Sécurisation des smart cards par masquage de signal informationnel sur canal secondaire

Fabien Chaillan

UNIVERSITE DU SUD TOULON VAR

THESE

SÉCURISATION DES SMART CARDS PAR MASQUAGE DE SIGNAL INFORMATIONNEL SUR CANAL SECONDAIRE

Pour obtenir le grade de

DOCTEUR EN SCIENCES DE L'UNIVERSITE DU SUD TOULON VAR

Faculté des Sciences et Techniques

Discipline : Traitement du Signal

Soutenue le 13 décembre 2006 par :

Fabien CHAILLAN

Devant le jury composé de :

Président du jury	:	**H. BARTHELEMY**	Université de Provence Aix-Marseille I
Co-Directeur de Thèse	:	**P. COURMONTAGNE**	ISEN-Toulon
Rapporteur	:	**R. GARELLO**	ENST-Bretagne
Directeur de Thèse	:	**C. JAUFFRET**	Université du Sud Toulon Var
Invité	:	**A. MALHERBE**	ST-Microelectronics
Rapporteur	:	**A. QUINQUIS**	ENSIETA

REMERCIEMENTS

J'adresse de profonds remerciements à Monsieur André Quinquis, rapporteur. Ces nombreuses remarques, parfois dures mais toujours justes, ont fait évoluer positivement le présent manuscrit ainsi que mon discours.

Je tiens à remercier chaleureusement Monsieur René Garello, rapporteur. Sa démarche scientifique m'a fait comprendre qu'il est essentiel, en Traitement du Signal, de donner du sens aux équations. Je le remercie également de m'avoir donné l'opportunité, au long de ces dernières années, de valoriser mes travaux dans le cycle de conférences "Oceans".

J'exprime ma reconnaissance à Monsieur Hérvé Barthélémy, président du jury, responsable de l'équipe Conception du Laboratoire Matériaux et Microélectronique de Provence (L2MP). J'ai eu l'honneur de pouvoir bénéficier de ses qualités d'écoute et de sa gentillesse. Le jeune chercheur que je suis adhère pleinement à sa vision de la Recherche.

Je voudrais témoigner ma reconnaissance à Monsieur Alexandre Malherbe, de la division Smart Cards de la société ST Microelectronics. Son professionnalisme, sa patience, son ouverture d'esprit, m'ont permis de mener à bien mes travaux dans le domaine de la sécurisation des cartes à puce, dont j'ignorais totalement les fondements avant notre collaboration, le tout dans une ambiance de travail des plus agréables. Je remercie d'ailleurs les membres de l'équipe Smart Cards qui m'ont fait la gentillesse de me consacrer du temps pour m'aider.

J'exprime ma profonde gratitude à Monsieur Claude Jauffret, Directeur de Thèse. Ses conseils avisés, son soutien de tous les instants, ses recadrages sur fond de franchise et de gentillesse, m'ont permis d'y voir plus clair durant les nombreux moments de doutes. Je tiens à le remercier pour la confiance qu'il m'a témoigné, ceci dès mon arrivée en Master, où notre rencontre a été déterminante pour la suite de mes études. Monsieur Jauffret m'a donné goût au Traitement du Signal et a cru en moi.

Je tiens à remercier Monsieur Philippe Courmontagne, Co-Directeur de Thèse, pour m'avoir encadré de façon optimale. De l'instant où nous nous sommes rencontrés jusqu'à ma soutenance, Philippe Courmontagne n'a eu de cesse de me faire progresser, de me guider dans mes recherches en me montrant la voie, avec une volonté permanente de valoriser mes travaux. Cette volonté nous a amené, entre autre, à présenter nos contributions dans les conférences Oceans, chacune étant synonyme d'instants inoubliables, de rencontres et de lieux pittoresques, sur trois continents, de Singapour à Boston en passant par Brest. Je voudrais que Philippe sache que je m'estime privilégié d'avoir été son disciple, qui plus est le premier, car rares sont les personnes dotées d'autant de qualités intrinsèques. Sa bonne humeur, son humour, son abnégation, son honnêteté, sa franchise, sa patience, son calme font de lui une personne hors du commun. Je me

complais à espérer que cette Thèse n'est que le premier chapitre de nos aventures.

Je remercie Messieurs Michel Lanoo et Rachid Bouchakour, Directeurs du L2MP, de m'avoir accueillis dans leur laboratoire.
Je remercie Monsieur Bernard Petitprez, Directeur de l'Institut Supérieur de l'Électronique et du Numérique de Toulon (ISEN Toulon), de m'avoir fourni les moyens nécessaires au bon déroulement de mes travaux et permis d'enseigner dans son école.

C'est avec beaucoup d'émotion que je remercie les membres du personnel de l'ISEN Toulon, tant il m'a été agréable de travailler en leur compagnie. Au cours des moments difficiles, j'ai pu bénéficier de leur soutien et de leur aide, qu'ils sachent que je ne les oublierai pas.

Je profite de l'occasion pour saluer et remercier les professeurs qui ont jalonné mon (long) parcours d'étudiant, à la faculté des Sciences de l'Université du Sud Toulon-Var ainsi qu'à l'Institut des Sciences de l'Ingénieur de Toulon et du Var. J'adresse d'ailleurs une pensée amicale à mes collègues de la promotion 2002 de l'option Mathématique.

Je voudrais remercier Marc Chaillan, mon père, pour l'ensemble de son oeuvre. De par son soutien moral, affectif et logistique de tous les instants, il a fait en sorte que je puisse franchir cette étape. C'est avec une grande fierté que je remercie mes parents. Ils m'ont toujours fait confiance et transmis la volonté de réaliser au mieux mes projets, le tout sur fond de valeurs simples mais essentielles.

Je remercie la famille et les amis qui m'ont soutenu tout au long de mes études, dans des conditions pas toujours faciles. Leurs bons mots, leurs attentions, nos larmes, nos franches parties de rigolades ainsi que tout ce qui ne se dit pas dans un tel document, m'ont fait aller de l'avant et tenir debout. Je me garde d'être nominatif de peur d'en oublier.

Enfin, je voudrais remercier, non sans émotion, ma mère, partie trop tôt, qui me manque.

TABLE DES MATIÈRES

TABLE DES FIGURES

CHAPITRE I

INTRODUCTION, DE L'UNIVERS DES CARTES À PUCE AU MASQUAGE DES SIGNAUX

Ce manuscrit traite de mes travaux de thèse réalisés entre octobre 2003 et octobre 2006 sous la direction commune du professeur C. Jauffret et de Ph. Courmontagne, consistant en la synthèse de techniques de masquage de signaux de consommation de courant de Smart Cards.
La thèse est financée par ST Microelectronics dans le cadre de la convention L2MP-STM établie entre mon laboratoire d'accueil, le Laboratoire Matériaux et Microélectronique de Provence et la société ST Microelectronics. Elle fait partie du thème de recherche intitulé "Gestion d'énergie" (PS23).
Ce contexte m'a permis de travailler au sein de l'équipe Conception du L2MP localisée à l'ISEN Toulon, en partenariat avec la division Smart Card de ST Microelectronics Rousset avec comme tuteur industriel Mr A. Malherbe.
Ces travaux sont la réponse à une spécification de besoin de ST Microelectronics division Smart Cards relative à la sécurisation de leurs cartes à puce. Il existe en effet au sein de ces dernières certains canaux, appelés canaux secondaires[1], où transitent des informations liées au fonctionnement de la carte. Ces fuites de courant constituent un point d'accroche pour le pirate, alors capable de se constituer une base de donnée substantielle d'activités de courant spécifiques[2]. A partir de la connaissance de ces données, par l'intermédiaire de traitements statistiques appropriés, il peut en déduire le comportement d'éléments constitutifs de la carte, ou alors le fonctionnement de l'algorithme cryptographique utilisé et ainsi gravement nuire à la sécurité de la carte.
En réponse à ce problème apparaît alors la nécessité de masquer ces signaux de consommation de courant, par le biais de nouvelles techniques de Traitement du Signal. A ce jour, les fabricants de Smart Cards protègent ces fuites de courant par ajout direct de bruit à corrélations microscopiques sur la consommation [Kus02].
Dans sa généralité, le problème du masquage d'une information est complexe à décrire car il dépend des caractéristiques physiques du signal à masquer. Dans le contexte particulier des signaux de consommation de carte à puce, le but est de concevoir des techniques de masquage de signaux tenant compte de la technologie Smart Card, à savoir des techniques qui conservent la puissance du signal à masquer et robustes face aux attaques des pirates.
La problématique consiste alors à définir une contre-mesure par l'intermédiaire d'un opérateur de masquage qui fait correspondre à une signature de courant une autre signature, appelée signal

[1] En anglais "side channel".
[2] Appelées signatures de courant.

masqué, de même puissance[3], à partir de laquelle il est difficile de retrouver la signature originale. Définir de tels opérateurs est l'objectif principal de cette thèse, la stratégie adoptée face au pirate est donc une stratégie de leurre, consistant à affirmer que si ce dernier acquiert des signatures masquées, il ne peut qu'obtenir de fausses informations concernant l'activité de la carte.

Deux techniques de masquage sont présentées, celle du masquage par décomposition des signaux, chapitre III, reposant sur la décomposition de l'observation sur une base hilbetienne appropriée, puis celle du masquage FAS-EM, chapitre IV, par utilisation conjointe de l'algorithme expectation maximization (EM) et du filtrage adapté stochastique (FAS) reposant sur la détection et l'estimation paramétrique non-bayesienne des signaux.
Dans le cadre du même financement et du même thème de recherche PS23, V. Telandro, microélectronicien de l'équipe conception du L2MP, a dans sa thèse travaillé sur le problème de la conception d'architectures Smart Card sécurisées. Or, dans le chapitre III, il sera nécessaire d'avoir à disposition un générateur de séquences pseudo-aléatoires innovant et efficace, et électroniquement implémentable. Devant la convergence d'intérêt suscitée par la réponse à ce problème, nous avons décidé d'unir nos compétences afin d'y répondre au mieux. Pour ma part, cela m'a amené à étudier le comportement d'un système dynamique non-linéaire chaotique, ainsi que son application à la genèse de séquences pseudo-aléatoires. Cette étude est présentée au chapitre II. V. Telandro y est largement cité tant notre collaboration a été étroite et soutenue.
En préambule à tout cela, ce chapitre d'introduction a pour but de plonger le lecteur dans l'univers qui a été le mien ces trois années durant.
Après une présentation du contexte de travail, il sera question de la présentation des Smart Cards, à travers leurs origines, leurs applications, et par conséquent de la nécessité pour ces dernières d'être sécurisées. Les principales techniques d'attaques seront ensuite énumérées, avec une attention particulière portée sur les attaques en puissance à partir de fuites de courant. Cette vue d'ensemble permet alors de définir quelles sont les données dont le pirate a besoin pour mener à bien son attaque. Cette information, qui s'ajoute à celle relative aux spécificités physiques des signatures de courant, permet de définir les contraintes liées à la physique du problème, dont la technique de masquage proposée doit tenir compte.
Le chapitre s'achève par la donnée du plan du manuscrit à travers la présentation des chapitres qui le constitue.

1 CADRE DE TRAVAIL

Ma thèse s'est déroulée au sein de l'équipe Conception du L2MP dans les locaux de l'ISEN Toulon. Mes interlocuteurs étaient ralliés autour du thème PS23 : sur le site de ST Microelectronics Rousset, Messieurs A. Malherbe et B. Duval, sur place mon encadrant, co-Directeur de thèse, Monsieur Ph. Courmontagne et mon Directeur de thèse Monsieur C. Jauffret, ainsi que Madame E. Kussener et Monsieur V. Telandro, les microélectroniciens de l'équipe Conception, avec qui j'ai régulièrement collaboré.
Le déroulement de mes travaux était ponctué de réunions avec l'ensemble de ces protagonistes.
Les moyens matériels à disposition étaient une station de calcul bi-processeur $2 \times 3,6Ghz$ avec $3Go$ de RAM et le logiciel de calcul scientifique Matlab©. Cette puissance de calcul est mise à contribution pour les calculs de trajectoires de système dynamique (chapitre II), ainsi que pour l'exécution de l'algorithme FAS-EM (chapitre IV).

[3] Si tel n'était pas le cas, une technique de masquage consisterait simplement à multiplier la signature par 0.

2 Les Smart Cards. Enjeux de leur sécurisation

Cette section fait le point sur la carte à puce, son fonctionnement ainsi que sur les enjeux de sa sécurisation.

2.1 Le concept de Smart Card

La carte à puce, est née en 1974, inventée par Moreno. Il s'agit d'un ordinateur embarqué, équipé d'un processeur et de mémoire. Le rôle de la carte est d'exécuter des algorithmes cryptographiques destinés à effectuer des opérations secrètes sur des informations privées ne devant être en aucun cas fuir du dispositif comprenant la carte et le lecteur. Le but du pirate est d'obtenir ces informations secrètes, indirectement via le canal secondaire, comme le montre la figure 1.

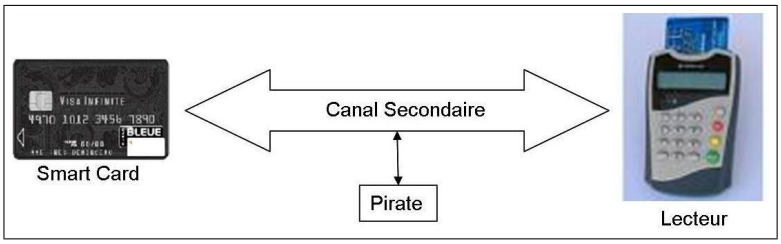


FIG. 1 – *Place du pirate au sein du dispositif Smart Card - Lecteur*

La carte communique avec un lecteur par l'intermédiaire de huit pattes : deux sont dédiées à l'alimentation, les six autres, pas nécessairement toutes exploitées, sont dédiées à la communication.
Une Smart Card n'a pas de source d'alimentation interne, elle est alimentée par le lecteur. Le signal d'horloge transitant par les pattes d'alimentation ne sert qu'à cadencer [4] le flux d'entrées/sorties, cependant, une horloge interne est présente à l'intérieur de la carte, mais plus difficilement accessible. Il est intéressant de remarquer que ces données sont publiques, ce sont les activités de la carte qui sont privées.
Ces spécificités techniques sont telles que des informations importantes transitent par des canaux où elles peuvent être observées, ce qui constitue une faille de sécurité.

2.2 Enjeux de la sécurisation des Smart Cards

Avant de rentrer dans le vif du sujet, il est intéressant de comprendre ne serait-ce que de façon rudimentaire les enjeux de la sécurité des Smart Cards.

2.2.1 Exigence de sécurité

Une fois commercialisées, les Smart Cards servent de support à des applications concrètes du quotidien de tout un chacun, telles que les opérations bancaires avec la Carte Bleue, le stockage de données personnelles avec la Carte Vitale, ou encore les systèmes d'accès aux lieux justement sécurisés avec la technologie sans contacts RFID en plein essor.
La part de la sécurité dans de tels dispositifs est donc conséquente, vu que le succès commercial à long terme de cet objet n'est en définitive fondé que sur son aspect sécuritaire, c'est-à-dire sur le fait qu'il est très difficile pour une tierce personne d'obtenir des informations d'une carte qui n'est pas la sienne. Il est clair que le nombre de cartes sur le marché est tel que quiconque

[4] A une fréquence de 5MHz.

aurait le pouvoir d'exploiter une défaillance de sécurité majeure aurait le pouvoir de déstabiliser l'économie mondiale. Pour s'en convaincre, en 2005, $296,6$ millions de carte bleues étaient en activité en Europe, qui ont servi à effectuer 16 milliards de transactions pour un montant total de $1,09$ trillions[5] d'euros[6].
Ainsi, la part prépondérante investie par les fabricants dans la sécurité des données et du dispositif Smart Card répond à une demande commerciale légitime, mais également à une exigence technologique voulant que le produit ait systématiquement au moins un degré d'avance sur toute personne nuisible, et sur la concurrence.

2.2.2 Étude du contexte par la théorie des jeux

Les enjeux de la sécurité des Smart Cards peuvent être analysés par la théorie des jeux. Seule une analyse rudimentaire est faite ici, ayant pour seule vertu d'apporter un point de vue qualitatif.
Schématiquement, les protagonistes sont deux personnes morales :

- l'encarteur, c'est-à-dire l'ensemble des intervenants impliqués dans la fabrication des Smart Cards, dans les domaines de la conception analogique, de la conception logicielle, de la fonderie, du conditionnement[7].
- le pirate, c'est-à-dire toute personne ou groupe de personnes engageant des moyens humains et matériels à des fins frauduleuses d'acquisition d'informations émanant du dispositif.

La configuration est la suivante, l'encarteur et le pirate jouent à un jeu dynamique[8] consistant à chaque tour à prendre la décision d'investir ou non. Cet investissement se traduit pour le pirate par l'engagement de moyens humains et matériels destinés à percer les failles de sécurité, en quelque sorte en cherchant le maillon faible du dispositif, puis en tirer profit, il se traduit pour l'encarteur par la sécurisation de ses dispositifs et par la volonté de rendre caduque toute intervention du pirate. La matrice des gains est présentée dans le tableau 1, les valeurs des gains n'ont qu'une valeur symbolique. Les décisions I, $\bar{I}$ signifient respectivement "Investir" et "Ne pas investir". Par exemple, $(2\,;\,-2)$ signifie que l'encarteur gagne symboliquement 2 alors que

		Pirate	
		I	$\bar{I}$
Encarteur	I	$(1\,;\,1)$	$(2\,;\,-2)$
	$\bar{I}$	$(-2\,;\,2)$	$(0\,;\,0)$

TAB. 1 – matrice des gains

le pirate perd 2. L'encarteur joue le premier.

- Si il joue I, autrement dit s'il décide d'investir dans la sécurisation de ses produits, alors le pirate joue à son tour. Il peut jouer I en augmentant ses moyens humains et technologiques pour ainsi espérer rester compétitif. Il peut également ne rien faire en jouant $\bar{I}$ et risquer de laisser l'encarteur prendre une avance définitive en matière d'évolution technologique.
- En revanche, si l'encarteur joue $\bar{I}$, et choisit donc de ne pas augmenter le niveau de sécurité de ses Smart Cards, alors le pirate à le choix de jouer I et s'octroyer ainsi la possibilité de profiter de la stagnation de l'encarteur pour prendre un ascendant technologique dangereux pour ce dernier. Il peut également jouer $\bar{I}$, dans ce cas exotique personne ne fait rien.

[5] 1 trillion d'euros est égal à 10^{18} euros.
[6] Source : www.carte-bleue.com
[7] Packaging
[8] Un jeu d'enchères

Ce jeu est *a priori* sans fin, mais en pratique il est plausible d'en imaginer une en intégrant le fait que les deux joueurs ont à disposition une somme d'argent finie à investir.
Pour une étape donnée, l'encarteur à tout intérêt à jouer I, les deux gains possibles dans ce cas étant supérieurs à ceux du choix $\bar{I}$. Sachant que l'encarteur a joué I, le pirate doit également jouer I pour ne pas perdre. Les deux joueurs se livrent alors une surenchère continue en jouant à chaque tour I, tout en n'ayant pas intérêt à jouer $\bar{I}$. $(I\ ;\ I)$ est donc le seul équilibre de Nash[9][Nas50] en sous-jeux.
Ce point de vue permet d'établir les prérogatives de chacun des protagonistes. Ainsi, les Smart Cards ne peuvent qu'avoir un niveau de sécurité qui augmente, tandis que le pirate a quant à lui tout intérêt à développer sans cesse de nouvelles techniques d'attaques.
La section suivante dresse un inventaire des techniques utilisées par les pirates pour attaquer les Smart Cards.

3 Techniques d'attaque sur Smart Card.

Cette section dresse un inventaire des techniques d'attaques sur les Smart Cards.
La rivalité encarteur/pirate s'exprime ici par le développement de techniques d'attaque de la part du pirate, et par le développement de contre mesures de la part du concepteur de carte à puce.
La sécurité des Smart Cards est un enjeu de taille, si bien qu'il existe une littérature conséquente traitant du sujet. Les travaux de thèse de [Lia06] ainsi que ceux de [Akk03], de par leur aspect récents et complets, font office de référence.

3.1 Attaques invasives et non-invasives, actives et passives

L'intervention du pirate sur le dispositif peut être de deux types, invasive ou non-invasive.
Les attaques invasives sont celles qui consistent à détruire la carte afin d'obtenir des informations sur cette dernière, à l'aide par exemple de microscopes évolués. L'intérêt est cependant limité et les moyens nécessaires sont coûteux. En effet, au prix du matériel nécessaire il faut ajouter celui d'une carte à multiplier par le nombre d'essais effectués.
D'autre part, les méthodes non-invasives consistent en la déduction d'informations relatives à la carte par l'intermédiaire d'autres informations transitant sur le canal secondaire.
Le canal secondaire[10] regroupe l'ensemble des sources d'informations de la Smart Card pouvant laisser transparaître des données qui permettraient au pirate par traitement approprié d'en déduire des éléments constitutifs de la carte ou encore percer des algorithmes cryptographiques. Ces sources peuvent être des consommations électriques mesurées sur des fuites de courant, des rayonnements électromagnétiques ou sonores, le résultat d'un calcul ayant subi une attaque par injection de fautes, ou tout autre source du moment que la mesure de cette dernière apporte de l'information sur le fonctionnement de la carte. Le piratage des cartes à puce passe donc par l'exploitation d'informations issues du canal secondaire. Précurseur dans le domaine, Kocher propose bon nombre de contributions sur les techniques d'attaques des Smart Cards, dont certaines devenues incontournables [Koc98].
Parmi les informations circulant dans ce canal secondaire, certaines sont identifiées puis utilisées par les pirates, à partir desquelles ils peuvent concevoir des techniques d'attaque.
Une attaque est qualifiée d'active si celle-ci communique des informations à la carte, elle est qualifiée de passive lorsqu'elle se contente de prélever des informations.

[9] Exprime l'absence de regrets.
[10] Encore appelé canal caché, de l'anglais side channel.

3.1.1 Les attaques en temps

Cette famille d'attaques a été introduite par Kocher [Koc96]. Cette dernière est basée sur le fait que le temps d'exécution d'un algorithme cryptographique est accessible à partir de l'horloge interne de la Smart Card. Le principe de fonctionnement d'une attaque en temps consiste alors à exploiter la connaissance de cette donnée, en utilisant le résultat proposé par Kocher établissant un lien entre le temps d'exécution de l'algorithme et les informations qu'il traite.

3.1.2 Les attaques par rayonnements

Lorsque la carte est en activité, les composants sollicités rayonnent des informations, par voie électromagnétique. Il est alors possible, par l'intermédiaire d'un banc de mesure, de prélever ces informations puis de les exploiter afin d'identifier l'activité effectuée par la carte au moment de la mesure [Qui01].
De même, les informations sonores peuvent être recueillies à l'aide d'un capteur acoustique puis exploitées. Ces techniques sont en devenir.

3.1.3 Les attaques par injection de fautes

Un moyen pour le pirate d'arriver à ses fins est d'introduire des erreurs dans les codes cryptographiques en profitant d'une faille algorithmique. Ces erreurs, anciennement induites par une surchauffe des composants, sont à présent provoquées par l'intermédiaire d'une action consistant à "secouer" l'alimentation, c'est-à-dire consistant à alimenter la carte avec une tension de forte mais brève amplitude, ou par l'intermédiaire de rayonnements, LASER ou d'autre types. Dans ce cas, le canal secondaire d'attaque sert de porte d'entrée aux données provoquant cette faute. Il peut s'agir par exemple du circuit test[11] présent sur la carte.

3.1.4 Les attaques en puissance

Les Smart Cards ne sont pas auto-alimentées. Le courant dont elles ont besoin est fourni par le lecteur. Ainsi, lorsque la carte effectue une opération, elle consomme du courant, et il est possible de mesurer cette consommation sur les fuites de courant présentes aux noeuds d'alimentation.
Le pirate peut alors, à partir de relevés de consommation, déduire par traitements spécifiques quelles opérations a effectué la carte, ou encore des valeurs de clef cryptographique. Ce type d'attaque est connu sous le nom d'attaque en puissance [Aig01]. Les plus connues sont la SPA[12] et la DPA[13]. Ces techniques sont largement décrites dans [Koc99].
Sommairement, la SPA consiste à étudier des consommations de courant relevées lors de l'exécution d'un code cryptographique, puis à identifier les opérations effectuées. Le DPA consiste à envoyer un message clair à l'algorithme cryptographique puis à construire un test d'hypothèses pour décider si oui ou non le message clair a été codé avec une clef à trouver. Si bien que lorsque le message est codé avec la bonne clef, un pic de détection apparaît. Pour fonctionner, cette technique requiert un nombre de signatures suffisamment important pour que le test soit significatif. Des variantes de la DPA telles que la HDPA[14] consistent à prendre en compte des points particuliers sur les relevés de consommation et les ajouter au test d'hypothèse pour augmenter la pertinence de ce dernier.

[11] Chip test en anglais
[12] Simple Power Analysis.
[13] Differential Power Analysis.
[14] High order Differential Power Analysis

Ce type d'attaque est très efficace et de nombreuses contre-mesures sont à l'étude, dans le domaine matériel et par le traitement du signal.
La classification des techniques d'attaque présentées est la suivante : celles nécessitant de fournir une information à la carte, comme l'injection de fautes, sont qualifiées d'actives. Les autres, se contentant de mesurer les informations comme une consommation de courant par exemple sont qualifiées de passives.

3.2 Conclusions

Cette section a permis de dresser un bref inventaire des techniques d'attaque destinées à exploiter les failles de sécurité d'une Smart Card. Ces failles, regroupées dans la notion de canal secondaire, proviennent d'origines physiques diverses. Dans le cadre des attaques en puissance, le leitmotiv du pirate est : "dis-moi ce que tu consommes et je te dirai qui tu es, et ce que tu es en train de faire.".
La qualité des résultats de telles attaques n'est plus à prouver, cela dit leur succès est conditionné par une hypothèse implicite très forte : les données à disposition correspondent bien à ce qui a été effectivement consommé par la carte[15].
Alors, une façon de répondre aux attaques en puissance consiste à masquer les signaux de consommation sur le canal secondaire, de sorte à fournir au pirate de fausses signatures ne pouvant alors que conduire à de fausses interprétations.
Donc, le fait de masquer ces consommations complique fortement la tâche du pirate, ce dernier étant leurré en raisonnant sur des consommations qui ne sont pas caractéristiques de la vraie consommation. Les techniques de masquage des signaux proposées dans cette thèse et présentées dans la section suivante, appliquées aux signaux issus de fuites de courant sur canal caché, servent donc de rempart aux attaques en puissance réalisées sur canaux cachés.

4 Plan de l'exposé

Ce premier chapitre permet de se plonger dans l'univers des cartes à puce et se pose la question de leur sécurisation. Par conception, ces dernières sont vulnérables sur différents points, autant de pistes pour les pirates qui ne cessent de développer des techniques d'attaque pour percer ses secrets.
Les techniques d'attaque en puissance permettent à partir de relevés de consommation de courant, pendant l'activité de la carte, de trouver des informations cachées. Une réponse possible à ces attaques consiste à développer des techniques originales de masquage des signaux à l'aide de techniques de traitement du signal, c'est l'objet de cette thèse. Il est clair que les techniques développées n'ont de valeur que si elles sont compatibles avec la technologie Smart Card, respectant entre autre la notion de conservation de la puissance.

La plupart des algorithmes cryptographiques ont besoin d'un générateur de nombres pseudo-aléatoires performant pour fonctionner, c'est-à-dire un dispositif capable de fournir des séquences assimilables à la réalisation d'un processus aléatoire. Il en est de même pour une des deux approches de masquage des signaux proposées, voilà pourquoi le second chapitre présente la réalisation d'un générateur pseudo-aléatoire, basé sur un système dynamique chaotique. Ce travail est réalisé en parallèle à celui d'un microélectronicien qui lui est chargé de concevoir le circuit correspondant.
Le système dynamique est obtenu après transformation de l'équation différentielle non-linéaire

[15] Les données sont intègres.

régissant le comportement du circuit. Ce dernier est alors étudié en profondeur afin d'en extraire ses propriétés et de montrer qu'il peut évoluer,sous certaines conditions, en mode chaotique. La notion de Chaos est alors définie et mise en évidence.
A partir du système évoluant en régime chaotique, un flux binaire est créé selon une approche originale, puis passé au crible de tests permettant d'affirmer ou non que ce dernier, construit de la sorte, est pseudo-aléatoire. Si le flux possède cette propriété, alors la succession des symboles 0 et 1 peut être considérée comme imprévisible. Une étude comparative est alors réalisée entre un flux issu de simulations numériques et un flux issu de l'échantillonnage d'un signal réel.

Le troisième chapitre présente une première technique de masquage appelée masquage par décomposition des signaux. Son principe est de substituer à une consommation de courant les coefficients de son développement sur une base de fonctions déterministes pondérées par des variables aléatoires décorrélées.
La base de Karhunen-Loève jouissant de ces propriétés, c'est sur cette dernière que les signaux vont être développés. Les éléments de la base ainsi que les coefficients associés doivent être déterminés, voilà pourquoi les fondements mathématiques justifiant un tel développement sont présentés, s'appuyant sur les résultats de l'analyse hilbertienne. En particulier, pour assurer la décorrélation des coefficients, les fonctions de base se doivent d'être solution d'une équation intégrale, il sera montré que cela revient à déterminer les éléments propres d'un opérateur compact d'Hilbert-Schmidt. Le principe général de substitution des coefficients est en suite donné, incluant entre autre une phase de permutation pseudo-aléatoire réalisée à l'aide des résultats du chapitre II. Le principe est alors décliné à travers cinq techniques nécessitant des moyens différents et conduisant à des résultats différents. leurs performances sont évaluées en termes de décorrélation statistique à l'ordre deux.
Les techniques servent alors au masquage d'un grand nombre de réalisations de consommation de courant de Smart Card fournies par ST Microelectronics. Les résultats obtenus sont encourageants, validés par ST Microelectronics sur le plan théorique, mais ce type d'approche ne respecte pas suffisamment les contraintes technologiques imposées et ceci en termes de complexité d'implantation électronique. En particulier, la technologie de conception actuelle ne permet pas la réalisation de certaines parties de la technique proposée. Cette restriction constitue l'intérêt d'une autre technique de masquage, présentée au chapitre suivant.

Dans le quatrième chapitre, une nouvelle technique de masquage est présentée, basée sur un modèle paramétrique des signaux. Elle consiste à estimer la consommation de courant à travers des paramètres la caractérisant, puis à partir de la connaissance de ces paramètres, à créer une contre signature faisant office de signal masqué. Dans cette partie seule l'extraction des paramètres a été réalisée, laissant le soin aux microélectroniciens de concevoir le circuit de contre mesure.
L'activité de courant est modélisée selon la notion de macromodèle. Caractérisé par Kussener [Kus02], le macromodèle est un ensemble d'inverseurs pilotés de sorte à reproduire l'activité de courant d'un microprocesseur de Smart Card. De cette modélisation électronique, il ressort qu'une activité de courant peut être vue comme la superposition d'activités de courant élémentaires, chacune d'entre elles pouvant être modélisée par une fonction de la famille gaussienne[16], paramétrée par son amplitude, sa localisation et son support temporel. La question de l'estimation du paramètre inconnu est alors posée. Parmi les techniques d'estimation disponibles, celle du maximum de vraisemblance est retenue. L'estimation de ce paramètre dans sa globalité n'est cependant pas un problème simple, en raison de la non-convexité de la fonction coût associée aux mesures et dépendant du paramètre. Devant ce problème, la notion de condition initiale pertinente devient une notion très importante.

[16]Inspirée de la densité de probabilité gaussienne.

Pour mener à bien cette phase d'optimisation, une proposition consiste à utiliser de façon couplée une technique d'estimation du maximum de vraisemblance et une technique de détection : l'algorithme expectation-maximization (EM) avec le filtrage adapté stochastique (FAS) utilisé en détection. Le choix de l'algorithme EM réside dans le fait qu'il permet de ramener l'estimation de K cellules, à K estimations d'une seule cellule. Par ailleurs, le rôle joué par le FAS est primordial en ce sens qu'il permet d'une part de rejeter tout ce qui ne s'apparente pas à du signal utile dans l'observation et d'autre part, à approcher au mieux les paramètres inconnus fournissant ainsi la condition initiale *adequat* à l'algorithme EM, facilitant ainsi sa convergence vers le paramètre voulu. Ce doublet FAS-EM donne des résultats très encourageants dans le cas de signatures fabriquées numériquement, mais également avec des données réelles, permettant d'obtenir des résultats supérieurs à ceux obtenus avec des techniques d'estimation classiques.

CHAPITRE II

CARACTÉRISATION D'UN SYSTÈME DYNAMIQUE NON-LINÉAIRE DE LA FAMILLE DOUBLE SCROLL. ROUTE VERS LE CHAOS, APPLICATION À LA GENÈSE DE NOMBRES PSEUDO-ALÉATOIRES

1 INTRODUCTION

Le but de ce chapitre est d'étudier le comportement d'un système dynamique en régime chaotique, puis de tirer parti des propriétés de ce dernier pour concevoir un générateur de nombres pseudo-aléatoires. Ce générateur, une fois validé, est utilisé pour effectuer des permutations pseudo-aléatoires dans la technique de masquage par décomposition des signaux présentée au chapitre suivant.
Cette étude est menée parallèlement aux travaux de thèse de V. Telandro, dont le but est de concevoir un circuit électronique analogique capable de générer un flux pseudo-aléatoire. L'objectif est donc d'étudier en profondeur le système dynamique associé au circuit, puis de concevoir un générateur pseudo-aléatoire à partir de ce système. Ce générateur sera un outil indispensable lors de la mise en oeuvre de la technique de masquage par décomposition des signaux du chapitre *III*. De plus, les propriétés mises en exergue servent à faire prendre à V. Telandro les choix de paramètres les plus judicieux possible, et prouvent que le travail qu'il mène repose sur des théories bien fondées.
Ces travaux sont utiles dans la mesure où le fonctionnement des SmartCards est tel que ses activités sont sécurisées par des algorithmes de cryptographie s'appuyant pour la plupart d'entre eux sur un générateur de nombre pseudo-aléatoire, évidemment le plus robuste possible, d'où l'importance d'une telle étude.
L'enjeu et l'originalité du travail consistent en la façon de créer un flux pseudo-aléatoire, sur la base de concepts théoriques respectant les contraintes de faisabilité imposées aux microélectroniciens[1], aboutissant à des techniques performantes et suffisamment simples pour être implémentées.
La clef de voûte de la technique proposée repose sur l'étude d'un système dynamique en régime chaotique, et par conséquent nécessite de visiter la théorie du Chaos, en partie du moins. Aussi

[1]Le flux ne peut être crée que par une série d'opérations simples (additions, multiplications), à partir d'un générateur en mode stable

complexe à étudier que passionnante, la théorie du Chaos déterministe est un des rares domaines des mathématiques capable de susciter l'intérêt des chercheurs de bon nombre de communautés, en particulier dans le domaine de la physique, de la chimie, de la biologie, des sciences économiques et sociales, et la curiosité du grand public. Preuve en est le nombre important d'articles relatifs au thème du Chaos parus dans la presse dite grand public. Le dictionnaire associe au mot chaos[2] la définition plus qu'intuitive suivante :

Désordre épouvantable, confusion générale.

Ainsi, la science du chaos consiste en l'étude des équations différentielles déterministes modélisant des systèmes physiques qui sous certaines conditions peuvent avoir un comportement fortement désordonné au cours de son évolution dans le temps, bien que régi par des équations simples, en tout cas déterministes. Le système évolue alors en régime chaotique. Ce type de phénomène peut être mis en évidence avec des systèmes discrets de dimension ≥ 1 et pour des systèmes continus de dimension ≥ 3.

Le chaos peut être vu comme une frontière abstraite entre ce qui est déterministe et ce qui est aléatoire. Phénoménologiquement parlant, un comportement chaotique peut être considéré comme un phénomène déterministe compliqué mais en aucun cas aléatoire[3]. Essayant de clarifier cette nuance pour le moins subtile, Poincarré, qui a beaucoup contribué au développement de cette science à une époque où les ordinateurs n'existaient pas, parle de ce qui "échappe à notre discernement".

De même que le calcul scientifique, la théorie du chaos a connu un essor particulièrement fulgurant dès l'avènement des calculateurs, permettant ainsi de visualiser puis d'expliquer des résultats jusqu'ici impossibles à établir, pire encore, impossibles à conjecturer puisque échappant à l'intuition.

Par exemple, la suite de Lehmer définie par

$$\begin{cases} u_{n+1} & \equiv & au_n + b \quad [M] \\ u_0 & & \text{donné} \end{cases},$$

avec $a = 16807$, $b = 0$ et $M = 2^{31} - 1$ est une suite chaotique, en dépit de la simplicité de son expression. Ses termes successifs sont difficilement prévisibles. Le déclic est venu de Lorenz, météorologue au M.I.T. qui en 1963, alors qu'il travaille sur un modèle d'atmosphère terrestre a mis en exergue un objet aux propriétés mathématiques atypiques, appelé, depuis les travaux de Ruelle et Takens en 1971, attracteur étrange [Rue80], caractéristique d'un comportement chaotique.

Depuis les premières découvertes des pionniers, les travaux de recherche sur le chaos ne cessent d'abonder dans tous les domaines, tant le travail à accomplir est encore important. Par exemple, le contrôle de l'apparition de tourbillons dans les écoulements turbulents est un enjeu majeur des mécaniciens des Fluides.

Il n'y avait donc aucune raison pour que l'Électronique échappe à cette déferlante chaotique vu que de façon générale, un circuit est régi par une équation différentielle dépendant de paramètres fixés par la physique du problème[4] et d'autres, appelés paramètres de contrôle, pouvant varier sur une certaine plage de valeurs admissibles. Cette équation est non-linéaire dès lors qu'il existe un composant dit non-linéaire dans le circuit. Ainsi, ce genre de circuits sont des candidats potentiels au chaos, car pouvant présenter des modes de fonctionnements, bien que stables, franchement désordonnés. Parmi la famille de circuits de ce type, une se distingue particulièrement tant le nombre d'articles à son sujet est impressionnant, la famille Double-Scroll[5]. L'étude et la

[2]Dans certains ouvrages, la distinction est faite entre le paradigme "Chaos" et le nom commun "chaos".

[3]Par exemple le cours de la bourse, la météo, la formation de tourbillons dans un écoulement turbulent

[4]Valeurs de capacités, de self, de transconductance par exemple

[5]L'anglicisme est ici conservé tant le mot est devenu est paradigme.

caractérisation de ces circuits la plus remarquable est celle de Chua, dans la contribution [Chu86] il démontre rigoureusement l'existence du chaos dans la famille Double-Scroll, s'appuyant sur les travaux de Shil'nikov expliqués dans [Shi93]. Les travaux de Kennedy, à force de didactique comme par exemple dans [Ken93], permettent de comprendre les nombreux problèmes liés à la conception de tels circuits, ces derniers devant respecter la maxime " faible coût, faible puissance" en fonction de la technologie de conception utilisée. Voilà pourquoi plusieurs déclinaisons de circuits appartenant à la famille Double-Scroll sont nées, comme le montre [Rad03]. C'est d'ailleurs sur la base de cet article qu'ont débuté les travaux de Telandro.
Ce chapitre est donc consacré à l'étude du système différentiel non-linéaire régissant ce circuit. Il va être montré que ce dernier peut se comporter de façon chaotique et ainsi, profitant du désordre engendré, servir de générateur de flux pseudo-aléatoire.

L'étude commence par la modélisation mathématique du problème, étape importante puisque assurant la continuité entre les travaux de Telandro et le début de ceux présentés ici. Cette étape permet de passer d'un problème composé d'une équation différentielle du troisième ordre non-linéaire obtenue en appliquant les lois physiques aux noeuds du circuit et un jeu de conditions initiales, à un problème équivalent adimensionné, comprenant un système différentiel non-linéaire de dimension 3 accompagné de trois conditions initiales, ne dépendant plus que du paramètre de contrôle.
L'étape suivante consiste à écrire le problème discret associé au système dynamique étudié (continu), puis vérifier que le premier converge vers le second lorsque le pas de discrétisation tend vers 0. Le schéma numérique proposé est celui de Runge-Kutta [Lam91].
Le modèle étant posé et les outils de simulation numérique affûtés, l'étape suivante concerne l'étude locale de la dynamique du système autour de ses points fixes. Cette étape renseigne sur la stabilité locale du système et permet par suite de dégager les valeurs du paramètre de contrôle candidates au chaos en vérifiant que la première hypothèse du théorème de Shil'nikov est vérifiée.
De la dynamique locale à la dynamique globale il n'y a qu'un pas, qu'il convient de franchir en regroupant les éléments localement établis, puis en vérifiant qu'alors, les indicateurs du chaos sont positifs, à savoir que : la seconde hypothèse du théorème de Shil'nikov est vérifiée, le système a un exposant de Lyapunov positif, le spectre du signal temporel solution du problème est riche en fréquences.
Le chaos étant alors établi, l'étude se penchera, en vue d'une application future, sur l'analyse de la distribution des points de la trajectoire sur une section de Poincarré particulière.
Le flux pseudo-aléatoire est alors créé par le biais d'une succession d'opérations sur des signaux spécifiques débouchant à la donnée du dit flux, une suite de 0 et de 1.
Enfin, une phase d'expérimentations consistera à caractériser statistiquement le flux généré avec celui de Telandro, permettant ainsi de proposer à ce dernier des solutions objectives lui permettant d'affirmer que son générateur présente les propriétés requises. Le choix est fait d'utiliser 5 tests statistiques faisant partie de la norme internationale de standard FIPS$140-1$ **??**.

2 MODÉLISATION

Dans le cadre du thème de recherche "gestion d'énergie" des Smart Cards de ST Microelectronics, les travaux de V. Telandro l'ont conduit à concevoir un circuit de technologie CMOS sur la base de l'étude proposée par Radwan et al. [Rad03].
L'objet de cette section est de transformer l'équation différentielle régissant ce circuit en un système dynamique non-linéaire tri-dimensionnel. Le formalisme adopté sera utilisée tout au long de ce chapitre.

Le circuit est régi par le système composé d'une équation différentielle du troisième ordre à coefficients constants et d'un jeu de conditions initiales,

$$(P)\begin{cases} \dfrac{d^3}{dt^3}\mathrm{V}_x - a\dfrac{g}{C}\dfrac{d^2}{dt^2}\mathrm{V}_x - a\left(\dfrac{g}{C}\right)^2\dfrac{d}{dt}\mathrm{V}_x - a\left(\dfrac{g}{C}\right)^3\mathrm{V}_x = -aV_R\left(\dfrac{g}{C}\right)^3 h_\epsilon(\mathrm{V}_x) \\ \mathrm{V}_x(0) = \mathrm{V}_{x_0} \quad \dfrac{d}{dt}\mathrm{V}_x(0) = \mathrm{V}_y \quad \dfrac{d^2}{dt^2}\mathrm{V}_x(0) = \mathrm{V}_z \end{cases} \tag{II.1}$$

où $\mathrm{V}_x(t)$ est la tension en Volts aux bornes du circuit vérifiant (P), V_R est la tension de référence en Volts, g est la transconductance en Siemens et C la capacité en Farad, a un paramètre de contrôle scalaire réel sans unité, les conditions initiales sont données en Volt pour V_{x_0}, en Volt/seconde pour V_y et en Volt/seconde^2 pour V_z. Le cheminement permettant d'aboutir au système (P) fait appel à des considérations physiques et électroniques rigoureusement détaillées dans [Tel06].
L'application non-linéaire [6] h_ϵ présente dans le second membre de l'équation différentielle est définie pour tout $u \in \mathbb{R}$ par

$$h_\epsilon(u) := \begin{cases} -1 & \text{si} \quad u < -\epsilon \\ \dfrac{1}{\epsilon}u & \text{si} \quad u \in [-\epsilon, \epsilon[\\ 1 & \text{si} \quad u \geq \epsilon \end{cases}, \tag{II.2}$$

avec $\epsilon < 1$. Cette dernière modélise un comparateur à seuil, elle est continue sur $\mathbb{R}$.

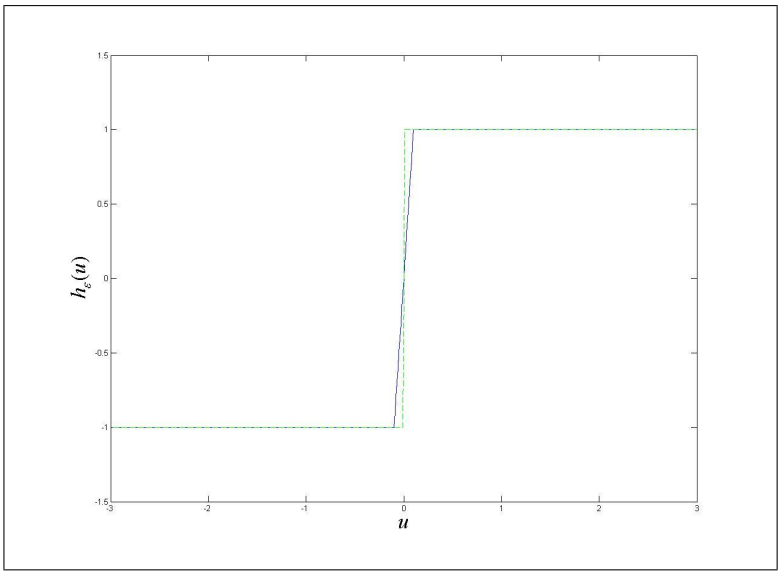


FIG. 1 – *Représentation graphique de h_ϵ avec $\epsilon = 10^{-1}$ en trait plein superposé à celle de $sign$ en traits pointillés*

[6] Car linéaire par morceaux

Remarque : *Intuitivement, l'application h_ϵ est définie de la sorte car*

$$\lim_{\epsilon \to 0} h_\epsilon(u) \quad = \quad sign(u).$$

Comme le montre la figure 1, l'application h_ϵ avec ϵ suffisamment petit est structurellement proche de la fonction $sign$, à ceci près qu'au voisinage de l'origine, h_ϵ est de coefficient directeur $1/\epsilon$ alors que $sign$ présente un saut brusque de -1 vers $+1$ matérialisé par un coefficient directeur infini. Or, certains écrivent le problème (P) en utilisant la fonction $sign$ au lieu de l'application h_ϵ , par exemple [Rad03], mais cela ne constitue qu'un cas limite, une vue de l'esprit qui ne saurait en aucun cas modéliser un phénomène réel. En effet, d'une part, en physique, une transition d'un état vers un autre ne peut pas être spontanée. Elle dure un certain temps, aussi petit soit-il, ce qui interdit unemodélisation par un saut vertical. D'autre part, pour tout $u \in \mathbb{R}$ la fonction $sign(u)$ est continue par morceaux, avec une discontinuité de première espèce en $u = 0$ et dérivable au sens des distributions, sa dérivée vaut $2\delta(u)$. D'autre part, $h_\epsilon(u)$ est continue sur $\mathbb{R}$ avec deux points anguleux en $u = \pm\epsilon$, dérivable au sens des fonctions, sa dérivée vaut $h_\epsilon^{'}(u) = \dfrac{1}{\epsilon}\Pi_\epsilon(u)$[7]. Alors, il vient

$$\lim_{\epsilon \to 0} h_\epsilon^{'}(u) = 2\delta(u).$$

Donc, la limite de la dérivée de h_ϵ tend vers la dérivée de $sign$.
Ce résultat est une conséquence directe du théorème III.7 du chapitre suivant.

Afin d'établir les propriétés mathématiques du système, il convient d'adimensionner ce dernier. Cela se fait par l'intermédiaire du changement de variable linéaire

$$x \quad := \quad \frac{\mathrm{V}_x}{V_R},$$

et de la définition d'un nouvel opérateur de dérivation temporelle

$$[\ \dot{}\ ] \quad := \quad \frac{C}{g}\frac{d}{dt}[\quad].$$

Cette phase de transformations s'effectue sans peine, en considérant notamment la linéarité de l'opérateur dérivée. Par suite, le problème (P) d'inconnue $x(t)$ s'écrit

$$(P) \begin{cases} V_R\left(\dfrac{g}{C}\right)^3 \dddot{x} - aV_R\left(\dfrac{g}{C}\right)^3 \ddot{x} - aV_R\left(\dfrac{g}{C}\right)^3 \dot{x} - aV_R\left(\dfrac{g}{C}\right)^3 x = -aV_R\left(\dfrac{g}{C}\right)^3 g_\eta(x) \\ x(0) = \dfrac{\mathrm{V}_x}{V_R} \quad \dot{x}(0) = \dfrac{\mathrm{V}_y}{V_R} \quad \ddot{x}(0) = \dfrac{\mathrm{V}_z}{V_R} \end{cases},$$

avec $\eta := \epsilon/V_R$, et g_η telle que pour tout $u \in \mathbb{R}$

$$g_\eta(u) := h_{\eta V_R}(V_R u) = \begin{cases} -1 & \text{si} \quad u < -\eta \\ \dfrac{1}{\eta}u & \text{si} \quad u \in [-\eta, \eta[\\ 1 & \text{si} \quad u \geq \eta \end{cases},$$

[7] $$\Pi_T(t) := \begin{cases} 1 & \text{si} \quad t \in]-T\,;\,T] \\ 0 & \text{sinon} \end{cases}$$

et $g_\eta(u)$ a les mêmes propriétés que $h_\epsilon(u)$, en particulier $g_\eta^{'}(u) = \frac{1}{\eta}\Pi_\eta(u)$.

En constatant que le terme $V_R\left(\frac{g}{C}\right)^3$ est facteur commun différent de 0 et en redéfinissant les conditions initiales par

$$\begin{cases} x_0 = \dfrac{\mathbf{V}_x}{V_R} \\ y_0 = \dfrac{\mathbf{V}_y}{V_R} \\ z_0 = \dfrac{\mathbf{V}_z}{V_R} \end{cases},$$

il est possible d'exprimer le problème (P) sous sa forme adimensionnée (P_a)

$$(P_a)\begin{cases} \dddot{x} - a\ddot{x} - a\dot{x} - a\,x = -a\,g_\eta(x) \\ \\ x(0) = x_0 \quad \dot{x}(0) = y_0 \quad \ddot{x}(0) = z_0 \end{cases} \tag{II.3}$$

Il s'agit d'un problème de Cauchy composé d'une équation différentielle non-linéaire d'ordre 3 non-homogène à coefficients constants. Si $a < 0$, tous les coefficients sont positifs, le problème (P_a) est elliptique, alors que dans le cas contraire, si $a > 0$, le coefficient 1 associé à la dérivée troisième est positif alors que les autres coefficients $-a$ sont négatifs, dans ce cas (P_a) est un problème parabolique. Enfin, concernant le coefficient réel a, il s'agit du paramètre de contrôle du problème, de lui dépend directement la stabilité des solutions du problème.

> ***Remarque :*** *Si $a = 0$, le problème (P_0) consiste à trouver $x(t)$ vérifiant les conditions initiales, tel que $\dddot{x} = 0$. L'expression de $x(t)$ s'obtient de façon simple par trois intégrations successives,*
>
> $$x(t) \;=\; \frac{z_0}{2}t^2 + y_0 t + x_0.$$
>
> *La solution est naturellement indépendante de a et pour toute condition initiale non nulle avec $sign(z_0) > 0$,*
>
> $$\lim_{t\to+\infty} x(t) \;=\; +\infty.$$
>
> *Ainsi, la solution de (P_0) est non bornée. Cette solution est écartée, car elle ne correspond pas à une solution physiquement réalisable.*

Par le changement de variable canonique

$$\begin{cases} x \;:=\; x \\ y \;:=\; \dot{x} \\ z \;:=\; \dot{y} = \ddot{x} \end{cases},$$

l'équation différentielle du problème (P_a) se ramène de façon équivalente à l'étude du système dynamique autonome composé de trois équations différentielles non-linéaires du premier ordre, couplées

$$(P_a)\begin{cases} \dot{x} &=& y \\ \dot{y} &=& z \\ \dot{z} &=& a\,x + a\,y + a\,z - a\,g_\eta(x) \end{cases} \tag{II.4}$$

auquel est adjoint les conditions initiales

$$\left\{ \begin{array}{rcl} x(0) & = & x_0 \\ y(0) & = & y_0 \\ z(0) & = & z_0 \end{array} \right.$$

Soit X,$\dot{X}$ et X_0 trois vecteurs de $\mathbb{R}^3$ tel que

$$X = \left[\begin{array}{c} x \\ y \\ z \end{array} \right], \quad X_0 = \left[\begin{array}{c} x_0 \\ y_0 \\ z_0 \end{array} \right], \quad \dot{X} = \left[\begin{array}{c} \dot{x} \\ \dot{y} \\ \dot{z} \end{array} \right].$$

Soit A la matrice carrée d'ordre 3 dépendant de a définie par

$$A = \left[\begin{array}{ccc} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & a & a \end{array} \right],$$

et soit b le vecteur de $\mathbb{R}^3$ dépendant de x et de a tel que

$$b(X) = \left[\begin{array}{c} 0 \\ 0 \\ -a g_\eta(x) \end{array} \right].$$

Alors, le problème (P_a) s'écrit sous forme vectorielle

$$(P_a) \left\{ \begin{array}{ll} \dot{X} = AX + b(X) \\ X_0 \quad \text{donné} \end{array} \right. \tag{II.5}$$

Cette dernière formulation montre que la dynamique du problème est à chaque instant la contribution d'une partie linéaire AX et d'une partie non-linéaire $b(X)$. Afin d'étudier graphiquement la trajectoire du problème (P_a) qui est un système à trois degrés de liberté, l'espace des phases est choisi isomorphe à un ensemble borné de $\mathbb{R}^3$ muni de sa structure Euclidienne. Il faut de plus lui conférer une structure affine afin de pourvoir travailler dans un espace où vivent des points et des vecteurs.
Fort de cela, soit $F_a(X)$ l'application définissant le champ de vecteurs de $\mathbb{R}^3 \rightarrow \mathbb{R}^3$ dépendant du paramètre de contrôle scalaire réel a.

$$F_a(X) \quad := \quad AX + b(X).$$

L'application $F_a(X)$ est continue sur $\mathbb{R}^3$ pour tout réel a et pour tout $X \in \mathbb{R}^3$, de plus,

$$\begin{array}{rcl} \text{div}(F_a(X)) & = & \nabla . F_a(X) \\ & = & \dfrac{\partial}{\partial x}\big(y\big) + \dfrac{\partial}{\partial y}\big(z\big) + \dfrac{\partial}{\partial z}\big(a\,x + a\,y + a\,z - a\,g_\eta(x)\big) \\ & = & a. \end{array}$$

La divergence renseigne sur la propriété du champs à contracter ou non les volumes[8].Ainsi, si $a > 0$ le champ de vecteur $F_a(X)$ est dissipatif, alors que si $a < 0$ le champ de vecteur $F_a(X)$ est conservatif. Autant dire que dans le contexte de cette étude le cas $a \geq 0$ ne présente pas d'intérêt.

[8]Il est possible de montrer que si δV est un élément élémentaire de volume, alors $\frac{d}{dt}[\delta V] = div(F_a(X))\delta V$

3 CARACTÉRISATION DES SOLUTIONS

Avant de poursuivre l'étude du problème (P_a), il faut auparavant caractériser l'existence et l'unicité éventuelle de la solution pour un vecteur de conditions initiales X_0 donné.
D'une part, la solution existe car le champs de vecteurs $F_a(X)$ est continu pour tout $X \in \mathbb{R}^3$, *a fortiori* pour tout X de l'espace des phases.
D'autre part, la solution est unique en vertu du théorème suivant

Théorème II.1. *Soit k une constante réelle strictement positive telle que*

$$k \;:=\; |a| + \max(2\,;\,\frac{1}{\eta}),$$

alors, pour tout $X_1 = \begin{bmatrix} x_1 \\ y_1 \\ z_1 \end{bmatrix}$ *et* $X_2 = \begin{bmatrix} x_2 \\ y_2 \\ z_2 \end{bmatrix}$ *avec* $X_1 \neq X_2$,

$$\|F_a(X_2) - F_a(X_1)\| \;\leq\; k\|X_2 - X_1\|,$$

la norme choisie étant la somme du module de chaque composante[9].

La démonstration du théorème est présentée en annexe A.
Ainsi, le problème (P_a), muni d'une condition initiale fixée, a une solution unique, au moins deux fois continûment dérivable. Il faut par conséquent s'attendre à obtenir des solutions régulières.

4 PROBLÈME DISCRET ASSOCIÉ À (P_a)

Le problème (P_a) est issu de la modélisation du comportement de la tension aux bornes d'un circuit analogique, sa solution est donc une fonction continue, dans un espace de dimension infinie. Or, pour la suite de cette étude, il est nécessaire d'avoir à disposition un outil numérique permettant de calculer de façon approchée, mais aussi précisément que possible, les solutions de (P_a).
Pour ce faire, la démarche proposée consiste à construire un problème discret (P_a^h), où h est un paramètre scalaire de discrétisation, dont les solutions sont des vecteurs de dimension finie, tel que lorsque h tend vers 0, (P_a^h) tend vers (P_a)[10]. Ainsi, lorsque (P_a^h) est résolu en lieu et place de (P_a), l'erreur commise sur la solution est de l'ordre de $\mathcal{O}(h^q)$[11], avec q un entier le plus grand possible. Il est important de construire une méthode numérique précise dans le cas de l'étude de l'évolution des systèmes dynamiques non-linéaires car ces derniers peuvent avoir des solutions fortement fluctuantes et changeant de comportement brusquement. Le fait de travailler avec un schéma numérique précis permet de ne pas passer à côté d'informations pertinentes, en particulier dans les voisinages de l'espace des phases où les effets des non-linéarités du système sont prépondérantes. Dans le cas du problème (P_a), intuitivement, cette zone correspond au sous-espace de frontière les plans d'équation $x = \pm\eta$.

---

[9] $\|X\| = \sum_{i=1}^{3} |X_i|$

[10] Notion de consistance du schéma.

[11] Notion de stabilité du schéma.
La consistance et la stabilité entraînent la convergence du schéma numérique vers le problème continu.

4.1 Méthode de Runge-Kutta

Parmi l'arsenal de schémas numériques à disposition, la méthode des différences finies est particulièrement bien adaptée à la résolution de problèmes tels que (P_a), et la méthode de Runge-Kutta [Gea71], convergente en $\mathcal{O}(h^4)$ répond aux exigences de précision qui viennent d'être préconisées. Soit $F_a^h(X)$ le champ de vecteurs défini pour tout X de l'espace des phases par

$$F_a^h(X) \quad := \quad \frac{1}{6}\left(F_a(X) + 2K_2 + 2K_3 + K_4\right),$$

avec

$$\begin{cases} K_2 & := & F_a(X + \dfrac{h}{2}F_a(X)) \\ K_3 & := & F_a(X + \dfrac{h}{2}K_2) \\ K_4 & := & F_a(X + hK_3) \end{cases}$$

Cet opérateur discret est consistant car clairement,

$$\lim_{h\to 0} F_a^h(X) \quad = \quad F_a(X),$$

il est stable dans la mesure où, par analogie avec le théorème II.1, il existe une constante k_h telle que

$$\|F_a^h(X_2) - F_a^h(X_1)\| \quad \leq \quad k_h\|X_2 - X_1\|.$$

4.2 Définition et propriétés du problème discret (P_a^h)

Soit le problème discret (P_a^h) défini par

$$(P_a^h)\begin{cases} X_{i+1} = X_i + hF_a^h(X_i) \\ X_0 \quad \text{donné,} \end{cases} \tag{II.6}$$

où les $\{X_i\}_{i\in\mathbb{N}}$ sont des vecteurs de l'espace des phases inclus dans $\mathbb{R}^3$. Le problème (P_a^h), pour un jeu de conditions initiales donné, est consistant et stable, par conséquent le problème discret (P_a^h) converge vers son pendant continu : le problème (P_a).
Le calcul, conduisant à l'expression des trois composantes de l'opérateur $F_a^h(X)$, est donné en annexe B. Cette expression amène plusieurs remarques. Tout d'abord, X_{i+1}, pour i fixé, est obtenu à partir de X_i au prix de simples produits et sommes, les termes constants[12] peuvent être calculés *a priori*. Ainsi, travailler en amont en explicitant le schéma numérique entraîne une accélération du temps de calcul puisque le volume d'opérations arithmétiques élémentaires à effectuer pour une itération, à savoir 23 multiplications, 20 additions, et les 8 appels de la fonction scalaire g_η, peuvent être traités par une entité de calcul de façon très rapide, sans avoir à stocker un important volume de données. Par ailleurs, explicitée de la sorte, la méthode peut être aisément mise sous forme parallèle.
L'outil de résolution numérique présenté va servir tout au long de ce chapitre à simuler informatiquement le problème (P_a) par le biais du problème discret associé (P_a^h). Les précautions ont été prises pour s'assurer que la méthode proposée est rapide, précise, et surtout convergente, c'est-à-dire que lorsque le paramètre de discrétisation h est petit, résoudre (P_a^h) au lieu de (P_a) fait commettre une erreur en $\mathcal{O}(h^4)$ sur la solution.

[12] C'est-à-dire tout sauf x, y et z

Remarque : *Nul n'est besoin de choisir une méthode numérique plus précise ou plus élaborée, comme par exemple les méthodes à pas adaptatif, vu la régularité théorique des solutions.*

5 ÉTUDE DE LA NATURE ET DE LA STABILITÉ DES POINTS FIXES DU SYSTÈME DYNAMIQUE (P_a).

Les points fixes de (P_a), si toutefois ils existent, sont solution de $F_a(X) = 0$. L'objet de cette section est de trouver ces derniers et de caractériser leurs propriétés, conditionnant directement la nature de la dynamique du système étudié : le problème (P_a).

Proposition II.1. *Le système dynamique (P_a) a trois points fixes P_{-1}, P_0 et P_1 indépendants de a, de coordonnées dans l'espace des phases*

$$P_{-1} = \begin{bmatrix} -1 \\ 0 \\ 0 \end{bmatrix}, \quad P_0 = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}, \quad P_1 = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}.$$

Preuve .

$$\begin{aligned} F(X) = 0 \quad &\Leftrightarrow \quad AX + b(X) = 0 \\ &\Leftrightarrow \quad \begin{cases} y & = & 0 \\ z & = & 0 \\ a\,x + a\,y + a\,z - a\,g_\eta(x) & = & 0 \end{cases} \\ &\Leftrightarrow \quad \begin{cases} y & = & 0 \\ z & = & 0 \\ x & = & g_\eta(x) \end{cases} \end{aligned}$$

Par suite, les solutions de $x = g_\eta(x)$ sont $x = \{-1, 0, 1\}$ et par conséquent les points P_{-1}, P_0 et P_1 de l'espace des phase sont les points fixes du système (P_a).

□

Remarque : *D'un point de vue géométrique, P_{-1} est le symétrique de P_1 par rapport à P_0. Ces trois points sont portés par l'axe de la variable x dans l'espace des phases. De façon générale, vu que $F_a(-X) = -F_a(X)$, le point P_0, origine du repère, est centre de symétrie.*

La suite de cette section porte sur l'étude du comportement du système autour de ces trois points fixes. Cela consiste à étudier le comportement de la solution du système pour toute condition initiale au voisinage de chacun de ses points fixes. En approximation du premier ordre, la dynamique du système au voisinage d'un point fixe P du système est décrite par

$$\delta_{\dot{X}} \quad = \quad J_P[F_a(X)]\delta_X, \tag{II.7}$$

où $J_P[F_a(X)]$ est la matrice jacobienne 3×3 de l'application $F_a(X)$ calculée au point P, et δ_X

est une perturbation autour du point P représentée par le vecteur de $\mathbb{R}^3$

$$\delta_X := \begin{bmatrix} \delta_x - P_x \\ \delta_y - P_y \\ \delta_z - P_z \end{bmatrix}.$$

Cette démarche permet de caractériser la stabilité des solutions et donc de montrer que les trajectoires sont attirées ou repoussées par les points fixes selon que ces derniers soient stables ou instables.
La matrice jacobienne de $F_a(X)$ est pour tout $X \in \mathbb{R}^3$

$$J_P[F_a(X)] = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a(1 - \frac{1}{\eta}\Pi_\eta(x)) & a & a \end{bmatrix},$$

Remarque :

- *L'application $X \mapsto J_P[F_a(X)]$ n'est pas continue en $X = \pm \begin{bmatrix} \eta \\ 0 \\ 0 \end{bmatrix}$.*
- *La contribution non-linéaire $b(X)$ de la dynamique est nulle dès lors que la composante x du vecteur X est telle que $|x| > \eta$*

La stabilité locale du problème (P_a) autour de ses deux points fixes est déterminée par l'intégration du système différentiel linéaire du premier ordre à coefficients constants

$$\begin{cases} \delta_{\dot{X}} &= J_P[F_a(X)]\,\delta_X \\ \delta_{X_0} & \text{vecteur donné} \end{cases}, \tag{II.8}$$

qui une fois intégré donne la solution

$$\delta_X(t) \;=\; e^{J_P[F_a(X)]t}\delta_{X_0},$$

continue par rapport à δ_{X_0}. Si $J_P[F_a(X)]$ est diagonalisable, la résolvante $e^{J_P[F_a(X)]t}$ du problème est une matrice telle que $e^{J_P[F_a(X)]t} = \Lambda e^{Dt}\Lambda^{-1}$, où D est la matrice diagonale contenant les valeurs propres de $J_P[F_a(X)]$, où Λ est la matrice de passage de la base associée à $J_P[F_a(X)]$ vers la base associée à D. Λ a pour colonnes les vecteurs propres de $J_P[F_a(X)]$. De plus, si A est diagonalisable avec des valeurs propres toutes de multiplicité 1, la solution $\delta_X(t)$ s'écrit, dans la base orthogonale $\{V_i\}_{i=1\ldots3}$ formée des vecteurs propres de $J_P[F_a(X)]$ qui dépendent de a,

$$\delta_X(t) \;=\; \beta_1 e^{\lambda_1 t}V_1 + \beta_2 e^{\lambda_2 t}V_2 + \beta_3 e^{\lambda_3 t}V_3,$$

avec $(\beta_1\,;\,\beta_2\,;\,\beta_3) \in \mathbb{R}^3_*$ dépendant de a et de δ_{X_0}. Autrement dit, la solution est une combinaison linéaire d'exponentielles éventuellement complexes. Pour chacune d'entre elles,

$$|e^{\lambda_j t}| = |e^{(Re[\lambda_j]+iIm[\lambda_j])t}| \;<\; e^{Re[\lambda_j]t} \quad \forall j = 1\ldots3. \tag{II.9}$$

Ainsi, la perturbation initiale δ_{X_0} s'amplifie , stagne ou est amortie au cours du temps selon que la partie réelle de chaque valeur propre de A correspondant à cette direction soit positive, nulle

ou négative. La partie imaginaire des valeurs propres est la contribution rotative correspondant à chacune des 3 valeurs autour du point fixe, dans le sens trigonométrique si la partie imaginaire est positive, et inversement.
Les deux prochaines sections sont consacrées à l'étude des points fixes P_{-1}, P_0 et P_1 du système (P_a) linéarisé autour de ces points. Le but est, à défaut de pouvoir décrire la dynamique du système non-linéaire d'une seule traite, de décrire la dynamique locale du système au voisinage de chaque sous-ensemble de l'espace des phases assujettis à perturber l'évolution de ce dernier, en l'occurrence les points fixes.

5.1 Caractérisation des points fixes P_{-1} et P_1

L'étude des points fixes P_{-1} et P_1 peut être menée conjointement car, en rappelant que $|\eta| < 1$

$$J_{P_{-1}}[F_a(X)] \quad = \quad J_{P_1}[F_a(X)] = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a & a & a \end{bmatrix} = A.$$

Les matrices Jacobiennes $J_{P_{-1}}[F_a(X)]$ et $J_{P_1}[F_a(X)]$ sont identiquement égales à A, donc de dimension 3×3 et indépendants de X.

Proposition II.2. *Les valeurs propres λ_1, λ_2 et λ_3 de A sont solutions de*

$$\lambda^3 - a\lambda^2 - a\lambda - a \quad = \quad 0,$$

et pour tout $a \neq 0$,

$$\begin{aligned} \lambda_1 &\in \mathbb{R} \\ \lambda_2 \in \mathbb{C} &= \alpha + i\omega \\ \lambda_3 \in \mathbb{C} &= \overline{\lambda_2}. \end{aligned}$$

La preuve de cette proposition est présentée en annexe C.
Par suite, les vecteurs propres permettent d'avoir une indication sur la direction du flot au voisinage des points fixes. Dans le cas des points fixes P_{-1} et P_1, les vecteurs propres V_1, V_2, V_3 respectivement associés aux valeurs propres λ_1,λ_2,λ_3 sont déterminés $\forall j = 1 \ldots 3$ par la relation d'équivalence

$$\begin{aligned} \Big[V_j \textit{ est vecteur propre de } A\Big] \quad &\Leftrightarrow \quad \Big[V_j \in \text{Ker}(A - \lambda_j Id)\Big] \\ &\Leftrightarrow \quad \Big[V_j \textit{ est solution de } (A - \lambda_j Id)X = 0 \quad \forall X \neq 0\Big] \end{aligned}$$

Or, pour tout $X \neq 0$ de l'espace des phases,

$$\begin{aligned} (A - \lambda_j Id)X \quad &= \quad 0 \Leftrightarrow \\ \begin{bmatrix} -\lambda_j & 1 & 0 \\ 0 & -\lambda_j & 1 \\ a & a & a - \lambda_j \end{bmatrix} X \quad &= \quad 0. \end{aligned}$$

Le vecteur X est de composantes $[x, y, z]^T$, donc le système d'équation équivalent est

$$\begin{cases} -\lambda_j x + y = 0 \\ -\lambda_j y + z = 0 \\ ax + ay + (a - \lambda_j)z = 0 \end{cases} \Leftrightarrow$$

de solutions

$$\left\{\begin{array}{l} y=\lambda_j x \\ z=\lambda_j y=\lambda_j^2 x \\ ax+ay+az-\lambda_j z=0 \end{array}\right. \Leftrightarrow$$

$$\left\{\begin{array}{l} y=\lambda_j x \\ z=\lambda_j y=\lambda_j^2 x \\ ax+a\lambda_j x+a\lambda_j^2 x-\lambda_j^3 x=0 \end{array}\right. \Leftrightarrow$$

$$\left\{\begin{array}{l} y=\lambda_j x \\ z=\lambda_j y=\lambda_j^2 x \\ -(\underbrace{-a-a\lambda_j-a\lambda_j^2+\lambda_j^3}_{=0})x=0 \end{array}\right.$$

car $X \neq 0$ et λ_j est naturellement solution du polynôme caractéristique. Les solutions de cette équation sont de la forme $\mathbb{R}[1\,;\,\lambda_j\,;\,\lambda_j^2]^T$, et ainsi, les vecteurs propres regroupés en colonnes dans la matrice de passage Λ sont,

$$\begin{aligned} \Lambda &= \left[\begin{array}{ccc} | & | & | \\ V_1 & V_2 & V_3 \\ | & | & | \end{array}\right] \Leftrightarrow \\ \Lambda &= \left[\begin{array}{ccc} 1 & 1 & 1 \\ \lambda_1 & \lambda_2 & \overline{\lambda_2} \\ \lambda_1^2 & \lambda_2^2 & (\overline{\lambda_2})^2 \end{array}\right] \Leftrightarrow \\ \Lambda &= \left[\begin{array}{ccc} 1 & 1 & 1 \\ \lambda_1 & \alpha+i\omega & \alpha-i\omega \\ \lambda_1^2 & (\alpha^2-\omega^2)+i(2\alpha\omega) & (\alpha^2-\omega^2)-i(2\alpha\omega) \end{array}\right]. \end{aligned}$$

A la valeur propre réelle λ_1 correspond le vecteur propre V_1 et aux valeurs propres complexes conjuguées λ_2 et λ_3 correspond le plan engendré par les vecteurs $Re[V_2]$ et $Im[V_2]$. Tout point $[x,y,z]^T$ de l'espace des phases appartient au plan si les trois vecteurs $Re[V_2]$, $Im[V_2]$ et $[x,y,z]^T$ sont liés, ce qui donne pour P_1

$$\left|\begin{array}{ccc} 1 & 0 & (x-1) \\ \alpha & \omega & y \\ \alpha^2-\omega^2 & 2\alpha\omega & z \end{array}\right| = 0 \Leftrightarrow$$

$$\left(\alpha^2+\omega^2\right)(x-1)-(2\alpha)y+z=0,$$

et donc pour P_{-1}

$$\left(\alpha^2+\omega^2\right)(x+1)-(2\alpha)y+z=0,$$

Remarque : *Les deux plans ont le même vecteur normal,*

$$n=\left[\begin{array}{c} (\alpha^2+\omega^2) \\ -2\alpha \\ 1 \end{array}\right],$$

donc les plans associés aux points P_1 et P_{-1} sont parallèles. Ceci est une conséquence directe de la propriété de symétrie par rapport à P_0 du champs de vecteurs $F_a(X)$.

La matrice Λ est une matrice de Vandermonde, donc

$$\begin{aligned}\det(\Lambda) &= (\lambda_1-\lambda_2)(\lambda_1-\lambda_3)(\lambda_3-\lambda_2)\\ &= -2i\omega((\lambda_1-\alpha)^2+\omega^2),\end{aligned}$$

les valeurs propres étant toujours distinctes si $a \neq 0$, la matrice Λ est régulière, d'inverse

$$\Lambda^{-1} = \frac{1}{-2i\omega((\lambda_1-\alpha)^2+\omega^2)} \begin{bmatrix} (\alpha^2+\omega^2)-2i\omega & 4i\alpha\omega & -2i\omega \\ \lambda_1(\lambda_1\alpha-\alpha^2+2\omega^2)+i\lambda_1\omega(2\alpha-\lambda_1) & (\alpha^2-\omega^2-\lambda_1^2)-2i\alpha\omega & (\lambda_1-\alpha)+i\omega \\ -\lambda_1(\lambda_1\alpha-\alpha^2-\lambda_1\omega^2)-i\lambda_1\omega(2\alpha-\lambda_1) & \lambda_1^2-\alpha^2+\omega^2-2i\alpha\omega & \alpha-\lambda_1+i\omega \end{bmatrix}.$$

Tout est à présent réuni pour expliciter la solution du système linéarisé autour de P_1 et P_{-1} correspondant à une condition initiale δ_{X_0},

$$\begin{aligned}\delta_X(t) &= e^{At}\delta_{X_0}\\ &= \Lambda e^{Dt}\Lambda^{-1}\delta_{X_0},\end{aligned}$$

où

$$e^{Dt} = \begin{bmatrix} e^{\lambda_1 t} & 0 & 0 \\ 0 & e^{\lambda_2 t} & 0 \\ 0 & 0 & e^{\lambda_3 t} \end{bmatrix}.$$

Après une phase de calcul matriciel et de regroupement des termes semblables, l'expression de la solution linéarisée du système est

$$\begin{cases} \delta_x(t) = \beta_1 e^{\lambda_1 t} + e^{\alpha t}(\beta_2\cos(\omega t)+\beta_3\sin(\omega t)) \\ \delta_y(t) = \beta_1\lambda_1 e^{\lambda_1 t} + e^{\alpha t}((\beta_2\alpha+\beta_3\omega)\cos(\omega t)+(\beta_3\alpha-\beta_2\omega)\sin(\omega t)) \\ \delta_z(t) = \beta_1\lambda_1^2 e^{\lambda_1 t} + e^{\alpha t}((\beta_2\alpha^2+2\beta_3\alpha\omega-\beta_2\omega^2)\cos(\omega t)+(\beta_3\alpha^2-2\beta_2\alpha\omega-\beta_3\omega^2)\sin(\omega t)) \end{cases}, \tag{II.10}$$

avec

$$\begin{cases} \beta_1 = \dfrac{(\alpha^2+\omega^2)\delta_{x_0}-2\alpha\delta_{y_0}+\delta_{z_0}}{(\lambda_1-\alpha)^2+\omega^2} \\ \beta_2 = \dfrac{\lambda_1(\lambda_1-2\alpha)\delta_{x_0}+2\alpha\delta_{y_0}-\delta_{z_0}}{(\lambda_1-\alpha)^2+\omega^2} \\ \beta_3 = \dfrac{\lambda_1(\alpha^2-\omega^2-\lambda_1\alpha)\delta_{x_0}+(\omega^2-\alpha^2+\lambda_1^2)\delta_{y_0}+(\alpha-\lambda_1)\delta_{z_0}}{\omega((\lambda_1-\alpha)^2+\omega^2)} \end{cases}$$

La physionomie de la solution II.10 confirme le rôle prépondérant des valeurs propres sur la dynamique du système. Celle-ci permet également d'interpréter plus facilement les comportements du système selon la valeur de a.
La figure 2 montre que dans le cas où $a = -1$, $\alpha = 0$. L'expression de la solution II.10 se simplifie grandement car alors, $\lambda_1 = -1$ et $\omega = 1$. cela donne,

$$\begin{cases} \delta_x(t) = \beta_1 e^{-t} + \beta_2\cos(t) + \beta_3\sin(t) \\ \delta_y(t) = -\beta_1 e^{-t} + \beta_3\cos(t) - \beta_2\sin(t) \\ \delta_z(t) = \beta_1 e^{-t} - \beta_2\cos(t) - \beta_3\sin(t) \end{cases},$$

avec

$$\begin{cases} \beta_1 = \dfrac{\delta_{x_0}+\delta_{z_0}}{2} \\ \beta_2 = \dfrac{\delta_{x_0}-\delta_{z_0}}{2} \\ \beta_3 = \dfrac{\delta_{x_0}+2\delta_{y_0}+\delta_{z_0}}{2} \end{cases}.$$

Au delà d'un certain temps t_0 correspondant à la fin du régime transitoire, les termes en e^{-t} sont négligeables, au profit des termes circulaires, et

$$t > t_0 \Rightarrow \left\{ \begin{array}{rcl} \delta_x(t) & = & \beta_2 \cos(t) + \beta_3 \sin(t) \\ \delta_y(t) & = & \beta_3 \cos(t) - \beta_2 \sin(t) \\ \delta_z(t) & = & -\beta_2 \cos(t) - \beta_3 \sin(t) \ = -\delta_x(t) \end{array} \right.$$

La solution est donc contenue dans le plan de l'espace des phases d'équation

$$\begin{array}{rcl} \delta_x(t) + \delta_z(t) & = & 0 \Leftrightarrow \\ x \pm 1 + z & = & 0, \end{array}$$

et vu que

$$\begin{array}{rcl} \delta_x(t)^2 + \delta_y(t)^2 & = & \beta_2^2 \cos^2(t) + 2\beta_2\beta_3 \cos(t)\sin(t) + \beta_3^2 \sin^2(t) \\ & & +\beta_3^2 \cos^2(t) - 2\beta_2\beta_3 \cos(t)\sin(t) + \beta_2^2 \sin^2(t) \\ & = & \beta_2^2 + \beta_3^2, \end{array}$$

alors, en $a = -1$, le système linéarisé tend vers un cycle limite qui est un cercle de centre $P_{\pm 1}$ et de rayon $\sqrt{\beta_2^2 + \beta_3^2}$.

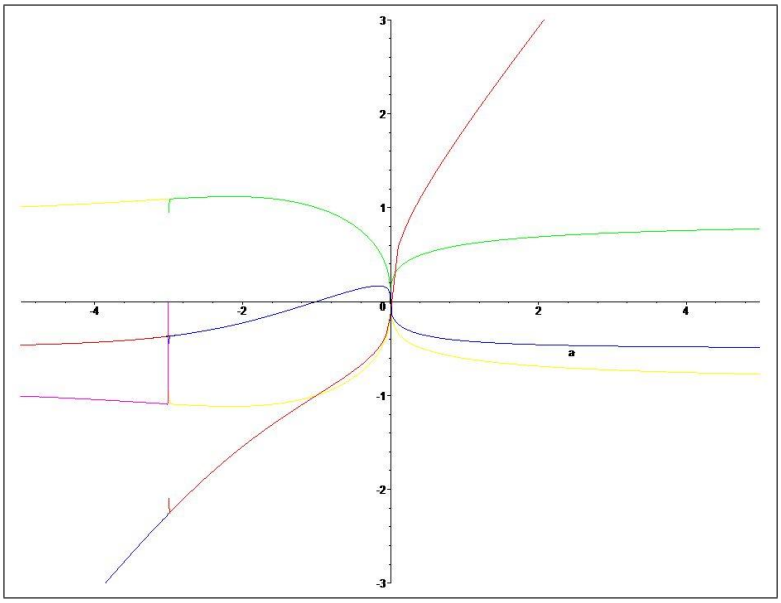


FIG. 2 – *Représentation graphique des applications qui a tout $a \in \mathbb{R}$ font correspondre les parties réelles et imaginaires des valeurs propres $\{\lambda_i\}_{i=1...3}$: $\lambda_1(a)$ (en rouge), $Re[\lambda_2(a)]$ (en bleu), $Im[\lambda_2(a)]$ (en vert), $Im[\lambda_3(a)]$ (en jaune) et si $a < -3$, $Im[\lambda_1(a)]$ (en magenta)*

La figure 2 permet d'observer le signe et la position des parties réelles des valeurs propres de A et d'après la relation (II.9) d'en déduire si les points fixes P_{-1} et P_1 sont stables ou instables.

– Si $a < -3$, alors $\lambda_1 < 0$, $Re[\lambda_2] < 0$ avec $|\lambda_1| < |\lambda_2|$. Les deux valeurs propres sont de parties réelles négatives, les points fixes sont stables. Toute trajectoire tend asymptotiquement vers le point fixe qui est un attracteur stable. La figure 3 montre un tel cas de figure.

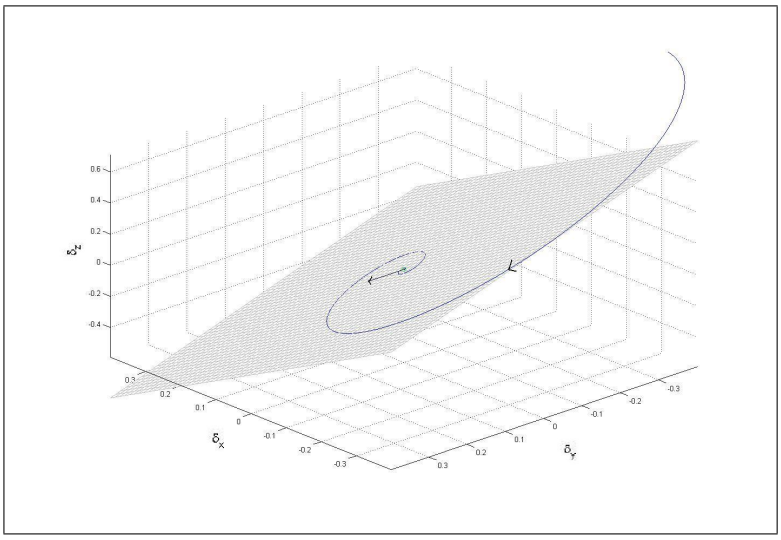


FIG. 3 – *Perturbation du système au voisinage de $P_{\pm 1}$ pour $a = -4$, accompagnée des sous-espaces propres (plan et vecteur)*

– Si $a \in [-3; -1[$, alors $\lambda_1 < 0$, $Re[\lambda_2] < 0$ avec $|\lambda_1| > |\lambda_2|$, pour les mêmes raisons que précédemment les points fixes sont stables, comme le montre la figure 4.

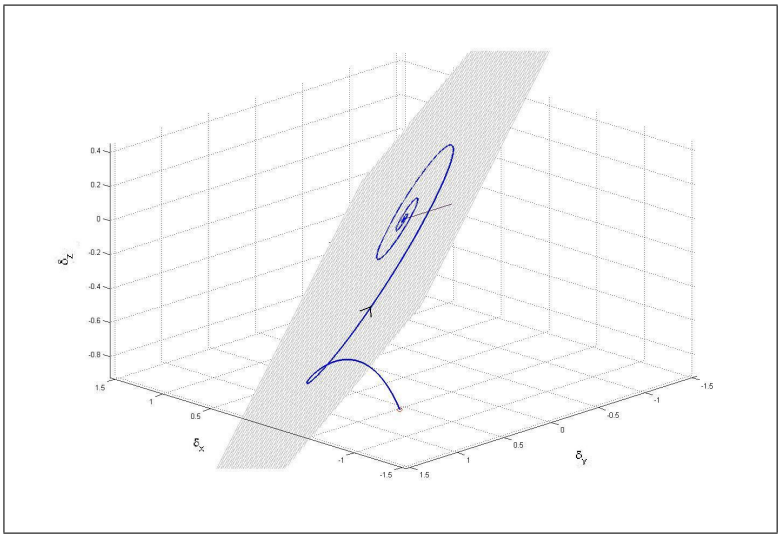


FIG. 4 – *Perturbation du système au voisinage de $P_{\pm 1}$ pour $a = -2$, accompagnée des sous-espaces propres (plan et vecteur)*

– Si $a = -1$, alors $\lambda_1 < 0$ et dans ce cas $Re[\lambda_2] = 0$. Les trajectoires tendent à s'enrouler autour du cycle limite qui est un cercle de centre $P_{\pm 1}$ et de rayon $\sqrt{\beta_2^2 + \beta_3^2}$, car le terme α amplifiant ou amortissant les termes rotatifs est nul. Ceci est illustré par la figure 5.

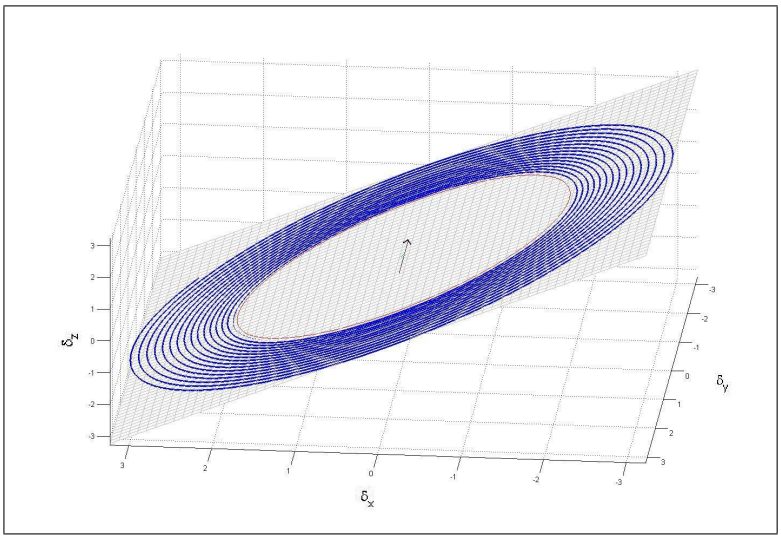


FIG. 5 – *Perturbation du système au voisinage de $P_{\pm 1}$ pour $a = -1$, accompagnée des sous-espaces propres (plan et vecteur) et du cycle limite (rouge)*

– Si $a \in]-1;0[$, alors $\lambda_1 < 0$, $Re[\lambda_2] > 0$ avec $|\lambda_1| > |\lambda_2|$, il s'agit là d'un point selle de type II instable[JLu04], comme le montre l'exemple sur la figure 6.

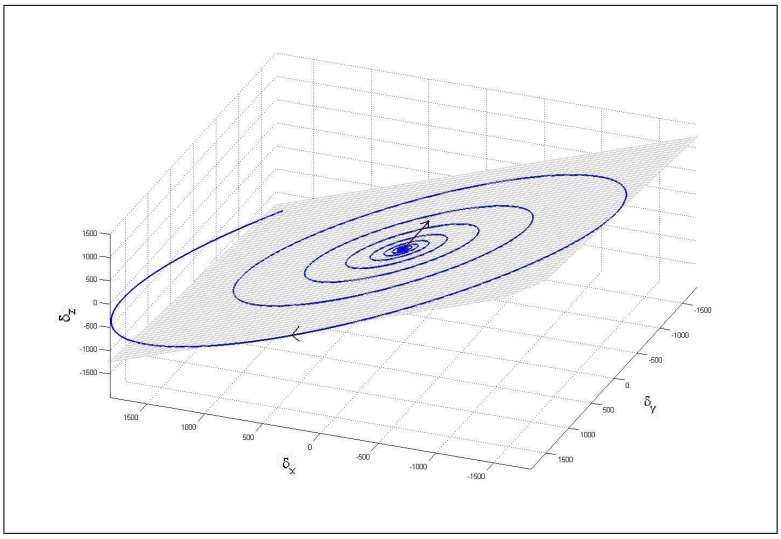


FIG. 6 – *Perturbation du système au voisinage de $P_{\pm 1}$ pour $a = -0,7$, accompagnée des sous-espaces propres (plan et vecteur)*

– Enfin, si $a > 0$, alors $\lambda_1 > 0$, $Re[\lambda_2] < 0$ avec $|\lambda_1| > |\lambda_2|$. Quelle que soit la valeur de a positive, les points fixes sont conjointement instables car d'une part les volumes sont en expansion dans cette zone[13] et d'autre part la figure 2 permet de se rendre compte que $|\lambda_1| >> |\lambda_2|$. La première valeur propre impose donc son comportement aux points fixes qui sont donc répulsifs, comme le montre la figure 7.

[13]Rappel, $div[F_a(X)] = a > 0$, si $a > 0$

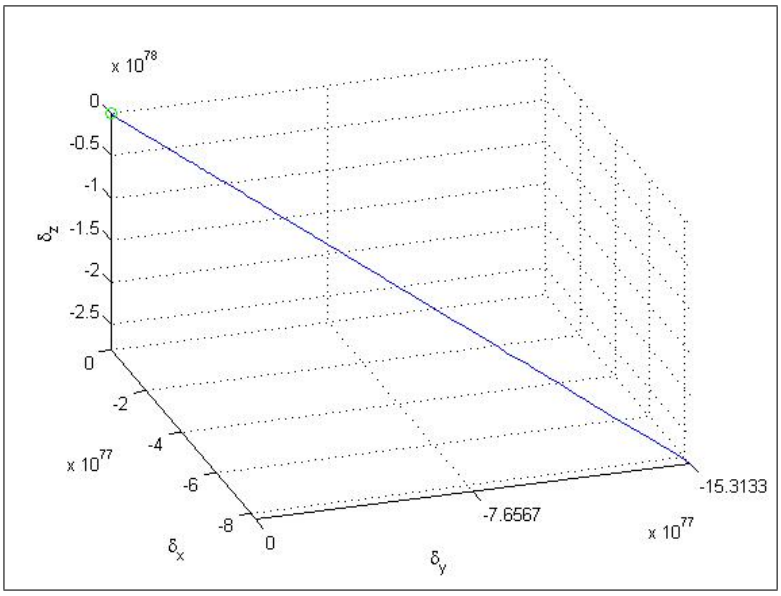


FIG. 7 – *Perturbation du système au voisinage de $P_{\pm 1}$ pour $a = 1$. La solution explose, repoussée par le noeud instable.*

5.2 Caractérisation du point fixe P_0

Pour tout point $X = [x, y, z]^T$ de l'espace des phases tel que $|x| < \eta$, la matrice Jacobienne de $F_a(X)$ évaluée au point P_0 s'écrit

$$J_{P_0}[F_a(X)] = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ a\left(1 - \dfrac{1}{\eta}\right) & a & a \end{bmatrix} = A_\eta.$$

La matrice A_η est indépendante de X mais dépend du paramètre de contrôle a, ainsi que du paramètre η qui bien que n'étant pas introduit comme un paramètre de contrôle proprement dit s'avère intervenir dans l'expression de A_η et *in extenso* dans l'expression de ses éléments propres. Donc, η conditionne aussi la nature de la dynamique du problème, il est nécessaire de tenir compte de son influence pour la suite.
Par analogie avec la section précédente, la nature et la stabilité du point fixe est déterminée par les signes des parties réelles des valeurs propres de A_η.

Proposition II.3. *Les valeurs propres λ_1, λ_2 et λ_3 de A_η sont solutions de*

$$\lambda^3 - a\lambda^2 - a\lambda - a = 0,$$

et pour tout $a \neq 0$,

$$\begin{aligned} &\lambda_1 \in \mathbb{R} \\ &\lambda_2 \in \mathbb{C} = \alpha + i\omega \\ &\lambda_3 \in \mathbb{C} = \overline{\lambda_2}. \end{aligned}$$

La preuve de cette proposition est présentée en annexe D.
Les expressions des vecteurs propres V_1,V_2,V_3, des sous espaces propres associés, de la matrice Λ, de son inverse ainsi que la solution II.10 établies précédemment pour les points fixes $P \pm 1$ demeurent formellement les mêmes pour P_0, seules les expressions de λ_1, α et ω sont différentes, ne serait-ce qu'à cause de la présence du terme η. Ce dernier est d'ailleurs fixé tel que $\eta = 0,1$, de sorte à se situer autour d'une plage de valeurs compatibles avec celles utilisées en pratique par les électroniciens.

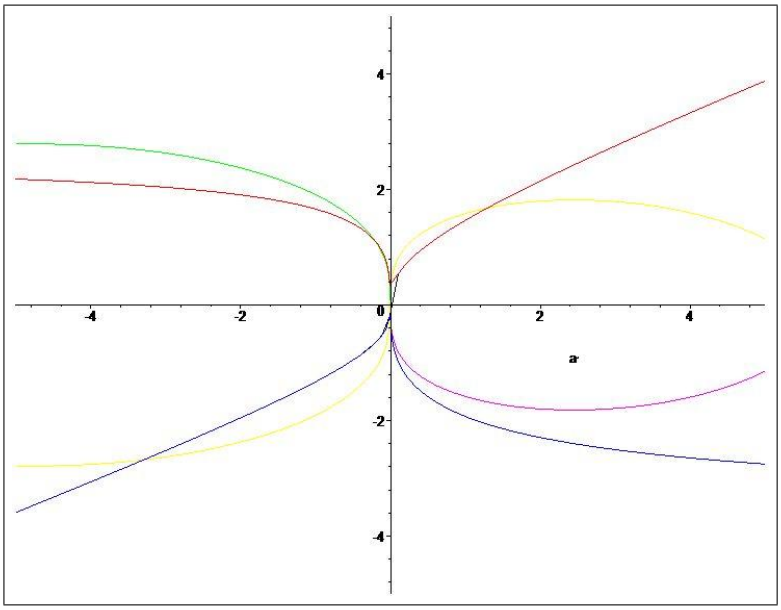


FIG. 8 – *Représentation graphique des applications qui a tout* $a \in \mathbb{R}$ *font correspondre les parties réelles et imaginaires des valeurs propres* $\{\lambda_i\}_{i=1...3}$ *:* $\lambda_1(a)$ *(en rouge),* $Re[\lambda_2(a)]$ *(en bleu),* $Im[\lambda_2(a)]$ *(en vert),* $Im[\lambda_3(a)]$ *(en jaune) et si* $a > 0$*,* $Im[\lambda_1(a)]$ *(en magenta).* $\eta = 0,1$.

La figure 8 permet d'affirmer que pour tout $a \in]-3\,;\,0[$, la valeur propre réelle est strictement positive alors que la partie réelle est négative telle que $|\lambda_1| > |\alpha|$, la partie imaginaire des valeurs propres complexes conjuguées ne s'annulent pas. Par conséquent, le point P_0 est un point point selle de type I instable. La figure 9 montre que la solution dans ce cas diverge.

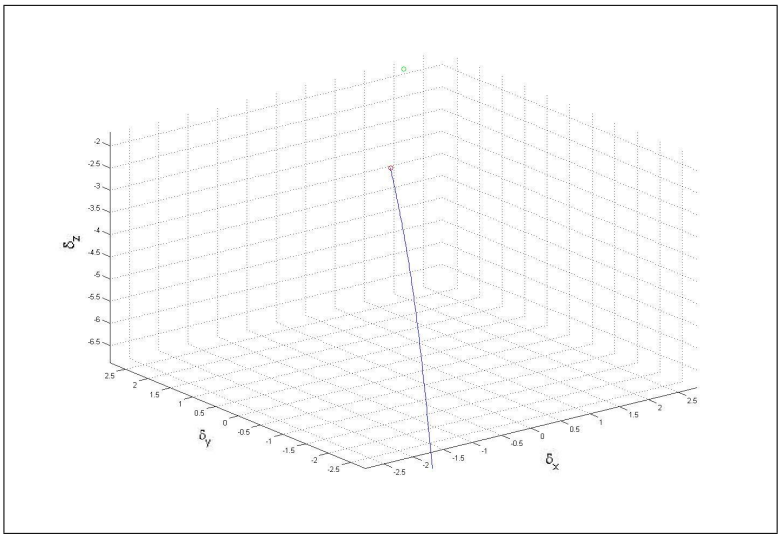


FIG. 9 – *Perturbation du système au voisinage de* P_0*. Pour* $a = -0,7$*, la solution diverge très rapidement*

5.3 Récapitulatif

L'étude locale du problème (P_a) dans la section précédente a permis d'établir que le système dynamique a trois points fixes hyperboliques instables, deux points selle de type II en P_1 et P_{-1} et un point selle de type I en P_0, et à chacun de ces points est respectivement associé un plan propre et un vecteur propre. De plus, l'unique intervalle où a prend ces valeurs, tel que le système puisse être chaotique, est l'intervalle $]-1\,;\,0[$ car c'est à l'intérieur de ce dernier qu'est vérifiée la première hypothèse du théorème de Shil'nikov, à savoir

$$|\alpha| \quad < \quad |\lambda_1|. \tag{II.11}$$

Pour fixer les idées, dans le cas de la valeur test $a = -0,7$,
- En $P_{\pm 1}$, $\lambda_1 \approx -0.848$, $\alpha \approx 0.074$ et $\omega \approx 0.905$,
- En P_0, $\lambda_1 \approx 1,531$, $\alpha \approx -1,115$ et $\omega \approx 1.694$.

6 DE LA DYNAMIQUE LINÉAIRE LOCALE À LA DYNAMIQUE NON-LINÉAIRE GLOBALE

L'influence des termes non-linéaires n'est effective que dans le sous-espace ouvert de l'espace des phases délimité par les plans d'équation $x = \pm\eta$. Cela permet de scinder l'espace des phases en trois sous-espaces D_{-1},D_0 et D_1 contenant respectivement les points P_{-1}, P_0 et P_1. Ces considérations géométriques permettent de caractériser les sous-ensembles remarquables de l'espace des phases, présentés en guise de récapitulatif sur la figure 10.

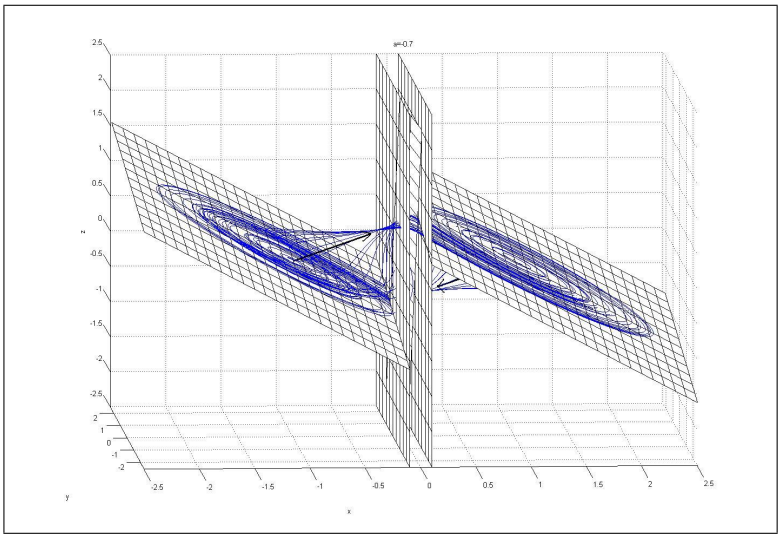


FIG. 10 – *Sous espaces propres associés aux trois points fixes lorsque pour* $a = -0,7$ *accompagnés des plans* $x = \pm\eta$.

A l'intérieur de ces trois régions, l'évolution des trajectoires est régie par le système II.8, avec $J_P[F_a(X)] = A$ lorsque $X \in D_{-1} \cup D_1$ et $J_P[F_a(X)] = A_\eta$ lorsque $X \in D_0$.
Dans ce contexte, toute trajectoire issue d'une condition initiale dans D_1[14] dans le cas où $a \in]-1\,;\,0[$ va être attirée par le point selle de type II P_1 qui par instabilité va repousser la trajectoire hors de chacun de ses voisinages. Or, pour certaines valeurs de a, il se peut que la trajectoire

[14]Le cas où la condition initiale est dans D_{-1} est identique par symétrie.

ainsi repoussée traverse le plan $x = \eta$ pour alors être gouvernée par la dynamique imposée par le point P_0, point selle de type I instable qui force la trajectoire à franchir le plan $x = -\eta$ et ainsi se trouver dans D_{-1}, attirée puis repoussée par le point selle de type II P_{-1} jusqu'à franchir à nouveau le plan. Ainsi, la trajectoire évolue dans le temps selon le cycle qui vient d'être décrit. Lorsque $a = -0,7$, ce genre d'évolution est effectif, comme le montre la figure II.10. Pour toute condition initiale, les trajectoires appartiennent à un ensemble appelé attracteur étrange, dont la déclinaison présentée ici appartient à la famille Double-Scroll.

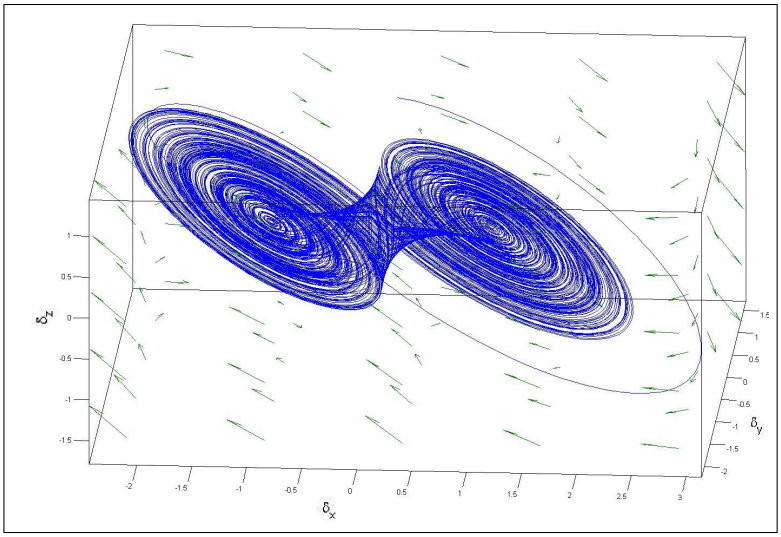


FIG. 11 – *Double Scroll obtenu avec* $a = -0,7$ *et* $x_0 = 0,02$, $y_0 = 1$ *et* $z_0 = 2$ *comme condition initiale. La trajectoire est représentée par* 100000 *points avec un pas de discrétisation* $h = 0,05$.

La section suivante a pour but de montrer que sous certaines conditions, comme par exemple celles de la figure 11, le système évolue de façon chaotique.

7 MISE EN ÉVIDENCE DU CHAOS DANS LE PROBLÈME (P_a)

Les trajectoires issues de conditions initiales distinctes ne peuvent s'entrecouper, et dans certains cas sont condamnées à évoluer dans un sous-espace borné de l'espace des phases[15]. Cette remarque qualitative est largement insuffisante pour prouver que le système est chaotique, voilà pourquoi l'objet de cette section est de fournir des arguments quantitatifs prouvant le chaos.

7.1 Seconde hypothèse du théorème de Shil'nikov

Cette hypothèse, de loin la plus difficile à mettre en évidence, permet de prouver rigoureusement que le chaos est présent dans le système étudié. Celle-ci consiste à mettre en évidence l'existence de trajectoires hétéroclinique, c'est-à-dire de trajectoires particulières tendant vers un point fixe lorsque $t \to +\infty$ et vers un autre lorsque $t \to -\infty$. L'article de Chua [Chu86] prouve rigoureusement que ce type de trajectoires existe dans la famille Double-Scroll. La démonstration, compliquée, repose sur des considérations géométriques, met en exergue des points remarquables invariants dans l'espace des phases. Dans cette étude seule l'existence de telles trajectoires sera montrée par le biais de simulations numériques. Dans son cours, accessible en ligne [Man02], Manneville donne une méthode empirique simple et efficace pour faire apparaître ce genre de trajectoires, la démarche est la suivante :

[15] La système est conservatif si et seulement si $a < 0$.

– Tout d'abord fixer une condition initiale, appelée H^+, la plus proche possible d'un des point fixe. Sans perte de généralité, si le point fixe choisi est le point P_0, alors H^+ est tel que

$$\vec{P_0H^+} = \varepsilon V_1,$$

où V_1 est le vecteur propre, engendrant la droite vectorielle, qui est la variété instable associée à la valeur propre réelle, ε est un scalaire réel le plus petit possible.

– Le même travail est réalisé avec comme condition initiale le point H^-, symétrique de H^+ par rapport à P_0, vérifiant donc

$$\vec{P_0H^-} = -\varepsilon V_1,$$

Que ce soit pour H^+ ou pour H^-, la trajectoire débute au voisinage proche du point fixe et évolue dans la direction suggérée selon le cas en s'éloignant de ce dernier. Après un certain temps, les trajectoires convergent vers P_{-1} ou P_1
En guise d'illustration, a est fixé à $-0,7$. Ce choix sera validé *a posteriori*. Dans le cas où $a = -0,7$, et avec $\eta = 10^{-1}$, les deux trajectoires hétérocliniques apparaissent, reliant asymptotiquement les points fixes comme le montre la figure 12

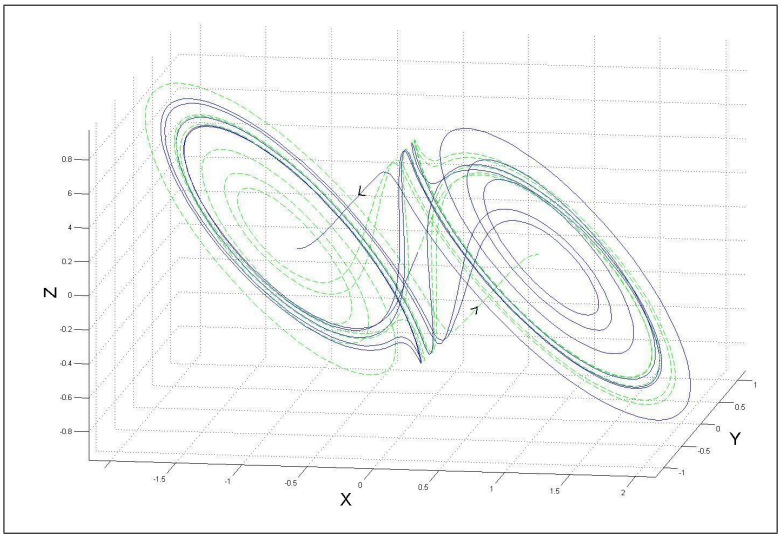


FIG. 12 – *Trajectoires hétérocliniques obtenues avec* $a = -0,7$. *Les trajectoires sont représentées par* 1000 *points avec un pas de discrétisation* $h = 0,1$, *issues de conditions initiales proches et symétriques par rapport à* P_0.

Les deux hypothèses du théorème de Shil'nikov sont vérifiées, cela permet d'affirmer que lorsque $a = -0,7$, le système est chaotique.

7.2 Exposants de Lyapunov

Les exposants de Lyapunov permettent de mettre en évidence une propriété très importante des systèmes dynamiques chaotiques, la sensibilité aux conditions initiales (S.C.I.). Cette propriété signifie que deux trajectoires issues de conditions initiales voisines parcourent l'espace des phases de façon différentes, en fait les trajectoires tendent à s'écarter puis se rapprocher sans cesse l'une de l'autre, elles n'ont pas la même destinée. La S.C.I. est une propriété forte du chaos, idéalement illustrée par le célèbre "effet papillon". Cela revient à supposer que l'hydrodynamique terrestre est régie par un système dynamique S.C.I. en état d'équilibre instable[16], si

[16]Faire si besoin est l'analogie avec une bille en équilibre sur une sphère.

bien qu'un battement d'aile de papillon, c'est-à-dire une perturbation qui déstabilise le système, peut selon la la propriété de S.C.I. modifier substantiellement l'évolution de l'état hydrodynamique, ce qui peut se manifester par l'apparition à long terme d'ouragans à des kilomètres d'où le battement d'ailes a eu lieu.
Plus concrètement, le point de vue de Lyapunov est de mesurer au cours du temps la distance entre deux trajectoires distinctes. Pour ce faire, le système est considéré *a priori* comme chaotique, dans ce cas, la S.C.I. est effective et donc la distance entre chacune des trois composantes des deux trajectoires évolue, à terme, de façon exponentielle. Si $d_x(0)$ est la distance entre les deux premières coordonnées des deux conditions initiales, alors, au temps t_0 fixé la distance $d_x(t_0)$ est telle qu'il existe un coefficient scalaire L_x vérifiant

$$d_x(t_0) \approx e^{L_x t_0} d_x(0),$$

ce qui amène, ne s'agissant que d'une approximation, à définir asymptotiquement L_x,

$$L_x := \lim_{t\to+\infty} \frac{1}{t} \ln\left(\frac{d_x(t)}{d_x(0)}\right),$$

et par analogie, L_y et L_z,

$$L_y := \lim_{t\to+\infty} \frac{1}{t} \ln\left(\frac{d_y(t)}{d_y(0)}\right),$$
$$L_z := \lim_{t\to+\infty} \frac{1}{t} \ln\left(\frac{d_z(t)}{d_z(0)}\right).$$

L_x, L_y et L_z sont les exposants de Lyapunov associé au problème (P_a), ils caractérisent la S.C.I. du système. En particulier, si un des exposants est positif, un second nul, et le troisième négatif, alors le système évolue dans un état chaotique [BPM88].

> ***Remarque :*** *Il est clair que d'après la définition des exposants, seule une approximation de ces derniers est possible, de plus, les erreurs dues à la précision finie d'un calculateur, dites erreurs numériques, font qu'il est difficile d'obtenir exactement la valeur* 0 *quelle que soit la méthode numérique utilisée.*

Ces derniers sont calculés pour $a = -0,7$ par le biais de l'algorithme proposé par Wolf et Al. [Wol85]. La représentation graphique de l'évolution du calcul présentée figure II.11 est obtenue avec le module Matlab© MATDS, conçu par Vasiliy N. Govorukhin, librement disponible sur la toile [Gov04].

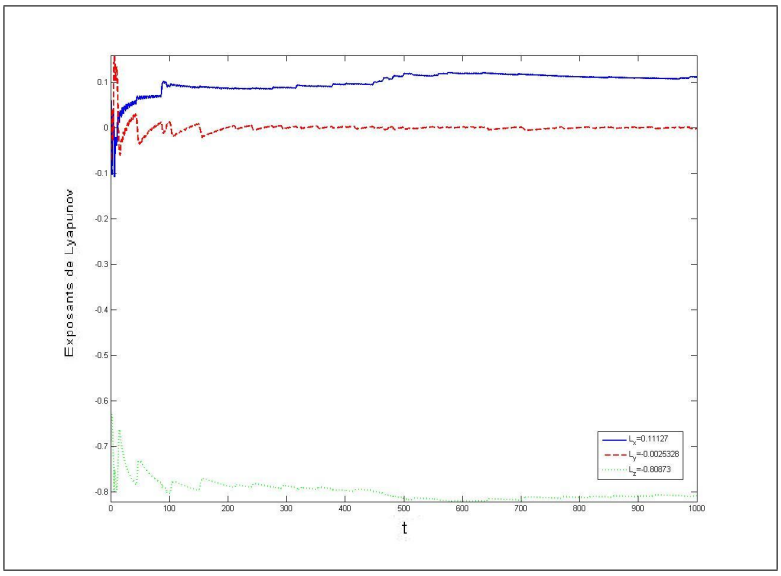


FIG. 13 – *Exposants de Lyapunov dans le cas où* $a = -0,7$.

Le calcul estimant la valeur des exposants donne

$$\begin{cases} L_x = 0,11127 \\ L_y = -0,0025328 \\ L_z = -0,80873 \end{cases},$$

interprété comme une signature de la forme $(+\,;\,0\,;\,-)$, ce qui confirme le caractère chaotique du système pour cette valeur [BPM88].

7.3 Diagramme de bifurcation

Jusqu'à présent, le cas $a = -0,7$ a fait office d'exemple pour illustrer l'aspect chaotique du système. Il est alors légitime de se demander pour quelle valeur de a le même comportement est visible. Cet intervalle de valeurs est déterminé empiriquement par l'intermédiaire du diagramme de bifurcation. Il s'agit d'une représentation graphique de dimension 2 où les valeurs du paramètre de contrôle sont portées en abscisse et où une valeur caractérisant l'état du système en régime stationnaire est portée en ordonnée. Le principe algorithmique est le suivant :

- Le paramètre de contrôle a est discrétisé sur l'intervalle $[-3\,;\,0[$, avec un pas Δa le plus petit possible.
- Pour chaque valeur de a, N_{tir} calculs de trajectoires issus d'autant de conditions initiales choisies dans l'espace des phases sont effectués jusqu'à un temps où le régime stationnaire est suffisamment installé. Seule la partie de chaque trajectoire pour $t > t_0$, temps à partir duquel le régime transitoire n'est plus, est retenue.
- La valeur moyenne de la première composante de chacune des N_{tir} sous-trajectoires est calculée puis portée en ordonnée.

Le processus peut s'avérer être long vu que $N_{tir}.(\left\lfloor \frac{3}{\Delta a} \right\rfloor + 1)$ calculs de trajectoires sont requis. Le temps t_0 est déterminé empiriquement sur la base de la lecture de plusieurs simulations numériques, amenant à faire le compromis d'un choix de calcul de trajectoires sur 600 échantillons avec un pas de discrétisation $h = 0,05$ pour que $t_0 = 300.h = 15$(sec). N_{tir} est également déterminé empiriquement, la limite concernant ce dernier étant uniquement fixée par la puissance de calcul à disposition. $N_{tir} = 50$ est en ce sens un bon compromis.

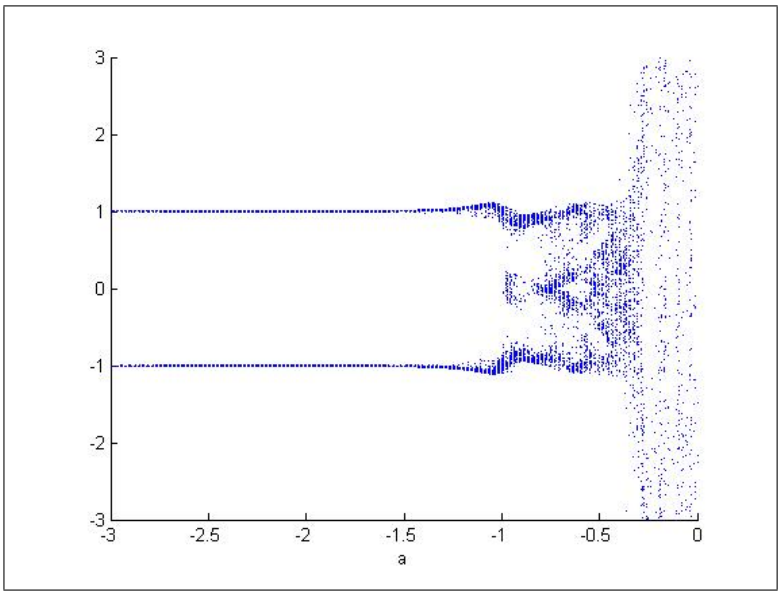


FIG. 14 – *Diagramme de bifurcation pour* $a \in [-3\,;\,0[$. *En ordonnée, pour chaque valeur de* a, *les* $N_{tir} = 50$ *valeurs moyennes de* 600 *échantillons de la solution de* (P_a).

Le résultat de cette simulation est présenté sur figure 14, et en version agrandie sur la zone $[-1\,;\,0[$. Les comportements observés en fonction de a sont identiques à ceux rencontrés lors de l'étude locale du système.

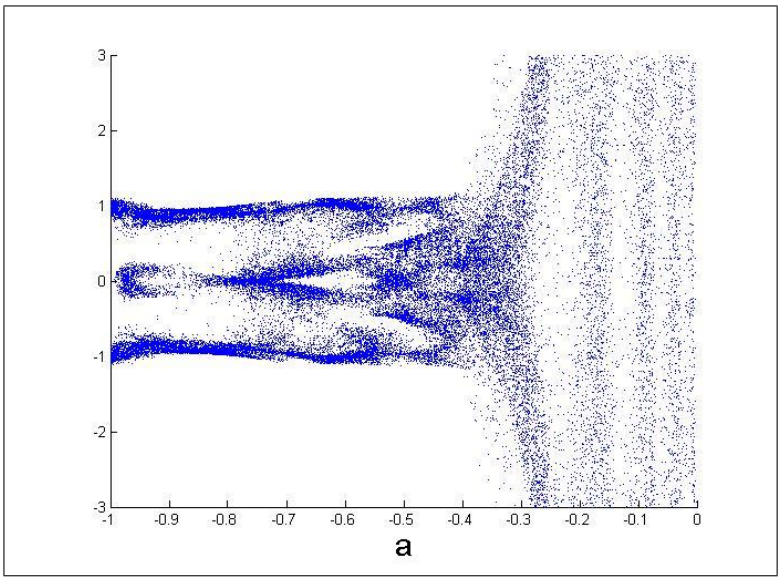


FIG. 15 – *Diagramme de bifurcation pour* $a \in [-1\,;\,0[$. *En ordonnée, pour chaque valeur de* a, *les* $N_{tir} = 50$ *valeurs moyennes de* 600 *échantillons de la solution de* (P_a).

Remarque : *La figure 15 permet de comprendre le choix si fréquent de* $a = -0,7$ *dans les travaux des électroniciens sur le Double Scroll. Ce choix de valeur assure qu'en cas de déviation de processus*[17]*, entraînant donc une variation de* a, *le système reste en mode chaotique et ne risque pas de bifurquer vers les modes stables ou instables.*

[17] Du à la vétusté des composants, par exemple.

Trois tendances se dégagent, jusqu'à $a = -1$, les trajectoires convergent toutes vers $x \pm 1$, première coordonnée des points fixes $P_{\pm 1}$.

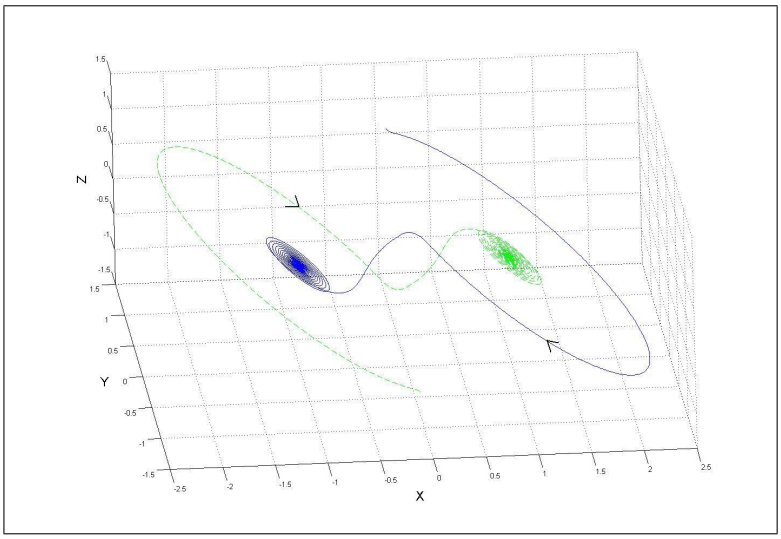


FIG. 16 – *Portrait de phase de deux trajectoires pour* $a = -1,1$ *sur* $N = 50000$ *points avec un pas* $h = 0,01$ *secondes.*

Puis, dans un intervalle inclus dans $]-0,99\,;\,-0,4[$ la répartition des valeurs est désordonnée autour des trois points fixes tout en restant bornée, le système évolue de façon chaotique.

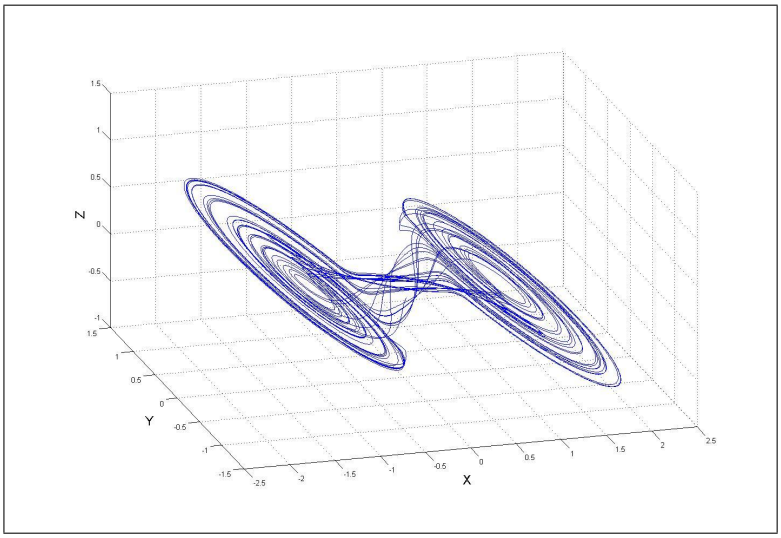


FIG. 17 – *Portrait de phase d'une trajectoire pour* $a = -0,5$ *sur* $N = 50000$ *points avec un pas* $h = 0,01$ *secondes.*

Enfin, les trajectoires divergent très rapidement si $[-0,4\,;\,0[$.

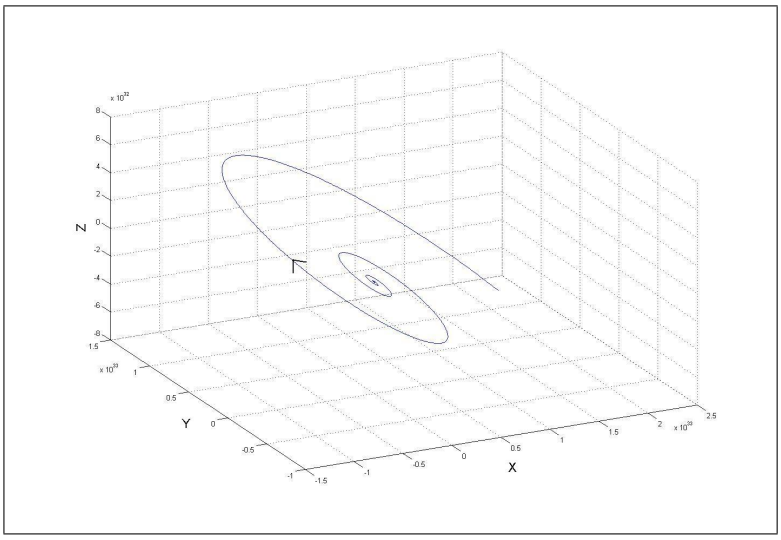


FIG. 18 – *Portrait de phase de deux trajectoires pour* $a = -0,3$ *sur* $N = 50000$ *points avec un pas* $h = 0,01$ *secondes.*

Deux enseignements sont à tirer de l'étude du diagramme de bifurcation. Tout d'abord, la plage de valeur où il y a présence de chaos si a appartient à un intervalle inclus dans $]-0,99\,;\,-0,4[$. Ce dernier diffère de ce qu'annonce Elwakil d'une part [Elw01] et Radwan d'autre part [Rad03], à savoir $a \in]-0,98\,;\,-0,48[$. Cette différence s'explique par le fait qu'eux travaillent sur un circuit électronique et non pas avec des simulations numériques comme c'est le cas ici. Cela a pour conséquence, en dépit de la convergence du problème discret vers le problème continu, d'engendrer des résultats différents en vertu de la propriété de S.C.I., une simple différence d'arrondi ou de troncature sur les conditions initiales ou sur le paramètre de contrôle par rapport à la version électronique du problème fait que nécessairement la trajectoire étudiée n'est pas celle escomptée mais une trajectoire voisine.
De son côté, Telandro trouve $a \in [-0,89\,;\,-0,49]$ avec une précision de 10^{-2}. La plage de chaos qu'il a trouvée est différente. Cela peut s'expliquer en pratique par le fait qu'il est très difficile de mesurer correctement a, ceci à cause d'éléments parasites qui modifient sa valeur effective.

Les systèmes dynamiques chaotiques, par leur propriété de S.C.I., sont tels que le simple fait de les étudier expérimentalement influe quantitativement sur la nature de leurs trajectoires. Cela signifie qu'une trajectoire observée n'est pas en fait celle correspondant au système étudié. Ceci est dû aux erreurs d'arrondis dans le cas numérique et aux erreurs de déviation de processus des composants dans le cas analogique. Dans les deux cas, l'impact de ces sources d'erreurs peut être qu'au mieux réduit, il y aura systématiquement une différence entre ce qui est mesuré et ce qui est effectif. Devant ce paradoxe chaotique, il est légitime de se demander s'il existe une similitude, au moins philosophique, avec la mécanique quantique.
Pour mettre en évidence cette similitude, une microscopique excursion dans le domaine de la mécanique quantique s'impose. La mécanique quantique peut être décrite sous un aspect probabiliste, mais cette description est contestée. A. Einstein, par exemple, réfutait cette vision des choses en considérant que la description n'est pas probabiliste mais déterministe et incomplète dans la mesure où elle ne tient pas compte de ce qu'il appelle les variables d'état cachées[18]. Il propose une vision déterministe basée sur les variables d'état complètes des particules étudiées. Quelle que soit l'interprétation choisie, à l'échelle microscopique, la mesure influe sur l'état

[18]Son argument était que "Dieu ne joue pas au dés"...

des particules mesurées. Les physiciens pour décrire cela parlent de "perturbation incontrôlable sur le destin des particules". Ainsi, l'analogie entre le paradoxe quantique microscopique et le paradoxe chaotique macroscopique est légitime, car dans ces deux domaines, le simple fait de vouloir observer le système à une incidence directe sur l'état du système.

Le diagramme de bifurcation permet ainsi de donner une plage de valeurs du paramètre de contrôle telle que le système évolue de façon chaotique. Cette plage est cependant difficile à obtenir en pratique, et les résultats sont différents suivant la voie d'analyse utilisée, ceci à cause de la propriété S.C.I. du système. La section suivante présente l'étude des propriétés spectrales liées au chaos.

7.4 Analyse spectrale

Cette section a pour but d'étudier le spectre du signal $x(t)$, solution de (P_a) en mode chaotique.
L'étude spectrale de tels signaux est assujettie à certaines restrictions faisant que la richesse spectrale ne peut être restituée en intégralité. Cette dernière permet cependant de mettre en évidence une vision possible du chaos consistant à considérer le phénomène observé comme multi-périodique[19]. Le spectre d'un signal chaotique [BPM88], en particulier, doit occuper une grande plage de fréquences.
Soit une solution $x(t)$ du problème (P_a) avec $a = -0,7$ et $X_0 = [0,1\,;\,0,1\,;\,0,1]^T$ disponible sous la forme de $N = 100000$ échantillons prélevés toutes les $h = 0,01$ secondes. Elle est présentée figure 19. Les brusques changements ayant lieu en moyenne toutes les $T_0 = 75$ secondes correspondent aux instants où les trajectoires cessent de graviter autour d'un point fixe pour migrer vers l'autre, et ceci de manière désordonnée, sans quoi $x(t)$ serait périodique de période T_0.

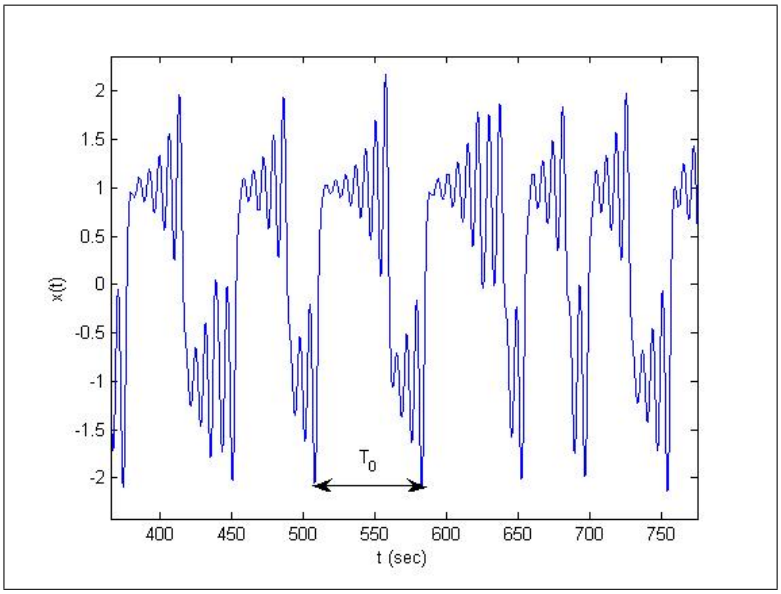


FIG. 19 – *Représentation graphique de $x(t)$, solution de (P_a) pour $a = -0,7$ sur $N = 100000$ points avec un pas $h = 0,01$ secondes.*

L'autocorrélation déterministe de $x(t)$ tend vers 0 au bout de 200 secondes, soit le cinquième de la durée totale de l'observation, traduisant ainsi la perte de mémoire du système qui légitime

[19]Cela revient à considérer le signal étudié comme la superposition finie de signaux périodiques de périodes incommensurables.

la notion de désordre dans le sens de l'absence d'évolution structurée à moyen terme.
L'autocorrélation de $x(t)$ est présentée figure 20, le système à un temps de cohérence court, d'où la perte assez rapide de la mémoire des positions précédent celle en cours d'une trajectoire donnée.

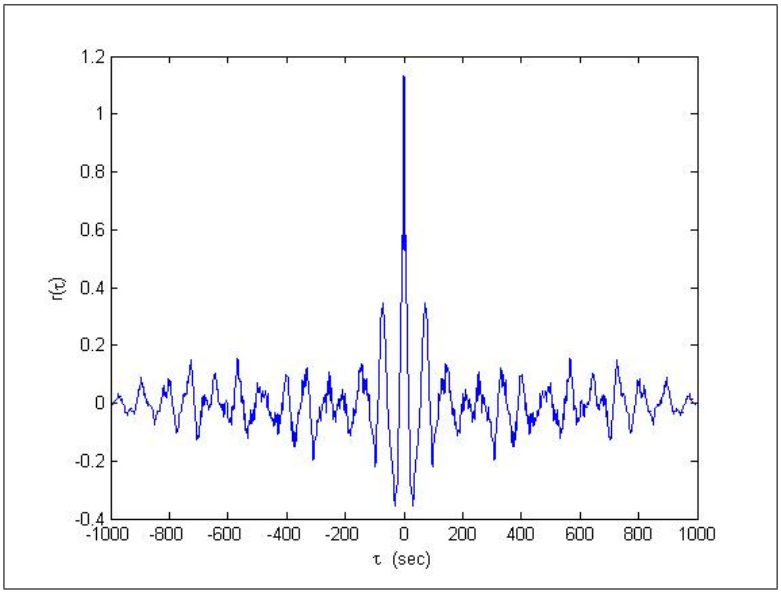


FIG. 20 – *Autocorrélation de la solution de* (P_a) *pour* $a = -0,7$ *sur* $N = 100000$ *points avec un pas* $h = 0,01$.

Le module du spectre de puissance de $x(t)$ est présentée figure 20 sur un intervalle de fréquence de l'ordre de sa fréquence maximale. Il a pour spécificité d'être riche en fréquences dans la mesure où il est constitué de plusieurs raies d'amplitudes différentes. Celles de plus forte amplitude sont localisées en $F_0 = 1/T_0$. Les autres permettent de voir le chaos sous un autre point de vue. A la multitude de raies observées correspond autant de périodes du système. Un phénomène chaotique est alors vu comme multi-périodique, mais où le nombre de périodes est tellement élevé qu'il rend l'évolution des trajectoires complexe, échappant du moins au discernement humain du moins et provoquant cette notion de désordre.

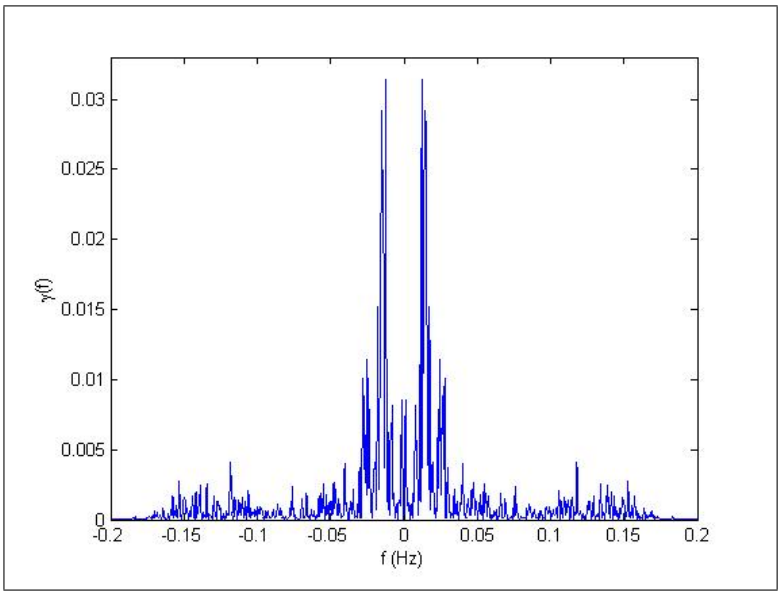


FIG. 21 – *Spectre de la solution de* (P_a) *pour* $a = -0,7$ *sur* $N = 100000$ *points avec un pas* $h = 0,01$.

Il faut noter que les limitations matérielles empêchent de discerner les autres périodes. De plus, l'analyse de Fourier ne permet pas d'obtenir une information sur les instants d'apparition de ces fréquences, pour cela il faut avoir recours à l'analyse multirésolution.
L'étude des propriétés spectrales permet de voir un phénomène chaotique comme la superposition d'un nombre fini de phénomènes périodiques de période incommensurables, synonyme de désordre.

8 CAS OÙ LA CONDITION INITIALE EST UNE VARIABLE ALÉATOIRE

Profitant des propriétés d'un système chaotique, en particulier de la S.C.I. , cette section examine le cas où la condition initiale est donnée par la réalisation d'une variable aléatoire.
Les propriétés du système en régime chaotique établies jusqu'ici montrent qu'il est un bon candidat en tant que générateur pseudo-aléatoire. En particulier, l'évolution désordonnée et la sensibilité aux conditions initiales font qu'il est difficile d'estimer l'évolution d'une trajectoire. Un bémol demeure cependant, l'aspect déterministe du chaos, car plusieurs calculs d'une trajectoire issue de la même condition initiale conduisent à des résultats similaires. Mais l'expérimentateur est-il en mesure de pouvoir fournir plusieurs fois exactement la même condition initiale ? Dans le cas d'une simulation numérique la réponse est oui, par exemple $[0,1\,;\,0,1\,;\,0,1]^T$. Mais la condition initiale $[\frac{\pi}{6}\,;\,e^{-0,1}\,;\,\frac{1}{7}]^T$, d'une machine à l'autre, pour des raisons d'arrondis évidentes, n'engendre pas les mêmes résultats. Dans le cas de l'étude d'un circuit analogique, la réponse est clairement non, à cause des fluctuations émanant des sources de bruit propres au circuit. Ici est donc mis en évidence la clef du succès du chaos en électronique, à partir d'un circuit souvent simple, mais ayant la propriété de S.C.I., et grâce aux bruits inhérents au circuit, il est presque sûrement impossible de démarrer ce dernier avec deux conditions initiales identiques et donc d'engendrer des trajectoires identiques.
Ainsi, avant de pouvoir comparer les résultats numériques obtenus avec ceux analogiques issus de la conception de circuits, il convient à ce stade de l'étude de prendre en compte un aspect important de la modélisation du problème jusqu'ici resté en filagramme, la nature de la condition initiale.

Dans les problèmes d'évolution tel que le problème (P_a), deux trajectoires correspondant à deux conditions initiales ne peuvent s'entrecouper[20], si bien que pour tout a fixé, l'idée est alors, afin de mieux modéliser le comportement du circuit, de considérer toute condition initiale comme la réalisation d'une variable aléatoire, peu importe sa loi, à réalisations dans l'espace des phases. Ce nouveau point de vue est une hypothèse supplémentaire à la modélisation du problème qui permet de montrer la proposition suivante.

Proposition II.4. *Soit la variable aléatoire continue $\mathbf{X}_0$ de loi quelconque, ayant pour réalisations X_0 à valeurs dans l'espace des phases.*
Soit ${}^1X_0$ et ${}^2X_0$ deux réalisations successives de $\mathbf{X}_0$. Alors, si ${}^1X_0$ et ${}^2X_0$ servent successivement de conditions initiales au problème (P_a), les deux trajectoires qu'ils engendrent sont presque sûrement distinctes.

Preuve . *Si ${}^1X_0$ est une réalisation disponible de $\mathbf{X}_0$, variable aléatoire continue, alors*

$$P(X = {}^2X_0/\,{}^1X_0) = 0, \tag{II.12}$$

il s'agit là d'une égalité presque sûre, donc ${}^2X_0$ est presque sûrement différente de ${}^1X_0$.
Par suite, les deux trajectoires issues des conditions initiales ${}^1X_0$ et ${}^2X_0$ ne peuvent presque sûrement pas se couper.

□

> ***Remarque :*** *La proposition n'est plus vraie si $\mathbf{X}_0$ est à réalisations discrètes de dimension finie. Il est donc impossible de vérifier numériquement son bien fondé. Il se peut dans ce cas que ${}^1X_0 = {}^2X_0$.*
> *Or, un signal de consommation relevé sur un circuit analogique peut être vu comme la superposition d'un signal utile correspondant à la vraie valeur avec un bruit gaussien correspondant à la résultante des différentes sources de bruits inhérentes au circuit générant cette consommation (Voir Chapitre III). Ainsi, dans le cas d'une consommation de courant réelle, la proposition est vraie.*

Ce résultat montre qu'il est en théorie improbable que deux conditions initiales soient rigoureusement identiques. De fait les trajectoires correspondantes engendrées sont distinctes.
Il a en particulier pour rôle, dans le cadre de la conception d'un générateur pseudo-aléatoire à l'aide d'un oscillateur chaotique étudié section suivante, de garantir le renouvellement du germe.

[20] Si ce n'est asymptotiquement en un éventuel point fixe. Ce cas de figure est impossible dans le cas du problème (P_a) vu que ce dernier n'a que des points fixes instables.

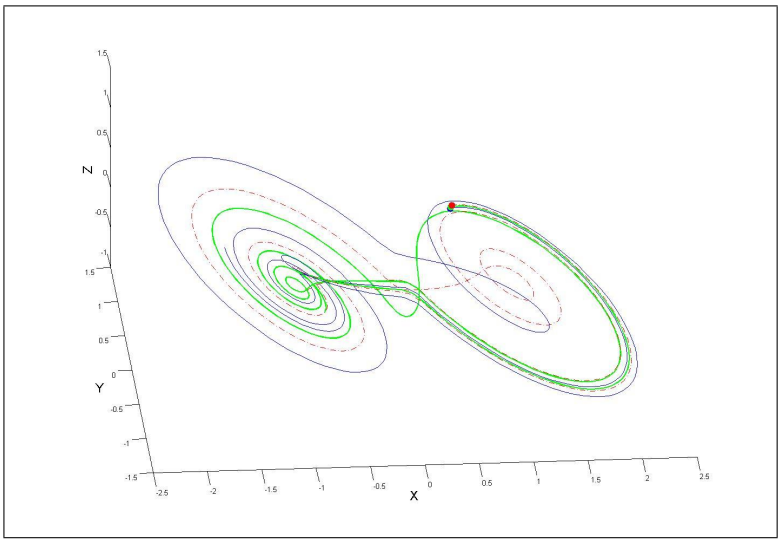


FIG. 22 – *Portrait de phase de deux trajectoires avec* $a = -0,7$ *sur* $N = 500$ *points avec un pas* $h = 0,1$. *Chaque trajectoire est issue de conditions initiales voisines,* $(0,49 \quad 0,49 \quad 0,49)$ *pour celle en trait plein,* $(0,51 \quad 0,51 \quad 0,51)$ *pour celle en trait pointillés.*

La figure 22 montre deux trajectoires obtenues à partir de conditions initiales distinctes mais proches, et met en évidence la différence de marche entre chacune d'elles une fois le régime stationnaire établi.

9 APPLICATION À LA CONCEPTION D'UN GÉNÉRATEUR PSEUDO-ALÉATOIRE À L'AIDE D'UN OSCILLATEUR CHAOTIQUE

La plupart des travaux réalisés à ce sujet, [Sto01, Joh99, Erg06, Yal04], suit un plan de travail consistant à prélever des points sur une trajectoire de Double Scroll à partir d'une section de Poincarré bien déterminée, puis par l'intermédiaire d'un oracle[21] de convertir les points relevés en une suite de 0 et de 1.
L'idée est la suivante, à partir d'une condition initiale, réalisation d'une variable aléatoire dans l'espace des phases, la trajectoire correspondante est calculée pour un temps idéalement infini, en pratique le plus grand possible. Les simulations numériques sont effectuées sur $N = 1000000$ de points avec un pas de discrétisation $h = 0,1$ secondes, ce qui correspond à une étude sur un temps d'environ moins de 28 heures. Le système est alors observé sur la section de Poincarré d'équation $x = 0$ afin d'examiner la répartition des points d'intersection de la trajectoire avec cette dernière.

> ***Remarque :*** *D'après la section précédente, le fait d'avoir une condition initiale différente à chaque expérimentation assure automatiquement le renouvellement du germe aléatoire.*

[21] Une règle de décision

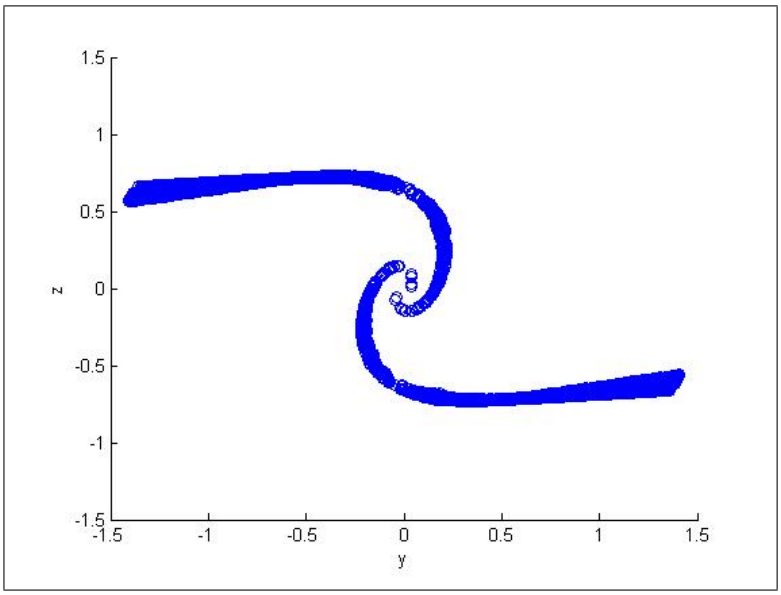


FIG. 23 – *Section de Poincarré* $x = 0$ *avec* $a = -0,7$ *sur* $N = 1000000$ *points avec un pas* $h = 0,1$.

La section de Poincarré $x = 0$ dans le cas où $a = -0,7$ est présentée figure 23. Les couples portés sur cet hyperplan de l'espace des phases se répartissent de façon homogène dans un sous-espace de frontière non-élémentaire, cette répartition peut être matérialisée à travers l'étude de l'application premier retour, à partir de laquelle il est possible d'obtenir les temps de retours $\{t_i\}_{i\in\mathbb{N}^*}$. Ce sont les temps correspondant aux passages à 0 de la composante $x(t)$, difficilement prévisibles, changeant dès lors que la condition initiale change.
Le terme "difficilement prévisibles" est le fruit d'un grand écart conceptuel[22] qui aboutit à la notion de "pseudo-aléatoire", ce qui explique le qualificatif attribué au générateur proposé.
D'après le circuit proposé par Telandro et al. [Tel06], soit $\{A_i\}_{i\in\mathbb{N}^*}$ et $\{\tau_i\}_{i\in\mathbb{N}^*}$ deux suites dépendant du signal étudié dépendant directement des instants de passage $\{t_i\}_{i\in\mathbb{N}^*}$ des trajectoires en $x = 0$ et de l'intervalle de temps entre deux de ces passages, le système évoluant en mode chaotique. Plus précisément soit

$$\left\{ \begin{array}{lcll} A_i & := & \alpha_A \left(\Lambda_{T/2}(t_i) * \text{Ш}_T(t_i)\right) + \beta_A & \forall i \in \mathbb{N}^* \\ \tau_i & := & t_{i+1} - t_i & \forall i \in \mathbb{N}^* \end{array} \right. ,$$

où $\Lambda_{T/2}(t)$ est la fonction triangle [23], α_A et β_A sont des scalaires non nuls permettant d'ajuster le gabarit[24] des triangles en fonction de celui de $x(t)$.
Dans le cas où la condition initiale est la réalisation d'une variable aléatoire, la caractérisation statistique de ces deux suites, pièces maîtresses du dispositif, permet d'évaluer les performances pseudo-aléatoires du signal généré. L'histogramme de la figure 24 montre la répartition des instants de passage à zéro pour une simulation numérique de $N = 100000$ points avec un pas $h = 0,1$ secondes. Ces instants semblent être répartis presque uniformément, autrement dit il arrive régulièrement qu'une trajectoire passe à travers la section de Poincarré $x = 0$.

[22] L'écart entre le concept de phénomène déterministe ou stochastique.
[23]

$$\Lambda_T(t) := \left\{ \begin{array}{ll} 1 - \dfrac{|t|}{T} & \text{si} \quad t \in]-T\,;\,T] \\ 0 & \text{sinon} \end{array} \right.$$

[24] Comprendre le $\min$ et le $\max$.

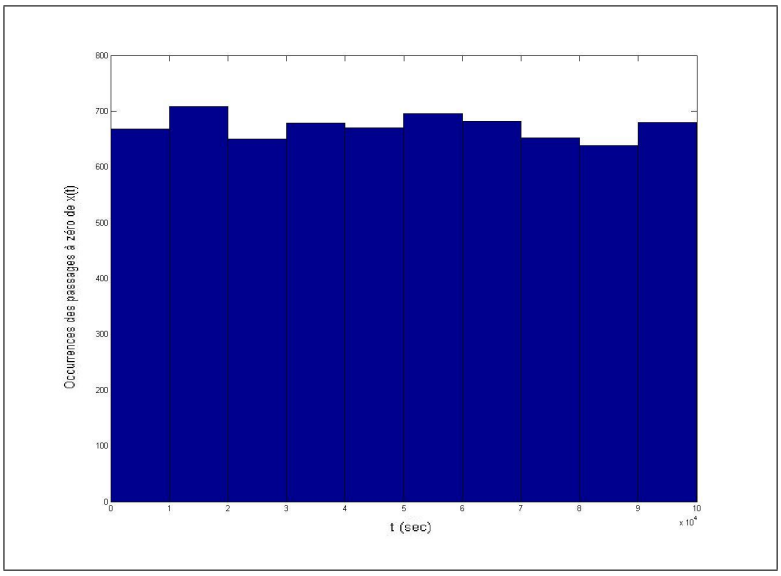


FIG. 24 – *Histogramme de la suite* $\{t_i\}_{i\in\mathbb{N}^*}$ *à partir d'une solution* $x(t)$ *obtenue avec* $a = -0,7$ *sur* $N = 1000000$ *points avec un pas* $h = 0,1$.

Par ailleurs, le représentation en histogramme de la suite $\{\tau_i\}_{i\in\mathbb{N}^*}$ est présentée figure 25.

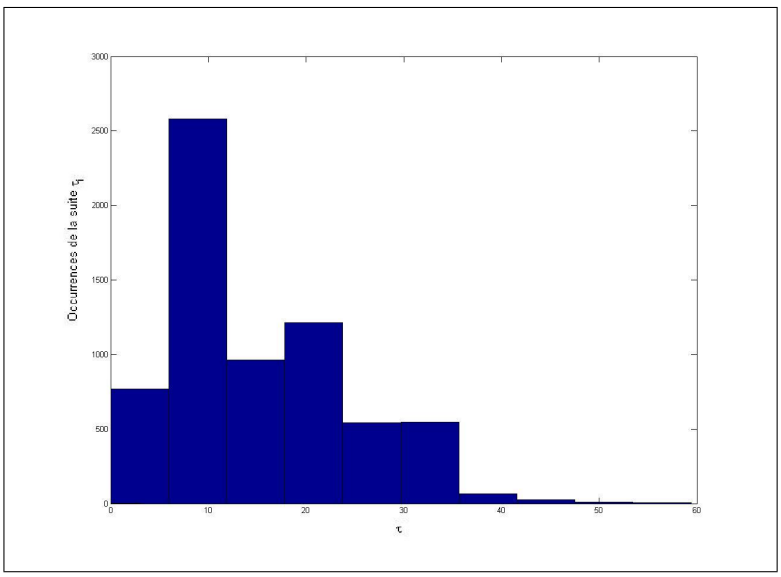


FIG. 25 – *Histogramme de la suite* $\{\tau_i\}_{i\in\mathbb{N}^*}$ *à partir d'une solution* $x(t)$ *obtenue avec* $a = -0,7$ *sur* $N = 1000000$ *points avec un pas* $h = 0,1$.

Cette représentation fait apparaître un pic d'occurrences autour d'environ $t = 9\,(sec)$. En pratique, cela signifie qu'il est fréquent d'obtenir un zéro environ toutes les $9\,(sec)$, sans pour autant que cela soit systematique. La figure 26 illustre ce propos.

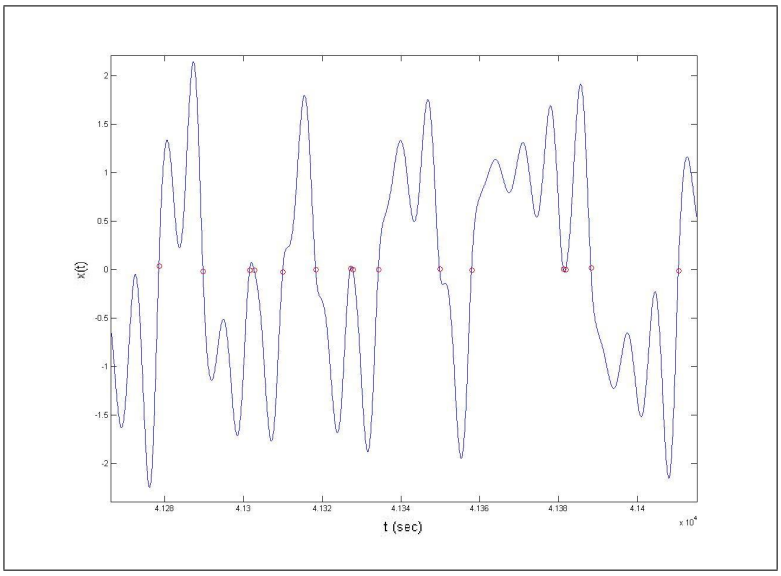


FIG. 26 – *Solution $x(t)$ obtenue avec $a = -0,7$ sur $N = 1000000$ points avec un pas $h = 0,1$. 3 brefs passages à zéros sont observables.*

Hormis cette classe pathologique, les valeurs de $\{t_i\}_{i\in\mathbb{N}^*}$ se répartissent dans les autres classes entre $t = 0$ secondes et environ $t = 35$ secondes, le temps entre deux zéros distincts est donc fluctuant.
Le paramètre h joue un rôle essentiel puisque d'un point de vue algorithmique numérique, un temps de passage à zéro tel que

$$|x(t_i)| < h$$

ne peut être détecté. Ainsi, le pas de discrétisation doit être suffisamment proche de zéro afin de minimiser un tel cas de figure.
Les valeurs de la suite $\{t_i\}_{i\in\mathbb{N}^*}$ servent à construite la suite $\{A_i\}_{i\in\mathbb{N}^*}$, obtenue par échantillonnage d'un signal triangulaire périodique aux instants $\{t_i\}_{i\in\mathbb{N}^*}$. En pratique, la période du signal triangulaire est fixée à $T = 11$ secondes, ce qui correspond à peu près à un tirage toute les périodes. La répartition des $\{A_i\}_{i\in\mathbb{N}^*}$ construits est présentée figure 27.

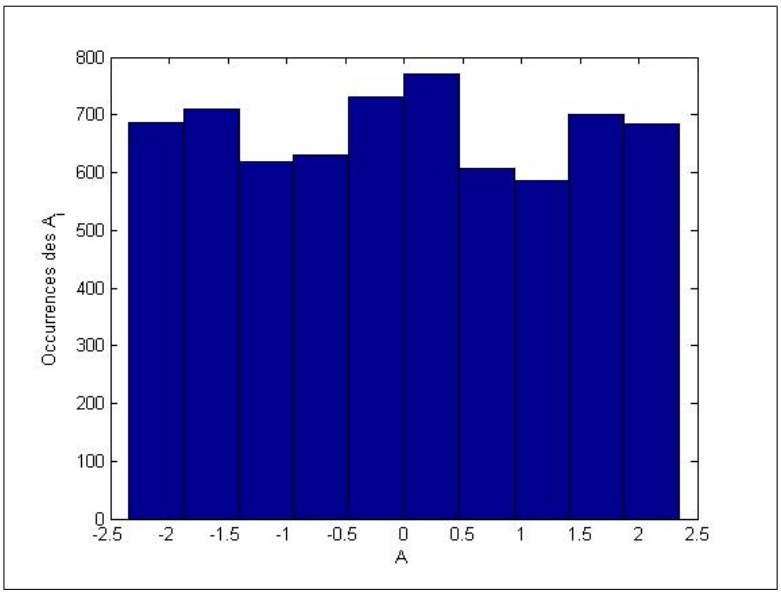


FIG. 27 – *Histogramme de la suite $\{A_i\}_{i\in\mathbb{N}^*}$ à partir d'une solution $x(t)$ obtenue avec $a = -0,7$ sur $N = 1000000$ points avec un pas $h = 0,1$.*

Cette dernière est quasi-symétrique et répartie sur l'intervalle $[-A_M\,;\,A_M]$ avec ici $A_M = 2,4$ secondes.
Soit à présent $\{U_i\}_{i\in\mathbb{N}^*}$ la suite construite par transformation affine des $\{A_i\}_{i\in\mathbb{N}^*}$ et de terme général

$$U_i \;:=\; \alpha_U A_i + \beta_U,$$

où α_U et β_U sont deux scalaires ajustés en fonction de la période T du signal triangulaire et servant à contrôler le flux pseudo-aléatoire. Les éléments de la suite $\{U_i\}_{i\in\mathbb{N}^*}$ servent quant à eux à définir le signal $s(t)$ de la façon suivante,

$$S(t) \;:=\; \left(\Pi_{\frac{U_i}{2}}(t) * \text{Ш}_{U_i}(t)\right)\left(\Pi_{\frac{\tau_i}{2}} * \text{Ш}_{\tau_i}(t)\right). \tag{II.13}$$

Il s'agit d'un signal créneau périodique, dont la période varie selon $\{U_i\}_{i\in\mathbb{N}^*}$[25] et change tous les $\{\tau_i\}_{i\in\mathbb{N}^*}$[26].
La figure 28 montre sur un intervalle de temps discret de 200 secondes[27] l'ensemble des signaux définis , à savoir $x(t)$, le triangle périodique et $S(t)$; ainsi que les passages à zéros de $x(t)$.

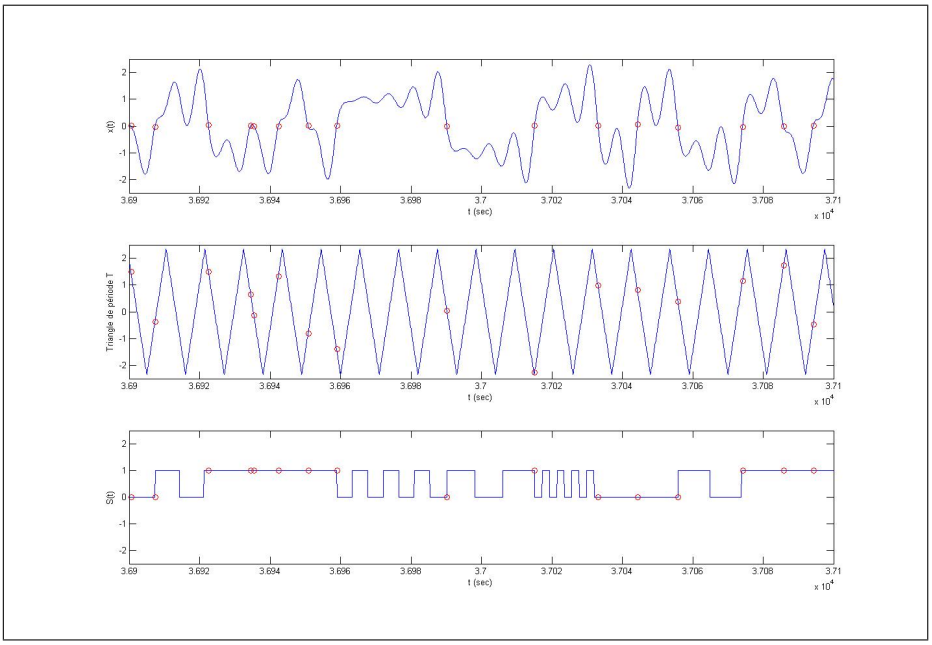


FIG. 28 – *Représentation sur* 2000 *points de* $x(t)$*, du triangle périodique, et de* $S(t)$ *obtenus avec* $a = -0,7$ *sur* $N = 1000000$ *points avec un pas* $h = 0,1$*. Les* t_i *sont cerclés.*

L'étape finale consiste à échantillonner $S(t)$ à une période T_e et ainsi collecter les échantillons créés en définissant la suite $\{s_i\}_{i\in\mathbb{N}^*}$,

$$S_e(t) \;:=\; \sum_{i\in\mathbb{N}^*} \underbrace{S(iT_e)}_{=:s_i}\,\delta(t - iT_e).$$

Alors, la suite $\{s_i\}_{i\in\mathbb{N}^*}$ devient, après le passage de l'oracle, une suite binaire pouvant servir de générateur de nombre pseudo-aléatoire.
Ce signal appartient à la classe des signaux binaires pseudo-aléatoires (SBPA). L'objet de la section suivante est de confronter le générateur ainsi créé à des tests statistiques afin d'évaluer ses performances, puis de faire de même avec des données réelles.

[25] Et donc $\{A_i\}_{i\in\mathbb{N}^*}$.
[26] Il faut donc que $U_i \leq \tau_i \quad \forall n \in \mathbb{N}^*$
[27] Soit $N = 2000$ points.

10 EXPÉRIMENTATIONS

Le but de cette section est de caractériser le flux pseudo-aléatoire construit à la section précédente.
Le problème se posant alors est “Comment évaluer une séquence pseudo-aléatoire ?”. Les qualificatifs “aléatoire” et “pseudo-aléatoire” sont attribués à une suite par postulat. Cela signifie que c’est l’observateur qui va juger *a priori* si le flux à disposition est un bon candidat, au point d’être qualifié d’“aléatoire” ou de “pseudo-aléatoire”. Une fois la séquence créée, il faut alors valider ou invalider *a posteriori* cette hypothèse à l’aide de tests statistiques issus du bon sens. Par exemple, l’utilisateur est en droit d’exiger qu’a partir d’un certain nombre d’échantillons à disposition il y ait en moyenne autant de 0 que de 1 dans sa séquence.
Les générateurs de ce type sont incontournables dans tout dispositif à connotation sécuritaire, tel qu’une Smart Card. Les algorithmes de cryptographie nécessitent pour fonctionner d’avoir à disposition un générateur de nombres ne se ressemblant pas sur un intervalle d’observation donné. Une défaillance du générateur[28] entraînerait alors des conséquences désastreuses en terme de sécurité, rendant alors à la merci du pirate l’ensemble des algorithmes utilisant le générateur. Nul n’est besoin d’argumenter plus pour comprendre que la qualité d’un générateur est primordiale dans le cadre du fonctionnement des Smart Card, et plus généralement dans le cadre de tout dispositif sécurisé.
Afin de standardiser les équipements de protection d’une Smart Card, l’Institut National des Standards et des Technologies (NIST), institution américaine, dans le cadre de l’administration des standards du traitement de l’information (FIPS) a défini 4 niveaux de sécurité des Smart Cards [Fip01]. Quel que soit le niveau envisagé, les flux aléatoires ou pseudo-aléatoires doivent satisfaire à une série de tests statistiques draconiens, dans la mesure où il suffit qu’un seul ne soit pas bon pour rejeter le générateur.
Dans cette section, les tests statistiques utilisés sont cinq tests issus de la norme FIPS et proposés dans [Men96], chapitre cinq. Certes il ne s’agit là que de cinq tests [29], néanmoins ces derniers permettent de caractériser suffisamment correctement le flux étudié. Le générateur sera considéré apte s’il satisfait aux cinq tests présentés dans la sous-section suivante.

10.1 Tests statistiques

Les cinq tests présentés servent à caractériser un flux supposé pseudo-aléatoire. Ces derniers sont construits de sorte à échouer en cas de redondance trop fréquente de certains symboles binaires, et réussir dans le cas contraire.
La séquence étudiée est supposée de longueur finie, mais de taille suffisamment grande pour que les tests aient un sens, donc $\{s_i\}_{i=1\ldots N_s}$ avec N_s le plus grand possible.

10.1.1 Test monobit

Le test monobit, ou encore test de la fréquence est aussi simple qu’intuitif. Ce dernier consiste à comparer le nombre de 1 et de 0 présents dans la séquence étudiée.
Si N_0 est le nombre de 0 et N_1 est le nombre de 1, alors la statistique X_1 définie par

$$X_1 \quad := \quad \frac{(N_0 - N_1)^2}{N_s},$$

est la réalisation d’une variable aléatoire $\mathbf{X}_1$ qui suit une loi du χ^2 à 1 degré de liberté,

$$\mathbf{X}_1 \quad \hookrightarrow \quad \chi^2(1),$$

[28] C’est-à-dire fonctionnant tel que des séquences similaires apparaissent régulièrement.
[29] Il en faudrait idéalement une infinité pour parler de générateur aléatoire

Remarque : *Ce test peut être construit très rapidement et permet donc d'éliminer tout aussi rapidement une séquence qui ne le satisfait pas.*

10.1.2 Test duobit

Appelé également test de fréquence, son principe est de vérifier que la proportion de symboles 00, 01, 10 et 11 est identique dans la séquence. Pour ce faire, soit N_{00}, N_{01}, N_{10} et N_{11}, les nombres d'occurrences respectifs de 00, 01, 10 et 11 et X_2 la statistique définie par

$$X_2 \quad := \quad \frac{4}{N_s - 1}(N_{00}^2 + N_{00}^2 + N_{00}^2 + N_{00}^2) - \frac{2}{N_s}(N_0^2 + N_1^2) + 1.$$

Cette dernière est la réalisation d'une variable aléatoire $\mathbf{X}_2$ qui suit une loi du χ^2 à 2 degrés de liberté,

$$\mathbf{X}_2 \quad \hookrightarrow \quad \chi^2(2),$$

10.1.3 Test du poker

Le test du poker consiste à vérifier que toutes les sous-séquences binaires possibles de longueur $M_s < N_s$ apparaissent en proportion identique dans la séquence totale[30].
M_s est déterminé comme étant le plus grand entier vérifiant

$$\left\lfloor \frac{N_s}{M_s} \right\rfloor \quad \geq \quad 5(2^{M_s}),$$

alors, si $K_3 = \left\lfloor \frac{N_s}{M_s} \right\rfloor$, la suite $\{s_i\}_{i=1\ldots N_s}$ peut être découpée en K_3 blocs de longueur M_s.
Sachant qu'il y a 2^{M_s} possibilités d'écrire un bloc binaire de taille M_s, soit N_i le nombre d'occurrences de la i^{me} possibilité, alors le test du poker est un succès si l'occurrence d'apparition d'une séquence de longueur M_s est la même pour tout $i = 1 \ldots 2^{M_s}$. Pour vérifier cela, soit X_3 la statistique définie par

$$X_3 \quad := \quad -K_3 + \frac{2^{M_s}}{K_3} \sum_{i=1}^{2^{M_s}} N_i^2.$$

Cette dernière est la réalisation d'une variable aléatoire $\mathbf{X}_3$ qui suit une loi du χ^2 à $2^{M_s} - 1$ degrés de liberté,

$$\mathbf{X}_3 \quad \hookrightarrow \quad \chi^2(2^{M_s} - 1),$$

Remarque : *Si $m = 1$, X_3 n'est rien d'autre que X_1*

[30] L'appellation "poker" vient de l'analogie de la séquence $\{s_i\}_{i=1\ldots N_s}$ avec un jeu de cartes, la sous-séquence de longueur M_s est alors une main du jeu

10.1.4 Test des trous et des blocs

Mondialement appelé runs[31] test, il vérifie que les proportions de sous-suites constituées de 0 (gaps) et de sous-suites constituées de 1 (blocs), de différentes tailles, sont identiques.
Si i est la longueur de la sous-suite (du run), alors le nombre théorique d'occurrences de cette sous-suite dans la suite entière est

$$e_i \quad = \quad \frac{N_s - i + 3}{2^{i+2}}.$$

Alors, si K_4 est l'entier vérifiant

$$K_4 \quad = \quad \underset{i=1\ldots N_s}{\operatorname{argmax}}[e_i \geq 5],$$

si B_i et G_i sont respectivement le nombre de blocs de 1 et de 0 de taille i pour $i = 1 \ldots K_4$, alors la statistique X_4 définie par

$$X_4 \quad := \quad \sum_{i=1}^{K_4} \frac{(B_i - e_i)^2}{e_i} + \sum_{i=1}^{K_4} \frac{(G_i - e_i)^2}{e_i},$$

est la réalisation d'une variable aléatoire $\mathbf{X}_4$ qui suit une loi du χ^2 à $2K_4 - 2$ degrés de liberté,

$$\mathbf{X}_4 \quad \hookrightarrow \quad \chi^2(2K_4 - 2),$$

10.1.5 Test de l'autocorrélation

Ce dernier test proposé consiste à vérifier l'absence de corrélations trop importantes dans le flux étudié. Il s'agit donc d'un test de redondance cyclique.
L'autocorrélation $A(d)$ est définie par

$$A(d) \quad := \quad \sum_{i=0}^{N_s - d} s_i \oplus s_{i+d} \quad \forall d = 1 \ldots \left\lfloor \frac{N_s}{2} \right\rfloor,$$

l'opérateur $\oplus$ désignant le ou exclusif (XOR).
La statistique X_5, construite à partir de $A(d)$, est alors définie par

$$X_5 \quad := \quad \frac{2A(d) - N_s + d}{\sqrt{N_s - d}},$$

réalisation d'un vecteur aléatoire $\mathbf{X}_5$ de dimension $\left\lfloor \frac{N_s}{2} \right\rfloor$ qui suit une loi normale centrée réduite,

$$\mathbf{X}_5 \quad \hookrightarrow \quad \mathcal{N}(\vec{0}, \mathrm{Id}_{\lfloor \frac{N_s}{2} \rfloor}),$$

> ***Remarque :*** *En toute rigueur, un test de gaussianité sur le vecteur X_5 est nécessaire. Seule une approche qualitative consistant à vérifier que plus de 99% des valeurs sont dans l'intervalle $[-3; 3]$ est effectuée.*

[31] L'anglicisme "run" désigne une succession de 0 ou de 1.

Pour les quatre premiers tests, les valeurs

$$\begin{aligned}\chi_1^s &:= \chi^2_{0,9}(1) \approx 2,702\\ \chi_2^s &:= \chi^2_{0,9}(2) \approx 4,607\\ \chi_3^s &:= \chi^2_{0,9}(2^{M_s}-1)\\ \chi_4^s &:= \chi^2_{0,9}(2K_4-2),\end{aligned}$$

représentent les seuils d'acceptation à 90% respectivement associés à X_1, X_2, X_3 et X_4. Alors, si les statistiques sont en dessous de leur seuil,

$$X_i \leq \chi_i^s \quad i = 1\dots 4$$

et si de plus X_5 est dans $[-3;3]$, alors l'hypothèse consistant à dire que le flux est pseudo-aléatoire est acceptée.

Remarque : *Les tests sont réalisés selon un ordre croissant de complexité. Par exemple, si un flux binaire ne passe pas le test χ_1, alors, l'hypothèse pseudo-aléatoire est rejetée avant même de confronter le flux aux tests suivants, plus complexes.*

10.2 Caractérisation d'un flux issu de simulations numériques

Cette section présente l'étude de la caractérisation pseudo-aléatoire d'un flux obtenu par simulations numériques par l'intermédiaire des tests

$$(X_1\,;\,X_2\,;\,X_3\,;\,X_4\,;\,X_5).$$

Le flux a été obtenu à partir de la méthode décrite dans la section 9, à partir d'une trajectoire chaotique du problème (P_a^h) avec $a = -0,7$, calculée sur $N = 2000000$ de points et un pas de discrétisation $h = 0,1$, obtenue en environ 8 heures de calculs[32]. La première composante de la trajectoire $x(t)$ est extraite, afin d'en calculer les instants de passage à zéro. Les $N_s = 13356$ instants recueillis servent à construire la séquence $\{s_i\}_{i=1\dots N_s}$ à l'aide de l'oracle valeur moyenne[33], l sera de nouveau utilisé dans la section 10.3. Cette séquence représente, sur un intervalle d'observation fini, le flux supposé pseudo-aléatoire.

- Pour X_1, il y a $N_0 = 2503$ zéros et $N_1 = 2497$ uns et ainsi, $X_1 = 0,007$.
- Pour X_2, le nombre d'occurrences de chaque mots de 2 bits est $N_{00} = 1256$, $N_{01} = 1247$, $N_{10} = 1246$ et $N_{11} = 1250$, soit $X_2 = 0,041$.
- Pour le test du Poker, $M_s = 7$, donc le flux est divisible en $K_3 = 714$ morceaux. Les occurrences de chacun des $2^{M_s} = 128$ mots possibles sont données figure 29. Après calculs, $X_3 = 139,6919$.

[32] Sur une station 2x3,6Ghz avec 3Go de RAM

[33] Si la valeur en cours est supérieure à la valeur moyenne, alors le symbole 1 est généré, dans le cas contraire c'est le symbole 0

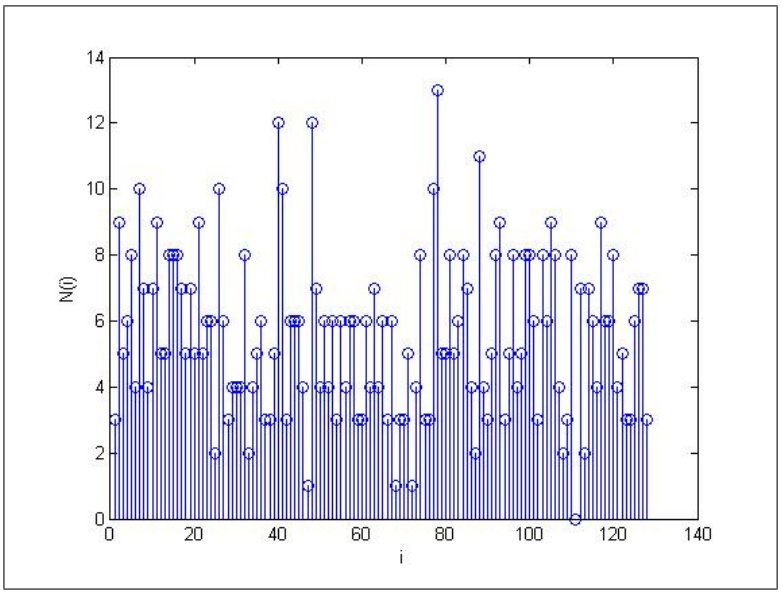


FIG. 29 – *Représentation des occurrences de chaque mot binaire de* 1 *à* 64 *dans* $\{s_i\}_{i=1\ldots N_s}$.

– Dans le cadre du test des trous et des blocs, la taille maximum de sous-suite est $K_4 = 8$. Les proportions idéales, celles de trous et celles de blocs sont illustrées figure 30, et $X_4 = 14,212$.

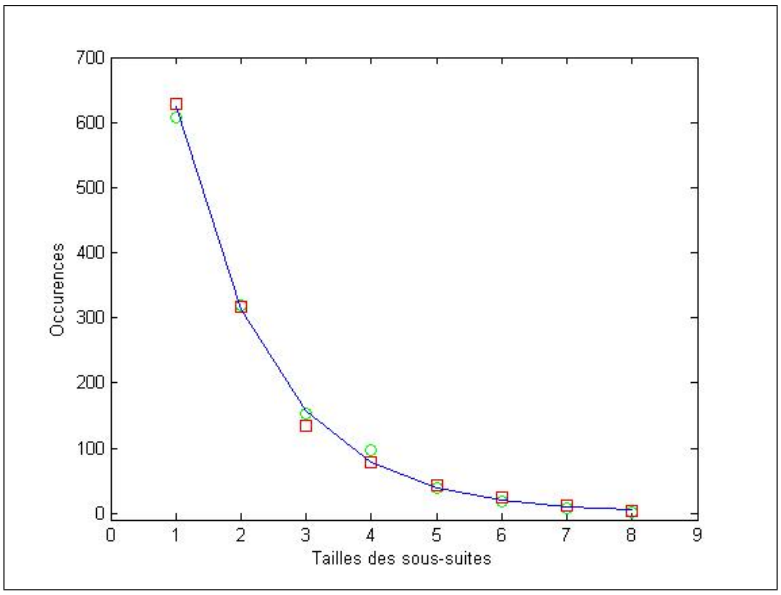


FIG. 30 – *Représentation des occurrences théoriques (trait plein), de trous (ronds) et de blocs (carrés).*

– Enfin, le test de l'autocorrélation, sur 2500 points, donne le résultat présenté figure 31, dont l'ensemble des valeurs est compris dans l'intervalle de confiance $[-3\,;\,3]$.

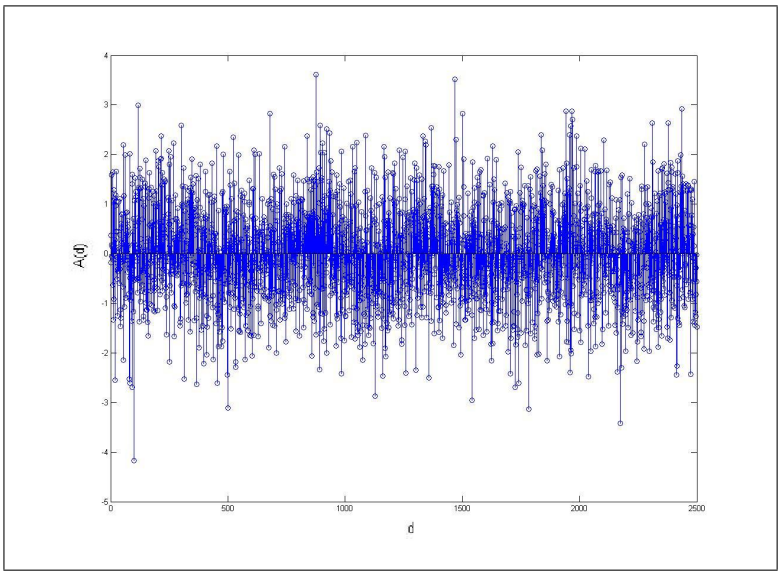


FIG. 31 – *Autocorrélation binaire de la suite* $\{s_i\}_{i=1...N_s}$ *pour des décalages positifs.*

L'ensemble des résultats est synthétisé dans le tableau 15.

	$\chi^2_{0,9}$	Score
X_1	$2,702$	$0,007$
X_2	$4,607$	$0,041$
X_3	$147,83$	$139,691$
X_4	$21,057$	$14,212$
X_5	99% des valeurs $\in [-3\,;\,3]$	oui

TAB. 15 – Récapitulatif des 5 tests

Les résultats obtenus sont tels que tous les tests sont positifs avec des scores particulièrement bons pour X_1 et X_2. Aucun traitement *a posteriori* n'est appliqué au flux. Cependant, il faut souligner le non respect de l'hypothèse des 20000 bits minimum requis, pour que les tests soient valides [Fip01]. L'étude de ce flux permet néanmoins d'établir une tendance statistique permettant de le qualifier de pseudo-aléatoire. Ces résultats sont à confirmer par des simulations avec des flux de taille $N > 20000$ pour rentrer en conformité avec le standard FIPS.
Si dans ce cas les tests n'étaient pas tous positifs, il est toujours possible d'utiliser des techniques de redressement des valeurs [Erg06]. Après avoir étudié un flux issu de simulations numériques, dans la prochaine section la série de tests est appliquée à un flux issu de données réelles.

10.3 Caractérisation d'un flux issu d'un circuit électronique

Les données sont issues du circuit électronique réalisé par V. Telandro [Tel06]. L'objectif est d'obtenir au moins les mêmes scores que ceux de la simulation numérique précédente. L'observation est un enregistrement de $T = 2.10^{-3}$ (sec) disponible sur $N = 13\,960\,321$ points correspondant au signal créneau II.13. La fréquence d'échantillonnage est de $F_e = 6,98$ (GHz). La figure 32 montre la représentation d'une portion de ce signal, dont les hauteurs de paliers sont 0 (V) où $1,8$ (V).

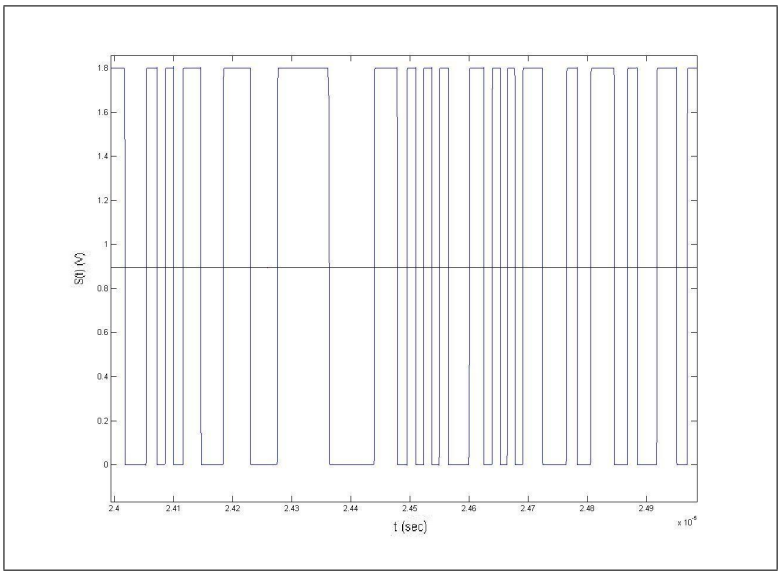


FIG. 32 – *Signal créneau observé sur* 10^{-6} *(sec) ainsi que sa valeur moyenne.*

Du signal sont recueillies $N_s = 10044$ valeurs, suivant un échantillonnage idéal, avec une fréquence $F = 5,02$ (MHz)[34]. Ce choix expérimental est le fruit de discussions avec V. Telandro, il correspond à une situation réaliste et de plus compatible avec les performances du matériel à disposition[35]. Cette approche permet de construire la séquence $\{s_i\}_{i=1...N_s}$ à l'aide de l'oracle valeur moyenne : si un échantillon à une valeur supérieure à la valeur moyenne, alors il génère un 1, et inversement pour le 0. Cette suite d'environ 10000 points est alors soumise aux cinq tests statistiques présentés dans la section précédente.

- Pour X_1, il y a $N_0 = 5065$ zéros pour $N_1 = 4979$ uns et ainsi, $X_1 = 0,736$.
- Concernant X_2, le nombre d'occurrences est $N_{00} = 2573$, $N_{01} = 2491$, $N_{10} = 2491$ et $N_{11} = 2488$, soit $X_2 = 1,234$.
- Pour le test du Poker, $M_s = 7$, le flux est divisible en $K_3 = 1434$ morceaux. Les occurrences de chacun des $2^{M_s} = 128$ mots possibles, données figure 33, et $X_3 = 138,954$.

[34] Qui n'a rien à voir avec F_e.

[35] Il n'est pas aisé de manipuler un fichier contenant des dizaines de millions de données

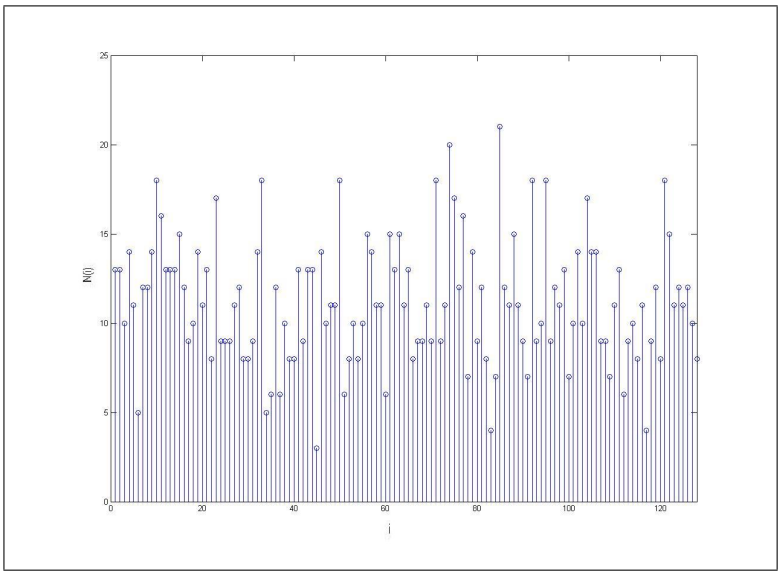


FIG. 33 – *Représentation des occurrences de chaque mot binaire de pendant décimal* 1 *à* 128 *dans* $\{s_i\}_{i=1...N_s}$.

– Dans le cadre du test des trous et des blocs, la taille maximum de sous-suite est $K_4 = 9$. Les proportions idéales, celles de trous et celles de blocs sont illustrées figure 34, et $X_4 = 22,855$.

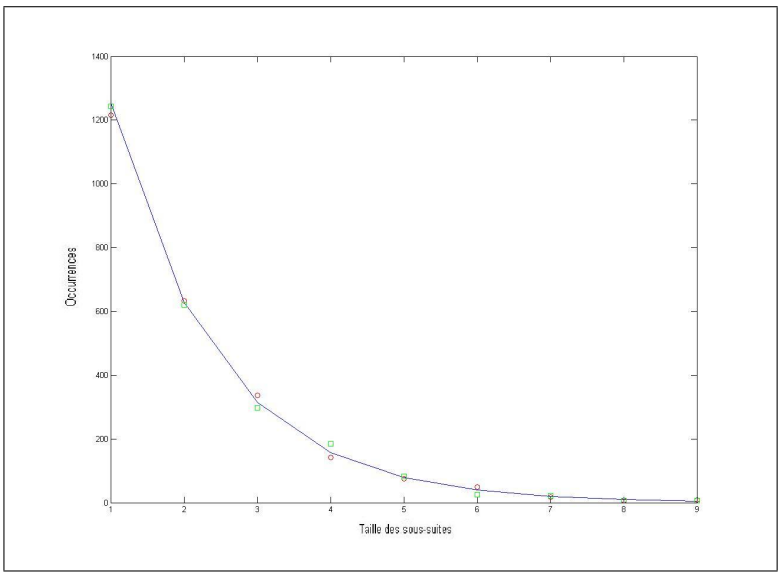


FIG. 34 – *Représentation des occurrences théoriques (trait plein), de trous (ronds) et de blocs (carrés).*

– Le test de l'autocorrélation est effectué sur 5022 points, le résultat est présenté figure 35, sauf exceptions ponctuelles, ses valeurs sont contenues dans l'intervalle de confiance $[-3\,;\,3]$.

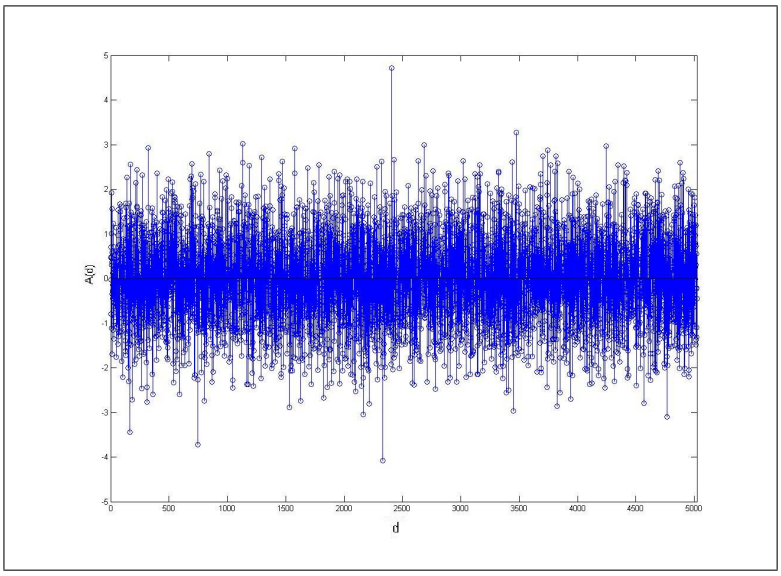


FIG. 35 – *Autocorrélation binaire de la suite* $\{s_i\}_{i=1...N_s}$ *pour des décalages positifs.*

L'ensemble des résultats est synthétisé dans le tableau 16.

	$\chi^2_{0,9}$	Score
X_1	$2,702$	$0,736$
X_2	$4,607$	$1,234$
X_3	$147,83$	$138,954$
X_4	$21,057$	$20,855$
X_5	99% des valeurs $\in [-3\,;\,3]$	oui

TAB. 16 – Récapitulatif des 5 tests

Ici encore, la tendance observée à la section précédente se confirme, à savoir que les résultats sont positifs. Cependant le test X_4 est proche de son seuil. Les scores sont tout de même plus qu'honorables, sachant qu'il faudrait au moins deux fois plus de bits pour que les tests soient complètement exhaustifs. De plus, là encore aucune technique *a posteriori* de redressement des données n'a été utilisée.
De ces résultats se dégage une tendance positive, qu'il faut confirmer par des simulations plus longues afin d'avoir à disposition une séquence de plus de 20000 bits[36].

11 CONCLUSION

Ce chapitre traite de l'étude et la caractérisation d'un système dynamique non-linéaire en régime chaotique, puis de son utilisation pour générer des nombres pseudo-aléatoires. Il est le fruit d'un travail commun avec V. Telandro dans le cadre de la sécurisation des Smart Cards pour ST Microelectronics, sa tâche étant d'implémenter sur silicium un circuit analogique basé sur un oscillateur chaotique lui aussi destiné à générer des séquences pseudo-aléatoires.
L'étude débute par la modélisation mathématique du problème, aboutissant au problème (P_a), composé d'une équation différentielle non-linéaire du troisième ordre, de paramètre de contrôle a, et d'un jeu de trois conditions initiales. Le problème est alors canoniquement ramené à un

[36]De leur côté également, les microélectroniciens ont besoin de moyens matériels conséquents pour obtenir une telle séquence.

système dynamique non-linéaire de dimension 3. L'existence et l'unicité du problème pour une condition initiale fixée est ensuite prouvée, légitimant la suite des travaux. Afin d'étudier numériquement le problème (P_a), le problème discret (P_a^h) est introduit. Ce dernier, stable, consistant, est convergeant vers le problème (P_a). Parmi les méthodes numériques disponibles dans la littérature pour étudier informatiquement (P_a^h), et donc (P_a), la méthode de Runge-Kutta, basée sur les différences finies, conjugue simplicité d'implémentation et précision puisque convergente en $\mathcal{O}(h^4)$, ce qui explique un tel choix.
La caractérisation commence par l'étude du système dynamique linéarisé au voisinage de ses points d'équilibre, qui renseigne sur le comportement local des solutions du problème. Les valeurs propres de la matrice Jacobienne sont calculées ainsi que les éléments propres en fonction du paramètre de contrôle a. Dans tous les cas, il y a une valeur propre réelle et deux valeurs propres complexes conjuguées auxquelles sont respectivement associés une droite et un plan propre. La compréhension de la dynamique locale aide grandement à la compréhension de la dynamique globale, et le regroupement de l'ensemble des résultats établis par le biais de simulations numériques permet de dégager les intervalles de valeurs de paramètre a correspondant aux comportements possibles des solutions de (P_a), à savoir convergentes vers un point ou vers un cycle limite, divergentes, ou chaotiques car décrivant un attracteur étrange : le Double Scroll. L'étude focalise sur cet intervalle et confirme notamment que le système est dans ce cas bien en évolution chaotique, grâce au théorème de Shil'nikov dont les hypothèses sont vérifiées, permettant d'établir rigoureusement la présence de chaos hétéroclinique. Il est alors intéressant d'analyser les indicateurs classique du chaos pour en faire ressortir les propriétés importantes pour la suite. Les exposants de Lyapunov sont calculés, retournant la signature $(+\,;\,0\,;-)$ synonyme de chaos. L'étude du diagramme de bifurcation associé à (P_a) permet d'avoir confirmation des valeurs de bifurcation du système, établies lors de l'étude de la dynamique locale. Il ressort que le système est chaotique si $a \in]-0,99\,;\,-0,4[$ Cet intervalle est différent de ceux trouvés par les microélectroniciens, cependant, la valeur $a = -0,7$ correspond dans tous les cas à un système dynamique chaotique. Enfin, l'étude spectrale d'une solution de (P_a) montre que dans le cas d'un fonctionnement en mode chaotique, le spectre est bien large bande, présentant de nombreux pics correspondant aux périodes propres de la solution. Ce nombre élevé de périodes entraîne cet aspect désordonné des trajectoires qui empêche de prédire aisément les futures valeurs de cette dernière.
C'est sur la base de cette constatation et de la propriété de S.C.I. que se poursuit l'étude. Si les électroniciens ne trouvent pas exactement les mêmes résultats que ceux issus des simulations numériques, c'est en particulier parce qu'il est presque sûrement impossible d'imposer au système exactement les mêmes conditions initiales. Ceci est dû aux bruits de différentes natures inhérents à tout circuit électronique.
Ainsi, il est possible de tirer profit du système en mode chaotique en prélevant des valeurs particulières sur les trajectoires de ce dernier. Dans le cas de cette étude, ces valeurs correspondent aux instants de passage à travers la section de Poincarré $x = 0$, ainsi qu'aux intervalles de temps de ces passages. Les signaux créés à partir de ces données servent à générer un flux supposé pseudo-aléatoire.
La phase d'expérimentation consiste à caractériser ce flux. Cette caractérisation se fait à l'aide de 5 tests statistiques issus de la norme de sécurité FIPS $140-2$. Le flux issu de simulations numériques aussi bien que celui issu du circuit de Telandro passe l'ensemble des tests avec un niveau de confiance de 90%. Il n'est donc pas nécessaire dans ce cas d'utiliser une quelconque technique de redressement du flux.
A travers le passage de ces 5 tests, une première étape à donc été remportée, la seconde consistant d'une part à travailler avec des échantillons beaucoup plus gros[37], au moins 20000, et d'autre

[37]Cela nécessite donc des moyens matériels plus importants.

part à prendre en compte beaucoup plus de tests parmi tous ceux existants [Fip01]. Ce volumineux travail reste à accomplir.
La méthode proposée dans ce chapitre permet donc d'avoir à disposition un générateur de nombre pseudo-aléatoire. La conception analogique de cette dernière ainsi que la caractérisation de ses performances ont permis de déposer un brevet avec l'équipe Smart Card de ST Microelectronics [ST06] .
Dans le cas où les générateurs ne satisfont pas les tests requis, il existe des techniques de redressement de flux [Erg06]. L'ajout d'une telle technique, bien qu'efficace, est d'un certain point de vue tendancieux vu que le concept d'*aléatoire* est basé sur l'absence d'intervention humaine lors de la réalisation d'un événement.
Le flux créé joue un rôle important dans le principe du masquage par décomposition des signaux du chapitre suivant puisque les bits générés, selon la technique basée sur l'oscillateur chaotique de ce chapitre, servent à réaliser des permutations pseudo-aléatoires des échantillons d'un signal, étape de sécurité qui s'avère être nécessaire.

CHAPITRE III

MASQUAGE PAR DÉCOMPOSITION DES SIGNAUX

1 INTRODUCTION

Le but de ce chapitre est de développer sous plusieurs déclinaisons une technique de masquage de signaux de consommation de courant, appelée masquage par décomposition des signaux.
Une telle approche consiste en la substitution du signal à masquer par des coefficients, qui bien que dépendants du signal ont la propriété d'être statistiquement décorrélés à l'ordre 2. Le signal masqué ainsi construit s'apparente à une suite blanche. Pour déterminer ces coefficients, le signal va être décomposé sur une base de fonctions, construite de sorte que la décorrélation à l'ordre 2 des coefficients de décomposition soit assurée.
Le contexte de sécurisation des noeuds d'alimentation des Smart Card ainsi que la physique du problème qui lui est lié impose le respect de certaines contraintes permettant la conception de techniques réalistes. Il faut en particulier que la puissance de l'observation soit identique à celle du signal masqué pour ne pas créer de sur- ou sous-consommation.
Hotelling a été le premier au début du $XX^{\text{ème}}$ siècle à se pencher sur le problème consistant à déterminer une transformation qui associe à une observation des échantillons décorrélés à l'ordre 2 [Hot33]. Il a été rejoint quelque années plus tard par Karhunen [Kar46] et Loève [Lov55] qui indépendamment l'un de l'autre ont permis à travers les articles cités d'établir de façon formelle ce qui est communément appelé le développement de Karhunen-Loève, consistant à développer un processus aléatoire sur une base engendrée par des fonctions déterministes telles que les coordonnées du processus, exprimées dans cette base, sont des variables aléatoires statistiquement décorrélées.
La décomposition des signaux trouve ses fondements dans les travaux de Fourier et Dirichlet au $XIX^{\text{ème}}$ siècle jusqu'a ceux de Hilbert au début du $XX^{\text{ème}}$ siècle, aboutissant entre autre, par le biais du théorème de la projection orthogonale, à la notion de développement de fonctions de carré sommable sur une base de fonctions orthogonales.
Une telle volonté de décomposer des fonctions est née d'au moins deux motivations. D'une part, vu qu'il est possible de décomposer tout vecteur d'un espace Euclidien de dimension finie sur une base de vecteurs d'un espace Euclidien de dimension finie, une extension naturelle de cette démarche serait de faire de même, non plus avec des vecteurs mais avec des fonctions, considérant alors qu'une fonction n'est rien d'autre qu'un vecteur de dimension infinie. D'autre part, dans certains domaines tels que l'étude des équations aux dérivées partielles de la physique, l'étude des équations intégrales, l'approche de Galerkine pour la méthode des éléments finis [Gar01], le traitement et la compression des données ou encore l'approximation des fonctions compliquées, le fait d'exprimer la solution lorsqu'elle existe sous la forme de son développe-

ment permet d'ouvrir de nouveaux horizons relatifs à l'étude des équations qui lui sont associées en simplifiant grandement le problème. En fait, cette démarche vérifie l'adage universel consistant à dire que lorsque l'on ne sait pas faire quelque chose, on se ramène à ce que l'on sait faire. Remis dans le contexte, cela signifie que l'étude d'un signal compliqué peut se ramener par décomposition à l'étude d'une famille de signaux élémentaires, une base de fonctions, dont la somme pondérée par des coefficients de décomposition convergerait au sens d'une certaine norme vers le signal étudié.
Tout au long de ce chapitre, les signaux seront modélisés par des processus aléatoires de second moment fini dont toutes les réalisations sont de carré sommable.
Après avoir introduit les espaces fonctionnels de travail adéquat, le développement de Karhunen-Loève sera présenté ainsi que certaines de ses applications. Puis, dans le cadre de ce développement, les fonctions de base seront vues comme étant les solutions d'une équation intégrale. Ainsi, afin d'établir l'existence de ces solutions et la classe à laquelle elles appartiennent, la voie choisie consiste à montrer que déterminer ces dernières est équivalent à rechercher les éléments propres d'un opérateur d'Hilbert-Schmidt. Le travail se ramènera alors à montrer que l'opérateur intégral considéré est de Hilbert-Schmidt puis de tirer partie des propriétés de ce dernier. Une fois ce cadre de travail construit, la technique de masquage dite par décomposition des signaux sera alors présentée, tout d'abord d'un point de vue général puis sous différentes déclinaisons correspondant à plusieurs cas de figure intervenant lors de la mise en oeuvre algorithmique de la méthode. Ainsi, afin de prendre en compte les contraintes de faisabilité électroniques une attention sera portée sur les aspects de la quantité de calcul[1] et de la résistance aux attaques[2]. Chaque déclinaison présentée donne selon ses propres critères des résultats différents qui seront interprétés qualitativement, quantitativement en termes de décorrélation à l'ordre 2 et illustrés par le masquage de signaux expérimentaux. Enfin, l'utilisation des techniques de masquage proposées ainsi que des moyens mis en place pour évaluer leurs performances en terme de décorrélation à l'ordre 2 et de résistance aux attaques seront appliqués aux données réelles qui sont des mesures d'activité de consommation de courant réalisées par ST Microelectronics.

2 ESPACES FONCTIONNELS DE TRAVAIL

2.1 Espaces de décomposition des signaux

Un espace de Hilbert séparable est un espace vectoriel normé complet dont la norme découle d'un produit scalaire, contenant un sous-espace partout dense et dénombrable.
Soit D un sous-ensemble compact de $\mathbb{R}$. Alors, $L^2(D)$ est un espace de Hilbert séparable, la démonstration complexe se trouve par exemple dans [Kol94, Akh93] (respectivement pp. 373-380 et pp. 17-18). A l'intérieur de cet espace, il est possible de décomposer tout signal $x(t) \in L^2(D)$ sur une base de fonctions de $L^2(D)$, de façon unique, cette base, de dimension infinie, est engendrée par une famille dénombrable de fonctions $\Psi_n(t) \in L^2(D) \quad \forall n \in \mathbb{N}^*$:

$$x(t) \;=\; \sum_{n=1}^{\infty} x_n \Psi_n(t) \quad \forall t \in D$$

Les coefficients de la décomposition sont obtenus par les produits scalaires calculés avec les éléments de la base $\{\Phi_n\}_{n\in\mathbb{N}^*}$,

$$x_n \;:=\; \langle x(t)\,;\,\Phi_n(t)\rangle \quad \forall t \in D.$$

[1] Conception de dispositifs faible coût, faible puissance
[2] Conception de dispositifs insensibles aux techniques d'attaques à base de corrélations

Les décompositions qui vont être utilisées par la suite, que ce soit dans ce chapitre avec le développement de Karhunen-Loève ou dans le chapitre suivant avec la théorie du filtrage adapté stochastique, sont fondées à partir de la notion générale de décomposition d'un signal aléatoire sur une base de fonctions déterministes. Il faut donc donner un cadre mathématique suffisamment précis à l'intérieur duquel il est légitimement possible de développer un processus aléatoire appartenant à une certaine classe sur une base appropriée.

2.2 Caractérisation et développement d'un processus aléatoire à réalisations dans $L^2(D)$

2.2.1 Caractérisation

Soit Ω un ensemble de réalisations possibles constituée de fonctions de $L^2(D)$. Les processus stochastiques rencontrés dans ce chapitre sont à réalisations réelles à valeurs dans D, centrées, de moments d'ordre 2 finis. L'ensemble des processus admissibles peut être vu comme la classe d'équivalence de $\mathbf{S}(t)$, un processus stochastique de $\Omega \times D \to \mathbb{R}$ centré, de moment d'ordre 2 fini, c'est-à-dire que pour tout $t \in D$ et pour tout $(t_1, t_2) \in D^2$

$$\left\{ \begin{array}{lcl} \mathbb{E}\left[\mathbf{S}(t)\right] & = & 0 \\ \mathbb{E}\left[\mathbf{S}(t_1)\mathbf{S}(t_2)\right] & < & +\infty \end{array} \right.$$

Ainsi, d'une part toute réalisation $S(t)$ de $\mathbf{S}(t)$ appartient à $L_2(D)$ et représente la classe d'équivalence des fonctions presque partout égales à $S(t)$. D'autre part, pour un temps $t_0 \in D$ donné, $\mathbf{S}(t_0)$ est une variable aléatoire réelle de moment d'ordre 2 finis représentative de la classe d'équivalence des variables aléatoires égales en moyenne quadratique à $\mathbf{S}(t_0)$ [Pay67].
Ainsi, pour être admissible, un processus doit vérifier simultanément

$$\left\{ \begin{array}{rcl} \forall \omega \in \Omega\,,\, \displaystyle\int_D S^2\, d\mu < \infty & \Leftrightarrow & \forall \omega \in \Omega\,,\, S(\omega,\,.\,) \in L^2_{\mathbb{R}}(D,\mu) \\ \forall t \in D\,,\, \mathbb{E}\left[\mathbf{S}^2\right] = \displaystyle\int_\Omega \mathbf{S}^2(t)\, dP < \infty & \Leftrightarrow & \forall t \in D\,,\, \mathbf{S}(\,.\,,t) \in L^2_{\mathbb{R}}(\Omega,P) \end{array} \right. \tag{III.1}$$

où μ est la mesure de Lebesgue[3] et P la mesure de probabilité associée à Ω. L'espace des processus stochastiques vérifiant III.1 muni du produit scalaire

$$\mathbb{E}\left[\,\langle \mathbf{U}(t)\,;\,\mathbf{V}(t)\rangle\,\right] \;:=\; \int_\Omega \int_D \mathbf{U}\mathbf{V}\, d\mu dP$$

et donc de la norme induite

$$\mathbb{E}\left[\,\|\mathbf{U}(t)\|^2\,\right] \;:=\; \int_\Omega \int_D \mathbf{U}^2\, d\mu dP,$$

où $\mathbf{U}(t)$ et $\mathbf{V}(t)$ sont deux processus admissibles, est un espace de Hilbert. Un travail complet et dense de caractérisation de tels processus est exposé dans le rapport préliminaire de Thèse de C. Fraschini [Fra06].

[3] Dans tout le chapitre la mesure de Lebesgue ne s'applique que sur des ensembles élémentaires, voilà pourquoi il a été choisi de ne pas être plus évasif sur le sujet.

2.2.2 Développement

Soit $\{\Psi_n(t)\}_{n\in\mathbb{N}}$ une base de fonctions déterministes de $L_2(D)$ et $\{\mathbf{s}_n\}_{n\in\mathbb{N}}$ une suite de variables aléatoires réelles centrées et décorrélées au second ordre,

$$\left\{\begin{array}{lcl}\mathbb{E}[\mathbf{s}_n] & = & 0\\ \mathbb{E}[\mathbf{s}_n\mathbf{s}_m] & = & \mathbb{E}[\mathbf{s}_n^2]\,\delta[n-m], \quad \forall(n,m)\in\mathbb{N}^2\end{array}\right.$$

où $\delta[n-m]$ est le symbole de Kroenecker.
L'objectif est de donner un développement possible d'un processus aléatoire admissible au sens de la section précédente sur une base de fonctions déterministes pondérées par des variables aléatoires décorrélées. Dans ces conditions, le processus stochastique $\mathbf{S}(t)$ est doublement orthogonal au sens décrit par [Bla81] chapitre IX et il se décompose, au sens de l'égalité en moyenne quadratique, de la façon suivante :

$$\mathbf{S}(t) \;=\; \sum_{n=1}^{\infty}\mathbf{s}_n\Psi_n(t) \quad \forall t\in D \tag{III.2}$$

avec

$$\Psi_n(t) \;:=\; \frac{\mathbb{E}[\mathbf{s}_n\mathbf{S}(t)]}{\mathbb{E}[\mathbf{s}_n^2]}, \tag{III.3}$$

cette relation permettant de déterminer la famille $\{\Psi_n(t)\}_{n\in\mathbb{N}}$ dès lors que les coefficients $\mathbf{s}_n$ sont connus.
$\mathbf{S}(t)$ est projeté sur fonctions déterministes de la base $\{\Phi_n(t)\}_{n\in\mathbb{N}^*}$. La valeur de cette projection est

$$\mathbf{s}_n := \int_D \mathbf{S}(t)\Phi_n(t)\,dt. \tag{III.4}$$

Les fonctions $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ doivent être telles que la décorrélation des coefficients $\{\mathbf{s}_n\}_{n\in\mathbb{N}}$ soit assurée. La proposition suivante donne une condition nécessaire et suffisante assurant cette décorrélation.

Proposition III.1. *Pour que la décorrélation des coefficients $\{\boldsymbol{s}_n\}_{n\in\mathbb{N}}$ soit assurée, il faut et il suffit que les fonctions $\{\Phi_n(t)\}$ vérifient pour tout $n\in\mathbb{N}$*

$$\int_D\int_D R(t_1\,;\,t_2)\Phi_n(t_1)\Phi_m(t_2)dt_1dt_2 \;=\; \mathbb{E}\left[\boldsymbol{s}_n^2\right]\delta[n-m] \quad \forall(n,m)\in\mathbb{N}^2. \tag{III.5}$$

où $R(t_1\,;\,t_2)$ est la covariance de $\mathbf{S}(t)$,

$$R(t_1\,;\,t_2) \;:=\; \mathbb{E}[\mathbf{S}(t_1)\mathbf{S}(t_2)] \quad \forall(t_1,t_2)\in D^2.$$

Preuve . *L'expression de la contrainte de décorrélation donne,*

$$\begin{array}{rcl}\mathbb{E}[\boldsymbol{s}_n\boldsymbol{s}_m] & = & \mathbb{E}\left[\boldsymbol{s}_n^2\right]\delta[n-m]\\ \mathbb{E}\left[\left(\displaystyle\int_D \boldsymbol{S}(t_1)\Phi_n(t_1)\,dt_1\right)\left(\int_D \boldsymbol{S}(t_2)\Phi_m(t_2)\,dt_2\right)\right] & = & \mathbb{E}\left[\boldsymbol{s}_n^2\right]\delta[n-m],\end{array}$$

et le théorème de Fubini permet de regrouper les termes du membre de droite,

$$\begin{array}{rcl}\mathbb{E}\left[\displaystyle\int_D\int_D \boldsymbol{S}(t_1)\boldsymbol{S}(t_2)\Phi_n(t_1)\Phi_m(t_2)\,dt_1dt_2\right] & = & \mathbb{E}\left[\boldsymbol{s}_n^2\right]\delta[n-m]\\ \displaystyle\int_D\int_D R(t_1\,;\,t_2)\Phi_n(t_1)\Phi_m(t_2)\,dt_1dt_2 & = & \mathbb{E}\left[\boldsymbol{s}_n^2\right]\delta[n-m]\end{array}$$

□

Sous l'hypothèse qu'une famille $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ a été déterminée en utilisant la relation III.5 et en injectant l'expression III.4 dans III.3, la relation de passage entre la famille de fonctions $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ et $\{\Psi_n(t)\}_{n\in\mathbb{N}}$ est :

$$\Psi_n(t) = \frac{1}{\mathbb{E}\left[\mathbf{s}_n^2\right]} \int_D R(t,t_2)\Phi_n(t_2)\,dt_2. \tag{III.6}$$

Les projections établies, que ce soit sur la base $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ ou sur la base orthonormale $\{\Psi_n(t)\}_{n\in\mathbb{N}}$ ainsi que la relation III.6 laissent supposer qu'il existe un lien d'orthogonalité entre ces deux familles. En effet,

Proposition III.2. *Les familles de fonction $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ et $\{\Psi_n(t)\}_{n\in\mathbb{N}}$ sont bi-orthonormales,*

$$\int_D \Psi_m(t)\Phi_n(t)\,dt = \delta[n-m] \quad \forall t \in D \quad \forall (n,m) \in \mathbb{N}^2.$$

Preuve . *Partant de l'équation III.5 et de la relation de passage III.6*

$$\begin{aligned}
\int_D \int_D R(t_1,t_2)\Phi_n(t_1)\Phi_m(t_2)dt_1dt_2 &= E[\boldsymbol{s}_n^2]\delta[n-m] \\
\int_D \left(\int_D R(t_1,t_2)\Phi_m(t_2)\,dt_2\right)\Phi_n(t_1)\,dt_1 &= E[\boldsymbol{s}_n^2]\delta[n-m] \\
\int_D \left(\mathbb{E}\left[\boldsymbol{s}_n^2\right]\Psi_m(t_1)\right)\Phi_n(t_1)\,dt_1 &= E[\boldsymbol{s}_n^2]\delta[n-m] \\
\int_D \Psi_m(t_1)\Phi_n(t_1)\,dt_1 &= \delta[n-m]
\end{aligned}$$

□

Ce résultat repose sur la décorrélation imposée aux coefficients de décomposition $\{\mathbf{s}_n\}_{n\in\mathbb{N}}$. Dans le cas où le signal $\mathbf{S}(t)$ est stationnaire à l'ordre 2, la fonction d'autocorrélation $R(t_1,t_2)$ ne dépend que relativement du temps comme fonction de $\tau := t_1 - t_2$. L'autocorrélation est alors définie par la fonction d'une seule variable $r(\tau) := R(t_1,t_2) = R(t_1-t_2\,;\,0)$ pour tout $\tau \in \mathbb{R}$, pour tout $t \in D$ et pour tout $(t_1,t_2) \in D^2$

$$\begin{cases} \mathbb{E}\left[\mathbf{S}(t)\right] &= 0 \\ \mathbb{E}\left[\mathbf{S}(t_1)\mathbf{S}(t_2)\right] &= r(\tau) \quad \forall t \in D \end{cases}$$

Dans ce cas, le développement ainsi que les résultats présentés demeurent valides, il suffit de remplacer les termes $R(t_1,t_2)$ par $r(t_1-t_2)$.
Ainsi, un processus aléatoire stationnaire à l'ordre 2 se décompose comme le suggère la relation III.2 sur une base de fonctions déterministes pondérées par des variables aléatoires centrées, décorrélées. Dans un premier temps, les variables aléatoires sont déterminées par projection de l'observation sur une famille de fonctions solution de l'équation III.5 puis les fonctions de base sont déterminées par le biais de la relation de passage III.6.
Cependant, les résultats établis jusqu'à présent sont encore abstraits, puisque il n'a pas encore été question d'une méthode permettant de calculer effectivement les coefficients de décomposition ainsi que les fonctions de base. Il reste également à voir comment tirer profit d'une telle démarche pour masquer des signaux. Ceci est l'objet des prochaines sections.

3 DÉVELOPPEMENT DE KARUNHEN-LOÈVE, APPLICATION AU MASQUAGE D'UN SIGNAL

3.1 Introduction

Introduit par Karhunen [Kar46] et Loève [Lov55] le développement de Karhunhen-Loève consiste à décomposer un processus aléatoire, vérifiant l'axiomatique III.1, sur une base orthonormale de fonctions déterministes pondérées par des variables aléatoires décorrélées. Ce type de développement est très utilisé en pratique dans des domaines aussi variés qu'importants tels que le débruitage, la détection, le traitement des données. Cette liste n'est pas exhaustive et laisse entrevoir l'universalité de la méthode tant il est possible de l'utiliser dans bien des domaines. Ce développement est également connu sous le nom d'analyse en composante principale ("Principal Componant Analysis", PCA) dans le domaine du traitement des données, et permet lorsque l'on a affaire à des volumes de données importants dépendant de nombreuses variables de déterminer quelles sont les variables les plus porteuses d'information et donc de réduire le nombre de ces dernières [Coo93]. Philippe Courmontagne, dans [CouHDR05], dresse un inventaire conséquent des différents champs d'application de cette technique ainsi que ses diverses appellations.
Dans cette partie, après avoir décrit et légitimé ce développement en constatant qu'il s'agit de celui exposé dans la section précédente, ses propriétés fondamentales seront mises à contribution en vue d'une opération de masquage d'un signal.

3.2 Principe du développement de Karunhen-Loève

Soit $\mathbf{S}(t)$ un processus aléatoire de $\Omega \times D \rightarrow \mathbb{R}$ vérifiant les conditions III.1, centré, de variance σ_S^2 supposée indépendante du temps, de second moment fini.
Il est possible de développer ce dernier sur une base orthonormale de fonctions pondérées par des variables aléatoires $\{\mathbf{s}_n\}_{n\in\mathbb{N}}$ centrées et décorrélées, c'est-à-dire vérifiant la relation III.2.
Les coefficients sont déterminés par projection de $\mathbf{S}(t)$ sur une base $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ suivant la relation III.4, la décorrélation des coefficients $\{\mathbf{s}_n\}_{n\in\mathbb{N}}$ est assurée dès lors que les fonctions vérifient l'équation III.5.

Proposition III.3. *En se plaçant dans le cas particulier où la base $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ est orthonormale, si les fonctions constitutives de cette base sont solutions de l'équation intégrale*

$$\int_D R(t_1,t_2)\Phi_n(t_1)\,dt_1 = \lambda_n \Phi_n(t_2) \quad \forall n \in \mathbb{N}, \tag{III.7}$$

avec $\lambda_n := E[\boldsymbol{s}_n^2]$, alors elles sont solution de l'équation intégrale III.5.

Preuve . *Supposons que pour tout $n \in \mathbb{N}$, $\Phi_n(t)$ vérifie III.7*

$$\int_D R(t_1,t_2)\Phi_n(t_1)\,dt_1 = \underbrace{\mathbb{E}\left[\boldsymbol{s}_n^2\right]}_{=\lambda_n}\Phi_n(t_2),$$

multiplions membre à membre par $\Phi_m(t_2)$ puis intégrons le tout sur D par rapport à la variable t_2,

$$\int_D\int_D R(t_1,t_2)\Phi_n(t_1)\Phi_m(t_2)\,dt_1dt_2 = \mathbb{E}\left[\boldsymbol{s}_n^2\right]\int_D \Phi_n(t_2)\Phi_m(t_2)\,dt_2.$$

Or, la base $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ *étant orthonormale,*

$$\int_D \Phi_n(t)\Phi_m(t)\,dt = \delta[n-m],$$

donc

$$\int_D\int_D R(t_1,t_2)\Phi_n(t_1)\Phi_m(t_2)\,dt_1dt_2 = \mathbb{E}\left[\boldsymbol{s}_n^2\right]\ \delta[n-m].$$

□

La détermination des fonctions $\Phi_n(t)$ pour tout entier n par l'équation III.7 est donc une condition suffisante de décorrélation des variables aléatoires $\mathbf{s}_n$ pour tout $n \in \mathbb{N}$.

Remarque :

– *Le développement de Karhunen-Loève est construit avec une base de fonctions* $\Phi_n(t)$ *orthogonales. Or, dans la section précédente il est dit que ces fonctions ne le sont pas forcement. Il faut donc garder à l'esprit que l'orthogonalité des fonctions de décomposition est propre à l'approche de Karhunen et Loève.*

– *En injectant III.7 dans la relation de passage III.6, il vient*

$$\Psi_n(t) \equiv \Phi_n(t) \quad \forall n \in \mathbb{N} \quad \forall t \in D.$$

Autrement dit, les bases $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ *et* $\{\Psi_n(t)\}_{n\in\mathbb{N}}$ *sont presque partout identiques dans le développement de Karhunen-Loève d'un processus aléatoire centré et stationnaire au second ordre. Le développement de Karhunen-Loève devient alors un développement sur une base de fonctions orthonormales.*

La section suivante a pour but de caractériser l'équation intégrale III.7.

3.3 Caractérisation de l'équation intégrale par un opérateur compact de Hilbert-Schmidt

L'équation III.7 est une équation intégrale de Fredholm linéaire homogène de seconde espèce, de noyau $R(t_1,t_2)$ défini sur D^2. Par construction le noyau est symétrique [4], défini non négatif. De plus, comme

$$R(t_1,t_2) \;=\; \mathbb{E}\left[\mathbf{S}(t_1)\mathbf{S}(t_2)\right],$$

définit un produit scalaire, d'après l'inégalité de Cauchy-Schwartz pour la norme de $L^2_{\mathbb{R}}(\Omega,P)$

$$\begin{aligned} |R(t_1,t_2)| &\leq \sqrt{\mathbb{E}\left[\mathbf{S}(t_1)^2\right]}\sqrt{\mathbb{E}\left[\mathbf{S}(t_2)^2\right]} \\ |R(t_1,t_2)| &\leq \sigma_S^2. \end{aligned}$$

Après mise au carré et intégration membre à membre sur le domaine D^2, il vient

$$\int\int_{D^2} |R(t_1,t_2)|^2\ dt_1dt_2 \leq \mu(D^2)\sigma_S^4, \tag{III.8}$$

où $\mu(D^2)$ est la mesure de Lebesgue du domaine élémentaire D^2. Cette majoration montre que $R(t_1,t_2) \in L^2(D^2)$ et donc qu'il s'agit d'un noyau de Hilbert-Schmidt.

[4] $R(t_1,t_2) := \mathbb{E}\left[\mathbf{S}(t_1)\mathbf{S}(t_2)\right] = \mathbb{E}\left[\mathbf{S}(t_2)\mathbf{S}(t_1)\right]$ si $\mathbf{S}(t)$ est un processus aléatoire réel, centré, de moment d'ordre 2 fini.

Soit à présent $\Phi(t_1)$ une fonction de $L^2(D)$ et A l'opérateur faisant correspondre à $\Phi(t_1)$ une fonction $\xi(t_1)$. A est défini par la relation d'équivalence :

$$\Big[A\Phi(t_1) = \xi(t_1)\Big] \Longleftrightarrow \Big[\int_D R(t_1,t_2)\Phi(t_2)\,dt_2 = \xi(t_1)\Big]$$

pour tout $(t_1, t_2) \in D^2$.
L'opérateur A appartient à la classe des opérateurs de Fredholm, et comme cela vient d'être montré, le noyau appartient à $L^2(D^2)$. A est donc un opérateur de Hilbert-Schmidt.
La motivation principale de l'introduction d'un tel opérateur est qu'alors la résolution de l'équation intégrale III.7 se ramène de façon équivalente à la détermination des éléments propres de A, c'est-à-dire :

$$\Big[\textit{Trouver}\,\Phi(t) \in L^2(D) \,/\, \int_D R(t_1,t_2)\Phi(t_2)\,dt_2 = \lambda\Phi(t_1)\Big]$$
$$\Updownarrow$$
$$\Big[\textit{Trouver les éléments propres de l'opérateur}\, A\Big]$$

Afin de caractériser les éléments propres de l'opérateur A, il est nécessaire de mettre en évidence certaines propriétés importantes de ce dernier :

Théorème III.1. *Si le noyau de l'équation intégrale de Fredholm définissant l'opérateur A appartient à $L^2(D^2)$, alors pour toute fonction $\Phi(t) \in L^2(D)$, l'opérateur A*

1. *envoie toute fonction de $L^2(D^2)$ dans $L^2(D^2)$,*
2. *a une norme vérifiant l'inégalité*

$$\|A\| \leq \sqrt{\int\int_{D^2} |R(t_1,t_2)|^2 \; dt_1 dt_2}. \tag{III.9}$$

3. *est linéaire,*
4. *est compact,*
5. *est autoadjoint,*

La preuve de ce théorème est donnée en annexe E.

Ainsi, l'opérateur A est un opérateur de Hilbert-Schmidt, compact, autoadjoint. Il est alors possible de lui appliquer le théorème de Hilbert-Schmidt [Kol94] et d'en déduire qu'il existe une base de fonctions propres $\{\Phi_n(t_1)\}_{n\in\mathbb{N}}$ de $L^2(D)$ associées à des valeurs propres non nulles $\{\lambda_n\}_{n\in\mathbb{N}}$.
De plus, les valeurs propres sont toutes réelles vu que d'une part

$$\langle A\Phi_n(t_1), \Phi_n(t_1)\rangle = \lambda_n \langle \Phi_n(t_1), \Phi_n(t_1)\rangle \tag{III.10}$$

et d'autre part, après avoir rappelé que le produit scalaire usuel de $L^2(D)$ est une forme sesquilinéaire

$$\begin{aligned}
\langle A\Phi_n(t_1), \Phi_n(t_1)\rangle &= \langle \Phi_n(t_1), A^*\Phi_n(t_1)\rangle \\
&= \langle \Phi_n(t_1), A\Phi_n(t_1)\rangle \\
&= \langle \Phi_n(t_1), \lambda_n\Phi_n(t_1)\rangle \\
&= \overline{\lambda_n}\,\langle \Phi_n(t_1), \Phi_n(t_1)\rangle\,,
\end{aligned} \tag{III.11}$$

par identification de III.10 avec III.11, il vient $\lambda_n = \overline{\lambda_n}$.
Les fonctions propres $\Phi_n(t_1)$ et $\Phi_m(t_1)$ pour $n \neq m$ correspondant respectivement à deux valeurs propres distinctes $\lambda_n \neq \lambda_m$ sont orthogonales car

$$\langle A\Phi_n(t_1), \Phi_m(t_1)\rangle = \lambda_n \langle \Phi_n(t_1), \Phi_m(t_1)\rangle$$

et

$$\langle A\Phi_n(t_1), \Phi_m(t_1)\rangle = \langle \Phi_n(t_1), A\Phi_m(t_1)\rangle = \lambda_m \langle \Phi_n(t_1), \Phi_m(t_1)\rangle ,$$

alors en retranchant les deux équations,

$$\Big[(\lambda_n - \lambda_m)\langle \Phi_n(t_1), \Phi_m(t_1)\rangle = 0\Big] \Rightarrow \Big[\langle \Phi_n(t_1), \Phi_m(t_1)\rangle = 0 \quad \forall n \neq m\Big].$$

Une conséquence importante de ce résultat est que si la famille de fonctions $\{\Phi_n(t_1)\}_{n\in\mathbb{N}}$ représente la famille de solution de l'équation intégrale III.5, alors la base engendrée par ces fonctions est orthogonale.
Par ailleurs, il existe pour n fixé un nombre fini q_n de fonctions propres $\Phi_n(t_1)$ linéairement indépendantes correspondant à une valeur propre λ_n. Ce nombre est appelé multiplicité de la valeur propre considérée, il vérifie[Kol94]

$$q_n \leq \frac{1}{\lambda_n^2}\int\int_{D^2} |R(t_1,t_2)|^2 \, dt_1 dt_2.$$

Enfin, l'important théorème de Mercer démontré dans [Bla81] (pp. 193-196) montre que le noyau d'un opérateur d'Hilbert-Schmidt peut se décomposer de la façon suivante :

$$R(t_1\,,\,t_2) = \sum_{n=1}^{\infty} \lambda_n \Phi_n(t_1)\Phi_n(t_2),$$

où la série est uniformément convergente dans D^2. En particulier,

$$R(t_1\,,\,t_1) = \mathbb{E}\left[\mathbf{S}^2(t)\right] = \sigma_S^2 = \sum_{n=1}^{\infty} \lambda_n \left(\Phi_n(t_1)\right)^2 . \tag{III.12}$$

Remarque : *Lorsque les signaux sont complexes les deux relations deviennent respectivement*

$$R(t_1,t_2) = \sum_{n=1}^{\infty} \lambda_n \Phi_n(t_1)\overline{\Phi_n(t_2)},$$

et

$$R(t_1,t_1) = \sigma_S^2 = \sum_{n=1}^{\infty} \underbrace{\lambda_n}_{=\mathbb{E}[\mathbf{s}_n^2]} |\Phi_n(t_1)|^2 .$$

Or, la fonction $R(t_1, t_2)$ est symétrique définie non négative car $\forall (a_i, a_j) \in \mathbb{C}^2$, $(i, j) \in \mathbb{N}^2$,

$$\begin{aligned}
\sum_{i=1}^{\infty}\sum_{j=1}^{\infty} a_i\overline{a_j}R(t_i,t_j) &= \sum_{i=1}^{\infty}\sum_{j=1}^{\infty} a_i\overline{a_j}\mathbb{E}\left[\mathbf{S}(t_i)\mathbf{S}(t_j)\right] \\
&= \mathbb{E}\left[\sum_{i=1}^{\infty}\sum_{j=1}^{\infty} a_i\overline{a_j}\mathbf{S}(t_i)\mathbf{S}(t_j)\right] \\
&= \mathbb{E}\left[\left(\sum_{i=1}^{\infty} a_i\mathbf{S}(t_i)\right)\left(\sum_{j=1}^{\infty}\overline{a_j}\mathbf{S}(t_j)\right)\right] \\
&= \mathbb{E}\left[\left|\sum_{i=1}^{\infty} a_i\mathbf{S}(t_i)\right|^2\right] \geq 0,
\end{aligned}$$

donc nécessairement, $\lambda_n \geq 0$ pour presque tout n.

3.4 Cas où le signal est stationnaire à l'ordre 2

Les fonctions de base admissibles, c'est-à-dire assurant la décorrélation des coefficients calculés à partir de ces dernières, sont fonctions propres orthonormales de l'équation III.7.
Sous l'hypothèse d'une observation stationnaire à l'ordre 2 l'équation se ramène à

$$\int_D r(t_1 - t_2)\Phi_n(t_2)\,dt_2 = \lambda_n\Phi_n(t_1) \quad \forall t_1 \in D. \tag{III.13}$$

Krasnov et al. [Kra77] (pp.73-74) et Papoulis [Pap02] (pp. 509-511) montrent que dans ce cas les fonctions solutions sont de Fourier.
En effet, $r(\tau)$ est une fonction de $L^2(D)$ qui est donc décomposable sur une base de cet espace, comme par exemple la base engendrée par la famille de fonctions solution de III.7 qui forme une base orthonormale de $L^2(D)$. Ainsi, la fonction d'autocorrélation de $\mathbf{S}(t)$ réel se décompose sur la base des $\{\Phi_n(\tau)\}_{n\in\mathbb{N}}$ pour tout $\tau \in D$ de la façon suivante :

$$r(\tau) = \sum_{m=1}^{\infty}\gamma_m\Phi_m(\tau)$$

avec

$$\gamma_m = \int_D r(t)\Phi_m(t)\,dt,$$

si bien qu'en injectant ce développement dans le membre de gauche de l'équation intégrale III.13, celui-ci devient

$$\begin{aligned}
\int_D r(t_1 - t_2)\Phi_n(t_2)\,dt_2 &= \int_D\left(\sum_{m=1}^{\infty}\gamma_m\Phi_m(t_1 - t_2)\right)\Phi_n(t_2)\,dt_2 \\
&= \sum_{m=1}^{\infty}\gamma_m\int_D \Phi_m(t_1 - t_2)\Phi_n(t_2)\,dt_2.
\end{aligned}$$

Alors, une condition suffisante permettant de satisfaire la relation III.13 est que pour tout $n \in \mathbb{N}$ et pour tout $t \in D$ les fonctions $\Phi_n(t)$ doivent vérifier

$$\int_D \Phi_m(t_1 - t_2)\Phi_n(t_2)\,dt_2 = \Phi_n(t_1)\delta[n - m], \tag{III.14}$$

car dans ce cas

$$\begin{aligned}\int_D r(t_1-t_2)\Phi_n(t_2)\,dt_2 &= \sum_{m=1}^{\infty}\gamma_m\left(\int_D \Phi_m(t_1-t_2)\Phi_n(t_2)\,dt_2\right)\\ &= \sum_{m=1}^{\infty}\gamma_m\big(\Phi_n(t_1)\delta[n-m]\big)\\ \int_D r(t_1-t_2)\Phi_n(t_2)\,dt_2 &= \gamma_n\Phi_n(t_1),\end{aligned}$$

et ainsi $\gamma_n = \lambda_n$. Il vient d'être montré que dans le cas où l'observation $\mathbf{S}(t)$ est réelle, centrée et stationnaire à l'ordre 2 il est possible de la décomposer sur une base de fonctions orthonormales vérifiant la relation III.14. Cette démarche permet de s'affranchir de l'étape de recherche des éléments propres de l'équation intégrale III.13 car dès que la relation III.14 est vérifiée, la relation III.13 l'est également, entraînant la décorrélation des coefficients de décomposition.
La famille de fonctions exponentielles complexes ou de façon équivalente la famille de fonctions sinusoïdales, telles que celles rencontrées dans l'écriture de la série de Fourier est un exemple simple et important de ce type de base puisque dans ce cas, pour tout $n \in \mathbb{N}$,

$$\Phi_n(t) := e^{2i\pi\frac{n}{\mu(D)}t},$$

alors, un rapide calcul montre que

$$\int_D e^{2i\pi\frac{m}{\mu(D)}(t_1-t_2)}e^{2i\pi\frac{n}{\mu(D)}t_2}\,dt_2 = e^{2i\pi\frac{n}{\mu(D)}t_1}\delta[n-m] \quad \forall(t_1,t_2)\in D^2.$$

La base $\left\{e^{2i\pi\frac{n}{T}t}\right\}_{n\in\mathbb{N}}$ est telle que toute observation réelle, centrée et stationnaire à l'ordre 2 décomposée sur cette dernière a des coefficients de décomposition décorrélés. En ce sens, Papoulis [Pap02] montre qu'il ne s'agit là que d'un cas particulier du développement de Karhunen-Loève.

3.5 Conclusion

Fort de ces considérations, il est possible d'affirmer que tout processus stochastique $\mathbf{S}(t)$ respectant III.1 est décomposable selon le développement de Karhunen-Loève.
Soit $\tilde{\mathbf{S}}_N(t)$ le processus stochastique

$$\tilde{\mathbf{S}}_N(t) = \sum_{n=1}^{N}\mathbf{s}_n\Phi_n(t) \tag{III.15}$$

où la famille $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ constitue une base orthogonale Hilbertienne de $L^2(D)$ dont chaque élément est fonction propre de l'équation intégrale III.9, et où les coefficients $\mathbf{s}_n$ sont obtenus par projection de $\tilde{\mathbf{S}}_N(t)$ sur chaque fonction propre $\Phi_n(t)$ pour tout $n = 1\ldots N$.
La proposition suivante synthétise l'ensemble des résultats venant d'être établis concernant le développement de Karhunen-Loève d'un processus aléatoire réel centré.

Proposition III.4. *Soit $\boldsymbol{S}(t)$ un processus stochastique réel et centré vérifiant III.1, développable sur une base de fonctions $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ de $L^2(D)$ de sorte que*

$$\boldsymbol{S}(t) = \sum_{n=1}^{\infty}\boldsymbol{s}_n\Phi_n(t) \quad \textit{avec} \quad \boldsymbol{s}_n = \int_D \boldsymbol{S}(t)\Phi_n(t)\,dt.$$

Si les fonctions constitutives de la base sont solutions de l'équation intégrale

$$\int_D R(t_1,t_2)\Phi_n(t_2)\,dt_2 = \lambda_n\Phi_n(t_1)\forall t_1\in D, \tag{III.16}$$

alors,

1. *Les coefficients de la décomposition sont deux à deux décorrélés,*

$$\mathbb{E}\left[\boldsymbol{s}_n \boldsymbol{s}_m\right] = \mathbb{E}\left[\boldsymbol{s}_n^2\right] \delta[n-m],$$

2. *Le processus stochastique défini par la série de fonctions $\tilde{S}_N(t)$ converge en moyenne quadratique vers $\boldsymbol{S}(t)$.*

La preuve est donnée en annexe F.

Remarque : *Les valeurs propres λ_n ainsi que les fonctions propres associées $\Phi_n(t)$ sont réelles pour tout entier n. De plus, la base engendrée par les $\{\Phi_n(t)\}_{\mathbb{N}}$, vecteurs propres d'un opérateur d'Hilbert-Schmidt est orthogonale.*

Les coefficients $\{\mathbf{s}_n\}_{n\in\mathbb{N}}$ étant deux à deux décorrélés, ils constituent une suite blanche.

4 CAS OÙ L'OBSERVATION EST UN SIGNAL UTILE PERTURBÉ PAR UN BRUIT BLANC

Le but de cette section est d'utiliser le développement de Karhunen-Loève pour montrer que les contre mesures d'attaques en puissance basées sur l'ajout de bruit blanc sont inefficaces.

Remarque : *La notion de bruit blanc est exclusivement théorique, dans la mesure où un processus aléatoire de fonction d'autocorrélation égale à une distribution de Dirac, donc de densité spectrale de puissance constante, n'a pas de sens physique. Les calculs qui vont être menés permettent cependant d'avoir une idée précise des conséquences du développement de Karhunen-Loève d'une observation dans un tel contexte. Un amalgame est fait entre la notion de bruit blanc et celle de bruit à corrélations microscopiques.*

Dans bon nombre de cas pratiques, l'observation $\mathbf{Z}(t)$ étudiée sur un intervalle de temps D est vue comme la superposition additive d'un signal utile $\mathbf{S}(t)$ et d'un bruit blanc $\mathbf{B}(t)$ tous deux aléatoires, centrés, de moment d'ordre 2 finis,

$$\mathbf{Z}(t) \quad = \quad \mathbf{S}(t) + \mathbf{B}(t),$$

les signaux $\mathbf{S}(t)$ et $\mathbf{B}(t)$ sont supposés indépendants, $\mathbf{B}(t)$ peut être considéré comme modélisant le bruit de mesure faisant que $\mathbf{Z}(t)$ est observé au lieu de $\mathbf{S}(t)$.
Si σ_S^2 et σ_B^2 sont les variances respectives du signal et du bruit, et si $\mathbf{S}_0(t)$ et $\mathbf{B}_0(t)$ sont les signaux réduits associés, alors III.17 s'écrit sous forme réduite,

$$\mathbf{Z}(t) \quad = \quad \sigma_S \mathbf{S}_0(t) + \sigma_B \mathbf{B}_0(t). \tag{III.17}$$

La covariance $R_{\mathrm{ZZ}}(t_1, t_2)$ de $\mathbf{Z}(t)$ s'écrit

$$\begin{aligned} R_{\mathrm{ZZ}}(t_1,t_2) &= \mathbb{E}\left[\mathbf{Z}(t_1)\mathbf{Z}(t_2)\right] \\ &= \mathbb{E}\left[\left(\sigma_S \mathbf{S}_0(t_1) + \sigma_B \mathbf{B}_0(t_1)\right)\left(\sigma_S \mathbf{S}_0(t_2) + \sigma_B \mathbf{B}_0(t_2)\right)\right] \\ &= \sigma_S^2 \mathbb{E}\left[(\mathbf{S}(t_1)\mathbf{S}(t_2))\right] + \sigma_S\sigma_B\left(\mathbb{E}\left[\left(\mathbf{S}(t_1)\mathbf{B}(t_2)\right)\right] + \mathbb{E}\left[(\mathbf{B}(t_1)\mathbf{S}(t_2))\right]\right) + \sigma_S^2 \mathbb{E}\left[(\mathbf{B}(t_1)\mathbf{B}(t_2))\right]. \end{aligned}$$

D'une part l'indépendance mutuelle de $\mathbf{S}(t)$ avec $\mathbf{B}(t)$ et le fait qu'au moins un des deux signaux soit centré fait que pour tout $(t_1, t_2) \in D^2$, au sens de la moyenne quadratique,

$$\mathbb{E}\left[\mathbf{S}(t_1)\mathbf{B}(t_2)\right] \quad = \quad \mathbb{E}\left[\mathbf{B}(t_1)\mathbf{S}(t_2)\right] = 0,$$

d'autre part $\mathbf{B}_0(t)$ est un bruit blanc de puissance unitaire donc par définition sa covariance réduite est

$$R_{\mathrm{B_0B_0}}(t_1,t_2) \quad = \quad \delta(t_2-t_1).$$

De ces deux remarques vient l'expression de la covariance $R_{\mathrm{ZZ}}(t_1,t_2)$ en fonction des covariances réduites du signal et du bruit,

$$\begin{aligned} R_{\mathrm{ZZ}}(t_1,t_2) &= \mathbb{E}\left[(\mathbf{S}(t_1)\mathbf{S}(t_2))\right] + \mathbb{E}\left[(\mathbf{B}(t_1)\mathbf{B}(t_2))\right] \\ &= R_{\mathrm{SS}}(t_1,t_2) + R_{\mathrm{BB}}(t_1,t_2) \\ &= \sigma_S^2 R_{\mathrm{S_0S_0}}(t_1,t_2) + \sigma_B^2\delta(t_2-t_1), \end{aligned} \tag{III.18}$$

où $R_{\mathrm{S_0S_0}}(t_1,t_2)$ est la covariance de $\mathbf{S}_0$.
Ainsi, $R_{\mathrm{ZZ}}(t_1,t_2)$ est la somme de la fonction de covariance du signal avec celle du bruit.
L'observation à valeurs sur un intervalle D est décomposée sur une base de Karhunen-Loève, c'est-à-dire que

$$\mathbf{Z}(t) = \sum_{n=1}^{\infty} \mathbf{z}_n \Phi_n(t) \tag{III.19}$$

avec les fonctions de base $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ déterminées par l'équation intégrale

$$\int_D R_{\mathrm{ZZ}}(t_1,t_2)\Phi_n(t_2)\,dt_2 = \lambda_n \Phi_n(t_1), \tag{III.20}$$

de sorte que les variables aléatoires $\{\mathbf{z}_n\}_{n\in\mathbb{N}}$ obtenues par

$$\mathbf{z}_n = \int_D \mathbf{Z}(t)\Phi_n(t)\,dt \tag{III.21}$$

soient décorrélées.
La proposition suivante montre que dans ce cas les fonctions propres de l'observation sont les mêmes que celle du signal utile, seules les valeurs propres sont modifiées par la présence du bruit.

Proposition III.5. *Soit pour tout $t \in D$ l'observation $\mathbf{Z}(t)$ définie par III.17 décomposée suivant la relation III.19. Alors, les fonctions $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ solutions de l'équation intégrale III.20 de noyau la fonction de covariance de l'observation $R_{\mathrm{ZZ}}(t_1,t_2)$ sont également solutions de*

$$\int_D R_{\mathrm{S_0S_0}}(t_1,t_2)\Phi_n(t_2)\,dt_2 = \lambda_n^S \Phi_n(t_1), \tag{III.22}$$

avec

$$\lambda_n^S := \frac{\lambda_n - \sigma_B^2}{\sigma_S^2},$$

pour tout entier n. Autrement dit, si les éléments propres de l'équation intégrale de l'observation sont les fonctions $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ et les valeurs propres λ_n, alors les éléments propres de l'équation intégrale du signal utile sont les mêmes fonctions $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ avec les valeurs propres λ_n^S.

Démonstration . *Les fonctions $\{\Phi_n(t)\}_{n\in\mathbb{N}}$ sont déterminées comme étant solutions de*

$$\int_D R_{\mathrm{ZZ}}(t_1,t_2)\Phi_n(t_2)\,dt_2 = \lambda_n \Phi_n(t_1),$$

donc d'après l'égalité III.18 cette relation prend pour expression,

$$\begin{aligned}
\int_D \left(\sigma_S^2 R_{\mathrm{S_0S_0}}(t_1,t_2) + \sigma_B^2\delta(t_2-t_1)\right)\Phi_n(t_2)\,dt_2 &= \lambda_n\Phi_n(t_1) \Leftrightarrow \\
\sigma_S^2\int_D R_{\mathrm{S_0S_0}}(t_1,t_2)\Phi_n(t_2)\,dt_2 &= \lambda_n\Phi_n(t_1) - \int_D \sigma_B^2\delta(t_1-t_2)\Phi_n(t_2)\,dt_2 \Leftrightarrow \\
\sigma_S^2\int_D R_{\mathrm{S_0S_0}}(t_1,t_2)\Phi_n(t_2)\,dt_2 &= \lambda_n\Phi_n(t_1) - \sigma_B^2\Phi_n(t_1) \Leftrightarrow \\
\int_D R_{\mathrm{S_0S_0}}(t_1,t_2)\Phi_n(t_2)\,dt_2 &= \underbrace{\frac{\lambda_n-\sigma_B^2}{\sigma_S^2}}_{=\lambda_n^S}\Phi_n(t_1)
\end{aligned}$$

□

Ainsi, les fonctions propres associées à l'observation, c'est-à-dire déterminées à partir de l'équation intégrale de noyau $R_{\mathrm{ZZ}}(t_1,t_2)$ sont les mêmes que celles associées au signal utile réduit, déterminées par l'équation intégrale de noyau $R_{\mathrm{S_0S_0}}(t_1,t_2)$.
L'influence du bruit apparaît dans l'expression des valeurs propres, celles du signal utile se déduisant facilement de celles de l'observation par retranchement de la puissance du bruit et normalisation.
Il est alors possible, dans ces conditions, de construire une approximation du signal utile $\mathbf{S}(t)$ par le biais d'une approximation $\tilde{\mathbf{Z}}_Q(t)$. Soit $\tilde{\mathbf{Z}}_Q(t)$ l'approximation de $\mathbf{S}(t)$ pour tout $t \in D$ définie par

$$\tilde{\mathbf{Z}}_Q(t) := \sum_{n=1}^{Q} \mathbf{z_n}\Phi_n(t),$$

où $Q \in \mathbb{N}^*$ est l'ordre de troncature à déterminer.

Proposition III.6. *Dans le cas où la base composée des fonctions $\{\Phi_n(t)\}_{n\in\mathbb{N}^*}$ est orthonormée[5], l'erreur d'approximation ϵ entre le signal utile $\mathbf{S}(t)$ et son approximation $\tilde{\mathbf{Z}}_Q(t)$ est*

$$\begin{aligned}
\epsilon &:= 2Q\sigma_B^2 + \sigma_S^2 - \sum_{n=1}^{Q}\lambda_n \\
&= \sigma_S^2\left(1 - \sum_{n=1}^{Q}\lambda_n^S\right) + Q\sigma_B^2.
\end{aligned}$$

Cette erreur ne dépend que de l'ordre de troncature Q.

[5] $\|\Phi_n(t)\|^2 = 1\,\forall n \in \mathbb{N}^*$

Preuve . *La démonstration reprend l'ensemble des résultats établis précédemment, les signaux* $\mathbf{S}_0(t)$ *et* $\mathbf{B}_0(t)$ *sont les pendants réduits*[6] *respectifs des signaux* $\mathbf{S}(t)$ *et* $\mathbf{B}(t)$ *tels que* $\mathbf{S}(t) = \sigma_S \mathbf{S_0}(t)$ *et* $\mathbf{B}(t) = \sigma_B \mathbf{B_0}(t)$. *Alors, la variable aléatoire* $\mathbf{s}_n$ *est définie par*

$$\mathbf{s}_n \;:=\; \int_D \mathbf{S}_0(t)\Phi_n(t)\,dt = \langle \mathbf{S}_0\,;\,\Phi_n\rangle\,,$$

et donc

$$\begin{aligned}\mathbf{z}_n &= \langle \mathbf{Z}\,;\,\Phi_n\rangle\\ &= \langle \sigma_{\mathbf{S}}\mathbf{S_0} + \sigma_{\mathbf{B}}\mathbf{B_0}\,;\,\Phi_n\rangle\\ &= \sigma_S \mathbf{s}_n + \sigma_B\,\langle \mathbf{B_0}\,;\,\Phi_n\rangle\,,\end{aligned}$$

impliquant, par indépendance mutuelle du signal avec le bruit[7]*, et en rappelant que* $\mathbb{E}\left[\mathbf{s}_n^2\right] = \lambda_n^S$ *et* $\mathbb{E}\left[\mathbf{z}_n^2\right] = \lambda_n$,

$$\begin{aligned}\mathbb{E}\left[\mathbf{z}_n^2\right] &= \mathbb{E}\left[\left(\sigma_S\mathbf{s}_n + \sigma_B\,\langle \mathbf{B_0}\,;\,\Phi_n\rangle\,\right)^2\right]\\ &= \sigma_S^2\mathbb{E}\left[\mathbf{s}_n^2\right] + \sigma_B^2\mathbb{E}\left[\left|\,\langle \mathbf{B_0}\,;\,\Phi_n\rangle\,\right|^2\right]\\ &= \sigma_S^2\lambda_n^S + \int\!\!\int_{D^2} \underbrace{R_{\mathbf{B}_0\mathbf{B}_0}(t_1\,;\,t_2)}_{=\delta(t_1-t_2)}\Phi_n(t_1)\Phi_n(t_2)\,dt_1dt_2\\ &= \sigma_S^2\lambda_n^S + \sigma_B^2\left\|\Phi_n(t)\right\|^2\\ &= \sigma_S^2\lambda_n^S + \sigma_B^2.\end{aligned}$$

et que

$$\begin{aligned}\mathbb{E}\left[\mathbf{z}_n\mathbf{s}_m\right] &= \mathbb{E}\left[\left(\sigma_S\mathbf{s}_n + \sigma_B\,\langle \mathbf{B_0}\,;\,\Phi_n\rangle\,\right)\mathbf{s}_m\right]\\ &= \sigma_S\mathbb{E}\left[\mathbf{s}_n\mathbf{s}_m\right]\\ &= \sigma_S\mathbb{E}\left[\mathbf{s}_n^2\right]\delta[n-m]\\ &= \sigma_S\lambda_n^S\delta[n-m].\end{aligned}$$

[6] $\mathbb{E}\left[\mathbf{S}_0^2(t)\right] = 1$ et $\mathbb{E}\left[\mathbf{B}_0^2(t)\right] = 1$

[7] Tous les termes croisés sont nuls.

L'expression de l'erreur est alors la suivante,

$$
\begin{aligned}
\epsilon &:= \mathbb{E}\left[\left\| \mathbf{S}(t) - \tilde{\mathbf{Z}}(t) \right\|^2 \right] \\
&= \mathbb{E}\left[\|\mathbf{S}(t)\|^2 \right] - 2\mathbb{E}\left[\left\langle \mathbf{S}(t)\,;\, \sum_{n=1}^{Q} \mathbf{z}_n \Phi_n(t) \right\rangle \right] + \mathbb{E}\left[\left\| \sum_{n=1}^{Q} \mathbf{z}_n \Phi_n(t) \right\|^2 \right] \\
&= \sigma_S^2 - 2\sum_{n=1}^{Q} \mathbb{E}\left[\langle \mathbf{S}(t)\,;\, \mathbf{z}_n \Phi_n(t) \rangle \right] + \mathbb{E}\left[\left\| \sum_{n=1}^{Q} \mathbf{z}_n \Phi_n(t) \right\|^2 \right] \\
&= \sigma_S^2 - 2\sigma_S \sum_{n=1}^{Q} \mathbb{E}\left[\mathbf{z}_n \mathbf{s}_n \right] + \mathbb{E}\left[\left\| \sum_{n=1}^{Q} \mathbf{z}_n \Phi_n(t) \right\|^2 \right] \\
&= \sigma_S^2 - 2\sigma_S^2 \sum_{n=1}^{Q} \mathbb{E}\left[\mathbf{s}_n^2 \right] + \mathbb{E}\left[\left\| \sum_{n=1}^{Q} \mathbf{z}_n \Phi_n(t) \right\|^2 \right] \\
&= \sigma_S^2 - 2\sigma_S^2 \sum_{n=1}^{Q} \mathbb{E}\left[\mathbf{s}_n^2 \right] + \mathbb{E}\left[\int_D \left(\sum_{n=1}^{Q} \sum_{m=1}^{Q} \mathbf{z}_n \Phi_n(t) \mathbf{z}_m \Phi_m(t) \right) dt \right] \\
&= \sigma_S^2 - 2\sigma_S^2 \sum_{n=1}^{Q} \mathbb{E}\left[\mathbf{s}_n^2 \right] + \sum_{n=1}^{Q} \sum_{m=1}^{Q} \mathbb{E}\left[\mathbf{z}_n \mathbf{z}_m \right] \int_D \Phi_n(t) \Phi_m(t)\, dt \\
&= \sigma_S^2 - 2\sigma_S^2 \sum_{n=1}^{Q} \mathbb{E}\left[\mathbf{s}_n^2 \right] + \sum_{n=1}^{Q} \mathbb{E}\left[\mathbf{z}_n^2 \right] \|\Phi_n(t)\|^2\, dt. \\
&= \sigma_S^2 - 2\sigma_S^2 \sum_{n=1}^{Q} \lambda_n^S + \sum_{n=1}^{Q} \mathbb{E}\left[\mathbf{z}_n^2 \right] \\
&= \sigma_S^2 - 2\sigma_S^2 \sum_{n=1}^{Q} \left(\frac{\lambda_n - \sigma_B^2}{\sigma_S^2} \right) + \sum_{n=1}^{Q} (\sigma_S^2 \lambda_n^S + \sigma_B^2) \\
&= \sigma_S^2 - 2\sum_{n=1}^{Q} \lambda_n + 2Q\sigma_B^2 + \sigma_S^2 \sum_{n=1}^{Q} \lambda_n^S + Q\sigma_B^2 \\
&= \sigma_S^2 - 2\sum_{n=1}^{Q} \lambda_n + 3Q\sigma_B^2 + \sigma_S^2 \sum_{n=1}^{Q} \left(\frac{\lambda_n - \sigma_B^2}{\sigma_S^2} \right) \\
&= \sigma_S^2 - 2\sum_{n=1}^{Q} \lambda_n + 3Q\sigma_B^2 + \sum_{n=1}^{Q} \lambda_n - Q\sigma_B^2 \\
&= \sigma_S^2 - \sum_{n=1}^{Q} \lambda_n + 2Q\sigma_B^2 \\
&= \sigma_S^2 - \sum_{n=1}^{Q} \left(\sigma_S^2 \lambda_n^S + \sigma_B^2 \right) + 2Q\sigma_B^2.
\end{aligned}
$$

L'expression de ϵ ne dépend que de Q et 'écrit

$$
\epsilon(Q) = \sigma_S^2 \left(1 - \sum_{n=1}^{Q} \lambda_n^S \right) + Q\sigma_B^2.
$$

□

A l'aide de ce résultat, il est possible de déterminer l'ordre de troncature Q tel que l'erreur d'approximation $\epsilon(Q)$ soit minimale, c'est-à-dire fixer Q tel que

$$\begin{array}{rcl} \epsilon(Q) & < & \epsilon(Q-1) \\ \epsilon(Q) & < & \epsilon(Q+1). \end{array}$$

D'une part

$$\begin{array}{rcl} \epsilon(Q) < \epsilon(Q-1) & \Rightarrow & \sigma_S^2 \left(1 - \sum_{n=1}^{Q} \lambda_n^S\right) + Q\sigma_B^2 < \sigma_S^2 \left(1 - \sum_{n=1}^{Q-1} \lambda_n^S\right) + (Q-1)\sigma_B^2 \\ & \Leftrightarrow & \lambda_Q^S > \dfrac{\sigma_B^2}{\sigma_S^2}, \end{array}$$

et d'autre part

$$\begin{array}{rcl} \epsilon(Q) < \epsilon(Q+1) & \Rightarrow & \sigma_S^2 \left(1 - \sum_{n=1}^{Q} \lambda_n^S\right) + Q\sigma_B^2 < \sigma_S^2 \left(1 - \sum_{n=1}^{Q+1} \lambda_n^S\right) + (Q+1)\sigma_B^2 \\ & \Leftrightarrow & \lambda_{Q+1}^S < \dfrac{\sigma_B^2}{\sigma_S^2}. \end{array}$$

Ainsi si ,

$$\left\{ \begin{array}{c} \lambda_Q^S > \dfrac{\sigma_B^2}{\sigma_S^2} \\ \lambda_{Q+1}^S < \dfrac{\sigma_B^2}{\sigma_S^2}, \end{array} \right.$$

Donc, si Q est fixé comme le plus grand entier vérifiant III.23, alors l'erreur d'approximation est minimale. $\rho := \sigma_S^2/\sigma_B^2$ est le rapport signal à bruit avant traitement de l'observation. Il est clair que si le rapport signal à bruit est favorable, ρ est grand, si bien qu'un grand nombre de valeurs propres sont retenues pour construire l'approximation ; de même que si le rapport signal à bruit est défavorable, ρ est petit, si bien qu'un faible nombre de valeurs propres sont retenues pour construire l'approximation. Ce comportement adaptatif est identique dans le cas du filtrage adapté stochastique. Par troncature appropriée de la série, il est possible de reconstruire le signal d'intérêt $\mathbf{S}(t)$ et par conséquent d'éliminer le bruit. Cette méthode de troncature de la base est également utilisée dans la théorie du filtrage adapté stochastique[8] et permet de répondre, par exemple, à des problèmes de restauration d'images SONAR [Cha05b1]. L'élimination naturelle du bruit blanc dans une observation peut s'avérer utile par exemple pour détecter des textures dans une image. Mais placé dans le contexte de la sécurisation des Smart Cards, la démarche présentée dans cette section met clairement en exergue l'insuffisance des techniques de sécurisation des circuits électroniques consistant à ajouter au signal de consommation un bruit blanc, comme le propose par exemple Kussener dans sa thèse [Kus02]. En effet, le développement d'une observation qui est la somme d'une activité de consommation et d'un bruit blanc sur une base de Karhunen-Loève suivi de la construction d'une approximation comme suggérée précédemment va éliminer naturellement le bruit.

[8] Dans ce cas le bruit n'est plus nécessairement blanc

5 UTILISATION DU DÉVELOPPEMENT POUR MASQUER UN SIGNAL

La proposition III.4 montre comment une observation modélisée par un processus stochastique vérifiant III.1 centré, de second moment fini peut être décomposée sur la base de Karhunen-Loève.

Dans ce contexte, soit le processus aléatoire $\mathbf{Y}(t)$ défini au sens des distributions sur l'intervalle D par :

$$\mathbf{Y}(t) := \sum_{n=1}^{\infty} \mathbf{z}_n \delta(t - nT_e), \tag{III.23}$$

où T_e est une constante positive où les $\{\mathbf{z}_n\}_{n\in\mathbb{N}}$ sont les coefficients de la décomposition de l'observation $\mathbf{Z}(t)$ définis en III.21.

$\mathbf{Y}(t)$ est centré car

$$\begin{aligned}
\mathbb{E}\left[\mathbf{Y}(t)\right] &= \mathbb{E}\left[\sum_{n=1}^{\infty} \mathbf{z}_n \delta(t - nT_e)\right] \\
&= \sum_{n=1}^{\infty} \mathbb{E}\left[\mathbf{z}_n\right] \delta(t - nT_e) \\
&= 0.
\end{aligned}$$

Compte tenu de la décorrélation de la suite de variables aléatoires $\{\mathbf{z}_n\}_{n\in\mathbb{N}}$, la fonction de covariance $R_{YY}(t_1, t_2)$ de $\mathbf{Y}(t)$ a pour expression :

$$\begin{aligned}
R_{YY}(t_1, t_2) &:= \mathbb{E}\left[\mathbf{Y}(t_1)\mathbf{Y}(t_2)\right] \\
&= \mathbb{E}\left[\left(\sum_{n=1}^{\infty} \mathbf{z}_n \delta(t_1 - nT_e)\right)\left(\sum_{m=1}^{\infty} \mathbf{z}_m \delta(t_2 - mT_e)\right)\right] \\
&= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \mathbb{E}\left[\mathbf{z}_n \mathbf{z}_m\right] \delta(t_1 - nT_e)\delta(t_2 - mT_e) \\
&= \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \mathbb{E}\left[\mathbf{z}_n^2\right] \delta[n - m]\delta(t_1 - nT_e)\delta(t_2 - mT_e) \\
&= \sum_{n=1}^{\infty} \mathbb{E}\left[\mathbf{z}_n^2\right] \delta(t_1 - nT_e)\delta(t_2 - nT_e)
\end{aligned}$$

et finalement,

$$R_{YY}(t_1, t_2) = \left(\sum_{n=1}^{\infty} \mathbb{E}\left[\mathbf{z}_n^2\right] \delta(t_1 - nT_e)\right) \delta(t_1 - t_2). \tag{III.24}$$

La variance de $\mathbf{Y}(t)$ vaut alors :

$$\begin{aligned}
\sigma_Y^2(t_1) &:= R_{YY}(t_1, t_1) \\
&= \sum_{n=1}^{\infty} \mathbb{E}\left[\mathbf{z}_n^2\right] \delta(t_1 - nT_e) \\
&= \sum_{n=1}^{\infty} \lambda_n \delta(t_1 - nT_e) \qquad \text{(III.25)} \\
& \qquad \text{(III.26)}
\end{aligned}$$

L'expression III.24 montre que le processus $\mathbf{Y}(t)$ n'est pas formellement stationnaire à l'ordre 2, cependant, la puissance de $\mathbf{Y}(t)$ est identique à celle de $\mathbf{Z}(t)$ au sens des distributions, car d'après III.25 chaque raie véhicule une partie de la puissance de $\mathbf{Z}(t)$. L'observation de masquage préserve donc la puissance du signal.
De plus, puisque la covariance $R_{YY}(t_1, t_2)$ peut s'écrire

$$R_{YY}(t_1, t_2) \quad = \quad \sigma_Y^2(t_1)\delta(t_1 - t_2),$$

pour tout $(t_1, t_2) \in D^2$ tel que $t_1 \neq t_2$, $R_{YY}(t_1, t_2) = 0$ le processus $\mathbf{Y}(t)$ est décorrélé à l'ordre 2.
Une telle approche a pour avantage dans un contexte de masquage de substituer une observation *a priori* riche en information par un signal décorrélé à l'ordre 2 qui de plus possède une variance dépendant du temps donc plus difficile à estimer. Cependant, le signal masqué existe au sens des distributions et de ce fait n'est pas physiquement réalisable. Deux solutions sont envisageables :

- Proposer un moyen d'approcher au mieux une distribution de Dirac par une suite de fonctions.
- Échantillonner l'observation sur une durée finie.

Le premier permet de traiter le problème pour des signaux continus mais demeure assez exotique alors que le second oblige à basculer dans le domaine des signaux discrets, mais demeure réaliste et servira de base de travail pour la phase expérimentale. Toujours est il que ces deux aspects font respectivement l'objet des deux prochaines sections.

5.1 Approximation de la distribution de Dirac

Le signal $\mathbf{Y}(t)$ masquant le signal informationnel $\mathbf{Z}(t)$ existe au sens des distributions, ce qui l'empêche d'être physiquement réalisable, en particulier à cause de la présence de distributions de Dirac. Un palliatif possible est d'approcher la distribution de Dirac par une suite de fonctions convergeant vers cette distribution. La proposition suivante fournit un moyen simple de construire de telles suites.

Proposition III.7. *Soit $g(t)$ une fonction positive sommable sur $\mathbb{R}$ telle que*

$$\int_{\mathbb{R}} |g(t)| \, dt = 1,$$

et soit U un scalaire appartenant à un ensemble ordonné tel que $\mathbb{N}$ ou $\mathbb{R}$. Alors, la suite de fonction $g_{\mathrm{U}}(t)$ définie par

$$g_{\mathrm{U}}(t) := Ug(Ut)$$

converge au sens des distributions vers la distribution de Dirac,

$$\lim_{U \to \infty} g_{\mathrm{U}}(t) = \delta(t)$$

La preuve de ce théorème est donnée, entre autre, dans [Rei91]. Il existe beaucoup de fonctions vérifiant les conditions exigées par la proposition III.7. C'est en particulier le cas de toute fonction faisant office de densité de probabilité, des gaussiennes, des portes. Il est possible de trouver des exemples dans [Rei91] ou bien [Rod91].
En pratique, soit $\epsilon > 0$, alors il existe deux entiers $a(\epsilon)$ et $b(\epsilon)$ tel que

$$\left| \int_{a(\epsilon)}^{b(\epsilon)} g(t) \, dt - 1 \right| \leq \epsilon.$$

Si ϵ est suffisamment petit, la valeur de l'intégrale est proche de 1 et par conséquent l'intervalle $[a(\epsilon); b(\epsilon)]$ est à ϵ près représentatif du support de $g(t)$. Par construction, $g_{\mathrm{U}}(t)$ est telle que

$$[a(\epsilon); b(\epsilon)] \subseteq \underset{t\in\mathbb{R}}{Supp}\,[g(t)] \quad \Rightarrow \quad [\frac{a(\epsilon)}{U}; \frac{b(\epsilon)}{U}] \subseteq \underset{t\in\mathbb{R}}{Supp}\,[g_{\mathrm{U}}(t)]\,.$$

Cette implication montre que le support de $g_{\mathrm{U}}(t)$ se déduit de celui de $g(t)$ par une réduction homothétique de facteur U[9]. Soit t_1 et t_2 deux réels tels que $t_2 > t_1$, d'une part

$$[t_1 + \frac{a(\epsilon)}{U}; t_1 + \frac{b(\epsilon)}{U}] \subseteq \underset{t\in\mathbb{R}}{Supp}\,[g_{\mathrm{U}}(t - t_1)]\,,$$

de même que

$$[t_2 + \frac{a(\epsilon)}{U}; t_2 + \frac{b(\epsilon)}{U}] \subseteq \underset{t\in\mathbb{R}}{Supp}\,[g_{\mathrm{U}}(t - t_2)]\,.$$

Ces deux intervalles caractérisent respectivement les supports de $g_{\mathrm{U}}(t - t_1)$ et $g_{\mathrm{U}}(t - t_2)$ à ϵ près. Ainsi, une condition nécessaire et suffisante pour assurer la disjonction à ϵ près de ces deux supports est,

$$t_1 + \frac{b(\epsilon)}{U} \leq t_2 + \frac{a(\epsilon)}{U} \Leftrightarrow U \geq \frac{b(\epsilon) - a(\epsilon)}{t_2 - t_1}.$$

Cette relation est telle que pour avoir U petit il faut que l'intervalle $[a(\epsilon); b(\epsilon)]$ de départ soit petit et que la distance entre t_1 et t_2 soit suffisamment grande. La borne inférieure de l'ensemble des U est alors définie à ϵ près.
En guise d'illustration, le cas de la suite de fonctions engendrée par une fonction gaussienne permet de mettre en évidence les propriétés énoncées. Soit la suite de fonctions $g_{\mathrm{U}}(t) := Ug(Ut)$ définie à partir d'une fonction $g(t)$ gaussienne,

$$g := \left\{ \begin{array}{ccc} \mathbb{R} & \rightarrow & \mathbb{R}^+ \\ t & \mapsto & \frac{1}{\sqrt{2\pi}} e^{\frac{-t^2}{2}} \end{array} \right. \tag{III.27}$$

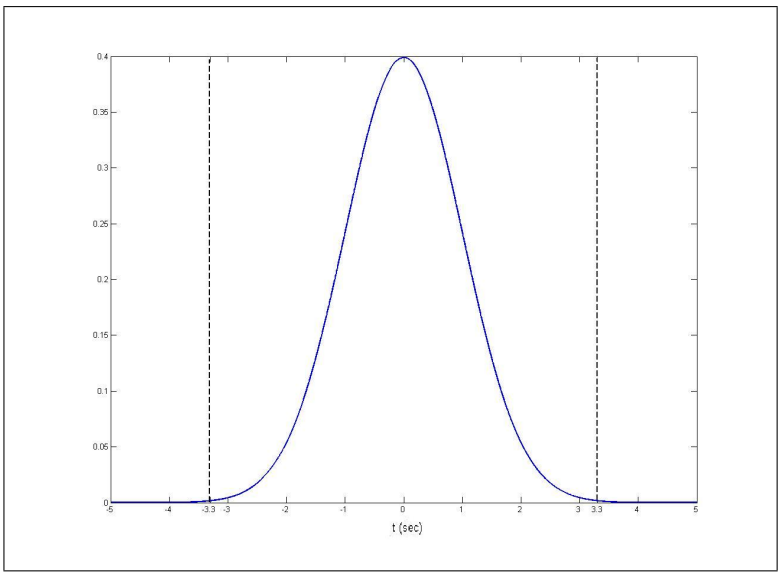


FIG. 1 – *Représentation graphique de $g(t)$ en trait plein. L'aire délimitée par : les traits en pointillées, l'axe des abscisses et le graphe de la fonction, vaut environ 0,9995*

[9]plus U augmente, plus le support de $g_{\mathrm{U}}(t)$ est petit, pour tendre lorsque U tend vers l'infini vers un singleton qui est le support de la distribution de Dirac.

Cette fonction appartient à la famille gaussienne, c'est entre autre une densité de probabilité, qui vérifie par définition l'hypothèse de la proposition III.7. Par application directe de cette proposition,

$$\lim_{U\to\infty} g_{\mathrm{U}}(t) = \lim_{U\to\infty} \frac{U}{\sqrt{2\pi}} e^{\frac{-U^2t^2}{2}} = \delta(t)$$

au sens des distributions.

En se donnant $\epsilon = 10^{-3}$, la lecture d'une table de loi normale montre que

$$\int_{-3,3}^{3,3} \frac{1}{\sqrt{2\pi}} e^{\frac{-t^2}{2}}\, dt \quad \approx \quad 0,9995,$$

le choix des bornes de l'intervalle de référence est alors,

$$\left\{ \begin{array}{rcl} a(10^{-3}) & = & -3,3 \\ b(10^{-3}) & = & 3,3 \end{array} \right. ,$$

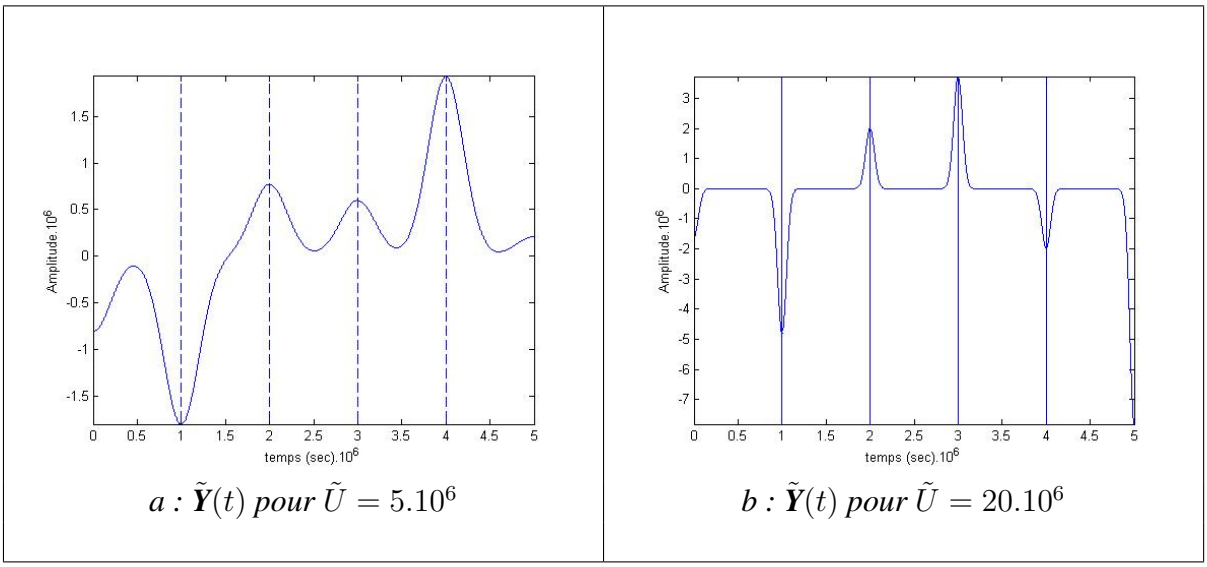
comme l'atteste la figure 1.
Le signal défini par la relation III.23 est une série de distributions de Dirac pondérées. Chacune de ces distributions sont espacées d'une période T_e. Alors, afin de pouvoir approcher chaque terme de cette série à l'aide de la suite de fonction $g_{\mathrm{U}}(t)$ définie par III.27 sans risque de recouvrement nuisible une condition nécessaire est

$$U \geq \frac{6,6}{T_e}.$$

L'idée est alors de définir un nouveau processus $\tilde{\mathbf{Y}}(t)$ par la relation

$$\tilde{\mathbf{Y}}(t) \quad := \quad \sum_{n=1}^{\infty} \mathbf{z}_n g_{\tilde{U}}(t - nT_e),$$

qui bien que différent de $\mathbf{Y}(t)$ car défini au sens des fonctions, est porteur de la même information, à savoir les coefficients $\{\mathbf{z}_n\}_{n\in\mathbb{N}}$.
Par exemple, si T_e est fixé à $10^{-6}sec$, alors $\tilde{U}$ est tel que $\tilde{U} > 6,6 \times 10^6$ pour une erreur de seulement 10^{-3}. De plus, l'amplitude maximale de $g_{\tilde{U}}(t)$ est supérieure à $\frac{\tilde{U}}{\sqrt{2\pi}}$ soit dans ce cas une amplitude d'environ $2,63 \times 10^6$, cette valeur est nécessairement importante vu la très petite taille du support correspondant.



a : $\tilde{\mathbf{Y}}(t)$ *pour* $\tilde{U} = 5.10^6$ *b :* $\tilde{\mathbf{Y}}(t)$ *pour* $\tilde{U} = 20.10^6$

FIG. 2 – *Zoom facteur* 10^6 *d'une réalisation de* $\tilde{\mathbf{Y}}(t)$ *sur* 5×10^{-6} *secondes*

Les figures 2 montrent une réalisation de $\tilde{\mathbf{Y}}(t)$. Dans le cas où $\tilde{U}$ est inférieur au seuil il y a enchevêtrement entre deux fonctions voisines. Dans le cas contraire, il apparaît qu'il n'y a pas de problème de recouvrement d'informations, mais en contrepartie que l'amplitude du signal atteint de très importantes valeurs. D'autre part,

$$\mathbb{E}\left[\tilde{\mathbf{Y}}(t)\right] = 0,$$

mais

$$\sigma^2_{\tilde{Y}}(t) = \sum_{n=1}^{\infty} \lambda_n g^2_{\tilde{U}}(t_1 - nT_e) \neq \sigma^2_Z.$$

Il n'y a donc pas conservation de la puissance dans ce cas, celle-ci n'est seulement effective qu'après passage à la limite ce qui va à l'encontre de la démarche consistant à fixer U. Le signal masqué $\tilde{\mathbf{Y}}(t)$ n'est donc pas physiquement réalisable dans ces conditions et ne peut pas être implémenté électroniquement.
La technique de masquage par décomposition des signaux est pour l'instant impossible à réaliser par ce biais, la suite de ce chapitre est dédiée à la mise en place de son pendant discret, puis de ses applications.

5.2 Masquage des signaux échantillonnés

L'objectif de cette section est d'appliquer le développement de Karhunen-Loève a la version échantillonnée de l'observation, profitant ainsi des résultats établis précédemment.
Soit $\mathbf{Z}(t)$ un processus stochastique vérifiant III.1, centré. Le processus est régulièrement échantillonné à la période T_e sur l'intervalle D, ce qui amène à définir au sens des distributions le signal $\mathbf{Z}^e(t)$ comme l'échantillonné de $\mathbf{Z}(t)$ sur D,

$$\mathbf{Z}^e(t) \quad := \quad \mathbf{Z}(t)\text{Ш}_{T_e}(t) \quad \forall t \in D.$$

Soit N l'entier correspondant au nombre d'échantillons prélevés sur cet intervalle de sorte que $T_e = \dfrac{\mu(D)}{N-1}$. dans ce cas, $\mathbf{Z}^e(t)$ a pour expression

$$\mathbf{Z}^e(t) \quad := \quad (\mathbf{Z}(t)\text{Ш}_{T_e}(t))\, 1_D(t) = \sum_{i=0}^{N-1} \mathbf{Z}(iT_e)\delta(t - iT_e) \quad \forall t \in D. \qquad \text{(III.28)}$$

où $1_D(t)$ est l'indicatrice de l'ensemble D.
Soit $\mathbf{Z}$ un vecteur aléatoire de dimension N, contenant les N échantillons $\{\mathbf{Z}(iT_e)\}_{i=0\dots N-1}$. La matrice de variance-covariance de $\mathbf{Z}$ est $\Gamma_{\mathbf{ZZ}} := \mathbb{E}\left[\mathbf{Z}\mathbf{Z}^T\right]$.
Une réalisation de $\mathbf{Z}$ est un vecteur de $\mathbb{R}^N$ dans un espace Euclidien muni du produit scalaire usuel. Ainsi, considérer l'ensemble $\{\mathbf{Z}(iT_e)\}_{i=0\dots N-1}$ ou le vecteur $\mathbf{Z}$ revient au même, car ces deux entités sont porteuses de la même information. En effet, il est toujours possible d'identifier l'ensemble $\{\mathbf{Z}(iT_e)\}_{i=0\dots N-1}$ à un vecteur $\mathbf{Z}$ par l'isomorphisme canonique qui associe chaque échantillon à une composante du vecteur $\mathbf{Z}$ pour tout $i = 0 \dots N-1$,

$$\mathbf{Z}(iT_e) \quad \mapsto \quad \mathbf{Z}[i+1] := \mathbf{Z}(iT_e)e_{i+1} \quad \forall i = 0 \dots N-1.$$

où $\{e_i\}_{i=1\dots N}$ est la base canonique de $\mathbb{R}^N$.
Le but de cette section est d'écrire le développement de Karhunen-Loève de $Z^e(t)$ pour $t \in D$.
Pour tout $n \in \mathbb{N}$, soit z_n^e la variable aléatoire définie par

$$\mathbf{z}_n^e \quad := \quad \int_D \mathbf{Z}^e(t)\Phi_n^e(t)\,dt \quad , \tag{III.29}$$

où $\Phi_n^e(t)$ est une fonction appartenant à une base orthonormale de $L^2(D)$. Ici encore, il est toujours possible d'identifier l'ensemble $\{\Phi_n^e(iT_e)\}_{i=0\dots N-1}$ à un vecteur $\Phi_n \in \mathbb{R}^N$ par l'isomorphisme canonique qui pour tout $i = 0 \dots N-1$ associe chaque échantillon à une composante du vecteur Φ_n,

$$\Phi_n^e(iT_e) \quad \mapsto \quad \Phi_n[i+1] := \Phi_n(iTe)e_{i+1} \quad \forall i = 0 \dots N-1,$$

et ainsi indifféremment considérer la suite d'échantillons $\{\Phi_n^e(iT_e)\}_{i=0\dots N-1}$ et le vecteur $\Phi_n \in \mathbb{R}$.
En utilisant la définition de $\mathbf{Z}^e(t)$ III.28, $\mathbf{z}_n^e$ a pour expression

$$\begin{aligned}
\mathbf{z}_n^e &= \int_D \mathbf{Z}^e(t)\Phi_n^e(t)\,dt \\
&= \int_D \left(\sum_{i=0}^{N-1} \mathbf{Z}(iT_e)\delta(t-iT_e)\right)\Phi_n^e(t)\,dt \\
&= \sum_{i=0}^{N-1} \mathbf{Z}(iT_e)\left(\int_D \Phi_n^e(t)\delta(t-iT_e)\right)dt \\
&= \sum_{i=0}^{N-1} \mathbf{Z}(iT_e)\Phi_n^e(iT_e),
\end{aligned}$$

soit en écriture vectorielle,

$$\mathbf{z}_n^e = \langle \mathbf{Z}, \Phi_n \rangle = \mathbf{Z}^T\Phi_n.$$

Pour tout $n \in \mathbb{N}$, les coefficients $\mathbf{z}_n^e$ sont centrés puisque

$$\mathbb{E}\left[\mathbf{z}_n^e\right] = \mathbb{E}\left[\mathbf{Z}^T\right]\Phi_n = 0.$$

et leur covariance vaut pour tout couple $(n;m) \in \mathbb{N}^2$

$$\begin{aligned}
\mathbb{E}\left[\mathbf{z}_n^e\mathbf{z}_m^e\right] &= \mathbb{E}\left[\left(\left(\mathbf{Z}^T\Phi_n\right)\right)^T\left(\mathbf{Z}^T\Phi_m\right)\right] \\
&= \mathbb{E}\left[\Phi_n^T\mathbf{Z}\mathbf{Z}^T\Phi_m\right] \\
&= \Phi_n^T\mathbb{E}\left[\mathbf{Z}\mathbf{Z}^T\right]\Phi_m \\
&= \Phi_n^T\Gamma_{\mathbf{ZZ}}\Phi_m \\
&= \Phi_m^T\Gamma_{\mathbf{ZZ}}\Phi_n.
\end{aligned}$$

Il s'agit d'une forme quadratique engendrée par la matrice $\Gamma_{ZZ} \in \mathcal{M}_{(N,N)}$[10] symétrique définie non négative.
Les fonctions sont déterminées de telle sorte que la décorrélation statistique à l'ordre 2 des variables aléatoires $\{\mathbf{z}_n^e\}_{n\in\mathbb{N}}$ soit assurée. Par analogie à ce qui a été fait dans le cas d'une observation continue, la décorrélation des coefficients est effective dès lors que la relation d'équivalence suivante est vérifiée,

$$\left[\mathbb{E}\left[\mathbf{z}_n^e \mathbf{z}_m^e\right] = \mathbb{E}\left[(\mathbf{z}_n^e)^2\right]\delta[n-m]\right] \Longleftrightarrow \left[\Phi_m^T \Gamma_{ZZ} \Phi_n = \underbrace{\mathbb{E}\left[(\mathbf{z}_n^e)^2\right]}_{=\lambda_n}\delta[n-m]\right].$$

La proposition suivante, à rapprocher de la proposition III.3, fournit une condition suffisante sur les $\{\Phi_n\}_{n\in\mathbb{N}}$ afin que la décorrélation des $\{\mathbf{z}_n^e\}_{n\in\mathbb{N}}$ soit effective.

Proposition III.8. *Soit $\{\phi_n\}_{i=1\ldots N}$ l'ensemble des solutions de l'équation aux valeurs propres*

$$\Gamma_{ZZ}\Phi_n = \lambda_n \Phi_n.$$

Alors, ces vecteurs propres sont également solution de

$$\Phi_m^T \Gamma_{ZZ} \Phi_n = \lambda_n \delta[n-m],$$

avec $n \neq m$, ce qui entraîne la décorrélation des variables aléatoires z_n^e et z_m^e.
Autrement dit si

1. *Φ_n est solution de $\Gamma_{ZZ}\Phi_n = \lambda_n \Phi_n$,*
2. *Φ_n est solution de $\Phi_m^T \Gamma_{ZZ} \Phi_n = \lambda_n \delta[n-m]$,*
3. *$\mathbb{E}\left[z_n^e z_m^e\right] = \mathbb{E}\left[(z_n^e)^2\right]\delta[n-m]$,*

alors $1 \Rightarrow 2$ et $2 \Leftrightarrow 3$.

Démonstration . *Il y a au plus N vecteurs propres Φ_n associés à la matrice Γ_{ZZ}. Ces vecteurs sont orthogonaux entre eux et peuvent toujours être normalisés, ce qui sera le cas ici,*

$$\Phi_m^T \Phi_n \quad = \quad \delta[n-m] \quad \forall n \neq m.$$

– $1 \Rightarrow 2$.
Soit Φ_n et Φ_m deux vecteurs propres distincts correspondant respectivement aux valeurs propres λ_n et λ_m avec $n \neq m$. Alors,

$$\begin{aligned} \Gamma_{ZZ}\Phi_n &= \lambda_n \Phi_n \\ \Phi_m^T \Gamma_{ZZ} \Phi_n &= \lambda_n \Phi_m^T \Phi_n = \lambda_n \langle \Phi_m ; \Phi_n \rangle \\ \Phi_m^T \Gamma_{ZZ} \Phi_n &= \lambda_n \delta[n-m]. \end{aligned}$$

– $2 \Leftrightarrow 3$.
Il s'agit d'un simple jeu de réécriture où chaque ligne est obtenue par équivalence de la précédente,

$$\begin{aligned} \Phi_m^T \Gamma_{ZZ} \Phi_n &= \lambda_n \delta[n-m] \\ \Phi_m^T \mathbb{E}\left[\mathbf{Z}\mathbf{Z}^T\right] \Phi_n &= \lambda_n \delta[n-m] \\ \mathbb{E}\left[\Phi_m^T \mathbf{Z}\mathbf{Z}^T \Phi_n\right] &= \mathbb{E}\left[(z_n^e)^2\right]\delta[n-m] \\ \mathbb{E}\left[\left(\left(\mathbf{Z}^T\Phi_m\right)\right)^T \left(\mathbf{Z}^T\Phi_n\right)\right] &= \mathbb{E}\left[(z_n^e)^2\right]\delta[n-m] \\ \mathbb{E}\left[z_n^e z_m^e\right] &= \mathbb{E}\left[(z_n^e)^2\right]\delta[n-m]. \end{aligned}$$

Les calculs pouvant être menés d'un sens comme dans l'autre, l'équivalence est effective.

[10] $\mathcal{M}_{(N,N)}$ désigne l'anneau des matrices carrées de dimension N

□

Remarque : *Ainsi déterminées les vecteurs Φ_n et les réels[11] λ_n sont les éléments propres de la matrice de variance-covariance $\Gamma_{\mathbf{ZZ}}$ de l'observation $\mathbf{Z}$. Le fait de travailler avec une observation discrète en dimension finie simplifie considérablement la démarche, il n'est en particulier plus nécessaire de passer par les opérateurs compacts pour donner un sens à la détermination des éléments propres, ces derniers étant obtenus par résolution d'un problème de recherche de valeurs et vecteurs propres de matrice.*

Soit $\mathbf{Y}$ un vecteur aléatoire à réalisations dans $\mathbb{R}^N$ contenant les N coefficients $\{\mathbf{z}_n^e\}_{i=1\ldots N}$. Une opération de masquage consiste en la substitution de l'observation $\mathbf{Z}$ avec le vecteur $\mathbf{Y}$ qui par construction est de composantes statistiquement décorrélées à l'ordre 2.
De façon générale, la démarche conduisant au masquage d'un signal $\mathbf{Z}$ de dimension N, par substitution de ce dernier avec un signal $\mathbf{Y}$ lui aussi de dimension N étant entendu que $\Gamma_{\mathbf{ZZ}}$ ne possède que des valeurs propres distinctes, est la suivante :

1. Calcul ou estimation de la matrice de variance-covariance $\Gamma_{\mathbf{ZZ}}$.
2. Détermination de N vecteurs orthogonaux Φ_n.
3. Calcul de N coefficients $\mathbf{z}_n$.
4. Substitution de $\mathbf{Z}$ par le $n-$uplet $\{\mathbf{z}_n\}_{n=1\ldots N}$, coordonnées du vecteur $\mathbf{Y}$.

Si $\Gamma_{\mathbf{ZZ}}$ a des valeurs propres de multiplicité plus grande que 1 et qu'il n'y a donc que $N' < N$ valeurs propres distinctes, le principe proposé demeure valable mais devient sous optimal. Il suffit dans ce cas de dupliquer les coefficients correspondants autant de fois que la multiplicité des valeurs propres auxquels ils sont associés le suggère. Cela aura pour effet d'avoir une réalisation du vecteur $\mathbf{Y}$ avec des composantes identiques qui ne seraient donc en aucun cas être décorrélées. En pratique, une permutation aléatoire des coefficients de Y, réalisation de $\mathbf{Y}$ contrecarre ce problème pathologique. D'autre part, si N est grand devant le nombre de valeurs propres de multiplicité supérieure à 1, l'effet est négligeable.

Afin de mener à bien cette opération de masquage par décomposition des signaux, plusieurs stratégies sont envisageables, selon que les vecteurs de base soit *a priori* connus ou pas, selon que la matrice de variance-covariance soient *a priori* connue ou pas, toutes conduisant à des résultats de qualité différente aussi bien sous l'aspect numérique, que sous l'aspect de la quantité de moyens à mettre en oeuvre et de la résistance aux attaques des pirates. La prochaine section traite de ces aspects expérimentaux.

6 APPLICATION AU MASQUAGE PAR DÉCOMPOSITION DES SIGNAUX

Cette partie a pour but la mise en application de la technique de masquage par décomposition proposée dans la section précédente. L'objectif est de masquer une observation $\mathbf{Z}$ vue comme un processus aléatoire centré, stationnaire au second ordre, à réalisations dans $\mathbb{R}^N$ par un autre

[11] $\Gamma_{\mathbf{ZZ}}$ est symétrique définie non-négative ($\forall X \in \mathbb{R}^N$, $X^T \mathbf{ZZ} X = X^T \mathbb{E}\left[ZZ^T\right] X = \mathbb{E}\left[\|Z^T X\|^2\right] \geq 0$), donc ses valeurs propres sont réelles supérieures ou égales à 0.

processus aléatoire $\mathbf{Y}$ centré à réalisations dans $\mathbb{R}^N$ constitué d'éléments statistiquement décorrélés. Plus précisément, l'observation $\mathbf{Z}$ est la somme d'un signal expérimental déterministe s et d'un bruit gaussien[12] $\mathbf{B}$ centré de matrice de variance covariance Γ_{BB}. $\mathbf{Z}$ est donc de moyenne d'ensemble s et de matrice de variance covariance $\Gamma_{\mathrm{ZZ}} = \Gamma_{\mathrm{BB}}$.
La première étape consiste à déterminer les N vecteurs orthogonaux Φ_n. Ces derniers peuvent être fixés *a priori* par le choix d'une base orthonormale de $\mathbb{R}^N$, ou alors déterminés par l'équation aux valeurs propres $\Gamma_{\mathrm{ZZ}}\Phi_n = \lambda_n\Phi_n$. Dans ce cas il y a deux alternatives, ou bien Γ_{ZZ} est *a priori* connue, ou bien il faut l'estimer en tirant partie de l'hypothèse de stationnarité à l'ordre 2 de $\mathbf{Z}$. Une fois les vecteurs propres déterminés, les N coefficients de décomposition $\mathbf{z}_n$ sont obtenus en calculant le produit scalaire de l'observation $\mathbf{Z}$ avec le vecteur Φ_n. Enfin, une ultime étape consiste à permuter aléatoirement les coefficients calculés, puis à les affecter au vecteur $\mathbf{Y}$ qui représente le signal masqué.

La figure 3 montre le principe de fonctionnement général de la technique de masquage par décomposition, recensant les différents cas de figure conduisant au calcul des coefficients qui vont venir se substituer à l'observation.

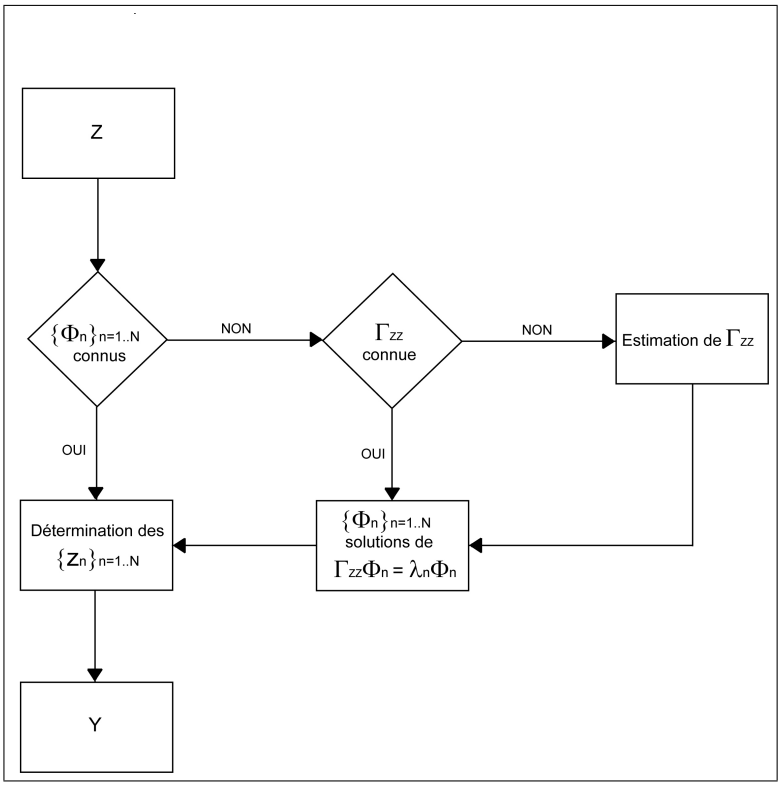


FIG. 3 – *Principe du masquage par décomposition de l'observation* $\mathbf{Z}$ *par le signal* $\mathbf{Y}$.

A partir du schéma de travail suggéré par la figure 3, la démarche expérimentale est la suivante : Dans un premier temps, les différentes techniques sont présentées à travers le cas du masquage d'une observation expérimentale $\mathbf{Z}$ de dimension N vue comme la somme d'un signal s centré, de dimension N modélisant une consommation idéale, et d'un bruit B de dimension N qui est un processus aléatoire gaussien de moyenne nulle et de matrice de variance covariance Γ_{BB}. Ainsi, $\mathbb{E}[\mathbf{Z}] = s$ et $\Gamma_{\mathrm{ZZ}} = \Gamma_{\mathrm{BB}}$.
400 échantillons de l'observation sont disponibles, cette dernière modélise un signal expérimental qui est une activité de consommation de courant additivement bruitée avec un rapport signal à bruit d'environ $40dB$. L'activité de courant est issue de la Thèse de Kussener [Kus02], il s'agit

[12]La gaussianité du bruit n'engendre ici pas de perte de généralité.

donc d'un signal expérimental réel qui va permettre d'avoir un premier aperçu des performances des techniques proposées.

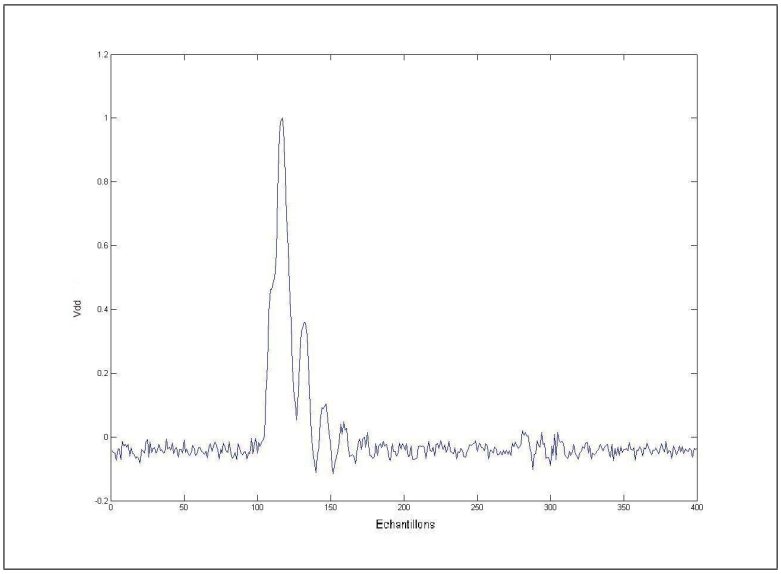


FIG. 4 – *Observation expérimentale* $\mathbf{Z}$ *modélisant une activité de consommation de courant centrée, normalisée en amplitude, additivement bruitée, sur* 400 *échantillons*

Une réalisation de l'observation est présentée à la figure 4. De l'appréciation visuelle de cette dernière, il apparaît que la difficulté principale lors de l'opération de masquage va être d'arriver à répartir au mieux la quantité de puissance moyenne véhiculée par les plus gros pics de consommation, vu que plus de 90% de la puissance moyenne est contenue dans les échantillons indexés de 100 à 150.
Pour chaque cas étudié, le résultat du traitement sera commenté avec une attention particulière portée sur l'étalement éventuel des pics de consommation. Les commentaires s'appuieront également sur l'autocorrélation et la densité spectrale de puissance du signal $\mathbf{Y}$, ce dernier devant s'apparenter à un bruit blanc, son autocorrélation doit avoir le gabarit d'un signal de Kroenecker pondéré par la puissance du signal alors que la densité spectrale de puissance doit occuper la totalité du domaine fréquentiel. Du point de vue du pirate qui tenterait à partir du signal masqué $\mathbf{Y}$ de retrouver la signature originale $\mathbf{Z}$, la meilleure des situations[13] est celle où il a en possession la signature de référence $\mathbf{Z}$. Fort de cette remarque, afin de définir un critère quantitatif de masquage, l'intercorrélation normalisée du signal natif $\mathbf{Z}$ avec le signal masqué $\mathbf{Y}$

$$r_{ZY}[k] := \frac{\sum_{n=1}^{N-k} Z_{n+k} Y_n}{\sum_{n=1}^{N} Z_n^2 \sum_{n=1}^{N} Y_n^2} \quad \forall k = 0 \ldots N-1$$

a été retenue. En effet, dans le cas où le pirate a la signature, en déterminant l'intercorrélation entre le signal natif et le signal masqué, tout se passe comme si $\mathbf{Y}$ était filtré par $\mathbf{Z}$ qui fait alors office de filtre adapté. Afin de garantir un masquage efficace, l'intercorrélation du signal masqué avec le signal natif ne doit pas avoir de pics significatifs traduisant des similitudes entre les deux signaux analysés. Le maximum de cette intercorrélation normalisée sera retenu et permettra par suite un travail de classification des différentes méthodes étudiées.

[13] et donc la pire pour l'encarteur

Cette section débute par une étude du cas intuitif qui consiste à permuter aléatoirement les échantillons du signal natif. Bien que cette approche n'ait rien à voir avec la technique exposée, elle sert néanmoins de point de départ et d'étalonnage. Les différentes déclinaisons de la technique de masquage par décomposition seront analysées : le cas où les fonctions de base sont connues, ce qui revient à utiliser une base de Fourier. Puis le cas où les fonctions de base ne sont pas connues où il faut déterminer la matrice de variance covariance de l'observation par estimation non paramétrique, puis par estimation paramétrique basée sur le principe du maximum de vraisemblance.
Dans un second temps, une fois la discussion des résultats de ces différentes approches effectuées, celles-ci seront utilisées pour masquer des activités de courant fournies par ST Microelectronics. Dans ce cas, l'observation est modélisée par $\mathbf{Z} = \mathbf{S} + \mathbf{B}$, le signal utile est à présent vu comme un processus stochastique de moment d'ordre 2 fini. Cette remarque intégrée, un ensemble de 11 signatures sera masqué puis les résultats interprétés.

6.1 Cas de la permutation aléatoire des échantillons du signal de consommation

Il s'agit là du cas le plus intuitif et le plus simple à mettre en oeuvre. Le principe est de créer le signal masqué en permutant aléatoirement les échantillons du signal natif disponible sous la forme d'un vecteur de $\mathbb{R}^N$.

6.1.1 Principe

L'opération de permutation s'effectue en appliquant au vecteur signal une matrice de permutation aléatoire. Cette matrice est telle que ses réalisations, qui appartiennent à $\mathcal{M}_{N,N}$, sont telles que chacune de ses colonnes[14] est un vecteur de la base canonique de $\mathbb{R}^N$. Pour N fixé, il y en a donc $N!$, chacune d'entre elles est par construction orthogonale.
L'avantage d'une telle opération est qu'elle ne nécessite que peu de moyens pour sa mise oeuvre, par exemple un générateur de nombres pseudo-aléatoires. voilà pourquoi la séquence pseudo-aléatoire régissant l'ordre des permutations est obtenue par la technique de genèse de flux pseudo-aléatoire basée sur le Chaos, présentée au chapitre précédent.

6.1.2 Mise en pratique

Le résultat d'une telle opération est présenté à la figure 5.

[14] Ou de façon équivalente, de ses lignes.

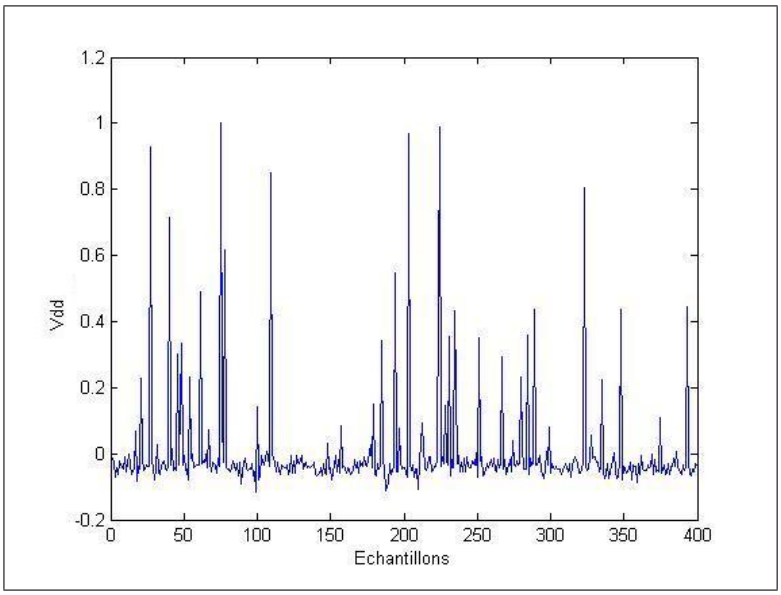
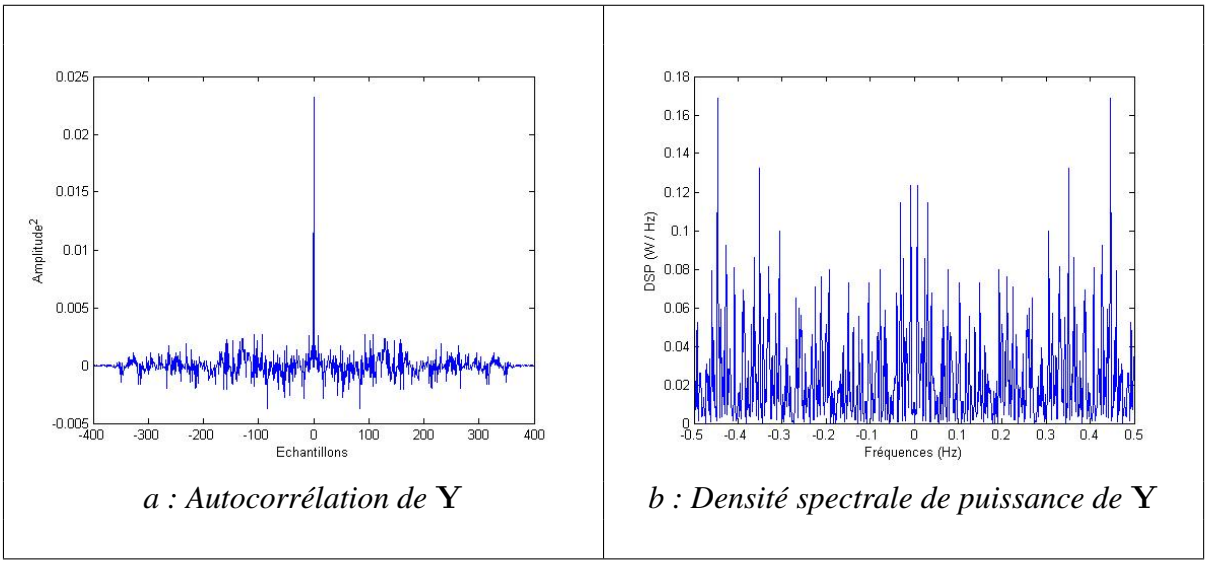


FIG. 5 – *Signal masqué* $\mathbf{Y}$ *obtenu par permutation pseudo-aléatoire des échantillons du signal natif* $\mathbf{Z}$

L'analyse visuelle de $\mathbf{Y}$ permet de dire que les pics de consommation ne sont plus isolés mais beaucoup plus nombreux et répartis sur l'ensemble de l'intervalle d'observation. L'étude de l'autocorrélation et de la densité spectrale de puissance de $\mathbf{Y}$ montre que ce dernier est conforme aux attentes, c'est-à-dire que la première présente un unique pic à l'origine alors que la seconde décrit un spectre très large bande, caractéristique d'une séquence d'éléments décorrélés. Ceci est illustré à la figure 6.



a : Autocorrélation de $\mathbf{Y}$ *b : Densité spectrale de puissance de* $\mathbf{Y}$

FIG. 6 – *Autocorrélation et densité spectrale de puissance du signal masqué* $\mathbf{Y}$

L'intercorrélation normalisée des signaux $\mathbf{Z}$ et $\mathbf{Y}$ est présentée à la figure 7, la lecture de cette dernière montre qu'il n'y a pas de pics de corrélation significatif permettant d'identifier distinctement la signature originale. Cette dernière présente un maximum de l'ordre de $0,17$, soit 17% de taux d'intercorrélation maximum.

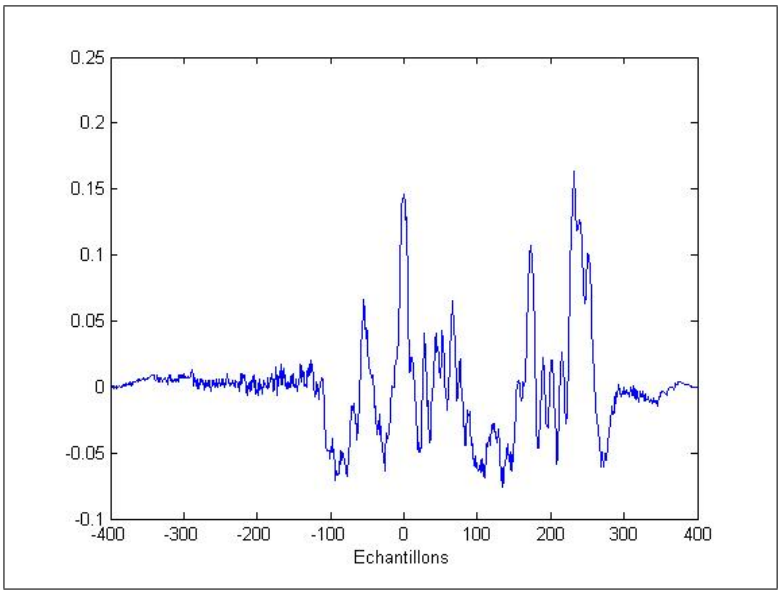


FIG. 7 – *Intercorrélation du signal masqué* $\mathbf{Y}$ *avec le signal natif* $\mathbf{Z}$

Cette méthode a pour avantage majeur d'être très simple à mettre en oeuvre, du moins vis à vis des autres techniques présentées ici, mais a cependant un défaut tout aussi majeur entraînant une faille de sécurité importante. En effet, le signal natif et le signal masqué sont liés par une relation matricielle, cette matrice est telle que chacune de ses réalisations est une matrice orthogonale[15] et chacune de ses colonnes est un des vecteurs de la base canonique de $\mathbb{R}^N$. Il est donc possible de retrouver exactement la signature $\mathbf{Z}$ en $N!$ permutations[16].
Dans le cas du signal expérimental utilisé, celui ci contient $N = 400$ échantillons, synonyme donc d'une reconstruction parfaite de ce dernier à partir du signal masqué en $400!$ opérations[17]. Cela montre que la méthode proposée, bien que donnant des résultats satisfaisants en terme de décorrélation des composantes du signal masqué, n'offre pas un niveau de sécurité suffisant. Néanmoins, il parait indispensable de terminer toute technique de masquage par décomposition par une ultime étape de permutation pseudo-aléatoire des coefficients calculés, car d'une part, d'un point de vue sécuritaire il faut alors au moins $N!$ opérations pour espérer retrouver la signature originale et d'autre part les permutations permettent mécaniquement de diminuer l'importance des phénomènes de corrélation d'échantillons successifs.
Ainsi, toutes les techniques présentées par la suite se terminent par une étape de permutation pseudo-aléatoire, agissant d'un certain point de vue comme un verrou.

6.1.3 Conséquences d'une opération de permutation aléatoire sur les propriétés statistiques d'un vecteur aléatoire centré, stationnaire au second ordre.

Le but de cette section est de caractériser statistiquement l'effet de l'opération de permutation aléatoire sur le signal obtenu, supposé centré et stationnaire au second ordre, ceci afin d'en évaluer la prépondérance dans le cadre global de la technique de masquage proposée.
Soit $\mathbf{P}$ une matrice de permutation aléatoire de dimension N. Chacune des $N!$ réalisations possibles est une matrice orthogonale, obtenue en permutant les lignes ou les colonnes de la matrice identité. Donc, pour toute réalisation P de $\mathbf{P}$,

$$P^{-1} \quad = \quad P^T.$$

[15] Son inverse est égal à sa transposée
[16] correspondant à $N!$ opérations, auxquelles il faut ajouter celles nécessaires à la reconnaissance de la signature
[17] Garder à l'esprit que plus la technologie avance, moins ce chiffre fait peur

La structure de $\mathbf{P}$ est telle que chacun de ses éléments peut valoir 1 avec une probabilité $\frac{(N-1)!}{N!} = \frac{1}{N}$ et 0 avec une probabilité $\frac{(N-1)}{N}$, donc

$$\mathbb{E}\left[\mathbf{P}\right] = \frac{1}{N}\mathbf{1}_N,$$

où $\mathbf{1}_N$ est la matrice carrée de dimension N ne contenant que des 1.
Soit $\mathbf{z}$ un vecteur aléatoire centré, stationnaire au second ordre, issu du masquage de l'observation $\mathbf{Z}$,

$$\mathbb{E}\left[\mathbf{z}\right] = 0 \quad \text{et} \quad \Gamma_{zz} = \mathbb{E}\left[\mathbf{z}\mathbf{z}^T\right].$$

Soit à présent le processus $\mathbf{Y}$, vecteur aléatoire de dimension N, construit à partir de $\mathbf{z}$ et $\mathbf{P}$,

$$\mathbf{Y} := \mathbf{P}\mathbf{z}.$$

Autrement dit, $\mathbf{Y}$ est obtenu à partir de $\mathbf{z}$ en permutant aléatoirement les coordonnées de ce dernier.
Une telle opération conserve la puissance moyenne puisque

$$\begin{aligned}
\sigma_Y^2 := \mathbb{E}\left[\|\mathbf{Y}\|^2\right] &= \mathbb{E}\left[\mathbf{Y}^T\mathbf{Y}\right] \\
&= \mathbb{E}\left[\mathbf{z}^T \underbrace{\mathbf{P}^T\mathbf{P}}_{=Id_N}\mathbf{z}\right] \\
&= \mathbb{E}\left[\mathbf{z}^T\mathbf{z}\right] \\
&= \mathbb{E}\left[\|\mathbf{z}\|^2\right] = \sigma_z^2.
\end{aligned}$$

Par ailleurs, en supposant que $\mathbf{P}$ et $\mathbf{z}$ sont indépendants, l'intercorrélation entre le vecteur $\mathbf{z}$ et le vecteur $\mathbf{Y}$[18] vaut

$$\begin{aligned}
\mathbb{E}\left[\mathbf{Y}\mathbf{z}^T\right] &= \mathbb{E}\left[\mathbf{P}\mathbf{z}\mathbf{z}^T\right] \\
&= \mathbb{E}\left[\mathbf{P}\right]\mathbb{E}\left[\mathbf{z}\mathbf{z}^T\right] \\
&= \frac{1}{N}\mathbf{1}_N\Gamma_{zz}.
\end{aligned}$$

Or,

$$\lim_{N\to+\infty} \frac{1}{N}\mathbf{1}_N\Gamma_{zz} = 0,$$

ce qui signifie que lorsque le nombre d'échantillons devient infiniment grand, la décorrélation entre le vecteur $\mathbf{z}$ et le vecteur $\mathbf{Y}$ est idéalement nulle. Ainsi, une opération de permutation aléatoire tend à éliminer les corrélations présentes entre les échantillons d'un vecteur.
Il reste à évaluer la corrélation éventuelle des échantillons après permutation alatoire, il faut alors calculer l'autocorrélation du vecteur $\mathbf{Y}$,

$$\begin{aligned}
\Gamma_{YY} &:= \mathbb{E}\left[\mathbf{Y}\mathbf{Y}^T\right] \\
&= \mathbb{E}\left[\mathbf{P}\mathbf{z}\mathbf{z}^T\mathbf{P}^T\right].
\end{aligned}$$

[18] $\mathbf{Y}$ est constitué des mêmes coordonnées que $\mathbf{z}$, mais rangées dans un ordre différent.

Remarque :

–

$$\begin{aligned} \textit{Trace}[\Gamma_{YY}] &= \textit{Trace}[\mathbb{E}\left[\mathbf{P}\mathbf{z}\mathbf{z}^T\mathbf{P}^T\right]] \\ &= \textit{Trace}[\mathbb{E}\left[\mathbf{P}^T\mathbf{P}\mathbf{z}\mathbf{z}^T\right]] \\ &= \textit{Trace}[\mathbb{E}\left[\mathbf{z}\mathbf{z}^T\right]] \\ &= \textit{Trace}[\Gamma_{zz}] \\ &= N\sigma_z^2. \end{aligned}$$

–

$$\begin{aligned} \textit{det}[\Gamma_{YY}] &= \textit{det}[\mathbb{E}\left[\mathbf{P}\mathbf{z}\mathbf{z}^T\mathbf{P}^T\right]] \\ &= \mathbb{E}\left[\textit{det}[\mathbf{P}^T\mathbf{P}\mathbf{z}\mathbf{z}^T]\right] \\ &= \mathbb{E}\left[\textit{det}[\mathbf{z}\mathbf{z}^T]\right] \\ &= \textit{det}[\Gamma_{zz}]. \end{aligned}$$

– Γ_{YY} *a les mêmes éléments diagonaux que* Γ_{zz}.

Reste alors à calculer les $N(N-1)$ éléments extra-diagonaux de cette matrice :

$$\begin{aligned} (\Gamma_{YY})_{ij} &= \mathbb{E}\left[\mathbf{Y}_i\mathbf{Y}_j\right] \quad i \neq j \\ &= \mathbb{E}\left[\mathbf{P}\mathbf{z}_i\mathbf{P}\mathbf{z}_j\right] \\ &= \mathbb{E}\left[\sum_{k=1}^{N}\mathbf{P}_{ik}z_k\sum_{l=1}^{N}\mathbf{P}_{jl}z_l\right] \\ &= \mathbb{E}\left[\sum_{k=1}^{N}\sum_{l=1}^{N}\mathbf{P}_{ik}\mathbf{P}_{jl}z_kz_l\right] \\ &= \sum_{k=1}^{N}\sum_{l=1}^{N}\mathbb{E}\left[\mathbf{P}_{ik}\mathbf{P}_{jl}\right]r_{zz}[l-k]. \end{aligned}$$

Il faut alors déterminer $\mathbb{E}\left[\mathbf{P}_{ik}\mathbf{P}_{jl}\right]$.

$\mathbf{P}_{ik}$ est une variable aléatoire binaire de loi $\{(1;\frac{1}{N});(0;\frac{N-1}{N})\}$.

D'autre part, $\mathbf{P}_{jl}/\mathbf{P}_{ik} = 1, i \neq j$ a pour loi $\{(1;\frac{1}{N-1});(0;\frac{N-2}{N-1})\}$, donc

$$\begin{aligned} \mathbb{E}\left[\mathbf{P}_{ik}\mathbf{P}_{jl}\right] &= 1 \times 1 \times \mathbb{P}(\mathbf{P}_{ik}=1,\mathbf{P}_{jl}=1,i\neq j) \\ &= \mathbb{P}(\mathbf{P}_{jl}=1/\mathbf{P}_{ik}=1,i\neq j)\mathbb{P}(\mathbf{P}_{ik}=1) \\ &= \frac{1}{N-1}\frac{1}{N}. \end{aligned}$$

Remarque : *Si* $k = l$, $\mathbb{P}(\mathbf{P}_{jl} = 1/\mathbf{P}_{ik} = 1, i \neq j) = 0$ *car il ne peut y avoir deux symboles* 1 *sur une même colonne.*

Ainsi, une composante extra-diagonale de la matrice de variance-covariance Γ_{YY} a pour expression

$$(\Gamma_{YY})_{ij} = \frac{1}{N(N-1)} \sum_{k=1}^{N} \sum_{l=1}^{N} r_{zz}[l-k].$$

Or, lorsque l et k parcourent l'ensemble $\{1; \ldots; N\}$, l'entier $m := l - k$ parcours quant à lui l'ensemble

$$\{\underbrace{-(N-1)}_{1 \text{ fois}}; \underbrace{-(N-2)}_{2 \text{ fois}}; \ldots; \underbrace{0}_{N \text{ fois}}; \ldots; \underbrace{(N-2)}_{2 \text{ fois}}; \underbrace{(N-1)}_{1 \text{ fois}}\}.$$

Donc, en invoquant la parité de $r_{zz}[m]$, la symétrie de l'intervalle de sommation, et le fait que $l - q \neq 0 \Leftrightarrow m \neq 0$,

$$\begin{aligned}
(\Gamma_{YY})_{ij} &= \frac{1}{N(N-1)} \sum_{m=0}^{N-1} (N - |m|) r_{zz}[m] \quad m \neq 0 \\
&= \frac{2}{N(N-1)} \sum_{m=1}^{N-1} (N-m) r_{zz}[m] \\
&= \frac{2}{(N-1)} \sum_{m=1}^{N-1} (1 - \frac{m}{N}) r_{zz}[m],
\end{aligned}$$

Ce qui permet d'affirmer que l'expression de $(\Gamma_{YY})_{ij}$ pour tout $i \neq j$ est

$$(\Gamma_{YY})_{ij} = \frac{2}{(N-1)} \sum_{m=1}^{N-1} (1 - \frac{m}{N}) r_{zz}[m].$$

Lorsque $N \to +\infty$, cette expression peut être vue comme une somme de Reimann[19], car alors $\mathbf{z}$ peut être considéré comme résultant de l'échantillonnage régulier à la période $\frac{T}{N}$ d'un processus aléatoire à temps continu $\mathbf{z}(t)$ de fonction d'autocorrélation $R_{zz}(\tau)$. Alors, $r_{zz}[m] := R_{zz}(m\frac{T}{N})$ et

$$\lim_{N \to +\infty} (\Gamma_{YY})_{ij} = \frac{2}{T} \int_0^T (1 - \frac{\tau}{T}) R_{zz}(\tau) d\tau.$$

Par suite, lorsque $T \to +\infty$, une condition suffisante de convergence vers 0 de l'intégrale est que $R_{zz}(\tau)$ soit sommable, ce qui est le cas pour des processus stationnaires au second ordre.

Ainsi, l'opération de permutation aléatoire d'un vecteur aléatoire a un effet de décorrélation sur les échantillons de ce dernier vu que plus le nombre d'échantillons est grand, plus Γ_{YY} se rapproche d'une matrice diagonale. D'un point de vue pratique, cette opération consiste à éliminer la notion d'information contiguë contenue dans un signal informationnel.

[19] $\lim_{N \to +\infty} \frac{1}{N-1} \sum_{m=1}^{N-1} f(a + (b-a)\frac{n}{N}) = \frac{1}{b-a} \int_a^b f(t) dt$

6.2 Cas où la base de décomposition est *a priori* connue

Dans le cas où la base de décomposition est connue, les N vecteurs de base $\Phi_n \in \mathbb{R}^N$ sont parfaitement déterminés avant le début du traitement, il n'est donc pas nécessaire d'obtenir ces derniers en cherchant les éléments propres de la matrice de variance covariance de l'observation, opération pouvant engendrer de lourds calculs. A travers cette remarque, il apparaît que la complexité de mise en oeuvre de cette famille de technique de masquage est faible, ce qui est de bonne augure, mais le fait de rendre connus les vecteurs de base est dangereux en terme de piratage vu qu'il est alors possible dans un temps raisonnable[20] de remonter au signal natif.
Dans la section 4, il a été montré que la base servant à l'écriture des séries de Fourier est une bonne candidate à ce type de démarche.
L'observation est disponible sous la forme d'un vecteur de $\mathbb{R}^N$, le but est de substituer à ces N composantes exactement N coefficients. Or, un développement sur une base de Fourier est tel que ou bien les vecteurs de base sont exponentiels complexes[21] auquel cas il faut considérer au plus N parties réelles et N parties imaginaires, ou alors les vecteurs de base sont réels sinusoïdaux[22], auquel cas il faut calculer $N + N$ coefficients. Dans les deux cas, le fait de doubler la quantité d'information à stocker n'est pas gênant en soi, mais ne peut faire qu'augmenter la redondance d'information, ce qui dans un contexte de masquage est proscrit. Pour remédier à ce problème, il est possible de considérer une base de la transformée en cosinus discrète [Bli93, CouHDR05], utilisée par exemple par la technique de compression d'images JPEG. Cette dernière associe à un vecteur z de $\mathbb{R}^N$ le vecteur c lui aussi de $\mathbb{R}^N$ tel que

$$c[n] := \sqrt{\frac{2}{N}}\alpha_n \sum_{i=1}^{N} z[i] \cos\left(\frac{(2i-1)(n-1)\pi}{2N}\right) \quad \forall n = 1 \dots N,$$

avec $\alpha_n := \begin{cases} \frac{1}{\sqrt{2}} & si \quad n = 1 \\ 1 & \forall n = 2 \dots N \end{cases}$. D'un point de vue vectoriel, le scalaire $c[n]$, à n fixé est la projection du vecteur z sur le vecteur Φ_n de coordonnées $\sqrt{\frac{2}{N}}\alpha_n \cos\left(\frac{(2i-1)(n-1)\pi}{2N}\right)$ pour tout $i = 1 \dots N$. La base considérée dans ce cas est constituée des vecteurs $\{\Phi_n\}_{n=1\dots N}$, chacun ayant pour composante

$$\Phi_n[i] := \sqrt{\frac{2}{N}}\alpha_n \cos\left(\frac{(2i-1)(n-1)\pi}{2N}\right) \quad \forall i = 1 \dots N. \tag{III.30}$$

Le traitement qui construit un signal masqué $\mathbf{Y}$ à partir d'une observation $\mathbf{Z}$ est le suivant :

1. Mise à disposition des N échantillons de l'observation $\mathbf{Z}$.
2. Constitution des N vecteurs de base selon la relation III.30,
3. Genèse des N coefficients $\mathbf{z}_n$ correspondant à la projection de l'observation sur chacun des vecteurs de base,
4. Substitution de l'observation par l'ensemble des coefficients pseudo-aléatoirement permutés réunis dans le vecteur $\mathbf{Y}$.

L'observation test illustrée à la figure 4 est soumise à cette technique de masquage. Une réalisation du signal masqué ainsi créé est proposée à la figure 8.

[20] Faisant abstraction de la permutation aléatoire finale des coefficients
[21] Conduisant au calcul des $\{c_n\}_{n=1\dots N}$
[22] Conduisant au calcul des $\{a_n\}_{n=1\dots N}$ et des $\{b_n\}_{n=1\dots N}$

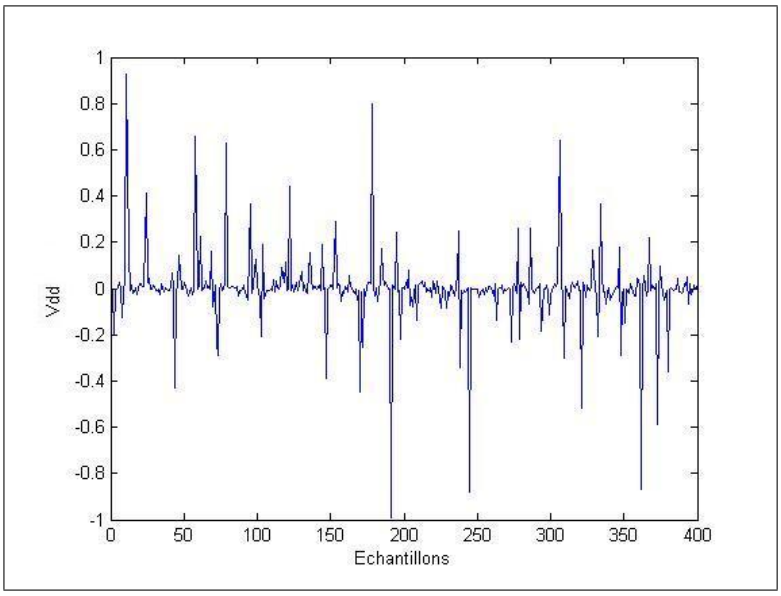
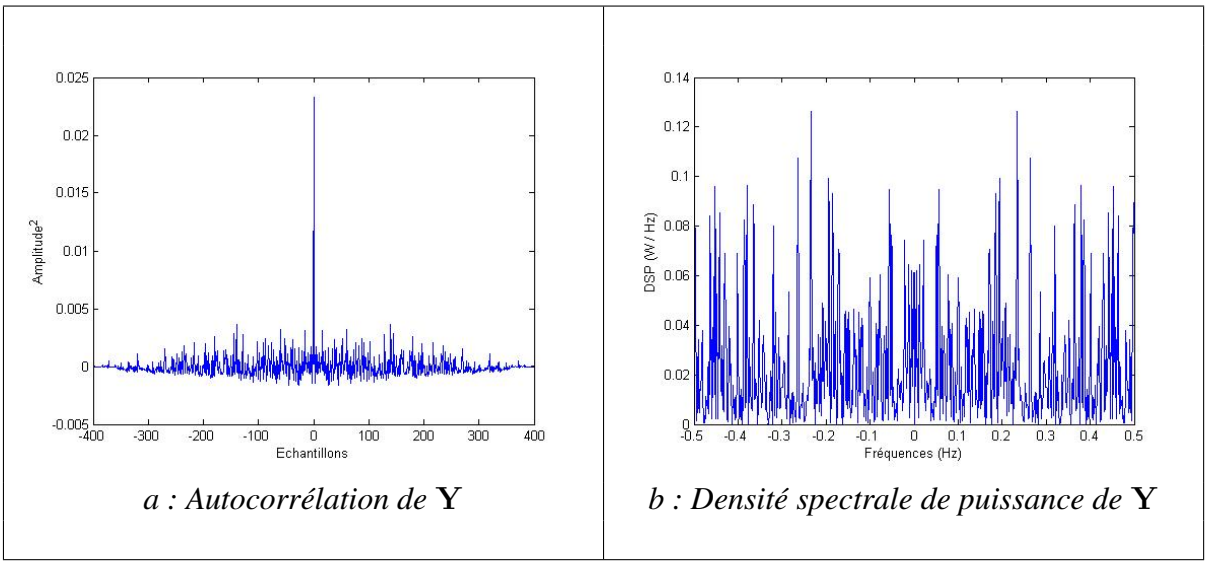


FIG. 8 – *Signal masqué* $\mathbf{Y}$

Comme cela a été montré auparavant, la puissance du signal masqué est identique à celle du signal utile. L'observation de la figure 8 montre que le signal masqué à des pics d'amplitude similaire à ceux de l'observation, mais pas localisés aux mêmes instants. Cette dernière montre que la puissance instantanée de l'observation a tendance à s'étaler sur l'ensemble de définition du signal de puissance moyenne identique à celle du signal natif.

Une conséquence de ce fait est la disparition des pics significatifs initialement présents. Il apparaît clairement que la fonction d'autocorrélation de $\mathbf{Y}$ visible sur la figure 9 s'apparente à celle idéale d'un bruit à corrélations microscopiques et qu'il n'y a pas d'autres pics de corrélation que le pic central. La faible occupation temporelle laisse augurer une large occupation fréquentielle, ce qui est confirmé par l'étude de la densité spectrale de puissance sur la figure 9 dont il ressort que le signal masqué $\mathbf{Y}$ est un signal riche en fréquences, ceci est caractéristique des signaux constitués d'échantillons faiblement corrélés.



a : Autocorrélation de $\mathbf{Y}$ *b : Densité spectrale de puissance de* $\mathbf{Y}$

FIG. 9 – *Autocorrélation et densité spectrale de puissance du signal masqué* $\mathbf{Y}$

L'analyse du signal masqué montre qualitativement que ce dernier remplit les conditions nécessaires pour être considéré comme blanc, à savoir à microcorrélations et de spectre large bande.

En se plaçant du point de vue du pirate, l'intercorrélation du signal natif avec le signal masqué présente à la figure 10 fait ressortir le plus gros pic de consommation, mais aux instants où apparaissent les pics du signal masqué, qui eux n'ont aucun lien avec les instants effectifs d'apparition des pics de consommation du signal natif. La technique de masquage présentée est donc robuste aux attaques basées sur la notion de corrélation. La valeur absolue du maximum d'intercorrélation normalisée est de $0,13$, c'est-à-dire un taux de corrélation maximum d'environ 13% entre les deux signaux.

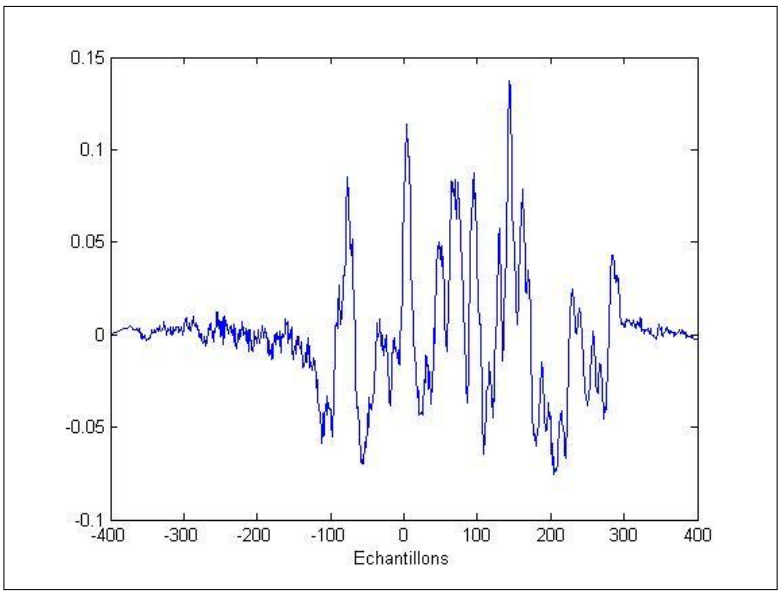


FIG. 10 – *Intercorrélation du signal masqué* $\mathbf{Y}$ *avec le signal natif* $\mathbf{Z}$

6.3 Cas où la base de décomposition n'est pas *a priori* connue

Dans cette partie de l'étude, les vecteurs de base ne sont pas *a priori* connus. Il faut donc les déterminer et pour ce faire, d'après le schéma 3 il faut résoudre l'équation aux valeurs propres

$$\Gamma_{ZZ}\Phi_n = \lambda_n\Phi_n, \tag{III.31}$$

ce qui revient à déterminer les éléments propres de la matrice de variance covariance de l'observation $\mathbf{Z}$. Deux cas de figure vont être envisagés. Ou bien Γ_{ZZ} est estimée à partir de l'observation $\mathbf{Z}$, ou bien Γ_{ZZ} est modélisée à partir d'un modèle général d'autocorrélation. Clairement, ces deux façons de faire doivent conduire à des résultats différents vu que sauf cas exceptionnel, la matrice générée par estimation et la matrice générée par modélisation n'ont aucune raison d'être semblables [23] et génèrent donc des vecteurs $\mathbf{Y}$ différents.
De plus, d'après les enseignements de la section 6.1, une ultime étape de permutation pseudo-aléatoire des coefficients vient se greffer en bout de chaîne de traitement. Le traitement qui a un signal natif $\mathbf{Z}$ fait correspondre le signal masqué $\mathbf{Y}$, dans le cas où la matrice de variance covariance du signal est à déterminer, est le suivant :

1. Mise à disposition des N échantillons de l'observation $\mathbf{Z}$.
2. Genèse de la matrice de variance covariance Γ_{ZZ} associée à l'observation, soit par modélisation, soit par estimation.

[23] $[A$ et $B]$ sont semblables $\Leftrightarrow$ $[\exists P$ régulière tel que $B = P^{-1}AP]$. Alors A et B ont mêmes éléments propres.

3. Recherche des vecteurs $\{\Phi_n\}_{n\in\mathbb{N}}$, vecteurs propres de Γ_{ZZ} en résolvant l'équation III.31.
4. Genèse des N coefficients $\mathbf{z}_n$ correspondant à la projection de l'observation sur chacun des vecteurs de base,
5. Substitution de l'observation par l'ensemble des coefficients pseudo-aléatoirement permutés.

Par rapport au cas où les vecteurs de base sont *a priori* connus, cette famille de méthode est plus complexe à mettre en oeuvre dans la mesure où il faut déterminer la matrice de variance covariance de l'observation, puis déterminer les vecteurs propres en résolvant l'équation III.31. En contrepartie, la tache du pirate est dans ce cas plus ardue pour retrouver la signature originale, puisque parmi les marches qu'il doit gravir pour revenir à l'observation native, il doit résoudre exactement la même équation aux valeurs propres.

6.3.1 Cas où la matrice de variance covariance est estimée

Une façon de déterminer Γ_{ZZ} est de l'estimer directement à partir de l'observation. Dans de nombreuses situations pratiques il est nécessaire d'avoir à disposition les statistiques d'ordre deux d'une observation, c'est par exemple le cas dans la théorie du filtrage adapté stochastique présenté au chapitre suivant et dans [Cav93]. La matrice de variance covariance Γ_{ZZ}, a pour expression

$$\Gamma_{ZZ} := \mathbb{E}\left[\mathbf{Z}\mathbf{Z}^T\right] = \begin{bmatrix} \mathbb{E}\left[\mathbf{Z}_1^2\right] & \cdots & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_N\right] \\ \vdots & \ddots & \vdots \\ \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_N\right] & \cdots & \mathbb{E}\left[\mathbf{Z}_N^2\right]. \end{bmatrix} \tag{III.32}$$

Si le signal est stationnaire à l'ordre 2, les coefficients $\{\mathbb{E}\left[\mathbf{Z}_i\mathbf{Z}_j\right]\}_{\substack{i=1\ldots N\\ j=1\ldots N}}$ de Γ_{ZZ} ont la propriété d'invariance par translation d'indice

$$\mathbb{E}\left[\mathbf{Z}_{i+k}\mathbf{Z}_{j+k}\right] = \mathbb{E}\left[\mathbf{Z}_i\mathbf{Z}_j\right],$$

$\forall(i,j) \quad / \quad |i-j| = k \in [-(N-1)\,;\,(N-1)]$.
Cette propriété confère à la matrice $\Gamma_{ZZ} \in \mathcal{M}(N,N)$ une structure de Toeplitz [24], qui combinée à la propriété de symétrie en fait une matrice circulante d'expression

$$\Gamma_{ZZ} = \begin{bmatrix} \sigma_Z^2 & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_2\right] & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_3\right] & \cdots & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_N\right] \\ \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_2\right] & \sigma_Z^2 & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_2\right] & \ddots & \vdots \\ \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_3\right] & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_2\right] & \sigma_Z^2 & \ddots & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_3\right] \\ \vdots & \ddots & \ddots & \ddots & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_2\right] \\ \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_N\right] & \cdots & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_3\right] & \mathbb{E}\left[\mathbf{Z}_1\mathbf{Z}_2\right] & \sigma_Z^2 \end{bmatrix} \tag{III.33}$$

D'après III.33, la matrice est complètement caractérisée par la donnée d'une de ses lignes ou de ses colonnes, par conséquent, estimer Γ_{ZZ} revient à estimer les N quantités

$$\left\{\sigma_Z^2, \mathbb{E}\left[\mathbf{Z}_i\mathbf{Z}_2\right], \mathbb{E}\left[\mathbf{Z}_i\mathbf{Z}_3\right], \cdots, \mathbb{E}\left[\mathbf{Z}_i\mathbf{Z}_N\right]\right\}, \quad \text{pour} \quad i \in [1,N] \quad \text{fixé},$$

ou encore écrit de façon condensée $\left\{\mathbb{E}\left[\mathbf{Z}_i\mathbf{Z}_k\right]_{\substack{k=1\ldots N\\ i\text{fixé}}}\right\}$, qui d'après l'hypothèse de stationnarité à l'ordre 2 ne dépendent que de $k-i$.

[24] Une matrice à coefficients constants sur ses N diagonales

En pratique, $i = 1$ ce qui correspond a première ligne de la matrice. Ainsi, les N valeurs $\{\mathbb{E}[\mathbf{Z}_1\mathbf{Z}_k]_{k=1\ldots N}\}$ ne dépendent que de $k-1$ donc que de k et ne sont rien d'autre que les coefficients de l'autocorrélation r de $\mathbf{Z}$ correspondant à des décalages positifs. L'estimation de la matrice Γ_{ZZ} se ramène donc à l'estimation de l'autocorrélation r du vecteur observation $\mathbf{Z}$. Dans le cas des signaux réels centrés et stationnaire à l'ordre 2, le vecteur r a pour composantes $r[k] := \mathbb{E}[\mathbf{Z}_n\mathbf{Z}_{n+k}]$, il est de dimension $(2N-1)$ si $\mathbf{Z}$ est de dimension N. Pour $k = 0\ldots N-1$, $r[k]$ décrit bien les N valeurs de la première ligne de Γ_{ZZ}.
Sous une hypothèse d'ergodicité du signal $\mathbf{Z}$ de réalisation Z à valeurs réelles, un estimateur biaisé [25] $\hat{r}[k]$ de $r[k]$ pour $k = 0\ldots N-1$ est

$$\hat{r}[k] \quad := \quad \frac{1}{N}\sum_{n=1}^{N-k} Z_n Z_{n+k} \quad \forall k = 0\ldots N-1. \tag{III.34}$$

Ainsi, l'algorithme conduisant à l'estimation de la matrice de variance covariance Γ_{ZZ} de l'observation $\mathbf{Z}$ centrée, à réalisations réelles, stationnaire à l'ordre 2 et ergodique est le suivant :

1. Estimation de $\{r[k]\}_{k=0\ldots N-1}$ à l'aide de III.34.
2. Construction de l'estimateur de Γ_{ZZ} par concaténation des $N-1$ permutations circulaires de $\hat{r}[k]$ de telle sorte à obtenir la structure matricielle III.33.

Cette démarche intervient lorsqu'est traité le point 2 de l'algorithme de la section précédente.
Le traitement complet a été appliqué à l'observation expérimentale illustrée à la figure 4, le résultat de ce traitement est présenté sur la figure 11. De l'appréciation qualitative de ce dernier ressort le fait que la puissance instantanée est répartie de façon plus homogène sur l'ensemble des échantillons tout en conservant une puissance moyenne identique à celle du signal natif. Cependant, des pics d'amplitude significative sont présents mais ne laissent pas entrevoir des motifs spécifiques présents dans l'observation native.

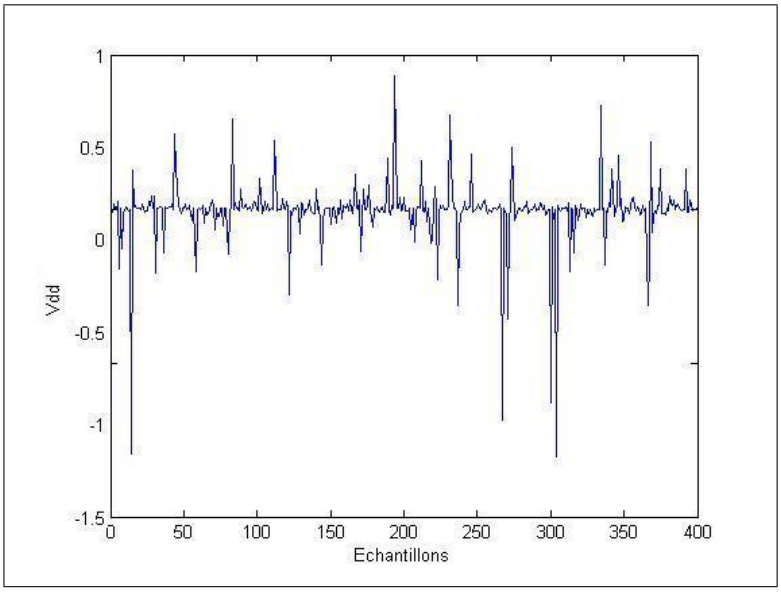
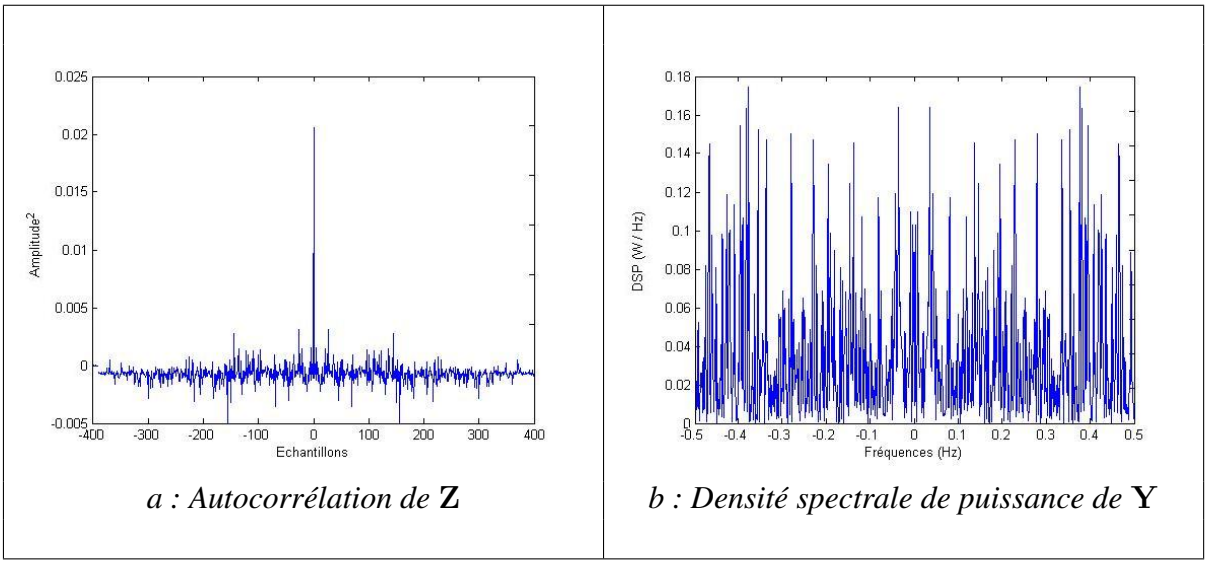


FIG. 11 – *Signal masqué* $\mathbf{Y}$

Concernant l'interprétation des statistiques d'ordre 2 du signal masqué, présentées sur la figure 12, bien que l'autocorrélation du signal s'apparente à celle d'un signal décorrélé il est à noter la

[25] L'estimateur biaisé atténue les effets de bords, voilà pourquoi il est préféré à son pendant non biaisé $\frac{1}{N-k}\sum_{n=1}^{N-k} Z_n Z_{n+k}$. De plus, l'estimateur biaisé est de variance plus faible. [Kay93]

présence de pics secondaires d'amplitude environ 20% de l'amplitude du pic central de l'autocorrelation. La densité spectrale de puissance du signal masqué montre sa richesse fréquentielle. En dépit des résultats acceptables en terme de statistique d'ordre 2, les pics de forte amplitude du signal masqué visibles sur la figure 11 font que l'intercorrelation normalisée du signal natif avec le signal masqué présentée sur la figure 13 a des zones significatives de corrélation dont le maximum relevé avoisine les 21% de taux de corrélation.



a : Autocorrélation de $\mathbf{Z}$ *b : Densité spectrale de puissance de* $\mathbf{Y}$

FIG. 12 – *Autocorrélation et densité spectrale de puissance du signal masqué* $\mathbf{Y}$

L'avantage d'une telle démarche est qu'elle ne nécessite pas d'avoir à stocker des informations *a priori*, ni matrice de variance covariance ni vecteurs de base, et que pour chaque réalisation, l'estimation de r sera différente donc Γ_{ZZ} aussi, donc ses vecteurs propres aussi et les coefficients de Y également. Vu que le tout change à chaque réalisation de l'observation et qu'il n'y a pas d'information *a priori* disponible, cela oblige le pirate, en plus des difficultés liées à la technique proprement dite, à mettre en oeuvre des techniques statistiques appropriées et ne peut lui permettre dans le pire des cas d'avoir qu'une estimation moyenne de la signature étudiée. En contrepartie, il est nécessaire d'effectuer la phase d'estimation à chaque fois, et de créer une nouvelle matrice pour chaque observation donc refaire les calculs pour chaque signature à masquer. A ce propos, la partie du traitement concernant la recherche des éléments propres de Γ_{ZZ} peut être menée à bien par l'algorithme de la puissance itérée [The87].

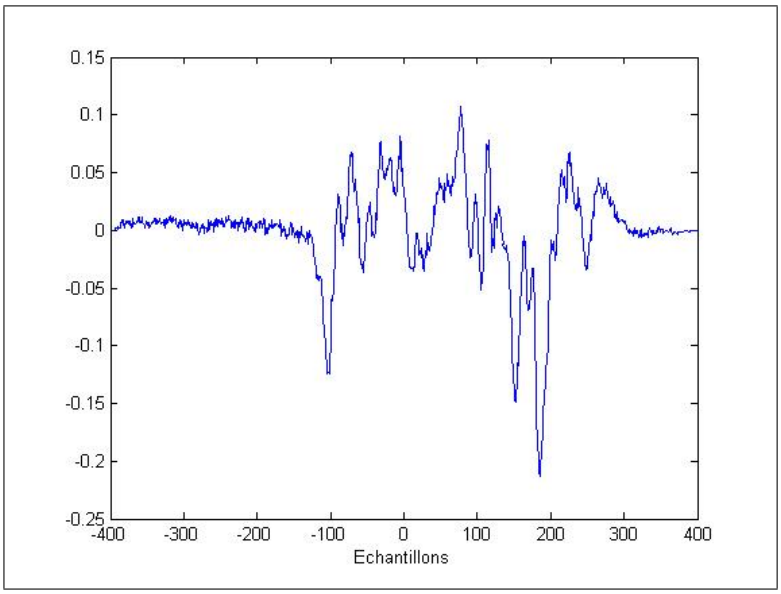


FIG. 13 – *Intercorrélation du signal masqué* $\mathbf{Y}$ *avec le signal natif* $\mathbf{Z}$

6.3.2 Cas où la matrice de variance covariance est modélisée

Dans la section précédente la matrice de variance covariance est directement estimée à partir de l'observation donc étroitement liée à cette dernière. L'inconvénient majeur de la technique précédemment proposée est qu'il est nécessaire d'estimer Γ_{ZZ} pour chaque signature traitée et donc de relancer toute la batterie de calculs conduisant à cette estimation dès lors qu'une nouvelle signature est traitée. De plus, il n'est pas nécessaire dans ce contexte de masquage de modéliser fidèlement l'autocorrélation de l'observation étudiée puisque cette dernière serait alors adaptée de façon optimale[26] à la signature sur laquelle elle a été estimée et de fait moins bien adaptée aux autres. Cela s'apparente plutôt à la démarche du pirate recherchant les informations statistiques d'une signature particulière. Partant de ces considérations, l'idée est alors d'estimer Γ_{ZZ} non pas directement à partir d'une observation mais indirectement en l'approchant à partir d'un modèle général d'autocorrélation, faisant alors l'hypothèse que deux signatures distinctes ont des autocorrélations ayant grossièrement le même gabarit. Cette hypothèse est motivée par la physique du problème faisant qu'une Smart Card est constituée d'un nombre fini de composants, de fonctionnalités ne pouvant donc générer qu'un nombre fini de signatures différentes[27]. Le modèle, dépendant éventuellement de paramètres, est calibré *a priori* sur la base des réalisations disponibles de l'observation considérée, le but n'est pas que ce dernier soit fortement adapté à un type de signature, mais qu'il décrive le comportement statistique moyen à l'ordre 2 de l'ensemble des signatures possibles. Cette démarche inductive permet d'avoir à disposition un modèle d'autocorrélation et par conséquent un modèle moyen de matrice de variance covariance. L'avantage d'une telle approche est que le modèle reste valide pour toutes les signatures, il peut donc être calculé et stocké une fois pour toutes avant le début du traitement.
Une certaine subjectivité demeure alors concernant le choix du modèle, ce dernier ne devant pas être adapté à une signature particulière et devant approcher moyennement l'ensemble des signatures. Un modèle d'autocorrélation moyen est proposé par [Cou99], où dans l'étude citée

[26] C'est-à-dire la plus adaptée au sens d'un certain critère objectif
[27] Cette hypothèse sera vérifiée *a posteriori* lors de l'étude du masquage de signatures réelles

est utilisé un modèle paramétrique exponentiel décroissant défini par

$$r[k] \;:=\; e^{-\alpha|k|} \quad \forall k = -(N-1)\ldots(N-1), \tag{III.35}$$

où α est un paramètre réel strictement positif permettant de contrôler la taille du support.
Le choix d'un tel modèle est motivé par le fait qu'il approche l'autocorrélation d'un grand nombre de signaux de la physique.
Afin de déterminer α, deux solutions sont envisageables.

Détermination expérimentale du paramètre α
La première, expérimentale, consiste a ajuster manuellement le paramètre α avant le traitement à l'aide de réalisations disponibles de telle sorte que la représentation graphique du modèle d'autocorrélation défini par III.35 épouse au mieux celle de l'estimation de l'autocorrélation paramétrique définie par la relation III.34.
Concernant le signal étudié, $\alpha = 0,1$ conduit à un modèle d'autocorrélation visible sur la figure 14. Paramétré ainsi, le modèle s'approche bien de l'estimé sans pour autant le faire de façon optimale. Une spécificité de ce modèle est que seules les liaisons statistiques entre deux échantillons proches sont considérés.

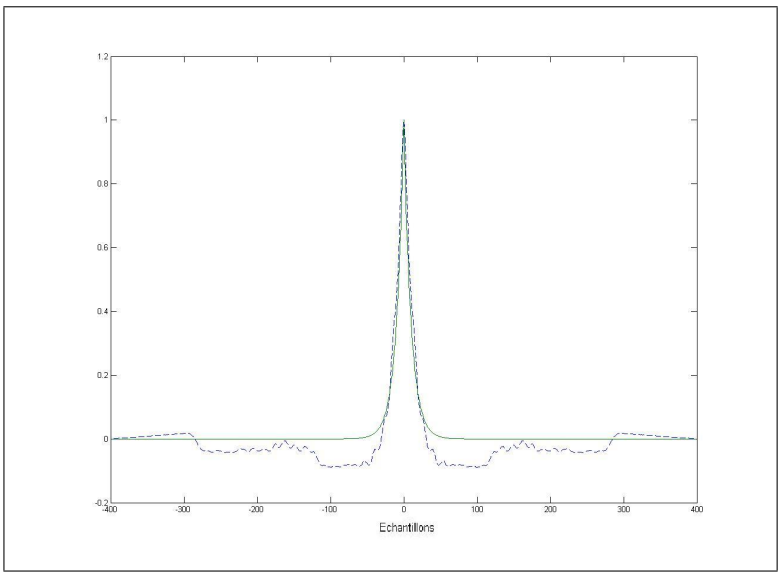


FIG. 14 – *Modèle paramétrique exponentiel de l'autocorrélation de l'observation avec $\alpha = 0,1$ en traits pleins superposé à l'estimation directe de cette dernière en traits pointillés*

En utilisant ce modèle, la technique de masquage proposée est appliquée au signal expérimental et le signal masqué correspondant est celui présenté sur la figure 15, montrant que le pic majeur d'activité n'est plus visible et qu'il n'y a que peu de similarités avec le signal expérimental original.

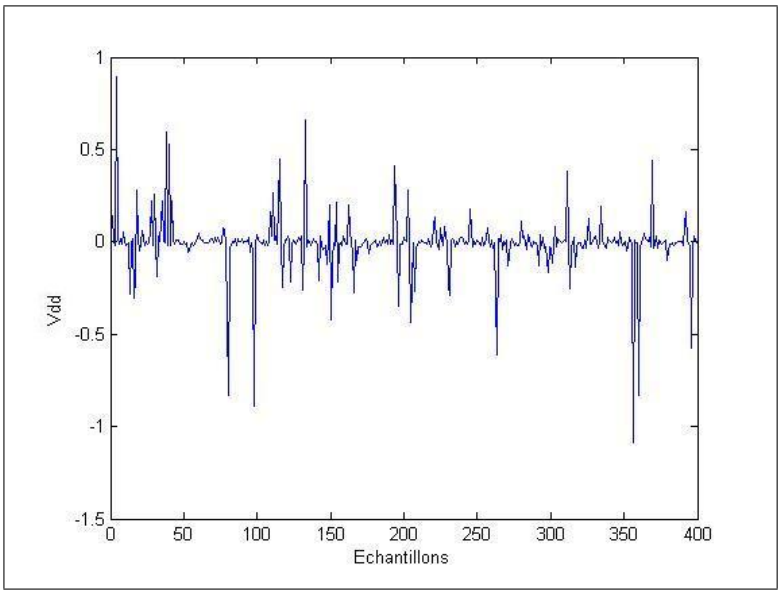
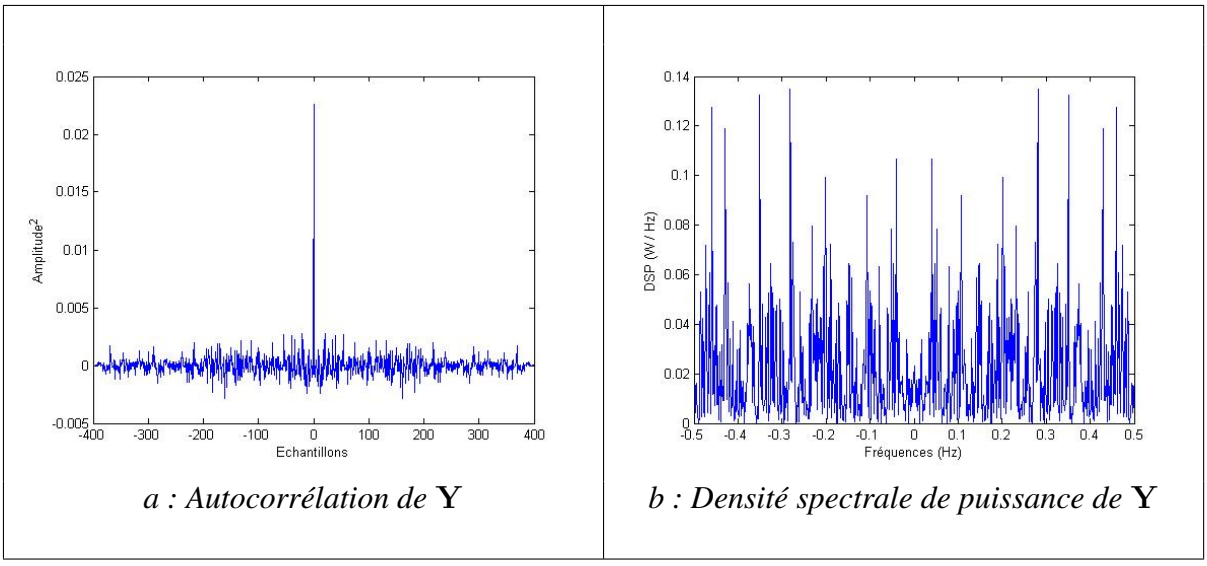


FIG. 15 – *Signal masqué* $\mathbf{Y}$

La figure 16 met en évidence les satisfaisantes propriétés statistiques de décorrélation à l'ordre 2 du signal masqué $\mathbf{Y}$ par le biais de son autocorrélation et de sa densité spectrale de puissance,



a : Autocorrélation de $\mathbf{Y}$ *b : Densité spectrale de puissance de* $\mathbf{Y}$

FIG. 16 – *Autocorrélation et densité spectrale de puissance du signal masqué* $\mathbf{Y}$

alors que sur la figure 17 un taux d'intercorrélation maximal d'environ $0,18$ en valeur absolue est relevé.

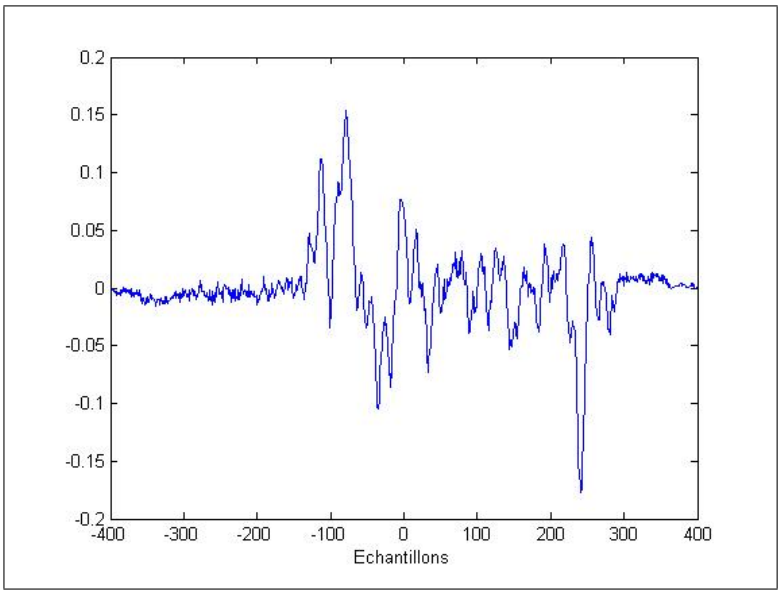


FIG. 17 – *Intercorrélation du signal masqué* $\mathbf{Y}$ *avec le signal natif* $\mathbf{Z}$

Il faut néanmoins signaler que la démarche consistant à déterminer le paramètre α manuellement à partir de la connaissance de plusieurs autocorrélations de réalisations disponibles va dans le sens de celle du pirate. En effet, ce dernier sur la base de différentes signatures qu'il possède va essayer par traitements statistiques appropriés telle que la DPA et l'ensemble de ses variantes, de déduire des tendances moyennes servant à interpréter le fonctionnement de la Smart Card. Ainsi, les résultats satisfaisant obtenus en masquant les signaux par décomposition avec la matrice de variance covariance de l'observation formée à partir du modèle paramétrique exponentiel amorti sont à nuancer car la démarche empirique utilisée pour déterminer le paramètre est la même que celle des pirates, ce qui laisse penser qu'il leur est relativement aisé dès lorsqu'ils ont une base de signatures à disposition de retrouver le modèle d'autocorrélation utilisé.

Détermination du paramètre α par le principe du maximum de vraisemblance
Dans la section précédente le paramètre α est déterminé manuellement, c'est-à-dire fixé dès lors qu'il est considéré comme acceptable au sens de l'interprétation humaine. Le but de cette partie est de déterminer α en le considérant comme la solution optimale au sens d'un critère objectif : le maximum de vraisemblance. L'observation $\mathbf{Z} = s + \mathbf{B}$ est telle que

$$\mathbf{Z} \hookrightarrow \mathcal{N}(s, \Gamma_{\mathrm{ZZ}}(\alpha)).$$

La matrice de variance covariance de l'observation $\Gamma_{\mathrm{ZZ}}(\alpha)$ est à présent paramétrée par α, paramètre scalaire réel . L'estimateur $\hat{\alpha}_{\mathrm{MLE}}$ va être calculé à partir de cette modélisation de l'observation. Or, cette dernière est valide pour une observation expérimentale comme celle servant de test aux techniques proposées[28]. Une telle démarche est effectivement optimale dans le cas où le signal d'intérêt s est connu. En revanche, pour la suite, dans le cadre de la modélisation des données réelles, le signal d'intérêt est vu comme un processus aléatoire qui sauf cas exceptionnel n'a aucune raison d'obéir à la même loi. En toute rigueur, l'estimateur construit n'est alors plus valide mais peut tout de même être vu comme une approximation automatique convenable du paramètre et ainsi engendrer un modèle moyen de matrice de variance covariance de l'observation. Cette erreur est assumée car la démarche s'inscrit dans le sens de la contrainte générale de sécurité imposée qui veut que les systèmes conçus ne soient pas efficaces sur une signature

[28] $\mathbf{Z} = s + \mathbf{B}$

spécifique, mais efficace pour un modèle moyen de signatures le plus général possible.
La suite de cette section traite de la détermination du paramètre $\hat{\alpha}_{\text{MLE}}$ maximisant la vraisemblance de l'observation expérimentale $\mathbf{Z}$.

Proposition III.9. *Soit* $\mathbf{Z}$ *un vecteur aléatoire de dimension* N *de réalisation le vecteur* Z. *Si* $\mathbf{Z} \hookrightarrow \mathcal{N}(0_N, \Gamma_{\text{ZZ}}(\alpha))$, *où* α *est un paramètre scalaire alors l'estimateur du maximum de vraisemblance* $\hat{\alpha}_{\text{MLE}}$ *est solution de l'équation*

$$\textit{Trace}\left[\Gamma_{\text{ZZ}}^{-1}(\alpha)\frac{d}{d\alpha}\left[\Gamma_{\text{ZZ}}(\alpha)\right]\Gamma_{\text{ZZ}}^{-1}(\alpha)\left(ZZ^T-\Gamma_{\text{ZZ}}(\alpha)\right)\right] \;=\; 0. \tag{III.36}$$

La preuve de la proposition est donnée par Kay [Kay93] page 185.
A partir de la structure matricielle III.33 et du modèle d'autocorrélation décrit par l'équation III.35, la matrice de variance covariance $\Gamma_{\text{ZZ}}(\alpha)$ a pour expression

$$\Gamma_{\text{ZZ}}(\alpha) \;=\; \begin{bmatrix} 1 & e^{-\alpha} & e^{-2\alpha} & \cdots & e^{-(N-1)\alpha} \\ e^{-\alpha} & 1 & e^{-\alpha} & \ddots & \vdots \\ e^{-2\alpha} & e^{-\alpha} & 1 & \ddots & e^{-2\alpha} \\ \vdots & \ddots & \ddots & \ddots & e^{-\alpha} \\ e^{-(N-1)\alpha} & \cdots & e^{-2\alpha} & e^{-\alpha} & 1 \end{bmatrix}$$

Le calcul du déterminant de $\Gamma_{\text{ZZ}}(\alpha)$ aboutit à deux expressions équivalentes,

$$\begin{aligned} det(\Gamma_{\text{ZZ}}(\alpha)) &= (1-e^{-2\alpha})^{N-1} \\ &= e^{-(\alpha+\ln(2))(N-1)}\sinh^{N-1}(\alpha), \end{aligned}$$

la première étant utile pour les calculs et la seconde permettant d'affirmer sans calculs, sous l'hypothèse $\alpha > 0$ que $det(\Gamma_{\text{ZZ}}(\alpha)) > 0$ et donc que $\Gamma_{\text{ZZ}}(\alpha)$ est régulière. L'expression de la matrice inverse est

$$\Gamma_{\text{ZZ}}^{-1}(\alpha) \;=\; \frac{1}{(1-e^{-2\alpha})}\begin{bmatrix} 1 & -e^{-\alpha} & & (0) & \\ -e^{-\alpha} & (1+e^{-2\alpha}) & -e^{-\alpha} & & \\ & \ddots & \ddots & \ddots & \\ & & -e^{-\alpha} & (1+e^{-2\alpha}) & -e^{-\alpha} \\ & (0) & & -e^{-\alpha} & 1 \end{bmatrix},$$

qui est une matrice tridiagonale[29].

De plus, $\Gamma_{\text{ZZ}}(\alpha)$ est constituée d'éléments infiniment dérivables, donc $\frac{d}{d\alpha}\left[\Gamma_{\text{ZZ}}(\alpha)\right]$ existe et son expression est

$$\frac{d}{d\alpha}\left[\Gamma_{\text{ZZ}}(\alpha)\right] \;=\; \begin{bmatrix} 0 & -e^{-\alpha} & -2e^{-2\alpha} & \cdots & -(N-1)e^{-(N-1)\alpha} \\ -e^{-\alpha} & 0 & -e^{-\alpha} & \ddots & \vdots \\ -2e^{-2\alpha} & -e^{-\alpha} & 0 & \ddots & -2e^{-2\alpha} \\ \vdots & \ddots & \ddots & \ddots & -e^{-\alpha} \\ -(N-1)e^{-(N-1)\alpha} & \cdots & -2e^{-2\alpha} & -e^{-\alpha} & 0 \end{bmatrix},$$

qui elle, est une matrice de Toeplitz.

[29] L'inverse d'une matrice de Toeplitz n'est en général pas une matrice tridiagonale, il s'agit là d'un cas particulier dû aux propriétés de la fonction exponentielle.

D'une part, le produit matriciel $\Gamma_{ZZ}^{-1}(\alpha)\frac{d}{d\alpha}\left[\Gamma_{ZZ}(\alpha)\right]\Gamma_{ZZ}^{-1}(\alpha)$ est une matrice tridiagonale d'expression

$$\Gamma_{ZZ}^{-1}(\alpha)\frac{d}{d\alpha}\left[\Gamma_{ZZ}(\alpha)\right]\Gamma_{ZZ}^{-1}(\alpha) \;=\; \frac{1}{(1-e^{-2\alpha})^2}\times$$

$$\begin{bmatrix} 2e^{-2\alpha} & -e^{-\alpha}(1+e^{-2\alpha}) & & & (0) \\ -e^{-\alpha}(1+e^{-2\alpha}) & 4e^{-2\alpha} & -e^{-\alpha}(1+e^{-2\alpha}) & & \\ & \ddots & \ddots & \ddots & \\ & & -e^{-\alpha}(1+e^{-2\alpha}) & 4e^{-2\alpha} & -e^{-\alpha}(1+e^{-2\alpha}) \\ (0) & & & -e^{-\alpha}(1+e^{-2\alpha}) & 2e^{-2\alpha} \end{bmatrix},$$

et d'autre part

$$ZZ^T - \Gamma_{ZZ}(\alpha) =$$

$$\begin{bmatrix} Z_1^2-1 & Z_1Z_2-e^{-\alpha} & Z_1Z_3-e^{-2\alpha} & \cdots & Z_1Z_N-e^{-(N-1)\alpha} \\ Z_2Z_1-e^{-\alpha} & Z_2^2-1 & Z_2Z_3-e^{-\alpha} & \ddots & \vdots \\ Z_3Z_1-e^{-2\alpha} & Z_3Z_2-e^{-\alpha} & Z_3^2-1 & \ddots & Z_3Z_N-e^{-2\alpha} \\ \vdots & \ddots & \ddots & \ddots & Z_{N-1}Z_N-e^{-\alpha} \\ Z_NZ_1-e^{-(N-1)\alpha} & \cdots & Z_NZ_{N-2}-e^{-2\alpha} & Z_NZ_{N-1}-e^{-\alpha} & Z_N^2-1 \end{bmatrix}.$$

L'étape suivante consiste à calculer la trace du produit de ces deux matrices,

$$\text{Trace}\left[\Gamma_{ZZ}^{-1}(\alpha)\frac{d}{d\alpha}\left[\Gamma_{ZZ}(\alpha)\right]\Gamma_{ZZ}^{-1}(\alpha)\left(ZZ^T-\Gamma_{ZZ}(\alpha)\right)\right] \;=\; \frac{1}{(1-e^{-2\alpha})^2}\times$$

$$\Big[2e^{-2\alpha}Z_1^2 - e^{-\alpha}Z_2Z_1 - e^{-3\alpha}Z_2Z_1 - e^{-2\alpha} + e^{-4\alpha}$$

$$+\sum_{i=2}^{N-1}[-e^{-\alpha}Z_{i-1}Z_i - e^{-3\alpha}Z_{i-1}Z_i + 4e^{-2\alpha}Z_i^2 - e^{-\alpha}Z_iZ_{i+1} - e^{-3\alpha}Z_iZ_{i+1} - 2e^{-2\alpha} + 2e^{-4\alpha}]$$

$$-e^{-\alpha}Z_{N-1}Z_N - e^{-3\alpha})Z_{N-1}Z_N + 2e^{-2\alpha}Z_N^2 - e^{-2\alpha} + e^{-4\alpha}\Big],$$

qui peut s'écrire, en factorisant l'expression par $2(N-1)e^{-\alpha}$

$$\text{Trace}\left[\Gamma_{ZZ}^{-1}(\alpha)\frac{d}{d\alpha}\left[\Gamma_{ZZ}(\alpha)\right]\Gamma_{ZZ}^{-1}(\alpha)\left(ZZ^T-\Gamma_{ZZ}(\alpha)\right)\right] \;=\; \frac{2(N-1)e^{-\alpha}}{(1-e^{-2\alpha})^2}\times$$

$$\Big[e^{-3\alpha} + \big(-1 + \frac{2}{N-1}\sum_{i=1}^{N} Z_i^2 - \frac{1}{N-1}(Z_1^2+Z_N^2)\big)e^{-\alpha}$$

$$-\big(\frac{1}{N-1}\sum_{i=1}^{N-1} Z_iZ_{i+1}\big) - \big(\frac{1}{N-1}\sum_{i=1}^{N-1} Z_iZ_{i+1}\big)e^{-2\alpha}\Big]$$

L'étape suivante consiste à annuler cette expression. Si l'on pose $x := e^{-\alpha}$ pour $\alpha > 0$, alors pour tout $x \in]0,1[$, $\alpha = -\ln(x)$, l'estimateur du maximum de vraisemblance $\hat{x}_{\text{MLE}}$ est solution du polynôme de degré 3

$$x^3 - ax^2 + bx - a = 0, \tag{III.37}$$

avec

$$\begin{cases} a := \dfrac{1}{N-1}\displaystyle\sum_{i=1}^{N-1} Z_i Z_{i+1} \\ b := \dfrac{2}{N-1}\displaystyle\sum_{i=1}^{N} Z_i^2 - \dfrac{1}{N-1}(Z_1^2 + Z_N^2) - 1 \end{cases}$$

Remarque : *Pour obtenir l'estimateur dans le cas où* $\mathbf{Z} \hookrightarrow \mathcal{N}(s, \Gamma_{\text{ZZ}}(\alpha))$*, il suffit de définir le changement de variable* $Z := Z - s$*.*

Ainsi, la détermination de l'estimateur se ramène à un problème de recherche des racines d'un polynôme de degré 3. Donc, 3 racines correspondant à 3 solutions potentielles sont déterminées, puis 3 solutions possibles pour $\hat{\alpha}_{\text{MLE}}$ qui correspondent à 3 modèles d'autocorrélation distincts. La solution retenue est celle dont le modèle d'autocorrélation construit à partir de cette dernière rend sa distance euclidienne avec l'autocorrélation des données estimée par III.35 minimale. Autrement dit la solution retenue est, parmi les trois racines possibles, celle qui engendre le modèle d'autocorrélation qui ressemble le plus à III.34.

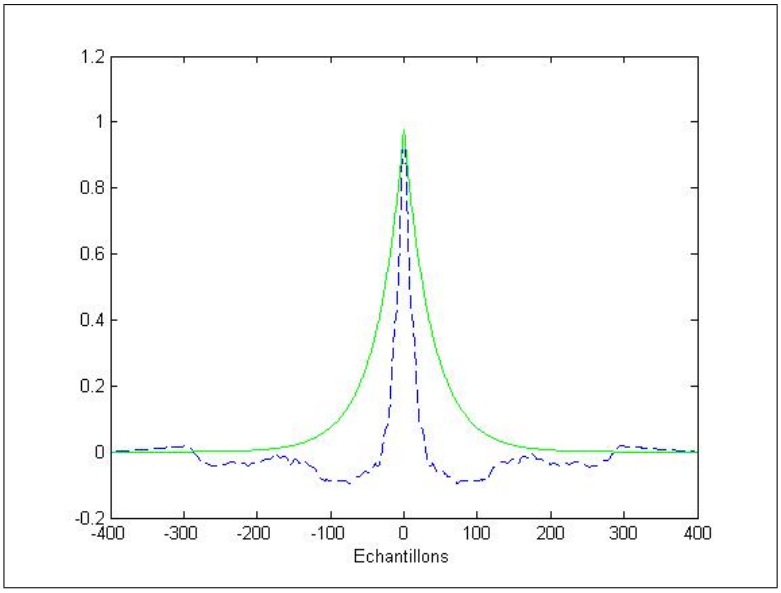


FIG. 18 – *Modèle exponentiel de l'autocorrélation de l'observation expérimentale avec* $\alpha = 0,027$ *en traits pleins superposé à l'estimation directe de cette dernière en traits pointillés*

Le paramètre est déterminé automatiquement par la méthode présentée ci-dessus avec l'observation expérimentale. Après calcul, il vient $\alpha = \hat{\alpha}_{\text{MLE}} \approx 0,027$, ce qui correspond à un choix cohérent comme l'atteste la figure 18.
Afin de quantifier les performances de l'estimateur, des simulations de Monté Carlo ont été effectuées afin d'évaluer la moyenne et la variance de l'estimateur. Il ressort de cette étude faite

avec 10000 tirages que $\mathbb{E}\left[\hat{\alpha}_{\text{MLE}}\right] = 0,027$ et $Var[\hat{\alpha}_{\text{MLE}}] = 10^{-6}$. Il faut cependant remarquer que la loi de l'observation ne correspond pas exactement à la loi utilisée pour déterminer $\hat{\alpha}_{\text{MLE}}$, cette erreur n'est pas rédhibitoire dans un contexte de masquage. En terme de robustesse de l'estimateur, il est intéressant de noter que plus la puissance du bruit augmente, meilleure est l'estimation, et inversement. En effet, dans le cas où la puissance du bruit σ_B^2 est beaucoup plus forte que celle du signal, l'observation expérimentale obtenue par addition du signal et du bruit se comporte comme s'il n'y avait en définitive que du bruit. Or, ici le bruit est gaussien centré de matrice de variance covariance $\sigma_B^2 \text{Id}_N$ alors que le paramètre est déterminé par le principe du maximum de vraisemblance selon l'hypothèse que l'observation est gaussienne centrée de matrice de variance covariance paramétrée. Donc, dans ce cas, la loi de l'observation est donc plus adaptée à la technique de détermination de l'estimateur. La technique de masquage est utilisée avec la matrice de variance covariance construite via le modèle d'autocorrélation exponentiel paramétré par $\alpha = 0,027$.
Il est également intéressant de comparer le gabarit des estimés construit à partir des paramètres déterminés manuellement et automatiquement à l'aide des figures 14 et 18. Le premier est efficace uniquement sur un temps de l'ordre du temps de cohérence de l'observation, alors qu'au contraire le modèle automatique n'est efficace qu'à partir du temps de cohérence.
Le signal masqué Y obtenu est celui présenté sur la figure 19. Le pic principal initialement présent est réparti sur l'ensemble des échantillons de l'observation et ceci à l'aide d'une technique entièrement automatisée.

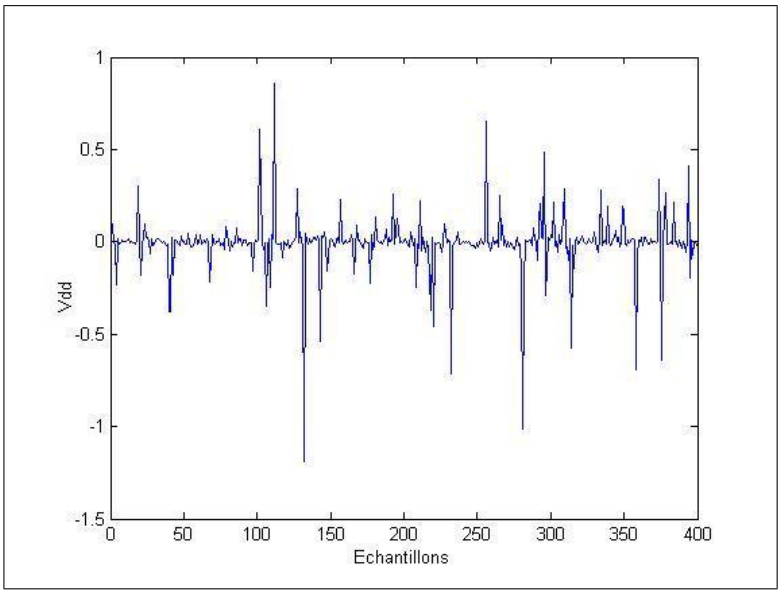
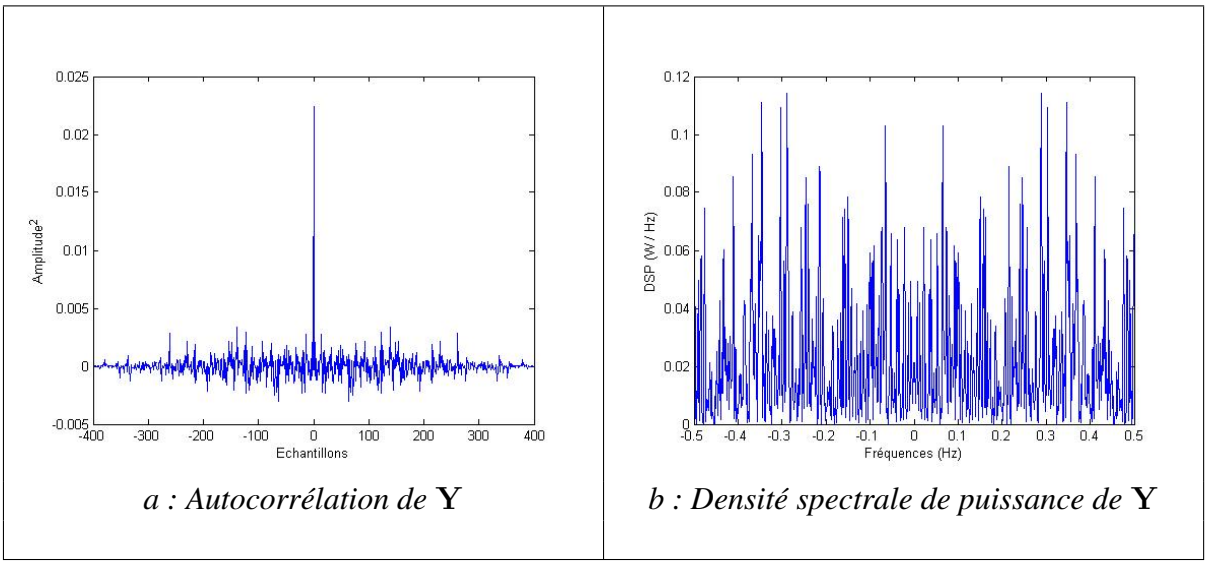


FIG. 19 – *Signal masqué* $\mathbf{Y}$

La figure 20 met en évidence les satisfaisantes propriétés statistiques de décorrélation à l'ordre 2 du signal masqué $\mathbf{Y}$ à travers l'interprétation de son autocorrélation et de sa large occupation fréquentielle à travers celle de sa densité spectrale de puissance.



a : Autocorrélation de $\mathbf{Y}$ *b : Densité spectrale de puissance de* $\mathbf{Y}$

FIG. 20 – *Autocorrélation et densité spectrale de puissance du signal masqué* $\mathbf{Y}$

L'intercorrélation normalisée de $\mathbf{Y}$ et $\mathbf{Z}$ présentée sur la figure 21 a une amplitude maximale d'environ $0,14$ en valeur absolue.

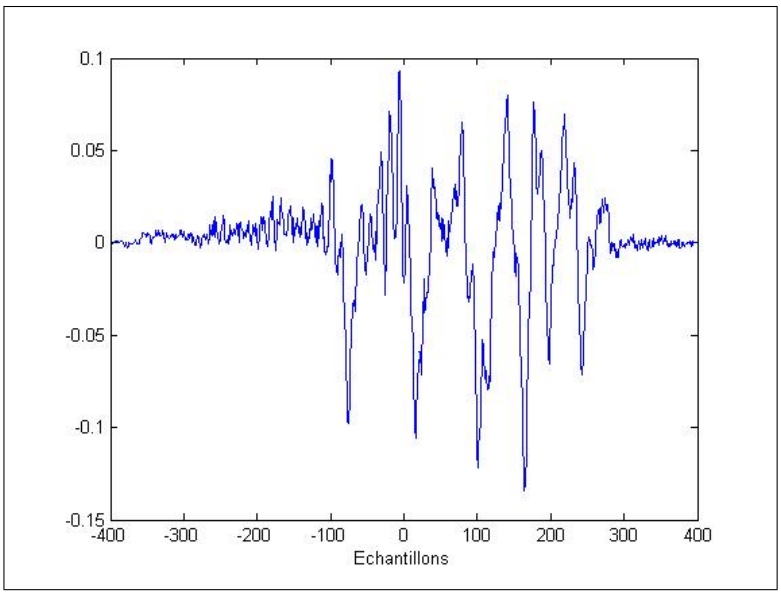


FIG. 21 – *Intercorrélation du signal masqué* $\mathbf{Y}$ *avec le signal natif* $\mathbf{Z}$

Bilan des deux approches

Toutes deux conduisent à la détermination d'un scalaire α qui permet de calibrer le modèle paramétrique d'autocorrélation de l'observation. La connaissance de ce dernier permet de construire le modèle de matrice de variance covariance correspondant. L'approche expérimentale est adaptée à la famille de signaux considérée[30] mais nécessite l'intervention humaine. Il faut alors, si la technologie change et donc si le gabarit des signatures change régler manuellement à nouveau le paramètre α. La démarche est en fait peu portable.

L'approche basée sur le principe du maximum de vraisemblance quant à elle s'adapte également

[30] En l'occurrence les signaux Smart Card

aux données à disposition. Le paramètre est déterminé automatiquement par une méthode élégante et en définitive simple.
Le modèle déterminé automatiquement est plus réaliste que celui déterminé manuellement car ce dernier tient compte des liaisons statistiques entre des echantillons éloignés. Cela dit, la modélisation utilisée pour valider l'expression de l'équation dont est solution l'estimateur est adaptée à des mesures expérimentales, l'est elle à des mesures réelles ?

6.4 Bilan des différentes approches proposées

Dans la section précédente, la technique de masquage d'un signal par substitution de ses échantillons par les coefficients de son développement de Karhunen-Loève a été présentée. Son principe est de remplacer les échantillons du signal d'observation par des coefficients décorrélés à l'ordre 2. Puis, dans cette section ont été présentées différentes approches permettant de la mettre en oeuvre. Les techniques présentées ont en commun un temps d'exécution d'environ une seconde lorsqu'exécutés sur une station de calcul équipée de deux processeurs cadencés à $3,6GHz$ chacun avec $3Go$ de mémoire vive[31]. Le taux moyen de corrélation maximum entre la signature originale et la signature masquée est voisin de 15%.
Elles présentent cependant des disparités en matière de coût de calculs, de quantité d'informations *a priori* à stocker et de robustesse aux attaques.
L'idée première fut de permuter les échantillons du signal. Intuitive, simple à mettre en oeuvre et donnant des résultats similaires a ceux obtenus avec des techniques plus élaborées, cette idée est à bannir car le pirate peut retrouver l'observation initiale en un nombre fini d'opérations et de manière exacte. Cependant, il est utile d'incorporer une étape de permutation aléatoire des échantillons à la fin de toute méthode de masquage, étape qui jouerait alors en quelque sorte le rôle de verrou.
Dans un second temps, le contexte était celui où les vecteurs de base de décomposition étaient connus. Dans ce cas, l'avantage est qu'il n'est pas nécessaire de résoudre l'équation aux valeurs propres dont les fonctions de base sont solutions, d'où une économie de calculs. En contrepartie, dès lors que les fonctions de bases sont connues du pirate, il est possible de retrouver la signature initiale, ce qui rend l'approche efficace mais perméable. L' idée suivante consistait à ne plus considérer connus les vecteurs de base, auquel cas il faut estimer la matrice de variance covariance dont ces derniers sont vecteurs propres. Estimer la matrice revient à estimer l'autocorrélation de l'observation, trois démarches ont été proposées. Il est possible d'estimer directement l'autocorrélation en construisant l'estimateur empirique de celle ci à partir des données. Dans ce cas rien n'est stocké avant le début du traitement, d'où une plus grande difficulté matérielle pour le pirate de revenir à l'observation. Or, cette technique est fortement adaptée au type de données que l'on traite dans le sens où à chaque observation va correspondre une matrice de variance covariance différente, alors qu'il a été posé en condition de concevoir des techniques générales, non propres à un type de signature donné. L'étape suivante consistait alors à déterminer la matrice de variance covariance à partir d'un modèle paramétrique général d'autocorrélation. Deux façons de déterminer le paramètre dont dépend l'autocorrélation de l'observation ont été proposées, soit manuellement auquel cas il faut stocker le paramètre, soit automatiquement selon le critère du maximum de vraisemblance auquel cas une étape de calculs supplémentaire est nécessaire. L'ensemble des résultats est présenté au tableau 9 sous forme comparative avec indiqué ce qui est spécifique à chaque technique en terme de stockage, de calculs et de maximum d' intercorrélation.

[31] Ceci est dû au fait que le nombre d'échantillons $N = 400$ est faible. Cependant, lors de l'étude de signaux de consommation de taille beaucoup plus grande, de fortes disparités de temps de calcul apparaîtront.

	A stocker	**A calculer**	**Maximum d'intercorrélation**
Permutations pseudo-aléatoires	-	Table de permutations	$0,16$
Base connue	Vecteurs de base	Table de permutations	$0,14$
Matrice estimée empiriquement	-	Estimation de l'autocorrélation Construction de la matrice Table de permutations	$0,20$
Matrice estimée par paramètre manuellement	Paramètre α Construction de la matrice	Table de permutations	$0,13$
Matrice estimée par paramètre automatiquement	-	Paramètre α Construction de la matrice Table de permutations	$0,13$

TAB. 9 – Bilan des performances des différentes techniques de masquage proposées

L'analyse du tableau 9 montre que le critère de l'intercorrélation, à lui seul, ne permet pas de créer de classement[32]. Il y a cependant un compromis à faire entre les performances en terme de décorrélation et la facilité pour le pirate de retrouver la signature, autrement dit un compromis performance/sécurité. Vu sous cette angle, c'est la dernière technique qui réalise le meilleur compromis. Cette logique est-elle respectée lors de l'étude des signaux réels ? Ceci est l'objet de la section suivante.

6.5 Expérimentations sur des signaux réels

Après avoir établi le bilan forces-faiblesses des différentes approches proposées et caractérisé leurs performances sur la base d'un signal expérimental, l'étape suivante consiste à appliquer la technique de masquage proposée à des signaux réels de consommation de courant.
Les signaux ont été fourni par ST Microelectronics et sont issus de la mesure par un oscilloscope de l'intensité de courant sur le noeud d'alimentation V_{dd} d'une Smart Card lorsque celle-ci effectue des opérations caractéristiques pouvant être intéressantes pour le pirate. Plus précisément, pour évaluer $I_{dd}(A)$ l'oscilloscope mesure par l'intermédiaire d'une résistance la tension $V_{dd}(V)$ et enlève la composante continue de cette dernière. Telle est la nature physique des observations disponibles qui peuvent être modélisées comme la réalisation d'un processus stochastique qui est la somme d'un signal utile $\mathbf{S}$ et d'un bruit $\mathbf{B}$,

$$\mathbf{Z} \quad = \quad \mathbf{S} + \mathbf{B},$$

tous deux sont des processus aléatoire stationnaires à l'ordre 2, l'observation est donc également vue comme un processus stochastique d'ordre 2. Cela doit être interprété dans le sens où si le processus n'est pas stationnaire à l'ordre 2, alors il est possible de le traiter par blocs à l'intérieur desquels la restriction de l'observation peut être considérée comme stationnaire à l'ordre 2.
L'objectif est de confirmer la qualité des résultats obtenus avec le signal expérimental au cours des sections précédentes notamment en terme de décorrélation à l'ordre 2 des échantillons du signal masqué.

[32]La diférence entre une intercorrélation maximale de $0,13$ et une intercorrélation maximale de $0,14$ est difficilement discernable

6.5.1 Pré-traitement des mesures

Les mesures fournies par ST Microelectronics ont été relevées sur un oscilloscope durant T secondes avec un pas d'échantillonnage $T_e = 0,1.10^{-6}\, sec$ donc une fréquence d'échantillonnage de $F_e = 10\, GHz$.
Les 11 signatures $\{Z_m\}_{m=0...10}$ mesurées sont centrées, puis analysées en fréquence par l'intermédiaire de leurs densités spectrale de puissance respectives.

Notion de ré-échantillonnage De cette analyse il ressort que toutes les signatures ont une faible occupation spectrale sur l'intervalle $[-\frac{F_e}{2}\,;\,\frac{F_e}{2}[\,=\,[-5\,;\,5[\,GHz$. Il est alors intéressant de sous-échantillonner les signatures disponibles, ceci pour deux raisons. Tout d'abord, l'opérateur de sous-échantillonnage se comporte comme un filtre passe bas de fréquence de coupure f_c et élimine donc les hautes fréquences parasites ; d'autre part il permet de réduire la taille des signaux tout en conservant l'information utile que ceux-ci véhiculent.
Pour toute signature la fréquence de coupure $f_c := \frac{k_c}{NT_e}$ est choisie de telle sorte que la puissance correspondant à la somme de la contribution de chaque échantillon du périodogramme dans l'intervalle $[-f_c\,;\,f_c[$ soit de l'ordre de $((1-\epsilon)\times 100)\,\%$ de la puissance totale du signal,

$$\forall \epsilon > 0 \quad \exists k_c \quad / \quad \left| \frac{1}{2N-1} \sum_{k=-k_c}^{k_c} |\gamma_{ZZ}[k]| - \frac{1}{N} \sum_{i=1}^{N} Z^2[i] \right| < \epsilon.$$

où $\gamma_{ZZ}[k]$ est la densité spectrale de puissance de $\mathbf{Z}$. Alors, il est possible de ré-échantillonner les signatures et ainsi réduire le nombre d'échantillons du signal d'un facteur η définit par

$$\begin{aligned} \eta &:= \frac{F_e}{2f_c} \\ &= \frac{F_e}{2}\frac{NT_e}{k_c} \\ &= \frac{N}{2k_c}, \end{aligned}$$

en d'autres termes de travailler avec des signaux de taille η fois plus petite tout en conservant l'information spectrale de chaque signature.
Cette technique a été appliquée à l'ensemble des 11 signatures avec un seuil de tolérance $\epsilon = 0,001$ correspondant à $99,9\%$ de la puissance totale. Les résultats sont présentés sur le tableau 10

	$T(\mu sec)$	N	$f_c(MHz)$	η	N_{SE}
Z_0	1	10002	615	8	1231
Z_1	0,2	2002	564	9	201
Z_2	0,5	5002	594	8	501
Z_3	50	500002	583	9	50001
Z_4	2	20002	597	8	2001
Z_5	5	50002	513	10	5001
Z_6	50	500002	510	10	50017
Z_7	2	20002	597	8	2001
Z_8	2	20002	518	10	2001
Z_9	2	20002	482	10	2001
Z_{10}	2	20002	454	11	2001

TAB. 10 – Sous échantillonnage des signatures

Pour les signatures Z_3 et Z_6, les techniques sont appliquées via un traitement par blocs de taille raisonnable, en effectuant la phase de permutation pseudo-aléatoire à la fin du traitement, après concaténation des blocs masqués. Différents tests ont montré qu'une taille de bloc de 1000 échantillons est compatible à la fois avec une taille assurant la stationnarité à l'ordre 2 sur chaque bloc et les capacités du matériel à disposition.

> ***Remarque :*** *ST Microelectronics préconise $f_c = 500\,MHz$, fréquence à laquelle correspond $\eta = 10$, ce choix n'engendre pas de perte d'information. La moyenne empirique des 11 fréquences de coupures du tableau 10 déterminées par la méthode présentée est de $548\,MHz$, il y a donc adéquation entre les résultats de la démarche algorithmique et la préconisation industrielle.*
> *La démarche est entièrement automatique*

En guise d'illustration, l'annexe G montre l'exemple du re-échantillonnage de la signature Z_0.

6.5.2 Masquage des signatures

Pour chacune des 5 techniques, les 11 représentations graphiques des signatures sont présentées en annexe H accompagnées de leur version masquée. Un test de contrôle sur la restitution de puissance est effectué, assurant ainsi que le signal masqué contient la même puissance que le signal natif. Les expérimentations ont été effectuées sur une station de calcul équipé d'un bi-processeur cadencé à $2 \times 3,6GHz$ avec $3Go$ de mémoire vive.

Interprétation Afin de donner une indication sur le temps de calcul associé à chaque technique, la signature Z_6 a été retenue car celle-ci est la plus volumineuse et comme il a été dit plus haut nécessite pour être traitée dans son intégralité un découpage par blocs. Il s'agit donc ici des temps de calcul dans le cas le pire.

	Permutation aléatoire	Base connue	Matrice estimée empiriquement	Matrice estimée par paramètre manuellement	Matrice estimée par paramètre automatiquement
Temps CPU (sec)	$0,4$	10	417	331	2098

TAB. 12 – Temps de calcul associés à la signature Z_6

Il apparaît de façon logique que le temps de calcul augmente crescendo au fur et à mesure que la complexité des techniques augmente. L'opération la plus lourde est celle de recherche des éléments propres, celle-ci ayant lieu dans les trois dernières techniques proposées et faisant ainsi grimper de façon fulgurante les temps d'exécution. De plus, les méthodes les plus sécurisées sont les plus lentes, alors que les plus rapides sont les plus vulnérables. Le signal Z_6 a été traité par blocs de taille 1000 échantillons, travailler avec une taille de blocs plus petite semble être une solution mais dans le cas d'une telle démarche il ne faudrait pas oublier d'étudier les répercutions sur la qualité du masquage.

Synthèse récapitulative En guise de synthèse, le tableau 13 indique le maximum d'intercorrélation arrondi à 10^{-2}, pour chaque technique et pour chaque signature. Il est rappelé que les signatures Z_3 et Z_6, en raison de leur taille importante, ont été traitées par blocs de 1000 échantillons.

	Permutation aléatoire	Base connue	Matrice estimée empiriquement	Matrice estimée par paramètre manuellement	Matrice estimée par paramètre automatiquement
Z_0	$0,08$	$0,10$	$0,1$	$0,09$	$0,09$
Z_1	$0,19$	$\mathbf{0,23}$	$0,22$	$0,16$	$0,17$
Z_2	$0,11$	$0,10$	$0,12$	$0,12$	$0,14$
Z_3	$0,02$	$0,02$	$0,02$	$\mathbf{0,01}$	$0,02$
Z_4	$0,06$	$0,06$	$0,08$	$0,07$	$0,06$
Z_5	$0,05$	$0,05$	$0,05$	$0,05$	$0,05$
Z_6	$0,02$	$0,02$	$0,02$	$0,02$	$0,02$
Z_7	$0,06$	$0,07$	$0,07$	$0,06$	$0,07$
Z_8	$0,06$	$0,09$	$0,07$	$0,07$	$0,08$
Z_9	$0,08$	$0,07$	$0,06$	$0,08$	$0,06$
Z_{10}	$0,08$	$0,07$	$0,09$	$0,08$	$0,07$

TAB. 13 – Maximum d'intercorrélation de chaque $\{Z_i\}_{i=0...10}$ avec $\{Y_i\}_{i=0...10}$ pour chaque technique. Le meilleur et le moins bon score sont affichés en caractères gras.

La première impression est la satisfaction du fait que les scores présentés sont environ 7 fois meilleurs que ceux obtenus avec l'observation expérimentale. Cela dit, en comparant les résultats plutôt moyens obtenus avec la signature Z_1 avec ceux très bons de la signature Z_3 il semble que la taille des observations soit un facteur important ayant une conséquence directe sur la qualité du masquage. En effet, Z_1 fait partie des plus petites signatures à disposition alors que Z_3 fait partie des plus grandes. La confrontation aux données réelles des techniques développées dans ce chapitre valide leur efficacité, mais pointe le fait que cette efficacité est directement liée à la taille des observations traitées. Une extension de l'étude consisterai alors à évaluer les performances sur des intervalle de temps plus court.

7 CONCLUSION

Ce chapitre traite du masquage par décomposition des signaux et de l'application de ce type de techniques au masquage de signaux de consommation de Smart Card.
L'observation, qui est le signal à masquer, est modélisée par un processus stochastique, de même que le signal obtenu après traitement, le signal masqué. Voilà pourquoi en premier lieu il était nécessaire de définir la classe à laquelle appartiennent ces signaux, en l'occurrence celle des processus aléatoires réels à réalisations de carré sommable et pour tout temps de second moment fini. Ces signaux appartenant à un espace hilbertien, il est donc possible de les décomposer sur une base hilbertienne de fonctions. Plus précisément, la décomposition peut avoir lieu soit au sens du produit scalaire des fonctions de carré sommable[33], soit au sens du produit scalaire des variables aléatoires de second moment fini[34]. Le choix d'une base de décomposition orthonormale conduit au développement de Karhunen-Loève, assurant que les coefficients de décomposition sont statistiquement décorrélés à l'ordre 2. Alors, il serait possible à partir de n'importe quelle observation admissible de construire à l'aide de ces coefficients une suite blanche qui viendrait se substituer aux échantillons de l'observation, tel est le principe général de la technique de masquage présentée ici. Les fonctions servant au calcul des coefficients sont

[33]Pour tout f et g réelles de carré sommable sur D, $\langle f\,;\,g\rangle = \int_D f(t)g(t)\,dt$

[34]Pour toute variable aléatoire $\mathbf{X}$ et $\mathbf{Y}$ réelles de second moment fini $\mathbb{E}\left[\mathbf{XY}\right] = \int_D xy\,dP(\Omega)$

déterminées comme étant solution d'une équation intégrale de Fredholm linéaire homogène de seconde espèce de noyau la fonction d'autocorrélation de l'observation, comme le noyau est de carré sommable, résoudre cette équation intégrale est équivalent à déterminer les éléments propres d'un opérateur compact autoadjoint de Hilbert-Schmidt. Se placer sous ce point de vue permet de déduire l'existence et l'unicité des fonctions de base et donc de donner la légitimité qui est la sienne au développement de Karhunen-Loève. Ce développement s'avère être particulièrement adapté aux observations qui sont la somme d'un signal et d'un bruit blanc car dans ce cas, l'influence du bruit n'apparaît pas dans la détermination des fonctions de base. Ceci a permis de mettre en évidence le défaut de sécurité des techniques de masquage basées sur l'ajout de bruit à corrélations microscopiques. Une fois cette précision faite, le calcul des moments du signal masqué montre que si le signal natif est centré avec une certaine puissance, alors le signal masqué est également centré de même puissance. Cela signifie que la technique de masquage par décomposition des signaux conserve la puissance, ce qui est une contrainte majeure imposée par la physique du problème.
L'ensemble des résultats est établi dans des espaces continus donc de dimension infinie et pour certains même au sens des distributions. De façon à proposer une solution toute analogique que les microélectroniciens pourraient implémenter, une technique d'approximation de la distribution de Dirac par une suite de fonctions fut proposée, mais celle-ci oblige à travailler avec des signaux de trop forte amplitude pour être réalisable. Une implémentation brutale de la technique proposée ne peut être effective qu'une fois réalisée l'étape passant de signaux à valeurs dans des espaces continus vers des signaux discrets, et c'est ainsi que le pendant discret de la technique fut présenté, en s'assurant en particulier qu'il y a toujours conservation de la puissance moyenne avant et après masquage. L'application de la technique de masquage par décomposition des signaux d'une observation dans le cas des signaux discrets peut être menée à bien par différents chemins. Tout d'abord, l'observation est stationnaire à l'ordre 2, les vecteurs propres peuvent donc être connus *a priori*. Dans le cas contraire, ils sont déterminés comme étant les vecteurs propres de la matrice de variance covariance de l'observation qui peut soit être déterminée empiriquement soit déterminée paramétriquement, paramètre qui lui peut être calculé manuellement ou automatiquement au sens du maximum de vraisemblance. A l'étude de ces quatre techniques il faut ajouter la plus intuitive d'entre elles qui consiste à permuter aléatoirement les échantillons de l'observation. Bien que présentant un trop grand risque de sécurité utilisée seule, elle convient parfaitement pour jouer le rôle de verrou utilisé en aval des traitements et ainsi augmenter la difficulté pour le pirate de remonter à la signature originale. Ces quatre différentes façons d'implémenter la technique de masquage par décomposition sont ainsi toutes terminées par une étape de permutation aléatoire des coefficients calculés. Dans le cadre d'une éventuelle implémentation électronique, l'opération de permutation aléatoire nécessite d'avoir à disposition un générateur pseudo-aléatoire efficace.
La suite du chapitre, consacrée à l'exposé de la phase d'expérimentation consiste en l'analyse d'une observation expérimentale réelle issue du macro modèle de la Thèse de Kussner [Kus02], permettant de quantifier les performances de masquage des quatre techniques en terme de décorrélation à l'ordre 2 et de dispersion de la puissance instantanée sur l'ensemble d'étude tout en conservant la puissance moyenne constante.
Enfin, pour chaque technique l'intercorrélation du signal original avec le signal masqué à été estimée et son maximum relevé afin de mesurer statistiquement la ressemblance entre les signaux. Les résultats obtenus relativement à ces critères sont bons, de maximums d'intercorrélation stabilisés autour de 15% si bien qu'il est difficile de les discriminer à ce stade. Cependant la prise en compte des critères de stockage mémoire, de volumes de calculs et de résistance aux attaques permet de dire que les méthodes les plus rapides ou demandant le moins de stockage d'informations sont les plus vulnérables, alors que les plus lourdes à mettre en oeuvre sont les

plus efficaces. Dans un second temps, les techniques ont été confrontées aux données réelles, des signaux de consommation de Smart Card fournies par ST Microelectronics. Ces signatures de taille beaucoup plus importante que celle du signal expérimental même après une étape de sous-échantillonnage permirent de valider les résultats obtenus précédemment avec des taux d'intercorrélation de l'ordre de 5%, jusqu'a 1%. Ainsi, choisir une de ces technique revient à réaliser un compromis basé sur les critères de la performance, du temps de calcul, du volume de donner à stocker et de la résistance aux attaques.
ST Microelectronics a été attentive à cette étude et intéressée par les résultats obtenus. Cependant, les contraintes de faisabilité sont à ce jour encore trop importantes pour envisager une implémentation sur carte. Cela n'exclut donc rien pour le futur, par exemple la technique où les fonctions de bases sont connues pourrait porter non plus sur une base de fonctions circulaires mais sur une base d'ondelettes facilement implémentable sous forme de filtre. Concernant la technique où la matrice de variance covariance dépend d'un paramètre, une idée serait de déterminer ce dernier par un tirage aléatoire, cela aurait pour conséquence de faire diminuer le taux d'intercorrélation et d'augmenter la résistance aux attaques puisque la matrice change à chaque nouveau masquage. Enfin, il pourrait être intéressant de développer des techniques de masquage par décomposition basées sur des variantes du développement de Karhunen-Loève comme par exemple celui de type Wavelet Karhunen-Loève proposé par Starck [Sta01] ou encore d'utiliser l'approche Fast Karhunen-Loève [Jai76] combinée aux techniques existantes pour accélérer le temps d'exécution.
Par ailleurs, une extension naturelle de la technique consisterait à ne plus seulement exiger la décorrélation des moments d'ordre 2 mais également celle des moments d'ordre supérieur, en vue d'augmenter le niveau de sécurité du masquage.
En définitive, ce chapitre d'achève sur la conclusion que la technique de masquage par décomposition donne de bons résultats en terme de traitement du signal, mais pas exploitable pour l'instant par les électroniciens dans le cadre d'une application Smart Card, ceci pour deux raisons et non des moindres : les déclinaisons de la technique réalisant les meilleurs compromis sécurité/performances sont celles dont le nombre de données à stocker est le plus important, ou bien de temps d'exécution le plus long. De plus, les produits scalaires réalisés sur l'observation sont irréalisables au regard des technologies de conception actuelles.
Une nouvelle approche peut consister en le développement d'une contre mesure qui aurait pour vocation de compenser la consommation du circuit que l'on cherche à masquer. Pour mener à bien une telle approche, des paramètres caractéristiques de la signature à masquer doivent être extraits de cette dernière. Une réponse à ce problème fait l'objet du chapitre suivant.

CHAPITRE IV

MASQUAGE DE SIGNAL PAR UTILISATION DU FILTRAGE ADAPTÉ STOCHASTIQUE ET DE L'ALGORITHME EXPECTATION-MAXIMISATION

1 INTRODUCTION

Le but de ce chapitre est de développer une technique de masquage de consommation de courant basée sur l'estimation paramétrique des signaux par l'intermédiaire de l'algorithme Expectation-Maximisation et du filtrage adapté stochastique. Cette approche se démarque des techniques proposées au chapitre *III* dans la mesure où elle prend en compte la modélisation de l'observation par des considérations issues de la physique du problème aboutissant à un modèle paramétrique de signal, alors que le masquage par décomposition des signaux est une approche non-paramétrique aveugle. L'étude s'inscrit donc dans une démarche fondamentalement différente, où l'observation est vue comme le mélange de la consommation effective, dépendant de paramètres caractéristiques, et d'un bruit de mesure supposé gaussien. De plus, là où le masquage par substitution consiste à remplacer les échantillons de l'observation par ceux d'une suite blanche, le but ici est d'estimer l'activité de courant par l'intermédiaire de ses paramètres, puis, d'après la connaissance de cet estimé à appliquer une contre mesure appropriée sur la consommation, afin de masquer l'activité tout en conservant sa puissance.
D'après les conclusions du chapitre *III*, la technique de masquage par substitution donne des résultats satisfaisants mais souffre de deux maux venant nuancer l'appréciation de cette dernière. Tout d'abord, il est possible selon la déclinaison choisie de retrouver la signature initiale en un temps acceptable. D'ailleurs, ce temps peut nettement se raccourcir en cas de défaillance du générateur pseudo-aléatoire réalisant les permutations finales. De plus, la technique n'est pas encore électroniquement implémentable, ce qui suggère une prise en compte encore plus importante de cet aspect, sans pour autant se brider l'esprit en refusant d'explorer certaines parties du Traitement du Signal sous prétexte qu'elles ne seraient pas réalisables.
Cette technique de masquage s'apparente à une technique de piratage puisqu'elle cherche, à partir de l'observation disponible, à retrouver des informations caractéristiques du fonctionnement du dispositif, ce qui n'est rien d'autre que de la rétro-ingénierie
En effet, dans le cadre d'attaques en puissance[1], le pirate désire, à partir de relevés de consommation déduire des informations relatives au fonctionnement de la carte par identification de motifs caractéristiques. Fort de cette idée, une solution de masquage consiste à estimer l'acti-

[1] Telles que la DPA et ses variantes.

vité, puis à appliquer à la consommation une correction conséquente, de sorte à la répartir au mieux et ainsi masquer les fuites de courant.
Par conséquent, ce chapitre s'intéresse au problème de l'estimation paramétrique d'une activité de courant. L'étude est menée dans sa globalité, du choix automatique de la condition initiale de l'algorithme calculant l'estimateur, aux performances optimales de l'estimateur choisi.
Ce chapitre débute par la modélisation mathématique du problème, basée sur des travaux de micro-électroniciens. L'étape s'achève par la donnée de l'équation de mesure associée à l'observation, basée sur un modèle de signal paramétrique.
Puis, en préambule de la phase d'estimation, le gradient et le hessien du modèle sont calculés, ainsi que les expressions utiles pour la suite découlant de ces deux quantités.
Dans un troisième temps, il sera montré que la question du choix de la condition initiale dans l'algorithme d'optimisation utilisé pour estimer les paramètres du modèle est primordiale, d'où la nécessité d'une technique de détection utilisée en amant de la chaîne de traitement, permettant de fournir un jeu de conditions initiales pertinentes à la routine d'optimisation. La technique de détection est construite via la théorie du filtrage adapté stochastique (FAS) présentée dans son ensemble dans [Cav93, CouHDR05].
Vient ensuite la partie du chapitre concernant l'estimation paramétrique de l'activité de courant selon le cirière du maximum de vraisemblance. A cause de la non-convexité de la fonction coût, les techniques d'optimisation classiques ne fonctionnent pas, il faut donc un algorithme adapté à la forme du modèle, d'où le choix de l'algorithme expectation-maximisation (EM) [Bil98], dont le principe est exposé accompagné de l'étude de ses performances.
Enfin, en guise d'expérimentation, l'ensemble (FAS-EM) est utilisé pour estimer des signatures issues du macro-modèle de Kussener et une consommation réelle.

2 MODÉLISATION MATHÉMATIQUE DU PROBLÈME

D'après les travaux de Kussener [Kus02] et de Oswald et al.[Osw05], le modèle paramétrique de consommation peut être vu comme la superposition d'activités de cellules élémentaires se déclenchant au cours d'une période d'horloge. En effet, Kussener a montré que le microprocesseur est un bloc majoritairement numérique dont on peut simplifier la structure en un ensemble de portes logiques élémentaires telles que des portes NAND, NOR. L'ensemble des transistors en séries est ramené à un seul transistor équivalent. De même, l'ensemble des transistors en parallèle se simplifie à un unique transistor, il est alors possible de dire qu'un ensemble de porte logiques élémentaires peut se mettre sous la forme d'un ensemble de portes inverseurs. Il s'agit d'une approche macromodèle, qui va être reprise ici pour légitimer le modèle paramétrique de signal utile choisi, en l'occurrence une superposition de signaux élémentaires.
Le courant est relevé sur un intervalle de temps $[0; T]$, où T est la durée d'observation.
Par construction, le signal utile, à savoir l'activité de courant, est vue comme la somme de contributions élémentaires issues de l'activité de cellules.
Une cellule est un ensemble d'inverseurs réalisant une activité élémentaire. Chaque cellule est caractérisée par trois données physiques :

- son amplitude A (A),
- σ (sec), un paramètre proportionnel à l'occupation temporelle de la cellule,
- son instant de déclenchement m (sec).

La donnée d'un triplet de ces valeurs est riche en informations. L'amplitude renseigne sur l'activité du dispositif qui a consommé une telle quantité de courant, $A \in]0\,;\, A_{Max}]$ où A_{Max} est le maximum de consommation possible, caractéristique de la technologie utilisée.
De même σ est caractéristique de la technologie CMOS utilisée. S'agissant d'une quantité représentative du support de l'observation, l'hypothèse est faite que la cellule ne peut pas avoir un

support temporel plus grand que l'intervalle d'observation, ainsi $\sigma \in]0\,;\,\sigma_{max}]$.
Enfin, la localisation temporelle de l'instant de déclenchement est directement liée à l'horloge cadençant le dispositif dont la consommation est observée. Celle-ci ayant lieu sur l'intervalle d'observation, $m \in [0\,;\,T_{max}]$.
Ainsi, l'hypothèse est faite que la donnée du triplet $[A\,;\,\sigma\,;\,m]$ est suffisante pour caractériser une cellule. Ce triplet va être vu comme un jeu de paramètres servant à définir un modèle analytique de signal.

2.1 Définition du modèle

Soit D un sous-ensemble de $\mathbb{R}^3_+$ tel que

$$D =]0\,;\,A_{max}] \times]0\,;\,\sigma_{max}] \times [0\,;\,T_{max}],$$

et soit

$$\theta := [A\,;\,\sigma\,;\,m]^T \in D.$$

$D \subset \mathbb{R}^3_+$ est l'ensemble admissible des paramètres du modèle.
Le choix du type de modèle analytique est large, mais il faut cependant garder à l'esprit que le modèle doit "ressembler" à l'observation et doit être cohérent avec le choix des paramètres. De plus, il doit être suffisamment régulier pour éviter tout problème de singularité inhérent au modèle. Tenant en compte cela, le choix se porte vers un modèle paramétrique de signal, de la famille de fonctions gaussiennes, appelée ici $s_k(t)$ définie pour tout $k = 1 \dots K$ par

$$s_k := \left\{ \begin{array}{ccc} [0;T] \times D & \rightarrow & \mathbb{R} \\ \\ (t, \theta_k) & \mapsto & s_k(t, \theta_k) = A_k e^{-\frac{1}{2}\left(\frac{t - m_k}{\sigma_k}\right)^2} \end{array} \right. \tag{IV.1}$$

Ce modèle est inspiré de la densité de probabilité gaussienne et de son aspect universel. A_k a une influence directe sur la dynamique du signal, σ_k sur son support temporel et m_k sur son instant d'apparition. Toute fonction $s_k(t, \theta_k)$ est infiniment dérivable sur $[0; T] \times D$, ce qui leur confère une très forte régularité. Cette propriété est importante pour la phase d'estimation section 6 et légitime l'existence et la continuité du gradient et du hessien de $s_k(t, \theta_k)$.
Le signal utile est vu comme la consommation d'une superposition de K cellules élémentaires [Osw05], soit $\{s_k(t, \theta_k)\}_{k=1\dots K}$ avec

$$\theta_k := [A_k\,;\,\sigma_k\,;\,m_k]^T,$$

il a donc pour expression analytique

$$s := \left\{ \begin{array}{ccc} [0;T] \times D^K & \rightarrow & \mathbb{R} \\ \\ (t, \theta) & \mapsto & s(t, \theta) = \displaystyle\sum_{k=1}^{K} s_k(t; \theta_k) \end{array} \right. , \tag{IV.2}$$

où le vecteur θ de dimension $3K$ est construit tel que

$$\theta := [\theta_1\,;\,\dots\,;\,\theta_K]^T.$$

L'observation est modélisée par le mélange additif du signal utile paramétrique $s(t, \theta)$ avec un bruit $\mathbf{B}(t)$, processus aléatoire gaussien, centré, de variance σ_B^2,

$$\mathbf{Z}(t) = s(t, \theta) + \mathbf{B}(t).$$

2.2 Gradients et hessiens de $s_k(t,\theta)$ et $s(t,\theta)$

Pour la suite de l'étude, il sera utile d'avoir à disposition les expressions du gradient et du hessien du signal utile.
Pour tout $k = 1 \dots K$, $s(t,\theta)$ a la propriété d'être infiniment différentiable par rapport à θ car c'est une somme de signaux $s_k(t;\theta_k)$ tous $C^\infty(D,\mathbb{R}^+)$. Ainsi, le gradient de $s(t,\theta)$, à savoir $\nabla_\theta[s(t,\theta)]$ ainsi que son Hessien $H_\theta[s(t,\theta)]$, respectivement opérateurs différentiels linéaires d'ordre 1 et 2 ont un sens. De plus, comme $\mathcal{C}^2(D,\mathbb{R}^+) \subset \mathcal{C}^\infty(D,\mathbb{R}^+)$ d'après le théorème de Schwartz les dérivées secondes du Hessien commutent. Fort de cette remarque et en appliquant les règles de dérivation relatives à la composition des fonctions et à la fonction exponentielle, il vient avec k fixé

$$\nabla_{\theta_k}[s_k(t,\theta_k)] = s_k(t,\theta_k) \cdot \begin{bmatrix} 1/A_k \\ \dfrac{(t-m_k)^2}{\sigma_k^3} \\ \dfrac{(t-m_k)}{\sigma_k^2} \end{bmatrix} \tag{IV.3}$$

où $\nabla_{\theta_k}[s_k(t,\theta_k)]$ est un vecteur de dimension 3, puis le calcul des dérivées secondes donne

$$H_{\theta_k}[s_k(t,\theta_k)] = s_k(t,\theta_k)\cdot \begin{bmatrix} 0 & \dfrac{(t-m_k)^2}{A_k\sigma_k^3} & \dfrac{t-m_k}{A_k\sigma_k^2} \\ \dfrac{(t-m_k)^2}{A_k\sigma_k^3} & \big((t-m_k)^2-3\sigma_k^2\big)\dfrac{(t-m_k)^2}{\sigma_k^6} & \big((t-m_k)^2-2\sigma_k^2\big)\dfrac{(t-m_k)}{\sigma_k^5} \\ \dfrac{t-m_k}{A_k\sigma_k^2} & \big((t-m_k)^2-2\sigma_k^2\big)\dfrac{(t-m_k)}{\sigma_k^5} & \big((t-m_k)^2-\sigma_k^2\big)\dfrac{1}{\sigma_k^4} \end{bmatrix},$$

matrice hessienne de $s_k(t,\theta_k)$, symétrique, de dimension $(3,3)$.

Proposition IV.1. *La matrice $H_{\theta_k}[s_k(t,\theta_k)]$ est singulière pour tout θ_k.*

Preuve . *Le déterminant de la matrice est calculé suivant la première ligne[2], ce qui donne*

$$\begin{aligned}
det(H_{\theta_k}[s_k(t,\theta_k)]) &= s_k^3(t,\theta_k)\Big[\\
&\quad -\frac{(t-m_k)^2}{A_k\sigma_k^3}\Big(\frac{(t-m_k)^2}{A_k\sigma_k^3}\big((t-m_k)^2-\sigma_k^2\big)\frac{1}{\sigma_k^4} \\
&\quad -\big((t-m_k)^2-2\sigma_k^2\big)\frac{(t-m_k)}{\sigma_k^5}\frac{(t-m_k)}{A_k\sigma_k^2}\Big) \\
&\quad +\frac{(t-m_k)}{A_k\sigma_k^2}\Big(\frac{(t-m_k)^2}{A_k\sigma_k^3}\big((t-m_k)^2-2\sigma_k^2\big)\frac{(t-m_k)}{\sigma_k^5} \\
&\quad -\big((t-m_k)^2-3\sigma_k^2\big)\frac{(t-m_k)^2}{\sigma_k^6}\frac{(t-m_k)}{A_k\sigma_k^2}\Big) \quad \Big] \\
&= s_k^3(t,\theta_k)\Big[\quad -\frac{(t-m_k)^2}{A_k\sigma_k^3}\frac{(t-m_k)^2}{A_k\sigma_k^7}\Big(\big((t-m_k)^2-\sigma_k^2\big)-\big((t-m_k)^2-2\sigma_k^2\big) \\
&\quad +\frac{(t-m_k)}{A_k\sigma_k^2}\frac{(t-m_k)^3}{A_k\sigma_k^8}\Big(\big((t-m_k)^2-2\sigma_k^2\big)-\big((t-m_k)^2-3\sigma_k^2\big) \quad \Big] \\
&= s_k^3(t,\theta_k)\Big[-\frac{(t-m_k)^4}{A_k^2\sigma_k^8}+\frac{(t-m_k)^4}{A_k^2\sigma_k^8}\Big] \\
&= 0
\end{aligned}$$

[2] ou indifféremment suivant la première colonne

□

Ainsi, les expressions de $\nabla_\theta[s(t,\theta)]$ et $H_\theta[s(t,\theta)]$ respectivement de dimension $(3K,1)$ et $(3K,3K)$, se déduisent facilement de celles de $\nabla_{\theta_k}[s_k(t,\theta_k)]$ et $H_{\theta_k}[s_k(t,\theta_k)]$, quant à eux de dimension $(3,1)$ et $(3,3)$:
d'une part,

$$\nabla_\theta[s(t,\theta)] = \begin{bmatrix} \nabla_\theta[s_1(t,\theta_1)] \\ \vdots \\ \nabla_\theta[s_K(t,\theta_K)] \end{bmatrix}$$

et d'autre part, le hessien de $s(t,\theta)$ à la structure d'une matrice diagonale par blocs,

$$H_\theta[s(t,\theta)] = \begin{bmatrix} H_\theta[s_1(t,\theta_1)] & & (0) \\ & \ddots & \\ (0) & & H_\theta[s_K(t,\theta_K)] \end{bmatrix}.$$

$H_\theta[s(t,\theta)]$ est également une matrice singulière.

3 TECHNIQUES D'ESTIMATION

Le but de cette section est de retenir une technique capable d'estimer la valeur du paramètre θ inconnu, puis de mettre en oeuvre la méthode retenue.

3.1 Formulation du problème

Soit l'équation de mesure paramétrique

$$\mathbf{Z} = s(\theta) + \mathbf{B} \tag{IV.4}$$

ayant pour réalisations

$$Z = s(\theta) + B \tag{IV.5}$$

Le problème consiste à déterminer, au su de Z, le θ qui maximise ou minimise un certain critère. Dans le cadre de cette étude, le choix est porté sur les estimateurs du maximum de vraisemblance $\hat{\theta}_{MV}$ et des moindres carrés $\hat{\theta}_{MC}$, équivalents dans le cadre additif gaussien, définis par

$$\hat{\theta}_{MV} := \max_{\theta \in D^K}[L(\theta/Z)]$$

et

$$\hat{\theta}_{MC} := \min_{\theta \in D^K}[Q(\theta/Z)]$$

avec

$$Q(./Z) := \begin{cases} D^K \subset \mathbb{R}^{3K} & \rightarrow & \mathbb{R}^+ \\ \theta & \mapsto & Q(\theta/Z) = \frac{1}{2}\left\|s(\theta) - Z\right\|^2 = \frac{1}{2}\sum_{n=1}^{N}\Big(s(t_n;\theta) - Z(t_n)\Big)^2 \end{cases} \tag{IV.6}$$

$Q(\theta)$ est $\mathcal{C}^\infty(D,\mathbb{R}^+)$ car elle est la composée de $s(t_n;\theta)\forall n = 1\cdots N$ et de la fonction carrée, toutes deux $\mathcal{C}^\infty(D,\mathbb{R}^+)$. Il sera utile pour la suite d'avoir à disposition son gradient $\nabla_\theta[Q(\theta)]$, de dimension $(3K,1)$ et sa matrice Hessienne $H_\theta[Q(\theta)]$, de dimension $(3K,3K)$. En utilisant les règles de dérivation vectorielle :

$$\nabla_\theta[Q(\theta)] = \sum_{n=1}^{N}\nabla_\theta[s(t_n;\theta)](s(t_n;\theta) - Z(t_n)) \tag{IV.7}$$

et

$$H_\theta[Q(\theta)] = \sum_{n=1}^{N} H_\theta[s(t_n;\theta)]\Big(s(t_n;\theta) - Z(t_n)\Big) + \sum_{n=1}^{N} \nabla_\theta[s(t_n;\theta)]\nabla_\theta[s(t_n;\theta)]^T \qquad \text{(IV.8)}$$

3.2 Etat de l'Art, réponses possibles au problème

Trois types d'algorithmes sont considérées dans cette étude, la force brute, les méta heuristiques, et les méthodes de gradient.

3.2.1 Force brute

La méthode de la force brute consiste à mailler l'ensemble admissible θ^K, puis à évaluer en chacun des noeuds du maillage la fonction coût pour en retenir le minimum. Cette approche garantit le renvoi du minimum global de $Q(\theta)$, si le nombre de noeuds est suffisamment grand. Or, le temps de calcul, égal au nombre de noeuds multiplié par le temps d'évaluation de la fonction $Q(\theta)$, est d'autant plus grand que la précision est fine. Le temps de calcul peut alors devenir très grand.
Il est possible d'améliorer les performances de la méthode en effectuant une première passe avec un maillage grossier, suivie d'une seconde avec un maillage plus fin.
Ce n'est pas un algorithme itératif, il n'est donc pas question ici de condition initiale.

3.2.2 Méta heuristiques

Les méthodes méta heuristiques telles que le recuit simulé se situent entre les algorithmes de gradients et les algorithmes stochastiques. Un algorithme célèbre est le recuit simulé. Le principe général est de parcourir la fonctionnelle à optimiser selon des tirages aléatoires, dont la variance est contrôlée par un schéma de température[3]. De façon très générale, si le point en cours piégé dans un extremum local, la température est haute, ce qui autorise de grands déplacements. Au contraire, si le point en cours est proche de la solution cherchée ou que le nombre d'itérations est élevé, la température est basse n'autorisant que de petits déplacements.
Les travaux de Souza De Cursi, pour leur clarté, font office de référence [Pog92, Sou92]. La convergence vers le minimum global de $Q(\theta)$ est garantie, mais le temps pour y arriver, bien que fini, n'est pas contrôlable. Ainsi, avec ce type de méthodes, seule une condition initiale proche de la vraie solution fait que l'algorithme converge vers le minimum global en un temps qui tout en restant de l'ordre de la dizaine de secondes demeure fortement dépendant des valeurs des paramètres de l'algorithme.

3.2.3 Méthodes d'annulation de gradient

Appelées "méthodes de gradient" par abus de langage, il s'agit d'une famille d'algorithmes itératifs qui requièrent la connaissance du gradient et/ou du hessien de $Q(\theta)$. Ils sont basés sur le fait qu'une condition nécessaire pour avoir un extremum est $\nabla_\theta[Q(\theta)] = 0$, il s'agit d'un minimum si $H_\theta[Q(\theta)]$ est définie positive. La fonction coût prise en θ_0 est alors remplacée par son développement limité à l'ordre 2 calculé en ce point, ce qui permet d'établir une formule de récurrence[Pil05]. Ainsi, l'algorithme de Newton-Raphson (NR) est, pour $j > 0$

$$\begin{cases} \hat{\theta}^{(j+1)} & = \hat{\theta}^{(j)} - \rho_j \Big(H_\theta[Q(\hat{\theta}^{(j)})] + \mu \mathrm{Id}_{3K}\Big)^{-1} \nabla_\theta[Q(\theta^{(j)})] \\ \hat{\theta}^{(0)} \text{donné} & \end{cases} \qquad \text{(IV.9)}$$

[3]La sémantique est empreintée à la physique des solides

Lorsque les termes d'ordre 2 sont négligés dans le hessien IV.8, il s'agit de l'algorithme de Gauss-Newton (GN) à utiliser si la matrice hessienne est singulière. Il s'agit de sa déclinaison préconditionnée à pas optimal. Le préconditionneur de Levenberg-Macquardt, matérialisé par le facteur μ, choisi petit, a tendance à relever les valeurs de la diagonale de $H_\theta[Q(\hat{\theta}^{(j)})]$, juste ce qu'il faut pour que le tout soit inversible.
D'autre part, $\rho_j \in]0\,;\,1[$ est déterminé à chaque itération tel que

$$\rho_j = \max_{\rho\in]0\,;\,1[} \left[Q\left[\hat{\theta}^{(j)} - \rho\Big(H_\theta[Q(\hat{\theta}^{(j)})] + \mu \mathrm{Id}_{3K}\Big)^{-1} \nabla_\theta[Q(\hat{\theta}^{(j)})]\right]\right]$$

ce qui permet de guider la solution de façon optimale jusqu'à convergence.
Si cet algorithme est exécuté avec une condition initiale proche du paramètre à estimer, la convergence est effective. Il n'en est pas de même pour toute condition initiale dans D^K, le même algorithme lancé cette fois loin du paramètre à estimer peut diverger en cas de non inversibilité ou converger vers une autre valeur de paramètre correspondant à un extremum local.
Ainsi, dans le cadre de l'optimisation difficile, le choix de la condition initiale est prépondérant.

3.2.4 Bilan

Les méthodes force brute et recuit simulé ont l'avantage de retourner le minimum global de la fonction coût. Le prix à payer est alors un temps de calcul important. Restent alors les méthodes itératives de gradient, mais ces dernières ne sont pas capables de retourner le le minimum global recherché, la convergence vers ce dernier n'étant pas garantie pour toute condition initiale. Cependant, si la condition initiale est suffisamment proche de la bonne solution, alors la convergence globale est effective. La solution retenue consiste à utiliser une méthode itérative de gradient couplée avec une technique apportant une condition initiale pertinente assurant la convergence vers la valeur du paramètre qui minimise la fonction coût. Le choix de la condition initiale est alors primordial.

4 DE L'IMPORTANCE DU CHOIX DE LA CONDITION INITIALE.

La donnée d'une condition initiale pertinente est requise. Derrière l'apparente banalité de cette notion de condition initiale se cache une spécificité dont il faut absolument tenir compte.
En effet, certains problèmes d'optimisation sont qualifiés de difficile, d'une part au sens de la physique qui en découle, et d'autre part parce qu'ils compromettent la convergence d'algorithmes pourtant performants. Ceci est dû au mauvais conditionnement numérique du modèle et à la qualité des données.
En particulier, il suffit que $Q(\theta)$ ne soit pas strictement convexe pour que les algorithmes basés sur le principe de l'annulation du gradient ne soit plus optimaux. En effet, si la fonction coût $Q(\theta)$ n'est pas strictement convexe, il se peut qu'elle ait des extrema locaux sur D^K qui *de facto* piègent les solutions. L'exemple de la figure 1 illustre ce fait.
Soit le problème de la recherche du maximum global de l'application f définie par

$$f := \left\{ \begin{array}{ccc} \mathbb{R}^2 & \to & \mathbb{R} \\ (x\,;\,y) & \mapsto & f(x\,;\,y)\cos(x)\sin(y)e^{-(x^2+y^2)/20} \end{array} \right.$$

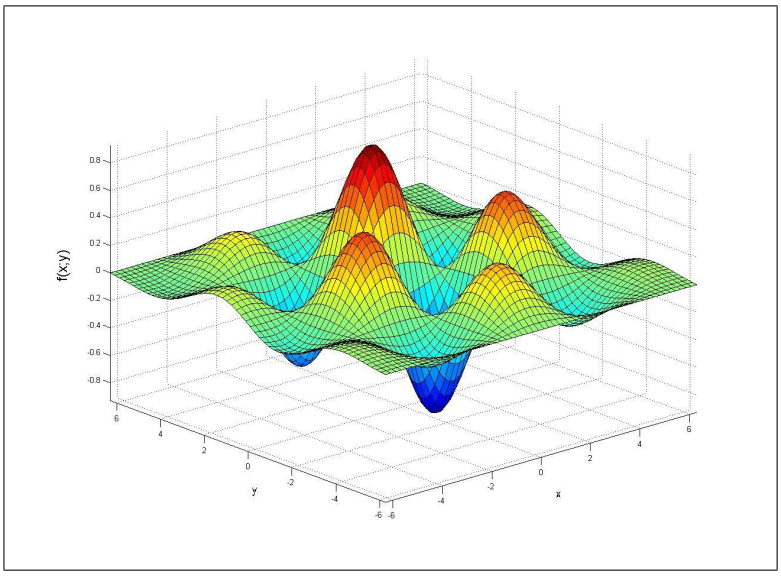


FIG. 1 – *Représentation graphique de* $f(x, y)$.

La représentation graphique de f, figure 1, montre que cette dernière présente des extrema locaux. Or, bien que la convergence de certains algorithmes soit garantie pour toute condition initiale, absolument rien n'assure la convergence vers le maximum global. La solution retenue est telle que le gradient de f est nul, elle peut correspondre en fait à n'importe quel extremum local, selon la condition initiale choisie.

4.1 Mise en oeuvre de la technique retenue.

Cette section définit l'équation de mesure découlant du modèle d'observation IV.2, ainsi que la matrice d'information de Fisher qui va permettre lors de la phase d'expérimentations d'obtenir l'expression de la borne de Cramèr-Rao permettant de donner une valeur minimale à la variance de l'estimateur recherché.
L'équation de mesure est en suite transformée sur le principe d'un modèle linéaire qui sera utile pour la suite du chapitre.

4.1.1 Equation de mesure

Les mesures sont collectées toutes les T_e secondes, soit

$$t_n := (n-1)T_e \quad \forall n = 1 \cdots N \quad T_e = T/(N-1).$$

L'observation est donc projetée en dimension finie, ce qui permet d'écrire l'équation vectorielle de mesure

$$\mathbf{Z} = \underbrace{\sum_{k=1}^{K} s_k(\theta_k)}_{s(\theta)} + \mathbf{B} \tag{IV.10}$$

dont une réalisation est

$$Z = \underbrace{\sum_{k=1}^{K} s_k(\theta_k)}_{s(\theta)} + B,$$

où $\mathbf{Z}$ de dimension $(N,1)$ est le vecteur d'observation

$$\mathbf{Z} = [\mathbf{Z}(t_1)\,;\,\ldots\,;\,\mathbf{Z}(t_N)]^T,$$

$s(\theta)$ est le vecteur de dimension $(N,1)$ contenant l'information utile,

$$s(\theta) = [s(t_1,\theta)\,;\,\ldots\,;\,s(t_N,\theta)]^T,$$

résultant de la somme des K vecteurs $s_k(\theta_k)$ de dimension $(N,1)$;

$$s_k(\theta_k) = [s_k(t_1,\theta_k)\,;\,\ldots\,;\,s_k(t_N,\theta_k)]^T,$$

$\mathbf{B}$ est le vecteur aléatoire gaussien de dimension $(N,1)$ représentant le bruit de mesure,

$$\mathbf{B} = [\mathbf{B}(t_1)\,;\,\ldots\,;\,\mathbf{B}(t_N)]^T,$$

avec $\mathbf{B} \hookrightarrow \mathcal{N}(0,\sigma_B^2 \mathrm{Id}_N)$.

4.1.2 Matrice d'information de Fisher

L'observation est telle que $Z \hookrightarrow \mathcal{N}(s(\theta),\sigma_B^2\mathrm{Id}_N)$. Ainsi, sa densité de probabilité s'écrit

$$p_Z(Z/\theta) = \frac{1}{(2\pi\sigma_B^2)^{N/2}} e^{-\frac{1}{2\sigma_B^2}\big(Z-s(\theta)\big)^T\big(Z-s(\theta)\big)}.$$

De plus, la vraisemblance $L(\theta/Z)$ est définie par

$$L(./Z) := \left\{ \begin{array}{ccc} D^K & \rightarrow & \mathbb{R}^+ \\ \theta & \mapsto & L(\theta/Z) = p_Z(Z/\theta) \end{array} \right.$$

Cette dernière sert à construire la matrice d'information de Fisher (FIM), notée $I(\theta/Z)$, de dimension $(3K,3K)$, telle que

$$I(\theta/Z) := \mathbb{E}\left[\nabla_\theta[ln\big(L(\theta/Z)\big)]\nabla_\theta^T[ln\big(L(\theta/Z)\big)]\right].$$

Dans ce cas additif gaussien, l'expression de cette dernière est obtenue sans peine[4],

$$\begin{aligned} ln\big(L(\theta/Z)\big) &= C - \frac{1}{2\sigma^2}\big(u-s(\theta)\big)^T\big(u-s(\theta)\big) \quad C>0 \text{ constante} \\ &\Rightarrow \nabla_\theta[ln\big(L(\theta/Z)\big)] = \frac{1}{\sigma_B^2}\nabla_\theta[s(\theta)]\Big(Z-s(\theta)\Big) \\ &\Rightarrow \nabla_\theta[ln\big(L(\theta/Z)\big)]\nabla_\theta^T[ln\big(L(\theta/Z)\big)] = \frac{1}{\sigma_B^4}\nabla_\theta[s(\theta)]\Big(Z-s(\theta)\Big)\Big(Z-s(\theta)\Big)^T\nabla_\theta^T[s(\theta)] \end{aligned}$$

$$\Rightarrow \mathbb{E}\left[\nabla_\theta[ln\big(L(\theta/Z)\big)]\nabla_\theta^T[ln\big(L(\theta/Z)\big)]\right] = \frac{1}{\sigma_B^4}\nabla_\theta[s(\theta)]\underbrace{\mathbb{E}\left[\Big(Z-s(\theta)\Big)\Big(Z-s(\theta)\Big)^T\right]}_{=\sigma_B^2\mathrm{Id}_N}\nabla_\theta^T[s(\theta)],$$

ce qui donne après simplifications,

$$I(\theta/Z) := \frac{1}{\sigma_B^2}\nabla_\theta[s(\theta)]\nabla_\theta^T[s(\theta)].$$

[4]Si ce n'est peut-être la formule du gradient d'une forme quadratique engendrée par une matrice symétrique Ξ : $\nabla_\theta[v^T(\theta)\Xi v(\theta)] = 2\nabla_\theta[v(\theta)]\Xi v(\theta)$

En particulier, pour une cellule k avec $\theta_k = [A_k\,;\,\sigma_k\,;\,m_k]^T$,

$$I(\theta_k/Z) \;=\; \frac{1}{\sigma_B^2}\nabla_{\theta_k}[s(\theta_k)]\nabla_{\theta_k}^T[s(\theta_k)] \tag{IV.11}$$

soit

$$I(\theta_k/Z) =$$

$$\frac{1}{\sigma_B^2}\sum_{n=1}^{N}\begin{bmatrix} \left(\frac{\partial}{\partial A_k}s(t_n,\theta_k)\right)^2 & \frac{\partial}{\partial A_k}s(t_n,\theta_k)\frac{\partial}{\partial \sigma_k}s(t_n,\theta_k) & \frac{\partial}{\partial A_k}s(t_n,\theta_k)\frac{\partial}{\partial m_k}s(t_n,\theta_k) \\ \frac{\partial}{\partial A_k}s(t_n,\theta_k)\frac{\partial}{\partial \sigma_k}s(t_n,\theta_k) & \left(\frac{\partial}{\partial \sigma_k}s(t_n,\theta_k)\right)^2 & \frac{\partial}{\partial \sigma_k}s(t_n,\theta_k)\frac{\partial}{\partial m_k}s(t_n,\theta_k) \\ \frac{\partial}{\partial m_k}s(t_n,\theta_k)\frac{\partial}{\partial A_k}s(t_n,\theta_k) & \frac{\partial}{\partial m_k}s(t_n,\theta_k)\frac{\partial}{\partial \sigma_k}s(t_n,\theta_k) & \left(\frac{\partial}{\partial m_k}s(t_n,\theta_k)\right)^2 \end{bmatrix},$$

et, d'après IV.3,

$$I(\theta_k/Z) = \quad \frac{1}{\sigma_B^2}\sum_{n=1}^{N}s^2(t_n,\theta_k)\begin{bmatrix} \frac{1}{A_k^2} & \frac{(t_n-m_k)^2}{A_k\sigma_k^3} & \frac{(t_n-m_k)}{A_k\sigma_k^2} \\ \frac{(t_n-m_k)^2}{A_k\sigma_k^3} & \frac{(t_n-m_k)^4}{\sigma_k^6} & \frac{(t_n-m_k)^3}{\sigma_k^5} \\ \frac{(t_n-m_k)}{A_k\sigma_k^2} & \frac{(t_n-m_k)^3}{\sigma_k^5} & \frac{(t_n-m_k)^2}{\sigma_k^4} \end{bmatrix}$$

Par extension, la matrice d'information de Fisher dans le cas de K cellules est une matrice de dimension $(3K, 3K)$, diagonale par blocs de taille $(3,3)$ qui ne sont rien d'autre que les $\{I(\theta_k/Z)\}_{k=1\ldots K}$,

$$I(\theta/Z) := \begin{bmatrix} I(\theta_1/Z) & & (0) \\ & \ddots & \\ (0) & & I(\theta_K/Z)] \end{bmatrix}.$$

4.1.3 Transformation de l'équation de mesure

Il est utile pour la suite d'avoir à disposition l'équation de mesure IV.10 sous la forme

$$\mathbf{Y} = \Xi\,\mathbf{X}(\theta). \tag{IV.12}$$

$\mathbf{Y}$ est un vecteur aléatoire à réalisations dans $\mathbb{R}^N$ représentant l'observation, Ξ est une matrice quelquonque de dimension (N, NK) et $\mathbf{X}(\theta)$ un vecteur aléatoire à réalisations dans $\mathbb{R}^{NK}$ représentant l'état dépendant du paramètre θ de dimension (3K,1).
Soit $\xi(\theta)$ le vecteur de dimension $(NK, 1)$ de coordonnées

$$\xi(\theta) := [s_1(t_1,\theta_1)\,;\cdots;\,s_1(t_1,\theta_K)\,;\cdots;\,s_1(t_N,\theta_1)\,;\cdots;\,s_K(t_N,\theta_K)]^T,$$

et M la matrice de dimension (N, NK) telle que

$$M := \begin{bmatrix} 1 & 1 & \cdots & 1 & & & & & & & (0) & \\ & & & & 1 & 1 & \cdots & 1 & & & & \\ & (0) & & & & & & & 1 & 1 & \cdots & 1 \end{bmatrix},$$

chaque ligne a comme éléments non nuls un bloc de 1 de longueur K.
Ainsi, en posant

$$\mathbf{Y} := \mathbf{Z},$$

l'équation de mesure devient

$$\begin{aligned} \mathbf{Y} &= M\xi(\theta) + \mathbf{B} \Leftrightarrow \\ \Xi\mathbf{X}(\theta) &= M\xi(\theta) + \mathbf{B}. \end{aligned}$$

Parmi les différents choix possibles de matrice Ξ,

$$\Xi := M$$

en est un judicieux car s'il existe un vecteur aléatoire $\mathbf{b}$ de dimension $(NK, 1)$ tel que

$$\mathbf{B} := \Xi\mathbf{b},$$

alors,

$$\mathbf{X}(\theta) = \xi(\theta) + \mathbf{b}$$

et ainsi

$$\begin{aligned} \Xi\mathbf{X}(\theta) &= \Xi\xi(\theta) + \Xi\mathbf{b} \Leftrightarrow \\ \mathbf{Y} &= \Xi\xi(\theta) + B. \end{aligned}$$

Il reste à caractériser statistiquement $\mathbf{b}$. Ses moments d'ordre 2 sont tels que

$$\left\{ \begin{array}{l} \mathbb{E}\left[\mathbf{B}\right] = 0 \Leftrightarrow \mathbb{E}\left[\Xi\mathbf{b}\right] = 0 \Leftrightarrow \mathbb{E}\left[\mathbf{b}\right] = 0 \\ \text{et} \\ \Gamma_{BB} = \mathbb{E}\left[\mathbf{B}\mathbf{B}^T\right] = \mathbb{E}\left[\Xi\mathbf{b}\mathbf{b}^T\Xi^T\right] = \Xi\Gamma_{bb}\Xi^T \end{array} \right. ,$$

mais plusieurs choix pour Γ_{bb} sont possibles. Cependant, Γ_{BB} est une matrice diagonale, une solution consiste à ce que Γ_{bb}, de dimension (NK, NK), le soit également,

$$\Gamma_{bb} := \left[\begin{array}{ccccccc} q_1 & & & & & & \\ & \ddots & & & & (0) & \\ & & q_K & & & & \\ & & & \ddots & & & \\ & & & & q_1 & & \\ & (0) & & & & \ddots & \\ & & & & & & q_K \end{array} \right].$$

Dans ce cas,

$$\left\{ \begin{array}{lcl} \Gamma_{BB} & = & \sigma_B^2 \mathrm{Id}_N \\ \\ \Xi\Gamma_{bb}\Xi^T & = & \left(\displaystyle\sum_{k=1}^{K} q_k \right) \mathrm{Id}_N \end{array} \right. , \implies \sum_{k=1}^{K} q_k = \sigma_B^2.$$

Les $\{q_k\}_{k=1\ldots K}$ véhiculent la puissance du bruit affectée à chacune des K cellules, voilà pourquoi un choix possible est de poser

$$q_k = \beta_k \sigma_B^2,$$

dans ce cas

$$\begin{aligned}\sum_{k=1}^{K} q_k &= \sum_{k=1}^{K} \beta_k \sigma_B^2 \quad \Leftrightarrow \\ \sigma_B^2 &= \sigma_B^2 \sum_{k=1}^{K} \beta_k \quad \Leftrightarrow \\ \sum_{k=1}^{K} \beta_k &= 1.\end{aligned}$$

Le cas le plus simple consiste à prendre $\beta_k := 1/K \quad \forall k = 1 \dots K$.

Remarque : *Les $\{\beta_k\}_{k=1\dots K}$ servent à tenir compte du fait qu'une cellule peut véhiculer plus de bruit qu'une autre, ou bien au contraire à considérer qu'elles sont toutes bruitées avec la même puissance.*

Finalement, l'équation de mesure IV.10 s'écrit $\mathbf{Y} = \Xi \mathbf{X}(\theta)$ avec

$$\begin{cases} \mathbf{Y} & \hookrightarrow & \mathcal{N}(s(\theta), \sigma_B^2 \mathrm{Id}_N) \\ \mathbf{X}(\theta) & \hookrightarrow & \mathcal{N}(\xi(\theta), \frac{\sigma_B^2}{K} \mathrm{Id}_{NK}) \end{cases}, \tag{IV.13}$$

Remarque : *Cette modélisation ouvre la porte à la possibilité d'utiliser l'algorithme EM. Par ailleurs elle est également le point de départ du filtre de Kalman-Bucy.*

La théorie du filtrage adapté stochastique utilisée en détection est un moyen de fournir automatiquement aux algorithmes choisis un jeu de conditions initiales pertinent, aidant ainsi à converger vers le minimum global de la fonction coût. Elle fait l'objet de la section suivante.

5 DÉTECTION D'UNE ACTIVITÉ DE COURANT PAR UTILISATION DU FILTRAGE ADAPTÉ STOCHASTIQUE

5.1 Introduction

Le but de la démarche est de détecter une activité de courant, sachant que les propriétés statistiques à l'ordre 2 de cette dernière sont connues. Cette étape se positionne en amont de la phase d'estimation proposée dans ce chapitre, sa finalité est de fournir une condition initiale pertinente et ainsi éviter les problèmes de convergence inhérents à l'optimisation non-convexe. L'estimation d'une activité de courant est légitime dans la mesure où l'on considère qu'il y a présence effective d'information utile. En d'autre termes, si le signal observé ne consomme pas sur un temps d'observation donné, l'estimation d'activité de courant sur cet intervalle de temps n'a pas de sens. De même, il est important que lorsque le dispositif consomme, l'observation ait lieu sur un intervalle de temps judicieusement choisi, contenant l'intégralité d'une période d'activité, évitant ainsi les observations contenant des relevés tronqués, conduisant nécessairement à des résultats d'estimation erronés vu que le support du modèle de signal utile que l'on se donne

est supposé appartenir à l'intervalle d'observation.
De façon générale, l'extraction ou la détection de l'information, dite signal utile, contenue dans une observation détériorée par la présence de termes perturbateurs additifs ou multiplicatifs est un problème courant en traitement du signal. L'une des techniques, proposée dans cette section, permettant de s'affranchir des termes perturbateurs, est basée sur une extension stochastique de la notion de filtrage adapté [Cav93], inventé par Cavassilas. Le modèle du signal utile n'étant jamais parfaitement connu, il est remplacé par un signal aléatoire permettant ainsi l'obtention d'une nouvelle écriture du rapport signal à bruit. L'optimisation de ce rapport permet d'obtenir un ensemble de filtres dont le regroupement contribue à un accroissement du rapport signal à bruit.
Ainsi, tout au long de cette section, l'observation $\mathbf{Z}(t)$, le signal utile qui est ici la consommation effective de courant $\mathbf{S}(t)$ et le bruit de mesure $\mathbf{B}(t)$ sont reliés par l'équation

$$\mathbf{Z}(t) = \mathbf{S}(t) + \mathbf{B}(t) \quad \forall t \in D, \tag{IV.14}$$

où $D = [0; T]$. Seules les statistiques d'ordre 2 des variables aléatoires $S(t)$ et $B(t)$ sont connues.

5.2 Signaux analogiques

Le signal et le bruit sont supposés centrés, stationnaires au moins au second ordre et indépendants. En utilisant les signaux réduits $\mathbf{S}_0(t)$ et $\mathbf{B}_0(t)$, la relation IV.14 peut encore s'écrire :

$$\mathbf{Z}(t) = \sigma_S \mathbf{S}_0(t) + \sigma_B \mathbf{B}_0(t) \quad \forall t \in D, \tag{IV.15}$$

avec $\sigma_S^2 = \mathbb{E}\left[\mathbf{S}^2(t)\right]$ et $\sigma_B^2 = \mathbb{E}\left[\mathbf{B}^2(t)\right]$.

D'après les résultats établis au chapitre III, l'observation $\mathbf{Z}(t)$ peut être écrite sous la forme suivante :

$$\mathbf{Z}(t) = \sum_{n=1}^{\infty} \mathbf{z}_n \Psi_n(t),$$

où $\{\mathbf{z}_n\}_{n\in\mathbb{N}^*}$ constitue une séquence infinie de variables aléatoires centrées et décorrélées :

$$\mathbb{E}\left[\mathbf{z}_n \mathbf{z}_m\right] = \mathbb{E}\left[\mathbf{z}_n^2\right] \delta[n-m]$$

et où les $\Psi_n(t)$ constituent une base de fonctions déterministes et linéairement indépendantes.
En considérant la décomposition simultanée du signal et du bruit :

$$\begin{cases} \mathbf{S}_0(t) = \sum_{n=1}^{\infty} \mathbf{s}_n \Psi_n(t) \\ \mathbf{B}_0(t) = \sum_{n=1}^{\infty} \mathbf{b}_n \Psi_n(t) \end{cases},$$

il vient :

$$\Psi_n(t) = \frac{\mathbb{E}\left[\mathbf{s}_n \mathbf{S}_0(t)\right]}{\mathbb{E}\left[\mathbf{s}_n^2\right]} \tag{IV.16}$$

et que

$$\Psi_n(t) = \frac{\mathbb{E}\left[\mathbf{b}_n \mathbf{B}_0(t)\right]}{\mathbb{E}\left[\mathbf{b}_n^2\right]}. \tag{IV.17}$$

Preuve . *D'une part*

$$\begin{aligned}\mathbb{E}\left[\mathbf{s}_m\mathbf{S}_0(t)\right] &= \mathbb{E}\left[\mathbf{s}_m\sum_{n=1}^{\infty}\mathbf{s}_n\Psi_n(t)\right]\\ &= \sum_{n=1}^{\infty}\mathbb{E}\left[\mathbf{s}_m\mathbf{s}_n\right]\Psi_n(t),\end{aligned}$$

et compte tenu de la décorrélation des variables aléatoires $\mathbf{s}_n$*, il vient*

$$\begin{aligned}\mathbb{E}\left[\mathbf{s}_m\mathbf{S}_0(t)\right] &= \sum_{n=1}^{\infty}\mathbb{E}\left[\mathbf{s}_m^2\right]\delta[n-m]\Psi_n(t)\\ &= \mathbb{E}\left[\mathbf{s}_m^2\right]\Psi_m(t)\end{aligned}$$

et par suite, l'expression de $\Psi_n(t)$*.*

□

Les variables aléatoires $\mathbf{s}_n$ et $\mathbf{b}_n$ sont déterminées par projection du signal, respectivement du bruit, sur une base de fonctions déterministes $\{\Phi_n(t)\}_{n\in\mathbb{N}^*}$

$$\mathbf{s}_n = \int_D \mathbf{S}_0(t)\Phi_n(t)dt$$

et

$$\mathbf{b}_n = \int_D \mathbf{B}_0(t)\Phi_n(t)dt.$$

si bien que

$$\begin{cases}\mathbb{E}\left[\mathbf{s}_n\mathbf{S}_0(t_1)\right] = \displaystyle\int_D \Gamma_{SS}(t_1-t_2)\Phi_n(t_2)dt_2\\ \\ \mathbb{E}\left[\mathbf{b}_n\mathbf{B}_0(t_1)\right] = \displaystyle\int_D \Gamma_{BB}(t_1-t_2)\Phi_n(t_2)dt_2\end{cases},$$

où $\Gamma_{SS}(.)$ et $\Gamma_{BB}(.)$ désignent respectivement les covariances du signal et du bruit.
Par suite et compte tenu des relations IV.16 et IV.17, il vient $\forall t \in D$:

$$\int_D \Gamma_{SS}(t_1-t_2)\Phi_n(t_2)dt_2 = \frac{\mathbb{E}\left[\mathbf{s}_n^2\right]}{\mathbb{E}\left[\mathbf{b}_n^2\right]}\int_D \Gamma_{BB}(t_1-t_2)\Phi_n(t_2)dt_2. \tag{IV.18}$$

Ainsi la décorrélation simultanée des variables aléatoires $\mathbf{s}_n$ et $\mathbf{b}_n$ est assurée dés lors que les $\Phi_n(t)$ sont les fonctions propres, solutions de l'équation intégrale précédente, associées aux valeurs propres λ_n définies comme suit :

$$\lambda_n = \frac{\mathbb{E}\left[\mathbf{s}_n^2\right]}{\mathbb{E}\left[\mathbf{b}_n^2\right]}. \tag{IV.19}$$

Concernant la détermination des fonctions déterministes $\Phi_n(t)$, l'alternative consiste en une extension de la théorie du filtrage adapté classique. Soit un signal utile stationnaire, déterministe $s(t)$, défini sur D, perturbé par un bruit ergodique, stationnaire $\mathbf{B}(t)$, le filtrage adapté consiste

en la détermination d'une fonction $h(t)$, définie sur D, optimisant le rapport signal sur bruit $\rho(t_1)$ à l'instant t_1, défini comme suit :

$$\rho(t_1) := \frac{\left| \int_D s(t_1 - t_2) h(t_2) dt_2 \right|^2}{\mathbb{E}\left[\left| \int_D \mathbf{B}(t_1 - t_2) h(t_2) dt_2 \right|^2 \right]}.$$

Par extension, lorsque le signal utile n'est plus déterministe mais une réalisation d'un processus stochastique, ce rapport peut s'écrire comme suit :

$$\rho(t_1) = \frac{\mathbb{E}\left[\left| \int_D \mathbf{S}(t_1 - t_2) \Phi(t_2) dt_2 \right|^2 \right]}{\mathbb{E}\left[\left| \int_D \mathbf{B}(t_1 - t_2) \Phi(t_2) dt_2 \right|^2 \right]},$$

soit en faisant intervenir les covariances du signal et du bruit :

$$\rho = \frac{\int_D \int_D \Gamma_{SS}(t_1 - t_2) \Phi(t_2) dt_1 dt_2}{\int_D \int_D \Gamma_{BB}(t_1 - t_2) \Phi(t_2) dt_1 dt_2}$$

Cette expression représente le rapport de deux formes quadratiques positives. Il apparaît ainsi comme étant un quotient de Rayleigh, maximal si $\Phi(t)$ est la fonction propre associée à la plus grande valeur propre de l'équation intégrale suivante, pour $t \in D$:

$$\int_D \Gamma_{SS}(t_1 - t_2) \Phi_n(t_2) dt_2 = \lambda_n \int_D \Gamma_{BB}(t_1 - t_2) \Phi_n(t_2) dt_2,$$

les valeurs propres λ_n étant classées par valeur décroissantes.
Ceci étant, lorsque les fonctions propres $\Phi_n(t)$ sont normalisées comme suit :

$$\int_D \int_D \Gamma_{BB}(t_1 - t_2) \Phi_n(t_1) \Phi_n(t_2) dt_1 dt_2 = 1,$$

les variables aléatoires b_n admettent une puissance unitaire :

$$\mathbb{E}\left[\mathbf{b}_n \mathbf{b}_m \right] = \delta[n - m].$$

Dans ces conditions et compte tenu de IV.19, on montre que

$$\mathbb{E}\left[\mathbf{s}_n \mathbf{s}_m \right] = \lambda_n \delta[n - m].$$

Afin de quantifier l'apport de la base de fonctions $\Phi_n(t)$ sur l'observation $\mathbf{Z}(t)$, considérons le moment quadratique de la $n^{\text{ème}}$composante de $\mathbf{Z}(t)$:

$$\begin{aligned}\mathbb{E}\left[z_n^2\right] &= \mathbb{E}\left[(\sigma_S s_n + \sigma_B b_n)^2\right] \\ &= \sigma_S^2\lambda_n + \sigma_B^2 + 2\int_D\int_D \mathbb{E}\left[\mathbf{S}_0(t_1)\mathbf{B}_0(t_2)\right]\Phi_n(t_1)\Phi_n(t_2)dt_1dt_2.\end{aligned}$$

L'indépendance entre les signaux centrés $\mathbf{S}_0(t)$ et $\mathbf{B}_0(t)$ conduit à l'élimination du terme intégral ($\mathbb{E}\left[\mathbf{S}(t_1)\mathbf{B}(t_2)\right] = 0$), d'où :

$$\mathbb{E}\left[z_n^2\right] = \sigma_S^2\lambda_n + \sigma_B^2,$$

et par suite le rapport signal sur bruit de la $n^{\text{ème}}$composante de $\mathbf{Z}(t)$ devient :

$$\frac{\sigma_S^2}{\sigma_B^2}\lambda_n,$$

où σ_S^2/σ_B^2 représente le rapport signal sur bruit avant traitement.
Ainsi toutes les fonctions propres $\Phi_n(t)$ associées aux valeurs propres λ_n plus grandes que 1 contribuent en une amélioration du rapport signal à bruit.
En ce qui concerne les fonctions de base déterministes $\Psi_n(t)$, on peut aisément montrer que ces dernières sont données par

$$\Psi_n(t_1) = \frac{1}{\lambda_n}\int_D \Gamma_{SS}(t_1 - t_2)\Phi_n(t_2)dt_2 \tag{IV.20}$$

ou par :

$$\Psi_n(t_1) = \int_D \Gamma_{BB}(t_1 - t_2)\Phi_n(t_2)dt_2. \tag{IV.21}$$

5.3 Signaux numériques

Soit un signal numérique $\mathbf{Z}$, représenté par un vecteur colonne constitué de N échantillons successifs. Ce dernier correspond à la superposition additive de deux signaux numériques, l'un représentatif du signal utile $\mathbf{S}$, l'autre du signal perturbateur $\mathbf{B}$. En considérant les signaux réduits $\mathbf{S_0}$ et $\mathbf{B_0}$, il vient :

$$\mathbf{Z} = \sigma_S\mathbf{S_0} + \sigma_B\mathbf{B_0}. \tag{IV.22}$$

Le signal et le bruit sont supposés stationnaires au moins au second ordre, centrés et indépendants.
L'observation $\boldsymbol{Z}$ peut être décomposée comme suit :

$$\mathbf{Z} = \sum_{n=1}^{N}\mathbf{z}_n\Psi_n, \tag{IV.23}$$

où les $\mathbf{z}_n$ constituent une séquence finie de variables aléatoires centrées et décorrélées et où $\{\Psi_n\}_{n\in\mathbb{N}^*}$ est une base de dimension N.
Les variables aléatoires z_n sont déterminées en effectuant le produit scalaire entre l'observation et une base de dimension N de vecteurs Φ_n :

$$\mathbf{z}_n = \mathbf{Z}^T\Phi_n. \tag{IV.24}$$

La décorrélation de ces variables aléatoires est assurée dés lors que les vecteurs $\Phi_{nn\in\mathbb{N}^*}$ correspondent aux solutions du problème aux valeurs propres généralisé suivant :

$$\Gamma_{S_0S_0}\Phi_n = \lambda_n\Gamma_{B_0B_0}\Phi_n, \tag{IV.25}$$

où $\Gamma_{S_0S_0}$ et $\Gamma_{B_0B_0}$ désignent respectivement les covariances réduites du signal utile et du bruit. Lorsque les vecteurs propres Φ_n sont normalisés comme suit,

$$\Phi_n{}^T \Gamma_{B_0B_0} \Phi_n = 1, \tag{IV.26}$$

ce qui est toujours possible, il vient pour expression des vecteurs de base Ψ_n de la décomposition de l'observation

$$\Psi_n = \Gamma_{B_0B_0} \Phi_n. \tag{IV.27}$$

Dans ces conditions, on montre que le rapport signal à bruit de la $n^{\text{ème}}$ composante de l'observation est :

$$\rho_n = \frac{\sigma_S^2}{\sigma_B^2} \lambda_n. \tag{IV.28}$$

Remarque : *Lorsque le signal perturbateur est un bruit blanc, le FAS n'est rien d'autre que le développement de Karhunen-Loève présenté au chapitre précédent.*

Une opération de filtrage peut consister à ne retenir que les composantes telles que le rapport signal à bruit ρ_n soit supérieur à un certain seuil, fixé à l'avance et bien entendu, plus grand que 1.
Le problème aux valeurs propres généralisé IV.25 est résolu comme suit :

$$\left(\Gamma_{B_0B_0}^{-1} \Gamma_{S_0S_0}\right) \Phi_n = \lambda_n \Phi_n,$$

soit en recherchant les vecteurs et valeurs propres de la matrice $\left(\Gamma_{B_0B_0}^{-1} \Gamma_{S_0S_0}\right)$.
En pratique, il en va autrement. En effet, les signaux $\mathbf{S}$ et $\mathbf{B}$ sont des signaux dont les densités spectrales de puissance sont à support compact. Généralement la bande passante $\Delta\nu_B$ du bruit est supérieure ou égale à celle du signal utile. La fréquence d'échantillonnage doit ainsi être supérieure ou égale à deux fois la largeur de bande du bruit pour satisfaire au critère de Shannon. Le rapport $c = \frac{\Delta\nu_B}{F_e}$ est toujours inférieur à 1, excepté pour un signal modélisé par une séquence de N variables aléatoires mutuellement décorrélées. Par conséquent, le nombre de degrés de liberté du signal numérique $\mathbf{B}$ n'est pas égal à sa dimension N, mais à cN. La matrice de covariance associée $\Gamma_{B_0B_0}$ présente donc un conditionnement, tel qu'elle ne peut être inversée, n'ayant que cN valeurs propres significatives. Ainsi, la résolution du problème aux valeurs propres généralisé revient à rechercher Φ_n dans un sous-espace de $\mathbb{R}^N$, et non plus dans l'espace vectoriel $\mathbb{R}^N$.
En pratique, la dimension K du sous-espace considéré, où K est telle que : $K \leq cN$, correspondra au nombre de valeurs propres de $\Gamma_{B_0B_0}$ jugées suffisamment significatives. En notant $\mathbf{\Phi^S}$, la matrice de dimension $N \times K$, constituée des K vecteurs propres Φ_n^S de $\Gamma_{S_0S_0}$ associés aux K scalaires λ_n^B, valeurs propres de la matrice de variance covariance réduite du bruit, les plus significatives, la détermination des Φ_n solutions de IV.25 sera réalisée comme suit :

$$\Phi_n = \widetilde{\Phi}_n^T \Phi^S,$$

où les $\widetilde{\Phi}_n$ correspondent aux solutions de :

$$\left(\widetilde{\Gamma}_{B_0B_0}^{-1} \widetilde{\Gamma}_{S_0S_0}\right) \widetilde{\Phi}_n = \lambda_n \widetilde{\Phi}_n,$$

avec $\widetilde{\Gamma}_{S_0S_0}$ et $\widetilde{\Gamma}_{B_0B_0}$ définies comme suit :

$$\begin{cases} \widetilde{\Gamma}_{S_0S_0} = \Phi^{S^T} \Gamma_{S_0S_0} \Phi^S \\ \widetilde{\Gamma}_{B_0B_0} = \Phi^{S^T} \Gamma_{B_0B_0} \Phi^S \end{cases}$$

Une autre solution peut consister en l'utilisation du préconditionneur de Levenberg-Macquardt présenté section 3.2.3, dans ce cas les valeurs des valeurs propres sont légèrement affectées, les vecteurs propres demeurant les mêmes.

5.4 Utilisation en détection

Afin d'utiliser la théorie du Filtrage Adapté Stochastique en détection, il convient d'établir le contexte ainsi que les hypothèses de travail adéquat.

- Le signal utile $\mathbf{S}(t)$ et le bruit $\mathbf{B}(t)$ sont centrés. Si tel n'est pas le cas, au moins l'un des deux suffit.
- Il y a Q valeurs propres vérifiant $\rho_n > 1$, ρ_n étant défini par IV.28. Autrement dit, Q valeurs propres faisant augmenter le rapport signal à bruit.
- Le Q-uplet constitué des coefficients $\mathbf{z}_n$ a un comportement gaussien.

D'après l'ensemble des résultats de la section précédente, l'expression de la matrice de variance-covariance de $\mathbf{B}(t)$ est, dans la base engendrée par les ϕ_n

$$\Gamma_{B_\Phi B_\Phi} = \sigma_B^2 \, \mathrm{Id}_Q,$$

et celle de l'observation $\mathbf{Z}(t)$ par :

$$\Gamma_{Z_\Phi Z_\Phi} = \begin{bmatrix} \sigma_S^2\lambda_1 + \sigma_B^2 & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \sigma_S^2\lambda_Q + \sigma_B^2 \end{bmatrix}.$$

Ces deux matrices sont de dimensions $Q \times Q$.
L'étape suivante consiste à former le rapport de vraisemblance relatif aux deux hypothèses suivantes :

$$\begin{cases} H_0 \;:\; p(\mathbf{z}/H_0) = \dfrac{1}{(2\pi)^{\frac{Q}{2}}\sqrt{|\Gamma_{B_\Phi B_\Phi}|}} e^{-\frac{1}{2}\left(z^T \Gamma^{-1}_{B_\Phi B_\Phi} z\right)} \\ H_1 \;:\; p(\mathbf{z}/H_1) = \dfrac{1}{(2\pi)^{\frac{Q}{2}}\sqrt{|\Gamma_{Z_\Phi Z_\Phi}|}} e^{-\frac{1}{2}\left(z^T \Gamma^{-1}_{Z_\Phi Z_\Phi} z\right)} \end{cases},$$

où H_0 correspond à l'hypothèse "il n'y a que du bruit dans l'observation", soit formellement $\mathbf{Z} = \mathbf{B}$, et H_1 à celle "il y a du signal utile dans l'observation", soit formellement $\mathbf{Z} = \mathbf{S} + \mathbf{B}$. Le vecteur $\mathbf{z}$ est un vecteur de dimension Q dont les éléments sont les $\mathbf{z}_n$ de la décomposition de l'observation, de réalisation :

$$z = [z_1, \dots, z_Q]^T.$$

Proposition IV.2. *le rapport de vraisemblance $\Lambda(z)$ s'écrit*

$$\Lambda(z) = \frac{p(z/H_1)}{p(z/H_0)} \underset{<_{D_0}}{\overset{>^{D_1}}{}} 1,$$

soit

$$\sum_{n=1}^{Q} z_n^2 \frac{\sigma_S^2\lambda_n}{\sigma_B^2\left(\sigma_S^2\lambda_n + \sigma_B^2\right)} \underset{<_{D_0}}{\overset{>^{D_1}}{}} \sum_{n=1}^{Q} \ln\left(\frac{\sigma_S^2}{\sigma_B^2}\lambda_n + 1\right), \tag{IV.29}$$

le premier membre de l'inégalité est par commodité identifié à une fonctionnelle appelée $T(z)$.

Preuve . *Partant de l'expression du rapport,*

$$\begin{aligned}
\Lambda(z) &\underset{<_{D_0}}{\overset{>^{D_1}}{}} 1 \\
\sqrt{\frac{|\Gamma_{B_\Phi B_\Phi}|}{|\Gamma_{Z_\Phi Z_\Phi}|}} e^{-\frac{1}{2}\left(z^T\left(\Gamma^{-1}_{Z_\Phi Z_\Phi}-\Gamma^{-1}_{B_\Phi B_\Phi}\right)z\right)} &\underset{<_{D_0}}{\overset{>^{D_1}}{}} 1 \\
-z^T\left(\Gamma^{-1}_{Z_\Phi Z_\Phi}-\Gamma^{-1}_{B_\Phi B_\Phi}\right)z &\underset{<_{D_0}}{\overset{>^{D_1}}{}} 2\ln\left(\sqrt{\frac{|\Gamma_{Z_\Phi Z_\Phi}|}{|\Gamma_{B_\Phi B_\Phi}|}}\right) = \ln\left(\frac{|\Gamma_{Z_\Phi Z_\Phi}|}{|\Gamma_{B_\Phi B_\Phi}|}\right).
\end{aligned}$$

Les matrices $\Gamma_{B_\Phi B_\Phi}$ et $\Gamma_{Z_\Phi Z_\Phi}$ étant diagonales, il vient :

$$\begin{cases}
|\Gamma_{Z_\Phi Z_\Phi}| = \prod_{n=1}^{Q}\left(\sigma_S^2\lambda_n+\sigma_B^2\right) \\
|\Gamma_{B_\Phi B_\Phi}| = \prod_{n=1}^{Q}\sigma_B^2 = \sigma_B^{2Q}
\end{cases},$$

d'où,

$$\begin{aligned}
\ln\left(\frac{|\Gamma_{Z_\Phi Z_\Phi}|}{|\Gamma_{B_\Phi B_\Phi}|}\right) &= \ln\left(\prod_{n=1}^{Q}\left(\sigma_S^2\lambda_n+\sigma_B^2\right)\right) - \ln\left(\sigma_B^{2Q}\right) \\
&= \ln\left(\sigma_B^{2Q}\prod_{n=1}^{Q}\left(\frac{\sigma_S^2}{\sigma_B^2}\lambda_n+1\right)\right) - \ln\left(\sigma_B^{2Q}\right) \\
&= \ln\left(\prod_{n=1}^{Q}\left(\frac{\sigma_S^2}{\sigma_B^2}\lambda_n+1\right)\right) \\
&= \sum_{n=1}^{Q}\ln\left(\frac{\sigma_S^2}{\sigma_B^2}\lambda_n+1\right).
\end{aligned}$$

Par ailleurs :

$$\Gamma^{-1}_{Z_\Phi Z_\Phi}-\Gamma^{-1}_{B_\Phi B_\Phi} = \begin{bmatrix}
\frac{-\sigma_S^2\lambda_1}{\sigma_B^2\left(\sigma_S^2\lambda_1+\sigma_B^2\right)} & \cdots & 0 \\
\vdots & \ddots & \vdots \\
0 & \cdots & \frac{-\sigma_S^2\lambda_Q}{\sigma_B^2\left(\sigma_S^2\lambda_Q+\sigma_B^2\right)}
\end{bmatrix},$$

d'où :

$$\left(\Gamma^{-1}_{Z_\Phi Z_\Phi}-\Gamma^{-1}_{B_\Phi B_\Phi}\right)z = \left(\frac{-\sigma_S^2\lambda_1 z_1}{\sigma_B^2\left(\sigma_S^2\lambda_1+\sigma_B^2\right)},\ldots,\frac{-\sigma_S^2\lambda_Q z_Q}{\sigma_B^2\left(\sigma_S^2\lambda_Q+\sigma_B^2\right)}\right),$$

et :

$$z^T\left(\Gamma^{-1}_{Z_\Phi Z_\Phi}-\Gamma^{-1}_{B_\Phi B_\Phi}\right)z = \sum_{n=1}^{Q} z_n^2\frac{-\sigma_S^2\lambda_n}{\sigma_B^2\left(\sigma_S^2\lambda_n+\sigma_B^2\right)}.$$

□

Le principe algorithmique du FAS utilisé en détection est à présent détaillé :

– Modélisation ou estimation des covariances réduites $\Gamma_{S_0S_0}$ et $\Gamma_{B_0B_0}$ du signal utile et du bruit.
– Estimation des puissances σ_S^2 et σ_B^2.
– Détermination des Φ_n par résolution du problème aux valeurs propres généralisé :

$$\Gamma_{S_0S_0}\Phi_n = \lambda_n \Gamma_{B_0B_0}\Phi_n.$$

– Identification du nombre Q de valeurs propres vérifiant :

$$\lambda_n > 1.$$

– Normalisation des Φ_n :

$$\Phi_n = \frac{\Phi_n}{\sqrt{{\Phi_n}^T \Gamma_{BB} \Phi_n}}.$$

– Détermination numérique des z_n de la décomposition de l'observation.

– Construction numérique de la fonctionnelle $T(z)$.
– Décision suivant la relation IV.29. L'algorithme de détection est proposé sous forme schématique mais explicite sur la figure 2.

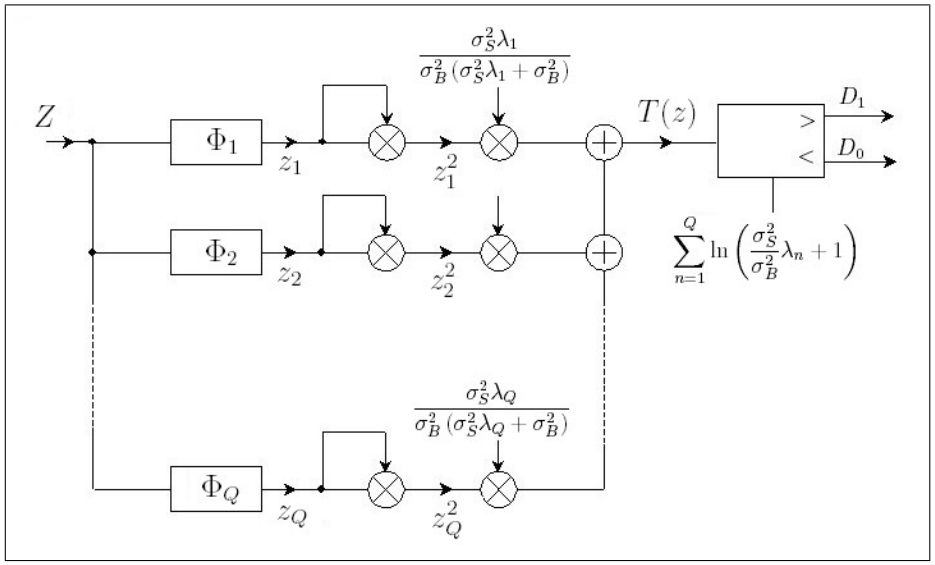


FIG. 2 – *Algorithme du Filtrage Adapté Stochastique utilisé en détection*

5.5 Application à la détection d'une activité de courant

Le but est de détecter la présence d'activité de courant dans une observation, puis de tirer profit des informations détectées afin de proposer un choix de conditions initiales pertinent vis-à-vis de la physique du problème. Un tel choix permettrait alors de contourner la difficulté, due à la non-convexité et aux problèmes d'échelle des paramètres à estimer, récurrente dans ce chapitre et plus généralement dans tout problème d'optimisation sortant des sentiers battus.
Comme l'indique l'algorithme précédent, la première étape consiste à modéliser et estimer au mieux les matrices de variance covariance du signal et du bruit. Il est clair que la qualité de ces estimations influe directement sur la qualité des résultats.
Afin de mettre au point et d'étalonner la technique, une observation test est construite, cette dernière est présentée figure 3

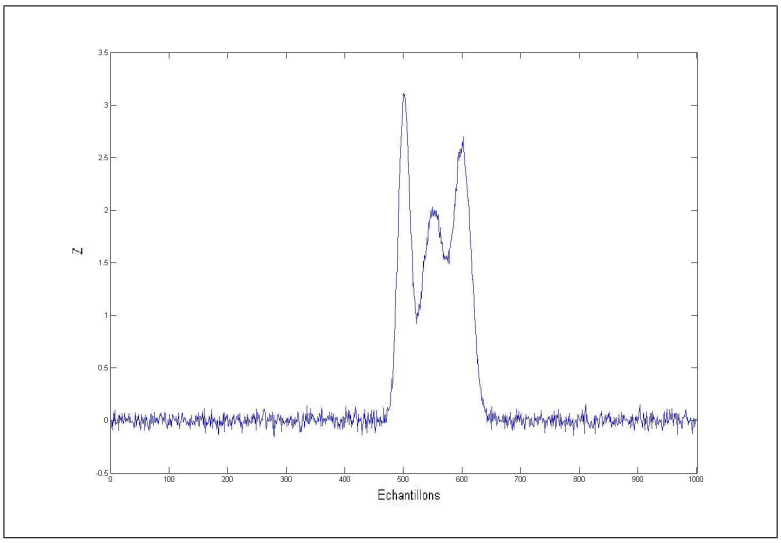


FIG. 3 – *Observation synthétique d'activité de courant*

Enfin, il est important de préciser que la technique de détection proposée n'a de sens que si les signaux mis en jeu sont stationnaire à l'ordre 2. Si tel n'est pas le cas sur l'intervalle d'étude complet, un traitement par fenêtre glissante est de rigueur[5].

5.5.1 Estimation de la matrice de variance covariance du signal utile

La question à se poser est "-détecter quoi ?". Or, d'après l'observation de la figure 3 et d'après la section relative à la modélisation du problème en début de chapitre, l'activité de courant est vue comme une superposition de contributions élémentaires représentées par des gaussiennes. La réponse est donc, "-une gaussienne", du moins une parmi d'autres. Donc, le signal utile est vu comme un processus aléatoire dont les réalisations ont l'allure d'une gaussienne. Ce dernier est supposé stationnaire à l'ordre 2, si bien qu'il est possible d'estimer son autocorrélation, à l'aide de la relation III.34 de la section 6.3.1 du chapitre *III*. Cette dernière est représentée figure 4 de taille identique à celle de la fenêtre d'observation, et sert à la construction de la matrice de variance covariance réduite du signal utile $\Gamma_{S_0 S_0}$, à partir du même protocole qu'en 6.3.1.

[5]Le prix à payer est alors une augmentation du temps global de calcul ainsi qu'un effet plus ou moins moyenneur sur l'observation fonction de la taille de la fenêtre d'observation

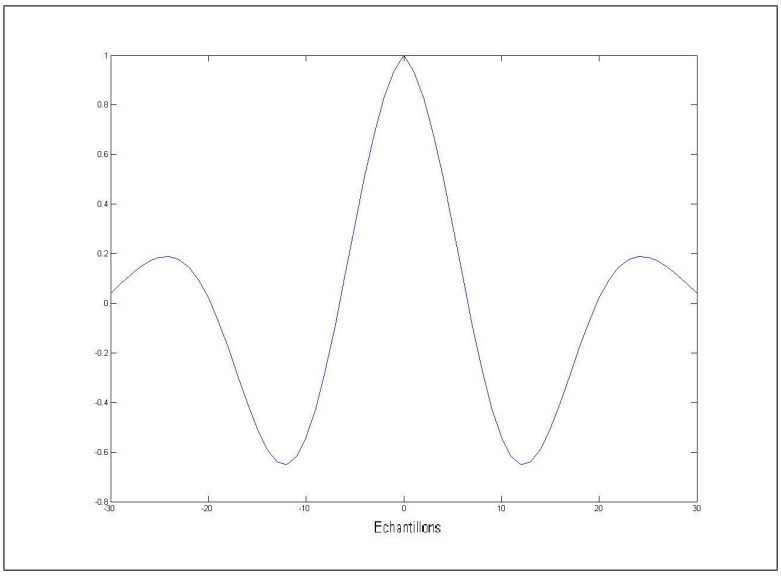


FIG. 4 – *Autocorrélation réduite du modèle de signal utile*

5.5.2 Estimation de la matrice de variance covariance du bruit

Généralement, un moyen efficace d'estimer la matrice de variance covariance réduite du bruit $\Gamma_{B_0B_0}$ en fonction des données est d'estimer cette dernière sur une portion de l'observation ou il n'y a pas ou très peu de signal utile. Par exemple, d'après la figure 3, les échantillons situés dans les intervalles $[0\,;\,400]$ ou $[600\,;\,1000]$ conviennent à partir du moment où leur mesure est inférieure à la taille de la fenêtre d'observation. A l'intérieur de l'intervalle choisi, l'autocorrélation est calculée, cette dernière est représentée figure 5 puis la matrice de variance covariance réduite $\Gamma_{B_0B_0}$ est construite.
Dans le cas d'une observation réelle de consommation de courant, la covariance du bruit est estimée par mesure de l'observation en absence d'activité de la carte.

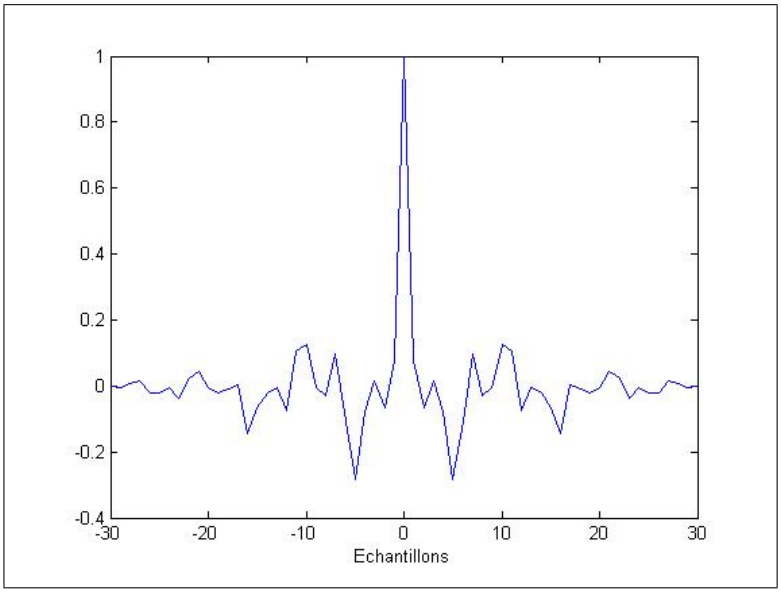


FIG. 5 – *Autocorrélation réduite du bruit*

5.5.3 Expérimentations

La taille de la fenêtre d'observation est le paramètre d'entrée de l'algorithme. Cette dernière conditionne directement la qualité du résultat, vu qu'elle est la dimension des autocorrélations du signal et du bruit. Sa détermination peut être fondée sur deux approches.

- Une approche visuelle, consistant à affirmer que la taille de la fenêtre doit être de l'ordre de l'occupation temporelle du motif à détecter dans l'observation. Bien qu'appartenant au domaine du bon sens, cette démarche est caduque dès lors que la puissance du bruit est importante[Cha06s1] car alors le motif à détecter n'est plus discernable à l'oeil nu dans l'observation.
- Une autre approche, axée sur les simulations numériques, consiste à faire varier la taille de la fenêtre, et relever pour chaque taille le maximum de la fonctionnelle obtenu. La taille finale de la fenêtre est le maximum des maxima obtenus.
  Par exemple, dans le cas de l'observation sur la figure 3, la plus grande taille de fenêtre maximisant la fonctionnelle est $N_{opt} = 21$ échantillons, comme le montre la figure 6.

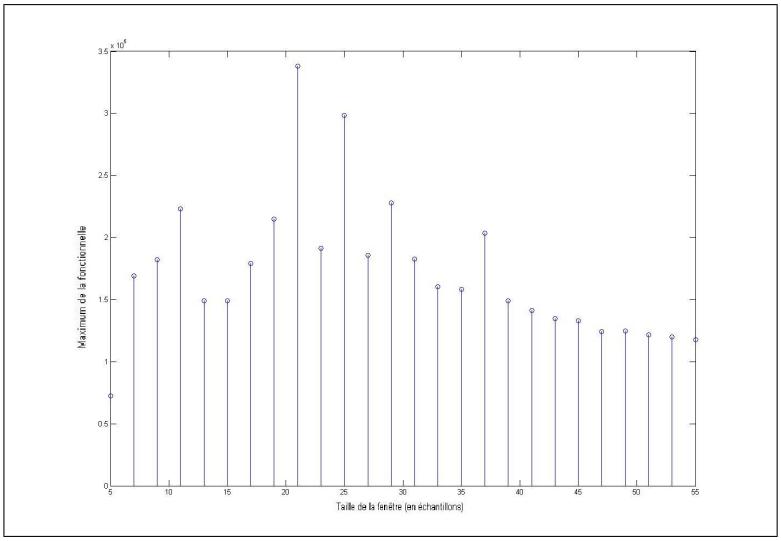


FIG. 6 – *Maximum de la fonctionnelle $T(z)$ en fonction de la taille de la fenêtre.*

A chaque observation correspond plusieurs dimensions possibles de fenêtre optimale, chacune étant adaptée à un gabarit de pic particulier. Le choix de taille de fenêtre le plus cohérent est celui qui permet de détecter les pics significatifs les plus importants.
Soit une observation Z issue de l'échantillonnage du signal $Z(t)$ sur $N = 1000$ points à raison d'un point toutes les $T_e = 10^{-3}$ secondes, réalisation de $\mathbf{Z}$, telle que

$$Z = s_1(\hat{\theta}_1) + s_2(\hat{\theta}_2) + s_3(\hat{\theta}_3) + B,$$

avec

$$\begin{aligned} \hat{\theta} &= [\hat{\theta}_1\,;\,\hat{\theta}_2\,;\,\hat{\theta}_3]^T \\ &= [3\,;\,0,01\,;\,0,5\,;\,2\,;\,0,02\,;\,0,55\,;\,2.5\,;\,0,015\,;\,0,6]^T \end{aligned} \qquad \text{(IV.30)}$$

et $\sigma_B^2 = 2,5 \times 10^{-3}$. La figure 3 montre Z, trois pics sont enchevêtrés et bruités.
Le but est de donner $\hat{\theta}_{FAS}$, sensé être proche de $\hat{\theta}$. Le FAS en détection est appliqué à l'observation avec une taille de fenêtre de $N_{opt} = 21$ échantillons. Les 100 premiers échantillons servent à construire la covariance du bruit. L'observation et la fonctionnelle sont présentées figure 7.

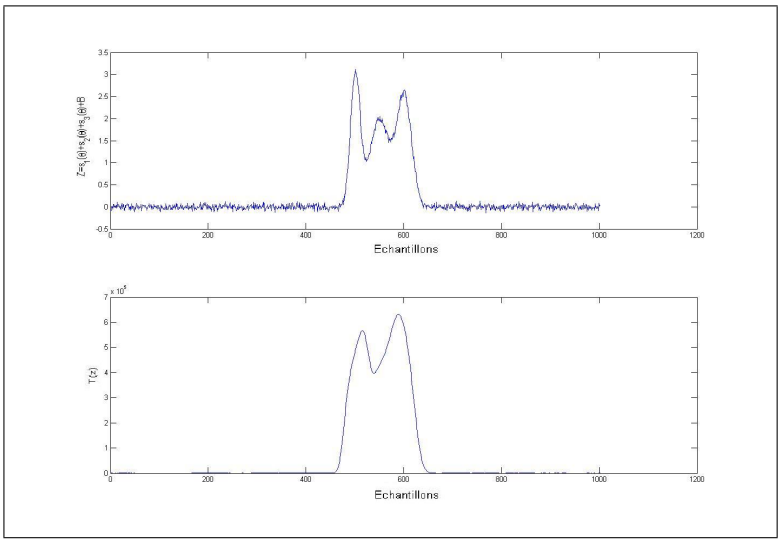


FIG. 7 – *Z et $T(z)$.*

Le principe est le suivant : Pour $k = 1 \dots K$,

1. Le FAS en détection est appliqué à Z avec N_{opt} comme taille de fenêtre.
2. L'argument qui maximise la fonctionnelle est repéré et noté n_{Tmax}. Puis, il sert d'approximation $(\hat{m}_k)_{FAS}$ de $\hat{m}_k$,

$$(\hat{m}_k)_{FAS} \quad := \quad T_e \, n_{Tmax}.$$

3. $(\hat{A}_k)_{FAS}$, connaissant $(\hat{m}_k)_{FAS}$, est approché tel que

$$(\hat{A}_k)_{FAS} \quad := \quad Z(n_{Tmax} \, T_e).$$

4. Enfin, $(\hat{\sigma^2}_k)_{FAS}$ est obtenu en utilisant le fait que $s_k(m + \dfrac{\sigma}{2} \, ; \, \theta) = Ae^{-\frac{1}{8}}$.

$$(\hat{\sigma}_k)_{FAS} \quad := \quad 2\Big(Z^{-1}\big(\, e^{-\frac{1}{8}}(\hat{A}_k)_{FAS} \,\big) - (\hat{m}_k)_{FAS}\Big).$$

5. Un nouveau signal Z_k est créé à partir de $(\hat{\theta}_k)_{FAS}$ et Z,

$$Z_k \quad := \quad Z - s_k((\hat{\theta}_k)_{FAS}).$$

6. Z_k devient Z, incrémentation de k, et retour à l'étape 1.

Dans le cas de l'observation Z de la figure 3, $K = 3$.
La détermination s'effectue donc en trois passes. Après la première passe de l'algorithme, le maximum est atteint pour $n_{Tmax} = 589$, soit $(\hat{m}_1)_{FAS} = 0,589$. Ce qui permet de trouver que $(\hat{\sigma}_1)_{FAS} = 0,021$ $(\hat{A}_1)_{FAS} = 3,157$. Le signal $Z_1 = Z - s_1((\hat{\theta}_1)_{FAS})$ est créé.
Le FAS est ensuite appliqué à Z_1, ce qui permet de calculer $n_{Tmax} = 514$, soit $(\hat{m}_2)_{FAS} = 0,514$ et $(\hat{\sigma}_2)_{FAS} = 0,024$. Puis, $(\hat{A}_2)_{FAS} = 0,879$. Le signal $Z_2 = Z_1 - s_2((\hat{\theta}_2)_{FAS})$ est créé.
Enfin, après le passage du FAS sur Z_2, $n_{Tmax} = 500$, soit $(\hat{m}_3)_{FAS} = 0,5$, $(\hat{\sigma}_3)_{FAS} = 0,002$. Puis, $(\hat{A}_3)_{FAS} = 0,55$.
Ainsi, en regroupant les résultats,

$$\hat{\theta}_{FAS} \quad = \quad [3,157 \, ; \, 0,021 \, ; \, 0,589 \, ; \, 0,879 \, ; \, 0,024 \, ; \, 0,514 \, ; \, 0,577 \, ; \, 0,002 \, ; \, 0,5],$$

à comparer avec IV.30 .
Le but n'est pas d'avoir $\hat{\theta}_{FAS}$ très proche de $\hat{\theta}$, mais juste une approximation cohérente des paramètres. C'est ce qui se passe avec l'exemple à trois cellules, où d'ailleurs les $\hat{m}_k$ sont bien détectés. Néanmoins, la section suivante qui porte sur l'estimation paramétrique de $\hat{\theta}$, reprend ce résultat et montre que si $\hat{\theta}_{FAS}$ fait office de condition initiale, l'algorithme utilisé converge bien vers $\hat{\theta}_{MV}$.
Le FAS utilisé en détection est donc un outil permettant de retrouver de l'information utile dans une observation bruitée en maximisant le rapport signal à bruit. Il permet en particulier d'obtenir une approximation de qualité moyenne de l'observation, mais rapide et automatique, suffisante pour fournir une condition initiale efficace à une routine d'optimisation.

6 ESTIMATION D'UNE ACTIVITÉ DE COURANT

A partir de l'observation IV.10, cette section montre comment construire un estimateur $\hat{\theta}$ du paramètre θ, optimal au sens du maximum de vraisemblance $\hat{\theta}_{MV}$.
Dans cette section est également utilisé le fait que dans le cas d'une observation additive gaussienne, les estimateurs $\hat{\theta}_{MV}$ et $\hat{\theta}_{MC}$ sont équivalents.
La démarche proposée est de s'intéresser tout d'abord au cas d'une seule cellule, $K = 1$, puis par extension au cas de l'activité de K cellules. L'algorithme EM est alors mis en place de sorte à remplacer le problème de la recherche de K cellules, par K problèmes de recherche d'une seule cellule.

6.1 Estimation de $\hat{\theta}_{MV}$

Le but est d'estimer $\hat{\theta}_{MV}$ ou de façon équivalente $\hat{\theta}_{MC}$ à partir d'une observation expérimentale idéale, construite avec $\hat{\theta}$ connu,

$$\mathbf{Z} \quad := \quad s(\hat{\theta}) + \mathbf{B}.$$

Le lot de mesures $\mathbf{Z}$ fait alors office d'observation dans le modèle IV.48, et le $\hat{\theta}_{MC}$ calculé à partir de ces données doit être proche de $\hat{\theta}$.
Le calcul de $\hat{\theta}_{MC}$ est effectué par l'algorithme de Gauss Newton IV.9.

6.2 Étude du résidu

Le résidu est le vecteur aléatoire de dimension N défini par

$$\zeta \quad := \quad \frac{Z - s(\hat{\theta}_{MV})}{\sigma_B}.$$

clairement, $\zeta \hookrightarrow \mathcal{N}(0,1)$ si bien que le carré de la norme euclidienne de ce vecteur suit une loi du χ^2 à $N - 3K$ degrés de liberté[6],

$$\|\zeta\|^2 \quad \hookrightarrow \quad \chi^2(N - 3K).$$

Il est alors possible d'appliquer à une réalisation de cette variable aléatoire le test du χ^2 de niveau $\alpha = 0,9$ [Pap02] p.p.361-364. d'une part, la valeur seuil $\chi^2_\alpha(N - 3K)$ est lue dans une table [Pap02] p.p.314, si après estimation la réalisation $\|\zeta\|^2$ est inférieure au seuil, alors le test est accepté, l'estimation est qualifiée de bonne.

[6]Le nombre d'échantillons moins le nombre de paramètres

Remarque : *Lorsque le nombre de mesures disponibles N est suffisamment grand, il est possible d'utiliser le résultat donné par [Joh94] affirmant que*

$$\sqrt{2\|\zeta\|^2} - \sqrt{2(N-3)-1} \quad \hookrightarrow \quad \mathcal{N}(0\,;\,1). \tag{IV.31}$$

En pratique, le test est accepté si la valeur est dans l'intervalle $[-3\,;\,3]$.

D'un point de vue physique, la minimisation du résidu atteste que la puissance de l'observation appelée σ_s^2 est conservée puisque pour un estimé donné,

$$\begin{aligned} \|Z - s(\hat{\theta}_{MV})\|^2 &= \sigma_B^2\zeta^2 \\ \sigma_Z^2 - 2Z^T s(\hat{\theta}_{MV}) + \sigma_s^2 &= \sigma_B^2\zeta^2 \\ \sigma_s^2 &= \sigma_B^2\zeta^2 - \sigma_Z^2 + 2Z^T s(\hat{\theta}_{MV}), \end{aligned}$$

or, si $\hat{\theta}_{MV}$ est bon, $Z \approx s(\hat{\theta}_{MV})$ et $\zeta \approx 0$, donc

$$\sigma_s^2 \approx \sigma_Z^2.$$

6.3 Performances optimales

Soit $\hat{\theta}_{MC}$ l'estimateur des moindres carrés pondérés.
Le fait que paramètre exact $\hat{\theta}$ soit connu permet, en amont du calcul de $\hat{\theta}_{MC}$, de donner l'expression de la matrice d'information de Fisher $I(\hat{\theta})$ et donc de la borne de Cramèr-Rao exacte $BCR(\hat{\theta}) = I^{-1}(\hat{\theta})$, toutes deux de dimension $(3,3)$, à partir de l'expression IV.11. Ces quantités sont, par construction, optimales et servent donc de référence, la borne de Cramèr-Rao renseigne sur la plus petite variance pouvant être atteinte par $\hat{\theta}_{MC}$.
Afin de caractériser statistiquement l'estimateur $\hat{\theta}_{MC}$, il faut déterminer ses statistiques d'ordre 2, à savoir $\mathbb{E}\left[\hat{\theta}_{MC}\right]$ puis $Cov(\hat{\theta}_{MC})$. Or, ces quantités sont difficilement accessibles car $\hat{\theta}_{MC}$ n'a pas de forme analytique. Une solution consiste alors à effectuer des simulations de Monte Carlo pour s'en approcher par l'intermédiaire du calcul de la moyenne empirique et de la matrice de variance covariance empirique . Pour ce faire, l'algorithme qui calcule θ_{MC} est exécuté N_{tir} fois à partir de N_{tir} observations différentes $\{Z^j\}_{j=1\ldots N_{tir}}$, construites selon les relations suivantes,

$$\mathbb{E}\left[\hat{\theta}_{MC}\right] \approx \bar{\theta}_{MC} = \frac{1}{N_{tir}} \sum_{j=1}^{N_{tir}} \hat{\theta}_{MC}^j \tag{IV.32}$$

et

$$Cov[\hat{\theta}_{MC}] \approx \frac{1}{N_{tir}-1} \sum_{j=1}^{N_{tir}} (\hat{\theta}_{MC}^j - \bar{\theta}_{MC})(\hat{\theta}_{MC}^j - \bar{\theta}_{MC})^T. \tag{IV.33}$$

En pratique, $\mathbb{E}\left[\hat{\theta}_{MC}\right]$ est à rapprocher de $\hat{\theta}$ et $Cov[\hat{\theta}_{MC}]$ est à comparer à $BCR(\hat{\theta}_{MC})$. Afin d'illustrer l'influence de ces deux quantités, il est possible de représenter dans l'espace isomorphe à $\mathbb{R}^3$ l'ensemble des N_{tir} estimés, entourés de l'ellipsoïde de confiance de niveau $\alpha = 0,9$.
En pratique, ce tracé est possible d'après la proposition suivante

Proposition IV.3. *soit R une matrice symétrique définie positive de dimension $(3\,;\,3)$, μ un vecteur de $\mathbb{R}^3$ fixé, X un vecteur de $\mathbb{R}^3$ et r un scalaire positif. Alors, l'ensemble*

$$(X-\mu)^T R^{-1} (X-\mu) = r^2 \tag{IV.34}$$

décrit un ellipsoïde de révolution.

Preuve . *R une matrice symétrique définie positive, donc régulière*[7] *et diagonalisable avec des valeurs propres réelles et positives, si bien qu'il existe une matrice de passage P de dimension $(3\,;\,3)$, orthogonale*[8]*, et une matrice diagonale D de dimension $(3\,;\,3)$ telles que*

$$R \;=\; PDP^T.$$

R se factorise facilement en un produit de deux matrices orthogonales,

$$R \;=\; PD^{\frac{1}{2}}D^{\frac{1}{2}}P^T = \left(PD^{\frac{1}{2}}\right)\left(PD^{\frac{1}{2}}\right)^T,$$

où $D^{\frac{1}{2}}$ est la matrice diagonale contenant la racine carrée des éléments de D. Par ailleurs,

$$\begin{aligned} R^{-1} &= \left(PDP^T\right)^{-1} \\ &= P^{-T}D^{-1}P^{-1} \\ &= PD^{-1}P^T \\ &= P(D^{\frac{1}{2}})^{-1}(D^{\frac{1}{2}})^{-1}P^T \end{aligned}$$

si bien que la forme quadratique engendré par R^{-1} se factorise elle aussi facilement,

$$\begin{aligned} (X-\mu)^T R^{-1}(X-\mu) &= (X-\mu)^T R^{-1}(X-\mu) \\ &= \underbrace{(X-\mu)^T P(D^{\frac{1}{2}})^{-1}}_{=\xi^T}\underbrace{(D^{\frac{1}{2}})^{-1}P^T(X-\mu)}_{:=\xi} \end{aligned}$$

Alors, pour tout r réel positif l'ensemble IV.34 est non-vide et son expression se ramène à

$$\|\xi\|^2 \;=\; r^2,$$

les valeurs propres de D étant toutes réelles positives, lorsque X parcours $\mathbb{R}^3$, l'ensemble décrit un ellipsoïde de révolution, centré en μ.
Il est utile pour la suite d'avoir à disposition une représentation paramétrique de cette dernière, pour cela soit le vecteur $\xi(\psi\,;\,\phi)$, paramétré en coordonnées sphériques de sorte à décrire une sphère de rayon r,

$$\xi(\psi\,;\,\phi) := r\begin{bmatrix} \cos(\psi)\sin(\phi) \\ \sin(\psi)\sin(\phi) \\ \cos(\phi) \end{bmatrix} \quad \forall\psi\in[0\,;\,2\pi]\,;\,\forall\phi\in[0\,;\,\pi[$$

et de ce qui précède,

$$\begin{aligned} \xi(\psi\,;\,\phi) &= (D^{\frac{1}{2}})^{-1}P^T(X-\mu) \Leftrightarrow \\ PD^{\frac{1}{2}}\xi(\psi\,;\,\phi) &= (X-\mu) \Leftrightarrow \\ X &= \mu + PD^{\frac{1}{2}}\xi(\psi\,;\,\phi), \end{aligned}$$

cette relation se prêtant parfaitement à la programmation.
D'un point de vue géométrique, la dernière équation montre que l'ellipsoïde que décrit X peut être vue comme l'image de la sphère unité $\xi(\psi\,;\,\phi)$ par la transformation de l'espace qui est la composée de la translation de vecteur μ d'une rotation dont l'angle est déterminé par la matrice P et d'une homothétie dont le rapport est caractèrisé par la matrice $(D^{\frac{1}{2}})^{-1}$. Ainsi, la sphère est décentrée puis déformée pour prendre la forme d'un ellipsoïde de révolution.

□

[7] R^{-1} a un sens.
[8] $P^{-1} = P^T$

6.4 Estimation d'une cellule bruitée, $K = 1$

Dans ce cas, l'observation représente l'activité d'une seule cellule bruitée. Cette dernière est disponible sous la forme d'un vecteur $\mathbf{Z}$ de dimension N, de coordonnées les échantillons du signal $\mathbf{Z}(t)$ échantillonné sur un intervalle de temps $[0\,;\,T]$ à la période T_e. Le modèle a pour expression, selon IV.4 et IV.5,

$$\mathbf{Z} \quad = \quad s(\theta) + \mathbf{B}, \tag{IV.35}$$

de coordonnées, selon IV.1 et IV.2,

$$\mathbf{Z}_n \quad = \quad Ae^{-\frac{1}{2\sigma^2}(nT_e - m)^2} + \mathbf{B}_n \quad \forall n = 1 \ldots N. \tag{IV.36}$$

Le bruit est représenté par le vecteur $\mathbf{B}$, gaussien, centré de matrice de variance covariance $\Gamma_{BB} := \sigma_B^2 \mathrm{Id}_N$.
Les paramètres à optimiser sont A, σ et m, regroupés dans le vecteur paramètre $\theta \in \mathbb{R}_+^3$ défini par

$$\theta \quad := \quad [A, \sigma, m]^T.$$

6.4.1 Expérimentation

L'observation construite est présentée figure 8. Dans ce cas, les 3 paramètres recherchés valent

$$\hat{\theta} \quad := \quad [3\,;\,0,01\,;\,0,5]^T,$$

le pas d'échantillonnage est pris à $T_e = 10^{-3}$ (sec) si bien que l'observation est disponible sous la forme de $N = 1001$ points.

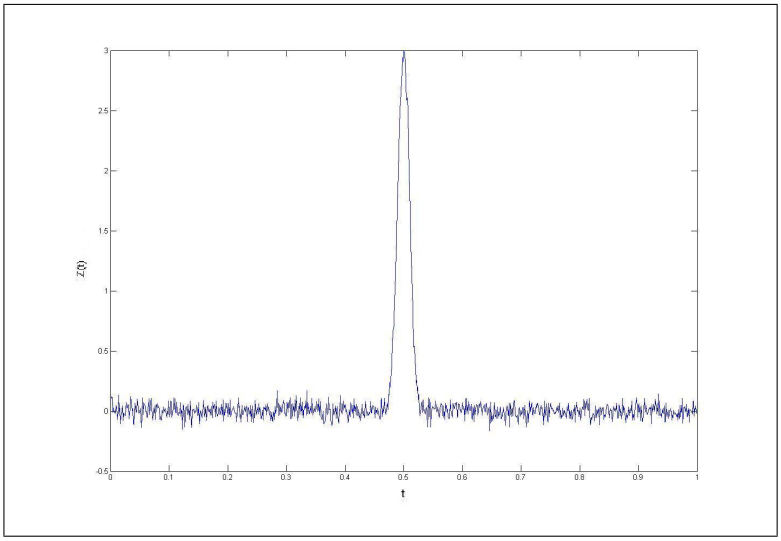


FIG. 8 – *Observation Z correspondant à une cellule bruitée.*

La matrice d'information de Fisher théorique est alors calculée selon l'expression IV.11, et par inversion la borne de Cramèr-Rao théorique,

$$BCR(\hat{\theta}) := \begin{bmatrix} 2,116.10^{-4} & -4,7016.10^{-7} & -4,0107.10^{-25} \\ -4,7016.10^{-7} & 3,1344.10^{-9} & -1,9117.10^{-25} \\ -4,0107.10^{-25} & -1,9117.10^{-25} & 3,1344.10^{-9} \end{bmatrix}.$$

Les valeurs sont extrêmement faibles, à la limite de la précision machine pour certaines. L'analyse de la borne laisse augurer la possibilité de construire un estimateur à très faible variance, donc de très bonne qualité.
Le FAS détection est appliqué à l'observation avec une taille de fenêtre de $M = 23$ pixels déterminée expérimentalement. Le résultat de cette détection est présentée figure 11. Le résultat est bon, il n'y a pas de fausse alarme.

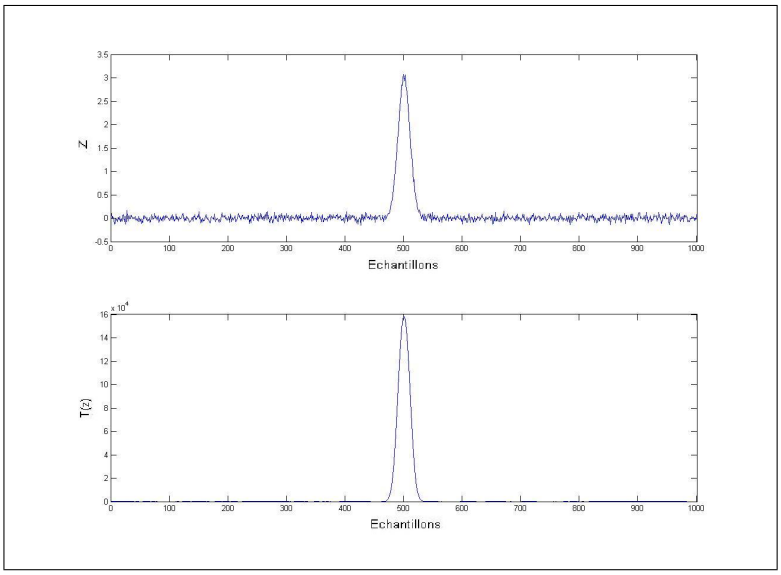


FIG. 9 – *Observation Z (haut) et fonctionnelle $T(z)$ (bas).*

Cela n'a rien de surprenant tant le rapport signal à bruit est favorable dans ce cas, $RSB \approx 120dB$. Ainsi, les paramètres sont récupérés selon la technique proposée section 5.5.3, donnant comme valeur

$$\hat{\theta}_{FAS} := [3,02\,;\,0,011\,;\,0,501]^T,$$

soit de très bons résultats vu la simplicité de la technique. $\hat{\theta}_{MC}$ est alors calculé par l'algorithme IV.9, qui converge[9] en seulement deux itérations et donne

$$\hat{\theta}_{MC} := [3,0066\,;\,0,0099835\,;\,0,50002]^T.$$

L'estimation est donc réussie, comme le montre la figure 10.

[9]Le test d'arret porte sur le résidu

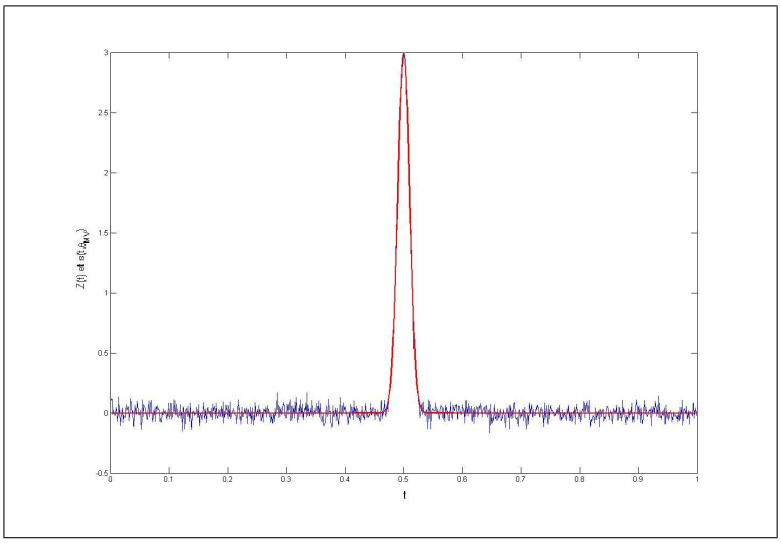


FIG. 10 – *Observation Z et estimé $s(\hat{\theta}_{MC})$ (trait gras).*

Le résidu ζ est alors calculé, son graphe est présenté figure 11, ce dernier, vu comme la réalisation d'un vecteur aléatoire, doit avoir le comportement d'un vecteur gaussien centré réduit.

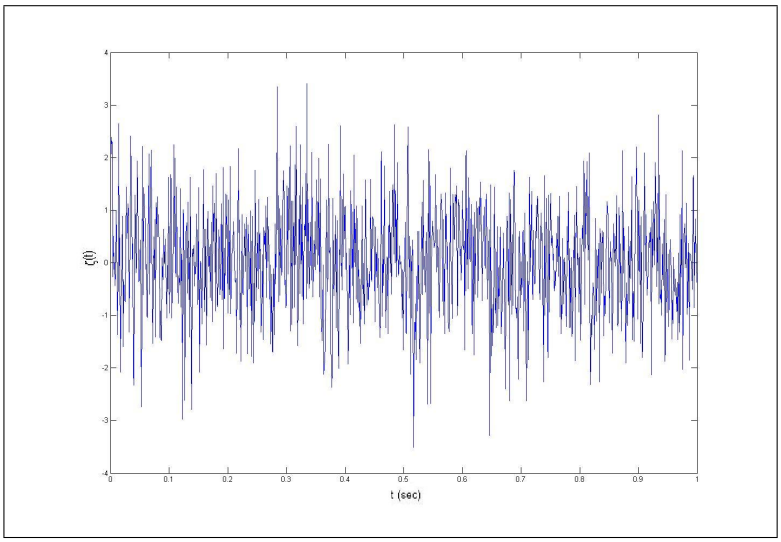


FIG. 11 – *Résidu ζ.*

Cette tendance est confirmé par le test du χ^2 à 998 degrés de liberté. Pour cette valeur le seuil est $\chi^2_s = 1055,6$ et le calcul montre que $\|\zeta\|^2 = 1050,1$. De plus,

$$\sqrt{2\|\zeta\|^2} - \sqrt{2(N-3)-1} \quad \approx \quad \sqrt{2100,2} - \sqrt{1995} \approx 1,16$$

qui peut bien être vue comme la réalisation d'une variable aléatoire gaussienne centrée réduite IV.31.
Fort de ce succès, les moments de $\hat{\theta}_{MC}$ sont estimés par simulations de Monte Carlo sur $N_{tir} = 1000$ tirages,

$$\mathbb{E}\left[\hat{\theta}_{MC}\right] \quad \approx \quad [3,0004\,;\,0,009998\,;\,0,5]^T$$

et

$$Cov[\hat{\theta}_{MC}] \approx \begin{bmatrix} 2,136.10^{-4} & -4,367.10^{-7} & 4,774.10^{-8} \\ -4,367.10^{-7} & 2,92.10^{-9} & -1,663.10^{-10} \\ 4,774.10^{-8} & -1,663.10^{-10} & 2,913.10^{-9} \end{bmatrix}.$$

Ces résultats sont à interpréter avec prudence, vu que certains éléments diagonaux de la matrice sont inférieurs à ceux de la borne. Cela est dû au bruit d'estimation de la matrice de variance covariance empirique, prépondérant dans le cas des valeurs traitées. L'interprétation la plus juste est que l'estimateur a une variance très proche de la BCR théorique et qu'il peut donc être qualifié d'efficace. En guise d'illustration, les figures 12 et 13 montrent les 1000 réalisations ainsi que l'ellipsoïde de confiance de niveau $0,9$[10], calculée dans la premier cas avec $BCR(\hat{\theta})$

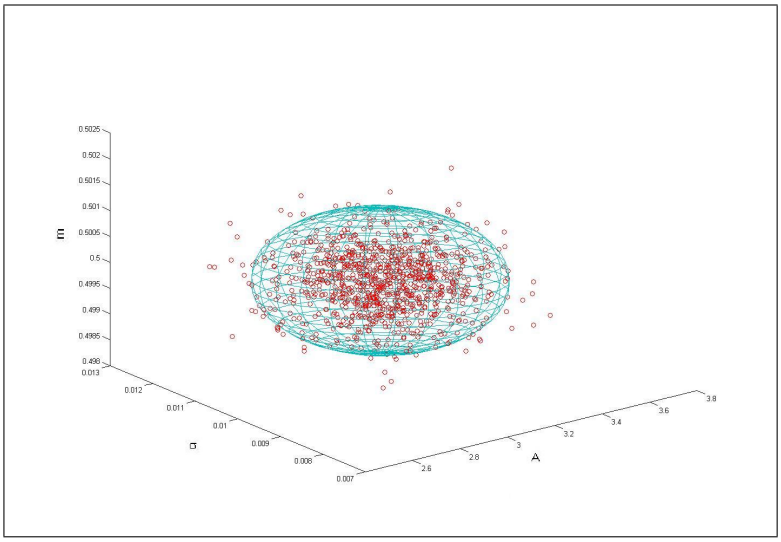


FIG. 12 – *Représentation des* 1000 *estimés ainsi que l'ellipsoïde de confiance de niveau* $0,9$ *calculé avec* $BCR(\hat{\theta})$

et dans le second avec $Cov[\hat{\theta}_{MC}]$ empirique.

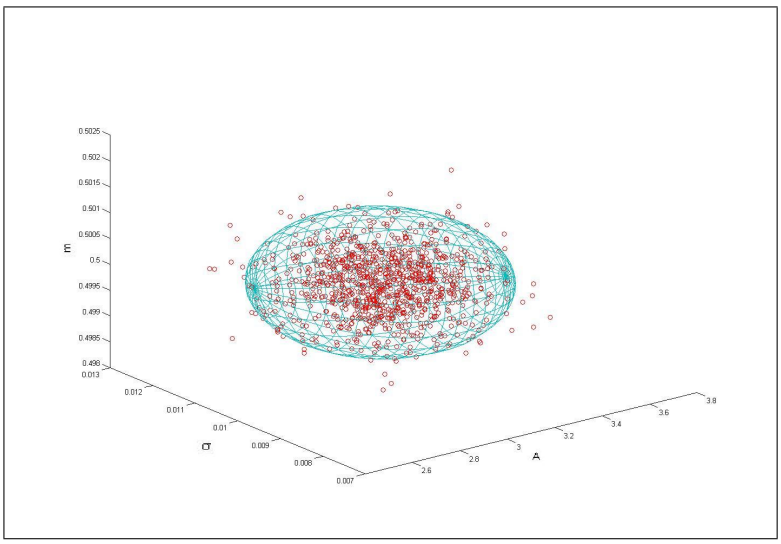


FIG. 13 – *Représentation des* 1000 *estimés ainsi que l'ellipsoïde de confiance de niveau* $0,9$ *calculé avec* $Cov[\hat{\theta}_{MC}]$

Dans des cas expérimentaux sur données réelles, le signal d'intérêt n'est pas disponible, si bien que la matrice d'information de Fisher non plus, ce qui signifie que seule la seconde ellipsoïde est disponible.
Cet exemple simple montre qu'il est aisé d'estimer 1 cellule, et ceci de façon précise. Ainsi, le

[10] 90% des valeurs doivent être à l'intérieur de l'ellipsoïde

problème général à K cellules fait partie de la classe de problèmes difficiles, sauf dans le cas $K = 1$.
A ce point de l'étude, l'idéal serait d'avoir à disposition un algorithme d'estimation capable de transformer la résolution d'un problème à K cellules en la résolution de K problèmes à 1 cellule. L'algorithme EM répond à cette problématique, voilà pourquoi la section suivante fait l'objet de son développement, avant de l'utiliser pour répondre à des problèmes à K cellules, avec $K > 1$.

6.5 Algorithme Expectation-Maximization (EM)

Cette section présente l'algorithme d'optimisation EM. La modélisation IV.12 y est utilisée. Le point de départ est donc identique à celui de la construction du filtre de Kalman. Il s'agit d'un algorithme calculant le paramètre qui maximise la vraisemblance d'une observation $\mathbf{Y}$, appelé donnée incomplète par l'intermédiaire de l'état $\mathbf{X}$, appelée donnée complète. Depuis 1977 et l'article de [Dem77], le nombre de travaux utilisant l'EM n'a cessé de croître, dans le domaine du traitement d'antenne ou de l'estimation de densité de probabilité multimodales par exemple, en témoigne l'abondante littérature relative au sujet. La technique est d'ailleurs déclinée sous une version recuit simulé [Cel89].
La façon de présenter cette méthode est inspirée de [Jau06], la présentant dans un cadre plus large que celui additif gaussien.

6.5.1 Principe général, $\mathbf{Y} = \Xi(\mathbf{X}(\theta))$

Compte tenu du fait que les vecteurs aléatoires $\mathbf{X}(\theta)$ et $\mathbf{Y}$ sont liés par la fonction Ξ, leurs densités de probabilité le sont également,

$$p_{\mathbf{X}(\theta)}(x;\theta) = p_{\mathbf{X}(\theta)/Y=X(\theta)}(x;\theta)p_{\mathbf{Y}}(\Xi(x);\theta),$$

où de façon équivalente en prenant membre à membre le logarithme ,

$$\ln\left(p_{\mathbf{Y}}(\Xi(x);\theta)\right) = \ln\left(p_{\mathbf{X}(\theta)}(x;\theta)\right) - \ln\left(p_{\mathbf{X}(\theta)/Y=\Xi(X(\theta))}(x;\theta)\right).$$

Cette relation, qui ressemble à la formule de Bayes, est la clef de voûte de l'algorithme EM.
Rien n'empêche de transformer cette égalité fonctionnelle en une égalité de processus aléatoires. Pour ce faire, il faut composer chaque fonction avec le vecteur aléatoire $\mathbf{X}(\theta)$, pour obtenir

$$\ln\left(p_{\mathbf{Y}}(\Xi(\mathbf{X}(\theta));\theta)\right) = \ln\left(p_{\mathbf{X}(\theta)}(\mathbf{X}(\theta);\theta)\right) - \ln\left(p_{\mathbf{X}(\theta)/Y=\Xi(X(\theta))}(\mathbf{X}(\theta);\theta)\right)$$

soit encore

$$\ln\left(p_{\mathbf{Y}}(\mathbf{Y};\theta)\right) = \ln\left(p_{\mathbf{X}(\theta)}(\mathbf{X}(\theta);\theta)\right) - \ln\left(p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)\right). \tag{IV.37}$$

L'étape suivante consiste à prendre l'espérance conditionnelle de la relation précédente, conditionnée par $\mathbf{Y} = y$, c'est-à-dire pour une réalisation de Y donnée et pour un paramètre quelconque θ'. Il vient,

$$\mathbb{E}\left[\ln\left(p_{\mathbf{Y}}(\mathbf{Y};\theta)\right)|\mathbf{Y}=y,\theta'\right] = \mathbb{E}\left[\ln\left(p_{\mathbf{X}(\theta)}(\mathbf{X};\theta)\right)|\mathbf{Y}=y,\theta'\right] - \mathbb{E}\left[\ln\left(p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)\right)|\mathbf{Y}=y,\theta'\right]$$

Explicitons les trois termes constituant cette relation. Concernant celui du membre gauche de l'égalité,

$$\mathbb{E}\left[\ln\left(p_{\mathbf{Y}}(\mathbf{Y};\theta)\right)|\mathbf{Y}=y,\theta'\right] = \int_{\mathbb{R}^n} \ln\left(p_{\mathbf{Y}}(y;\theta)\right)p_{\mathbf{X}|\mathbf{Y}=y}(u,\theta')du = \ln\left(p_{\mathbf{Y}}(y;\theta)\right). \tag{IV.38}$$

Concernant les deux du membre droit de l'égalité, d'une part

$$\mathbb{E}\left[\ln\left(p_{\mathbf{X}(\theta)}(\mathbf{X};\theta)\right)|\mathbf{Y}=y,\theta'\right]=\int_{\mathbb{R}^n}\ln\left(p_{\mathbf{X}(\theta)}(u;\theta)\right)p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(u,\theta')du, \tag{IV.39}$$

d'autre part,

$$\mathbb{E}\left[\ln\left(p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)\right)|\mathbf{Y}=y,\theta'\right]=\int_{\mathbb{R}^n}\ln\left(p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(u;\theta)\right)p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(u,\theta')du. \tag{IV.40}$$

La quantité IV.38 est la log-vraisemblance $l(\theta)$ de l'observation y et par conséquent ne dépend que de θ, ce qui permet de définir pou toute observation y

$$l:=\left\{\begin{array}{ccc} D^K & \rightarrow & \mathbb{R} \\ \theta & \mapsto & l(\theta)=\ln\left(p_{\mathbf{Y}}(y;\theta)\right)\end{array}\right.$$

D'autre part, u étant une variable d'intégration muette, les deux relations (IV.39) et (IV.40) ne dépendent uniquement que de θ et θ', cela invite à définir deux fonctions :

$$U:=\left\{\begin{array}{ccc} D^K & \rightarrow & \mathbb{R} \\ \theta & \mapsto & U(\theta;\theta')=\mathbb{E}\left[\ln\left(p_{\mathbf{X}(\theta)}(\mathbf{X}(\theta);\theta)\right)/\mathbf{Y}=y,\theta'\right] \quad \forall\theta'\in D\end{array}\right. , \tag{IV.41}$$

$U(\theta;\theta')$ est l'espérance mathématique conditionnelle de la log-vraisemblance de $\mathbf{X}(\theta)$, et

$$V:=\left\{\begin{array}{ccc} D^K & \rightarrow & \mathbb{R} \\ \theta & \mapsto & V(\theta;\theta')=\mathbb{E}\left[\ln\left(p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)\right)/\mathbf{Y}=y,\theta'\right] \quad \forall\theta'\in D\end{array}\right.$$

Avec ce formalisme, la relation (IV.37) s'écrit de façon plus simple,

$$l(\theta)=U(\theta;\theta')-V(\theta;\theta') \quad \forall\theta'\in D^K. \tag{IV.42}$$

$l(\theta)$ est la grandeur que l'on cherche à maximiser dans le cadre traditionnel de l'estimation paramétrique du maximum de vraisemblance d'une observation. Or, le contexte duquel l'observation est issue, fait que cette maximisation est difficile, ceci principalement en raison de la présence d'extrema locaux de la fonction coût $Q(\theta)$ définie dans la section 4. Ainsi, l'idée sous-jacente au vu de la relation IV.42 est de maximiser $U(\theta;\theta')$ en lieu et place de la log-vraisemblace $L(\theta)$. Ceci est possible grâce au théorème suivant.

Proposition IV.4.

$$V(\theta;\theta')\leq V(\theta';\theta') \quad \forall\theta\,,\,\theta'\in D^K.$$

Preuve . *La démonstration repose sur l'inégalité de Jensen* [11]*, ainsi que sur la linéarité de l'opérateur d'espérance et de la fonction logarithme.*

$$\begin{aligned} V(\theta;\theta')-V(\theta';\theta') &= \mathbb{E}\left[\ln\left(p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)\right)/\mathbf{Y}=y,\theta'\right]-\mathbb{E}\left[\ln\left(p_{\mathbf{X}(\theta')/\mathbf{Y}=y}(\mathbf{X}(\theta');\theta')\right)/\mathbf{Y}=y,\theta'\right] \\ &= \mathbb{E}\left[ln\left[\frac{p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)}{p_{\mathbf{X}(\theta')/\mathbf{Y}=y}(\mathbf{X}(\theta');\theta')}\right]/\mathbf{Y}=y,\theta'\right] \\ &\leq ln\left[\mathbb{E}\left[\frac{p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)}{p_{\mathbf{X}(\theta')/\mathbf{Y}=y}(\mathbf{X}(\theta');\theta')}/\mathbf{Y}=y,\theta'\right]\right]\end{aligned}$$

[11] Si f est une fonction continue et concave, alors pour $\{x_n\}_{n=1\ldots N}$, $\frac{1}{N}\sum_{n=1}^{N}f(x_n)\leq f(\frac{1}{N}\sum_{n=1}^{N}x_n)$.

Or, en explicitant le membre droit de l'inégalité,

$$\begin{aligned}\mathbb{E}\left[\frac{p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)}{p_{\mathbf{X}(\theta')/\mathbf{Y}=y}(\mathbf{X}(\theta');\theta')}/\mathbf{Y}=y,\theta'\right] &= \int_{\mathbb{R}^{NK}}\frac{p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(u;\theta)}{p_{\mathbf{X}(\theta')/\mathbf{Y}=y}(u;\theta')}p_{\mathbf{X}(\theta')/\mathbf{Y}=y}(u;\theta')\,du \\ &= \int_{\mathbb{R}^{NK}} p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(u;\theta)\,du \\ &= 1,\end{aligned}$$

et ainsi

$$\begin{aligned}ln\left[\mathbb{E}\left[\frac{p_{\mathbf{X}(\theta)/\mathbf{Y}=y}(\mathbf{X}(\theta);\theta)}{p_{\mathbf{X}(\theta')/\mathbf{Y}=y}(\mathbf{X}(\theta');\theta')}/\mathbf{Y}=y,\theta'\right]\right] &= 0 \Leftrightarrow \\ & V(\theta;\theta')-V(\theta';\theta')\leq 0.\end{aligned}$$

□

Ce résultat implique que

$$\begin{aligned}U(\theta;\theta') &\geq U(\theta';\theta') \Rightarrow \\ U(\theta;\theta')-V(\theta;\theta') &\geq U(\theta';\theta')-V(\theta';\theta') \\ l(\theta) &\geq l(\theta').\end{aligned}$$

Autrement dit, si pour θ' donné, θ'' maximise la fonction $\theta \mapsto U(\theta;\theta')$, alors la vraisemblance augmente : $l(\theta'') \geq l(\theta')$.

Remarque : *Le calcul de $V(\theta;\theta')$ n'est donc pas utile.*

Cette démarche itérative ainsi induite constitue le principe de base de l'algorithme EM.
Si le j-uplet $\{\hat{\theta}^{(0)};\hat{\theta}^{(1)};\ldots;\hat{\theta}^{(j-1)}\}$ est connu, alors, $\hat{\theta}^{(j)}$ est obtenu au prix de deux étapes, l'étape *Expectation - E* puis l'étape *Maximization - M*,

$$\begin{cases}\text{E} : \text{Calcul de} & U(\theta;\hat{\theta}^{(j-1)}) \\ \text{M} : \text{Calcul de} & \theta^{(j)} = \underset{\theta\in D^K}{\operatorname{argmax}}[U(\theta;\hat{\theta}^{(j-1)})]\end{cases}$$

Ce résultat est tout à fait général, en rappelant qu'aucune hypothèse n'est faite sur Ξ.
Par ailleurs, pour pourvoir implémenter cet algorithme, il faut être en mesure de pouvoir calculer la quantité $U(\theta;\hat{\theta}^{(j-1)})$, définie par IV.41, ce qui dans la majeure partie des cas est impossible, analytiquement du moins, sauf dans le cas linéaire gaussien. Voilà l'objet de la prochaine section.

6.5.2 Cas gaussien linéaire où $\mathbf{Y} = \Xi\mathbf{X}(\theta)$

Le cas linéaire gaussien est intéressant à double titre. D'une part, il correspond au modèle d'observation choisi en début de chapitre, lorsque ce dernier est écrit sous la forme IV.13. D'autre part, il est possible dans ce cas de déterminer analytiquement $U(\theta;\theta')$ et donc d'utiliser l'algorithme EM pour déterminer θ_{MV}. Ceci est possible en vertu de la proposition suivante, qui apparaît également dans la construction du filtre de Kalman-Bucy. Le déroulement de la théorie s'appuie sur l'article de Jauffret et Santori [Jau06], dont il ne s'agit ici que d'un cas particulier.

Proposition IV.5. *Soit* $\mathbf{X}$ *et* $\mathbf{Y}$ *deux vecteurs aléatoires gaussiens tels que*

$$\begin{cases} \mathbf{X} & \hookrightarrow & \mathcal{N}(\mu_X, \Gamma_{XX}) \\ \mathbf{Y} & \hookrightarrow & \mathcal{N}(\mu_Y, \Gamma_{YY}) \end{cases},$$

ayant pour réalisation X *et* Y*, et avec* Γ_{YY} *inversible, alors,*

$$\mathbf{X}/\mathbf{Y} = Y \quad \hookrightarrow \quad \mathcal{N}\left(\mu_X + \Gamma_{XY}\Gamma_{YY}^{-1}(Y - \mu_Y), \Gamma_{XX} - \Gamma_{XY}\Gamma_{YY}^{-1}\Gamma_{XY}^T\right),$$

avec

$$\Gamma_{XY} \quad := \quad \mathbb{E}\left[(\mathbf{X} - \mu_X)(\mathbf{Y} - \mu_Y)^T\right]$$

.

La preuve est donnée par [Kay93], p.p. 337-339.

Corollaire IV.1. *Si de plus, il existe une matrice* Ξ *telle que* $Y = \Xi X$*, alors*

$$\begin{aligned} \Gamma_{XY} &= \mathbb{E}\left[(\mathbf{X} - \mu_X)(\mathbf{Y} - \mu_Y)^T\right] \\ &= \mathbb{E}\left[(\mathbf{X} - \mu_X)(\Xi\mathbf{X} - \Xi\mu_X)^T\right] \\ &= \mathbb{E}\left[(\mathbf{X} - \mu_X)(\mathbf{X} - \mu_X)^T\Xi^T\right] \\ &= \Gamma_{XX}\Xi^T \end{aligned}$$

, et

$$\begin{aligned} \Gamma_{YY} &= \mathbb{E}\left[(\mathbf{Y} - \mu_Y)(\mathbf{Y} - \mu_Y)^T\right] \\ &= \mathbb{E}\left[(\Xi\mathbf{Y} - \Xi\mu_Y)(\Xi\mathbf{Y} - \Xi\mu_Y)^T\right] \\ &= \Xi\mathbb{E}\left[(\mathbf{X} - \mu_X)(\mathbf{X} - \mu_X)^T\Xi^T\right] \\ &= \Xi\Gamma_{XX}\Xi^T \end{aligned}$$

. Dans ce cas,

$$\begin{cases} \mu_X + \Gamma_{XY}\Gamma_{YY}^{-1}(Y - \mu_Y) &= \underbrace{\mu_X + \Gamma_{XX}\Xi^T(\Xi\Gamma_{XX}\Xi^T)^{-1}(Y - \Xi\mu_X)}_{(1)} \\ & \textit{et} \\ \Gamma_{XX} - \Gamma_{XY}\Gamma_{YY}^{-1}\Gamma_{XY}^T, &= \underbrace{\Gamma_{XX} - \Gamma_{XX}\Xi^T(\Xi\Gamma_{XX}\Xi^T)^{-1}\Xi\Gamma_{XX}}_{(2)} \end{cases}$$

et finalement

$$\mathbf{X}/\mathbf{Y} = Y \quad \hookrightarrow \quad \mathcal{N}\Big((1), (2)\Big)$$

.

Ainsi, l'application de ces résultats au modèle IV.13 permet de donner l'expression de la loi conditionnelle de $\mathbf{X}$, sachant que Y, réalisation de $\mathbf{Y}$, est disponible, avec $\mu_X = \xi(\theta)$ et $\Gamma_{XX} = \frac{\sigma_B^2}{K}\mathrm{Id}_{NK}$,

$$\begin{cases} \mu_X + \Gamma_{XX}\Xi^T(\Xi\Gamma_{XX}\Xi^T)^{-1}(Y - \Xi\mu_X) &= \xi(\theta) + \frac{\sigma_B^2}{K}\Xi^T(\frac{\sigma_B^2}{K}\Xi\Xi^T)^{-1}(Y - \Xi\xi(\theta)) \\ &= \xi(\theta) + \Xi^T(\Xi\Xi^T)^{-1}(Y - \Xi\xi(\theta)) \\ & \text{et} \\ \Gamma_{XX} - \Gamma_{XX}\Xi^T(\Xi\Gamma_{XX}\Xi^T)^{-1}\Xi\Gamma_{XX} &= \frac{\sigma_B^2}{K}\mathrm{Id}_{NK} - \frac{\sigma_B^4}{K^2}\Xi^T(\frac{\sigma_B^2}{K}\mathrm{Id}_{NK}\Xi\Xi^T)^{-1}\Xi \\ &= \frac{\sigma_B^2}{K}(\mathrm{Id}_{NK} - \Xi^T(\Xi\Xi^T)^{-1}\Xi), \end{cases}$$

sous réserve que $\Xi\Xi^T$ soit régulière[12], ce qui est le cas dès lors que $K \geq 1$. Le calcul matriciel montre que

$$\Xi\Xi^T = KId_N,$$

Donc, l'évènement $\mathbf{X}(\theta)/\mathbf{Y} = Y$ obéit à une loi gaussienne,

$$\mathbf{X}/\mathbf{Y} = Y \hookrightarrow \mathcal{N}\left(\xi(\theta) + \frac{1}{K}\Xi^T(Y - \Xi\xi(\theta)), \frac{\sigma_B^2}{K}(\mathrm{Id}_{NK} - \frac{1}{K}\Xi^T\Xi)\right). \quad \text{(IV.43)}$$

Grâce à ce résultat, le calcul de $U(\theta;\theta')$ défini par IV.41 est désormais possible. Tout d'abord, d'après IV.43,

$$\begin{aligned} p_X(x/\theta) &= \frac{1}{\sqrt{2\pi(\frac{\sigma_B^2}{K})^{NK}}} e^{-\frac{1}{2}(x-\xi(\theta))^T(\frac{\sigma_B^2}{K}\mathrm{Id}_{NK})^{-1}(x-\xi(\theta))} \\ &= Ce^{-\frac{K}{2\sigma_B^2}(x-\xi(\theta))^T(x-\xi(\theta))} \end{aligned}$$

où C est une constante réelle strictement positive.

$$ln(p_X(x)) = c - \frac{K}{2\sigma_B^2}(x - \xi(\theta))^T(x - \xi(\theta)). \quad \text{(IV.44)}$$

Donc, en composant la relation fonctionnelle IV.44 avec le vecteur aléatoire $X(\theta)$

$$ln(p_X(\mathbf{X}(\theta))) = c - \frac{K}{2\sigma_B^2}(\mathbf{X}(\theta) - \xi(\theta))^T(\mathbf{X}(\theta) - \xi(\theta)),$$

$U(\theta,\theta')$ est obtenu par passage à l'espérance conditionnelle,

$$\begin{aligned} U(\theta,\theta') &= \mathbb{E}[ln(p_X(\mathbf{X}(\theta)))/\mathbf{Y} = Y, \theta'] \\ &= c - \frac{K}{2\sigma_B^2}\mathbb{E}[(\mathbf{X}(\theta) - \xi(\theta))^T(\mathbf{X}(\theta) - \xi(\theta))/\mathbf{Y} = Y, \theta'], \quad \text{(IV.45)} \\ &= c - \frac{K}{2\sigma_B^2}\mathbb{E}[\mathbf{X}^T(\theta)\mathbf{X}(\theta) - \mathbf{X}^T(\theta)\xi(\theta) - \xi^T(\theta)\mathbf{X}(\theta) + \xi^T(\theta)\xi^(\theta)/\mathbf{Y} = Y, \theta'] \\ &= c - \frac{K}{2\sigma_B^2}\Big(\mathbb{E}[\mathbf{X}^T(\theta)\mathbf{X}(\theta)/\mathbf{Y} = Y, \theta'] - \mathbb{E}[\mathbf{X}^T/\mathbf{Y} = Y, \theta']\xi(\theta) \\ &\quad -\xi^T(\theta)\mathbb{E}[\mathbf{X}(\theta)/\mathbf{Y} = Y, \theta'] + \xi^T(\theta)\xi(\theta)\Big). \quad \text{(IV.46)} \end{aligned}$$

Si par définition,

$$\begin{aligned} \hat{X}(\theta') &:= \mathbb{E}[\mathbf{X}(\theta)/\mathbf{Y} = Y, \theta'] \\ &= \xi(\theta') + \frac{1}{K}\Xi^T(Y - \Xi\xi(\theta')), \end{aligned}$$

alors il est possible d'exprimer $U(\theta,\theta')$ sous une forme plus explicite.
Le terme $\mathbf{X}^T(\theta)\mathbf{X}(\theta)$ est une forme quadratique, donc

$$\begin{aligned} \mathbf{X}^T(\theta)\mathbf{X}(\theta) &= \text{Trace}\left[\mathbf{X}^T(\theta)\mathbf{X}(\theta)\right] \\ &= \text{Trace}\left[\mathbf{X}(\theta)\mathbf{X}^T(\theta)\right], \end{aligned}$$

[12]Pour les modèles linéaires, ceci est une condition nécessaire et suffisante d'observabilité

l'opérateur Trace étant invariant par permutation circulaire. Ainsi d'après IV.43,

$$\begin{aligned}\mathbb{E}[\mathbf{X}^T(\theta)\mathbf{X}(\theta)/\mathbf{Y}=Y,\theta'] &= \text{Trace}\left[\mathbb{E}[\mathbf{X}^T(\theta)\mathbf{X}(\theta)/\mathbf{Y}=Y,\theta']\right]\\ &= \text{Trace}\left[\frac{\sigma_B^2}{K}(\text{Id}_{NK}-\frac{1}{K}\Xi^T\Xi)+\hat{X}(\theta')\hat{X}^T(\theta')\right]\\ &= d+\text{Trace}\left[\hat{X}(\theta')\hat{X}^T(\theta')\right]\\ &= d+\hat{X}^T(\theta')\hat{X}(\theta'),\end{aligned}$$

où d est une constante. Alors, l'expression de $U(\theta\,;\,\theta')$, toujours d'après IV.43 devient

$$\begin{aligned}U(\theta,\theta') &= \gamma-\frac{K}{2\sigma_B^2}\Big(\hat{X}^T(\theta')\hat{X}(\theta')-\hat{X}^T(\theta')\xi(\theta)-\xi^T(\theta)\hat{X}(\theta')+\xi^T(\theta)\xi(\theta)\Big)\\ &\gamma-\frac{K}{2\sigma_B^2}\Big((\hat{X}(\theta')-\xi(\theta))^T(\hat{X}(\theta')-\xi(\theta))\Big),\end{aligned}\qquad\text{(IV.47)}$$

avec γ une constante positive ne dépendant ni de θ, ni de θ'.
Ainsi, la connaissance de $\hat{X}(\theta')$ entraîne celle de $U(\theta,\theta')$. De plus, d'après l'expression IV.47, maximiser $U(\theta,\theta')$ revient à trouver le θ qui minimise la distance euclidienne entre $\hat{X}(\theta')$, qui est connu, et $\xi(\theta)$.

En définitive, si le j-uplet $\{\hat{\theta}^{(0)}\,;\hat{\theta}^{(1)}\,;\,\ldots\,;\,\hat{\theta}^{(j-1)}\}$ est connu, alors, $\hat{\theta}^{(j)}$ est obtenu par

$$\begin{cases}\text{E} \;:\; \text{Calcul de}\quad \hat{X}(\theta^{(j-1)})\\ \\ \text{M} \;:\; \text{Calcul de}\quad \theta^{(j)}=\underset{\theta\in D^K}{\text{argmin}}[\frac{1}{2}\Big(\hat{X}(\theta^{(j-1)})-\xi(\theta)\Big)^T\Big(\hat{X}(\theta^{(j-1)})-\xi(\theta)\Big)]\end{cases}$$

A présent, il est possible d'affirmer que $\hat{\theta}_{MV}$ peut être déterminé par le principe algorithmique itératif énoncé ci-dessus. Il reste à expliciter les composantes des vecteurs concernés.
D'une part, $\hat{X}(\theta^{(j-1)})$ est un vecteur de $\mathbb{R}^{NK}$ qui a pour composantes

$$\begin{aligned}\hat{X}_{(k,n)}(\theta^{(j-1)}) &= s_k(t_n\,;\,\theta^{(j-1)})+\frac{1}{K}\left(Z_n-\sum_{l=1}^{K}s_l(t_n\,;\,\theta^{(j-1)})\right)\\ &\forall k=1\ldots K\quad,\quad\forall n=1\ldots N\end{aligned}$$

et d'autre part

$$\begin{aligned}\underset{\theta\in D^K}{\text{argmin}}[\frac{1}{2}(\hat{X}(\theta^{(j-1)})-\xi(\theta))^T(\hat{X}(\theta^{(j-1)})-\xi(\theta))] &= \frac{1}{2}\sum_{n=1}^{N}\sum_{k=1}^{K}\Big(s_k(t_n\,;\,\theta^{(j)})-\hat{X}_{(k,n)}(\theta^{(j)})\Big)^2\\ &= \frac{1}{2}\sum_{n=1}^{K}\sum_{k=1}^{N}\Big(s_k(t_n\,;\,\theta^{(j)})-\hat{X}_{(k,n)}(\theta^{(j)})\Big)^2.\end{aligned}$$

Cette inversion de l'ordre de sommation dans IV.48 est capitale, car s'agissant de la somme de termes positifs, la minimisation peut se faire en K minimisations parallèles. Ainsi, l'algorithme EM appliqué à l'équation de mesure IV.2 transforme le problème difficile de recherche de $\hat{\theta}_{MV}$ de dimension $3K$ en K problèmes plus simples de recherche de $(\hat{\theta}_{MV})_k$, pour $k=1\ldots K$, chacun de dimension 3 :

$$\begin{cases} \text{E} \quad : \quad \text{Pour } k = 1 \dots K, \quad \hat{X}_{(k,n)}(\theta^{(j-1)}) = s_k(t_n\,;\,\theta^{(j-1)}) + \frac{1}{K}\left(Z_n - \sum_{l=1}^{K} s_l(t_n\,;\,\theta^{(j-1)})\right) \\ \text{M} \quad : \quad \text{Pour } k = 1 \dots K, \quad \underset{\theta \in D}{\operatorname{argmin}} \left[\frac{1}{2}\sum_{n=1}^{N}\left(s_k(t_n\,;\,\theta^{(j)}) - \hat{X}_{(k,n)}(\theta^{(j)})\right)^2\right] \end{cases}$$

Cette technique semble répondre parfaitement au problème, puisque dans la section précédente il a été montré qu'estimer l'activité d'une cellule est possible avec de bons résultats. Cependant, dans [Fed88] il est précisé que l'algorithme peut diverger ou converger vers un extremum local. La convergence vers $\hat{\theta}$ n'est pas garantie pour toute condition initiale θ_0. Il faut donc là encore coupler l'algorithme EM avec en amont le filtrage adapté stochastique utilisé en détection pour assurer la convergence vers le maximum global de la vraisemblance. Le FAS peut intervenir entre l'étape E et l'étape M, sachant que chaque $\hat{X}_k(\theta^{(j-1)})$ véhicule l'activité de la k^{me} cellule. Le principe est le suivant,

- Le FAS est appliqué à l'observation avec plusieurs taille de fenêtres afin de déterminer $\hat{\theta}_{FAS}$.
- Ce paramètre sert de condition initiale à l'algorithme FAS-EM, $\theta_0 = \hat{\theta}_{FAS}$.
- L'algorithme EM est utilisé pour trouver $\hat{\theta}_{MV}$, mais entre l'étape E et l'étape M le FAS est exécuté sur chaque vecteur $\hat{X}_k(\theta^{(j-1)})$, et ceci à chaque itération j jusqu'a convergence.

Cette approche est illustrée dans la prochaine section où l'association FAS-EM est utilisée pour estimer une observation test, puis dans celle d'après pour estimer l'activité de consommation de données réelles.

6.6 Estimation d'une superposition de cellules bruitée, $K \geq 1$

Il s'agit dans cette section d'évaluer les performances de l'association de l'algorithme EM et du filtrage adapté stochastique utilisé en détection pour estimer une observation composée de 3 cellules, disponible sous la forme d'un vecteur $\mathbf{Z}$ de dimension N, issu de l'échantillonnage du signal $\mathbf{Z}(t)$ sur un intervalle de temps $[0\,;\,1]$ à la période $T_e = 10^{-3}$ (sec). Le modèle a pour expression, selon IV.35, IV.4 et IV.5, avec $K = 3$,

$$\mathbf{Z} \quad = \quad s_1(\theta_1) + s_2(\theta_2) + s_3(\theta_3) + \mathbf{B}. \tag{IV.48}$$

Le bruit est représenté par le vecteur $\mathbf{B}$, gaussien, centré de matrice de variance covariance $\Gamma_{BB} := \sigma_B^2 \mathrm{Id}_N$. Les paramètres à optimiser sont regroupés dans le vecteur paramètre $\theta \in \mathbb{R}_+^9$ défini par

$$\theta \quad := \quad [A_1\,;\,\sigma_1\,;\,m_1\,;\,A_2\,;\,\sigma_2\,;\,m_2\,;\,A_3\,;\,\sigma_3\,;\,m_3].$$

Dans le cadre de cette étude, l'observation est la même que celle utilisée dans la section 5.5.3 (voir figure 3), avec $\hat{\theta}$ défini par IV.30.

6.6.1 Estimation

La matrice d'information de Fisher théorique peut être calculée, cette dernière est une matrice $(9\,;\,9)$ composé de trois blocs de taille $(3\,;\,3)$ correspondant a chacune des trois cellules, ce qui permet de calculer la borne de Cramèr-Rao théorique. L'inverse d'une matrice diagonale

par blocs est une matrice diagonale par blocs [The87], donc la borne est également diagonale par blocs de taille $(3\,;\,3)$,

$$BCR(\hat{\theta_1}) := \begin{bmatrix} 2,1157.10^{-4} & -4,7016.10^{-7} & -4,0107.10^{-25} \\ -4,7016.10^{-7} & 3,1344.10^{-9} & -1,9117.10^{-25} \\ -4,0107.10^{-25} & -1,9117.10^{-25} & 3,1344.10^{-9} \end{bmatrix},$$

$$BCR(\hat{\theta_2}) := \begin{bmatrix} 1,0579.10^{-4} & -7,0524.10^{-7} & -7.3413.10^{-23} \\ -7,0524.10^{-7} & 1,4105.10^{-8} & 2.7672.10^{-24} \\ -7.3413.10^{-23} & 2.7672.10^{-24} & 1.4105.10^{-8} \end{bmatrix},$$

$$BCR(\hat{\theta_3}) := \begin{bmatrix} 1,4105.10^{-4} & -5,6419.10^{-7} & 1,1037.10^{-22} \\ -5,6419.10^{-7} & 6,7703.10^{-9} & 7,2856.10^{-24} \\ 1,1037.10^{-22} & 7,2856.10^{-24} & 6,7703.10^{-9} \end{bmatrix},$$

et

$$BCR(\hat{\theta}) = \begin{bmatrix} BCR(\hat{\theta}_1) & & (0) \\ & BCR(\hat{\theta}_2) & \\ (0) & & BCR(\hat{\theta}_3)] \end{bmatrix}.$$

L'algorithme EM est lancé avec $\theta_0 = \hat{\theta}_{FAS}$. A chaque itération, le FAS est appliqué à chacun des 3 vecteurs $\hat{X}_1^j(\theta_1)$, $\hat{X}_2^j(\theta_2)$ et $\hat{X}_3^j(\theta_3)$, chacun véhiculant l'information lié à la cellule qui lui est attitrée. Les figures 14, 15 et 16 montrent ce qui se passe lors de la première itération.

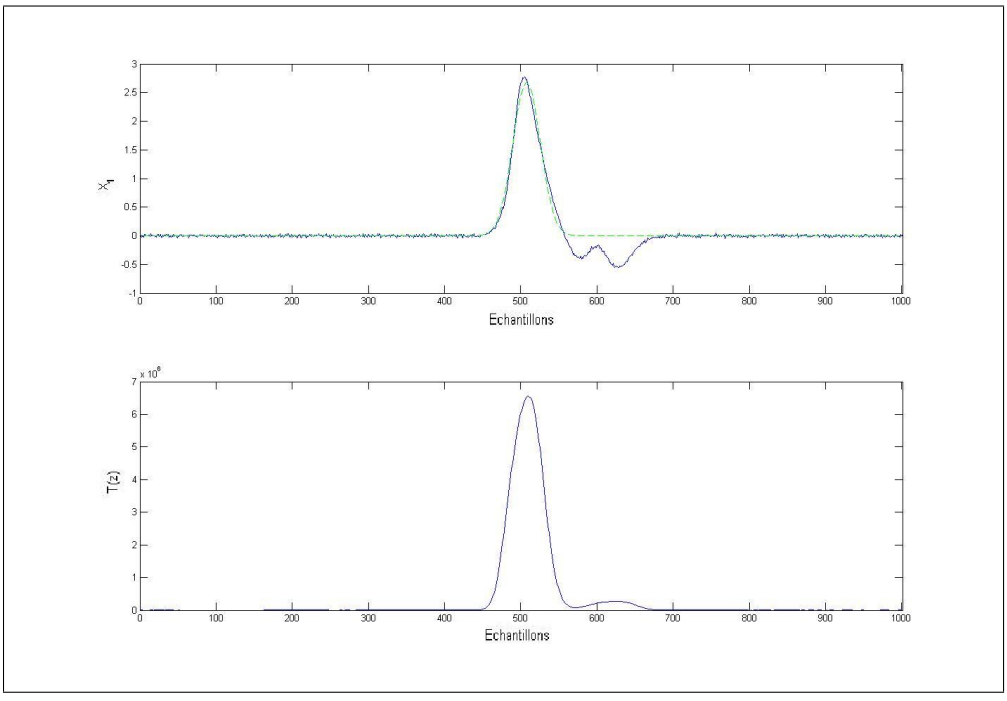


FIG. 14 – *Calcul* $\hat{X}_1^1(\theta_1^1)$ *et estimation de* θ_1^2

avec

$$\hat{\theta_1}^1_{FAS} = [2,27\,;\,0,016\,;\,0,51],$$

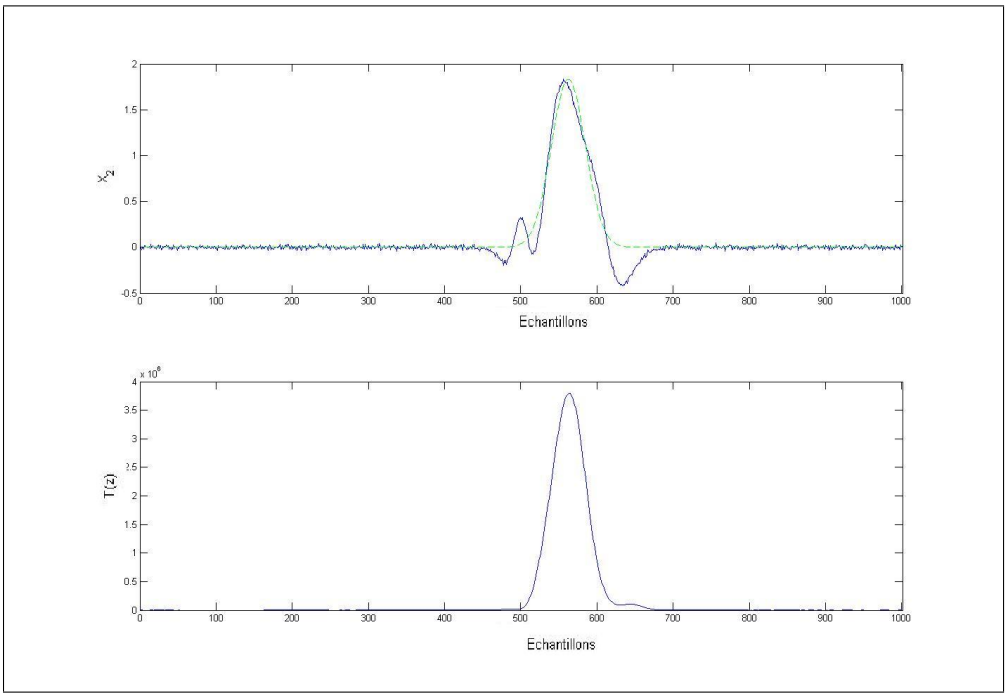


FIG. 15 – *Calcul* $\hat{X}_2^1(\theta_2^1)$ *et estimation de* θ_2^2

avec

$$\hat{\theta_2}^1_{FAS} = [1,66\,;\,0,018\,;\,0,56],$$

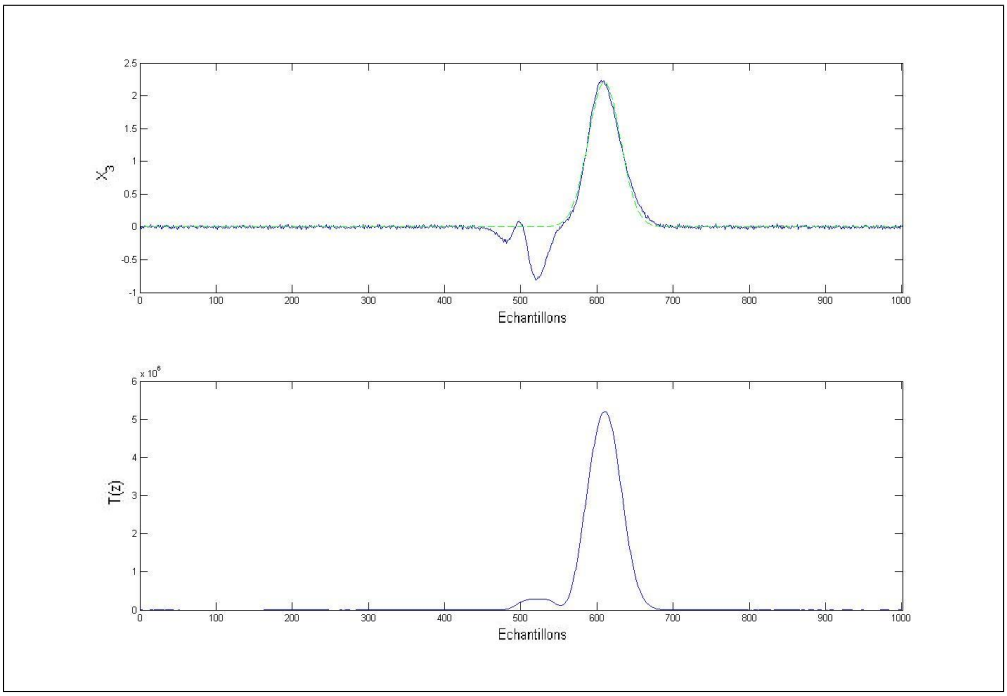


FIG. 16 – *Calcul* $\hat{X}_3^1(\theta_3^1)$ *et estimation de* θ_3^2

et avec

$$\hat{\theta_3}^1_{FAS} = [2,05\,;\,0,022\,;\,0,61],$$

L'algorithme fait suffisamment bien son travail d'isolation individuelle de cellule pour rendre l'estimation facile, cellule par cellule. Il est clair que c'est de ce point que dépend le succès de l'optimisation.
Le processus est réitéré jusqu'à convergence en moyenne en 7 itérations, la solution trouvée, en un temps de calcul de l'odre de la dizaine de secondes est

$$\hat{\theta}_{MV} \quad = \quad [2,968\,;\,0,011\,;\,0,5\,;\,2,042\,;\,0,017\,;\,0,55\,;\,2,57\,;\,0,049\,;\,0,599].$$

Cette dernière sert à construire l'estimée de la consommation, le résultat est présenté figure 17.

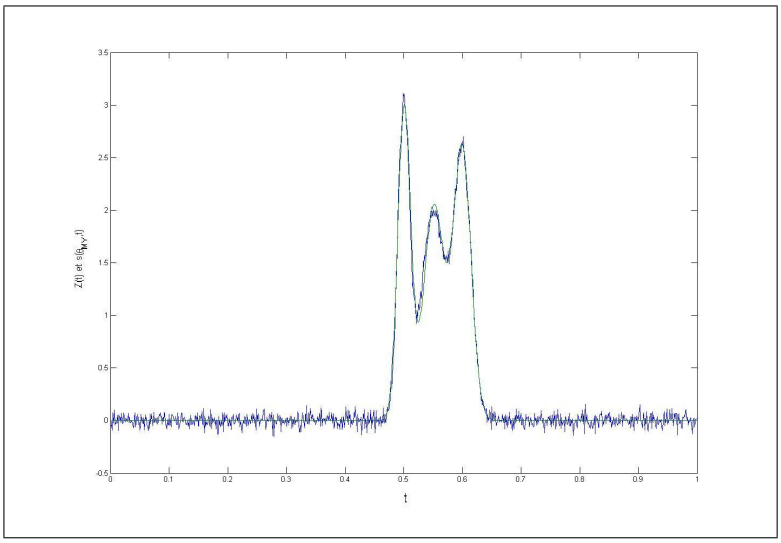


FIG. 17 – *Observation Z et estimée $s(\hat{\theta}_{MV})$*

Le résultat est conforme aux attentes, comme le confirme le tracé du résidu ζ, figure 18

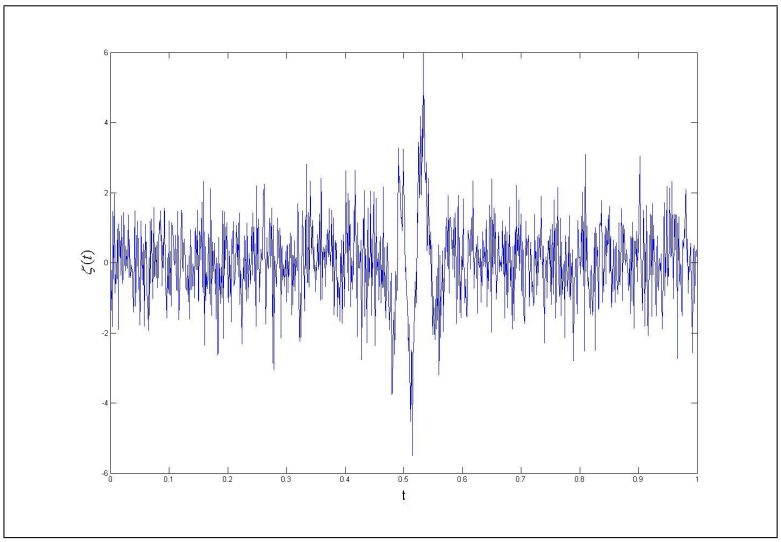


FIG. 18 – *Résidu ζ*

L'estimée épouse correctement l'observation, mais le résidu présente de brusque sauts dus aux erreurs d'estimation, l'isolement de chaque cellules n'étant pas parfait. Sauf cas idéal où les cellules ne s'enchevêtrerait pas, il est presque impossible qu'il n'y ait pas de recouvrement.

6.6.2 Performances optimales

La moyenne empirique ainsi que la matrice de variance covariance empirique sont ensuite calculés selon IV.32 et IV.33,

$$\mathbb{E}\left[\hat{\theta}_{MC}\right] \approx [2,9927\,;\,0,0021\,;\,0,5003\,;\,2,0132\,;\,0,0034\,;\,0,5501\,;\,2,5303\,;\,3.24.10^{-6}\,;\,0,5996].$$

et

$$\begin{aligned} diag(Cov[\hat{\theta}_{MC}]) \approx\ & [9,7001.10^{-4}\,;\,1,1367.10^{-4}\,;\,2.1107.10^{-7}\,; \\ & 6,4517.10^{-4}\,;\,3,9047.10^{-4}\,;\,6.8842.10^{-7}\,; \\ & 5,7087.10^{-4}\,;\,2,5625.10^{-4}\,;\,7,3519.10^{-9}]. \end{aligned}$$

Contrairement à $BCR(\hat{\theta})$, $Cov[\hat{\theta}_{MC}]$ n'est pas diagonale par blocs, c'est une matrice pleine dont seuls les termes diagonaux sont présentés. Cela atteste du fait qu'il y a du recouvrement d'information entre les cellules, alors que cette prise en compte n'était pas effective dans le calcul de $BCR(\hat{\theta})$.
Les résultats sont concluants, excepté pour l'estimation de σ_3 mais cette lacune ne nuit pas au bien fondé du résultat.
L'algorithme EM couplé au FAS permet donc d'estimer une observation faite de trois cellules différentes, là où cela est très difficile avec une démarche d'optimisation classique. La résolution du problème envisagée directement avec un algorithme de gradient fait que ce dernier accroche sur une seule cellule en considérant les autres comme du bruit. L'efficacité de l'algorithme est donc substantielle, sans pour autant que sa convergence vers la solution escomptée soit garantie. Le choix de la condition initiale est là encore primordial, et le FAS en détection joue en ce sens un rôle déterminant. Le même problème résolu à partir d'une condition initiale plus éloignée ne donne plus du tout de bons résultats. L'association FAS-EM est donc bilatère, chacune des techniques ayant besoin de l'autre pour exister.

7 EXPERIMENTATIONS

Cette section traite du cas de l'estimation d'un signal réel issu de la modélisation macro modèle de Kussener Ses travaux montrent que ce type de signaux modélise l'activité de courant d'un micro processeur.
Le signal est étudié sur un intervalle de temps de $8,8.10^2$ (μ sec) contenant une période d'horloge complète. Il est disponible sous la forme de $N = 901$ échantillons représentant une consommation de courant (mA) obtenus après échantillonnage à la fréquence $F_e = 10GHz$. L'observation, appelée Z, est présentée figure 19, elle a été recalée en ordonnée de sorte à valoir 0 aux bords de l'intervalle d'observation. Certains pics sont d'amplitude négative.
Les pics d'amplitudes positives représentent un comportement de charge. A chaque commutation du macromodèle, ces pics sont générés au même titre que les portes logiques au sein du microprocesseur. Les pics négatifs sont dans le cas réel d'amplitude négligeable leur origine est lié au transfert de charge entre le capacités intrinsèques du macromodèle. Il est a noter que lors d'une simulation, le macromodèle est étudié seul avec une alimentation non stabilisée. La présence de ses pics négatifs devient négligeable dés lors que le macromodèle est placé dans son environnement réel. La conséquence de cette spécificité physique de l'observation est que les pics d'amplitude négative peuvent être négligés lors de la phase d'estimation.

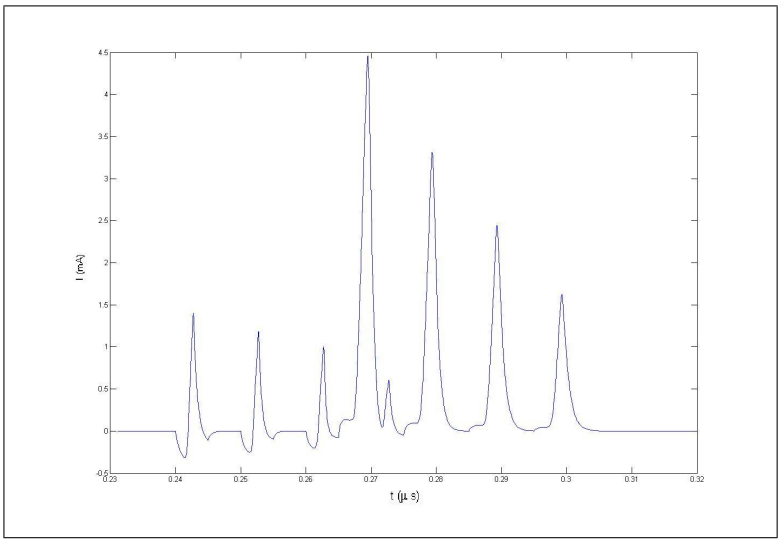


FIG. 19 – *Observation Z*

La première constatation est que le niveau de bruit est très faible, Z est donc dans une condition de rapport signal à bruit très favorable. De plus, dans cet exemple il y a peu d'enchevêtrement d'information entre les cellules, ce qui en fait un cas plus simple que celui à 3 cellules étudié précédemment. Le nombre de cellules est $K = 8$, ce qui signifie que le domaine de recherche du paramètre inconnu est inclus dans $\mathbb{R}^{24}$. soit un nombre de paramètres important capable de mettre en défaut toute approche classique.
Le but est alors d'estimer ce paramètre à l'aide de la technique FAS-EM selon la même démarche que dans le cas $K = 3$.
Le FAS est appliqué à l'observation afin de construire la condition initiale en posant $\theta_0 := \theta_{FAS}$, les résultats obtenus sont

$$\begin{aligned}\hat{\theta_0} \;=\; & [1,4015\,;\; 1,3732.10^{-3}\,;\; 0,2427\,;\\ & 1,1836\,;\; 1,3732.10^{-3}\,;\; 0,2527\,;\\ & 0,994\,;\; 1,3732.10^{-3}\,;\; 0,2627\,;\\ & 4,4574\,;\; 9,8.10^{-4}\,;\; 0,2695\,;\\ & 0,605\,;\; 1,3732.10^{-3}\,;\; 0,2727\,;\\ & 3,3157\,;\; 9,8.10^{-4}\,;\; 0,2794\,;\\ & 2,4452\,;\; 9,8.10^{-4}\,;\; 0,2893\,;\\ & 1,6224\,;\; 1,77.10^{-3}\,;\; 0,2992].\end{aligned}$$

L'algorithme EM est ensuite lancé à partir de cette dernière, et pour chaque itération, entre l'étape E et l'étape M, le FAS est appliqué sur chacune des K cellules isolées. Le résultat, après 10 itérations, est présenté figure 20.

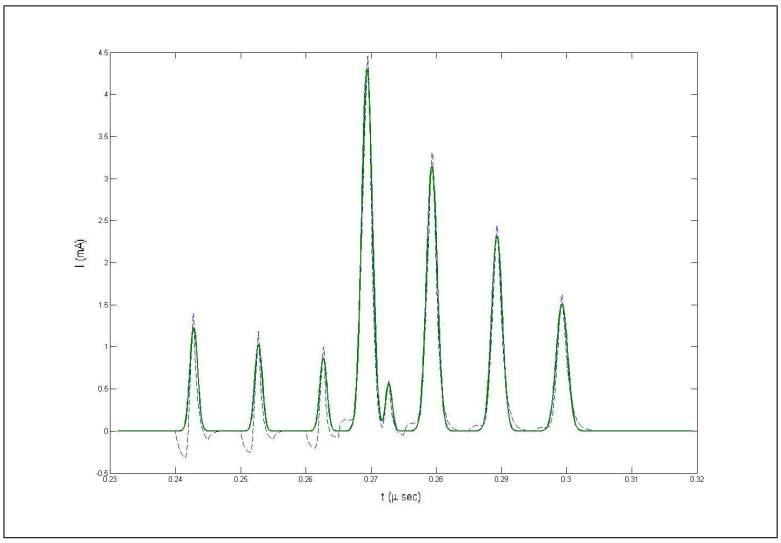


FIG. 20 – *Observation Z (traits pointillés) accompagnée de $s(t, \hat{\theta}_{MV})$*

Le paramètre trouvé est

$$\begin{aligned}\hat{\theta}_{MC} \;=\; & [1,2261\,;\; 5,7924.10^{-4}\,;\; 0,2427\,;\\ & 1,0322\,;\; 5,5197.10^{-4}\,;\; 0,2527\,;\\ & 0,8672\,;\; 5,386.10^{-4}\,;\; 0,2627\,;\\ & 4,307\,;\; 7,8918.10^{-4}\,;\; 0,2693\,;\\ & 0,55997\,;\; 4,8864.10^{-4}\,;\; 0,2727\,;\\ & 3,1412\,;\; 8,0038.10^{-4}\,;\; 0,2793\,;\\ & 2,312\,;\; 7,9831.10^{-4}\,;\; 0,2893\,;\\ & 1,5046\,;\; 8,6198.10^{-4}\,;\; 0,2992].\end{aligned}$$

A la lecture de la figure 20 les résultats sont bons dans la mesure où l'estimée $s(\hat{\theta}_{MV})$ colle à l'observation. Cependant, il est possible de constater que les rebonds négatifs, qui n'ont pas de sens physique, présents en amont des trois premières cellules ne sont pas estimés. Cela est du au fait que le détecteur est conçu pour identifier un modèle de signal utile particulier auquel les rebonds négatifs ne ressemble pas.
La qualité de l'estimé est confirmée par l'étude du résidu ζ, ce dernier est présenté figure 21,

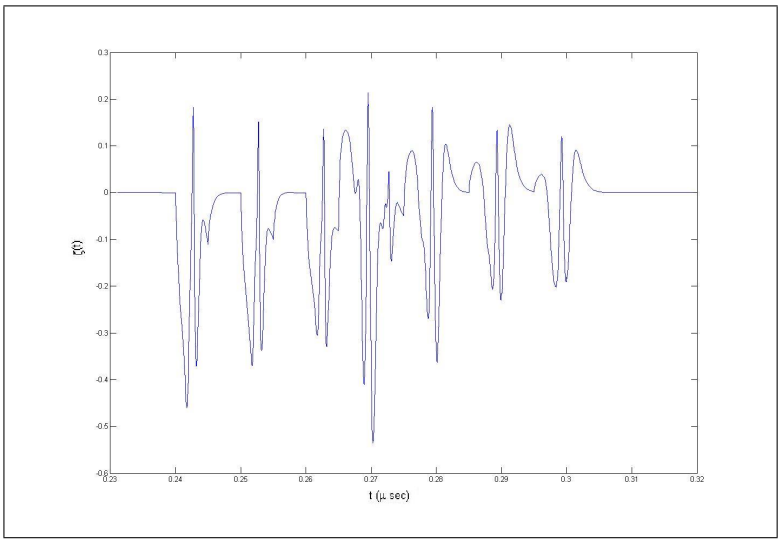


FIG. 21 – *Résidu* ζ

ce dernier a ses valeurs incluses dans l'intervalle $[-3\,;\,3]$. Le test du χ^2 est d'ailleurs largement positif puisque le seuil est fixé à 931 pour 877 degrés de liberté[13] et $\|\zeta\|^2 = 21,948$. Le temps de calcul est de l'ordre de la minute, néanmoins il est possible de paralléliser le code de façon quasi naturelle de sorte à ce que chaque unité de calcul ait une optimisation à sa charge sur les K nécessaires. Ainsi, en théorie du moins et non sans moyens matériels lourds, il est possible de ramener le temps de calcul à la hauteur de celui d'une seule cellule, qui lui est de l'ordre de la dizaine de secondes. Les résultats ont été validés *a posteriori* par les microélectroniciens ayant fournit cette observation. D'après l'étude de ce signal macromodèle, il est donc possible d'affirmer que l'estimation d'une observation composée de 8 cellules est réalisable, avec une précision correcte. La qualité du résultat n'est pas altérée par la présence de pics négatifs qui ne sont pas détectés donc pas estimés. Toutefois, la qualité de ces résultats est à tempérer puisque dans ce cas, les cellules sont peu enchevêtrées, il n'y a donc que peu de recouvrement d'information.

8 CONCLUSION

Ce chapitre présente une nouvelle technique d'estimation paramétrique, dont le principe repose sur le couplage du filtrage adapté stochastique utilisé en détection (FAS) et de l'algorithme expectation maximization (EM). Cette technique est appliquée à l'estimation d'activité de courant de Smart Card, vue à travers un modèle physique.
Le fondement de cette étude repose sur les travaux de Kussener, qui a montré que l'activité d'un micro processeur peut être modélisée simplement à partir du contrôle d'inverseurs, et de Oswald qui a montré qu'une consommation de courant peut être vue comme la somme de sources élémentaires bruitées.
Par ailleurs, la technique de masquage par décomposition des signaux présentée au chapitre précèdent est efficace, mais montre ses limites lorsqu'il s'agit d'envisager une application concrète en terme d'implémentation. Il apparaissait donc nécessaire de proposer une alternative, une technique prenant plus en compte la physique du problème et telle qu'il soit possible de l'utiliser concrètement pour une opération de masquage des signaux. L'idée de fond est alors de fournir à un dispositif de masquage un jeu de paramètres, suffisant pour caractériser la signature à masquer. Ces paramètres sont constitutifs de la consommation et peuvent donc par suite être modifiés à loisir par un dispositif électronique approprié.

[13] 901 échantillons moins 24 paramètres.

Mais avant cela, il faut être en mesure de fournir ce jeu de paramètres, voilà pourquoi l'objet de ce chapitre porte sur l'estimation paramétrique d'une activité de courant. De la façon la plus générale qu'il soit, cette activité est modélisée comme une observation qui est la somme d'un signal utile dépendant de paramètres à estimer et d'un bruit. Le signal utile est la somme de signaux élémentaires, modélisé par des fonctions de la famille gaussienne, chaque cellule dépend donc d'une amplitude, d'un paramètre de dilatation et d'un retard. Le but est alors d'estimer chacun de ces trois paramètres pour chaque cellule, le paramètre inconnu total étant la concaténation de chacun des triplets.
Ce type de problème fait partie de l'optimisation difficile, vu que la fonction coût associée à l'observation n'est pas strictement convexe par rapport aux paramètres. Cela signifie concrètement que la fonction coût peut avoir des extrema locaux qui peuvent piéger toute méthode d'estimation basée sur le calcul de gradient et ainsi ne pas retourner le paramètre voulu.
Bien sûr, il existe des techniques capables de s'affranchir de ce type de difficultés, comme par exemple la force brute ou le recuit simulé. Cependant, dans le premier cas le volume de calculs est trop important alors que dans le second la difficulté réside dans le choix pertinent d'un schéma de température. De plus, la convergence globale de l'algorithme est garantie, mais au sens de la convergence presque sûre. Ainsi, rien n'empêche l'algorithme de converger en un temps infini, du moins très long. Restent les méthodes itératives à base de gradient, dont la convergence globale n'est pas assurée, sauf si la condition initiale est proche de la véritable solution.
C'est précisément sur ce point d'accroche que porte l'étude, car une possibilité serait d'avoir à disposition en amont de la phase d'estimation une technique capable de déterminer une condition initiale pertinente, à défaut d'être parfaite. Voilà pourquoi le filtrage adapté stochastique utilisé en détection est préconisé ici. Cette technique permet de détecter un signal utile dont sont seulement connus ses premiers moments, noyé dans du bruit, même dans des conditions de rapport signal à bruit défavorables.
Le FAS est devenu une technique abondamment utilisée, aussi bien à travers ses déclinaisons $1D$ comme c'est le cas dans [Cav93, Lev93, Cha06s1] que dans le cas $2D$ en permettant, en association avec l'analyse multi résolution, la détection et la restauration de structures particulières sur des images SONAR ou RADAR [Cha05b1, Cha05b2, Cha06s2, Cou06].
Après avoir montré que les trois paramètres inconnus sont déterminés sans peine dans le cas où l'observation est constituée d'une cellule bruitée, la suite de l'étude porte sur l'extension de ce cas à celui de plusieurs cellules. Pour répondre à cette problématique, la solution proposée consiste à utiliser l'algorithme EM, parfaitement adapté au modèle de signal utile, avec le filtrage adapté stochastique utilisé en détection. Le FAS est utilisé une première fois pour définir l'intervalle d'observation, puis à chaque itération de l'algorithme EM entre l'étape E et l'étape M. Afin d'évaluer les performances de la technique proposée, un cas difficile est étudié, consistant en une observation construite avec trois cellules proches en localisation temporelle. Les résultats sont satisfaisants, mais pas parfaits, ceci étant dû au recouvrement d'informations lié à l'enchevêtrement des cellules. Cela dit, l'association FAS-EM demeure très efficace au vu de la qualité de l'estimateur retourné mais également du fait qu'une méthode de gradient classique ne peut, sauf exception rare converger globalement pour ce type de problème comme le fait le FAS-EM.
La technique est ensuite confrontée aux données réelles. Il s'agit d'une signature de courant issue du macro modèle de Kussener, se présentant comme l'activité de 8 cellules. Le paramètre inconnu est de dimension 24, l'algorithme FAS-EM ramène alors la résolution d'un problème de dimension 24 en la résolution de 8 problèmes de dimension 3. L'optimisation est alors une réussite, l'objectif étant alors atteint : fournir un jeu de paramètres caractérisant complètement une consommation de courant.

Cependant, avec cet exemple, le niveau de bruit est très faible, une étude de robustesse est donc nécessaire pour estimer les limites de la méthode en terme de rapport signal à bruit. L'autre facteur limitant est le fait que les cellules soient resserrées ou pas. Par exemple, partant d'une configuration à deux cellules dont les caractéristiques sont identifiables par le traitement proposé dans ce chapitre. Il est toujours possible de resserrer ces deux cellules jusqu'à ce que l'algorithme n'en voit plus qu'une seule. Or, la seule façon de remédier à cette difficulté est de suivre la règle suivante : plus les cellules sont resserrées, plus la condition initiale doit être précise. Cela signifie alors qu'il faut améliorer les performances du FAS en détection. Il y a deux axes possibles allant dans ce sens, ou bien fournir *a priori* des modèles d'autocorrélation de signal utile et de bruit retranscrivant plus fidèlement le signal et le bruit[14], ou bien étendre la théorie du FAS aux statistiques d'ordre supérieur.
Dans le cadre de la conception d'une technique de masquage des signaux, les électroniciens, sur la base de la donnée des paramètres, sont alors capables en modifiant ces valeurs de masquer la consommation estimée. La minimisation du résidu implique la conservation de la puissance, et il est nettement plus aisé de procéder avec une vingtaine de paramètres que sur le signal dans sa globalité. A l'écriture de ces lignes, un travail en vue d'un dépôt de brevet est en cours avec l'équipe Smart Cards de ST Microelectronics afin de concevoir une déclinaison plus simple de la technique, adaptée aux signaux analogiques.
Selon le partenaire industriel, la technique FAS-EM est implémentable si :

- Il est possible de mettre l'estimateur sous forme récursive (par l'intermédiaire d'un filtre de Kalman étendu, par exemple).
- L'intervalle de recherche des paramètres est restreint, ce qui consiste à ne considérer qu'un nombre restreint de cellules élémentaires possibles, correspondant à une activité élémentaire spécifique de la carte.

Le but recherché par les électroniciens serait alors d'anticiper la consommation sur le cycle d'horloge à venir.
En ce sens, les contraintes électroniques liées au problème sont donc respectées, à savoir conservation de la puissance et faisabilité électronique.

[14] En définitive des modèles d'autocorrélation plus "adaptés".

CHAPITRE V

CONCLUSIONS ET PERSPECTIVES

Ce manuscrit relate mes travaux de Thèse effectués entre 2003 et 2006 sur le thème de la sécurisation des Smart Cards par masquage de signal sur canal secondaire.
Cette Thèse est financée par la société ST Microelectronics dans le cadre de la convention entre mon laboratoire d'accueil, le Laboratoire Matériaux et Microélectronique de Provence et ST Microelectronics. Elle s'inscrit dans le projet de recherche PS23 "Gestion d'énergie", mettant en partenariat l'équipe Conception du L2MP avec la division Smart Cards de ST Microelectronics.
Le premier chapitre, introductif, permet de définir le contexte motivant ces travaux. Les Smart Cards sont de véritables ordinateurs embarqués ayant pour mission de stocker et faire transiter des données importantes de façon sécurisée. Leur utilisation, dans le domaine bancaire par exemple, a atteint de si grandes proportions que les secrets qu'elles cachent font l'objet de convoitises. Une Smart Card n'a donc d'utilité que, si et seulement si, elle est dotée d'un niveau de sécurité élevé.
En ce sens, le pirate, personne morale voulant s'accaparer ces informations, met en oeuvre des techniques de plus en plus élaborées pour arriver à ses fins, profitant des informations transitant, lorsque la carte fonctionne, à travers un canal virtuel appelé canal secondaire ou encore canal caché.
Deux approches s'opposent pour acquérir ces données. Une approche invasive, consistant à détruire la carte puis explorer son contenu, à l'aide d'un puissant microscope par exemple, et une approche non-invasive, qui n'entraîne pas la destruction de la carte, consistant à prélever les données à partir de fuites d'informations à l'intérieur du canal secondaire. Il est possible de prélever ces fuites à partir de sources diverses, telles que,

- le temps d'exécution d'algorithmes cryptographiques,
- le rayonnement électromagnétique et sonore,
- la réaction du dispositif aux injections de fautes,
- la consommation en courant.

Ces points d'accroche permettent au pirate, après acquisition de ce type de données, de concevoir des techniques d'attaques efficaces. Elles sont qualifiées d'actives, comme l'injection de fautes par exemple, si l'opérateur doit fournir des données à la carte pour examiner son comportement, ou au contraire, de passives, si l'opérateur se contente de mesurer des informations émanant de la carte lors de son fonctionnement.
Mes travaux s'intéressent au cas des attaques en puissance. Le principe de ces dernières consiste à exploiter statistiquement des relevés de consommation de courant, pour alors être en mesure, au su de ces informations, de déterminer quelle opération a provoqué cette consommation. Plusieurs techniques, comme par exemple la DPA, ont montré leur efficacité et ne cessent d'être améliorées. Ce type d'attaque constitue le meilleur compromis prix/performance pour le pirate. Cela dit, leur efficacité est conditionnée par une hypothèse forte consistant à supposer que les relevés de consommation qu'il a collectée, correspondent effectivement bien à ce que la puce a

consommé. Cette hypothèse est le point d'ancrage de mes travaux, car si le pirate travaille avec des signatures fausses, il ne pourra qu'en déduire des informations fausses.
Les techniques d'attaque évoluent très rapidement, il serait donc à moyen terme inutile de concevoir une technique de masquage faite pour résister à un type d'attaque particulier. Une telle approche rendrait la méthode trop rapidement obsolète. La problématique consiste alors à concevoir des techniques de masquage destinées à empêcher le pirate de collecter des signatures de courant, sans nuire pour autant au bon fonctionnement de la carte. Ainsi, toute technique de masquage des signaux proposée doit fournir un signal masqué qui ne ressemble pas à l'original, soit de même puissance sur un intervalle d'observation donné, ait un sens physique semblable à la signature originale et soit suffisamment général pour ne pas être appliqué spécifiquement à un type particulier d'attaque, ceci dans le but de leurrer le pirate.

Dans le chapitre *II*, il a été question de la caractérisation d'un système dynamique non-linéaire de la famille Double Scroll et de son application à la genèse de nombres pseudo-aléatoires.
L'étude est née d'un double besoin : concevoir, d'une part, un générateur de nombres pseudo-aléatoires, composante importante de la technique de masquage par décomposition, présentée au chapitre *III* et constituer, d'autre part, un apport théorique aux travaux de conception analogique de Telandro, travaillant en parallèle sur le problème.
La modélisation du problème, partant de l'équation différentielle non-linéaire du troisième ordre que vérifie le circuit, aboutit à la donnée d'un système différentiel non linéaire du premier ordre constitué de trois équations. Le système une fois mis sous forme adimensionnée, dépend d'un paramètre de contrôle qui conditionne le comportement des trajectoires du système. L'étude du système commence par la détermination de la nature des trois points fixes du système, tous des points "selle" instables, permettant de décrire la dynamique locale à l'aide du système linéarisé autour de chaque point fixe. Il ressort que chaque point fixe est doté d'un sous-espace tangent composé d'un plan et d'une droite vectorielle. L'étude de la dynamique locale permet de définir une première plage de valeur admissible pour le paramètre de contrôle.
Le passage entre la dynamique linéaire locale et non-linéaire globale est ensuite accompli, le but étant de définir pour quelles valeurs du paramètre de contrôle le système peut évoluer de façon chaotique, à travers l'étude des indicateurs du chaos tels que le diagramme de bifurcation, la mise évidence de deux trajectoires hétéroclinique et le calcul des exposants de Lyapunov. Ainsi, lorsque le système évolue de façon chaotique, la trajectoire qu'il décrit tourne autour d'un des points fixes extérieurs et une fois son amplitude suffisamment importante, est attirée à l'aide du point fixe central vers l'autre point fixe pour y graviter jusqu'à être à nouveau attirée par son symétrique, et cela sans cesse. L'attracteur étrange décrit par la trajectoire s'appelle le Double Scroll.
Les systèmes évoluant de façon chaotique ont la propriété d'être sensible aux conditions initiales, ce qui signifie que deux conditions initiales proches mais distinctes engendrent deux trajectoires aux destins différents. Par extension, si la condition initiale est la réalisation d'une variable aléatoire, alors les trajectoires engendrées sont presque sûrement différentes, ces dernières ne pouvant pas s'entrecouper.
Afin de concevoir un générateur de nombres pseudo-aléatoires, l'idée est alors d'utiliser le système dynamique en mode chaotique à partir d'une condition initiale qui est la réalisation d'une variable aléatoire, puis de prélever sur ce dernier des valeurs correspondant aux instants, où la trajectoire traverse une section de Poincarré particulière. Ces valeurs servent à modifier le gabarit d'un signal créneau, qui après une transformation homothétique simple et passage par l'oracle "valeur moyenne" fournit une séquence binaire. Ce flux est censé être pseudo-aléatoire, de plus le renouvellement du germe est automatiquement assuré à chaque remise en route du système par la propriété de sensibilité aux conditions initiales.

Afin de caractériser statistiquement les propriétés du flux, ce dernier est passé au crible de cinq tests statistiques discriminants. Des expérimentations sont alors réalisées, d'une part, sur un flux issu de simulations numériques et, d'autre part, sur un flux issu de données réelles. Dans les deux cas, les résultats sont tous positifs. Ceci est encourageant dans la mesure, où les tests, pour des raisons matérielles, n'ont été effectués que sur des échantillons de 10000 bits là où 20000 bits minimum sont requis par les organismes de certification. Cela dit, la méthode a été reconnue par la communauté scientifique et industrielle par l'intermédiaire d'un acte de conférence, présenté par Telandro [Tel06], et d'un brevet avec ST Microelectronics déposé conjointement [ST06]. L'avantage de la méthode est qu'il n'est pas nécessaire d'ajouter en post-traitement une technique de redressement des valeurs. Une perspective prioritaire consiste à mettre les moyens matériels en oeuvre pour pouvoir travailler avec des échantillons d'au moins 20000 bits et ainsi confirmer le succès de cette nouvelle approche.

Dans le chapitre *III*, une première technique de masquage a été présentée : le masquage par décomposition des signaux. Il s'agit d'une approche aveugle, ne tenant pas compte de la physionomie du signal à masquer, consistant à développer ce dernier, alors vu comme un processus stochastique, sur une base spécifique, puis à substituer ses échantillons par les coefficients de décomposition trouvés. La base retenue est celle de Karhunen-Loève, car dans cette dernière, les fonctions de base sont déterminées de sorte que les coefficients de décomposition soient statistiquement décorrélés à l'ordre deux. La détermination de ces fonctions de base est obtenue par la résolution d'une équation intégrale de Fredholm. Les fonctions de base sont alors considérées comme les fonctions propres d'un opérateur compact d'Hilbert-Schmidt, ce qui légitime leur existence, leur nature et, en définitive, l'écriture du développement.
Il est d'ailleurs montré que ce développement est tel que les fonctions propres sont invariantes par ajout de bruit blanc. Ainsi, lorsque le signal observé est la somme d'un signal utile et d'un bruit blanc, il est possible de construire une approximation du signal utile, proche au sens de l'erreur quadratique moyenne du signal d'intérêt, s'affranchissant ainsi du bruit à corrélation microscopique. Cette propriété sert alors à montrer que l'ensemble des techniques de masquage basées sur l'ajout de bruit blanc sont inefficaces en terme de sécurisation.
La méthode de masquage des signaux proposée est en suite déclinée suivant cinq moutures correspondant à cinq façons différentes de définir les fonctions propres. Dans chaque cas, une phase de permutations pseudo-aléatoires des coefficients est réalisée, faisant office de verrou, et ceci sur la base de la technique développée au chapitre *II*. Puis, chacune d'entre-elles est utilisée pour masquer des signatures de courant fournies par ST Microelectronics. La qualité du masquage est mesurée en terme de décorrélation à l'ordre deux. De l'analyse des résultats obtenus, il ressort que chacune de ces déclinaisons présente des forces et faiblesses différentes, en terme de moyens matériels et de performances. Il y a donc un compromis à réaliser entre ces deux points.
En dépit de la qualité des résultats obtenus, validés par ST Microelectronics, plusieurs restrictions pondèrent ce succès. En particulier, une implémentation électronique n'est aujourd'hui pas possible en raison des limitations technologiques. Le fait de travailler avec des signaux échantillonnés nécessite la présence de convertisseurs analogique-numérique ainsi qu'un bloc de traitement numérique de type DSP. Ces derniers sont particulièrement gourmands en taille, ce qui tranche avec la volonté et la nécessité des électroniciens de concevoir des dispositifs occupant le moins de place possible et consommant le moins possible de courant. De plus, certaines déclinaisons présentées nécessitent de stocker certaines quantités, ce qui constitue un danger en terme de sécurité car le pirate peut alors tenter de s'accaparer ces dernières et par rétro-ingénierie retrouver la signature originale.
A défaut d'être rejetée, la technique est mise de côté, en attendant que la technologie avance.

Les limites atteintes par la technique de masquage des signaux par décomposition ont permis cependant de recadrer mes recherches. Voilà pourquoi la technique FAS-EM, association du filtrage adapté stochastique (FAS) utilisé en détection et de l'algorithme Expectation-Maximization (EM), présentée au chapitre IV, tient compte de ces contraintes : là où le masquage par décomposition est une technique aveugle, celle présentée ici est basée sur une modélisation paramétrique de l'observation. La méthode présentée est née suite aux travaux de thèse de Kussener ayant abouti à la notion de macromodèle, montrant que le comportement d'un microprocesseur peut être modélisé simplement avec des portes logiques, et suite à ceux d'Oswald qui montre que dans ce cas, une activité de courant peut être vue comme la superposition d'activités élémentaires, additivement bruitées. L'idée consiste alors à modéliser l'observation telle que cette dernière soit la somme d'un signal utile et d'un bruit. Le signal utile est lui-même la somme de signaux élémentaires. Chaque signal élémentaire dépend de trois paramètres, qu'il convient alors d'estimer afin que le modèle colle le plus possible aux mesures.
Le modèle de signal élémentaire choisi appartient à la famille gaussienne, car une sommation finie de fonctions de ce type permet d'engendrer des signaux de gabarit similaire aux consommations rencontrées. De plus, il est possible d'adapter le gabarit de chaque gaussienne en modifiant son amplitude, son échelle et son instant d'apparition. Ce triplet constitue les paramètres du signal élémentaires, à multiplier par le nombre de gaussiennes sommées, pour obtenir le nombre total de paramètres à déterminer.
Ces derniers sont déterminés selon le critère du maximum de vraisemblance, leur estimation se fait en optimisant une fonction coût, non-convexe, si bien que les algorithmes classiquement utilisés, basés sur des méthodes d'annulation de gradient, ne peuvent garantir le renvoi du paramètre optimal recherché, car convergeant vers les extrema locaux de la fonction coût.
Il existe des algorithmes garantissant le renvoi du minimum global, tels que la force brute et le recuit simulé, mais l'inconvénient majeur de ces deux approches, en dépit de leur efficacité, est que le temps de calcul nécessaire pour obtenir une solution acceptable est trop long.
Une autre solution consiste à utiliser les méthodes de gradient, mais à partir d'une condition initiale proche de la vraie solution. Cette condition initiale pertinente est obtenue, dans ce mémoire, à l'aide du filtrage adapté stochastique (FAS) utilisé en détection, qui nécessite la connaissance *a priori* des autocorrélations du signal utile et du bruit. Celle du signal utile est obtenue par la moyenne empirique d'autocorrélations déterministes de signaux élémentaires gaussiens pour différentes valeurs de paramètres, alors que celle du bruit est estimée sur un intervalle de temps où il n'est supposé y avoir que du bruit dans l'observation. Ces modèles permettent de construire un test d'hypothèse simple, capable d'exprimer la présence ou non de signal utile dans l'observation. L'utilisation du FAS en détection donne dans ce contexte de bons résultats, validés par une expérimentation sur une observation faite de la superposition de trois signaux élémentaires bruités.
L'algorithme EM est parfaitement adapté à ce type de modèle, puisqu'il permet, en théorie, de remplacer l'estimation de tous les paramètres par l'estimation disjointe de chaque triplet indépendamment les uns des autres. L'étape E consiste à isoler chacune des activités, alors que l'étape M sert à déterminer le triplet de paramètres inconnus correspondant. Voilà pourquoi pour chaque partie constituée, le FAS est appliqué avant l'étape M, ce qui permet de guider l'algorithme vers la solution correcte.
Des expérimentations sont alors réalisées sur une observation test afin de calibrer l'ensemble, puis sur une observation réelle issue du macromodèle afin de valider la technique FAS-EM sur des signatures ayant un sens physique. Les résultats sont bons dans la mesure, où s'il n'y a pas un niveau de bruit trop élevé et si les activités ne présentent pas de recouvrement trop important, il est possible d'estimer une signature issue de l'activité de 8 cellules élémentaires.
Certains bémols sont cependant à souligner. Une certaine subjectivité demeure quant au choix

de la taille de la fenêtre d'observation lors de l'utilisation du FAS. Une solution consisterait alors adopter la même démarche que celle du pirate, c'est-à-dire à constituer une base de donnée de signatures élémentaires[1], puis d'utiliser le FAS sur l'observation étudiée avec chacune des signatures enregistrées dans la base, afin d'identifier au mieux les différentes activités présentes dans l'observation. Une autre solution consisterait à utiliser les statistiques d'ordre supérieur. En effet, en utilisant le fait que le kurtosis d'une densité de probabilité gaussienne centrée vaut 3, il serait alors possible d'intégrer ce facteur afin de construire un détecteur plus performant.
De plus, le FAS est tel que plus le modèle d'autocorrélation du signal utile est fin, meilleure est la détection. Il serait alors intéressant de construire un tel type de modèle, en considérant par exemple une situation bayésienne, où les paramètres seraient des variables aléatoires, ce qui permettrait de définir la densité de probabilité associée au signal utile, alors considéré comme un processus aléatoire. Son expression serait, par la suite, injectée dans le rapport de vraisemblance aidant à construire le détecteur.
Par ailleurs, le FAS est une technique qui ne cesse de se développer et dont le nombre d'application ne cesse d'abonder, ce qui m'a permis, en parallèle des travaux présentés dans ce manuscrit, de m'intéresser aux problèmes liés à la détection d'objets en environnement bruité, ainsi qu'au débruitage d'images RADAR et SONAR en présence d'un bruit multiplicatif, connu sous l'appellation de speckle. Le FAS en dimension deux y est abondamment utilisé et a permis la rédaction de deux articles, ainsi que la participation à plusieurs conférences nationales et internationales [Cha05, Cha06, Cha05b1, Cha05b2, Cha06s1, Cha06s2, Cou06].

[1] Le nombre d'activités possible de la carte étant fini, l'ensemble des signatures possibles l'est donc également.

ANNEXE A

DÉMONSTRATION DU THÉORÈME II.1

L'outil de majoration utilisé pour démontrer le théorème est l'inégalité triangulaire.

$$\begin{aligned}\|F_a(X_2) - F_a(X_1)\| &\leq \|A(X_2 - X_1) + (b(X_2) - b(X_1))\| \\ &\leq \|A(X_2 - X_1)\| + \|b(X_2) - b(X_1)\|.\end{aligned}$$

En utilisant l'expression II.4 du problème (P_a), il vient pour la partie linéaire

$$\|A(X_2 - X_1)\| \leq (|a| + 1)(|y_2 - y_1| + |z_2 - z_1|) + |a|\,|x_2 - x_1|,$$

alors que pour la partie non-linéaire

$$\|b(X_2) - b(X_1)\| = |a|\,|g_\eta(x_2) - g_\eta(x_1)|,$$

il faut donc distinguer plusieurs cas de figure car

$$g_\eta(x_2) - g_\eta(x_1) = \begin{cases} \frac{1}{\eta}(x_2 - x_1) & \text{si } |x_1| < \eta \text{ et } |x_2| < \eta \\ -1 - \frac{1}{\eta}x_1 & \text{si } |x_1| < \eta \text{ et } x_2 < -\eta \\ 1 - \frac{1}{\eta}x_1 & \text{si } |x_1| < \eta \text{ et } x_2 > \eta \\ 0 & \text{si } x_1 < -\eta \text{ et } x_2 < -\eta \\ 1 + \frac{1}{\eta}x_2 & \text{si } x_1 < -\eta \text{ et } |x_2| < \eta \\ 2 & \text{si } x_1 < -\eta \text{ et } x_2 > \eta \\ -2 & \text{si } x_1 > \eta \text{ et } x_2 < -\eta \\ -1 + \frac{1}{\eta}x_2 & \text{si } x_1 > \eta \text{ et } |x_2| < \eta \\ 0 & \text{si } x_1 > \eta \text{ et } x_2 > \eta \end{cases},$$

avec par définition $|\eta| < 1$. Le but est alors de majorer $|g_\eta(x_2) - g_\eta(x_1)|$ dans chaque cas de sorte que cette dernière ajoutée à la majoration des termes linéaires, donne le résultat escompté.

– Si $|x_1| < \eta$ et $|x_2| < \eta$, en utilisant le fait que $\frac{1}{\eta} > 1$

$$\begin{aligned}\|F_a(X_2) - F_a(X_1)\| &\leq (|a| + 1)(|y_2 - y_1| + |z_2 - z_1|) + |a|\,|x_2 - x_1| + \frac{1}{\eta}|x_2 - x_1| \\ &\leq (|a| + \frac{1}{\eta})(|y_2 - y_1| + |z_2 - z_1|) + (|a| + \frac{1}{\eta})|x_2 - x_1| \\ &\leq (|a| + \frac{1}{\eta})\|X_2 - X_1\|.\end{aligned}$$

– Si $|x_1| < \eta$ et $x_2 < -\eta$, alors

$$\begin{aligned}\|F_a(X_2) - F_a(X_1)\| &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + |1+\frac{1}{\eta}x_1| \\ &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + 1 + \underbrace{\frac{1}{\eta}|x_1|}_{<1} \\ &\leq |a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + \underbrace{2}_{<2|x_2-x_1|} \\ &\leq (|a|+2)\|X_2-X_1\|.\end{aligned}$$

– Si $|x_1| < \eta$ et $x_2 > \eta$,

$$\begin{aligned}\|F_a(X_2) - F_a(X_1)\| &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + |\underbrace{1}_{<\frac{x_2}{\eta}} - \frac{1}{\eta}x_1| \\ &\leq (|a|+\frac{1}{\eta})(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + \frac{1}{\eta}\,|x_2-x_1| \\ &\leq (|a|+\frac{1}{\eta})\|X_2-X_1\|.\end{aligned}$$

– Si $x_1 < -\eta$ et $x_2 < -\eta$,

$$\begin{aligned}\|F_a(X_2) - F_a(X_1)\| &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| \\ &\leq (|a|+1)\|X_2-X_1\|.\end{aligned}$$

– Si $x_1 < -\eta$ et $|x_2| < \eta$

$$\begin{aligned}\|F_a(X_2) - F_a(X_1)\| &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + |1+\frac{1}{\eta}x_2| \\ &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + 1 + \underbrace{\frac{1}{\eta}|x_2|}_{<1} \\ &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + \underbrace{2}_{<2|x_2-x_1|} \\ &\leq (|a|+2)\|X_2-X_1\|.\end{aligned}$$

– Si $x_1 < -\eta$ et $x_2 > \eta$,

$$\begin{aligned}\|F_a(X_2) - F_a(X_1)\| &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + \underbrace{2}_{<2|x_2-x_1|} \\ &\leq (|a|+2)\|X_2-X_1\|.\end{aligned}$$

– Si $x_1 > \eta$ et $x_2 < -\eta$, par analogie à ce qui précède,

$$\|F_a(X_2) - F_a(X_1)\| \leq (|a|+2)\|X_2-X_1\|.$$

– Si $x_1 > \eta$ et $|x_2| < \eta$,

$$\begin{aligned}\|F_a(X_2) - F_a(X_1)\| &\leq (|a|+1)(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + |\frac{1}{\eta}x_2 - \underbrace{1}_{<\frac{x_1}{\eta}}| \\ &\leq (|a|+\frac{1}{\eta})(|y_2-y_1|+|z_2-z_1|) + |a|\,|x_2-x_1| + \frac{1}{\eta}\,|x_2-x_1| \\ &\leq (|a|+\frac{1}{\eta})\|X_2-X_1\|.\end{aligned}$$

– Si $x_1 > \eta$ et $x_2 > \eta$, le résultat est immédiat,

$$\|F_a(X_2) - F_a(X_1)\| \quad \leq \quad (|a| + 1)\|X_2 - X_1\|.$$

Ainsi, dans tous les cas de figure, en posant

$$k \quad := \quad |a| + \max(2\,;\, \frac{1}{\eta}),$$

le théorème est démontré.

□

ANNEXE B

EXPRESSION ANALYTIQUE DE L'OPÉRATEUR $F_a^h(X)$

Tout d'abord,

$$X + \frac{h}{2}F_a(X) \;=\; \begin{bmatrix} x + \frac{h}{2}y \\ y + \frac{h}{2}z \\ z + \frac{ah}{2}(x + y + z - g_\eta(x)) \end{bmatrix},$$

donc

$$K_2 = F_a(X + \frac{h}{2}F_a(X)) \;=\; \begin{bmatrix} y + \frac{h}{2}z \\ z + \frac{ah}{2}(x + y + z - g_\eta(x)) \\ \Big((a + \frac{1}{2}ha^2)x + (a + \frac{1}{2}ha + \frac{1}{2}ha^2)y + (a + \frac{1}{2}ha + \frac{1}{2}ha^2)z \\ -\frac{1}{2}ha^2 g_\eta(x) - ag_\eta(x + \frac{h}{2}y)\Big) \end{bmatrix}.$$

La connaissance de l'expression de K_2 permet de calculer celle de K_3,

$$X + \frac{h}{2}K_2 \;=\; \begin{bmatrix} x + \frac{h}{2}y + \frac{h^2}{4}z \\ a\frac{h^2}{4}x + (1 + \frac{h^2}{4}a)y + (\frac{h}{2} + \frac{h^2}{4}a)z - \frac{h^2}{4}ag_\eta(x) \\ \Big((\frac{h}{2}a + \frac{h^2}{4}a^2)x + (\frac{h}{2}a + \frac{h^2}{4}a + \frac{h^2}{4}a^2)y + (1 + \frac{h^2}{4}a + \frac{h}{2}a + \frac{h^2}{4}a^2)z \\ -\frac{h^2}{4}a^2 g_\eta(x) - \frac{h}{2}ag_\eta(x + \frac{h}{2}y)\Big) \end{bmatrix},$$

puis,

$$K_3 = F_a(X + \frac{h}{2}K_2) = \begin{bmatrix} a\frac{h^2}{4}x + (1 + \frac{h^2}{4}a)y + (\frac{h}{2} + \frac{h^2}{4}a)z - \frac{h^2}{4}ag_\eta(x) \\ \Big((\frac{h}{2}a + \frac{h^2}{4}a^2)x + (\frac{h}{2}a + \frac{h^2}{4}a + \frac{h^2}{4}a^2)y + (1 + \frac{h^2}{4}a + \frac{h}{2}a + \frac{h^2}{4}a^2)z \\ -\frac{h^2}{4}a^2 g_\eta(x) - \frac{h}{2}ag_\eta(x + \frac{h}{2}y)\Big) \\ \Big((a + \frac{h^2}{4}a^2 + \frac{h}{2}a^2 + \frac{h^2}{4}a^3)x + (a + \frac{h}{2}a + \frac{h}{2}a^2 + \frac{h^2}{2}a^2 + \frac{h^2}{4}a^3)y \\ +(\frac{h}{4}a + a + \frac{h}{2}a + \frac{h}{2}a^2 + \frac{h^2}{2}a^2 + \frac{h^2}{4}a^3)z - (\frac{h^2}{4}a^2 + \frac{h^2}{4}a^3)g_\eta(x) \\ -a^2\frac{h}{2}g_\eta(x + \frac{h}{2}y) - ag_\eta(x + \frac{h}{2}y + \frac{h^2}{4}z)\Big) \end{bmatrix}.$$

Enfin, K_4 se calcule à partir de K_3 par la relation $K_4 = F_a(X + hK_3)$, tout d'abord,

$$X + hK_3 = \begin{bmatrix} (1 + a\frac{h^3}{4})x + (h + a\frac{h^3}{4})y + (\frac{h^2}{2} + a\frac{h^3}{4})z - a\frac{h^3}{4}g_\eta(x) \\ \Big((a\frac{h^2}{2} + a^2\frac{h^3}{4})x + (1 + a\frac{h^3}{4} + a\frac{h^2}{2} + a^2\frac{h^3}{4})y + (h + a\frac{h^3}{4} + a\frac{h^2}{2} + a^2\frac{h^3}{4})z \\ -a^2\frac{h^3}{4}g_\eta(x) - a\frac{h^2}{2}g_\eta(x + \frac{h}{2}y)\Big) \\ \Big((ah + a^2\frac{h^3}{4} + a^2\frac{h^2}{2} + a^3\frac{h^3}{4})x + (a\frac{h^2}{2} + ah + a^2\frac{h^3}{2} + a^2\frac{h^2}{2} + a^3\frac{h^3}{4})y \\ +(1 + a\frac{h^3}{4} + a\frac{h^2}{2} + a^2\frac{h^3}{2} + ah + a^2\frac{h^2}{2} + a^3\frac{h^3}{4})z \\ -(a^2\frac{h^3}{4} + a^3\frac{h^3}{4})g_\eta(x) - a^2\frac{h^2}{2}g_\eta(x + \frac{h}{2}y) - ahg_\eta(x + \frac{h}{2}y + \frac{h^2}{4}z)\Big) \end{bmatrix},$$

et l'image de ce vecteur par l'application F_a donne l'expression de K_4,

$$K_4 = F_a(X + hK_3) =$$

$$\begin{bmatrix} \Big((a\frac{h^2}{2}+a^2\frac{h^3}{4})x+(1+a\frac{h^3}{4}+a\frac{h^2}{2}+a^2\frac{h^3}{4})y \\ +(h+a\frac{h^3}{4}+a\frac{h^2}{2}+a^2\frac{h^3}{4})z-a^2\frac{h^3}{4}g_\eta(x)-a\frac{h^2}{2}g_\eta(x+\frac{h}{2}y)\Big) \\ \\ \Big((ah+a^2\frac{h^3}{4}+a^2\frac{h^2}{2}+a^3\frac{h^3}{4})x+(a\frac{h^2}{2}+ah+a^2\frac{h^3}{2}+a^2\frac{h^2}{2}+a^3\frac{h^3}{4})y \\ +(1+a\frac{h^3}{4}+a\frac{h^2}{2}+a^2\frac{h^3}{2}+ah+a^2\frac{h^2}{2}+a^3\frac{h^3}{4})z \\ -(a^3\frac{h^3}{4}+a^2\frac{h^3}{4})g_\eta(x)-a^2\frac{h^2}{2}g_\eta(x+\frac{h}{2}y)-ahg_\eta(x+\frac{h}{2}y+\frac{h^2}{4}z)\Big) \\ \\ \Big((a+a^2\frac{h^3}{4}+a^2\frac{h^2}{2}+a^3\frac{h^3}{4}+a^2h+a^3\frac{h^3}{4}+a^3\frac{h^2}{2}+a^4\frac{h^3}{4})x \\ +(ah+a^2\frac{h^3}{4}+a+a^2\frac{h^3}{4}+a^2\frac{h^2}{2}+a^3\frac{h^3}{4}+a^2\frac{h^2}{2}+a^2h+a^3\frac{h^3}{2}+a^3\frac{h^2}{2}+a^4\frac{h^3}{4})y \\ +(a\frac{h^2}{2}+a^2\frac{h^3}{4}+ah+a^2\frac{h^3}{4}+a^2\frac{h^2}{2}+a^3\frac{h^3}{4}+a+a^2\frac{h^3}{4}+a^2\frac{h^2}{2}+a^2\frac{h^3}{2}+a^2h+a^3\frac{h^2}{2}+a^4\frac{h^3}{4})z \\ -ag_\eta(\,(1+a\frac{h^3}{4})x+(h+a\frac{h^3}{4})y+(\frac{h^2}{2}+a\frac{h^3}{4})z-a\frac{h^3}{4}g_\eta(x)\,) \\ -(a^3\frac{h^3}{4}+a^4\frac{h^3}{4}+a^2\frac{h^3}{4}+a^3\frac{h^3}{4})g_\eta(x)-(a^2\frac{h^2}{2}+a^3\frac{h^2}{2})g_\eta(x+\frac{h}{2}y)-a^2hg_\eta(x+\frac{h}{2}y+\frac{h^2}{4}z)\Big) \end{bmatrix}.$$

Toutes les informations sont réunies pour expliciter $F_a^h(X) = \frac{1}{6}\left(F_a(X)+2K_2+2K_3+K_4\right)$,

après une lourde mais nécessaire phase de calcul et un regroupement approprié des termes,

$$F_a^h(X) = \begin{cases} C_a(ah+4)x + (1+C_a(4+(1+a)h))y + (\frac{h}{2}+C_a(4+(a+1)h))z \\ -C_a(ah+2)g_\eta(x) - 2C_a g_\eta(x+\frac{h}{2}y) \\ \\ (a\frac{h}{2}+\frac{h^2}{12}+C_a(2+h(1+a)))x + (a\frac{h}{2}+C_a(4(1+a)+ah(2+a)))y \\ +(1+a\frac{h}{2}+C_a(4(1+a)+h(1+a)^2))z \\ -(a\frac{h}{6}+C_a(2a+ah(1+a)))g_\eta(x) - ahg_\eta(x+\frac{h}{2}y+\frac{h^2}{4}z) \\ \\ (2a(1+a\frac{h}{3})+aC_a(2(2+a)+h(1+6a+a^2)))x \\ +(\frac{a}{2}(2+h(1+a))+aC_a(4a(2+a)+ah(2+3a+a^2)))y \\ +(a(\frac{7}{12}h+1+a\frac{h}{2})+C_a(2+8a+4a^2+ah(5+a+a^2)))z \\ -(\frac{a}{6}(1+ah)+C_a(2a(1+a)+ah(1+a)^2))g_\eta(x) \\ -(\frac{a}{6}(2+ah)+2aC_a(1+a))g_\eta(x+\frac{h}{2}y) \\ -\frac{a}{6}(2+ah)g_\eta(x+\frac{h}{2}y+\frac{h^2}{4}z) \\ -\frac{a}{6}g_\eta(\,(1+a\frac{h^3}{4})x + (h+a\frac{h^3}{4})y + (\frac{h^2}{2}+a\frac{h^3}{4})z - a\frac{h^3}{4}g_\eta(x)\,) \end{cases}$$

avec $C_a := a\frac{h^2}{24}$.

ANNEXE C

PREUVE DE LA PROPOSITION II.2

Les valeurs propres de A sont par définition solutions du polynôme de degré 3

$$det(A - \lambda Id) \quad = \quad 0,$$

qui s'exprime en explicitant le membre de gauche de l'expression et en développant le déterminant suivant la première colonne,

$$\begin{aligned} det(A-\lambda Id) = 0 \quad &\Leftrightarrow \quad \begin{vmatrix} -\lambda & 1 & 0 \\ 0 & -\lambda & 1 \\ a & a & a-\lambda \end{vmatrix} = 0 \\ &\Leftrightarrow \quad -\lambda(-\lambda(a-\lambda)-a)+a \\ &\Leftrightarrow \quad \lambda^3 - a\lambda^2 - a\lambda - a = 0. \end{aligned}$$

La résolution analytique par radicaux de cette équation polynomiale de degré 3 s'effectue selon la méthode de Cardan [Esc97].

- Si $a = 0$, le cas est trivial puisqu'il s'agit alors de résoudre $x = 0$ de solution évidente $x = 0$.
- Si $a = -3$, l'expression du polynôme fait apparaître une identité remarquable permettant ainsi de le factoriser simplement, puis de calculer ses racines,

$$\begin{aligned} \lambda^3 + 3\lambda^2 + 3\lambda + 3 \quad &= \quad 0 \quad \Leftrightarrow \\ (\lambda+1)^3 + 2 \quad &= \quad 0 \quad \Leftrightarrow \\ \underbrace{(\lambda+1)}_{z=\lambda+1}{}^3 \quad &= \quad -2 \quad \Leftrightarrow \\ z^3 \quad &= \quad -2 \quad = 2e^{i\pi} \quad \Leftrightarrow \\ z^3 \quad &= \quad 2e^{i\pi}. \end{aligned}$$

Cette équation se résout en égalisant les modules et les arguments[1] des expression de gauche et de droite de l'égalité, ainsi

$$\begin{aligned} z^3 = 2e^{i\pi} \quad &\Leftrightarrow \quad \begin{cases} |z|^3 \quad &= \quad 2 \\ 3\,arg(z) \quad &\equiv \quad \pi \quad [2\pi] \end{cases} \\ &\Leftrightarrow \quad \begin{cases} \{|z| \quad &= \quad \sqrt[3]{2} \\ arg(z) \quad &\equiv \quad \frac{\pi}{3} \quad [\frac{2\pi}{3}] \end{cases} \end{aligned}$$

[1] L'égalité de deux arguments est une congruence, à interpréter comme une relation d'équivalence définie par $a \equiv b \quad [r] \Leftrightarrow \exists q \in \mathbb{Z}^* / a = bq + r$

et l'expression des 3 racines est

$$\lambda = \begin{cases} -1 - \sqrt[3]{2} \\ \text{ou} \\ -1 + \sqrt[3]{2}\, e^{i\frac{\pi}{3}} \\ \text{ou} \\ -1 + \sqrt[3]{2}\, e^{-i\frac{\pi}{3}} \end{cases} .$$

En particulier,

$$\begin{cases} \lambda_1 = -1 - \sqrt[3]{2} \approx -2,26 \\ Re[\lambda_2] = -1 + \dfrac{\sqrt[3]{2}}{2} \approx -0,37 \\ Im[\lambda_2] = \dfrac{\sqrt[3]{2}\sqrt{3}}{2} \approx 1,09 \end{cases} . \tag{C.1}$$

Donc, dans le cas où $a = -3$, le spectre est composé d'une valeur propre réelle négative et de deux valeurs propres complexes conjuguées de partie réelle négative.

– Dans le dernier cas de figure, si $a \in \mathbb{R} - \{-3; 0\}$, il convient d'écrire le polynôme sous sa forme normale

$$z^3 + pz + q = 0, \tag{C.2}$$

obtenue pour tout $a \in \mathbb{R}^*$ par l'intermédiaire du changement de variable $\lambda = z + a/3$. Par substitution il vient

$$\begin{aligned} (z + a/3)^3 - a(z + a/3)^2 - a(z + a/3) - a &= 0 \Leftrightarrow \\ z^3 + az^2 + \frac{1}{3}a^2 z + \frac{1}{27}a^3 - az^2 - \frac{2}{3}a^2 z - \frac{1}{9}a^3 - az - \frac{1}{3}a^2 - a &= 0 \Leftrightarrow \\ z^3 + pz + q &= 0 \end{aligned}$$

avec

$$\begin{cases} p := -\dfrac{1}{3}a^2 - a = -\dfrac{a}{3}(a+3) \\ q := \dfrac{1}{27}a^3 - \dfrac{1}{9}a^3 - \dfrac{1}{3}a^2 - a = -\dfrac{a}{27}(2a^2 + 9a + 27) \end{cases}$$

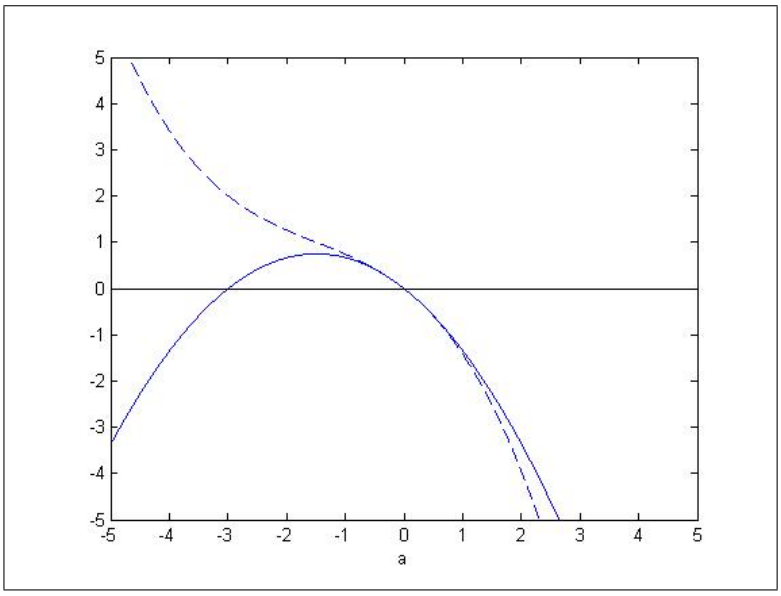


FIG. 1 – *Représentation graphique de p (trait plein) et q (traits pointillés) en fonction de a.*

La représentation graphique conjointe des applications $a \mapsto p(a)$ et $a \mapsto q(a)$ de la figure 1 permet d'établir que si $a \geq -3$, alors p et q sont de même signe et inversement si $a < -3$, alors p et q sont de signe opposé.
L'étape suivante consiste à poser le changement de variable

$$z = u + v$$

L'application de ce changement de variable par substitution dans l'équation C.2, puis une étape d'identification conduisent à

$$\begin{aligned}
(u+v)^3 + p(u+v) + q &= 0 \Leftrightarrow \\
u^3 + 3u^2v + 3uv^2 + v^3 + pu + pv + q &= 0 \Leftrightarrow \\
u^3 + v^3 + q + (3uv + p)(u+v) &= 0 \Leftrightarrow \\
\left\{ \begin{array}{lcl} u^3 + v^3 & = & -q \\ uv & = & -p/3 \end{array} \right.
\end{aligned}$$

Si ces conditions sont respectées, alors

$$\left\{ \begin{array}{lcl} u^3 + v^3 & = & -q \\ u^3 v^3 & = & -\dfrac{p^3}{27} \end{array} \right. ,$$

donc, le couple $(u^3; v^3)$ est solution de l'équation du second degré en w

$$w^2 + qw - \frac{p^3}{27} = 0 \tag{C.3}$$

L'expression du discriminant de cette équation est

$$\begin{aligned}
\Delta &= q^2 + \frac{4}{27}p^3 \Leftrightarrow \\
\Delta &= \frac{1}{27}a^2\left(14a + 3a^2 + 27\right) \Rightarrow \\
\Delta &\geq 0,
\end{aligned}$$

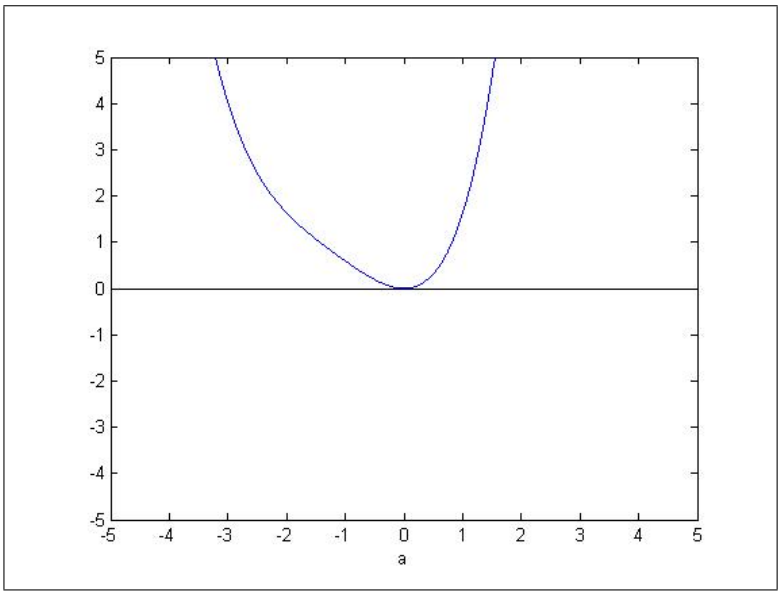


FIG. 2 – *Représentation graphique de Δ en fonction de a.*

la figure 2 montre la représentation graphique de l'application $a \mapsto \Delta(a)$. Cette dernière est telle que pour tout réel $a \neq 0$, $\Delta > 0$, donc les deux racines w_1 et w_2 de C.3 sont réelles et

$$\begin{cases} w_1 = u^3 & = & \dfrac{-q+\sqrt{\Delta}}{2} \\ w_2 = v^3 & = & \dfrac{-q-\sqrt{\Delta}}{2} \end{cases}$$

Le signe de l'application $a \mapsto w_1(a)$, comme le montre la figure 3, est tel que si $a > -3$ alors w_1 est strictement positif ; alors que si $a < -3$, w_1 est négatif.

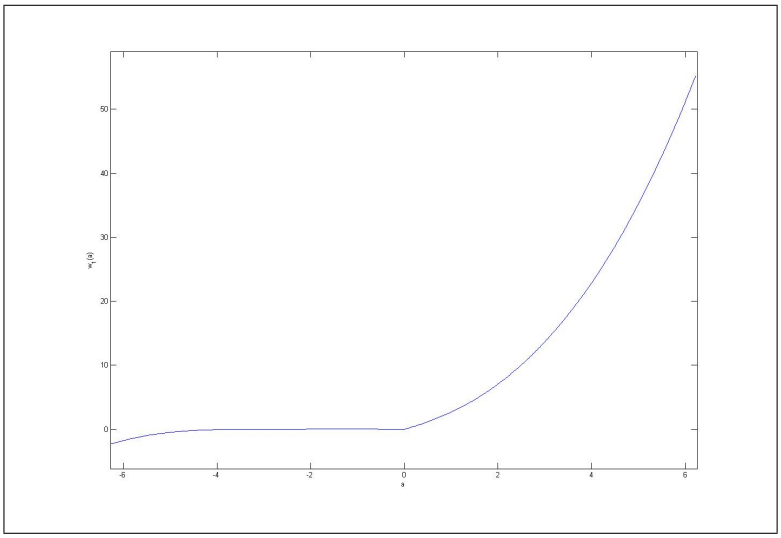


FIG. 3 – *Représentation graphique de w_1 en fonction de a.*

Dans le cas où $a > 0$, l'étape suivant consiste à extraire les racines cubiques de u^3 et v^3. Or, la connaissance de la première équivaut à celle de la seconde car $uv = -p/3$, donc v se déduit facilement de u dont l'expression s'obtient en résolvant dans $\mathbb{C}$ l'équation $u^3 = w_1$ avec w_1 un nombre éventuellement complexe tel que $w_1 = \dfrac{-q+\sqrt{\Delta}}{2}$ dépendant donc de a,

$$\begin{aligned} u^3 = w_1 &\Leftrightarrow |u|^3 e^{i3arg(u)} = |w| e^{i\,arg(w_1)} \\ &\Leftrightarrow \begin{cases} |u|^3 & = & |w_1| \\ 3\,arg(u) & \equiv & arg(w_1) \quad [2\pi] \end{cases} \\ &\Leftrightarrow \begin{cases} |u| & = & \sqrt[3]{|w_1|} \\ arg(u) & \equiv & arg(w_1) \quad [\dfrac{2\pi}{3}] \end{cases} \\ &\Leftrightarrow u = \begin{cases} \sqrt[3]{|w_1|} e^{i\,arg(w_1)} \\ \text{ou} \\ \sqrt[3]{|w_1|} e^{i\,(arg(w_1)+\frac{2\pi}{3})} \\ \text{ou} \\ \sqrt[3]{|w_1|} e^{i\,(arg(w_1)-\frac{2\pi}{3})} \end{cases} \end{aligned}$$

Ainsi,

$$u = \begin{cases} \sqrt[3]{w_1} \\ \text{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{2\pi}{3}} \\ \text{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{4\pi}{3}} \end{cases} \qquad \text{et comme } v = -\frac{p}{3u}, \qquad v = \begin{cases} -\dfrac{p}{3\sqrt[3]{w_1}} \\ \text{ou} \\ -\dfrac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{2\pi}{3}} \\ \text{ou} \\ -\dfrac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{4\pi}{3}} \end{cases}$$

si bien que d'après les changements de variables successifs effectués pour en arriver là,

$$\lambda = u + v + a/3 = \begin{cases} \sqrt[3]{w_1} - \dfrac{p}{3\sqrt[3]{w_1}} + a/3 \\ \text{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{2\pi}{3}} - \dfrac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{2\pi}{3}} + a/3 \\ \text{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{4\pi}{3}} - \dfrac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{4\pi}{3}} + a/3 \end{cases}$$

et,toutes simplifications faites, pour tout $a > -3$, l'expression des racines λ_1, λ_2 et λ_3 en fonction de a,

$$\begin{cases} \lambda_1 &=& R(a) + \dfrac{a(a+3)}{9R(a)} + \dfrac{a}{3} \\ \lambda_2 &=& -\dfrac{1}{2}\left(R(a) + \dfrac{a(a+3)}{9R(a)}\right) + i\dfrac{\sqrt{3}}{2}\left(R(a) - \dfrac{a(a+3)}{9R(a)}\right) + \dfrac{a}{3} &=& \alpha + i\omega \\ \lambda_3 &=& -\dfrac{1}{2}\left(R(a) + \dfrac{a(a+3)}{9R(a)}\right) - i\dfrac{\sqrt{3}}{2}\left(R(a) - \dfrac{a(a+3)}{9R(a)}\right) + \dfrac{a}{3} &=& \alpha - i\omega \end{cases} \tag{C.4}$$

avec

$$R(a) \;:=\; \frac{1}{6}\sqrt[3]{8a^3 + 36a^2 + 108a + 12\sqrt{9a^4 + 42a^3 + 81a^2}},$$

$R(a)$ étant une quantité réelle et positive.
Donc, dans le cas où $a \geq -3$, le spectre de A est composé d'une racine réelle λ_1 et deux racines complexes conjuguées λ_2 et λ_3.
Dans le cas où $a < -3$, $w_1 < 0$. Le passage à la racine cubique présente donc une difficulté qu'il convient de contourner en arguant que

$$\begin{array}{rcl} w_1 < 0 & \Leftrightarrow & -w_1 > 0 \\ \text{donc} & & \\ \sqrt[3]{w_1} &=& \sqrt[3]{-(-w_1)} \\ &=& \sqrt[3]{(-w_1)e^{i\pi}} \\ &=& \sqrt[3]{(-w_1)}e^{\frac{i\pi}{3}}. \end{array}$$

Alors, l'expression des racines est

$$\lambda = u+v+a/3 = \left\{ \begin{array}{l} \sqrt[3]{w_1} e^{\frac{i\pi}{3}} - \frac{p}{3\sqrt[3]{w_1}} e^{\frac{-i\pi}{3}} + a/3 \\ \text{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{2\pi}{3}} e^{\frac{i\pi}{3}} - \frac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{2\pi}{3}} e^{-\frac{i\pi}{3}} + a/3 \\ \text{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{4\pi}{3}} e^{\frac{i\pi}{3}} - \frac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{4\pi}{3}} e^{\frac{i\pi}{3}} + a/3 \end{array} \right. ,$$

si bien que pour tout $a < -3$

$$\left\{ \begin{array}{rcl} \lambda_1 &=& \frac{1}{2}\left(R(a) + \frac{a(a+3)}{9R(a)}\right) + i\frac{\sqrt{3}}{2}\left(R(a) - \frac{a(a+3)}{9R(a)}\right) + \frac{a}{3} = \alpha' + i\omega' \\ \lambda_2 &=& -R(a) - \frac{a(a+3)}{9R(a)} + \frac{a}{3} \\ \lambda_3 &=& \frac{1}{2}\left(R(a) + \frac{a(a+3)}{9R(a)}\right) - i\frac{\sqrt{3}}{2}\left(R(a) - \frac{a(a+3)}{9R(a)}\right) + \frac{a}{3} = \alpha' - i\omega' \end{array} \right.$$

Les expressions des racines sont différentes selon que $a > -3$ ou $a > -3$, si bien que chacune présente une discontinuité de seconde espèce en $a = -3$. Or, les règles de calcul des limites[2] appliquées à $R(a)$ montrent que

$$\left\{ \begin{array}{rcl} \lim\limits_{a\to -3} R(a) &=& 0 \\ \lim\limits_{\substack{a\to -3 \\ a>-3}} \frac{a(a+3)}{9R(a)} &=& -\sqrt[3]{2} \\ \lim\limits_{\substack{a\to -3 \\ a<-3}} \frac{a(a+3)}{9R(a)} &=& -\sqrt[3]{2} e^{\frac{2i\pi}{3}} \\ &=& -\frac{1}{2}\sqrt[3]{2} + i\frac{\sqrt{3}}{2}\sqrt[3]{2} \end{array} \right.$$

Ces résultats permettent d'établir que

$$\begin{array}{rcl} \lim\limits_{\substack{a\to -3 \\ a>-3}} \lambda_1(a) &=& \lim\limits_{\substack{a\to -3 \\ a<-3}} \lambda_2(a) \\ &=& -1 - \sqrt[3]{2} \\ &\approx& -2,26, \end{array}$$

$$\begin{array}{rcl} \lim\limits_{\substack{a\to -3 \\ a>-3}} \alpha(a) &=& \lim\limits_{\substack{a\to -3 \\ a<-3}} \alpha'(a) \\ &=& -1 + \frac{\sqrt[3]{2}}{2} \\ &\approx& -0,37, \end{array}$$

[2]En particulier, le comportement en l'origine d'une fraction rationnelle est régi par les termes de plus bas degré du numérateur et du dénominateur

et

$$\begin{aligned}\lim_{\substack{a\to -3\\ a>-3}} \omega(a) &= \lim_{\substack{a\to -3\\ a<-3}} \omega^{'}(a)\\ &= \frac{\sqrt[3]{2}\sqrt{3}}{2}\\ &\approx 1,09.\end{aligned}$$

Ces trois limites ne sont rien d'autre que les racines trouvées dans le cas $a = -3$. Bien que les racines aient une discontinuité de seconde espèce en $a = -3$, l'application l de $\mathbb{R} \to \mathbb{C}^3$ telle que pour tout $a \in \mathbb{R}$,

$$l(a) = \left\{ \begin{array}{l} \lambda_1(a) \\ \lambda_2(a) \\ \lambda_3(a) \end{array} \right. ,$$

ne présente quant à elle qu'une discontinuité de première espèce. Cette application est donc prolongeable par continuité en $a = 0$ et $a = -3$ en posant

$$l(0) := \left[\begin{array}{c} 0 \\ 0 \\ 0 \end{array} \right] \quad \text{et} \quad l(-3) := \left[\begin{array}{c} -1 - \sqrt[3]{2} \\ -1 + \frac{\sqrt[3]{2}}{2} + i\frac{\sqrt[3]{2}\sqrt{3}}{2} \\ -1 + \frac{\sqrt[3]{2}}{2} - i\frac{\sqrt[3]{2}\sqrt{3}}{2} \end{array} \right]. \tag{C.5}$$

L'existence de ce prolongement par continuité du spectre permet de montrer que $a = -3$ n'est pas une valeur pathologique, c'est-à-dire qu'il n'y a pas de changement de dynamique brusque en ce point. Le cas $a = -3$ est de la même nature que ceux tels que $a < -1$, à ceci prêt qu'à la traversée de ce point, la position des valeurs propres change. Le prolongement l est visible sur la figure 2, il suffit pour cela de considérer sur le graphe la réunion des courbes contiguës. Les courbes concernées sont séparées par un point en $a = 0$ et $a = -3$ pouvant être vu comme un "trou" qu'il convient de "boucher" à l'aide des points d'affixe donnée par (C.5).
Finalement, les précautions suffisantes sont prises pour affirmer que pour tout $a \neq 0$, la matrice A a trois valeurs propres, une réelle et deux complexes conjuguées. Leur position relative change aux points $a = 0$ et $a = -3$ comme la montre la figure 2.

ANNEXE D

PREUVE DE LA PROPOSITION II.3

Preuve . *Les valeurs propres de A_η sont solutions de*

$$det(A_\eta - \lambda Id) \quad = \quad 0,$$

qui s'exprime en explicitant le membre de gauche de l'expression et en développant le déterminant suivant la première colonne,

$$\begin{aligned} det(A_{eta} - \lambda Id) = 0 \quad \Leftrightarrow \quad & \begin{vmatrix} -\lambda & 1 & 0 \\ 0 & -\lambda & 1 \\ a(1-\frac{1}{\eta}) & a & a-\lambda \end{vmatrix} = 0 \\ \Leftrightarrow \quad & -\lambda(-\lambda(a-\lambda)-a) + a(1-\frac{1}{\eta}) \\ \Leftrightarrow \quad & \lambda^3 - a\lambda^2 - a\lambda - a + \frac{a}{\eta} = 0. \end{aligned}$$

Là encore la méthode de Cardan permet d'obtenir l'expression analytique des racines,

- *Si $a = 0$, alors l'équation différentielle se réduit à $x = 0$ de solution évidente $x(t) = 0$.*
- *Si $a = -3$, le polynôme se factorise simplement,*

$$\begin{aligned} \lambda^3 + 3\lambda^2 + 3\lambda + 3 - \frac{3}{\eta} \quad &= \quad 0 \quad \Leftrightarrow \\ (\lambda+1)^3 + 2 - \frac{3}{\eta} \quad &= \quad 0 \quad \Leftrightarrow \\ \underbrace{(\lambda+1)}_{z=\lambda+1}{}^3 \quad &= \quad \frac{3}{\eta} - 2 \quad \Leftrightarrow \\ z^3 \quad &= \quad \frac{3}{\eta} - 2. \end{aligned}$$

Or,

$$\begin{aligned} 0 < \eta < 1 \quad &\Leftrightarrow \\ \frac{1}{\eta} > 1 \quad &\Leftrightarrow \\ \frac{3}{\eta} - 2 > 1 > 0 \qquad &., \end{aligned}$$

donc

$$z^3 = \frac{3}{\eta} - 2 \quad \Leftrightarrow \quad \left\{ \begin{array}{rcl} |z|^3 & = & \frac{3}{\eta} - 2 \\ 3\, arg(z) & \equiv & 0 \quad [2\pi] \end{array} \right.$$
$$\Leftrightarrow \quad \left\{ \begin{array}{rcl} |z| & = & \sqrt[3]{\frac{3}{\eta} - 2} \\ arg(z) & \equiv & 0 \quad [\frac{2\pi}{3}] \end{array} \right.$$

et l'expression des 3 racines est

$$\lambda = \left\{ \begin{array}{l} -1 - \sqrt[3]{\frac{3}{\eta} - 2} \\ \textit{ou} \\ -1 + \sqrt[3]{\frac{3}{\eta} - 2}\, e^{i\, 2\frac{\pi}{3}} \\ \textit{ou} \\ -1 + \sqrt[3]{\frac{3}{\eta} - 2}\, e^{-i\, 2\frac{\pi}{3}} \end{array} \right. ,$$

ou encore, en distinguant parties réelles et imaginaires

$$\left\{ \begin{array}{rcl} \lambda_1 & = & -1 - \sqrt[3]{\frac{3}{\eta} - 2} \\ Re[\lambda_2] & = & -1 - \frac{1}{2}\sqrt[3]{\frac{3}{\eta} - 2} \\ Im[\lambda_2] & = & \frac{\sqrt{3}}{2}\sqrt[3]{\frac{3}{\eta} - 2} \end{array} \right. . \tag{D.1}$$

Si $\eta = 0,1$ *,*

$$\left\{ \begin{array}{rcl} \lambda_1 & \approx & 2,03 \\ Re[\lambda_2] & \approx & -2,52 \\ Im[\lambda_2] & \approx & 2,63 \end{array} \right. . \tag{D.2}$$

Ainsi, dans le cas où $a = -3$*, le spectre est composé d'une valeur propre réelle positive et de deux complexes conjuguées de partie réelle positive.*

– *Si* $a \in \mathbb{R} - \{-3; 0\}$*, La forme normale est obtenue pour tout* $a \in \mathbb{R}^*$ *en posant* $\lambda = z + a/3$*, ce qui donne*

$$z^3 + pz + q \;=\; 0,$$

avec

$$\left\{ \begin{array}{rcl} p & := & -\frac{1}{3}a^2 - a = -\frac{a}{3}(a+3) \\ q & := & -\frac{2}{27}a^3 - \frac{1}{3}a^2 - a + \frac{a}{\eta} = -\frac{a}{27}(2a^2 + 9a + 27(1 - \frac{1}{\eta})) \end{array} \right.$$

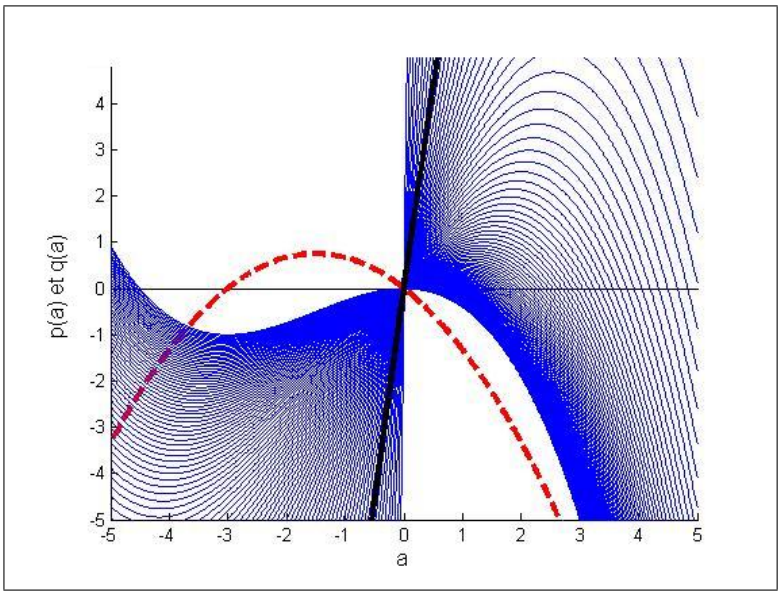


FIG. 1 – *Représentation graphique de p (trait pontillés), et de q (traits pleins) en fonction de a pour différentes valeurs de η. En gras le cas où $\eta = 0,1$.*

La figure 1 montre que si $-3 \leq a < 0$, alors p et q sont de signe opposé avec $q \leq 0$ pour tout $\eta \in]0\,;\,1[$, il faut donc poser le changement de variable

$$z \;=\; u - v.$$

et l'appliquer à l'équation normale,

$$\begin{aligned}
(u-v)^3 + p(u-v) + q &= 0 \Leftrightarrow \\
u^3 - 3u^2v + 3uv^2 - v^3 + pu - pv + q &= 0 \Leftrightarrow \\
u^3 - v^3 + q + (-3uv + p)(u-v) &= 0 \Leftrightarrow \\
\left\{ \begin{array}{rcl} u^3 - v^3 & = & -q \\ uv & = & p/3 \end{array} \right.
\end{aligned}$$

Pour obtenir le système d'équations

$$\left\{ \begin{array}{rcl} u^3 + (-v)^3 & = & -q \\ u^3(-v)^3 & = & -\dfrac{p^3}{27} \end{array} \right. ,$$

donc, le couple $(u^3; (-v)^3)$ est solution de l'équation du second degré en w

$$w^2 + qw - \frac{p^3}{27} \;=\; 0 \qquad \text{(D.3)}$$

de discriminant

$$\begin{aligned}
\Delta &= q^2 + \frac{4}{27}p^3 \Leftrightarrow \\
\Delta &= \frac{1}{27}a^2\left(3a^2 + 14a + 27 - \frac{1}{\eta}(4a^2 + 18a + 27(2 - \frac{1}{\eta}))\right)
\end{aligned}$$

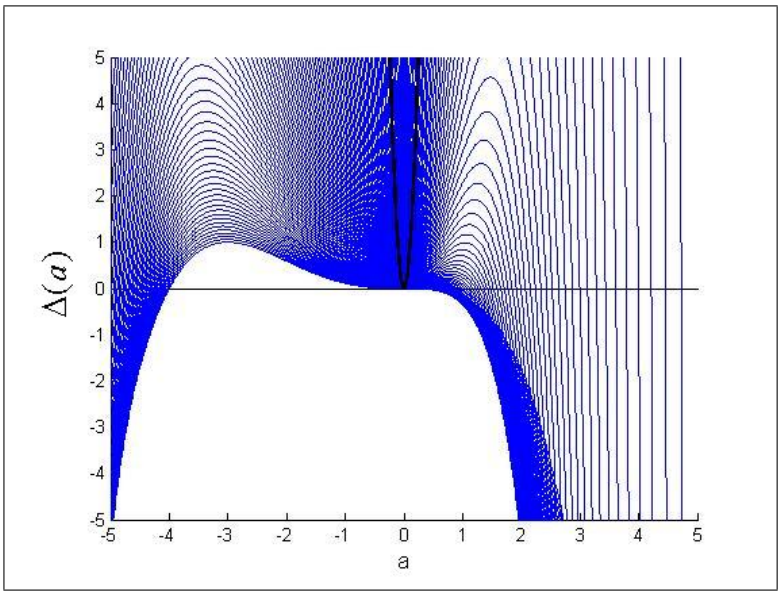


FIG. 2 – *Représentation graphique de l'application qui a tout* $a \in \mathbb{R}$ *associe* $\Delta(a)$ *pour plusieurs valeurs de* $\eta \in]0\,;\,1[$. *La courbe en gras est celle où* $\eta = 0,1$.

Comme le montre la figure 2, si $\eta = 0,1$, *alors* $\Delta > 0$ *et les deux racines* w_1 *et* w_2 *de D.3 sont réelles si bien que*

$$\begin{cases} w_1 = u^3 & = & \dfrac{-q+\sqrt{\Delta}}{2} \\ w_2 = (-v)^3 & = & \dfrac{-q-\sqrt{\Delta}}{2} \end{cases}$$

Dans le cas où $\eta = 0,1$, *d'après la figure 3,* w_1 *est réel si* $a \in]-4\,;\,0[$, *de plus si* $a < 0$, *alors* $w_1 > 0$ *alors que si* $a > 0$, *alors* $w_1 < 0$.

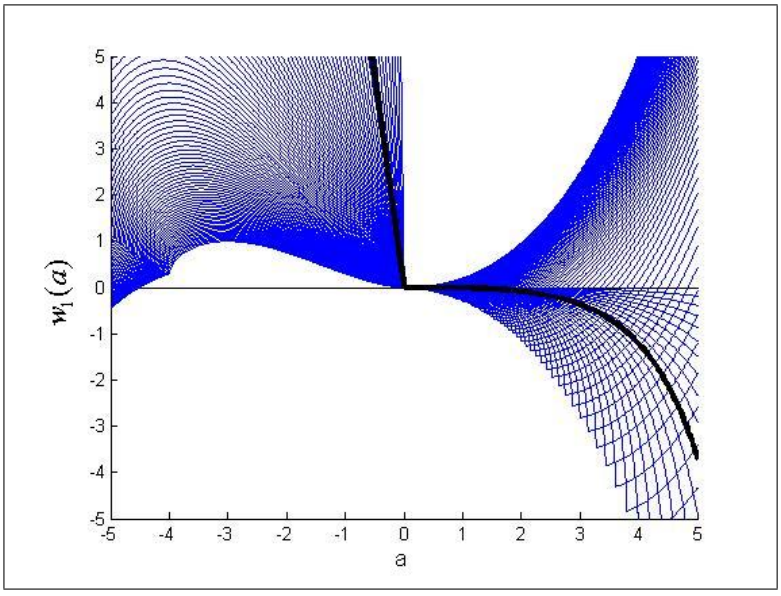


FIG. 3 – *Représentation graphique de l'application qui a tout* $a \in \mathbb{R}$ *associe* $w_1(a)$ *pour plusieurs valeurs de* $\eta \in]0\,;\,1[$. *La courbe en gras est celle où* $\eta = 0,1$.

Seules les racines cubiques de u *sont calculées car* u *et* v *sont liés par la relation uv=p/3,*

de plus, dans $\mathbb{C}$ *l'équation* $u^3 = w_1$ *avec* w_1 *un nombre réel tel que* $w_1 = \dfrac{-q+\sqrt{\Delta}}{2}$,

$$\begin{aligned}
u^3 = w_1 &\Leftrightarrow |u|^3 e^{i3arg(u)} = |w| e^{i\,arg(w_1)} \\
&\Leftrightarrow \left\{ \begin{array}{lcl} |u|^3 & = & |w_1| \\ 3\,arg(u) & \equiv & arg(w_1) \quad [2\pi] \end{array} \right. \\
&\Leftrightarrow \left\{ \begin{array}{lcl} |u| & = & \sqrt[3]{|w_1|} \\ arg(u) & \equiv & \dfrac{arg(w_1)}{3} \quad [\dfrac{2\pi}{3}] \end{array} \right. \\
&\Leftrightarrow u = \left\{ \begin{array}{l} \sqrt[3]{|w_1|} e^{i\dfrac{arg(w_1)}{3}} \\ \textit{ou} \\ \sqrt[3]{|w_1|} e^{i\dfrac{arg(w_1)}{3}} e^{i\dfrac{2\pi}{3}} \\ \textit{ou} \\ \sqrt[3]{|w_1|} e^{i\dfrac{arg(w_1)}{3}} e^{-i\dfrac{2\pi}{3}} \end{array} \right.
\end{aligned}$$

Ainsi, si $a \in]-3\,;\,0[$, $w_1 \in \mathbb{R}$ *et*

$$u = \left\{ \begin{array}{l} \sqrt[3]{w_1} \\ \textit{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{2\pi}{3}} \\ \textit{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{4\pi}{3}} \end{array} \right. \qquad \textit{et comme } v = \frac{p}{3u}, \qquad v = \left\{ \begin{array}{l} \dfrac{p}{3\sqrt[3]{w_1}} \\ \textit{ou} \\ \dfrac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{2\pi}{3}} \\ \textit{ou} \\ \dfrac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{4\pi}{3}} \end{array} \right.$$

si bien que d'après les changements de variables successifs effectués,

$$\lambda = u - v + a/3 = \left\{ \begin{array}{l} \sqrt[3]{w_1} - \dfrac{p}{3\sqrt[3]{w_1}} + a/3 \\ \textit{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{2\pi}{3}} - \dfrac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{2\pi}{3}} + a/3 \\ \textit{ou} \\ \sqrt[3]{w_1}\, e^{i\frac{4\pi}{3}} - \dfrac{p}{3\sqrt[3]{w_1}}\, e^{-i\frac{4\pi}{3}} + a/3 \end{array} \right.$$

et,toutes simplifications faites, pour tout $a \in]-3;0[$, *l'expression des racines* λ_1, λ_2 *et* λ_3 *en fonction de* a,

$$\left\{ \begin{array}{lcl} \lambda_1 & = & R(a) + \dfrac{a(a+3)}{9R(a)} + \dfrac{a}{3} \\ \lambda_2 & = & -\dfrac{1}{2}\left(R(a) + \dfrac{a(a+3)}{9R(a)}\right) + i\dfrac{\sqrt{3}}{2}\left(R(a) - \dfrac{a(a+3)}{9R(a)}\right) + \dfrac{a}{3} = \alpha + i\omega \\ \lambda_3 & = & -\dfrac{1}{2}\left(R(a) + \dfrac{a(a+3)}{9R(a)}\right) - i\dfrac{\sqrt{3}}{2}\left(R(a) - \dfrac{a(a+3)}{9R(a)}\right) + \dfrac{a}{3} = \alpha - i\omega \end{array} \right. \tag{D.4}$$

avec

$$R(a) := \frac{\sqrt[3]{4a}}{6} \sqrt[3]{2a^2 + 9a + 27(1-\frac{1}{\eta}) + 3\sqrt{3}\sqrt{(3-\frac{4}{\eta})a^2 + 2(7-\frac{9}{\eta})a + 27(1-\frac{1}{\eta})^2}},$$

Le problème de singularité rencontré dans la section précédente lors de l'étude des points $P_{\pm 1}$ en $a = -3$, n'a plus lieu d'être vu que $R(a)$ ne s'annule pas en $a = -3$. Donc, dans le cas où $a \in]-3\,;\,0[$, le spectre de A est composé d'une racine réelle λ_1 et deux racines complexes conjuguées λ_2 et λ_3.

□

ANNEXE E

PREUVE DU THÉORÈME III.3

1. Remarquons tout d'abord en utilisant l'inégalité de Cauchy-Schwartz que

$$\begin{aligned} |\xi(t_1)|^2 &= \left| \int_D R(t_1,t_2)\Phi(t_2)\,dt_2 \right|^2 \\ &\leq \int_D |R(t_1,t_2)|^2\,dt_2 \int_D |\Phi(t)|^2\,dt. \end{aligned}$$

La première intégrale du membre droit de cette inégalité existe en raison du théorème de Fubini appliqué à la relation III.8. Il en est de même pour la seconde puisque par hypothèse $\Phi(t_2) \in L^2(D)$.
En intégrant membre à membre l'inégalité selon t_1, il vient

$$\int_D |\xi(t_1)|^2\,dt_1 \leq \int\int_{D^2} |R(t_1,t_2)|^2\,dt_1 dt_2 \int_D |\Phi(t)|^2\,dt \tag{E.1}$$

D'après l'inégalité III.8 , l'intégrabilité de $|\xi(t_1)|^2$ est assurée et par conséquent $\xi(t_1) \in L^2(D)$.

2. La norme de l'opérateur A est

$$\|A\| := \sup_{\|\phi(t)\|\neq 0} \frac{\|A\Phi(t)\|_{L^2(D)}}{\|\Phi(t)\|_{L^2(D)}}$$

Or, des inégalités III.8 et E.1 il vient

$$\|A\Phi(t)\|^2_{L^2(D)} = \int_D |\xi(t_1)|^2\,dt_1 \leq \|\Phi(t)\|^2_{L^2(D)}\,\mu(D^2)\sigma_S^4$$

Ce qui donne, après mise à la racine carrée de part et d'autre de l'inégalité

$$\|A\| \leq \sqrt{\int\int_{D^2} |R(t_1,t_2)|^2\,dt_1 dt_2} \leq \mu(D)\sigma_S^2.$$

3. La propriété de linéarité de l'intégrale fait que pour toute fonction $\Phi_1(t)$ et $\Phi_2(t)$ toute deux dans $L^2(D)$ et pour tout couple $(\alpha,\beta) \in \mathbb{R}^2$

$$\begin{aligned} A\left[\alpha\Phi_1(t_1) + \beta\Phi_2(t_1)\right] &= \int_D R(t_1,t_2)(\alpha\Phi_1(t2) + \beta\Phi_2(t2))\,dt_2 \\ &= \alpha\int_D R(t_1,t_2)\Phi_1(t_2)\,dt_2 + \alpha\int_D R(t_1,t_2)\Phi_2(t_2)\,dt_2 \\ &= \alpha A\Phi_1(t_1) + \beta A\Phi_2(t_1) \end{aligned}$$

ce qui démontre que l'opérateur A est linéaire.

4. Montrons que A peut être vu comme la limite d'une suite d'opérateurs compacts $\{A_N\}_{N\in\mathbb{N}}$. $R(t_1,t_2)$ est un noyau de Hilbert-Schmidt, donc décomposable sur une base Hilbertienne de fonctions de $L^2(D^2)$. Soit la base Hilbertienne de $L^2(D)$ constituée de la famille de fonctions $\{\eta_n(t_1)\}_{n\in\mathbb{N}}$, alors la famille $\{\eta_n(t_1)\eta_m(t_2)\}_{(n,m)\in\mathbb{N}^2}$ est une base Hilbertienne de $L^2(D^2)$. Il est alors possible de décomposer le noyau $R(t_1,t_2)$ sur cette base :

$$R(t_1,t_2)=\sum_{n=1}^{\infty}\sum_{m=1}^{\infty}a_{nm}\eta_n(t_1)\eta_m(t_2)$$

où a_{nm} est la projection orthogonale de $R(t_1,t_2)$ sur la base engendrée par la famille de fonctions $\{\eta_n(t_1)\eta_m(t_2)\}_{(n,m)\in\mathbb{N}^2}$. Considérons la somme partielle associée à cette décomposition :

$$R_N(t_1,t_2):=\sum_{n=1}^{N}\sum_{m=1}^{N}a_{nm}\eta_n(t_1)\eta_m(t_2)$$

et définissons l'opérateur A_N qui a toute fonction $\Phi(t_1)\in L^2(D)$ associe $\xi(t_1)\in L^2(D)$ par

$$\Big[A_N\Phi(t_1)=\xi(t_1)\Big]\Leftrightarrow\Big[\int_D R_N(t_1,t_2)\Phi(t_2)\,dt_2=\xi(t_1)\Big]$$

Explicitons $\xi(t_1)$,

$$\begin{aligned}
\xi(t_1) &= \int_D R_N(t_1,t_2)\Phi(t_2)\,dt_2\\
&= \sum_{n=1}^{N}\sum_{m=1}^{N}a_{nm}\eta_n(t_1)\underbrace{\int_D\eta_m(t_2)\Phi(t_2)\,dt_2}_{=b_m}\\
&= \sum_{n=1}^{N}\eta_n(t_1)\underbrace{\sum_{m=1}^{N}a_{nm}b_m}_{=c_n}\\
\xi(t_1) &= \sum_{n=1}^{N}c_n\eta_n(t_1)
\end{aligned}$$

Autrement dit, l'opérateur A_N associe à toute fonction $\Phi(t_1)\in L^2(D)$ une fonction $\xi(t_1)$ à valeur dans le sous-espace de $L^2(D)$ de dimension finie engendré par les N fonctions $\{\eta_n(t_1)\}_{n=1\ldots N}$. L'opérateur A_N est donc compact.
Par ailleurs, $R_N(t_1,t_2)$ étant la somme partielle associée à la décomposition de $R(t_1,t_2)$,

$$\lim_{N\to\infty}\|R(t_1,t_2)-R_N(t_1,t_2)\|=\lim_{N\to\infty}\int\int_{D^2}|R(t_1,t_2)-R_N(t_1,t_2)|^2\,dt_1dt_2=0.$$

A partir de ce résultat et en considérant l'opérateur $A-A_N$ en lieu et place de A dans l'inégalité III.9, il vient

$$\lim_{N\to\infty}\|A-A_N\|=0,$$

ce qui prouve que A est la limite d'une suite convergente d'opérateurs compacts A_N. Or, d'après [Kol94] (pp. 234), la limite d'une suite convergente d'opérateurs compact est un opérateur compact, donc A est un opérateur compact.

5. Pour démontrer cette assertion, il est nécessaire d'étendre la définition du produit scalaire ainsi que les domaines d'arrivée respectifs des fonctions $\Phi_1(t)$, $\Phi_2(t)$ et $R(t_1,t_2)$ au champs des complexes, de conférer au noyau une symétrie hermitienne, $R(t_2,t_1) = \overline{R(t_1,t_2)}$.
Soit A^* l'opérateur adjoint de A pour le produit scalaire usuel de $L^2(\mathbb{C})$ défini par

$$\langle A\Phi_1(t_1), \Phi_2(t_1)\rangle = \langle \Phi_1(t_1), A^*\Phi_2(t_1)\rangle .$$

En utilisant le théorème de Fubini, explicitons A^* :

$$\begin{aligned}
\langle A\Phi_1(t_1), \Phi_2(t_1)\rangle &= \int_D \left(\int_D R(t_1,t_2)\Phi_1(t_2)\, dt_2 \right) \overline{\Phi_2(t_1)}\, dt_1 \\
&= \int\int_{D^2} R(t_1,t_2)\Phi_1(t_2)\overline{\Phi_2(t_1)}\, dt_1 dt_2
\end{aligned}$$

par permutation des variables t_1 et t_2 l'égalité se transforme en

$$\begin{aligned}
&= \int\int_{D^2} R(t_2,t_1)\Phi_1(t_1)\overline{\Phi_2(t_2)}\, dt_2 dt_1 \\
&= \int_D \Phi_1(t_1) \left(\int_D R(t_2,t_1)\overline{\Phi_2(t_2)}\, dt_2 \right) dt_1 \\
&= \int_D \Phi_1(t_1) \left(\overline{\int_D \overline{R(t_2,t_1)}\Phi_2(t_2)\, dt_2} \right) dt_1 \\
\langle A\Phi_1(t_1), \Phi_2(t_1)\rangle &= \langle \Phi_1(t_1), A^*\Phi_2(t_1)\rangle
\end{aligned}$$

Donc, si $R(t_1,t_2)$ est le noyau de l'opérateur A , alors $\overline{R(t_2,t_1)}$ est le noyau de l'opérateur A^*, adjoint de A.
Ce résultat permet d'affirmer que A est autoadjoint dans $L^2(D)$ si et seulement si $R(t_1,t_2)$ est hermitien, symétrique dans le cas réel. Or, par définition de $R(t_1,t_2)$, ce dernier est réel et symétrique, donc l'opérateur A défini par le noyau $R(t_1,t_2)$ est autoadjoint dans $L^2(D)$.

ANNEXE F

PREUVE DE LA PROPOSITION III.4

1. Le calcul de la covariance des variables aléatoires $\mathbf{s}_n$ et $\mathbf{s}_m$, où n et m sont deux entiers distincts s'écrit, en utilisant le théorème de Fubini pour réarranger l'ordre des intégrales,

$$\begin{aligned}\mathbb{E}\left[\mathbf{s}_n\mathbf{s}_m\right] &= \mathbb{E}\left[\left(\int_D \mathbf{S}(t_1)\Phi_n(t_1)\,dt_1\right)\left(\int_D \mathbf{S}(t_2)\Phi_m(t_2)\,dt_2\right)\right] \\ &= \int\int_{D^2} R(t_1,t_2)\Phi_n(t_1)\Phi_m(t_2)\,dt_1dt_2 \\ &= \int_D\left(\int_D R(t_1,t_2)\Phi_m(t_2)\,dt_2\right)\Phi_n(t_1)\,dt_1.\end{aligned}$$

   Or, l'expression entre parenthèses vérifie III.16, donc par substitution

$$\begin{aligned}\mathbb{E}\left[\mathbf{s}_n\mathbf{s}_m\right] &= \int_D\left(\lambda_m\Phi_m(t_1)\right)\Phi_n(t_1)\,dt_1 \\ &= \lambda_m\int_D \Phi_m(t_1)\Phi_n(t_1)\,dt_1.\end{aligned}$$

   La famille de fonctions $\{\Phi_n(t)\}_{\mathbb{N}}$ étant constituée d'éléments deux-à-deux orthogonaux d'après la remarque 3.5,

$$\begin{aligned}\mathbb{E}\left[\mathbf{s}_n\mathbf{s}_m\right] &= \lambda_n\delta[n-m] \\ &= \mathbb{E}\left[\mathbf{s}_n^2\right]\delta[n-m].\end{aligned}$$

2. Évaluons la moyenne quadratique entre $\mathbf{S}(t)$ et la série $\sum_{n=1}^{\infty}\mathbf{s}_n\Phi_n(t) = \lim_{N\to\infty}\tilde{S}_N(t)$. Les signaux sont réels, il n'est pas nécessaire de faire apparaître de valeur conjuguée dans les calculs,

$$\begin{aligned}\mathbb{E}\left[\left|\mathbf{S}(t_1)-\sum_{n=1}^{\infty}\mathbf{s}_n\Phi_n(t_1)\right|^2\right] &= \mathbb{E}\left[\mathbf{S}(t)^2 - 2\sum_{n=1}^{\infty}\mathbf{s}_nS(t_1)\Phi_n(t_1) + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\mathbf{s}_n\mathbf{s}_m\Phi_n(t_1)\Phi_m(t_1)\right] \\ &= \mathbb{E}\left[\mathbf{S}(t)^2\right] - 2\sum_{n=1}^{\infty}\mathbb{E}\left[\mathbf{s}_n\mathbf{S}(t_1)\right]\Phi_n(t_1) \\ &\quad + \sum_{n=1}^{\infty}\sum_{m=1}^{\infty}\mathbb{E}\left[\mathbf{s}_n\mathbf{s}_m\right]\Phi_n(t_1)\Phi_m(t_1). \qquad \text{(F.1)}\end{aligned}$$

Or, d'une part, en utilisant l'équation III.16,

$$\begin{aligned}\mathbb{E}\left[\mathbf{s}_n\mathbf{S}(t_1)\right] &= \mathbb{E}\left[\left(\int_D \mathbf{S}(t_2)\Phi_n(t_2)\,dt_2\right)\mathbf{S}(t_1)\right] \\ &= \int_D R(t_1,t_2)\Phi_m(t_2)\,dt_2 \\ &= \lambda_n\Phi_n(t_1) \end{aligned} \tag{F.2}$$

et d'autre part il vient d'être montré que

$$\mathbb{E}\left[\mathbf{s}_n\mathbf{s}_m\right] = \lambda_n\delta[n-m]. \tag{F.3}$$

Alors, en injectant F.2 et F.3 dans F.1, et en regroupant les deux derniers termes, il vient

$$\mathbb{E}\left[\left|\mathbf{S}(t_1)-\sum_{n=1}^{\infty}\mathbf{s}_n\Phi_n(t_1)\right|^2\right] = \mathbb{E}\left[\mathbf{S}(t_1)^2\right]-\sum_{n=1}^{\infty}\lambda_n\left(\Phi_n(t_1)\right)^2.$$

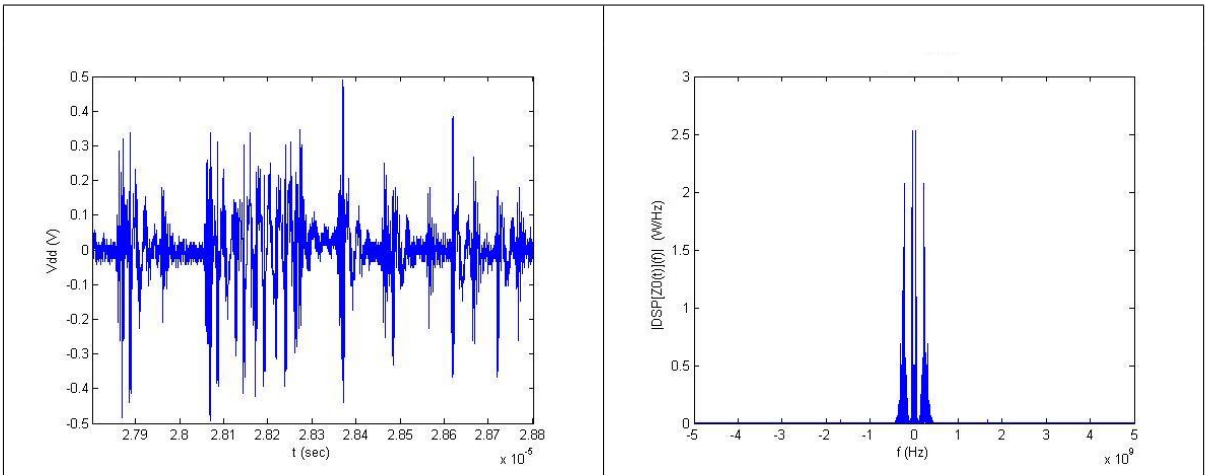
Par la relation de fermeture III.12 conséquence du théorème de Mercer , nous avons

$$\begin{aligned}\mathbb{E}\left[\left|S(t_1)-\sum_{n=1}^{\infty}\mathbf{s}_n\Phi_n(t_1)\right|^2\right] &= \mathbb{E}\left[S(t_1)^2\right]-R(t_1,t_1) \\ &= \sigma_S^2-\sigma_S^2=0.\end{aligned}$$

ANNEXE G

EXEMPLE DE RE-ÉCHANTILLONNAGE D'UNE SIGNATURE

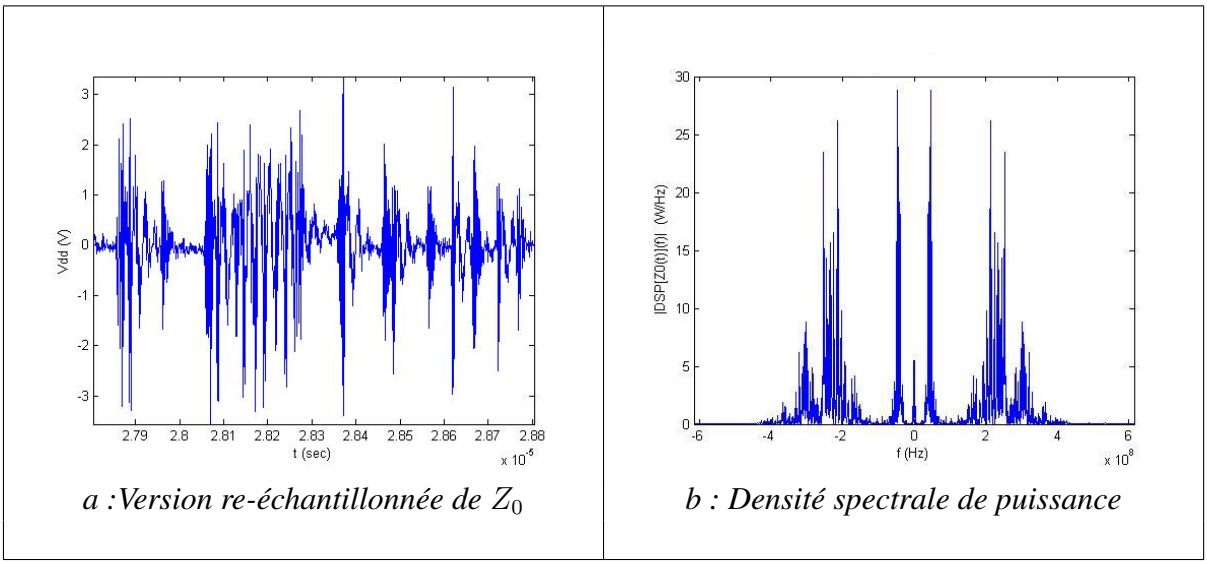
Afin d'illustrer le fonctionnement de la technique de sous-échantillonnage proposée, cette dernière a été appliquée à la signature Z_0. La figure 1 montre la représentation graphique de Z_0 ainsi que sa densité spectrale de puissance, laissant apparaître une faible occupation spectrale. ce signal fait office de bon candidat au re-échantillonnage.



a : Représentation graphique de Z_0 *b : Densité spectrale de puissance de* Z_0

FIG. 1 – Z_0 *sur* 10002 *points (a), accompagné du module de sa densité spectrale de puissance (b)*

L'application de la technique conduit à $f_c = 615\,MHz$. Le signal re-échantillonné ainsi que sa densité spectrale de puissance sont représentés graphiquement sur la figure 2, il ressort que l'occupation spectrale est optimisée d'une part et que le signal sous-échantillonné, temporellement observé n'est pas altéré d'autre part.



a :Version re-échantillonnée de Z_0

b : Densité spectrale de puissance

FIG. 2 – *Représentation graphique de la version re-échantillonnée de Z_0 sur 1231 points (a), accompagnée du module de sa densité spectrale de puissance (b)*

Là où Z_0 est une observation faite de 10002 points, son pendant sous-échantillonné n'en est fait que de 1231, le tout à quantité d'information égale.
Une fois l'ensemble des signaux re-échantillonné, ils vont être confrontés aux déclinaisons de la technique de masquage proposée.

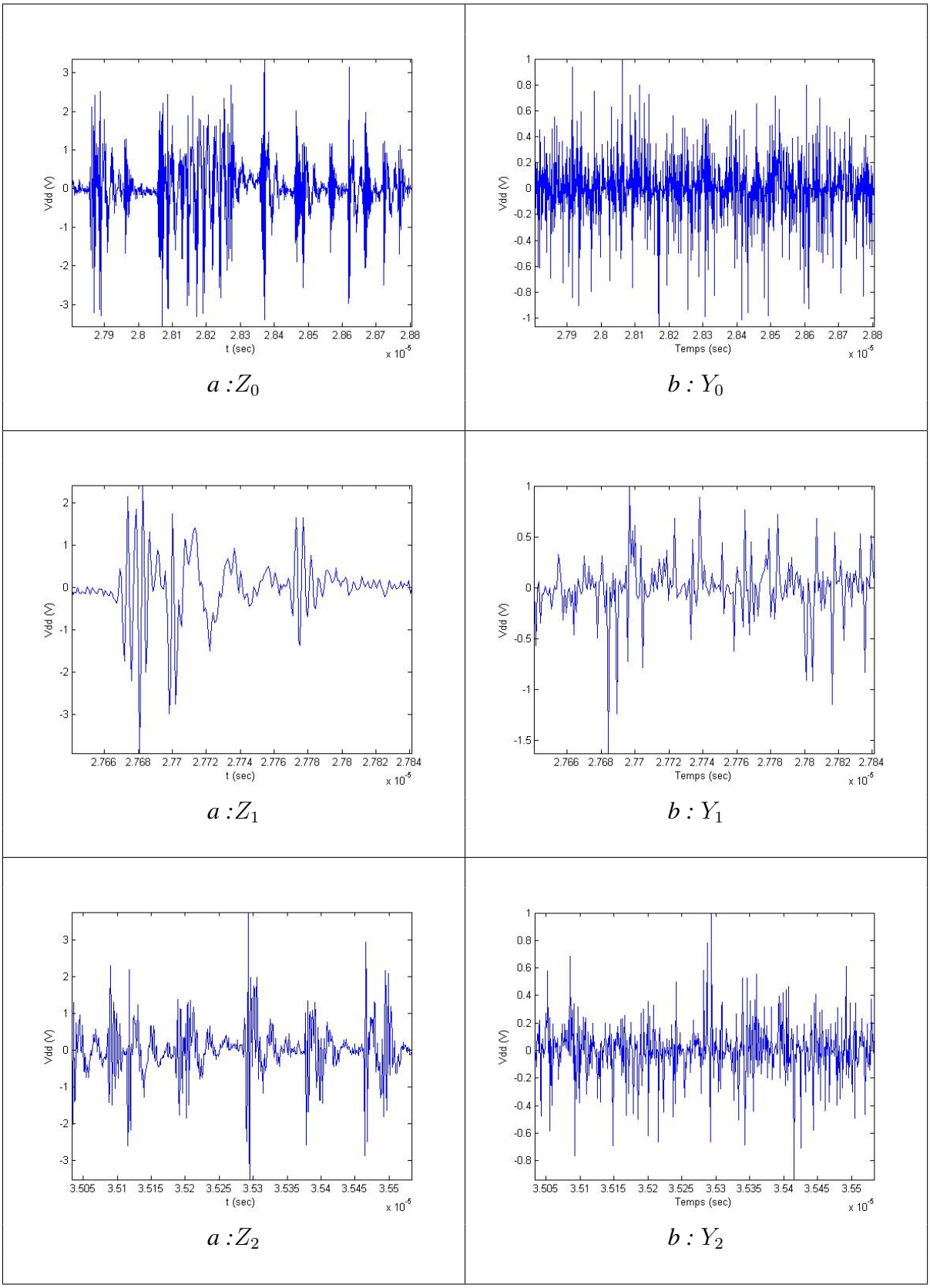
ANNEXE H

MASQUAGE DE SIGNATURES RÉELLES DE COURANT PAR DÉCOMPOSITION DES SIGNAUX.

L'annexe présente les résultats du masquage des signatures Z_0 à Z_{10} de la section 6 du chapitre *III*, pour les cinq déclinaisons de la technique de masquage par décomposition des signaux :

- Permutation pseudo aléatoire.
- Base connue.
- Matrice de variance covariance estimée empiriquement.
- Matrice de variance covariance estimée par paramètre manuellement.
- Matrice de variance covariance estimée par paramètre automatiquement.

1 PERMUTATION PSEUDO ALÉATOIRE

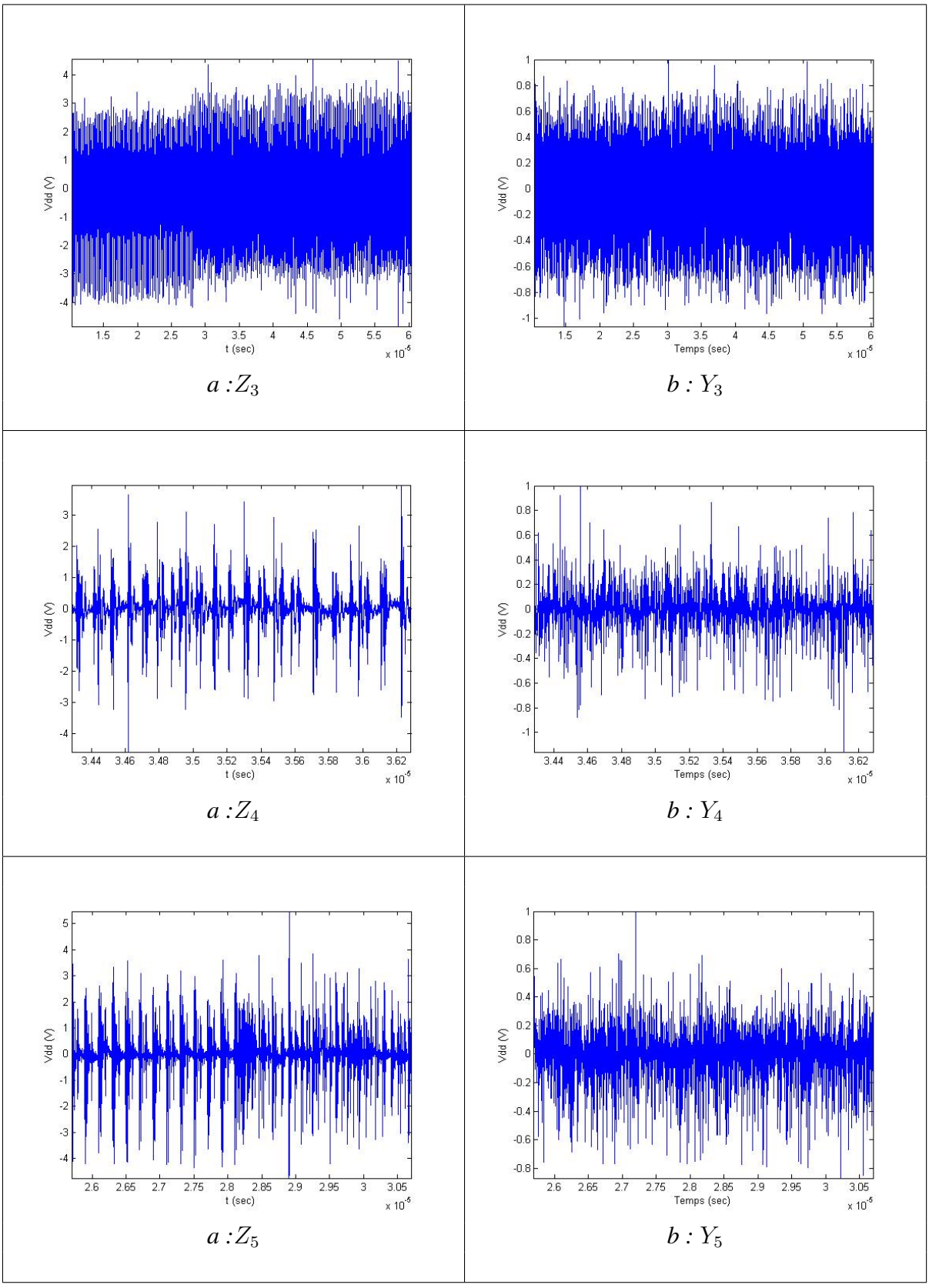


$a : Z_0$ $b : Y_0$

$a : Z_1$ $b : Y_1$

$a : Z_2$ $b : Y_2$

FIG. 1 – *Z_i (a) accompagnés de leurs Y_i respectifs (b), $i = 0 \ldots 2$*

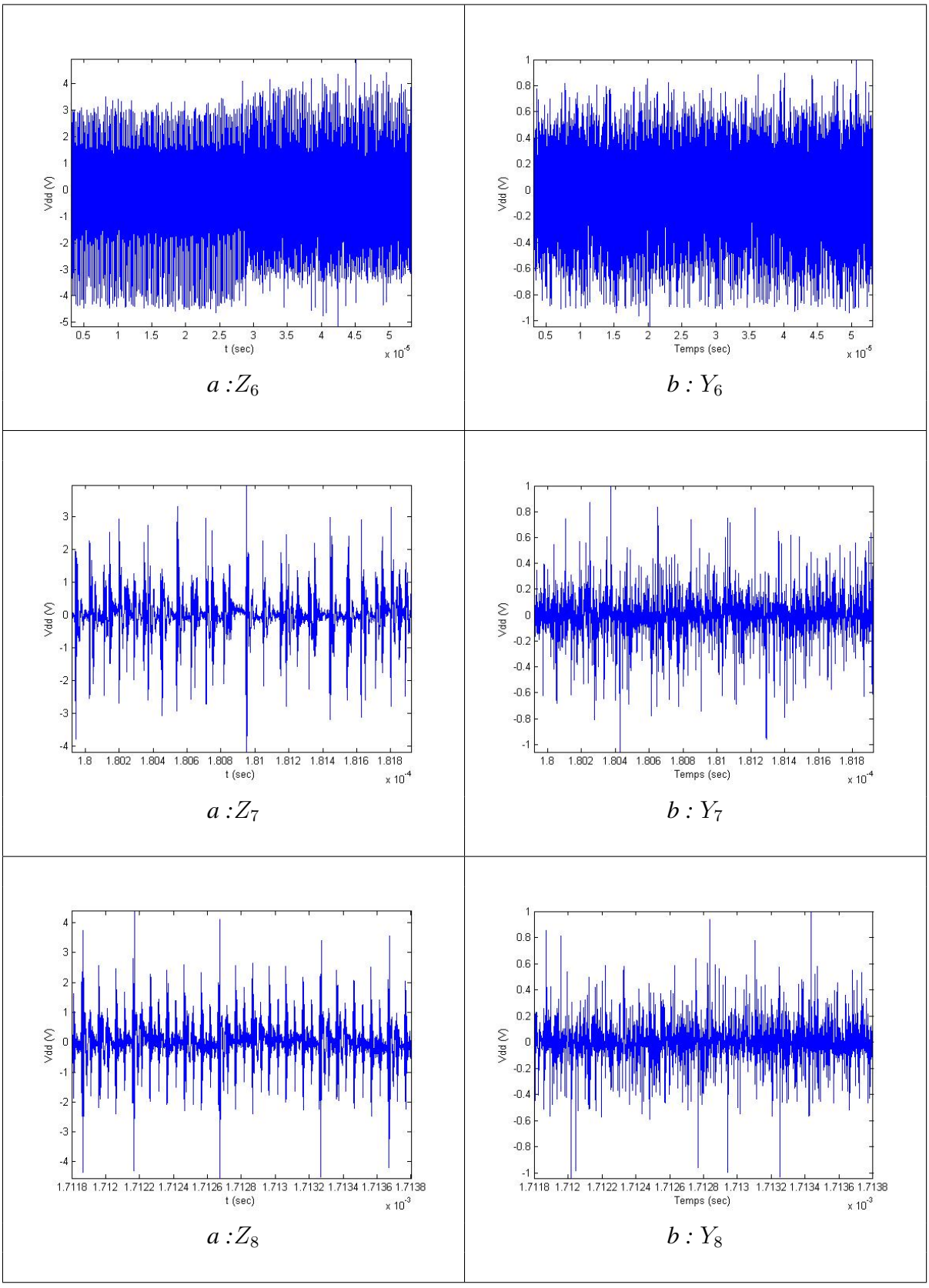


a : Z_3 *b* : Y_3

a : Z_4 *b* : Y_4

a : Z_5 *b* : Y_5

FIG. 2 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 3 \ldots 5$

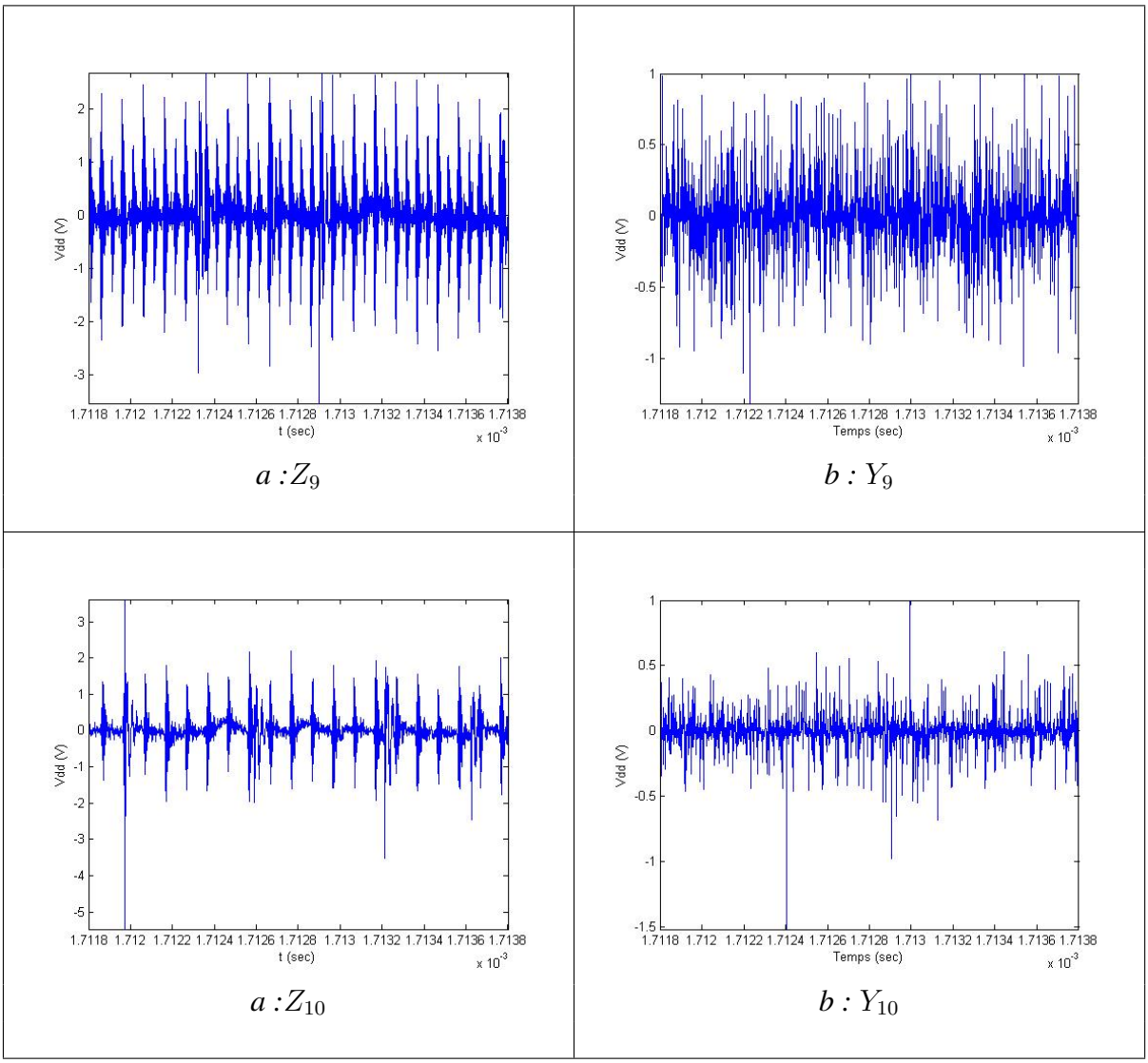


a : Z_6 *b* : Y_6

a : Z_7 *b* : Y_7

a : Z_8 *b* : Y_8

FIG. 3 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 6 \ldots 8$

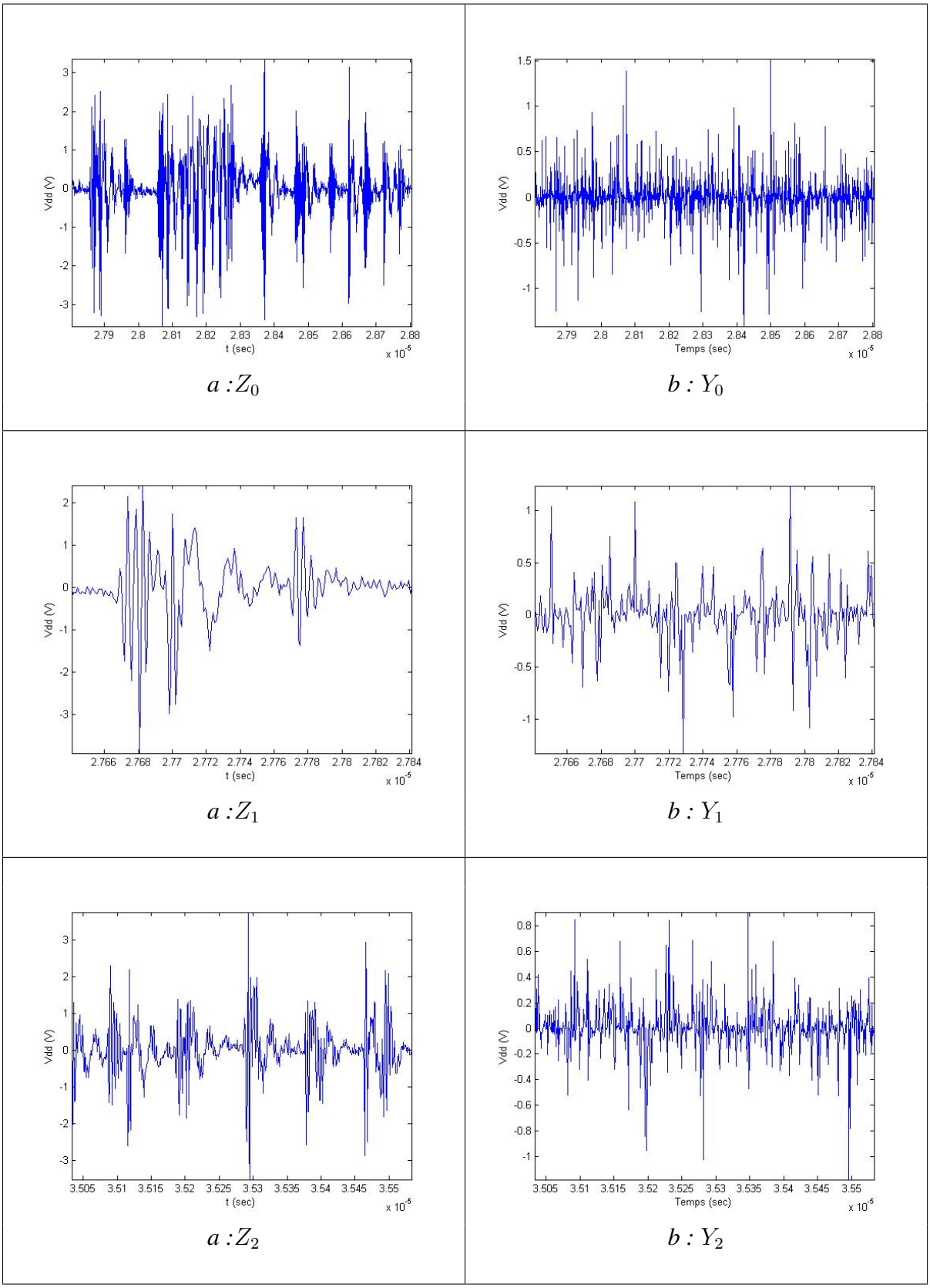


a : Z_9 *b* : Y_9

a : Z_{10} *b* : Y_{10}

FIG. 4 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 9 \ldots 10$

2 VECTEURS DE BASE CONNUS

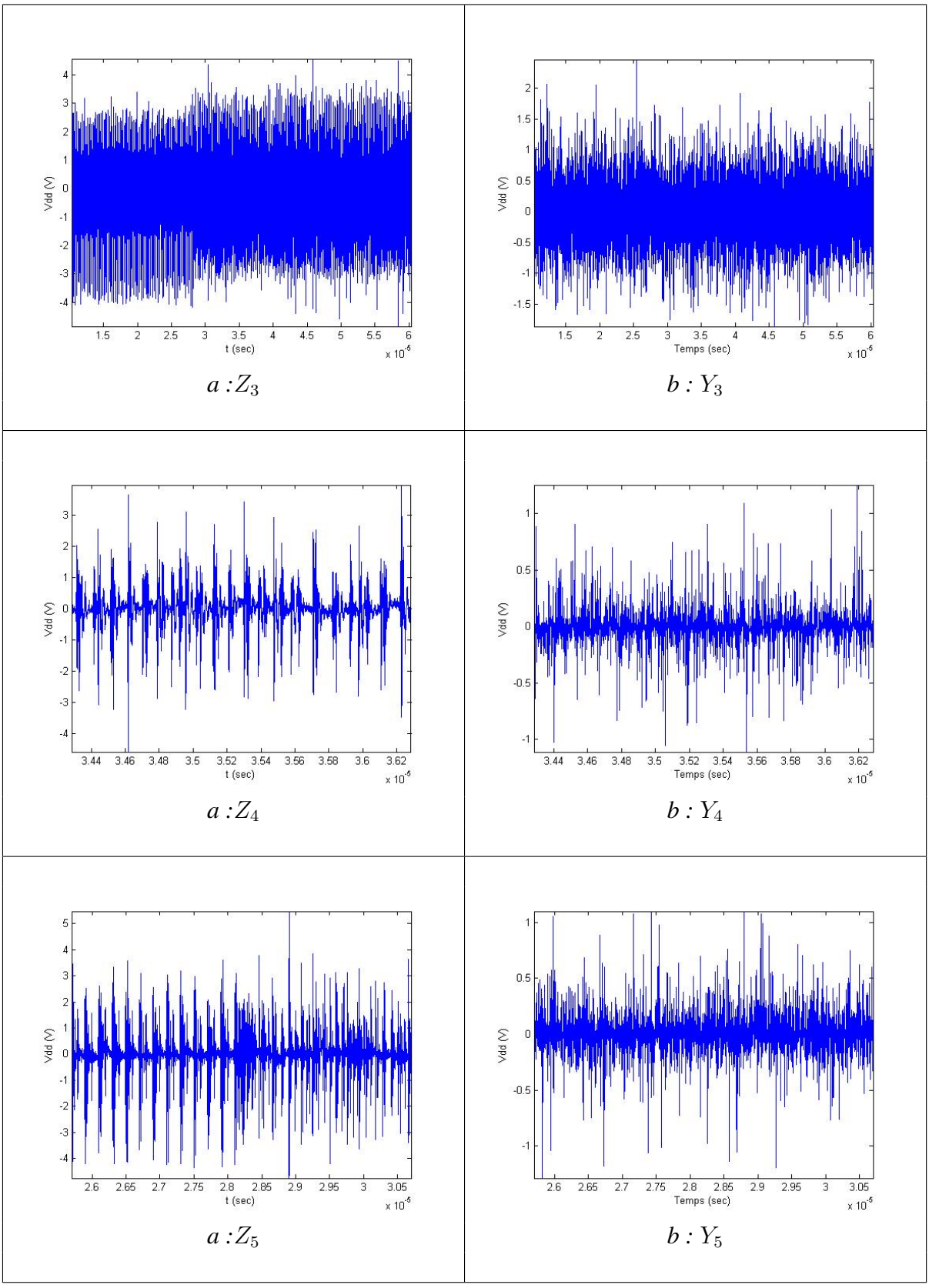


a : Z_0 *b* : Y_0

a : Z_1 *b* : Y_1

a : Z_2 *b* : Y_2

FIG. 5 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 0 \ldots 2$

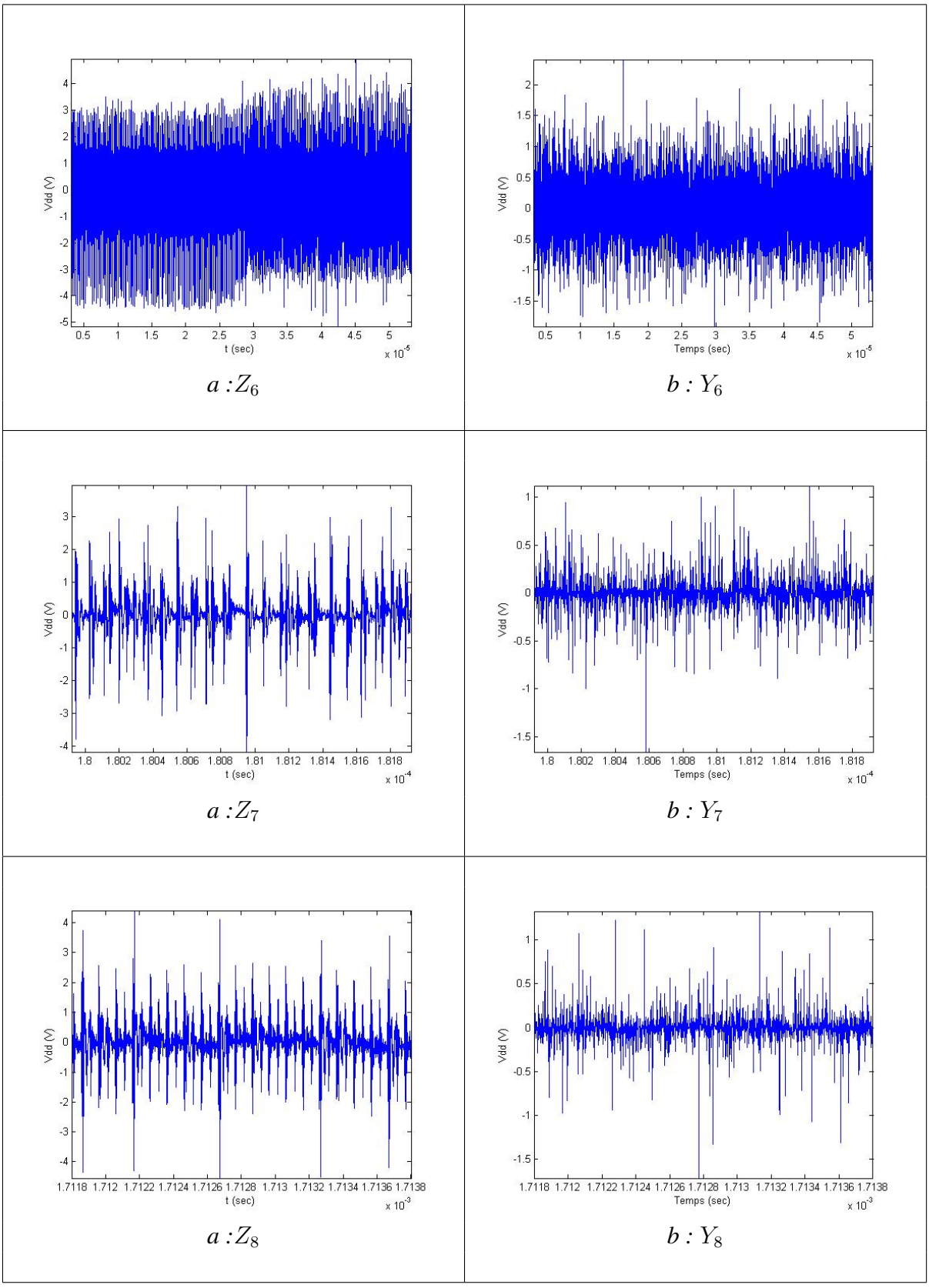


a : Z_3 *b* : Y_3

a : Z_4 *b* : Y_4

a : Z_5 *b* : Y_5

FIG. 6 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 3 \ldots 5$

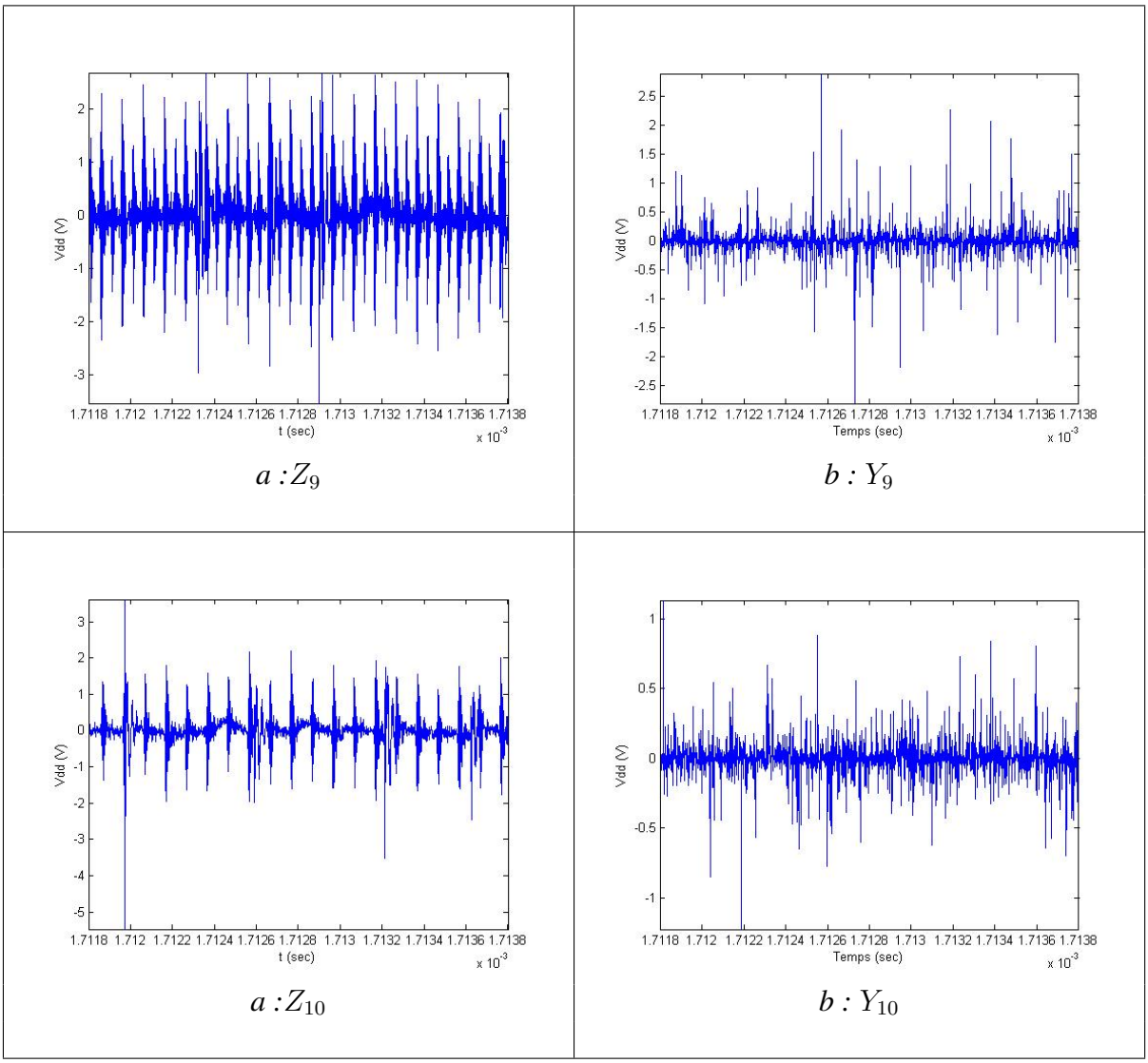


a : Z_6 *b* : Y_6

a : Z_7 *b* : Y_7

a : Z_8 *b* : Y_8

FIG. 7 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 6 \ldots 8$

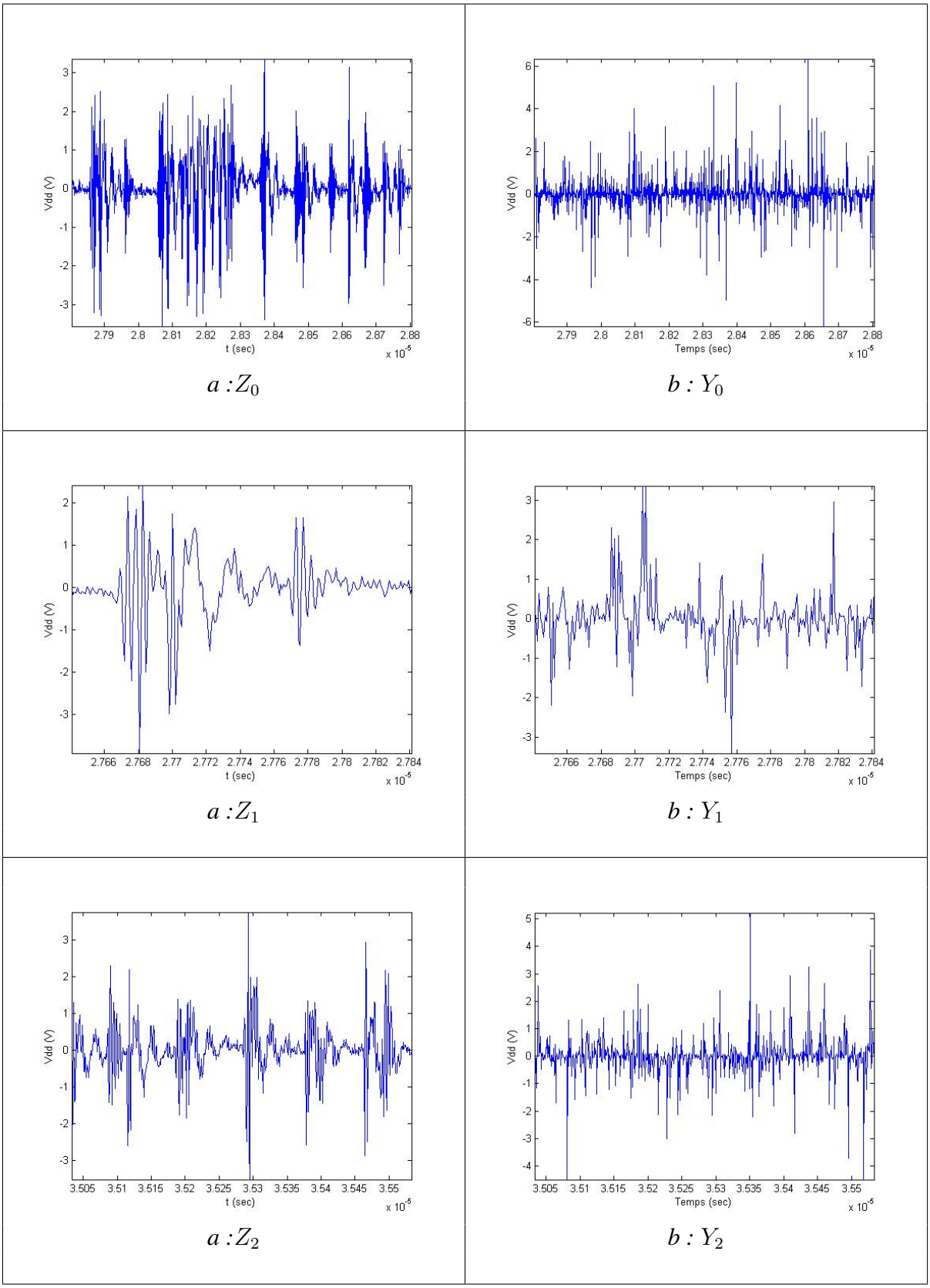


a : Z_9 *b* : Y_9

a : Z_{10} *b* : Y_{10}

FIG. 8 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 9 \ldots 10$

3 MATRICE DE VARIANCE COVARIANCE ESTIMÉE EMPIRIQUEMENT

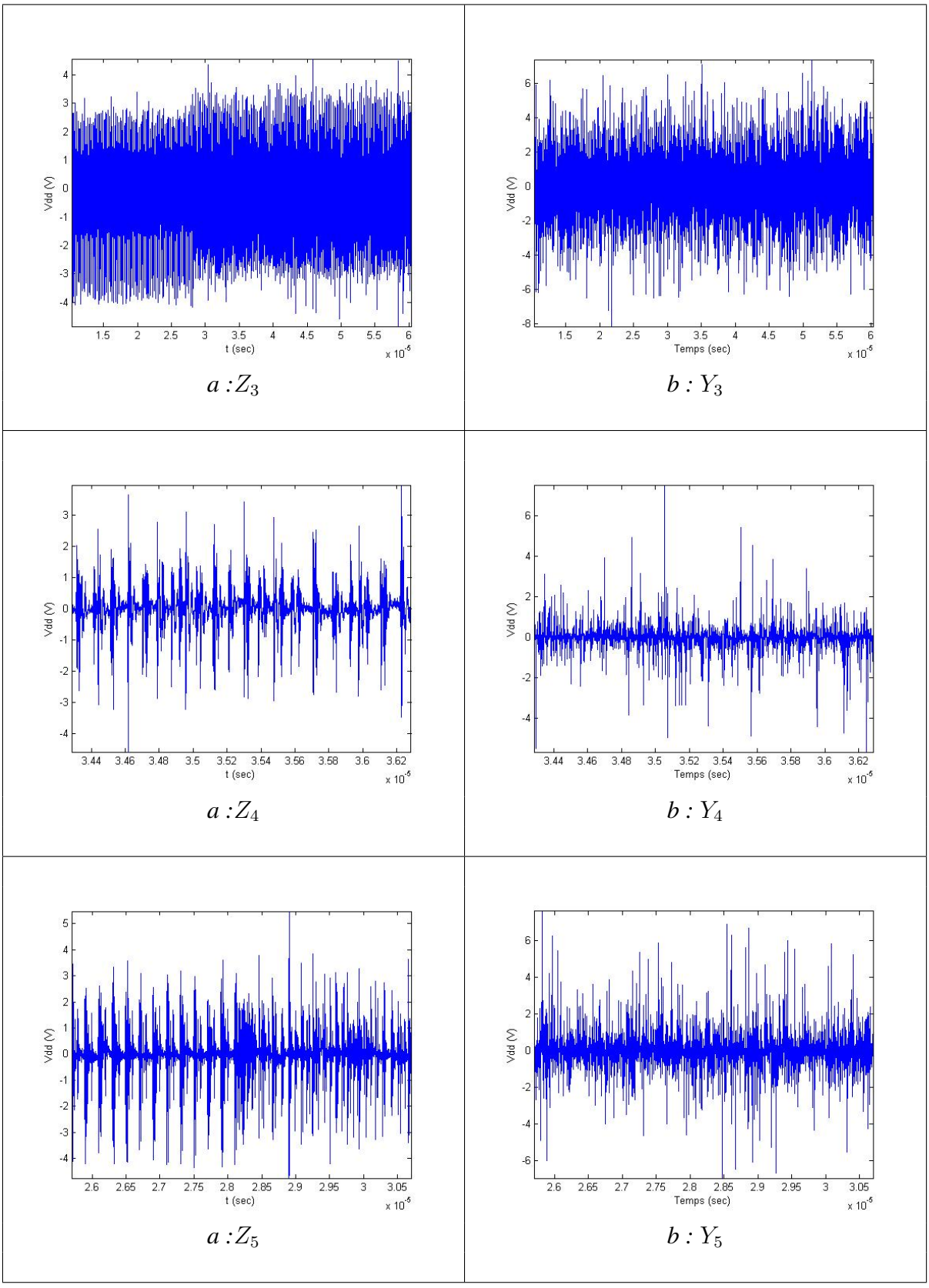


a : Z_0 *b* : Y_0

a : Z_1 *b* : Y_1

a : Z_2 *b* : Y_2

FIG. 9 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 0 \ldots 2$

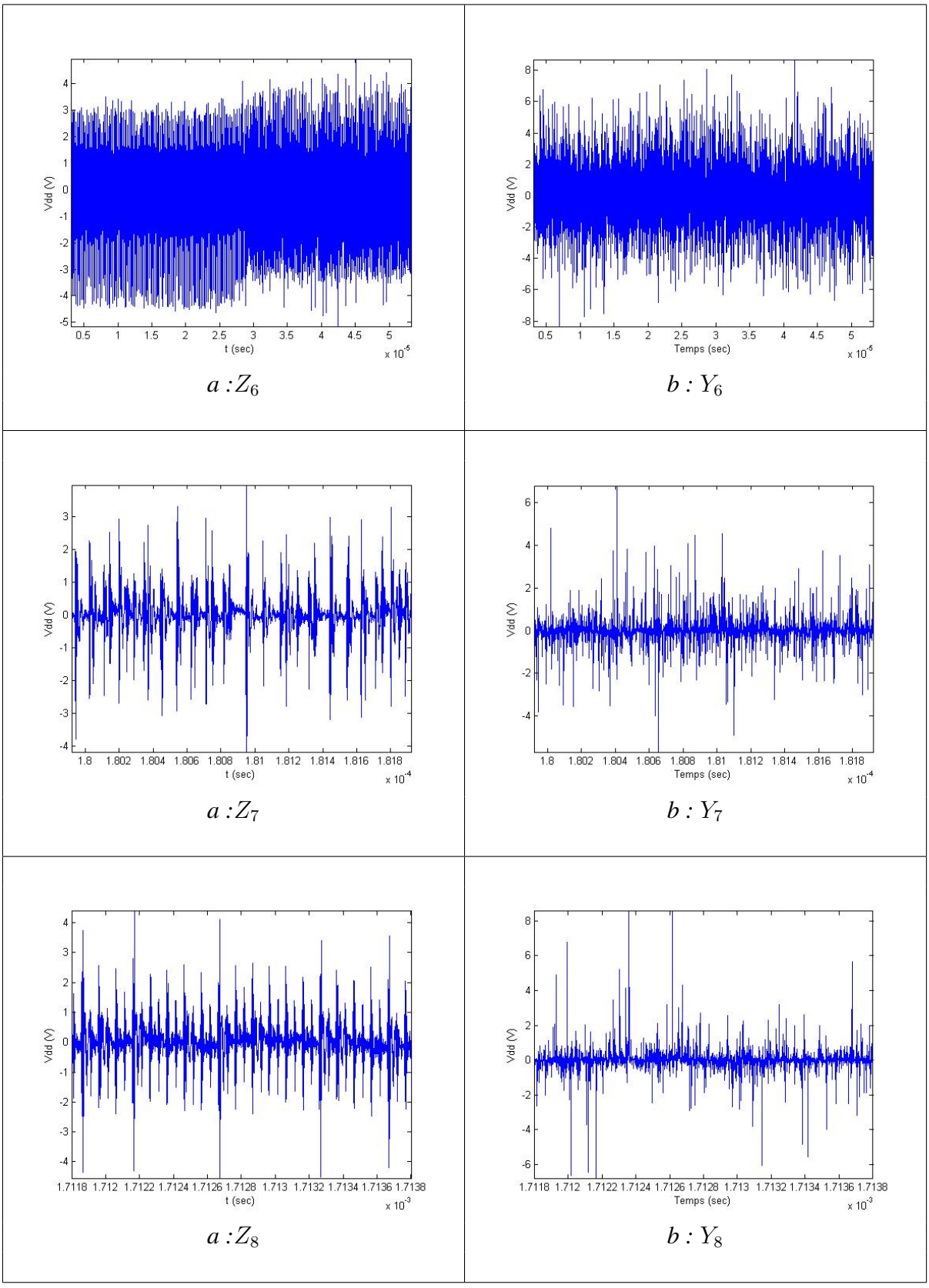


a : Z_3 *b* : Y_3

a : Z_4 *b* : Y_4

a : Z_5 *b* : Y_5

FIG. 10 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 3 \ldots 5$

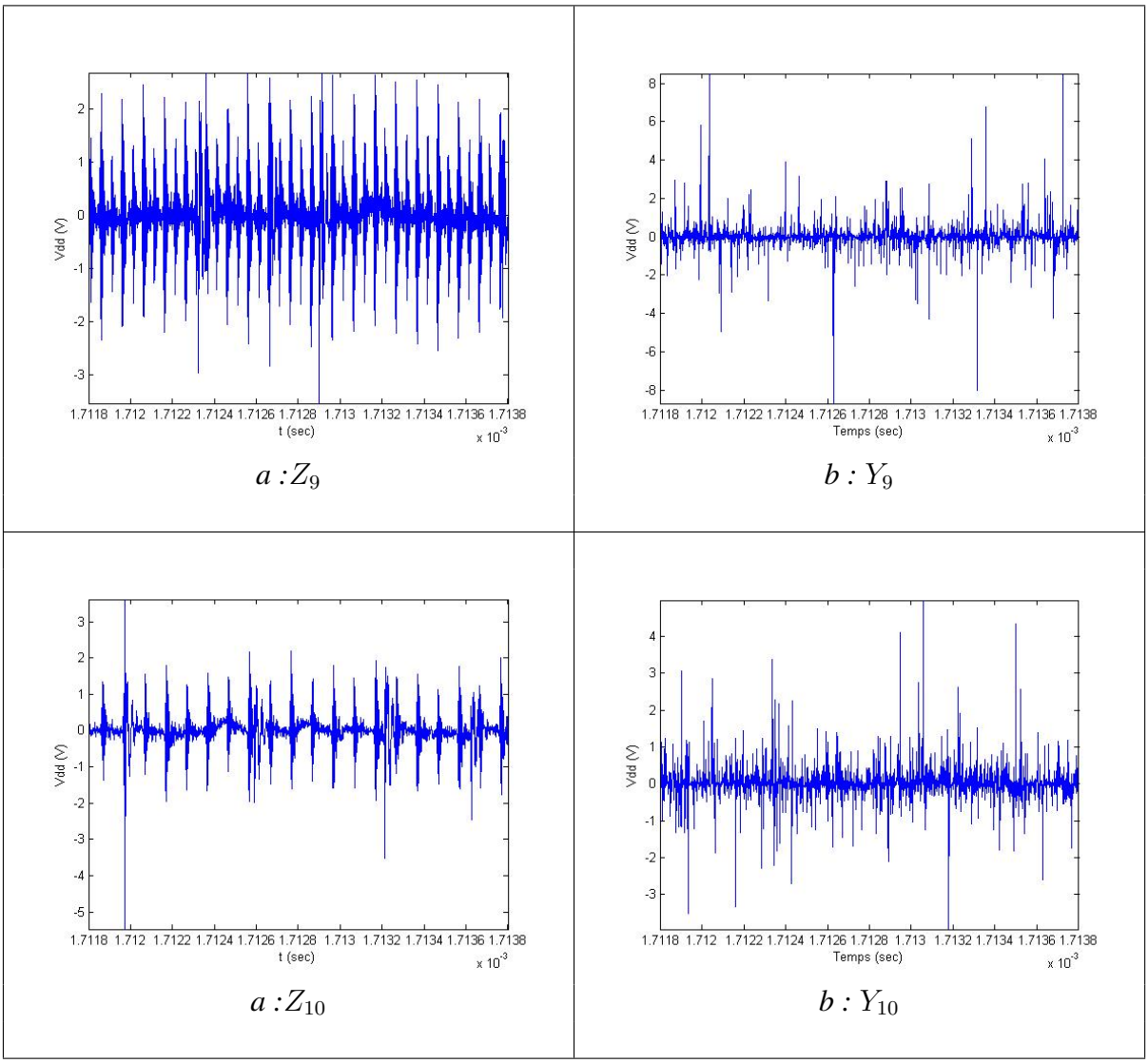


a : Z_6 *b* : Y_6

a : Z_7 *b* : Y_7

a : Z_8 *b* : Y_8

FIG. 11 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 6 \ldots 8$

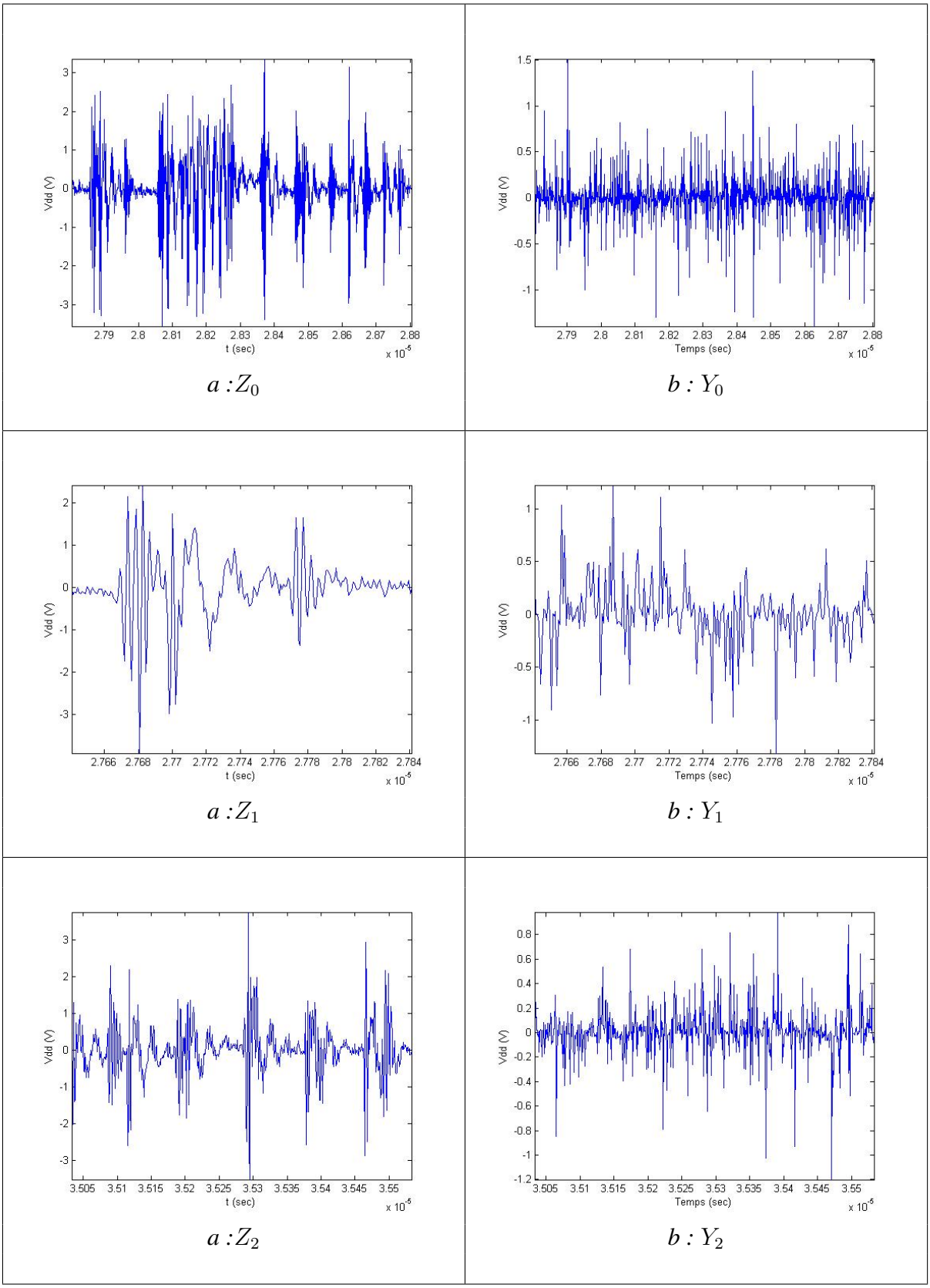


a : Z_9 *b* : Y_9

a : Z_{10} *b* : Y_{10}

FIG. 12 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 9 \ldots 10$

4 MATRICE DE VARIANCE COVARIANCE DÉPENDANT D'UN PARAMÈTRE ESTIMÉ MANUELLEMENT

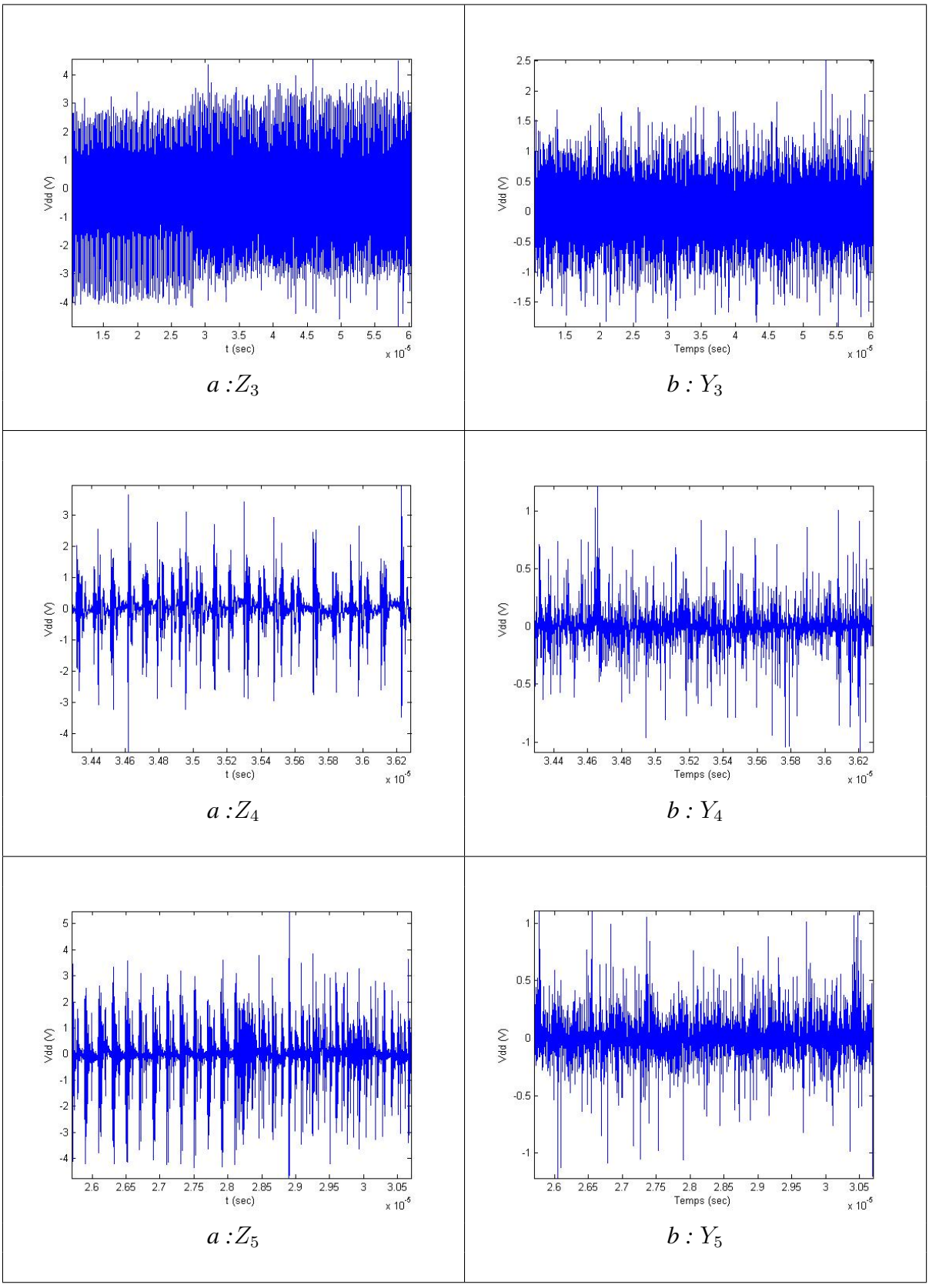


$a : Z_0$ $b : Y_0$

$a : Z_1$ $b : Y_1$

$a : Z_2$ $b : Y_2$

FIG. 13 – *Z_i (a) accompagnés de leurs Y_i respectifs (b), $i = 0 \ldots 2$*

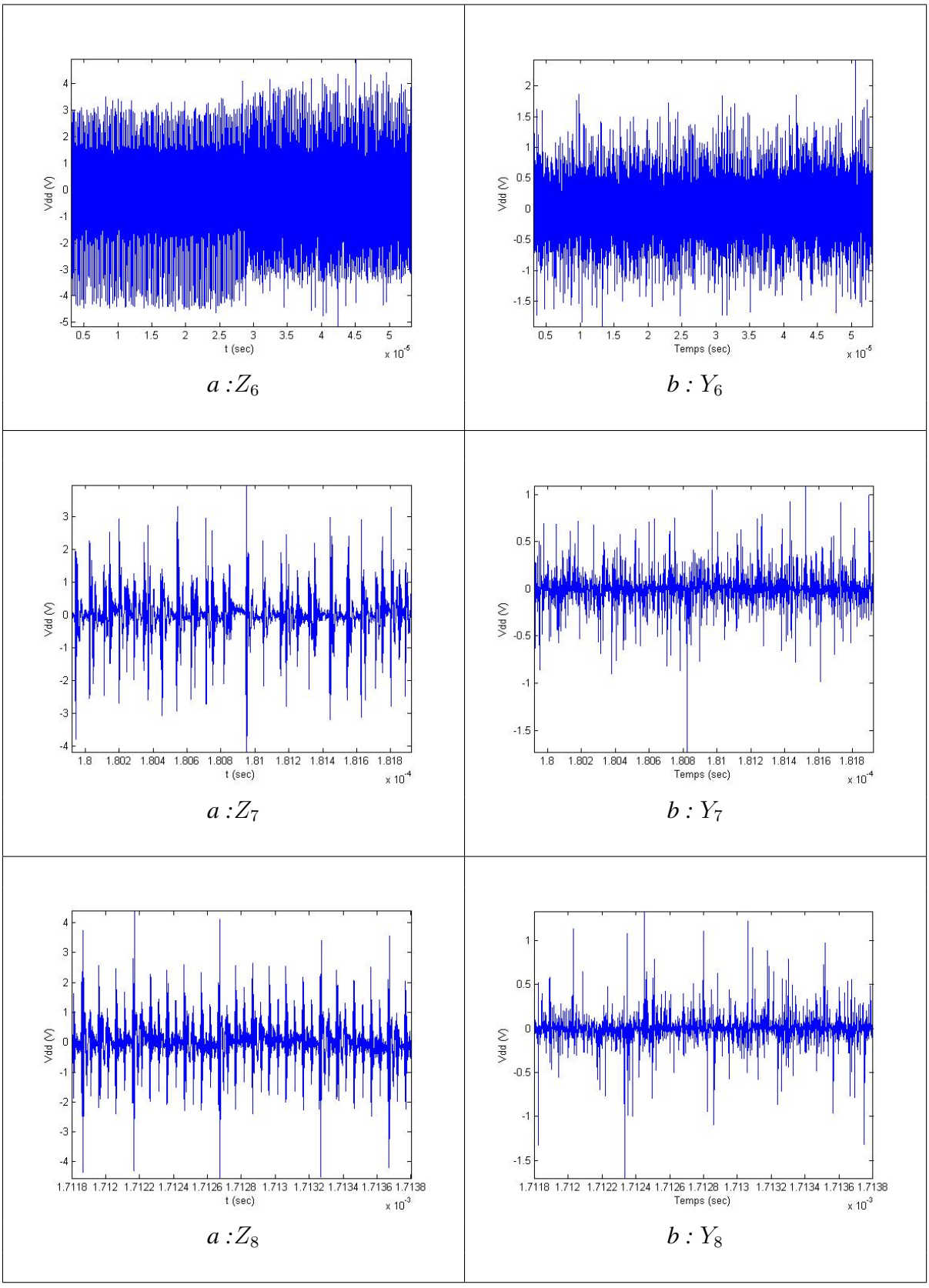


a : Z_3 *b* : Y_3

a : Z_4 *b* : Y_4

a : Z_5 *b* : Y_5

FIG. 14 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 3 \ldots 5$

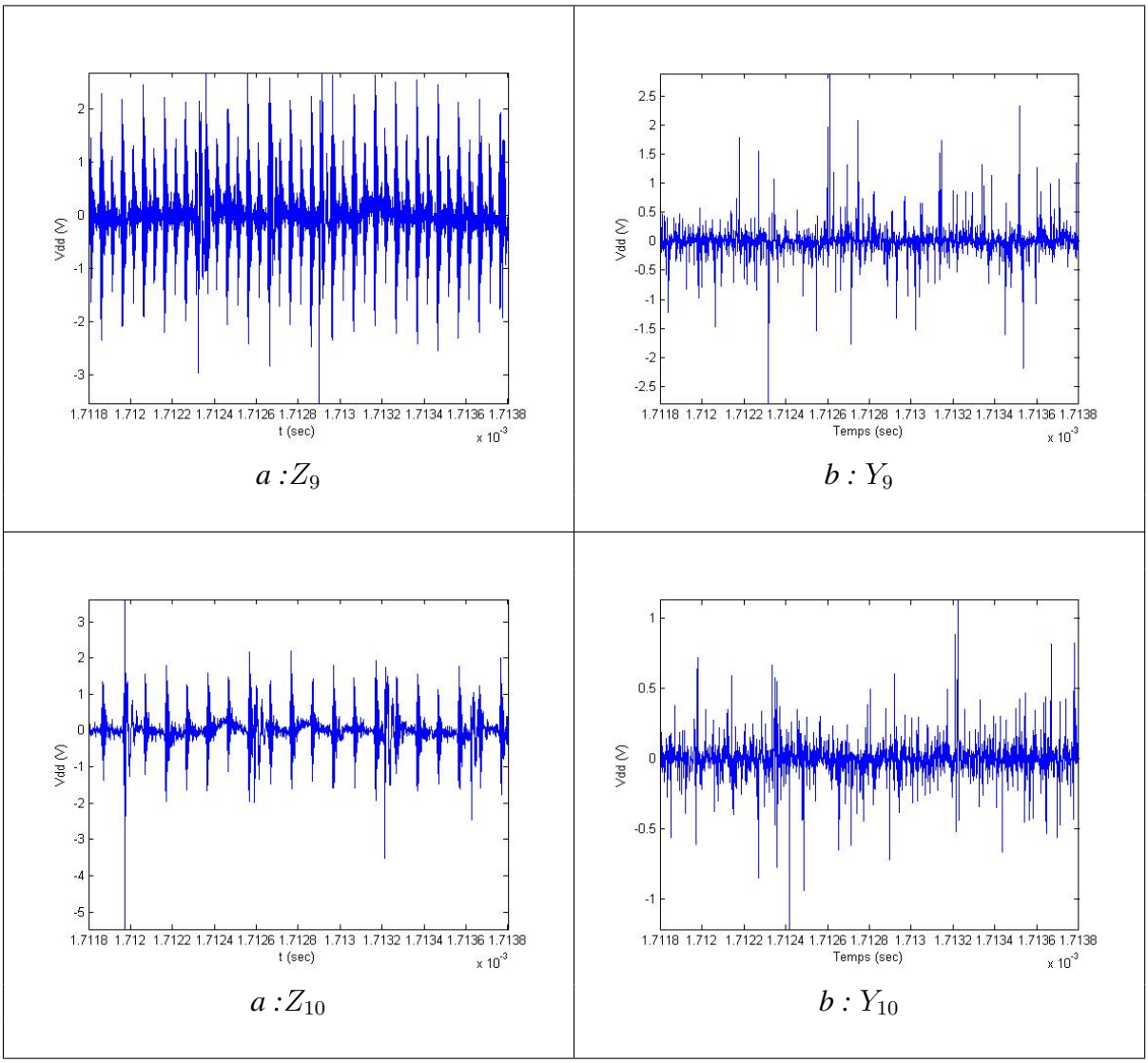


a : Z_6 *b* : Y_6

a : Z_7 *b* : Y_7

a : Z_8 *b* : Y_8

FIG. 15 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 6 \ldots 8$

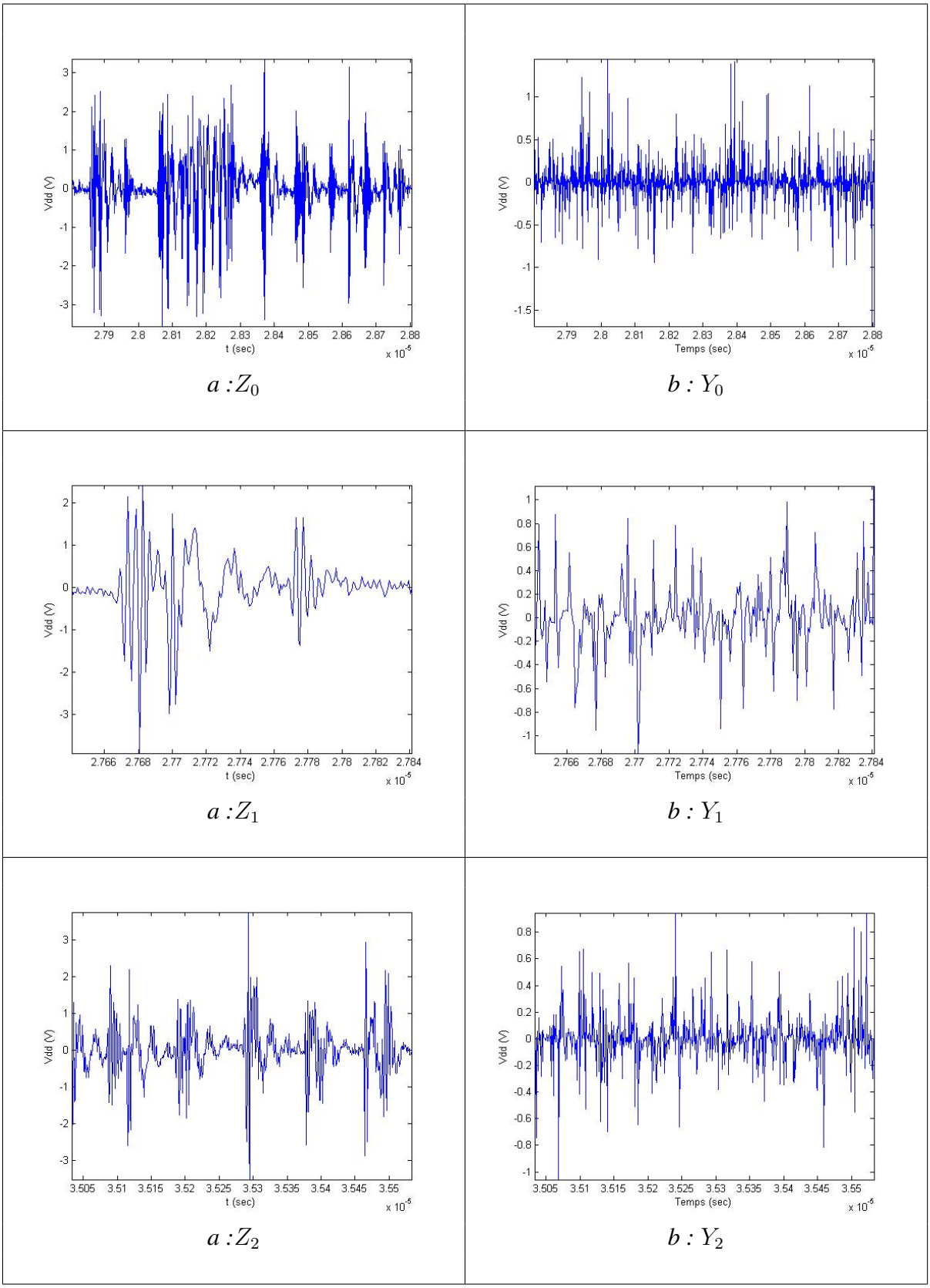


a : Z_9 *b* : Y_9

a : Z_{10} *b* : Y_{10}

FIG. 16 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 9 \ldots 10$

5 MATRICE DE VARIANCE COVARIANCE DÉPENDANT D'UN PARAMÈTRE ESTIMÉ AUTOMATIQUEMENT

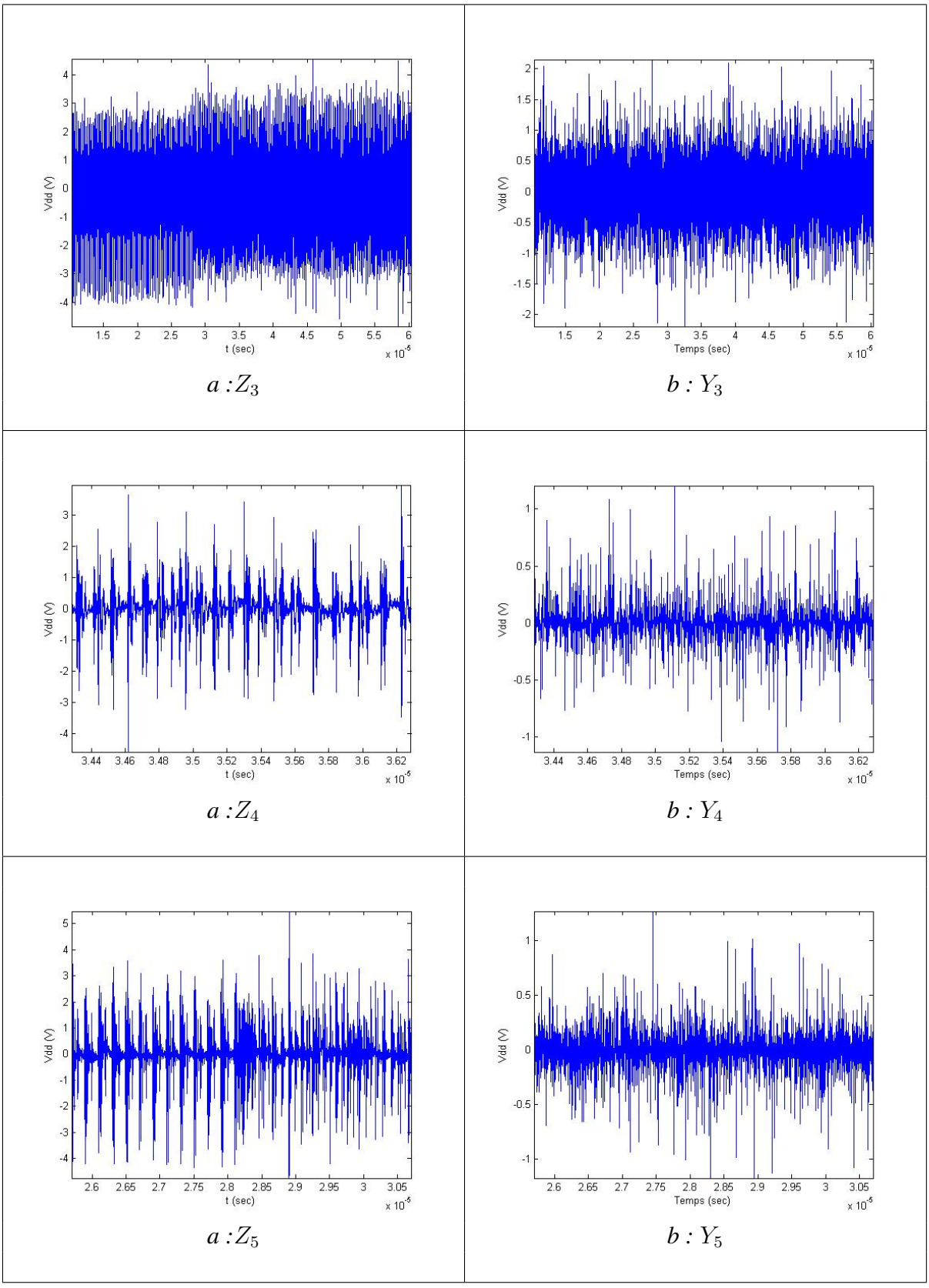


$a : Z_0$ $b : Y_0$

$a : Z_1$ $b : Y_1$

$a : Z_2$ $b : Y_2$

FIG. 17 – *Z_i (a) accompagnés de leurs Y_i respectifs (b), $i = 0 \ldots 2$*

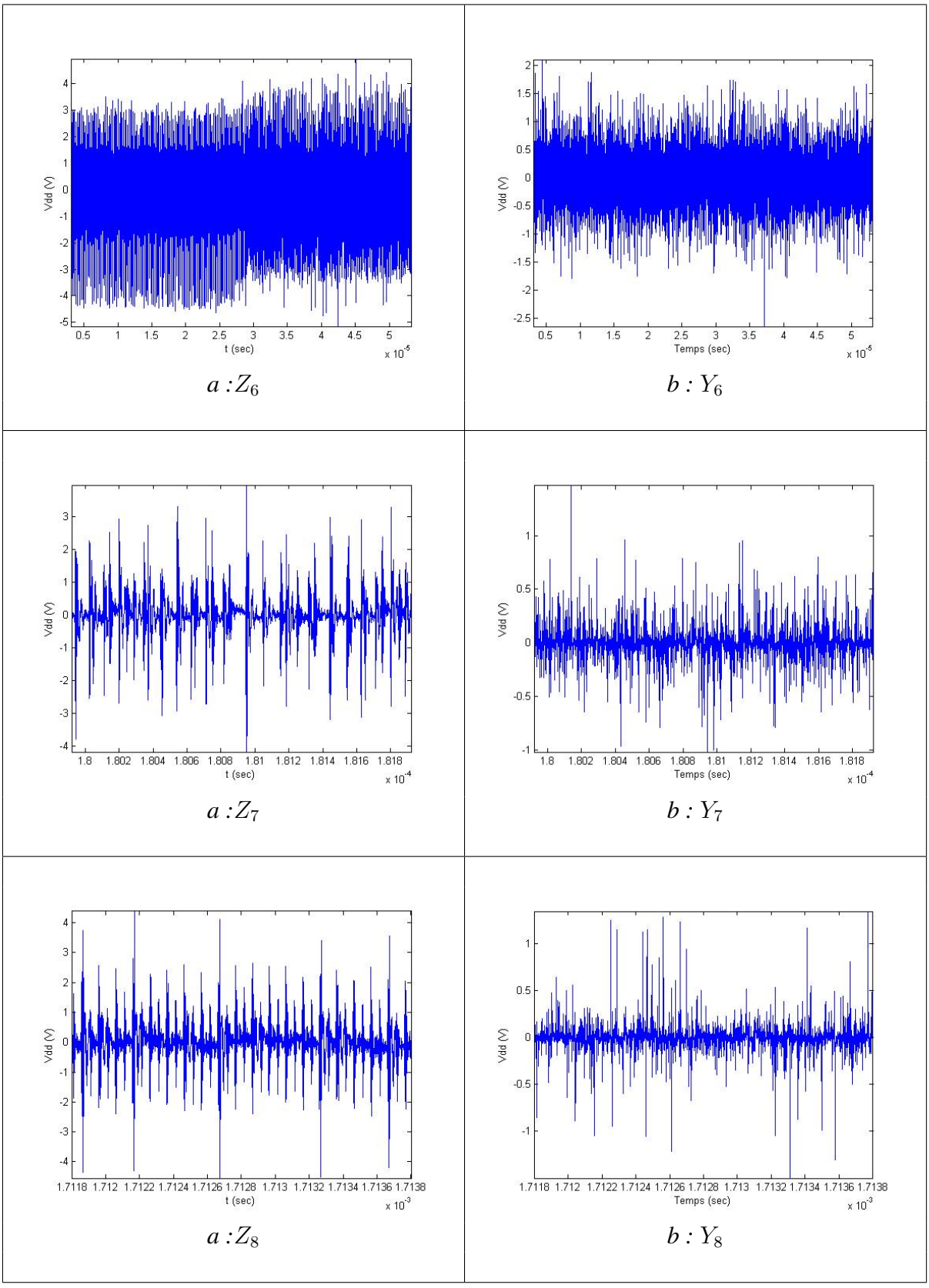


a : Z_3 *b* : Y_3

a : Z_4 *b* : Y_4

a : Z_5 *b* : Y_5

FIG. 18 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 3 \ldots 5$

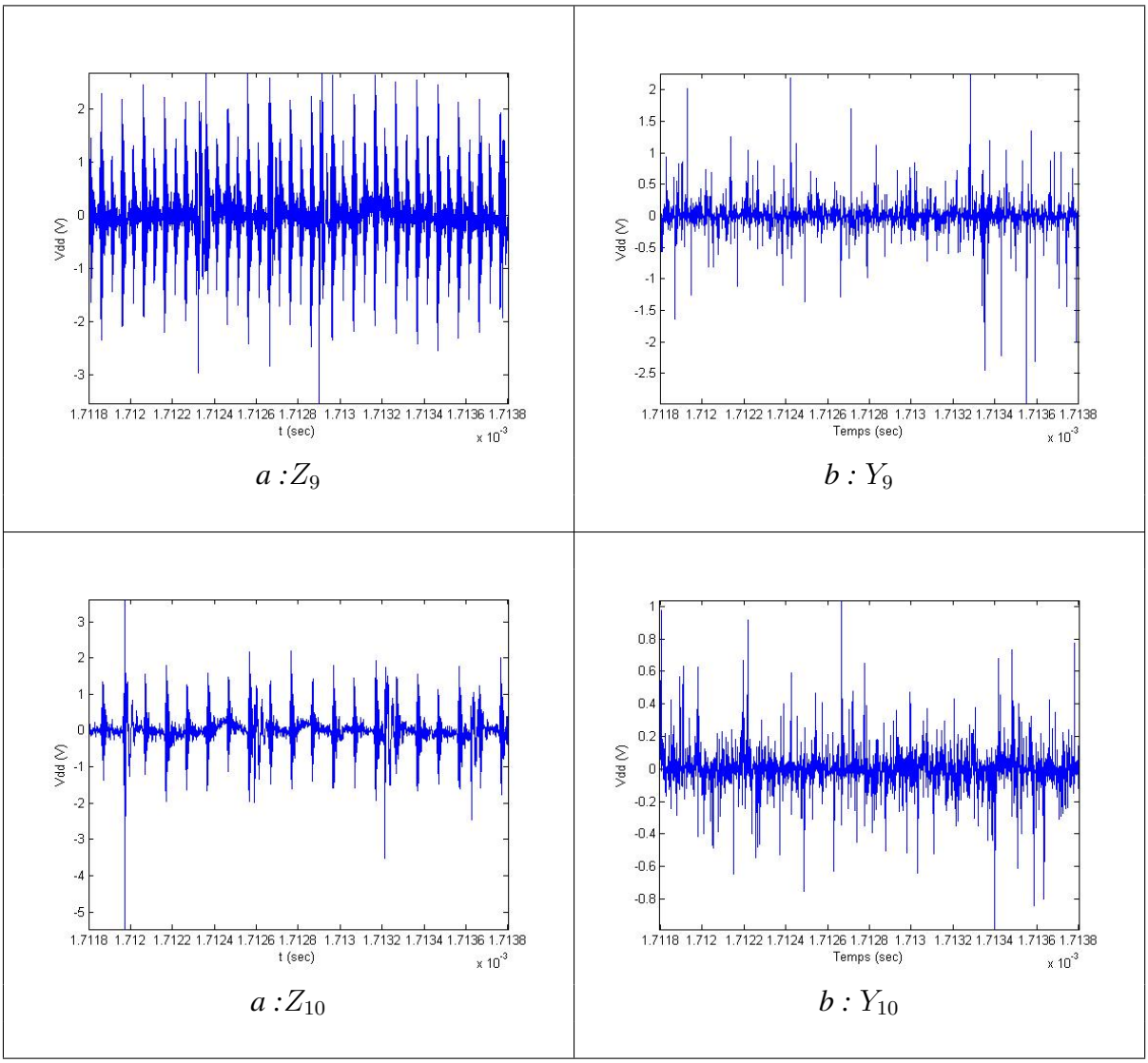


a : Z_6 *b* : Y_6

a : Z_7 *b* : Y_7

a : Z_8 *b* : Y_8

FIG. 19 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 6 \ldots 8$



a : Z_9 *b* : Y_9

a : Z_{10} *b* : Y_{10}

FIG. 20 – *Z_i (a) accompagnés de leurs Y_i respectifs (b),* $i = 9 \ldots 10$

BIBLIOGRAPHIE

[Sch02] W. Rankl, W. Effing, *Smart Card Handbook.*, Third edition, Wiley, 2002.

[Nas50] J. Nash, *Non-cooperative games.*, Thèse de Doctorat, Département de Mathématiques, Université de Princeton, 1950b.

[Ebe04] N. Eber, *Théorie des Jeux.*, collection les Topos, Dunod, 2004.

[Lia06] P. Y. Liardet, *Ingénierie cryptographique - Implantations sécurisées* , Thèse de Doctorat, 2006.

[Akk03] M.L. Akkar, *Attaques et méthodes de protections de systèmes cryptographiques embarquées*, Thèse de Doctorat, 2004.

[Koc96] P. Kocher, *Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", in Proc. of Cyrpto 96*, LNCS 1109, Springer, 1996, pp. 104–113.

[Koc98] P. Kocher, J. Jaffe, B. Jun *Introduction to differential power alalysis and related attacks*,Technical report , Cryptography Research Inc., 1998.

[Qui01] J. J. Quisquater, D. samyde, *Electromagnetic analysis (EMA) measures and counter measures for Smart Cards*, Proc. E, N^o 2140, LNCS, Springer-Verlag, 2001.

[Aig01] M. Aigner, E. Oswald, *Power Analysis Tutorial*, Institute for Applied Information Processing and Communication, University of Technology Graz, 2001.

[Koc99] P. Kocher, J. Jaffe, B. Jub, *Differential Power Analysis*, Proc. of Advances in Cryptology, CRYPTO '99, M. Wiener, LNCS, vol. 1666,p.p. 388-397, Springer-Verlag, 1999.

[Gar01] J. Garrigues, *La méthode des éléments finis,* Cours en ligne, http ://esm2.imt-mrs.fr/gar/efhtml/ , 2001.

[Akh93] N. I. Akhiezer, I. M. Glazman *Theory of Linear Operators in Hilbert Space,* Dover Publication, Inc, New-York, 1993.

[Cou05] P. Courmontagne, *Ingénierie du Signal, Théorie et Pratique,* Ellipses, Paris, 2005.

[Kol94] A. Kolmogorov, S. Fomine *Eléments de la Théorie des Fonctions et de l'Analyse Fonctionnelle,* 3^e édition, Editions MIR, Moscou, Ellipses, 1994.

[Fra06] C. Fraschini, *le filtrage adapté stochastique appliquée aux transmissions à 3,45GHz* Rapport interne L2MP, 2006.

[CouHDR05] P. Courmontagne, Décomposition des signaux aléatoires stationnaires et non-stationnaires. , Habilitation à Diriger les Recherches, p.p. 23-59, 2005.

[Bla81] A. Blanc-Lapierre, B. Picinbono *Fonctions Aléatoires,* Masson, Paris, 1981.

[Rei91] H. Reinhard, *Cours de mathématiques du signal*, Dunod, Paris, 1991.

[Rod91] F. Roddier, *Distributions et transformation de Fourier*, McGraw-Hill, Paris, 1991.

[Pap02] A. Papoulis, S. U. Pillai *Probability, Random Variables and Stochastic Processes,* (4^{th} edition), McGraw-Hill, 2002.

[Kra77] M. Krasnov, A. Kissélev, G. Makarenko *Équations Intégrales,* Editions Mir, Moscou, 1977.

[The87] P. Lascaux, R. Théodor, *Analyse numérique matricielle appliquée à l'art de l'ingénieur*(Tome 2), Masson, 1987.

[Car23] Carleman, *Sur les équations intégrales singulières à noyau réel et symétrique*, Upsula, 1923. JFM 49.0272.01

[Pay67] R. Payen, *Fonctions aléatoires du second ordre à valeurs dans un espace de Hilbert*, Annales de l'institut Henri Poincaré (B) Probabilités et Statistiques, 3 no. 4, pp. 323-396, 1967

[Coo93] D. Cook, A. Buja and J. Cabrera, *Projection pursuit indices based on orthonormal function expansions*, Journal of Computational and Graphical Statistics, 2(3), pp. 225-250, 1993.

[Cou99] P. Courmontagne, *A new formulation for the Karhunen-Loève expansion*, Signal Processing, 79, pp. 235-249, 1999.

[Hot33] H. Hotelling, *Analysis of a complex of statistical variables into principal components*, Journal of Educational Psychology , 24, pp. 417-441,498-520, 1933.

[Kar46] K. Karhunen, *Zur spektraltheorie stochastischer prozesse*, Ann. Acad. Sci. Fennicae, 37, pp. 1-37, 1946.

[Lov55] M.M. Loève, *Probability theory*, Princeton,N.J. , Van Nostrand, 1955.

[Sta01] J.L. Starck, P. Querre, *Multispectral Image Restoration by the Wavelet-Karhunen-Loeve Transform*, Signal Processing , 81, 12, pp 2449-2459, 2001.

[Jai76] A. Jain, *A Fast Karhunen-Loeve Transform for a Class of Random Processes*, IEEE Transactions on Communications, Vol. 24, Issue 9, pp. 1023 - 1029, 1976.

[Kus02] E. Kussener, *Conception de circuits intégrés de régulation intelligente pour les microprocesseurs sécurisés (Carte à puce)*, Thèse de doctorat Microélectronique Conception, Université de Lille I, 2002 .

[Bli93] J.F. Blinn, *What's the deal with the DCT*, IEEE Computer Graphics and Applications, pp.78-83, 1993 .

[Rad03] A.G. Radwan, A.M. Soliman, A.L. El-Sedeek, *MOS realization of the Double-Scroll-Like Chaotic equation*, IEEE transactions on circuits and systems-1 : Fundamental theory and applications, Vol. 50, No. 2, 2003.

[Tel06] V. Telandro, B. Duval, F. Chaillan, E. Kussener, *Chaos Based Random Clock Generator*, Electronic Proceedings of the IEEE Midwest Symposium on Circuits and Systems (MWSCAS'06), San Juan, Puerto Rico, August 2006.

[Lam91] J. D. Lambert, D. C. Lambert, *Numerical Methods for Ordinary Differential Systems : The Initial Value Problem*, Ch. 5, Wiley, 1991.

[JLu04] J. Lü, G. Chen, X. Yu, H. Leung, *Design and Analysis of Multiscroll Chaotic Attractors from Saturated Function Series*, IEEE transactions on circuits and systems-1 : Fundamental theory and applications, Regular paper, 2004.

[Rue80] D. Ruelle, *Les attracteurs étranges*, La Recherche, No 108, p. 132, 1980.

[Chu86] L.O. Chua, M. Komuro, T. Matsumoto, *The Double Scroll Family*, IEEE Trans. on circuits and systems, Vol. 33, No 11, 1986.

[Shi93] C.P. Silva, *Shil'nikov Theorem - A Tutorial*, IEEE Trans. on circuits and systems, Vol. 40, No 10, 1993.

[Man02] P. Manneville , *Dynamique non-linéaire et Chaos*, Physique des liquides, École Polytechnique, Cours, 2002.

[Elw01] A.S. Elwakil, M.P. Kennedy, *Construction of classes of circuit-independent Chaotic oscillators using passive-only nonlinear devices*, IEEE Trans. on circuits and systems, Vol. 48, No 3, 2001.

[Gov04] Govorukhin V.N. *MATDS, a MATLAB-based program for dynamical system investigation*, http ://kvm.math.rsu.ru/matds/index.htm.

[Wol85] A. Wolf, J.B. Swift, H.L. Swinney, J.A. Vastano, *Determining Lyapunov exponents from a time series*, Elsevier Science Publishers, North-Holland Physics Publishing Division, Physica 16D, 285-317, 1985.

[Fip01] L. Evans, P.J. Bond, A.L. Bement, *Security requirements for cryptographic modules*, FIPS 140-2, NIST, 2001.

[Men96] A. Menezes, P. van Oorschot, S. Vanstone *Handbook of Applied Cryptography.*, CRC Press, 1996.

[Ken93] M. P. Kennedy, *Three steps to chaos-part II : A Chua's circuit primer*, IEEE Trans. Circuits and Systems 40, p.p. 657Ű674, 1993.

[Gea71] C.W. Gear, *Numerical Initial Value Problems in Ordinary Differential Equations*, Englewood Cliffs, Prentice-Hall, 1971.

[Esc97] J.P. Escofier, *Théorie de Galois*, p.p. 13-16, Masson, 1997.

[BPM88] P. Bergé, Y. Pomeau, C. Vidal, *L'ordre dans le Chaos*, Hermann, 1988.

[Sto01] T. Stojanovski, J. Pihl, L. Kocarev, *Chaos-Based Random Number Generators - Part II : Practical Realization*, IEEE Trans. on circuits and systems, Vol. 48, No 3, p.p. 382-385 , 2001.

[Joh99] A.J. Johansson, H. Floberg, *Random Number Generation by Chaotic Double Scroll Oscillator on Chip*, Electronic Proceedings of IEEE ISCAS'99 in Orlando, USA, June 1999.

[Erg06] S. Ergün, S. Özoguz, *Truly Random Number Generators Based On Double Scroll Attractor*, Electronic Proceeding of the IEEE Midwest Symposium on Circuits and Systems (MWSCAS'06), San Juan, Puerto Rico, Aug. 2006.

[Yal04] M.E. Yalcin, J.A.K. Suykens, J. Vandewalle, *True random bit generation from a double-scroll attractor*, IEEE Transactions on Circuits and Systems I : Regular Papers, Vol. 51, Issue 7, p.p. 1395- 1404, Juin 2004.

[ST06] V. Telandro, F. Chaillan et E. Kussener, *Générateur d'un Flux Numérique Pseudo-Aléatoire*, brevet numéro 06114520.7-, priorité : FR/25.05.05/ FRA 0551377, date de dépôt : 24.05.06.

[Cha05] F. Chaillan, Ph. Courmontagne, *Amélioration par utilisation du Filtrage Adapté Stochastique de la détection de sillages sur les images SAR*, Traitement du Signal, article à paraître, 2005.

[Cha06] F. Chaillan, C. Fraschini, Ph. Courmontagne, *Speckle Noise Reduction in SAS imagery*, Signal Processing, accepted paper, 2006.

[Joh94] N. L. Johnson, S. Kotz, N. Balakrishnan, *Continuous Univariate Distributions*, volume 1, Wiley Series in probability and Mathematical statistics, 1994.

[Osw05] E. Oswald, *Advances in Elliptic Curve Cryptography*, Chap. V, Side-Channel Analysis edited by I. Blake, G. Seroussi and N. Smart, LMS 317, Cambridge University Press, 2005

[Kay93] S. M. Kay, *Fundamentals of Statistical Signal Processing : Estimation Theory*, Upper Saddle River, New Jersey : Prentice-Hall, Inc., 1993.

[Pil05] D. Pillon, C. Jauffret, *Trajectographie passive par mesure d'angle*, Technique de l'ingénieur, TE 6 705, 2005.

[Pog92] M. Pogu, J.E. Souza De Cursi, *Minimisation stochastique de fonctionnelles non-convexes en dimension finie*, Publications du service de mathématiques de l'ECN, Avril 1992.

[Sou92] J.E. Souza De Cursi, *Recuit simulé et application a l'approximation par des sommes d'exponentielles*, Publications du service de mathématiques de l'ECN, Septembre 1992.

[Cav93] J.-F. Cavassilas, B. Xerri, *Extension de la notion de filtre adapté. Contribution à la détection de signaux courts en présence de termes perturbateurs*, Traitement du Signal, Vol. 10, N^o 3, pp. 215 221, 1993.

[Dem77] A.P. Dempster, N.M. Laird, D.B. Rubin, *Maximum likelihood from incomplete data via the EM algorithm*, IEEE trans. on acoustics, speech, and signal processing, Vol. 36, N^o 14, Avril 1988.

[Cel89] G. Celeux, J. Diebolt, *Une version de type recuit simulé de l'algorithme EM*, Rapport de recherche, INRIA Roquencourt, programme 5, N^o 1123, novembre 1989.

[Fed88] M. Feder, E. Weinstein, *Parameter estimation of superimposed signals using the EM algorithm*, IEEE trans. on acoustics, speech, and signal processing, Vol. 36, N^o 4, Avril 1988.

[Bil98] J.A. Bilmes, *A Gentle tutorial of the EM algorithm and its application to parameter estimation for gaussian mixture and hidden Markov models*, International Computer Science Institute, Avril 1998.

[The87] P. Lascaux, R. Théodor, *Analyse numérique matricielle appliquée à l'art de l'ingénieur*(Tome 1), Masson, 1987.

[Gha97] Z. Ghahraman, G.E. Hinton, *The EM algorithm for mixtures of factor analysers*, Rapport technique du département Computer Science, Université de Toronto, Fevrier 1997.

[Jau06] C. Jauffret, A. Santori, *Borne de Cramèr-Rao et algorithme EM*, rapport interne GESSY, Mars 2006.

[Cha06s1] F. Chaillan, Ph. Courmontagne, *Detection of short signals in a noisy underwater environment*, Electronic Proceedings of IEEE OCEANS'06, Singapore, May 2006.

[Cha05b1] F. Chaillan, C. Fraschini, Ph. Courmontagne, *Stochastic matched filtering method applied to SAS imagery*, Electronic Proceedings of IEEE OCEANS'05, Brest, France, Juin 2005.

[Cha05b2] F. Chaillan, C. Fraschini, M. Amate, Ph. Courmontagne, *Multiresolution analysis of SAS images*, Electronic Proceedings of IEEE OCEANS'05, Brest, France, Juin 2005.

[Cha06s2] F. Chaillan, C. Fraschini, Ph. Courmontagne, *Coupling the Stochastic Matched Filter and the à Trous algorithm for SAS image de-noising*, Electronic Proceedings of IEEE OCEANS'06, Singapore, Asia, May 2006.

[Cou06] Ph. Courmontagne, F. Chaillan, *On the use of the Stochastic Matched Filter for Ship Wake Detection in SAR Images*, Electronic Proceedings of IEEE OCEANS'06, Boston, USA, September 2006.

[Lev93] C. Lévèque, J. F. Cavassilas, *généralisation du concept de filtre adapté, application au filtrage d'images SAR d'états de surface de la mer.*, 14^{me} colloque GRETSI, Juan-les-Pins, Vol. 1, p.p. 539-543, 1993.