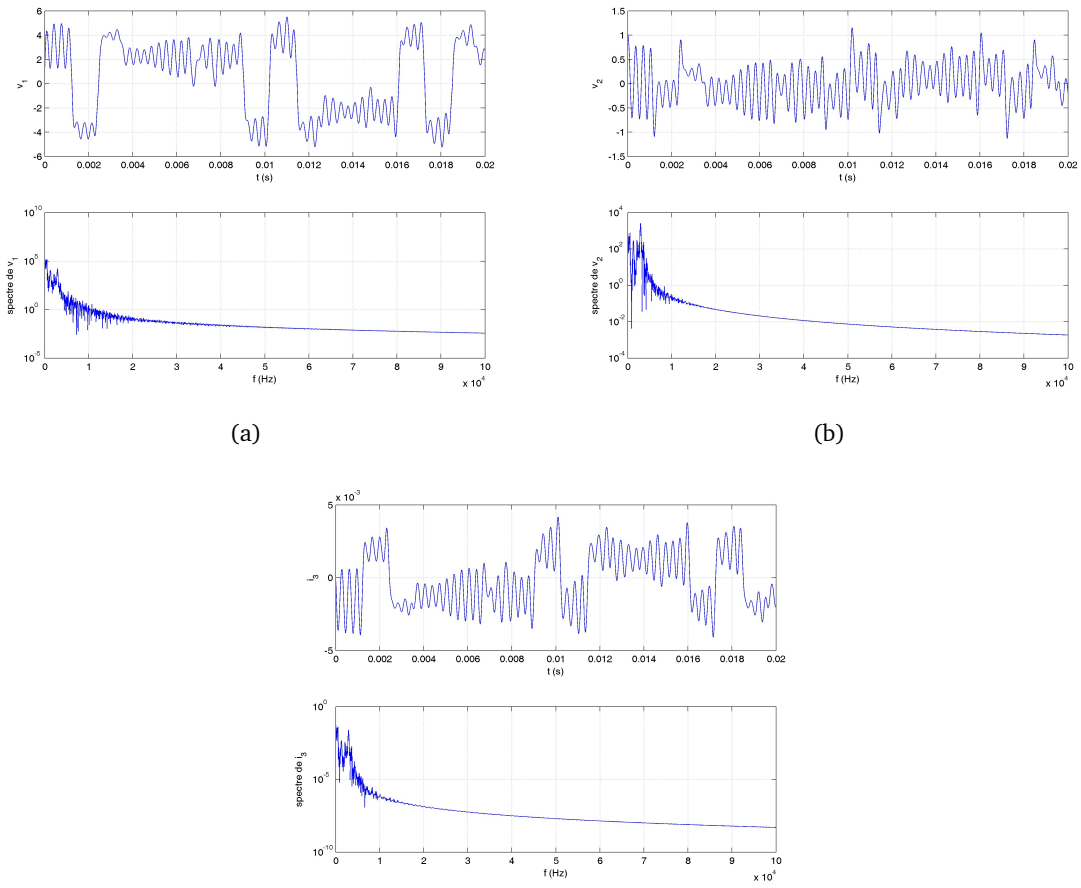
(c) $\varepsilon = 0,5, \sigma = 3$ (d) $\varepsilon = 1, \sigma = 1$

FIG. 2.1 - *Portraits de phase pour différentes valeurs de ε et σ*

La figure 2.2 représente les trajectoires de chacun des trois états du système (2.1), ainsi que les spectres de puissance correspondants, pour les valeurs de paramètres indiquées à la figure 2.1(b).

2.2.2 Système chaotique à tangente hyperbolique

D'après l'expression (2.2), la partie non linéaire du circuit de Chua est une fonction affine par morceaux, qui n'est donc pas dérivable sur $\mathbb{R}$. Ces ruptures de pente (et donc ces sauts dans la



(a) (b)

(c)

FIG. 2.2 - *Séries temporelles et spectres des trois états du circuit de Chua modifié*

valeur de la dérivée de f) confèrent au circuit de Chua un attracteur chaotique particulier, notamment la célèbre *double spirale* (voir la figure B.8 de l'annexe B). Dans l'article [Alaoui 00], le phénomène de multiplication des spirales a été mis en parallèle avec l'augmentation du nombre de points de rupture de pente de la nonlinéarité de Chua.
Parallèlement, [Franz 96] a proposé de remplacer la partie non linéaire "standard" du circuit de Chua par une autre fonction non linéaire impaire à valeurs réelles. Cet article analyse ainsi (plus facilement qu'avec une fonction affine par morceaux) le système chaotique obtenu en choisissant comme fonction non linéaire un polynôme de degré trois.
En adoptant ce principe, nous avons choisi de conserver la structure du circuit de Chua standard (sans dimension), tout en modifiant la partie non linéaire et en ajoutant un retour d'état comportant un retard.

Notations : pour alléger l'écriture, on note $x_\tau(t)$ au lieu de $x(t-\tau)$.

Le système chaotique retenu comme émetteur est décrit par le modèle suivant :

$$\begin{cases} \dot{x}_1(t) &= -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) &= x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &= -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_{1\tau}(t)) \end{cases} \tag{2.11}$$

qui peut se mettre sous la forme plus compacte :

$$\dot{x}(t) = Ax(t) + F\left(x(t)\right) + H\left(x_\tau(t)\right) \tag{2.12}$$

avec

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \tag{2.13}$$

$$F(x(t)) = \begin{pmatrix} -\alpha\delta \tanh(x_1(t)) \\ 0 \\ 0 \end{pmatrix} \tag{2.14}$$

$$H(x_\tau(t)) = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin(\sigma x_1(t-\tau)) \end{pmatrix} \tag{2.15}$$

La partie linéaire reprend donc la structure du circuit de Chua sans dimension. La fonction tangente hyperbolique est choisie comme fonction non linéaire intervenant dans la dynamique de la première variable d'état x_1. Il s'agit bien d'une fonction impaire. Comme dans la référence [Wang 01], nous avons ajouté une nonlinéarité fonction de x_1, comportant un retard τ. Ce retour d'état avec retard assure un comportement chaotique au système (2.12).

Abréviation : Dans la suite de ce mémoire, le système chaotique (2.11), dont la partie non linéaire non retardée est choisie sous la forme d'une tangente hyperbolique, sera appelé *SCTH* (Système Chaotique à Tangente Hyperbolique).

Notons que les deux fonctions non linéaires F et H sont Lipschitziennes (voir la définition (1.24)), de constantes respectives :

$$k_F = |\alpha\delta| \tag{2.16}$$

$$k_H = |\varepsilon\sigma| \tag{2.17}$$

Du fait de la présence du retard, le *SCTH* est un système de dimension infinie : ainsi, les conditions initiales ne sont pas données par la valeur des trois états uniquement à l'origine, c'est-à-dire en un seul point, mais par la valeur des trois états sur tout l'intervalle $[-\tau, 0]$. Cet intervalle étant un ensemble non dénombrable, on peut considérer qu'il faut définir un nombre infini de condi-

tions initiales, d'où la dimension infinie caractérisant tout système à retard.
Pour établir le comportement chaotique de l'émetteur choisi, nous allons procéder comme suit. Les valeurs des paramètres sont les suivantes :

α	β	γ	δ	ε	σ	τ
9	14	5	-1	100	10^4	1

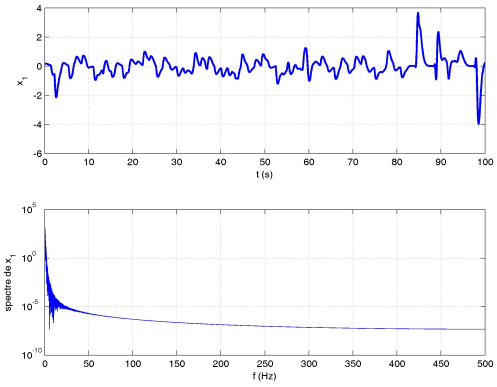
TAB. 2.2 - *Paramètres du système* (2.11)

1. Dans un premier temps, on trace les séries temporelles et spectrales des trois états du système (2.11), ce qui correspond à la figure 2.3, puis les trois fonctions d'autocorrélation correspondantes, à la figure 2.4. Pour chaque simulation, on choisit l'état initial $x_0 = (\ 0,1 \quad 0,1 \quad 0,1\ )$. Ces figures montre bien que les signaux chaotiques ressemblent à du bruit, mais sont assez éloignés d'un véritable bruit blanc. En particulier, la fonction d'autocorrélation d'un bruit blanc est un pic de Dirac, alors que sur la figure 2.4, on retrouve l'allure d'un pic de Dirac, mais on ne peut certainement pas conclure qu'un signal chaotique est un bruit blanc.
2. Dans un deuxième temps, la figure 2.5 indique que le système (2.11) est très sensible aux conditions initiales : les trajectoires des trois états sont très différentes alors que les conditions initiales diffèrent de $0,01\%$ (on a choisi $x_0 = (\ 1 \quad 1 \quad 1\ )$ et $x_0 = (\ 1 \quad 1 \quad 1,0001\ )$).
3. Enfin, nous allons étudier ce qui constitue un critère (admis en pratique par les spécialistes du chaos, voir les ouvrages de référence [Wiggins 90], [Alligood 96], [Dang-Vu 00]) de vérification du caractère chaotique du système (2.11), à savoir l'étude des bifurcations. Il s'agit d'une analyse du changement de comportement du système, tous les paramètres étant fixés (voir tableau 2.3), sauf un, appelé *paramètre de bifurcation*. Nous avons choisi

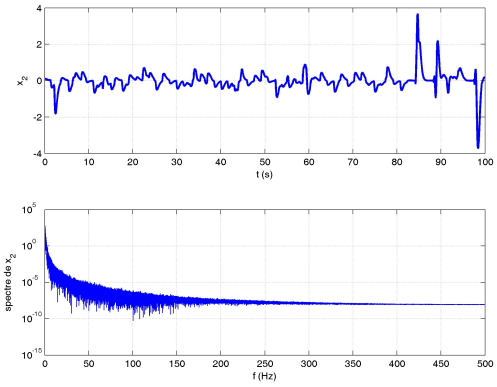
α	β	γ	δ	ε	τ
9	14	5	-1	10	1

TAB. 2.3 - *Paramètres fixés pour l'étude des bifurcations*

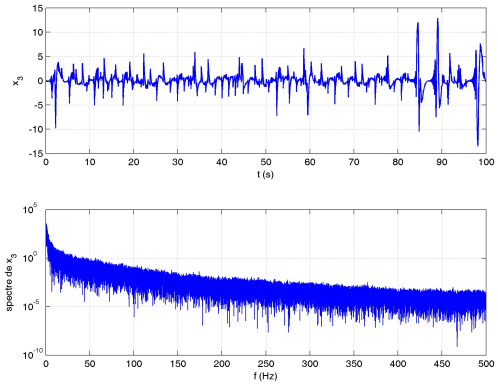
comme paramètre de bifurcation le paramètre σ. Nous allons montrer que pour certaines valeurs de σ, le système (2.11) n'est pas chaotique. Lorsqu'on fait varier σ, on observe ce que l'on appelle une *route vers le chaos*, caractéristique de tout système chaotique. Les figures 2.6 et 2.7 illustrent ce changement progressif de comportement : lorsque $\sigma = 0$, l'attracteur est un point d'équilibre. Puis, lorsque σ augmente, l'attracteur prend différentes formes : tout d'abord une boucle simple - aussi appelée cycle limite d'ordre un - pour $\sigma = 1,76$, puis une boucle double - ou cycle limite d'ordre deux - pour $\sigma = 1,77$, puis une boucle quadruple... pour arriver à un attracteur chaotique lorsque $\sigma = 2$.



(a) État x_1



(b) État x_2



(c) État x_3

FIG. 2.3 - *Trajectoires et spectres de puissance des trois états du* SCTH

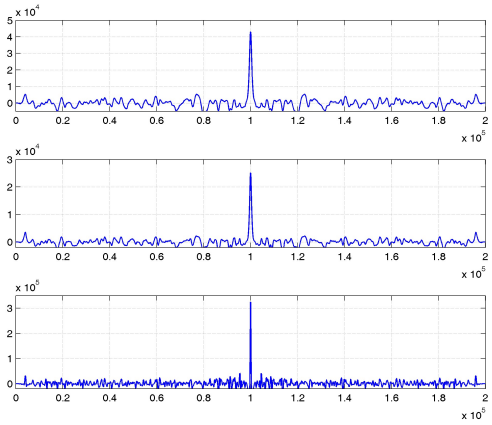


FIG. 2.4 - *Fonctions d'autocorrélation des trois états du* SCTH

Pour mieux visualiser la route vers le chaos, on construit un *diagramme de bifurcations*. Pour cela, on détermine un plan de coupe, identique pour tous les attracteurs, qui va

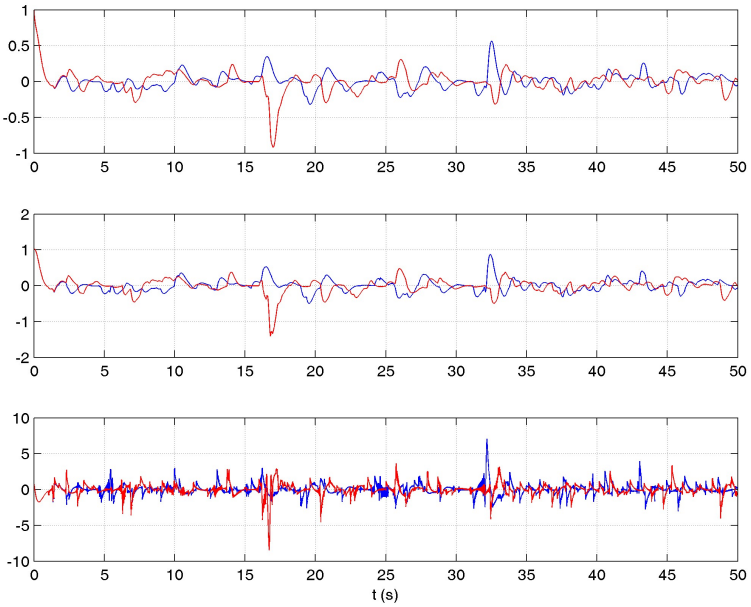
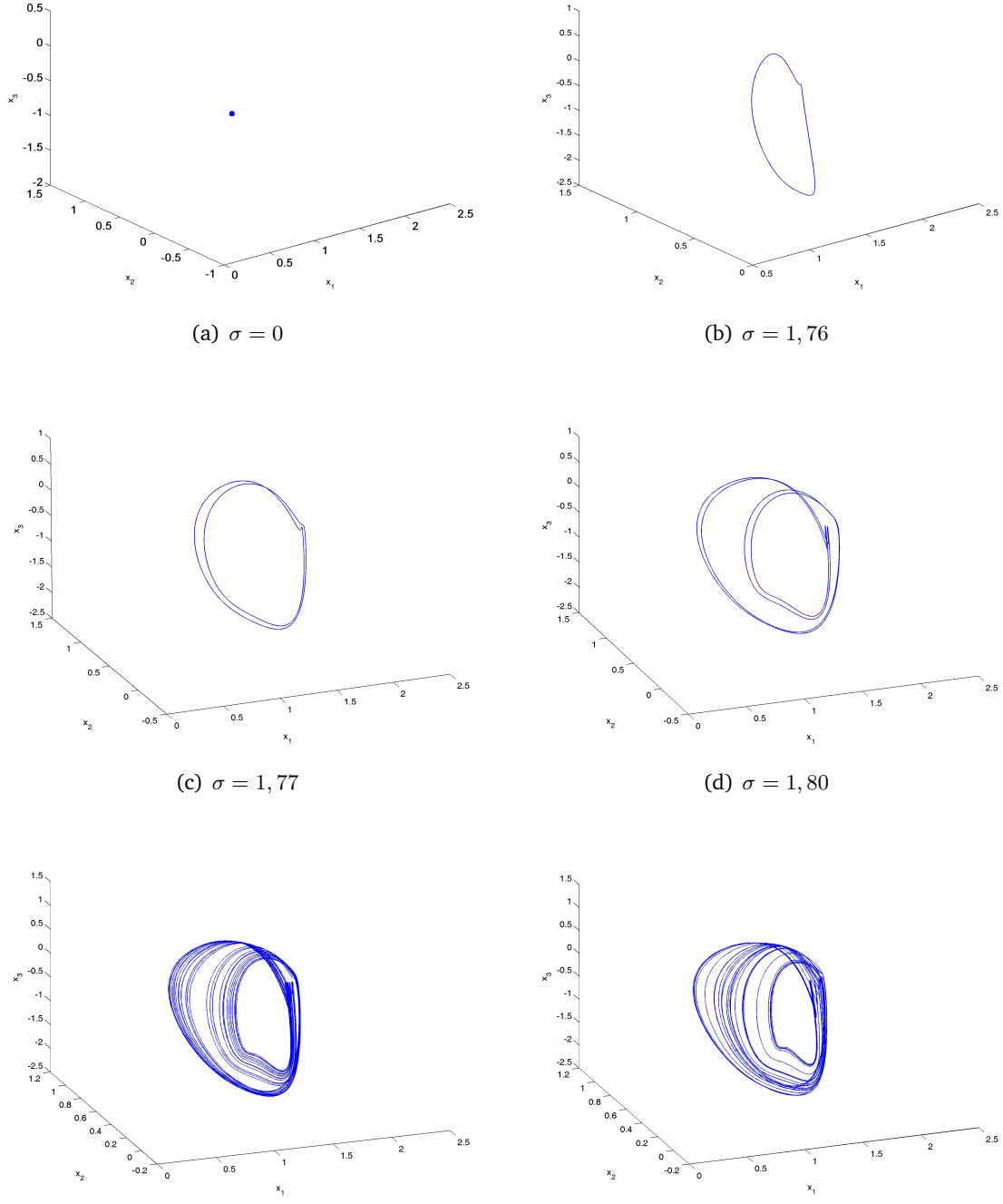


FIG. 2.5 - *Sensibilité aux conditions initiales du* SCTH

permettre de visualiser en dimension deux le changement qualitatif de comportement du système. Ici, on choisit le plan d'équation $x_3 = -1$. Lorsque l'attracteur est un cycle limite d'ordre un (*cf.* figure 2.6(b)), il reste deux points à l'intersection de ce plan et de l'attracteur. Lorsque l'attracteur est un cycle limite d'ordre deux (*cf.* figure 2.6(c)), il reste quatre points à l'intersection de ce plan et de l'attracteur... et ainsi de suite. Pour visualiser sur le même diagramme les points conservés en fonction de la valeur du paramètre de bifurcation, on garde uniquement leur composante selon l'axe x_1. On obtient alors le diagramme de bifurcations représenté à la figure 2.8.

Les simulations ont été faites avec une grande précision, et les 100000 premiers points ont été supprimés pour éviter les phénomènes transitoires. On observe une transition vers le chaos par doublement de période, ainsi que des fenêtres d'ordre : autour de la valeur $\sigma = 1,83$, le comportement redevient cyclique, et le zoom de la figure 2.9 montre le même motif de doublement de période.

La structure des systèmes émetteurs considérés étant maintenant définie, la suite de ce chapitre est consacrée à la conception du récepteur. Parmi les approches existantes présentées au paragraphe 1.3, et en lien avec le paragraphe 1.1, nous avons retenu l'approche à base d'observateurs non linéaires.
Tout au long de nos travaux de recherche, nous avons établi plusieurs schémas de synchronisation qui sont détaillés dans la partie suivante. Une distinction est faite selon le type d'observateur synthétisé : d'ordre plein, d'ordre réduit ou robuste.

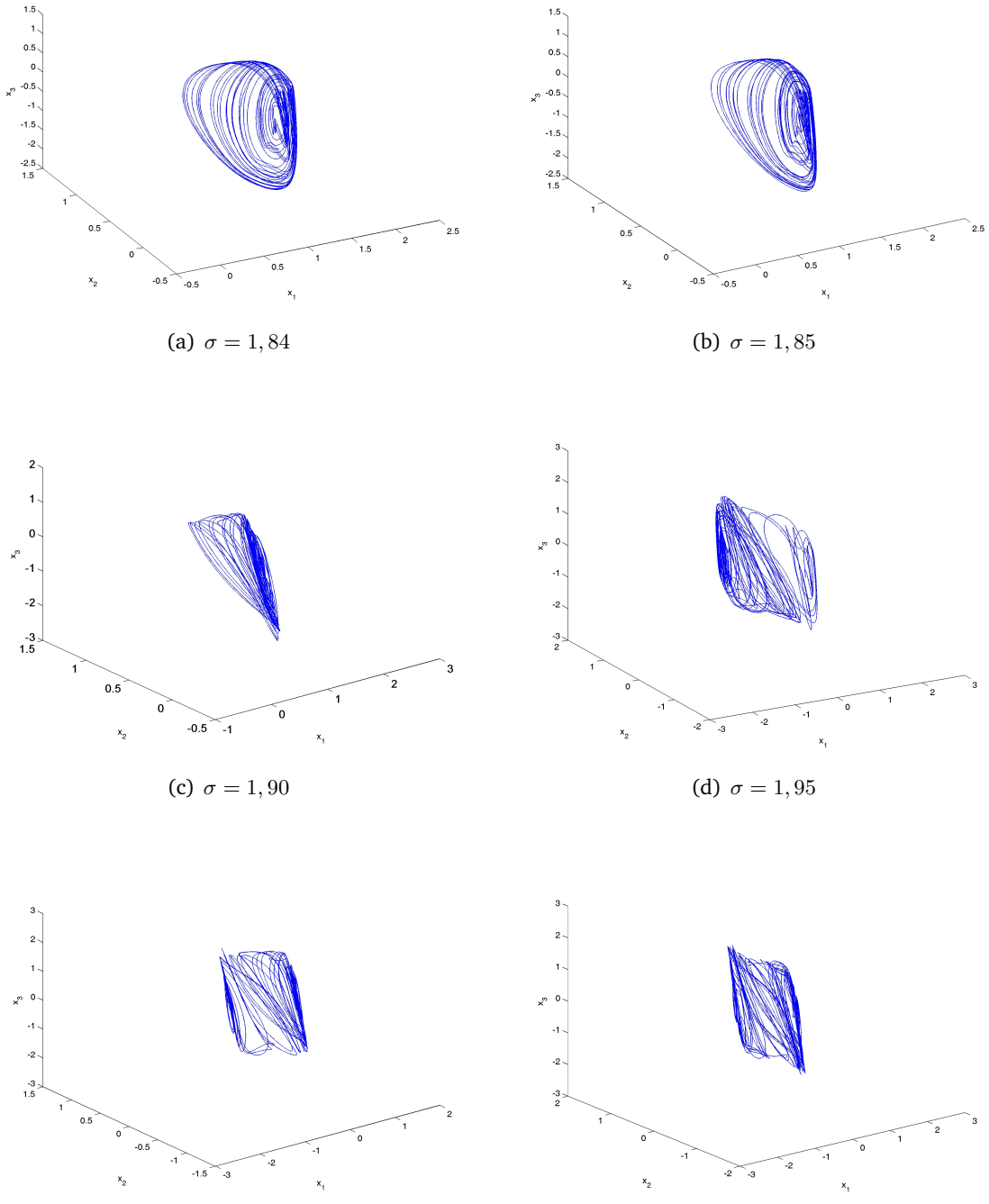


(a) $\sigma = 0$ (b) $\sigma = 1,76$

(c) $\sigma = 1,77$ (d) $\sigma = 1,80$

(e) $\sigma = 1,81$ (f) $\sigma = 1,82$

FIG. 2.6 - *Route vers le chaos*



(a) $\sigma = 1,84$ (b) $\sigma = 1,85$

(c) $\sigma = 1,90$ (d) $\sigma = 1,95$

(e) $\sigma = 1,96$ (f) $\sigma = 2$

FIG. 2.7 - *Suite de la route vers le chaos*

2.3 Observateurs d'ordre plein

2.3.1 Synthèse d'un observateur non linéaire : approche analytique

Dans cette section, on détaille la construction d'un observateur pour une classe de systèmes non linéaires dont la structure est celle du circuit de Chua modifié (2.1). Nous proposons une résolu-

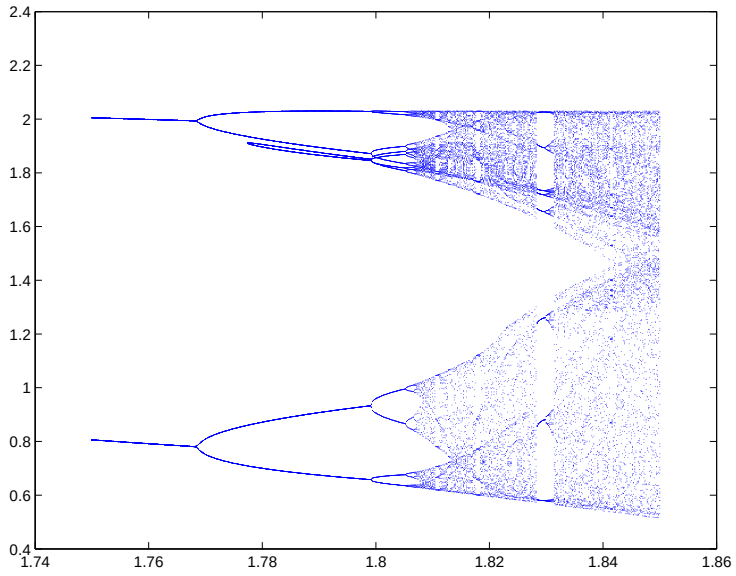


FIG. 2.8 - *Diagramme de bifurcations*

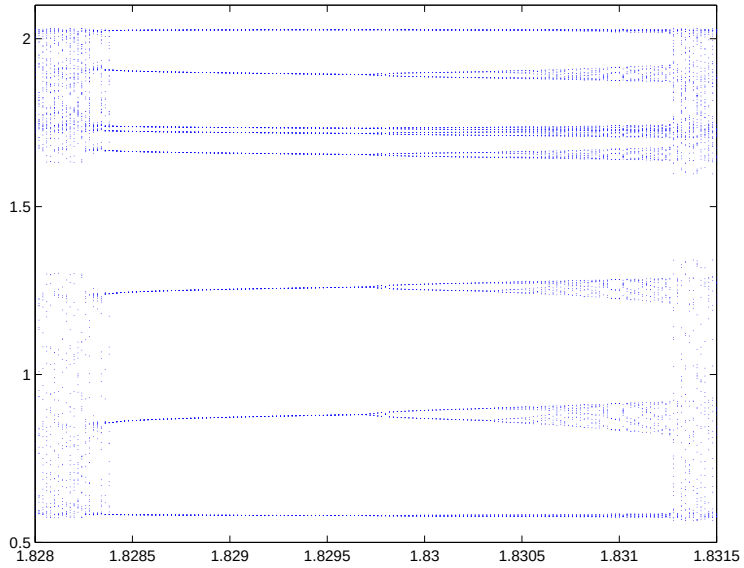


FIG. 2.9 - *Zoom autour de la valeur* $\sigma = 1,83$

tion analytique de l'équation de Riccati associée à l'analyse de la convergence de cet observateur, spécifiquement adapté à la structure de systèmes décrits ci-dessous.

On reprend le système décrit par les équations (2.4) à (2.8), et on simplifie l'expression du modèle, de la même façon que pour le circuit de Chua standard (voir le paragraphe B.2.3 en annexe). On aboutit alors à un circuit de Chua modifié sans dimension :

$$\begin{cases} \dot{x}(t) &= Ax(t) + F(x(t)) + H(x_\tau(t)) \\ y(t) &= Cx(t) \end{cases} \tag{2.18}$$

avec

$$A = \begin{pmatrix} -\alpha & \alpha & 0 \\ 1 & -1 & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \tag{2.19}$$

$$F(x(t)) = \begin{pmatrix} -\alpha f(x_1(t)) \\ 0 \\ 0 \end{pmatrix} \tag{2.20}$$

$$f(x_1(t)) = bx_1(t) + \frac{1}{2}(a-b)(|x_1(t)+1| - |x_1(t)-1|) \tag{2.21}$$

$$H(x_\tau(t)) = \begin{pmatrix} 0 \\ 0 \\ -h(x_{1\tau}(t)) \end{pmatrix} \tag{2.22}$$

$$h(x_{1\tau}(t)) = \varepsilon \sin(\sigma x_{1\tau}(t)) \tag{2.23}$$

2.3.1.1 Synthèse de l'observateur

On choisit la forme standard d'un observateur non linéaire du système (2.18) :

$$\dot{\hat{x}}(t) = A\hat{x}(t) + F(\hat{x}(t)) + H(\hat{x}_\tau(t))) + L(y(t) - C\hat{x}(t)) \tag{2.24}$$

On définit alors le vecteur d'erreur d'estimation $e(t) = x(t) - \hat{x}(t)$. D'après (2.18) et (2.24), la dynamique de l'erreur est donnée par :

$$\dot{e}(t) = (A - LC)e(t) + F(x(t)) - F(\hat{x}(t)) + H(x_\tau(t)) - H(\hat{x}_\tau(t)) \tag{2.25}$$

Notations : pour alléger les formules, on notera, uniquement dans le paragraphe 2.3.1

$$\begin{aligned} F &= F(x(t)) \\ \hat{F} &= F(\hat{x}(t)) \\ \tilde{F} &= F(x(t) - \hat{x}(t)) \end{aligned} \tag{2.26}$$

$$\begin{aligned} H &= H(x_\tau(t)) \\ \hat{H} &= H(\hat{x}_\tau(t)) \\ \tilde{H} &= H(x_\tau(t)) - H(\hat{x}_\tau(t)) \end{aligned} \tag{2.27}$$

Le théorème suivant présente des conditions suffisantes de synchronisation du système (2.24) avec l'émetteur (2.18).

Théorème 2.3.1 ([Cherrier 04a])**.** *S'il existe deux matrices symétriques, définies positives P et Q telles que*

$$(A - LC)^T P + P(A - LC) + \gamma_F P^2 + \gamma_H I_3 = -Q \tag{2.28}$$

où

$$\gamma_F = 1 + k_F^2 \tag{2.29a}$$

$$\gamma_H = 1 + k_H^2 \tag{2.29b}$$

alors le système (2.24) *est un observateur asymptotique du système* (2.18). ■

Démonstration : s'agissant d'un système à retard, il est classique [Kharitonov 99], [Richard 03] de définir une fonctionnelle de Lyapunov-Krasovskii :

$$V(e, e_\tau) = e^T P e + \xi \int_{-\tau}^{0} e(t+\theta)^T e(t+\theta) d\theta \tag{2.30}$$

où P est une matrice symétrique définie positive et $\xi > 0$.
L'erreur de synchronisation e converge vers 0 si [Gu 03] :

$$V(e, e_\tau) > 0 \tag{2.31a}$$

$$\dot{V}(e, e_\tau) < 0 \tag{2.31b}$$

pour $e \neq 0$.
La première condition est facilement vérifiée puisque $P > 0$ et $\xi > 0$.
La dérivée de V le long des trajectoires de (2.25) a pour expression :

$$\dot{V}(e, e_\tau) = e^T \left((A - LC)^T P + P(A - LC) + \xi I_3 \right) e + 2e^T P(F - \hat{F}) + 2e^T P(H - \hat{H}) - \xi e_\tau^T e_\tau \tag{2.32}$$

Si on applique l'inégalité de Cauchy-Schwarz à la fonction F (de constante de Lipschitz k_F), on

obtient :

$$2e^T P(F - \hat{F}) \leqslant 2\|e^T P\|\|F - \hat{F}\| \leqslant 2k_F\|e^T P\|\|e\| \tag{2.33}$$

L'inégalité de Young donne alors :

$$2k_F\|e^T P\|\|e\| \leqslant k_F^2 e^T PPe + \|e\|^2 \tag{2.34}$$

En procédant de manière analogue avec la fonction H, on arrive à :

$$2e^T P(H - \hat{H}) \leqslant e^T PPe + k_H^2\|e_\tau\|^2 \tag{2.35}$$

En remplaçant (2.33), (2.34) et (2.35) dans (2.32), on obtient :

$$\begin{aligned} \dot{V}(e, e_\tau) \leqslant \quad & e^T \left((A - LC)^T P + P(A - LC) + \xi I_3\right) e + k_F^2 e^T PPe + \|e\|^2 \\ & + e^T PPe + k_H^2\|e_\tau\|^2 - \xi\|e_\tau\|^2 \end{aligned} \tag{2.36}$$

puis en regroupant :

$$\dot{V}(e, e_\tau) \leqslant e^T \left((A - LC)^T P + P(A - LC) + (\xi + 1)I_3 + (1 + k_F^2)P^2\right) e + (k_H^2 - \xi)\|e_\tau\|^2 \tag{2.37}$$

Pour satisfaire la condition (2.31), il faut que $k_H^2 - \xi \leqslant 0$. On choisit alors $\xi = k_H^2$. L'expression (2.37) devient donc :

$$\dot{V}(e, e_\tau) \leqslant e^T \left((A - LC)^T + P(A - LC) + (1 + k_F^2)P^2 + (1 + k_H^2)I_3\right) e \tag{2.38}$$

Si on remplace (2.28) et (2.29) dans l'expression précédente, on obtient finalement :

$$\dot{V}(e, e_\tau) \leqslant -e^T Qe \tag{2.39}$$

Donc la condition (2.31) est vérifiée, et $\hat{x}$ converge vers l'état réel x. □

2.3.1.2 Résolution analytique

En exploitant la symétrie de la matrice d'état A (2.19) (par rapport aux états x_1 et x_3), nous proposons une résolution analytique de l'équation de type Riccati (2.28), en choisissant :

$$C = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix} \tag{2.40}$$

On note

$$L = \begin{pmatrix} l_1 \\ l_2 \\ l_3 \end{pmatrix} \tag{2.41}$$

Pour simplifier les calculs, on fait l'hypothèse que la matrice P est diagonale :

$$P = \begin{pmatrix} p_1 & 0 & 0 \\ 0 & p_2 & 0 \\ 0 & 0 & p_3 \end{pmatrix} \tag{2.42}$$

avec p_1, p_2, p_3 strictement positifs.
La matrice Q est alors nécessairement de la forme :

$$\begin{pmatrix} q_1 & q_4 & 0 \\ q_4 & q_2 & q_5 \\ 0 & q_5 & q_3 \end{pmatrix} \tag{2.43}$$

En utilisant les notations précédentes, l'équation de type Riccati (2.28) se met sous la forme :

$$\begin{pmatrix} \gamma_F p_1^2 - 2\alpha p_1 + \gamma_H & (\alpha - l_1)p_1 + p_2 & 0 \\ (\star) & -2p_2(1+l_2) + \gamma_F p_2^2 + \gamma_H & p_2 - (\beta + l_3)p_3 \\ (\star) & (\star) & -2\gamma p_3 + \gamma_F p_3^2 + \gamma_H \end{pmatrix} = -Q \tag{2.44}$$

Cette relation matricielle est équivalente au système d'équations suivant :

$$\gamma_F p_1^2 - 2\alpha p_1 + \gamma_H + q_1 = 0 \tag{2.45a}$$
$$\gamma_F p_2^2 - 2(1+l_2)p_2 + \gamma_H + q_2 = 0 \tag{2.45b}$$
$$\gamma_F p_3^2 - 2\gamma p_3 + \gamma_H + q_3 = 0 \tag{2.45c}$$
$$(\alpha - l_1)p_1 + p_2 + q_4 = 0 \tag{2.45d}$$
$$p_2 - (\beta + l_3)p_3 + q_5 = 0 \tag{2.45e}$$

Les inconnues de ce système d'équations sont les coefficients l_1, l_2, l_3 du gain L, ainsi que les coefficients des matrices P et Q, *i.e.* p_i et q_j, $i = 1, 3$, $j = 1, 5$.
La première équation (2.45a) est une équation du second degré en p_1, dont le discriminant est donné par :

$$\Delta_1 = 4\alpha^2 - 4\gamma_F(q_1 + \gamma_H) \tag{2.46}$$

Il est positif (et dans ce cas seulement il existe une solution p_1) si et seulement si :

$$q_1 \leqslant \frac{\alpha^2}{\gamma_F} - \gamma_H \tag{2.47}$$

Dans ce cas, si le coefficient α est positif, la racine positive de (2.45a) est :

$$p_1 = \frac{\alpha + \sqrt{\Delta_1}}{\gamma_F} \tag{2.48}$$

De même, la deuxième équation (2.45b) est du second degré en p_2, et son discriminant a pour expression :

$$\Delta_2 = 4(1 + l_2)^2 - 4\gamma_F(q_2 + \gamma_H) \tag{2.49}$$

Δ_2 est positif *ssi* :

$$q_2 \leqslant \frac{(1 + l_2)^2}{\gamma_F} - \gamma_H \tag{2.50}$$

avec l_2 choisi arbitrairement. On a alors :

$$p_2 = \frac{1 + l_2 + \sqrt{\Delta_2}}{\gamma_F} \tag{2.51}$$

De façon analogue, le discriminant de la troisième équation (2.45b) en p_3 est :

$$\Delta_3 = 4\gamma^2 - 4\gamma_F(q_3 + \gamma_H) \tag{2.52}$$

Δ_3 est positif *ssi* :

$$q_3 \leqslant \frac{\gamma^2}{\gamma_F} - \gamma_H \tag{2.53}$$

et on a alors :

$$p_3 = \frac{\gamma + \sqrt{\Delta_3}}{\gamma_F} \tag{2.54}$$

Les deux dernières équations permettent de trouver les autres coefficients du gain L :

$$l_1 = \alpha + \frac{p_2 + q_4}{p_1} \tag{2.55}$$

$$l_3 = -\beta + \frac{p_2 + q_5}{p_3} \tag{2.56}$$

La procédure pour construire P, Q et le gain L peut être résumée comme suit (il subsiste un certain degré de liberté dans le choix de certains paramètres, car il s'agit d'un système non linéaire de cinq équations à onze inconnues).

(i) On choisit les coefficients q_i, $i = 1, 5$ et le coefficient l_2 satisfaisant les conditions (2.47), (2.50), (2.53) et garantissant $Q > 0$;

(ii) les coefficients de la matrice P sont donnés respectivement par (2.48), (2.51) et (2.54) ;

(iii) les deux autres coefficients du gain, l_1 et l_3, sont donnés respectivement par (2.55) et (2.56).

2.3.1.3 Simulations

Les valeurs suivantes sont fixées pour le système (2.18)-(2.23) :

$$\begin{array}{l} \alpha = 10 \quad \beta = 5 \quad \gamma = 10 \\ a = -0,3 \quad b = -0,2 \\ \tau = 1 \quad \varepsilon = 0,1 \quad \sigma = 10 \end{array} \tag{2.57}$$

En appliquant la méthode précédente, on obtient le gain suivant :

$$L = \begin{pmatrix} 19,43 \\ 20 \\ 4,43 \end{pmatrix} \tag{2.58}$$

Les matrices P et Q sont données par :

$$P = \begin{pmatrix} 1,32 & 0 & 0 \\ 0 & 2,42 & 0 \\ 0 & 0 & 1,32 \end{pmatrix} \tag{2.59}$$

et

$$Q = \begin{pmatrix} 7 & 10 & 0 \\ 10 & 41,1 & 10 \\ 0 & 10 & 7 \end{pmatrix} \tag{2.60}$$

La figure 2.10 montre les trois composantes du vecteur d'erreur d'estimation d'état.

Remarque 2.3.1. Cette synthèse d'observateur, exploitant la structure particulière du système (2.18) (et notamment une certaine symétrie de la matrice A définie en (2.19)), prouve que l'on peut trouver une expression analytique du gain L, et ainsi éviter un certain conservatisme indissociable des techniques classiques de résolution des équations de type Riccati. Cependant, les calculs développés dans ce paragraphe ne se révèlent pas adaptés pour les systèmes chaotiques : en effet, il semble y avoir une incompatibilité numérique entre les conditions (2.45) et un comportement chaotique du système (2.18). Les hypothèses nécessaires sur les variables de l'équation (2.44) ne peuvent pas être vérifiées (d'après nos multiples essais infructueux), dès lors que le système (2.18) exhibe un comportement chaotique. En revanche, dans nos simulations, les conditions (2.45) sont bien vérifiées, mais en contrepartie le système initial n'a pas un comportement chaotique.
Les sections suivantes présentent des résolutions plus classiques d'équations de type Riccati, en exploitant les résultats de la théorie des LMI et des BMI. Lors de l'utilisation de schémas de synchronisation au cœur d'un système de communications, nous ne retiendrons pas la méthode qui vient d'être présentée. Cette approche pourra être envisagée par la suite dans un autre contexte d'estimation d'état non linéaire. ♦

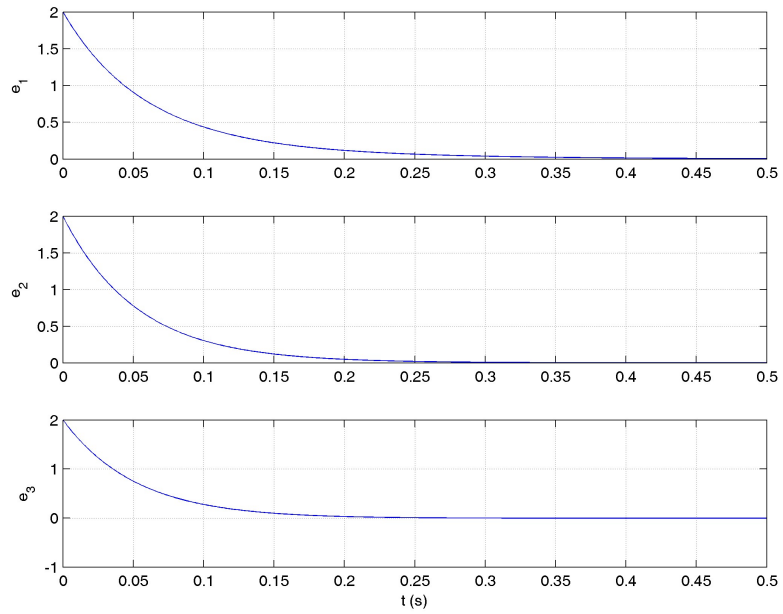


FIG. 2.10 - *Composantes du vecteur d'erreur d'estimation de l'état* $e(t)$

2.3.2 Convergence asymptotique et exponentielle : utilisation de techniques LMI

Nous détaillons dans ce paragraphe un schéma de synchronisation utilisant un observateur d'ordre plein, dont l'émetteur est le *SCTH* (2.11) décrit au paragraphe 2.2.2 :

$$\left\{\begin{array}{lcl} \dot{x}_1(t) &=& -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta \tanh(x_1(t)) \\ \dot{x}_2(t) &=& x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &=& -\beta x_2(t) - \gamma x_3(t) + \varepsilon \sin(\sigma x_{1\tau}(t)) \end{array}\right. \tag{2.61}$$

Les valeurs des paramètres données dans le tableau 2.2 (page 47) montrent que les constantes de Lipschitz k_F (2.16) et surtout k_G (2.17) peuvent être très grandes (k_G peut ainsi atteindre 10^8). Pour pouvoir facilement prendre en compte de telles constantes de Lipschitz, nous proposons de choisir

$$C = \left(\begin{array}{ccc} 1 & \zeta & 0 \end{array} \right) \tag{2.62}$$

où ζ est un paramètre choisi arbitrairement.
On déduit alors de (2.62) :

$$y(t) = x_1(t) + \zeta x_2(t) \tag{2.63}$$

2.3.2.1 Transformation du système

En remplaçant x_1 par son expression en fonction de y et x_2 tirée de (2.63), le modèle dynamique de l'émetteur (2.61) se met sous la forme équivalente :

$$\begin{cases} \dot{x}(t) = \tilde{A}x(t) + \tilde{B}y(t) + \tilde{F}(x(t), y(t)) + \tilde{H}(x_\tau(t), y_\tau(t)) \\ y(t) = Cx(t) \end{cases} \tag{2.64}$$

avec

$$\tilde{A} = \begin{pmatrix} 0 & \alpha(1+\zeta) & 0 \\ 0 & -(1+\zeta) & 1 \\ 0 & -\beta & -\gamma \end{pmatrix} \tag{2.65}$$

$$\tilde{B} = \begin{pmatrix} -\alpha \\ 1 \\ 0 \end{pmatrix} \tag{2.66}$$

$$\tilde{F}(x(t), y(t)) = \tilde{F} = \begin{pmatrix} \alpha\delta \tanh(y(t) - \zeta x_2(t)) \\ 0 \\ 0 \end{pmatrix} \tag{2.67}$$

$$\tilde{H}(x_\tau(t), y_\tau(t)) = \tilde{H} = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin\left(\sigma(y(t-\tau) - \zeta x_2(t-\tau))\right) \end{pmatrix} \tag{2.68}$$

On constate alors que la constante de Lipschitz de $\tilde{F}$ est majorée en fonction de ζ, en utilisant (2.67) et les notations (2.26) :

$$\tilde{F} - \hat{\tilde{F}} = \begin{pmatrix} \alpha\delta \tanh(y(t) - \zeta x_2(t)) - \alpha\delta \tanh(y(t) - \zeta \hat{x}_2(t)) \\ 0 \\ 0 \end{pmatrix} \tag{2.69}$$

D'où

$$\begin{aligned} \|\tilde{F} - \hat{\tilde{F}}\| &\leqslant \alpha\delta\zeta \|x_2(t) - \hat{x}_2(t)\| \\ &\leqslant k_F \zeta \|e(t)\| \end{aligned} \tag{2.70}$$

De même, avec (2.68), (2.27), la constante de Lipschitz de $\tilde{H}$ est majorée en fonction de ζ :

$$\tilde{H} - \hat{\tilde{H}} = \begin{pmatrix} 0 \\ 0 \\ \varepsilon \sin\left(\sigma(y(t-\tau) - \zeta x_2(t-\tau))\right) - \varepsilon \sin\left(\sigma(y(t-\tau) - \zeta \hat{x}_2(t-\tau))\right) \end{pmatrix} \tag{2.71}$$

D'où

$$\begin{aligned} \|\tilde{H} - \hat{\tilde{H}}\| &\leqslant \varepsilon\sigma\zeta \|x_2(t-\tau) - \hat{x}_2(t-\tau)\| \\ &\leqslant k_H \zeta \|e(t-\tau)\| \end{aligned} \tag{2.72}$$

Puisque le paramètre ζ est arbitraire, en particulier il peut être choisi aussi petit que l'on veut, donc la transformation présentée permet effectivement de maîtriser les constantes de Lipschitz des nonlinéarités du système émetteur.

Remarque 2.3.2. Ce choix de C sera justifié dans le chapitre suivant. On peut d'ores et déjà indiquer que le signal $x_3(t)$, plus complexe que les trajectoires des deux autres états (se reporter à la figure 2.3 pour une comparaison) est réservé pour l'étape de cryptage du système de communications que nous proposons au chapitre 3. Il est donc nécessaire de ne pas transmettre d'information sur $x_3(t)$ dans le signal utilisé pour synchroniser le récepteur. Cela élimine la possibilité de prendre $C = \begin{pmatrix} 1 & \zeta & \phi \end{pmatrix}$ avec $|\phi| \ll 1$ différent de zéro. Cette forme de matrice C est en effet la seule qui permette d'aboutir, de façon analogue au raisonnement précédent, aux mêmes transformations des constantes de Lipschitz (2.70) et (2.72). On en conclut que nécessairement $\phi = 0$. ♦

2.3.2.2 Synthèse de l'observateur

Dans la suite, on omet la variable temporelle t pour alléger l'écriture, lorsque cela ne nuit pas à la compréhension des calculs.
Le modèle dynamique du récepteur est choisi de la forme suivante :

$$\dot{\hat{x}} = \tilde{A}\hat{x} + \tilde{B}y + \tilde{F}(\hat{x}, y) + \tilde{H}(\hat{x}_\tau, y_\tau) + K(y - C\hat{x}) \tag{2.73}$$

soit, sous la forme plus compacte :

$$\dot{\hat{x}} = \tilde{A}\hat{x} + \tilde{B}y + \hat{\tilde{F}} + \hat{\tilde{H}} + K(y - C\hat{x}) \tag{2.74}$$

On définit le vecteur d'erreur de synchronisation : $e = x - \hat{x}$. En utilisant (2.64) et (2.74), la dynamique de l'erreur a pour expression :

$$\dot{e} = A_K e + \tilde{F} - \hat{\tilde{F}} + \tilde{H} - \hat{\tilde{H}} \tag{2.75}$$

avec

$$A_K = \tilde{A} - KC \tag{2.76}$$

Le théorème suivant énonce une condition suffisante de synchronisation du récepteur (2.73) avec l'émetteur (2.64).

Théorème 2.3.2 (Convergence asymptotique [Cherrier 05b])**.** *Si les conditions suivantes sont vérifiées :*
(i) la paire $(\tilde{A}, C)$ est détectable ;
(ii) il existe deux matrices P et Q respectivement symétrique définie positive et définie positive

solutions des BMI suivantes :

$$\begin{pmatrix} A_K^T P + P A_K + Q + \mu I_3 & P \\ P & -\frac{1}{\lambda} I_3 \end{pmatrix} < 0 \tag{2.77}$$

$$Q \geqslant \rho I_3 \tag{2.78}$$

avec $\lambda = \zeta k_F + \zeta k_H$, $\mu = \zeta k_F$ *et* $\rho = \zeta k_H$

alors (2.73) *est un observateur asymptotique de* (2.64). ■

Démonstration : on définit une fonctionnelle de Lyapunov-Krasovskii :

$$V(e, e_\tau) = e^T P e + \int_{-\tau}^{0} e(t+\theta)^T Q e(t+\theta) d\theta \tag{2.79}$$

où P et Q sont deux matrices respectivement symétrique définie positive et définie positive.
L'erreur de synchronisation e converge vers 0 si [Gu 03] :

$$V(e, e_\tau) \geqslant 0 \tag{2.80a}$$
$$\dot{V}(e, e_\tau) \leqslant 0 \tag{2.80b}$$

La première condition est facilement vérifiée puisque P et Q sont définies positives.
La dérivée de V le long des trajectoires de (2.75) a pour expression :

$$\dot{V} = \dot{e}^T P e + e^T P \dot{e} + e^T Q e - e_\tau^T Q e_\tau \tag{2.81}$$

soit, en remplaçant $\dot{e}$ par son expression (2.75) :

$$\dot{V} = e^T \left(A_K^T P + P A_K + Q \right) e + 2 e^T P (\tilde{F} - \hat{\tilde{F}}) + 2 e^T P (\tilde{H} - \hat{\tilde{H}}) - e_\tau^T Q e_\tau \tag{2.82}$$

Si on applique les inégalités de Cauchy-Schwarz et de Young successivement, on obtient ensuite en utilisant (2.70) et (2.72) :

$$\begin{aligned} 2 e^T P (\tilde{F} - \hat{\tilde{F}}) &\leqslant 2 \| e^T P \| \| \tilde{F} - \hat{\tilde{F}} \| \\ &\leqslant 2 \zeta k_F \| e^T P \| \| e \| \\ &\leqslant \zeta k_F e^T P P e + \zeta k_F e^T e \end{aligned} \tag{2.83}$$

et

$$\begin{aligned} 2 e^T P (\tilde{H} - \hat{\tilde{H}}) &\leqslant 2 \| e^T P \| \| \tilde{H} - \hat{\tilde{H}} \| \\ &\leqslant 2 \zeta k_H \| e^T P \| \| e_\tau \| \\ &\leqslant \zeta k_H e^T P P e + \zeta k_H e_\tau^T e_\tau \end{aligned} \tag{2.84}$$

Les majorations (2.83) et (2.84) donnent une majoration de $\dot{V}$ déduite de (2.82) :

$$\dot{V} \leqslant e^T \left(A_K^T P + P A_K + Q + \lambda P^2 + \mu I_3\right) e + e_\tau^T \left(\rho I_3 - Q\right) e_\tau \tag{2.85}$$

avec $\lambda = \zeta k_F + \zeta k_H$, $\mu = \zeta k_F$ et $\rho = \zeta k_H$.
D'après la condition (2.78), et en notant $W = -(A_K^T P + P A_K + Q + \lambda P^2 + \mu I_3)$, on obtient :

$$\dot{V} \leqslant -e^T W e \tag{2.86}$$

La condition (2.80b) est vérifiée si (2.78) l'est et que $W < 0$. Cela implique en particulier que la paire $(\tilde{A}, C)$ est détectable.
En appliquant le complément de Schur, l'inégalité $W < 0$ se met sous la forme :

$$\begin{pmatrix} A_K^T P + P A_K + Q + \mu I_3 & P \\ P & -\frac{1}{\lambda} I_3 \end{pmatrix} < 0, \quad \lambda = 1 + \zeta k_F, \quad \mu = \zeta k_F \tag{2.87}$$

ce qui démontre la condition (2.77) et ainsi le vecteur d'erreur de synchronisation $e(t)$ tend bien vers zéro. □

Remarque 2.3.3. La BMI (2.87) peut être résolue numériquement. Il faut tout d'abord linéariser le bloc en haut à gauche sous la forme (on rappelle que $A_K = \tilde{A} - KC$) :

$$A_K^T P + P A_K + Q + \mu I_3 = \tilde{A}^T P + P\tilde{A} - C^T L^T - LC + Q + \mu I_3 \tag{2.88}$$

en posant $L = PK$ (P est inversible). On obtient donc la LMI équivalente :

$$\begin{pmatrix} \tilde{A}^T P + P\tilde{A} - C^T L^T - LC + Q + \mu I_3 & P \\ P & -\frac{1}{\lambda} I_3 \end{pmatrix} < 0 \tag{2.89}$$

qui est bien linéaire en P et L. Lorsqu'on a trouvé des valeurs satisfaisantes de P et L, il suffit d'écrire $K = P^{-1}L$ pour obtenir le gain de l'observateur (2.73).

En fait, on peut démontrer un résultat plus fort que le théorème 2.3.2, à savoir que l'observateur (2.73) converge de façon exponentielle vers l'état du système (2.64). Ce résultat fait l'objet du corollaire suivant.

Corollaire 2.3.3 (Convergence exponentielle)**.** *S'il existe un gain K et deux matrices P, Q respectivement symétrique, définie positive et définie positive, et un réel strictement positif η tels que*

$$\begin{pmatrix} (A-KC)^T P + P(A-KC) + \mu I_3 + Q + 2\eta P & 0 & P \\ 0 & -e^{-2\eta\tau} Q + \rho I & 0 \\ P & 0 & -\frac{1}{\lambda} I_3 \end{pmatrix} \leqslant 0 \tag{2.90}$$

avec $\lambda = \zeta k_F + \zeta k_H$, $\mu = \zeta k_F$, $\rho = \zeta k_H$, alors l'erreur de synchronisation converge exponentiellement vers zéro, selon la formule :

$$\|e(t)\| \leqslant \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\| \tag{2.91}$$

avec $\alpha_1 = \lambda_M(P) + \tau \lambda_M(Q)$ et $\alpha_2 = \lambda_m(P)$.

Démonstration : on reprend l'expression (2.75) de la dynamique de l'erreur et on définit une nouvelle fonctionnelle de Lyapunov-Krasovskii, comme proposé dans [Mondie 05] :

$$V'(e, e_\tau) = e^T P e + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta \tag{2.92}$$

où P et Q sont deux matrices respectivement symétrique, définie positive et définie positive, et $\eta > 0$.
La norme du vecteur d'erreur de synchronisation $e(t)$ converge exponentiellement vers 0 s'il existe $\phi > 0$ tel que :

$$V'(e, e_\tau) \geqslant 0 \tag{2.93a}$$

$$\dot{V}'(e, e_\tau) \leqslant e^{-\phi t} \max_{\theta \in [-\tau, 0]} V'(e(0), e(\theta)) \tag{2.93b}$$

Comme les matrices P et Q sont définies positives, la première condition (2.93a) est vérifiée grâce à :

$$\lambda_m(P) \|e(t)\|^2 \leqslant V'(e, e_\tau) \leqslant (\lambda_M(P) + \tau \lambda_M(Q)) \max_{\theta \in [-\tau, 0]} \|e(\theta)\|^2 \tag{2.94}$$

Si on dérive l'expression (2.92) de la fonctionnelle de Lyapunov-Krasovskii, on obtient :

$$\dot{V}' = \dot{e}^T P e + e^T P \dot{e} + e^T Q e - e^{-2\eta\tau} e_\tau^T Q e_\tau - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta \tag{2.95}$$

Or, d'après (2.75), il vient :

$$\dot{e}^T P e + e^T P \dot{e} = e^T \left(A_K^T P + P A_K \right) e + 2 e^T P (\tilde{F} - \hat{\tilde{F}}) + 2 e^T P (\tilde{H} - \hat{\tilde{H}}) \tag{2.96}$$

donc, en utilisant (2.83) et (2.84), on obtient la majoration suivante :

$$\dot{e}^T P e + e^T P \dot{e} \leqslant e^T \left(A_K^T P + P A_K \right) e + \zeta k_F e^T P P e + \zeta k_F e^T e + \zeta k_H e^T P P e + \zeta k_H e_\tau^T e_\tau \tag{2.97}$$

puis celle de $\dot{V}'$:

$$\dot{V}' \leqslant \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T \mathcal{M} \begin{pmatrix} e \\ e_\tau \end{pmatrix} - 2\eta \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta \tag{2.98}$$

avec

$$\mathcal{M} = \begin{pmatrix} A_K^T P + P A_K + \lambda P^2 + \mu I + Q & 0 \\ 0 & -e^{-2\eta\tau} Q + \rho I \end{pmatrix} \tag{2.99}$$

et $\lambda = \zeta k_F + \zeta k_H$, $\mu = k_F$, $\rho = \zeta k_H$.
Par ailleurs, on peut mettre l'expression (2.92) sous la forme :

$$V' = \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T \mathcal{N} \begin{pmatrix} e \\ e_\tau \end{pmatrix} + \int_{-\tau}^{0} e^T(t+\theta) e^{2\eta\theta} Q e(t+\theta) d\theta \tag{2.100}$$

avec

$$\mathcal{N} = \begin{pmatrix} P & 0 \\ 0 & 0 \end{pmatrix} \tag{2.101}$$

En utilisant (2.98) et (2.100), on obtient :

$$\dot{V}' + 2\eta V' \leqslant \begin{pmatrix} e \\ e_\tau \end{pmatrix}^T (\mathcal{M} + 2\eta\mathcal{N}) \begin{pmatrix} e \\ e_\tau \end{pmatrix} \tag{2.102}$$

Or

$$\mathcal{M} + 2\eta\mathcal{N} = \begin{pmatrix} A_K^T P + P A_K + \lambda P^2 + \mu I + Q + 2\eta P & 0 \\ 0 & -e^{-2\eta\tau} Q + \rho I \end{pmatrix} \tag{2.103}$$

Si on applique le complément de Schur, l'expression précédente devient :

$$\begin{pmatrix} A_K^T P + P A_K + \mu I_3 + Q + 2\eta P & 0 & P \\ 0 & -e^{-2\eta\tau} Q + \rho I & 0 \\ P & 0 & -\frac{1}{\lambda} I_3 \end{pmatrix} \leqslant 0 \tag{2.104}$$

La condition (2.90) est donc équivalente à $\mathcal{M} + 2\eta\mathcal{N} \leqslant 0$ et donc, d'après (2.102) :

$$\dot{V}' + 2\eta V' \leqslant 0 \tag{2.105}$$

ce qui implique $\dot{V}' \leqslant -2\eta V'$.
D'où, par intégration :

$$V'(e, e_\tau) \leqslant e^{-2\eta t} \max_{\theta \in [-\tau, 0]} V'(e(0), e(\theta)) \tag{2.106}$$

La condition (2.93b) est donc vérifiée, avec $\phi = 2\eta$.
Par ailleurs, le membre de gauche de l'inégalité (2.94) donne :

$$\|e(t)\| \leqslant \sqrt{\frac{V'(e, e_\tau)}{\lambda_m(P)}} \tag{2.107}$$

D'après (2.94), (2.106) et (2.107), on obtient finalement :

$$\|e(t)\| \leqslant \sqrt{\frac{\alpha_1}{\alpha_2}} e^{-\eta t} \max_{\theta \in [-\tau, 0]} \|e(\theta)\| \tag{2.108}$$

avec $\alpha_1 = \lambda_M(P) + \tau \lambda_M(Q)$ et $\alpha_2 = \lambda_m(P)$, ce qui démontre la formule (2.91). □

2.3.2.3 Simulations

Dans ces simulations, les paramètres de l'émetteur (2.61) ont les valeurs indiquées dans le tableau 2.4.

α	β	γ	δ	ε	σ	τ
9	14	5	0.5	10	10^4	1

TAB. 2.4 - *Paramètres du système* (2.61)

Remarque 2.3.4. Les systèmes chaotiques sont des systèmes très sensibles à de petites variations de leurs paramètres. Les valeurs numériques illustrant la plupart des simulations présentées dans ce mémoire comportent un nombre inhabituel de décimales : cette précision est nécessaire pour appliquer les résultats obtenus. ♦

On s'intéresse uniquement à la vérification de la convergence exponentielle étudiée précédemment, sachant que la convergence exponentielle est une propriété plus forte que la convergence asymptotique.
Les états initiaux de l'émetteur et de l'observateur sont respectivement :

$$x_0 = \begin{pmatrix} 0,1 & 0,1 & 0,1 \end{pmatrix}^T \tag{2.109}$$

$$\hat{x}_0 = \begin{pmatrix} -0,1 & -0,1 & -0,1 \end{pmatrix}^T \tag{2.110}$$

L'intégration numérique se fait par la méthode de Runge-Kutta d'ordre quatre, avec un pas d'intégration égal à une milliseconde.
Après un changement de variable approprié, la BMI (2.90) est mise sous forme de LMI équivalente. Ensuite on applique un algorithme d'optimisation convexe, et on obtient le gain suivant pour l'observateur (2.73), en choisissant $\zeta = 10^{-5}$:

$$K = \begin{pmatrix} 46,20227407747760 \\ 44,67211651386433 \\ -39,35359557513618 \end{pmatrix} \tag{2.111}$$

la matrice P correspondante :

$$P = \begin{pmatrix} 10,67806901949104 & -5,2057308147326 & 1,0373955343056 \\ (\star) & 5,362463079740826 & 0,12069535790816 \\ (\star) & (\star) & 1,274317869299573 \end{pmatrix} \tag{2.112}$$

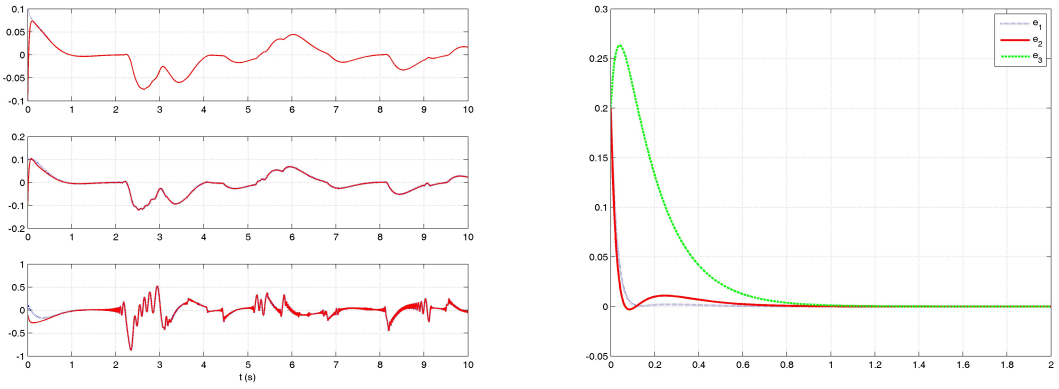
et la matrice Q :

$$Q = \begin{pmatrix} 176,64650402305 & 0,001469259380 & -0,000052051711 \\ (\star) & 29,720566040812 & 5,20517112358 \\ (\star) & (\star) & 6,842761356546 \end{pmatrix} \tag{2.113}$$

Le coefficient η est fixé à la valeur $0,85$ et garantit la convergence exponentielle selon la formule (2.91), avec les valeurs suivantes $\alpha_1 = 18,83117929851526$ et $\alpha_2 = 0,79116488503818$, donc en remplaçant les valeurs numériques dans (2.91), on obtient :

$$\|e(t)\| \leqslant 0,978e^{-0,85t} \tag{2.114}$$

car les conditions initiales choisies ici donnent $\max\limits_{\theta\in[-\tau,0]} \|e(\theta)\| = 0,2$.
La figure (2.11) montre d'une part les trajectoires des états réels et reconstruits (Fig. 2.11(a)), d'autre part les trois composantes de l'erreur de synchronisation $e(t)$ (Fig. 2.11(b)).



(a) États réels et estimés

(b) Composantes de $e(t)$

FIG. 2.11 - *Synchronisation à base d'observateur d'ordre plein*

Remarque 2.3.5. On constate sur des simulations que le fait de diminuer la valeur du paramètre ζ influence directement la vitesse de convergence de l'erreur vers zéro. Ainsi, si on prend pour ζ une valeur dix fois plus petite que dans la simulation précédente, c'est-à-dire $\zeta = 10^{-6}$, alors on peut choisir $\eta = 2,5$ (au lieu de $0,85$), et d'après la formule (2.91) $e(t)$ converge plus vite vers zéro. Si on prend une valeur cent fois plus petite que dans la simulation, c'est-à-dire $\zeta = 10^{-7}$, alors η peut être fixé à la valeur $4,5$. Comme les paramètres ζ et η interviennent de façon

hautement non linéaire dans le processus de résolution de la BMI (2.90), il semble difficile de quantifier leur influence directe sur la vitesse de convergence de l'erreur vers zéro. ♦

2.3.2.4 Extension des résultats

On peut étendre les résultats précédents à un système non linéaire de dimension n quelconque, possédant la structure suivante :

$$\begin{aligned} \dot{X}(t) &= AX(t) + F(X(t)) + H(X(t-\tau)) \\ Y(t) &= CX(t) \end{aligned} \tag{2.115}$$

On ordonne les composantes du vecteur d'état et on suppose qu'il existe un entier $p < n$ tel que :

$$F(X(t)) = F\left(X_1(t), \ldots, X_p(t)\right) \tag{2.116}$$

et

$$H(X(t-\tau)) = H\left(X_1(t-\tau), \ldots, X_p(t-\tau)\right) \tag{2.117}$$

Les fonctions F et H sont supposées lipschitziennes, de constantes respectives k_F et k_H.
On fait une hypothèse supplémentaire sur la matrice C, qui va permettre de maîtriser de grandes constantes de Lipschitz k_F et k_H :

$$C = \left(\begin{array}{c|c} I_p & \bar{C} \end{array} \right) \tag{2.118}$$

où $\bar{C}$ a une structure particulière : sur chaque ligne, tous les coefficients sont nuls sauf un, noté ζ_i, situé à l'intersection de la $i^{ème}$ ligne et de la $j(i)^{eme}$ colonne, pour $i = 1, n$.
Ce choix particulier pour la matrice C implique que les p sorties du système (2.115) s'écrivent :

$$Y_i(t) = X_i(t) + \zeta_i X_{j(i)}(t), \quad p < j(i) \leqslant n \tag{2.119}$$

On opère de la même manière qu'au paragraphe 2.3.2.1. On met le système (2.115) sous la forme :

$$\begin{aligned} \dot{X} &= \tilde{A}X + \tilde{B}Y + \tilde{F} + \tilde{H} \\ Y &= CX \end{aligned} \tag{2.120}$$

Les matrices $\tilde{A}$ et $\tilde{B}$ se déduisent des matrices A et C. Il faut tout d'abord réaliser les partitions suivantes :

$$X = \left(\begin{array}{c} \bar{X} \\ \bar{\bar{X}} \end{array} \right) \tag{2.121}$$

avec $\dim \bar{X} = (p \times n)$, et

$$A = \left(\begin{array}{c|c} \bar{A} & \bar{\bar{A}} \end{array} \right) \tag{2.122}$$

avec $\dim \bar{A} = (n \times p)$ et $\dim \bar{\bar{A}} = (n \times (n-p))$. On peut alors écrire :

$$AX = \begin{pmatrix} \bar{A} & \bar{\bar{A}} \end{pmatrix} \begin{pmatrix} Y - \bar{C}\bar{\bar{X}} \\ \bar{\bar{X}} \end{pmatrix} = \bar{A}Y - \bar{A}\bar{C}\bar{\bar{X}} + \bar{\bar{A}}\bar{\bar{X}} \tag{2.123}$$

D'où les expressions, obtenues en identifiant les termes des formules (2.123) et (2.120) :

$$\tilde{A} = \begin{pmatrix} 0_{n\times p}| & \bar{A}\bar{C} + \bar{\bar{A}} \end{pmatrix} \tag{2.124}$$

$$\tilde{B} = \bar{A} \tag{2.125}$$

Ensuite, en utilisant (2.116), (2.117) et (2.119), on trouve l'expression des fonctions $\tilde{F}$ et $\tilde{H}$:

$$\tilde{F} = F\left(Y_1(t) - \zeta_1 X_{j(1)}(t), \ldots, Y_p(t) - \zeta_p X_{j(p)}(t)\right) \tag{2.126}$$

et

$$\tilde{H} = H\left(Y_1(t-\tau) - \zeta_1 X_{j(1)}(t-\tau), \ldots, Y_p(t-\tau) - \zeta_p X_{j(p)}(t-\tau)\right) \tag{2.127}$$

On en déduit les nouvelles inégalités, comme au paragraphe 2.3.2.1, avec les notations (2.26), (2.27) :

$$\begin{array}{rcl} \|\tilde{F} - \hat{\tilde{F}}\| & = & \|F\left(Y_1(t) - \zeta_1 X_{j(1)}(t), \ldots, Y_p(t) - \zeta_p X_{j(p)}(t)\right) \\ & & -F\left(Y_1(t) - \zeta_1 \hat{X}_{j(1)}(t), \ldots, Y_p(t) - \zeta_p \hat{X}_{j(p)}(t)\right)\| \\ & \leqslant & k_F \zeta_{max} \| \left(X_{j(1)}(t) - \hat{X}_{j(1)}(t), \ldots,\ X_{j(p)}(t) - \hat{X}_{j(p)}(t)\right)\| \\ & \leqslant & k_F \zeta_{max} \|\epsilon(t)\| \end{array} \tag{2.128}$$

où $\zeta_{max} = \max_{i=1,p} \zeta_i$ et $\epsilon(t) = X(t) - \hat{X}(t)$.
Le même raisonnement sur la fonction $\tilde{H}$ aboutit à :

$$\|\tilde{H} - \hat{\tilde{H}}\| \leqslant k_H \zeta_{max} \|\epsilon(t)\| \tag{2.129}$$

Les observateurs asymptotique et exponentiel détaillés précédemment ne sont pas spécifiques à l'exemple (2.61), la procédure de synthèse reste valable en dimension quelconque. Par conséquent, les résultats précédents, c'est-à-dire le théorème 2.3.2 et le corollaire 2.3.3, peuvent être appliqués dans le cas général du système (2.115).

Remarque 2.3.6. Par la suite, on peut ajouter des contraintes supplémentaires sur $\bar{C}$, par exemple imposer qu'une colonne particulière soit nulle (comme nous l'avons imposé dans la remarque 2.3.2), afin de ne pas transmettre d'information sur l'état correspondant, qui peut être utilisé par ailleurs. ♦

2.4 Observateurs d'ordre réduit

Il n'est pas toujours nécessaire de concevoir un observateur qui reconstruit tous les états de l'émetteur, puisque le signal transmis $y(t)$ contient déjà des informations sur les états du système à observer. Dans cette section, l'émetteur choisi est le *SCTH* (2.11) et nous proposons un observateur réduit (d'ordre deux) pour ce système, construit selon une procédure utilisant des transformations matricielles.
Dans la suite de ce mémoire, un Observateur d'Ordre Réduit sera désigné par l'abréviation *OOR*.

2.4.1 Synthèse de l'observateur d'ordre réduit

On rappelle le modèle de l'émetteur chaotique choisi :

$$\left\{\begin{array}{lcl} \dot{x}_1(t) &=& -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta\tanh(x_1(t)) \\ \dot{x}_2(t) &=& x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &=& -\beta x_2(t) - \gamma x_3(t) + \varepsilon\sin(\sigma x_{1\tau}(t)) \end{array}\right. \tag{2.130}$$

et le signal transmis :

$$y(t) = Cx(t) \tag{2.131}$$

On détaille dans cette partie le cas où $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix}$ comme au paragraphe 2.3.2. On utilise la relation $y = x_1 + \zeta x_2$ pour mettre le modèle (2.130) sous la forme (2.64)-(2.68) :

$$\left\{\begin{array}{l} \dot{x}(t) = \tilde{A}x(t) + \tilde{B}y(t) + \tilde{F}(x(t), y(t)) + \tilde{H}(x_\tau(t), y_\tau(t)) \\ y(t) = Cx(t) \end{array}\right. \tag{2.132}$$

Les matrices $\tilde{A}$, $\tilde{B}$ et les fonctions $\tilde{F}$, $\tilde{H}$ ont été définies au paragraphe 2.3.2.1.
Le signal transmis contient en particulier des informations sur le premier état x_1. Il n'est donc pas nécessaire d'estimer directement x_1 au niveau du récepteur, la reconstruction des deux autres états par un OOR et la connaissance du signal $y(t)$ vont permettre de déduire une estimation de $x_1(t)$.
On va tout d'abord créer un système auxiliaire dont la dynamique de x_1 est absente. Pour cela, on élimine x_1 par projection. Comme il s'agit de la première composante de l'état, il suffit de trouver une matrice E orthogonale au vecteur $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$.
Pour pouvoir récupérer des informations sur l'état x_1 qui n'est pas reconstruit par l'observateur réduit, on doit faire une hypothèse supplémentaire sur E :

Hypothèse 2.4.1. La matrice $\begin{pmatrix} E \\ C \end{pmatrix}$ est de plein rang colonne. ♦

Si on multiplie l'équation d'état à gauche par la matrice E, on obtient le système singulier :

$$E\dot{x} = E\tilde{A}x + E\tilde{B}y + E\tilde{F}(x) + E\tilde{H}(x_\tau) \tag{2.133}$$

donc, par hypothèse sur E, le système (2.132) se met sous la forme :

$$\left\{ \begin{array}{lcl} E\dot{x} & = & A_1 x + B_1 y + H_1(x_\tau) \\ y & = & Cx \end{array} \right. \tag{2.134}$$

avec les notations

$$\begin{array}{l} A_1 = E\tilde{A} \\ B_1 = E\tilde{B} \\ H_1 = E\tilde{H} \end{array} \tag{2.135}$$

En accord avec l'hypothèse 2.4.1, il existe deux matrices P et Q de dimensions appropriées telles que

$$\left(\begin{array}{cc} P & Q \end{array} \right) \left(\begin{array}{c} E \\ C \end{array} \right) = I_3 \tag{2.136}$$

On peut écrire :

$$\left(\begin{array}{cc} P & Q \end{array} \right) = \left(\left(\begin{array}{c} E \\ C \end{array} \right)^T \left(\begin{array}{c} E \\ C \end{array} \right) \right)^{-1} \left(\begin{array}{c} E \\ C \end{array} \right)^T \tag{2.137}$$

Nous présentons une procédure de construction d'un OOR du système (2.132). Nous proposons un observateur dont l'état z est une combinaison linéaire des états x_2 et x_3 :

$$z = Tx = \left(\begin{array}{c} z_1 \\ z_2 \end{array} \right) \tag{2.138}$$

Le modèle dynamique de cet OOR est le suivant :

$$\begin{array}{l} \dot{z} = Nz + Ky + r(z, y, z_\tau, y_\tau) \\ \hat{z} = z + TQy \end{array} \tag{2.139}$$

Les matrices N, K et la fonction $r(z, y, z_\tau, y_\tau)$ sont déterminées dans la suite.
Le théorème suivant utilise les résultats de [Boutayeb 95] et [Cherrier 06c] et donne des conditions suffisantes de convergence de l'OOR (2.139).

Théorème 2.4.1 ([Cherrier 06c]). *Si les conditions suivantes sont vérifiées :*

(i) condition de détectabilité

$$rank \left(\begin{array}{c} sE - A_1 \\ C \end{array} \right) = \dim x, \ \forall s \geqslant 0 \tag{2.140}$$

(ii) il existe une matrice N telle que

$$NTPE - TP\left(A_1 + B_1C\right) + KC = 0 \tag{2.141}$$

(iii) la matrice $\begin{pmatrix} TPE \\ C \end{pmatrix}$ *est inversible ;*

(iv) il existe une matrice symétrique définie positive U et une matrice définie positive Ω telles que :

$$\begin{pmatrix} N^TU + UN + \Omega & UTP \\ (\star) & -\frac{1}{k_{H_1}} I_2 \end{pmatrix} < 0 \tag{2.142}$$

et

$$k_{H_1} I_2 - \Omega < 0 \tag{2.143}$$

alors la fonction $r(z, y, z_\tau, y_\tau)$ peut être définie par :

$$r(z, y, z_\tau, y_\tau) = TPH_1(\hat{x}_\tau) \tag{2.144}$$

où

$$\hat{x} = \begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} \begin{pmatrix} \hat{z} \\ y \end{pmatrix} \tag{2.145}$$

Dans ce cas, l'OOR (2.139) *est asymptotiquement convergent et $\hat{x}$ tend vers x.* ■

Démonstration : le vecteur d'erreur d'estimation d'état réduit est défini par $e = \hat{z} - z$. D'après (2.136) et (2.139), on peut écrire :

$$e = (z + TQy) - z = TQCx = T(I_3 - PE)x = z - TPEx \tag{2.146}$$

Par dérivation de l'équation précédente, la dynamique de e est donnée par :

$$\dot{e} = Nz + Ky + r(z, y, z_\tau, y_\tau) - TP\left(A_1x + B_1y + H_1(x_\tau)\right) \tag{2.147}$$

On remplace alors z par son expression en fonction de e, déduite de (2.146) et (2.147) devient :

$$\begin{array}{rcl} \dot{e} & = & N(e + TPEx) + KCx + r(z, y, z_\tau, y_\tau) - TPA_1x - TPB_1y - TPH_1(x_\tau) \\ & = & Ne + (NTPE - TP(A_1 + B_1C) + KC)x + r(z, y, z_\tau, y_\tau) - TPH_1(x_\tau) \end{array} \tag{2.148}$$

D'après les hypothèses (2.141) et (2.144) du théorème 2.4.1, l'équation précédente se réduit à :

$$\dot{e} = Ne + TP\left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) \tag{2.149}$$

On définit une fonctionnelle de Lyapunov-Krasovskii, U étant une matrice symétrique définie

positive et Ω une matrice définie positive :

$$V = e^T U e + \int_{-\tau}^{0} e(t+\theta)^T \Omega e(t+\theta) d\theta \tag{2.150}$$

D'une part, on a $\lambda_m(U)\|e\|^2 \leqslant V$ et $U > 0$, donc $V \geqslant 0$.
D'autre part, la dérivée de V le long des trajectoires de (2.149) est donnée par :

$$\dot{V} = e^T \left(N^T U + UN + \Omega\right) e + 2e^T UTP \left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) - e_\tau^T \Omega e_\tau \tag{2.151}$$

Comme précédemment, on applique les inégalités de Cauchy-Schwarz et de Young successivement :

$$2e^T UTP \left(H_1(\hat{x}_\tau) - H_1(x_\tau)\right) \leqslant k_{H_1} e^T (UTP)(UTP)^T e + k_{H_1} \|e_\tau\|^2 \tag{2.152}$$

D'où la majoration de $\dot{V}$:

$$\dot{V} \leqslant e^T \left(N^T U + UN + k_{H_1}(UTP)(UTP)^T\right) e + e_\tau^T \left(k_{H_1} I_2 - \Omega\right) e_\tau \tag{2.153}$$

En utilisant le complément de Schur, avec les hypothèses (2.142) et (2.143), on obtient $\dot{V} \leqslant 0$ et l'erreur d'estimation converge vers zéro.

En utilisant la relation (2.145), on obtient :

$$\begin{pmatrix} TPE \\ C \end{pmatrix} (\hat{x} - x) = \begin{pmatrix} \hat{z} \\ y \end{pmatrix} - \begin{pmatrix} TPEx \\ Cx \end{pmatrix} \tag{2.154}$$

On vient de montrer que $e \to 0$, donc (2.146) implique $\hat{z} \to TPEx$. Par conséquent, comme la matrice $\begin{pmatrix} TPE \\ C \end{pmatrix}$ est inversible par hypothèse, (2.154) assure que $\hat{x} \to x$. □

Nous indiquons la procédure de recherche des gains N et K de l'observateur réduit. Pour cela, on suppose que les matrices C et E ont été choisies de telle sorte que la condition de détectabilité (2.140) soit remplie.

Procédure
La relation (2.136) et l'équation de Sylvester (2.141) permettent d'écrire (on note $A_2 = A_1 + B_1 C$ pour alléger les formules) :

$$NT - TPA_2 = MC \tag{2.155}$$

avec

$$M = NTQ - K \tag{2.156}$$

La matrice $\begin{pmatrix} TPE \\ C \end{pmatrix}$ étant supposée inversible, il existe par conséquent deux matrices L_1 et L_2 de dimensions appropriées telles que

$$\begin{pmatrix} TPE \\ C \end{pmatrix}^{-1} = \begin{pmatrix} L_1 & L_2 \end{pmatrix} \tag{2.157}$$

En multipliant (2.155) à droite par L_2, on obtient :

$$M = NTL_2 - TPA_2L_2 \tag{2.158}$$

car $CL_2 = 1$.
De même, en multipliant (2.141) à droite par L_1, il vient :

$$N = TPA_2L_1 \tag{2.159}$$

L'astuce de [Boutayeb 95] consiste alors à introduire une matrice R telle que $\begin{pmatrix} R \\ C \end{pmatrix}$ soit inversible et qui soit liée à $\begin{pmatrix} TPE \\ C \end{pmatrix}$ par la relation :

$$\begin{pmatrix} TPE \\ C \end{pmatrix} = \begin{pmatrix} I_2 & -F \\ 0 & 1 \end{pmatrix} \begin{pmatrix} R \\ C \end{pmatrix} \tag{2.160}$$

Si on développe cette égalité, il vient en particulier :

$$TPE = R - FC \tag{2.161}$$

Ce qui, en utilisant (2.136), revient à :

$$\begin{aligned} &T(I_3 - QC) = R - FC \\ &T = R + (TQ - F)\,C \\ &T = R + SC \end{aligned} \tag{2.162}$$

avec

$$S = TQ - F \tag{2.163}$$

On remplace alors l'expression (2.161) de T dans (2.159) :

$$N = RPA_2L_1 - SCPA_2L_1 \tag{2.164}$$

Remarque 2.4.1. Si la paire (RPA_2L_1, CPA_2L_1) est détectable, alors la matrice S peut être choisie pour garantir la stabilité du gain N par une technique de placement de pôles. En fait, il

est démontré dans [Darouach 95] que cette condition de détectabilité est équivalente à l'hypothèse (2.140) du théorème 2.4.1. ♦

Nous présentons maintenant un résumé de la procédure à appliquer pour trouver N et K. Les matrices P et Q peuvent être déterminées par la formule (2.137) dès que les matrices C et E sont fixées :

– on choisit une matrice R telle que la matrice $\begin{pmatrix} R \\ C \end{pmatrix}$ soit inversible ;

– on calcule L_1 : en utilisant (2.157) et (2.160), on déduit la relation

$$L_1 = \begin{pmatrix} R \\ C \end{pmatrix}^{-1} \begin{pmatrix} I_2 \\ 0 \end{pmatrix} \tag{2.165}$$

– on cherche une matrice S (par une technique de placement de pôles) qui stabilise N, en utilisant la relation (2.164) et si on trouve une matrice U solution de la LMI (2.142), la synchronisation est garantie ;

– on calcule T et F grâce aux formules (2.161) et (2.163) ;

– on calcule L_2 en utilisant (2.157) et (2.160)

$$L_2 = \begin{pmatrix} R \\ C \end{pmatrix}^{-1} \begin{pmatrix} -F \\ 1 \end{pmatrix} \tag{2.166}$$

– finalement, en utilisant (2.158) on obtient M, puis avec (2.156) on obtient K :

$$K = NTQ - M \tag{2.167}$$

2.4.1.1 Simulations

Les valeurs des paramètres du système (2.130) pour cette simulation sont regroupées dans le tableau 2.5.

α	β	γ	δ	ε	σ	τ
9	14	5	$0,5$	10	10^4	1

TAB. 2.5 - *Paramètres du système* (2.130)

Pour appliquer la procédure détaillée au paragraphe précédent, on choisit :

$$C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix} \tag{2.168}$$

avec $\zeta = 0,00001$,

$$E = R = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{2.169}$$

On trouve les gains suivants pour l'observateur (2.139) :

$$N = \begin{pmatrix} -1,00001 & 1 \\ -14 & -5 \end{pmatrix} \tag{2.170}$$

et

$$K = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \tag{2.171}$$

Les autres matrices intervenant dans la procédure sont :

$$\begin{gathered} L_1 = \begin{pmatrix} -0,00001 & 0 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \quad L_2 = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \quad S = \begin{pmatrix} 1 \\ 1 \end{pmatrix} \\ T = \begin{pmatrix} 1 & 1,00001 & 0 \\ 1 & 1,00001 & 1 \end{pmatrix} \quad F = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \quad M = \begin{pmatrix} -1,00001 \\ -19 \end{pmatrix} \end{gathered} \tag{2.172}$$

Les matrices U et Ω, solutions des LMI (2.142) et (2.143) sont données par :

$$U = \begin{pmatrix} 4,30276274636934 & 0,66879305291552 \\ (\star) & 0,42626830406180 \end{pmatrix} \tag{2.173}$$

$$\Omega = \begin{pmatrix} 4,51940446124179 & 1,267869928378402 \\ (\star) & 1,70288595984081 \end{pmatrix} \tag{2.174}$$

Les états initiaux du *SCTH* (2.130) et de l'observateur réduit (2.139) sont respectivement :

$$x_0 = \begin{pmatrix} 0,1 & 0 & 0,1 \end{pmatrix}^T \tag{2.175}$$

$$z_0 = \begin{pmatrix} 10 & 5 \end{pmatrix}^T \tag{2.176}$$

La figure 2.12 montre les trois composantes du vecteur d'erreur de synchronisation $e(t)$. Les simulations sont réalisées avec une méthode d'intégration numérique de Runge-Kutta d'ordre quatre, de pas $10^{-3}s$.

2.4.2 Extension des résultats

Dans ce paragraphe, nous continuons la généralisation en dimension quelconque des résultats établis, généralisation initiée au paragraphe 2.3.2.4. On considère à nouveau le système (2.120)

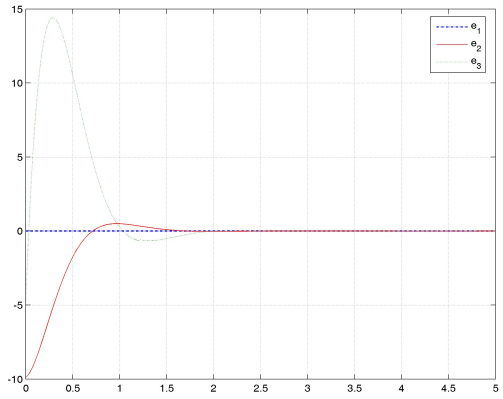


FIG. 2.12 - *Composantes de* $e(t)$

de dimension n :

$$\begin{aligned} \dot{X} &= \tilde{A}X + \tilde{B}Y + \tilde{F} + \tilde{H} \\ Y &= CX \end{aligned} \tag{2.177}$$

On a supposé en (2.118) que la matrice C peut être décomposée sous la forme $C = \left(\begin{array}{c|c} I_p & \bar{C} \end{array} \right)$, pour maîtriser de grandes constantes de Lipschitz au niveau des nonlinéarités. Alors on construit un système auxiliaire dont la dynamique des p premiers états est absente : la matrice E, de dimension $(p \times n)$, doit être orthogonale à la matrice identité de dimension p. On obtient le système singulier suivant (qui généralise (2.134)) :

$$\left\{ \begin{array}{rcl} E\dot{x} & = & A_1 x + B_1 y + F_1(x) + H_1(x_\tau) \\ y & = & Cx \end{array} \right. \tag{2.178}$$

avec les mêmes notations.
On reprend la même structure d'observateur réduit :

$$\begin{aligned} \dot{z} &= Nz + Ky + r(z, y, z_\tau, y_\tau) \\ \hat{z} &= z + TQy \end{aligned} \tag{2.179}$$

Le théorème 2.4.1 peut être transposé comme suit.

Corollaire 2.4.2. *On reprend les hypothèses du théorème 2.4.1 avec une modification, au niveau de la LMI* (2.142) *: on suppose qu'il existe une matrice symétrique définie positive* U *et une matrice définie positive* Ω *telles que les LMI suivantes soient vérifiées :*

$$\left(\begin{array}{cc} N^T U + UN + \Omega + k_{F_1} I_2 & UTP \\ (\star) & -\frac{1}{k_{F_1} + k_{H_1}} I_2 \end{array} \right) < 0 \tag{2.180}$$

et

$$k_{H_1} I_2 - \Omega < 0 \tag{2.181}$$

La fonction r change également :

$$r(z, y, z_\tau, y_\tau) = TPF_1(\hat{x}) + TPH_1(\hat{x}_\tau) \tag{2.182}$$

■

Démonstration : on prend la même fonctionnelle de Lyapunov-Krasovskii que dans la preuve du théorème 2.4.1. La suite du raisonnement peut se transposer directement. □

2.5 Observateur robuste

La robustesse au bruit est un critère à prendre en compte parfois dans l'estimation de l'état d'un système, en particulier dans les systèmes de communications qui seront étudiés dans le chapitre suivant. Il s'agit alors de reconstruire l'état malgré la présence de perturbations ou de bruit, dans la dynamique du système et/ou sur la sortie. La synchronisation de l'observateur ne peut donc pas se faire de façon parfaite, mais sous certaines conditions, il est possible de trouver un gain de l'observateur garantissant une borne supérieure sur l'erreur d'estimation.

Classiquement, la théorie $\mathcal{H}_\infty$ considère la norme suivante pour un signal w :

$$\|w\|_2^2 = \int_0^\infty \|w(t)\|^2 dt \tag{2.183}$$

Cette norme, appelée norme $\mathcal{L}_2$, notée $\|.\|_2$, qui peut être vue comme l'énergie du signal, sera utilisée uniquement dans cette section consacrée à la robustesse. On considère la classe de systèmes dynamiques dont le modèle est le suivant :

$$\begin{cases} \dot{x}(t) = Ax(t) + F(x(t)) + H(x_\tau(t)) + Dw(t) \\ y(t) = Cx(t) + Ew(t) \end{cases} \tag{2.184}$$

où $w \in \mathbb{R}$ est un bruit à énergie bornée, au sens de la norme $\|.\|_2$ définie précédemment. Le fait d'utiliser le même bruit w dans la dynamique du système et sur la sortie y n'est pas restrictif, car le choix des matrices D et E est totalement libre. On peut donc toujours se ramener à ce cas.
On fait toujours les mêmes hypothèses sur les fonctions non linéaires F et H, à savoir qu'elles sont lipschitziennes, de constantes respectives k_F et k_H.

2.5.1 Synthèse d'un observateur robuste

On cherche à construire un observateur du système (2.184) qui estime l'état $x(t)$ avec une précision fixée (cette précision possédant une borne inférieure - à déterminer - en-dessous de

laquelle on ne peut pas trouver de gain pour la structure d'observateur proposée ci-dessous). Voici la dynamique de l'observateur proposé :

$$\dot{\hat{x}}(t) = A\hat{x}(t) + F(\hat{x}(t)) + H(\hat{x}_\tau(t)) + K(y - C\hat{x}(t)) \tag{2.185}$$

En définissant l'erreur d'estimation $e(t) = x(t) - \hat{x}(t)$, on cherche à minimiser le critère :

$$\mathcal{J} = \sup_{w/0<\|w\|_2^2<\infty} \frac{\|e\|_2^2}{\|w\|_2^2} \tag{2.186}$$

Le problème à résoudre peut donc s'énoncer de la manière suivante : trouver un gain K pour l'observateur (2.185) et trouver le réel positif λ minimal tel que $\mathcal{J} < \lambda^2$. Nous proposons une solution à ce problème sous la forme du théorème suivant.

Théorème 2.5.1. *S'il existe un gain K, des matrices P et Q respectivement symétrique définie positive et définie positive, et un scalaire λ solutions de la BMI et de la LMI suivantes :*

$$\begin{pmatrix} A_K^T P + P A_K + (1+k_F)I + (k_F+k_H)P^2 + Q & (D-KE)^T P \\ (\star) & -\lambda^2 \end{pmatrix} < 0 \tag{2.187}$$

avec la notation $A_K = A - KC$, et

$$k_H I - Q < 0 \tag{2.188}$$

alors le critère $\mathcal{J}$ est vérifié, et on a $\|x - \hat{x}\|_2^2 < \lambda^2 \|w\|_2^2$. ■

Démonstration : La dynamique de l'erreur a pour expression :

$$\dot{e}(t) = (A - KC)e(t) + F(x(t)) - F(\hat{x}(t)) + H(x(t)) - H(\hat{x}(t)) + (D - KE)w \tag{2.189}$$

La fonctionnelle de Lyapunov-Krasovskii standard $V(e, e_\tau)$ (voir l'annexe A) est complétée de la manière suivante :

$$\mathcal{V}(e, e_\tau, \lambda, w) = V(e, e_\tau) + \int_0^t \left(\|e(s)\|^2 - \lambda^2 \|w(s)\|^2 \right) ds \tag{2.190}$$

Si on parvient à montrer que $\mathcal{V} > 0$ et que $\dot{\mathcal{V}} < 0$, alors on pourra conclure que $\|e\|_2^2 < \lambda^2 \|w\|_2^2$. On développe l'expression de $\mathcal{V}$:

$$\mathcal{V} = e^T P e + \int_{-\tau}^0 e(t+\theta)^T Q e(t+\theta) d\theta + \int_0^t \left(\|e(s)\|^2 - \lambda^2 \|w(s)\|^2 \right) ds \tag{2.191}$$

P et Q étant deux matrices respectivement symétrique définie positive et définie positive.

Par conséquent, on obtient immédiatement la minoration $0 < \mathcal{V}$.

En utilisant (2.184), (2.185) et (2.189) et en dérivant (2.191), on arrive à (on conserve les

notations introduites en (2.26) et (2.27)) :

$$\begin{aligned}\dot{\mathcal{V}} &= e^T\left(A_K^TP + PA_K + Q + I\right)e + 2e^TP(F-\hat{F}) + 2e^TP(H-\hat{H}) - e_\tau^TQe_\tau - \lambda^2w^Tw \\ &\quad + w^T(D-KE)^TPe + e^TP(D-KE)w\end{aligned} \tag{2.192}$$

Comme en (2.83) et (2.84), on majore les termes $2e^TP(F-\hat{F})$ et $2e^TP(F-\hat{H})$, pour aboutir à :

$$\begin{aligned}\dot{\mathcal{V}} &\leqslant e^T\left(A_K^TP + PA_K + Q + (1+k_F)I + (k_F+k_H)P^2\right)e + e_\tau^T\left(k_HI - Q\right)e_\tau - \lambda^2w^Tw \\ &\quad + w^T(D-KE)^TPe + e^TP(D-KE)w\end{aligned} \tag{2.193}$$

On introduit alors la matrice suivante :

$$M = \begin{pmatrix} A_K^TP + PA_K + (1+k_F)I + (k_F+k_H)P^2 + Q & (D-KE)^TP \\ (\star) & -\lambda^2 \end{pmatrix} \tag{2.194}$$

et l'inégalité (2.193) se met sous la forme :

$$\dot{\mathcal{V}} \leqslant \begin{pmatrix} e \\ w \end{pmatrix}^T M \begin{pmatrix} e \\ w \end{pmatrix} + e_\tau^T\left(k_HI - Q\right)e_\tau \tag{2.195}$$

Si les conditions (2.187) et (2.188) sont vérifiées, alors $\|e\|_2^2 < \lambda^2\|w\|_2^2$. □

Pour pouvoir résoudre la BMI (2.187), on effectue un changement de variable en posant $L = PK$. En appliquant le, complément de Schur (C.2.1), on peut alors écrire l'équivalence suivante, d'après (2.194) :

$$M < 0 \Leftrightarrow \begin{pmatrix} A^TP + PA - C^TL^T - LC + (1+k_F)I + Q & D^TP - E^TL^T & P \\ (\star) & -\lambda^2 & 0 \\ (\star) & (\star) & \dfrac{-1}{k_F+k_H}I \end{pmatrix} < 0 \tag{2.196}$$

Cette nouvelle inégalité matricielle, linéaire en les variables P, L et Q, ainsi que la LMI (2.188) peuvent être résolues numériquement par un algorithme d'optimisation convexe. L'inconnue λ est soit fixée pour imposer une borne sur l'erreur d'estimation, soit à déterminer, pour trouver ainsi la valeur minimale de λ pour laquelle ces deux LMI sont réalisables.

2.5.2 Application au *SCTH*

Le système dynamique considéré est le *SCTH* (2.61), avec les paramètres donnés dans le tableau 2.6.

Nous voulons déterminer un gain K qui minimise la valeur de λ, en utilisant la procédure décrite au paragraphe précédent. Nous trouvons ainsi $\lambda_{min} = 1,52961852295909$, et le gain K obtenu

α	β	γ	δ	ε	σ	τ
9	14	5	0.5	10	10	1

TAB. 2.6 - *Paramètres du* SCTH

est donné par :

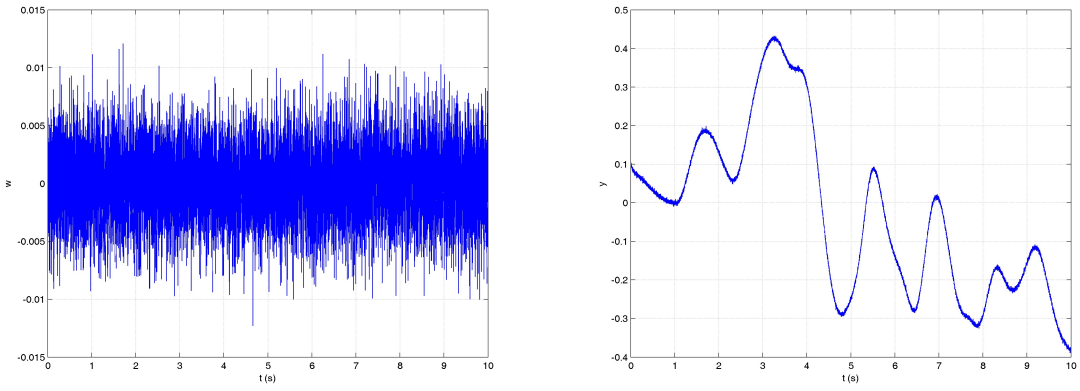
$$K = \begin{pmatrix} 87,44523513355328 \\ 4,69756674735193 \\ -25,72152752198859 \end{pmatrix} \tag{2.197}$$

Les matrices auxiliaires P et Q sont les suivantes :

$$P = \begin{pmatrix} 0,07495121631167 & 0,04397709221432 & 0,17194777688032 \\ (\star) & 5,62570909900333 & 1,17603243038692 \\ (\star) & (\star) & 0,79935005194030 \end{pmatrix} \tag{2.198}$$

$$Q = \begin{pmatrix} 1,16859581011479 & 0,86976650699722 & 0,39975988445420 \\ (\star) & 5,55052751149408 & 2,08334973438473 \\ (\star) & (\star) & 1,95751410544859 \end{pmatrix} \tag{2.199}$$

Les simulations sont faites en utilisant une méthode d'intégration de Runge-Kutta d'ordre quatre, de pas égal à une milliseconde. On prend, uniquement dans cette application, les mêmes états initiaux pour le système et pour l'observateur, à savoir $x_0 = \hat{x}_0 = \begin{pmatrix} 0,1 & 0,1 & 0,1 \end{pmatrix}^T$. La matrice C est toujours choisie de la forme $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix}$ avec $\zeta = 0,01$. On considère ici que seule la sortie est affectée par le bruit w, soit $D = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix}^T$ et $E = 1$. On a choisi un bruit w gaussien normal centré. Ce bruit, ainsi que le signal $y = Cx + w$, sont représentés à la figure 2.13. Le rapport signal sur bruit (ou Signal to Noise Ratio en anglais, noté SNR) vaut 36 dB environ.

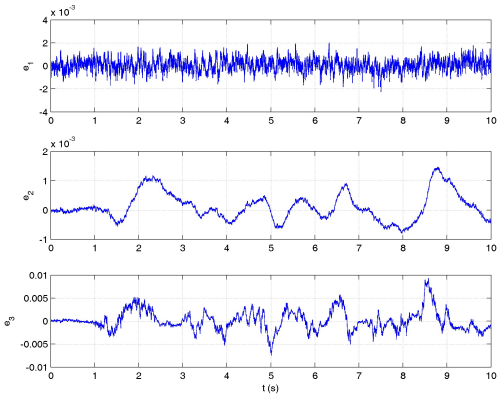


(a) Bruit $w(t)$ (b) Signal $y(t)$ bruité avec SNR=36 dB

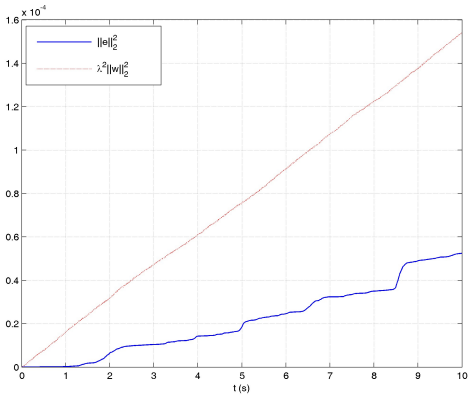
FIG. 2.13 - *Bruit et sortie bruitée*

La figure 2.14(a) montre les erreurs d'estimation des trois états du système : on constate que ces

erreurs ne tendent pas vers zéro, mais qu'elles sont bornées, proches de zéro. La figure 2.14(b) représente la norme $\mathcal{L}_2$ (2.183) des signaux e et $\lambda^2 w$: cette figure prouve que le critère $\mathcal{J}$ est bien vérifié.



(a) Composantes du vecteur d'erreur d'estimation $e(t)$



(b) Normes $\mathcal{L}_2$ de e et $\lambda^2 w$

FIG. 2.14 - *Erreurs d'estimation et normes $\mathcal{L}_2$*

On peut souligner qu'on retrouve le cas traité dans les paragraphes précédents, où $w = 0$: dans ce cas, l'erreur de synchronisation converge bien vers zéro.

2.6 Conclusion

Dans ce chapitre, nous avons présenté plusieurs schémas de synchronisation. Le choix des émetteurs s'est fixé sur une structure particulière de systèmes chaotiques, structure qui a été exploitée pour concevoir les récepteurs correspondants, sous la forme d'observateurs non linéaires. Des conditions suffisantes de synchronisation ont été établies, principalement sous la forme de BMI que l'on peut linéariser et de LMI. En appliquant une démarche classique en théorie de l'estimation, nous avons proposé différents types d'observateurs non linéaires, à savoir d'ordre plein, d'ordre réduit, robuste. L'analyse de leur synchronisation, asymptotique ou exponentielle, a fait appel à la théorie de la stabilité de Lyapunov-Krasovskii, qui concerne les systèmes à retards. La méthode développée possède cependant un conservatisme assez important, car les majorations qui interviennent dans les différentes démonstrations utilisent la propriété de Lipschitz des nonlinéarités du système émetteur, ce qui aboutit à des majorations très larges, trop larges. Il faudrait donc trouver une technique qui réduise ce conservatisme, en évitant de recourir à cette propriété de Lipschitz, qui reste malgré tout très employée dans la littérature, faute de mieux. On peut noter toutefois que les conditions suffisantes établies dans ce chapitre sont vérifiées par les systèmes considérés dans ce mémoire : l'estimation de l'état des systèmes chaotiques choisis comme émetteurs est performante. Cette capacité de synchronisation va être appliqué aux systèmes de communications dans le chapitre suivant.

CHAPITRE

3

Restauration d'entrées inconnues

Sommaire

Dans ce chapitre, nous nous intéressons à la reconstruction d'entrées inconnues, qui seront désignées dans la suite par les termes « message (secret) », ou « information ». Nous avons choisi le contexte des communications sécurisées comme application des schémas de synchronisation détaillés au chapitre précédent. Dans un premier temps, nous rappelons la progression historique du cryptage, à travers les siècles. Dans un deuxième temps, nous présentons les techniques commerciales de cryptage les plus employées actuellement. Après ces considérations générales sur la cryptographie, ou science du cryptage, nous analysons plus précisément les systèmes de communications sécurisées utilisant les systèmes chaotiques et exploitant la synchronisation à base d'observateurs. Cet examen des avantages et des inconvénients des différentes méthodes présentées au paragraphe 1.4 nous a permis de dégager des points importants pour élaborer un nouveau schéma de communications chaotiques. Notre but est de pouvoir transmettre tout type de message. La méthode proposée a recours aux propriétés fondamentales du chaos, et constitue un nouveau moyen de masquer l'information lors de sa transmission. Nous avons retenu le principe à deux voies de transmission : le premier signal transmis est dévolu à la synchronisation du récepteur. Cette synchronisation a été détaillée dans le chapitre précédent : nous utilisons l'observateur d'ordre plein conçu au paragraphe 2.3 comme récepteur. Un second signal chaotique généré par l'émetteur permet, lorsque la synchronisation est établie, de transmettre l'information par modulation de phase. L'efficacité de ce principe est testée sur des simulations variées, à savoir la transmission d'un message sonore, d'une image puis d'un texte (dans l'hypothèse de conditions de transmission parfaites). La suite de ce chapitre est consacrée à l'étude de quelques points de sécurité, dans le but d'éprouver la technique de masquage chaotique proposée. Cette démarche s'apparente à la *cryptanalyse*, opposée à la cryptographie (la cryptanalyse regroupe les techniques de déchiffrement sans la clé de cryptage). La fin de ce chapitre consiste à étudier l'impact de la présence de bruit de transmission sur la restauration de message.

3.1 Position du problème

Les procédés de cryptage constituent un domaine en plein essor. En effet, les processus chargés de sécuriser des données sont au cœur de nombreuses technologies : qu'il s'agisse de communications avec des téléphones portables, de transmission de données chiffrées par l'intermédiaire de cartes bancaires, de sites Internet... la cryptographie intervient constamment dans la vie quotidienne.

Historiquement, le cryptage existe depuis très longtemps, depuis que l'Homme a voulu communiquer des données confidentielles. Il a été développé pour préserver le secret dans la transmission de messages. Actuellement sa pratique s'est étendue, et il est plus largement utilisé pour interdire l'accès à des données sensibles et ainsi garantir la confidentialité dans des applications informatiques notamment. Le paragraphe suivant a pour but de présenter les techniques de cryptage, de plus en plus élaborées, qui ont été mises au point au fil des siècles.

3.1.1 Un peu d'histoire

Première méthode

Le premier texte chiffré connu a pour support une tablette d'argile retrouvée en Irak. Il est daté du XVI^{ème} siècle avant J.-C. Un potier avait gravé une recette secrète en supprimant les consonnes et en modifiant l'orthographe du texte.

Le bâton de Plutarque

Il s'agit d'une technique de cryptage par *transposition* (ou par changement de l'ordre des mots, la seconde grande classe de cryptage étant la *substitution*), mise au point par les Grecs entre le X^{ème} et le VII^{ème} siècle avant J.-C. Ils utilisent le bâton de Plutarque, autour duquel est enroulée une bande de cuir, puis ils y inscrivent le message. La bande de cuir est ensuite déroulée (le message est alors illisible) et envoyée au destinataire qui doit posséder un bâton identique (en taille et en diamètre) à celui de l'émetteur pour pouvoir lire le message.

Le code de César

Il s'agit d'un procédé par substitution mono-alphabétique utilisé dans l'armée romaine. Le système est simple : il revient à décaler les lettres de l'alphabet d'un nombre de lettres convenu. Ce système est très peu sûr, il est sensible notamment à des attaques statistiques, qui exploitent la fréquence de chaque lettre dans la langue considérée.

Le carré de Polybe

Ce procédé de substitution a été mis au point par l'historien grec Polybe. Il utilise un carré de vingt-cinq cases contenant chacune une lettre : chaque lettre est représentée par un groupe de deux chiffres, correspondant à sa ligne et sa colonne. Ce système de chiffrement peut être compliqué avec un mot de passe supplémentaire.

Le chiffre de Vigenère

En 1586, le diplomate français Blaise de Vigenère élabore une technique de chiffrement par substitution poly-alphabétique. Le chiffrement repose sur un mot de passe, dont chaque lettre indique le décalage à appliquer sur le texte original. Cet algorithme est très simple à utiliser et le déchiffrement est tout aussi aisé, toujours grâce à des attaques statistiques.

La machine Enigma

En 1919, un ingénieur hollandais dépose un brevet de machine à crypter électromécanique. Ce concept est repris par Arthur Scherbius pour créer en Allemagne une société destinée à fabriquer une machine à chiffrer, appelée Enigma. La simplicité et l'ingéniosité du codage attirent

l'attention des militaires. Chaque lettre est remplacée par une autre, mais la substitution change d'une lettre à l'autre. Quand on appuie sur une touche du clavier, un circuit électrique est fermé et une lampe s'allume pour indiquer la lettre codée. Parmi les points forts d'Enigma, on peut citer le nombre très important de clés ou encore la réversibilité.
En conclusion de ce paragraphe sur l'histoire du cryptage, on peut souligner que les techniques élaborées ont été adaptées, au fil des siècles, à la force des attaques. En effet, plus l'enjeu est important, plus les ennemis potentiels possèdent des moyens efficaces pour déchiffrer les messages transmis. Par conséquent la nécessité d'un niveau de sécurité de plus en plus élevé a contribué à renforcer la complexité des algorithmes de chiffrement, pour aboutir aux procédés de cryptage actuels.

3.1.2 Techniques de cryptage actuelles

Cette présentation des techniques commerciales de cryptage a pour but uniquement de situer le contexte et l'état actuels de la cryptographie. Dans ce mémoire, nous conservons un point de vue théorique sur le cryptage/décryptage, considéré sous l'angle de la reconstruction d'entrées inconnues. Nous ne mettrons donc pas en oeuvre ces techniques commerciales, les seules comparaisons seront effectuées avec des techniques de cryptage par le chaos, qui présentent des points communs avec la méthode que nous proposons.
Les techniques présentées précédemment montrent que le cryptage repose sur une transformation de l'information, de façon à en interdire l'accès à un récepteur non autorisé. Les processus de cryptage ont été largement développés au cours des dernières décennies, notamment grâce à l'utilisation intensive de l'informatique et des codages numériques. Le domaine de la cryptographie est assez confidentiel : les dernières avancées ne sont bien sûr pas divulguées, par conséquent nous allons maintenant présenter les techniques les plus utilisées, appartenant au domaine public.
Les procédés de cryptage actuels sont illustrés par la figure 3.1. L'émetteur veut transmettre un message que seul le récepteur doit être capable de déchiffrer. Il effectue ainsi une procédure de chiffrement, puis transmet le message crypté par l'intermédiaire d'un canal public. Le récepteur effectue alors l'opération inverse, ou décryptage, pour récupérer le message original. L'efficacité du système repose sur la connivence entre l'émetteur et le récepteur à propos des fonctions de cryptage/décryptage. Il est nécessaire de vérifier que ces fonctions restent secrètes et ne peuvent pas être reconstituées à partir de la seule donnée du message crypté. Pour limiter les risques, il faut pouvoir changer régulièrement de technique de cryptage/décryptage, d'où l'utilisation de clés. Les clés sont des paramètres indispensables dans la définition des fonctions de cryptage (clé 1 sur le schéma) et de décryptage (clé 2 sur le schéma). Ces fonctions peuvent éventuellement être rendues publiques, les clés seules restant secrètes. Cependant, un protocole doit être mis au point entre l'émetteur et le récepteur pour fixer les clés.

En pratique, un processus de cryptage doit vérifier deux conditions. D'une part, il ne doit pas

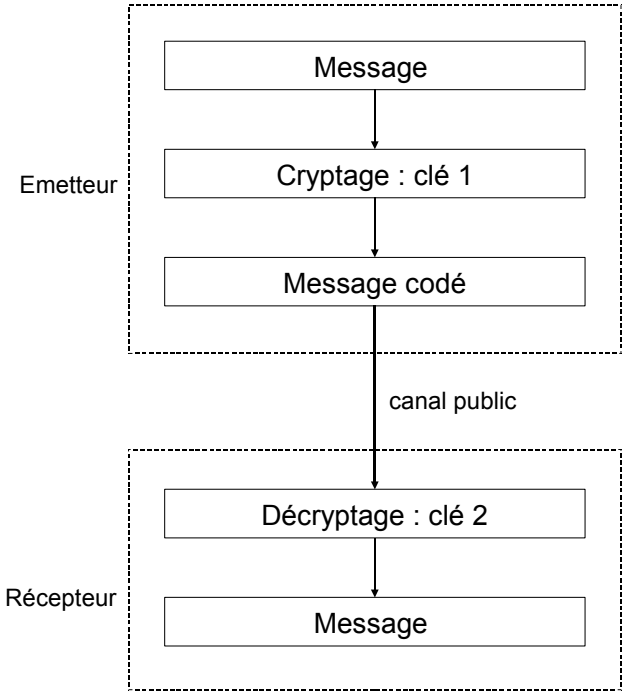


FIG. 3.1 - *Principe du cryptage*

être trop élaboré : les algorithmes de cryptage et de décryptage doivent être suffisamment rapides (donc peu complexes) pour ne pas ralentir excessivement leur mise en oeuvre. D'autre part, il doit être suffisamment difficile (voire impossible) de casser le code : la complexité du chiffrement est satisfaisante si les tentatives d'attaques échouent par découragement devant la complexité de la tâche. En résumé, le cryptage/décryptage doit être le plus rapide possible, et le temps nécessaire aux attaques doit être le plus long possible.
Concrètement, le choix de la technique de cryptage doit tenir compte des intentions et des moyens des intrus, et des risques encourus. La découverte de la clé est liée au temps et à la puissance des ordinateurs disponibles au niveau des espions. L'estimation de ce risque d'intrusion influence directement la fréquence de changement de clé.
Les techniques actuelles de cryptage sont divisées en deux grandes catégories : symétriques ou asymétriques.

Cryptage asymétrique (ou à clé publique)

Les techniques de cryptage asymétrique mettent en jeu des fonctions de cryptage et de décryptage différentes. Le plus souvent, il s'agit de la même opération, réalisée avec deux clés différentes. Cette approche élimine le problème de diffusion des clés. A chaque récepteur sont associées deux clés. La première, appelée clé publique, est connue de tous les émetteurs potentiels. Elle permet de crypter un message, qui ne peut être décrypté que par le récepteur autorisé, grâce à la seconde clé, appelée clé privée. Seule la clé privée est secrète, et ce secret n'est pas

partagé entre l'émetteur et le récepteur. Le récepteur peut créer une liste de clés publiques, et lui seul saura décrypter (grâce à la clé privée connue de lui seul) les messages cryptés à l'aide d'une de ces clés.
L'algorithme asymétrique 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 (*i.e.* 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. Parmi les autres techniques de cryptage asymétriques, on peut mentionner l'algorithme ElGamal, qui exploite le calcul logarithmique discret. On peut souligner que malgré de nombreuses études à ce sujet, les bases de l'algorithme RSA n'ont jamais été démontrées, ni infirmées.
En résumé, ces techniques asymétriques sont beaucoup utilisées pour chiffrer des messages courts, notamment par les navigateurs Internet, par les systèmes d'exploitation ou par d'autres produits informatiques. RSA fait partie des standards proposés pour Internet aussi bien que pour les réseaux de commerce électronique et les réseaux financiers. Il représente également une excellente solution pour la diffusion des clés des techniques de cryptage symétriques, que nous allons détailler dans le paragraphe suivant.

Cryptage symétrique

Le cryptage à clé symétrique utilise des clés de cryptage et de décryptage identiques. Aussi l'émetteur et le récepteur doivent-ils partager une clé commune : cela nécessite un moyen de communication secret, utilisé à chaque changement de clé. Le cryptage symétrique n'est efficace que s'il est complété par une méthode d'échange de clés bien sécurisé (il est classique d'utiliser l'algorithme RSA pour crypter les nouvelles clés).
Les algorithmes de cryptage symétrique sont fondés sur deux opérations élémentaires : la transposition et la substitution. La nature et l'ordre des opérations de transposition sont déterminés par la clé.
Voici quelques détails supplémentaires sur la méthode DES (Data Encryption Standard) adoptée comme standard par le gouvernement américain en 1977 (le DES n'est plus certifié par le gouvernement américain depuis 1988, mais il reste dans les faits un standard) :

(i) étant donné un bloc de texte clair x (de taille 64 bits), une chaîne x_0 est construite en changeant l'ordre des bits de x suivant une permutation initiale P fixée. On écrit $x_0 = P(x) = L_0R_0$ où L_0 contient les 32 premiers bits de la chaîne x_0 et R_0 contient les 32 restants ;

(ii) on effectue 16 itérations d'une certaine fonction f. On calcule L_iR_i suivant les règles $L_i = R_{i-1}$ et $R_i = L_{i-1} + f(R_{i-1}, K_i)$, où + est le "ou" exclusif bit à bit de deux chaînes, et K_1,... K_{16} sont des chaînes de 48 bits calculées à partir de la clé K ;

(iii) la permutation inverse P^{-1} est appliquée à $R_{16}L_{16}$ pour obtenir finalement le texte chiffré $P^{-1}(R_{16}L_{16})$.

Le décryptage utilise le même algorithme, mais en sens inverse.

Le DES est un système qui peut être facilement implanté : des opérations telles que le "ou" exclusif, les permutations... sont des opérations de base pour un ordinateur et peuvent donc être traitées très rapidement. 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.

Il existe des variantes de l'algorithme DES, dont la plus connue est le triple-DES.

3.1.3 Systèmes de communications chaotiques

3.1.3.1 Introduction

Deux alternatives ont été proposées durant la dernière décennie pour pallier les problèmes à venir du cryptage algorithmique, à savoir la cryptographie chaotique et la cryptographie quantique. Cette dernière, fondée sur le principe d'incertitude d'Heisenberg, qui offre une clé incassable, ne sera pas traitée dans ce mémoire.

La demande de processus de cryptage se faisant actuellement de plus en plus forte, d'intenses recherches en cryptographie sont menées pour mettre au point de nouvelles techniques. Des systèmes pseudo-chaotiques discrets sont ainsi utilisés depuis longtemps pour générer des clés chiffrées [Stinson 95]. Les systèmes chaotiques représentent donc un fort potentiel d'applications dans les systèmes de communications sécurisées. Aussi les propriétés du chaos ont-elles abouti à la mise au point de techniques cryptographiques variées, qui ont été détaillées dans le chapitre 1. Depuis les années 1990, les manifestations du chaos ne représentent plus des phénomènes nuisibles : en effet, la théorie OGY [Ott 90] 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 leur sont consacrées. Il est ainsi apparu qu'il existe des analogies entre les propriétés intrinsèques des systèmes chaotiques et les propriétés des cryptosystèmes classiques

[Alvarez 06a].

– 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 quel que soit le message à crypter.
– La *SCI* (Sensibilité aux Conditions Initiales, voir l'annexe B), ainsi que la sensibilité dans les paramètres du système, et la propriété de *mixage* correspondent 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 l'annexe B), à savoir la SCI, l'ergodicité, le mixage... 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 mentioner 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 la dernière partie de ce chapitre. Une autre propriété fondamentale des systèmes chaotiques réside dans leur comportement asymptotique apériodique, contrairement aux générateurs pseudo-aléatoires qui peuvent être périodiques (même si la période est très grande) : à l'heure actuelle, on ne sait pas générer des suites de nombres totalement aléatoires.

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 2, est

donc un processus caractéristique et fondamental des techniques de cryptage à base de systèmes chaotiques.

3.1.3.2 Choix de la méthode

Avantages et inconvénients des méthodes existantes

Nous avons mis au point un nouveau système de communications sécurisées après avoir passé en revue les avantages et inconvénients des méthodes existantes. Cet examen des différentes techniques détaillées au paragraphe 1.4 a contribué à l'élimination de certains principes, intrinsèquement "faibles" au niveau de la sécurité. Nous avons également tenu compte des attaques détaillées dans la littérature. Une étude destinée à quantifier le niveau de sécurité du principe de cryptage que nous avons mis au point sera réalisée à la fin de ce chapitre.

• Nous avons tout d'abord écarté le principe du masquage par addition, décrit au paragraphe 1.4.2. Le message étant ajouté à la porteuse chaotique, la synchronisation ne peut pas être parfaite : 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 (voir les figures des spectres des systèmes de Lorenz, Rössler et Chua dans l'annexe B, ainsi que les spectres du *SCTH* à la figure 2.3), mais cette condition limite le choix de messages pouvant être transmis.

En outre, des techniques plus élaborées de cryptanalyse ont été appliquées à cette technique de cryptage par addition, notamment dans les articles [Short 94], [Yang 98b] qui utilisent des applications de premier retour, ou dans la référence [Alvarez 05], qui exploite des techniques de filtrage.

• Nous avons également écarté la technique de cryptage par commutation, décrite au paragraphe 1.4.3. 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'autre 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 de l'information 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, la référence [Yang 95] exploite une méthode de détection des changements de paramètres de l'émetteur, tandis que [Zhou 97a] utilise des applications de premier retour et une fonction d'autocorrélation pour reconstruire le message. [Yang 98a] parvient à reconstituer le message sans connaître la valeur des paramètres de l'émetteur, ni même sa structure, en tirant profit de la robustesse de la synchronisation généralisée (voir définition au

paragraphe 1.3.2).

• Les techniques de cryptage par modulation ne semblent pas résister à des attaques spécifiques, exploitant la signature intrinsèque de chaque attracteur chaotique. En effet, l'article [Short 96] 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...), plus ou moins facilement selon la complexité du chaos considérée. Deux autres possibilités pour reconstituer l'information à partir du message transmis par l'émetteur sont détaillées dans les références [Yang 98b] et [Alvarez 04]. Ces attaques menant à la restauration non autorisée du message secret semblent concerner également le cryptage par inclusion, qui repose sur les techniques de synthèse d'UIO.

• 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.

• Nous avons enfin fait le choix de ne pas adopter une technique de cryptage mixte, qui fait appel à des notions de cryptographie classique. Ces méthodes restent en dehors du sujet de ce mémoire.

Après avoir écarté les techniques de cryptage chaotique précédentes, si on se réfère à la liste des méthodes décrites au paragraphe 1.4, il reste les techniques de cryptage reposant sur une transmission à deux voies. Nous avons ainsi décidé de conserver le principe de la transmission de deux signaux au récepteur, afin de proposer une nouvelle façon de transmettre des messages de façon sécurisée. Nous allons, dans le même temps, tenter de pallier certains problèmes qui sont énoncés dans la (vaste) littérature consacrée au cryptage par les systèmes chaotiques.

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, qui consiste à choisir l'émetteur chaotique, a déjà été abordée dans le paragraphe 2.2, mais nous allons justifier notre démarche maintenant. En fait, 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 paragraphe 3.4. 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, exposé dans les références [Pecora 90], [Abarbanel 93], sera abordé dans le chapitre 4. Ces attaques tentent de reconstituer la géométrie de l'attracteur chaotique correspondant à l'émetteur en 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 du cryptosystème, consiste à prendre comme émetteur un système hyperchaotique ou un système chaotique comportant un retard, systèmes dont le comportement peut être rendu très complexe. C'est la raison principale pour laquelle nous avons choisi comme émetteur le *SCTH* (2.11).

La deuxième étape implique la conception d'un récepteur qui se synchronise avec l'émetteur choisi. Elle a été réalisée dans le chapitre précédent.

La troisième étape consiste à mettre au point une technique de transmission du message et à garantir un certain niveau de sécurité. L'analyse des systèmes de communications chaotiques existants menée au paragraphe précédent nous a conduits à faire certains choix.
Les articles [Millérioux 98], [Jiang 02] ont tenté de renforcer la sécurité des cryptosystèmes, en séparant totalement les étapes de cryptage et de synchronisation. Nous détaillons plus précisément la référence [Jiang 02], car le cas des systèmes à temps continu y est traité. Cet article propose ainsi d'envoyer au récepteur deux signaux générés par l'émetteur chaotique. Le premier est une combinaison linéaire des états du système, il est uniquement dévolu à la synchronisation. Le second signal transmis réalise le cryptage, ou le masquage, du message par l'intermédiaire d'une fonction mathématique inversible qui prend comme arguments le message et un état du système qui n'a pas été utilisé dans le premier signal transmis. Dès que la synchronisation (théoriquement parfaite) est établie au niveau du récepteur, grâce au premier signal, le récepteur est capable de restaurer le message à partir du second signal reçu, en appliquant la fonction inverse de décryptage. Cependant, la fonction choisie dans cet article pour crypter le message n'est pas assez complexe, et laisse apparaître le message (voir le paragraphe 3.4.4 sur les analyses spectrales).

Cette technique de transmission à deux voies nous paraît très prometteuse et ce, à deux niveaux.
Tout d'abord, le premier signal, permettant à l'observateur d'estimer l'état de l'émetteur, est transmis de façon indépendante du message : il ne contient aucune information sur le message, donc aucune perturbation qui pourrait gêner la synchronisation. En outre, si les conditions de synchronisation détaillées au chapitre précédent sont vérifiées, le récepteur peut se synchroniser avec l'émetteur, sans rupture, ni perte de qualité (contrairement aux techniques de commutation). Par conséquent, l'estimation d'état est optimale au niveau du récepteur, tant au niveau de la qualité (il n'y a pas de perte de synchronisation) que de la rapidité (le signal chaotique seul est transmis), qualités qui nous paraissent primordiales pour un cryptosystème performant.

Ensuite, le principe de cryptage à deux voies sépare totalement les étapes de synchronisation et de transmission de l'information. La reconstruction des entrées inconnues peut ainsi s'appuyer

sur une estimation de l'état de l'émetteur quasi parfaite, et la synchronisation se fait indépendamment du cryptage. La transmission des deux signaux peut être réalisée sur un ou deux canaux, pas nécessairement en même temps, et sans interaction entre les deux signaux, ce qui représente un gage de sécurité supplémentaire.

Remarque 3.1.1. Bien qu'une expérimentation reste au-delà de la portée de ce mémoire, il faut souligner un point qui appartient au domaine du traitement du signal, et qui concerne justement l'utilisation de deux canaux, et d'éventuels problèmes de bande passante résultants.

3.2 Description de la méthode : modulation de phase chaotique

3.2.1 Masquage de l'information : approche intuitive

En reprenant la proposition de l'article [Jiang 02] à propos du second signal transmis pour masquer l'information, après quelques simulations avec des fonctions différentes, il s'avère que toute fonction mathématique mêlant un signal chaotique et le message ne peut pas assurer un niveau de sécurité suffisant. En effet, il suffit de regarder le spectre du second signal pour s'en rendre compte : si la bande de fréquence du message n'est pas cachée dans la partie "utile" du spectre du signal chaotique, elle apparaît clairement (voir la figure 3.19(b)). Par conséquent, nous pouvons écarter toute fonction mathématique standard pour masquer le message.
La méthode de masquage de l'information que nous avons mise en oeuvre est représentée par le schéma de la figure 3.2. Nous proposons une technique de modulation de phase pour cacher le

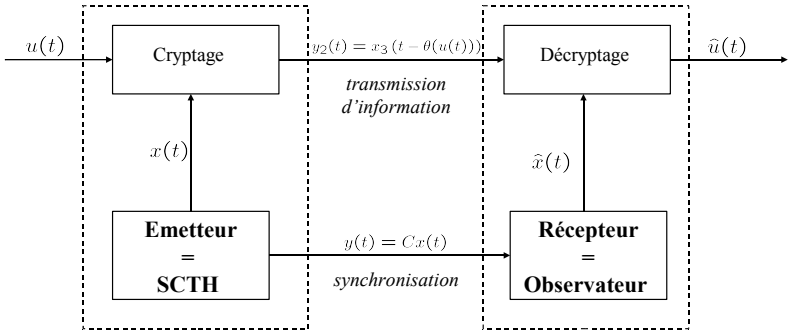


FIG. 3.2 - *Principe du système de communications proposé*

message à transmettre. Le masquage de l'information est réalisé par l'envoi d'un second signal chaotique au récepteur, qui est capable de reconstruire le message lorsque le processus de synchronisation est achevé. La figure 2.3 montre que la trajectoire du troisième état du *SCTH* est plus complexe que celle des deux autres états (cette complexité est due à la présence du retard directement dans la dynamique de x_3). Suite à cette observation, nous avons choisi d'injecter le message $u(t)$ contenant l'information en modulant la phase du signal $x_3(t)$. Cette remarque justifie *a posteriori* le choix de la matrice C fait au paragraphe 2.3.2, à l'équation (2.62), qui définit le premier signal $y(t)$ transmis au récepteur, signal consacré uniquement à la synchronisation.

En effet, ce signal $y(t)$ ne doit pas dépendre explicitement du troisième état, qui a été choisi pour masquer l'information.
On suppose que $u(t)$ est borné. Sans perte de généralité, on suppose également que $u(t) \in [0, 1]$. Le second signal transmis a pour expression :

$$y_2(t) = x_3\left(t - \theta\left(u(t)\right)\right) \tag{3.1}$$

la fonction θ étant une fonction à valeurs dans $\mathbb{R}_+$. La figure 3.3 illustre la relation (3.1). On constate que la fonction $\theta(u(t))$ représente le retard, variable dans le temps, du signal $y_2(t)$ sur le signal $x_3(t)$. La technique de décryptage peut également être interprétée grâce à la figure 3.3 :

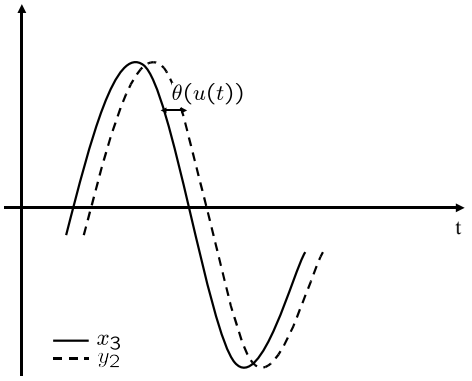
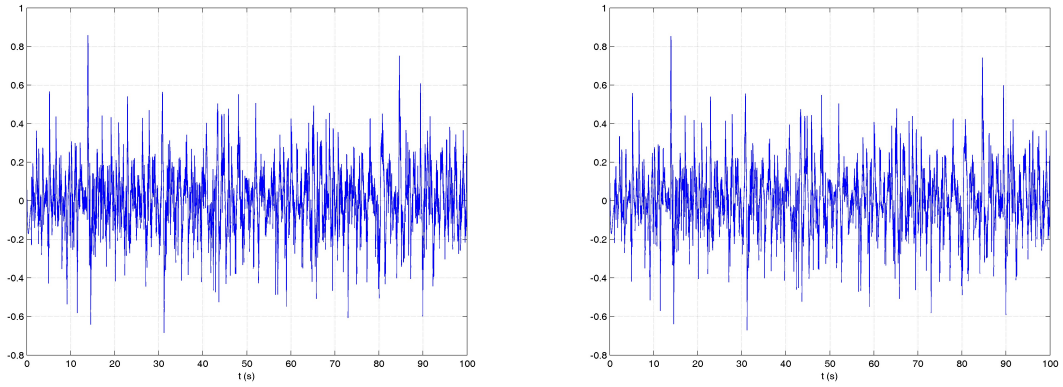


FIG. 3.3 - *Modulation de phase*

à chaque instant t, on recherche le décalage temporel entre $y_2(t)$ et $x_3(t)$.
Cette remarque impose des conditions sur la fonction θ, ainsi que sur le signal $x_3(t)$.
Tout d'abord, la fonction θ doit être bornée, par une constante positive T_u, très petite devant la constante de temps du système chaotique émetteur. En effet, si la fonction θ prend des valeurs trop importantes (supérieures à la constante de temps du signal x_3), on peut se retrouver dans la situation illustrée à la figure 3.5(a) : il est impossible de savoir si le point A sur la courbe de $y_2(t)$ correspond au point A_1, A_2 ou A_3 sur la courbe de $x_3(t)$. Il faut donc imposer $0 < \theta < T_u$, avec T_u très inférieure à la constante de temps de x_3. En pratique, cette hypothèse implique également que la constante T_u est inférieure ou égale au pas d'intégration de la simulation, pour les mêmes raisons de reconstruction du retard. Par ailleurs, il existe une conséquence visuelle de cette borne imposée sur la fonction retard : si le retard est très petit devant la constante de temps de $x_3(t)$, le signal $y_2(t)$ conserve un aspect chaotique. Cette propriété visuelle nous semble importante pour bénéficier des avantages des signaux chaotiques (notamment l'aspect aléatoire) dans le cryptosystème que nous avons mis au point, mais nous n'avons pas cherché à démontrer que le signal transmis $y_2(t)$ est chaotique. La figure 3.4 montre les trajectoires des signaux $x_3(t)$ et $y_2(t)$ correspondant à la simulation du paragraphe 3.3.1.
Ensuite, pour pouvoir restaurer le message $u(t)$, il faut que la fonction θ soit inversible. En effet,

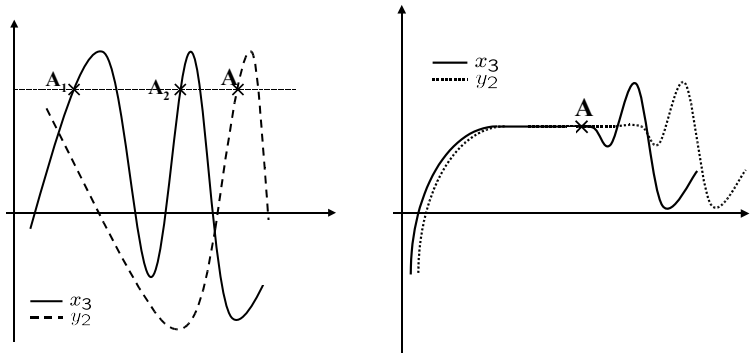


(a) Signal $x_3(t)$ (b) Signal $y_2(t)$

FIG. 3.4 - *Comparaison des signaux $x_3(t)$ et $y_2(t)$*

la fonction de décryptage va consister, au niveau du récepteur, à estimer à chaque instant le retard variable $\theta(u(t))$, puis à appliquer θ^{-1} pour retrouver la valeur $u(t)$.

Une dernière condition nécessaire pour pouvoir estimer le retard variable concerne le signal porteur. Ce signal ne doit pas être constant sur des intervalles (de longueur non nulle) de $\mathbb{R}$, sinon, on est dans l'impossibilité de trouver la valeur de $\theta(u(t))$ sur cet intervalle. Cette situation problématique est illustrée par le schéma de la figure 3.5(b). En effet, comme le retard est



(a) Retard trop important (b) Signal porteur constant

FIG. 3.5 - *Problèmes pour l'estimation du retard variable*

variable, il est impossible de retrouver le point de la courbe de $x_3(t)$ correspondant au point A sur la courbe de $y_2(t)$. Une façon simple de pallier ce problème consiste à choisir comme porteuse un signal qui varie vite, et qui n'est jamais constant sur un intervalle de longueur non nulle. Les signaux chaotiques sont donc bien adaptés à cette technique de transmission d'information.

3.2.2 Restauration de l'information : approche analytique

Comme la fonction : $t \mapsto x_3(t)$ est de classe $\mathcal{C}^\infty$, on peut appliquer la formule de Taylor-Lagrange avec reste intégral au rang n, et on obtient :

$$\begin{aligned} y_2(t) - x_3(t) &= y_2(t) - x_3(t - \theta(u(t))) \\ &= \sum_{k=1}^{n} \frac{(-\theta(u(t)))^k}{k!} x_3^{(k)}(t) - \int_{t-\theta(u(t))}^{t} \frac{(t - \theta(u(t)) - s)^n}{n!} x_3^{(n+1)}(s) ds \end{aligned} \tag{3.2}$$

Nous avons choisi comme fonction $\theta(u)$:

$$\theta\left(u(t)\right) = T_u u(t) \tag{3.3}$$

où T_u est une constante arbitraire.

A la lueur des remarques précédentes, on impose $0 < T_u \ll T_3$, où T_3 est la constante de temps du signal $x_3(t)$. Dans ce cas, la formule (3.2) se met sous la forme :

$$y_2(t) - x_3(t) = \sum_{k=1}^{n} \frac{(-T_u u(t))^k}{k!} x_3^{(k)}(t) - \int_{t-T_u u(t)}^{t} \frac{(t - T_u u(t) - s)^n}{n!} x_3^{(n+1)}(s) ds \tag{3.4}$$

Plus explicitement, cette formule exprimée à l'ordre un donne :

$$y_2(t) - x_3(t) = -T_u u(t) \dot{x}_3(t) - \frac{1}{2} \int_{t-T_u u(t)}^{t} (t - T_u u(t) - s)^2 \ddot{x}_3(s) ds \tag{3.5}$$

Le reste intégral peut être majoré de la manière suivante :

$$\left| \int_{t-T_u u(t)}^{t} (t - T_u u(t) - s)^2 \ddot{x}_3(s) ds \right| \leqslant \frac{1}{2} \left(T_u u(t)\right)^3 \left\| \ddot{x}_3 \right\|_\infty \tag{3.6}$$

Sachant que le *SCTH* est un système chaotique, son attracteur définit un domaine borné de $\mathbb{R}^3$. Par conséquent $x_3(t)$ est borné et ses dérivées également : en particulier $\left\| \ddot{x}_3 \right\|_\infty \leqslant c$. On obtient donc la nouvelle majoration du reste intégral (on rappelle que l'on a supposé $0 \leqslant u(t) \leqslant 1$) :

$$\left| \int_{t-T_u u(t)}^{t} (t - T_u u(t) - s)^2 \ddot{x}_3(s) ds \right| \leqslant \frac{c}{2} T_u^3 \tag{3.7}$$

La constante T_u étant arbitraire (et indépendante de la valeur de c, la seule condition à vérifier est $T_u \ll T_3$), on peut rendre le reste intégral aussi petit qu'on le souhaite. On peut donc écrire l'approximation suivante au premier ordre de la formule de Taylor-Lagrange :

$$y_2(t) - x_3(t) = -T_u u(t) \dot{x}_3(t) \tag{3.8}$$

On en déduit l'expression de $u(t)$ en fonction de $y_2(t)$ et $x_3(t)$:

$$u(t) = \frac{x_3(t) - y_2(t)}{T_u \dot{x}_3(t)} \tag{3.9}$$

Au niveau du récepteur, le signal $y_2(t)$ est disponible, ainsi qu'une estimation de $x_3(t)$ et $\dot{x}_3(t)$ (estimation provenant d'un des observateurs conçus au paragraphe 2), d'où la formule de restauration de l'entrée inconnue $u(t)$:

$$\hat{u}(t) = \frac{\hat{x}_3(t) - y_2(t)}{T_u \dot{\hat{x}}_3(t)} \tag{3.10}$$

Remarque 3.2.1. Les deux formules précédentes nécessitent de diviser par $\dot{x}_3(t)$ et $\dot{\hat{x}}_3(t)$ respectivement. Cela suppose que ces valeurs ne sont pas nulles (on exclut le cas de fonctions constantes). Dans le cas contraire, on fait une approximation à l'ordre deux. En effet, la dérivée première et la dérivée seconde ne peuvent pas s'annuler en même temps sur un intervalle de longueur non nulle, donc on obtient :

$$y_2(t) - x_3(t) = \frac{1}{2}(T_u u(t))^2 \ddot{x}_3(t) - \frac{1}{6}\int_{t-T_u u(t)}^{t} (t - T_u u(t) - s)^3 x_3^{(3)}(s) ds \tag{3.11}$$

On en déduit l'approximation au deuxième ordre :

$$y_2(t) - x_3(t) = \frac{1}{2}(T_u u(t))^2 \ddot{x}_3(t) \tag{3.12}$$

le reste intégral étant majoré par un terme de l'ordre de T_u^4. En exploitant l'hypothèse $u(t) \in [0, 1]$, on peut inverser la formule précédente et ainsi obtenir une expression de $u(t)$ en fonction de $y_2(t)$, $x_3(t)$ et $\ddot{x}_3(t)$. Si ponctuellement plusieurs dérivées successives sont nulles, on utilise la formule (3.4) à un ordre supérieur. ♦

En pratique, $x_3(t)$ étant chaotique, on peut toujours appliquer la formule (3.9) ou (3.10). En effet, un signal chaotique oscille très vite entre deux bornes (et ici le signal choisi x_3 oscille particulièrement vite grâce à la présence du retard), il n'est jamais constant sur un intervalle de longueur non nulle. La dérivée du signal est donc alternativement positive et négative, avec des changements de signe très fréquents. Cela signifie qu'elle s'annule en de nombreux points. Cependant, en pratique, les simulations sont numériques : le pas d'intégration numérique est fixé à chaque simulation, et la probabilité que la dérivée du signal soit exactement égale à zéro est quasi nulle, car il s'agit d'un signal qui varie vite.

3.3 Simulations

On rappelle le modèle dynamique de l'émetteur choisi, à savoir le *SCTH* :

$$\left\{\begin{array}{rcl} \dot{x}_1(t) &=& -\alpha x_1(t) + \alpha x_2(t) - \alpha\delta\tanh(x_1(t)) \\ \dot{x}_2(t) &=& x_1(t) - x_2(t) + x_3(t) \\ \dot{x}_3(t) &=& -\beta x_2(t) - \gamma x_3(t) + \varepsilon\sin(\sigma x_{1\tau}(t)) \end{array}\right. \tag{3.13}$$

Les valeurs numériques des paramètres sont données dans le tableau 3.1.

α	β	γ	δ	ε	σ	τ
9	14	5	$0,5$	100	10^4	1

TAB. 3.1 - *Paramètres du système* (3.13)

La synchronisation est établie en reprenant un des observateurs conçus au chapitre 2. Nous avons choisi l'observateur exponentiel d'ordre plein proposé au paragraphe 2.3.2, dont le modèle dynamique est décrit à l'équation (2.73), les valeurs numériques des gains étant données à la section 2.3.2.3. On rappelle que le signal transmis au récepteur pour établir la synchronisation avec l'émetteur (3.13) est défini par $y(t) = Cx(t)$ avec $C = (\ 1 \quad \zeta \quad 0\ )$, $\zeta = 10^{-5}$.

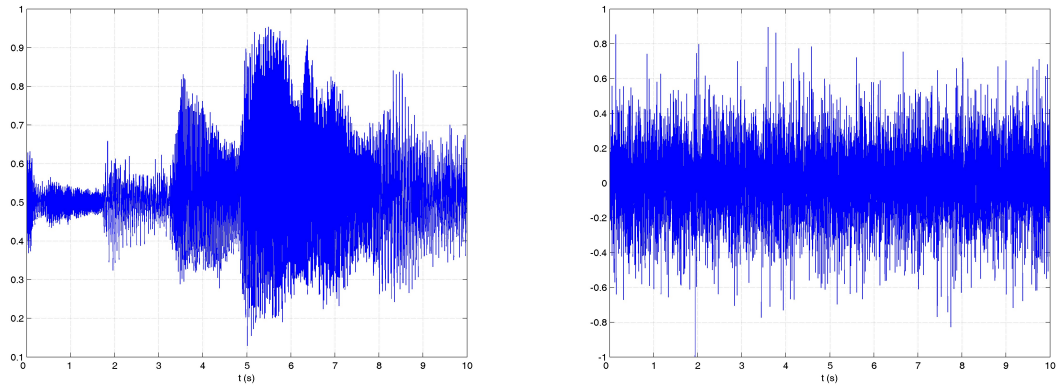
Remarque 3.3.1. On peut dès maintenant prévoir l'apparition d'un phénomène qui va perturber la restauration du message : si on considère l'expression de $\hat{u}(t)$ (3.10), il apparaît que l'estimation de l'entrée inconnue dépend de la qualité de la synchronisation (*i.e.* des signaux $\hat{x}_3(t)$ et $\dot{\hat{x}}_3(t)$). Puisque le récepteur ne connaît pas l'état initial de l'émetteur, il lui faut quelques instants pour converger de façon satisfaisante vers l'état courant de l'émetteur : ce temps de synchronisation dépend notamment du système considéré, et des valeurs des paramètres. Il peut être déterminé expérimentalement : par exemple, à la figure 2.11(b), il faut moins d'une seconde au récepteur pour se synchroniser avec l'émetteur. Par conséquent, si le message est transmis avant que le récepteur ait eu le temps de se synchroniser, les premiers points reconstruits seront erronés. On peut adopter deux points de vues pour trouver une solution à ce désagrément. La première solution consiste à ajouter un message vide avant le message contenant l'information à transmettre, de telle sorte que les points erronés ne dégradent pas la restauration de $u(t)$. Le second point de vue considère le cryptosystème proposé dans son ensemble. On peut en effet faire l'hypothèse suivante : l'émetteur envoie les signaux $y(t)$ et $y_2(t)$ en continu, et donc le récepteur est déjà synchronisé lorsque la transmission cryptée du message commence. On constate ici l'importance de la propriété de synchronisation continue (dans le sens où il n'y a pas de rupture de synchronisation). Par conséquent, dans toutes les simulations concernant la transmission sécurisée d'informations, les conditions initiales de l'émetteur seront fixées aléatoirement, puisque l'insertion du message dans le second signal transmis peut se faire à n'importe quel moment.

♦

On teste le système de transmission sécurisée décrit au paragraphe précédent sur trois types de messages, à savoir un son, une image, et un texte.

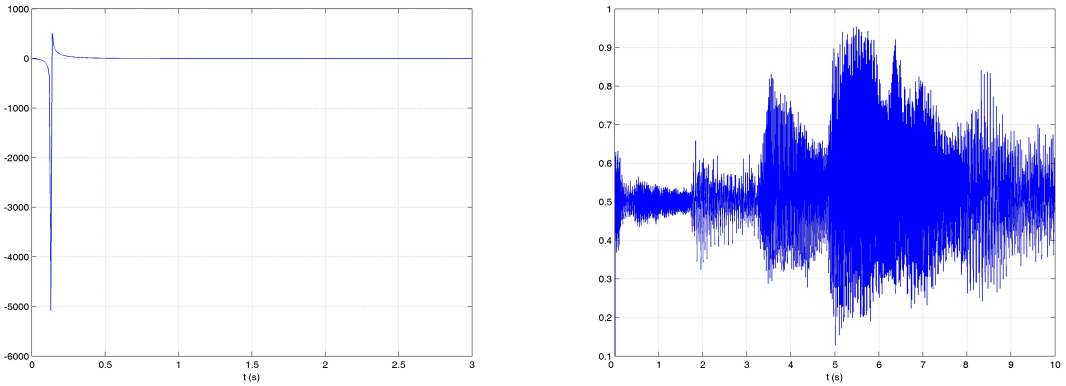
3.3.1 Transmission d'un son

Pour cette simulation, on a choisi un pas d'intégration de $0,01$ s pour la méthode de Runge-Kutta d'ordre quatre, et on a fixé $T_u = 0,01$ s dans la formule (3.3).
Le message original est représenté sur la figure 3.6(a), et le message crypté correspondant, c'est-à-dire $y_2(t)$, est tracé à la figure 3.6(b). On rappelle que par hypothèse $u(t) \in [0, 1]$, donc le signal sonore a été normalisé avant la mise en oeuvre de la transmission.



(a) Son original (b) Message crypté

FIG. 3.6 - *Messages sonores original et crypté*



(a) Différence $u(t) - \hat{u}(t)$ (b) Message décrypté

FIG. 3.7 - *Reconstruction du message sonore*

La figure 3.7 montre la différence entre le message original et le message décrypté (à gauche), ainsi que le message reconstruit $\hat{u}(t)$ (à droite). On constate bien une erreur sur la reconstruction

des premiers points du message, conformément à la remarque 3.3.1.

3.3.2 Transmission d'une image

On garde les mêmes paramètres de simulation qu'au paragraphe précédent. L'image originale, la célèbre photographie de Lena couramment utilisée en traitement d'image, est représentée à la figure 3.8. A partir d'une image en couleurs, définie par trois matrices codant chacune l'intensité d'une couleur de base (rouge, vert et bleu), on génère un signal à une dimension : les lignes de la première matrice sont concaténées pour former un seul vecteur. On poursuit le processus avec la deuxième matrice qui prolonge ce vecteur, et on termine de manière analogue avec la troisième matrice. Les coefficients de ce vecteur sont alors normalisés, pour obtenir le signal $u(t) \in [0, 1]$.

La figure 3.9(a) montre l'image cryptée correspondant au signal y_2 transmis au récepteur, et

FIG. 3.8 - *Photographie de Lena*

la figure 3.9(b) montre l'image reconstruite. On constate que les premiers points (en haut à gauche, par construction) de l'image reconstruite présentent des erreurs.

3.3.3 Transmission d'un texte

Les paramètres de simulation précédemment indiqués sont conservés. Le texte à transmettre est reproduit à la figure 3.10. A l'aide du code ASCII, on génère un vecteur dont les composantes sont des entiers compris entre 0 et 255. Ce vecteur est alors normalisé pour obtenir $u(t) \in [0, 1]$.

On applique le processus de cryptage, et le texte correspondant au signal y_2 transmis au récepteur est transcrit à la figure 3.11. La figure 3.12 montre le texte correspondant au signal décrypté : à partir du signal $\hat{u}(t)$, on applique le processus inverse toujours avec le code ASCII et on obtient le texte décrypté. Grâce à l'ajout d'un message vide, la reconstitution du texte est parfaite pour cette simulation.

(a) Image cryptée (b) Image décryptée

FIG. 3.9 - *Reconstruction de l'image*

```
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide

Baudelaire "Harmonie du soir", extrait des Fleurs du mal
Voici venir les temps où vibrant sur sa tige
Chaque fleur s'évapore ainsi qu'un encensoir;
Les sons et les parfums tournent dans l'air du soir;
Valse mélancolique et langoureux vertige!

Chaque fleur s'évapore ainsi qu'un encensoir;
Le violon frémit comme un coeur qu'on afflige;
Valse mélancolique et langoureux vertige!
Le ciel est triste et beau comme un grand reposoir.

Le violon frémit comme un coeur qu'on afflige,
Un coeur tendre, qui hait le néant vaste et noir!
Le ciel est triste et beau comme un grand reposoir;
Le soleil s'est noyé dans son sang qui se fige.

Un coeur tendre, qui hait le néant vaste et noir,
Du passé lumineux recueille tout vestige!
Le soleil s'est noyé dans son sang qui se fige...
Ton souvenir en moi luit comme un ostensoir!

fin de message
```

FIG. 3.10 - *Texte original*

Remarque 3.3.2. Dans le cadre de ce mémoire, la méthode développée au paragraphe 3.2 a été appliquée uniquement dans un contexte de communications reposant sur les systèmes chaotiques. On peut cependant considérer la méthode proposée sous un autre angle. En effet, il s'agit, dans des conditions bien particulières, d'estimer un retard de transmission. Par exemple,

FIG. 3.11 - *Texte correspondant au signal transmis*

on pourrait envisager d'appliquer les résultats du paragraphe 3.2 dans le cas d'un système classique d'acquisition de mesures, soumis à des retards variables, bornés et inconnus. Il faut pour cela reconstruire l'état (non retardé) du système, ensuite la formule (3.10) permet d'estimer $u(t)$, considéré ici comme un retard variable. Ainsi la méthode que nous avons conçue est-elle très générale, et peut donner lieu à des applications dans le domaine du diagnostic notamment.

3.4 Quelques points de sécurité

Le système de communication proposé aux paragraphes précédents comporte deux étapes distinctes, à savoir une étape de synchronisation et une étape de transmission de l'information par modulation de phase. Il semble donc logique d'examiner la question de la sécurité au niveau de chaque étape. La sécurité du processus de synchronisation a été abordée succinctement lors du choix de l'émetteur chaotique, au chapitre 2. La synchronisation peut être en butte principalement à des attaques exploitant les informations contenues dans le signal transmis au récepteur : par des méthodes de reconstruction à base de retards, il est possible de reconstituer la géométrie de l'attracteur chaotique correspondant à l'émetteur. Une parade à ce type d'intrusion consiste à choisir comme émetteur un système hyperchaotique, ou un système comportant un retard, cette dernière solution étant celle que nous avons retenue et qui a abouti au choix du *SCTH*. Nos

```
ÿÿÿÿÿÿÿÿÿÿÿÿÿ□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□$
‡□qE□□C□E□□Ê□□□□:É□□hÿ□°□□□□□2□w·□□□□ÿ□□*D>e□□□□□□□
ÿ□□rg;□□□□□¿□□□□□□□□□□□□□ÿR□□Ÿ□ü□e□□□□ÏÿÿNÀyc:□‘R□J
j □□•]□p]•□□™ÿ□g□n’:m^gi!xmoj kf˜t^Åh□webi ycsza`e□
xhOf jgts`ÿf vidd qfssa De vjde message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide message vide message vide
message vide message vide

Baudelaire "Harmonie du soir", extrait des Fleurs du mal
Voici venir les temps où vibrant sur sa tige
Chaque fleur s'évapore ainsi qu'un encensoir;
Les sons et les parfums tournent dans l'air du soir;
Valse mélancolique et langoureux vertige!

Chaque fleur s'évapore ainsi qu'un encensoir;
Le violon frémit comme un coeur qu'on afflige;
Valse mélancolique et langoureux vertige!
Le ciel est triste et beau comme un grand reposoir.

Le violon frémit comme un coeur qu'on afflige,
Un coeur tendre, qui hait le néant vaste et noir!
Le ciel est triste et beau comme un grand reposoir;
Le soleil s'est noyé dans son sang qui se fige.

Un coeur tendre, qui hait le néant vaste et noir,
Du passé lumineux recueille tout vestige!
Le soleil s'est noyé dans son sang qui se fige...
Ton souvenir en moi luit comme un ostensoir!

fin de message
```

FIG. 3.12 - *Texte décrypté*

réflexions sur la sécurité de la synchronisation sont à l'origine du chapitre 4, dédié aux multi-modèles chaotiques. La suite du chapitre 3 est consacrée à une étude de la sécurité du processus de cryptage que nous avons élaboré.

3.4.1 Cryptanalyse classique

Les techniques de cryptanalyse classique sont bien codifiées. Elles se répartissent selon quatre types d'attaques, définis comme suit, en fonction des données nécessaires.

- *L'attaque par force brute* (Brute-force attack). Le cryptanalyste essaie toutes les combinaisons de clés possibles jusqu'à l'obtention du texte clair.
- *L'attaque sur texte chiffré seul.* (Ciphertext-only attack) Le cryptographe dispose uniquement du message chiffré par l'algorithme et fait des hypothèses sur le texte clair (des expressions, des mots, le sens du message). Le manque d'information rend la cryptanalyse plus ardue.
- *L'attaque à texte clair connu* (Known-plaintext attack). Le cryptanalyste possède des messages ou parties de messages en clair et leur version chiffrée.
- *L'attaque à texte clair choisi* (Chosen-plaintext attack). Le cryptanalyste possède des messages en clair, il peut générer les versions chiffrées de ces messages (il a accès à la machine à crypter) avec l'algorithme que l'on peut dès lors considérer comme une boîte noire. Les techniques de

cryptage asymétrique sont notamment sensibles à ce type d'attaque.
– *L'attaque à texte chiffré choisi* (Chosen-ciphertext attack). Le cryptanalyste possède des messages chiffrés et demande la version en clair de certains de ces messages pour mener l'attaque.

Sur la base de ces techniques de cryptanalyse classique, l'article [Alvarez 06a] propose quelques éléments indispensables à analyser lorsqu'un nouveau schéma de communications à base de systèmes chaotiques est conçu. Nous allons essayer de mesurer le niveau de sécurité du processus de transmission de données proposé. Cette analyse se décompose en trois points : la définition de la clé (élément sur lequel repose toute la sécurité du cryptosystème) et l'analyse de sa sensibilité ; l'analyse des propriétés de confusion et diffusion qui permettent de quantifier la sécurité de la clé ; et enfin la cryptanalyse spécifique au chaos, par des attaques spectrales.

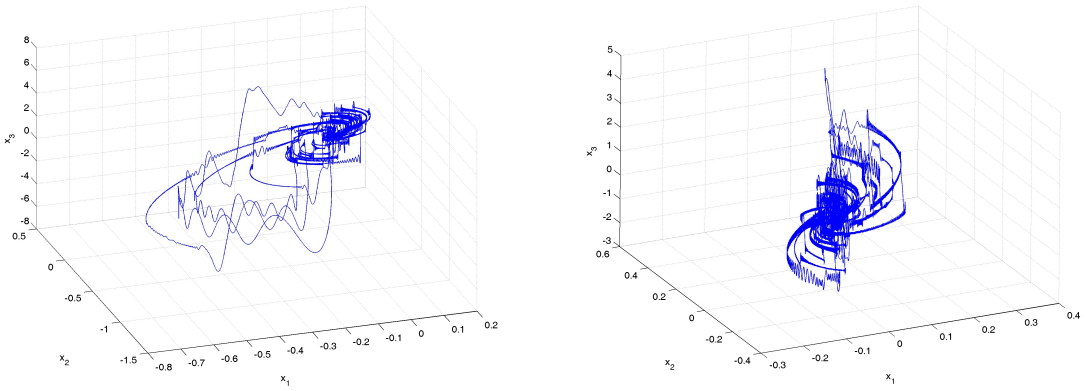
3.4.2 La clé : principe de Kerckhoff

3.4.2.1 Définition de la clé

Il nous faut tout d'abord énoncer le principe de Kerckhoff (cryptologue néerlandais du XIX^{ème} siècle) qui est fondamental en cryptanalyse : la sécurité doit être mesurée en considérant que, hormis la clé, le cryptanalyste connaît dans le détail le système cryptographique (il pourrait en être le concepteur). En effet, la clé constitue, comme son nom l'indique, le sésame permettant d'aboutir à la solution : toute la sécurité doit reposer sur la clé, et pas sur le système d'encryptage lui-même. Si la plupart des travaux sur les cryptosystèmes chaotiques n'exhibent pas explicitement de clé, c'est que les paramètres mêmes du système chaotique émetteur ont longtemps été considérés comme les clés. En effet, les systèmes chaotiques sont caractérisés par une grande sensibilité dans leurs paramètres. Il est donc possible de supposer qu'un cryptanalyste, qui ne connaît rien au sujet du système chaotique émetteur utilisé ne peut pas décrypter le signal intercepté. Cependant, si on reprend le principe de Kerckhoff, c'est-à-dire, si on fait l'hypothèse que le cryptanalyste connaît la structure de l'émetteur, par des techniques avancées de reconstruction à retard, il peut reconstituer l'attracteur chaotique, et identifier partiellement les paramètres du système. Il convient donc de ne pas se contenter de la sécurité apparente fournie par cette sensibilité dans les paramètres du système chaotique émetteur.

Pour être considéré comme crédible, un cryptosystème, selon [Alvarez 06a], doit exhiber une clé secrète, dont la connaissance est indispensable pour pouvoir déchiffrer le signal transmis par l'émetteur. Nous allons donc nous attacher à montrer que la méthode de masquage chaotique que nous avons élaborée possède une clé, et indiquer des valeurs possibles pour cette clé. Si on se reporte aux différents attracteurs chaotiques représentés aux pages 50 et 51, on se rend compte que la valeur de σ influence le comportement du *SCTH*. Si on regarde attentivement l'expression de la troisième composante de la fonction non linéaire H (2.15), à savoir $\varepsilon \sin(\sigma x_1(t-\tau))$, on remarque que le paramètre σ définit la vitesse à laquelle le signal retardé $x_{1\tau}$ intervient dans la fonction sinus. Comme x_1 est un signal chaotique, il varie très vite, et un petit changement de valeur de σ transforme profondément $\varepsilon \sin(\sigma x_1(t-\tau))$. La figure 3.13 propose deux attrac-

teurs correspondant à deux valeurs de σ, les autres paramètres ayant les valeurs fixées dans le tableau page 100. On constate que les deux attracteurs sont différents, alors que les conditions initiales sont les mêmes, et que le paramètre σ varie seulement de $0,01\%$. Ces considérations



(a) $\sigma = 10000$ (b) $\sigma = 10001$

FIG. 3.13 - *Attracteurs correspondant à deux valeurs proches de* σ

nous laissent à penser que le paramètre σ peut endosser le rôle de la clé dans la méthode de transmission par modulation de phase chaotique que nous proposons.

3.4.2.2 Sensibilité de la clé

Pour caractériser la clé du cryptosystème proposé, il faudrait préciser l'ensemble des valeurs qu'elle peut prendre. En suivant les indications de l'article [Alvarez 06a], cela revient à déterminer les valeurs pour lesquelles la clé est une clé "forte", c'est-à-dire très longue à trouver par une attaque à force brute, tout en garantissant que, pour ces valeurs, l'émetteur exhibe un comportement chaotique. On ne cherchera pas ici à définir explicitement l'espace des clés. Notre but n'est pas, en effet, de faire une cryptanalyse approfondie du cryptosystème mis au point, nous étudions simplement quelques points de sécurité qui nous semblent le minimum à vérifier lorsqu'on propose un nouveau système de communications chaotiques sécurisées. La recherche de cet ensemble de clés fortes est liée à l'étude du chaos généré par le *SCTH*, puisqu'il s'agit de trouver toutes les valeurs de σ et des autres paramètres qui garantissent à la fois un comportement chaotique, et une extrême sensibilité dans la clé. Nous avons choisi au chapitre 2 de ne pas nous engager dans une étude rigoureuse du chaos, par conséquent nous n'allons pas détailler plus avant l'espace des clés.

Nous proposons toutefois de quantifier la sensibilité de la clé à de petits changements, au niveau de la restauration du message. On se place toujours dans l'hypothèse de Kerckhoff, en supposant que l'intrus connaît toute la structure du dispositif de cryptage proposé, ainsi que la valeur de tous les paramètres, sauf la clé.

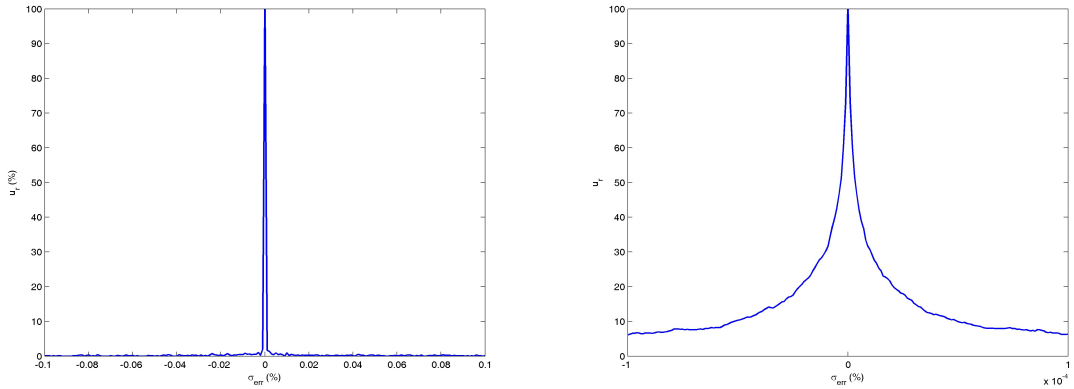
Un premier test consiste à choisir une clé pour l'émetteur ($\sigma = 10000$), et à fixer une clé très

légèrement différente au niveau du récepteur : $\tilde{\sigma} = 10000,01$. La figure 3.14 montre le texte déchiffré dans ces conditions (le texte clair est celui de la page 103). On constate que la restauration du message n'est pas possible dans ces conditions.

FIG. 3.14 - *Texte décrypté avec une erreur de* $10^{-4}\%$ *sur la clé*

Le résultat précédent nous incite à quantifier plus précisément la sensibilité du déchiffrement dans la clé σ. Dans ce but, on propose de tracer le taux de reconstruction en fonction du taux d'erreur sur σ au niveau du récepteur. La valeur de la clé fixée pour le récepteur est notée $\tilde{\sigma}$ pour éviter toute confusion. On choisit $\sigma = 10000$ au niveau de l'émetteur. On va faire varier $\tilde{\sigma}$ de manière symétrique autour de cette valeur, et mesurer sur le signal décrypté le taux d'erreur de reconstruction. Pour cela, on fait varier $\tilde{\sigma}$ dans l'intervalle $[9990; 10010]$, par pas de $0,1$, ce qui correspond à 201 simulations. L'erreur σ_{err} (exprimée en $\%$) sur $\tilde{\sigma}$ varie donc de zéro (pour $\tilde{\sigma} = \sigma$) à $0,1\%$ (pour $\tilde{\sigma} = 9990$ ou $\tilde{\sigma} = 10010$), soit $\sigma_{err} \in [-0,1; 0,1]$. Pour mesurer le taux de reconstruction de u, on calcule la quantité u_r égale au nombre de points de l'intervalle de simulation qui vérifient $\hat{u}(t) \in [u(t) - \lambda_u, u(t) + \lambda_u]$, où le paramètre λ_u quantifie la tolérance au niveau de l'erreur de reconstruction . La valeur de λ_u doit être déterminée en fonction du type de message. Ici, puisqu'il s'agit d'un texte, dont chaque caractère correspond à un entier compris entre 0 et 255, on prend $\lambda_u = \frac{1}{256}$. Pour obtenir un nombre significatif, ce nombre de points corrects est divisé par le nombre total de points du message, et exprimé en pourcentage. Pour éviter que les points reconstruits hors synchronisation ne détériorent le véritable taux de reconstruction, on élimine les 500 premiers points de nos calculs. Le taux de reconstruction u_r est tracé en fonction de σ_{err}, et la figure 3.15(a) montre la courbe obtenue. On constate qu'il

y a reconstruction parfaite (cela se traduit par $u_r = 100\%$) uniquement pour le cas $\sigma_{err} = 0$, c'est-à-dire $\tilde{\sigma} = \sigma$. Dans tous les autres cas, dès que $\tilde{\sigma}$ est différent de σ, le taux de reconstruction est proche de zéro.
On affine les résultats de cette simulation, en fixant la borne supérieure de l'erreur sur la clé au taux de $10^{-4}\%$, et le pas à 10^{-4}. La courbe de la figure 3.15(b) illustre cette seconde simulation. Ce taux d'erreur de $10^{-4}\%$ sur la clé est à mettre en relation avec la figure 3.13 : puisque les attracteurs générés par deux *SCTH* dont les paramètres σ diffèrent de $10^{-4}\%$ sont différents, il paraît logique qu'une erreur de $10^{-4}\%$ sur la clé au niveau du récepteur perturbe fortement la restauration du message. Ces simulations traduisent parfaitement la sensibilité de la clé σ à de petits changements, au niveau de la restauration d'entrées inconnues.



(a) Erreur maximale de $0,1\%$ sur la clé (b) Erreur maximale de $10^{-4}\%$ sur la clé

FIG. 3.15 - *Taux de reconstruction en fonction du taux d'erreur sur la clé*

Remarque 3.4.1. Même si nous n'avons pas exhibé précisément l'espace des clés, on constate que la sensibilité augmente avec la valeur de σ : si cette valeur est multipliée par dix, alors un taux d'erreur dix fois plus petit (ce qui correspond à $\tilde{\sigma} \in [-0,01; 0,01]\%$) conduit au résultat de la figure 3.15(a), etc... Par conséquent, pour garantir un niveau de sécurité important, il faut choisir des valeurs élevées pour σ. ♦

On peut noter que la méthode proposée respecte l'une des règles énoncées dans l'article [Kelber 05], selon laquelle les nonlinéarités de l'émetteur chaotique doivent varier en fonction de la clé et/ou du message à transmettre. Dans notre cas, puisque la clé est le paramètre σ, elle influence directement la fonction non linéaire H (2.15).

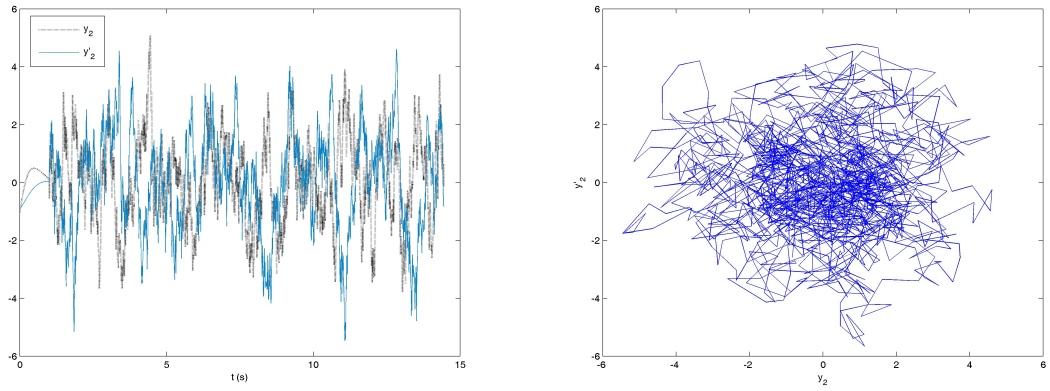
3.4.3 Analyse de la sécurité : confusion et diffusion

Les propriétés fondamentales de confusion et diffusion, que doit posséder tout cryptosystème fiable, ont été identifiées par Shannon en 1949 dans l'article [Shannon 49]. Le but de la confusion est de cacher toute relation existante entre le message clair, le message crypté et la clé. Le

but de la diffusion est de répartir les effets conjugués du message clair et de la clé sur la plus grande longueur possible de message crypté. Ces deux principes rendent la cryptanalyse très difficile. Plus précisément, un système de communications qui possède une bonne confusion et une bonne diffusion résiste aux attaques détaillées au paragraphe 3.4.1.

Propriété de diffusion

Cette propriété s'apparente à la propriété d'avalanche qui s'énonce comme suit : deux clés aussi proches que l'on veut dans l'espace des clés, ou deux messages clairs très peu différents produisent des signaux cryptés totalement différents.
Nous allons réaliser la simulation suivante : on transmet deux fois le même message, le cryptage étant réalisé grâce à deux clés très peu différentes.La première clé $\sigma = 10000$ correspond au signal crypté $y_2(t)$, et la seconde clé $\sigma = 10000,01$ au signal $y_2'(t)$. La figure 3.16(a) représente les deux signaux cryptés $y_2(t)$ et $y_2'(t)$. On trace ensuite le premier signal transmis en fonction du second. La figure 3.16(b) montre la courbe ainsi générée (en supprimant les 500 premiers points pour éviter le phénomène transitoire d'établissement de la synchronisation). Les signaux cryptés



(a) Signaux cryptés correspondant à des clés différant de $10^{-4}\%$

(b) $y_2'(t)$ en fonction de $y_2(t)$

FIG. 3.16 - *Test de diffusion*

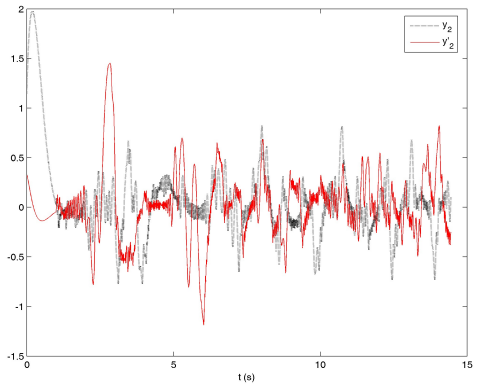
(correspondant au même message clair) générés avec deux clés très peu différentes (l'écart est de $10^{-4}\%$) sont totalement différents Le point essentiel qui donne naissance à cette propriété ici réside dans la sensibilité de la clé, comme cela a été étudié au paragraphe 3.4.2.2. En effet, on peut faire la simulation précédente en imposant des conditions initiales identiques pour l'envoi du message : on obtient des figures analogues aux figures 3.16(a) et 3.16(b). En conclusion, la propriété de diffusion que possède la méthode de cryptage proposée dans ce mémoire repose principalement sur la structure particulière du modèle dynamique de l'émetteur, à savoir le *SCTH*, qui garantit une grande sensibilité de la clé σ.

Remarque 3.4.2. La propriété de diffusion se vérifie également avec deux messages très peu

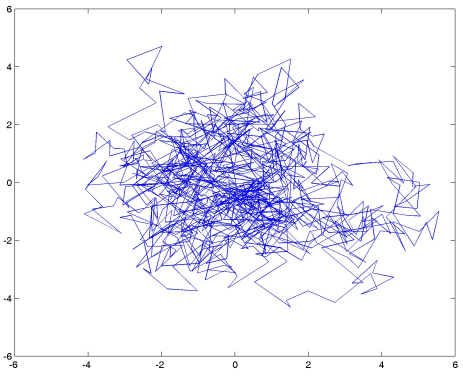
différents. Dans ce cas, la diffusion repose sur la sensibilité aux conditions initiales. Plus précisément, si on garde les mêmes conditions initiales et deux messages très proche, les signaux cryptés sont très proches. Cette remarque découle immédiatement du principe de cryptage par modulation de phase, et du caractère déterministe des systèmes chaotiques. ♦

Propriété de confusion

Afin de montrer que le cryptosystème que nous proposons possède la propriété de confusion, nous réalisons une simulation analogue à la précédente : le même message est transmis deux fois au récepteur, mais cette fois sans changer la clé entre les deux envois. La figure 3.17 donne une preuve que les deux signaux cryptés avec la même clé, correspondant au même message clair, sont totalement différents. Ce résultat est dû au processus de synchronisation, qui est réalisé en continu : à chaque envoi de message, l'état de l'émetteur (qui correspond à l'état initial pour la transmission d'information en cours) change. Cela signifie que la méthode de transmission d'information que nous avons élaborée exploite au mieux les propriétés des systèmes chaotique et de leur synchronisation : on exploite ici l'extrême sensibilité aux conditions initiales, et la capacité du récepteur à se synchroniser sans connaître l'état initial de l'émetteur. Il faut souligner que le processus de cryptage seul (à savoir la modulation de phase chaotique) ne peut pas posséder la propriété de confusion si l'état initial de l'émetteur ne change pas à chaque envoi de message : puisque l'émetteur est un système déterministe, le même état initial génère la même trajectoire. Par conséquent, si on envoie un message deux fois, avec le même état initial au niveau de l'émetteur, le signal modulé sera le même. Il est donc fondamental que la synchronisation s'établisse de façon continue, pour que l'état de l'émetteur change (de manière chaotique) à chaque nouvelle transmission d'information. On peut en conclure que le processus de cryptage à base de synchronisation chaotique que nous proposons possède effectivement la propriété de confusion.



(a) Signaux cryptés correspondant au même message clair



(b) $y'_2(t)$ en fonction de $y_2(t)$

FIG. 3.17 - *Test de confusion*

Pour approfondir le résultat précédent, on peut remarquer que, pour un message clair donné, il n'y a pas unicité du message crypté transmis au récepteur. En effet, si on envisage plusieurs envois d'un même message $u(t)$, dès lors que les instants où le message est masqué par la porteuse chaotique et envoyé sont différents, alors les deux signaux cryptés correspondants sont différents. Cette propriété provient de la SCI exhibée par les systèmes chaotiques. En revanche, du côté du récepteur autorisé, quel que soit le message crypté correspondant à $u(t)$, la restauration produira le même résultat $\hat{u}(t)$. C'est la traduction de la formule de décryptage (3.10), qui s'appuie sur la synchronisation. La force du procédé de transmission d'information par synchronisation et modulation de phase chaotique que nous proposons apparaît là : pour un message clair donné, il existe potentiellement une infinité de messages cryptés, qui correspondent tous au même message décrypté. Cette propriété remarquable repose principalement sur deux notions fondamentales exploitées dans nos travaux, à savoir la sensibilité aux conditions initiales, exhibée par les systèmes chaotiques, et la synchronisation à base d'observateurs, qui rend possible la modulation puis la restauration du message clair.

3.4.4 Cryptanalyse spécifique au chaos : attaque spectrale

La référence [Alvarez 06a] mentionne, parallèlement à la cryptanalyse classique, à la définition de la clé, et à la vérification des propriétés de confusion et diffusion, des attaques dirigées exclusivement contre les cryptosystèmes chaotiques. Ces attaques sont de trois sortes : l'extraction du signal porteur, l'estimation de la clé, et enfin l'extraction du message. Une parade contre la première attaque est détaillée dans le chapitre suivant. L'étude de la clé menée au paragraphe 3.4.2.2 a révélé une très grande sensibilité à de faibles erreurs (de l'ordre de 10^{-4}), qui sont en opposition avec le deuxième type d'attaque. Il nous reste à traiter les attaques visant à l'extraction du message, par des techniques d'analyse spectrale.
Certains cryptosystèmes chaotiques ne résistent pas aux attaques spectrales : dès l'instant où le message est ajouté au niveau de la sortie $y(t)$ transmise au récepteur, il peut être retrouvé dans le spectre de puissance du signal $y(t)$. Ce problème majeur des transmissions cryptées exploitant le chaos n'est pas apparu tout de suite, lors de la mise au point des premières techniques : il était couramment admis que le spectre des signaux chaotiques était infiniment large et continu. Or, ce n'est bien entendu pas le cas. Cette faille a été facilement exploitée dans l'article [Alvarez 05], pour la cryptanalyse de la technique de masquage additif. Ce défaut se retrouve également dans l'exemple proposé dans l'article [Jiang 02], à l'origine de la transmission à deux voies : la technique utilisée pour cacher le message dans le second signal transmis ne permet pas de cacher le spectre du message dans celui du signal chaotique (sauf si le spectre du message est composé uniquement de basses fréquences, là où le spectre du signal chaotique est le plus élevé).
Pour pouvoir établir une comparaison avec le procédé de transmission par modulation de phase chaotique que nous avons élaboré, les deux techniques précédentes ont été testées en choisissant comme émetteur le *SCTH*, et comme signal à transmettre $u(t) = 0,05\sin(100\pi t)$. La figure 3.18 montre le spectre du signal porteur $x_3(t)$, l'axe des abscisses étant gradué en Hertz. La courbe

de la figure 3.19(a) représente le spectre du signal $x_3(t) + u(t)$, correspondant à la technique de cryptage par addition, et la courbe de la figure 3.19(b) représente le spectre celui du signal $x_3^2(t) + (1 + x_3^2(t))u(t)$, comme suggéré dans [Jiang 02] pour un schéma de transmission à deux voies. Ces deux densités spectrales de puissance présentent un pic (correspondant à la fréquence de $u(t)$) à l'abscisse 50 Hz.

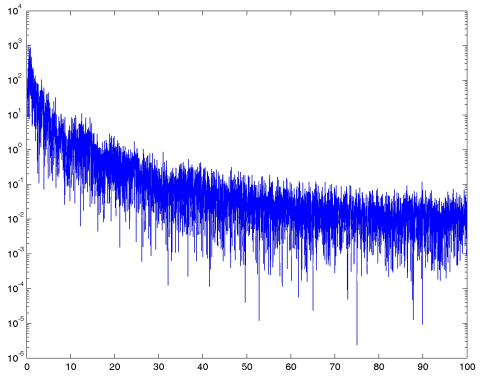


FIG. 3.18 - *Signal chaotique* $x_3(t)$

La simulation suivante tend à prouver que le système de transmissions sécurisées que nous proposons résiste à ce type d'attaque spectrale. Le signal à transmettre est toujours $u(t) = 0,05\sin(100\pi t)$. La figure 3.19(c) montre le spectre de $y_2(t) = x_3(t - T_u u(t))$. On constate que le spectre du message n'apparaît pas ici sous forme d'un pic reconnaissable, contrairement aux autres méthodes testées.

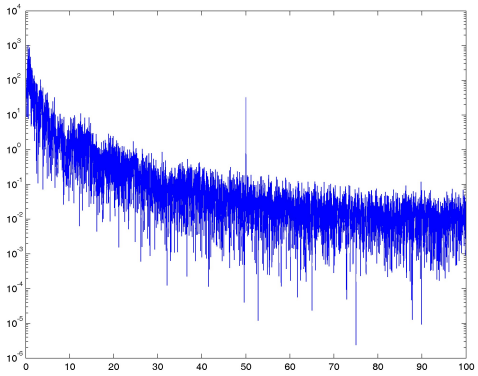
3.5 Robustesse au bruit de transmission

La dernière partie de ce chapitre aborde la question de la robustesse au bruit, qui se pose pour tout système de communication analogique : l'émetteur est relié au récepteur par un canal, élément physique qui permet de transmettre les informations. Selon la nature du canal, les signaux sont de nature différente :

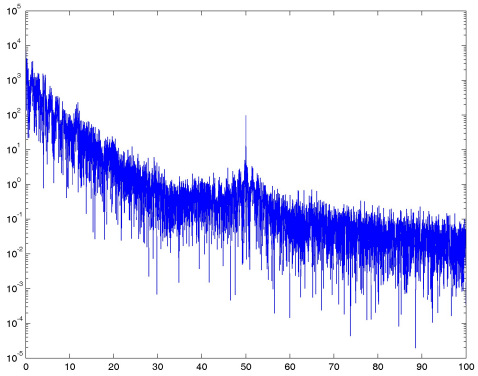
– atmosphère : ondes électromagnétiques ou ondes Hertziennes ;
– câble coaxial : signaux électriques (tensions, courants) ;
– fibre optique : ondes électromagnétiques optiques (lumière visible, infra-rouge).

Quelque soit le canal utilisé, il perturbe le signal en lui ajoutant du bruit et ce bruit peut rendre le message plus ou moins compréhensible par le récepteur.

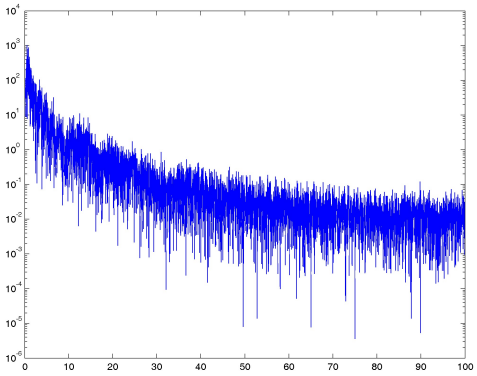
Dans ce paragraphe, nous étudions l'impact, sur la qualité de restauration du message, du bruit affectant le signal dévolu à la synchronisation. Cette hypothèse sur la présence de bruit sur le signal $y(t)$ permet d'appliquer les résultats théoriques de la section 2.5 : dans les simulations



(a) Cryptage par addition



(b) Transmission à deux voies : méthode de l'article [Jiang 02]



(c) Transmission à deux voies : cryptage par modulation de phase

FIG. 3.19 - *Résultats des attaques spectrales*

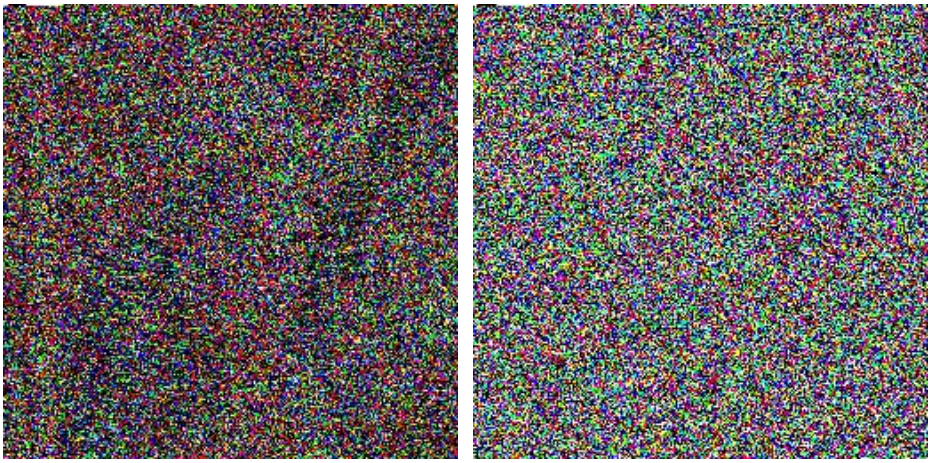
qui suivent, le récepteur choisi est l'observateur robuste dont le modèle dynamique est donné à l'équation (2.185).

3.5.1 Compromis robustesse-sécurité

On conserve les paramètres du *SCTH* donnés dans le tableau de la page 100. On considère la transmission de l'image de Lena (l'image originale est représentée à la figure 3.8). On considère un bruit additif $b(t)$ gaussien, normal centré perturbant le signal $y(t)$. 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* (ou SNR, Signal to Noise Ratio), exprimé en décibels :

$$SNR(y,b) = 20\log_{10}\frac{\|y(t)\|}{\|b(t)\|} \tag{3.14}$$

Plus ce rapport est grand, moins le bruit perturbe le signal original. Dans cette première simulation, le rapport $SNR(y, b)$ vaut 60 dB. La figure 3.20 montre l'image reconstituée en présence de bruit sur $y(t)$, avec un rapport signal sur bruit de 75 dB à gauche, de 60 dB à droite.



(a) SNR=75 dB (b) SNR=60 dB

FIG. 3.20 - *Images décryptées en présence de bruits de transmission, pour différents SNR, avec* $\sigma = 10^4$

Les conditions de simulation, et notamment la valeur de la clé σ ne permettent pas de restaurer l'image originale de façon satisfaisante. Nous allons faire d'autres tests, en changeant uniquement la valeur de la clé : on choisit $\sigma = 10$. La figure 3.21 montre l'image reconstruite pour différents SNR. Ces simulations illustrent parfaitement le compromis entre la robustesse et la

(a) SNR=75 dB (b) SNR=60 dB (c) SNR=40 dB

FIG. 3.21 - *Images décryptées en présence de bruits de transmission, pour différents SNR, avec* $\sigma = 10$

sécurité qui se pose dans tout cryptosystème analogique. Soit on privilégie un niveau de sécurité important, et d'après les résultats du paragraphe 3.4, cela correspond à de grandes valeurs de la clé σ. Soit la valeur de σ est diminuée (et la sécurité également) pour obtenir une meilleure estimation du message, en présence de bruit de transmission.
Nous n'avons pas traité le cas d'un signal $y_2(t)$ bruité. Au niveau du récepteur, ce signal est utilisé pour reconstituer le message clair, grâce à la formule (3.10). On constate que la sensibilité à des perturbations intervient à deux niveaux dans la formule de décryptage. La présence d'un bruit

additif sur le canal de transmission de $y_2(t)$ intervient directement, en facteur du terme $\frac{1}{T_u \dot{\hat{x}}_3(t)}$ (qui peut être très grand). La présence du bruit sur $y(t)$, comme nous venons de le voir apporte des erreurs dans l'estimation des signaux $x_3(t)$ et $\dot{x}_3(t)$. On sait gérer ces erreurs en choisissant un observateur robuste, mais on ne peut pas totalement les éliminer. La figure 3.22 représente l'image décryptée, lorsqu'on considère la présence de bruit sur les deux signaux transmis, avec le même rapport signal sur bruit de 75 dB : avec un faible niveau de bruit, la restauration reste donc correcte.

FIG. 3.22 - *Image décryptée en présence de bruit sur $y(t)$ et $y_2(t)$*

3.6 Conclusion

A travers ce troisième chapitre, nous avons présenté une application importante de la synchronisation à base d'observateurs sous la forme d'un système de communications sécurisées. La problématique est celle de la restauration d'entrées inconnues, avec des contraintes de sécurité supplémentaires.

Après avoir retracé l'évolution historique de la cryptographie à travers différentes méthodes utilisées depuis le XVI^{ème} siècle avant J.-C., nous avons détaillé les techniques commerciales de cryptage actuellement mises en œuvre, qui reposent sur deux principes fondamentalement éloignés : le cryptage asymétrique, à clé publique, et le cryptage symétrique. Pour mieux cerner notre problématique, nous nous sommes replacés dans un contexte de cryptage exploitant la synchronisation et les caractéristiques fondamentales du chaos. Après un examen des divers systèmes de communications chaotiques présents dans la littérature, nous avons retenu le principe de la transmission à deux voies. Cette technique permet notamment d'exploiter les schémas de synchronisation à base d'observateurs non linéaires du chapitre précédent. Nous avons ainsi pu proposer une nouvelle façon de noyer l'information à transmettre dans un second signal chaotique. La méthode que nous proposons consiste à réaliser une modulation de la phase de ce second signal chaotique en fonction du message. Puisqu'on suppose que la fonction de modu-

lation est de faible amplitude, le signal transmis reste d'apparence chaotique et ne laisse pas transparaître le message, ce qui constitue une condition impérative pour nous. A la suite de la description du procédé de cryptage, son efficacité a été testée sur différents types de messages, à savoir un signal sonore, une image, et un texte. Dans les trois cas, la restauration de l'entrée inconnue se révèle excellente, sous l'hypothèse de conditions parfaites (ni bruit, ni retard dans la transmission).

Pour compléter la présentation de cette nouvelle technique de cryptage, nous nous devions d'aborder la question de la sécurité de la transmission d'informations. Il n'était pas dans notre objectif de tester les attaques de la cryptographie classique, c'est pourquoi nous avons testé quelques points adaptés aux systèmes chaotiques. Le premier concerne la définition de la clé secrète, conformément au principe de Kerckhoff, et la quantification de sa sensibilité à de petites erreurs, au niveau de la restauration de message. Les résultats obtenus montrent un taux de reconstruction de l'information faible dès que le récepteur commet une légère erreur sur la valeur de la clé. Dans un deuxième temps, nous avons vérifié que le cryptosystème proposé possède les propriétés de confusion et de diffusion. On peut souligner que le système de cryptage mis au point exploite au mieux les propriétés des systèmes chaotiques et de la synchronisation : si on considère un message clair à transmettre, il existe une infinité de messages cryptés correspondant à ce message, mais il n'existe qu'un seul message pouvant être restauré par le récepteur. Le dernier point de sécurité que nous avons abordé consiste à analyser le spectre des signaux cryptés, dans le cas où le message clair est un signal périodique. Il s'avère que la technique de transmission d'informations que nous avons élaborée résiste à ce type d'attaques, contrairement à certains systèmes de communications existants.

A la fin de ce chapitre, nous avons envisagé le cas où le cryptosystème proposé est perturbé par la présence de bruit de transmission. L'observateur robuste détaillé au chapitre 2, choisi comme récepteur, permet d'atténuer l'influence d'un bruit additif sur le signal $y(t)$ sur l'erreur de synchronisation. Les simulations, pour différents niveaux de bruit, montrent la nécessité d'un compromis entre la sécurité et la robustesse. Ainsi la restauration du message est meilleure pour de petites valeurs du paramètre σ, ce qui correspond à un niveau de sécurité moindre. Au contraire, lorsque la clé prend une valeur importante, la restauration du message n'est pas possible. Dans le cadre d'une extension des résultats obtenus, nous avons souligné que la méthode proposée appartient au domaine général de la restauration d'entrées inconnues, et peut donc être envisagée sous d'autres angles. Le signal $u(t)$ peut ainsi être considéré comme un retard de transmission, variable et inconnu, que l'on est capable d'estimer en suivant la procédure décrite dans ce chapitre. Pour cette généralisation, il n'est plus question de traiter des questions de sécurité. Le paramètre σ peut être considéré comme un paramètre parmi d'autres, et dans ce cas on a toute latitude pour fixer sa valeur. La robustesse peut alors être étudiée, sans que cela implique une dégradation de la sécurité.

Toutes les études sur la sécurité des cryptosystèmes chaotiques le disent : une grande complexité

des signaux transmis constitue un gage supplémentaire de sécurité. Pour renforcer la résistance du processus de communications sécurisées détaillé dans ce chapitre à une cryptanalyse plus poussée, on pourrait envisager d'introduire d'autres retards dans la dynamique des deux autres états du système, et de mettre au point des procédures adéquates pour estimer l'état du système résultant, qui serait très complexe. Ce point constitue à l'heure actuelle une idée à creuser. Élargir le spectre des signaux chaotiques transmis par l'émetteur constitue sans doute une parade à toutes les attaques reposant sur des analyses spectrales. Un autre point de sécurité concerne l'évaluation de la longueur maximale du message à transmettre. Cette longueur maximale est à mettre en relation avec les techniques de reconstruction de l'attracteur : l'efficacité de ces dernières repose sur un nombre élevé de données, nombre qui augmente avec la complexité de l'attracteur. Par conséquent, la présence du retard dans la dynamique du *SCTH* contribue à augmenter le nombre de données nécessaires pour appliquer des techniques de reconstruction. Une façon simple de contrer les attaques de reconstruction de l'attracteur consiste à changer très souvent la clé du cryptosystème (par une autre technique de cryptage, par exemple la méthode RSA). Un autre moyen est présenté dans le chapitre suivant.

CHAPITRE

4

Multimodèles chaotiques

Sommaire

4.1 Introduction

Ce chapitre a pour but de proposer une nouvelle famille (infinie) de systèmes chaotiques, et de concevoir des observateurs spécifiques. On a déjà évoqué le fait que chaque système chaotique possède des caractéristiques propres qui lui confèrent une sorte de "signature", qui le distingue des autres systèmes chaotiques. Un examen, même rapide, des courbes correspondant à différents systèmes chaotiques dans l'annexe B permet de s'en convaincre : les séries temporelles et les spectres des trois systèmes chaotiques de Lorenz, Rössler et Chua sont très différents, et par conséquent potentiellement identifiables. Ces constatations sont visibles sur les courbes tracées respectivement sur les figures B.3, B.5, et B.9. Par ailleurs l'attracteur correspondant possède des propriétés géométriques intrinsèques qui lui confèrent une forme caractéristique. Ces quelques remarques laissent supposer que les signaux chaotiques, lorsqu'ils sont examinés attentivement, ne peuvent pas réellement être confondus avec du bruit. Des techniques de reconstruction notamment par plongement, utilisant des retards sont détaillées dans les articles [Abarbanel 93], [Pecora 97] et sont précisées dans la suite de ce chapitre. Elles exploitent les informations contenues dans toute série temporelle d'un système chaotique, pour reconstituer la géométrie de l'attracteur. Cette reconstruction, même imparfaite, donne une idée générale de la famille de l'attracteur chaotique, donc du modèle dynamique correspondant et fournit ainsi des bases à une éventuelle identification des paramètres. Une parade possible pour lutter contre ce type d'attaque consisterait à "mixer" différents attracteurs, pour obtenir un nouveau type d'attracteur, qui hériterait ainsi des propriétés des attracteurs originaux. Le fait de mélanger les influences de divers systèmes chaotiques pourrait contrer les attaques à base de reconstruction à retard. Pour cela, nous voulons nous inspirer des techniques de commutation présentées au paragraphe 1.4.3, et utilisées pour le cryptage, mais sans reprendre tout le principe, car il présente deux inconvénients majeurs. En effet, aux instants de commutation, d'une part on peut voir le changement de système chaotique, et d'autre part la synchronisation est perdue et prend quelques fractions de secondes pour s'établir de nouveau. On rappelle que l'on tente de trouver un moyen de générer des familles de systèmes chaotiques, dont on cherchera ensuite à estimer l'état. Le schéma de synchronisation ainsi réalisé sera finalement intégré au sein du système de cryptage décrit au chapitre précédent (qui ne supporte pas la moindre perte de synchronisation). En fait, on conserve l'idée de base du principe de commutation, à savoir que l'on dispose de plusieurs systèmes chaotiques au niveau de l'émetteur. Mais on décide d'adoucir la transition d'un système à l'autre. Pour cela, on reprend le principe des multimodèles linéaires et on le détourne pour créer une nouvelle famille de systèmes chaotiques. Dans un premier temps, on détaille le concept de multimodèle standard, ainsi que la stabilité de ce type de systèmes. Dans un second temps, on détourne le principe classique des multimodèles de son objectif premier pour créer de nouveaux systèmes chaotiques, puis on propose des observateurs dont la structure est adaptée aux multimodèles chaotiques. Les résultats obtenus sont ensuite étendus aux systèmes à retard. Des simulations dans les deux cas (sans puis avec retard) testent la synchronisation des observateurs synthétisés et, dans le cas des systèmes sans retard, un diagramme de bifurcations donne

un élément de preuve du caractère chaotique du multimodèle proposé.

4.2 Définition d'un multimodèle

Les multimodèles constituent une représentation particulière des systèmes non linéaires. En effet, étant donné un système non linéaire qui possède plusieurs points de fonctionnement, par linéarisation on obtient autant de modèles linéaires locaux. Ces sous-modèles sont alors interpolés pour aboutir à un multimodèle linéaire, dont le modèle dynamique est une approximation (plus ou moins fine, selon le nombre de modèles locaux) du modèle dynamique du système non linéaire original.
Pour préciser ce processus d'obtention d'un multimodèle, on considère le système non linéaire suivant :

$$\dot{x}(t) = f(x(t), u(t)) \tag{4.1}$$

Au voisinage d'un point de fonctionnement (x_i, u_i), la linéarisation du système (4.1) est donnée par :

$$\dot{x}(t) = A_i(x(t) - x_i) + B_i(u(t) - u_i) + f(x_i, u_i) \tag{4.2}$$

soit, sous forme compacte :

$$\dot{x}(t) = A_i x(t) + B_i u(t) + d_i \tag{4.3}$$

avec

$$A_i = \frac{\partial f}{\partial x}(x_i, u_i), \quad B_i = \frac{\partial f}{\partial u}(x_i, u_i), \quad d_i = f(x_i, u_i) - A_i x_i - B_i u_i \tag{4.4}$$

Si le système non linéaire (4.1) est linéarisé autour de p points de fonctionnement (x_i, u_i), $i = 1, p$, alors on définit le multimodèle issu de (4.1) comme suit :

$$\dot{x}(t) = \sum_{i=1}^{p} \mu_i(\xi(t)) \left(A_i x(t) + B_i u(t) + d_i\right) \tag{4.5}$$

où $\mu_i(.)$ est la fonction d'activation du $i^{ème}$ modèle local. Les fonctions d'activation vérifient les propriétés suivantes :

$$\begin{cases} \sum_{i=1}^{p} \mu_i(\xi) = 1 \\ 0 \leq \mu_i(\xi) \leq 1 \ \forall i = 1, p \end{cases} \tag{4.6}$$

A chaque instant, la valeur de μ_i détermine la façon dont le $i^{ème}$ modèle local agit dans la dynamique du multimodèle (4.5). En effet, s'il existe $i \in \{1, \dots p\}$ tel que $\mu_i(\xi) = 1$, d'après (4.5) et (4.6), seul le $i^{ème}$ modèle est actif, tandis que si $0 < \mu_i(\xi) < 1$, alors il existe $j \in \{1, \dots p\}, j \neq i$ tel que $\mu_j(\xi) > 0$, donc au moins deux modèles locaux sont actifs.
La variable ξ peut dépendre des mesures y, de l'entrée u (qui sont les seuls signaux disponibles), ou encore de l'état x.

Remarque 4.2.1. Il existe d'autres techniques pour obtenir un multimodèle. Nous ne détaillons

pas ces méthodes dans ce mémoire, pour un état de l'art approfondi, le lecteur pourra se reporter à [Chadli 02].

4.3 Analyse de la stabilité

On considère ici la stabilité quadratique des multimodèles. Cette approche fait appel à la théorie de Lyapunov classique. Elle repose sur des fonctions de Lyapunov quadratiques. Cette méthode, bien que parfois conservative, a le mérite d'être simple à mettre en oeuvre.
On considère ici un multimodèle en boucle ouverte :

$$\dot{x}(t) = \sum_{i=1}^{p} \mu_i(\xi(t)) A_i x(t) \tag{4.7}$$

tel que les fonctions μ_i vérifient (4.6).

Proposition 4.3.1 ([Boyd 94])**.** *Le multimodèle* (4.7) *est globalement asymptotiquement stable s'il existe une matrice symétrique définie positive P telle que les LMI suivantes soient réalisables*

$$A_i^T P + P A_i < 0, \quad \forall i = 1, p \tag{4.8}$$

▲

Démonstration. On définit la fonction de Lyapunov quadratique suivante :

$$V(x(t)) = x^T(t) P x(t) \tag{4.9}$$

Il suffit alors de dériver (4.9) le long des trajectoires de (4.7).
On peut remarquer que l'existence d'une telle matrice P dépend de deux conditions, à savoir que les matrices A_i doivent être de Hurwitz (ce qui implique la stabilité de chaque modèle local) ; la seconde condition nécessaire est que la somme $\sum_{i=1}^{p} A_i$ doit être de Hurwitz (il suffit de faire la somme des p LMI (4.8) pour le voir).

4.4 Estimation de l'état de multimodèles chaotiques

4.4.1 Construction d'un multimodèle chaotique

Nous avons vu au chapitre précédent que la sécurité d'un système de communications chaotiques est conditionnée notamment par la complexité du (des) signal (signaux) transmis au récepteur : plus la façon de générer le chaos est complexe, plus le système de communications peut résister aux attaques. Dans cette partie, nous proposons une technique destinée à contrer les attaques à base de reconstruction à retard. Il s'agit de la principale faille des schémas de communications utilisant la synchronisation des systèmes chaotiques : Ruelle et Takens ont montré qu'à partir

d'une série temporelle d'un des états $x(t)$ du système chaotique, il est possible de reconstruire l'attracteur, ou plus précisément un espace topologiquement équivalent à l'espace de phase original. La méthode repose sur l'introduction d'un retard τ (qui reste à déterminer), et consiste à construire des vecteurs de dimension m de données successives (m n'est pas connu *a priori*) :

$$[x(n), x(n+\tau), \ldots, x\left(n+(m-1)\tau\right)] \tag{4.10}$$

On parle alors d'espace d'immersion, si $m \geqslant 2D+1$, où D est la *dimension d'immersion* (ou de plongement) : elle correspond à l'entier juste supérieur à la dimension de l'attracteur, dimension non entière en général. Cette dimension d'immersion doit être déterminée avant de pouvoir appliquer la méthode de reconstruction à retard.
Deux problèmes majeurs se posent. Dans un premier temps, le choix crucial du décalage temporel τ peut s'avérer délicat. Diverses méthodes ont été élaborées, qui sont au-delà du sujet de ce mémoire. Le second problème réside dans la taille de la série temporelle elle-même : l'application de la méthode suppose un nombre infini d'échantillons non bruités (ou le moins possible). Par conséquent, les techniques de communications qui transmettent des séries temporelles de différents attracteurs chaotiques possèdent une certaine protection contre les attaques à base de reconstruction à retard : chaque série correspondant à un attracteur est assez courte, et immédiatement suivie par une série correspondant à un autre attracteur. . . Par exemple, dans la littérature on peut citer les techniques de cryptage par commutation, ou par modulation (voir références aux paragraphes 1.4.3, 1.4.4), qui cependant se sont révélées inefficaces faces à d'autres attaques : les articles [Short 94], [Short 96], [Yang 98b] exploitent le fait que la présence du message dans la dynamique de l'émetteur transforme l'attracteur chaotique. Par ailleurs, les systèmes chaotiques à commutation proposent une nouvelle façon de générer du chaos [Millérioux 03] : ces systèmes sont définis par plusieurs sous-modèles, qui commutent à des instants précis.

Nous proposons une nouvelle classe de systèmes chaotiques, sous la forme de multimodèles chaotiques. Nous reprenons la méthode de construction du multimodèle détaillée au paragraphe précédent.
On dispose pour cela de p systèmes chaotiques, désignés dans la suite par l'expression« modèle de base » :

$$\dot{x}(t) = A_i x(t) + f_i(x(t)) \tag{4.11}$$

En utilisant le même procédé qu'à l'équation (4.5), on obtient le multimodèle chaotique suivant :

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{p} \mu_i(\xi(t)) \left(A_i x(t) + f_i(x(t))\right) \\ y(t) = Cx(t) \end{cases} \tag{4.12}$$

Les fonctions f_i sont des fonctions non linéaires, choisies de telle sorte que chaque modèle de base (4.11) ait un comportement chaotique. On suppose en outre que les nonlinéarités vérifient

la condition de Lipschitz (1.24), et que les fonctions d'interpolation μ_i vérifient (4.6). Il s'agit bien d'une nouvelle classe de systèmes chaotiques, dédiés à la synchronisation dans le cadre de ce mémoire. La transition d'un modèle à l'autre se fait de façon continue, et ne dépend pas d'une entrée inconnue, contrairement aux techniques de cryptage (par commutation ou par modulation notamment). Il s'agit donc bien d'une nouvelle classe de systèmes non linéaires, chaotiques. Il n'est pas question ici de relier la construction de cette nouvelle famille de systèmes chaotiques à une technique particulière de cryptage. Après la mise au point de schémas de synchronisation de multimodèles chaotiques à base d'observateurs spécifiques, il sera possible d'appliquer une technique de cryptage utilisant la synchronisation chaotique, par exemple la technique de cryptage par modulation de phase que nous avons détaillée au chapitre précédent.

Remarque 4.4.1. Dans la suite, on suppose que $\xi(t) = y(t)$, car dans notre cas, le signal $y(t)$ est le seul connu par le récepteur. ♦

Nous montrerons, au paragraphe 4.4.3.1, grâce à un diagramme de bifurcations, que le multimodèle généré à partir de deux circuits de Chua est chaotique.

La synchronisation du multimodèle chaotique (4.12) nécessite la construction d'un récepteur adéquat. Aussi proposons-nous la structure d'observateur suivante :

$$\dot{\hat{x}}(t) = \sum_{i=1}^{p} \mu_i(y(t)) \left(A_i\hat{x}(t) + f_i(\hat{x}(t)) + K_i(y(t) - C\hat{x}(t))\right) \tag{4.13}$$

On peut reconnaître une structure d'observateur classique, adaptée spécifiquement aux multimodèles, avec p gains K_i à déterminer.

Convergence asymptotique

Le théorème suivant énonce des conditions suffisantes permettant au système (4.13) d'estimer l'état du multimodèle chaotique (4.12).

Théorème 4.4.1 ([Cherrier 06e])**.** *S'il existe une matrice symétrique définie positive P et des gains K_i, $i = 1, p$, tels que les p BMI suivantes soient vérifiées :*

$$\begin{pmatrix} (A_i - K_iC)^T P + P(A_i - K_iC) + k_{f_i} I & P \\ P & -\frac{1}{k_{f_i}} I \end{pmatrix} < 0 \tag{4.14}$$

alors le système (4.13) *est un observateur du multimodèle* (4.12) *: $\hat{x}(t) \to x(t)$ quand $t \to \infty$.* ■

Démonstration : La dérivée du vecteur d'erreur de synchronisation $e(t) = x(t) - \hat{x}(t)$ est donnée par :

$$\dot{e}(t) = \sum_{i=1}^{p} \mu_i(y(t)) \left((A_i - K_iC)e + f_i(x(t)) - f_i(\hat{x}(t))\right) \tag{4.15}$$

Pour alléger les notations, on pose :

$$\mathcal{M} = \sum_{i=1}^{p} \mu_i(y(t)) \left(A_i - K_i C\right) \tag{4.16}$$

et $\tilde{f}_i(t) = f_i(x(t)) - f_i(\hat{x}(t))$, $i = 1, p$.
On introduit alors la fonction de Lyapunov $V(t) = e^T(t)Pe(t)$, P étant une matrice symétrique définie positive.
Le vecteur d'erreur de synchronisation $e(t)$ converge asymptotiquement vers zéro si :

(i) $V(t) \geqslant 0$

(ii) $\dot{V}(t) \leqslant 0$

Par hypothèse sur P, on obtient immédiatement :

$$0 < \lambda_m(P)\|e\|^2 \leq V(t) \leq \lambda_M(P)\|e\|^2 \tag{4.17}$$

En utilisant les notations précédentes, la dérivée de V le long des trajectoires de (4.15) s'écrit :

$$\dot{V}(t) = e^T(t) \left(\mathcal{M}^T P + P\mathcal{M}\right) e(t) + 2e^T(t)P \sum_{i=1}^{p} \mu_i(y(t))\tilde{f}_i(t) \tag{4.18}$$

En appliquant les inégalités de Cauchy-Schwarz et de Young, il vient, pour $i = 1, p$:

$$e^T P\tilde{f}_i \leq k_{f_i} e^T PPe + k_{f_i} e^T e \tag{4.19}$$

D'où :

$$\dot{V} \leqslant e^T(t) \left(\mathcal{M}^T P + P\mathcal{M} + \sum_{i=1}^{p} \mu_i(y(t)) k_{f_i} P^2 + \sum_{i=1}^{p} \mu_i(y(t)) k_{f_i} I \right) e(t) \tag{4.20}$$

Si la condition suivante est remplie :

$$\mathcal{M}^T P + P\mathcal{M} + \sum_{i=1}^{p} \mu_i(y) k_{f_i} P^2 + \sum_{i=1}^{p} \mu_i(y) k_{f_i} I < 0 \tag{4.21}$$

ce qui revient à vérifier, par convexité, que pour tout $i = 1, p$ on a :

$$(A_i - K_i C)^T P + P(A_i - K_i C) + k_{f_i} P^2 + k_{f_i} I < 0 \tag{4.22}$$

alors on peut conclure que $\dot{V}(t) \leqslant 0$. En appliquant le complément de Schur, les équations de type Riccati (4.22) peuvent être mises sous forme de BMI (4.14). □

Convergence exponentielle

En fait, on peut montrer une propriété plus forte que la convergence asymptotique de l'observateur, à savoir la convergence exponentielle, qui fait l'objet du corollaire suivant.

Corollaire 4.4.2. *On reprend les hypothèses du théorème 4.4.1, et on modifie légèrement les BMI* (4.14) *: on suppose qu'il existe des matrices Q et Q_i, $i = 1, p$ définies positives telles que pour tout i :*

$$\begin{pmatrix} (A_i - K_i C)^T P + P (A_i - K_i C) + k_{f_i} I + Q_i & P \\ P & -\frac{1}{k_{f_i}} I \end{pmatrix} < 0 \tag{4.23}$$

et

$$Q_i < Q \tag{4.24}$$

alors l'erreur de synchronisation $e(t) = x(t) - \hat{x}(t)$ converge exponentiellement vers zéro, selon la formule :

$$\|e(t)\| \leqslant \rho \|e(0)\| e^{-\frac{\nu}{2} t} \tag{4.25}$$

avec

$$\rho = \sqrt{\frac{\lambda_M(P)}{\lambda_m(P)}} \tag{4.26a}$$

$$\nu = \frac{\lambda_m(Q)}{\lambda_M(P)} \tag{4.26b}$$

■

Démonstration : On repart des équations de type Riccati (4.22), et on fait une hypothèse plus forte. On suppose qu'il existe des matrices définies positives Q_i telles que :

$$(A_i - K_i C)^T P + P(A_i - K_i C) + k_{f_i} P^2 + k_{f_i} I < -Q_i \tag{4.27}$$

Si en outre, il existe une matrice définie positive Q telle que $Q_i < Q$ pour tout $i = 1, p$, alors par convexité, il vient :

$$\dot{V} \leqslant -e^T Q e \tag{4.28}$$

On en déduit :

$$\dot{V} \leqslant -\lambda_m(Q) \|e\|^2 \tag{4.29}$$

On fait alors apparaître le facteur $\lambda_M(P)$, pour pouvoir utiliser (4.17) :

$$\dot{V} \leqslant -\frac{\lambda_m(Q)}{\lambda_M(P)} \lambda_M(P) \|e\|^2 \tag{4.30}$$

On obtient finalement :

$$\dot{V} \leqslant -\nu V \tag{4.31}$$

avec ν donné par la formule (4.26).
En intégrant (4.31), il vient :

$$V(t) \leqslant V(0)e^{-\nu t} \tag{4.32}$$

Or (4.17) implique en particulier :

$$\|e(t)\| \leqslant \sqrt{\frac{V(t)}{\lambda_m(P)}} \tag{4.33}$$

Donc, en utilisant (4.32) et (4.26), on obtient :

$$\begin{aligned} \|e(t)\| &\leqslant \sqrt{\frac{V(0)e^{-\nu t}}{\lambda_m(P)}} \\ &\leqslant \rho\|e(0)\|e^{-\frac{\nu}{2}t} \end{aligned} \tag{4.34}$$

ce qui termine la démonstration. □

4.4.2 Extension aux multimodèles chaotiques à retard

Le processus de construction détaillé au paragraphe précédent peut être adapté en choisissant comme modèles de base, des systèmes chaotiques à retard. Le multimodèle à retard résultant est le suivant :

$$\begin{cases} \dot{x}(t) = \sum_{i=1}^{p} \mu_i(y(t)) \left(A_i x(t) + f_i(x(t)) + h_i(x_\tau(t))\right) \\ y(t) = Cx(t) \end{cases} \tag{4.35}$$

L'observateur du système (4.35) possède la même structure que l'observateur (4.13) :

$$\dot{\hat{x}}(t) = \sum_{i=1}^{p} \mu_i(y(t)) \left(A_i \hat{x}(t) + f_i(\hat{x}(t)) + h_i(\hat{x}_\tau(t)) + K_i(y(t) - C\hat{x}(t))\right) \tag{4.36}$$

On adapte également le théorème 4.4.1.

Corollaire 4.4.3 ([Cherrier 06c])**.** *S'il existe une matrice P symétrique définie positive, une matrice Q définie positive, et p gains K_i tels que*

$$\begin{pmatrix} (A_i - K_i C)^T P + P(A_i - K_i C) + Q + k_{f_i} I & P \\ P & -\frac{1}{k_{f_i} + k_{h_i}} I \end{pmatrix} < 0 \tag{4.37}$$

et

$$Q > \max_{i=1,p}(k_{h_i}) I \tag{4.38}$$

alors le système (4.36) *est un observateur asymptotique du multimodèle chaotique à retard* (4.35).
■

Démonstration : On note $e = x - \hat{x}$ le vecteur d'erreur de synchronisation. On reprend le raisonnement et les notations de la démonstration du théorème 4.4.1. La dynamique de l'erreur

a pour expression :

$$\dot{e} = \sum_{i=1}^{p} \mu_i(y) \left((A_i - K_i C)e + f_i(x) - f_i(\hat{x}) + h_i(x_\tau) - h_i(\hat{x}_\tau) \right) \tag{4.39}$$

On introduit la fonctionnelle de Lyapunov-Krasovskii :

$$V(e, e_\tau) = e^T P e + \int_{-\tau}^{0} e(t+\theta)^T Q e(t+\theta) d\theta \tag{4.40}$$

On a clairement $0 < \lambda_m(P)\|e\|^2 \leqslant V$. La dérivée de V le long des trajectoires de (4.39) est donnée par :

$$\dot{V} = e^T \left(\mathcal{M}P + P\mathcal{M} + Q \right) e + 2e^T P \sum_{i=1}^{p} \mu_i(y) \tilde{f}_i + 2e^T P \sum_{i=1}^{p} \mu_i(y) \tilde{h}_i - e_\tau^T Q e_\tau \tag{4.41}$$

Comme précédemment, on applique les inégalités de Cauchy-Schwarz et Young, et on obtient :

$$\dot{V} \leqslant e^T \left(\mathcal{M}P + P\mathcal{M} + Q + \sum_{i=1}^{p} \mu_i(y)(k_{f_i} + k_{h_i})P^2 + \sum_{i=1}^{p} \mu_i(y) k_{f_i} I \right) e + e_\tau^T \left(\sum_{i=1}^{p} \mu_i(y) k_{h_i} I - Q \right) e_\tau \tag{4.42}$$

Par convexité, si les équations de type Riccati suivantes sont vérifiées pour $i = 1, p$:

$$(A_i - K_i C)^T P + P(A_i - K_i C) + Q + (k_{f_i} + k_{h_i})P^2 + k_{f_i} I < 0 \tag{4.43}$$

et

$$k_{h_i} I - Q < 0 \tag{4.44}$$

alors $\dot{V}(e, e_\tau) < 0$. Ces deux conditions correspondent aux hypothèses (4.37) et (4.38) du théorème.
On a donc démontré que $\hat{x}(t) \to x(t)$ quand $t \to \infty$. □

Remarque 4.4.2. En ce qui concerne les fonctions d'activation μ_i, on peut souligner que leur expression ne joue aucun rôle dans les démonstrations précédentes, les seules conditions requises étant énoncées en (4.6). En pratique, pour réaliser un "mixage" effectif entre les différents modèles de base, il faut choisir des fonctions d'activation qui ne privilégient pas un modèle, mais qui permettent une réelle transition entre les différents systèmes chaotiques. Cela permet d'une part, de renforcer la complexité du signal transmis au récepteur, et d'autre part de garantir une synchronisation continue, dans le sens où il n'y a pas de perte de synchronisation, contrairement aux systèmes qui commutent entre plusieurs émetteurs. ♦

4.4.3 Simulations

Ce paragraphe illustre la synchronisation des multimodèles chaotiques que nous avons abordée en théorie précédemment. Des tests sont réalisés sur deux exemples. Le premier considère comme modèles chaotiques de base des circuits de Chua avec différents paramètres (correspondant à différents attracteurs). En outre, le paragraphe 4.4.3.1 montre numériquement que le multimodèle généré possède un comportement chaotique, par le tracé d'un diagramme de bifurcations. Dans un second exemple, nous testons la synchronisation d'un multimodèle chaotique comportant un retard, dont les modèles de base sont des *SCTH*. Enfin le dernier paragraphe est consacré à l'intégration d'un schéma de synchronisation de multimodèle au sein d'un processus de communications, la technique de transmission sécurisée du message étant celle développée au chapitre 3.

4.4.3.1 Application au circuit de Chua

Pour ce premier exemple, nous avons choisi comme modèles de base deux circuits de Chua classiques, avec deux ensembles de paramètres distincts. La dynamique du circuit de Chua sans dimension est redonnée ici :

$$\begin{cases} \dot{x_1} &= -\alpha x_1 + \alpha x_2 - \alpha f(x_1) \\ \dot{x_2} &= x_1 - x_2 + x_3 \\ \dot{x_3} &= -\beta x_2 - \gamma x_3 \end{cases} \tag{4.45}$$

avec

$$f(x_1) = bx_1 + \frac{1}{2}(a-b)\left(|x_1+1| - |x_1-1|\right) \tag{4.46}$$

Simulation du multimodèle

Les paramètres choisis pour les deux modèles de base sont donnés dans les tableaux 4.1 et 4.2. Les attracteurs correspondants se trouvent à la figure 4.1. Les simulations sont faites avec

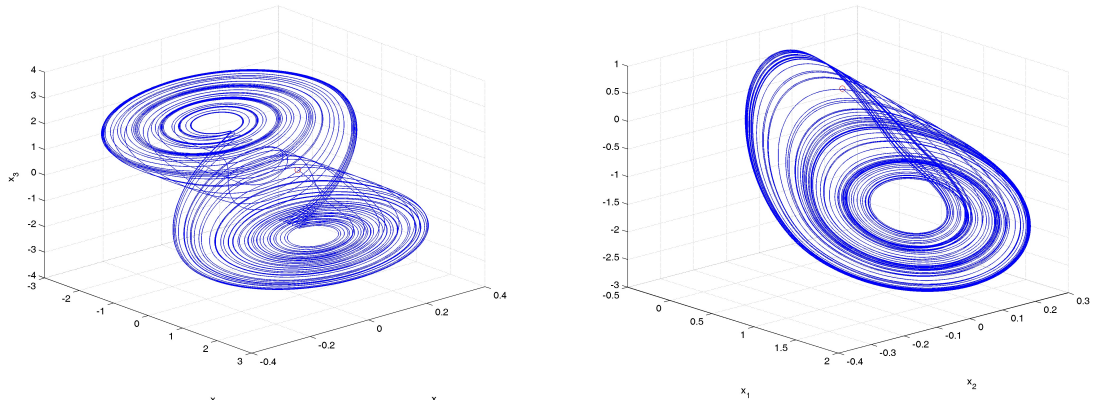
α_1	β_1	γ_1	a_1	b_1
9	14	0	$-1,14$	$-0,7$

TAB. 4.1 - *Paramètres du premier modèle de base*

α_2	β_2	γ_2	a_2	b_2
$9,5$	15	0	$-1,1$	$-0,7$

TAB. 4.2 - *Paramètres du second modèle de base*

une méthode d'intégration de Runge-Kutta d'ordre quatre, de pas égal à une milliseconde. Les



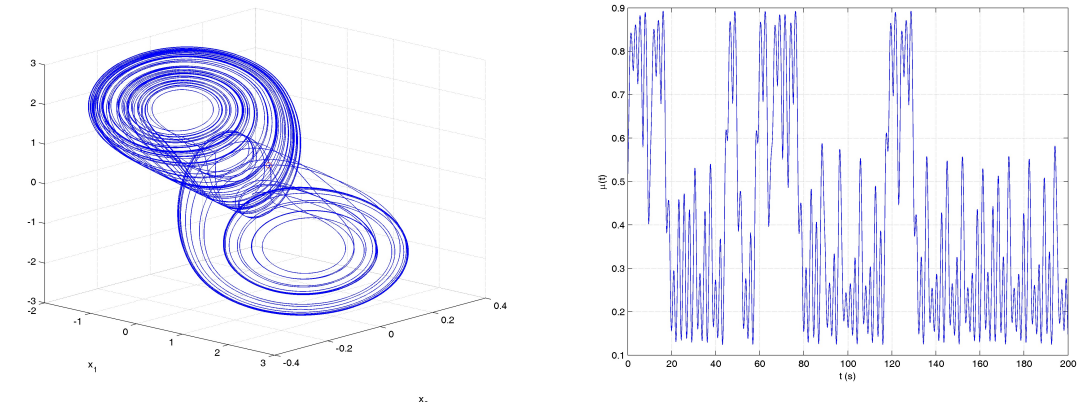
(a) Attracteur du sous-système 1 (b) Attracteur du sous-système 2

FIG. 4.1 - *Attracteurs des modèles de base du multimodèle chaotique de type Chua*

conditions initiales sont $x_0 = \begin{pmatrix} 0,1 & 0,1 & 0,1 \end{pmatrix}^T$.
La fonction d'activation μ choisie est la suivante :

$$\mu(y) = \frac{1 + tanh(\omega y)}{2} \tag{4.47}$$

Le paramètre ω est fixé arbitrairement de telle sorte que la fonction μ réalise une réelle transition continue entre les deux sous-systèmes de Chua, et pas seulement une commutation entre eux. Les simulations du multimodèle résultant sont visibles à la figure 4.2(a), ω ayant été fixé à la valeur $0,5$, et la fonction μ correspondante est tracée à la figure 4.2(b).



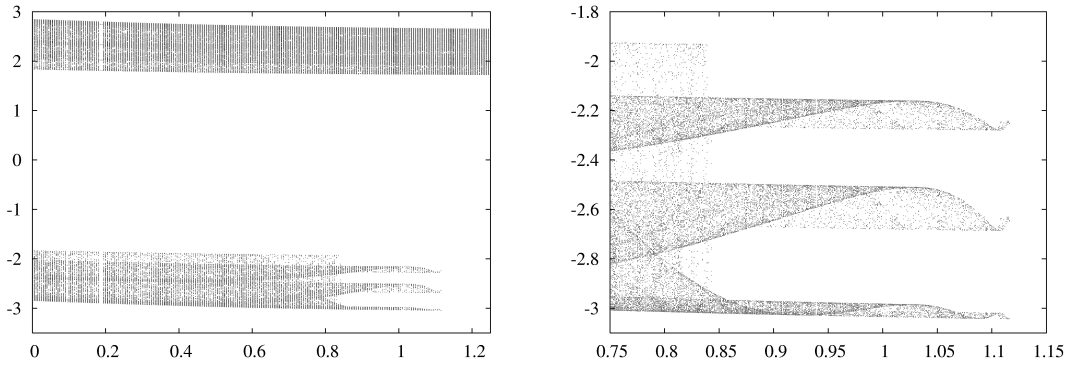
(a) Multimodèle à base de systèmes de Chua (b) Fonction $\mu(t)$

FIG. 4.2 - *Multimodèle chaotique et fonction d'activation associée*

Analyse des bifurcations

Le comportement chaotique du multimodèle à base de circuits de Chua est analysé numérique-

ment dans différentes régions de l'espace des paramètres. Nous ne présentons pas d'analyse plus approfondie, cela reste hors de la portée de ce mémoire. La figure 4.3 montre une route vers le chaos spécifique, par doublement de période (ou plutôt par division de période). Les paramètres du multimodèle sont fixés par les valeurs données dans les tableaux 4.1-4.2, et ω varie en tant que paramètre de bifurcation : $\omega \in [0; 1,25]$. On se place dans le plan d'équation $x_2 = 0$, et on reporte dans le diagramme la coordonnée suivant l'axe x_3 des points qui sont à l'intersection entre l'attracteur et ce plan. Pour éviter le régime transitoire, on élimine les 10^7 premières valeurs. Les simulations ont été faites avec une grande précision pour différentes conditions initiales et



(a) (b) Zoom

FIG. 4.3 - *Diagramme de bifurcation vis à vis du paramètre ω*

pour différentes variations de paramètres, permettant de vérifier nos résultats. Pour obtenir des résultats fiables sur le plan numérique, le pas d'intégration numérique a été fixé à 10^{-4} s.
On constate que pour de petites valeurs de ω, le multimodèle est chaotique et présente un attracteur à double spirale similaire à celui de Chua, visible sur la figure 4.1(a). Cependant, la forme de l'attracteur évolue, puisqu'il n'est constitué que d'une seule spirale lorsque μ privilégie le second modèle de base, ce qui correspond approximativement à des valeurs de ω supérieures à $1,116$. Au-delà de ce seuil, la seconde spirale (celle du bas sur la figure 4.2(a)) disparaît, et seul persiste un attracteur à simple spirale. Nos simulations numériques montrent que le multimodèle à base de systèmes de Chua est chaotique en général, pour les valeurs fixées dans les tableaux 4.1-4.2, quelle que soit la valeur de ω. On peut remarquer qu'il existe des fenêtres où le comportement n'est plus chaotique : par exemple, autour de la valeur $\omega \approx 0,1825$, le système présente une spirale 4-périodique.

Synchronisation

L'émetteur étant déterminé, on s'intéresse maintenant à la conception du récepteur. On choisit $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix}$ avec $\zeta = 0,1$ pour maîtriser l'amplitude des constantes de Lipschitz des nonlinéarités, comme au chapitre 2 (voir page 59).

Les états initiaux de l'émetteur et du récepteur sont les suivants :

$$x_0 = \begin{pmatrix} 0,1 & 0,1 & 0,1 \end{pmatrix}^T \tag{4.48}$$

$$\hat{x}_0 = \begin{pmatrix} -0,1 & 0,01 & -0,1 \end{pmatrix}^T \tag{4.49}$$

En utilisant les résultats du Corollaire 4.4.2 et une procédure de résolution des BMI correspondantes, on trouve les gains suivants pour l'observateur (4.13) :

$$K_1 = \begin{pmatrix} 11,419981627642 \\ 59,750898307782 \\ 103,474125696083 \end{pmatrix} \tag{4.50}$$

$$K_2 = \begin{pmatrix} 11,851591992933 \\ 62,814208155331 \\ 109,009094424559 \end{pmatrix} \tag{4.51}$$

Les matrices auxiliaires sont :

$$P = \begin{pmatrix} 3,51043865400960 & -2,00113769871303 & 0,51125333574415 \\ (\star) & 3,65447972536984 & -1,41484800424127 \\ (\star) & (\star) & 0,68844456270232 \end{pmatrix} \tag{4.52}$$

$$Q = \begin{pmatrix} 10,66079073945656 & 0,02413039500517 & -0,00462850587275 \\ (\star) & 10,42189982890535 & 0,04628505872748 \\ (\star) & (\star) & 7,64405606986856 \end{pmatrix} \tag{4.53}$$

$$Q_1 = \begin{pmatrix} 5,32878814403720 & 0,02813745441342 & 0,00111363297663 \\ (\star) & 5,05022734534426 & -0,01113632976634 \\ (\star) & (\star) & 1,25277380266573 \end{pmatrix} \tag{4.54}$$

$$Q_2 = \begin{pmatrix} 5,32816650045085 & 0,03435389027683 & -0,01347561033962 \\ (\star) & 4,98806298671028 & 0,13475610339618 \\ (\star) & (\star) & 1,25948550628620 \end{pmatrix} \tag{4.55}$$

La figure 4.4 montre la convergence exponentielle vers zéro des trois composantes de $e(t)$, en accord avec la formule (4.25) : pour cette simulation, on a $\nu = 1,28472981093510$, $\rho = 64,95142673319106$ et $\|e(0)\| = 0,29681644159312$.

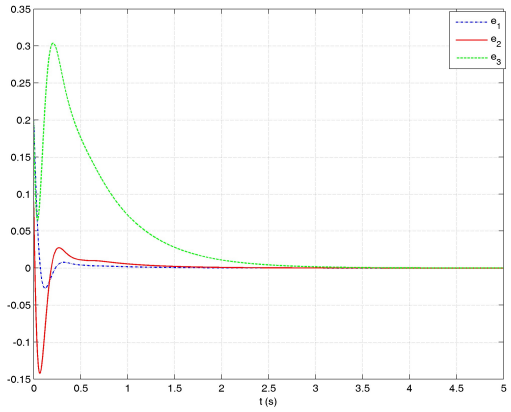


FIG. 4.4 - *Composantes du vecteur d'erreur de synchronisation* $e(t)$

4.4.3.2 Application au *SCTH*

Dans ce second exemple pour illustrer la synchronisation des multimodèles chaotiques à retard, nous considérons comme modèle de base le *SCTH*, dont la dynamique est rappelée ci-dessous :

$$\begin{cases} \dot{x}_1 &= -\alpha x_1 + \alpha x_1 - \alpha\delta \tanh(x_1) \\ \dot{x}_2 &= x_1 - x_2 + x_3 \\ \dot{x}_3 &= -\beta x_2 - \gamma x_3 + \varepsilon \sin(\sigma x_{1\tau}) \end{cases} \tag{4.56}$$

Simulation du multimodèle

Les paramètres choisis pour les deux modèles de base sont donnés dans les tableaux 4.3 et 4.2.

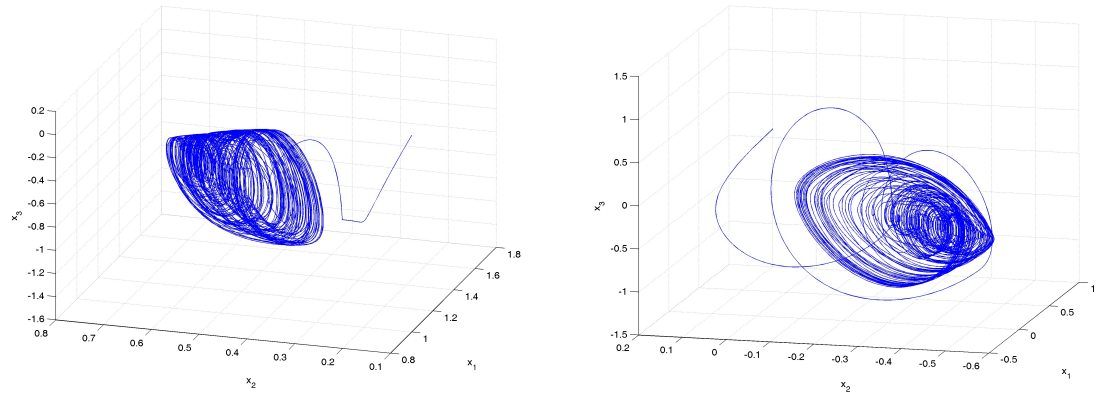
α_1	β_1	γ_1	δ_1	ε_1	σ_1	τ_1
40	35	20	-1	10	10	1

TAB. 4.3 - *Paramètres du premier modèle de base*

α_1	β_1	γ_1	δ_1	ε_1	σ_1	τ_1
20	15	5	1	10	10	1

TAB. 4.4 - *Paramètres du second modèle de base*

Les attracteurs correspondants se trouvent à la figure 4.5. Les simulations sont faites avec une méthode d'intégration de Runge-Kutta d'ordre quatre, de pas égal à une milliseconde. Les conditions initiales sont $x_0 = \begin{pmatrix} 1 & 0,1 & 0,1 \end{pmatrix}^T$.



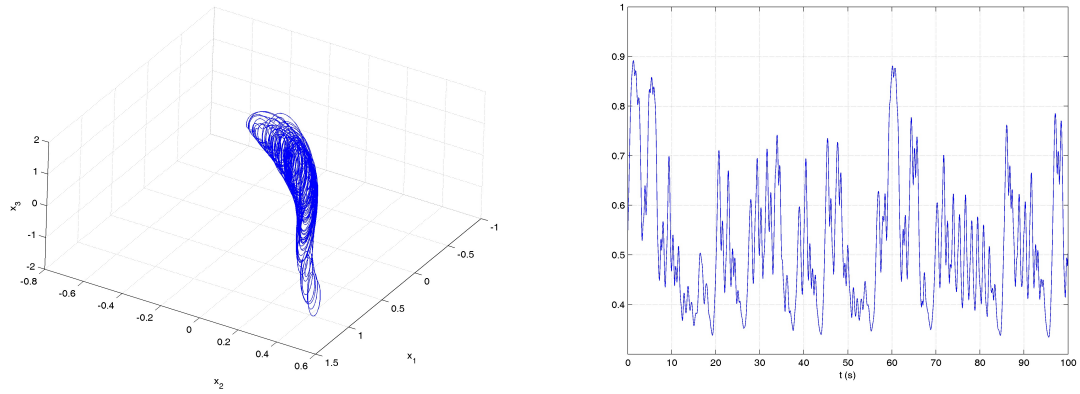
(a) Attracteur du sous-système 1 (b) Attracteur du sous-système 2

FIG. 4.5 - *Attracteurs des modèles de base du multimodèle chaotique à retard de type* SCTH

La fonction d'activation μ choisie est la même qu'en (4.47) :

$$\mu(y) = \frac{1 + tanh(\omega y)}{2} \tag{4.57}$$

Les simulations du multimodèle résultant sont visibles à la figure 4.6(a), ω ayant été fixé à la valeur $0,8$, et la fonction μ correspondante est tracée à la figure 4.6(b).



(a) Multimodèle à base de *SCTH* (b) Fonction $\mu(t)$

FIG. 4.6 - *Multimodèle chaotique et fonction d'activation associée*

Synchronisation

Après le choix de l'émetteur, on s'intéresse maintenant à la construction d'un récepteur qui se synchronise avec celui-ci. La matrice C est toujours choisie de la forme $C = \begin{pmatrix} 1 & \zeta & 0 \end{pmatrix}$ avec $\zeta = 0,01$ pour maîtriser les constantes de Lipschitz des nonlinéarités, comme au chapitre 2 (voir page 59).

On fixe les états initiaux suivants :

$$x_0 = \begin{pmatrix} 0,1 & 0,1 & 0,1 \end{pmatrix}^T \tag{4.58}$$

$$\hat{x}_0 = \begin{pmatrix} -0,1 & 0,01 & -0,1 \end{pmatrix}^T \tag{4.59}$$

L'application du Corollaire 4.4.3 nécessite la résolution des BMI (4.37) et des LMI (4.38). L'utilisation d'algorithmes numériques d'optimisation convexe donne les gains suivants pour l'observateur (4.36) :

$$K_1 = \begin{pmatrix} -15,23840832709735 \\ 42,89669416998163 \\ -10,48391247200285 \end{pmatrix} \tag{4.60}$$

$$K_2 = \begin{pmatrix} -2,98973382521585 \\ 23,40909314532922 \\ -3,70286483343027 \end{pmatrix} \tag{4.61}$$

Les matrices auxiliaires trouvées sont :

$$P = \begin{pmatrix} 0,58719804146663 & -0,19931700391235 & 0,17140889382350 \\ (\star) & 0,50889519595473 & -0,10716188126479 \\ (\star) & (\star) & 0,28640236616071 \end{pmatrix} \tag{4.62}$$

$$Q = \begin{pmatrix} 4,42298519960214 & 0,01412142885433 & -0,00108020634568 \\ (\star) & 3,01098352845890 & 0,10802063456779 \\ (\star) & (\star) & 1,86837508214555 \end{pmatrix} \tag{4.63}$$

La figure 4.7 montre les résultats de la synchronisation. Les simulations ont été réalisées avec un pas d'intégration numérique de $0,001$ s.

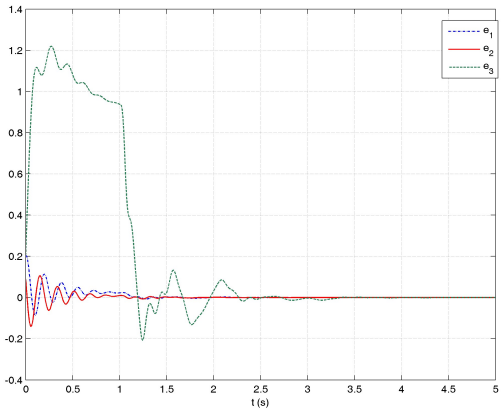


FIG. 4.7 - *Composantes du vecteur d'erreur de synchronisation* $e(t)$

4.4.3.3 Application au cryptage

Nous avons choisi d'intégrer le schéma de synchronisation du paragraphe 4.4.3.2 dans le système de transmission d'information présenté au chapitre 3. L'émetteur choisi est donc le multimodèle à retard dont les modèles chaotiques de base sont des *SCTH*. Le cas du multimodèle à base de circuits de Chua est similaire, et ne sera pas traité ici.

Transmission d'une image

Le message à transmettre est une nouvelle fois la photographie de Lena, représentée à la figure 3.8.

On reprend les conditions de simulation du schéma de synchronisation détaillées au paragraphe 4.4.3.2. La figure 4.8 montre l'erreur de reconstruction $u(t) - \hat{u}(t)$. La figure 4.9, quant à elle,

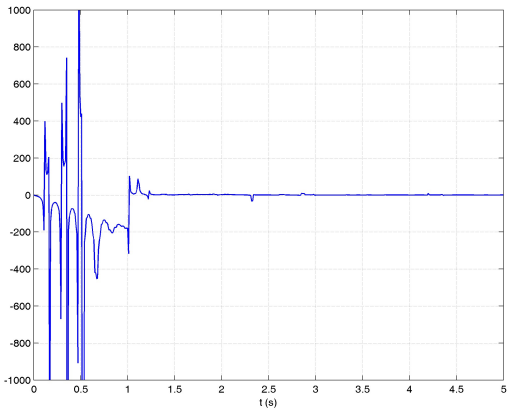
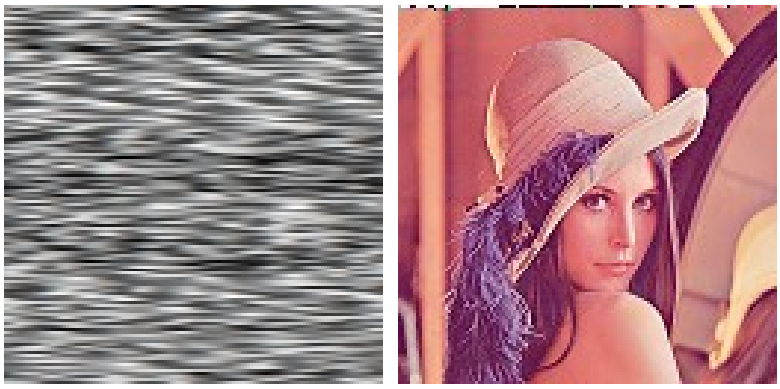


FIG. 4.8 - *Erreur de reconstruction* $u(t) - \hat{u}(t)$

représente l'image transmise (à gauche), et l'image reconstruite (à droite). Comme nous l'avons vu au chapitre 3, les premiers points de l'image reconstruite (en haut à gauche) ne sont pas corrects. On peut remarquer que, le temps de synchronisation étant plus long ici qu'à l'exemple de la page 100, il y a plus de points incorrects.

4.5 Conclusion

Dans ce chapitre, nous avons utilisé la théorie des multimodèles classiques pour construire une nouvelle classe de systèmes chaotiques. Un multimodèle chaotique est créé à partir de plusieurs modèles de base chaotiques. L'activation ou non de chaque modèle de base est déterminée à chaque instant par une fonction d'interpolation μ, qui dépend dans notre cas des sorties du système chaotique. Un schéma de synchronisation à base d'observateurs spécifiques aux multimodèles a ensuite été élaboré dans deux cas : pour des multimodèles chaotiques avec et sans retard. Des conditions suffisantes de synchronisation ont été formulées en termes de LMI et BMI.



(a) Image correspondant au signal transmis

(b) Image correspondant au signal reconstruit

FIG. 4.9 - *Images cryptée et décryptée*

Lorsque ces conditions sont remplies, la synchronisation est maintenue aussi longtemps que le signal $y(t)$ est transmis au récepteur : nous soulignons qu'il n'y a pas de perte de synchronisation (comme cela peut se produire lorsqu'il y a commutation entre plusieurs émetteurs). Le processus de synchronisation a été testé sur deux exemples. Le premier est construit à partir de circuits de Chua classiques. Nous avons présenté un élément de preuve, sous la forme d'un diagramme de bifurcations, que le multimodèle résultant est chaotique. Les modèles de bases chaotiques du second exemple sont des *SCTH*. Les conditions de synchronisation étant réunies, ce multimodèle à base de *SCTH* a servi d'émetteur dans un système de communications, le récepteur étant l'observateur construit précédemment. Nos résultats ont été illustrés par la transmission et la reconstruction d'une image.

Nous avons utilisé dans ce chapitre une approche quadratique pour l'analyse de la synchronisation. Ce choix correspond à nos attentes en matière de synchronisation et de reconstruction d'entrées inconnues. Cependant, une approche poly-quadratique pourrait réduire le conservatisme de la démonstration.

Concernant la sécurité, nous n'avons pas voulu faire double emploi avec le paragraphe 3.4. Cependant, nous avons déjà souligné au chapitre précédent que la définition de l'espace des clés est étroitement liée à l'étude approfondie du caractère chaotique exhibé par le système émetteur. Dans le cas du multimodèle chaotique à base de circuits de Chua, on a montré que le paramètre ω qui intervient dans la fonction d'activation peut servir de paramètre de bifurcations. Par conséquent, il semblerait logique que ce paramètre puisse servir de clé de cryptage. En effet, on constate sur les diagrammes de la figure 4.3 que sur certains intervalles, une petite variation de la valeur de ω induit un changement qualitatif de l'attracteur généré par le multimodèle, notamment autour de la valeur $0,8$. Nous n'avons pas approfondi ce point, qui constitue une perspective intéressante à ces travaux sur les multimodèles.

Un moyen efficace de renforcer la sécurité serait de considérer une fonction d'activation μ de variable $x(t)$, et pas seulement $y(t)$, car le signal $y(t)$ est potentiellement à la disposition de

tout intrus. Cela rend cependant le problème de l'estimation d'état notablement plus complexe, car au niveau du récepteur apparaît le terme $\mu(\hat{x}(t))$, et certaines factorisations ne sont plus possibles dans l'analyse de la synchronisation. Ce point, bien que difficile, nous semble très important à creuser, car l'apport au niveau de la sécurité serait substantiel.

Conclusion générale

«La plus grande faiblesse de la pensée contemporaine me paraît résider dans la surestimation extraordinaire du connu par rapport à ce qui reste à connaître »

André Breton, 1937

Dans ce mémoire, nous avons appliqué des résultats théoriques d'estimation d'état à un problème de transmission sécurisée de données exploitant les propriétés des systèmes chaotiques.

Afin de situer au mieux notre contribution par rapport aux travaux existants, un état de l'art a été proposé dans le premier chapitre. Il s'articule autour de quatre thèmes principaux. Nous avons d'abord rappelé les résultats principaux de la théorie de l'estimation d'état non linéaire, en général, puis en présence d'entrées inconnues. Ces domaines théoriques ont ensuite été reliés au problème de la synchronisation des systèmes chaotiques, qui constituent une classe particulière de systèmes non linéaires. Enfin le dernier thème concerne les systèmes de communications chaotiques et rassemble les résultats précédents : il s'agit d'un problème de restauration d'entrées inconnues, reposant sur la capacité de synchronisation des systèmes chaotiques.

Dans le deuxième chapitre, nous avons présenté plusieurs schémas de synchronisation à base d'observateurs. Les systèmes considérés appartiennent à une classe de systèmes chaotiques, dont la dynamique comporte un retard. La présence du retard rend le comportement de ces systèmes extrêmement complexe. Différentes techniques d'estimation d'état ont été appliquées pour résoudre le problème de la conception d'observateurs spécifiques, d'ordre plein et réduit. Nous avons établi des conditions suffisantes de synchronisation, asymptotique et exponentielle, exprimées en termes de BMI et de LMI. L'utilisation de techniques de linéarisation et d'algorithmes

d'optimisation convexe permet de déterminer les gains des différents observateurs. La fin de ce chapitre détaille la conception d'un observateur robuste au bruit. Dans l'hypothèse d'un bruit borné, nous avons indiqué une procédure de synthèse du gain de l'observateur reposant sur la théorie $\mathcal{H}_\infty$. Des conditions suffisantes de synchronisation, exprimées sous forme d'inégalités matricielles linéaires et bilinéaires, garantissent une borne optimale (exprimée en fonction de la borne du bruit) sur l'erreur d'estimation. Les différents résultats obtenus ont été validés par des simulations numériques.

Le troisième chapitre est dédié à la mise au point d'un nouveau procédé de transmission sécurisée d'information, exploitant les propriétés fondamentales des systèmes chaotiques et leur capacité de synchronisation. Une présentation rapide de différentes techniques de cryptage nous a permis de situer le contexte des cryptosystèmes chaotiques. Après examen des techniques détaillées dans la littérature, nous avons élaboré un système cryptographique chaotique reposant sur le principe de transmission à deux voies : l'envoi de deux signaux générés par l'émetteur permet de dissocier les phases de synchronisation et de cryptage/décryptage. L'étape de synchronisation étant assurée par l'un des observateurs conçus au chapitre 2, nous avons mis au point un processus pour noyer le message à transmettre dans un signal chaotique. La méthode proposée consiste à réaliser une modulation de la phase du signal chaotique, en fonction du message. L'efficacité de ce nouveau cryptosystème chaotique est testée à l'aide de différentes simulations, correspondant à la transmission d'un signal sonore, d'une image et d'un texte : le déchiffrement est excellent, lorsqu'il n'y a aucune perturbation sur la transmission. La question de la sécurité du système de transmission chaotique a été abordée à travers différents points. Le premier concerne la définition de la clé du cryptosystème. Nous avons ainsi étudié la sensibilité de l'estimation du message en fonction d'erreurs, commises au niveau du récepteur, sur la clé : les résultats obtenus indiquent qu'un récepteur non autorisé, qui ne connaît pas exactement la clé utilisée par l'émetteur, ne peut pas déchiffrer le message crypté. Le deuxième point concerne la vérification des propriétés de confusion et diffusion : les résultats obtenus montrent qu'à un message clair correspondent une infinité de messages cryptés. Par conséquent, il semble difficile d'exploiter le message crypté pour en retirer des indications sur le message original. Le dernier point de sécurité abordé consiste à tester des attaques spécifiques aux cryptosystèmes chaotiques, sous forme d'analyse spectrale. Contrairement à d'autres systèmes proposés dans la littérature, celui que nous avons mis au point n'est pas sensible à ce type d'attaque. On peut conclure de ces divers tests de sécurité que le cryptosystème proposé exploite au mieux les propriétés fondamentales des systèmes chaotiques, et le principe de leur synchronisation. L'étude de la restauration de message en présence de bruit sur le canal de transmission (du signal dévolu à la synchronisation) met en évidence le compromis entre la robustesse et la sécurité : plus la clé est grande, plus le niveau de sécurité est élevé, et plus la qualité de la restitution du message est médiocre.

Dans le quatrième et dernier chapitre, nous avons présenté un moyen de renforcer la sécurité du processus de synchronisation. Nous avons utilisé la théorie des multimodèles linéaires

pour construire une nouvelle famille de systèmes chaotiques : des multimodèles non linéaires chaotiques sont ainsi créés à partir de plusieurs modèles chaotiques (dits de base). A chaque instant, une fonction d'activation détermine l'interpolation entre les différents modèles de base. Le multimodèle chaotique résultant possède un comportement particulièrement complexe, ce qui devrait renforcer sa résistance face aux attaques (dites de reconstruction à retard). Nous avons élaboré des schémas de synchronisation à base d'observateurs spécifiques pour cette classe de systèmes. Le cas de multimodèles avec et sans retard a été envisagé. Différentes conditions suffisantes de synchronisation (asymptotique et exponentielle) ont été établies en termes de BMI et de LMI, et garantissent une reconstruction continue de l'état de l'émetteur, dans le sens où il n'y a pas de perte de synchronisation. Le premier exemple illustre le cas des multimodèles sans retard : les modèles de base choisis sont des circuits de Chua. Sur cet exemple, le tracé d'un diagramme de bifurcations montre que le multimodèle généré possède un comportement chaotique. Les résultats de synchronisation ont été validés pour cet exemple, ainsi que pour un multimodèle à retard, dont les modèles de base sont des *SCTH*. Ce dernier multimodèle a été choisi comme émetteur dans un cryptosystème chaotique reprenant le principe de cryptage par modulation de phase chaotique.

Les problèmes abordés dans ce mémoire 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 réel aboutissement de cette thèse. Comme cela a déjà été réalisé pour le circuit de Chua notamment, il faudrait construire un dispositif électronique correspondant au SCTH, et un récepteur adapté. Comme pour tout système physique, on peut supposer que les valeurs des paramètres des différents composants électroniques possèdent une part d'imprécision. Cela ouvre la voie à une réflexion sur la synchronisation des systèmes chaotiques incertains. On peut cependant noter, au vu des résultats du paragraphe 3.4.2, que la valeur de la clé ne peut pas supporter beaucoup d'imprécision.

Un autre prolongement possible concerne la robustesse au bruit de transmission. Nous avons traité au paragraphe 2.5 la robustesse de la synchronisation en présence de bruit borné sur le signal $y(t)$. L'observateur proposé constitue un moyen de garantir une borne optimale sur l'erreur d'estimation. Il a été utilisé comme récepteur du cryptosystème au paragraphe 3.5 qui traite le problème de la reconstruction du message en présence de bruit sur le canal de transmission, affectant uniquement le premier signal dévolu à la synchronisation. Des tests expérimentaux ont d'ores et déjà été réalisés sur deux ordinateurs équipés de cartes dSpace. Par ailleurs, en conservant le principe du cryptage par modulation de phase chaotique, il serait intéressant de trouver une technique de restauration de l'information qui soit également robuste au bruit.

Sur le plan théorique, nous avons volontairement laissé de côté une étude approfondie du ca-

ractère chaotique des systèmes non linéaires considérés, à savoir le SCTH et les multimodèles du chapitre 4. En effet, une étude rigoureuse sur le plan mathématique se situe au-delà de la portée de ce mémoire, et constitue un point à creuser. Cette étude pourrait servir à déterminer plus précisément l'espace des clés introduit au paragraphe 3.4.2.
Par ailleurs, nous espérons mener des tests à court terme sur la résistance des multimodèles chaotiques face aux attaques de reconstruction à retard.

Les systèmes sur lesquels nous avons porté notre attention sont des systèmes à temps continu. Nous avons laissé de côté les systèmes chaotiques à temps discret, comme les applications de Hénon, de Lozi, l'application logistique... On pourrait donc considérer une adaptation de nos travaux dans le cadre des systèmes discrets.
Enfin, et nous l'avons mentionné à plusieurs reprises, les résultats présentés dans ce mémoire peuvent être étendus à un problème général d'estimation d'état en présence d'un retard de transmission variable et inconnu, qui constitue une classe particulière de perturbations. On peut d'ores et déjà trouver des applications potentielles dans le domaine du diagnostic notamment. Cette généralisation est actuellement à l'étude.

Annexe

A Sur la stabilité des systèmes dynamiques

Sommaire

Tout au long de ce mémoire, nous utilisons des résultats largement répandus dans la littérature sur la stabilité des systèmes continus, résultats qui sont rappelés dans cette annexe.

A.1 Stabilité au sens de Lyapunov

Par définition, l'analyse de la stabilité d'un système consiste à étudier son comportement lorsqu'il est déplacé d'un point d'équilibre. Cela passe par l'analyse de la trajectoire de l'état du système lorsque son état initial est proche d'un point ou d'une trajectoire d'équilibre [Hahn 03], [Vidyasagar 93], [Parks 93]. Les principales notions de stabilité sont présentées ici, à savoir la stabilité asymptotique, la stabilité exponentielle, en relation avec la théorie de Lyapunov, et la théorie de Lyapunov-Krasovskii, qui concerne les systèmes à retard.
On considère l'ensemble des systèmes non linéaires décrits par l'équation dynamique suivante :

$$\begin{aligned} \dot{x}(t) &= f(x(t), t) \\ x(t_0) &= x_0 \end{aligned} \tag{A.1}$$

où $x(t) \in \mathbb{R}^n$ et $f : \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^n$ est continue.

Définition A.1.1 (Point d'équilibre)**.**
Un point $x_e \in \mathbb{R}^n$ est un point d'équilibre de (A.1) si $f(x_e, t) = 0$, pour tout $t \geqslant 0$. ♦

On note $\chi(t, t_0, x_0)$ la solution, à l'instant $t \geqslant t_0$ du système (A.1), de conditions initiales $x(t_0) = x_0$.

Dans ce mémoire, les propriétés de stabilité ne sont utilisées que pour analyser la dynamique des erreurs d'observation. Aussi nous restreignons-nous à l'étude de la stabilité du système (A.1) autour du point d'équilibre $x_e = 0$.

Définition A.1.2 (Stabilité)**.**
On dit que l'origine est un point d'équilibre stable (au sens de Lyapunov) si toute trajectoire de conditions initiales proches de $x_e = 0$ en t_0 reste suffisamment proche de x_e pour $t \geqslant t_0$, autrement dit, si :

$$\forall \varepsilon > 0, \quad \forall t_0 \geqslant 0, \quad \exists \delta > 0 \quad / \quad \|x_0\| < \delta \quad \Rightarrow \quad \|\chi(t, t_0, x_0)\| < \varepsilon \tag{A.2}$$

Dans le cas contraire, on dit que l'origine est instable. ♦

Définition A.1.3 (Attractivité)**.**
On dit que $x_e = 0$ est un point d'équilibre attractif pour le système (A.1) si :

$$\exists \eta > 0 \quad / \quad \forall t \geqslant t_0 \quad \|x_0\| < \eta \quad \Rightarrow \quad \lim_{t \to \infty} \chi(t, t_0, x_0) = 0 \tag{A.3}$$

Lorsque $\eta \to \infty$, on dit que l'origine est globalement attractive. ♦

La notion d'attractivité signifie que, après un certains temps et de possibles larges déviations, toute trajectoire du système convergera vers son état d'équilibre. Cependant, un système attractif n'est pas nécessairement stable, au sens de la définition A.1.2, c'est pourquoi on introduit alors la notion de stabilité asymptotique qui garantit que l'état du système converge vers son état d'équilibre sans trop s'en éloigner.

Définition A.1.4 (Stabilité asymptotique)**.**
On dit que l'origine est un point d'équilibre [globalement] asymptotiquement stable si elle est stable et [globalement] attractive. ♦

Les définitions de stabilité uniforme, d'attractivité uniforme et stabilité asymptotique (globalement) uniforme se déduisent facilement des définitions précédentes : il suffit que les bornes δ et η ne dépendent pas de t_0.
Dans l'équation (A.3), si on remplace la convergence asymptotique par une convergence exponentielle, on obtient une notion plus forte que la stabilité asymptotique.

Définition A.1.5 (Stabilité exponentielle)**.**
On dit que l'origine est un point d'équilibre localement exponentiellement stable du système (A.1) si :

$$\exists \alpha, \beta > 0 \quad / \quad \forall t \geqslant t_0, \quad \forall x_0 \in \mathcal{B}(0,r) \quad \|\chi(t, t_0, x_0)\| \leqslant \alpha e^{-\beta(t-t_0)} \tag{A.4}$$

où $\mathcal{B}(0,r)$ est la boule ouverte de centre zéro, de rayon $r > 0$.
Lorsque $\mathcal{B}(0,r) = \mathbb{R}^n$, on parle de stabilité exponentielle globale. ♦

Pour contourner le problème de la résolution explicite de l'équation différentielle $\dot{x}(t) = f(x(t), t)$, on a recours à la théorie de Lyapunov.

A.2 Méthode directe de Lyapunov

La philosophie de cette méthode s'appuie sur une observation fondamentale de la physique : si l'énergie totale d'un système est dissipée de manière continue alors le système devra rejoindre finalement un point d'équilibre. On pourra donc conclure à la stabilité d'un système par l'examen de la variation d'une fonction scalaire V, représentant l'énergie totale.

Définition A.2.1.
Soit $V(x,t) : \mathbb{R}^n \times \mathbb{R}^+ \to \mathbb{R}^+$ une fonction continue. V est dite propre définie positive si :
(i) $\forall t \in \mathbb{R}^+, \quad \forall x \in \mathbb{R}^n \setminus \{0\}, \quad V(x,t) > 0$
(ii) $\forall t \in \mathbb{R}^+, \quad V(x,t) = 0 \quad \Rightarrow x = 0$
(iii) $\forall t \in \mathbb{R}^+, \quad \lim_{\|x\| \to \infty} V = \infty$

♦

Définition A.2.2 (Fonction de Lyapunov)**.**
Une fonction $V(x,t)$ continûment différentiable en ses arguments est une fonction de Lyapunov locale (respectivement globale) au sens large pour le système (A.1) si elle est propre, définie positive et s'il existe un voisinage de l'origine $\mathcal{V}_0$ tel que :

$$\forall x \in \mathcal{V}_0 (\text{respectivement } x \in \mathbb{R}^n, \quad \dot{V}(x,t) = \frac{\partial V}{\partial t}(x,t) + \left[\frac{\partial V(x,t)}{\partial x}\right]' f(x,t) \leqslant 0 \tag{A.5}$$

Si $\dot{V}(x,t) < 0$, V est appelée fonction de Lyapunov au sens strict pour (A.1). ♦

La méthode directe de Lyapunov donne une condition suffisante garantissant la stabilité du point d'équilibre 0.

Définition A.2.3 (Méthode directe de Lyapunov)**.**
Si le système différentiel (A.1) admet une fonction de Lyapunov locale au sens large (respectivement au sens strict), alors l'origine est un point d'équilibre localement stable (respectivement asymptotiquement stable).
Si la fonction de Lyapunov est globale, on parle alors de stabilité globale (respectivement de stabilité asymptotique globale). ♦

Définition A.2.4.
L'origine de (A.1) est localement exponentiellement stable s'il existe des constantes $\alpha, \beta, \gamma > 0$, un entier $p \geqslant 0$, et une fonction de Lyapunov locale $V(x,t) : \mathcal{V}_0 \times \mathbb{R}^+ \to \mathbb{R}^+$ tels que, pour tout $x \in \mathcal{V}_0$:
(i) $\alpha\|x\|^p \leqslant V(x,t) \leqslant \beta\|x\|^p$
(ii) $\dot{V}(x,t) < -\gamma V(x,t)$
Si $\mathcal{V}_0 = \mathbb{R}^n$, l'origine est globalement exponentiellement stable. ♦

Il n'existe, en général (sauf dans le cas linéaire), aucune méthode systématique pour trouver une fonction candidate de Lyapunov. Il est toutefois assez classique d'utiliser une fonction de Lyapunov quadratique, de type $V(x,t) = x^T(t)Px(t)$, où la matrice P est symétrique et définie positive. Ce choix présente l'avantage d'être simple à mettre en oeuvre. Cependant, il induit généralement des conditions très conservatives. Par ailleurs, si aucune fonction convenable n'est trouvée, on ne peut rien dire quant à la stabilité éventuelle du point d'équilibre.

A.3 Cas des systèmes à retard

Dans le cas des systèmes à retard, la méthode de Lyapunov a été généralisée par Krasovskii [Krasovskii 63]. Les différentes méthodes élaborée depuis sont résumées dans [Kharitonov 99], [Richard 03].
On considère les systèmes dont le modèle dynamique est de la forme :

$$\dot{x} = f(x, x_\tau, t) \tag{A.6}$$

On suppose que l'origine est un point d'équilibre du système (A.6). Les deux propositions suivantes établissent des conditions de stabilité asymptotique et exponentielle de cet équilibre.

Proposition A.3.1 ([Richard 03])**.** *On suppose que la fonction $f(.)$ prend des valeurs bornées sur des ensembles bornés. L'origine du système* (A.6) *est asymptotiquement stable s'il existe une fonctionnelle $V(x, x_\tau)$ (appelée fonctionnelle de Lyapunov-Krasovskii) telle que*
– *V est définie positive et décroissante ;*
– *il existe des fonctions u, et v définies positives vérifiant :*

$$u(x(t)) \leqslant V(x, x_\tau(t)) \leqslant v(max_{\theta\in[-\tau,0]}x(\theta)) \tag{A.7}$$

– *la dérivée de V le long des trajectoires de* (A.6) *est définie négative sur un voisinage de l'origine.*

▲

Proposition A.3.2 ([Kharitonov 99])**.** *L'origine du système* (A.6) *est exponentiellement stable si et seulement s'il existe une fonctionnelle $V(x, x_\tau)$ et des réels strictement positifs α_1, α_2 et β tels que*

$$\alpha_1\|x(t)\|^2 \leqslant V(x, x_\tau) \leqslant \alpha_2 \max_{\theta\in[-\tau,0]} \|x(\theta)\|^2 \tag{A.8a}$$

$$\dot{V}(x, x_\tau) \leqslant -\beta\|x(t)\|^2 \tag{A.8b}$$

▲

Comme dans le cas des systèmes dynamiques sans retard, on peut exhiber des fonctionnelles de Lyapunov-Krasovskii "classiques" :

$$\begin{aligned} V_1(x, x_\tau) &= x^T(t)Px(t) \\ V_2(x, x_\tau) &= x^T(t)\int_{-\tau}^{0} Qx(t+\theta)d\theta \\ V_3(x, x_\tau) &= \int_{-\tau}^{0} x^T(t+\theta)Sx(t+\theta)d\theta \end{aligned} \tag{A.9}$$

Annexe

B

Sur les systèmes chaotiques

Sommaire

Cette annexe est dédiée aux systèmes chaotiques, dont les propriétés intrinsèques sont exploitées dans les schémas de cryptographie considérés dans ce mémoire. Une étude approfondie du chaos dépassant largement le cadre de ce mémoire, nous nous contentons de définir brièvement la notion de chaos. Quelques attracteurs célèbres sont présentés ensuite.

B.1 Caractérisation du chaos

« Une cause très petite, et qui nous échappe, détermine un effet considérable que nous ne pouvons pas ne pas voir, et alors nous disons que cet effet est dû au hasard. Si nous connaissions exactement les lois de la Nature et la situation de l'Univers à l'instant initial, nous pourrions prédire la situation de ce même Univers à l'instant ultérieur. Mais, lors même que les lois naturelles n'auraient plus de secret pour nous, nous ne pourrions connaître la situation initiale qu'approximativement. Si cela nous permet de prévoir la situation ultérieure avec la même approximation, c'est tout ce qu'il nous faut, nous disons que le phénomène a été prévu, qu'il est régi par des lois ; mais il n'en est pas toujours ainsi, il peut arriver que de petites différences dans les conditions initiales en engendrent de très grandes dans les phénomènes finaux ; une petite erreur sur les premières produirait une erreur énorme sur les derniers. La prédiction devient impossible et nous avons le phénomène fortuit. »

Henri Poincaré, 1908

B.1.1 Définition

Il est très délicat de définir ce qu'est un système chaotique, étant donné qu'il n'existe pas une définition précise. En pratique, on peut dire qu'un système chaotique a un comportement borné en régime permanent, qui ne correspond pas à un point d'équilibre, qu'il n'est ni périodique, ni quasi-périodique. Dans ce mémoire, nous nous intéressons uniquement aux systèmes continus : il est généralement admis que le chaos au sens de Shil'nikov [Silva 93] est la référence. Parmi les caractéristiques principales permettant d'évoquer un comportement chaotique, on peut retenir les trois suivantes :
(i) un système chaotique est un système déterministe ;
(ii) il exhibe une extrême sensibilité aux conditions initiales (SCI) ;
(iii) il présente un comportement asymptotique apériodique.
La sensibilité aux conditions initiales est plus connue sous le nom d'*effet papillon*. Étant données deux conditions initiales arbitrairement proches, les trajectoires issues de ces conditions initiales divergent, à une vitesse caractéristique du système, jusqu'à ce qu'elles deviennent non corrélées. Ce phénomène est illustré par la figure B.1 : il s'agit de deux trajectoires de l'état x_1 du *SCTH* (2.11), avec une différence de $0,01\%$ sur la première composante de l'état initial. Cette propriété a une importance capitale : elle rend les systèmes chaotiques imprévisibles. En effet, les imprécisions sur les conditions initiales, les erreurs de mesure, le bruit altèrent de manière signi-

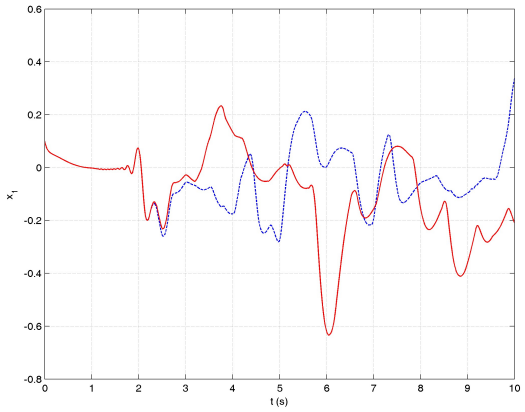


FIG. B.1 - *Sensibilité aux conditions initiales*

ficative le comportement macroscopique du système chaotique. Une autre formulation consiste à dire que les observations sont plus précises que les prédictions pour un tel système. Cette constatation est à l'origine du caractère prétendument aléatoire des signaux chaotiques.

En général, les trajectoires d'un système dynamique chaotique sont attirées vers un attracteur étrange (néanmoins, il existe des attracteurs chaotiques qui ne sont pas étranges - par exemple, l'application logistique pour certaines valeurs de paramètres - et des attracteurs étranges non chaotiques - comme l'ensemble de Cantor). Dans le cadre de ce mémoire, on assimilera les deux types d'attracteurs. Un attracteur étrange est caractérisé par :

(i) un volume nul ;
(ii) une séparation exponentiellement rapide de trajectoires initialement proches ;
(iii) une dimension souvent fractale (*i.e.* non entière)
(iv) l'existence d'une mesure invariante permettant de définir des grandeurs moyennes. Cette mesure est liée à la notion d'ergodicité : les caractéristiques macroscopiques de l'attracteur ne dépendent pas des conditions initiales. Un grand nombre d'expériences possédant des conditions initiales différentes ne change pas la mesure.

La naissance d'un attracteur étrange est liée à l'existence de deux processus, à savoir l'*étirement*, responsable de l'instabilité et de la SCI, et le *repliement*, responsable du côté étrange, fractal de l'attracteur.

B.1.2 Exposants de Lyapunov

Les exposants de Lyapunov [Wiggins 90] généralisent la notion de valeurs propres pour les systèmes non linéaires. Ils quantifient la divergence exponentielle (ou la convergence) de trajectoires proches à un moment donné dans l'attracteur d'un système dynamique. Dans ce paragraphe, les définitions sont données pour les systèmes continus, de dimension finie, dont le

modèle dynamique (d'ordre n) est le suivant :

$$\dot{x}(t) = f(x(t)) \tag{B.1}$$

On considère une orbite de l'attracteur $x(t)$, de condition initiale $x(0) = x_0$ et une sphère infinitésimale de dimension n de centre x_0 et de rayon r. Lorsque le système évolue jusqu'à $t > 0$, la sphère a été déformée en un ellipsoïde d'axes principaux p_i (classés selon l'ordre suivant : $p_1 \geqslant p_2 \geqslant \ldots \geqslant p_n$). La taille de p_i, par rapport à r, représente la divergence ou la convergence de trajectoires de conditions initiales proches de x_0. Les taux de croissance ou décroissance de ces axes principaux sont donnés par $\ln(p_i/r)/t$. Les exposants de Lyapunov correspondent aux valeurs limites de ces taux de croissance ou décroissance. Mathématiquement, on peut exprimer ce raisonnement comme suit.
On note dans la suite $f(x(t)) = f_t(x(0))$ pour préciser la dépendance dans l'état initial $x(0)$.
On considère un état initial proche de $x(0)$, avec ε petit, et on écrit le développement limité :

$$f_t(x(0) + \varepsilon) = f_t(x(0)) + J_t\varepsilon + \bigcirc(\|\varepsilon\|^2) \tag{B.2}$$

où J_t est la matrice jacobienne de f à l'origine : $J_t = \dfrac{\partial f_t}{\partial x}(x(0))$.
On peut montrer que la matrice limite

$$\Lambda_{x(0)} = \lim_{t\to\infty} \left(J_t^T J_t\right)^{\frac{1}{2t}} \tag{B.3}$$

existe et ne dépend pas de $x(0)$.

Définition B.1.1 (Exposants de Lyapunov)**.** Les logarithmes λ_i des valeurs propres de la matrice $\Lambda_{x(0)}$ sont appelés exposants de Lyapunov du système (B.1). ♦

Voici quelques propriétés des exposants de Lyapunov :
- par définition, les exposants de Lyapunov quantifient les expansions ($\lambda_i > 0$) ou contractions ($\lambda_i < 0$) dans les directions propres du flux ;
- la somme des exposants de Lyapunov représente le taux moyen d'expansion ou de contraction du volume de l'espace de phase autour de l'attracteur ; par conséquent, on doit avoir $\sum_i \lambda_i < 0$;
- les exposants de Lyapunov permettent de caractériser le régime permanent des systèmes non chaotiques :
  - pour un point d'équilibre asymptotiquement stable, $\lambda_i < 0$ pour tout $i = 1, n$;
  - pour un cycle limite asymptotiquement stable, $\lambda_1 = 0$ et $\lambda_i < 0$ pour $i = 2, n$;
  - pour un tore de dimension K, $\lambda_1 = \ldots = \lambda_K = 0$ et $\lambda_i < 0$ pour $i = K + 1, n$.

  On peut souligner qu'un attracteur non chaotique ne possède pas d'exposant de Lyapunov positif.

– Si on se réfère au point précédent, ce qui distingue un attracteur étrange d'un attracteur non chaotique est l'existence d'un exposant de Lyapunov positif. Comme la somme des exposants doit toujours être négative, en dimension trois un système chaotique possède donc un exposant de Lyapunov nul, un positif, et un négatif (de valeur absolue plus grande que l'exposant positif).

Il existe des algorithmes numériques pour calculer les exposants de Lyapunov d'un système dynamique, à partir de son modèle dynamique, notamment celui de Wolf [Wolf 85], [Parker 89]. Ces algorithmes nécessitent le calcul de la jacobienne de f, ce qui n'est pas possible avec des fonctions linéaires par morceaux, comme pour le circuit de Chua. Par ailleurs, ces calculs s'avèrent beaucoup plus délicats lorsqu'il s'agit de systèmes à retard, donc de dimension infinie, comme le *SCTH*. Cette classe de systèmes a longuement été étudiée dans l'article de Farmer [Farmer 82].

En pratique, la vérification de quelques propriétés d'un système dynamique suffit pour pouvoir le considérer comme chaotique :
– vérifier la SCI ;
– tracer les trajectoires des états et leur spectre de puissance ;
– tracer différents attracteurs ;
– tracer un diagramme de bifurcations ;
– calculer les exposants de Lyapunov.

B.2 Exemples de systèmes chaotiques

La sensibilité aux conditions initiales a été découverte dès la fin du XIX^{ème} siècle par Henri Poincaré, à l'origine de la célèbre phrase (La science et l'hypothèse, 1908) : « Un dixième de degré en plus ou en moins en un point quelconque (...), un cyclone éclate ici et non pas là. » Cependant, la théorie du chaos ne s'est véritablement développée qu'à partir des années 1960. Les systèmes chaotiques célèbres sont peu nombreux. Nous allons détailler les trois principaux systèmes à temps continu, à savoir les systèmes de Lorenz et Rössler, et le circuit de Chua.

B.2.1 Système de Lorenz

Les travaux du savant américain Edward Lorenz (né en 1917), professeur de mathématiques au MIT et passionné de météorologie, ont changé le cours de la théorie des mathématiques. Dans les années 1960, les scientifiques pensaient que le monde était régi par des lois, que l'univers était réglé comme une horloge, et par conséquent, que l'avenir devenait prévisible, sous réserve de pouvoir effectuer des calculs. La météorologie consiste à prévoir le déplacement de grandes masses d'air, qui montent sous l'effet de la chaleur dégagée par la terre et les océans, et qui descendent lorsqu'elles sont refroidies en altitude. Le problème majeur de l'étude des phénomènes de convection résidait dans les calculs : soit les savants établissaient des modèles précis à l'aide

des lois d'écoulement des fluides et des lois de la convection, mais qui comportaient des milliers de variables, soit ils simplifiaient les équations, en privilégiant la compréhension du processus, au détriment de prévisions exactes. Lorenz a choisi cette seconde voie pour présenter un modèle très simplifié, auquel il a donné son nom :

$$\begin{cases} \dot{x}_1 = -\sigma x_1 + \sigma x_2 \\ \dot{x}_2 = \gamma x_1 - x_2 - x_1 x_3 \\ \dot{x}_3 = x_1 x_2 - \beta x_3 \end{cases} \tag{B.4}$$

L'ordinateur a joué un grand rôle dans la découverte de Lorenz. Cet ordinateur, un Royal McBee LGP-300, était muni de tubes à vide et occupait la moitié d'une pièce. Le temps de calcul étant très long, Lorenz décide de diminuer la précision des conditions initiales (de l'ordre de un pour mille) avant de lancer la même simulation, pour s'assurer de certains résultats. Après examen des nouveaux résultats, Lorenz pense que son ordinateur a flanché une nouvelle fois : les deux jeux de données de sortie, semblables au début, divergent très vite, correspondant à des interprétations météorologiques aussi éloignées qu'une tempête sur le pôle Nord et une sécheresse sous les tropiques. Pourtant, ces deux résultats provenaient du même système très simple, de conditions initiales extrêmement proches : cette divergence était nécessairement due à la présence de termes non linéaires dans les équations du modèle. Lorenz venait de mettre en évidence une propriété de certains systèmes non linéaires : d'infimes différences dans les conditions initiales finissaient 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 régi par des lois rigoureuses et parfaitement déterministes, que toute prévision de leur comportement est impossible.
En 1972, Lorenz fait une conférence à l'American Association for the Advancement of Science intitulée (malgré lui) : « Prédictibilité : le battement d'ailes d'un papillon au Brésil peut-il provoquer une tempête au Texas ? ». Cette métaphore, qui n'a pas été voulue par Lorenz, est devenue emblématique du phénomène de SCI. Elle est souvent interprétée à tort de façon causale : ce serait le battement d'aile du papillon qui déclencherait la tempête. A la suite de cette conférence, Lorenz précise sa pensée en écrivant : « De crainte que le seul fait de demander, suivant le titre de cet article, "un battement d'aile de papillon au Brésil peut-il déclencher une tornade au Texas ?", fasse douter de mon sérieux, sans même parler d'une réponse affirmative, je mettrai cette question en perspective en avançant les deux propositions suivantes :

– si un seul battement d'ailes d'un papillon peut avoir pour effet le déclenchement d'une tornade, alors il en va ainsi également de tous les battements précédents et subséquents de ses ailes, comme de ceux de millions d'autres papillons, pour ne pas mentionner les activités d'innombrables créatures plus puissantes, en particulier de notre propre espèce ;
– si le battement d'ailes d'un papillon peut déclencher une tornade, il peut aussi l'empêcher. »

L'attracteur de Lorenz est tracé à la figure B.2, les paramètres étant fixés aux valeurs suivantes : $\sigma = 10$, $\gamma = 28$, $\beta = 8/3$. Les conditions initiales sont $x_0 = \begin{pmatrix} 0,1 & 0,1 & 0,1 \end{pmatrix}$, et l'intégration numérique est réalisée par une méthode de Runge-Kutta d'ordre quatre, de pas $0,01$ s.

La figure B.3 montre les trajectoires des trois états du système (B.4), ainsi que leur densité

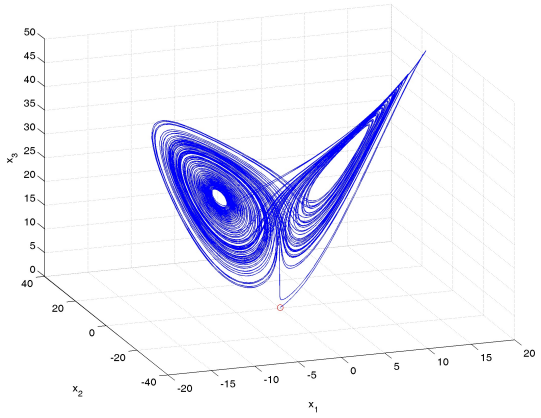


FIG. B.2 - *Attracteur de Lorenz*

spectrale de puissance.

B.2.2 Système de Rössler

En 1976, un biochimiste allemand, Otto Rössler (né en 1940) a essayé de construire un attracteur chaotique semblable à celui de Lorenz, mais plus facile à analyser. Il a tenté de concevoir le système le plus simple possible, capable de générer du chaos. Le modèle dynamique résultant est donné ci-dessous :

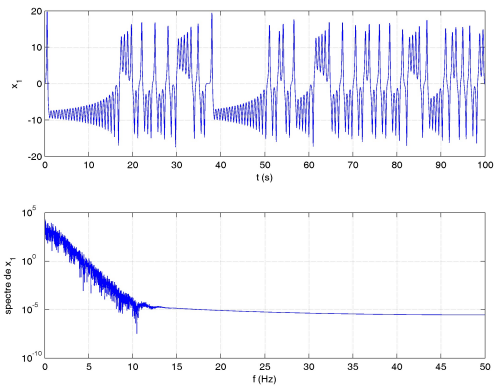
$$\begin{cases} \dot{x}_1 = -x_2 - x_3 \\ \dot{x}_2 = x_1 + ax_2 + 0,01x_1 \ln(x_3) \\ \dot{x}_3 = c + x_3(x_1 - b) \end{cases} \tag{B.5}$$

L'attracteur étudié par Rössler est tracé à la figure B.4, les paramètres étant fixés aux valeurs suivantes : $a = 0,2$, $b = 5,7$, $c = 0,2$. Les conditions initiales sont $x_0 = \begin{pmatrix} 0,01 & 0,01 & 0,01 \end{pmatrix}$

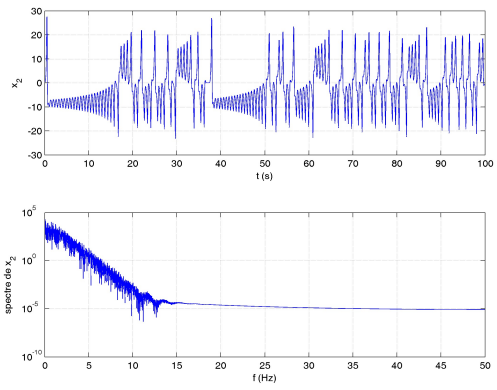
La figure B.5 montre les trajectoires des trois états du système (B.5), ainsi que leur densité spectrale de puissance.

B.2.3 Circuit de Chua

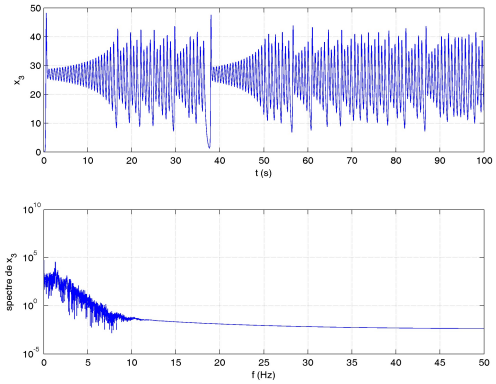
Le circuit de Chua, présenté dans les références [Chua 93a], [Chua 93b], est le troisième et dernier système chaotique que nous détaillons dans cette annexe. Il est devenu célèbre au milieu des années 1980, car il constitue un générateur de chaos électronique assez simple. Il comporte deux résistances, deux condensateurs, une inductance, et une résistance non linéaire, *appelée diode de Chua*, voir figure B.6. Le modèle dynamique correspondant est le suivant :



(a) État x_1



(b) État x_2



(c) État x_3

FIG. B.3 - *Trajectoires et spectres de puissance des trois états du système de Lorenz*

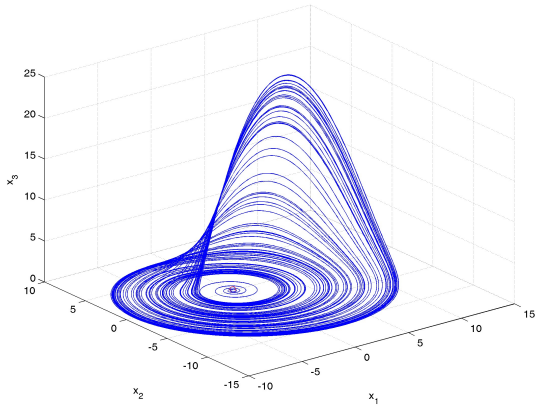
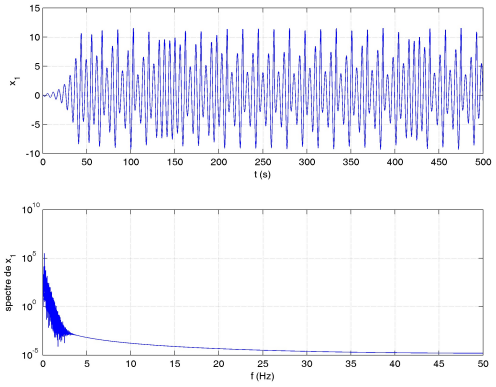
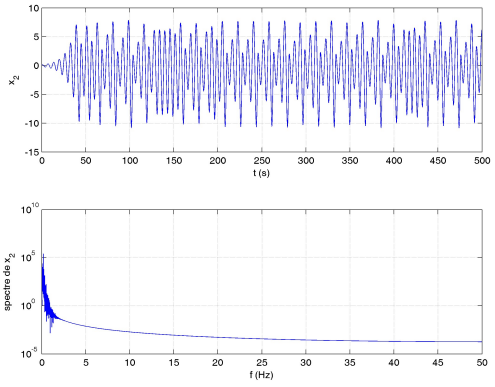


FIG. B.4 - *Attracteur de Rössler*

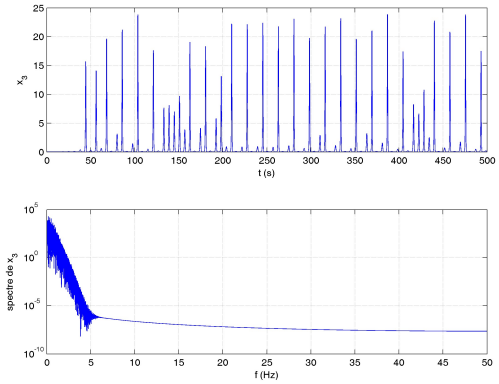
$$\begin{cases} \dot{v}_1 &= \dfrac{1}{C_0}\left(G(v_2 - v_1) - f(v_1)\right) \\ \dot{v}_2 &= \dfrac{1}{C_1}\left(G(v_1 - v_2) + i_3\right) \\ \dot{i}_3 &= -\dfrac{1}{L}\left(v_2 + R_0 v_3\right) \end{cases} \tag{B.6}$$



(a) État x_1



(b) État x_2



(c) État x_3

FIG. B.5 - *Trajectoires et spectres de puissance des trois états du système de Rössler*

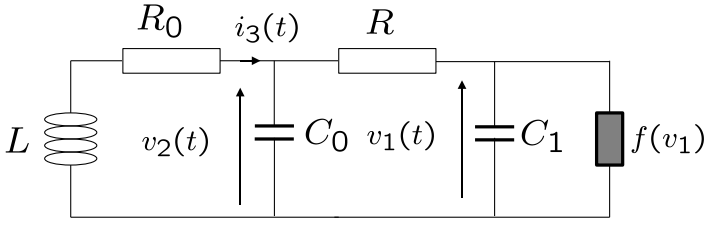


FIG. B.6 - *Circuit de Chua*

avec $x = \begin{pmatrix} v_1 \\ v_2 \\ i_3 \end{pmatrix}$, et $G = \frac{1}{R}$.

La fonction f, représentée à la figure B.7, a pour expression :

$$f(v_1) = G_b v_1 + 0.5(G_a - G_b)(|v_1 + E| - |v_1 - E|) \tag{B.7}$$

On définit le changement de variables suivant : $x = \frac{v_1}{E}$, $y = \frac{v_2}{E}$, $z = \frac{R}{E} i_3$, $\alpha = \frac{C_1}{C_0}$, $\beta = \frac{R^2 C_1}{L}$,

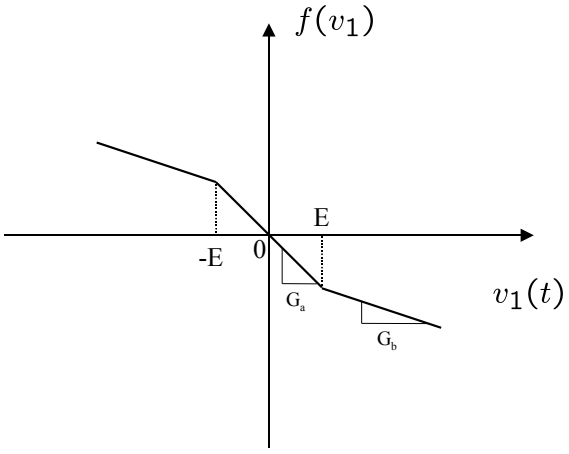


FIG. B.7 - *Caractéristique de la diode de Chua*

$\gamma = \frac{RR_0C_1}{L}$, $a = RG_a$, $b = RG_b$. L'échelle de temps est changée : t est remplacé par $\tau = \frac{t}{RC_1}$. Le modèle (B.6) prend alors la forme suivante, appelée modèle sans dimension du circuit de Chua :

$$\begin{cases} \dot{x} &= -\alpha x + \alpha y - \alpha f(x) \\ \dot{y} &= x - y + z \\ \dot{z} &= -\beta y - \gamma z \end{cases} \tag{B.8}$$

Pour les valeurs de paramètres suivantes : $\alpha = 9$, $\beta = 14$, $\gamma = 0$, $a = -1,14$, $b = -0,7$, le système (B.8) exhibe un attracteur chaotique à double spirale, caractéristique du circuit de Chua, représenté à la figure B.8 La figure B.9 montre les trajectoires des trois états du système

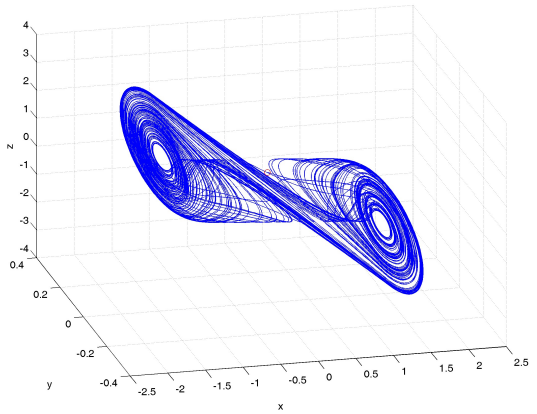
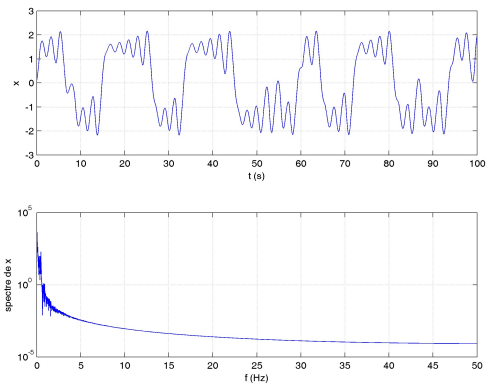
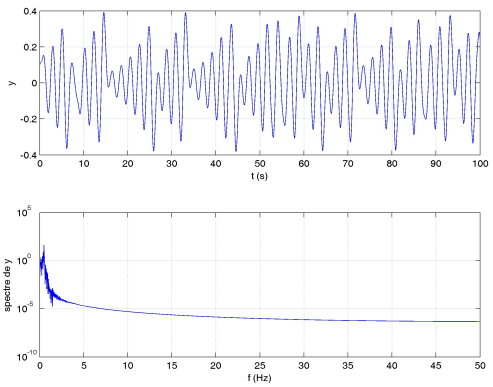


FIG. B.8 - *Attracteur de Chua à double spirale*

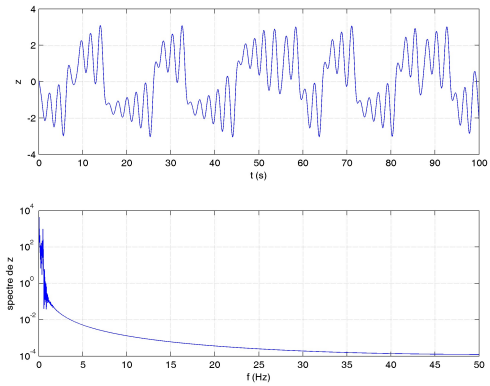
(B.8), ainsi que leur densité spectrale de puissance.



(a) État x_1



(b) État x_2



(c) État x_3

FIG. B.9 - *Trajectoires et spectres de puissance des trois états du circuit de Chua*

Annexe

C Sur les inégalités matricielles linéaires et bilinéaires

Sommaire

Nous donnons dans cette annexe quelques rappels de techniques qui sont utilisées dans ce mémoire pour résoudre des inégalités matricielles (linéaires ou bilinéaires).

C.1 Formulation du problème

Définition C.1.1. Une LMI est une inégalité matricielle de la forme

$$\mathcal{A}(x) = \sum_{i=1}^{n} x_i A_i + B > 0 \tag{C.1}$$

où les matrices A_i, $i = 1, n$ et B sont des matrices symétriques de dimension n, et x est un vecteur de $\mathbb{R}^n$. ♦

On peut remarquer que l'ensemble $\{x \in \mathbb{R}^n / \mathcal{A}(x) > 0\}$ est un ensemble convexe. C'est pourquoi une LMI peut être considérée comme une contrainte convexe.
Dans ce mémoire, nous devons résoudre à plusieurs reprises un des problèmes d'optimisation convexe exprimés sous la forme de LMI, à savoir le *problème de réalisabilité*.

Définition C.1.2 (Problème de réalisabilité)**.** Il s'agit de trouver un vecteur x tel que la contrainte $\mathcal{A}(x) > 0$ soit satisfaite. Ce problème peut être résolu en cherchant le vecteur x minimisant le scalaire t de telle sorte que :

$$-\mathcal{A}(x) < tI_n \tag{C.2}$$

Si la valeur minimale de t est négative, alors le problème (C.1) est réalisable.

Il existe plusieurs algorithmes de résolution numérique de telles LMI. La technique que nous avons utilisée pour résoudre nos problèmes est celle exploitée par le logiciel MatLab (plus précisément la fonctions *feasp*), à savoir la méthode projective détaillée dans l'article [Nemirovskii 94]. La solution exhibée par MatLab est une solution particulière de la LMI à résoudre.

C.2 Complément de Schur

Le complément de Schur est l'exemple le plus classique de contraintes de type LMI rencontré tout au long de ce mémoire.

Lemme C.2.1 (Complément de Schur [Boyd 94])**.** *Soient trois matrices $Q(x) = Q(x)^T$, $R(x) = R(x)^T$ et $S(x)$, affines par rapport à la variable x. Les LMI suivantes sont équivalentes :*

i) $\begin{pmatrix} Q(x) & S(x) \\ S(x)^T & R(x) \end{pmatrix} < 0$

ii) $R(x) > 0, \quad Q(x) - S(x)R(x)^{-1}S(x)^T > 0$ ■

C.3 Inégalités matricielles bilinéaires

Les inégalités matricielles bilinéaires (ou BMI selon l'acronyme anglo-saxon) représentent une généralisation des LMI.

Définition C.3.1. Une BMI est une contrainte de la forme :

$$\mathcal{A}(x) = \sum_{i=1}^{n} x_i A_i + \sum_{i=1}^{n} \sum_{j=1}^{n} x_i x_j A_{ij} + B > 0 \tag{C.3}$$

où les matrices A_i, A_{ij}, $i, j = 1, n$ et B sont des matrices symétriques de dimension n, et x est un vecteur de $\mathbb{R}^n$. ♦

Les BMI ne sont pas des problèmes convexes, et peuvent donc avoir plusieurs solutions locales. Les techniques d'optimisation convexe développées pour résoudre des LMI ne peuvent pas être utilisées pour résoudre des BMI.
Tout au long de ce mémoire, nous avons utilisé une technique qui permet de résoudre des BMI dans certains cas, sous la forme d'un changement de variable approprié. Il s'agit d'une astuce mathématique, qui consiste à introduire une nouvelle variable à la place du produit de deux variables de la BMI, ce qui permet de linéariser le problème. L'un des facteurs du produit doit être inversible, c'est une condition nécessaire pour pouvoir appliquer un tel changement de variables.

Bibliographie

[Abarbanel 93] H.D.I. Abarbanel, R. Brown, J.J. Sidorowich & L.Sh. Tsimring. *The analysis of observed data in physical systems*. Rev. Mod. Phys., vol. 65, no. 4, pages 1331–1392, 1993.

[Ahan 03] M. Ahan, X. Wang, X. Gong, G.W. Wei & C.-H. Lai. *Complete synchronization and generalized synchronization of one-way coupled time-delay systems*. Physical Review E, vol. 68, no. 3, page 036208, 2003.

[Alaoui 00] M.A. Aziz Alaoui. *Multispiral chaos*. In Proceedings of the 2nd IEEE Conference on Control of Oscillations and Chaos, vol. 1, pages 88–91, 2000.

[Alessandri 04] A. Alessandri. *Observer design for nonlinear systems by using input-to-state stability*. In Proceedings of the 43rd IEEE Conference on Decision and Control, Atlantis, Paradise Island, Bahamas, 2004.

[Alligood 96] K.T. Alligood, T.D. Sauer & J.A. Yorke. Chaos : An introduction to dynamical systems. Springer, 1996.

[Alvarez-Ramirez 01] J. Alvarez-Ramirez, H. Puebla & I. Cervantes. *Convergence rate of observer-based approach for chaotic synchronization*. Physics Letters A, vol. 289, pages 193–198, 2001.

[Alvarez 04] G. Alvarez, F. Montoya, M. Romera & G. Pastor. *Breaking parameter modulated chaotic secure communication system*. Chaos, Solitons and Fractals, vol. 21, no. 4, pages 783–787, 2004.

[Alvarez 05] G. Alvarez, L. Hernández, J. Muñoz, F. Montoya & S. Li. *Security analysis of communication system based on the synchronization of different order chaotic systems*. Physics Letters A, vol. 345, no. 4, pages 245–250, 2005.

[Alvarez 06a] G. Alvarez & S. Li. *Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems*. International Journal of Bifurcation and Chaos, vol. 16, no. 8, pages 2129–2151, 2006.

[Álvarez 06b] Gonzalo Álvarez & Shujun Li. *Some basic cryptographic requirements for chaos-based cryptosystems*. accepted by International Journal of Bifurcation and Chaos in May 2005, tentatively scheduled for publication in vol. 16, no. 7, 2006, preprint available online at `http://www.hooklee.com/pub.html`, 2006.

[Arcak 01] M. Arcak & P. Kokotovic. *Nonlinear observer : a circle criterion design and robustness analysis*. Automatica, vol. 37, no. 12, pages 1923–1930, 2001.

[Aubry 99] D. Aubry. *Contribution à la synthèse d'observateurs pour les systèmes non linéaires*. Thèse, Université Henri Poincaré - Nancy I, 1999.

[Aziz-Alaoui 06] M.A. Aziz-Alaoui. *Synchronization of chaos*. Encyclopedia of Mathematical Physics, vol. 5, pages 213–226, 2006.

[Baumann 86] W.T. Baumann & W.J. Rugh. *Feedback control of nonlinear systems by extended linearization*. IEEE Transactions on Automatic Control, vol. 31, no. 1, pages 40–46, 1986.

[Besançon 04] G. Besançon, Q. Zhang & H. Hammouri. *High-gain observer based state and parameter estimation in nonlinear systems*. In Proceedings of NOLCOS, IFAC Symposium on Nonlinear Control Systems, Stuttgart, Germany, 2004.

[Bestle 83] D. Bestle & M. Zeitz. *Canonical form observer design for nonlinear time-variable systems*. International Journal of Control, vol. 38, pages 419–431, 1983.

[Bhattacharyya 78] S.P. Bhattacharyya. *Observer design for linear systems with unknown inputs*. IEEE Transactions on Automatic Control, vol. 23, pages 483–484, 1978.

[Biagiola 04] S.I. Biagiola & J. L. Figueroa. *A high gain nonlinear observer : application to the control of an unstable nonlinear process*. Comp. Chem. Eng., vol. 28, pages 1881–1898, 2004.

[Boccaletti 02] S. Boccaletti, J. Kurths, G. Osipov, D.L. Valladares & C.S. Zhou. *The synchronization of chaotic systems*. Physics Reports, vol. 366, pages 1–101, 2002.

[Boutayeb 95] M. Boutayeb & M. Darouach. *Observers design for non linear descriptor systems*. In Proceedings of the 34th IEEE Conference on Decision and Control, New Orleans, Louisiana, USA, 1995.

[Boutayeb 02] M. Boutayeb, M. Darouach & H. Rafaralahy. *Generalized state-space observers for chaotic synchronization and secure communication*. IEEE Transactions on Circuits and Systems I, vol. 49, no. 3, pages 345–349, 2002.

[Boyd 94] S. Boyd, L. ElGhaoui, E. Feron & V. Balakrishnan. Linear matrix inequalities in systems and control theory. SIAM, Phildelphia, PA, 1994.

[Busawon 99] K.K. Busawon & M. Saif. *A state observer for nonlinear systems*. IEEE Transactions on Automatic Control, vol. 44, no. 11, pages 2098–2103, 1999.

[Carroll 91] T.L. Carroll & L.M. Pecora. *Synchronizing chaotic circuits*. IEEE Transactions on Circuits and Systems, vol. 38, no. 4, pages 453–456, 1991.

[Carroll 92] T.L. Carroll & L.M. Pecora. *A circuit for studying the synchronization of chaotic systems*. International Journal of Bifurcation and Chaos, vol. 2, pages 659–667, 1992.

[Celikovský 05] S. Celikovský & G. Chen. *Secure synchronization of a class of chaotic systems from a nonlinear observer approach*. IEEE Transactions on Automatic Control, vol. 50, no. 1, pages 76–82, 2005.

[Chadli 02] M. Chadli. *Stabilité et commande de systèmes décrits par des mulitmodèles*. Thèse, Institut National Polytechnique de Lorraine, 2002.

[Chen 93] G. Chen. Approximate kalman filtering. World Scientific Series in Approximations and Decompositions, 1993.

[Chen 03] J.Y. Chen, K.W. Wong & L.M. Cheng. *A secure communication scheme based on the phase synchronization of chaotic systems*. Chaos, vol. 13, no. 2, pages 508–514, 2003.

[Chen 05] M. Chen, D. Zhou & Y. Shang. *A new observer-based synchronization scheme for private communication*. Chaos, Solitons and Fractals, vol. 24, pages 1025–1030, 2005.

[Cherrier 02] E. Cherrier, M. Boutayeb & J. Ragot. *State estimation of uncertain parameter systems. Approach by intervals*. In 17th IAR, Annual Meeting, Grenoble, France, 2002.

[Cherrier 03a] E. Cherrier, M. Boutayeb & J. Ragot. *Estimation des bornes de l'état d'un système incertain. Approche par intervalles*. In JDA'03 "Journées Doctorales d'Automatique", Valenciennes, France, 2003.

[Cherrier 03b] E. Cherrier, M. Boutayeb & J. Ragot. *Evaluation des bornes d'un système incertain. Approche par intervalles*. JESA, Journal Européen des Systèmes Automatisés, numéro spécial : "Application des outils de calculs ensemblistes", vol. 37, no. 9, pages 1181–1192, 2003.

[Cherrier 04a] E. Cherrier & M. Boutayeb. *Observer-based approach for synchronization of modified Chua's circuit*. In Proceedings of NOLCOS, IFAC Symposium on Nonlinear Control Systems, Stuttgart, Germany, 2004.

[Cherrier 04b] E. Cherrier, M. Boutayeb & J. Ragot. *Observer-based approach for a time-delay system. Application to synchronization of modified Chua's circuit*. In 3rd Workshop on Advanced Control and Diagnosis, Karlsruhe, Germany, 2004.

[Cherrier 05a] E. Cherrier, M. Boutayeb & J. Ragot. *Observer-based approach for synchronization of a time-delayed Chua's circuit*. In Proceedings of ISCAS, IEEE International Symposium on Circuit and Systems, Kobe, Japan, 2005.

[Cherrier 05b] E. Cherrier, M. Boutayeb & J. Ragot. *Observers based synchronization and input recovery for a class of chaotic models*. In Proceedings of the joint 44th IEEE Conference on Decision and Control and European Control Conference, Seville, Spain, 2005.

[Cherrier 05c] E. Cherrier, M. Boutayeb & J. Ragot. *Synchronisation basée observateur d'un système chaotique comportant un retard : Application à un circuit de Chua modifié*. In JDMACS, Lyon, France, 2005.

[Cherrier 06a] E. Cherrier, M. Boutayeb & J. Ragot. *Observateurs non linéaires de multimodèles. Application à la synchronisation et aux communications*. In Proceedings of CIFA, IEEE Conférence Internationale Francophone d'Automatique, Bordeaux, France, 2006.

[Cherrier 06b] E. Cherrier, M. Boutayeb & J. Ragot. *Observer-based exponential synchronization of chaotic multimodels*. In Proceedings of the 26th American Control Conference, New York City, USA, 2006. soumis.

[Cherrier 06c] E. Cherrier, M. Boutayeb & J. Ragot. *Observers based synchronization and input recovery for a class of nonlinear systems*. IEEE Transactions on Circuits and Systems I, vol. 53, no. 9, 2006.

[Cherrier 06d] E. Cherrier, M. Boutayeb & J. Ragot. *Observers based synchronization and input recovery for a class of nonlinear systems. Application to image transmission*. In 5th Workshop on Physics in Signal and Image Processing, Mulhouse, France, 2006. Soumis.

[Cherrier 06e] E. Cherrier, M. Boutayeb & J. Ragot. *Observers based synchronization of multimodels with application to communication systems*. IEEE Transactions on Circuits and Systems II, 2006. Soumis.

[Cherrier 06f] E. Cherrier, M. Boutayeb & J. Ragot. *Robust observer design for a class of nonlinear delayed systems. Application to experimental synchronization*. In Proceedings of the European Control Conference, Kos, Greece, 2006. Soumis.

[Cherrier 06g] E. Cherrier, M. Boutayeb & J. Ragot. *State estimation in presence of unknown delay measurements*. In 4th Workshop on Advanced Control and Diagnosis, Nancy, France, 2006. Soumis.

[Chua 93a] L.O. Chua, C.W. Wu, A. Huang & G.-Q. Zhong. *A universal circuit for studying and generating chaos-Part I : routes to chaos*. IEEE Transactions on Circuits and Systems I, vol. 40, no. 10, pages 732–744, 1993.

[Chua 93b] L.O. Chua, C.W. Wu, A. Huang & G.-Q. Zhong. *A universal circuit for studying and generating chaos-Part II : strange attractors*. IEEE Transactions on Circuits and Systems I, vol. 40, no. 10, pages 744–761, 1993.

[Ciccarella 93] G. Ciccarella, M. Dalla Mora & A. Germani. *A Luenberger-like observer for nonlinear systems*. International Journal of Control, vol. 57, no. 3, pages 537–556, 1993.

[Corless 98] M. Corless & J. Tu. *State and input estimation for a class of uncertain systems*. Automatica, vol. 34, no. 6, pages 757–764, 1998.

[Cuomo 93] K.M. Cuomo, A.V. Oppenheim & S.H. Strogatz. *Synchronization of Lorenz-based chaotic circuits with applications to communications*. IEEE Transactions on Circuits and Systems II, vol. 40, no. 10, pages 626–633, 1993.

[Daafouz 06] J. Daafouz, M. Fliess & G. Millérioux. *Une approche intrinsèque des observateurs linéaires à entrées inconnues*. In Proceedings of CIFA, IEEE Conférence Internationale Francophone d'Automatique, Bordeaux, France, 2006.

[Dang-Vu 00] H. Dang-Vu & C Delcarte. Bifurcations et chaos. Ellipses, 2000.

[Darouach 94] M. Darouach, M. Zasadzinski & S.J. Xu. *Full-order observers for lienar systems with unknown inputs*. IEEE Transactions on Automatic Control, vol. 39, no. 3, pages 606–609, 1994.

[Darouach 95] M. Darouach & M. Boutayeb. *Design of observers for descriptor systems*. IEEE Transactions on Automatic Control, vol. 40, no. 7, pages 1323–1327, 1995.

[Darouach 96] M. Darouach, M. Zasadzinski & M. Hayar. *Reduced-order observer design for descriptor systems with unknown inputs*. IEEE Transactions on Automatic Control, vol. 41, no. 7, pages 1068–1072, 1996.

[Dawson 92] D.M. Dawson, Z. Qu & J.C. Carroll. *On the state observation and output feedback problems for nonlinear uncertain dynamic systems*. Systems & Control Letters, vol. 18, pages 217–222, 1992.

[Dedieu 93] H. Dedieu, M.P. Kennedy & M. Hasler. *Chaos shift keying : modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits*. IEEE Transactions on Circuits and Systems I, vol. 40, no. 10, pages 634–642, 1993.

[Deza 93] F. Deza, D. Bossanne, E. Busvelle, J. P. Gauthier & D. Rakotopara. *Exponential observer for nonlinear systems*. IEEE Transactions on Automatic Control, vol. 38, no. 3, pages 482–484, 1993.

[Fairman 84] F.W. Fairman, S.S. Mahil & L. Luk. *Disturbance decoupled observer design via singular value decomposition*. IEEE Transactions on Automatic Control, vol. AC-29, pages 84–86, 1984.

[Farmer 82] J.D. Farmer. *Chaotic attractors of an infinite-dimensional dynamical system*. Physica D, vol. 4, pages 366–393, 1982.

[Farza 04] M. Farza, M.M'Saad & L. Rossignol. *Observer design for a class of MIMO nonlinear systems*. Automatica, vol. 40, no. 1, pages 135–143, 2004.

[Feki 03] M. Feki. *Observer-based chaotic synchronization in the presence of unknown inputs*. Chaos, Solitons and Fractals, vol. 15, pages 831–840, 2003.

[Feldmann 96] U. Feldmann, M. Hasler & W. Schwarz. *Communication by chaotic signals : The inverse system approach*. Int. J. Circuit Theory Appl., vol. 24, pages 551–579, 1996.

[Femat 01] R. Femat, R.Jauregui-Ortiz & G. Solís-Perales. *A chaos-based communication scheme via robust asymptotic feedback*. IEEE Transactions on Circuits and Systems I, vol. 48, no. 10, pages 1161–1169, 2001.

[Franz 96] M. Franz. *Chua's equation with cubic nonlinearity*. International Journal of Bifurcation and Chaos, vol. 6, pages 2175–2222, 1996.

[Gaddouna 94] B. Gaddouna, D. Maquin & J. Ragot. *Fault detection observers for systems with unknown inputs*. In Proceedings of SAFEPROCESS'94, IFAC/IMACS Symposium on Fault Detection, Supervision and Safety for Technical Processes, Espoo, Finland, 1994.

[Gauthier 92] J.P. Gauthier, H. Hammouri & S. Othman. *A simple obsever for nonlinear systems : Application to bioreactors*. IEEE Transactions on Automatic Control, vol. 37, no. 6, pages 875–880, 1992.

[Gu 03] K. Gu, V.L. Kharitonov & J. Chen. Stability of time-delay systems. Birkhäuser, 2003.

[Ha 04] Q.P. Ha & H. Trinh. *State and input simultaneous estimation for a class of nonlinear systems*. Automatica, vol. 40, pages 1779–1785, 2004.

[Haeri 06] M. Haeri & B. Khademian. *Comparison between different synchronization methods of identical chaotic systems*. Chaos, Solitons and Fractals, vol. 29, no. 4, pages 1002–1022, 2006.

[Hahn 03] W. Hahn. Theory and application of lyapunov's direct method. Prentice Hall, Englewood Cliffs, 2003.

[Halle 93] K.S. Halle, C.W. Wu, M. Itoh & L.O. Chua. *Spread spectrum communication through modulation of chaos*. International Journal of Bifurcation and Chaos, vol. 3, pages 469–477, 1993.

[Hammouri 88] H. Hammouri & J.P. Gauthier. *Bilinearization up to output injection*. Systems & Control Letters, vol. 11, pages 139–149, 1988.

[Hammouri 96] H. Hammouri & M. Kinaert. *A new procedure for time-varying linearization up to output injection*. Systems & Control Letters, vol. 28, no. 3, pages 151–157, 1996.

[Hammouri 99] H. Hammouri, M. Kinaert & E.H. El Yaagoubi. *Observer-based approach to fault detection and isolation for nonlinear systems*. IEEE Transactions on Automatic Control, vol. 44, no. 10, pages 1879–1884, 1999.

[Hostetter 73] G. Hostetter & J.S. Meditch. *Observing systems with unmeasurable inputs*. IEEE Transactions on Automatic Control, vol. 18, pages 307–308, 1973.

[Hou 92] M. Hou & P.C. Muller. *Design of observers for linear systems with unknown inputs*. IEEE Transactions on Automatic Control, vol. 37, pages 871–875, 1992.

[Inoue 01] E. Inoue & T. Ushio. *Chaos communication using unknown input observers*. Electronics and Communications in Japan, vol. J82-A, no. 12, pages 1801–1807, 2001.

[Jazwinski 70] A.H. Jazwinski. Stochastic processes and filtering theory. New York Academic, 1970.

[Jiang 02] Z.-P. Jiang. *A note on chaotic secure communication systems*. IEEE Transactions on Circuits and Systems I, vol. 49, no. 1, pages 92–96, 2002.

[Jiang 03] G.-P. Jiang, G. Chen & 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, pages 2343–2351, 2003.

[Jiang 05] G.-P. Jiang & 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, pages 437–443, 2005.

[Jo 00] N.H. Jo & J.H. Seo. *Input output linearization approach to state observer design for nonlinear system*. IEEE Transactions on Automatic Control, vol. 45, no. 12, pages 2388–2393, 2000.

[Johnson 71] C.D. Johnson. *Accomodation of external disturbances in linear regulator and servomechanism problems*. IEEE Transactions on Automatic Control, vol. 16, pages 635–644, 1971.

[Kalman 60] R.E. Kalman. *A new approach to linear filtering*. Transactions of the ASME Journal of Basic Engineering, vol. 82, pages 35–45, 1960.

[Kazantzis 98] N. Kazantzis & C. Kravaris. *Nonlinear observer design using Lyapunov's auxiliary theorem*. Systems & Control Letters, vol. 34, no. 5, pages 241–247, 1998.

[Kelber 05] K Kelber & W. Schwarz. *General design rules for chaos-based encryption systems*. In Proceedings of NOLTA2005, International Symposium on Nonlinear Theory and its Applications, Bruges, Belgium, pages 465–468, 2005.

[Keller 87] H. Keller. *Nonlinear observer design by transformation into a generalized observer canonical form*. International Journal of Control, vol. 46, no. 6, pages 1915–1930, 1987.

[Kharitonov 99] V.L. Kharitonov. *Robust stability analysis of time-delay systems : a survey*. Annual Reviews in Control, vol. 23, pages 185–196, 1999.

[Kobayashi 87] N. Kobayashi & T. Nakamizo. *An observer design for linear systems with unknown inputs*. IEEE Transactions on Automatic Control, vol. AC-25, pages 113–115, 1987.

[Kocarev 92] L. Kocarev, K.S. Halle, K. Eckert, L.O. Chua & U. Parlitz. *Experimental demonstration of secure communications via chaotic synchronization*. International Journal of Bifurcation and Chaos, vol. 2, pages 709–713, 1992.

[Kocarev 95] L. Kocarev & U. Parlitz. *General approach for chaotic synchronization with application to communication*. Physical Review Letters, vol. 74, no. 25, pages 5028–5031, 1995.

[Koenig 02] D. Koenig & S. Mammar. *Design of proportional-integral observer for unknown input descriptor systems*. IEEE Transactions on Automatic Control, vol. 47, no. 12, pages 2057–2062, 2002.

[Kolumbán 97] G. Kolumbán, M. P. Kennedy & L. O. Chua. *The role of synchronization in digital communications using chaos - part I : Fundamentals of digital communications*. IEEE Transactions on Circuits and Systems I, vol. 44, pages 927–936, 1997.

[Kolumbán 98] G. Kolumbán, M. P. Kennedy & L. O. Chua. *The role of synchronization in digital communications using chaos - part II : chaotic modulation and chaotic synchronization*. IEEE Transactions on Circuits and Systems I, vol. 45, pages 1129–1140, 1998.

[Kou 75] S.R. Kou, D.L. Elliott & T.J. Tarn. *Exponential observers for nonlinear dynamic systems*. Information and Control, vol. 29, pages 204–216, 1975.

[Krasovskii 63] N.N. Krasovskii. Stability of motion. Stanford University Press,Stanford CA, USA (translation by J. Brenner), 1963.

[Kreisselmeier 03] G. Kreisselmeier & R. Engel. *Nonlinear observers for autonomous Lipschitz continuous systems*. IEEE Transactions on Automatic Control, vol. 48, no. 3, pages 451–464, 2003.

[Krener 83] A.J. Krener & A. Isidori. *Linearization by output injection and nonlinear observers*. Systems & Control Letters, vol. 3, pages 47–52, 1983.

[Krener 85] A.J. Krener & W. Respondek. *Nonlinear observers with linearizable error dynamics*. SIAM Journal on Control and Optimization, vol. 23, pages 197–216, 1985.

[Kudva 80] P. Kudva, N. Viswabadham & A. Ramakrishna. *Observers for linear systems with unknown inputs*. IEEE Transactions on Automatic Control, vol. 25, pages 113–115, 1980.

[Levine 86] J. Levine & R. Marino. *Nonlinear system immersion, observers and finite dimensional filters*. Systems & Control Letters, vol. 7, pages 133–142, 1986.

[Li 86] C. Li, X. Liao & K.-W. Wong. *Chaotic lag synchronization of coupled time-delayed systems and its application in secure communication*. Systems & Control Letters, vol. 7, pages 133–142, 1986.

[Liao 99] T.-L. Liao & 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, pages 1144–1150, 1999.

[Liu 02] C.-S. Liu & H. Peng. *Inverse-dynamics based state and disturbance observers for linear time-invariant systems*. Journal of Dynamic Systems, Measurement, and Control, vol. 124, pages 375–381, 2002.

[Luenberger 71] D.G. Luenberger. *An introduction to observers*. IEEE Transactions on Automatic Control, vol. 16, no. 6, pages 596–602, 1971.

[Mainieri 99] R. Mainieri & J. Rehacek. *Projective synchronization in three-dimensional chaotic systems*. Physical Review Letters, vol. 82, no. 15, pages 3042–3045, 1999.

[Millérioux 97] G. Millérioux. *Chaotic synchronization conditions based on control theory for systems described by discrete piecewise linear maps*. International Journal of Bifurcation and Chaos, vol. 7, no. 7, pages 1635–1649, 1997.

[Millérioux 98] G. Millérioux & C. Mira. *Coding scheme based on chaos synchronization from noninvertible maps*. International Journal of Bifurcation and Chaos, vol. 8, no. 10, pages 2019–2029, 1998.

[Millérioux 03] G. Millérioux & J. Daafouz. *An observer-based approach for input independent global chaos synchronization of discrete time switched systems*. IEEE Transactions on Circuits and Systems I, vol. 50, no. 10, pages 1270–1279, 2003.

[Millérioux 04] G. Millérioux & J. Daafouz. *Unknown input observers for message-embedded chaos synchronization of discrete-time systems*. International Journal of Bifurcation and Chaos, vol. 14, no. 4, pages 1357–1368, 2004.

[Millérioux 06] G. Millérioux & J. Daafouz. *Chaos synchronization : from the genesis to polytopic observers*. In Proceedings Chaos'06, IFAC Conference on Analysis and Control of Chaotic Systems, Reims, France, pages 345–350, 2006.

[Misawa 89] E.A. Misawa & J.K. Heydrick. *Nonlinear observers - A state-of-the-art survey*. Journal of Dynamic Systems, vol. 111, pages 344–352, 1989.

[Mondie 05] S. Mondie & V.L. Kharitonov. *Exponential estimates for retarded time-delay systems : an LMI approach*. IEEE Transactions on Automatic Control, vol. 50, no. 2, pages 268–273, 2005.

[Morgül 96] O. Morgül & E. Solak. *Observer based synchronization of chaotic systems*. Physical Review E, vol. 54, no. 5, pages 4803–4811, 1996.

[Morgül 99] O. Morgül & M. Feki. *A chaotic masking scheme by using synchronized chaotic systems*. Physics Letters A, vol. 251, pages 169–176, 1999.

[Nemirovskii 94] A. Nemirovskii & P. Gahinet. *The projective method for solving linear matrix inequalities*. In Proceedings of the American Control Conference, Baltimore, Maryland, pages 840–844, 1994.

[Nicosia 89] S. Nicosia, P. Tomei & A. Tornambé. *An approximate observer for a class of nonlinear systems*. Systems & Control Letters, vol. 12, pages 43–51, 1989.

[Nijmeijer 97] H. Nijmeijer & I.M.Y. Mareels. *An observer looks at synchronization*. IEEE Transactions on Circuits and Systems I, vol. 44, no. 10, pages 882–890, 1997.

[Nikoukhah 98] R. Nikoukhah. *A new methodology for observer design and implementation*. IEEE Transactions on Automatic Control, vol. 43, no. 2, pages 229–234, 1998.

[Nørgaard 00] M. Nørgaard, N.K. Poulsen & O. Ravn. *New developments in state estimation for nonlinear systems*. Automatica, vol. 36, pages 1627–1638, 2000.

[Ogorzalek 93] M.J. Ogorzalek. *Taming chaos - Part I : synchronization*. IEEE Transactions on Circuits and Systems I, vol. 40, no. 10, pages 693–699, 1993.

[Oppenheim 92] A.V. Oppenheim, G.W. Wornell, S.H. Isabelle & K.M. Cuomo. *Signal processing in the context of chaotic signals*. In Proceedings of the IEEE ICASSP, San Francisco, CA, vol. 4, pages 117–120, 1992.

[Ott 90] E. Ott, C. Grebogi & J.A. Yorke. *Controlling chaos*. Physical Review Letters, vol. 64, no. 11, pages 1196–1199, 1990.

[Parker 89] T.S. Parker & L.O. Chua. *Practical Numerical Algorithms for Chaotic Systems*. Springer-Verlag, 1989.

[Parks 93] P.C. Parks & V. Hahn. *Stability theory*. Prentice Hall, New York, 1993.

[Parlitz 93] U. Parlitz, L.O. Chua, L. Kocarev, K.S. Halle & A. Shang. *Trnasmission of digital signals by chaotic synchronization*. International Journal of Bifurcation and Chaos, vol. 2, pages 973–977, 1993.

[Parlitz 99a] U. Parlitz, L. Junge & L. Kocarev. *Chaos synchronization*. In H. Nijmeijer & T.I. Fossen, éditeurs, New directions in nonlinear observer design, pages 511–525. Springer Verlag, 1999.

[Parlitz 99b] U. Parlitz & L. Kocarev. *Synchronization of chaotic systems*. In H.G. Schuster, éditeur, Handbook of Chaos Control, pages 271–303. Wiley-VCH, 1999.

[Pecora 90] L.M. Pecora & T.L. Carroll. *Synchronization in chaotic systems*. Physical Review Letters, vol. 64, no. 8, pages 821–824, 1990.

[Pecora 97] L.M. Pecora, T.L. Carroll, G. Johnson & D. Mar. *Fundamentals of synchronization in chaotic systems, concepts and applications*. Chaos, vol. 7, no. 4, pages 520–543, 1997.

[Pertew 05] A.M. Pertew, H.J. Marquez & Q. Zhao. *$\mathcal{H}_\infty$ synthesis of unknown input observers for non-linear Lipschitz systems*. International Journal of Control, vol. 78, no. 15, pages 1155–1165, 2005.

[Primbs 96] J. Primbs. *Survey of nonlinear observer design techniques*, 1996. http ://citeseer.ist.psu.edu/primbs96survey.html.

[Raghavan 94] S. Raghavan & J.K. Hedrick. *Observer design for a class of nonlinear systems*. International Journal of Control, vol. 59, no. 2, pages 515–528, 1994.

[Rajamani 98] R. Rajamani. *Observer for Lipschitz nonlinear systems*. IEEE Transactions on Automatic Control, vol. 43, no. 3, pages 397–401, 1998.

[Rapaport 00] A. Rapaport & A. Maloum. *Embedding for exponential observers of nonlinear systems*. In Proceedings of the 39th IEEE Conference on Decision and Control, Sydney, Australia, 2000.

[Reif 98] K. Reif, F. Sonnemann & R. Unbehauen. *An EKF-based nonlinear observer with a prescribed degree of stability*. Automatica, vol. 34, no. 9, pages 1119–1123, 1998.

[Richard 03] J.-P. Richard. *Time delay systems : an overview of some recent advances and open problems*. Automatica, vol. 39, no. 10, pages 1667–1694, 2003.

[Rosenblum 96] M.G. Rosenblum, A.S. Pikovsky & J. Kurths. *Phase synchronization of chaotic oscillators*. Physical Review Letters, vol. 76, pages 1804–1807, 1996.

[Rulkov 95] N.F. Rulkov, M.M. Sushchik, L.S. Tsimring & H.D.I. Abarbanel. *Generalized synchronization of chaos in directionally coupled chaotic systems*. Physical Review E, vol. 51, pages 980–994, 1995.

[Seliger 91] R. Seliger & P.M. Frank. *Fault-diagnosis by disturbance decoupled nonlinear observers*. In Proceedings of the 30th IEEE Conference on Decision and Control, Brighton, England, 1991.

[Shannon 49] C.E. Shannon. *Communication Theory of Secrecy Systems*. Bell System Technical Journal, vol. 28, no. 4, pages 656–715, 1949.

[Sharma 04] R. Sharma & M. Aldeen. *Estimation of unknown disturbances in nonlinear systems*. In Control 2004, University of Bath, UK, 2004.

[Short 94] K.M. Short. *Steps towards Unmasking Secure Communications*. International Journal of Bifurcation and Chaos, vol. 4, no. 4, pages 959–977, 1994.

[Short 96] K.M. Short. *Unmasking a modulated chaotic communications scheme*. International Journal of Bifurcation and Chaos, vol. 6, no. 2, pages 367–375, 1996.

[Silva 93] C.P. Silva. *Shil'nikov's Theorem - A Tutorial*. IEEE Transactions on Circuits and Systems I, vol. 40, no. 10, pages 675–682, 1993.

[Slotine 87] J.-J.E. Slotine, J.K. Heydrick & E.A. Misawa. *On sliding observers for nonlinear systems*. Journal of Dynamic Systems, vol. 109, pages 245–252, 1987.

[Sobhy 01] M.I. Sobhy & A.R. Shehata. *Methods of Attacking Chaotic Encryption and Countermeasures*. In Proceedings of the International Conference on Accoustics, Speech and Signal Processing, Salt Lake City, 2001.

[Stinson 95] D. Stinson. Cryptography : theory and practice. CRC Press, 1995.

[Tang 02] S. Tang, H.F. Chen, S.K. Hwang & J.M. Liu. *Message encoding and decoding through chaos modulation in chaotic optical communications*. IEEE Transactions on Circuits and Systems I, vol. 49, no. 2, pages 163–169, 2002.

[Thau 73] F.E. Thau. *Observing the state of non-linear dynamic systems*. International Journal of Control, vol. 17, no. 3, pages 471–479, 1973.

[Vidyasagar 93] M. Vidyasagar. Nonlinear systems analysis. Prentice Hall, Englewood Cliffs, 1993.

[Walcott 87a] B.L. Walcott, M.J. Corless & S.H. Zak. *Comparative study of non-linear state-observation techniques*. International Journal of Control, vol. 45, no. 6, pages 2109–2132, 1987.

[Walcott 87b] B.L. Walcott & S.H. Zak. *State observation of nonlinear uncertain dynamical systems*. IEEE Transactions on Automatic Control, vol. 32, no. 2, pages 166–170, 1987.

[Wang 75] S.-H. Wang, E.J. Davison & P. Dorato. *Observing the states of systems with unmeasurable disturbances*. IEEE Transactions on Automatic Control, vol. 20, pages 716–717, 1975.

[Wang 00] X.F. Wang, G. Chen & X. Yu. *Anticontrol of chaos in continuous-time systems via time-delay feedback*. Chaos, vol. 10, no. 4, pages 771–779, 2000.

[Wang 01] X.F. Wang, G.-Q. Zhong, K.-S. Tang, K.F. Man & Z.-F. Liu. *Generating chaos in Chua's circuit via time-delay feedback*. IEEE Transactions on Circuits and Systems I, vol. 48, no. 9, pages 1151–1156, 2001.

[Wiggins 90] S. Wiggins. Introduction to applied nonlinear dynamical systems and chaos. Springer-Verlag, 1990.

[Wolf 85] A. Wolf, J. Swift, H. Swinney & J. Vastano. *Determining lyapunov exponents from a time-series*. Physica D, vol. 16, pages 285–317, 1985.

[WU 93] C.W. WU & L.O. Chua. *A simple way to synchronize chaotic systems with application to secure communications systems*. International Journal of Bifurcation and Chaos, vol. 3, pages 1619–1627, 1993.

[Wünnenberg 90] J. Wünnenberg. *Observer-based fault detection in dynamic systems*. Thèse, Université de Duisburg, Allemagne, 1990.

[Xia 89] X.H. Xia & W.B. Gao. *Nonlinear observer design by observer error linearization*. SIAM Journal on Control and Optimization, vol. 29, no. 1, pages 199–216, 1989.

[Yalcine 01] M.E. Yalcine, J.A.K. Suykens & J. Vandewalle. *Master-slave synchronization of Lur'e systems with time-delay*. International Journal of Bifurcation and Chaos, vol. 2, no. 2, pages 1707–1722, 2001.

[Yamada 83] T. Yamada & H. Fujisaka. *Stability theory of synchronized motion in coupled-oscillator systems*. Prog. Theor. Phys., vol. 69, no. 1, pages 32–47, 1983.

[Yang 88] F. Yang & R.W. Wilde. *Observers for linear systems with unknown inputs*. IEEE Transactions on Automatic Control, vol. 33, pages 677–681, 1988.

[Yang 95] T. Yang. *Recovery of digital signals from chaotic switching*. International Journal of Circuit Theory and Applications, no. 23, pages 611–615, 1995.

[Yang 96] T. Yang & L.O. Chua. *Secure communication via chaotic parameter modulation*. IEEE Transactions on Circuits and Systems I, vol. 43, no. 9, pages 817–819, 1996.

[Yang 97a] T. Yang & L.O. Chua. *Impulsive stabilization for cotrol and synchronization of chaotic systems : Theory and application to secure communications*. IEEE Transactions on Circuits and Systems I, vol. 44, no. 10, pages 976–988, 1997.

[Yang 97b] T. Yang, C.W. Wu & L.O. Chua. *Cryptography based on chaotic systems*. IEEE Transactions on Circuits and Systems I, vol. 44, no. 5, pages 469–472, 1997.

[Yang 98a] T. Yang, L.-B. Yang & C.-M. Yang. *Breaking chaotic switching using generalized synchronization : examples*. IEEE Transactions on Circuits and Systems I, vol. 45, no. 10, pages 1062–1067, 1998.

[Yang 98b] T. Yang, L.-B. Yang & C.-M. Yang. *Cryptanalysing chaotic secure communications using return maps*. Physics Letters A, vol. 245, pages 495–510, 1998.

[Yang 04] T. Yang. *A survey of chaotic secure communication systems*. Int. J. of Comput. Cognition, vol. 11, no. 6, pages 81–130, 2004.

[Zeitz 87] M. Zeitz. *The extended Luenberger observer for nonlinear systems*. Systems & Control Letters, vol. 9, pages 149–156, 1987.

[Zhou 97a] C.-S. Zhou & 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, pages 429–435, 1997.

[Zhou 97b] H. Zhou & X.-T. Ling. *Problems with the chaotic inverse system encryption approach*. IEEE Transactions on Circuits and Systems I, vol. 44, no. 3, pages 268–271, 1997.

[Zhou 04] T. Zhou, G. Chen & Q. Yang. *A simple time-delay feedback anticontrol method made rigorous*. Chaos, vol. 14, no. 3, pages 662–668, 2004.

[Zhu 02] F. Zhu & Z. Han. *A note on observers for Lipschitz nonlinear systems*. IEEE Transactions on Automatic Control, vol. 47, no. 10, pages 1751–1754, 2002.

Autorisation de soutenance

INSTITUT NATIONAL
POLYTECHNIQUE
DE LORRAINE

AUTORISATION DE SOUTENANCE DE THESE
DU DOCTORAT DE L'INSTITUT NATIONAL
POLYTECHNIQUE DE LORRAINE

o0o

VU LES RAPPORTS ETABLIS PAR :
Madame Geneviève DAUPHIN-TANGUY, Professeur, LAGIS, Ecole Centrale de Lille, Villeneuve d'Ascq

Monsieur Mohamed M'SAAD, Professeur, Laboratoire Greyc, ENSICAEN, Caen

Le Président de l'Institut National Polytechnique de Lorraine, autorise :

Madame PAWLOWSKI Estelle épouse CHERRIER

NANCY BRABOIS
2, AVENUE DE LA
FORET-DE-HAYE
BOITE POSTALE 3
F - 54501
VANDŒUVRE CEDEX

à soutenir devant un jury de l'INSTITUT NATIONAL POLYTECHNIQUE DE LORRAINE, une thèse intitulée :

"Estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires"

en vue de l'obtention du titre de :

DOCTEUR DE L'INSTITUT NATIONAL POLYTECHNIQUE DE LORRAINE

Spécialité : « **Automatique et traitement du signal** »

Fait à Vandoeuvre, le 10 octobre 2006
Le Président de l'I.N.P.L.,
L. SCHUFFENECKER

TEL. 33/03.83.59.59.59
FAX. 33/03.83.59.59.55

Résumé De façon générale, cette thèse porte sur l'estimation de l'état et des entrées inconnues pour une classe de systèmes non linéaires. De façon plus particulière, le problème est abordé sous l'angle de la conception d'un système de transmission sécurisée d'informations exploitant les propriétés des systèmes chaotiques et leur capacité de synchronisation. Les travaux présentés traitent trois points principaux, à savoir le choix de l'émetteur, le développement du récepteur, et la mise au point du processus de transmission de l'information ou du message.
L'émetteur retenu est un système non linéaire chaotique dont la dynamique comporte un retard, ce qui lui confère un comportement particulièrement complexe. La conception du récepteur repose sur la synthèse d'un observateur non linéaire, dont la stabilité et la convergence garantissent la synchronisation avec l'émetteur. L'insertion du message est réalisée par modulation de la phase d'un signal porteur chaotique. Le décryptage de l'information s'apparente à une restauration d'entrée inconnue au niveau du récepteur.
Une étude de la sécurité du processus de cryptage a été menée, reposant sur des techniques standard de cryptanalyse. Des multimodèles chaotiques ont été proposés pour renforcer la sécurité du processus de synchronisation.

Mots-clés observateurs non linéaires, stabilité au sens de Lyapunov-Krasovskii, systèmes chaotiques à retard, multimodèles chaotiques, synchronisation, cryptosystèmes, cryptanalyse, synthèse $\mathcal{H}_\infty$

Abstract In a general way, this thesis deals with state and unknown input estimation for a class of nonlinear systems. In a more particular way, the problem is addressed from a secure communication system design point of view, based on chaotic systems properties and synchronization ability. Our work deals with three main points : selection of the transmitter, design of the receiver, and development of the information (or message) transmission process.
The chosen transmitter is a time-delay nonlinear chaotic system : the main reason is that a very complex behavior is brought about by the delayed state feedback. The receiver design relies on a nonlinear observer synthesis, whose stability and convergence ensure synchronization with the transmitter. The message insertion is realized through a chaotic carrier phase modulation. The decryption process is similar to an unknown input recovery, at the receiver side.
The security of the proposed encryption/decryption process is studied using standard cryptanalysis techniques. Chaotic multimodels are defined to tighten up the synchronization process security.

Keywords nonlinear observers, stability in the sense of Lyapunov-Krasovskii, Delayed chaotic systems, chaotic multimodels, synchronization, cryptosystems, cryptanalysis, $\mathcal{H}_\infty$ filtering