Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse

Floriane Anstett

Ecole doctorale IAEM Lorraine
UFR ESSTIN

Département de formation doctorale en automatique

Les systèmes dynamiques chaotiques pour le chiffrement : synthèse et cryptanalyse

THÈSE

présentée et soutenue publiquement le 12 juillet 2006

pour l'obtention du

Doctorat de l'Université Henri Poincaré – Nancy 1

spécialité automatique

par

Floriane Anstett

Composition du jury

Président :	P. Guillot	Maître de conférences à l'Université Paris 8
Rapporteurs :	M. Hasler	Professeur à l'Ecole Polytechnique Fédérale de Lausanne
	G. Garcia	Professeur à l'Institut National des Sciences Appliquées de Toulouse
Examinateurs :	L. Denis-Vidal	Maître de conférences HDR à l'Université des Sciences et Techniques de Lille
	G. Bloch	Professeur à l'Université Henri Poincaré - Nancy 1
	G. Millérioux	Professeur à l'Université Henri Poincaré - Nancy 1

Centre de Recherche en Automatique de Nancy — CNRS - UMR 7039

Remerciements

Il est de coutume de remercier toutes les personnes ayant contribué de loin ou de près au bon déroulement d'une thèse. Je ne dérogerai pas à cette tradition et j'en profiterai donc pour exprimer toute ma gratitude à tous ceux qui ont accepté de s'embarquer avec moi dans cette aventure et à qui je n'ai jamais osé la témoigner spontanément.

Je commencerai tout naturellement par remercier mon directeur de thèse, Gérard Bloch, et mon co-encadrant, Gilles Millérioux. Il va sans dire que sans eux, l'idée de travailler sur un sujet aussi attrayant et passionnant ne m'aurait pas effleuré l'esprit car j'ignorais jusqu'alors l'existence du chaos. Je tiens surtout à les remercier pour leurs conseils judicieux et avisés, leur disponibilité et leur rigueur scientifique, qui m'ont permis d'avancer et de progresser considérablement dans mes travaux. Par ailleurs, ils se sont toujours inquiétés de savoir si ma thèse se déroulait dans les meilleures conditions. Incontestablement, je ne réalise pas la chance que j'ai eue de travailler avec eux. Enfin, j'ajouterai, et ils comprendront l'allusion, qu'ils ont joué un grand rôle dans la préparation de mes présentations orales bien que leur modestie tentera d'affirmer le contraire.

Ensuite, je tiens tout particulièrement à remercier Jean Rodolphe Roche pour m'avoir guidé dans la recherche d'un polytope minimal, Claude Moog pour avoir consacré son temps à répondre à mes interrogations sur l'identifiabilité, Ghislaine Joly-Blanchard et Lilianne Denis-Vidal pour leur accueil à Compiègne et Jean-Marie Ory pour son aide sur la densité spectrale d'un signal.

Je tiens à adresser un petit mot spécialement à Sylvie Ferrari pour sa grande disponibilité et serviabilité. Sa bonne humeur n'a d'égale que sa gentillesse.

Je souhaite également remercier tous les enseignants du département ISYPRO qui ont fait de mon lieu de travail un lieu chaleureux et convivial. Entre autres, Eric et Jean-Luc pour les innombrables cafés offerts en toute jovialité, Christophe, à qui l'on doit un voyage en Savoie, ainsi que tous les autres.

Je remercie aussi toutes les personnes que je n'ai pas pu nommer ici et qui ont participé directement ou non à cette épopée.

Je ne manquerai pas de remercier tendrement mon fiancé, qui partageant mes efforts, a toujours été d'une patience, d'un soutien et d'un réconfort exceptionnels. Je lui dois en grande partie l'aboutissement de ce travail.

Enfin, je dédie ce mémoire à mes parents qui m'ont permis de mener à bien cette tâche. Leur exemplarité, leur sagesse et leur sérenité m'ont aidée à dépasser les limites de mon possible.

"It may well be doubted whether human ingenuity can construct an enigma... which human ingenuity may not, by proper application, resolve."
Edgar Allan Poe
The works of Edgar Allan Poe : volume 1 - The Gold Bug, 1843

Table des matières

Introduction

Η τοι μεν πρωτιστα χαος γενετ . . .
"Au commencement exista le Chaos, puis la Terre à la large poitrine, demeure toujours sûre de tous les Immortels qui habitent le faite de l'Olympe neigeux ; ensuite le sombre Tartare, placé sous les abîmes de la Terre immense ; enfin l'Amour, le plus beau des dieux, l'Amour, qui amollit les âmes, et, s'emparant du coeur de toutes les divinités et de tous les hommes, triomphe de leur sage volonté. "
Hésiode
Théogonie, 116.

"Le préjugé foncier est de croire que l'ordre, la clarté, la méthode doivent tenir à l'être vrai des choses, alors qu'au contraire, le désordre, le chaos, l'imprévu, n'apparaissent que dans un monde faux ou insuffisamment connu, bref sont une erreur ; c'est là un préjugé moral, qui vient de ce que l'homme sincère, digne de confiance, est un homme d'ordre, de principes, et a coutume d'être, somme toute, un être prévisible et pédantesque."
F. Nietzsche
La Volonté de Puissance, Tome 1 - 1901

Depuis la nuit des temps, le chaos était synonyme de désordre et de confusion, s'opposait à l'ordre et à la méthode et devait être évité. La science était caractérisée par le déterminisme, la prévisibilité et la réversibilité. La vision déterministe, qui était celle notamment de Newton (1642-1727) ou de Laplace (1749-1827), reposait sur le fait que l'univers serait régi par des lois immuables et qu'il serait possible de connaître l'avenir et le passé à partir du simple présent. Poincaré (1854-1912) fut l'un des premiers à entrevoir la théorie du chaos. Il découvrit la notion de sensibilité aux conditions initiales à travers le problème de l'interaction de trois corps célestes. En effet, l'étude de l'interaction de deux corps peut facilement être menée par les lois de Newton, mais la considération d'un troisième corps implique des comportements complexes s'apparentant au hasard. La sensibilité aux conditions initiales est l'une des caractéristiques du chaos. Elle correspond au fait que de petites causes entraînent de grands effets. Plus tard, en 1960, le phénomène a été mis en évidence par un météorologiste, Lorenz. Il implémenta un programme informatique simplifié, impliquant trois équations différentielles, pour modéliser quelque élément météorologique. Désirant reproduire une séquence temporelle obtenue la veille, il initialisa sa simulation avec les mêmes valeurs que celles utilisées la veille mais comportant quelques décimales en moins. Il s'attendait à obtenir des résultats identiques. Pourtant, les résultats s'étaient rapidement écartés de ceux prévus, pour devenir complètement décorrélés des précédents. Ainsi, un petit changement initial entraîna un énorme changement final. Ce phénomène, qui traduit cette sensibilité aux conditions initiales, est connu sous le nom d'effet papillon. Le battement d'ailes d'un papillon, aujourd'hui à Pékin, engendrerait une tempête, le mois prochain à New York.
Le terme "chaos" définit un état particulier d'un système dont le comportement ne se répète jamais, est très sensible aux conditions initiales, est imprédictible à long terme, mais n'en est pas moins déterministe. Des chercheurs d'horizons divers ont alors commencé à s'intéresser à des

problèmes non linéaires jusqu'alors sans solution parce qu'imprédictibles et regroupés sous la dénomination de chaos. Ils ont cherché à répondre à des questions telles que : comment se forment les nuages ? Les arythmies cardiaques ou les variations d'une population animale obéissent-elles à des règles ? Les mouvements commerciaux ou les marchés financiers peuvent-ils s'expliquer ? ... Le modèle du biologiste Robert May décrit l'évolution de la population d'une espèce en fonction des contraintes du milieu (famines, épidémies, prédateurs, ...) et obéit à une dynamique chaotique (équation logistique). Richard Cohen, physicien et cardiologue, a montré lors de simulations que le caractère chaotique du rythme cardiaque pourrait expliquer l'apparition de crise cardiaque. William Baumol et Jess Benhabib, économistes, se sont intéressés à la théorie du chaos et à ses applications à l'économie. D'autres exemples peuvent être trouvés dans [Gleick, 1991] qui retrace l'histoire et le rôle que le chaos a joué dans la science. Le chaos a ainsi trouvé de nombreuses applications dans les domaines tant physique que biologique, chimique ou économique, par exemple.

Depuis 1990, une application particulière qui a retenu l'attention des chercheurs est le chiffrement de données. En effet, l'émergence des nouvelles technologies de l'information et de la communication et la mondialisation des échanges (Internet, messagerie électronique, commerce électronique, ...) doivent faire face au problème de la sécurité des données. Par exemple, le code bancaire ne doit pas être intercepté par un adversaire lors d'un paiement sur Internet. Les informations échangées électroniquement au sein d'un groupe industriel ne doivent pas être filtrées par les entreprises concurrentes ... La cryptographie, ou "écriture secrète", d'abord utilisée pour des applications militaires, répond à ce problème. L'occasion est toute trouvée de présenter trois personnages célèbres en cryptographie, Alice, Bob et Charlie. Alice, l'émetteur, souhaite envoyer un message à Bob, le destinataire, par l'intermédiaire d'un canal non sécurisé. Pour cela, Alice va transformer, ou "chiffrer", son message afin d'en cacher le sens à tous ceux qui ne sont pas autorisés à le connaître. Charlie, l'adversaire, tente de faire échouer la communication entre Alice et Bob. Il cherche par exemple à intercepter ou à modifier le message. La cryptanalyse, "analyse de l'écriture secrète", permet d'attester la sécurité des schémas de chiffrement pour éviter que l'adversaire ne parvienne à ses fins.
Dans les schémas de chiffrement basé sur le chaos, l'information à masquer est injectée dans un générateur de chaos, l'émetteur. L'imprédictibilité à long terme des systèmes chaotiques rend ainsi difficile l'interception de l'information par un adversaire. En fait, les systèmes chaotiques possèdent des propriétés proches de celles requises par les schémas de chiffrement en cryptographie usuelle. Il est donc raisonnable de penser que les systèmes chaotiques peuvent être utilisés à des fins de chiffrement. Le récepteur, quant à lui, a pour rôle de reconstruire l'information.

Les travaux réalisés dans cette thèse s'inscrivent dans ce contexte particulier. Leur objectif est d'étudier la synthèse et la cryptanalyse des schémas de chiffrement basés sur le chaos. Ils s'organisent autour de trois points principaux et originaux, qui sont :

- De nombreux travaux dans la littérature portent sur les systèmes chaotiques pour le chiffrement, mais très peu s'attachent au lien entre le chiffrement par le chaos et le chiffrement usuel. La connexion entre le chiffrement usuel et le chiffrement par le chaos est établie.

- Le problème de la reconstruction de l'information, côté récepteur, est traité.

- Un élément majeur d'un schéma de chiffrement est sa sécurité. Ce point n'a quasiment pas été abordé dans la littérature pour les schémas basés sur le chaos. La robustesse de ces schémas face à des attaques pirates est étudiée.

Le Chapitre 1 est constitué de rappels sur les systèmes non linéaires avec un accent particulier porté sur les systèmes à temps discret. En effet, dans la suite de la thèse, les systèmes à temps continu ne seront plus considérés. Les régimes permanents des systèmes autonomes sont rappelés ainsi que les bifurcations associées. Le chaos est défini de façon formelle. Les conditions de stabilité des systèmes non linéaires, en particulier celles des systèmes linéaires à paramètres variants (systèmes LPV), sont détaillées. La justification de l'intérêt porté aux systèmes LPV est que la plupart des systèmes chaotiques peuvent se réécrire sous cette forme. Les résultats de stabilité seront utilisés dans les chapitres suivants lors de la synthèse d'observateurs non linéaires pour la synchronisation du chaos.

Le Chapitre 2 aborde la notion de cryptographie. Les deux principaux schémas de chiffrement en cryptographie usuelle, le chiffrement à clé publique et le chiffrement symétrique, par blocs ou par flot, sont décrits. Plusieurs modes de chiffrement de l'information incluant une dynamique chaotique, proposés dans la littérature, sont présentés : le masquage additif, la modulation chaotique, la modulation paramétrique et le chiffrement par inclusion. Une comparaison entre le chiffrement par le chaos et le chiffrement usuel par flot est menée [Millérioux et al., 2003] [Anstett et al., 2005b] [Anstett et al., 2005c] [Anstett et al., 2005d]. Dans la suite, nous nous intéressons à la modulation chaotique, à la modulation paramétrique et au chiffrement par inclusion.

Le Chapitre 3 est dédié à la modulation chaotique. Côté récepteur, la reconstruction de l'information nécessite la synchronisation de l'émetteur et du récepteur. Par synchronisation, on entend la convergence de la trajectoire d'état du récepteur vers celle de l'émetteur. Un observateur joue le rôle du récepteur et la stabilité de l'erreur de reconstruction d'état doit être garantie. Quelques structures d'observateurs non linéaires à temps discret, proposées dans la littérature, sont rappelées. Puis, l'étude se concentre sur les observateurs polytopiques qui ont l'avantage de prendre en compte la spécificité du problème liée au caractère chaotique des dynamiques. Le but est de réduire le conservatisme des conditions de stabilité de l'erreur de reconstruction d'état et d'étendre ainsi la classe des systèmes utilisés pour le chiffrement. Une méthode systématique de synthèse d'observateur polytopique, qui intègre la recherche du polytope minimal intervenant dans la description LPV, est proposée [Millérioux et al., 2005]. Son application à la modulation chaotique est illustrée sur un exemple de simulation.

Le Chapitre 4 traite de la modulation paramétrique. Dans ce schéma, côté émetteur, l'information à masquer module les paramètres d'un système chaotique. Pour réaliser la synchronisation, un observateur adaptatif assurant la reconstruction simultanée état/paramètre peut être utilisé. Quelques structures d'observateurs adaptatifs issues de la littérature sont rappelées. Puis, un observateur adaptatif polytopique est proposé [Millérioux et al., 2005] [Anstett et al., 2004]. Sa synthèse est basée sur la méthode élaborée dans le Chapitre 3, en considérant le vecteur d'état étendu. Là encore, contrairement à la plupart des observateurs usuels, les observateurs polytopiques prennent en compte la spécificité chaotique. Enfin, un exemple de reconstruction simultanée état/paramètre basée sur cette approche est donné dans un contexte de modulation paramétrique.

Dans le Chapitre 5, la cryptanalyse du chiffrement par inclusion est réalisée. La cryptanalyse, étape déterminante dans la validation d'un schéma de chiffrement, fait largement défaut pour le chiffrement par inclusion. Dans ce schéma, la sécurité repose sur les paramètres du système chaotique, supposés jouer le rôle de clé secrète. La difficulté de reconstruire ces paramètres pour

un adversaire doit alors être évaluée selon les attaques envisagées : attaque brute, attaque à texte clair choisi ... Un formalisme général basé sur le concept d'identifiabilité est élaboré [Anstett et al., 2005a] [Anstett et al., 2005c]. Les différentes définitions de l'identifiabilité sont récapitulées et les approches permettant de tester l'identifiabilité paramétrique sont présentées. Ce formalisme est ensuite appliqué sur des schémas usuels de chiffrement par inclusion, afin de tester leur sécurité.

L'Annexe A est constituée de diverses définitions. Dans l'Annexe B, des rappels d'algèbre, utilisés dans la description des approches permettant de tester l'identifiabilité paramétrique, sont effectués. L'Annexe C traite de la complexité des algorithmes.

Dans la Conclusion, il est montré que les différents concepts de l'Automatique utilisés dans ces travaux trouvent également d'autres applications que le chiffrement. Des perspectives de travaux futurs y sont également proposées.

Les travaux menés ont fait l'objet des publications suivantes.

[Millérioux et al., 2003] Millérioux, G., Bloch, G., Amigo, J. M., Bastos, A., and Anstett, F. (2003). Real-time video communication secured by a chaotic key stream cipher. In *Proc. of IEEE 16th European Conference on Circuits Theory and Design, ECCTD'03*, pages 245–248, Krakow, Poland. September 1-4.

[Anstett et al., 2004] Anstett, F., Millérioux, G., and Bloch, G. (2004). Global adaptive synchronization based upon polytopic observers. In *Proc. of IEEE International Symposium on Circuits and Systems, ISCAS'04*, volume 4, pages IV-728 – 731, Vancouver, Canada. May 23-26.

[Anstett et al., 2005d] Anstett, F., Millérioux, G., and Bloch, G. (2005d). Systèmes dynamiques et chiffrement en continu. *Journées Codage et Cryptographie*, Aussois, France. 30 Janvier-04 Février.

[Anstett et al., 2005b] Anstett, F., Millérioux, G., and Bloch, G. (2005b). Chiffrement par flot chaotique : cryptanalyse et identifiabilité. *Journées Doctorales et Nationales du GDR MACS*, Lyon, France. 5-7 Septembre.

[Millérioux et al., 2005] Millérioux, G., Anstett, F., and Bloch, G. (2005). Considering the attractor structure of chaotic maps for observer-based synchronization problems. *Mathematics and Computers in Simulation*, 68(1) :67–85, February.

[Anstett et al., 2005c] Anstett, F., Millérioux, G., and Bloch, G. (2005c). Message-embedded cryptosystems : cryptanalysis and identifiability. In *Proc. of the 44th IEEE Conference on Decision and Control and European Conference on Control, CDC-ECC'05*, pages 2548-2553, Sevilla, Spain. December 12-15.

[Anstett et al., 2005a] Anstett, F., Millérioux, G., and Bloch, G. (2005a). Chaotic cryptosystems : cryptanalysis and identifiability. *IEEE Trans. on Circuits and Systems I*. En révision.

Chapitre 1

Systèmes non linéaires

1.1 Introduction

Dans cette thèse, nous étudions l'utilisation des systèmes chaotiques à des fins de chiffrement de données. Dans ce contexte, l'émetteur est régi par une dynamique non linéaire chaotique. Dans ce chapitre, quelques rappels sur les systèmes non linéaires autonomes sont effectués. Les résultats fondamentaux qui y sont exposés peuvent être trouvés, parmi de nombreux ouvrages sur les systèmes non linéaires, dans [Nijmeijer and Van Der Schaft, 1990] [Slotine and Li, 1991] [Khalil, 1996] et, plus particulièrement pour les systèmes chaotiques, dans [Chen and Dong, 1998]. La notion d'espace d'état est rappelée dans la Section 1.2. La Section 1.3 traite des régimes permanents des systèmes dynamiques autonomes. La Section 1.4 introduit la notion de chaos qui sera largement considérée dans ce mémoire. Quelques rappels portent sur les bassins d'attraction (Section 1.5) et les bifurcations (Section 1.6).
Dans un contexte de chiffrement basé sur le chaos, la récupération de l'information chiffrée nécessitera la synchronisation de l'émetteur et du récepteur. Il s'agit alors de garantir la convergence à zéro de l'erreur de reconstruction d'état. Dans la Section 1.7, les méthodes directes et indirectes de Lyapunov, permettant de tester la stabilité des systèmes non linéaires autonomes, sont exposées.
De nombreux systèmes chaotiques peuvent être réécrits sous une forme appelée LPV (Linear Parameter Varying). Les systèmes LPV ou systèmes linéaires à paramètres variants sont décrits par une équation affine en l'état, mais non linéaire, car dépendant d'un vecteur de paramètres variant dans le temps. Dans la Section 1.8, le problème de la stabilité des systèmes linéaires à paramètres variants est adressé.

1.2 Notion d'espace d'état

Un **S**ystème **L**inéaire **I**nvariant dans le **T**emps (SLIT), autonome, de dimension n, a pour représentation d'état :

$$\text{Cas continu} \begin{cases} \dot{x}(t) = Ax(t) \\ y(t) = Cx(t) \end{cases} \qquad \text{Cas discret} \begin{cases} x_{k+1} = Ax_k \\ y_k \quad = Cx_k \end{cases} \tag{1.1}$$

où $A \in \mathbb{R}^{n \times n}$ est la matrice d'état, $C \in \mathbb{R}^{p \times n}$ la matrice d'observation, $x(t) \in \mathbb{R}^n$ (respectivement $x_k \in \mathbb{R}^n$) est le vecteur d'état et $y(t) \in \mathbb{R}^p$ (resp. $y_k \in \mathbb{R}^p$) le vecteur de sortie.
Les équations différentielles (resp. récurrentes) représentent des systèmes qui possèdent une dynamique.

Un système non linéaire autonome, de dimension n, a pour représentation d'état, en temps continu :

$$\begin{cases} \dot{x}(t) = f(x(t)) \\ y(t) = h(x(t)) \end{cases} \tag{1.2}$$

en temps discret :

$$\begin{cases} x_{k+1} = f(x_k) \\ y_k \quad = h(x_k) \end{cases} \tag{1.3}$$

où $f : \mathbb{R}^n \to \mathbb{R}^n$ est une fonction non linéaire et $h : \mathbb{R}^n \to \mathbb{R}$ une fonction éventuellement non linéaire.

Le vecteur d'état $x(t) = [x^{(1)}(t) \dots x^{(n)}(t)]^T$, en temps continu, ou $x_k = [x_k^{(1)} \dots x_k^{(n)}]^T$, en temps discret, évolue dans l'espace d'état ou espace de phase. Dans le cas particulier où $n = 2$, l'espace de phase est dit plan de phase. Soit $x(t)$ la solution du système (1.2) issue de la condition initiale $x(0)$ (ou x_k la solution du système (1.3) issue de x_0). La trajectoire $x(t)$ (ou x_k) dans l'espace d'état est appelée *trajectoire de phase* ou *orbite* du système, issue de la condition initiale $x(0)$ (ou x_0). La figure 1.1 illustre le plan de phase et une trajectoire de phase pour un système en temps continu.

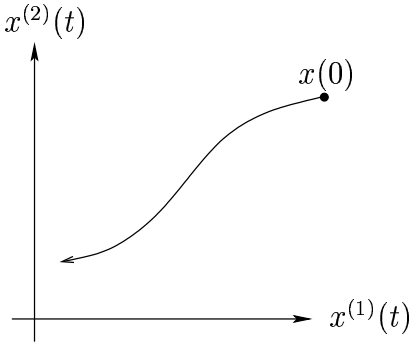


FIG. 1.1 – Plan de phase et trajectoire de phase

1.3 Régimes permanents des systèmes dynamiques autonomes

On s'intéresse aux régimes permanents des systèmes linéaires (1.1), puis à ceux des systèmes non linéaires (1.2) et (1.3).

1.3.1 Systèmes linéaires

Définition d'un point d'équilibre
Un point d'équilibre (ou *point fixe*), noté x^*, est un point qui vérifie, en temps continu :

$$Ax^* = 0 \tag{1.4}$$

en temps discret :

$$Ax^* = x^* \tag{1.5}$$

Un point d'équilibre est une singularité (point singulier) de l'espace de phase.
Pour les systèmes linéaires, lorsque A est non singulière ($\det(A) \neq 0$), on a $x^* = 0$; dans le cas contraire ($\det(A) = 0$), il y a une infinité de points d'équilibre.

Stabilité d'un point d'équilibre
Le point d'équilibre x^* est stable si, lorsqu'on écarte le système de ce point d'équilibre, il y revient, quelles que soient les conditions initiales $x(0)$ (resp. x_0) prises dans un voisinage de x^*.
Le point d'équilibre x^* est stable si les valeurs propres λ_i de A ont leurs parties réelles strictement négatives (temps continu) ou sont situées strictement à l'intérieur du cercle unité (temps discret). Dans ce cas, on a, en temps continu :

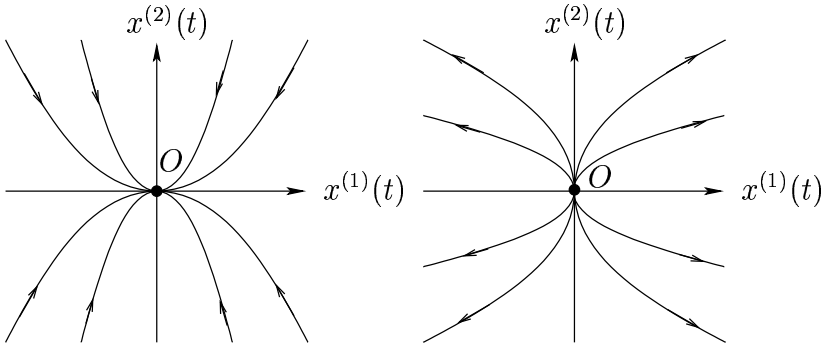
$$\forall x(0), \quad \lim_{t\to\infty} x(t) = x^* \tag{1.6}$$

en temps discret :

$$\forall x_0, \quad \lim_{k\to\infty} x_{k+1} = \lim_{k\to\infty} x_k = x^* \tag{1.7}$$

Nature d'un point d'équilibre
Pour $n = 2$, il existe trois types de point d'équilibre, *noeud*, *col*, et *foyer*, suivant les valeurs propres λ_1 et λ_2 du système (1.1) ($\lambda_1 \neq 0$ et $\lambda_2 \neq 0$). Sur les figures, données pour des systèmes à temps continu, les flèches indiquent le sens croissant du temps et O indique le point d'équilibre.

- *Noeud*
  Si les valeurs propres λ_i de A sont réelles et ont même signe, le point d'équilibre est un noeud.
  En temps continu, si $\lambda_1 < \lambda_2 < 0$, le noeud est stable (figure 1.2(a)). En temps discret, si $0 < \lambda_1 < \lambda_2 < 1$ ou si $-1 < \lambda_1 < \lambda_2 < 0$, le noeud est stable.
  En temps continu, si $\lambda_1 > \lambda_2 > 0$, le noeud est instable (figure 1.2(b)). En temps discret, si $1 < |\lambda_1| < |\lambda_2|$, le noeud est instable.



(a) Noeud stable (b) Noeud instable

FIG. 1.2 – Point d'équilibre de type noeud

- *Col*
  Si les valeurs propres sont réelles et de signe opposé (temps continu) ou si $|\lambda_1| < 1$ et $|\lambda_2| > 1$ (temps discret), le point d'équilibre est un col, représenté sur la figure 1.3.

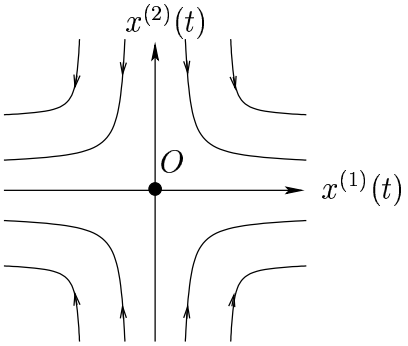
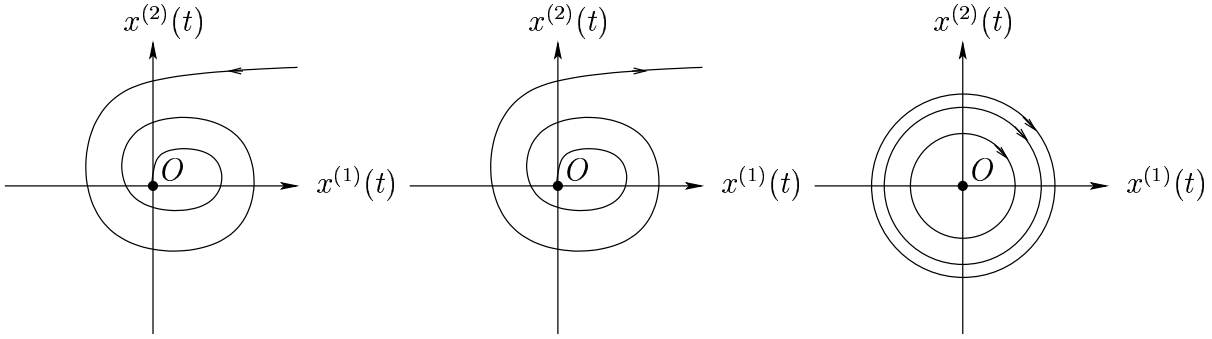


FIG. 1.3 – Point d'équilibre de type col

– *Foyer*
Si les valeurs propres sont complexes conjuguées, $\lambda_{1,2} = a \pm jb$, le point d'équilibre est un foyer.
Si $a < 0$ (temps continu) ou si $|\lambda_1| < 1$ et $|\lambda_2| < 1$ (temps discret), le foyer est stable (figure 1.4(a)).
Si $a > 0$ (temps continu) ou si $|\lambda_1| > 1$ et $|\lambda_2| > 1$ (temps discret), le foyer est instable (figure 1.4(b)).



(a) Foyer stable (b) Foyer instable (c) Centre

FIG. 1.4 – Point d'équilibre de type foyer

Si $\lambda_{1,2} = \pm jb$ ($a = 0$), le point d'équilibre est de type centre (figure 1.4(c)), mais, en pratique, a n'est jamais strictement nul.

Le seul régime permanent issu d'une condition initiale est le point d'équilibre stable.

1.3.2 Systèmes non linéaires

Définition d'un point d'équilibre
Considérons le système (1.2) en temps continu ou (1.3) en temps discret. Un point d'équilibre x^* est un point qui vérifie, en temps continu :

$$f(x^*) = 0 \tag{1.8}$$

en temps discret :

$$f(x^*) = x^* \tag{1.9}$$

Dans le cas des systèmes non linéaires, on peut avoir $x^* \neq 0$ et il peut avoir plusieurs points d'équilibre.

Cycle limite (temps continu)
Un cycle limite, qui n'existe que pour les systèmes à temps continu, est une oscillation de période fixe T : $x(t+T) = x(t)$.
Pour les systèmes linéaires, les oscillations dépendent des conditions initiales et sont sinusoïdales pour un point d'équilibre de type centre. Pour les systèmes non linéaires, les oscillations, en régime permanent, ne dépendent pas des conditions initiales et sont éventuellement non sinusoïdales.
Par exemple, l'oscillateur de Van Der Pol, défini par les équations différentielles (1.10), présente un cycle limite, représenté sur la figure 1.5. Lorsque les trajectoires du système tendent vers le cycle limite, représentée en trait plein gras sur la figure 1.5, le régime ne dépend plus des conditions initiales.

$$\begin{cases} \dot{x}^{(1)}(t) = x^{(2)}(t) \\ \dot{x}^{(2)}(t) = -x^{(1)}(t) + (1 - (x^{(1)}(t))^2)x^{(2)}(t) \end{cases} \tag{1.10}$$

Un critère d'existence et de stabilité des cycles limites est basé sur l'approximation du premier

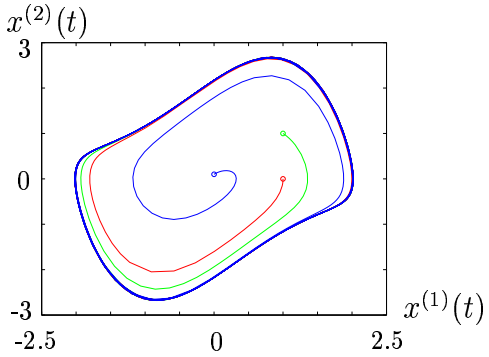


FIG. 1.5 – Cycle limite de l'oscillateur de Van Der Pol

harmonique.

Cycle d'ordre K (temps discret)
Un cycle d'ordre K n'a de sens que pour les systèmes à temps discret. Il est défini par un ensemble fini de points x^{*i}, $i = 1, \ldots, K$, $K > 1$ qui vérifient les deux relations suivantes :

$$\begin{cases} x^{*i}_{k+K} = x^{*i}_k \\ \\ x^{*i}_{k+l} \neq x^{*i}_k, \quad 1 < l < K \end{cases} \tag{1.11}$$

Pour $K = 1$, le cycle se réduit à un point d'équilibre. Ainsi, un cycle d'ordre K est une généralisation d'un point d'équilibre.

Les x^{*i}, $i = 1, \ldots, K$, sont des points d'équilibre pour f^K (K compositions de la fonction non linéaire f (1.3)). La figure 1.6 donne un exemple de cycle d'ordre $K = 3$, dans le plan de phase. Un cycle d'ordre K est stable si $|\lambda_i(J_K \ldots J_1)| < 1$. $\lambda_i(J_K \ldots J_1)$ représente la ième valeur propre

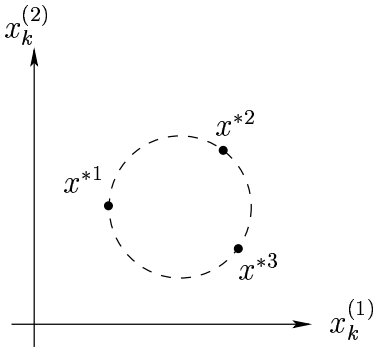


FIG. 1.6 – Exemple de cycle d'ordre 3

du produit des matrices jacobiennes [1]$(J_K \ldots J_1)$.

Courbe invariante fermée (temps discret)
Une courbe invariante fermée, notée Γ, est une variété de dimension 1 sur laquelle les x_k se répartissent par applications successives de f (équation (1.3))
Dans une courbe invariante fermée, il n'y a plus la notion de périodicité comme dans les cycles d'ordre K.
La figure 1.7 illustre un exemple de courbe invariante fermée, obtenue après un transitoire, pour la récurrence suivante :

$$\begin{cases} x_{k+1}^{(1)} = \theta^{(1)} x_k^{(1)} + x_k^{(2)}, & \theta^{(1)} = -1.5 \\ x_{k+1}^{(2)} = (x_k^{(1)})^2 + \theta^{(2)}, & \theta^{(2)} = -1.6 \end{cases} \tag{1.12}$$

avec la condition initiale $x_0 = [1 \quad 2]^T$.

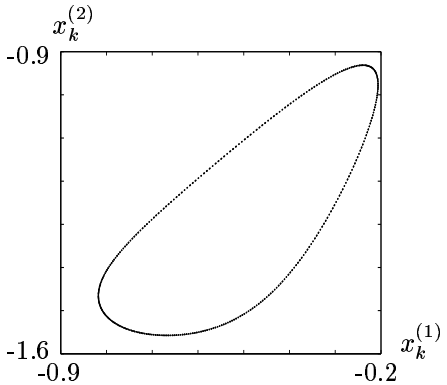


FIG. 1.7 – Exemple de courbe invariante fermée

[1] Voir Annexe A, Définition 28

Il existe un dernier régime permanent des systèmes non linéaires autonomes qui est plus complexe et qui est appelé attracteur chaotique. Avant de l'exposer, la définition du chaos est donnée dans la section suivante.

1.4 Chaos

1.4.1 Définition du chaos

Il n'existe pas de définition du chaos adoptée de façon universelle dans la littérature. On rappelle une définition intéressante, proposée par Devaney [Devaney, 1989] pour les systèmes à temps discret.

Définition 1. Soient $(\mathcal{X}, \delta)$ un espace métrique compact[1] et $f : \mathcal{X} \to \mathcal{X}$, une fonction.
Le système dynamique à temps discret

$$x_{k+1} = f(x_k) \tag{1.13}$$

est dit *chaotique* si les conditions suivantes sont vérifiées.

- *Sensibilité aux conditions initiales*
  Il existe un nombre réel $\epsilon > 0$ tel que, pour tout $x_0 \in \mathcal{X}$ et pour tout $\beta > 0$, il existe un point $y_0 \in \mathcal{X}$ et un entier $k > 0$, vérifiant :

$$\delta(x_0, y_0) < \beta \Rightarrow \delta(x_k, y_k) > \epsilon \tag{1.14}$$

- *Transitivité topologique*
  La fonction f est topologiquement transitive s'il existe $x_k \in \mathcal{X}$ tel que l'orbite $\{f^K(x_k) | K \in \mathbb{Z}^+\}$ est dense[2] dans $\mathcal{X}$. f^K représente la K-ième composition de la fonction f.

- *Densité des orbites périodiques*
  L'ensemble des orbites périodiques $\{x_0 \in \mathcal{X}; \exists k > 0, x_k = x_0\}$ est dense dans $\mathcal{X}$.

Dans la condition de transitivité topologique, $f^K(x_k)$ est le résultat de K compositions de la fonction f. $\{f^K(x_k) | K \in \mathbb{Z}^+\}$ représente l'ensemble des compositions de f et est appelé orbite. La condition de transitivité topologique est équivalente à la condition suivante : f est topologiquement transitive s'il existe deux ensembles ouverts non vides E et F de $\mathcal{X}$ et un entier $K > 0$, tels que $f^K(E) \cap F \neq \emptyset$.

Un système chaotique est décrit par un ensemble d'équations dynamiques non linéaires et déterministes. Bien que ses équations définissent complètement son évolution, il est *imprédictible à long terme*. Cette non prédictibilité à long terme provient du fait que les systèmes chaotiques sont *très sensibles aux conditions initiales*. Deux trajectoires issues de conditions initiales proches vont vite devenir décorrélées.
La précision avec laquelle les conditions initiales doivent être spécifiées pour prédire le comportement futur, sur un intervalle de temps donné, croît, en général, de façon exponentielle avec la longueur de l'intervalle de prédiction. La prédiction à long terme devient alors impossible.

Dans l'espace de phase, le chaos donne lieu à des trajectoires, appelées attracteur chaotique. La figure 1.8 montre un exemple d'attracteur chaotique. Pour cette figure, la récurrence (1.12)

[1] Voir Annexe A, Définitions 29 et 31
[2] Voir Annexe A, Définition 32

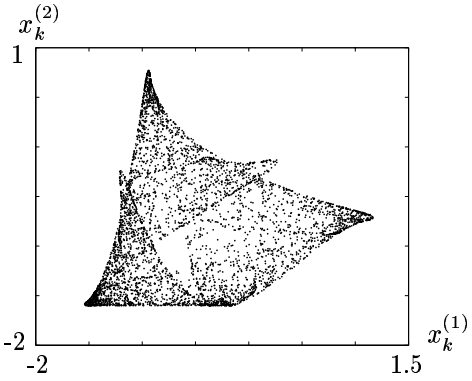


FIG. 1.8 – Exemple d'attracteur chaotique

est utilisée avec les paramètres $\theta^{(1)} = -0.42$ et $\theta^{(2)} = -1.6$.

Pour prouver qu'une fonction est chaotique, la notion de conjugaison topologique peut être utilisée.

Définition 2. Deux fonctions $f : \mathcal{X}_1 \to \mathcal{X}_1$ et $g : \mathcal{X}_2 \to \mathcal{X}_2$ sont topologiquement conjuguées s'il existe une fonction bijective continue $h : \mathcal{X}_1 \to \mathcal{X}_2$, telle que son inverse h^{-1} est continue et $f \circ h = h \circ g$.

Le théorème suivant est énoncé dans [Devaney, 1989].

Théorème 1. Si f est une fonction chaotique et que g est topologiquement conjuguée à f, alors g est chaotique.

Exemple 1. Soient $\mathcal{X}_1$ et $\mathcal{X}_2$ deux ensembles compacts, définis respectivement par $\mathcal{X}_1 = [0; 1]$ et $\mathcal{X}_2 = [-1; 1]$. Considérons les fonctions $f : \mathcal{X}_1 \to \mathcal{X}_1$, $g : \mathcal{X}_2 \to \mathcal{X}_2$ et $h : \mathcal{X}_1 \to \mathcal{X}_2$, définies respectivement par :

$$\begin{aligned} f(x_k) &= 4x_k(1 - x_k) \\ g(x_k) &= 2x_k^2 - 1 \\ h(x_k) &= 0.5(1 - x_k) \end{aligned} \tag{1.15}$$

Les fonctions f et g sont topologiquement conjuguées à travers h car $f \circ h = h \circ g = 1 - x_k^2$. Il a été montré que f, représentant la fonction logistique rappelée dans la Section 1.4.2, est chaotique. Comme f est chaotique, g est également chaotique, d'après le Théorème 1.

1.4.2 Quelques exemples de récurrences chaotiques

Récurrence logistique

La récurrence logistique, utilisée par le biologiste Robert May en 1976 [May, 1976], décrit l'évolution de la population d'une espèce. Elle est de dimension 1 et a pour représentation d'état :

$$x_{k+1} = \theta x_k(1 - x_k) \tag{1.16}$$

avec $0 < \theta \leq 4$. Le vecteur d'état $x_k \in [0; 1]$ représente la population à l'année k, et le paramètre θ représente un facteur de croissance de la population.

Récurrence de Hénon

La récurrence de Hénon [Hénon, 1976], de dimension 2, a pour représentation d'état :

$$\begin{cases} x_{k+1}^{(1)} = -1.4(x_k^{(1)})^2 + x_k^{(2)} + 1 \\ x_{k+1}^{(2)} = 0.3x_k^{(1)} \end{cases} \tag{1.17}$$

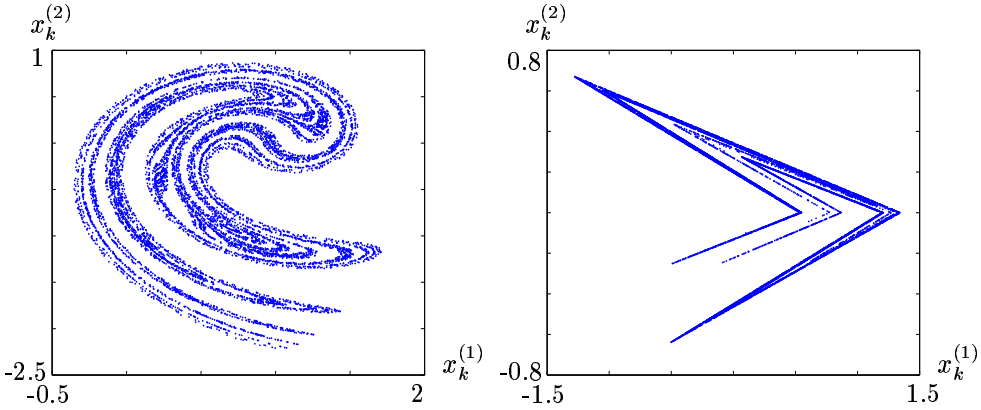
L'attracteur de Hénon et son bassin d'attraction (voir Section 1.5) sont représentés sur la figure 1.10.

Récurrence d'Ikeda

Cette récurrence de dimension 2, utilisée en optique par le physicien Ikeda [Ikeda, 1979], admet la représentation d'état suivante :

$$\begin{cases} x_{k+1}^{(1)} = 1 + 0.9(x_k^{(1)}\cos(\theta_k) - x_k^{(2)}\sin(\theta_k)) \\ x_{k+1}^{(2)} = 0.9(x_k^{(1)}\sin(\theta_k) + x_k^{(2)}\cos(\theta_k)) \\ \theta_k = 0.4 - \dfrac{6}{1 + (x_k^{(1)})^2 + (x_k^{(2)})^2} \end{cases} \tag{1.18}$$

L'attracteur correspondant à cette récurrence est représenté sur la figure 1.9(a).



(a) Récurrence d'Ikeda (b) Récurrence de Lozi

FIG. 1.9 – Attracteurs chaotiques

Récurrence de Lozi

La récurrence de Lozi, de dimension 2, peut être trouvée dans [Peitgen et al., 1992] et est donnée par la représentation d'état suivante :

$$\begin{cases} x_{k+1}^{(1)} = -1.7|x_k^{(1)}| + x_k^{(2)} + 1 \\ x_{k+1}^{(2)} = 0.5x_k^{(1)} \end{cases} \tag{1.19}$$

L'attracteur correspondant à cette récurrence est représenté sur la figure 1.9(b).

1.4.3 Exposants de Lyapunov

Les valeurs propres de la matrice dynamique A des systèmes linéaires permettent de caractériser les points d'équilibre et leur stabilité. Les exposants de Lyapunov sont une généralisation de ces valeurs propres et permettent de caractériser un attracteur Ω. Les exposants de Lyapunov sont des grandeurs qui mesurent la divergence entre différentes trajectoires au sein d'un attracteur.

Soit un système dynamique autonome :

$$x_{k+1} = f(x_k) \tag{1.20}$$

On considère d'abord que ce système est de dimension $n = 1$. Soient deux conditions initiales très proches, x_0 et x'_0. La trajectoire issue de la condition initiale x_0 est $x_k = f^k(x_0)$, et celle issue de la condition initiale x'_0 est $x'_k = f^k(x'_0)$.
Si les trajectoires x_k et x'_k s'écartent à un rythme exponentiel après k itérations, alors :

$$|x'_k - x_k| = |x'_0 - x_0| \exp(k\lambda) \tag{1.21}$$

$\lambda \in \mathbb{R}$ correspond au taux de divergence des deux trajectoires. Il vient :

$$\lambda = \frac{1}{k} \ln \left| \frac{x'_k - x_k}{x'_0 - x_0} \right| \tag{1.22}$$

Si l'on considère que les deux conditions initiales sont très proches, leur différence $\epsilon = |x'_0 - x_0|$ tend vers 0 et, lorsque k tend vers l'infini, il vient :

$$\lambda_L = \lim_{k \to \infty} \frac{1}{k} \lim_{\epsilon \to 0} \ln \left| \frac{x'_k - x_k}{x'_0 - x_0} \right| \tag{1.23}$$

Cette relation est équivalente à :

$$\lambda_L = \lim_{k \to \infty} \frac{1}{k} \lim_{\epsilon \to 0} \ln \left| \frac{x'_k - x_k}{x'_{k-1} - x_{k-1}} \cdot \frac{x'_{k-1} - x_{k-1}}{x'_{k-2} - x_{k-2}} \cdot \ldots \cdot \frac{x'_1 - x_1}{x'_0 - x_0} \right| \tag{1.24}$$

ce qui se réécrit aussi :

$$\lambda_L = \lim_{k \to \infty} \frac{1}{k} \lim_{\epsilon \to 0} \sum_{i=0}^{k-1} \ln \left| \frac{x'_{i+1} - x_{i+1}}{x'_i - x_i} \right| = \lim_{k \to \infty} \frac{1}{k} \lim_{\epsilon \to 0} \sum_{i=0}^{k-1} \ln \left| \frac{f(x'_i) - f(x_i)}{x'_i - x_i} \right| \tag{1.25}$$

Finalement, cette relation devient :

$$\lambda_L = \lim_{k \to \infty} \frac{1}{k} \sum_{i=0}^{k-1} \ln \left| \frac{df(x_i)}{dx_i} \right| \tag{1.26}$$

Le terme λ_L est appelé *exposant de Lyapunov* de la trajectoire $x_k = f^k(x_0)$ et ne doit pas être confondu avec λ ou λ_i, valeur propre d'un système linéaire. λ_L mesure le taux moyen de convergence ou de divergence de deux trajectoires issues de conditions initiales très proches. S'il est positif, les trajectoires divergent. Très souvent dans la littérature, si $\lambda_L > 0$, le système est dit chaotique. Intuitivement, cela reflète la sensibilité aux conditions initiales.

La relation (1.26) se généralise aux systèmes de dimension $n > 1$, qui possèdent alors n exposants de Lyapunov. Chacun d'entre eux mesure le taux de divergence suivant un des axes de l'espace de phase. On a alors $x_k = f^k(x_0)$ avec $x_k = [x_k^{(1)} \dots x_k^{(n)}]^T \in \mathbb{R}^n$ et $f = [f_1 \dots f_n]^T$. Les n exposants de Lyapunov λ_{Li} s'écrivent :

$$\lambda_{Li} = \lim_{k\to\infty} \frac{1}{k} \ln \left|\lambda_i\big(J_k \dots J_1\big)\right|, \quad i = 1, \dots, n \tag{1.27}$$

$\lambda_i\big(J_k \dots J_1\big)$ représente la ième valeur propre du produit des matrices $(J_k \dots J_1)$. Les J_k sont les matrices jacobiennes[1] issues de la linéarisation de f autour de x_k.

Une condition nécessaire pour qu'un système dynamique à temps discret (1.20) soit chaotique est qu'au moins un de ses exposants de Lyapunov soit positif.

1.5 Bassin d'attraction d'un attracteur

Un *attracteur* Ω d'un système dynamique est un ensemble particulier d'états, sous-ensemble de l'espace d'état, qui est le régime permanent du système. Un *bassin d'attraction* $\mathcal{D}$ est l'ensemble des initialisations telles que les itérés issus de celles-ci tendent vers l'attracteur Ω considéré.

Pour les systèmes linéaires, le seul attracteur possible, sauf cas dégénérés, est un point fixe stable. Le bassin d'attraction est alors l'espace de phase complet ($\mathcal{D} = \mathbb{R}^n$).

Pour les systèmes non linéaires, l'attracteur peut être constitué d'un ou de plusieurs points d'équilibre, d'un cycle limite, d'un cycle d'ordre K, d'une courbe invariante fermée ou d'un attracteur chaotique. Plusieurs attracteurs peuvent coexister dans l'espace de phase. A chaque attracteur, noté alors Ω_i, correspond un bassin d'attraction $\mathcal{D}_i$. En général, $\mathcal{D}_i$ est un sous-ensemble de $\mathbb{R}^n$.
Le bassin d'attraction obtenu pour l'attracteur chaotique de Hénon est illustré sur la figure 1.10. La récurrence de Hénon est décrite par :

$$\begin{cases} x_{k+1}^{(1)} = \theta^{(1)}(x_k^{(1)})^2 + x_k^{(2)} + 1, & \theta^{(1)} = -1.4 \\ x_{k+1}^{(2)} = \theta^{(2)} x_k^{(1)}, & \theta^{(2)} = 0.3 \end{cases} \tag{1.28}$$

Dans la plupart des cas, la frontière des bassins d'attraction ne peut pas être explicitée analytiquement. Elle peut être estimée par simulations numériques.

1.6 Bifurcations

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

Nous nous intéressons à des bifurcations locales, c'est-à-dire ayant lieu au voisinage d'un point

[1] Voir Annexe A, Définition 28

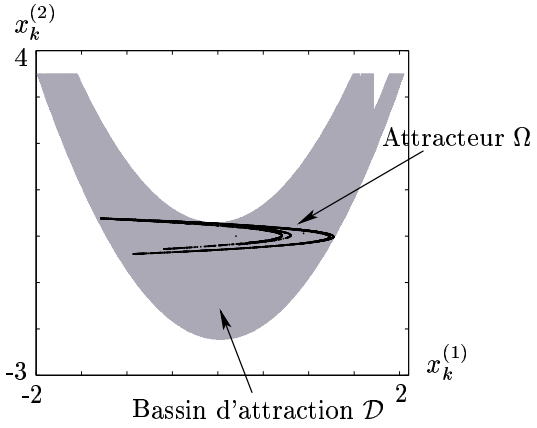


FIG. 1.10 – L'attracteur de Hénon et son bassin d'attraction

d'équilibre. Pour cela, nous considérons des systèmes dépendant d'un paramètre μ, de la forme, en temps continu :

$$\dot{x}(t) = f(x(t), \mu) \tag{1.29}$$

en temps discret :

$$x_{k+1} = f(x_k, \mu) \tag{1.30}$$

La valeur de bifurcation sera notée μ_0.
Soit x^* un point d'équilibre du système (1.29), satisfaisant $f(x^*, \mu) = 0$, ou un point d'équilibre du système (1.30), satisfaisant $f(x^*, \mu) = x^*$. Si le point d'équilibre est stable (resp. instable) quand $\mu > \mu_0$ et instable (resp. stable) quand $\mu < \mu_0$, alors μ_0 est une valeur de bifurcation. Nous allons voir quelques exemples de bifurcations locales, pour les systèmes de dimension 2.

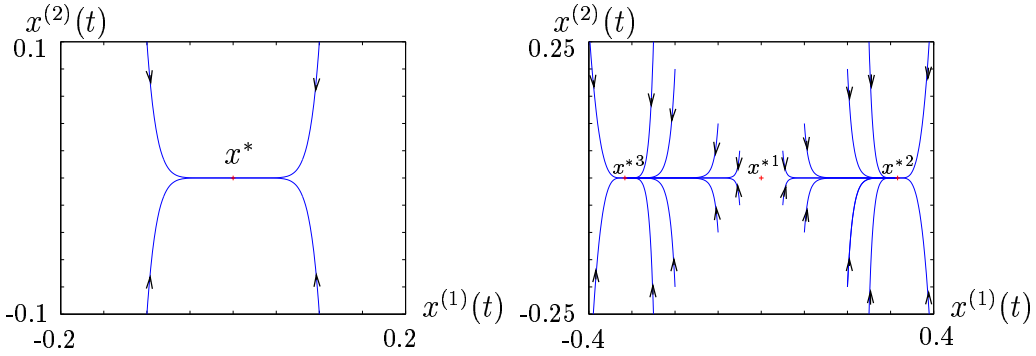
1.6.1 Bifurcation Fold ou Pitchfork

Considérons un système de la forme (1.29) ou (1.30). On suppose que le système possède un unique point d'équilibre de type noeud stable quand $\mu < \mu_0$. Si la valeur de μ augmente et $\mu > \mu_0$, le noeud stable devient un col et deux autres points d'équilibre, de type noeud stable, apparaissent. Cette bifurcation est connue sous le nom de Fold ou Pitchfork.

Considérons, par exemple, le système à temps continu suivant :

$$\begin{cases} \dot{x}^{(1)}(t) = \mu x^{(1)}(t) - (x^{(1)}(t))^3 \\ \dot{x}^{(2)}(t) = -x^{(2)}(t) \end{cases} \tag{1.31}$$

Quand $\mu < 0$, le système possède un unique point d'équilibre $x^* = [0 \quad 0]^T$. Les valeurs propres du système linéarisé autour de x^* sont $\lambda_1 = \mu$ et $\lambda_2 = -1$. Ce point d'équilibre x^* est donc de type noeud stable, il est représenté sur la figure 1.11(a).
Quand $\mu > 0$, le système (1.31) possède trois points d'équilibre $x^{*1} = [0 \quad 0]^T$, $x^{*2} = [\sqrt{\mu} \quad 0]^T$ et $x^{*3} = [-\sqrt{\mu} \quad 0]^T$. Au point d'équilibre x^{*1}, les valeurs propres du système linéarisé sont $\lambda_1 = \mu$ et $\lambda_2 = -1$ et ce point d'équilibre est un col. Aux points d'équilibre x^{*2} et x^{*3}, les valeurs propres du système linéarisé sont $\lambda_1 = -2\mu$ et $\lambda_2 = -1$ et ces points d'équilibre sont de type noeud stable. Les trois points d'équilibre sont représentés sur la figure 1.11(b). La valeur $\mu_0 = 0$ est la valeur de bifurcation.



(a) Noeud stable ($\mu = -0.1$) (b) Noeuds stables et col ($\mu = 0.1$)

FIG. 1.11 – Bifurcation Fold

1.6.2 Bifurcation de Neimark-Hopf

Considérons un système de la forme (1.29) ou (1.30). On suppose que le système possède un point d'équilibre de type foyer stable, si $\mu < \mu_0$. Si la valeur du paramètre μ augmente et $\mu > \mu_0$, le point d'équilibre de type foyer se déstabilise et un cycle limite (temps continu) ou une courbe invariante fermée (temps discret) se forme. Cette bifurcation est connue sous le nom de Hopf pour les systèmes à temps continu et de Neimark pour les systèmes à temps discret.

Considérons, par exemple, le système à temps continu suivant :

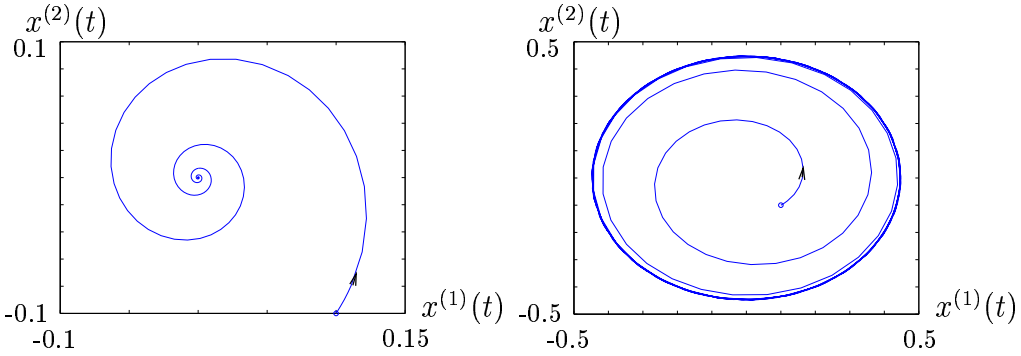
$$\begin{cases} \dot{x}^{(1)}(t) = -x^{(2)}(t) + x^{(1)}(t)(\mu - ((x^{(1)}(t))^2 + (x^{(2)}(t))^2)) \\ \dot{x}^{(2)}(t) = x^{(1)}(t) + x^{(2)}(t)(\mu - ((x^{(1)}(t))^2 + (x^{(2)}(t))^2)) \end{cases} \tag{1.32}$$

Ce système possède le point d'équilibre $x^* = [0 \quad 0]^T$. Les valeurs propres du système linéarisé autour de x^* sont $\lambda_{1,2} = \mu \pm j$. Par conséquent, x^* est de type foyer. Quand $\mu < 0$, le point d'équilibre x^*, représenté sur la figure 1.12(a), est stable. Quand $\mu > 0$, x^* est instable et un cycle limite se forme. Cette situation est représentée sur la figure 1.12(b). $\mu_0 = 0$ est la valeur de bifurcation.

1.6.3 Bifurcation doublement de période ou Flip

Considérons un système de la forme (1.30), qui, pour $\mu < \mu_0$, possède un point fixe stable. Si on augmente μ au-delà de la valeur μ_0, le point d'équilibre se déstabilise et une bifurcation se produit qui donne lieu à un cycle d'ordre 2 stable. Puis, si μ continue d'augmenter, le cycle d'ordre 2 se déstabilise et chacun des deux points du cycle bifurque à son tour. Cette nouvelle bifurcation donne naissance à un cycle d'ordre 4 stable.
Si μ augmente toujours, des bifurcations continuent d'apparaître en doublant la période du cycle à chaque fois, d'où le nom de cette bifurcation ("period doubling", en anglais), conduisant ainsi à une suite infinie de bifurcations et éventuellement au chaos.

Prenons l'exemple de la récurrence de Hénon dont on rappelle ici la représentation d'état (le paramètre μ étant variable) :



(a) Foyer stable ($\mu = -0.2$) (b) Foyer instable et cycle limite ($\mu = 0.2$)

FIG. 1.12 – Bifurcation de Hopf

$$\begin{cases} x_{k+1}^{(1)} = -\mu(x_k^{(1)})^2 + x_k^{(2)} + 1, & \mu > 0 \\ x_{k+1}^{(2)} = \theta^{(1)} x_k^{(1)}, & \theta^{(1)} = 0.3 \end{cases} \tag{1.33}$$

Pour $0 < \mu < 0.36$, le système possède un point fixe stable. Si μ est compris dans l'intervalle $0.36 < \mu < 0.91$, le point fixe se déstabilise et un cycle d'ordre 2 stable apparaît. Puis, si $0.91 < \mu < 1.15$, le cycle d'ordre 2 se déstabilise et un cycle d'ordre 4 stable apparaît et ainsi de suite. La figure 1.13 illustre cette bifurcation doublement de période pour la récurrence de Hénon. Elle a été obtenue en simulant le système (1.33) pour différentes valeurs de μ.

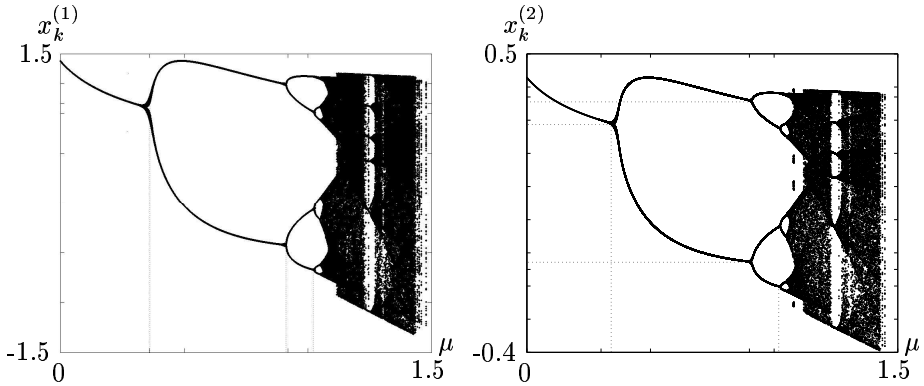


FIG. 1.13 – Bifurcation Period Doubling

1.6.4 Bifurcations vers chaos

Certaines bifurcations, comme celles de type Neimark-Hopf ou de type doublement de période, peuvent conduire au chaos. Un exemple d'apparition d'un attracteur chaotique par la bifurcation de Neimark est décrit ci-dessous.

Considérons la récurrence suivante :

$$\begin{cases} x_{k+1}^{(1)} = x_k^{(1)} \cos\varphi - x_k^{(2)} \sin\varphi \\ x_{k+1}^{(2)} = x_k^{(1)} \sin\varphi + x_k^{(2)} \cos\varphi + \alpha\big(-0.3x_k^{(2)} + 2(x_k^{(2)})^2 + 4(x_k^{(2)})^3 \big) \end{cases} \tag{1.34}$$

avec le paramètre $\varphi = 3.03$ rad.

Lorsque $\alpha < 0$, le système (1.34) possède un point d'équilibre $x^* = [0 \quad 0]^T$. Les valeurs propres du système linéarisé autour de x^* sont complexes conjuguées et leur module est inférieur à 1. x^* est donc de type foyer stable. Les deux exposants de Lyapunov sont négatifs.
Quand $\alpha = 0$, le point d'équilibre de type foyer se déstabilise et une courbe invariante fermée apparaît (figure 1.15(a)). $\alpha_0 = 0$ est une valeur de bifurcation.
Si α augmente et $0 < \alpha < 1.977$, l'un des exposants de Lyapunov, noté λ_{L1}, oscille entre des valeurs positives (comportement apériodique) et des valeurs négatives (cycles d'ordre K stables). La courbe invariante fermée se déforme progressivement, faisant apparaître des oscillations (figure 1.15(c)).
Quand $\alpha \geq 1.977$, l'exposant de Lyapunov λ_{L1} reste positif, signifiant que le système (1.34) reste chaotique (figure 1.16(c)).
Le tableau 1.1 donne quelques valeurs des exposants de Lyapunov λ_{L1} et λ_{L2} en fonction des valeurs du paramètre α et la figure 1.14 représente l'évolution de λ_{L1} en fonction de α.

α	-0.5	0	0.5	1	1.4	1.977
λ_{L1}	-0.0806	3.14×10^{-17}	-8.3345×10^{-6}	4.905×10^{-6}	0.0236	0.1867
λ_{L2}	-0.0806	-2.13×10^{-18}	-0.3064	-0.3609	-0.2582	-0.1448

TAB. 1.1 – Valeurs des exposants de Lyapunov λ_{L1} et λ_{L2} en fonction du paramètre α

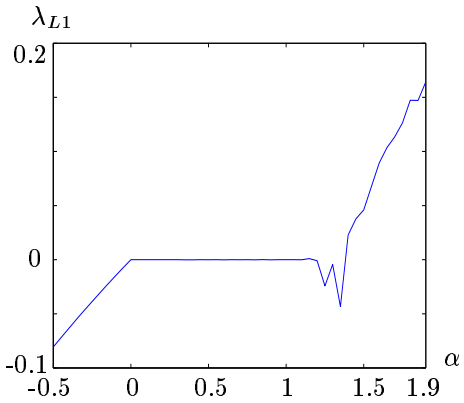
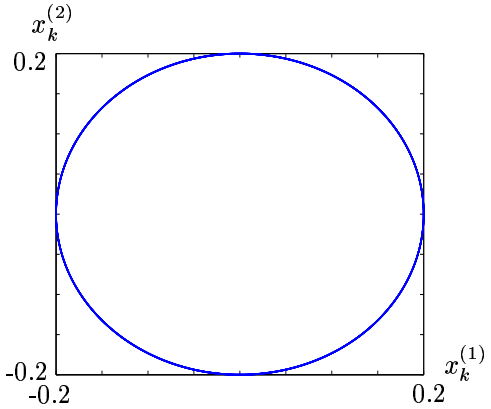


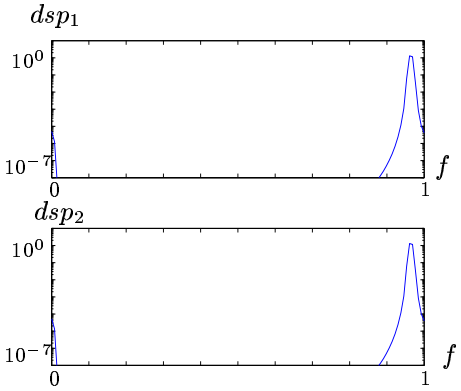
FIG. 1.14 – Evolution de l'exposant de Lyapunov λ_{L1}

Les figures 1.15(b), 1.15(d), 1.16(b) et 1.16(d) représentent le spectre de puissance du signal chaotique $x_k^{(1)}$, noté dsp_1, et le spectre de puissance de $x_k^{(2)}$, noté dsp_2, de la récurrence (1.34), respectivement pour les différentes valeurs de α utilisées précédemment. Si $0 \leq \alpha < 1.4$, l'exposant de Lyapunov λ_{L1} oscille autour de zéro et le spectre de puissance s'élargit progressivement (figures 1.15(b) et 1.15(d)). Plus α augmente ($1.4 \leq \alpha \leq 1.977$), plus λ_{L1}, qui est positif,

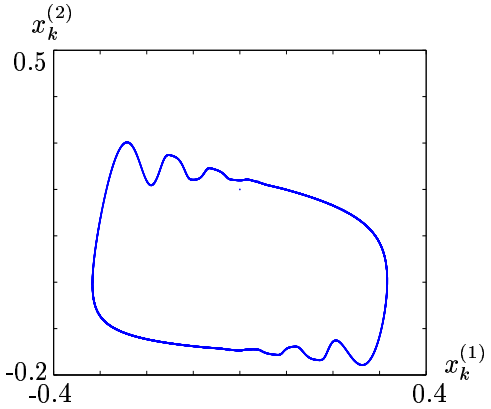
augmente et plus le spectre de puissance s'élargit (figures 1.16(b) et 1.16(d)). La figure 1.17 représente le spectre de puissance d'un signal pseudo-aléatoire, à titre de comparaison.
Les signaux issus des systèmes chaotiques possédant un large spectre en fréquence, leur fonction d'autocorrélation est réduite. Cette caractéristique des systèmes chaotiques est intéressante pour le chiffrement d'information car elle permet de cacher une information à masquer au sein d'un signal s'apparentant à un bruit, supposant rendre ainsi difficile son interception par un adversaire.



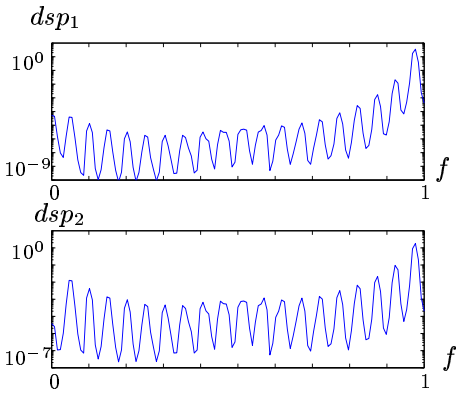
(a) Courbe invariante fermée ($\alpha = 0$)



(b) Spectres de puissance ($\alpha = 0$)

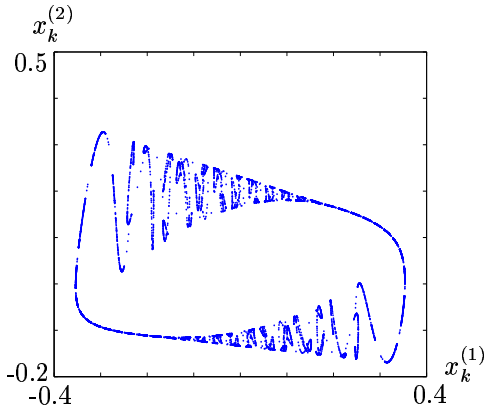


(c) Attracteur ($\alpha = 1$)

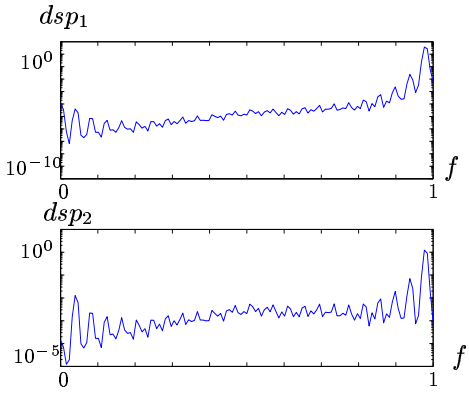


(d) Spectres de puissance ($\alpha = 1$)

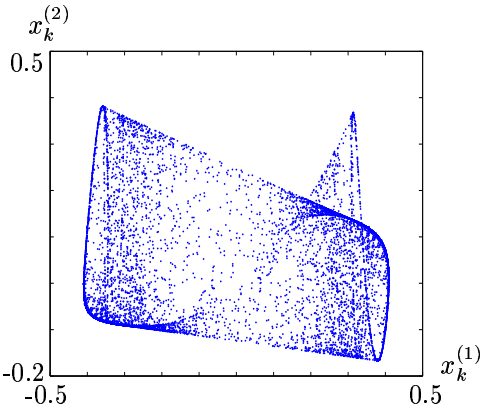
FIG. 1.15 – Attracteurs et spectres de puissance



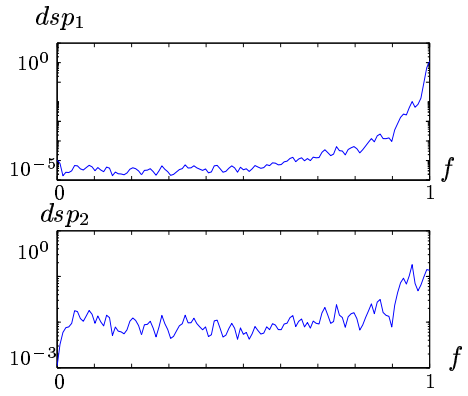
(a) Attracteur ($\alpha = 1.4$)



(b) Spectres de puissance ($\alpha = 1.4$)



(c) Attracteur ($\alpha = 1.977$)



(d) Spectres de puissance ($\alpha = 1.977$)

FIG. 1.16 – Attracteurs chaotiques et spectres de puissance

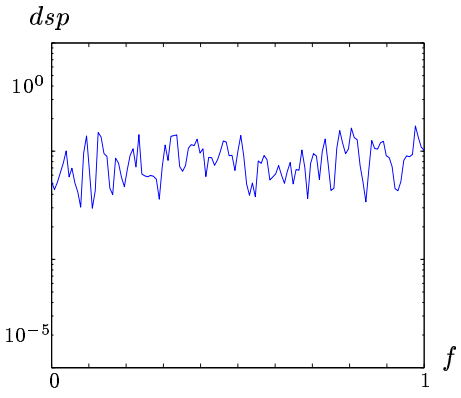


FIG. 1.17 – Spectre de puissance d'un signal pseudo-aléatoire

Dans un contexte de chiffrement basé sur le chaos qui sera introduit dans le Chapitre 2, la récupération de l'information chiffrée nécessitera la synchronisation de l'émetteur et du récepteur. Il s'agit alors de garantir la convergence à zéro de l'erreur de reconstruction d'état $\epsilon_k = x_k - \hat{x}_k$. La section suivante traite de la stabilité des régimes permanents de type point fixe. Ces résultats constituent une base essentielle pour la synthèse d'observateurs non linéaires dans le Chapitre 3.

Usuellement, les résultats ci-dessous sont présentés pour le vecteur d'état x_k. Dans le cadre de cette étude, comme on s'intéresse à la stabilité de l'erreur de reconstruction d'état ϵ_k, les résultats sont énoncés pour ϵ_k.

1.7 Méthodes de Lyapunov

Considérons l'équation dynamique :

$$\epsilon_{k+1} = f(\epsilon_k) \tag{1.35}$$

où $\epsilon_k = [\epsilon_k^{(1)} \dots \epsilon_k^{(n)}]^T \in \mathbb{R}^n$ et la fonction $f = [f_1 \dots f_n]^T$ est continuement dérivable sur $\mathbb{R}^n$.

Le point d'équilibre ϵ^* vérifie $f(\epsilon^*) = \epsilon^*$.
Il existe deux méthodes de Lyapunov pour tester la stabilité du point d'équilibre ϵ^*, la méthode directe et la méthode indirecte.

1.7.1 Méthode indirecte de Lyapunov

La méthode indirecte, aussi appelée première méthode de Lyapunov, consiste à linéariser le système (1.35) autour d'un point d'équilibre ϵ^* et à tester la stabilité du système ainsi linéarisé :

$$\epsilon_{k+1} = J(\epsilon^*)\epsilon_k \tag{1.36}$$

où $J(\epsilon^*)$ est le jacobien[1] de la fonction f (système (1.35)), évalué autour du point d'équilibre ϵ^*.

La ième valeur propre de la matrice jacobienne $J(\epsilon^*)$ sera notée λ_i.
Le théorème suivant peut être trouvé dans [Khalil, 1996] pour les systèmes à temps discret.

Théorème 2 (Méthode indirecte de Lyapunov). Le point d'équilibre ϵ^* est localement asymptotiquement stable si $|\lambda_i| < 1$, pour tout $i = 1, \dots, n$.

La méthode indirecte ne permet de tester que la stabilité locale du système (1.35). Une autre approche qui étudie sa stabilité globale est la méthode directe de Lyapunov, présentée dans la section suivante.

1.7.2 Méthode directe de Lyapunov

Dans la méthode directe, aussi appelée seconde méthode de Lyapunov, on cherche une fonction scalaire, de type "énergétique", qui admet une différence négative entre deux états successifs. Cette fonction est appelée fonction de Lyapunov. La seconde méthode de Lyapunov est rappelée, par exemple, dans [Khalil, 1996] et [Slotine et al., 1987].

[1] Voir Annexe A, Définition 28

Définition 3. Une fonction de Lyapunov est une fonction scalaire $V : \mathbb{R}^n \to \mathbb{R}$, continue en ϵ_k, telle que :

1. $V(0) = 0$,
2. $V(\epsilon_k) > 0$, $\forall \epsilon_k \neq 0$,
3. $V(\epsilon_k) \to \infty$ si $\epsilon_k \to \infty$.

Théorème 3 (Méthode directe de Lyapunov). Le point d'équilibre $\epsilon^* = 0$ est globalement et asymptotiquement stable s'il existe une fonction de Lyapunov $V : \mathbb{R}^n \to \mathbb{R}$, telle que :

$$\Delta V(\epsilon_{k+1}, \epsilon_k) = V(\epsilon_{k+1}) - V(\epsilon_k) < 0, \quad \forall \epsilon_k \neq 0 \tag{1.37}$$

Remarque 1. Si le point d'équilibre ϵ^* n'est pas 0, on s'y ramène par un changement de variable du type $\epsilon_k^{'} = \epsilon_k - \epsilon^*$.

La méthode directe est basée sur le principe de perte d'énergie d'un système. En effet, si l'énergie du système se dissipe continuement, c'est-à-dire décroît avec le temps, alors ce système tend à se ramener à un état d'équilibre stable.

L'avantage de la méthode directe de Lyapunov est qu'elle ne nécessite pas la connaissance des solutions des équations du système, parfois difficile voire impossible à expliciter analytiquement. Elle permet de remplacer l'étude de la convergence d'un vecteur ϵ_k de dimension n non exprimable analytiquement par l'étude de la convergence d'une fonction scalaire exprimable analytiquement. En revanche, la difficulté de cette méthode est de trouver une fonction de Lyapunov appropriée. En effet, le Théorème 3 n'est pas constructif dans le choix de la fonction de Lyapunov et ne permet donc pas de conclure si on ne trouve pas une telle fonction.
Par exemple, la fonction de Lyapunov peut avoir une forme quadratique $V(\epsilon_k) = \epsilon_k^T P \epsilon_k$, avec $P > 0$.

La section suivante traite de la stabilité d'une classe particulière de systèmes non linéaires, les systèmes linéaires à paramètres variants ou appelés systèmes LPV (**L**inear **P**arameter **V**arying). Ces systèmes sont décrits par une équation affine en l'état, mais non linéaire, car dépendant d'un vecteur de paramètres variant dans le temps. On s'y intéresse car de nombreux systèmes chaotiques peuvent être réécrits sous une forme LPV, comme nous le verrons au Chapitre 3. L'erreur de reconstruction d'état ϵ_k pourra également être réécrite sous forme LPV et l'étude de la stabilité sera fondamentale dans le contexte de synchronisation du chaos pour le chiffrement.

1.8 Stabilité des systèmes LPV

Les systèmes LPV sont une classe particulière de systèmes non linéaires. Ils sont décrits par une équation affine en l'état, mais non linéaire, car la matrice dynamique $\mathcal{A}_\epsilon$ dépend d'un vecteur de paramètres variant dans le temps :

$$\epsilon_{k+1} = \mathcal{A}_\epsilon(\rho_k)\epsilon_k \tag{1.38}$$

où $\rho_k \in \mathbb{R}^L$ est le vecteur de paramètres supposés mesurés. Ce vecteur est supposé être mesurable directement ou indirectement. Il peut représenter des incertitudes variant dans le temps ou des variations autour de valeurs nominales correspondant à des points de fonctionnement.

L'étude des systèmes LPV a été initiée pour la synthèse de lois de commande dites à séquencement de gains où la synthèse du correcteur se ramène à la synthèse de plusieurs correcteurs linéaires pour une famille de modèles linéarisés et à une procédure d'interpolation [Shamma and Athans, 1990] [Rugh, 1991]. Même si l'on aboutit à de bons résultats en pratique, ces heuristiques ne prennent pas en compte les variations paramétriques et ne donnent donc aucune garantie de stabilité et de performance si ce n'est pour des variations très lentes des paramètres [Shamma and Athans, 1991]. C'est pourquoi l'approche LPV s'est avérée très utile pour simplifier la phase d'interpolation et les problèmes d'implémentation du correcteur à gains séquencés. Elle permet notamment de considérer le correcteur comme une seule entité où l'aspect séquencement de gains est réalisé par la dépendance paramétrique du correcteur.
En France, l'étude de ces systèmes a commencé au CERT-ONERA où des résultats importants relatifs aux problèmes de robustesse notamment ont été développés avec une application privilégiée dans le domaine de l'aéronautique [Apkarian et al., 1995] [Apkarian and Gahinet, 1995] [Biannic, 1996] [Apkarian et al., 2000].

Il existe plusieurs types de dépendance paramétrique de $\mathcal{A}_\epsilon$ par rapport à ρ_k. Une dépendance particulière est la dépendance affine. Dans ce cas, il existe une infinité de contraintes à vérifier pour tester la stabilité. Une autre dépendance est la dépendance polytopique. Pour une dépendance polytopique, il sera montré, dans le Chapitre 3, que le nombre de contraintes pour tester la stabilité est fini et correspond au nombre de sommets du polytope.

On dit que le système (1.38) est polytopique lorsque la matrice d'état $\mathcal{A}_\epsilon$ peut s'exprimer sous la forme :

$$\mathcal{A}_\epsilon(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k) A_\epsilon^{(i)} \tag{1.39}$$

avec le vecteur ξ_k dépendant du paramètre mesurable ρ_k et appartenant à l'ensemble compact[1] convexe S :

$$S = \{\mu_k \in \mathbb{R}^N, \quad \mu_k = [\mu_k^{(1)} \dots \mu_k^{(N)}]^T, \quad \mu_k^{(i)} \geq 0 \quad \forall i, \quad \sum_{i=1}^{N} \mu_k^{(i)} = 1\} \tag{1.40}$$

Comme S est un ensemble convexe, l'ensemble des matrices $A_\epsilon^{(i)}$, $i = 1, \dots, N$, définit une enveloppe convexe $\mathcal{D}_{\mathcal{A}_\epsilon}$, aussi appelée *polytope convexe*. Les matrices $A_\epsilon^{(i)}$ sont constantes et sont appelées matrices sommets ("vertices", en anglais) de $\mathcal{D}_{\mathcal{A}_\epsilon}$.

Définition 4. Soit F un ensemble fini de points. L'*enveloppe convexe* ("convex hull", en anglais) de F est le plus petit ensemble convexe S contenant F.

La figure 1.18 illustre un exemple d'enveloppe convexe. L'enveloppe convexe de l'ensemble des points est représentée en trait plein. L'ensemble représenté en trait pointillé est seulement un ensemble convexe.
Un polytope est la généralisation à toutes dimensions de la notion de polygone pour deux dimensions et de polyèdre pour trois dimensions. Une classe de polytopes est celle des polytopes *convexes*.

[1] Voir Annexe A, Définition 31

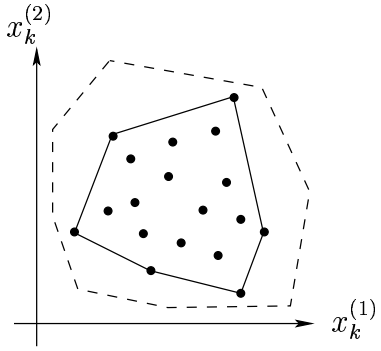


FIG. 1.18 – Enveloppe convexe d'un ensemble de points

Dans la suite du mémoire, tous les polytopes considérés sont convexes même si le mot *convexe* est omis.

Comme on s'intéresse à la stabilité globale du système (1.38), on utilise la méthode directe de Lyapunov. La fonction de Lyapunov peut avoir une forme quadratique ou une forme plus générale, dite polyquadratique. Nous allons commencer par étudier les conditions de stabilité dans le cas d'une fonction de Lyapunov quadratique, puis nous aborderons la forme polyquadratique.

1.8.1 Stabilité quadratique

Soit une fonction de Lyapunov quadratique $V(\epsilon_k) = \epsilon_k^T P \epsilon_k$, avec P une matrice définie positive ($P > 0$) et symétrique. Cette fonction vérifie les propriétés :

1. $V(0) = 0^T P 0 = 0$,
2. $V(\epsilon_k) = \epsilon_k^T P \epsilon_k > 0$ (car $P > 0$),
3. $V(\epsilon_k) \to \infty$ si $\epsilon_k \to \infty$.

Théorème 4. Le système (1.38) est quadratiquement stable si :

$$\Delta V(\epsilon_{k+1}, \epsilon_k) = V(\epsilon_{k+1}) - V(\epsilon_k) = \epsilon_{k+1}^T P \epsilon_{k+1} - \epsilon_k^T P \epsilon_k < 0, \quad \forall \epsilon_k \neq 0 \tag{1.41}$$

En remplaçant ϵ_{k+1} par $\mathcal{A}_\epsilon(\rho_k)\epsilon_k$, il vient :

$$\Delta V(\epsilon_{k+1}, \epsilon_k) = \epsilon_k^T \mathcal{A}_\epsilon^T(\rho_k) P \mathcal{A}_\epsilon(\rho_k) \epsilon_k - \epsilon_k^T P \epsilon_k \tag{1.42}$$

En factorisant à gauche par ϵ_k^T et à droite par ϵ_k, on obtient :

$$\Delta V(\epsilon_{k+1}, \epsilon_k) = \epsilon_k^T \big(\mathcal{A}_\epsilon^T(\rho_k) P \mathcal{A}_\epsilon(\rho_k) - P\big) \epsilon_k \tag{1.43}$$

Puisque la relation (1.41) est vérifiée $\forall \epsilon_k$, alors :

$$\mathcal{A}_\epsilon^T(\rho_k) P \mathcal{A}_\epsilon(\rho_k) - P < 0 \tag{1.44}$$

En remplaçant $\mathcal{A}_\epsilon(\rho_k)$ par sa décomposition polytopique (1.39), il vient :

$$\Big(\sum_{i=1}^{N} \xi_k^{(i)} (A_\epsilon^{(i)})^T\Big) P \Big(\sum_{i=1}^{N} \xi_k^{(i)} A_\epsilon^{(i)}\Big) - P < 0 \tag{1.45}$$

On peut montrer qu'en utilisant notamment le complément de Schur[1] [Daafouz and Millérioux, 2002], l'inégalité (1.45) est équivalente à :

$$\begin{pmatrix} P & (A_\epsilon^{(i)})^T P^T \\ PA_\epsilon^{(i)} & P \end{pmatrix} > 0, \quad \forall i \in I = \{1, \ldots, N\} \tag{1.46}$$

ce qui nous amène au théorème suivant.

Théorème 5. Le système (1.38) est quadratiquement stable si et seulement s'il existe une matrice P symétrique définie positive, de dimension appropriée, telle que :

$$\begin{pmatrix} P & (A_\epsilon^{(i)})^T P \\ PA_\epsilon^{(i)} & P \end{pmatrix} > 0, \quad \forall i \in I \tag{1.47}$$

La fonction de Lyapunov associée est $V(\epsilon_k) = \epsilon_k^T P \epsilon_k$.

Les relations (1.47) constituent un système linéaire de N inégalités matricielles, où P est inconnue. Ces inégalités sont aussi appelées *LMI* (**L**inear **M**atrix **I**nequalities). Elles sont indépendantes de ϵ_k et assurent donc la stabilité globale du système.

Remarque 2. Si $N = 1$, $A_\epsilon^{(i)} = A$ et on se ramène à l'inégalité usuelle, pour les systèmes linéaires :

$$A^T P A - P < 0 \tag{1.48}$$

L'étude de la stabilité quadratique grâce à la méthode directe de Lyapunov est intéressante car la condition de stabilité porte sur une fonction scalaire et ne dépend plus de ϵ_k. Si le Théorème 5 est vérifié, la convergence du système est globale (dans ce cas, $\mathcal{D} = \mathbb{R}^n$).
Cependant, cette approche quadratique ne prend pas en compte les variations du paramètre ρ_k. Par conséquent, elle est conservative et restreint donc la classe des systèmes stabilisables. Une meilleure approche, qui intègre ces variations tout en conservant la propriété de convergence globale, consiste à choisir une fonction de Lyapunov de type polyquadratique de la forme $V(\epsilon_k) = \epsilon_k^T \mathcal{P}_k \epsilon_k$.

1.8.2 Stabilité polyquadratique

Considérons toujours le système (1.38). On définit une fonction de Lyapunov dite polyquadratique [Daafouz et al., 2002] :

$$V(\epsilon_k) = \epsilon_k^T \mathcal{P}_k \epsilon_k \tag{1.49}$$

avec $\mathcal{P}_k > 0$, $\forall k$, obéissant à la même décomposition polytopique que celle (1.39) de $\mathcal{A}_\epsilon(\rho_k)$, c'est-à-dire :

$$\mathcal{P}_k = \sum_{i=1}^{N} \xi_k^{(i)} P_i \tag{1.50}$$

où les matrices P_i sont constantes.

Le théorème suivant, énoncé dans [Daafouz et al., 2002] et [Millérioux and Daafouz, 2003b], donne une condition nécessaire et suffisante de stabilité polyquadratique d'un système de la forme (1.38).

[1] Voir Annexe A, Lemme 2

Théorème 6. Le système (1.38) est polyquadratiquement stable si et seulement s'il existe des matrices G_i et des matrices symétriques définies positives S_i et S_j, de dimensions appropriées, telles que l'ensemble d'inégalités matricielles :

$$\begin{pmatrix} G_i + G_i^T - S_i & G_i^T (A_\epsilon^{(i)})^T \\ A_\epsilon^{(i)} G_i & S_j \end{pmatrix} > 0 \tag{1.51}$$

soit faisable $\forall (i,j) \in I \times I$.

La stabilité quadratique correspond à un cas particulier de la stabilité polyquadratique où la fonction de Lyapunov est $V(\epsilon_k) = \epsilon_k^T \mathcal{P}_k \epsilon_k$ avec $\mathcal{P}_k = P$ une matrice constante et, en ce sens, elle est restrictive par rapport à la stabilité polyquadratique.

1.9 Conclusion

Dans la suite, nous ne nous intéresserons qu'aux systèmes non linéaires à temps discret. En effet, on envisage d'implémenter plus facilement des systèmes à temps discret que des systèmes à temps continu.

Les signaux issus de certains systèmes chaotiques possèdent un large spectre en fréquence. Cette caractéristique est intéressante pour le chiffrement d'information car elle permet de cacher une information à masquer au sein d'un signal s'apparentant à un bruit, supposant rendre ainsi difficile son interception par un adversaire. En fait, les systèmes chaotiques possèdent des propriétés proches de celles requises en cryptographie usuelle. Le Chapitre 2 introduit la notion de cryptographie et présente différents schémas de chiffrement basés sur l'utilisation des systèmes dynamiques chaotiques.
Les résultats énoncés sur la stabilité seront appliqués dans le Chapitre 3 lors de la reconstruction de l'information, côté récepteur.

Chapitre 2

Chiffrement usuel et chiffrement basé sur le chaos

2.1 Introduction

Pendant longtemps, le chaos a été considéré comme "dangereux" ou indésirable par la communauté scientifique. Cependant, dans les années 90, des scientifiques ont réalisé que le chaos pouvait être contrôlé et ont commencé à chercher ses applications possibles. Les signaux issus des systèmes chaotiques sont imprédictibles à long terme, peuvent présenter des propriétés spectrales et statistiques proches de l'aléatoire (signaux à large spectre, autocorrélation réduite), bien qu'issus de systèmes déterministes. Ces caractéristiques sont liées aux propriétés requises par les schémas de chiffrement, telles que la confusion et la diffusion de Shannon, usuellement rencontrées en cryptographie [Barthélemy et al., 2005]. En 1990, [Pecora and Carroll, 1990] ont montré que les systèmes chaotiques peuvent être synchronisés. Une des applications du chaos qui a alors intéressé les chercheurs est l'utilisation de systèmes chaotiques à des fins de chiffrement. De nombreux schémas de chiffrement basés sur le chaos ont été proposés dans la littérature. En revanche, très peu de travaux ont réellement fait un lien entre les algorithmes de chiffrement standard et ceux basés sur la génération de séquences chaotiques. On notera cependant des premiers travaux comparatifs dans [Gotz et al., 1997] [Dachselt et al., 1998] [Kocarev, 2001].
En cryptographie usuelle, parmi une grande variété de mécanismes de chiffrement, on distingue le chiffrement à clé publique et le chiffrement symétrique. Dans ce chapitre, nous établissons le lien entre le chiffrement symétrique standard et le chiffrement par inclusion basé sur le chaos [Anstett et al., 2005b] [Anstett et al., 2005c] [Anstett et al., 2005d].

La Section 2.2 est une introduction générale à la cryptographie. Puis, la Section 2.3 présente les deux algorithmes principaux de cryptographie standard, le chiffrement à clé publique et le chiffrement symétrique. La Section 2.4 est consacrée aux différents schémas de chiffrement par le chaos rencontrés dans la littérature, le masquage additif, la modulation chaotique, la modulation paramétrique et le chiffrement par inclusion. Les structures des émetteurs et des récepteurs du chiffrement symétrique et du chiffrement par inclusion y sont comparées.

2.2 Introduction générale à la cryptographie

Une introduction à la cryptographie peut être trouvée dans [Menezes et al., 1996] [Schneier, 1996].

2.2.1 Un peu d'histoire

La fonction première de la cryptographie est de cacher le sens d'un message à tous ceux qui ne sont pas autorisés à le connaître. Les quelques indications historiques qui suivent peuvent être trouvées dans de nombreuses sources, [Kahn, 1996] par exemple. Elles visent à montrer, outre l'ancienneté du problème de chiffrement, l'émergence progressive des notions de substitution, de confusion et de clé de chiffrement.

La cryptographie existe depuis que les hommes ont appris à communiquer entre eux. Vers 600 ans avant J.-C., Nabuchodonosor, roi de Babylone, écrivait le message qu'il souhaitait transmettre à ses généraux, sur le crâne préalablement rasé de ses esclaves. Il attendait que leurs cheveux repoussent avant de les envoyer chez ses généraux, qui rasaient de nouveau les cheveux des messagers pour lire le texte. Dans l'Antiquité, les Grecs employaient, en temps de guerre, un dispositif appelé une scytale. Ce dispositif consistait en une bande étroite de parchemin sur laquelle ils écrivaient après l'avoir enroulée en spirales autour d'un cylindre de bois. Une fois la bande déroulée, le texte ne pouvait être lu que par une personne possédant un cylindre de même diamètre sur lequel elle pouvait enrouler la bande.
Une méthode plus sûre qui se rapproche davantage des systèmes cryptographiques est le code de César (50 ans avant J.-C.). Pour masquer ses messages, Jules César utilisait une substitution, c'est-à-dire qu'il remplaçait chaque lettre du message par une autre lettre de l'alphabet, décalée d'une quantité fixe de la lettre d'origine. Ce code était peu sûr car l'alphabet comprenant 26 lettres, il existait seulement 26 façons différentes de chiffrer un message. Mais, la faible alphabétisation de la population le rendait assez efficace. De par sa simplicité de mise en oeuvre, il a même été réutilisé par l'armée russe pendant la première guerre mondiale. Les systèmes cryptographiques qui suivirent gardèrent ce principe de substitution.
Plus tard, en 1467, Leone Battista Alberti proposa un procédé de substitution polyalphabétique. Son principe était de remplacer chaque lettre du message par une lettre d'un autre alphabet et de changer plusieurs fois d'alphabet au cours du procédé. Vers 1500, l'abbé Jean Trithème imagina un dispositif consistant à remplacer une lettre du message par un groupe de mots. Ces groupes de mots étaient choisis de telle manière qu'un texte latin cohérent, une prière ou une glorification religieuse résultaient de la succession de ces groupes de mots.
L'inconvénient majeur de ces procédés cryptographiques fondés sur la substitution était le problème de la fréquence d'apparition des lettres. Par exemple, dans la langue française, la lettre "e" a une plus grande fréquence d'apparition dans les mots que la lettre "z". Cette fréquence d'apparition est conservée dans le texte codé, pouvant ainsi conduire à son décodage.
Pour renforcer la sécurité, les algorithmes basés sur la substitution ont été développés et améliorés. Ainsi, en 1586, le diplomate français Blaise de Vigenère proposa une technique plus élaborée, basée sur une substitution polyalphabétique. Il utilisa une clé littérale, ou mot de passe, dont chaque lettre indiquait le décalage alphabétique à appliquer sur les lettres du message. L'inconvénient de ce procédé résidait dans l'échange de la clé qui n'était pas sécurisé et qui pouvait conduire à l'interception de la clé.
En 1918, Arthur Scherbius fit breveter sa machine à crypter, appelée Enigma. Son principe fut que chaque lettre du message était remplacée par une autre, la règle de substitution changeant d'une lettre à une autre. Ce procédé permettait d'évincer le problème de la fréquence d'apparition des lettres ainsi que celui de l'échange de la clé. Cette machine fut utilisée pendant la seconde guerre mondiale. Cependant, quelque peu lente et encombrante, cette machine était inexploitable en terrain hostile. Ainsi, l'ingénieur américain Philip Johnston eut l'idée d'utiliser la langue navajo comme procédé cryptographique. La méconnaissance quasi totale de cette langue ainsi que

sa construction grammaticale très particulière, la rendant impénétrable aux étrangers, décidèrent de son utilisation, lors de la campagne du Pacifique pendant la seconde guerre mondiale.
Le développement des ordinateurs, des techniques de communication et la mondialisation des échanges (Internet, commerce électronique, ...) sont confrontés à de nouveaux problèmes de sécurité de l'information. De ce fait, la cryptographie n'a plus seulement la vocation de préserver la confidentialité des données, mais elle a aussi pour rôle de préserver le contenu des messages de toute modification non souhaitée, de s'assurer de l'identité de l'émetteur et du destinataire afin d'éviter toute usurpation d'identité, ... Les systèmes cryptographiques existant jusqu'alors doivent être perfectionnés pour faire face à ces nouveaux problèmes.
Dans les années 70, Horst Feistel a mené à IBM, un projet de recherche sur le chiffrement, qui inspira plus tard le schéma de chiffrement symétrique DES. En 1976, Whitfield Diffie et Martin Hellmann proposent la cryptographie à clé publique. Ce schéma permet de pallier le problème de l'échange de clé, rencontré dans la substitution polyalphabétique de Vigenère. Le chiffrement du message est fondé sur des problèmes mathématiques difficiles à résoudre. Ce procédé est détaillé dans la Section 2.3.1, où un exemple d'algorithme à clé publique, RSA, est présenté.
Un autre procédé célèbre est la cryptographie symétrique, dont quelques exemples sont le schéma de Vigenère et, beaucoup plus récemment, l'algorithme DES. Dans ce cas, les clés pour coder et décoder le message sont les mêmes. L'émetteur et le destinataire doivent alors s'accorder sur une clé qui doit être gardée secrète. Le chiffrement est fondé sur une combinaison complexe de substitutions. Cet algorithme est présenté dans la Section 2.3.2.
Les deux algorithmes principaux, le chiffrement à clé publique et le chiffrement symétrique, sont toujours utilisés actuellement.

2.2.2 Définitions

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

Lorsqu'un cryptosystème est synthétisé, il faut s'assurer qu'il est effectivement robuste face à des attaques pirates. Cette étape de validation est appelée la cryptanalyse. Elle consiste à tester les cryptosystèmes afin de déceler leurs éventuelles faiblesses. La notion de cryptanalyse est détaillée dans le Chapitre 5.

Parmi une grande variété de mécanismes de chiffrement, les deux algorithmes principaux en cryptographie standard sont le chiffrement à clé publique et le chiffrement symétrique, présentés dans la section suivante.

2.3 Chiffrement en cryptographie standard

Toutes les notions abordées dans cette section peuvent être trouvées dans [Menezes et al., 1996] [Delfs and Knebl, 2002] [Barthélemy et al., 2005].

2.3.1 Chiffrement à clé publique

Le chiffrement à clé publique, ou chiffrement asymétrique, a été proposé par Diffie et Hellman, en 1976. Dans un tel schéma, la clé de chiffrement est différente de celle de déchiffrement. N'importe qui peut utiliser la clé de chiffrement, ou clé publique, pour chiffrer un message, mais seul celui qui possède la clé de déchiffrement, ou clé privée, peut déchiffrer le message chiffré résultant.
De plus, la clé de déchiffrement K^d ne peut pas être calculée (du moins dans un temps raisonnable) à partir de la clé de chiffrement K^e. Ce type de schéma repose directement sur l'existence de fonctions à sens unique. Une fonction est dite à sens unique quand il est facile de calculer K^e en connaissant K^d, mais très difficile de calculer K^d connaissant K^e. Parfois, des fonctions à sens unique qui possèdent en plus une trappe sont utilisées. Une fonction à sens unique est dite à trappes quand il est très difficile de calculer K^d à partir de K^e, sauf si on connaît une information supplémentaire.

Lorsqu'Alice, l'émetteur, et Bob, le destinataire, veulent communiquer de façon sécurisée, Bob choisit une paire de clés de chiffrement et de déchiffrement (K^e, K^d). Il envoie la clé publique K^e à Alice, par l'intermédiaire d'un canal qui n'est pas forcément sécurisé. Alice transforme le message m en texte chiffré $c = e(K^e, m)$, où e représente une fonction de chiffrement, et envoie ce texte chiffré c à Bob. De son côté, Bob reçoit le texte chiffré c et calcule $m = d(K^d, c)$ où d est une fonction de déchiffrement et K^d est la clé privée connue uniquement de Bob. Ainsi, Bob récupère le message initial m. Ce schéma est illustré sur la figure 2.1.

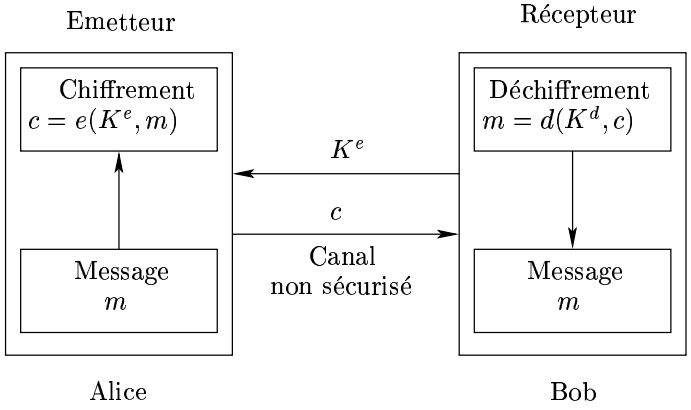


FIG. 2.1 – Chiffrement à clé publique

Le chiffrement à clé publique ne protège pas du problème d'authentification et de non répudiation. Pour pallier le problème d'authentification, Bob envoie des "défis" à Alice qui souhaite s'identifier. Alice ne pourra résoudre ces défis que dans la mesure où elle connaît un secret, détenu par elle seule ou commun à Bob et elle. Par exemple, pour payer par carte bancaire, le défi à relever est de taper le code secret associé à la carte, connu uniquement de son propriétaire.
Pour éviter le problème de non répudiation, un algorithme de signature numérique est ajouté. Une signature numérique est l'analogie numérique d'une signature manuscrite. La signature doit dépendre du message à signer et d'une clé secrète connue uniquement de l'entité qui signe. Une tierce entité, non corrompue, doit être capable de vérifier la signature sans avoir accès au message.

Un exemple de chiffrement à clé publique est le schéma RSA, proposé par Rivest, Shamir et Adleman, en 1978. Ce schéma est encore très largement utilisé (sites web commerciaux, par exemple). Il repose sur la difficulté de factoriser des grands nombres et s'appuie donc sur la théorie des nombres.
La génération des clés publique et privée peut être résumée par les étapes suivantes :

- Bob choisit deux grands nombres premiers (de longueur 1024 ou 2048 bits, en général), p et q, et calcule $n = pq$.
- Bob choisit aussi, de façon aléatoire, un entier $K^e < n$ qui est premier avec $(p-1)(q-1)$.
- Il calcule K^d tel que $K^e K^d = 1 \bmod (p-1)(q-1)$.
- Bob publie la clé publique, formée de (K^e, n), et les entiers p et q sont détruits pour ne pas être divulgués. Il garde la clé privée K^d.

Pour envoyer un message à Bob, Alice calcule $c = m^{K^e} \bmod n$ et envoie c à Bob. Pour déchiffrer c, Bob calcule $m = c^{K^d} \bmod n$.
Dans ce schéma, la fonction de chiffrement est une fonction à sens unique et possède une trappe. En effet, toute personne connaissant la clé publique (K^e, n) et la factorisation de n peut calculer K^d.

2.3.2 Chiffrement symétrique

Par opposition au chiffrement à clé publique, le chiffrement symétrique est aussi appelé chiffrement à clé secrète. La clé de chiffrement peut être calculée à partir de la clé de déchiffrement et vice versa. En général, les clés de chiffrement et de déchiffrement sont identiques. L'émetteur et le destinataire doivent se mettre d'accord préalablement sur une clé qui doit être gardée secrète, car la sécurité d'un tel algorithme repose sur cette clé.

Le chiffrement à clé publique et le chiffrement symétrique présentent chacun des avantages [Menezes et al., 1996]. Par exemple, le temps de chiffrement/déchiffrement du chiffrement à clé publique est supérieur à celui du chiffrement symétrique. Un des problèmes principaux du chiffrement symétrique est l'échange préalable de la clé secrète. Le chiffrement à clé publique peut être préféré pour générer de petites séquences comme des signatures ou des clés secrètes pour le chiffrement symétrique. Le chiffrement symétrique peut être préféré pour chiffrer des grandes quantités de données.

Les schémas de chiffrement symétrique peuvent être classés en deux catégories, le chiffrement par blocs et le chiffrement par flot, détaillés ci-après.

Chiffrement par blocs

Dans un schéma de chiffrement par blocs, le message est divisé en blocs de bits, de longueur fixe. Chaque bloc est chiffré l'un après l'autre. Le chiffrement peut être effectué par substitutions (les bits d'un bloc sont substitués par d'autres bits) et par transpositions (les bits d'un bloc sont permutés entre eux). La substitution permet d'ajouter de la *confusion*, c'est-à-dire de rendre la relation entre le message et le texte chiffré aussi complexe que possible. La transposition permet d'ajouter de la *diffusion*, c'est-à-dire de réarranger les bits du message afin d'éviter que toute redondance dans le message ne se retrouve dans le texte chiffré.
On distingue le chiffrement par blocs itératifs. Une fonction constituée de combinaisons complexes de substitutions et de transpositions, appelée fonction de tour ou fonction de ronde, est appliquée itérativement. Une itération est appelée un tour ou une ronde. Chaque ronde prend en entrée la sortie de la ronde précédente (ou un bloc du texte clair pour la première ronde) et chiffre cette entrée à l'aide de la fonction de ronde et d'une sous-clé de ronde générée à partir de la clé secrète K. La fonction de chiffrement n'est pas la fonction de ronde, mais elle est constituée par l'ensemble de toutes les rondes.

Un exemple de chiffrement par blocs itératifs est le célèbre schéma DES (**D**ata **E**ncryption **S**tandard), adopté par le gouvernement américain, en 1977, comme algorithme de chiffrement standard officiel. Dans ce schéma, le texte clair est divisé en blocs de longueur 64 bits. La clé a également une longueur de 64 bits, dont 56 bits sont générés aléatoirement et utilisés dans l'algorithme et dont 8 bits sont utilisés pour la détection d'erreurs lors de la transmission. Le chiffrement d'un bloc s'effectue avec 16 rondes. La clé secrète K est dérivée de 16 "sous-clés" K_i, une pour chaque ronde. Chaque entrée de ronde est partagée en une partie gauche L_i et une partie droite R_i, de même longueur. Pour $i = 0, \ldots, 15$, les quantités R_{i+1} et L_{i+1} sont calculées :

$$\begin{cases} R_{i+1} = L_i \oplus f(R_i, K_i) \\ L_{i+1} = R_i \end{cases} \tag{2.1}$$

où f est la fonction de ronde.
Pour renforcer la sécurité, il existe des variantes du DES qui consistent à utiliser une clé K de longueur plus importante et à répéter plusieurs fois l'algorithme sur chaque bloc, comme le triple-DES.
Les longueurs des clés ne permettent pas toujours de résister à des attaques de plus en plus performantes grâce au progrès des ordinateurs. Pour pallier ce problème, le schéma DES est amélioré et devient le schéma AES (**A**dvanced **E**ncryption **S**tandard), en 1997.

Chiffrement par flot

Le chiffrement par flot est aussi appelé chiffrement en continu. Dans ce schéma, le message est chiffré un bit à la fois. La fonction de chiffrement est la même pour chaque bit, mais elle dépend d'une clé K_k qui varie dans le temps, dite dynamique. La génération de la clé dynamique dépend d'une clé secrète θ dite statique.

Dans un schéma de chiffrement par flot, lorsqu'Alice et Bob veulent communiquer de façon sécurisée, ils doivent se rencontrer préalablement et secrètement pour se mettre d'accord sur la clé secrète θ qu'ils partagent et qu'ils vont employer lors de la génération de K_k. Quelque temps plus tard, quand Alice souhaite envoyer un message m_k à Bob, elle transforme le message m_k en texte chiffré $c_k = e(K_k, m_k)$, où e représente une fonction de chiffrement. Elle envoie le texte

chiffré c_k à Bob par l'intermédiaire d'un canal qui n'est pas forcément sécurisé. De son côté, Bob reçoit le texte chiffré c_k et calcule $m_k = d(K_k, c_k)$ où d est une fonction de déchiffrement. Ainsi, Bob récupère le message initial m_k. Ce principe est illustré sur la figure 2.2.

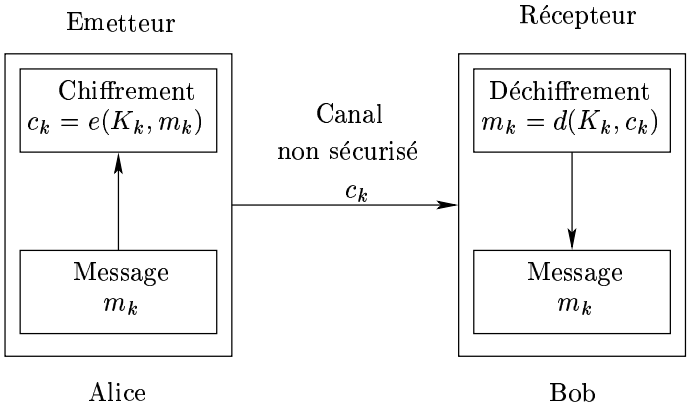


FIG. 2.2 – Chiffrement par flot

Un exemple de chiffrement par flot, proposé par Vernam en 1917, est le *masque jetable* ("one-time pad"), aussi appelé *chiffre de Vernam*. Dans ce schéma, le texte chiffré c_k est le résultat d'une combinaison du texte clair m_k avec la clé K_k, de même taille, par un OU exclusif (XOR) :

$$c_k = m_k \oplus K_k \tag{2.2}$$

A partir du texte chiffré, le texte clair peut être retrouvé par l'opération inverse :

$$m_k = c_k \oplus K_k \tag{2.3}$$

Le flot de clés K_k est utilisé une et une seule fois pour chiffrer les informations claires m_k, d'où le nom de masque *jetable*. De plus, le flot de clés K_k est généré de façon aléatoire et indépendemment des flots passés.

Dans le chiffrement par flot, il existe deux manières différentes de synchroniser les générateurs de clé afin de récupérer le message original. La première est appelée chiffrement par flot synchrone et la seconde est appelée chiffrement par flot autosynchrone. Elles sont toutes deux détaillées dans le paragraphe suivant.

Chiffrement par flot synchrone

Dans un schéma de chiffrement par flot synchrone, représenté sur la figure 2.3, l'émetteur est donné par :

$$\begin{cases} K_k = f_\theta(K_{k-1}) \\ c_k = e(K_k, m_k) \end{cases} \tag{2.4}$$

où f_θ est une fonction, θ la clé statique, K_k la clé dynamique, m_k le texte clair et c_k le texte chiffré. La clé dynamique K_k est générée par une dynamique interne f_θ qui ne dépend ni du texte clair m_k, ni du texte chiffré c_k. Le récepteur est donné par :

$$\begin{cases} \hat{K}_k = f_{\hat{\theta}}(\hat{K}_{k-1}) \\ \hat{m}_k = d(\hat{K}_k, c_k) \end{cases} \tag{2.5}$$

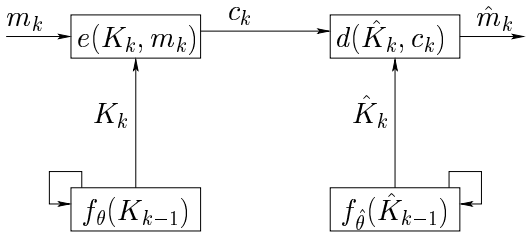


FIG. 2.3 – Chiffrement par flot synchrone

La récupération du texte clair nécessite une synchronisation des séquences des clés dynamiques à l'émission et à la réception. La fonction de déchiffrement d est telle que $\hat{m}_k = m_k$ si $\hat{K}_k = K_k$. Le flot de clés étant issu de récurrences autonomes, les générateurs de clés doivent être initialisés de part et d'autre de façon identique. La clé statique θ représente la condition initiale K_0. Si, pour une raison quelconque la synchronisation est perdue durant la transmission, l'émetteur et le récepteur doivent être réinitialisés à la même valeur pour resynchroniser leur transmission.

Chiffrement par flot autosynchrone

Dans un schéma de chiffrement par flot autosynchrone, représenté sur la figure 2.4, l'émetteur est donné par :

$$\begin{cases} K_k = f_\theta(c_{k-1}, \ldots, c_{k-j}) \\ c_k = e(K_k, m_k) \end{cases} \tag{2.6}$$

où f_θ est une fonction paramétrée par la clé statique θ, qui génère le flot de clés K_k. A l'inverse du chiffrement par flot synchrone, K_k dépend seulement des valeurs passées du texte chiffré c_k. En revanche, comme précédemment, c_k est produit par la fonction de chiffrement e qui combine la clé K_k et le texte clair m_k. Le récepteur est donné par :

$$\begin{cases} \hat{K}_k = f_{\hat{\theta}}(c_{k-1}, \ldots, c_{k-j}) \\ \hat{m}_k = d(\hat{K}_k, c_k) \end{cases} \tag{2.7}$$

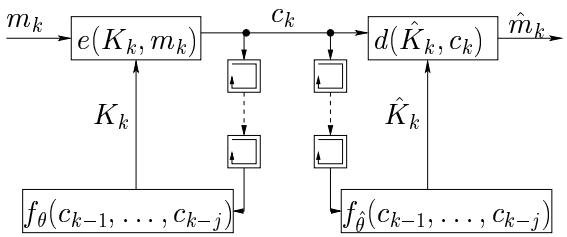


FIG. 2.4 – Chiffrement par flot autosynchrone

Si un symbole du texte chiffré est perdu ou est erroné, les j clés K_k suivantes seront calculées de façon erronée par le récepteur, après quoi les clés suivantes $\hat{K}_k$ seront à nouveau correctes.

Comme pour le chiffrement par flot synchrone, la récupération du texte clair nécessite la synchronisation des séquences des clés dynamiques à l'émission et à la réception et la fonction de déchiffrement d est telle que $\hat{m}_k = m_k$ si $\hat{K}_k = K_k$. A l'inverse du chiffrement par flot synchrone, les séquences des clés dynamiques se synchronisent automatiquement et θ est un paramètre de la dynamique f_θ.

Une définition de la sécurité d'un cryptosystème est proposée par Shannon (1948) et peut être trouvée dans [Barthélemy et al., 2005].

Définition 5. Un cryptosystème est à sécurité parfaite (ou inconditionnelle) si le texte chiffré n'apporte aucune information sur le texte clair.

Théorème 7. [Shannon] Soit un cryptosystème impliquant un texte clair m_k, un texte chiffré c_k et une clé K_k de même longueur. Il est dit à sécurité parfaite si et seulement si :
- toutes les clés K_k sont équiprobables,
- pour chaque m_k et pour chaque c_k, il existe une unique clé K_k vérifiant $e(K_k, m_k) = c_k$.

Par conséquent, les séquences de clés doivent être aléatoires. Un des problèmes est de générer des séquences parfaitement aléatoires. On peut, par défaut, utiliser un générateur pseudo-aléatoire. Un générateur pseudo-aléatoire est un algorithme déterministe qui produit, à partir d'une séquence initiale de bits de longueur q, une séquence de bits de longueur $u > q$, dont la distribution est indiscernable d'une distribution uniforme. Un exemple est donné par les registres à décalage à rétroaction linéaire ("Linear feedback shift register") [Menezes et al., 1996].

Dans le chiffrement symétrique, les deux idées fondamentales sont la génération de clés dynamiques complexes et la synchronisation des générateurs de clés à l'émission et à la réception. Ces deux idées sont reprises dans le chiffrement par le chaos. La section suivante présente des schémas de chiffrement basés sur le chaos.

2.4 Chiffrement basé sur le chaos

Le principe des schémas de chiffrement basé sur le chaos consiste à mélanger l'information m_k avec une séquence chaotique issue d'un émetteur, décrit généralement par une représentation d'état avec le vecteur d'état x_k. Seule la sortie y_k de l'émetteur est transmise au récepteur. Le récepteur a pour rôle d'extraire l'information originale du signal reçu y_k. La récupération de l'information est généralement basée sur la synchronisation des états x_k de l'émetteur et des états $\hat{x}_k$ du récepteur, c'est-à-dire :

$$\lim_{k\to\infty} ||x_k - \hat{x}_k|| = 0, \quad \forall \hat{x}_0 \tag{2.8}$$

ou :

$$\exists k_f, \quad ||x_k - \hat{x}_k|| = 0, \quad \forall k > k_f, \quad \forall \hat{x}_0 \tag{2.9}$$

La relation (2.8) correspond à une convergence asymptotique et (2.9) correspond à une convergence en un nombre fini d'itérations.

Différentes techniques d'injection de l'information dans un système chaotique ont été proposées dans la littérature, telles que le masquage additif [Cuomo et al., 1993b], la modulation chaotique [Dedieu et al., 1993], la modulation paramétrique [Parlitz et al., 1993], l'approche par inclusion. Un aperçu de ces techniques peut être trouvé dans [Hasler, 1998] [Yang, 2004], aussi bien pour les systèmes à temps discret que pour les systèmes à temps continu. Dans cette section, ces différentes techniques sont présentées dans le cas des systèmes à temps discret.

2.4.1 Masquage additif

Le masquage additif est lié aux travaux de [Wu and Chua, 1993] et de [Cuomo et al., 1993a], initialement effectués pour les systèmes à temps continu. Le principe de ce schéma consiste à effectuer une simple addition entre le signal de sortie de l'émetteur y_k et l'information m_k. L'émetteur (générateur de chaos) et le récepteur ont pour représentation d'état, respectivement :

$$\begin{cases} x_{k+1} = f(x_k) \\ y_k \quad = h(x_k) + m_k \end{cases} \tag{2.10}$$

$$\begin{cases} \hat{x}_{k+1} = f(\hat{x}_k) \\ \hat{y}_k \quad = h(\hat{x}_k) \end{cases} \tag{2.11}$$

où x_k (resp. $\hat{x}_k$) $\in \mathbb{R}^n$ est le vecteur d'état de l'émetteur (resp. du récepteur), $y_k \in \mathbb{R}$ (resp. $\hat{y}_k$) la sortie de l'émetteur (resp. du récepteur), $m_k \in \mathbb{R}$ l'information à masquer.
La figure 2.5 illustre ce mode de masquage.

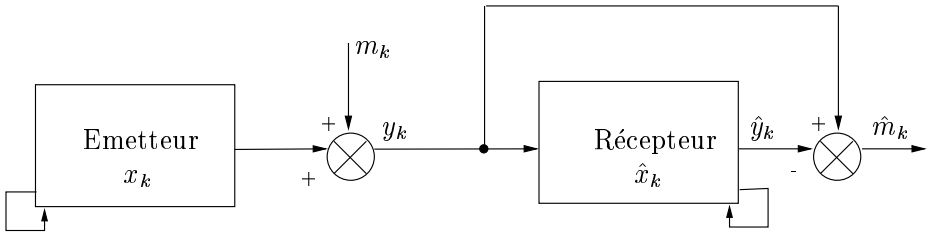


FIG. 2.5 – Masquage additif

La reconstruction de l'information nécessite la synchronisation (2.8) ou (2.9) de l'émetteur et du récepteur. L'information est alors récupérée en soustrayant la sortie du récepteur avec celle de l'émetteur :

$$\hat{m}_k = y_k - \hat{y}_k \tag{2.12}$$

Le principal inconvénient de cette approche est que l'information jouant le rôle d'une perturbation qui ne peut pas être en général totalement rejetée, la synchronisation n'est jamais exacte, même si l'amplitude du signal information est faible par rapport à celle du signal de sortie. Par conséquent, cette méthode n'est pas satisfaisante.

2.4.2 Modulation chaotique

La modulation chaotique, due à [Dedieu et al., 1993], est aussi connue sous le nom de "chaos shift-keying" ou "chaotic switching", en anglais.

Côté émetteur, à chaque symbole $m_k = m_i$ de l'information, appartenant à un ensemble fini $\{m_1, \ldots, m_N\}$, correspond un signal y_k issu d'un système chaotique décrit par :

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_k \quad = h_i(x_k) \end{cases} \tag{2.13}$$

où $i \in \{1, \ldots, N\}$, $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}$ la sortie. Le cas le plus simple correspond à une information binaire. Dans ce cas, seulement deux systèmes émetteur (2.13), avec $i = \{1, 2\}$, sont nécessaires, l'un correspondant à $m_1 = 0$ et l'autre à $m_2 = 1$.
Ce schéma de modulation est représenté sur la figure 2.6. Le rôle du récepteur est de détecter

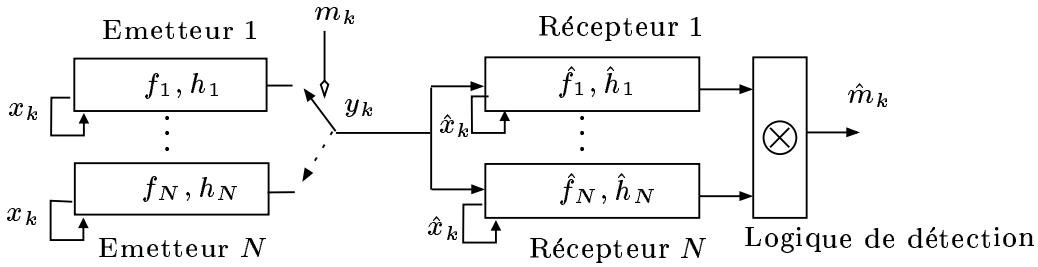


FIG. 2.6 – Modulation chaotique

quel émetteur a produit la sortie y_k. Pour cela, le récepteur est composé d'autant de systèmes que l'émetteur, décrits par :

$$\begin{cases} \hat{x}_{k+1} = \hat{f}_i(\hat{x}_k) \\ \hat{y}_k \quad = \hat{h}_i(\hat{x}_k) \end{cases} , \quad i = 1, \ldots, N \tag{2.14}$$

Il existe deux méthodes de détection, l'une cohérente et l'autre non cohérente. La détection non cohérente utilise des approches statistiques basées principalement sur l'analyse de la corrélation entre y_k et $\hat{y}_k$.
La détection cohérente nécessite la synchronisation de l'émetteur et du récepteur. Seulement un des N récepteurs peut se synchroniser selon la valeur courante m_i. Une logique de détection permet alors de reconstruire l'information, en analysant les erreurs de reconstruction $y_k - \hat{y}_k$ associées à chaque récepteur. Un banc d'observateurs peut jouer le rôle de récepteur, en garantissant la convergence à zéro de l'erreur de reconstruction d'état. La synthèse d'observateurs non linéaires fera l'objet du Chapitre 3.

2.4.3 Modulation paramétrique

La modulation paramétrique consiste à moduler un ou plusieurs paramètres du générateur de chaos par l'information m_k. Il en résulte un "mélange" multiplicatif entre le ou les paramètres du générateur de chaos et l'information.
Quand l'information prend un nombre fini de valeurs, on parle de modulation discrète. Le cas le plus simple correspond à une information binaire m_k [Dedieu et al., 1993] [Parlitz et al., 1993] [Cruz and Nijmeijer, 2000], où un "1" est codé en transmettant un signal chaotique et où un "0" est codé en transmettant un autre signal chaotique, mais peut être étendu à un cas plus général [Palaniyandi and Lakshmanan, 2001]. La figure 2.7 illustre ce schéma de masquage. Le système émetteur peut être décrit par la représentation d'état :

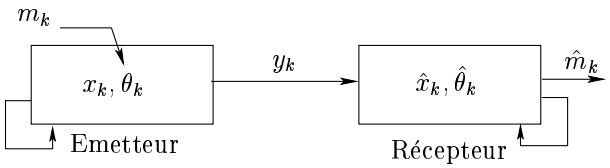


FIG. 2.7 – Modulation paramétrique

$$\begin{cases} x_{k+1} = f(x_k, \theta_k) \\ y_k \quad = h(x_k) \end{cases} \tag{2.15}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}$ la sortie, $\theta_k \in \mathbb{R}^l$ le vecteur des paramètres modulés. La fonction f est non linéaire et les fonctions g et h sont linéaires. Le paramètre θ_k varie dans le temps car il est modulé par l'information m_k. Quand $m_k = m_i$, $\theta_k = \theta_i$.

La modulation discrète peut être étendue au cas où l'information m_k ne prend plus un nombre fini de valeurs. On parle alors de modulation continue.
Pour la partie émetteur, le principe reste identique à celui de la modulation discrète. Toute la problématique se situe, côté récepteur, dans la récupération des paramètres. En effet, le récepteur doit se synchroniser sur l'émetteur. La récupération des paramètres modulés peut alors se baser sur l'estimation simultanée état/paramètre, via un observateur adaptatif. Les observateurs adaptatifs seront développés dans le Chapitre 4.

2.4.4 Chiffrement par inclusion

Dans ce schéma, le signal information est injecté dans un générateur de chaos jouant le rôle d'émetteur, qui admet la représentation d'état suivante :

$$\begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k \quad = h_\theta(x_k, m_k) \end{cases} \tag{2.16}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}$ la sortie, $m_k \in \mathbb{R}$ l'information à masquer, $\theta = [\theta_1, \ldots, \theta_l] \in \Theta \subset \mathbb{R}^l$ le vecteur de paramètres constants du système chaotique. Chaque symbole m_k est injecté dans la dynamique non linéaire chaotique f_θ, paramétrée par θ, générant x_k. Seule la sortie y_k est transmise au récepteur, x_k étant un vecteur d'état interne qui n'est pas accessible. Ce schéma est représenté sur la figure 2.8.
Le récepteur a pour représentation d'état générale :

$$\begin{cases} \hat{x}_{k+1} = g_{\hat{\theta}}(\hat{x}_k, y_k) \\ \hat{m}_k \quad = d(\hat{x}_k, y_k) \end{cases} \tag{2.17}$$

Le récepteur doit être synthétisé de telle sorte que l'information m_k puisse être reconstruite avec pour seule donnée la sortie de l'émetteur y_k. En effet, l'état interne x_k n'est pas directement transmis au récepteur, mais est nécessaire pour reconstruire l'information. La fonction $g_{\hat{\theta}}$ est choisie de telle sorte que si $\hat{\theta} = \theta$, alors $\hat{x}_k = x_k$, quel que soit $\hat{x}_0$ et indépendamment de l'information m_k qui joue le rôle d'une entrée externe au système dynamique, soit, en considérant une convergence asymptotique :

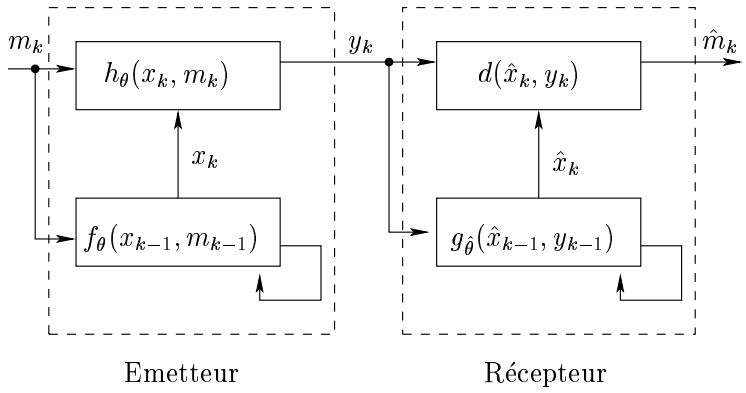


FIG. 2.8 – Chiffrement par inclusion

$$\lim_{k\to\infty} ||x_k - \hat{x}_k|| = 0, \quad \forall m_k, \quad \forall \hat{x}_0 \tag{2.18}$$

soit, en considérant une convergence en un nombre fini d'itérations :

$$\exists k_f, \quad ||x_k - \hat{x}_k|| = 0, \quad \forall k > k_f, \quad \forall m_k, \quad \forall \hat{x}_0 \tag{2.19}$$

Lorsque (2.18) ou (2.19) est vérifiée, on dit que l'émetteur et le récepteur se synchronisent globalement, indépendamment de l'entrée (**I**nput **I**ndependent **G**lobal **S**ynchronization, IIGS) [Millérioux and Daafouz, 2004].

La synchronisation de x_k et de $\hat{x}_k$ est formulée comme un problème d'inversion de systèmes dans [Feldmann et al., 1996] et comme un problème d'observation à entrées inconnues dans [Takahashi and Peres, 1999] pour les systèmes de Lur'e, dans [Millérioux and Daafouz, 2003a] [Millérioux et al., 2003] pour les systèmes linéaires par morceaux et dans [Millérioux and Daafouz, 2004] pour les systèmes admettant une forme polytopique.

2.4.5 Chiffrement par flot et chiffrement par inclusion

De façon similaire au chiffrement par flot, la fonction de déchiffrement d est telle que $\hat{m}_k = m_k$ si $\hat{x}_k = x_k$. Mais contrairement au chiffrement par flot synchrone, il n'est pas nécessaire que les deux générateurs de clés aient le même état initial x_0.

D'après (2.17), la reconstruction du texte clair m_k nécessite la connaissance du vecteur d'état interne x_k qui n'est pas transmis. x_k joue donc le rôle de la clé dynamique. En fait, le vecteur d'état x_k joue le même rôle que la clé K_k pour le chiffrement par flot.
D'autre part, le vecteur de paramètres θ, nécessaire pour reconstruire x_k, joue le rôle de la clé statique.
Par ailleurs, y_k et c_k, seuls signaux transmis sur le canal, jouent le même rôle.

Si la synchronisation est perdue pour une raison quelconque, le chiffrement par inclusion permet une resynchronisation automatique, ce qui est un avantage par rapport au chiffrement par flot synchrone. Ce point est principalement dû à l'inclusion de m_k dans la dynamique f_θ du système (2.16).

2.5 Conclusion

Nous avons présenté les deux schémas principaux de chiffrement en cryptographie usuelle, le chiffrement à clé publique et le chiffrement symétrique. Dans le chiffrement symétrique, on distingue le chiffrement par bloc et le chiffrement par flot synchrone et autosynchrone. Puis, nous avons décrit des schémas de chiffrement basés sur le chaos, le masquage additif, la modulation chaotique, la modulation paramétrique et le chiffrement par inclusion. Une étude comparative a mis en évidence que les structures des émetteurs et des récepteurs du chiffrement par inclusion et du chiffrement par flot présentent des similitudes. En fait, le chiffrement par inclusion est un "mélange" du chiffrement par flot synchrone avec le chiffrement par flot autosynchrone. Sa clé est générée par une dynamique interne (comme pour le chiffrement par flot synchrone) et dépend du texte chiffré (comme pour le chiffrement par flot autosynchrone). Le chiffrement par inclusion présente l'avantage du chiffrement par flot autosynchrone (resynchronisation automatique) sans révéler l'inconvénient du chiffrement par flot synchrone (initialisation aux mêmes valeurs des générateurs de clés côté émetteur et côté récepteur).

Dans la suite, nous étudierons la modulation chaotique, la modulation paramétrique et le chiffrement par inclusion. Pour ces trois schémas, le problème est de synchroniser l'émetteur et le récepteur afin de reconstruire l'information. Ce problème de synchronisation peut être formulé comme un problème de synthèse d'observateurs non linéaires.
Le Chapitre 3 est dédié aux observateurs non linéaires dans le contexte de la modulation chaotique. Il s'agit de garantir la convergence à zéro de l'erreur de reconstruction d'état. Les résultats du Chapitre 1 concernant la stabilité des régimes permanents de type point fixe pourront alors être appliqués.
Pour la modulation paramétrique, un observateur adaptatif peut jouer le rôle de récepteur, assurant ainsi la reconstruction simultanée état/paramètre. Le Chapitre 4 est consacré aux observateurs adaptatifs dans le cadre de l'estimation simultanée état/paramètre.
Une étape essentielle de validation, qui fait largement défaut à ce jour, est la cryptanalyse. Nous nous intéressons plus particulièrement au chiffrement par inclusion et à la possibilité de reconstruire les paramètres constants du système chaotique, supposés jouer le rôle de clé secrète. Ce problème est directement lié au concept d'identifiabilité paramétrique, qui sera présenté dans le Chapitre 5.

Chapitre 3

Observateurs non linéaires à temps discret pour la modulation chaotique

3.1 Introduction

L'objet de ce chapitre est la modulation chaotique, introduite dans le Chapitre 2. On rappelle que, dans ce schéma, à chaque valeur de l'information $m_i \in \{m_1 \ldots, m_N\}$ à masquer correspond un signal particulier y_k, issu d'un émetteur régi par une dynamique chaotique.

$$\begin{cases} x_{k+1} = f_i(x_k) \\ y_k \quad\; = h_i(x_k) \end{cases} \tag{3.1}$$

où $i \in \{1, \ldots, N\}$ est l'indice qui dépend de la valeur courante de l'information, $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}^p$ le vecteur de sortie.
Ce schéma est rappelé sur la figure 3.1.

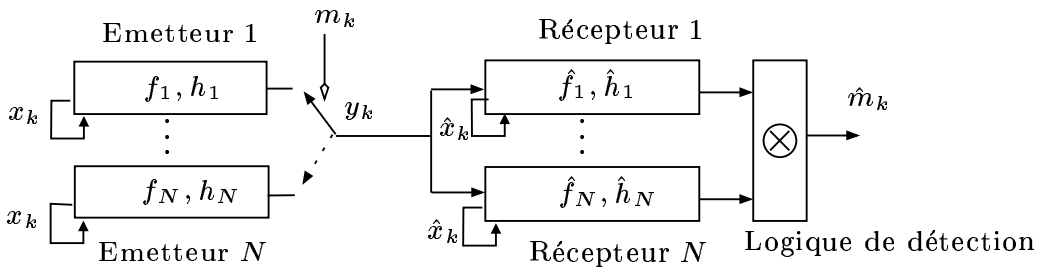


FIG. 3.1 – Modulation chaotique

Dans la suite, par souci de simplification, on omettra l'indice i et on notera $f_i = f$ et $h_i = h$.

Il y a autant d'émetteurs que de valeurs possibles pour l'information (ensemble fini). La reconstruction de l'information nécessite la synchronisation de l'émetteur et du récepteur. Le récepteur est composé d'autant de systèmes que l'émetteur, mais seulement un des récepteurs peut se synchroniser selon la valeur de l'information. Une détection logique permet alors de décider quel récepteur utiliser.
Dans ce chapitre, nous nous intéressons au problème de synchronisation de l'émetteur et du récepteur. Le récepteur est un observateur non linéaire à temps discret.

Une propriété essentielle des systèmes chaotiques est que le vecteur d'état est borné et évolue dans un ensemble compact et invariant de l'espace de phase, c'est-à-dire l'attracteur chaotique associé. Cette particularité peut être prise en compte lors de la synthèse d'observateurs particuliers, appelés polytopiques. Nous montrons que la plupart des systèmes chaotiques peuvent se réécrire sous forme LPV. Le paramètre variant étant fonction de l'état, il peut également se réécrire sous forme LPV. De plus, quand il est borné, il admet une description polytopique. L'erreur de reconstruction d'état correspondante, dont on cherche à garantir sa convergence à zéro, peut alors aussi se décomposer sous forme LPV polytopique. Nous montrons que le conservatisme des conditions de stabilité polyquadratique peut être réduit en considérant les sommets du polytope minimal dans lequel le paramètre réside [Millérioux et al., 2005].

Dans la Section 3.2, quelques structures d'observateurs non linéaires à temps discret, tirées de la littérature, sont rappelées. Dans la Section 3.3, la description convexe d'une récurrence chaotique est donnée et l'observateur polytopique proposé est présenté. Puis, dans la Section 3.4, quelques méthodes de recherche d'un polytope minimal sont décrites. La décomposition polytopique fait l'objet de la Section 3.5. Un récapitulatif de la méthode de synthèse d'observateur proposée est élaboré dans la Section 3.6. Dans la Section 3.7, un exemple de reconstruction d'état avec un observateur polytopique est donné dans un contexte de modulation chaotique.

3.2 Rappels sur les observateurs non linéaires

3.2.1 Filtre étendu de Kalman

On considère les systèmes non linéaires de la forme (3.1) où les fonctions f et h sont supposées être dérivables.
Le filtre étendu de Kalman a été introduit pour la première fois dans [Cox, 1964]. Son utilisation dans le contexte de la synchronisation du chaos en tant que récepteur a été proposée dans [Cruz and Nijmeijer, 2000]. La reconstruction d'état s'opère en deux étapes : une étape de prédiction et une étape d'estimation. L'étape de prédiction est donnée par :

$$\begin{cases} \hat{x}_{k+1/k} = f(\hat{x}_k) \\ \Upsilon_{k+1/k} = F_k \Upsilon_k F_k^T + Q_k \end{cases} \tag{3.2}$$

où $\hat{x}_{k+1/k} \in \mathbb{R}^n$ est la prédiction à un pas du vecteur d'état x_{k+1}. $\Upsilon_{k+1/k}$ est la matrice de covariance de l'erreur de prédiction $\epsilon_{k+1/k} \triangleq x_{k+1} - \hat{x}_{k+1/k}$. Q_k est une matrice de pondération définie positive. La matrice F_k est le jacobien[1] de la fonction f au point $x_k = \hat{x}_k$.

L'étape d'estimation est décrite par :

$$\begin{cases} \hat{x}_{k+1} = \hat{x}_{k+1/k} + K_{k+1}(y_{k+1} - h(\hat{x}_{k+1/k})) \\ \Upsilon_{k+1} = (\mathbf{1}_n - K_{k+1}H_{k+1})\Upsilon_{k+1/k} \end{cases} \tag{3.3}$$

où $\hat{x}_{k+1} \in \mathbb{R}^n$ est l'estimation du vecteur d'état x_{k+1}. Υ_{k+1} est la matrice de covariance de l'erreur d'estimation $\epsilon_{k+1} \triangleq x_{k+1} - \hat{x}_{k+1}$. La matrice H_k est le jacobien[1] de la fonction h en $x_k = \hat{x}_k$.

La matrice K_k représente le gain de Kalman et vérifie :

$$K_{k+1} = \Upsilon_{k+1/k} H_{k+1}^T (H_{k+1} \Upsilon_{k+1/k} H_{k+1}^T + R_{k+1})^{-1} \tag{3.4}$$

[1] Voir Annexe A, Définition 28

où R_k est une matrice de pondération définie positive.

La stabilité de l'erreur d'estimation d'état est établie en utilisant la fonction de Lyapunov définie par $V(\epsilon_{k+1}) = \epsilon_{k+1}^T \Upsilon_{k+1}^{-1} \epsilon_{k+1}$, avec Υ_{k+1} donné par (3.3).

L'avantage du filtre de Kalman étendu est que la reconstruction d'état est possible même si le système est bruité (bruits gaussiens). Dans ce cas, la matrice Q_k représente la covariance des bruits dynamiques et R_k celle des bruits de mesures. En revanche, pour le calcul du gain, la méthode étant basée sur une linéarisation de la dynamique le long de la trajectoire, il est difficile d'assurer la convergence globale de l'erreur de reconstruction d'état. Néanmoins, des conditions de convergence globale sont établies par linéarisation exacte dans [Boutayeb et al., 1997].
Une alternative est de transformer le système non linéaire (3.1) en un système de Lur'e et de synthétiser un observateur pour le système ainsi transformé. L'erreur de reconstruction d'état possède alors une forme linéaire et sa convergence globale peut être assurée, comme expliqué dans la section suivante.

3.2.2 Observateurs par linéarisation avec injection de la sortie

On considère des systèmes non linéaires de la forme :

$$\begin{cases} x_{k+1} = f(x_k) \\ y_k \quad\;\; = h(x_k) \end{cases} \tag{3.5}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état et $y_k \in \mathbb{R}$ la sortie.
Une approche proposée dans [Lin and Byrnes, 1995] consiste à trouver un changement de coordonnées $z = T(x)$, où T est une transformation inversible, qui transforme le système non linéaire (3.5) en un système sous forme de Lur'e :

$$\begin{cases} z_{k+1} = Az_k + \varphi(y_k) \\ y_k \quad\;\; = Cz_k \end{cases} \tag{3.6}$$

où $z_k \in \mathbb{R}^n$ et $y_k \in \mathbb{R}$. Le système (3.6) est affine en z_k. $\varphi(y_k)$ est une fonction non linéaire dépendant uniquement de la sortie y_k qui est accessible. Les matrices constantes $A \in \mathbb{R}^{n\times n}$ et $C \in \mathbb{R}^{1\times n}$ ont respectivement la forme suivante :

$$A = \begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \end{bmatrix}, \quad C = \begin{bmatrix} 1 & 0 & \dots & 0 \end{bmatrix} \tag{3.7}$$

où $\alpha_i \in \mathbb{R}$.
La difficulté de l'approche consiste à prouver l'existence d'une transformation T. Une condition nécessaire et suffisante pour transformer (3.5) en (3.6) est donnée dans [Lin and Byrnes, 1995].

Théorème 8. Le système (3.5) est localement équivalent au système de Lur'e (3.6) via la transformation $z = T(x)$ si et seulement si :

(i) la matrice

$$\mathcal{O}(x_0) = \left[\begin{array}{c} \dfrac{\partial h(x_k)}{\partial x_k} \\ \dfrac{\partial h \circ f(x_k)}{\partial x_k} \\ \vdots \\ \dfrac{\partial h \circ f^{n-1}(x_k)}{\partial x_k} \end{array} \right]_{x_k = x_0} \tag{3.8}$$

est de rang n,

(ii) $h \circ f^n(x_k) = \sum_{i=1}^{n} \alpha_i h \circ f^{i-1}(x_k)$, pour tout x_k dans un voisinage de x_0, $\alpha_i \in \mathbb{R}$, $i = \{1, \ldots, n\}$, où $f^i(x_k) \triangleq f(f^{i-1}(x_k))\ \forall i \geq 1$ et $f^0(x_k) \triangleq x_k$.

Le changement de coordonnées est alors défini par :

$$\begin{aligned} z_{k+1}^{(i)} &= z_k^{(i+1)} = h \circ f^i(x_k) \qquad i = 1, \ldots, n-1 \\ z_{k+1}^{(n)} &= \sum_{i=1}^{n} \alpha_i z_k^i = h \circ f^n(x_k) \end{aligned} \tag{3.9}$$

L'observateur synthétisé pour le système (3.6) est de la forme :

$$\left\{ \begin{array}{ll} \hat{z}_{k+1} & = A\hat{z}_k + \varphi(y_k) + L(y_k - \hat{y}_k) \\ \hat{y}_k & = C\hat{z}_k \end{array} \right. \tag{3.10}$$

Le terme L représente le gain de l'observateur. L'erreur de reconstruction d'état $\epsilon_{k+1} \triangleq z_{k+1} - \hat{z}_{k+1}$, est obtenue en soustrayant (3.10) à (3.6) :

$$\epsilon_{k+1} = (A - LC)\epsilon_k \tag{3.11}$$

L'erreur ϵ_{k+1} a une forme linéaire en ϵ_k. Pour garantir sa convergence à zéro, le gain L est choisi de telle sorte que la matrice $(A - LC)$ soit Hurwitz[1].
Finalement, la reconstruction de l'état $\hat{x}_k$ est donnée par $\hat{x} = T^{-1}(\hat{z})$.

Les résultats ont été étendus au cas où $y_k \in \mathbb{R}^p$ dans [Lin and Byrnes, 1995].

La classe des systèmes pour lesquels l'erreur de reconstruction d'état est linéaire, est étendue dans [Huijberts, 1999] [Lilge, 1999] [Huijberts et al., 2000]. Dans ce cas, on cherche une transformation T telle que le système (3.5) puisse être réécrit sous la forme dite de Lur'e étendue :

$$\left\{ \begin{array}{ll} z_{k+1} & = Az_k + \varphi(y_k, y_{k-1}, \ldots, y_{k-N}) \\ y_k & = Cz_k \end{array} \right. \tag{3.12}$$

La fonction non linéaire φ dépend d'un nombre fini N de valeurs passées de la sortie y_k qui est accessible. Les matrices A et C ont respectivement la forme :

$$A = \left[\begin{array}{cccc} 0 & \ldots & 0 & 0 \\ 1 & \ldots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \ldots & 1 & 0 \end{array} \right], \quad C = \left[\begin{array}{cccc} 0 & \ldots & 0 & 1 \end{array} \right] \tag{3.13}$$

[1] voir Annexe A, Définition 33

Le système (3.5) est équivalent à (3.12) si et seulement si la matrice d'observabilité $\mathcal{O}(x_k)$

$$\mathcal{O}(x_k) = \begin{bmatrix} h(x_k) \\ h \circ f(x_k) \\ \vdots \\ h \circ f^{n-1}(x_k) \end{bmatrix} \tag{3.14}$$

est un difféomorphisme[1] global [Lilge, 1999].

L'observateur synthétisé pour le système (3.12) est :

$$\begin{cases} \hat{z}_{k+1} = A\hat{z}_k + \varphi(y_k, y_{k-1}, \ldots, y_{k-N}) + L(y_k - \hat{y}_k) \\ \hat{y}_k \quad = C\hat{z}_k \end{cases} \tag{3.15}$$

L'erreur de reconstruction d'état ϵ_{k+1} est obtenue en soustrayant (3.15) à (3.12) :

$$\epsilon_{k+1} = (A - LC)\epsilon_k \tag{3.16}$$

Comme précédemment, l'erreur de reconstruction d'état est linéaire. Pour assurer la stabilité du système, le gain L est choisi de telle sorte que $(A - LC)$ soit Hurwitz.

Les observateurs présentés ci-dessus ne tiennent pas compte de la spécificité liée au chaos. Dans la section suivante, des observateurs particuliers appelés polytopiques, qui prennent en compte cette particularité liée au chaos, sont présentés. Le principe est de réécrire le système chaotique sous forme LPV (cf. Chapitre 1).

3.3 Observateur polytopique

3.3.1 Description convexe d'une récurrence chaotique

Il n'existe pas de structure générique pour décrire l'ensemble des systèmes chaotiques. En effet, beaucoup de systèmes non linéaires possédant une valeur adéquate pour leurs paramètres peuvent présenter un comportement chaotique. Nous nous intéressons à des systèmes chaotiques qui peuvent être écrits sous la forme :

$$\begin{cases} x_{k+1} = A(x_k)x_k + E(x_k) \\ y_k \quad = Cx_k \end{cases} \tag{3.17}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état et $y_k \in \mathbb{R}^p$ le vecteur de sortie. La matrice d'état $A \in \mathbb{R}^{n \times n}$ et le vecteur $E \in \mathbb{R}^n$ varient dans le temps car ils dépendent de x_k.

Le système (3.17) permet de représenter de nombreux systèmes chaotiques. En effet, lorsque x_k visite la région R_i de l'espace d'état et que $A(x_k) = A_i$ et $E(x_k) = E_i$ sont constants, avec $\bigcup_{i=1}^{N} R_i \subseteq \mathbb{R}^n$, cela revient à considérer la classe des systèmes linéaires par morceaux ("piecewise linear systems", en anglais). Un système linéaire par morceaux est défini par :

$$x_{k+1} = A_i x_k + E_i \quad \text{si } x_k \in R_i, \quad i = 1, \ldots, N \tag{3.18}$$

[1] voir Annexe A, Définition 34

Un exemple de système linéaire par morceaux est la Tent map dont la représentation d'état est la suivante :

$$x_{k+1} = \begin{cases} 2x_k & \text{si } x_k < 0.5 \\ 2(1-x_k) & \text{si } x_k \geq 0.5 \end{cases} \tag{3.19}$$

Lorsque la dépendance de A par rapport à x_k est polynomiale, cela revient à considérer tout un ensemble de récurrences chaotiques telles que la récurrence logistique, la récurrence de Hénon, la récurrence d'Ikeda, ... (cf. Chapitre 1).

Dans la suite, par souci de simplification, on traitera le cas où $E = 0$. Le système (3.17) devient alors :

$$\begin{cases} x_{k+1} = A(x_k)x_k \\ y_k \quad = Cx_k \end{cases} \tag{3.20}$$

Une propriété essentielle d'un système chaotique est que le vecteur d'état est borné et évolue dans un ensemble compact et invariant de l'espace de phase, l'attracteur chaotique Ω. En tenant compte de cette propriété, on effectue un changement de variable, afin de réécrire la matrice d'état A, qui dépend de façon non linéaire de x_k, sous la forme d'une autre matrice, notée $\mathcal{A}$, qui dépend de façon linéaire d'un vecteur ρ_k qui est fonction de x_k. Les systèmes chaotiques admettant la forme (3.20) peuvent alors se réécrire sous une forme convexe.
La proposition suivante [Millérioux et al., 2005] énonce les conditions de réécriture du système (3.20) sous forme polytopique convexe.

Proposition 1. Considérons (3.20) avec x_k évoluant dans un attracteur chaotique Ω. S'il existe une fonction $\Psi : \mathbb{R}^n \to \mathbb{R}^L$ définie par $\rho_k = \Psi(x_k)$ et telle que :

(i) $\mathcal{A}$ vérifiant $\mathcal{A}(\rho_k) = \mathcal{A}(\Psi(x_k)) = A(x_k)$ soit de classe[1] C^1 par rapport à ρ_k,

(ii) ρ_k reste borné lorsque x_k est borné,

alors il existe un entier N, un vecteur $\xi_k \in S(\mathcal{D}_\rho)$ et des matrices $A^{(i)}$ tels que (3.20) peut être réécrit sous la forme polytopique :

$$\begin{cases} x_{k+1} = \mathcal{A}(\rho_k)x_k \\ y_k \quad = Cx_k \end{cases} \tag{3.21}$$

avec :

$$\mathcal{A}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k)A^{(i)} \tag{3.22}$$

$\rho_k \in \mathbb{R}^L$ est le vecteur des paramètres variants, qui est fonction de l'état x_k et qui est mesurable à travers la sortie. ρ_k étant fonction de x_k, le vecteur ξ_k appartient à l'ensemble convexe compact

$$S(\mathcal{D}_\rho) = \{\mu_k \in \mathbb{R}^N, \mu_k = [\mu_k^{(1)} \dots \mu_k^{(N)}]^T, \mu_k^{(i)} \geq 0 \quad \forall i, \sum_{i=1}^{N} \mu_k^{(i)} = 1\}.$$

$\mathcal{D}_\rho$ est un polytope convexe auquel appartient ρ_k et l'ensemble convexe compact S dépend de ce polytope. Les matrices $A^{(i)}$ définissent un polytope convexe $\mathcal{D}_\mathcal{A}$ dont les sommets sont les matrices constantes $A^{(1)}, \dots, A^{(N)}$.
Le système (3.21) est un système LPV.

[1] Voir Annexe A, Définition 35

Preuve 1. D'une part, supposons qu'il existe une fonction Ψ telle que $\mathcal{A}$, satisfaisant $\mathcal{A}(\rho_k) = \mathcal{A}(\Psi(x_k)) = A(x_k)$, soit de classe C^1 par rapport à ρ_k (condition (i)). Puisque $\mathcal{A}$ dépend linéairement de ρ_k, cette matrice peut s'écrire :

$$\mathcal{A}(\rho_k) = \mathcal{A}_0 + \sum_{j=1}^{L} \rho_k^{(j)} A^{I_j} \tag{3.23}$$

$\mathcal{A}_0$ est une matrice qui exprime la partie constante de $\mathcal{A}$. Les matrices A^{I_j} sont constantes et ont tous leurs éléments nuls sauf ceux qui dépendent linéairement de ρ_k. Elles peuvent se mettre sous la forme :

$$A^{I_j} = \begin{array}{c} \\ l \end{array} \overset{\overset{c}{\downarrow}}{\begin{bmatrix} 0 & \dots & 0 \\ \vdots & 1 & \vdots \\ 0 & \dots & 0 \end{bmatrix}} \tag{3.24}$$

A la colonne c, ligne l, correspond la position de la composante $\rho_k^{(j)}$.
D'autre part, comme le système (3.17) est chaotique, l'état interne x_k évolue dans un ensemble compact Ω. La condition (ii) garantit que ρ_k est borné quand x_k l'est. Par conséquent, ρ_k appartient également à un ensemble compact Ω_ρ, l'image de Ω par Ψ, et donc il existera toujours un polytope convexe $\mathcal{D}_\rho$ tel que $\Omega_\rho \subset \mathcal{D}_\rho$. Il existe alors toujours un entier $N < \infty$ et un vecteur $\xi_k \in S(\mathcal{D}_\rho)$ tels que :

$$\rho_k = \sum_{i=1}^{N} \xi_k^{(i)} \rho_{o_i} \tag{3.25}$$

$S(\mathcal{D}_\rho)$ est l'ensemble convexe compact qui dépend du polytope $\mathcal{D}_\rho$.
La relation (3.25) représente la forme implicite de la dépendance de ξ_k à ρ_k.

La relation (3.25) s'écrit, composante par composante, $\rho_k^{(j)} = \sum_{i=1}^{N} \xi_k^{(i)} \rho_{o_i}^{(j)}$ et (3.23) devient :

$$\mathcal{A}(\rho_k) = \mathcal{A}_0 + \sum_{j=1}^{L} \Big(\sum_{i=1}^{N} \big(\xi_k^{(i)} \rho_{o_i}^{(j)} A^{I_j} \big) \Big) \tag{3.26}$$

Comme $\sum_{i=1}^{N} \xi_k^{(i)} = 1$, on peut écrire :

$$\mathcal{A}_0 = \sum_{i=1}^{N} \xi_k^{(i)} \mathcal{A}_0 \tag{3.27}$$

Puisque $\xi_k^{(i)}$ ne dépend que de i (et non de j) :

$$\mathcal{A}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)} \underbrace{\Big(\mathcal{A}_0 + \sum_{j=1}^{L} \rho_{o_i}^{(j)} A^{I_j} \Big)}_{A^{(i)}} \tag{3.28}$$

Finalement en identifiant (3.28) et (3.22), les matrices $A^{(i)}$ ont pour expression :

$$A^{(i)} = \mathcal{A}_0 + \sum_{j=1}^{L} \rho_{o_i}^{(j)} A^{I_j} \tag{3.29}$$

■

L'équation (3.22) signifie que $\mathcal{A}$ appartient à un polytope convexe $\mathcal{D}_{\mathcal{A}}$. La structure de ce polytope dépend implicitement de la structure de l'attracteur chaotique Ω. En effet, $\mathcal{D}_{\mathcal{A}}$ dépend de $\mathcal{D}_\rho$ (figure 3.2), le polytope à l'intérieur duquel évolue le vecteur ρ_k, ρ_k étant lui-même fonction du vecteur d'état x_k appartenant à l'attracteur chaotique.

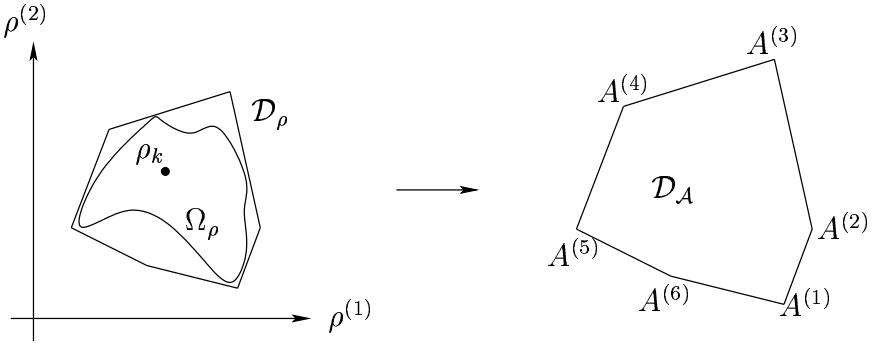


FIG. 3.2 – Ensemble compact Ω_ρ, polytope $\mathcal{D}_\rho$ et polytope $\mathcal{D}_{\mathcal{A}}$

La reconstruction d'état pour les systèmes chaotiques réécrits sous la forme (3.21)-(3.22) est détaillée ci-dessous.

3.3.2 Reconstruction d'état

On suppose que la Proposition 1 est vérifiée, c'est-à-dire que le système chaotique (3.20) admet une description polytopique (3.21)-(3.22). Le vecteur ρ_k est disponible à chaque instant, car il est mesurable à travers la sortie. La reconstruction du vecteur d'état x_k peut alors être assurée par l'observateur suivant :

$$\begin{cases} \hat{x}_{k+1} = \mathcal{A}(\rho_k)\hat{x}_k + \mathcal{L}(\rho_k)(y_k - \hat{y}_k) \\ \hat{y}_k \quad\;\; = C\hat{x}_k \end{cases} \tag{3.30}$$

où $\mathcal{L}$ est un gain dépendant du vecteur de paramètres ρ_k donc variant dans le temps. L'erreur de reconstruction d'état $\epsilon_k \triangleq x_k - \hat{x}_k$, est obtenue en soustrayant (3.30) à (3.21) :

$$\epsilon_{k+1} = (\mathcal{A}(\rho_k) - \mathcal{L}(\rho_k)C)\epsilon_k \tag{3.31}$$

La dynamique de l'erreur de reconstruction (3.31) est linéaire en ϵ_k, mais à temps variant car les matrices $\mathcal{A}$ et $\mathcal{L}$ dépendent du paramètre ρ_k. (3.31) est un système LPV dont on cherche à garantir la convergence globale à zéro. Un choix judicieux du gain $\mathcal{L}$ est le suivant :

$$\mathcal{L}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)} L_i \tag{3.32}$$

(3.32) signifie que $\mathcal{L}$ appartient à un polytope $\mathcal{D}_{\mathcal{L}}$ dont les matrices sommets associées sont $L_1, \ldots, L_N$. C'est pourquoi l'observateur (3.30) est appelé polytopique. Le vecteur ξ_k doit coïncider avec celui qui intervient dans (3.22), ce qui est toujours possible (cf. Section 3.5) car ξ_k dépend de ρ_k qui est supposé accessible à travers la sortie. Avec la description polytopique de $\mathcal{A}$ (3.22) et celle de $\mathcal{L}$ (3.32), la dynamique (3.31) peut se réécrire sous la forme :

$$\epsilon_{k+1} = (\sum_{i=1}^{N} \xi_k^{(i)} (A^{(i)} - L_i C))\epsilon_k \tag{3.33}$$

avec $\xi_k \in S(\mathcal{D}_\rho)$. (3.33) est l'équation d'un système LPV polytopique. Le Théorème 6 (Chapitre 1, Section 1.8.2) devient, en posant $A_\epsilon^{(i)} = A^{(i)} - L_i C$:

Proposition 2. L'erreur de reconstruction (3.33) converge globalement s'il existe des matrices G_i, des matrices symétriques définies positives P_i et F_i, de dimensions appropriées, telles que l'ensemble d'inégalités matricielles suivant :

$$\left[\begin{array}{cc} G_i + G_i^T - P_i & G_i^T A^{(i)} - F_i^T C \\ (A^{(i)})^T G_i - C^T F_i & P_j \end{array} \right] > 0 \tag{3.34}$$

soit faisable $\forall (i,j) \in (1,\ldots,N) \times (1,\ldots,N)$ et $L_i = (G_i^{-1})^T F_i^T$.

Dans [Daafouz and Bernussou, 2001], il est montré que la fonction de Lyapunov $V(\epsilon_k) = \epsilon_k^T \mathcal{P}_k \epsilon_k$, avec $\mathcal{P}_k = \sum_{i=1}^{N} \xi_k^{(i)} P_i$ et $\xi_k \in S(\mathcal{D}_\rho)$, vérifie, $\forall \epsilon_k \neq 0$:

$$V(\epsilon_{k+1}) - V(\epsilon_k) < 0 \quad \forall \xi_k \in S(\mathcal{D}_\rho) \tag{3.35}$$

L'objet de la section suivante est de réduire le conservatisme des conditions de stabilité (3.34).

3.3.3 Réduction du conservatisme

Le vecteur de paramètres ρ_k réside dans un ensemble compact convexe Ω_ρ (équation (3.25)), qui dépend implicitement de la structure de l'attracteur chaotique Ω. Le conservatisme des conditions de stabilité polyquadratique peut être réduit en considérant les sommets de l'enveloppe convexe minimale $\mathcal{D}_\rho^*$ dans laquelle le vecteur de paramètres ρ_k est englobé.

Proposition 3. [Millérioux et al., 2005] Pour la récurrence chaotique de forme convexe (3.21), les conditions les moins conservatives qui assurent la stabilité polyquadratique de (3.21) sont obtenues pour les matrices $A^{(i)}$ dérivées de ρ_{o_i} correspondant au polytope convexe minimal $\mathcal{D}_\rho^*$.

En effet, considérons un polytope $\mathcal{D}_\rho$ arbitraire qui contient l'ensemble Ω_ρ (figure 3.3).
D'une part, considérons des points $\rho_k^* \in \mathcal{D}_\rho$ particuliers pour lesquels (3.35) n'est pas vérifiée. Prenons un polytope $\mathcal{D}_{\rho'}$ tel que $\mathcal{D}_\rho \subset \mathcal{D}_{\rho'}$ (figure 3.3(a)). Tous les points ρ_k^* sont aussi inclus dans $\mathcal{D}_{\rho'}$ et (3.35) n'est toujours pas vérifiée en remplaçant $\mathcal{D}_\rho$ par $\mathcal{D}_{\rho'}$. Réciproquement, considérons que le polytope $\mathcal{D}_{\rho'}$ vérifie $\Omega_\rho \subseteq \mathcal{D}_{\rho'} \subset \mathcal{D}_\rho$ (figure 3.3(b)). Dans ce cas, $\mathcal{D}_{\rho'}$ ne contient plus forcément les points particuliers ρ_k^*. Par conséquent, (3.35) peut être vérifiée pour $\rho_k^* \in \mathcal{D}_{\rho'}$.
D'autre part, supposons qu'il n'existe pas de points $\rho_k^* \in \mathcal{D}_\rho$ pour lesquels (3.35) ne soit plus

vérifiée. Considérons un polytope $\mathcal{D}_{\rho'}$ tel que $\mathcal{D}_\rho \subset \mathcal{D}_{\rho'}$ (figure 3.3(c)). Par conséquent, il peut exister des points $\rho_k^* \in \mathcal{D}_{\rho'}$ tels que (3.35) n'est plus vérifiée. Réciproquement, considérant un polytope $\mathcal{D}_{\rho'}$ tel que $\Omega_\rho \subseteq \mathcal{D}_{\rho'} \subset \mathcal{D}_\rho$, il ne peut exister de points $\rho_k^* \in \mathcal{D}_{\rho'}$ tels que (3.35) ne soit pas vérifiée (figure 3.3(d)).
En conclusion, le polytope optimal est celui correspondant à l'enveloppe convexe de Ω_ρ.

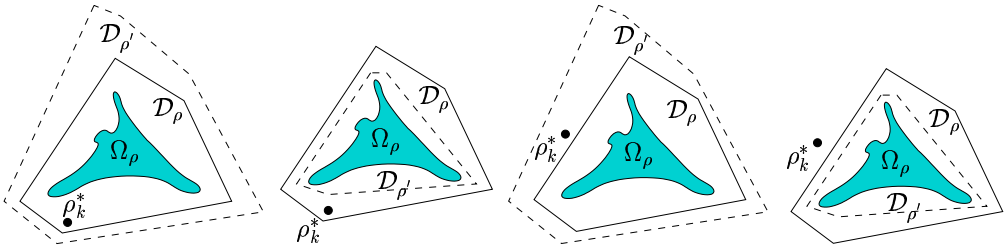


FIG. 3.3 –

3.4 Recherche du polytope convexe minimal

Les différentes méthodes de recherche du polytope convexe minimal $\mathcal{D}_\rho^*$ sont présentées ci-dessous.

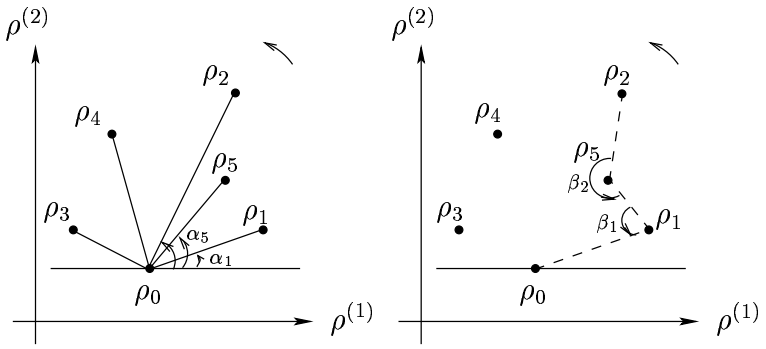
Pour déterminer l'enveloppe convexe minimale d'un ensemble de points en dimension deux, il existe de nombreux algorithmes comme la marche de Graham, l'algorithme "Quick hull", l'approche par échantillonnage et l'approche par programmation linéaire. En revanche, en dimension supérieure à deux, le problème est plus complexe et les algorithmes doivent être étendus ou adaptés quand cela est possible. Nous allons présenter ces algorithmes en dimension deux et leur éventuelle extension en dimension supérieure à deux.

Dans toute la suite, nous considérons un ensemble fini de points $\Lambda = \{\rho_0, \ldots, \rho_K\}$, appelé également liste. Les points ρ_i, $i = 0, \ldots, K$, sont rangés dans Λ dans leur ordre d'apparition au cours du temps. En dimension deux, on a $\rho_i = [\rho_i^{(1)} \quad \rho_i^{(2)}]^T$.

3.4.1 Algorithme de Graham

L'algorithme de Graham [Graham, 1973] ("Graham scan", en anglais) est basé sur le principe que deux faces consécutives, formées par trois points consécutifs de l'enveloppe convexe, forment forcément un angle inférieur à π. L'algorithme se déroule en deux étapes, le tri des points consécutifs et le calcul des angles entre les faces consécutives.
Tout d'abord, il faut choisir un point de l'ensemble Λ, sommet de l'enveloppe convexe, qui va servir de référence pour le tri des points. On peut choisir, par exemple, le point qui a l'ordonnée minimale. Si plusieurs points ont la même ordonnée minimale, on peut choisir celui qui a la plus grande abscisse, par exemple. Ce point de référence est noté ρ_0.
La première étape consiste en un tri des points ρ_i de Λ, par rapport à la valeur de l'angle α_i entre la droite horizontale passant par ρ_0 et la droite $(\rho_0\rho_i)$. Les différents points sont alors classés dans

l'ordre croissant des valeurs de cet angle et on notera Λ_t la liste des points ainsi triés. Pour cela, il faut fixer un sens arbitraire, par exemple, le sens trigonométrique. Cette étape de tri est illustrée sur la figure 3.4(a). Pour cet exemple, la liste des points ainsi triés est $\Lambda_t = \{\rho_0\rho_1\rho_5\rho_2\rho_4\rho_3\}$.



(a) Tri des points consécutifs (b) Marche de Graham

FIG. 3.4 – Etapes de l'algorithme de Graham

Le tri des points ne nécessite pas le calcul explicite des angles α_i, mais est basé sur le calcul du produit vectoriel des vecteurs $\rho_0\vec{\rho}_i$ et $\rho_0\vec{\rho}_j$, respectivement de coordonnées $(\rho_i^{(1)} - \rho_0^{(1)}; \rho_i^{(2)} - \rho_0^{(2)})$ et $(\rho_j^{(1)} - \rho_0^{(1)}; \rho_j^{(2)} - \rho_0^{(2)})$:

$$\alpha_i < \alpha_j \Leftrightarrow Q = (\rho_i^{(2)} - \rho_0^{(2)})(\rho_j^{(1)} - \rho_0^{(1)}) - (\rho_j^{(2)} - \rho_0^{(2)})(\rho_i^{(1)} - \rho_0^{(1)}) < 0 \tag{3.36}$$

En effet, si $\alpha_i < \alpha_j$, cela signifie que le point ρ_j est à gauche du vecteur $\rho_0\vec{\rho}_i$.
L'avantage d'utiliser cette relation est que la comparaison des angles ne nécessite que des opérations simples (additions, multiplications).
La deuxième étape est appelée "Marche de Graham". Elle consiste à tester si l'angle entre deux faces consécutives (formées par trois points consécutifs triés ρ_i, ρ_j et ρ_l) est inférieur à π. Si l'angle entre ρ_i, ρ_j et ρ_l, noté β_j, est inférieur à π, le point ρ_j est un sommet de l'enveloppe convexe. En revanche, si $\beta_j > \pi$, le point ρ_j n'est pas un sommet de l'enveloppe convexe. Dans ce cas, il est retiré de la liste des points triés Λ_t et on recommence le test avec la nouvelle liste $\Lambda_t - \{\rho_j\}$, jusqu'à avoir parcouru tous les points. A la fin du test, la liste Λ_t contient uniquement les sommets de l'enveloppe convexe. Comme précédemment, cette comparaison ne nécessite pas le calcul des angles, mais est basée sur le calcul du produit vectoriel des vecteurs $\rho_i\vec{\rho}_j$ et $\rho_i\vec{\rho}_l$, respectivement de coordonnées $(\rho_j^{(1)} - \rho_i^{(1)}; \rho_j^{(2)} - \rho_i^{(2)})$ et $(\rho_l^{(1)} - \rho_i^{(1)}; \rho_l^{(2)} - \rho_i^{(2)})$:

$$\beta_j \leq \pi \Leftrightarrow (\rho_j^{(1)} - \rho_i^{(1)})(\rho_l^{(2)} - \rho_i^{(2)}) - (\rho_l^{(1)} - \rho_i^{(1)})(\rho_j^{(2)} - \rho_i^{(2)}) \leq 0 \tag{3.37}$$

La figure 3.4(b) illustre une étape de la marche de Graham. Par exemple, sur cette figure, le point ρ_1 appartient à l'enveloppe convexe car $\beta_1 < \pi$, alors que ρ_5 n'appartient pas à l'enveloppe convexe car $\beta_2 > \pi$. On supprime ρ_5 de la liste Λ_t et on recommence le test avec la nouvelle liste $\Lambda_t = \{\rho_0\rho_1\rho_2\rho_4\rho_3\}$, jusqu'à ce que tous les points de Λ_t soient parcourus et que tous les angles testés soient inférieurs à π. Dans cet exemple, les sommets de l'enveloppe convexe sont finalement $\{\rho_0\rho_1\rho_2\rho_4\rho_3\}$ et le polytope convexe minimal est représenté sur la figure 3.5.
Un avantage de cette approche est que la complexité de l'algorithme est $\sigma(K \log K)$[1], K étant

[1] Voir Annexe C

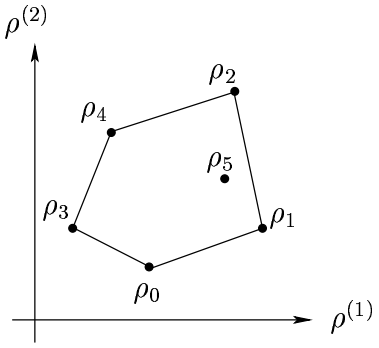


FIG. 3.5 – Polytope convexe minimal

le nombre de points de Λ, ce qui est assez faible. L'inconvénient de cette approche est qu'elle ne peut pas être généralisée à des dimensions supérieures à 2.

3.4.2 "Quick Hull"

Plusieurs versions de l'algorithme "Quick Hull" ont été proposées dans [Eddy, 1977] et [Preparata and Shamos, 1985]. Cet algorithme est basé sur une approche du type "diviser pour mieux régner". En effet, le principe est que les points situés à l'intérieur d'un triangle, dont les sommets sont des points de l'ensemble Λ, n'appartiennent pas à l'enveloppe convexe et ne sont plus considérés pour la recherche des points extrêmes.
On commence par choisir deux points de référence, ρ_0 et ρ_1, dont on est sûr qu'ils appartiennent à l'enveloppe convexe (figure 3.6). On peut choisir, par exemple, les points qui ont respectivement l'abscisse maximale et l'abscisse minimale. La droite passant par ces deux points de référence, $(\rho_0\rho_1)$, divise l'ensemble Λ en deux sous-ensembles. Dans chaque sous-ensemble, on cherche le point qui possède la plus grande distance euclidienne à la droite $(\rho_0\rho_1)$. Ces deux points, notés ρ_i et ρ_j, sont assurés d'appartenir à l'enveloppe convexe. Les points situés strictement à l'intérieur des triangles $\rho_0\rho_1\rho_i$ et $\rho_0\rho_1\rho_j$ n'appartiennent pas à l'enveloppe convexe. Par conséquent, ces points sont supprimés de la liste Λ. On recommence la procédure avec des nouvelles droites de référence passant par deux points choisis arbitrairement dont on vient de prouver qu'ils appartiennent à l'enveloppe convexe. On répète cette procédure jusqu'à ce que toutes les droites possibles passant par deux points de Λ soient parcourues.
La figure 3.6 illustre cette démarche. La droite $(\rho_0\rho_1)$ divise l'ensemble de points en deux régions. Les points ρ_2 et ρ_3 ont, respectivement dans chaque région, la plus grande distance euclidienne à la droite $(\rho_0\rho_1)$. Ils appartiennent donc à l'enveloppe convexe. Le point ρ_5, situé à l'intérieur du triangle $\rho_0\rho_1\rho_2$, n'appartient pas à l'enveloppe convexe. Il est donc supprimé de la liste. On recommence la procédure avec une nouvelle droite de référence, par exemple $(\rho_0\rho_2)$. Finalement, les points extrêmes sont $\{\rho_0\rho_1\rho_2\rho_3\rho_4\}$.
Comme la Marche de Graham, cet algorithme a une complexité de $\sigma(K \log K)$. L'avantage de cet algorithme est qu'il peut être étendu à des dimensions supérieures à 2.
En dimension 3, cet algorithme a été étudié par [Allison and Noga, 1997]. Le principe est que les points situés à l'intérieur d'un tétraèdre, dont les sommets sont des éléments de Λ, n'appartiennent pas à l'enveloppe convexe et ne sont plus considérés dans la recherche des points extrêmes. Comme précédemment, pour commencer la division, on choisit trois points de référence ρ_0, ρ_1 et ρ_2, dont on est sûr qu'ils appartiennent à l'enveloppe convexe. Ces trois points

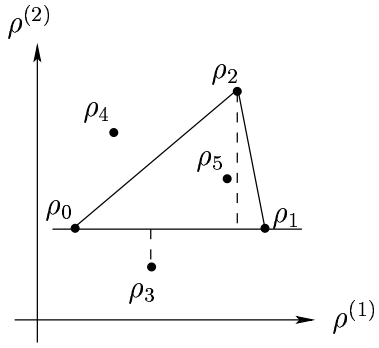


FIG. 3.6 – Quick Hull

forment une face triangulaire qui divise l'espace. On cherche le point ρ_i qui possède la plus grande distance euclidienne à la face initiale. Les points situés à l'intérieur du tétraèdre $\rho_0\rho_1\rho_2\rho_i$ ne sont pas des points extrêmes. Ils sont supprimés de la liste et la procédure est réitérée jusqu'à ce que tous les points soient parcourus.
En dimension 3, la complexité de l'algorithme est $\sigma(K^2)$.

3.4.3 Echantillonnage aléatoire

Une autre approche pour trouver les points extrêmes d'un ensemble de points Λ, appelée échantillonnage aléatoire ("random sampling", en anglais), est due à [Chatterjee and Chatterjee, 1990].
Le principe de cette approche consiste à projeter les points de l'ensemble Λ sur une droite choisie arbitrairement. Les points de la droite ayant respectivement l'abscisse minimale et l'abscisse maximale appartiennent à l'enveloppe convexe. Cette procédure est réitérée avec des nouvelles droites choisies arbitrairement, jusqu'à ne plus trouver de nouveaux points extrêmes. L'inconvénient de cette approche est que des projections sur des droites différentes peuvent conduire à trouver la même paire de points extrêmes. Pour supprimer cette perte d'efficacité, l'échantillonnage aléatoire est restreint en éliminant les projections qui ne conduisent pas à une nouvelle paire de points extrêmes. Cette élimination est basée sur le principe suivant. Si deux droites arbitraires, qui forment respectivement un angle avec l'axe des abscisses α_1 et α_2, conduisent à la même paire de points extrêmes, alors toute droite formant un angle α avec l'axe des abscisses, $\alpha_1 < \alpha < \alpha_2$, conduira à la même paire de points extrêmes. Par conséquent, toute droite ayant un angle α avec l'axe des abscisses, $\alpha_1 < \alpha < \alpha_2$, ne sera pas testée puisqu'elle n'apporte pas de nouvelle paire de points extrêmes. Cette approche est illustrée sur la figure 3.7. Dans cet exemple, la projection des points de Λ sur la droite D_1 montrent que ρ_2 et ρ_3 sont des points extrêmes. La projection sur D_2 met en évidence les mêmes points extrêmes. Par conséquent, toute droite formant un angle $\alpha_1 < \alpha < \alpha_2$ conduira aux mêmes points extrêmes et n'aura donc pas besoin d'être testée. D'autre part, la projection sur la droite D_3 montre que ρ_1 et ρ_4 appartiennent à l'enveloppe convexe de Λ.

Cette approche peut être étendue à des dimensions $L > 2$. Dans ce cas, les points de l'ensemble Λ sont projetés sur un hyperplan arbitraire de dimension $L - 1$.

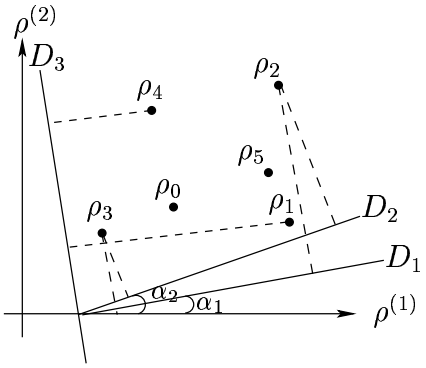


FIG. 3.7 – Echantillonage aléatoire

3.4.4 Approche par programmation linéaire

Définition 6. Un élément d'un ensemble fini de points est appelé *point extrême* s'il n'est pas combinaison convexe des autres points de l'ensemble.

Le problème de trouver l'enveloppe convexe d'un ensemble de points peut se ramener à un problème de programmation linéaire [Pardalos et al., 1995]. Par définition, un point extrême de Λ n'est pas combinaison convexe des autres points de Λ. On peut alors considérer le programme linéaire suivant :

$$\begin{aligned} &\min \quad z_j \\ &\text{sous les contraintes : } \sum_{i=0}^{K-1} z_i \rho_i = \rho_j, \quad \sum_{i=0}^{K-1} z_i = 1, \quad z_i \geq 0, \quad i = 0, \ldots, K-1 \end{aligned} \tag{3.38}$$

Le théorème suivant, énoncé dans [Pardalos et al., 1995], donne une condition nécessaire et suffisante pour que le point ρ_j soit un point extrême de Λ.

Théorème 9. La solution du programme linéaire (3.38) est positive si et seulement si ρ_j est un point extrême de Λ.

Si ρ_j est un point extrême de Λ, il n'est pas combinaison convexe des autres points de Λ et 1 est l'unique solution optimale de (3.38). Si, au contraire, ρ_j n'est pas un point extrême de Λ, il est combinaison convexe des autres points de Λ et 0 est toujours une solution optimale de (3.38). Dans ce cas, ρ_j est retiré de l'ensemble Λ et la procédure est réitérée jusqu'à avoir parcouru tous les points de Λ.
Cette approche peut facilement être étendue à des dimensions $L > 2$.

3.4.5 Conclusion

Grâce aux approches précédentes, on peut trouver les sommets ρ_{o_i} du polytope minimal $\mathcal{D}_\rho^*$. On rappelle que le paramètre variant ρ_k du système chaotique peut s'écrire sous forme LPV polytopique :

$$\rho_k = \sum_{i=1}^{N} \xi_k^{(i)} \rho_{o_i} \tag{3.39}$$

Ce paramètre ρ_k étant fonction de l'état x_k, il est accessible à chaque instant (cf. Proposition 1). Connaissant ρ_k et ρ_{o_i}, $i = 1, \ldots, N$, il faut déterminer le vecteur ξ_k à chaque instant, ce qui fait l'objet de la section suivante.

3.5 Décomposition polytopique

Le problème revient à chercher la matrice W_k telle que, à chaque instant :

$$U_k = ZW_k \tag{3.40}$$

sous la contrainte :

$$\xi_k^{(i)} \geq 0, \quad i = 1, \ldots, N \tag{3.41}$$

avec :

$$U_k = \begin{bmatrix} \rho_k^{(1)} \\ \vdots \\ \rho_k^{(L)} \\ 1 \end{bmatrix}, \quad Z = \begin{bmatrix} \rho_{o_1}^{(1)} & \ldots & \rho_{o_i}^{(1)} & \ldots & \rho_{o_N}^{(1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \rho_{o_1}^{(L)} & \ldots & \rho_i^{(L)} & \ldots & \rho_{o_N}^{(L)} \\ 1 & \ldots & 1 & \ldots & 1 \end{bmatrix}, \quad W_k = \begin{bmatrix} \xi_k^{(1)} \\ \vdots \\ \xi_k^{(i)} \\ \vdots \\ \xi_k^{(N)} \end{bmatrix} \tag{3.42}$$

Les composantes relatives à la dernière ligne des matrices correspondent à la contrainte $\sum_{i=1}^{N} \xi_k^{(i)} = 1$.
Les quantités $\rho_k^{(j)}$ représentent les composantes du vecteur ρ_k. Les quantités $\rho_{o_i}^{(j)}$ sont les composantes des sommets ρ_{o_i} du polytope minimal $\mathcal{D}_\rho^*$. N est le nombre de sommets du polytope. A chaque instant, le vecteur U_k, de dimension $(L+1)$, est mesuré. La matrice Z, de dimension $(L+1) \times N$, est constante et connue, après recherche des sommets (Section 3.4). Nous devons donc déterminer à chaque instant le vecteur W_k, de dimension N.

La figure 3.8 montre un exemple de polytope convexe minimal à 5 sommets, en dimension 2, qui englobe un ensemble de points donnés. Dans cet exemple, on a :

$$\underbrace{\begin{pmatrix} \rho_k^{(1)} \\ \rho_k^{(2)} \\ 1 \end{pmatrix}}_{U_k} = \underbrace{\begin{pmatrix} \rho_{o_1}^{(1)} & \rho_{o_2}^{(1)} & \rho_{o_3}^{(1)} & \rho_{o_4}^{(1)} & \rho_{o_5}^{(1)} \\ \rho_{o_1}^{(2)} & \rho_{o_2}^{(2)} & \rho_{o_3}^{(2)} & \rho_{o_4}^{(2)} & \rho_{o_5}^{(2)} \\ 1 & 1 & 1 & 1 & 1 \end{pmatrix}}_{Z} \underbrace{\begin{pmatrix} \xi_k^{(1)} \\ \xi_k^{(2)} \\ \xi_k^{(3)} \\ \xi_k^{(4)} \\ \xi_k^{(5)} \end{pmatrix}}_{W_k} \tag{3.43}$$

avec $U_k \in \mathbb{R}^3$, $Z \in \mathbb{R}^{3\times 5}$ et $W_k \in \mathbb{R}^5$.

En toute généralité, le nombre de sommets N et la dimension du polytope L sont quelconques l'un par rapport à l'autre. Cependant, dans la plupart des cas, $N > L+1$, signifiant qu'il y a plus d'inconnues (N) que d'équations $(L+1)$. Pour calculer W_k à chaque instant, on peut utiliser la pseudo-inverse de Z. Le problème est que, le nombre de sommets N pouvant être élevé, la

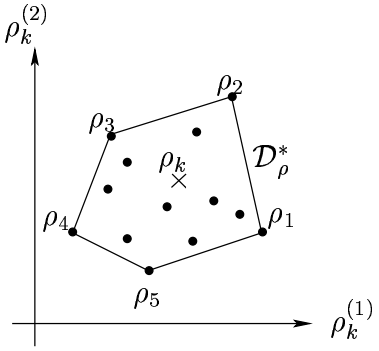


FIG. 3.8 – Exemple de polytope convexe minimal à 5 sommets

matrice Z de dimension $(L+1) \times N$ peut être très importante. Une solution pour la réduire, présentée ci-dessous dans le cas où la dimension $L = 2$, est basée sur la combinaison linéaire de 3 sommets du polytope minimal $\mathcal{D}_\rho^*$.

Tout point ρ_k contenu *strictement* à l'intérieur du polytope convexe minimal est situé à l'intérieur d'un triangle formé par trois des sommets du polytope, notés $\bar{\rho}_{o_p}$, $\bar{\rho}_{o_q}$ et $\bar{\rho}_{o_r}$. Par conséquent, ρ_k peut s'écrire comme la combinaison linéaire de ces trois sommets et ξ_k est solution de :

$$\underline{U}_k = \underline{Z}\underline{W}_k \tag{3.44}$$

avec :

$$\underline{U}_k = \begin{bmatrix} \rho_k^{(1)} \\ \rho_k^{(2)} \\ 1 \end{bmatrix}, \quad \underline{Z} = \begin{bmatrix} \bar{\rho}_{o_p}^{(1)} & \bar{\rho}_{o_q}^{(1)} & \bar{\rho}_{o_r}^{(1)} \\ \bar{\rho}_{o_p}^{(2)} & \bar{\rho}_{o_q}^{(2)} & \bar{\rho}_{o_r}^{(2)} \\ 1 & 1 & 1 \end{bmatrix}, \quad \underline{W}_k = \begin{bmatrix} \xi_k^{(p)} \\ \xi_k^{(q)} \\ \xi_k^{(r)} \end{bmatrix} \tag{3.45}$$

Cette solution donne à chaque instant trois des $\xi_k^{(i)}$ de (3.39), $i = 1, \ldots, N$, qui sont strictement positifs, car le point ρ_k est situé à l'intérieur du triangle et est donc combinaison convexe des sommets du triangle. Les $(N-3)$ autres $\xi_k^{(i)}$ sont nuls.
D'autre part, si le point ρ_k n'est pas situé strictement à l'intérieur du polytope mais est un sommet, tous les $\xi_k^{(i)}$ seront nuls sauf un.

Pour trouver les points $\bar{\rho}_{o_p}$, $\bar{\rho}_{o_q}$ et $\bar{\rho}_{o_r}$ qui sont les sommets d'un triangle englobant ρ_k, on peut faire appel à la méthode de Delauney (voir par exemple, [Du, 1996]). Le principe de cette méthode consiste à tester la position du point ρ_k par rapport aux droites orientées $(\bar{\rho}_{o_p}\bar{\rho}_{o_q})$, $(\bar{\rho}_{o_p}\bar{\rho}_{o_r})$ et $(\bar{\rho}_{o_r}\bar{\rho}_{o_q})$, où $\bar{\rho}_{o_p}$, $\bar{\rho}_{o_q}$ et $\bar{\rho}_{o_r}$ sont des sommets de l'enveloppe convexe. Pour cela, on choisit arbitrairement trois points $\bar{\rho}_{o_p}$, $\bar{\rho}_{o_q}$ et $\bar{\rho}_{o_r}$, sommets de l'enveloppe convexe. Pour tester si ρ_k est à l'intérieur du triangle $\bar{\rho}_{o_p}\bar{\rho}_{o_q}\bar{\rho}_{o_r}$, il suffit de calculer :

$$Q_1 = (\bar{\rho}_{o_q}^{(1)} - \bar{\rho}_{o_p}^{(1)})(\rho_k^{(2)} - \bar{\rho}_{o_p}^{(2)}) - (\rho_k^{(1)} - \bar{\rho}_{o_p}^{(1)})(\bar{\rho}_{o_q}^{(2)} - \bar{\rho}_{o_p}^{(2)}) \tag{3.46}$$

$$Q_2 = (\bar{\rho}_{o_r}^{(1)} - \bar{\rho}_{o_p}^{(1)})(\rho_k^{(2)} - \bar{\rho}_{o_p}^{(2)}) - (\rho_k^{(1)} - \bar{\rho}_{o_p}^{(1)})(\bar{\rho}_{o_r}^{(2)} - \bar{\rho}_{o_p}^{(2)}) \tag{3.47}$$

Par convention, si $Q_1 < 0$ (resp. $Q_1 > 0$), ρ_k est situé à droite (resp. à gauche) de la droite orientée $(\bar{\rho}_{o_p}\bar{\rho}_{o_q})$. De même, si $Q_2 < 0$ (resp. $Q_2 > 0$), ρ_k est situé à droite (resp. à gauche) de la droite orientée $(\bar{\rho}_{o_p}\bar{\rho}_{o_r})$.

Si $Q_1 < 0$ et $Q_2 > 0$, alors ρ_k est situé à l'intérieur du triangle $\bar{\rho}_{o_p}\bar{\rho}_{o_q}\bar{\rho}_{o_r}$.

La figure 3.9 illustre la méthode de Delauney. Dans cet exemple, on a :

$$Q_1 = (\bar{\rho}_{o_3}^{(1)} - \bar{\rho}_{o_5}^{(1)})(\rho_k^{(2)} - \bar{\rho}_{o_5}^{(2)}) - (\rho_k^{(1)} - \bar{\rho}_{o_5}^{(1)})(\bar{\rho}_{o_3}^{(2)} - \bar{\rho}_{o_5}^{(2)}) \tag{3.48}$$

et

$$Q_2 = (\bar{\rho}_{o_3}^{(1)} - \bar{\rho}_{o_1}^{(1)})(\rho_k^{(2)} - \bar{\rho}_{o_1}^{(2)}) - (\rho_k^{(1)} - \bar{\rho}_{o_1}^{(1)})(\bar{\rho}_{o_3}^{(2)} - \bar{\rho}_{o_1}^{(2)}) \tag{3.49}$$

$Q_1 < 0$, signifiant que ρ_k est à droite de $(\bar{\rho}_{o_3}\bar{\rho}_{o_5})$. De plus, $Q_2 > 0$, signifiant que ρ_k est aussi à gauche de $(\bar{\rho}_{o_3}\bar{\rho}_{o_1})$. Par conséquent, ρ_k est situé à l'intérieur du triangle $\bar{\rho}_{o_1}\bar{\rho}_{o_3}\bar{\rho}_{o_5}$. Par ailleurs, on a :

$$Q_3 = (\bar{\rho}_{o_3}^{(1)} - \bar{\rho}_{o_4}^{(1)})(\rho_k^{(2)} - \bar{\rho}_{o_4}^{(2)}) - (\rho_k^{(1)} - \bar{\rho}_{o_4}^{(1)})(\bar{\rho}_{o_3}^{(2)} - \bar{\rho}_{o_4}^{(2)}) \tag{3.50}$$

$Q_3 > 0$, signifiant que ρ_k est aussi à gauche de $(\bar{\rho}_{o_3}\bar{\rho}_{o_4})$. Par conséquent, le triangle $\bar{\rho}_{o_3}\bar{\rho}_{o_4}\bar{\rho}_{o_5}$ n'englobe pas ρ_k.

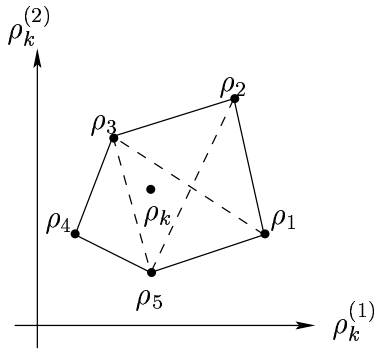


FIG. 3.9 – Localisation par la méthode de Delauney

L'approche précédente pour calculer la matrice Z peut être étendue à des dimensions $L > 2$. Le principe reste le même. En dimension L, tout point ρ_k sera combinaison linéaire de $(L+1)$ sommets du polytope convexe minimal dans le cas où ρ_k n'est pas un sommet. On cherche donc un polygone à $(L+1)$ sommets qui englobe strictement le point ρ_k. Pour cela, on parcourt l'ensemble des sommets du polytope et on calcule les $\xi_k^{(i)}$ avec ces $(L+1)$ sommets. On aura à chaque instant, un nombre L de $\xi_k^{(i)}$ strictement positifs (ou un $\xi_k^{(i)}$ strictement positif si ρ_k est un sommet du polytope) et un nombre $(N-L)$ de $\xi_k^{(i)} = 0$ (ou $(N-1)$ des $\xi_k^{(i)} = 0$ si ρ_k est un sommet du polytope). Par exemple, en dimension 3, on cherche à englober le point ρ_k dans un tétraèdre à 4 sommets. La méthode de Delauney peut également être étendue à des dimensions supérieures à 2.

3.6 Récapitulatif

L'approche pour synthétiser un observateur polytopique peut se résumer en deux étapes, l'une effectuée hors ligne et l'autre effectuée en temps réel.

Etape hors ligne

– Simulation du système (3.21) et constitution de la liste Λ.

- Recherche des sommets ρ_{o_i} du polytope minimal $\mathcal{D}_\rho^*$ englobant Ω_ρ par l'une des approches présentées dans la Section 3.4.

- Détermination des matrices sommets $A^{(i)}$ du polytope $\mathcal{D}_\mathcal{A}$ par (3.29).

- Calcul des gains L_i (résolution des LMI (3.34)).

Etape en temps réel

- Calcul du vecteur ξ_k par (3.40) ou par (3.44).

- Calcul du gain $\mathcal{L}$ par (3.32).

- Calcul du vecteur $\hat{x}_k$ par (3.30).

Dans la section suivante, un exemple illustre cette approche de synthèse d'observateur polytopique dans un contexte de modulation chaotique.

3.7 Application à la modulation chaotique

Dans un schéma de modulation chaotique, considérons l'émetteur suivant, composé par les deux systèmes :

$$\Sigma^1 \begin{cases} x_{k+1}^{(1,1)} = -x_k^{(2,1)} + \alpha_1(-0.78x_k^{(1,1)} - 0.28(x_k^{(1,1)})^2 + 0.98(x_k^{(1,1)})^2(1-(x_k^{(1,1)})^2)x_k^{(2,1)}) \\ x_{k+1}^{(2,1)} = (1+0.12\alpha_1)x_k^{(1,1)} \\ y_k^1 \quad = x_k^{(1,1)} \end{cases} \tag{3.51}$$

$$\Sigma^2 \begin{cases} x_{k+1}^{(1,2)} = -x_k^{(2,2)} + \alpha_2(-0.78x_k^{(1,2)} - 0.28(x_k^{(1,2)})^2 + 0.98(x_k^{(1,2)})^2 x_k^{(2,2)}) \\ x_{k+1}^{(2,2)} = (1+0.12\alpha_2)x_k^{(1,2)} \\ y_k^2 \quad = x_k^{(1,2)} \end{cases} \tag{3.52}$$

avec $\alpha_1 = 1.057$, $\alpha_2 = 0.9$ et $x_k^1 = [x_k^{(1,1)} \quad x_k^{(2,1)}]^T$ (resp. $x_k^2 = [x_k^{(1,2)} \quad x_k^{(2,2)}]^T$) représentant le vecteur d'état du système Σ^1 (resp. Σ^2). L'information m_k peut prendre deux valeurs m_1 et m_2. Selon sa valeur courante, la sortie y_k^1 du système Σ^1 ou celle y_k^2 du système Σ^2 est commutée. Ce schéma de modulation chaotique est représenté sur la figure 3.10.

1. Etape hors ligne

1.1 Simulation des systèmes Σ^1 et Σ^2 et constitutions des listes Λ^1 et Λ^2

On cherche une fonction $\Psi^1 = [\Psi_1^1 \quad \Psi_2^1]^T$ telle que $\rho_k^1 = \Psi_1(x_k^1)$ et la matrice $\mathcal{A}^1$, vérifiant

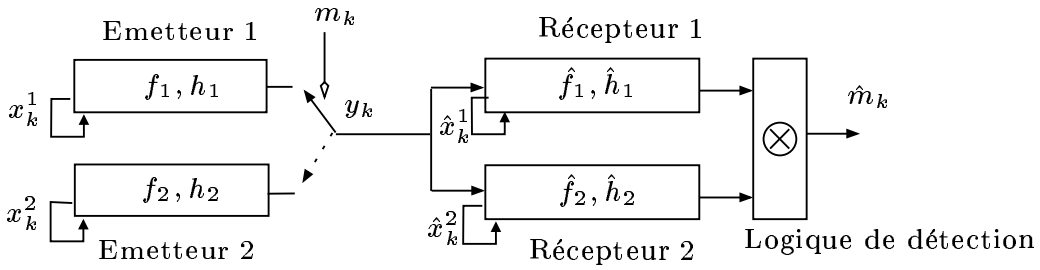


FIG. 3.10 – Modulation chaotique

$\mathcal{A}^1(\rho_k^1) = \mathcal{A}^1(\Psi^1(x_k^1))$, soit de classe C^1 par rapport à ρ_k^1. On propose $\Psi_1^1(\rho_k^1) = \rho_k^{(1,1)} = \alpha_1(-0.78 - 0.28x_k^{(1,1)})$ et $\Psi_2^1(\rho_k^1) = \rho_k^{(2,1)} = -1 + 0.98\alpha_1(x_k^{(1,1)})^2(1 - (x_k^{(1,1)})^2)$. Le système (3.51) admet alors la forme convexe (3.21), avec :

$$\mathcal{A}^1(\rho_k^1) = \begin{bmatrix} \rho_k^{(1,1)} & \rho_k^{(2,1)} \\ 1 + 0.12\alpha_1 & 0 \end{bmatrix}, \quad \rho_k^1 = \begin{bmatrix} \alpha_1(-0.78 - 0.28x_k^{(1,1)}) \\ -1 + 0.98\alpha_1(x_k^{(1,1)})^2(1 - (x_k^{(1,1)})^2) \end{bmatrix} \tag{3.53}$$

La liste Λ^1 contient les points ρ_k^1 simulés.

Par ailleurs, on cherche une fonction $\Psi^2 = [\Psi_1^2 \quad \Psi_2^2]^T$ telle que $\rho_k^2 = \Psi^2(x_k^2)$ et la matrice $\mathcal{A}^2$, vérifiant $\mathcal{A}^2(\rho_k^2) = \mathcal{A}^2(\Psi^2(x_k^2))$, soit de classe C^1 par rapport à ρ_k^2. On propose $\Psi_1^2(\rho_k^2) = \rho_k^{(1,2)} = \alpha_2(-0.78 - 0.28x_k^{(1,2)})$ et $\Psi_2^2(\rho_k^2) = \rho_k^{(2,2)} = -1 + 0.98\alpha_2(x_k^{(1,2)})^2$. Le système (3.52) admet la forme convexe (3.21), avec :

$$\mathcal{A}^2(\rho_k^2) = \begin{bmatrix} \rho_k^{(1,2)} & \rho_k^{(2,2)} \\ 1 + 0.12\alpha_2 & 0 \end{bmatrix}, \quad \rho_k^2 = \begin{bmatrix} \alpha_2(-0.78 - 0.28x_k^{(1,2)}) \\ -1 + 0.98\alpha_2(x_k^{(1,2)})^2 \end{bmatrix} \tag{3.54}$$

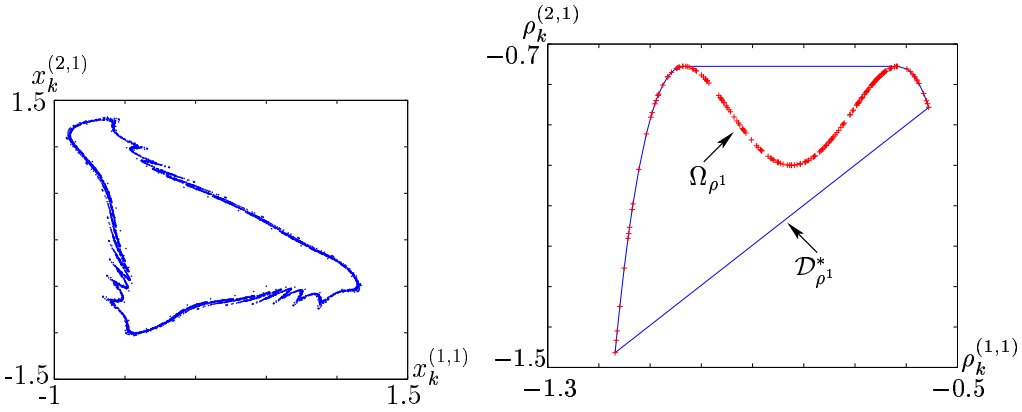
La liste Λ^2 contient les points ρ_k^2 simulés.

1.2 Recherche des sommets $\rho_{o_i}^1$ du polytope minimal $\mathcal{D}_{\rho^1}^*$ et des sommets $\rho_{o_i}^2$ du polytope minimal $\mathcal{D}_{\rho^2}^*$

Comme le système (3.51) est chaotique, x_k^1 réside dans un attracteur chaotique Ω^1, représenté sur la figure 3.11(a). Comme ρ_k^1 dépend de x_k^1, il évolue dans un ensemble compact Ω_{ρ^1}, qui est l'image de Ω^1 par Ψ^1. La recherche du polytope minimal $\mathcal{D}_{\rho^1}^*$ englobant Ω_{ρ^1} est effectuée avec l'algorithme appelé Quick Hull. La figure 3.11(b) représente le polytope minimal $\mathcal{D}_{\rho^1}^*$ englobant ρ_k^1. L'algorithme renvoie $N = 42$ sommets.
De même, le système (3.52) étant chaotique, x_k^2 réside dans un attracteur chaotique Ω^2, représenté sur la figure 3.12(a). Comme ρ_k^2 dépend de x_k^2, il évolue dans un ensemble compact Ω_{ρ^2}, qui est l'image de Ω^2 par Ψ^2. La recherche du polytope minimal $\mathcal{D}_{\rho^2}^*$ englobant ρ_k^2 est effectuée avec l'algorithme Quick Hull. La figure 3.12(b) représente le polytope minimal $\mathcal{D}_{\rho^2}^*$ englobant Ω_{ρ^2}. L'algorithme renvoie $N = 199$ sommets.

1.3 Détermination des matrices sommets $A^{(i,1)}$ et $A^{(i,2)}$

Les matrices sommets $A^{(i,1)}$ et $A^{(i,2)}$ sont calculées conformément à (3.29), avec :



(a) Attracteur chaotique Ω^1 (b) Polytope minimal $\mathcal{D}^*_{\rho^1}$ englobant Ω_{ρ^1}

FIG. 3.11 – Décomposition polytopique pour le système Σ^1

$$\mathcal{A}_0^1 = \begin{bmatrix} 0 & 0 \\ 1+0.12\alpha_1 & 0 \end{bmatrix}, \quad \mathcal{A}_0^2 = \begin{bmatrix} 0 & 0 \\ 1+0.12\alpha_2 & 0 \end{bmatrix},$$
$$A^{I_{1,1}} = A^{I_{1,2}} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad A^{I_{2,1}} = A^{I_{2,2}} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \tag{3.55}$$

1.4 Calcul des gains L_i^1 et L_i^2

Le récepteur est composé de deux observateurs polytopiques (schéma 3.1) correspondant respectivement aux systèmes (3.51) et (3.52) et de la forme (3.30).
Pour chaque observateur, les LMI (3.34) sont résolues avec les matrices $A^{(i,1)}$ et $A^{(i,2)}$, respectivement. Ces LMI sont faisables et les gains respectifs $L_i^1 = (G_i^1)^{-1}F_i^1$ et $L_i^2 = (G_i^2)^{-1}F_i^2$ sont dérivés de leurs solutions.

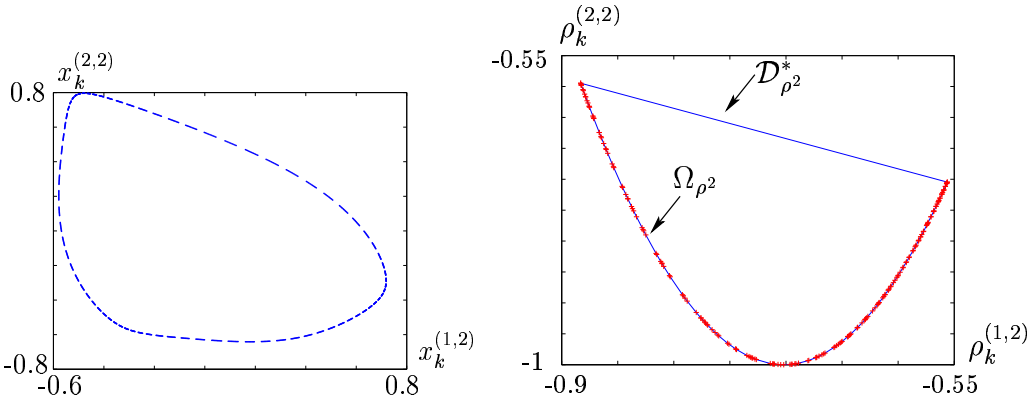
2. Etape en temps réel

2.1 Calcul des vecteurs ξ_k^1 et ξ_k^2

Les vecteurs ξ_k^1 et ξ_k^2 respectivement pour les systèmes Σ^1 et Σ^2 sont calculés à chaque instant par (3.40) ou par (3.44).

2.2 Calcul des gains $\mathcal{L}_1$ et $\mathcal{L}_2$

Les gains polytopiques $\mathcal{L}_1$ et $\mathcal{L}_2$ sont donnés par (3.32) avec les gains L_i^1 et L_i^2 et les vecteurs ξ_k^1 et ξ_k^2, calculés précédemment.



(a) Attracteur chaotique Ω^2 (b) Polytope minimal $\mathcal{D}^*_{\rho^2}$ englobant Ω_{ρ^2}

FIG. 3.12 – Décomposition polytopique pour le système Σ^2

2.3 Calcul des vecteurs $\hat{x}_k^1$ et $\hat{x}_k^2$

La reconstruction du vecteur d'état $\hat{x}_k^1$ est donnée par :

$$\begin{cases} \hat{x}_{k+1}^1 = \mathcal{A}^1(\rho_k^1)\hat{x}_k^1 + \mathcal{L}^1(\rho_k)(y_k^1 - \hat{y}_k^1) \\ \hat{y}_k^1 \quad = \hat{x}_k^{(1,1)} \end{cases} \tag{3.56}$$

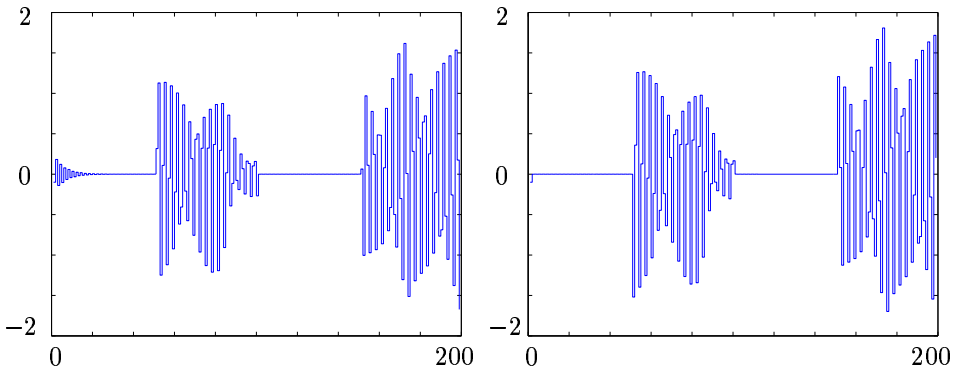
La reconstruction du vecteur d'état $\hat{x}_k^2$ est donnée par :

$$\begin{cases} \hat{x}_{k+1}^2 = \mathcal{A}^2(\rho_k^2)\hat{x}_k^2 + \mathcal{L}^2(\rho_k)(y_k^2 - \hat{y}_k^2) \\ \hat{y}_k^2 \quad = \hat{x}_k^{(1,2)} \end{cases} \tag{3.57}$$

Les figures 3.13(a) et 3.13(b) représentent la convergence des erreurs de reconstruction d'état $x_k^{(1,1)} - \hat{x}_k^{(1,1)}$ et $x_k^{(2,1)} - \hat{x}_k^{(2,1)}$, respectivement, pour le système Σ^1.
Les figures 3.14(a) et 3.14(b) représentent la convergence des erreurs de reconstruction d'état $x_k^{(1,2)} - \hat{x}_k^{(1,2)}$ et $x_k^{(2,2)} - \hat{x}_k^{(2,2)}$, respectivement, pour le système Σ^2.
Pour reconstruire l'information m_k, une logique de détection est utilisée en analysant les erreurs de reconstruction associées à chaque récepteur. Dans cet exemple, quatre changements de valeurs de l'information sont détectés et l'information reconstruite $\hat{m}_k$ est représentée sur la figure 3.15.

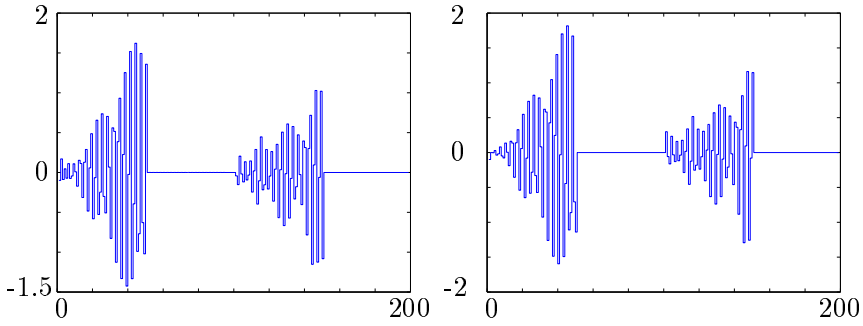
3.8 Conclusion

Les résultats de ce chapitre constituent une base essentielle pour la synthèse d'observateur adaptatif dans le cadre de la modulation paramétrique. Le chapitre suivant est dédié à un mode de récupération des paramètres pour le schéma de la modulation paramétrique. La récupération des paramètres est basée sur l'estimation simultanée état/paramètre et un observateur polytopique adaptatif peut jouer le rôle de récepteur.



(a) $x_k^{(1,1)} - \hat{x}_k^{(1,1)}$ (b) $x_k^{(2,1)} - \hat{x}_k^{(2,1)}$

FIG. 3.13 – Erreur de reconstruction du vecteur d'état x_k^1 du système Σ^1



(a) $x_k^{(1,2)} - \hat{x}_k^{(1,2)}$ (b) $x_k^{(2,2)} - \hat{x}_k^{(2,2)}$

FIG. 3.14 – Erreur de reconstruction du vecteur d'état x_k^2 du système Σ^2

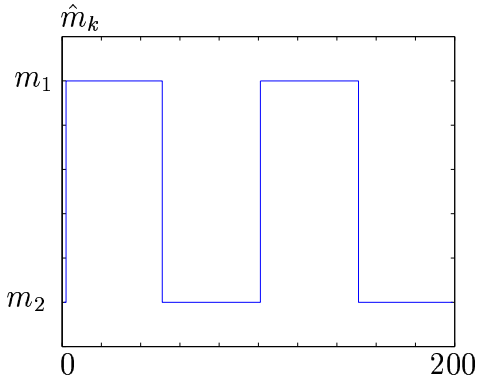


FIG. 3.15 – Information reconstruite $\hat{m}_k$

Chapitre 4

Estimation simultanée état/paramètre pour la modulation paramétrique

4.1 Introduction

Dans ce chapitre, nous nous intéressons à la modulation paramétrique, présentée dans le Chapitre 2. On rappelle que, dans ce schéma, côté émetteur, les paramètres d'une récurrence chaotique sont modulés par une information à masquer.

$$\begin{cases} x_{k+1} = f(x_k, \theta_k) \\ y_k \quad\;\; = h(x_k) \end{cases} \tag{4.1}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}^p$ le vecteur de sortie et $\theta_k \in \mathbb{R}^l$ le vecteur des paramètres modulés.
Ce schéma est rappelé sur la figure 4.1. Toute la problématique se situe, côté récepteur, dans la

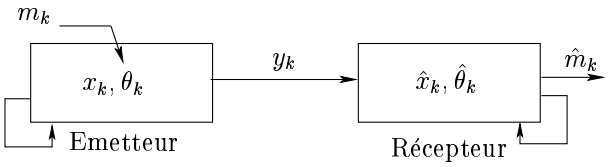


FIG. 4.1 – Modulation paramétrique

récupération des paramètres modulés. En effet, l'émetteur et le récepteur doivent se synchroniser. Ce problème de synchronisation peut être formulé comme un problème d'estimation simultanée état/paramètre, résolu par un observateur adaptatif. On considère le vecteur d'état étendu, qui inclut le vecteur d'état et le vecteur des paramètres.
De nombreux observateurs adaptatifs ont été proposés dans la littérature, pour les systèmes à temps continu. En revanche, très peu de travaux portent sur la synthèse d'observateurs adaptatifs pour les systèmes à temps discret. Nous proposons un observateur adaptatif particulier, appelé polytopique [Millérioux et al., 2005]. Les résultats du Chapitre 3 peuvent alors être appliqués sur le système étendu.
On rappelle qu'une particularité des systèmes chaotiques est que le vecteur d'état est borné et évolue dans un ensemble compact invariant de l'espace de phase, bien défini par l'attracteur chaotique associé. Contrairement à la plupart des observateurs, les observateurs polytopiques

ont la particularité de prendre en compte cette spécificité liée au chaos.

Dans la Section 4.2, quelques structures d'observateurs adaptatifs existant dans la littérature sont rappelées. Dans la Section 4.3, nous présentons un observateur adaptatif polytopique. Dans la Section 4.4, un exemple de reconstruction simultanée état/paramètre avec cette approche est donné dans un contexte de modulation paramétrique.

4.2 Observateurs adaptatifs

On considère des systèmes non linéaires de la forme (4.1).
Un observateur adaptatif permet d'estimer conjointement le vecteur d'état x_k et le vecteur des paramètres θ_k d'un système (4.1). Dans certains cas, ces paramètres sont constants ou varient suffisament lentement pour être considérés constants. Dans ce cas, ils sont notés θ. Dans d'autres cas, ces paramètres varient dans le temps. Ils sont alors notés $\theta(t)$ en temps continu ou θ_k en temps discret.

4.2.1 Systèmes linéaires

La synthèse d'observateurs adaptatifs est étudiée depuis les années 70 pour des systèmes linéaires invariants dans le temps. Une méthode de synthèse d'observateur adaptatif a été proposée pour des systèmes à temps continu dans [Luders and Narendra, 1974] [Kreisselmeier, 1977], qui sont les premières références sur le sujet. Cette méthode requiert une transformation de la dynamique du système afin de mettre le système considéré sous une forme faisant apparaître les paramètres de façon simplifiée via un changement linéaire de coordonnées $z(t) = Tx(t)$:

$$\begin{cases} \dot{z}(t) = A_o z(t) + \psi(y(t))\theta \\ y(t) = C_o z(t) \end{cases} \tag{4.2}$$

avec $z(t) \in \mathbb{R}^n$, $y(t) \in \mathbb{R}$, $\theta \in \mathbb{R}^l$. La fonction ψ est bornée et connue à chaque instant. Les matrices A_o et C_o sont sous forme canonique observable, respectivement :

$$A_o = \begin{bmatrix} -a_{n-1} & 1 & 0 & \dots & 0 \\ -a_{n-2} & 0 & 1 & \dots & 0 \\ \vdots & 0 & 0 & \ddots & 0 \\ -a_1 & 0 & 0 & \ddots & 1 \\ -a_0 & 0 & 0 & \dots & 0 \end{bmatrix}, \quad C_o = \begin{bmatrix} 1 & 0 & \dots & 0 \end{bmatrix} \tag{4.3}$$

Les termes a_i, $a_i \in \mathbb{R}$, représentent les coefficients du polynôme caractéristique $\Psi(\lambda)$ défini par $\Psi(\lambda) = \det(\lambda \mathbf{1}_n - A_o) = \lambda^n + a_{n-1}\lambda^{n-1} + \ldots + a_1\lambda + a_0$.
L'observateur adaptatif correspondant s'écrit :

$$\begin{cases} \dot{\hat{z}}(t) = A_o \hat{z}(t) + \psi(y(t))\hat{\theta}(t) + K(y(t) - \hat{y}(t)) \\ \hat{y}(t) = C_o \hat{z}(t) \\ \dot{\hat{\theta}}(t) = \Gamma \psi(y(t))(y(t) - \hat{y}(t)) \\ \hat{x}(t) = T^{-1}(\hat{z}(t)) \end{cases} \tag{4.4}$$

La loi d'adaptation des paramètres fait intervenir l'erreur de sortie $y(t) - \hat{y}(t)$. K est le gain de l'observateur et Γ est le gain d'adaptation choisi arbitrairement. L'erreur de reconstruction

d'état $\epsilon_z(t)$, définie par $\epsilon_z(t) = z(t) - \hat{z}(t)$, est obtenue en soustrayant (4.4) à (4.2) :

$$\dot{\epsilon}_z(t) = (A_o - KC_o)\epsilon_z(t) + \psi(y(t))(\theta - \hat{\theta}(t)) \tag{4.5}$$

Le gain K est calculé de telle sorte que la matrice $(A_o - KC_o)$ soit Hurwitz[1]. Il est montré que si la condition d'excitation persistante

$$\exists T_1 > 0, \exists \alpha > 0, \quad \int_t^{t+T_1} \psi(y(\tau))\psi(y(\tau))^T d\tau \geq \alpha \mathbf{1}_n, \quad \forall t \geq 0 \tag{4.6}$$

est vérifiée, les erreurs de reconstruction $\epsilon_z(t)$ et $\epsilon_\theta(t) = \theta - \hat{\theta}(t)$ convergent à zéro.

Cette méthode a été étendue au cas des systèmes non linéaires [Bastin and Gevers, 1988]. On distingue deux cas, les systèmes non linéaires linéarisables par changement de coordonnées avec injection de la sortie et les systèmes non linéarisables. On traitera le cas des systèmes à temps continu puis celui des systèmes à temps discret.

4.2.2 Systèmes non linéaires linéarisables à temps continu

On considère les systèmes non linéaires de la forme :

$$\begin{cases} \dot{x}(t) = f(x(t)) + \varphi_0(x(t), y(t)) + \sum_{i=1}^{l} \theta^{(i)} \varphi_i(x(t), y(t)) \\ y(t) = h(x(t)) \end{cases} \tag{4.7}$$

avec $x(t) \in \mathbb{R}^n$, $y(t) \in \mathbb{R}$, $\theta = [\theta^{(1)} \dots \theta^{(l)}]^T \in \mathbb{R}^l$, f une fonction non linéaire dépendant de $x(t)$, φ_0 et $\varphi = [\varphi_1 \dots \varphi_l]^T$ deux fonctions non linéaires de $x(t)$ et de $y(t)$.

Cette section est inspirée de [Fradkov et al., 1999] où différentes approches pour la synthèse d'observateur adaptatif sont résumées pour les systèmes non linéaires (4.7) et sont rappelées ci-dessous.

Approche 1

Supposons que le système (4.7) puisse se mettre sous une forme particulière appelée "forme observateur adaptatif" :

$$\begin{cases} \dot{z}(t) = A_o z(t) + \psi_0(y(t)) + B \sum_{i=1}^{l} \theta^{(i)} \phi_i(y(t)) \\ y(t) = C_o z(t) \end{cases} \tag{4.8}$$

où $B = [b_1 \dots b_n]^T \in \mathbb{R}^n$ un vecteur constant tel que $b_1 \neq 0$ et tel que le polynôme $b_1 + b_2\lambda + \dots + b_n\lambda^{n-1}$ a toutes ses racines ayant leur partie réelle négative. La fonction $\phi = [\phi_1 \dots \phi_l]^T$ est continue par morceaux et bornée. Les conditions de transformation de (4.7) en (4.8) peuvent être trouvées dans [Marino and Tomei, 1992].
L'observateur adaptatif correspondant au système (4.8) est :

[1] Voir Annexe A, Définition 33

$$\begin{cases} \dot{\hat{z}}(t) = A_o\hat{z}(t) + \psi_0(y(t)) + B\sum_{i=1}^{l}\hat{\theta}^{(i)}(t)\phi_i(y(t)) + K(y(t) - \hat{y}(t)) \\ \hat{y}(t) = C_o\hat{z}(t) \\ \dot{\hat{\theta}}(t) = \gamma\phi(y(t))(y(t) - \hat{y}(t)) \\ \hat{x}(t) = \mathcal{T}^{-1}(\hat{z}(t)) \end{cases} \tag{4.9}$$

K est le gain de l'observateur et γ est une matrice symétrique définie positive choisie arbitrairement, appelée gain adaptatif. L'erreur de reconstruction d'état $\epsilon_z(t) \triangleq z(t) - \hat{z}(t)$, est obtenue en soustrayant (4.9) à (4.8) :

$$\dot{\epsilon}_z(t) = (A_o - KC_o)\epsilon_z(t) + B\Big(\sum_{i=1}^{l}(\theta^{(i)} - \hat{\theta}^{(i)}(t))\phi_i(y(t))\Big) \tag{4.10}$$

Le gain K est donné par :

$$K = \frac{1}{b_1}(A_oB + \mu B) \tag{4.11}$$

avec $\mu \in \mathbb{R}$, $\mu > 0$, une constante choisie arbitrairement.
Le gain K est choisi de telle sorte que la matrice $(A_o - KC_o)$ soit Hurwitz. Il est montré que si la condition d'excitation persistante

$$\exists T_1 > 0, \alpha > 0, \quad \int_t^{t+T_1}\phi(y(\tau))\phi(y(\tau))^T d\tau \geq \alpha\mathbf{1}_n, \quad \forall t \geq 0 \tag{4.12}$$

est vérifiée, les erreurs de reconstruction $\epsilon_z(t)$, $\epsilon_\theta(t) = \theta - \hat{\theta}(t)$ et $\epsilon(t) = \mathcal{T}^{-1}(z(t)) - \mathcal{T}^{-1}(\hat{z}(t)) = x(t) - \hat{x}(t)$ convergent à zéro.

Approche 2

Par analogie avec le cas linéaire, l'approche de [Marino and Tomei, 1992] consiste à trouver un changement de coordonnées avec injection de la sortie, de la forme $z(t) = \mathcal{T}(x(t))$, où $\mathcal{T}$ est un difféomorphisme[1] indépendant de θ. Ce difféomorphisme permet de transformer le système non linéaire (4.7) en un système de la forme :

$$\begin{cases} \dot{z}(t) = A_oz(t) + \psi_0(y(t)) + \sum_{i=1}^{l}\theta^{(i)}\psi_i(y(t)) \\ y(t) = C_oz(t) \end{cases} \tag{4.13}$$

$\psi = [\psi_1 \dots \psi_l]^T$ est une fonction non linéaire de la sortie $y(t)$. Elle est continue par morceaux et bornée. Les matrices A_o et C_o sont sous forme canonique observable, respectivement :

$$A_o = \begin{bmatrix} 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 0 \end{bmatrix}, \quad C_o = \begin{bmatrix} 1 & 0 & \dots & 0 \end{bmatrix} \tag{4.14}$$

La différence entre les formes canoniques observables (4.3) et (4.14) est que les coefficients a_i n'apparaissent plus dans la matrice A_o car ils apparaissent dans la fonction $\psi_0(y(t))$.

[1] Voir Annexe A, Définition 34

La forme canonique observable (4.13) a la propriété d'être linéaire en les quantités inconnues (états et paramètres) et éventuellement non linéaire en la sortie. La difficulté de la méthode est de prouver l'existence de la transformation $\mathcal{T}$. Une condition nécessaire et suffisante pour transformer le système (4.7) sous la forme (4.13) est donnée dans [Marino, 1990].

Afin de synthétiser un observateur pour ce système, un second changement de coordonnées, faisant intervenir un difféomorphisme qui dépend des paramètres θ, est introduit [Marino and Tomei, 1992] :

$$\eta(t) = z(t) - M(t)\theta \tag{4.15}$$

La matrice $M(t) \in \mathbb{R}^{n\times l}$ a la structure suivante :

$$M(t) = \begin{bmatrix} 0 \\ N(t) \end{bmatrix} \tag{4.16}$$

La matrice $N(t) \in \mathbb{R}^{(n-1)\times l}$ obéit à :

$$\dot{N}(t) = \begin{bmatrix} -b_2 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -b_{n-1} & 0 & 0 & 1 & \\ -b_n & 0 & \dots & 0 & 0 \end{bmatrix} N(t) + \begin{bmatrix} -b_2 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -b_{n-1} & 0 & \dots & 1 & 0 \\ -b_n & 0 & \dots & 0 & 1 \end{bmatrix} \psi(y(t)) \tag{4.17}$$

Le système (4.13) devient, après transformation :

$$\begin{cases} \dot{\eta}(t) = A_o\eta(t) + \psi_0(y(t)) + (A_oM(t) + \psi(y(t)) - \dot{M}(t))\theta \\ y(t) = C_o\eta \end{cases} \tag{4.18}$$

Le système (4.18) est sous "forme observateur adaptatif" (4.8) avec $A_oM(t) + \psi(y(t)) - \dot{M}(t) = B\phi(y(t))$. Comme précédemment, $B = [1 \quad b_2 \dots b_n]^T$ est tel que le polynôme caractéristique $1 + b_2\lambda + \dots + b_n\lambda^{n-1}$ a toutes ses racines ayant leur partie réelle négative. La matrice $M(t)$ vérifie :

$$\dot{M}(t) = (A_o - BC_oA_o)M(t) + (\mathbf{1}_n - BC_o)\psi(y(t)) \tag{4.19}$$

L'équation (4.19) est appelée filtre auxiliaire.
L'observateur correspondant au système (4.18) a une structure similaire à (4.9) :

$$\begin{cases} \dot{\hat{\eta}}(t) = A_o\hat{\eta}(t) + \psi_0(y(t)) + (A_oM(t) + \psi(y(t)) - \dot{M}(t))\hat{\theta}(t) + K(y(t) - \hat{y}(t)) \\ \hat{y}(t) = C_o\hat{\eta}(t) \\ \dot{\hat{\theta}}(t) = \gamma(A_oM(t) + \psi(y(t)) - \dot{M}(t)))(y(t) - \hat{y}(t)) \\ \dot{M}(t) = (A_o - BC_oA_o)M(t) + (\mathbf{1}_n - BC_o)\psi(y(t)) \\ \hat{z}(t) = \hat{\eta}(t) + M(t)\hat{\theta}(t) \end{cases} \tag{4.20}$$

L'erreur de reconstruction d'état $\epsilon_\eta(t) \triangleq \eta(t) - \hat{\eta}(t)$ est obtenue en soustrayant (4.20) à (4.18) :

$$\dot{\epsilon}_\eta(t) = (A_o - KC_o)\epsilon_\eta(t) + (A_oM(t) + \psi(y(t)) - \dot{M}(t))(\theta - \hat{\theta}(t)) \tag{4.21}$$

Le gain K de l'observateur est choisi comme (4.11) pour assurer la stabilité de (4.21). Comme précédemment, il est montré que si la condition d'excitation persistante

$$\exists T_1 > 0, \exists \alpha > 0, \quad \int_t^{t+T_1} (A_oM(\tau) + \psi(y(\tau)) - \dot{M}(\tau))(A_oM(\tau) + \psi(y(\tau)) - \dot{M}(\tau))^T d\tau \geq \alpha\mathbf{1}_n \tag{4.22}$$

est vérifiée, les erreurs de reconstruction $\epsilon_\eta(t)$, $\epsilon_\theta(t) = \theta - \hat{\theta}(t)$, $\epsilon_z(t) = z(t) - \hat{z}(t)$ et $\epsilon(t) = \mathcal{T}^{-1}(z(t)) - \mathcal{T}^{-1}(\hat{z}(t)) = x(t) - \hat{x}(t)$ convergent à zéro.

Une méthode similaire est proposée dans [Bastin and Gevers, 1988] avec une formulation différente. Dans [Marino and Tomei, 1995], des résultats sur la conception d'observateurs adaptatifs à convergence exponentielle avec un taux de décroissance garanti sont présentés.
Dans le cas où les paramètres varient dans le temps et où la dynamique est soumise à des perturbations bornées, une approche est proposée dans [Marino et al., 2001]. Dans ce cas, le système (4.18) devient :

$$\begin{cases} \dot{\eta}(t) = A_o\eta(t) + \psi_0(y(t)) + C_o(A_oM(t) + \psi(y(t)))\theta(t) + \Psi_e(t)w_e(t) \\ y(t) = C_o\eta(t) \end{cases} \tag{4.23}$$

où $\Psi_e(t) = [\Psi(y(t)) \quad -M(t)]^T$, $w_e = [w(t)^T \quad \dot{\theta}(t)^T]^T$ et $w(t) \in \mathbb{R}^n$ représente des perturbations bornées. L'observateur (4.20) peut alors être synthétisé pour le système (4.23) et les résultats précédents restent valables.

Approche 3

Dans [Fradkov and Markov, 1997] [Fradkov et al., 2000], une approche est proposée pour les systèmes de la forme (4.8).
L'observateur est synthétisé dans le but d'assurer la convergence à zéro des erreurs de reconstruction de l'état et des paramètres. L'observateur proposé a la forme :

$$\begin{cases} \dot{\hat{z}}(t) = A\hat{z}(t) + \psi_0(y(t)) + B\Big(\sum_{i=1}^{l} \hat{\theta}^{(i)}(t)\phi_i(y(t)) + \hat{\theta}_0(t)K(y(t) - \hat{y}(t))\Big) \\ \hat{y}(t) = C\hat{z}(t) \\ \dot{\hat{\theta}}(t) = -\Gamma\phi(y(t))(y(t) - \hat{y}(t)) \\ \dot{\hat{\theta}}_0(t) = -\Gamma_0(y(t) - y(t))^2 \end{cases} \tag{4.24}$$

Les algorithmes d'adaptation de $\hat{\theta}$ et $\hat{\theta}_0$ sont déterminés par des techniques de "speed-gradient" [Fradkov and Markov, 1997]. K représente le gain de l'observateur. Γ et Γ_0 sont les gains d'adaptation.
L'erreur de reconstruction d'état $\epsilon(t) \triangleq z(t) - \hat{z}(t)$ obéit à :

$$\dot{\epsilon}(t) = A\epsilon(t) + B\sum_{i=1}^{l} \theta^{(i)}\phi_i(y(t)) - B\hat{\theta}_0K(y(t) - \hat{y}(t)) \tag{4.25}$$

Le gain K est choisi de telle sorte que le système linéaire ayant pour fonction de transfert $W(\lambda) = KC(\lambda\mathbf{1}_n - A)^{-1}B$ est hyper-minimum phase[1].
Basée sur le Lemme de Kalman-Yakubovich, une condition nécessaire et suffisante pour qu'un système soit hyper-minimum phase est la suivante :

Lemme 1. [Fradkov and Markov, 1997] Considérons des matrices $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times l}$, $K \in \mathbb{R}^{l\times p}$, $C \in \mathbb{R}^{p\times n}$ et supposons que $\text{rang}(B) = l$. Il existe une matrice $P \in \mathbb{R}^{n\times n}$ symétrique définie positive et une matrice $Q \in \mathbb{R}^{l\times p}$, telles que :

$$P\bar{A} + \bar{A}^TP < 0, \quad PB = C^TK^T, \quad \bar{A} = A + BQC \tag{4.26}$$

[1] Voir Annexe A, Définition 36

si et seulement si le système

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = KCx(t) \end{cases} \tag{4.27}$$

est hyper minimum phase.

Pour assurer la convergence de $\hat{\theta}$ vers la vraie valeur θ, la fonction φ doit vérifier la condition de persistance d'excitation :

$$\exists T_1 > 0, \exists \alpha > 0, \quad \int_t^{t+T_1} \varphi(y(\tau))\varphi(y(\tau))^T d\tau \geq \alpha \mathbf{1}_n, \quad \forall t \geq 0 \tag{4.28}$$

Ces résultats ne concernent qu'une classe de systèmes non linéaires qui peuvent être linéarisés par changement de coordonnées avec injection de la sortie. Pour les systèmes non linéaires non linéarisables, d'autres techniques sont proposées et font l'objet du paragraphe ci-dessous.

4.2.3 Systèmes non linéaires non linéarisables à temps continu

1ère classe de systèmes

On considère les systèmes non linéaires de la forme :

$$\begin{cases} \dot{x}(t) = A(t)x(t) + \varphi_0(y(t)) + \psi(y(t))\theta \\ y(t) = C(t)x(t) \end{cases} \tag{4.29}$$

où $x(t) \in \mathbb{R}^n$, $y(t) \in \mathbb{R}$ et $\theta \in \mathbb{R}^l$. Les matrices $A(t)$ et $C(t)$ varient dans le temps et sont connues à chaque instant. La fonction ψ est bornée.

Dans [Zhang and Xu, 2001], l'observateur adaptatif correspondant au système (4.29) a la forme :

$$\begin{cases} \dot{\hat{x}}(t) = A(t)\hat{x}(t) + \varphi_0(y(t)) + \psi(y(t))\hat{\theta}(t) + K(t)(y(t) - \hat{y}(t)) + \gamma(t)\dot{\hat{\theta}}(t) \\ \hat{y}(t) = C(t)\hat{x}(t) \\ \dot{\hat{\theta}}(t) = \Gamma\gamma(t)^T C(t)^T (y(t) - \hat{y}(t)) \\ \dot{\gamma}(t) = (A(t) - K(t)C(t))\gamma(t) + \psi(y(t)) \end{cases} \tag{4.30}$$

La matrice $\gamma(t)$ est générée par un filtrage auxiliaire linéaire du signal $\psi(y(t))$. $\gamma(t)$ joue le même rôle que $M(t)$ dans (4.19). Γ est un gain d'adaptation choisi arbitrairement.
L'erreur de reconstruction d'état $\epsilon(t) \triangleq x(t) - \hat{x}(t)$ obéit à :

$$\dot{\epsilon}(t) = (A(t) - K(t)C(t))\epsilon(t) + \psi(y(t))(\theta - \hat{\theta}(t)) - \gamma(t)\dot{\hat{\theta}}(t) \tag{4.31}$$

Le gain de l'observateur $K(t)$ est choisi de telle sorte que $(A(t) - K(t)C(t))$ soit stable. La convergence à zéro de l'erreur de reconstruction des paramètres est assurée si la fonction ψ vérifie la condition de persistance d'excitation :

$$\exists T_1 > 0, \exists \alpha > 0, \quad \int_t^{t+T_1} \psi(y(\tau))\psi(y(\tau))^T d\tau \geq \alpha \mathbf{1}_n, \quad \forall t \geq 0 \tag{4.32}$$

[Zhang and Xu, 2001] ont montré que quand les paramètres inconnus varient dans le temps et $\dot{\theta}(t)$ est borné, alors l'observateur (4.30) donne une estimation de l'état $\hat{x}(t)$ et des paramètres $\hat{\theta}(t)$ avec une erreur de reconstruction bornée pour l'état et pour les paramètres.

Des algorithmes pour la synthèse d'observateurs adaptatifs ont été proposés par [Cho and Rajamani, 1997], lorsque la matrice $A(t)$ est constante mais que les fonctions φ_0 et ψ dépendent de $x(t)$ avec des non linéarités de type Lipschitz[1].

2ème classe de systèmes

On considère des systèmes non linéaires de la forme [Besancon, 2000] :

$$\begin{cases} \dot{z}(t) = f(z(t), y(t)) \\ \dot{y}(t) = g(z(t), y(t)) + h(z(t), y(t))\theta \\ y(t) = Cx(t) \end{cases} \tag{4.33}$$

avec :

$$x(t) = \begin{bmatrix} z(t) \\ y(t) \end{bmatrix} \tag{4.34}$$

où $y(t) \in \mathbb{R}$ est la sortie et $z(t) \in \mathbb{R}^{n-1}$ représente les composantes du vecteur d'état $x(t)$ non mesurées. f, g et h sont des fonctions non linéaires de $z(t)$ et de $y(t)$.

L'observateur adaptatif proposé est :

$$\begin{cases} \dot{\hat{z}}(t) = f(\hat{z}(t), y(t)) \\ \dot{\hat{y}}(t) = g(\hat{z}(t), y(t)) + h(\hat{z}(t), y(t))\hat{\theta}(t) + K(y(t) - \hat{y}(t)) \\ \dot{\hat{\theta}}(t) = \Gamma h(\hat{z}(t), y(t))(y(t) - \hat{y}(t)) \end{cases} \tag{4.35}$$

Γ est un gain adaptatif et K est le gain de l'observateur. L'erreur de reconstruction d'état $\epsilon(t)$ et celle des paramètres $\epsilon_\theta(t)$ sont définies, respectivement par :

$$\epsilon(t) = \begin{bmatrix} z(t) - \hat{z}(t) \\ y(t) - \hat{y}(t) \end{bmatrix}, \quad \epsilon_\theta(t) = \theta - \hat{\theta}(t) \tag{4.36}$$

La convergence de l'observateur est basée sur une fonction de Lyapunov $V(\epsilon(t), \epsilon_\theta(t))$, vérifiant :

$$V(\epsilon(t), \epsilon_\theta(t)) = V_1(z(t) - \hat{z}(t)) + \alpha V_2(y(t) - \hat{y}(t)) + \alpha V_3(\theta - \hat{\theta}) \tag{4.37}$$

où V_1, V_2 et V_3 sont trois fonctions définies positives et $\alpha > 0$. La décroissance de $\dot{V}$ est établie pour α suffisamment petit.

Les travaux présentés jusqu'ici concernent les systèmes à temps continu. En revanche, très peu de travaux portent sur les systèmes à temps discret, exceptés ceux présentés ci-après.

4.2.4 Systèmes non linéaires à temps discret

L'approche de [Zhang and Xu, 2001] a été étendue au cas des systèmes non linéaires à temps discret [Guyader and Zhang, 2003]. On considère les systèmes non linéaires :

[1] Voir Annexe A, Définition 37

$$\begin{cases} x_{k+1} = A_k x_k + \varphi_0(y_k) + \psi(y_k)\theta \\ y_k \quad = C_k x_k \end{cases} \tag{4.38}$$

où $x_k \in \mathbb{R}^n$, $y_k \in \mathbb{R}$ et $\theta \in \mathbb{R}^l$. Les matrices A_k et C_k varient dans le temps et sont connues à chaque instant. L'observateur proposé correspondant au système (4.38) est :

$$\begin{cases} \hat{x}_{k+1} = A_k \hat{x}_k + \varphi_0(y_k) + \psi(y_k)\hat{\theta}_k + K_k(y_k - \hat{y}_k) + \gamma_{k+1}(\hat{\theta}_{k+1} - \hat{\theta}_k) \\ \hat{y}_k \quad = C_k \hat{x}_k \\ \hat{\theta}_{k+1} = \hat{\theta}_k + \mu_k \gamma_k^T C_k^T (y_k - \hat{y}_k) \\ \gamma_{k+1} = (A_k - K_k C_k)\gamma_k + \psi(y_k) \end{cases} \tag{4.39}$$

où l'équation vérifiée par γ_k est celle d'un filtre auxiliaire. K_k est le gain de l'observateur et μ_k un gain positif, borné, qui vérifie :

$$||\sqrt{\mu_k} C_k \gamma_k|| \leq 1, \quad \forall k \geq 0 \tag{4.40}$$

avec $||.||$ la norme spectrale de la matrice correspondante, définie par :

$$||\sqrt{\mu_k} C_k \gamma_k|| = \sqrt{\max(\lambda)} \tag{4.41}$$

où λ représente la valeur propre de $(\sqrt{\mu_k} C_k \gamma_k)^T (\sqrt{\mu_k} C_k \gamma_k)$.

L'erreur de reconstruction d'état $\epsilon_k \triangleq x_k - \hat{x}_k$ obéit à :

$$\epsilon_{k+1} = (A_k - K_k C_k)\epsilon_k + \psi(y_k)(\theta - \hat{\theta}_k) - \gamma_{k+1}(\hat{\theta}_{k+1} - \hat{\theta}_k) \tag{4.42}$$

Le gain K_k est choisi de telle sorte que $(A_k - K_k C_k)$ soit stable. Pour assurer la convergence des paramètres, la fonction ψ doit vérifier la condition de persistance d'excitation suivante :

$$\exists T_1 > 0, \exists \alpha > 0, \quad \sum_{i=k}^{k+T_1} \psi^T(y_i)\psi(y_i) \geq \alpha \mathbf{1}, \quad \forall k \tag{4.43}$$

[Guyader and Zhang, 2003] ont montré que quand la dynamique, la sortie et les paramètres du système (4.38) sont bruités (bruits bornés de moyenne nulle), l'observateur (4.39) donne une estimation de l'état et des paramètres avec une erreur de reconstruction bornée pour l'état et pour les paramètres.
Le filtre de Kalman étendu (**E**xtended **K**alman **F**ilter, EKF) permet également d'estimer conjointement le vecteur d'état et les paramètres. Sa structure est rappelée dans le paragraphe suivant.

4.2.5 Filtre de Kalman étendu

On considère les systèmes non linéaires de la forme (4.1). On considère le vecteur d'état étendu $\bar{x}_k$ défini par :

$$\bar{x}_k = \begin{bmatrix} x_k \\ \theta_k \end{bmatrix} \tag{4.44}$$

Le système (4.1) devient :

$$\begin{cases} \bar{x}_{k+1} = \bar{f}(\bar{x}_k) \\ y_k \quad = \bar{h}(\bar{x}_k) \end{cases} \tag{4.45}$$

où $y_k \in \mathbb{R}^p$ et $\bar{x}_k \in \mathbb{R}^{n+l}$.

De façon similaire au Chapitre 3, la reconstruction d'état s'opère en deux étapes, une étape de prédiction de l'état et une étape d'estimation de l'état. L'étape de prédiction est donnée par :

$$\begin{cases} \hat{\bar{x}}_{k+1/k} = \bar{f}(\hat{\bar{x}}_k) \\ \Upsilon_{k+1/k} = F_k \Upsilon_k F_k^T + Q_k \end{cases} \tag{4.46}$$

$\hat{\bar{x}}_{k+1/k}$ représente la prédiction à un pas du vecteur $\bar{x}_{k+1}$. $\Upsilon_{k+1/k}$ est la matrice de covariance de l'erreur de prédiction $\epsilon_{k+1/k} \triangleq \bar{x}_{k+1} - \hat{\bar{x}}_{k+1/k}$. Q_k est une matrice de pondération définie positive. La matrice F_k est le jacobien[1] de la fonction $\bar{f}$ au point $\bar{x}_k = \hat{\bar{x}}_k$

L'équation d'estimation de l'état est donnée par :

$$\begin{cases} \hat{\bar{x}}_{k+1} = \hat{\bar{x}}_{k+1/k} + K_{k+1}(y_{k+1} - \bar{h}(\hat{\bar{x}}_{k+1/k})) \\ \Upsilon_{k+1} = (\mathbf{1}_n - K_{k+1} H_{k+1}) \Upsilon_{k+1/k} \end{cases} \tag{4.47}$$

$\hat{\bar{x}}_{k+1}$ est l'estimation du vecteur $\bar{x}_{k+1}$. Υ_{k+1} est la matrice de covariance de l'erreur d'estimation $\epsilon_{k+1} \triangleq \bar{x}_{k+1} - \hat{\bar{x}}_{k+1}$. K_k est le gain de Kalman et est donné par :

$$K_{k+1} = \Upsilon_{k+1/k} H_{k+1}^T (H_{k+1} \Upsilon_{k+1/k} H_{k+1}^T + R_{k+1})^{-1} \tag{4.48}$$

où R_k est une matrice de pondération définie positive.
La matrice H_k est le jacobien[1] de la fonction $\bar{h}$ au point $\bar{x}_k = \hat{\bar{x}}_k$.

La fonction de Lyapunov V est définie par $V(\epsilon_{k+1}) = \epsilon_{k+1}^T \Upsilon_{k+1}^{-1} \epsilon_{k+1}$, avec Υ_{k+1} donné par (4.47).

De même qu'au Chapitre 3, le filtre de Kalman ne tient pas compte de la spécificité liée au chaos. Dans la section suivante, nous proposons un observateur adaptatif polytopique qui permet de prendre en compte la spécificité liée au chaos.

4.3 Observateur adaptatif polytopique

Comme évoquée au Chapitre 3, une particularité des systèmes dynamiques non linéaires réside dans la nature de leurs régimes permanents. Un régime chaotique est caractérisé dans l'espace d'état par des trajectoires non convergentes mais bornées, évoluant dans un attracteur chaotique. Cette spécificité peut être intégrée dans la synthèse d'observateurs adaptatifs polytopiques pour la reconstruction simultanée état/paramètre [Anstett et al., 2004] [Millérioux et al., 2005].

On restreint la classe générale de systèmes de la forme (4.1) à la forme :

$$\begin{cases} x_{k+1} = f(x_k) + \psi(x_k)\theta_k \\ y_k \quad = h(x_k) \end{cases} \tag{4.49}$$

On suppose que ce système peut se réécrire sous la forme :

$$\begin{cases} x_{k+1} = A(x_k)x_k + \psi(x_k)\theta_k + E(x_k) \\ y_k \quad = Cx_k \end{cases} \tag{4.50}$$

[1] Voir Annexe A, Définition 28

où $A \in \mathbb{R}^{n\times n}$, $E \in \mathbb{R}^n$ et $C \in \mathbb{R}^{1\times n}$ caractérisent les fonctions f et h.
Dans la suite, on considère le cas où $E(x_k) = \mathbf{0}_n$.
Le vecteur d'état étendu $\bar{x}_k$ est défini par :

$$\bar{x}_k = \begin{bmatrix} x_k \\ \theta_k \end{bmatrix} \tag{4.51}$$

En considérant le vecteur d'état étendu $\bar{x}_k$, le système (4.50) devient :

$$\begin{cases} \bar{x}_{k+1} = \bar{A}(x_k)\bar{x}_k \\ y_k \quad = \bar{C}\bar{x}_k \end{cases} \tag{4.52}$$

avec :

$$\bar{A}(x_k) = \begin{bmatrix} A(x_k) & \psi(x_k) \\ \mathbf{0}_{l\times n} & \mathbf{1}_l \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} C & \mathbf{0}_{l\times 1} \end{bmatrix} \tag{4.53}$$

Si la Proposition 1 (Chapitre 3) appliquée au système augmenté (4.52) est vérifiée, (4.52) peut être réécrit sous la forme LPV :

$$\begin{cases} \bar{x}_{k+1} = \bar{\mathcal{A}}(\rho_k)\bar{x}_k \\ y_k \quad = \bar{C}\bar{x}_k \end{cases} \tag{4.54}$$

où la matrice $\bar{\mathcal{A}}(\rho_k)$ admet une description polytopique :

$$\bar{\mathcal{A}}(\rho_k) = \begin{bmatrix} \mathcal{A}(\rho_k) & \Phi(\rho_k) \\ \mathbf{0}_{l\times n} & \mathbf{1}_l \end{bmatrix} = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k)\bar{A}^{(i)} \tag{4.55}$$

avec $\mathcal{A}(\rho_k) = \mathcal{A}(\Psi(x_k)) = A(x_k)$ et $\Phi(\rho_k) = \Phi(\varphi(x_k)) = \psi(x_k)$. Les matrices $\bar{A}^{(i)}$ sont données par (voir Chapitre 2, Section 3.5) :

$$\bar{A}^{(i)} = \bar{\mathcal{A}}_0 + \sum_{j=1}^{L} \rho_k^{(j)} \bar{A}^{I_j} \tag{4.56}$$

On rappelle que la condition (ii) de la Proposition 1 (Chapitre 3) amène que ρ_k est borné quand x_k l'est. Par conséquent, ρ_k évolue dans un ensemble compact qui est inclus dans un polytope $\mathcal{D}_\rho$ et peut toujours se décomposer sous la forme :

$$\rho_k = \sum_{i=1}^{N} \xi_k^{(i)} \rho_{o_i} \tag{4.57}$$

L'observateur polytopique suivant peut alors être synthétisé :

$$\begin{cases} \hat{\bar{x}}_{k+1} = \bar{\mathcal{A}}(\rho_k)\hat{\bar{x}}_k + \bar{\mathcal{L}}(\rho_k)(y_k - \hat{y}_k) \\ \hat{y}_k \quad = \bar{C}\hat{\bar{x}}_k \end{cases} \tag{4.58}$$

où $\bar{\mathcal{L}}$ est un gain dépendant de ρ_k, donc variant dans le temps. A partir de (4.54) et de (4.58), on peut écrire l'équation vérifiée par l'erreur de reconstruction d'état $\epsilon_k \triangleq \bar{x}_k - \hat{\bar{x}}_k$, et obéissant à :

$$\epsilon_{k+1} = (\bar{\mathcal{A}}(\rho_k) - \bar{\mathcal{L}}(\rho_k)\bar{C})\epsilon_k \tag{4.59}$$

La dynamique de reconstruction est linéaire en ϵ_k, mais à temps variant car les matrices $\bar{\mathcal{A}}$ et $\bar{\mathcal{L}}$ dépendent de ρ_k. Par conséquent, (4.59) est un système LPV dont on cherche à garantir la stabilité globale autour de zéro. Cette garantie peut être obtenue par un choix judicieux de $\bar{\mathcal{L}}$ essentiellement guidé par la recherche d'une fonction de Lyapunov adéquate. On impose au gain $\bar{\mathcal{L}}$ une forme polytopique :

$$\bar{\mathcal{L}}(\rho_k) = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k)\bar{L}_i \tag{4.60}$$

Le vecteur ξ_k de (4.60) doit coïncider avec celui qui intervient dans la décomposition polytopique de ρ_k (4.57), ce qui est toujours possible puisque ξ_k dépend de ρ_k supposé accessible à chaque instant à travers la sortie y_k. L'expression (4.60) et la décomposition convexe (4.55) de $\bar{\mathcal{A}}(\rho_k)$ permettent de réécrire (4.59) :

$$\epsilon_{k+1} = \sum_{i=1}^{N} \xi_k^{(i)}(\rho_k)(\bar{A}^{(i)} - \bar{L}_i\bar{C})\epsilon_k \tag{4.61}$$

Imposer à $\bar{\mathcal{L}}$ la forme polytopique (4.60) signifie que $\bar{\mathcal{L}}$ est contraint d'appartenir à un polytope $\mathcal{D}_{\bar{\mathcal{L}}}$ dont les sommets sont $\bar{\mathcal{L}}(\bar{L}_1, \ldots, \bar{L}_N)$.

La convergence globale de (4.61) est assurée en appliquant la Proposition 2 du Chapitre 3 avec $\bar{A}^{(i)}$:

Théorème 10. Le système (4.61) converge asymptotiquement vers zéro s'il existe des matrices symétriques définies positives P_i, des matrices G_i et F_i, telles que, pour toutes paires $(i,j) \in \{1,\ldots,N\} \times \{1,\ldots,N\}$, l'ensemble suivant des inégalités matricielles soit vérifié :

$$\begin{bmatrix} G_i + G_i^T - P_i & G_i^T\bar{A}^{(i)} - F_i^T C \\ (\bar{A}^{(i)})^T G_i - C^T F_i & P_j \end{bmatrix} > 0 \tag{4.62}$$

avec $\bar{L}_i = (G_i^{-1})^T F_i^T$.

(4.62) garantit l'existence d'une fonction de Lyapunov polyquadratique $V : \mathbb{R}^n \to \mathbb{R}^+$, définie par $V(\epsilon_k) = \epsilon_k^T \mathcal{P}_k \epsilon_k$, avec $\mathcal{P}_k = \sum_{i=1}^{N} \xi_k^{(i)} P_i$ et $\xi_k \in S(\mathcal{D}_\rho) = \{\mu_k \in \mathbb{R}^N, \quad \mu_k = [\mu_k^{(1)} \ldots \mu_k^{(N)}]^T, \quad \mu_k^{(i)} \geq 0 \quad \forall i, \quad \sum_{i=1}^{N} \mu_k^{(i)} = 1\}$, et vérifiant :

$$V(\epsilon_{k+1}) - V(\epsilon_k) < 0, \quad \forall \xi_k \in S(\mathcal{D}_\rho) \tag{4.63}$$

L'équation (4.63) rend compte de la stabilité polyquadratique de (4.61).

Proposition 4. Afin que le système (4.61) converge polyquadratiquement vers zéro, il est nécessaire que $\Phi(\rho_k)$ ne s'annule jamais, quel que soit ρ_k appartenant à $\mathcal{D}_\rho$.

Preuve 2. Les matrices $\bar{\mathcal{A}}(\rho_k)$, $\bar{\mathcal{L}}(\rho_k)$ et $\bar{C}$ peuvent être réécrites sous la forme partitionnée suivante :

$$\bar{\mathcal{A}}(\rho_k) = \begin{bmatrix} \mathcal{A}(\rho_k) & \Phi(\rho_k) \\ \mathbf{0}_{l\times n} & \mathbf{1}_l \end{bmatrix}, \quad \bar{\mathcal{L}}(\rho_k) = \begin{bmatrix} \mathcal{L}_1 \\ \mathcal{L}_2 \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} C & \mathbf{0}_{l\times 1} \end{bmatrix} \tag{4.64}$$

où les matrices $\mathcal{L}_1$ et $\mathcal{L}_2$ sont de dimensions appropriées. L'expression $\bar{\mathcal{A}}(\rho_k) - \bar{\mathcal{L}}(\rho_k)\bar{C}$ peut alors se réécrire :

$$\bar{\mathcal{A}}(\rho_k) - \bar{\mathcal{L}}(\rho_k)\bar{C} = \begin{bmatrix} \mathcal{A}(\rho_k) - \mathcal{L}_1 C & \Phi(\rho_k) \\ -\mathcal{L}_2 C & \mathbf{1}_l \end{bmatrix} \tag{4.65}$$

S'il existe des points $\rho_k \in \mathcal{D}_\rho$ tels que $\Phi(\rho_k) = 0$, le polynôme caractéristique de $\bar{\mathcal{A}}(\rho_k) - \bar{\mathcal{L}}(\rho_k)\bar{C}$, défini par $\det(\bar{\mathcal{A}}(\rho_k) - \bar{\mathcal{L}}(\rho_k)\bar{C} - \lambda \mathbf{1}_{(l+n)\times(l+n)})$, est :

$$(1-\lambda)^l \det(\mathcal{A}(\rho_k) - \mathcal{L}_1 C - \lambda \mathbf{1}_n) \tag{4.66}$$

avec $\lambda \in \mathbb{C}$. Par conséquent, $\lambda = 1$ est une valeur propre. Dans ce cas, la condition nécessaire de détectabilité pour la stabilité polyquadratique de (4.61) n'est plus vérifiée.

■

4.4 Application à la modulation paramétrique

Dans un contexte de modulation paramétrique, considérons l'émetteur régi par le système chaotique suivant :

$$\begin{cases} x_{k+1}^{(1)} = \cos\phi x_k^{(1)} - \sin\phi x_k^{(2)} \\ x_{k+1}^{(2)} = \sin\phi x_k^{(1)} - (\cos\phi - 0.3\alpha)x_k^{(2)} + 2\alpha(x_k^{(2)})^2 + 4\theta_k\alpha((x_k^{(2)})^3 + 0.005) \\ y_k \quad = x_k^{(2)} \end{cases} \tag{4.67}$$

avec $\phi = 3.03$ rad, $\alpha = 2.7$ et $x_k = [x_k^{(1)} \quad x_k^{(2)}]^T$. Le paramètre $\theta_k \in \mathbb{R}$ est modulé par l'information claire m_k. Il est constant par morceaux. $\theta_k = \theta_1$ quand $m_k = m_1$ et $\theta_k = \theta_2$ quand $m_k = m_2$. Seul l'état $x_k^{(2)}$ est transmis au récepteur. Afin de reconstruire l'information m_k, côté récepteur, nous souhaitons estimer simultanément l'état $x_k^{(1)}$ et le paramètre modulé θ_k. La reconstruction simultanée état/paramètre va s'effectuer en deux étapes, l'une hors ligne et l'autre en temps réel.

1. Etape hors ligne

1.1 Simulation du système (4.67) et constitution de la liste Λ

Le système (4.67) est de la forme (4.50) avec :

$$\begin{aligned} A(x_k) &= \begin{bmatrix} \cos\phi & -\sin\phi \\ \sin\phi & -\cos\phi + 0.3\alpha + 2\alpha x_k^{(2)} \end{bmatrix}, \quad \psi(x_k) = \begin{bmatrix} 0 \\ 4\alpha((x_k^{(2)})^3 + 0.005) \end{bmatrix}, \\ E(x_k) &= \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \qquad\qquad C = \begin{bmatrix} 0 & 1 \end{bmatrix} \end{aligned} \tag{4.68}$$

Le vecteur d'état étendu $\bar{x}_k$ est défini par :

$$\bar{x}_k = \begin{bmatrix} x_k^{(1)} \\ x_k^{(2)} \\ \theta_k \end{bmatrix} \tag{4.69}$$

En considérant le vecteur d'état étendu $\bar{x}_k$, le système (4.67) est de la forme (4.52) avec :

$$\bar{A}(x_k) = \begin{bmatrix} A(x_k) & \psi(x_k) \\ \mathbf{0}_{1\times 2} & 1 \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \tag{4.70}$$

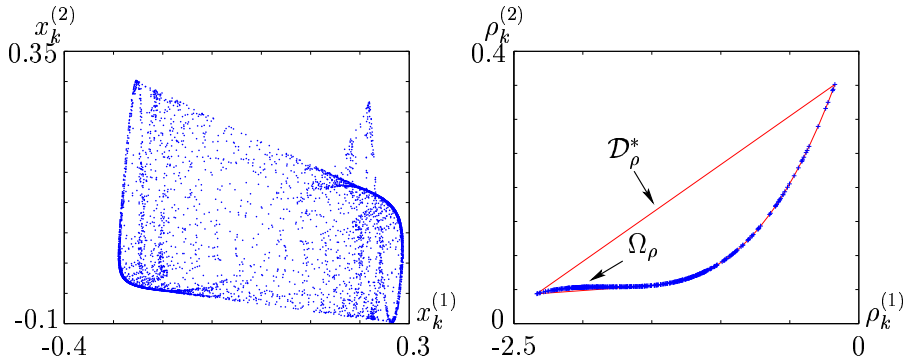
On cherche une fonction $\Psi = [\Psi_1 \quad \Psi_2]^T$ telle que $\rho_k = \Psi(\bar{x}_k)$ et la matrice $\bar{\mathcal{A}}$, vérifiant $\bar{\mathcal{A}}(\rho_k) = \bar{\mathcal{A}}(\Psi(\bar{x}_k))$, soit de classe C^1 par rapport à ρ_k. On propose $\Psi_1(\rho_k) = \rho_k^{(1)} = \cos\phi - 0.3\alpha + 2\alpha x_k^{(2)}$ et $\Psi_2(\rho_k) = \rho_k^{(2)} = 4\alpha((x_k^{(2)})^3 + 0.005)$. Le système (4.67) peut être réécrit sous forme polytopique (4.54) avec les matrices :

$$\bar{\mathcal{A}}(\rho_k) = \begin{bmatrix} \cos\phi & -\sin\phi & 0 \\ \sin\phi & \rho_k^{(1)} & \rho_k^{(2)} \\ 0 & 0 & 1 \end{bmatrix}, \quad \bar{C} = \begin{bmatrix} 0 & 1 & 0 \end{bmatrix} \tag{4.71}$$

La quantité ρ_k est disponible à chaque instant car elle dépend de $x_k^{(2)}$ qui est transmis.
La liste Λ contient les points ρ_k simulés.

1.2 Recherche des sommets ρ_{o_i} du polytope minimal $\mathcal{D}_\rho^*$

Comme x_k est chaotique, x_k réside dans un attracteur chaotique Ω, représenté sur la figure 4.2(a). Comme ρ_k dépend de x_k, il évolue dans un ensemble compact Ω_ρ, qui est l'image de Ω



(a) Attracteur chaotique Ω

(b) Polytope minimal $\mathcal{D}_\rho^*$ englobant Ω_ρ

FIG. 4.2 – Attracteur chaotique et polytope minimal

par Ψ. La marche de Graham a été appliquée pour trouver le polytope minimal $\mathcal{D}_\rho^*$ englobant Ω_ρ, représenté sur la figure 4.2(b). L'algorithme renvoie $N = 224$ sommets.

1.3 Détermination des matrices sommets $\bar{A}^{(i)}$

Les matrices $\bar{A}^{(i)}$ sont calculées conformément à (4.56) avec $L = 2$ et :

$$\bar{\mathcal{A}}_0 = \begin{bmatrix} \cos\phi & -\sin\phi & 0 \\ \sin\phi & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \bar{A}^{I_1} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \bar{A}^{I_2} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix} \tag{4.72}$$

1.4 Calcul des gains L_i

Le récepteur est un observateur polytopique de la forme (4.58). Les LMI (4.62) sont résolues avec les matrices $\bar{A}^{(i)}$ calculées comme expliqué précédemment. Ces LMI sont faisables et les gains $\bar{L}_i = G_i^{-1} F_i$ sont dérivés de leur solution.

2. Etape en temps réel

2.1 Calcul du vecteur ξ_k

Le vecteur ξ_k est calculé à chaque instant par (3.40) ou par (3.44) (voir Chapitre 3).

2.2 Calcul du gain $\mathcal{L}$

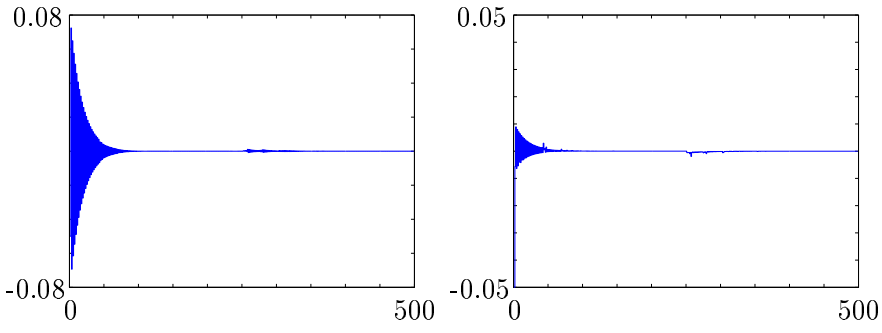
Le gain polytopique $\mathcal{L}$ est donné par (4.60) avec les gains L_i et le vecteur ξ_k calculés précédemment.

2.3 Calcul du vecteur $\bar{x}_k$

La reconstruction du vecteur d'état $\bar{x}_k$ est donnée par :

$$\begin{cases} \hat{\bar{x}}_{k+1} = \bar{\mathcal{A}}(\rho_k)\hat{\bar{x}}_k + \mathcal{L}(\rho_k)(y_k - \hat{y}_k) \\ \hat{y}_k \quad\quad = \bar{C}\hat{\bar{x}}_k \end{cases} \tag{4.73}$$

Les figures 4.3(a) et 4.3(b) représentent les erreurs de reconstruction des états $x_k^{(1)}$ et $x_k^{(2)}$, respectivement. La figure 4.4 représente le paramètre θ_k (trait pointillé) et le paramètre reconstruit $\hat{\theta}_k$ (trait plein).



(a) $x_k^{(1)} - \hat{x}_k^{(1)}$ (b) $x_k^{(2)} - \hat{x}_k^{(2)}$

FIG. 4.3 – Erreurs de reconstruction d'état

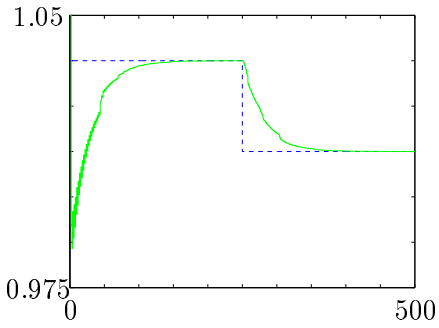


FIG. 4.4 – Trait pointillé : θ_k, trait plein : $\hat{\theta}_k$

4.5 Conclusion

Tout schéma adaptatif nécessite un temps de convergence. Pendant ce temps de convergence, le paramètre et donc l'information sont reconstruits de manière erronée. Par conséquent, l'information doit rester constante pendant ce temps de convergence et cela devient un inconvénient car le débit d'informations est limité.

Le chiffrement par inclusion permet de pallier les différents problèmes rencontrés dans le masquage additif, la modulation chaotique et la modulation paramétrique.
Dans le masquage additif, la synchronisation est imparfaite.
Dans la modulation chaotique et la modulation paramétrique, la synchronisation nécessite un transitoire. L'information étant reconstruite de façon erronée pendant le transitoire, elle doit rester constante pendant ce temps. Le débit d'information est alors limité.
Dans le chiffrement par inclusion, le récepteur est synchronisé de telle sorte qu'il assure une synchronisation globale indépendante de l'information. Par conséquent, aucune hypothèse sur la limitation du débit d'information est émise. Comme le chiffrement par inclusion ne présente pas les inconvénients précédents, seul ce schéma sera étudié d'un point de vue de sa cryptanalyse, dans le chapitre suivant.

Chapitre 5

Cryptanalyse du chiffrement par inclusion et identifiabilité paramétrique

5.1 Introduction

Dans ce chapitre, on s'intéresse au schéma de chiffrement par inclusion, présenté dans le Chapitre 2. On rappelle que, dans ce schéma, l'émetteur est régi par :

$$\Sigma_\theta \begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k \quad\;\; = h_\theta(x_k, m_k) \end{cases} \tag{5.1}$$

Ce schéma est rappelé sur la figure 5.1.

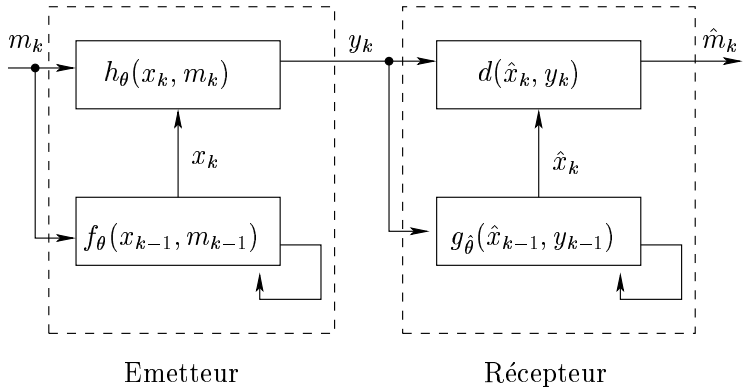


FIG. 5.1 – Chiffrement par inclusion

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

Pour répondre à cette question, nous considérons une attaque particulière, appelée attaque brute ("brute-force attack"). Dans cette attaque, on suppose que l'adversaire n'a pas d'autre stratégie que d'essayer exhaustivement toutes les valeurs possibles pour les paramètres (ensemble fini), afin de trouver la valeur réelle. La situation la plus défavorable pour un adversaire, et la plus favorable pour la sécurité du système, est qu'il existe une unique valeur possible pour les paramètres, pour un comportement entrée/sortie donné. Dans ce cas, la probabilité de trouver la bonne valeur est la plus faible pour l'adversaire.
L'unicité des valeurs des paramètres est directement liée au concept d'identifiabilité. Très peu de travaux ont établi ce lien, excepté dans [Dedieu and Ogorzalek, 1997]. Nous proposons un formalisme général basé sur ce concept d'identifiabilité. Des travaux préliminaires ont été effectués dans [Anstett et al., 2005a] [Anstett et al., 2005c].
Il existe différentes méthodes pour tester l'identifiabilité paramétrique des systèmes à temps discret, comme l'approche basée sur l'égalité des sorties ou celle basée sur la relation entrée/sortie. La dernière approche, dédiée aux systèmes polynomiaux, est constructive. En effet, elle permet non seulement de conclure quant à l'identifiabilité paramétrique mais aussi de reconstruire les paramètres identifiables dans un contexte d'attaque à texte clair choisi (une séquence de l'entrée et la séquence correspondante de la sortie sont connues).
Nous montrons que les cryptosystèmes chaotiques présentant des non linéarités de type polynomial peuvent toujours être facilement cassés par une attaque à texte clair choisi. Dans ce contexte, la faiblesse de ces cryptosystèmes est révélée et ce, indépendamment du comportement du système, chaotique ou non.

Dans la Section 5.2, une introduction à la cryptanalyse et à quelques attaques est présentée. Dans la Section 5.3, différentes définitions de l'identifiabilité, issues de la littérature, sont données ainsi que les éventuelles relations entre ces définitions. Puis, dans la Section 5.4, une approche pour tester l'identifiabilité des paramètres, basée sur l'égalité des sorties, est présentée. Dans la Section 5.5, une autre approche pour tester l'identifiabilité paramétrique, basée sur la relation entrée/sortie, est détaillée. Cette approche fait notamment appel à des notions d'algèbre, rappelées dans l'Annexe B. Enfin, dans la Section 5.7, la cryptanalyse paramétrique des cryptosystèmes à temps discret, présentant des non linéarités de type polynomial, est étudiée. Quelques exemples illustrent la faiblesse de ces cryptosystèmes.

5.2 Cryptanalyse

Alice et Bob essaient de communiquer de façon sécurisée. un adversaire, Charlie, tente de faire échouer la communication secrète entre Alice et Bob. Il peut, par exemple, intercepter le signal transitant sur le canal dans le but de récupérer le texte clair, il peut modifier le signal transitant sur le canal, ou encore il peut se faire passer pour l'une des entités Alice ou Bob. Toutes ces tentatives, et il en existe de nombreuses autres, sont des attaques sur le cryptosystème. La figure 5.2 illustre ce schéma pour le chiffrement par inclusion.
La cryptanalyse est l'étude des probabilités de succès des attaques possibles sur les cryptosystèmes afin de déceler leurs éventuelles faiblesses [Delfs and Knebl, 2002]. Un des principaux objectifs de la cryptanalyse est de tester si un adversaire peut déchiffrer le texte clair ou récupérer la clé secrète. Pour cela, le cryptanalyste se met à la place de l'adversaire.

La cryptographie et la cryptanalyse sont deux domaines d'études évoluant constamment et en parallèle. En effet, de nouveaux cryptosystèmes, toujours plus complexes, sont développés pour

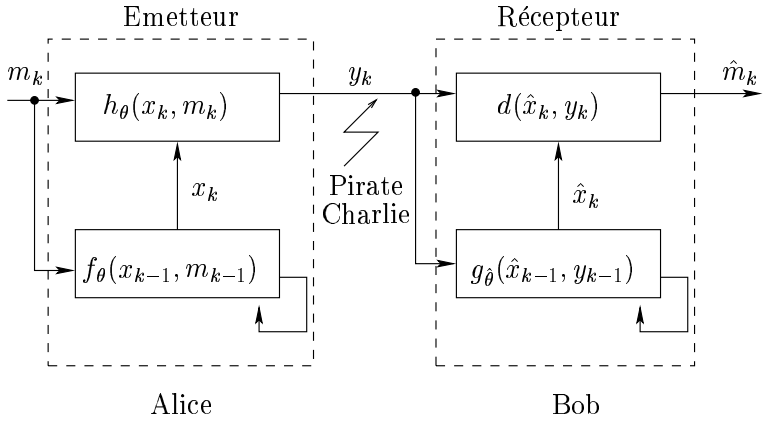


FIG. 5.2 – Schéma de communication

remplacer ceux qui ont été "cassés" par la cryptanalyse et de nouvelles techniques de cryptanalyse sont inventées pour tester ces nouveaux cryptosystèmes. Le problème du cryptographe est de concevoir des systèmes sûrs et de faire en sorte que la durée nécessaire pour "casser" un cryptosystème soit supérieure à sa durée de validité. La tendance actuelle est de chercher des à prouver la sécurité d'un système sur la base d'hypothèses sur la puissance de calcul requise ou sur la quantité de texte clair/choisi connue.
La réussite pratique d'une attaque dépend d'un certain nombre d'éléments, comme les connaissances nécessaires a priori, l'effort demandé (complexité, temps de calcul), la quantité et la qualité des informations pouvant être déduites de l'attaque (déchiffrement de la clé secrète, algorithme de chiffrement découvert sans connaître la clé secrète, informations sur le texte clair, ...), ...
La complexité de l'attaque se caractérise par le temps en nombre d'opérations effectuées (addition, XOR, ...), par la mémoire nécessaire et par la quantité de données (texte clair et texte chiffré) requises.

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

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

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

5.2.1 Hypothèse de Kerckhoff

La cryptanalyse des schémas de cryptage peut être effectuée sous un certain nombre d'hypothèses. Une hypothèse fondamentale, connue sous le nom de *principe de Kerckhoff* [Barthélemy et al., 2005], est que l'adversaire connaît complètement l'algorithme de cryptage, à l'exception

de la clé secrète qui est inconnue. Dans ce cas, la sécurité du cryptosystème repose entièrement sur la clé secrète. Cette hypothèse signifie que la sécurité d'un schéma de cryptage ne doit pas reposer sur la confidentialité du schéma, c'est-à-dire la fonction de chiffrement employée, mais sur la confidentialité de la clé.
Le but de l'adversaire est alors de retrouver le texte clair ou une quelconque information sur le texte clair, ce qui, dans la plupart des cas, nécessite la connaissance de la clé secrète. D'autres hypothèses peuvent alors être formulées. Elles ne concernent que des attaques passives et sont décrites dans [Menezes et al., 1996]. L'objectif commun de ces attaques est de systématiquement retrouver le texte clair à partir du texte chiffré ou de déduire la clé secrète. Ces attaques sont rappelées ci-après, elles sont classées de la plus réaliste à la plus hypothétique.

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

- *Attaque à texte clair connu* ("known plaintext attack")
  l'adversaire connaît une séquence du texte clair et la séquence correspondante du texte chiffré.

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

- *Attaque adaptative à texte clair choisi* ("adaptive chosen plaintext attack")
  Cette attaque est une attaque à texte clair choisi où le choix du texte clair peut dépendre du texte chiffré reçu précédemment.

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

- *Attaque adaptative à texte chiffré choisi* ("adaptive chosen ciphertext attack")
  Cette attaque est une attaque à texte chiffré choisi où le choix du texte chiffré peut dépendre du texte clair reçu précédemment.

5.2.2 Attaque brute

L'attaque la plus élémentaire est appelée *attaque brute* ou *recherche exhaustive*. Elle consiste à essayer de façon exhaustive toutes les valeurs possibles de la clé secrète. Pour décider si la clé testée est correcte, il faut connaître le texte chiffré et une information sur le texte clair (par exemple, savoir si le texte clair est une image, un texte dans une langue donnée, ...). En effet, pour la clé correspondant à celle recherchée, le déchiffrement du texte chiffré produira le texte clair attendu (par exemple, un texte cohérent dans une langue donnée, une image, ...).
Cette attaque est la plus coûteuse en temps de calcul et en mémoire à cause de la recherche exhaustive. Une manière de définir un cryptosystème comme sécurisé est qu'il n'existe aucune autre méthode moins coûteuse (temps de calcul, mémoire, ...) que la recherche exhaustive [Schneier, 1996].

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

5.2.3 Attaque algébrique

Dans une attaque algébrique, le système de chiffrement est représenté par un système d'équations algébriques multivariables dépendant de l'information, de la clé secrète et du texte chiffré. Le principe de cette attaque est de tenir compte de la structure algébrique du système et de résoudre le système d'équations afin de récupérer la clé secrète qui est donnée par la solution de ce système d'équations.

Dans la suite, nous nous intéressons au chiffrement par inclusion. On rappelle que dans ce schéma, l'émetteur a pour représentation d'état générale :

$$\begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k \quad\ = h_\theta(x_k, m_k) \end{cases} \tag{5.2}$$

où $x_k \in \mathbb{R}^n$ est le vecteur d'état, $y_k \in \mathbb{R}$ la sortie, $m_k \in \mathbb{R}$ l'information à masquer, $\theta = [\theta_1, \ldots, \theta_l] \in \Theta \subset \mathbb{R}^l$ les paramètres du système chaotique, supposés jouer le rôle de clé secrète. Nous ne considérons que le cas pratique où le système (5.2) est mono-entrée mono-sortie, mais les résultats présentés pourront être étendus à des cas multi-entrées multi-sorties. Seul le signal de sortie y_k est transmis au récepteur par l'intermédiaire d'un canal de transmission qui n'est pas sécurisé. Nous nous attacherons au cas où le système (5.2) présente des non linéarités de type polynomial. Ce type de non linéarités se retrouve dans un grand nombre de systèmes chaotiques (récurrence logistique, de Hénon, d'Ikeda, ...).

Nous allons effectuer la cryptanalyse de ce schéma à travers des attaques particulières, de type passif, qui s'attachent au problème de récupération des paramètres θ supposés jouer le rôle de la clé secrète. On se place sous l'hypothèse de Kerckhoff. Dans ce cas, la sécurité du cryptosystème repose entièrement sur la clé secrète et non sur la méconnaissance du schéma de chiffrement. On se met alors à la place d'un adversaire qui connaît la structure du système (5.2) ainsi que le signal y_k transitant sur le canal. La question qui se pose alors est : à partir de ces connaissances, est-il possible de retrouver les paramètres ?
Pour répondre à cette question, on considère une attaque brute ou recherche exhaustive. Dans ce contexte, on admet que l'adversaire n'a pas d'autre stratégie que d'essayer exhaustivement toutes les valeurs possibles pour le vecteur de paramètres θ. On considère que l'ensemble des paramètres Θ est un ensemble fini. Dans un contexte de recherche exhaustive, la situation la plus défavorable pour un adversaire, qui est la plus favorable pour la sécurité du système, est qu'il existe une unique valeur pour chaque paramètre. En effet, dans ce cas, l'adversaire doit essayer toutes les valeurs possibles pour retrouver chaque paramètre et la probabilité de trouver le bon candidat est la plus faible. Le problème de l'unicité de la valeur des paramètres est lié au concept d'identifiabilité.

Il existe de nombreuses définitions de l'identifiabilité dans la littérature. Dans la section suivante, nous effectuons la synthèse de ces définitions, pour les systèmes à temps continu et les systèmes à temps discret et établissons les éventuelles relations entre les différentes définitions. Pour le problème de cryptanalyse qui nous intéresse, le lecteur peut directement se référer aux Définitions 20 et 25 qui seront considérées dans la suite de notre étude.

5.3 Définitions de l'identifiabilité

Parmi les différentes définitions de l'identifiabilité existant dans la littérature, on distingue des définitions analytiques et des définitions algébriques. Ces définitions sont répertoriées dans [Noiret, 2000] pour les systèmes à temps continu.

On considère le système admettant la représentation d'état, en temps continu :

$$\Sigma_\theta \begin{cases} \dot{x}(t) = f_\theta(x(t), m(t)) \\ y(t) = h_\theta(x(t), m(t)) \end{cases} \tag{5.3}$$

en temps discret :

$$\Sigma_\theta \begin{cases} x_{k+1} = f_\theta(x_k, m_k) \\ y_k \quad\;\; = h_\theta(x_k, m_k) \end{cases} \tag{5.4}$$

où $x(t)$ (respectivement x_k) $\in \mathbb{R}^n$, $m(t)$ (resp. m_k) $\in \mathbb{R}^m$, $y(t)$ (resp. y_k) $\in \mathbb{R}^p$, $\theta \in \Theta \subset \mathbb{R}^l$, f_θ est une fonction non linéaire et h_θ une fonction éventuellement non linéaire, toutes deux paramétrées par θ. Le problème est de tester l'identifiabilité du système, c'est-à-dire du vecteur de paramètres θ.

Les définitions sont données telles que leurs auteurs les ont énoncées, mais avec des notations unifiées par souci de clarté.
On distinguera les définitions de l'identifiabilité locale de celles de l'identifiabilité globale, l'identifiabilité locale étant une condition nécessaire pour l'identifiabilité globale. La propriété d'identifiabilité locale est vraie pour $\theta \in v(\theta) \subset \Theta$ où $v(\theta)$ est un voisinage de θ et la propriété d'identifiabilité globale est vraie pour $\theta \in \Theta$.

5.3.1 Définitions analytiques

Systèmes à temps continu

Considérons le système à temps continu donné par (5.3).

Les Définitions 7 à 12, 16 et 17 sont des définitions structurelles de l'identifiabilité. Une propriété est dite *structurelle* si elle est vraie pour toutes les valeurs des paramètres sauf éventuellement pour un ensemble de mesure nulle (ensemble de valeurs atypiques des paramètres). Cet ensemble de mesure nulle conduit à des singularités où aucune conclusion sur l'identifiabilité n'est possible.

Dans les Définitions 7 à 12, $y(m(t), \theta)$ définit le comportement entrée/sortie du système Σ_θ (5.3) dépendant du vecteur de paramètres θ, c'est-à-dire la sortie $y(t)$ du système (5.3) pour l'entrée $m(t)$. Les Définitions 7 à 12 proposent une étude sur la plage de temps $[0, +\infty[$. L'entrée $m(t)$ et la plage de temps peuvent être choisies arbitrairement et ne sont donc pas spécifiées.

Les Définitions 7 à 9 concernent l'identifiabilité structurelle d'un paramètre particulier de Σ_θ.

Définition 7. [Walter and Pronzato, 1997] Le paramètre $\theta^{(i)}$ est *structurellement localement identifiable* si, pour presque tout $\theta \in \Theta$, il existe un voisinage $v(\theta)$ de θ, tel que :

$$\hat{\theta} \in v(\theta), \quad y(m(t), \theta) = y(m(t), \hat{\theta}) \Rightarrow \hat{\theta}^{(i)} = \theta^{(i)} \tag{5.5}$$

Définition 8. [Walter and Pronzato, 1997] Le paramètre $\theta^{(i)}$ est *structurellement globalement identifiable* si pour presque tout $\theta \in \Theta$:

$$y(m(t),\theta) = y(m(t),\hat{\theta}) \Rightarrow \hat{\theta}^{(i)} = \theta^{(i)} \tag{5.6}$$

Définition 9. [Walter and Pronzato, 1997] Le paramètre $\theta^{(i)}$ est *structurellement non identifiable* si, pour presque tout $\theta \in \Theta$, il n'existe pas de voisinage $v(\theta)$ de θ, tel que :

$$\hat{\theta} \in v(\theta), \quad y(m(t),\theta) = y(m(t),\hat{\theta}) \Rightarrow \hat{\theta}^{(i)} = \theta^{(i)} \tag{5.7}$$

Les Définitions 10 à 12 sont plus générales que les définitions précédentes car elles étendent la notion d'identifiabilité à tout le système.

Définition 10. [Walter and Pronzato, 1997] Un système Σ_θ est *structurellement localement identifiable* si tous les paramètres $\theta^{(i)}$, $i = 1, \ldots, l$, sont structurellement localement identifiables.

Définition 11. [Walter and Pronzato, 1997] Un système Σ_θ est *structurellement globalement identifiable* si tous les paramètres $\theta^{(i)}$, $i = 1, \ldots, l$, sont structurellement globalement identifiables.

Définition 12. [Walter and Pronzato, 1997] Un système Σ_θ est *structurellement non identifiable* s'il existe au moins un paramètre $\theta^{(i)}$ structurellement non identifiable.

Pour un système donné, les propriétés d'identifiabilité précédentes peuvent être vraies pour un choix particulier de la condition initiale $x(0)$ mais fausses pour un autre.

Lorsque $x(0)$ est fixée, on remplace $y(m(t),\theta)$ par $y(x(0),m(t),\theta)$. En revanche, si l'on cherche à identifier $x(0)$ en plus des paramètres, on peut considérer le vecteur étendu des paramètres $\theta_e = [\theta \quad x(0)]^T$.

Si les conditions initiales $x(0)$ ne sont pas spécifiées, il existe en général un ensemble de trajectoires de sortie, noté $\bar{y}(m(t),\theta)$, pour une entrée $m(t)$ et un vecteur de paramètres θ donnés. Deux trajectoires issues de deux conditions initiales différentes peuvent converger, après un transitoire. Dans ce cas, il convient d'étudier l'identifiabilité du système après ce transitoire car on ne tient pas compte des conditions initiales. Pour cela, on teste l'intersection des ensembles $\bar{y}(m(t),\theta)$ et $\bar{y}(m(t),\hat{\theta})$ et non leur égalité comme dans les définitions précédentes, du fait du transitoire.

Définition 13. [Ljung and Glad, 1994] Un système Σ_θ est *globalement identifiable* en $\theta \in \Theta$ s'il existe une entrée $m(t)$ telle que :

$$\bar{y}(m(t),\theta) \neq \emptyset, \quad \bar{y}(m(t),\theta) \cap \bar{y}(m(t),\hat{\theta}) \neq \emptyset \Rightarrow \hat{\theta} = \theta \tag{5.8}$$

Définition 14. [Ljung and Glad, 1994] Un système Σ_θ est *localement identifiable* en $\theta \in \Theta$ s'il existe un voisinage ouvert $v(\theta)$ de θ tel que le système Σ_θ est globalement identifiable en θ sur $v(\theta)$.

Ces définitions ne sont pas structurelles car elles sont valables pour la valeur particulière θ et non pour presque tout $\theta \in \Theta$.

Comme pour la condition initiale, les propriétés d'identifiabilité 7 à 12 peuvent être vraies pour un choix particulier de l'entrée $m(t)$ et de la plage de temps, mais fausses pour un autre.

Dans les Définitions 15 à 17, $\{y(x(0), m(t), \theta)\}_{t_0}^{t_1}$ représente le comportement entrée/sortie du système Σ_θ (5.3), dépendant du vecteur de paramètres θ, c'est-à-dire la sortie $y(t)$ du système (5.3) issue de la condition initiale $x(0)$, pour l'entrée $m(t)$, sur l'intervalle de temps $[t_0, t_1]$. $\mathcal{M}_{t_0}^{t_1}$ est l'ensemble des entrées mesurables et bornées qui sont définies sur $[t_0, t_1]$. La notion de paramètres indiscernables est nécessaire pour définir l'identifiabilité d'un système.

Définition 15. [Vajda et al., 1989] Les paramètres θ et $\hat{\theta}$, $\hat{\theta} \in \Theta$, sont *indiscernables* à travers les expériences spécifiées par $x(0)$ et $\mathcal{M}_{t_0}^{t_1}$ si $\{y(x(0), m(t), \theta)\}_{t_0}^{t_1} = \{y(x(0), m(t), \hat{\theta})\}_{t_0}^{t_1}$, pour tout $m(t) \in \mathcal{M}_{t_0}^{t_1}$.

Les paramètres θ et $\hat{\theta}$ indiscernables sont notés $\hat{\theta} \sim \theta$.

Définition 16. [Vajda et al., 1989] Le système Σ_θ est *structurellement localement identifiable* si, pour presque tout $\theta \in \Theta$, il existe un voisinage $v(\theta)$ de θ, tel que :

$$\hat{\theta} \in v(\theta), \quad \hat{\theta} \sim \theta \Rightarrow \hat{\theta} = \theta \tag{5.9}$$

Définition 17. [Vajda et al., 1989] Le système Σ_θ est *structurellement globalement identifiable* si pour presque tout $\theta \in \Theta$:

$$\hat{\theta} \sim \theta \Rightarrow \hat{\theta} = \theta \tag{5.10}$$

En accord avec [Noiret, 2000], on peut noter que la Définition 16 implique la Définition 10. En effet, si un système est identifiable sur l'intervalle $[t_0, t_1]$, une étude sur l'intervalle $[t_0, t_2]$, $t_2 > t_1$, n'apportera pas d'information supplémentaire sur l'identifiabilité du système.
De la même manière, la Définition 17 implique la Définition 11.

D'autres définitions de l'identifiabilité ont été proposées dans [Tunali and Tarn, 1987]. Ces définitions sont également énoncées pour une condition initiale $x(0)$ et un ensemble d'entrées fixés. Cependant, l'ensemble des entrées considérées est restreint par rapport aux définitions précédentes.

Systèmes à temps discret

Considérons le système à temps discret admettant la représentation d'état (5.4).

Pour les Définitions 19 et 20, $\{y(x_0, m_k, \theta)\}_{t_0}^{t_1}$ définit le comportement entrée/sortie du système Σ_θ (5.4), dépendant du vecteur de paramètres θ, c'est-à-dire la sortie y_k du système (5.4) issue de la condition initiale x_0, pour l'entrée m_k, sur l'intervalle de temps $[t_0, t_1]$. Les Définitions 19 et 20 sont énoncées pour un ensemble fixé d'entrées admissibles, dont la définition est rappelée ci-dessous.

Définition 18. [Nõmm and Moog, 2004] Une séquence d'entrée sur un horizon d'itérations $[0, T]$, notée $\{m_k\}_0^T$, est appelée *entrée admissible sur* $[0, T]$ si le système (5.4) admet une unique solution locale.

Définition 19. [Nõmm and Moog, 2004] Le système Σ_θ (5.4) est *localement fortement x_0-identifiable* en θ pour la séquence d'entrées admissibles $\{m_k\}_0^T$, s'il existe un voisinage ouvert de θ, $v(\theta) \subset \Theta$, tel que pour tout $\hat{\theta} \in v(\theta)$ et pour tout $\theta \in v(\theta)$:

$$\hat{\theta} \neq \theta \Rightarrow \{y_k(x_0, m_k, \hat{\theta})\}_0^T \neq \{y_k(x_0, m_k, \theta)\}_0^T \tag{5.11}$$

La Définition 19 n'est pas structurelle puisqu'elle est valable uniquement pour la valeur particulière θ.

Définition 20. [Nõmm and Moog, 2004] Le système Σ_θ (5.4) est *structurellement identifiable* s'il existe $T > 0$, un sous-ensemble ouvert $\mathcal{X}_0 \subset \mathcal{X}$ et des sous-ensembles denses[1] $v(\theta) \subset \Theta$ et $\mathcal{M}_0^T \subset \mathcal{M}$, tels que, quels que soient $x_0 \in \mathcal{X}_0$, $\theta \in v(\theta)$ et $\{m_k\}_0^T \in \mathcal{M}_0^T$, le système Σ_θ (5.4) est localement fortement x_0-identifiable en θ pour la séquence d'entrées admissibles $\{m_k\}_0^T$.

Remarque 3. Dans la définition ci-dessus, le sous-ensemble $\mathcal{X}_0$ est ouvert afin d'éviter de considérer un ensemble atypique de mesure nulle qui conduirait à des singularités et où aucune conclusion sur l'identifiabilité n'est possible. De plus, les Définitions 19 et 20 sont données pour la condition initiale prise à l'instant particulier $k = 0$. En revanche, on peut considérer n'importe quel instant k car le système (5.4) est invariant (au décalage).

5.3.2 Définitions algébriques

Pour les définitions algébriques, nous supposons que les fonctions f_θ et h_θ des systèmes à temps continu (5.3) et à temps discret (5.4) respectivement, sont polynomiales. Comme expliqué dans [Ljung and Glad, 1994], cette restriction n'est pas une contrainte sévère. Par exemple, la relation $x(t) = \sin(y(t))$ peut aussi s'écrire $(\dot{x}(t))^2 = (\dot{y}(t))^2(1 - (x(t))^2)$.
Dans les définitions algébriques, les conditions initiales ne sont pas prises en compte.

Systèmes à temps continu

Considérons le système Σ_θ à temps continu donné par (5.3).

Définition 21. [Diop and Fliess, 1991] Le vecteur de paramètres θ est *algébriquement identifiable* si et seulement s'il est algébrique sur $k < m, y >$.

$k < m, y >$ est un corps différentiel[2] des variables $m(t)$ et $y(t)$. La définition précédente signifie que θ est algébriquement identifiable si et seulement s'il vérifie une équation algébrique dépendant uniquement de $m(t)$, de $y(t)$ et de leurs dérivées, de la forme :

$$\mathcal{L}(\theta, y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots) = 0 \tag{5.12}$$

Comme il s'agit de résoudre une équation algébrique, plusieurs valeurs des paramètres peuvent être solution. Par exemple, la relation $\mathcal{L} = 0$ peut avoir la forme suivante :

$$\ddot{y}(t) - (\theta^{(1)})^2 \dot{y}(t) - y(t) - m(t) = 0 \tag{5.13}$$

Dans ce cas, deux solutions, notées $\theta_{1,2}^{(1)}$, existent pour $\theta^{(1)}$, données par :

$$\theta_{1,2}^{(1)} = \pm\sqrt{\frac{\ddot{y}(t) - y(t) - m(t)}{\dot{y}(t)}} \tag{5.14}$$

Si $\dot{y}(t) \neq 0$, le paramètre $\theta^{(1)}$ est algébriquement identifiable.
Si l'on s'intéresse au cas où il existe une unique valeur possible pour les paramètres, on peut utiliser la définition suivante.

[1] Voir Annexe A, Définition 32
[2] Voir Annexe A, Définition 39

Définition 22. [Diop and Fliess, 1991] Le vecteur de paramètres θ est *rationnellement identifiable* si et seulement s'il appartient à $k < m, y >$.

Cette définition signifie que le vecteur de paramètres peut s'exprimer comme une unique fraction rationnelle de polynômes dépendant de $m(t)$, de $y(t)$ et de leurs dérivées.
Par exemple, si l'on a la relation suivante :

$$\ddot{y}(t) - \theta^{(1)}\dot{y}(t) - y(t) - m(t) = 0 \tag{5.15}$$

le paramètre $\theta^{(1)}$ peut être réécrit, si $\dot{y}(t) \neq 0$:

$$\theta^{(1)} = \frac{\ddot{y}(t) - y(t) - m(t)}{\dot{y}(t)} \tag{5.16}$$

Le paramètre $\theta^{(1)}$ est rationnellement identifiable.

La Définition 22 est équivalente à celle de l'identifiabilité globale de [Ljung and Glad, 1994] :

Définition 23. Le système Σ_θ est globalement identifiable si et seulement s'il peut être réécrit sous forme de régression linéaire telle que, pour $i = 1, \ldots, l$:

$$P_i(y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots)\theta^{(i)} - Q_i(y(t), \dot{y}(t), \ldots, m(t), \dot{m}(t), \ldots) = 0 \tag{5.17}$$

où P_i et Q_i sont des polynômes dépendant uniquement de $y(t)$, de $m(t)$ et de leurs dérivées.

Systèmes à temps discret

Considérons le système Σ_θ à temps discret donné par (5.4).
L'extension de la Définition 21 donnée pour les systèmes à temps continu, aux systèmes à temps discret est la suivante :

Définition 24. [Nõmm and Moog, 2004] Le système Σ_θ est *algébriquement identifiable* s'il existe un entier positif T, un sous-ensemble ouvert $\mathcal{X}_0 \subset \mathcal{X}$, des sous-ensembles denses $\Theta \subset \mathbb{R}^l$ et $\mathcal{M}_0^T \in \mathcal{M}$, et une fonction méromorphe[1] $\phi : \mathbb{R}^l \times \mathbb{R}^{T+1} \times \mathbb{R}^{T+1} \to \mathbb{R}^l$, tels que :

$$\det(\frac{\partial \phi}{\partial \theta}) \neq 0 \tag{5.18}$$

et

$$\phi(\theta, y_0, \ldots, y_T, m_0, \ldots, m_T) = 0 \tag{5.19}$$

pour tout $(\theta, y_0, \ldots, y_T, m_0, \ldots, m_T)$ où $(\theta, x_0, m_0, \ldots, m_T) \in \Theta \times \mathcal{X}_0 \times \mathcal{M}_0^T$.

Le fait de poser $\det(\frac{\partial \phi}{\partial \theta}) \neq 0$ suppose que l'on est loin des singularités, c'est-à-dire que le système est suffisamment excité.
Par exemple, considérons la fonction ϕ :

$$\phi(\theta, y_k, y_{k+1}, y_{k+2}, m_k, m_{k+1}) = \begin{bmatrix} (\theta^{(1)} + \theta^{(2)})y_k - y_{k+1} - m_k \\ (\theta^{(1)} + \theta^{(2)})y_{k+1} - y_{k+2} - m_{k+1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{5.20}$$

[1] Voir Annexe A, Définition 41

Dans cet exemple, on a :

$$\det(\frac{\partial \phi}{\partial \theta}) = \begin{vmatrix} y_k & y_k \\ y_{k+1} & y_{k+1} \end{vmatrix} = 0 \tag{5.21}$$

Comme le déterminant est nul, les paramètres $\theta^{(1)}$ et $\theta^{(2)}$ ne sont pas identifiables.

Considérons à présent, la fonction ϕ :

$$\phi(\theta, y_k, y_{k+1}, y_{k+2}, y_{k+3}, m_k, m_{k+1}) = \begin{bmatrix} (\theta^{(1)})^2 y_k + \theta^{(2)} y_{k+1} + (y_{k+2})^2 - m_k \\ (\theta^{(1)})^2 y_{k+1} + \theta^{(2)} y_{k+2} + (y_{k+3})^2 - m_{k+1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix} \tag{5.22}$$

Dans cet exemple, on a :

$$\det(\frac{\partial \phi}{\partial \theta}) = \begin{vmatrix} 2\theta^{(1)} y_k & y_{k+1} \\ 2\theta^{(1)} y_{k+1} & y_{k+2} \end{vmatrix} = 2\theta^{(1)}(y_k y_{k+2} - (y_{k+1})^2) \tag{5.23}$$

Le déterminant n'est pas nul si $y_k y_{k+2} - (y_{k+1})^2 \neq 0$. Dans ce cas, les paramètres $\theta^{(1)}$ et $\theta^{(2)}$ sont algébriquement identifiables.

Comme pour la Définition 21, la Définition 24 signifie que plusieurs valeurs des paramètres peuvent être solution.

De même que la Définition 21 est étendue aux systèmes à temps discret en la Définition 24, la Définition 22 peut également être étendue aux systèmes à temps discret. Aucune extension n'étant donnée dans la littérature, nous proposons la définition suivante.

Définition 25. Le système Σ_θ (5.4) est globalement identifiable si et seulement s'il peut se réécrire sous la forme d'une régression linéaire telle que, pour $i = 1, \ldots, l$:

$$P_i(y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N})\theta^{(i)} - Q_i(y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N}) = 0 \tag{5.24}$$

où P_i et Q_i sont des polynômes dépendant uniquement de m_k, de y_k et de leurs itérés.

La différence entre les Définitions 21 et 22 est l'unicité des valeurs pour les paramètres. De même, la différence entre les Définitions 24 et 25 est l'unicité des valeurs pour les paramètres, requise dans la Définition 25. En ce sens, la Définition 25 nous intéresse pour notre étude.

Dans la suite, par "*système identifiable*", on entend unicité de la valeur des paramètres, c'est-à-dire qu'à un comportement entrée/sortie donné, correspond une unique valeur des paramètres. Un système sera dit identifiable si tous ses paramètres le sont. De plus, pour "*identifiable au sens de la définition analytique*", on retiendra la Définition 20, et pour "*identifiable au sens de la définition algébrique*", on retiendra la Définition 25.
Nous allons présenter deux approches qui permettent de tester l'identifiabilité des paramètres des systèmes à temps discret. La première, basée sur l'égalité des sorties permet de tester l'identifiabilité au sens de la définition analytique. La deuxième, basée sur la relation entrée/sortie et dédiée aux systèmes polynomiaux, permet de tester l'identifiabilité au sens de la définition algébrique. Cette dernière approche est constructive dans le sens où elle permet non seulement de conclure quant à l'identifiabilité des paramètres mais aussi de reconstruire les paramètres dans un contexte d'attaque à texte clair choisi. Dans cette attaque, l'adversaire choisit une séquence

de l'information m_k et analyse la séquence correspondante de la sortie y_k. Pour notre étude, on pourrait tout aussi bien se placer dans un contexte d'attaque à texte clair connu car le principal est de connaître une séquence de l'information (choisie ou non) et la séquence correspondante de la sortie.

Dans la suite, nous considérons le système à temps discret (5.2).

Dans la Section suivante, nous présentons une approche pour tester l'identifiabilité au sens de la définition analytique.

5.4 Approche basée sur l'égalité des sorties

L'approche basée sur l'égalité des sorties est directement dérivée de la Définition 20. Les trajectoires $y_k(x_0, m_k, \theta)$ contiennent des informations sur le vecteur de paramètres θ. L'approche consiste à tester si l'égalité des trajectoires de sortie des systèmes Σ_θ et $\Sigma_{\hat{\theta}}$, sur l'intervalle $[0-T]$, implique l'égalité des vecteurs de paramètres θ et $\hat{\theta}$. Le théorème suivant énonce une condition *suffisante* d'identifiabilité structurelle du système Σ_θ (5.2). La condition initiale x_0 et l'entrée m_k sont spécifiées dans les Définitions 18, 19 et 20.

Théorème 11. Le système Σ_θ est structurellement identifiable pour presque tout $\theta \in \Theta$ si, quels que soient x_0, m_k, il existe $T > 0$, tel que :

$$\{y_k(x_0, m_k, \theta)\}_0^T = \{y_k(x_0, m_k, \hat{\theta})\}_0^T \Rightarrow \hat{\theta} = \theta \tag{5.25}$$

La preuve de ce théorème est une conséquence directe de l'implication (5.11).

Ce théorème porte sur l'identifiabilité globale du système. Si l'on se restreint à l'identifiabilité locale, seule la considération d'un voisinage de θ permet de conserver la propriété d'unicité de la solution. Par exemple, le paramètre θ^2 est localement identifiable pour $\theta \in \Theta$ et globalement identifiable dans un voisinage de θ. En effet, il existe une unique valeur pour ce paramètre, qui est $-\theta$ dans un voisinage $v_1(\theta)$ et qui est $+\theta$ dans un voisinage $v_2(\theta)$.

T est un entier positif et représente le nombre d'itérations requis pour prouver le Théorème 11. Si T tend vers l'infini, cela signifie que la relation précédente ne peut pas être prouvée. Dans ce cas, aucune conclusion sur l'identifiabilité structurelle ne peut être donnée. Comme T est inconnu a priori, le Théorème 11 est seulement une condition suffisante d'identifiabilité structurelle.

Remarque 4. Dans le cas des systèmes à temps continu, cette approche est fortement connectée à celle basée sur le développement en séries de Taylor de la trajectoire de sortie, initiée par [Pohjanpalo, 1978]. Pour tester leur égalité, les trajectoires de sortie $y(t)$ sont approximées par leur développement en séries de Taylor. Les coefficients du développement en séries de Taylor sont uniques et contiennent des informations sur les paramètres. Le principe est alors de tester si l'égalité de ces coefficients implique l'égalité des vecteurs de paramètres θ et $\hat{\theta}$.

Dans la Section suivante, nous présentons une approche pour tester l'identifiabilité au sens de la définition algébrique.

5.5 Approche basée sur la relation entrée/sortie

Cette approche permet de tester l'identifiabilité au sens de la Définition algébrique 25. On considère que les fonctions f_θ et h_θ sont polynomiales.

5.5.1 Principe de l'approche

Si la Définition 25 est satisfaite, chaque paramètre $\theta^{(i)}$ peut se réécrire sous la forme suivante :

$$\theta^{(i)} = \frac{Q_i(y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N})}{P_i(y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N})} \tag{5.26}$$

sauf si P_i s'annule. La condition $P_i \neq 0$ est appelée *condition d'excitation persistante*. L'ensemble des valeurs de y_k et de m_k correspondant à $P_i = 0$ est l'ensemble des mesure nulle, en général. Cet ensemble de mesure nulle peut être omis en considérant uniquement l'ensemble des entrées admissibles (Définition 18).

Pour obtenir la relation (5.24), nous devons éliminer les états internes x_k et leurs itérés dans le système (5.2), considérés comme indéterminés. Cela conduit à une relation dépendant uniquement du vecteur de paramètres θ, de la sortie y_k, de l'entrée m_k et de leurs itérés. Cette relation est appelée *relation entrée/sortie* et est de la forme :

$$\mathcal{L}_1(\theta, y_k, \ldots, y_{k+s}, m_k, \ldots, m_{k+s}) = 0 \tag{5.27}$$

où s est l'indice d'observabilité du système (5.2) [Nijmeijer and Van Der Schaft, 1990], défini comme suit.
Soit f_θ^i la ième composition de la fonction f_θ, $f_\theta^i(x_k) \triangleq f_\theta(f_\theta^{i-1}(x_k))\ \forall i \geq 1$ et $f_\theta^0(x_k) \triangleq x_k$. L'indice d'observabilité s est un entier positif tel que, $\forall x_k \in v(x_k)$ où $v(x_k)$ est un voisinage de x_k :

$$\begin{aligned} &\operatorname{rang}\Big(\frac{\partial\big(h_\theta(x_k), (h_\theta \circ f_\theta)(x_k), \ldots, (h_\theta \circ f_\theta^{s-1})(x_k)\big)}{\partial x_k}\Big) = s \\ &\operatorname{rang}\Big(\frac{\partial\big(h_\theta(x_k), (h_\theta \circ_\theta f)(x_k), \ldots, (h_\theta \circ f_\theta^{s-1})(x_k), (h_\theta \circ f_\theta^{s})(x_k)\big)}{\partial x_k}\Big) = s \end{aligned} \tag{5.28}$$

Nous considérons trois approches d'élimination de variables dédiées aux systèmes polynomiaux, c'est-à-dire d'obtention de la relation entrée/sortie : l'approche basée sur les bases de Gröbner, l'approche basée sur l'ensemble caractéristique et celle basée sur le résultant de deux polynômes. Ces approches utilisent des notions d'algèbre qui sont rappelées dans l'Annexe B. Seule la définition d'un ordre lexicographique est énoncée ci-dessous.

Définition 26. Un *ordre lexicographique* des variables $x_k^{(1)}, \ldots, x_k^{(n)}$, noté $<$, est un ordre total portant sur le nom des variables et de leurs itérés, tel que, $\forall i = 1, \ldots, n$, $\forall j = 1, \ldots, n$:

$$\begin{aligned} &- \quad x_k^{(i)} < x_{k+l}^{(i)}, && \forall l \in \mathbb{N} \\ &- \quad x_k^{(i)} < x_l^{(j)} \Rightarrow x_{k+t}^{(i)} < x_{l+t}^{(j)}, && \forall l \in \mathbb{N}, \quad \forall t \in \mathbb{N} \\ &- \quad x_k^{(i)} < x_k^{(j)} \Rightarrow (x_k^{(i)})^\alpha < (x_k^{(j)})^\beta, && \forall \alpha \in \mathbb{N}, \quad \forall \beta \in \mathbb{N} \end{aligned} \tag{5.29}$$

Par exemple, selon l'ordre lexicographique $x_k^{(1)} < x_k^{(2)}$, l'ensemble des variables $\{x_k^{(1)}, x_k^{(1)}x_k^{(2)}, (x_k^{(1)})^2, x_{k+1}^{(1)}, x_{k+1}^{(2)}\}$ sera ordonné comme suit :

$$x_k^{(1)} < (x_k^{(1)})^2 < x_{k+1}^{(1)} < x_k^{(1)}x_k^{(2)} < x_{k+1}^{(2)} \tag{5.30}$$

5.5.2 Bases de Gröbner

Le premier algorithme d'obtention des bases de Gröbner est dû à [Buchberger, 1965] dans les années 60, qui a donné le nom de son directeur de thèse, Wolfgang Gröbner, à cet algorithme. Il a été appliqué pour la première fois au problème de l'identifiabilité par [Ljung and Glad, 1994] dans le cas de systèmes à temps continu.

Le principe de l'approche est le suivant. Comme la paire (m_k, y_k) satisfait le système (5.2), elle satisfera également les équations obtenues par multiplication et par addition de (5.2), c'est-à-dire l'idéal engendré par (5.2). Pour un ordre lexicographique fixé, il suffit alors de chercher une base de cet idéal dont une expression ne contient plus les variables à éliminer x_k, mais contient seulement y_k, m_k, leurs itérés et le vecteur de paramètres θ. Cette expression de la base est de la forme recherchée (5.27). Une telle base est appelée base de Gröbner (voir Annexe B pour une définition plus formelle).

5.5.3 Ensemble caractéristique

La théorie de l'ensemble caractéristique a été introduite par Ritt [Ritt, 1950]. L'ensemble des définitions nécessaires pour définir un ensemble caractéristique est donné dans l'Annexe B.

La méthode de l'ensemble caractéristique permet d'obtenir, à partir du système (5.2) et de ses itérés, un ensemble de la forme triangulaire suivante :

$$\begin{aligned} A_1 &= (y_k, \ldots, y_{k+s}, m_k, \ldots, m_{k+s}, \theta^{(1)}, \ldots, \theta^{(l)}) = 0 \\ A_2 &= (y_k, \ldots, y_{k+s}, m_k, \ldots, m_{k+s}, \theta^{(1)}, \ldots, \theta^{(l)}, x_k^{(1)}) = 0 \\ &\vdots \\ A_{n+1} &= (y_k, \ldots, y_{k+s}, m_k, \ldots, m_{k+s}, \theta^{(1)}, \ldots, \theta^{(l)}, x_k^{(1)}, \ldots, x_k^{(n)}) = 0 \end{aligned} \tag{5.31}$$

La relation $A_1 = 0$ représente la relation entrée/sortie (5.27).

Les composantes $x_k^{(i)}$ du vecteur d'état peuvent aussi être exprimées, à partir de $\{A_2, \ldots, A_{n+1}\}$, comme une fonction dépendant uniquement de l'entrée m_k, de la sortie y_k, de leurs itérés et du vecteur de paramètres θ. Cela provient de la forme triangulaire de (5.31). En particulier, la condition initiale x_k peut alors être déduite de $\{A_2, \ldots, A_{n+1}\}$.

5.5.4 Résultant de deux polynômes

Pour expliquer le principe de l'élimination basée sur le résultant de polynômes, quelques définitions s'avèrent nécessaires et sont rappelées dans l'Annexe B. Elles peuvent être trouvées dans [Wang, 2001].

Définition 27. Le déterminant de la matrice de Sylvester[1] M de deux polynômes p et q est appelé le *résultant* de p et q, et sera noté $R(p, q)$.

[1] voir Annexe B, Section B.3

Théorème 12. Soient deux polynômes $p = a_0 + a_1 x_k + \ldots + a_m x_k^m$ et $q = b_0 + b_1 x_k + \ldots + b_n x_k^n$. Le résultant $R(p, q)$ de p et q est nul si et seulement si les polynômes ont un zéro commun ou si $a_0 = b_0 = 0$.

Considérons deux polynômes p et q, dépendant tous deux des variables $x_k^{(1)}$ et $x_k^{(2)}$. Supposons que l'on souhaite éliminer la variable $x_k^{(2)}$. Les polynômes p et q peuvent être vus comme des polynômes dépendant uniquement de la variable $x_k^{(2)}$ et dont les coefficients sont des fonctions de $x_k^{(1)}$. Le résultant de ces deux polynômes peut être calculé. Comme les coefficients des polynômes sont des fonctions de $x_k^{(1)}$, le résultant sera un polynôme dépendant uniquement de $x_k^{(1)}$ et la variable $x_k^{(2)}$ sera ainsi éliminée. D'après le Théorème 12, pour que les deux polynômes aient un zéro commun, le résultant doit être nul. Par conséquent, poser le résultant égal à zéro donne une équation uniquement en $x_k^{(1)}$.
Cette approche peut être étendue à des polynômes multivariables. Dans ce cas, les variables sont éliminées les unes après les autres, selon l'ordre lexicographique fixé, en calculant successivement les résultants.

5.5.5 Procédure récapitulative

L'approche basée sur la relation entrée/sortie, proposée pour tester l'identifiabilité des paramètres, peut se résumer par les étapes suivantes.

1. Le système (5.2) est itéré s fois, où s représente l'indice d'observabilité du système (5.2). Généralement, s est la dimension n du système.
2. Une méthode d'élimination, les bases de Gröbner, l'ensemble caractéristique ou le résultant, est appliquée au système (5.2) et à ses itérés, afin d'éliminer l'état interne x_k, considéré comme indéterminé, et d'obtenir la relation entrée/sortie (5.27). Cette élimination peut être effectuée par des logiciels de calcul symbolique (Maxima, Maple, ...).
3. La relation entrée/sortie (5.27) est itérée jusqu'à la dimension l du vecteur de paramètres, afin d'obtenir autant d'équations que d'inconnues :

$$\begin{aligned} &\mathcal{L}_1(\theta, y_k, \ldots, y_{k+s}, m_k, \ldots, m_{k+s}) = 0 \\ &\vdots \\ &\mathcal{L}_l(\theta, y_k, \ldots, y_{k+N}, m_k, \ldots, m_{k+N}) = 0 \end{aligned} \tag{5.32}$$

   où N est $s + l - 1$.
4. On vérifie si, à partir de (5.32), la relation (5.24) peut être obtenue pour chaque paramètre.

Remarque 5. Dans [Wang, 2001], il est expliqué qu'il n'y a pas d'approche d'élimination meilleure que les autres. Tout dépend du type de problème considéré, de sa complexité, de l'implémentation faite de l'algorithme.

5.6 Résumé

Le problème considéré dans ce chapitre est de tester l'unicité des valeurs des paramètres constants θ du système non linéaire à temps discret (5.4). Ce problème est directement lié au concept d'identifiabilité paramétrique.
Plusieurs définitions de l'identifiabilité existent dans la littérature. Nous retiendrons la Définition

analytique 20 et la Définition algébrique 25. Pour les définitions algébriques, nous considérons des systèmes présentant des non linéarités polynomiales.
Pour tester l'identifiabilité analytique (Définition 20), l'approche considérée est basée sur l'égalité des sorties.
Pour tester l'identifiabilité algébrique (Définition 25), l'approche utilisée est celle basée sur la relation entrée/sortie, dédiée aux systèmes à non linéarités polynomiales. Pour obtenir la relation entrée/sortie, trois approches d'élimination de variables sont considérées, les bases de Gröbner, l'ensemble caractéristique et le résultant de polynômes.

A partir de ces différents outils, la cryptanalyse paramétrique des cryptosystèmes chaotiques est effectuée dans la section suivante.

5.7 Cryptanalyse paramétrique

Dans cette section, la cryptanalyse paramétrique des cryptosystèmes chaotiques à temps discret, de la forme générale (5.2) et présentant des non linéarités polynomiales, est étudiée. On se met à la place d'un adversaire qui est supposé connaître la structure du système ainsi que le signal de sortie y_k qui transite sur le canal, d'après l'hypothèse de Kerckhoff. A partir de ces connaissances, l'adversaire cherche à récupérer les paramètres du système chaotique, supposés jouer le rôle de clé secrète. Nous considérons deux attaques.
La première attaque est une attaque brute qui consiste à essayer exhaustivement toutes les valeurs possibles pour les paramètres. Pour évaluer la sécurité dans ce contexte, nous testons l'identifiabilité des paramètres, c'est-à-dire si, à un comportement entrée/sortie donné, correspond une unique valeur pour le vecteur de paramètres. Cette situation est la meilleure pour la sécurité du système.
La seconde attaque est une attaque à texte clair choisi. Dans ce contexte, l'adversaire connaît une séquence du signal d'entrée $\{m_k\}$ et analyse la séquence correspondante du signal de sortie $\{y_k\}$. Pour évaluer la sécurité dans ce contexte, nous testons si les paramètres peuvent être reconstruits à partir de la relation entrée/sortie. Cette approche correspond à une attaque algébrique.
Ces deux attaques, testées à travers les approches basées respectivement sur l'égalité des sorties et sur la relation entrée/sortie, sont illustrées par les exemples suivants.

5.7.1 Exemple 1

Considérons le cryptosystème chaotique où l'information m_k est injectée dans la récurrence suivante [Barbot, 2003] :

$$\left\{ \begin{array}{lcl} x_{k+1}^{(1)} & = & (1+\theta^{(1)})x_k^{(1)} + x_k^{(1)}x_k^{(2)} + m_k \\ x_{k+1}^{(2)} & = & (1-\theta^{(2)})x_k^{(2)} - (x_k^{(1)})^2 m_k \\ y_k & = & x_k^{(1)} \end{array} \right. \tag{5.33}$$

Le système (5.33) est de la forme (5.2), avec :

$$f_\theta(x_k, m_k) = \left[\begin{array}{c} (1+\theta^{(1)})x_k^{(1)} + x_k^{(1)}x_k^{(2)} + m_k \\ (1-\theta^{(2)})x_k^{(2)} - (x_k^{(1)})^2 m_k \end{array} \right], \quad h_\theta(x_k, m_k) = x_k^{(1)} \tag{5.34}$$

La condition initiale est $x_0 = [x_0^{(1)} \quad x_0^{(2)}]^T$.
Dans la suite, l'identifiabilité structurelle du vecteur de paramètres $[\theta^{(1)} \quad \theta^{(2)}]^T$ $(l = 2)$, au sens

de la définition analytique, est testée avec l'approche basée sur l'égalité des sorties. L'identifiabilité au sens de la définition algébrique est testée avec l'approche basée sur la relation entrée/sortie.

Approche basée sur l'égalité des sorties

Pour $k = 0, 1, 2$, les valeurs de la trajectoire de sortie $\{y_k(x_0, m_k, \theta)\}_0^2$, notées $y_k(\theta)$ pour des raisons de simplicité, sont :

$$\begin{aligned}
y_0(\theta) &= x_0^{(1)} \\
y_1(\theta) &= (1+\theta^{(1)})x_0^{(1)} + x_0^{(1)}x_0^{(2)} + m_0 \\
y_2(\theta) &= (1+\theta^{(1)})((1+\theta^{(1)})x_0^{(1)} + x_0^{(1)}x_0^{(2)} + m_0) + ((1-\theta^{(2)})x_0^{(2)} - (x_0^{(1)})^2 m_0)((1+\theta^{(1)})x_0^{(1)} \\
&\quad + x_0^{(1)}x_0^{(2)} + m_0) + m_1
\end{aligned} \tag{5.35}$$

Les conditions (5.25) deviennent :

$$y_0(\hat{\theta}) = y_0(\theta) \quad \Rightarrow \quad x_0^{(1)} = x_0^{(1)} \tag{5.36}$$

$$y_1(\hat{\theta}) = y_1(\theta) \quad \Rightarrow \quad (\hat{\theta}^{(1)} - \theta^{(1)})x_0^{(1)} = 0 \tag{5.37}$$

$$\begin{aligned}
y_2(\hat{\theta}) = y_2(\theta) \Rightarrow \quad & ((\hat{\theta}^{(1)})^2 - (\theta^{(1)})^2 + 2\hat{\theta}^{(1)} - 2\theta^{(1)})x_0^{(1)} + (2\hat{\theta}^{(1)} - 2\theta^{(1)} - \hat{\theta}^{(1)}\hat{\theta}^{(2)} + \theta^{(1)}\theta^{(2)} + \theta^{(2)} \\
& -\hat{\theta}^{(2)})x_0^{(1)}x_0^{(2)} + (\hat{\theta}^{(2)} - \theta^{(2)})x_0^{(1)}(x_0^{(2)})^2 - (\hat{\theta}^{(1)} - \theta^{(1)})(x_0^{(1)})^3 m_0 \\
& -(\hat{\theta}^{(1)} - \theta^{(1)})m_0 - (\hat{\theta}^{(2)} - \theta^{(2)})x_0^{(2)}m_0 = 0
\end{aligned} \tag{5.38}$$

(5.36) est triviale et est toujours vérifiée. Supposant que $x_0^{(1)} \neq 0$ et $x_0^{(2)} \neq 0$, (5.37) conduit à $\hat{\theta}^{(1)} = \theta^{(1)}$ et ensuite, (5.38) conduit à $\hat{\theta}^{(2)} = \theta^{(2)}$. Par conséquent, le Théorème 11 est vérifié pour $T = 2$ et les paramètres $\theta^{(1)}$ et $\theta^{(2)}$ sont structurellement identifiables.
Notons que $x_0^{(1)} = 0$ et $x_0^{(2)} = 0$ est une mesure nulle ($x_0^{(1)} = 0$ et $x_0^{(2)} = 0$ n'appartiennent pas à $\mathcal{X}_0$) qui conduit à une singularité où aucune conclusion sur l'identifiabilité paramétrique n'est possible.

Approche basée sur la relation entrée/sortie

Pour obtenir la relation entrée/sortie $\mathcal{L}_1 = 0$ (5.27), le système (5.33) est itéré jusqu'à son indice d'observabilité qui se révèle être aussi sa dimension ($s = n = 2$) :

$$\begin{cases}
x_{k+1}^{(1)} - (1+\theta^{(1)})x_k^{(1)} - x_k^{(1)}x_k^{(2)} - m_k = 0 \\
x_{k+2}^{(1)} - (1+\theta^{(1)})x_{k+1}^{(1)} - x_{k+1}^{(1)}x_{k+1}^{(2)} - m_{k+1} = 0 \\
x_{k+1}^{(2)} - (1-\theta^{(2)})x_k^{(2)} + (x_k^{(1)})^2 m_k = 0 \\
x_{k+2}^{(2)} - (1-\theta^{(2)})x_{k+1}^{(2)} + (x_{k+1}^{(1)})^2 m_{k+1} = 0 \\
y_k - x_k^{(1)} = 0 \\
y_{k+1} - x_{k+1}^{(1)} = 0 \\
y_{k+2} - x_{k+2}^{(1)} = 0
\end{cases} \tag{5.39}$$

L'état $x_k^{(2)}$ n'est pas directement transmis. Par conséquent, $x_k^{(2)}$ est choisi pour être le plus grand dans l'ordre lexicographique suivant :

$$x_k^{(1)} < x_k^{(2)} \tag{5.40}$$

Approche basée sur les bases de Gröbner
Le logiciel de calcul symbolique Maxima, disponible en ligne à `http ://maxima.sourceforge.net`, permet de calculer, avec la fonction `poly_buchberger`, la base de Gröbner de l'idéal associé à (5.39), avec l'ordre lexicographique (5.40). Une des expressions de la base de Gröbner est la relation entrée/sortie $\mathcal{L}_1 = 0$:

$$\begin{array}{l}\theta^{(1)}\theta^{(2)}y_k y_{k+1} + \theta^{(2)}(-y_{k+1}^2 + y_k y_{k+1} + m_k y_{k+1}) \\ -y_{k+2}y_k + y_{k+1}^2 - y_k^3 y_{k+1} m_k - m_k y_{k+1} + m_{k+1} y_k = 0\end{array} \tag{5.41}$$

Les autres expressions de la base ne présentent pas d'intérêt pour notre étude puisqu'elles impliquent le vecteur d'état. Puis, la relation entrée/sortie (5.41) est itérée une fois pour avoir autant d'équations que d'inconnues ($l = 2$), ce qui conduit à $\mathcal{L}_2 = 0$:

$$\begin{array}{l}\theta^{(1)}\theta^{(2)}y_{k+1} y_{k+2} + \theta^{(2)}(-y_{k+2}^2 + y_{k+1} y_{k+2} + m_{k+1} y_{k+2}) \\ -y_{k+3}y_{k+1} + y_{k+2}^2 - y_{k+1}^3 y_{k+2} m_{k+1} - m_{k+1} y_{k+2} + m_{k+2} y_{k+1} = 0\end{array} \tag{5.42}$$

(5.41) et (5.42) peuvent se réécrire sous la forme (5.26) pour chaque paramètre. En effet, la fonction `solve` de Maxima calcule avec succès :

$$\begin{aligned}\theta^{(1)} &= \frac{Q_1(y_k, \ldots, y_{k+3}, m_k, \ldots, m_{k+2})}{P_1(y_k, \ldots, y_{k+3}, m_k, \ldots, m_{k+2})} \\ \theta^{(2)} &= \frac{Q_2(y_k, \ldots, y_{k+3}, m_k, \ldots, m_{k+2})}{P_2(y_k, \ldots, y_{k+3}, m_k, \ldots, m_{k+2})}\end{aligned} \tag{5.43}$$

avec :

$$\begin{array}{l}P_1(y_k, \ldots, y_{k+3}, m_k, \ldots, m_{k+2}) = \\ y_k y_{k+1}^2 y_{k+3} - 2y_k y_{k+1} y_{k+2}^2 + (m_{k+1} y_k y_{k+1}^4 + y_{k+1}^3 - (m_k y_k^3 + m_k) y_{k+1}^2 + (2m_{k+1} - m_{k+2}) y_k y_{k+1}) y_{k+2}\end{array}$$

$$\begin{array}{l}Q_1(y_k, \ldots, y_{k+3}, m_k, \ldots, m_{k+2}) = \\ (y_{k+1}^3 - (y_k + m_k) y_{k+1}^2) y_{k+3} - y_k y_{k+2}^3 + ((2y_k - m_k y_k^3) y_{k+1} + 2m_{k+1} y_k) y_{k+2}^2 \\ +(m_{k+1} y_{k+1}^5 - (m_{k+1} y_k + m_k m_{k+1}) y_{k+1}^4 - y_{k+1}^3 + (m_k y_k^3 - m_{k+2} + m_k) y_{k+1}^2 + (m_k m_{k+1} y_k^3 \\ +(m_{k+2} - 2m_{k+1}) y_k + m_k m_{k+2}) y_{k+1} - m_{k+1}^2 y_k) y_{k+2}\end{array}$$

$$P_2(y_k, \ldots, y_{k+3}, m_k, \ldots, m_{k+2}) = y_k y_{k+2}^2 + (-y_{k+1}^2 + m_k y_{k+1} - m_{k+1} y_k) y_{k+2}$$

$$\begin{array}{l}Q_2(y_k, \ldots, y_{k+3}, m_k, \ldots, m_{k+2}) = \\ -(y_k y_{k+1} y_{k+3} - 2y_k y_{k+2}^2 + (m_{k+1} y_k y_{k+1}^3 + y_{k+1}^2 - (m_k y_k^3 + m_k) y_{k+1} + (2m_{k+1} - m_{k+2}) y_k) y_{k+2})\end{array} \tag{5.44}$$

Par conséquent, $\theta^{(1)}$ et $\theta^{(2)}$ sont identifiables et peuvent être facilement reconstruits en effectuant une attaque à texte clair choisi.

Approche basée sur l'ensemble caractéristique
Les polynômes définissant le système (5.33) sont :

$$\begin{array}{rcl} B_1 & = & x_{k+1}^{(1)} - (1+\theta^{(1)})x_k^{(1)} - x_k^{(1)}x_k^{(2)} - m_k \\ B_2 & = & x_{k+1}^{(2)} - (1-\theta^{(2)})x_k^{(2)} - (x_k^{(1)})^2 m_k \\ B_3 & = & y_k - x_k^{(1)} \end{array} \tag{5.45}$$

D'après l'ordre lexicographique (5.40), le terme de tête[1] de B_1 est $x_k^{(1)}x_k^{(2)}$, le terme de tête de B_2 est $x_{k+1}^{(2)}$ et le terme de tête de B_3 est $x_k^{(1)}$. Afin de calculer l'ensemble caractéristique, les polynômes B_1 et B_2 doivent être réduits par rapport au polynôme B_3. Il vient :

$$\begin{array}{rcl} B_1 & = & y_{k+1} - (1+\theta^{(1)})y_k - y_k x_k^{(2)} - m_k \\ B_2 & = & x_{k+1}^{(2)} - (1-\theta^{(2)})x_k^{(2)} - y_k^2 m_k \\ B_3 & = & y_k - x_k^{(1)} \end{array} \tag{5.46}$$

Le terme de tête de B_1 est $y_k x_k^{(2)}$ et l'état $x_k^{(1)}$ ou ses itérés n'apparaissent plus dans B_1. Par conséquent, B_1 est réduit par rapport à B_3. Le terme de tête de B_2 est toujours $x_{k+1}^{(2)}$. Comme l'état $x_k^{(1)}$ et ses itérés n'apparaissent plus dans B_2, B_2 est réduit par rapport à B_3. En revanche, le polynôme B_2 doit être réduit par rapport à B_1. Il vient :

$$\begin{array}{rcl} B_1 & = & y_{k+1} - (1+\theta^{(1)})y_k - y_k x_k^{(2)} - m_k \\ B_2 & = & \theta^{(1)}\theta^{(2)} y_k y_{k+1} + \theta^{(2)}(-y_{k+1}^2 + y_k y_{k+1} + m_k y_{k+1}) \\ & & -y_{k+2}y_k + y_{k+1}^2 - y_k^3 y_{k+1} m_k - m_k y_{k+1} + m_{k+1} y_k \\ B_3 & = & y_k - x_k^{(1)} \end{array} \tag{5.47}$$

Le terme de tête de B_2 est à présent y_{k+2}. Il est réduit par rapport à B_1. Les polynômes B_1, B_2 et B_3 sont tous réduits les uns par rapport aux autres. Ils sont donc autoréduits et l'ensemble caractéristique du système (5.33) est :

$$\begin{array}{l} A_1(y_k, y_{k+1}, y_{k+2}, m_k, m_{k+1}, m_{k+2}, \theta^{(1)}, \theta^{(2)}) = B_2 \\ = \theta^{(1)}\theta^{(2)} y_k y_{k+1} + \theta^{(2)}(-y_{k+1}^2 + y_k y_{k+1} + m_k y_{k+1}) - y_{k+2}y_k + y_{k+1}^2 - y_k^3 y_{k+1} m_k - m_k y_{k+1} + m_{k+1} y_k \\ \\ A_2(y_k, y_{k+1}, y_{k+2}, m_k, m_{k+1}, m_{k+2}, \theta^{(1)}, \theta^{(2)}, x_k^{(1)}) = B_3 \\ = y_k - x_k^{(1)} \\ \\ A_3(y_k, y_{k+1}, y_{k+2}, m_k, m_{k+1}, m_{k+2}, \theta^{(1)}, \theta^{(2)}, x_k^{(1)}, x_k^{(2)}) = B_1 \\ = y_{k+1} - (1+\theta^{(1)})y_k - y_k x_k^{(2)} \end{array} \tag{5.48}$$

Dans l'ensemble caractéristique (5.48), $A_1 = 0$ représente la relation entrée/sortie. Elle est identique à (5.41). Par conséquent, on aboutit à la même conclusion que précédemment. $\theta^{(1)}$ et $\theta^{(2)}$ peuvent être calculés à partir de A_1 et de ses itérés et sont donnés par (5.43) et (5.44) ; les paramètres $\theta^{(1)}$ et $\theta^{(2)}$ sont identifiables.

Approche basée sur le résultant

D'après l'ordre lexicographique fixé, on commence par éliminer l'état $x_{k+1}^{(2)}$, à l'aide des polynômes $p_1 = x_{k+2}^{(1)} - (1+\theta^{(1)})x_{k+1}^{(1)} - x_{k+1}^{(1)}x_{k+1}^{(2)} - m_{k+1} = 0$ et $q_1 = x_{k+1}^{(2)} - (1-\theta^{(2)})x_k^{(2)} + (x_k^{(1)})^2 m_k = 0$.

[1] Voir Annexe B, Définition 46

p_1 et q_1 peuvent être vus comme deux polynômes dépendant de la seule variable $x_{k+1}^{(2)}$ et dont les coefficients sont des fonctions de $x_k^{(2)}$, $x_k^{(1)}$, $x_{k+1}^{(1)}$ et $x_{k+2}^{(1)}$. On a $m = 1$ et $n = 1$. La matrice de Sylvester de p_1 et q_1, de dimension 2×2, est donnée par :

$$M_1 = \begin{bmatrix} x_{k+1}^{(1)} & -x_{k+2} + (1 + \theta^{(1)} x_{k+1}^{(1)} + m_{k+1} \\ 1 & -(1 - \theta^{(2)}) x_k^{(2)} - (x_k^{(1)})^2 m_k \end{bmatrix} \tag{5.49}$$

Le résultant de p_1 et q_1 est :

$$R(p_1, q_1) = |M_1| = x_{k+2}^{(1)} - (1 + \theta^{(1)}) x_{k+1}^{(1)} - m_{k+1} - (x_k^{(1)})^2 m_k - (1 - \theta^{(2)}) x_{k+1}^{(1)} x_k^{(2)} \tag{5.50}$$

D'après le Théorème 12, pour que p_1 et q_1 aient un zéro commun, on annule $R(p_1, q_1)$.
Puis, on va éliminer $x_k^{(2)}$, à l'aide des polynômes $p_2 = x_{k+1}^{(1)} - (1 + \theta^{(1)}) x_k^{(1)} - x_k^{(1)} x_k^{(2)} - m_k = 0$ et $q_2 = R(p_1, q_1) = 0$. p_2 et q_2 peuvent être vus comme deux polynômes dépendant de la seule variable $x_k^{(2)}$ et dont les coefficients sont des fonctions de $x_k^{(1)}$, $x_{k+1}^{(1)}$ et $x_{k+2}^{(1)}$. On a $m = 1$ et $n = 1$. La matrice de Sylvester de p_2 et q_2, de dimension 2×2, est donnée par :

$$M_2 = \begin{bmatrix} x_k^{(1)} & -x_{k+1}^{(1)} + (1 + \theta^{(1)}) x_k^{(1)} + m_k \\ -(1 - \theta^{(2)}) x_{k+1}^{(1)} & x_{k+2}^{(1)} - (1 + \theta^{(1)} x_{k+1}^{(1)} - m_{k+1} - (x_k^{(1)})^2 x_{k+1}^{(1)} m_k \end{bmatrix} \tag{5.51}$$

Le résultant de p_2 et q_2 est :

$$\begin{aligned} R(p_2, q_2) = |M_2| = {} & \theta^{(1)} \theta^{(2)} x_k^{(1)} x_{k+1}^{(1)} + \theta^{(2)} (-(x_{k+1}^{(1)})^2 + x_k^{(1)} x_{k+1}^{(1)} + m_k x_{k+1}^{(1)}) - x_{k+2}^{(1)} x_k^{(1)} + (x_{k+1}^{(1)})^2 \\ & - (x_k^{(1)})^3 x_{k+1}^{(1)} m_k - m_k x_{k+1}^{(1)} + m_{k+1} x_k^{(1)} \end{aligned} \tag{5.52}$$

Comme $y_k = x_k^{(1)}$, on a :

$$\begin{aligned} R(p_2, q_2) = {} & \theta^{(1)} \theta^{(2)} y_k y_{k+1} + \theta^{(2)} (-y_{k+1}^2 + y_k y_{k+1} + m_k y_{k+1}) - y_{k+2} y_k + y_{k+1}^2 - y_k^3 y_{k+1} m_k \\ & - m_k y_{k+1} + m_{k+1} y_k \end{aligned} \tag{5.53}$$

D'après le Théorème 12, pour que p_2 et q_2 aient un zéro commun, on annule $R(p_2, q_2)$. La relation $R(p_2, q_2) = 0$ représente la relation entrée/sortie $\mathcal{L}_1 = 0$.
La fonction `eliminate` de Maxima permet de trouver la relation entrée/sortie par cette approche basée sur le résultant.
La relation entrée/sortie $R(p_2, q_2) = 0$ est identique à (5.41). Par conséquent, on aboutit à la même conclusion que précédemment. $\theta^{(1)}$ et $\theta^{(2)}$ peuvent être calculés à partir de $R(p_2, q_2) = 0$ et de ses itérés et sont donnés par (5.43) et (5.44) ; les paramètres $\theta^{(1)}$ et $\theta^{(2)}$ sont identifiables.

Conclusion

L'approche basée sur l'égalité des sorties et l'approche basée sur la relation entrée/sortie conduisent à la même conclusion.

Dans un contexte d'attaque brute, comme les paramètres $\theta^{(1)}$ et $\theta^{(2)}$ sont identifiables, ils conduisent à un unique comportement entrée/sortie et pourraient donc jouer le rôle de clé secrète.
Cependant, bien que les paramètres $\theta^{(1)}$ et $\theta^{(2)}$ soient identifiables, ils ne peuvent pas jouer le rôle de clé secrète, car une attaque à texte clair choisi permet de les reconstruire.

5.7.2 Exemple 2

Considérons le cryptosystème chaotique où l'information m_k est injectée dans la récurrence de Hénon :

$$\begin{cases} x_{k+1}^{(1)} &= \theta^{(1)}(x_k^{(1)})^2 + \theta^{(2)}x_k^{(2)} + m_k \\ x_{k+1}^{(2)} &= \theta^{(3)}x_k^{(1)} + \theta^{(4)}m_k \\ y_k &= x_k^{(1)} \end{cases} \tag{5.54}$$

Le système (5.54) est de la forme (5.2), avec :

$$f_\theta(x_k, m_k) = \begin{bmatrix} \theta^{(1)}(x_k^{(1)})^2 + \theta^{(2)}x_k^{(2)} + m_k \\ \theta^{(3)}x_k^{(1)} + \theta^{(4)}m_k \end{bmatrix}, \quad h_\theta(x_k, m_k) = x_k^{(1)} \tag{5.55}$$

Dans cet exemple, l'identifiabilité du vecteur de paramètres $[\theta^{(1)} \quad \theta^{(2)} \quad \theta^{(3)} \quad \theta^{(4)}]^T$ $(l = 4)$ est testée uniquement avec l'approche basée sur la relation entrée/sortie. L'élimination du vecteur d'état est effectuée avec l'approche basée sur les bases de Gröbner.
Comme $x_k^{(2)}$ n'est pas directement transmis, il est choisi comme étant le plus grand et l'ordre lexicographique correspondant est :

$$x_k^{(1)} < x_k^{(2)} \tag{5.56}$$

L'indice d'observabilité du système (5.54) est égal à la dimension du système, $n = 2$. En effet, on a :

$$\text{rang} \begin{bmatrix} \dfrac{\partial h_\theta(x_k)}{\partial x_k^{(1)}} & \dfrac{\partial h_\theta(x_k)}{\partial x_k^{(2)}} \\ \dfrac{\partial (h_\theta \circ f_\theta)(x_k)}{\partial x_k^{(1)}} & \dfrac{\partial (h_\theta \circ f_\theta)(x_k)}{\partial x_k^{(2)}} \end{bmatrix} = \text{rang} \begin{bmatrix} 1 & 0 \\ 2\theta^{(1)}x_k & \theta^{(2)} \end{bmatrix} = 2,$$

$$\text{rang} \begin{bmatrix} \dfrac{\partial h_\theta(x_k)}{\partial x_k^{(1)}} & \dfrac{\partial h_\theta(x_k)}{\partial x_k^{(2)}} \\ \dfrac{\partial (h_\theta \circ f_\theta)(x_k)}{\partial x_k^{(1)}} & \dfrac{\partial (h_\theta \circ f_\theta)(x_k)}{\partial x_k^{(2)}} \\ \dfrac{\partial (h_\theta \circ f_\theta^2)(x_k)}{\partial x_k^{(1)}} & \dfrac{\partial (h_\theta \circ f_\theta^2)(x_k)}{\partial x_k^{(2)}} \end{bmatrix} =$$

$$\text{rang} \begin{bmatrix} 1 & 0 \\ 2\theta^{(1)}x_k & \theta^{(2)} \\ 4(\theta^{(1)})^2 x_k^{(1)}(\theta^{(1)}(x_k^{(1)})^2 + m_k + \theta^2 x_k^{(2)}) + \theta^{(2)}\theta^{(3)} & 2\theta^{(1)}\theta^{(2)}(\theta^{(2)}x_k^{(2)} + m_k + \theta^{(1)}(x_k^{(1)})^2) \end{bmatrix} = 2 \tag{5.57}$$

Pour obtenir la relation entrée/sortie $\mathcal{L}_1 = 0$, le système (5.54) est itéré une fois :

$$\begin{cases} x_{k+1}^{(1)} - \theta^{(1)}(x_k^{(1)})^2 - \theta^{(2)}x_k^{(2)} - m_k = 0 \\ x_{k+2}^{(1)} - \theta^{(1)}(x_{k+1}^{(1)})^2 - \theta^{(2)}x_{k+1}^{(2)} - m_{k+1} = 0 \\ x_{k+1}^{(2)} - \theta^{(3)}x_k^{(1)} - \theta^{(4)}m_k = 0 \\ x_{k+2}^{(2)} - \theta^{(3)}x_{k+1}^{(1)} - \theta^{(4)}m_{k+1} = 0 \\ y_k - x_k^{(1)} = 0 \\ y_{k+1} - x_{k+1}^{(1)} = 0 \\ y_{k+2} - x_{k+2}^{(1)} = 0 \end{cases} \tag{5.58}$$

Le logiciel Maxima calcule, avec la fonction `poly_buchberger`, la base de Gröbner de l'idéal associé au système (5.58), avec l'ordre lexicographique (5.56). Une des expressions de la base de Gröbner est la relation entrée/sortie recherchée (5.27) :

$$\theta^{(1)}y_{k+1}^2 + \theta^{(2)}\theta^{(3)}y_k - y_{k+2} + m_{k+1} + \theta^{(2)}\theta^{(4)}m_k = 0 \tag{5.59}$$

Les autres expressions de la base ne présentent pas d'intérêt pour notre étude car elles contiennent le vecteur d'état interne. Puis, la relation entrée/sortie (5.59) est itérée $l - 1 = 3$ fois, ce qui conduit à $\mathcal{L}_2 = 0$, $\mathcal{L}_3 = 0$ et $\mathcal{L}_4 = 0$, respectivement :

$$\begin{array}{l} \theta^{(1)}y_{k+2}^2 + \theta^{(2)}\theta^{(3)}y_{k+1} - y_{k+3} + m_{k+2} + \theta^{(2)}\theta^{(4)}m_{k+1} = 0 \\ \theta^{(1)}y_{k+3}^2 + \theta^{(2)}\theta^{(3)}y_{k+2} - y_{k+4} + m_{k+3} + \theta^{(2)}\theta^{(4)}m_{k+2} = 0 \\ \theta^{(1)}y_{k+4}^2 + \theta^{(2)}\theta^{(3)}y_{k+3} - y_{k+5} + m_{k+4} + \theta^{(2)}\theta^{(4)}m_{k+3} = 0 \end{array} \tag{5.60}$$

L'ensemble d'équations (5.59) et (5.60) ne peut pas être réécrit sous la forme (5.24), excepté pour le paramètre $\theta^{(1)}$:

$$P_1(y_k, \ldots, y_{k+5}, m_k, \ldots, m_{k+4})\theta^{(1)} - Q_1(y_k, \ldots, y_{k+5}, m_k, \ldots, m_{k+4}) = 0 \tag{5.61}$$

avec :

$$\begin{array}{l} P_1(y_k, \ldots, y_{k+5}, m_k, \ldots, m_{k+4}) = \\ -m_k y_{k+1} y_{k+3}^2 + m_{k+1} y_k y_{k+3}^2 + m_k y_{k+2}^3 - m_{k+2} y_k y_{k+2}^2 - m_{k+1} y_{k+1}^2 y_{k+2} + m_{k+2} y_{k+1}^3 \\ \\ Q_1(y_k, \ldots, y_{k+5}, m_k, \ldots, m_{k+4}) = \\ -(y_{k+1}(m_k(y_{k+4} - m_{k+3}) + m_{k+1}m_{k+2}) + y_k(m_{k+1}(m_{k+3} - y_{k+4}) + m_{k+2}y_{k+3} - m_{+2}^2) \\ +y_{k+2}(m_k(m_{k+2} - y_{k+3}) - m_{k+2}y_{k+1} - m_{k+1}^2) + m_{k+1}y_{k+2}^2) \end{array} \tag{5.62}$$

Conclusion

Les relations (5.26) sont uniquement satisfaites pour $\theta^{(1)}$ et seul $\theta^{(1)}$ est identifiable. Dans le contexte d'une attaque brute, il pourrait jouer le rôle de clé secrète, contrairement aux autres paramètres $\theta^{(2)}$, $\theta^{(3)}$ et $\theta^{(4)}$ pour lesquels plusieurs paires $(\theta^{(2)}, \theta^{(3)})$ ou $(\theta^{(2)}, \theta^{(4)})$ vérifient les relations (5.59) et (5.60).

En revanche, selon (5.24) et ici (5.61), il est clair qu'en effectuant une attaque à texte clair choisi, le paramètre $\theta^{(1)}$ peut facilement être reconstruit avec P_1 et Q_1 (5.62). Par conséquent, $\theta^{(1)}$ ne peut finalement pas jouer le rôle de clé secrète.

5.7.3 Exemple 3

Considérons le cryptosystème chaotique, inspiré de [Papadimitriou et al., 2001], qui obéit, côté émetteur, à :

$$\begin{cases} x_{k+1}^{(1)} &= \theta^{(1)} x_k^{(1)}(1-x_k^{(1)}) + m_k \\ x_{k+1}^{(2)} &= \theta^{(1)} x_k^{(3)}(1-x_k^{(3)}) + \theta^{(2)} x_k^{(1)} + \theta^{(3)} x_k^{(2)} + \theta^{(4)} x_k^{(3)} \\ x_{k+1}^{(3)} &= \theta^{(5)} x_k^{(2)} \\ y_k &= x_k^{(2)} \end{cases} \tag{5.63}$$

Le système (5.63) est de la forme (5.2), avec :

$$\begin{aligned} f_\theta(x_k, m_k) &= \begin{bmatrix} \theta^{(1)} x_k^{(1)}(1-x_k^{(1)}) + m_k \\ \theta^{(1)} x_k^{(3)}(1-x_k^{(3)}) + \theta^{(2)} x_k^{(1)} + \theta^{(3)} x_k^{(2)} + \theta^{(4)} x_k^{(3)} \\ \theta^{(5)} x_k^{(2)} \end{bmatrix}, \\ h_\theta(x_k, m_k) &= x_k^{(2)} \end{aligned} \tag{5.64}$$

Dans la suite, l'identifiabilité du vecteur de paramètres $[\theta^{(1)} \quad \theta^{(2)} \quad \theta^{(3)} \quad \theta^{(4)} \quad \theta^{(5)}]^T$ $(l = 5)$ est testée uniquement avec l'approche basée sur la relation entrée/sortie.

Les états $x_k^{(1)}$ et $x_k^{(3)}$ ne sont pas directement transmis à travers y_k. Nous pouvons tout aussi bien choisir l'état $x_k^{(1)}$ que $x_k^{(3)}$ pour être le plus grand dans l'ordre lexicographique. $x_k^{(3)}$ est choisi le plus grand dans l'ordre lexicographique suivant :

$$x_k^{(2)} < x_k^{(1)} < x_k^{(3)} \tag{5.65}$$

Pour obtenir la relation entrée/sortie, le système (5.63) est itéré jusqu'à son indice d'observabilité qui est aussi sa dimension $(s = n = 3)$. Puis, la base de Gröbner de l'idéal associé au système (5.63) est calculée, avec l'ordre lexicographique (5.65). Ce calcul peut être effectué avec, par exemple, le logiciel Maxima et sa fonction `poly_buchberger`. Une des expressions de cette base est la relation entrée/sortie :

$$\begin{aligned} &-\theta^{(1)}(\theta^{(5)})^4 y_k^4 + 2(\theta^{(1)})^2(\theta^{(5)})^3(\theta^{(1)} + \theta^{(4)}) y_k^3 \\ &+\theta^{(1)}(\theta^{(5)})^2(-(\theta^{(4)})^2 - 2\theta^{(1)}\theta^{(4)} + \theta^{(1)}\theta^{(2)} - (\theta^{(1)})^2) y_k^2 \\ &+\theta^{(1)}\theta^{(2)}\theta^{(5)}(\theta^{(4)} - \theta^{(1)}) y_k + \theta^{(2)}(\theta^{(4)}\theta^{(5)} + \theta^{(1)}\theta^{(5)} \\ &-\theta^{(1)}\theta^{(3)}) y_{k+1} - \theta^{(1)}(\theta^{(2)}(\theta^{(5)})^2 + (\theta^{(3)})^2) y_{k+1}^2 \\ &-2\theta^{(1)}\theta^{(3)}\theta^{(5)}(\theta^{(4)} + \theta^{(1)} y_k y_{k+1} + 2(\theta^{(1)})^2\theta^{(3)}(\theta^{(5)})^2 y_k^2 y_{k+1} \\ &+\theta^{(2)}(\theta^{(3)} + \theta^{(1)}) y_{k+2} - \theta^{(1)} y_{k+2} \\ &+2\theta^{(1)}\theta^{(5)}(\theta^{(4)} + \theta^{(1)}) y_k y_{k+2} - 2(\theta^{(1)})^2(\theta^{(5)})^2 y_k^2 y_{k+2} \\ &+2\theta^{(1)}\theta^{(3)} y_{k+1} y_{k+2} - \theta^{(1)} y_{k+1}^2 - \theta^{(2)} y_{k+3} + (\theta^{(2)})^2 m_{k+1} = 0 \end{aligned} \tag{5.66}$$

Puis, la relation entrée/sortie (5.66) est itérée, ce qui conduit à $\mathcal{L}_i = 0$, $i = 2, \ldots, 5$. A partir de $\mathcal{L}_i = 0$, $i = 1, \ldots, 5$, cinq expressions de la forme $P_i(y_k, \ldots, y_{k+7}, m_k, \ldots, m_{k+7})\theta^{(i)} - Q_i(y_k, \ldots, y_{k+7}, m_k, \ldots, m_{k+7}) = 0$, qui ne sont pas données ici pour des raisons de simplicité, peuvent être obtenues avec succès, en dépit de la complexité apparente de (5.66). Les polynômes P_i et Q_i, $i = 1, 2, 3, 4, 5$, ont été calculés avec Maxima (fonction `solve`). Par conséquent, les paramètres $\theta^{(1)}$, $\theta^{(2)}$, $\theta^{(3)}$, $\theta^{(4)}$ et $\theta^{(5)}$ sont identifiables.

Dans le contexte d'une attaque brute, comme les paramètres sont identifiables, ils pourraient

jouer le rôle de clé secrète. Cependant, il est clair qu'en effectuant une attaque à texte clair choisi, ils peuvent être facilement reconstruits. En conclusion, les paramètres $\theta^{(1)}$, $\theta^{(2)}$, $\theta^{(3)}$, $\theta^{(4)}$ et $\theta^{(5)}$ ne peuvent pas jouer le rôle de clé secrète.

5.7.4 Conclusion

Du point de vue de la cryptanalyse paramétrique, les conclusions suivantes peuvent être tirées.

Si le vecteur de paramètres est identifiable, il est plus difficile pour un adversaire de trouver la valeur des paramètres par une attaque brute. En effet, la probabilité de trouver la valeur des paramètres est la plus faible. Par conséquent, le vecteur de paramètres pourrait être un bon candidat pour jouer le rôle de clé secrète contre une attaque brute.
Si le vecteur de paramètres n'est pas identifiable, l'adversaire a une probabilité plus importante de trouver une des valeurs par une attaque brute, puisqu'il existe plusieurs valeurs possibles. Par conséquent, ce vecteur de paramètres est un mauvais candidat pour jouer le rôle d'une clé secrète contre une attaque brute.

Si une expression explicite, dépendant uniquement des quantités connues, peut être établie facilement pour chaque paramètre, l'adversaire est capable de récupérer les paramètres et par conséquent la clé secrète. Dans le cas d'une attaque à texte clair choisi, les quantités connues sont l'entrée, la sortie et leurs itérés. Dans ce contexte, la récupération des paramètres peut toujours être effectuée facilement d'un point de vue calculatoire, pour des cryptosystèmes présentant des non linéarités de type polynomial.

En conclusion, les cryptosystèmes impliquant des non linéarités polynomiales sont faibles contre des attaques algébriques. On peut noter que cette faiblesse est indépendante du comportement exhibé par le système, chaotique ou non.

Conclusion

Le travail développé dans ce mémoire a porté sur la synthèse et la cryptanalyse des schémas de chiffrement basés sur le chaos. Il s'est articulé autour de trois axes principaux : la comparaison du chiffrement par inclusion avec le chiffrement par flot, le problème de la reconstruction de l'information côté récepteur pour la modulation chaotique et la modulation paramétrique et la robustesse du chiffrement par inclusion face à des attaques pirates.
Dans un premier temps, quelques rappels sur les systèmes dynamiques non linéaires autonomes, en particulier ceux exhibant un comportement chaotique, et sur la stabilité des systèmes LPV ont été effectués.
Puis, une étude comparative a porté sur les structures des émetteurs et des récepteurs du chiffrement par inclusion et du chiffrement par flot. Il apparaît que le chiffrement par inclusion est un "mélange" du chiffrement par flot autosynchrone avec celui synchrone. Le chiffrement par inclusion présente l'avantage du chiffrement par flot autosynchrone (resynchronisation automatique) sans avoir l'inconvénient du chiffrement par flot synchrone (perte de synchronisation).
Pour la modulation chaotique, une méthode systématique de synthèse d'observateurs polytopiques a été proposée, afin de réduire le conservatisme des conditions de stabilité de l'erreur de reconstruction d'état. La plupart des systèmes chaotiques pouvant se réécrire sous forme LPV polytopique, la méthode proposée est basée sur la recherche du polytope minimal englobant les paramètres variants. Cet observateur permet de prendre en compte la spécificité liée au chaos.
Dans le cas de la modulation paramétrique, la reconstruction de l'information nécessite l'estimation simultanée du vecteur d'état et des paramètres modulés, côté récepteur. Nous avons proposé un observateur adaptatif polytopique pour jouer le rôle du récepteur.
Enfin, la cryptanalyse du chiffrement par inclusion a été effectuée. Nous avons proposé une méthode systématique pour déterminer si les paramètres du système chaotique peuvent jouer le rôle de clé secrète. Pour cela, une approche basée sur le concept de l'identifiabilité paramétrique a été élaborée. Un résultat fondamental de ces travaux est que les cryptosystèmes chaotiques présentant des non linéarités polynomiales sont faibles devant les attaques algébriques. En effet, il a été ainsi montré que les paramètres identifiables peuvent facilement être reconstruits par des attaques algébriques. Il en découle que la robustesse du chiffrement par inclusion ne repose pas sur le caractère chaotique du cryptosystème.

Pour ces travaux, des concepts et des méthodes de l'Automatique ont été utilisés pour une application originale, le chiffrement. Ces méthodes peuvent également être employées ou adaptées à d'autres applications, dont quelques exemples sont présentés ici.
La reconstruction d'état d'un système à l'aide d'observateurs est une étape importante qui intervient dans le domaine du diagnostic. Par ailleurs, les résultats obtenus pour l'observation des systèmes LPV peuvent être appliqués, par dualité, à la commande de ces systèmes.
Le concept d'identifiabilité est employé pour la modélisation des systèmes. La modélisation intervient fréquemment en biologie ou en chimie. La modélisation consiste à proposer une loi

d'évolution pour un système (choix des grandeurs d'état, des paramètres, ...). Le problème est alors de déterminer un ensemble de valeurs pour les paramètres inconnus du modèle. Avant d'identifier ou d'estimer ces paramètres, il faut s'assurer que cela est possible, c'est-à-dire qu'ils sont identifiables.
La recherche de l'enveloppe convexe d'un ensemble fini de points possède de nombreuses applications dans les domaines de la programmation linéaire, de la reconnaissance de formes, du traitement d'images, de la robotique (planification de trajectoire), ...
La triangulation de Delaunay, empruntée aux Mathématiques, est utilisée, en général, pour générer le maillage d'un domaine. La génération de maillage intervient dans la reconstruction de surface à partir de données partielles dont les applications sont multiples. Par exemple, en médecine, on cherche à reconstruire des modèles tri-dimensionnels des organes à partir de coupes obtenues par un scanner. En géologie, on cherche à reconstruire la structure du sous-sol à partir de mesures sismiques, ...

Le travail réalisé dans ce mémoire ne constitue pas une fin en soi, mais s'ouvre vers des contributions futures. Quelques idées sont listées de façon non exhaustive, ci-dessous.

Le chiffrement par inclusion et le chiffrement par flot présentent des points communs au niveau des structures de leurs émetteurs et de leurs récepteurs. Cependant, ces deux modes de chiffrement révèlent une différence fondamentale. Le chiffrement basé sur le chaos utilise des flots de clés réelles, contrairement au chiffrement usuel qui utilise des flots de clés binaires. Un point important qui n'a pas été abordé ici est celui des effets de la troncature dus à une implémentation machine de ces générateurs chaotiques. Théoriquement, un générateur chaotique produit des séquences apériodiques dans un ensemble compact. Lorsque ces générateurs sont implémentés sur une machine à précision finie, les séquences ne sont plus réellement chaotiques. En effet, comme l'ensemble dans lequel x_k prend ses valeurs devient fini, les séquences vont évoluer dans un cycle de période finie. Il faudrait alors étudier les conséquences de cette troncature sur les propriétés du générateur implémenté. On pourrait, par exemple, examiner la longueur de la période (élevée ou non, limite acceptable). On pourrait aussi tester si la distribution des séquences reste proche de la distribution uniforme comme pour un générateur pseudo-aléatoire. En d'autres termes, il faudrait s'assurer que le générateur tronqué peut encore jouer le rôle d'un générateur pseudo-aléatoire.

En cryptographie usuelle, pour définir la qualité d'un générateur pseudo-aléatoire, des tests statistiques sont effectués : test de fréquence (il consiste à déterminer si le nombre de "0" et le nombre de "1" sont approximativement identiques dans une séquence donnée), test d'autocorrélation (il consiste à tester la corrélation entre une séquence donnée et la même séquence mais décalée), ... Il conviendrait d'effectuer ou d'adapter ces tests aux générateurs chaotiques utilisant des flots de clé réelles pour discuter de leur qualité de générateur pseudo-aléatoire.

La faiblesse du chiffrement par inclusion face à des attaques algébriques a été prouvée. Néanmoins, d'autres points restent à étudier sur ce schéma.
Tout d'abord, l'effet de l'injection de l'information sur le caractère chaotique du système n'a pas été analysé. En effet, on peut montrer qu'un système non linéaire autonome est chaotique (fonctions topologiquement conjuguées, exposants de Lyapunov). En revanche, il est plus difficile de savoir si le système conserve son caractère chaotique lorsqu'une information est injectée. Ce problème ne semble pas avoir été abordé dans la littérature. Une solution pourrait être de tester si la dynamique non autonome est topologiquement conjuguée à la dynamique chaotique

autonome. Il conviendrait également d'étudier les propriétés du générateur associé et de s'assurer qu'elles vérifient celles requises par les générateurs pseudo-aléatoires.
Ensuite, concernant la cryptanalyse du chiffrement par inclusion, seule une attaque algébrique a été réalisée. Comme en cryptographie usuelle, il serait judicieux de lister toutes les autres attaques nécessaires à réaliser pour attester la robustesse d'un cryptosystème chaotique.
Par ailleurs, la faiblesse du chiffrement par inclusion étant révélée, il faut, à présent, s'attacher à trouver des solutions pour améliorer la robustesse de ce schéma. Une solution qui peut être envisagée est d'ajouter un module de préchiffrement e de l'information. La fonction de préchiffrement dépend du vecteur d'état interne et de l'information à masquer. Le résultat u_k de ce préchiffrement est ensuite injecté dans la dynamique chaotique au lieu de l'information elle-même. Le système émetteur devient alors :

$$\begin{cases} x_{k+1} = f_\theta(x_k, u_k) \\ u_k \quad = e(x_k, m_k) \\ y_k \quad = h_\theta(x_k, u_k) \end{cases} \tag{67}$$

Le problème est de déterminer cette fonction de préchiffrement e. Si e est polynomiale, on peut alors remplacer u_k par son expression $e(x_k, m_k)$ dans les fonctions f_θ et h_θ et effectuer une attaque algébrique. On procède à l'élimination de x_k et les paramètres identifiables peuvent être reconstruits par une attaque à texte clair connu. Par conséquent, la fonction de préchiffrement ne peut pas être polynomiale, mais il reste à la déterminer afin de garantir la robustesse du cryptosystème face à des attaques algébriques et à d'autres attaques.
Il serait également pertinent d'étudier la complexité de l'attaque algébrique proposée en fonction du degré des polynômes du cryptosystème. En effet, il pourrait être testé si l'augmentation de ce degré entraîne une augmentation significative de la complexité de l'attaque. Peut-être est-il ainsi possible de formuler des hypothèses sur le degré des polynômes afin d'obtenir une complexité telle que le cryptosystème soit considéré comme sûr face à cette attaque.
Une autre possibilité est d'utiliser des systèmes chaotiques qui présentent des non linéarités plus complexes que celles polynomiales. Il faut alors déterminer le type de non linéarités qui peut convenir et vérifier s'il existe des méthodes d'élimination de variable dans le cas non polynomial.

Un point particulier qui concerne l'identifiabilité paramétrique est le choix des approches d'élimination de variables (bases de Gröbner, ensemble caractéristique, résultant). Des comparaisons ont déjà été effectuées dans la littérature. Ces travaux aboutissent à la conclusion qu'aucune approche n'est plus performante que l'autre, tout dépendant de la structure et de la complexité du système. Partant de cette constatation, peut-être est-il possible de dresser une liste de classes de systèmes pour lesquelles une approche s'avère plus performante que les autres. Il serait intéressant d'étudier l'évolution de la complexité des algorithmes en fonction de la dimension et de la structure du système. Cela permettrait d'évaluer les ressources matérielles nécessaires pour un adversaire et éventuellement de construire des systèmes plus complexes.

Par ailleurs, il conviendrait d'effectuer la cryptanalyse des autres schémas de chiffrement basés sur le chaos comme la modulation chaotique et la modulation paramétrique, ce qui n'a pas été abordé ici. En revanche, concernant la cryptanalyse paramétrique de ces schémas, l'approche basée sur l'identifiabilité, proposée dans ces travaux pour le chiffrement par inclusion, peut directement être transposée.

Le problème de la synthèse et de la cryptanalyse des schémas de chiffrement restera toujours un problème ouvert. Les technologies informatiques (ressources mémoires, processeurs, ...) évo-

luant constamment, elles permettent une analyse plus poussée de la robustesse des schémas de chiffrement et obligent donc de concevoir des schémas de plus en plus sophistiqués.

Nomenclature

$\bar{J}(.)$	Critère à minimiser
$\bar{x}_k$	Vecteur d'état étendu $\bar{x}_k = \begin{bmatrix} x_k \\ \theta \end{bmatrix}$
δ	Distance
ϵ_k	Erreur de reconstruction d'état
exp(.)	Fonction exponentielle
$\hat{m}_k$	Signal information reconstruit
$\hat{x}_k$	Vecteur d'état estimé d'un système dynamique en temps discret
$\hat{y}_k$	Vecteur de sortie estimé d'un système dynamique en temps discret
λ, λ_i	Valeur propre, ième valeur propre
λ_L	Exposant de Lyapunov
ln(.)	Logarithme népérien
$\mathbb{A}$	Anneau de polynômes, $\mathbb{A} = \mathbb{R}[x_k^{(1)}, \ldots, x_k^{(n)}]$
$\mathbb{C}$	Ensemble des complexes
$\mathbb{R}$	Ensemble des nombres réels
$\mathbb{Z}$	Ensemble des entiers
$\mathbf{0}_n$	Matrice nulle de dimension n
$\mathbf{1}_n$	Matrice identité de dimension n
$\mathcal{A}(\rho_k)$	Matrice dynamique à description polytopique
$\mathcal{D}$	Bassin d'attraction
$\mathcal{D}_\rho^*$	Polytope minimal auquel appartient ρ_k
$\mathcal{D}_\mathcal{A}$	Polytope auquel appartient $\mathcal{A}$
$\mathcal{D}_\rho$	Polytope auquel appartient ρ_k
$\mathcal{G}$	Base de Gröbner d'un idéal
$\mathcal{L}(\rho_k)$, $\bar{\mathcal{L}}(\rho_k)$	Gains d'un observateur polytopique
$\mathcal{M}$	Ensemble des entrées m_k

$\mathcal{P}_k$	Matrice définie positive à temps variant, $\mathcal{P}_k = \sum_{i=1}^{N} \xi_k^{(i)} P_i$
$\mathcal{X}$	Ensemble des états x_k
$\mathcal{Y}$	Ensemble des sorties y_k
Ω	Attracteur chaotique
Ω_ρ	Ensemble compact auquel appartient ρ_k
ρ_k	Vecteur des paramètres variant d'un système à description polytopique
ρ_{o_i}	Sommets du polytope $\mathcal{D}_\rho$
Σ_θ	Système dynamique dépendant du vecteur de paramètres θ
Θ	Ensemble des paramètres θ d'un système dynamique
$\theta^{(i)}$	ième composante du vecteur des paramètres d'un système chaotique
$\|\|x_k\|\|$	Norme euclidienne $\sqrt{x_k^T x_k}$ du vecteur x_k
A, A_θ	Matrice dynamique
$A^{(i)}$ ($\bar{A}^{(i)}$)	Sommets du polytope $\mathcal{D}_\mathcal{A}$ ($\mathcal{D}_{\bar{\mathcal{A}}}$)
B, B_θ	Matrice de commande
C, C_θ	Matrice d'observation
c_k	Texte chiffré
d	Fonction de déchiffrement
e	Fonction de chiffrement
F^{-1}	Inverse de la matrice F
F^T	Transposée de la matrice F
f_θ, h_θ, g_θ	Transformations ponctuelles associées à un système dynamique
F_i, G_i	Matrices inconnues d'une LMI
I	Idéal de polynômes
j	Variable complexe, $j^2 = -1$
$J_i(.)$	Matrice jacobienne
k	Temps discret
L	Dimension du vecteur ρ_k
l	Dimension du vecteur des paramètres
M	Matrice de Sylvester
m	Dimension du vecteur de commande
m_k	Signal information ou texte clair
N	Nombre de sommets d'un polytope

n	Dimension d'un système dynamique
p	Dimension du vecteur de sortie
P, P_i	Matrices définies positives
R	Résultant de deux polynômes
S	Ensemble convexe $\{\mu_k \in \mathbb{R}^N, \quad \mu_k = [\mu_k^{(1)} \dots \mu_k^{(N)}], \quad \mu_k^{(i)} \geq 0, \quad i = 1, \dots, N, \quad \sum_{i=1}^{N} \mu_k^{(i)} = 1\}$
s	Indice d'observabilité
t	Temps continu
V	Fonction de Lyapunov
$v(\theta)$	Voisinage de θ
$x(t)$	Vecteur d'état d'un système dynamique en temps continu
x^*	Point d'équilibre
x_k	Vecteur d'état d'un système dynamique en temps discret
$x_k^{(i)}$	ième composante du vecteur d'état d'un système dynamique en temps discret
y_k	Vecteur de sortie d'un système dynamique en temps discret

Annexe A

Définitions

Définition 28. Soit $f : \mathbb{R}^n \to \mathbb{R}^m$ une fonction vectorielle :

$$f(x) = \begin{bmatrix} f_1(x^{(1)}, \ldots, x^{(n)}) \\ f_2(x^{(1)}, \ldots, x^{(n)}) \\ \vdots \\ f_m(x^{(1)}, \ldots, x^{(n)}) \end{bmatrix} \tag{A.1}$$

La matrice jacobienne J_i est la matrice des dérivées partielles du premier ordre de la fonction vectorielle f au point x_i :

$$J_i = \begin{bmatrix} \frac{\partial f_1(x)}{\partial x^{(1)}} & \cdots & \frac{\partial f_1(x)}{\partial x^{(n)}} \\ \vdots & \vdots & \vdots \\ \frac{\partial f_m(x)}{\partial x^{(1)}} & \cdots & \frac{\partial f_m(x)}{\partial x^{(n)}} \end{bmatrix} \Bigg|_{x=x_i} \tag{A.2}$$

Définition 29. Un espace métrique (X, δ) est un ensemble X muni d'une fonction $\delta : X \times X \to \mathbb{R}$, appelée distance, telle que, pour tout $x, y, z \in X$:

$$\begin{aligned} &\bullet\ \delta(x, y) \geq 0 \\ &\bullet\ \delta(x, y) = 0 \Leftrightarrow x = y \\ &\bullet\ \delta(x, y) = \delta(y, x) \\ &\bullet\ \delta(x, z) \leq \delta(x, y) + \delta(y, z) \end{aligned} \tag{A.3}$$

Définition 30. Un ensemble U est *ouvert* si pour tout point $x \in U$, il existe $\epsilon > 0$ tel que l'intervalle $[x - \epsilon; x + \epsilon]$ est contenu dans U.
Un ensemble F est *fermé* si le complément de F est ouvert.

Définition 31. Un sous-ensemble F de $\mathbb{R}^n$ fermé et borné est dit *compact*.

Définition 32. Soient F et X deux ensembles. F est dense dans X si F est inclus dans X et si pour tout point $x \in X$, chaque voisinage de x contient au moins un point de F.

Lemme 2. [Complément de Schur]

$$\begin{bmatrix} Q & S \\ S^T & R \end{bmatrix} > 0 \tag{A.4}$$

avec $Q = Q^T$ et $R = R^T$, est équivalent à :

$$R > 0 \quad \text{et} \quad Q - SR^{-1}S^T > 0 \tag{A.5}$$

ou

$$Q > 0 \quad \text{et} \quad R - S^TQ^{-1}S > 0 \tag{A.6}$$

Définition 33. Une matrice $A \in \mathbb{R}^{n\times n}$ est appelée matrice de Hurwitz si toutes ses valeurs propres ont leur partie réelle négative.

Définition 34. Soient E et F deux sous-ensembles ouverts de $\mathbb{R}^n$. Une fonction $f : E \to F$ est appelée *difféomorphisme* si :
- f est dérivable,
- f est bijective,
- l'inverse de f, f^{-1}, est dérivable.

Définition 35. Soient I un intervalle de $\mathbb{R}$, $f : I \to \mathbb{R}$ une fonction et n un entier naturel non nul. La fonction f est dite de *classe* C^n, ou n fois continuement dérivable, sur I si elle est n fois dérivable sur I et si la fonction $f^{(n)}$ est continue sur I.
La fonction f est dite de *classe* C^0 sur I si elle est continue sur I.

Définition 36. Soit le système décrit par :

$$\begin{cases} \dot{x}(t) = Ax(t) + Bm(t) \\ y(t) = Cx(t) \end{cases} \tag{A.7}$$

où $x(t) \in \mathbb{R}^n$, $m(t) \in \mathbb{R}^m$ et $y(t) \in \mathbb{R}^p$.
La fonction de transfert de ce système est :

$$W(\lambda) = C(\lambda \mathbf{1}_n - A)^{-1}B \tag{A.8}$$

où $\lambda \in \mathbb{C}$.
Le système (A.7) est dit minimum phase si le polynôme $\varphi(\lambda) = \det(\lambda \mathbf{1}_n - A)\det W(\lambda)$ a toutes ses racines ayant leur partie réelle négative.
Le système (A.7) est dit hyper minimum phase s'il est minimum phase et si la matrice $CB = \lim_{\lambda\to\infty} W(\lambda)$ est symétrique définie positive.

Définition 37. Une fonction $f : \mathbb{R} \to \mathbb{R}$ est une *fonction de Lipschitz* si :

$$|f(x) - f(y)| \leq c|x - y|, \quad \forall x, \forall y \tag{A.9}$$

où $c \in \mathbb{R}$ est une constante.

Définition 38. Un corps F est un anneau commutatif, muni de l'identité, tel que :
- $1 \neq 0$,
- Si $a \in F$, $a \neq 0$, alors il existe $b \in F$, tel que $a \times b = 1$.

Définition 39. Un corps différentiel est un corps F muni de l'opération de dérivation $\dot{(.)} : F \to F$. La dérivation doit satisfaire les deux propriétés suivantes :
- Additivité : $\dot{(a + b)} = \dot{a} + \dot{b}$
- Règle de Leibniz : $\dot{ab} = a\dot{b} + \dot{a}b$

Définition 40. Soit $U \subset \mathbb{C}$ un sous-ensemble de l'ensemble des complexes $\mathbb{C}$. Une fonction $f : U \to \mathbb{C}$ est holomorphe si f a une dérivée complexe en chaque point $z_0 \in U$, c'est-à-dire si :

$$\lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0} \tag{A.10}$$

existe $\forall z_0 \in U$.

Définition 41. Soit $U \subset \mathbb{C}$ un sous-ensemble de l'ensemble des complexes $\mathbb{C}$. Une fonction $f : U \to \mathbb{C}$ est méromorphe si elle est holomorphe sur U sauf sur un ensemble de points qui sont des pôles pour f.

Annexe B

Rappels d'algèbre

Cette annexe contient les définitions d'algèbre nécessaires pour décrire les approches d'élimination de variables utilisées dans le Chapitre 5, l'approche par les bases de Gröbner, l'approche basée sur l'ensemble caractéristique et celle basée sur le résultant de deux polynômes.

Quelques notions d'algèbre différentielle peuvent être trouvées dans [Kolchin, 1973] pour les systèmes à temps continu. Cependant, ces notions peuvent tout aussi bien être définies avec l'opérateur de dérivation (cas du temps continu) qu'avec l'opérateur de différence (cas du temps discret). La plupart des définitions rappelées ici est extraite d'un cours sur la résolution des systèmes de F. Boulier, disponible en ligne à `http ://www.lifl.fr/~boulier`.

B.1 Bases de Gröbner

Définition 42. Un *anneau* est un triplet $(\mathbb{A}, +, \times)$ tel que :
- $\mathbb{A}$ est un ensemble.
- $+$ est une loi de composition interne associative qui admet un élément neutre et un inverse ($(\mathbb{A}, +)$ est un groupe commutatif).
- $\times$ est une loi de composition interne associative et distributive par rapport à $+$.

Par exemple, l'ensemble des rationnels muni de l'addition (pour $+$) et de la multiplication (pour $\times$) est un anneau.

Définition 43. L'anneau des polynômes, noté $\mathbb{A} = \mathbb{R}[x_k^{(1)}, \ldots, x_k^{(n)}]$, est l'ensemble des polynômes dont l'ensemble des indéterminées est $\{x_k^{(1)}, \ldots, x_k^{(n)}\}$ et dont les coefficients sont des réels. Sa loi de composition $+$ est l'addition et sa loi de composition $\times$ est la multiplication.

Définition 44. Un *idéal de polynômes* est un sous-ensemble I de $\mathbb{A}$, tel que :
- $\forall r \in I, \quad \forall q \in I, \quad r + q \in I,$
- $\forall r \in I, \quad \forall q \in \mathbb{A}, \quad r \times q \in I.$

Dans la suite, par abus de langage, par *idéal*, on entend idéal de polynômes.

Exemple 2. L'ensemble $I = \{0\}$ est un idéal de $\mathbb{A}$. En effet, $0+0 = 0$ appartient à I et $0 \times a = 0$ appartient toujours à I, quel que soit $a \in \mathbb{A}$.
L'ensemble des nombres pairs est un idéal de $\mathbb{Z}$. En effet, la somme de deux nombres pairs est un nombre pair et le produit d'un nombre pair avec n'importe quel entier est encore un nombre pair.

Exemple 3. Dans $\mathbb{Z}$, l'idéal généré par 5 est l'ensemble des entiers multiples de 5 :
$I = \{0, -5, 5, -10, 10, -15, 15, \ldots\}$.

Définition 45. Un *ordre lexicographique* des variables $x_k^{(1)}, \ldots, x_k^{(n)}$, noté $<$, est un ordre total portant sur le nom des variables et de leurs itérés, tel que, $\forall i = 1, \ldots, n$, $\forall j = 1, \ldots, n$:

$$\begin{aligned} &- \quad x_k^{(i)} < x_{k+l}^{(i)}, && \forall l \in \mathbb{N} \\ &- \quad x_k^{(i)} < x_l^{(j)} \Rightarrow x_{k+t}^{(i)} < x_{l+t}^{(j)}, && \forall l \in \mathbb{N}, \quad \forall t \in \mathbb{N} \\ &- \quad x_k^{(i)} < x_k^{(j)} \Rightarrow (x_k^{(i)})^\alpha < (x_k^{(j)})^\beta, && \forall \alpha \in \mathbb{N}, \quad \forall \beta \in \mathbb{N} \end{aligned} \tag{B.1}$$

Il existe plusieurs ordres lexicographiques différents. En fait, il en existe un différent pour chaque permutation de variables dans l'ordre.

Définition 46. Pour un ordre donné de $\{x_k^{(1)}, \ldots, x_k^{(n)}\}$ et un polynôme $q \in \mathbb{A}$, le plus grand terme dans q d'après l'ordre choisi est appelé le *terme de tête* de q. Le *degré algébrique* du terme de tête est la puissance de ce terme.

Exemple 4. Considérons le polynôme q donné par $q = (x_{k+1}^{(1)})^2 + x_k^{(2)} + (x_k^{(1)} x_k^{(2)})^2 + (x_k^{(1)})^3$ et l'ordre lexicographique $x_k^{(2)} < x_k^{(1)}$. Alors, le terme de tête de q est $(x_{k+1}^{(1)})^2$ et a pour degré algébrique 2.

Définition 47. Une système de réécriture est un ensemble de règles de substitution de la forme *monôme=polynôme*. Le monôme est le terme de tête de la règle de réécriture par rapport à un ordre fixé.

Exemple 5. Soit $\mathcal{S}$ le système de réécriture défini par le système polynomial suivant :

$$\begin{cases} x_{k+1}^{(1)} = \theta^{(1)} x_k^{(1)} + x_k^{(2)} \\ x_{k+1}^{(2)} = \theta^{(2)} x_k^{(1)} \end{cases} \tag{B.2}$$

et soit l'ordre lexicographique $x_k^{(1)} < x_k^{(2)}$.
Le terme $x_k^{(2)}$ se réécrit par S en le polynôme $x_k^{(2)} = x_{k+1}^{(1)} - \theta^{(1)} x_k^{(1)}$.

Définition 48. Soient un système de réécriture $\mathcal{S}$, le polynôme $p = m - z$ correspondant à cette règle de réécriture (m est un monôme et z est un polynôme) et $q = m_1 + \ldots + m_n$ un polynôme. q est *réductible* par $\mathcal{S}$ si l'un des monômes m_i est divisible par m, c'est-à-dire s'il existe un indice $1 \leq i \leq n$ et un monôme $m_i^{'}$ tels que $m_i = m m_i^{'}$. On dit que le polynôme $z = q - m_i^{'} p$ s'obtient en réduisant q une fois par $\mathcal{S}$.

Exemple 6. Considérons le système :

$$\begin{cases} (x_k^{(1)})^2 + (x_k^{(2)})^2 - 1 = 0 \\ x_k^{(1)} - x_k^{(2)} = 0 \end{cases} \tag{B.3}$$

et considérons l'ordre lexicographique : $x_k^{(1)} < x_k^{(2)}$. Ce système peut se réécrire en le système de réécriture $\mathcal{S}$ suivant :

$$\mathcal{S} \begin{cases} (x_k^{(2)})^2 - 1 + (x_k^{(1)})^2 = 0 & \text{(a)} \\ x_k^{(2)} - x_k^{(1)} = 0 & \text{(b)} \end{cases} \tag{B.4}$$

Notons $q = (x_k^{(2)})^3$ et $p = x_k^{(2)} - (x_k^{(1)})^2 x_k^{(2)}$. On a $q = p - x_k^{(2)}\mathcal{S}_1$, où $\mathcal{S}_1 = (x_k^{(2)})^2 - 1 + (x_k^{(1)})^2$ (B.4(a)). Le monôme $(x_k^{(2)})^3$ peut s'écrire comme $(x_k^{(2)})^3 = x_k^{(2)}(x_k^{(2)})^2$ où $(x_k^{(2)})^2$ est le monôme de tête de la règle avec laquelle la réduction est effectuée ($\mathcal{S}$ (B.4(a))) et $x_k^{(2)}$ est le monôme de tête de p. Par conséquent, le monôme $(x_k^{(2)})^3$ est divisible par le monôme $x_k^{(2)}$, donc $q = (x_k^{(2)})^3$ est réductible par rapport à $\mathcal{S}$.

Définition 49. On appelle *forme normale* d'un polynôme p par un système de réécriture $\mathcal{S}$ tout polynôme irréductible q tel que p se réécrit en q par $\mathcal{S}$.

Exemple 7. Considérons l'exemple 6 précédent. D'après l'ordre lexicographique fixé et en poussant les réductions, $(x_k^{(2)})^3$ peut se réécrire en deux formes normales : $(x_k^{(2)})^3 = x_k^{(1)} - (x_k^{(1)})^3$ et $(x_k^{(2)})^3 = (x_k^{(1)})^3$.

Définition 50. Soient $p, q \in \mathbb{A}$. Notons $\alpha = [\alpha_1 \dots \alpha_n]^T$ le degré algébrique maximum de la variable $x_k = [x_k^{(1)} \dots x_k^{(n)}]^T$ du polynôme p, $\beta = [\beta_1 \dots \beta_n]^T$ le degré algébrique maximum de la variable x_k du polynôme q et $\gamma = \min(\alpha, \beta)$. Le S-polynôme de p et q, noté $S(p,q)$, est défini par :

$$S(p,q) = lc(q)(x_k)^{\beta-\gamma}p - lc(p)(x_k)^{\alpha-\gamma}q \tag{B.5}$$

où $lc(q)$ et $lc(p)$ représentent les coefficients des termes de tête de q et p respectivement.

Exemple 8. Considérons les polynômes p et q définis par :

$$\begin{aligned} p &= 3x_k^{(1)}(x_k^{(2)})^2 x_k^{(3)} + 1 \\ q &= 2x_k^{(1)}(x_k^{(3)})^3 + (x_k^{(3)})^3 \end{aligned} \tag{B.6}$$

Considérons également l'ordre lexicographique $x_k^{(3)} < x_k^{(2)} < x_k^{(1)}$. On a $\alpha = [1 \quad 2 \quad 1]^T$, $\beta = [1 \quad 0 \quad 3]^T$ et $\gamma = [1 \quad 0 \quad 1]^T$. D'après l'ordre lexicographique fixé, le terme de tête de p est $x_k^{(1)}(x_k^{(2)})^2 x_k^{(3)}$ et son coefficient est $lc(p) = 3$. Le terme de tête de q est $x_k^{(1)}(x_k^{(3)})^3$ et son coefficient est $lc(q) = 2$. Le S-polynôme de p et q est :

$$\begin{aligned} &S(p,q) = 2(x_k^{(1)})^0(x_k^{(2)})^0(x_k^{(3)})^2(3x_k^{(1)}(x_k^{(2)})^2 x_k^{(3)} + 1) - 3(x_k^{(1)})^0(x_k^{(2)})^2(x_k^{(3)})^0(2x_k^{(1)}(x_k^{(3)})^3 + (x_k^{(3)})^3) \\ &= -3(x_k^{(2)})^2(x_k^{(3)})^3 + 2(x_k^{(3)})^2 \end{aligned} \tag{B.7}$$

Définition 51. Soit un ordre fixé. Soient $\mathcal{G}$ un ensemble de polynômes de $\mathbb{A}$ et I l'idéal que $\mathcal{G}$ engendre. Les conditions suivantes sont équivalentes :

1. Tout polynôme de $\mathbb{A}$ admet une unique forme normale par $\mathcal{G}$.
2. Tout polynôme de I admet zéro pour forme normale par $\mathcal{G}$.
3. Tout S-polynôme $S(p,q)$ ($\forall p \in \mathcal{G}$, $\forall q \in \mathcal{G}$) admet zéro pour forme normale par $\mathcal{G}$.
4. L'ensemble $\mathcal{G}$ est une base de Gröbner de I.

La définition précédente signifie qu'une base de Gröbner $\mathcal{G}$ d'un idéal I est un système de réécriture qui permet de réécrire tout polynôme de $\mathbb{A}$ en un unique polynôme et qui permet de réécrire tout polynôme de I en zéro.

B.2 Ensemble caractéristique

Définition 52. Un polynôme q_i est dit *réduit* par rapport au polynôme q_j si q_i ne contient ni le terme de tête de q_j avec un degré algébrique plus grand ou égal que celui du terme de tête de q_j, ni ses itérés. Un ensemble de polynômes $q = \{q_1, \ldots, q_i\}$ qui sont tous réduits les uns par rapport aux autres, est appelé *ensemble autoréduit.*

Exemple 9. Considérons les polynômes $q_1 = x_k^{(1)} - x_k^{(2)}$ et $q_2 = (x_k^{(1)})^2 - x_k^{(3)} - 1$. Considérons également l'ordre lexicographique $x_k^{(1)} < x_k^{(2)} < x_k^{(3)}$. Le terme de tête de q_1 est $x_k^{(2)}$ (degré algébrique 1) et celui de q_2 est $x_k^{(3)}$ (degré algébrique 1). Le polynôme q_1 ne comprend pas $x_k^{(3)}$, le terme de tête de q_2, ni ses itérés. Par conséquent, q_1 est réduit par rapport à q_2. D'autre part, q_2 ne comprend pas le terme de tête de q_1. Par conséquent, q_2 est réduit par rapport à q_1. Comme q_1 et q_2 sont réduits l'un par rapport à l'autre, on dit que l'ensemble $\{q_1, q_2\}$ est autoréduit.

Définition 53. Deux ensembles autoréduits $q = \{q_1, q_2, \ldots, q_i\}$ et $r = \{r_1, r_2, \ldots, r_o\}$ sont dits ordonnés en ordre croissant par rapport à leurs termes de tête, tels que $q_1 < q_2 < \ldots < q_i$ et $r_1 < r_2 < \ldots < r_o$, s'ils vérifient les conditions suivantes :

- S'il existe un entier l, $l \leq min(i, o)$, tel que $ordre(q_j) = ordre(r_j)$, $j = 1, \ldots, l-1$, $ordre(q_l) < ordre(r_l)$, alors l'ensemble q est d'ordre inférieur à l'ensemble r.

- Si $i < o$ et $ordre(q_j) = ordre(r_j)$, $j = 1, \ldots, i$, alors q est aussi d'ordre inférieur à r.

Exemple 10. Considérons les ensembles de polynômes $q = \{q_1, q_2\}$ et $r = \{r_1, r_2, r_3\}$, avec respectivement :

$$\begin{cases} q_1 = x_{k+2}^{(1)} - \theta^{(1)}(1 - x_{k+1}^{(1)})x_k^{(1)} = 0 \\ q_2 = x_k^{(1)} - x_k^{(2)} = 0 \end{cases} \tag{B.8}$$

$$\begin{cases} r_1 = x_{k+2}^{(1)} - \theta^{(2)}(x_{k+1}^{(1)})^2 - x_k^{(1)} = 0 \\ r_2 = x_k^{(1)} - (x_k^{(2)})^2 = 0 \\ r_3 = x_{k+1}^{(1)} - \theta^{(3)}(x_k^{(1)})^2 - x_k^{(3)} = 0 \end{cases} \tag{B.9}$$

Considérons l'ordre lexicographique $x_k^{(1)} < x_k^{(2)} < x_k^{(3)}$. Le terme de tête de q_1 est $x_{k+2}^{(1)}$ et celui de q_2 est $x_k^{(2)}$. Ces termes de tête ont tous deux un ordre algébrique de 1. Le terme de tête de q_1 n'apparaît pas dans q_2 avec un degré égal ou supérieur. Par conséquent, q_1 est réduit par rapport à q_2. D'autre part, le terme de tête de q_2 n'apparaît pas dans q_1. Par conséquent, q_2 est réduit par rapport à q_1. L'ensemble q est autoréduit.
Le terme de tête de r_1 est $x_{k+2}^{(1)}$, celui de r_2 est $(x_k^{(2)})^2$ et celui de r_3 est $x_k^{(3)}$. Aucun des trois termes de tête n'apparaît avec un degré égal ou supérieur dans r_1, r_2 et r_3. Par conséquent, les trois polynômes sont réduits les uns par rapport aux autres et l'ensemble r est dit autoréduit.
q_1 et r_1 ont le même terme de tête. Par conséquent, $ordre(q_1) = ordre(r_1)$. Par ailleurs, d'après l'ordre lexicographique choisi, le terme de tête de r_2 a un plus grand ordre que celui de q_2. En effet, $x_k^{(2)}$ a un ordre algébrique égal à 1, alors que $(x_k^{(2)})^2$ a un ordre algébrique de 2. Par conséquent, $ordre(q_2) < ordre(r_2)$. D'après la Définition 53, la relation d'ordre entre les ensembles q et r est $ordre(q) < ordre(r)$.

Définition 54. Un ensemble de polynômes autoréduit d'ordre inférieur est appelé *ensemble caractéristique.*

Exemple 11. Dans l'exemple 10, l'ensemble q est un ensemble caractéristique.

B.3 Résultant de deux polynômes

Considérons deux polynômes donnés par $p = a_0 + a_1 x_k + a_2 x_k^2 + \ldots + a_m x_k^m$ et $q = b_0 + b_1 x_k + b_2 x_k^2 + \ldots + b_n x_k^n$, de degrés m et n, respectivement. La matrice de Sylvester M associée aux polynômes p et q est la matrice de dimension $(m+n) \times (m+n)$, de la forme :

$$M = \begin{bmatrix} a_0 & a_1 & \ldots & \ldots & a_m & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & \ldots & a_m & \ldots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & a_0 & a_1 & \ldots & \ldots & a_m \\ b_0 & b_1 & \ldots & b_n & 0 & \ldots & \ldots & 0 \\ 0 & b_0 & b_1 & \ldots & b_n & 0 & \ldots & 0 \\ 0 & 0 & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & b_0 & b_1 & \ldots & b_n & 0 \\ 0 & \ldots & \ldots & 0 & b_0 & b_1 & \ldots & b_n \end{bmatrix} \tag{B.10}$$

La première ligne de la matrice M (B.10) est constituée des coefficients a_i du polynôme p, complétés par des zéros. La seconde ligne est identique à la première mais ses éléments sont décalés une fois vers la droite et le premier élément de la ligne devient zéro. Les $(n-2)$ lignes suivantes sont obtenues de la même manière, en décalant successivement les éléments vers la droite et en complétant les premiers éléments par des zéros. La $(n+1)$-ième ligne est constituée des coefficients b_i du polynôme q, complétés par des zéros. Les lignes suivantes sont obtenues comme précédemment, en décalant successivement les éléments vers la droite et en complétant les premiers éléments par zéro.

Exemple 12. Considérons les polynômes $p = 1 + 2x_k + 3x_k^2$ et $q = 5 + 4x_k + 6x_k^3$. On a $m = 2$ et $n = 3$. La matrice de Sylvester est de dimension 5×5 et est donnée par :

$$M = \begin{bmatrix} 1 & 2 & 3 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 \\ 0 & 0 & 1 & 2 & 3 \\ 5 & 4 & 0 & 6 & 0 \\ 0 & 5 & 4 & 0 & 6 \end{bmatrix} \tag{B.11}$$

Annexe C

Complexité des algorithmes

Une fois qu'un algorithme est conçu pour résoudre un problème donné, il faut s'assurer de son efficacité. En effet, pour un même problème, on peut disposer de plusieurs algorithmes plus ou moins efficaces. La notion d'efficacité est indépendante de la machine sur laquelle est implémenté l'algorithme. L'efficacité d'un algorithme est l'évaluation du nombre d'opérations élémentaires (évaluation d'expressions, affectation de variables, boucles, ...) devant être exécutées. L'efficacité est aussi appelée coût. L'analyse du coût dépend de la configuration considérée. En effet, le nombre d'opérations peut varier pour deux données différentes mais de même taille. Les différentes configurations sont :

- *Configuration "pire des cas"* : configuration où l'algorithme effectue un nombre maximum d'opérations.

- *Configuration "meilleur des cas"* : configuration où l'algorithme effectue un nombre minimum d'opérations.

- *Configuration "moyenne"* : moyenne des configurations "pire des cas" et "meilleur des cas".

En général, on considère la configuration "pire des cas" (ou éventuellement "moyenne").
L'analyse du coût consiste à trouver une fonction $T(n)$ qui représente le nombre d'opérations élémentaires en fonction de la taille des données n, dans la configuration choisie. On étudie le comportement asymptotique de $T(n)$ et on cherche une borne supérieure pour $T(n)$, notée $\sigma(f(n))$ et appelée complexité de l'algorithme. σ est aussi appelée symbole de Landau. Les fonctions de référence les plus communes sont répertoriées dans le tableau suivant :

Fonctions de référence	Complexité
$\sigma(1)$	constante
$\sigma(n)$	linéaire
$\sigma(\log(n))$	logarithmique
$\sigma(n\log(n))$	"linéarithmique"
$\sigma(n^2)$	quadratique
$\sigma(n^c)$	polynomiale
$\sigma(n!)$	factorielle

TAB. C.1 – Fonctions de référence les plus communes et complexités associées

Glossaire

AES : Advanced Encryption Standard

DES : Data Encryption Standard

EKF : Extended Kalman Filter

IIGS : Input Independent Global Synchronization

LMI : Linear Matrix Inequalities
LPV : Linear Parameter Varying

RSA : Rivest Shamir Adleman

SLIT : Système Linéaire Invariant dans le Temps

Index

Bibliographie

[Allison and Noga, 1997] Allison, D. C. S. and Noga, M. T. (1997). Computing the three-dimensional convex hull. *Computer Physics Communications*, 103(1) :74–82.

[Anstett et al., 2004] Anstett, F., Millérioux, G., and Bloch, G. (2004). Global adaptive synchronization based upon polytopic observers. In *Proc. of IEEE International Symposium on Circuits and Systems, ISCAS'04*, volume 4, pages IV–728 – 731, Vancouver, Canada. May 23-26.

[Anstett et al., 2005a] Anstett, F., Millérioux, G., and Bloch, G. (2005a). Chaotic cryptosystems : cryptanalysis and identifiability. *IEEE Trans. on Circuits and Systems I*. En révision.

[Anstett et al., 2005b] Anstett, F., Millérioux, G., and Bloch, G. (2005b). Chiffrement par flot chaotique : cryptanalyse et identifiabilité. *Journées Doctorales et Nationales du GDR MACS*, Lyon, France. 05 - 07 septembre.

[Anstett et al., 2005c] Anstett, F., Millérioux, G., and Bloch, G. (2005c). Message-embedded cryptosystems : cryptanalysis and identifiability. In *Proc. of the 44th IEEE Conference on Decision and Control and European Control Conference, CDC-ECC'05*, pages 2548–2553, Sevilla, Spain. December 12-15.

[Anstett et al., 2005d] Anstett, F., Millérioux, G., and Bloch, G. (2005d). Systèmes dynamiques et chiffrement en continu. *Journées Codage et Cryptographie*, Aussois, France. 30 janvier - 04 février.

[Apkarian and Gahinet, 1995] Apkarian, P. and Gahinet, P. (1995). A convex characterization of gain-scheduled H_∞ controllers. *IEEE Trans. Automatic on Control*, 40 :853–864.

[Apkarian et al., 1995] Apkarian, P., Gahinet, P., and Becker, G. (1995). Self-scheduled $\mathcal{H}_\infty$ control of linear parameter-varying systems : a design example. *Automatica*, 31(7) :1251–1261.

[Apkarian et al., 2000] Apkarian, P., Pellanda, P., and Tuan, H. (2000). Mixed H_2/H_∞ multi-channel linear parameter-varying control in discrete time. *Systems and Control Letters*, 41 :333–346.

[Barbot, 2003] Barbot, J.-P. (2003). Observability bifurcations : application to cryptography. *4ème Ecole Internationale d'Automatique de Lille*, pages 1–19.

[Barthélemy et al., 2005] Barthélemy, P., Rolland, R., and Véron, P., editors (2005). *Cryptographie*. Hermès Science.

[Bastin and Gevers, 1988] Bastin, G. and Gevers, M. (1988). Stable adaptive observers for nonlinear time-varying systems. *IEEE Trans. on Automatic Control*, 33(7) :650–658.

[Besancon, 2000] Besancon, G. (2000). Remarks on nonlinear adaptive observer design. *Systems and Control Letters*, 41(4) :271–280.

[Biannic, 1996] Biannic, J. (1996). *Commande robuste des systèmes à paramètres variables. Application en aéronautique*. Thèse de doctorat, ENSAE, CERT-ONERA.

[Boutayeb et al., 1997] Boutayeb, M., Rafaralahy, H., and Darouach, M. (1997). Convergence analysis of the Extended Kalman Filter as an observer for nonlinear discrete-time systems. *IEEE Trans. on Automatic Control*, 42(4) :581–586.

[Buchberger, 1965] Buchberger, B. (1965). *An algorithm for finding a basis for the residue class ring of zero-dimensional polynomial ideal.* Thèse de doctorat, Math. Inst. Univ. of Innsbrück, Austria.

[Chatterjee and Chatterjee, 1990] Chatterjee, S. and Chatterjee, S. (1990). A note of finding extreme points in multivariate space. *Computational Statistics and Data Analysis*, 10 :87–92.

[Chen and Dong, 1998] Chen, G. and Dong, X. (1998). *From chaos to order.* World Scientific, Singapore.

[Cho and Rajamani, 1997] Cho, Y. M. and Rajamani, R. (1997). A systematic approach to adaptive observer synthesis for nonlinear systems. *IEEE. Trans. on Automatic Control*, 42(4) :534–537.

[Cox, 1964] Cox, H. (1964). On the estimation of state variables and parameters for noisy dynamic systems. *IEEE Trans. on Automatic Control*, 9 :5–12.

[Cruz and Nijmeijer, 2000] Cruz, C. and Nijmeijer, H. (2000). Synchronization through filtering. *International Journal of Bifurcation and Chaos*, 110(4) :763–775.

[Cuomo et al., 1993a] Cuomo, K. M., Oppenheim, A. V., and Strogatz, S. H. (1993a). Robustness and signal recovery in a synchronized chaotic system. *International Journal of Bifurcation and Chaos*, 3(6) :1629–1638.

[Cuomo et al., 1993b] Cuomo, K. M., Oppenheim, A. V., and Strogatz, S. H. (1993b). Synchronization of Lorenz-based chaotic circuits with applications to communications. *IEEE Trans. Circuits Syst. II : Anal. Digit. Sign. Process.*, 40(10) :626–633.

[Daafouz and Bernussou, 2001] Daafouz, J. and Bernussou, J. (2001). Parameter dependent Lyapunov functions for discrete time systems with time varying parametric uncertainties. *Systems and Control Letters*, 43 :355–359.

[Daafouz and Millérioux, 2002] Daafouz, J. and Millérioux, G. (2002). Poly-quadratic stability and global chaos synchronization of discrete time hybrid systems. *Special Issue of Mathematics and Computers in Simulation*, 58 :295–307.

[Daafouz et al., 2002] Daafouz, J., Millérioux, G., and Iung, C. (2002). A poly-quadratic stability based approach for switched systems. *International Journal of Control*, 75 :1302–1310.

[Dachselt et al., 1998] Dachselt, F., Kelber, K., Vandewalle, J., and Schwarz, W. (1998). Chaotic versus classical stream ciphers – a comparative study. In *Proc. of International Symposium on Circuits and Systems, ISCAS'98*, volume IV, pages 518–521, Monterey. 31 May - 3 June.

[Dedieu et al., 1993] Dedieu, H., Kennedy, M. P., and Hasler, M. (1993). Chaos shift keying : modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits. *IEEE Trans. Circuits Syst. II : Anal. Digit. Sign. Process.*, 40 :634–642.

[Dedieu and Ogorzalek, 1997] Dedieu, H. and Ogorzalek, M. (1997). Identifiability and identification of chaotic systems based on adaptive synchronization. *IEEE Trans. Circuits Syst. I : Fund. Theo. Appl*, 44(10) :948–962.

[Delfs and Knebl, 2002] Delfs, H. and Knebl, H. (2002). *Introduction to cryptography.* Springer-Verlag, Berlin.

[Devaney, 1989] Devaney, R. L. (1989). *An introduction to chaotic dynamical systems.* Addison-Wesley, Redwood City, CA.

[Diop and Fliess, 1991] Diop, S. and Fliess, M. (1991). Nonlinear observability, identifiability and persistent trajectories. In *Proc. of the 30th Conference on Decision and Control*, pages 714–718, Brighton, England. December 11-13.

[Du, 1996] Du, C. (1996). An algorithm for automatic Delaunay triangulation of arbitrary planar domains. *Advances in Engineering Software*, 27 :21–26.

[Eddy, 1977] Eddy, W. F. (1977). *ACM Trans. Math. Soft.*, 3(398).

[Feldmann et al., 1996] Feldmann, U., Hasler, M., and Schwarz, W. (1996). Communication by chaotic signals : the inverse system approach. *Int. J. of Circuit Theo. Appl.*, 24 :551–579.

[Fradkov et al., 2000] Fradkov, A., Nijmeijer, H., and Markov, A. (2000). Adaptive observer-based synchronization for communication. *Int. J. of Bifurcation and Chaos*, 10(12) :2807–2813.

[Fradkov and Markov, 1997] Fradkov, A. L. and Markov, A. Y. (1997). Adaptive synchronization of chaotic systems based on speed-gradient method and passification. *IEEE Trans. Circuits. Syst. I : Fundamental Theo. Appl*, 44(10) :905–912.

[Fradkov et al., 1999] Fradkov, A. L., Nijmeijer, H., and Pogromsky, A. Y. (1999). Adaptive observer-based synchronization. In Chen, G., editor, *Controlling Chaos and Bifurcations in Engineering Systems*, pages 417–438. CRC Press.

[Gleick, 1991] Gleick, J. (1991). *La théorie du chaos. Vers une nouvelle science.* Flammarion.

[Gotz et al., 1997] Gotz, M., Kelber, K., and Schwarz, W. (1997). Discrete-time chaotic encryption systems - part 1 : statistical design approach. *IEEE Trans. Circuits. Syst. I : Fundamental Theo. Appl.*, 44(10) :963–970.

[Graham, 1973] Graham, R. L. (1973). An efficient algorithm for determining the convex hull of a finite planar set. *Information Processing Letters*, 2(1) :132–133.

[Guyader and Zhang, 2003] Guyader, A. and Zhang, Q. (2003). Adaptive observer for discrete time linear time varying systems. In *Proc. of 13th IFAC/IFORS Symposium on Identification and System Parameter Estimation, SYSID'2003*, Rotterdam, The Netherlands. August 27-29.

[Hasler, 1998] Hasler, M. (1998). Synchronization of chaotic systems and transmission of information. *International Journal of Bifurcation and Chaos*, 8(4).

[Hénon, 1976] Hénon, M. (1976). A two-dimensional mapping with a strange attractor. *Communications of Mathematical Physics*, 50 :69–77.

[Huijberts, 1999] Huijberts, H. J. C. (1999). *New directions in nonlinear observer design*, chapter On existence of extended observer forms for nonlinear discrete-time systems, pages 79–92. Springer Verlag, Berlin.

[Huijberts et al., 2000] Huijberts, H. J. C., Nijmeijer, H., and Pogromsky, A. Y. (2000). An observer point of view on synchronization of discrete-time systems. In *IEEE International Symposium on Circuits and Systems*, volume 3, pages 491–494, Geneva. May 28-31.

[Ikeda, 1979] Ikeda, K. (1979). Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system. *Opt. Commun.*, 30 :257–261.

[Kahn, 1996] Kahn, D. (1996). *The codebreakers.* Scribner Book Company.

[Khalil, 1996] Khalil, H. K. (1996). *Nonlinear systems.* Prentice Hall, New Jersey.

[Kocarev, 2001] Kocarev, L. (2001). Chaos-based cryptography : a brief overview. *IEEE Circuits Syst. Mag.*, 1(3) :6–21.

[Kolchin, 1973] Kolchin, E. (1973). *Differential algebra and algebraic groups.*

[Kreisselmeier, 1977] Kreisselmeier, G. (1977). Adaptive observers with exponential rate convergence. *IEEE Trans. on Automatic Control*, 22(1) :2–8.

[Lilge, 1999] Lilge, T. (1999). *New directions in nonlinear observer design*, chapter Nonlinear discrete-time observers for synchronization problems, pages 491–510. Springer Verlag, Berlin.

[Lin and Byrnes, 1995] Lin, W. and Byrnes, C. (1995). Remarks on linearization of discrete-time autonomous systems and nonlinear observer design. *Systems and Control Letters*, 25 :31–40.

[Ljung and Glad, 1994] Ljung, L. and Glad, T. (1994). On global identifiability for arbitrary model parametrizations. *Automatica*, 30(2) :265–276.

[Luders and Narendra, 1974] Luders, G. and Narendra, K. S. (1974). A new canonical form for an adaptive observer. *IEEE Trans. on Automatic Control*, 19 :841–847.

[Marino, 1990] Marino, R. (1990). Adaptive observers for single output nonlinear systems. *IEEE Trans. on Automatic Control*, 35(9) :1054–1058.

[Marino et al., 2001] Marino, R., Santosuosso, G. L., and Tomei, P. (2001). Robust adaptive observers for nonlinear systems with bounded disturbances. *IEEE Trans. on Automatic Control*, 46(6) :967–972.

[Marino and Tomei, 1992] Marino, R. and Tomei, P. (1992). Global adaptive observers for nonlinear systems via filtered transformations. *IEEE Trans. on Automatic Control*, 37(8) :1239–1245.

[Marino and Tomei, 1995] Marino, R. and Tomei, P. (1995). Adaptive observers with arbitrary exponential rate of convergence for nonlinear systems. *IEEE Trans. on Automatic Control*, 40(7) :1300–1304.

[May, 1976] May, R. (1976). Simple mathematical models with complicated dynamics. *Nature*, 261 :459–470.

[Menezes et al., 1996] Menezes, A., Oorschot, P. V., and Vanstone, S. (1996). *Handbook of applied cryptography*. CRC Press.

[Millérioux et al., 2005] Millérioux, G., Anstett, F., and Bloch, G. (2005). Considering the attractor structure of chaotic maps for observer-based synchronization problems. *Mathematics and Computers in Simulation*, 68(1) :67–85.

[Millérioux et al., 2003] Millérioux, G., Bloch, G., Amigo, J. M., Bastos, A., and Anstett, F. (2003). Real-time video communication secured by a chaotic key stream cipher. In *Proc. of IEEE 16th European Conference on Circuits Theory and Design, ECCTD'03*, pages 245–248, Krakow, Poland.

[Millérioux and Daafouz, 2003a] Millérioux, G. and Daafouz, J. (2003a). An observer-based approach for input independent global chaos synchronization of discrete-time switched systems. *IEEE Trans. Circuits Syst. I : Fund. Theo. Appl*, pages 1270–1279.

[Millérioux and Daafouz, 2003b] Millérioux, G. and Daafouz, J. (2003b). Polytopic observer for global synchronization of systems with output measurable nonlinearities. *International Journal of Bifurcation and Chaos*, 13(3) :703–712.

[Millérioux and Daafouz, 2004] Millérioux, G. and Daafouz, J. (2004). Unknown input observers for message-embedded chaos synchronization of discrete-time systems. *International Journal of Bifurcation and Chaos*, 14(4) :1357–1368.

[Nijmeijer and Van Der Schaft, 1990] Nijmeijer, H. and Van Der Schaft, A. J. (1990). *Nonlinear dynamical control systems*. Springer.

[Noiret, 2000] Noiret, C. (2000). *Utilisation du calcul formel pour l'identifiabilité de modèles paramétriques et nouveaux algorithmes en estimation des paramètres.* Thèse de doctorat, Université de Technologie de Compiègne.

[Nõmm and Moog, 2004] Nõmm, S. and Moog, C. H. (2004). Identifiability of discrete-time nonlinear systems. In *Proc. of the 6th IFAC Symposium on Nonlinear Control Systems, NOLCOS*, pages 477–489, Stuttgart, Germany. September 1-3.

[Palaniyandi and Lakshmanan, 2001] Palaniyandi, P. and Lakshmanan, M. (2001). Secure digital signal transmission by multistep parameter modulation and alternative driving of transmitter variables. *International Journal of Bifurcation and Chaos*, 11(7) :2031–2036.

[Papadimitriou et al., 2001] Papadimitriou, S., Bezerianos, A., Bountis, T., and Pavlides, G. (2001). Secure communication protocols with discrete nonlinear chaotic maps. *Journal of Systems Architecture*, 47 :61–72.

[Pardalos et al., 1995] Pardalos, P. M., Li, Y., and Hager, W. W. (1995). Linear programming approaches to the convex hull problem in $\mathbb{R}^n$. *Computers Math. Applic.*, 29(7) :23–29.

[Parlitz et al., 1993] Parlitz, U., Chua, L. O., Kocarev, L., Halle, K. S., and Shang, A. (1993). Transmission of digital signals by chaotic synchronization. *International Journal of Bifurcation and Chaos*, 3(2) :973–977.

[Pecora and Carroll, 1990] Pecora, L. M. and Carroll, T. L. (1990). Synchronization in chaotic systems. *Phys. Rev. Lett.*, 64 :821–824.

[Peitgen et al., 1992] Peitgen, H. O., Jürgens, H., and Saupe, D. (1992). *Chaos and fractals : new frontiers of science.* Springer-Verlag, New York.

[Pohjanpalo, 1978] Pohjanpalo, H. (1978). System identifiability based on the power series expansion of the solution. *Mathematical Biosciences*, 41 :21–33.

[Preparata and Shamos, 1985] Preparata, F. P. and Shamos, M. I. (1985). *Computational geometry.* Springer-Verlag.

[Ritt, 1950] Ritt, J. F. (1950). *Differential algebra.* Providence, RI : American Mathematical Society.

[Rugh, 1991] Rugh, W. (1991). Analytical framework for gain scheduling. *IEEE Contr. Sys. Mag.*, 11(1) :74–84.

[Schneier, 1996] Schneier, B., editor (1996). *Applied cryptography.* John Wiley and Sons.

[Shamma and Athans, 1990] Shamma, J. and Athans, M. (1990). Analysis of gain scheduled control for nonlinear plants. *IEEE Trans. Autom. Contr.*, 35 :898–907.

[Shamma and Athans, 1991] Shamma, J. and Athans, M. (1991). Guaranteed properties of gain scheduled control for linear parameter varying plants. *Automatica*, 27 :559–564.

[Slotine et al., 1987] Slotine, J. J. E., Hedrick, J. K., and Misawa, E. A. (1987). On sliding observers for nonlinear systems. *J. Dyn. Syst. Meas. Contr.*, 109 :245–252.

[Slotine and Li, 1991] Slotine, J. J. E. and Li, W. (1991). *Applied nonlinear control.* Prentice Hall, New Jersey.

[Takahashi and Peres, 1999] Takahashi, R. H. and Peres, P. L. D. (1999). Unknown input observers for uncertain systems : a unifying approach. *European Journal of Control*, 5(2) :261–275.

[Tunali and Tarn, 1987] Tunali, E. T. and Tarn, T. (1987). New results for identifiability of nonlinear systems. *IEEE Trans. on Automatic Control*, 32(2) :146–154.

[Vajda et al., 1989] Vajda, S., Godfrey, K. R., and Rabitz, H. (1989). Similarity transformation approach to identifiability analysis of nonlinear compartmental models. *Mathematical Biosciences*, 93(2) :217–248.

[Walter and Pronzato, 1997] Walter, E. and Pronzato, L. (1997). *Identification of parametric models from experimental data*. Springer-Verlag.

[Wang, 2001] Wang, D. (2001). Elimination theory, methods, and practice. In Lin, D., Li, W., and Yu, Y., editors, *Mathematics and Mathematics-Mechanization*, pages 91–137, Jinan. Shandong Education Publishing House. Disponible à `http ://www-calfor.lip6.fr/~wang/`.

[Wu and Chua, 1993] Wu, C. W. and Chua, L. O. (1993). A simple way to synchronize chaotic systems with applications to secure communications systems. *International Journal of Bifurcation and Chaos*, 3(6) :1619–1627.

[Yang, 2004] Yang, T. (2004). A survey of chaotic secure communication systems. *International Journal of Computational Cognition*, 2(2) :81–130. Disponible à `http ://www.YangSky.com/yangijcc.htm`.

[Zhang and Xu, 2001] Zhang, Q. and Xu, A. (2001). Global adaptive observer for a class of nonlinear systems. In *Proc. of the 40th IEEE Conference on Decision and Control*, volume 4, pages 3360–3365, Orlando, Florida. December 4-7.

Résumé

Le travail porte sur la synthèse et la cryptanalyse des schémas de chiffrement basé sur le chaos. Ces schémas utilisent, côté émetteur, des systèmes dynamiques non linéaires exhibant un comportement chaotique. La séquence complexe ainsi produite est utilisée pour masquer une information. Plusieurs modes de chiffrement sont étudiés : la modulation chaotique, la modulation paramétrique et le chiffrement par inclusion, principalement dans le cas des systèmes chaotiques à temps discret. Pour ces schémas, la reconstruction de l'information nécessite la synchronisation de l'émetteur et du récepteur. Un observateur joue le rôle du récepteur.
Tout d'abord, le lien entre le chiffrement par le chaos et le chiffrement usuel est établi.
Concernant la modulation chaotique, nous proposons, pour le déchiffrement, une méthode systématique de synthèse d'observateur polytopique, tenant compte de la spécificité du problème liée au chaos. Dans la modulation paramétrique, côté émetteur, l'information claire module les paramètres d'un système chaotique. Pour réaliser la synchronisation, un observateur adaptatif polytopique assurant la reconstruction simultanée état/paramètre est proposé.
Enfin, la cryptanalyse du chiffrement par inclusion est effectuée. Nous considérons des systèmes présentant uniquement des non linéarités polynomiales qui englobent un grand nombre de systèmes chaotiques usuels. La sécurité de ce schéma repose sur les paramètres du système chaotique, supposés jouer le rôle de clé secrète. Un formalisme général, basé sur le concept de l'identifiabilité, est élaboré pour tester la reconstructibilité de ces paramètres. Les différentes définitions de l'identifiabilité sont récapitulées et des approches permettant de tester l'identifiabilité sont présentées. Ce formalisme est appliqué sur des schémas usuels de chiffrement par inclusion afin de tester leur sécurité.

Mots-clés : Systèmes non linéaires à temps discret, dynamiques chaotiques, systèmes polytopiques, observateurs, observateurs adaptatifs, identifiabilité paramétrique, cryptanalyse.

Abstract

The work deals with the synthesis and the cryptanalysis of chaos-based encryption schemes. These schemes involve, at the transmitter side, nonlinear dynamic systems exhibiting chaotic behavior. The complex sequence thus generated is used to mask an information. Several encryption schemes are studied : the chaotic switching, the parameter modulation and the message-embedding, mostly in the case of chaotic discrete-time systems. For these schemes, the information reconstruction requires the synchronization between the transmitter and the receiver. An observer plays the role of the receiver.
First, the connection between chaos-based encryption and standard encryption is established.
In the case of chaotic switching, we propose, for the decryption, a systematic method to design polytopic observer taking into account the specificity of chaos. In the parameter modulation, at the transmitter side, the parameters are modulated by the plaintext. To achieve the synchronization, a polytopic adaptive observer ensuring the joint state and modulated parameter estimation is proposed.
Finally, the cryptanalysis of the message-embedding scheme is performed. We consider chaotic discrete-time cryptosystems involving only polynomial nonlinearities which include a large number of usual chaotic systems. In this scheme, the security is based on the system parameters expected to act as the secret key. A general formalism based on the identifiability concept is proposed to test the parameters reconstructibility. The different identifiability definitions are summarized and the approaches to test the parametric identifiability are presented. This formalism is applied to usual chaotic message-embedding schemes in order to test their security.

Keywords : Nonlinear discrete-time systems, chaotic dynamic, polytopic systems, observers, adaptive observers, parametric identifiability, cryptanalysis.