

présentée à

L'U.F.R DES SCIENCES ET TECHNIQUES
DE L'UNIVERSITÉ DE FRANCHE-COMTÉ

pour obtenir le

GRADE DE DOCTEUR DE L'UNIVERSITÉ
DE FRANCHE-COMTÉ
Spécialité Sciences pour l'Ingénieur

SYSTÈME D'INTERFÉRENCES
RADIOFRÉQUENCES POUR LA CRYPTOGRAPHIE
PAR CHAOS APPLIQUÉE AUX TRANSMISSIONS
HERTZIENNES

par

Aurélien PALLAVISINI

Soutenue le 9 Juillet 2007 devant la commission d'examen :

Président	Hervé Maillotte	Directeur de Recherche CNRS, directeur du département d'Optique de l'institut FEMTO-ST, Besançon
Rapporteurs	Raymond QUÉRÉ Safwan EL ASSAD	Professeur, Université de Limoges Maître de Conférences HDR, École Polytechnique de l'Université de Nantes
Examineurs	Nadia BUTTERLIN Roger TAULEIGNE	Maître de Conférences HDR, Université de Franche-Comté, directrice de l'ISIFC, Besançon Maître de Conférences ENSEA, Cergy
Directeur de Thèse	Laurent LARGER	Professeur, Université de Franche-Comté, Besançon

*... à mes parents,
Marie Claire et Itole
à mon frère
Johann,
à mes grands parents,
Germaine et Aimé.*

Remerciements

J'ai pu, pendant 3 années, effectuer ma thèse au laboratoire GTL-CNRS Télécom à Metz. Changé de ville très rapidement n'a pas été simple ; mais le soutien de l'ensemble des personnes que j'ai pu côtoyer professionnellement et amicalement à Metz m'ont permis de facilement m'intégrer en Moselle.

Dès mon arrivée au laboratoire, j'ai pu compter sur une équipe formidable que je n'oublierai jamais. L'aide scientifique et technique de Marc H., Fred P., Johann C., Xavier B. et Matthieu B. associée à la constante bonne humeur de David B., Jérôme et Murielle V., Olivier G., Jacky sans oublier Serge dit serain.

J'aimerais également adressé un remerciement spécial à Sam M. et Olivier K., sans qui le travail expérimental n'aurait pas autant avancé en si peu de temps ; un travail de qualité qui n'est pas passé inaperçu dans la rédaction de ce manuscrit. J'adresserai un immense merci à Laurent L. qui, par sa pédagogie et sa disponibilité, a su éclaircir les points techniques et théoriques bloquants. De plus, il a su me faire confiance à la suite de mon Master pour me proposer un sujet de recherche tout à fait adapté qui m'a permis de m'insérer facilement dans la vie professionnelle.

Mon arrivée dans cette ville lorraine que je ne connaissais pas a également été rythmée par ma vie extra-professionnelle où le soutien de mes amis footeux comme Rondel, Cécé, Tophe, Nono et Romain ont eu une importance fondamentale pour pouvoir m'imprégner de la vie mosellane.

Je remercie également Sylvie et Audrey, respectivement le soleil du sud-ouest et la sympathie jurassienne, qui m'ont fait découvrir la ville de Metz et ces alentours, et comment s'amuser sans parler de travail... Merci pour leur soutien sans faille.

Je remercie mes parents pour leur soutien et également pour m'avoir offert la bible de l'électronique à savoir *electronic communication techniques* - Paul H. Young pour mon anniversaire...

Je pense sincèrement que sans toutes ces personnes, ce manuscrit n'existerait pas et je tiens à les en remercier. La présence de tous, qu'elle soit professionnelle ou autre, a

vraiment permis de vivre 3 années exceptionnelles à Metz, une ville et un moment de ma vie que je n'oublierai sans doute jamais.

Table des matières

Introduction	1
1 Les systèmes non linéaires : généralités	7
1.1 Introduction	7
1.2 Systèmes linéaires, exemples	8
1.2.1 Oscillateur classique	8
1.2.2 Influence d'un retard dans une boucle d'oscillation	12
1.3 Systèmes et comportements fortement non linéaires	14
1.3.1 Stabilisation de l'amplitude des oscillations	14
1.3.2 Quelques phénomènes non linéaires	15
1.3.3 Oscillateur de Chua	16
1.3.4 Dynamique non linéaire à retard	18
1.4 Outils et techniques de caractérisation	24
1.4.1 Analyse statistique : quelques définitions	25
1.4.2 Analyse dans le domaine fréquentiel	27
1.4.3 Espace des phases et types d'attracteurs	29
1.4.4 Notions de bifurcation	31
1.4.5 Les types de bifurcation et ses diagrammes	33
1.4.6 Exposants de Lyapunov	36
1.5 Applications des différents types d'oscillateurs	38
1.5.1 Télécommunications à porteuse harmonique	38
1.5.2 Télécommunications à étalement de spectre	39
1.5.3 Cryptographie par chaos	41
2 La cryptographie par chaos en fréquence	51
2.1 Introduction	51
2.2 Les transmissions hertziennes : la modulation de fréquence	52
2.2.1 Quelques rappels sur les radiofréquences et les hyperfréquences en télécommunication	52
2.2.2 Rappels et définition de la modulation en fréquence	55

2.2.3	Les techniques de démodulation de signaux FM	55
2.2.4	Les antennes de transmission	59
2.3	Système électronique de cryptographie par chaos	62
2.3.1	Conversion de la dynamique chaotique	63
2.3.2	La fonction non linéaire	64
2.3.3	Retard temporel	67
2.3.4	Filtre assurant la dynamique limitante du système en bande de base	68
2.3.5	Caractérisation du chaos en fréquence de l'oscillateur HF	70
2.3.6	Système de réception et de réplique du chaos	72
2.3.7	Synchronisation et extraction de l'information	74
2.3.8	Perspectives d'adaptation aux fréquences UHF	77
2.4	Système d'interférences RF	77
2.4.1	L'oscillateur commandé en tension	78
2.4.2	Principe de réalisation de la fonction non linéaire	79
2.4.3	Le retard temporel	87
2.4.4	La dynamique limitante	88
2.5	Caractérisation de l'oscillateur chaotique	89
2.5.1	Définition du modèle mathématique	89
2.5.2	Simulations numériques des comportements dynamiques	90
2.5.3	Paramètres de l'oscillateur	92
2.5.4	Analyse temporelle, spectrale et statistique	93
2.5.5	Diagrammes de bifurcation	96
2.5.6	Espace des phases	99
2.5.7	Exposants et dimension de Lyapunov	100
2.6	Réception et réplique de la porteuse chaotique	102
2.6.1	La boucle à verrouillage de phase : synchronisation	103
2.6.2	Réplique du chaos	105
2.6.3	Conditions de fonctionnement et de simulations	110
2.6.4	Les effets de la constante de temps sur la non linéarité	111
2.7	Applications aux communications cryptées	113
2.7.1	Analyse du signal chaotique contenant l'information	113
2.7.2	Conclusion	118
3	Résultats expérimentaux	121
3.1	Introduction	121
3.2	Analyse des composants de l'oscillateur	122
3.2.1	Caractéristique de l'oscillateur commandé en tension	122
3.2.2	La non linéarité	124

3.2.3	Relevé expérimental de la fonction d'interférence	132
3.3	Analyse des interférences RF	136
3.3.1	Faibles différences de chemin RF	136
3.3.2	Grandes différences de chemin RF	138
3.3.3	Choix des paramètres de l'interféromètre RF	140
3.4	Caractérisation de l'oscillateur chaotique	142
3.4.1	Evolution temporelle et spectrale	143
3.4.2	Diagramme de bifurcation	145
3.5	La réplication du chaos en fréquence	152
3.5.1	Accordabilité des fonctions de l'émetteur et du récepteur	153
3.5.2	Synchronisation entre deux signaux chaotiques	154
3.5.3	Influence de l'ordre d'interférence ΔT	155
3.5.4	Influence du gain normalisé β	156
3.6	Système de cryptographie	158
3.6.1	Codage d'un message analogique	158
3.6.2	Codage d'un message numérique	159
3.7	Conclusion	161
3.8	Perspectives expérimentales	161
	Conclusion générale et perspectives	165
	Annexes	169
A	Cartes électroniques du chaos en fréquence (BF)	169
B	Résolution de l'équation différentielle du second ordre par la méthode Runge-Kutta du quatrième ordre	177
C	Calcul de l'influence du compensateur d'erreur dans la matrice [S] obtenue	181
D	Calcul du chaînage de plusieurs quadripôles	183
E	Schémas des cartes électroniques et opto-électroniques réalisées	185
E.1	Support de la diode laser CATV (modulation et alimentation)	185
E.2	Schéma électronique d'une partie de l'émetteur	186
E.3	Schéma électronique d'une partie du récepteur	187
E.4	Typon	188
E.5	Photographie des cartes électroniques de l'émetteur et du récepteur	189
E.5.1	Emetteur	189

E.5.2	Récepteur	189
E.5.3	Support de la diode laser	190

Bibliographie	191
----------------------	------------

Introduction

L'histoire des télécommunications est liée à la fois à l'évolution des sciences physiques, mais aussi à des besoins liés à l'évolution de la société [1]. Depuis l'antiquité, l'homme n'a cessé de chercher les différents moyens (parole, geste de la main, signaux de fumée, tam-tam, document écrit...) pour transmettre un message à son correspondant, et donc pour communiquer. Ainsi, l'être humain, à travers les époques successives, a fourni ses efforts intellectuels aussi bien que physiques afin de découvrir des méthodes de communication adéquates.

C'est en 1790 que le physicien Claude Chappe présente, à la nouvelle assemblée nationale, un projet d'une ligne permanente de télégraphe optique. L'idée de Chappe n'est pas d'associer un signal à une lettre mais à un mot ou à une expression. En 1794, la première ligne télégraphique optique fut créée entre Paris et Lille.

Contrairement aux premiers inventeurs du télégraphe, l'américain Samuel Morse est un scientifique. Il recherche un système simple et pratique. Son télégraphe exécute des signaux codés à l'aide d'un levier à ressort actionné à la main. Celui-ci, en fermant ou en ouvrant un circuit, provoque dans l'appareil récepteur des signaux identiques. Le code est composé seulement de deux éléments (un signal court, un signal long), la combinaison de quatre d'entre eux suffit pour constituer les lettres de l'alphabet. En 1839, l'anglais William Cooke installe sa première ligne de télégraphe électrique. La vitesse de transmission de 280000 milles par seconde (celle de l'électricité), doit permettre une transmission dans le monde entier. La liaison trans-manche sera installée en 1851 grâce à une technique, mise au point par l'allemand Siemens, permettant d'isoler un câble électrique en milieu marin. Il faudra attendre quinze ans pour qu'une liaison transatlantique soit opérationnelle. Cette opération s'est effectuée grâce au plus grand paquebot de l'époque sur lequel fut chargé un câble de 4000 *km*.

Comme pour de nombreuses inventions, la TSF a bénéficié des découvertes de différentes personnes :

- Le physicien anglais Olivier Lodge construit en 1894 un récepteur d'ondes hertziennes avec un tube à limaille.
- Le physicien français Edouard Branly mène des recherches sur les corps conducteurs et étudie l'évolution de la conductibilité en fonction de différents rayonnements

calorifiques et lumineux. En 1890, il remarque que, sous l'effet d'une étincelle, un tube à limaille de fer devient alternativement conducteur ou isolant.

Marconi a besoin d'argent pour fiabiliser l'émetteur/récepteur complet qu'il a mis au point et le mettre sur le marché. Il trouvera cet appui auprès de sa famille pour fabriquer et commercialiser les premiers postes TSF. Son premier marché sera l'équipement des phares isolés en mer. Mais c'est surtout l'armée qui fera appel à Marconi pour équiper la flotte britannique. En 1901, il s'associe avec la compagnie d'assurance maritime Lloyd's pour transmettre des informations sur les navires. La Lloyd's possède en effet un réseau de plus de mille agents, dans les principaux ports du monde, chargés de recueillir l'information sur l'arrivée et la circulation des navires.

L'histoire est relativement vaste concernant les télécommunications, avec un développement scientifique et social, avec un intérêt et une dépendance grandissants pour les nouveaux modes de télécommunications. Ces modes de télécommunications sont en perpétuelle évolution, avec la recherche de meilleurs débits, de plus grandes facilités d'utilisation, de meilleure mobilité et, de plus en plus, avec des contraintes de confidentialité.

De nos jours plus particulièrement, les télécommunications hertziennes sont devenues un moyen de communication de plus en plus développé avec un nombre d'utilisateurs en constante augmentation (fig.1).

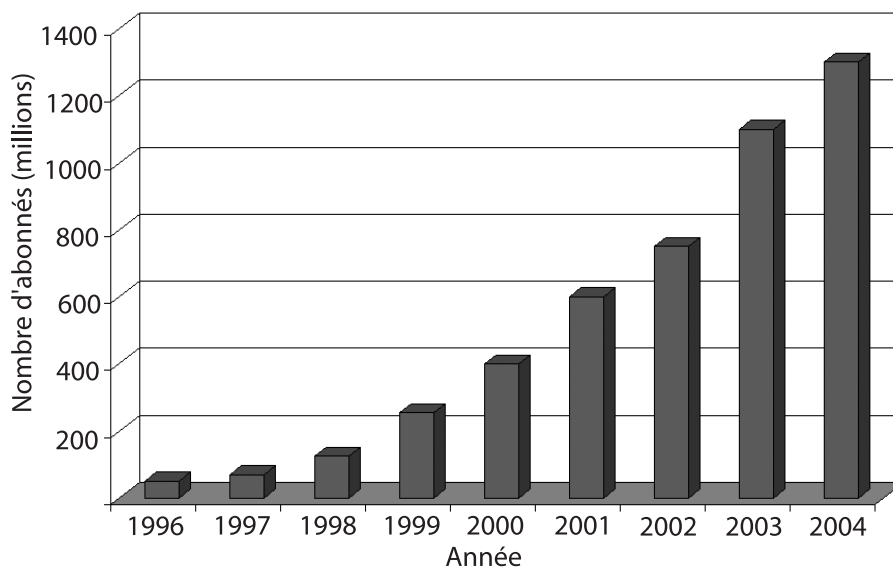


FIG. 1 – Evolution du marché de la téléphonie mobile

La banalisation et la généralisation des communications hertziennes modernes impliquent son utilisation aussi pour des messages à caractère confidentiel. La nature numérique de ce mode de communication offre certes toute une panoplie de techniques cryptographiques algorithmiques, mais la montée en puissance des calculateurs met, chaque jour,

un peu plus en péril la sécurité supposée de cette cryptographie numérique. L'objet de ce travail de thèse concerne précisément l'étude d'une solution de caractérisation différente de la cryptographie algorithmique contemporaine.

Cultivée depuis l'antiquité, la cryptographie (du grec *kryptos*, caché, et *graphein*, écrire) est plusieurs fois millénaire. Dans la Chine antique on utilisait déjà la stéganographie, c'est à dire l'art de dissimuler un message secret dans un texte d'aspect anodin. En Inde, le célèbre "Kâma-Sûtra" recommandait aux femmes d'apprendre - entre autres choses - l'art des écritures secrètes qui doit leur permettre de dissimuler leurs liaisons. En Mésopotamie, une autre grande civilisation de l'antiquité, on remplaçait des mots par des nombres. En Grèce, on utilisait un instrument appelé "scytale" pour mélanger les lettres d'un message...

L'histoire de la cryptographie [2], c'est l'histoire d'une guerre. La guerre qui oppose, depuis des siècles, ceux qui ont quelque chose à cacher (qu'ils soient militaires, scientifiques, politiciens, financiers ou même amants illégitimes) et ceux qui aimeraient bien savoir ce qu'on leur cache (les ennemis, les concurrents, les espions, les escrocs et même les maris jaloux). Les deux camps se livrent une lutte sans fin. Ainsi, dès que l'un a trouvé un nouveau moyen de chiffrer ses messages, l'autre se dépêche de trouver un moyen de les décrypter. Et, jusqu'à présent, il y est toujours parvenu. Ce n'est qu'une question de temps et de moyens.

Le principe général de la cryptographie algorithmique consiste à trouver une transformation mathématique complexe qui permet, à partir d'un message clair, d'obtenir un message dit "chiffré", d'apparence quasi-aléatoire, où les règles du langage ont disparu. La sécurité dépend alors de la difficulté à inverser cette transformation, à partir d'informations sur la "quasi-disparition" des règles du langage. Le message chiffré doit donc apparaître le plus possible comme "aléatoire" ou "incohérent". Dans un tout autre contexte, mais avec des propriétés ressemblantes, la physique, en général, s'est intéressée, durant ces dernières années, à des phénomènes d'apparence "aléatoires" ou "incohérents", mais d'origine tout à fait déterministe [3] : ceux produits par des systèmes dynamiques dit chaotiques.

Il existe d'innombrables exemples de comportement chaotique dans notre vie quotidienne. Les trajectoires d'une feuille tombant d'un arbre, celles des volutes d'une fumée s'élevant dans les airs, celles d'un objet lancé dans un cours d'eau, en font partie et sont effectivement difficiles à prévoir. Une autre illustration que l'on peut en donner est celle d'un jeu de boules de billard à obstacles convexes. Théoriquement, il est possible de faire en sorte qu'une boule de billard frappe trois faces d'une table de billard en leur centre, où seraient placés des obstacles convexes, avant de revenir à sa position initiale. Dans la réalité, d'infimes inexactitudes dans la direction initiale entraînent des trajectoires tota-

lement différentes (fig.) [4].

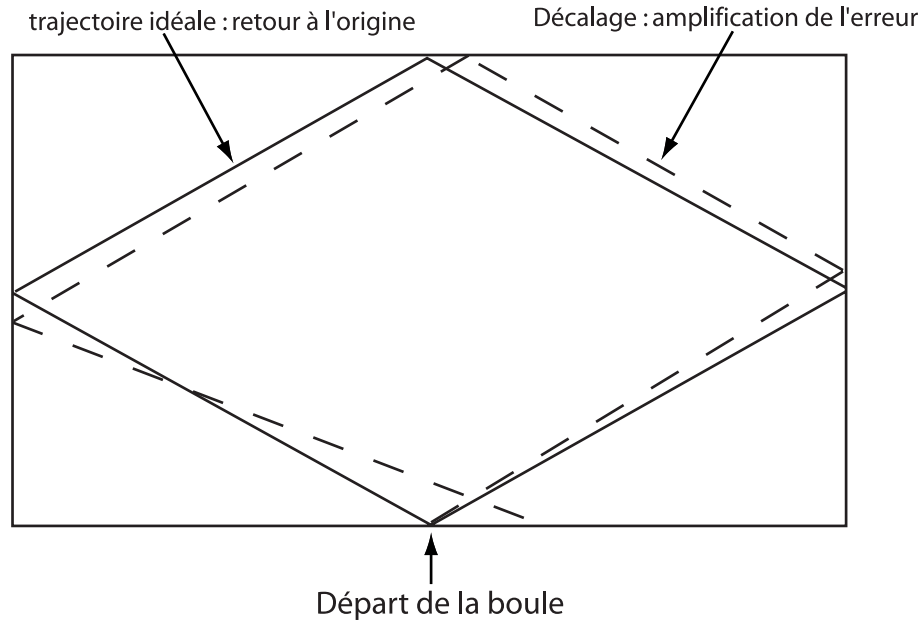


FIG. 2 – Différence de trajectoire de boules de billard

La théorie du chaos a été reconnue, d'un point de vue médiatique, en tant que telle à partir des années 1960 grâce aux travaux d'un certain nombre de chercheurs (dont Lorenz), et grâce à l'émergence de nouveaux outils de calculs (ordinateurs). Ainsi, un système chaotique est un système complexe, régi par un certain nombre de lois déterministes (comme celles de la météorologie par exemple), dépendant de plusieurs paramètres, et dont la caractéristique d'ensemble fondamentale est son extrême sensibilité aux conditions initiales [5]. Le comportement de tels systèmes est imprévisible, bien que leurs composantes soient gouvernées par des lois simples, connues, déterministes. Les méthodes théoriques et mathématiques sont souvent complexes et partiellement efficaces pour la prévision de tels systèmes ; on en est parfois réduit à tenir compte de la statistique, du seul calcul des probabilités pour analyser des comportements chaotiques.

Les deux points que sont le chaos et la transmission hertzienne évoqués précédemment peuvent être réunis pour donner naissance à la cryptographie par chaos. Celle-ci a pour but de masquer dans un pseudo-bruit d'origine chaotique un message d'information, pour parer aux éventuelles attaques et piratages qui sont en constante progression depuis quelques années. La cryptographie par chaos est un principe de cryptographie à clés secrètes. La connaissance de celles-ci est indispensable de chaque côté de la transmission pour le chiffrement/masquage et le déchiffrement. Le système décrit tout au long de ce manuscrit est un oscillateur permettant de générer un signal dont la fréquence, bien que

déterministe, possède une évolution pseudo-aléatoire car chaotique. Ce signal est la porteuse de notre modulation en fréquence qui va masquer le signal d'information. De plus, le fait d'utiliser une porteuse chaotique en modulation de fréquence rend le système proposé compatible avec un grand nombre d'applications actuelles de ce format de modulation.

Ce travail de thèse se décompose en quatre parties :

- Le premier chapitre sera un rappel des systèmes déjà réalisés dans le contexte de la cryptographie par chaos. Il énoncera également quelques techniques d'analyse permettant d'étudier le signal chaotique émis par notre oscillateur.
- Un second chapitre présentera plus en détail un premier système de cryptographie par chaos en fréquence. Ce premier système, ainsi que le second conçu en plus haute fréquence, utilisent une large partie électronique, c'est pourquoi quelques notions utilisées dans les phénomènes de propagation en radiofréquences et en électronique rapide seront présentées. Au cours de ce chapitre, nous enchaînerons directement sur la présentation du système réalisé lors de cette thèse. Les simulations numériques à partir des calculs mathématiques appuieront les études électroniques et les phénomènes physiques abordés dans la partie expérimentale.
- Le troisième et dernier chapitre essaiera d'approuver expérimentalement l'exactitude du modèle mathématique mis en place. Nous énoncerons les problèmes rencontrés dans la conception du système et l'influence qu'ils peuvent avoir dans l'opération de synchronisation entre chaos, opération essentielle en vue du décodage de l'information.

Bonne lecture...

Chapitre 1

Les systèmes non linéaires : généralités

*La seule vraie science est
la connaissance des faits*
Buffon, Histoire Naturelle

1.1 Introduction

Ce premier chapitre a pour objectif de donner une introduction générale sur les comportements dynamiques non linéaires et leur application à la sécurisation de l'information. Il commencera par une présentation des systèmes dynamiques «quasi-linéaires» , sur la base d'oscillateurs électroniques classiques et de leurs conditions de démarrage des oscillations. La limitation de l'amplitude de ces oscillations nous amènera assez naturellement aux phénomènes non linéaires, qui seront également décrits sur la base d'autres exemples électroniques. Une classe particulière d'oscillateurs non linéaires directement concernée par ce travail de thèse sera ensuite décrite : les dynamiques non linéaires à retard. Une étude des solutions dynamiques d'un modèle simplifié de ces dynamiques à retard, le modèle discret, nous permettra de mettre en évidence la richesse de comportements possibles en fonction de la valeur de certains paramètres. Après cette approche ciblée sur des exemples précis, nous évoquerons un certains nombres d'outils mathématiques utiles dans l'analyse et la compréhension des divers comportements dynamiques (des oscillations périodiques aux régimes chaotiques), qui seront effectivement rencontrés dans la suite. Nous finirons ensuite en essayant de montrer le lien entre oscillations chaotiques et systèmes de communication.

1.2 Systèmes linéaires, exemples

1.2.1 Oscillateur classique

Conditions d'oscillation

Un oscillateur est un amplificateur contre-réactionné dans des conditions instables, à forte sélectivité et variations en amplitude et en phase. Dans le domaine de Laplace, si $A(p)$ définit la fonction de transfert de l'amplificateur et $B(p)$ celle d'un filtre sélectif qui va déterminer la fréquence d'oscillation, le système est décrit par la figure suivante avec des blocs linéaires :

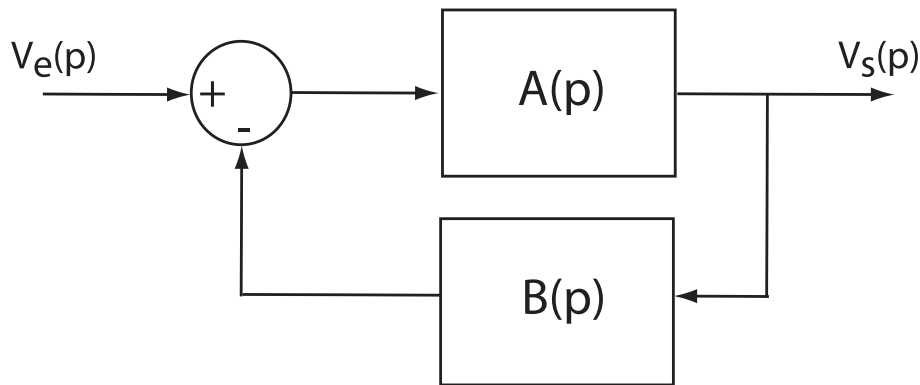


FIG. 1.1 – Synoptique d'un oscillateur harmonique

Ainsi, la fonction de transfert de l'ensemble (V_s/V_e) sera :

$$H(p) = \frac{A(p)}{1 + A(p) B(p)} \quad (1.1)$$

Le système n'oscillera que sous certaines conditions. Si $A(p) B(p) = -1$, le dénominateur s'annule et la fonction de transfert devient infinie, ce qui peut s'interpréter en considérant que la tension de sortie est non nulle alors que la tension d'entrée est nulle. Dans certaines circonstances uniquement, cet ensemble peut constituer un oscillateur. En effet, un amplificateur opérationnel avec son entrée inverseuse à la masse et rebouclé sur son entrée non-inverseuse rentre par exemple dans ces conditions d'instabilité mais ne constitue pas, pour autant, un oscillateur. La tension de sortie se sature à $+V_{sat}$ et le système est stable (d'un point de vue électrique). Ceci est dû au fait que les conditions d'instabilité sont vérifiées à fréquence nulle. L'appellation générale d'oscillateur n'inclut pas ce type de comportement. Les conditions d'instabilité sont les conditions limites de démarrage des oscillations de Barkhausen (1.2) .

$$\begin{cases} |A(p) B(p)| > 1 \\ \arg[A(p)] + \arg[B(p)] = (2k + 1)\pi \end{cases} \quad (1.2)$$

Nous pouvons remarquer l'influence de variations ϵ des gains $|A(p)|$ et $|B(p)|$ en supposant que les conditions de Barkhausen soient vérifiées pour la phase à la pulsation ω_0 . Le signal $s(t)$ correspond à la sortie du système oscillant.

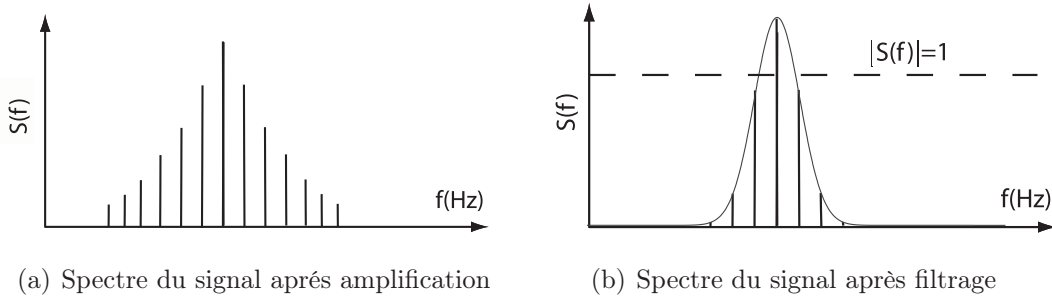


FIG. 1.2 – Différents signaux dans la boucle ouverte de l'oscillateur

Ainsi, pour qu'un signal oscillant puisse apparaître, il est nécessaire que le système vérifie pour une certaine pulsation ω_0 :

$$|A(j\omega_0) B(j\omega_0)| > 1 \quad (1.3)$$

C'est la condition d'oscillation. Néanmoins, le signal qui apparaît à la pulsation ω_0 est divergent, son amplitude croît exponentiellement. Donc à partir d'une certaine amplitude, l'amplificateur sort de sa plage de fonctionnement linéaire (saturation) comme le montre la figure 1.2(a) avec la génération d'harmoniques. Il apparaît une distorsion due à l'écrtage ; c'est pourquoi, dans la pratique, ces conditions de Barkhausen sont effectivement vérifiées, mais uniquement au démarrage de l'oscillation. Un filtrage sélectif permet de déterminer la fréquence d'oscillation (fig.1.2(b)). Ce filtrage n'est cependant pas parfait. La solution périodique de grande amplitude observée en régime permanent, fait intervenir des non-linéarités qui ne sont pas décrites par l'approche des petits signaux de Barkhausen. Ce sont des méthodes spécifiques aux systèmes non linéaires dont la plus simple est la méthode du premier harmonique [6].

Il existe plusieurs types d'oscillateurs comme les oscillateurs à réseau RC¹, les oscillateurs à réseau LC² comme l'oscillateur de Colpitts et de Clapp, les oscillateurs piézo-électriques et les oscillateurs commandés en tension sur lesquels nous reviendrons ultérieurement.

¹Résistance/Capacité

²Inductance/Capacité

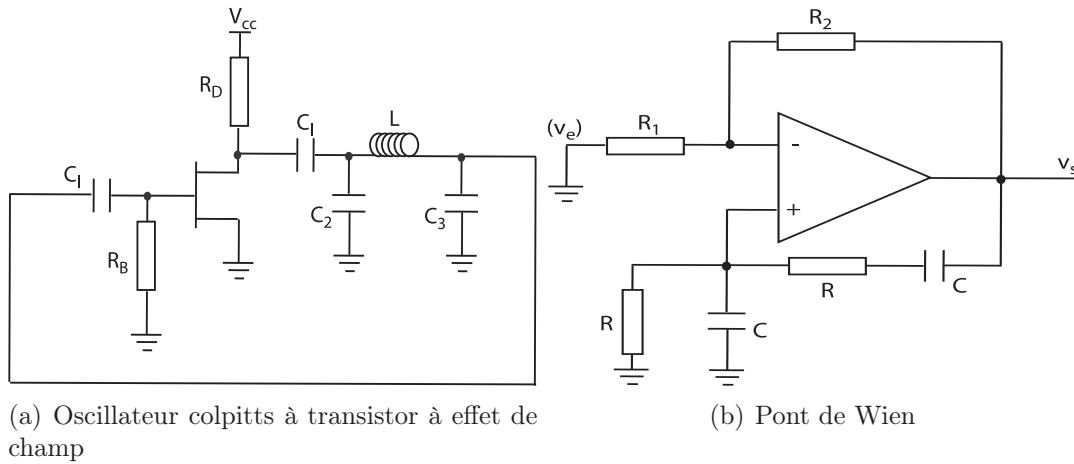


FIG. 1.3 – Différents types d'oscillateur

Exemple : l'oscillateur de Colpitts

Il existe une grande variété de montages utilisant un réseau de contre-réaction de type LC. Le plus utilisé est le montage de Colpitts. Pour mieux appréhender le fonctionnement de cet oscillateur, il faut revenir au fonctionnement de l'oscillateur de la figure 1.3(a) en le décomposant en deux parties : l'amplification $A(j\omega)$ et le circuit de résonance $B(j\omega)$ (fig.1.4).

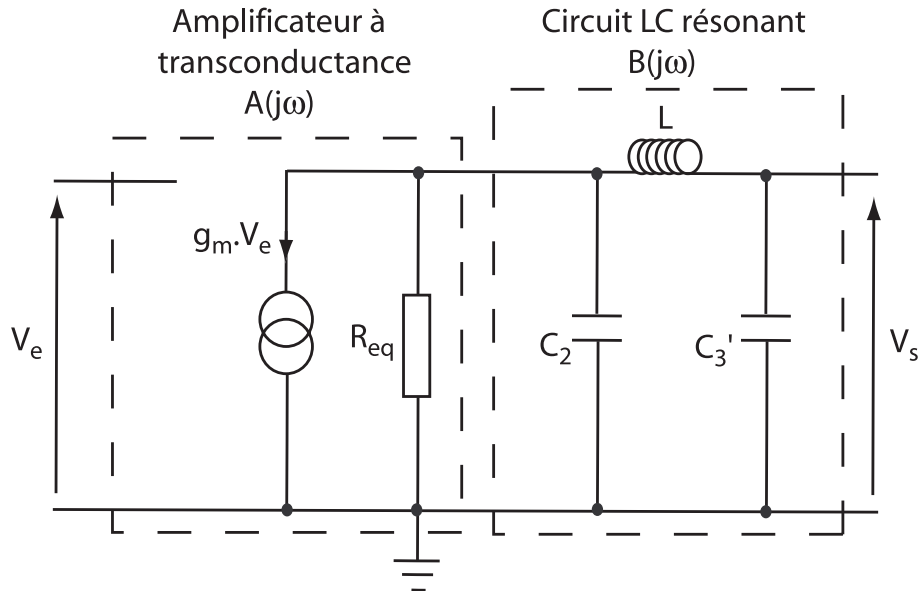


FIG. 1.4 – Principe de l'oscillateur Colpitts en boucle ouverte

La décharge des condensateurs induit un courant i dans le circuit résonant. Ce courant induit la magnétisation de la self. L'énergie électrostatique du condensateur est convertie en énergie magnétique dans la self. Une fois la self magnétisée et les condensateurs

déchargés, le courant s'inverse. L'échange d'énergie se produit alors de la self vers le condensateur, et le système revient à l'état de départ. Grâce à ce circuit résonant, nous remarquons que la condition de phase est automatiquement respectée. Les tensions aux bornes des deux condensateurs sont en opposition de phase :

$$\arg(v_{C_2}) - \arg(v_{C_3}) = \pi \quad (1.4)$$

La figure 1.4 permet de simplifier le calcul du gain en boucle ouverte. L'impédance d'entrée du FET est essentiellement capacitive, cette capacité d'entrée C_e est incluse dans $C'_3 = C_3 + C_e$. La résistance R_{eq} correspond à la résistance R_D et la résistance de sortie du FET. Cette résistance est supposée très supérieure à l'impédance du condensateur C_3 . Ainsi, le gain de l'oscillateur en boucle ouverte $G(\omega) = V_s/V_e$ est :

$$G(j\omega) = \frac{-g_m R_{eq}}{(-L C'_3 \omega^2 + 1) + j R_{eq} [(C_2 + C'_3) \omega - L C_2 C'_3 \omega^3]} \quad (1.5)$$

En annulant la partie imaginaire de l'équation (1.5), nous pouvons extraire la fréquence d'oscillation :

$$\Im[G(\omega)] = 0 \Rightarrow \omega_{osc} = \sqrt{\frac{1}{L} \left(\frac{1}{C_2} + \frac{1}{C'_3} \right)} \quad (1.6)$$

La fréquence d'oscillation est bien la fréquence d'accord de la self accordée par les deux condensateurs en série. En définissant la valeur du gain à la fréquence d'oscillation, nous pouvons obtenir le gain qui est la condition limite d'oscillation :

$$G(\omega_{osc}) = \Re(G(\omega_{osc})) = \frac{g_m R_{eq} C_2}{C'_3} \geq 1 \quad (1.7)$$

Il faut bien noter que ce résultat ne donne aucune information sur l'amplitude du signal fourni. Il est, en pratique, complètement irréaliste. En effet, cette amplitude ne peut être limitée que par les non-linéarités des composants : un oscillateur est nécessairement non linéaire. Dans le cas général, le calcul exact du comportement du circuit est très difficile. Une solution approchée est possible lorsque le circuit résonant $B(j\omega)$ est un passe-bande très sélectif. Il s'agit, dans ce cas là, d'appliquer la méthode dite du premier harmonique.

Si l'amplificateur reçoit à son entrée un signal sinusoïdal d'amplitude $v_1 = a \cos(\omega t)$, il délivre en sortie un signal $v_2 = \sum_{n=0}^{\infty} b_n \cos(\omega_n t + \varphi_n)$.

Pour une faible amplitude du signal v_1 , le signal v_2 se limite à son fondamental ($b_n = 0$ pour $n \geq 2$) et le quotient des nombres complexes associés $G = b/a e^{j\varphi}$ est le gain de l'amplificateur.

Lorsque l'amplitude du signal d'entrée est élevée, des harmoniques s'ajoutent au fondamental du signal de sortie engendrant un taux de distorsion assez important. Le premier

terme, qui est le fondamental, est souvent appelé premier harmonique. Le gain au premier harmonique peut alors être défini :

$$A_1 = \frac{b_1}{a} e^{j\varphi_1} \quad (1.8)$$

Lorsque le niveau du signal d'entrée augmente, le signal de sortie se rapproche de plus en plus d'un signal rectangulaire dont l'amplitude b_1 du fondamental n'augmente plus. Le gain au premier harmonique diminue donc de plus en plus. Cette notion peut être appliquée aux oscillateurs si le circuit de contre-réaction ($B(j\omega)$ dans notre cas) est suffisamment sélectif.

Dans le cas où v_1 est purement sinusoïdal, le premier harmonique en sortie de l'amplificateur a comme amplitude complexe $[A_1(a, \omega) a]$. Cette composante est la seule qui soit amplifiée par le circuit de réaction qui est passif, donc linéaire, et de gain $\beta(\omega)$. Le signal à sa sortie est $a A_1(a, \omega) \beta(\omega) = a$. La condition d'oscillation s'écrit donc :

$$A_1(a, \omega) \beta(\omega) \equiv 1 \quad (1.9)$$

Cette méthode ne donne de bons résultats que si le quadripôle de réaction est très sélectif et, est finalement d'un intérêt limité.

1.2.2 Influence d'un retard dans une boucle d'oscillation

Nous allons maintenant observer l'influence d'un retard que nous allons placer dans la boucle oscillante. Cet oscillateur est composé d'un filtre passe-bande sélectif (du second ordre, avec des constantes de temps τ_1 et τ_2 associée respectivement aux fréquences de coupure basse et haute) et d'un retard T placés en boucle fermée.

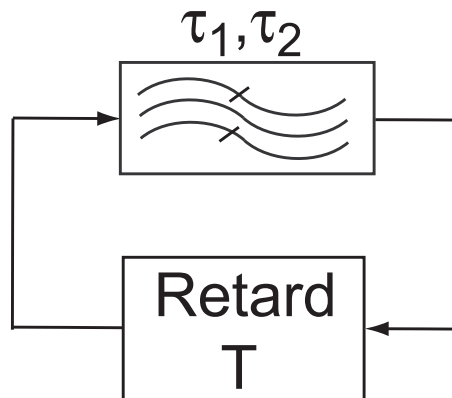
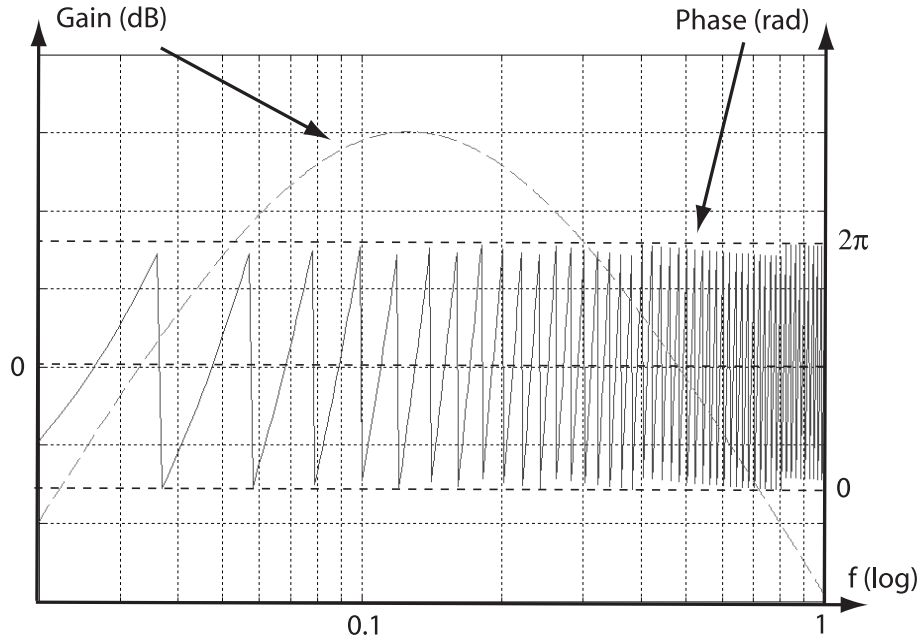


FIG. 1.5 – Synoptique d'un oscillateur harmonique à retard

Le retard dans une boucle d'oscillation va permettre d'introduire un déphasage supplémentaire qui est proportionnel à la valeur de la fréquence angulaire.

FIG. 1.6 – Conditions de gain et de phase d'un oscillateur à retard ($T = 10 \tau_2$)

Ainsi, le condition de phase suit la relation suivante :

$$\arctan \left[\frac{1 - \tau_1 \tau_2 \omega^2}{(\tau_1 + \tau_2) \omega} \right] + \omega T = 2k\pi \quad (1.10)$$

avec $k \in \mathbb{N}$. Le nombre de solution de l'équation précédente est infinie et c'est la condition de gain qui va permettre de limiter le nombre de fréquences d'oscillation (fig.1.6). Toutefois, les solutions et la condition de phase sont très denses sur l'axe des pulsations si le retard est important. Un filtrage extrêmement sélectif est alors nécessaire pour forcer une oscillation monomode.

Le retard temporel est un élément indispensable à la génération de signaux hyperchaotiques. Ce décalage temporel va entraîner un effet du passé «lointain» sur la prédiction du futur «proche» . L'un des phénomènes typiques causé par le retard, notamment dans les asservissements, est l'apparition d'oscillations amorties ou entretenues à l'origine de l'instabilité du système [7]. Un retard provoque, en effet, un fort déphasage, qui est une cause importante d'instabilité dans les systèmes bouclés.

Nous allons sommairement rappeler le problème du retard dans les systèmes de contrôle ou simplement dans les systèmes électroniques connus qui sont à l'origine stable.

Beaucoup de systèmes réels présentent un retard entre l'entrée et la sortie, comme par exemple les systèmes asservis (fig.1.7). La fonction de transfert entre l'entrée et la sortie est analytiquement simple dans le domaine de Laplace :

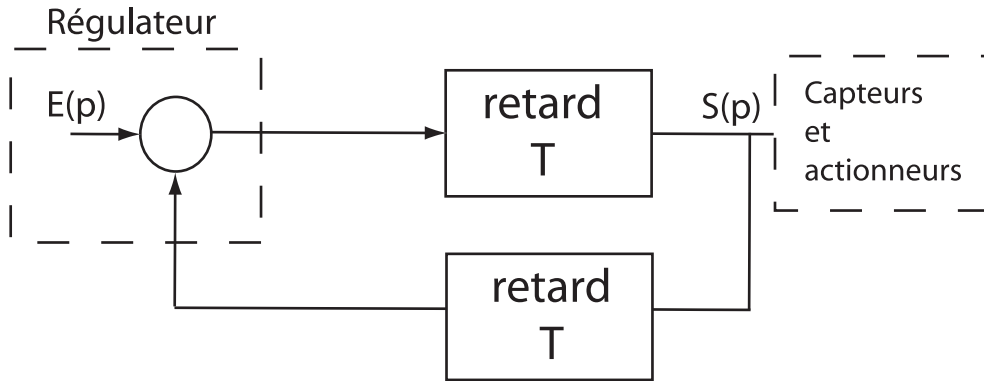


FIG. 1.7 – Le retard dans un système d'asservissement

$$H(p) = \frac{S(p)}{E(p)} = \frac{G e^{-Tp}}{1 + G e^{-2Tp}} \quad (1.11)$$

où T correspond au retard de transmission entre l'entrée et la sortie, et entre la sortie et l'entrée dans le retour de la boucle. Cette fonction de transfert pose quelques problèmes techniques car elle est d'ordre infinie. Elle possède donc une infinité de pôles et, par conséquent, est susceptible de conduire, en boucle fermée, à un comportement instable. L'instabilité est fonction du gain G . En effet, la fonction de transfert précédente deviendra instable pour $G \geq 1$.

Les oscillateurs à retard sont l'une des applications où les instabilités engendrées par un retard sont exploitées.

1.3 Systèmes et comportements fortement non linéaires

Tous les oscillateurs, même ceux en régime harmonique, sont en fait intrinsèquement non linéaires en régime permanent. Seules les conditions de démarrage de leurs oscillations sont linéaires (faibles amplitudes).

1.3.1 Stabilisation de l'amplitude des oscillations ou apparition de non-linéarités

Dans l'exemple du pont de Wien (fig.1.3(b)), la stabilisation des oscillations par écrêtage produit un signal de sortie avec un taux de distorsion important. Pour réduire la distorsion, une non-linéarité est introduite dans le système pour stabiliser le signal avant saturation de l'amplificateur opérationnel. L'effet non linéaire intervient au niveau d'une augmentation ou d'une réduction du gain (variation de la résistance globale de contre-réaction). Ces méthodes de contrôle de l'amplitude des oscillations sont principalement appliquées aux oscillateurs à amplificateurs opérationnels.

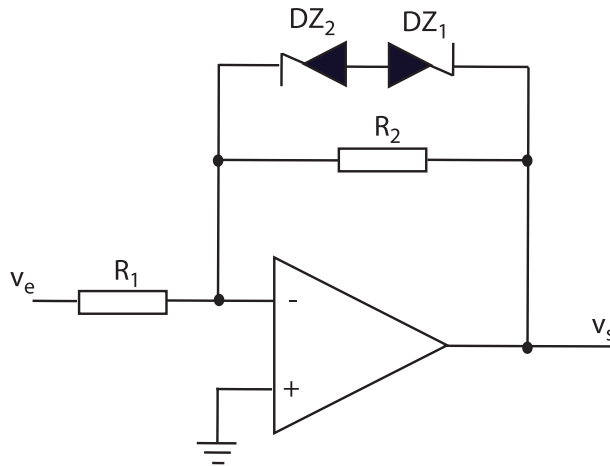


FIG. 1.8 – Amplificateur opérationnel mis en régime non linéaire par diodes zener

1.3.2 Quelques phénomènes non linéaires

Un système est qualifié de non linéaire s'il n'obéit pas au principe de superposition. Cette définition est large et autorise de ce fait un grand nombre de comportements non linéaires comme :

- les systèmes paramétriques dont la fonction de transfert est fonction du signal (cas des circuits contenant une thermistance ou un varactor)
- Les systèmes à hystérésis, type relais ou trigger de Schmitt. L'analyse de leur performance en présence de bruit est relativement compliquée.
- Les systèmes à non-linéarités indépendantes du temps, type $y = f(x)$.

Il s'agit du dernier type de non-linéarité qui nous intéresse. Cette non-linéarité indépendante du temps est vulgairement appelé système amnésique. Mathématiquement, elle est de la forme suivante :

$$\begin{cases} x = (x_1, x_2, \dots, x_i) \\ F(x) = (f_1(x_1, x_2, \dots, x_i), f_2(x_1, x_2, \dots, x_i), \dots, f_i(x_1, x_2, \dots, x_i)) \end{cases} \quad (1.12)$$

Il existe beaucoup de phénomènes dynamiques non linéaires en physique comme, par exemple, les oscillations anharmoniques du pendule pesant en mécanique, les mouvements de convection dans les fluides...

En électronique, certains composants bien connus sont intrinsèquement non linéaires comme la diode (fig.1.9(c)), qui est utilisée pour le redressement ou dans les amplificateurs logarithmiques.

Les amplificateurs opérationnels présentent également des non-linéarités comme la saturation (fig.1.9(a)) et le slew-rate (fig.1.9(b)).

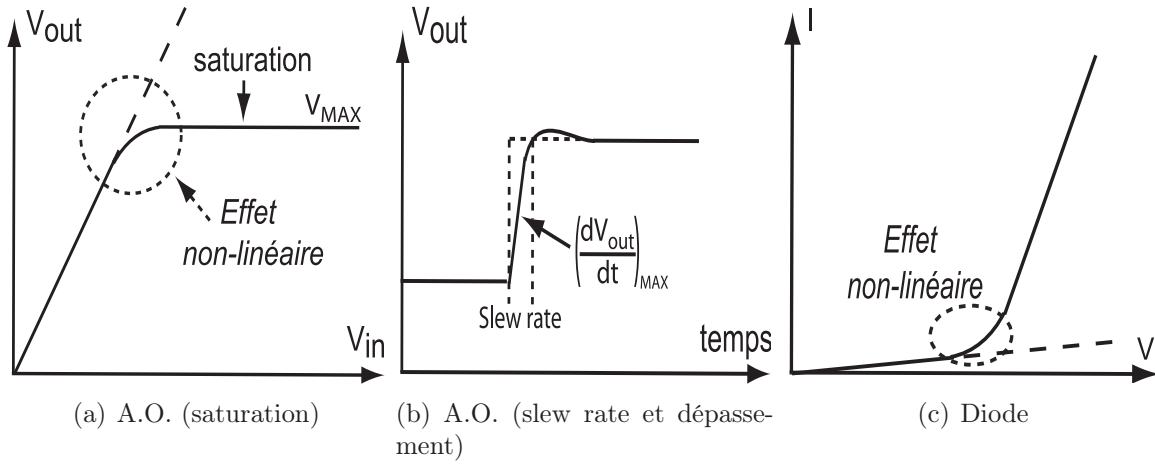


FIG. 1.9 – non-linéarité de certains composants électroniques

Mathématiquement, la fonction $I = f(V)$ d'une diode (fig.1.9(c)) se définit par la relation suivante :

$$I = I_0 \exp(\alpha V - 1) \quad (1.13)$$

où $\alpha = e/(n k_B T)$ est une constante faisant intervenir «le facteur d'idéalité» n de la diode, la constante de Boltzmann, et la température. Si on se limite aux petits signaux, un développement de Taylor est possible en V :

$$I \approx I_0 \left(\alpha V + \frac{\alpha^2 V^2}{2!} + \dots \right) \quad (1.14)$$

En général, on peut limiter le développement jusqu'à un certain ordre, les termes d'ordre supérieur étant négligeables pour les valeurs effectives de α et de l'amplitude de V .

Les oscillateurs comme l'oscillateur de Van der Pol et l'oscillateur anharmonique ont un fonctionnement basé sur un tel comportement non linéaire.

1.3.3 Oscillateur de Chua

Ce type d'oscillateur reste théoriquement très stable mais en pratique, lorsque l'on recherche une solution oscillante croissante, le système atteint rapidement une limite de stabilité introduite par la non-linéarité des composants (le phénomène de saturation est un exemple). Par conséquent, en introduisant un composant non linéaire sur la plage d'utilisation de la variable électrique, nous arrivons à la description du circuit de Chua [8].

L'une des raisons qui expliquent la popularité du circuit de Chua (fig.1.10(a)) est sa simplicité et sa capacité à générer une large variété de dynamiques complexes. En effet,

l'ensemble de ces évolutions est décrit mathématiquement par une équation différentielle linéaire par morceaux, à 3 dimensions [9].

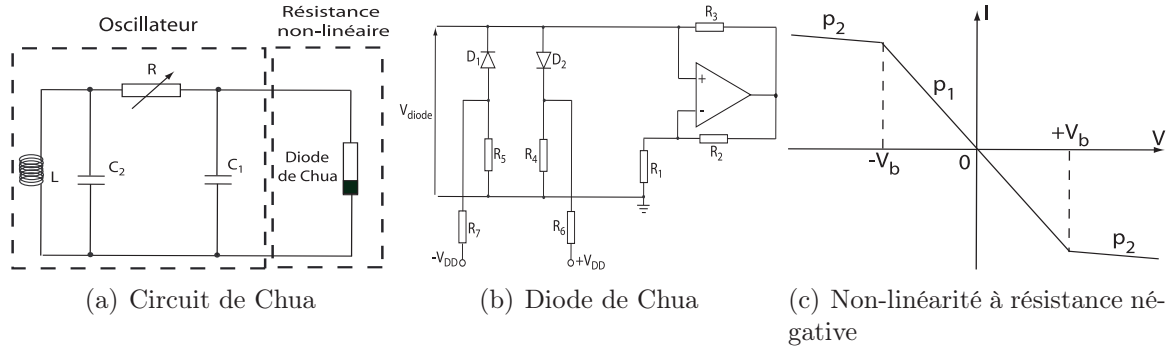


FIG. 1.10 – Oscillateur chaotique de Chua

La non-linéarité est réalisée par une diode de Chua. Cette oscillateur chaotique génère un chaos de basse dimension qui peut être facilement interprétable mathématiquement (1.15).

$$\begin{cases} C_1 \frac{dV_{C1}}{dt} = R^{-1} (V_{C2} - V_{C1}) - f(V_{C1}) \\ C_2 \frac{dV_{C2}}{dt} = R^{-1} (V_{C1} - V_{C2}) + I_L \\ L \frac{dI_L}{dt} = V_{C2} \end{cases} \quad (1.15)$$

où la non-linéarité $f(V_{C1})$ est la description mathématique du comportement de la résistance négative introduit par le circuit, et est appelée communément diode de Chua (fig.1.10(b)) :

$$f(V_{C1}) = p_2 V_{C1} + \frac{1}{2}(p_2 - p_1)[|V_{C1} + V_b| - |V_{C1} - V_b|] \quad (1.16)$$

p_1 et p_2 sont les pentes de la non-linéarité (fig.1.10(c)).

Le signal chaotique généré par cet oscillateur peut être mathématiquement interprété et prouve ainsi le déterminisme de l'ensemble des variations des courants et tensions présents dans le circuit électronique.

Toutefois, le signal chaotique généré par l'oscillateur de Chua est de petite dimension (< 3). En effet, les notions de dimension et de complexité dans cet oscillateur interviennent à de faibles degrés. La dimension du signal chaotique augmentera de manière significative dans les dynamiques à retard.

1.3.4 Dynamique non linéaire à retard

Notre préoccupation est ici de trouver un système permettant de générer un chaos de grande dimension. Il s'agit des systèmes hyperchaotiques (dimension de l'espace des phases supérieure à 3). Un oscillateur de ce type fut imaginé par Ikeda à la fin des années 1970 [10]. Il s'agit d'un système optique (fig.1.11).

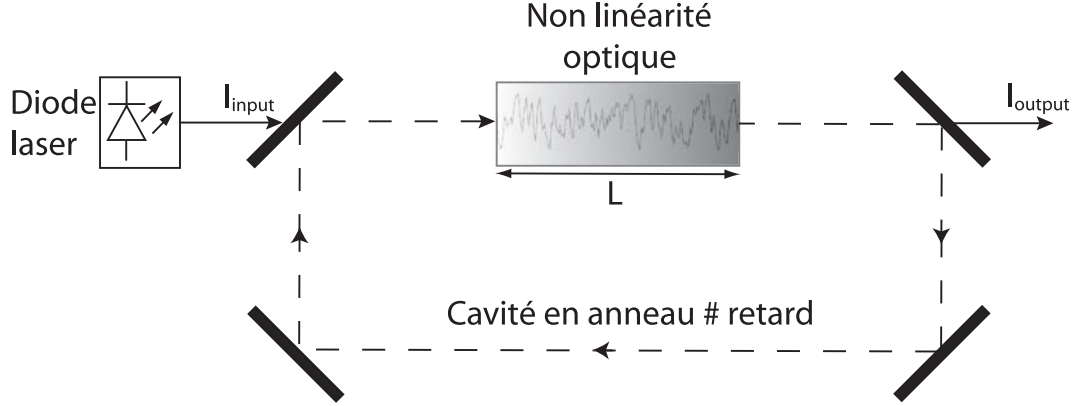


FIG. 1.11 – Système d'Ikeda

Cet oscillateur optique permet de générer un chaos de grande dimension par rapport aux systèmes non linéaires dont le retard temporel était négligeable.

$$\tau \frac{d\phi}{dt}(t) + \phi(t) = \phi_{NL}(t) \quad (1.17)$$

où τ est la constante de temps du système, et $\phi(t)$ la variable dynamique du système qui correspond à la phase optique du faisceau de sortie. La fonction non linéaire $\phi_{NL}(t)$ est définie comme telle :

$$\begin{cases} \phi_{NL}(t) = n_2 I(t) \frac{L}{C} \omega \\ I(t) = |E(t)|^2 = |E_0 + E(t-T) e^{j\phi(t-T)}|^2 \end{cases} \quad (1.18)$$

Le retard est réalisé par la longueur de la cavité en anneau. Les valeurs de la constante de temps et du retard sont prises de façon à avoir $T \gg \tau$. L'équation différentielle non linéaire à retard (1.17) montre que le régime chaotique adopté par le système est déterministe.

Sur la base de cet exemple optique, nous pouvons proposer le synoptique plus général de générateur de chaos à retard, permettant d'observer une dynamique chaotique de grande dimension.

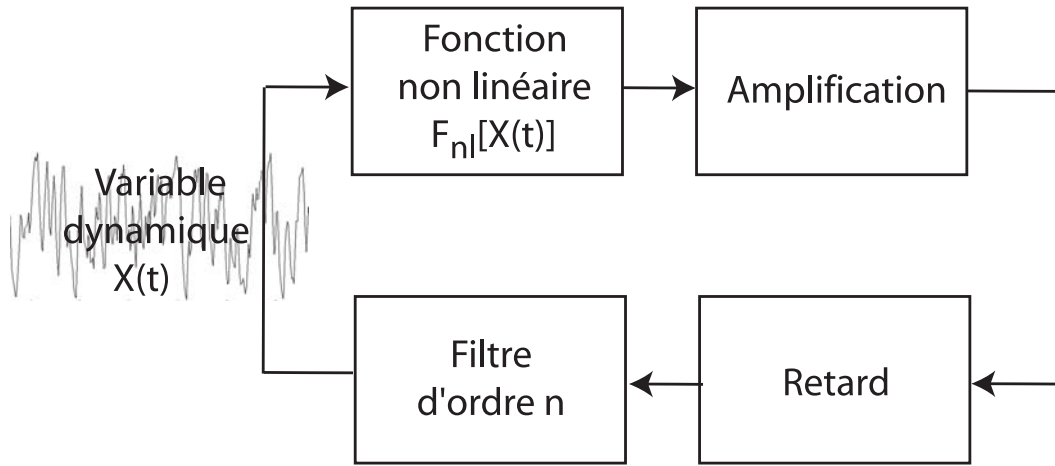


FIG. 1.12 – Système non linéaire à retard

Ce synoptique met en évidence les paramètres qu'il est nécessaire de connaître pour pouvoir analyser correctement le comportement chaotique de cet oscillateur. Il représente un oscillateur auto-entretenu qui est qualifié d'autonome.

Influence des paramètres non linéaires sur la stabilité du système

Les explications suivantes constituent une analyse préliminaire de stabilité, qui sera développée plus en détails dans les paragraphes 1.4.4 et 1.4.5 traitant des phénomènes de bifurcation. En effet, dans une première approche simplificatrice, la dynamique (1.17) et (1.18) peut également se décrire en utilisant la relation itérative suivante :

$$X_{i+1} = \beta \cdot \cos(X_i + \Phi) \quad (1.19)$$

Plusieurs types de points fixes peuvent être mis en évidence. Pour déterminer les points fixes de la non-linéarité, nous traçons sur un même graphique la fonction non linéaire et la première bissectrice ($Y = X$). Les points fixes sont mathématiquement définis comme les solutions de l'équation $X = F_{NL}[X]$. Ces valeurs sont les intersections entre la première bissectrice et la fonction non linéaire. Cinq points fixes se trouvent sur la figure 1.13, nous avons distingué trois types de points fixes A , B et C . Après avoir choisi arbitrairement une condition initiale, nous allons tracer alternativement une ligne verticale qui intercepte la fonction non linéaire puis une droite horizontale qui intercepte la bissectrice. Cette démarche est répétée plusieurs fois pour donner la figure 1.13 à gauche, où apparaissent les itérés successifs de la dynamique discrète.

Un grand nombre d'itérations est nécessaire pour que les segments horizontaux et verticaux convergent vers une valeur finale qui se confond avec le point fixe A . Ce point fixe est de type stable à convergence spirale. La pente de la droite asymptotique à ce point

fixe vaut $-1 < \text{pente} < 0$.

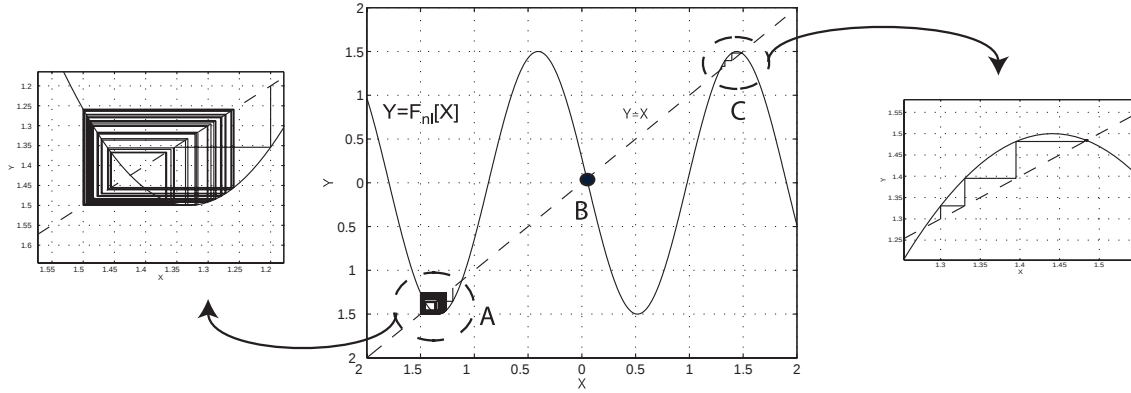


FIG. 1.13 – Différents types de point fixe

Le point fixe noté C est également un point fixe stable. La pente de la droite asymptotique de ce point est beaucoup plus faible que la précédente (le point fixe est relativement proche de l'extremum de la fonction non linéaire) et la convergence spirale ne s'observe de ce fait que pour de très faibles amplitudes.

Le troisième point noté B est totalement différent des deux premiers. Il s'agit d'un point fixe instable à divergence spirale. La pente de la fonction non linéaire pour ce point fixe est supérieure en valeur absolue à celle de la première bissectrice ($\text{pente} < -1$) [11].

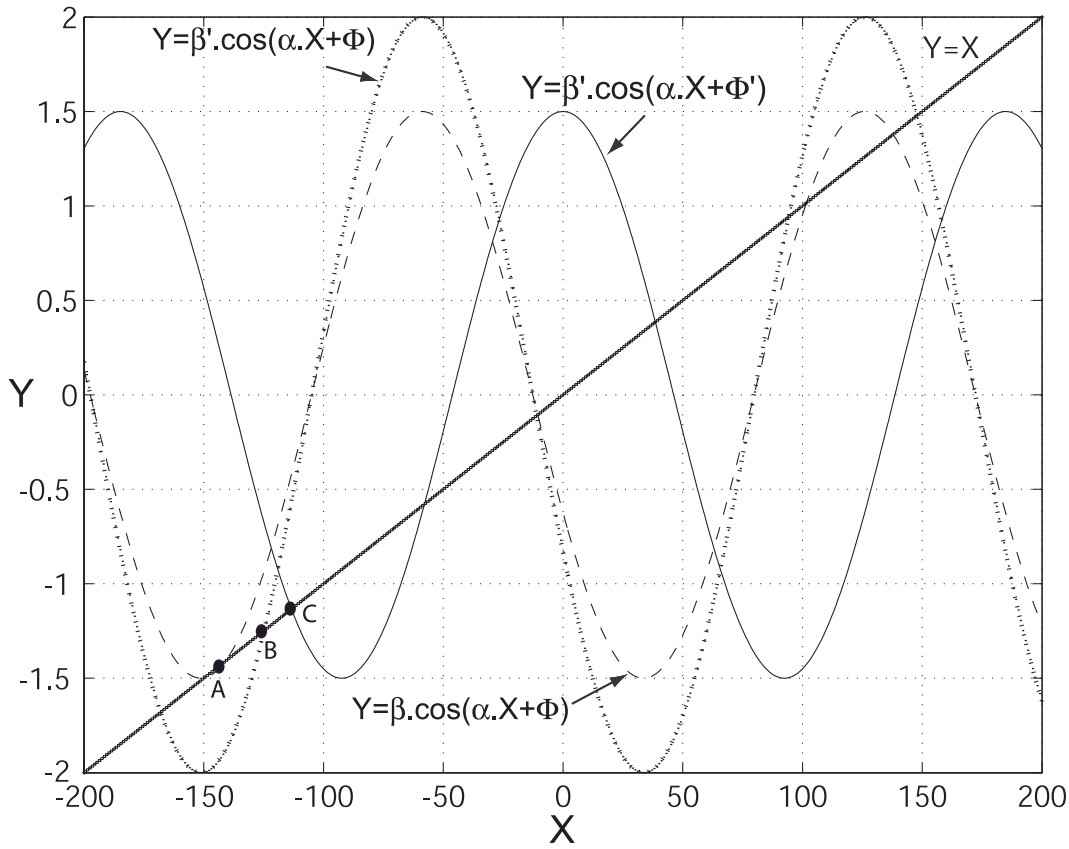
Intuitivement, nous savons que la pente de la droite asymptotique qui va définir la stabilité du système est liée au déphasage Φ et l'amplitude appelée β (fig.1.14).

En effet, les points A , B et C montrent très bien l'influence que peuvent avoir le déphasage Φ et l'amplitude β . Les pentes des droites asymptotiques des points A , B et C sont différentes et entraînent des réactions différentes lorsque le système est soumis à une éventuelle perturbation.

- β est le gain global observé dans la boucle. Il est normal de penser que la stabilité du système sera plus ou moins grande suivant la valeur du gain comme pour la plupart des oscillateurs décrits dans la première partie, qu'ils soient linéaires ou non linéaires.
- Φ est le déphasage de cette non-linéarité. Pour des variations de celui-ci, la non-linéarité va glisser suivant l'axe des abscisses. De ce fait, les intersections entre la courbe non linéaire et la première bissectrice seront situées sur une pente de valeur différente entraînant un type de dynamique différent.

Le tableau 1.1 résume pour la valeur de la dérivée de la fonction non linéaire au point fixe, les types de stabilité locale auxquels nous pouvons être confrontés.

Un nœud et un point fixe sont différents par le signe de la dérivée de la fonction non linéaire au point fixe initial. Ensuite la valeur absolue de cette dernière définira le critère

FIG. 1.14 – Fonction non linéaire pour différents Φ et β

Type de stabilité	Valeur de $F_{NL}[X_F]$
point fixe stable	$0 < F_{NL}[X_F] < 1$
point fixe instable	$F_{NL}[X_F] > +1$
nœud stable	$-1 < F_{NL}[X_F] < 0$
nœud instable	$F_{NL}[X_F] < -1$

TAB. 1.1 – Type de stabilité d'une fonction non linéaire

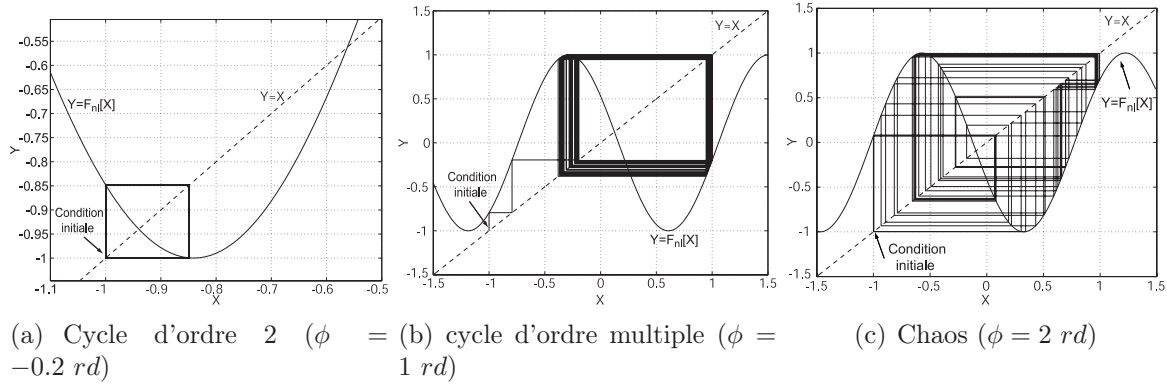
de stabilité.

Dans le cas d'un point fixe instable, il se pose naturellement la question du régime dynamique asymptotique que peut adopter le système (1.19).

Après plusieurs itérations permettant d'éliminer les phénomènes transitoires, nous pourrions observer si le régime du système est stationnaire, périodique ou chaotique [12].

La figure 1.15(a) représente temporellement une évolution périodique. Celle-ci peut être assimilée à l'état adopté par le système après une bifurcation de Hopf³ (voir les parties 1.4.4 et 1.4.5 page 31). En effet, les différentes itérations vont rejoindre successivement deux valeurs. Il s'agit d'un cycle d'ordre 2.

³changement de stabilité d'un point fixe lors de l'évolution d'un paramètre du système dynamique, et

FIG. 1.15 – Type de cycle pour différentes valeurs de déphasage ϕ

La figure 1.15(b) adopte le même principe. Cependant, les itérations ne semblent pas se répéter au bout de deux étapes, et le cycle est maintenant d'ordre n . Cette valeur n caractérise le nombre d'itération de la fonction non linéaire nécessaires pour retrouver la valeur du départ du cycle.

Enfin, la figure 1.15(c) représente une solution chaotique. Les différentes itérations couvrent de manière dense l'ensemble de la région de l'intervalle $[-1; 1]$.

Influence du nombre d'extrema sur la dimension du chaos

Le nombre d'extrema de la fonction non linéaire a une grande importance sur la dimension de la solution chaotique parcourue par la dynamique dans l'espace des phases [13].

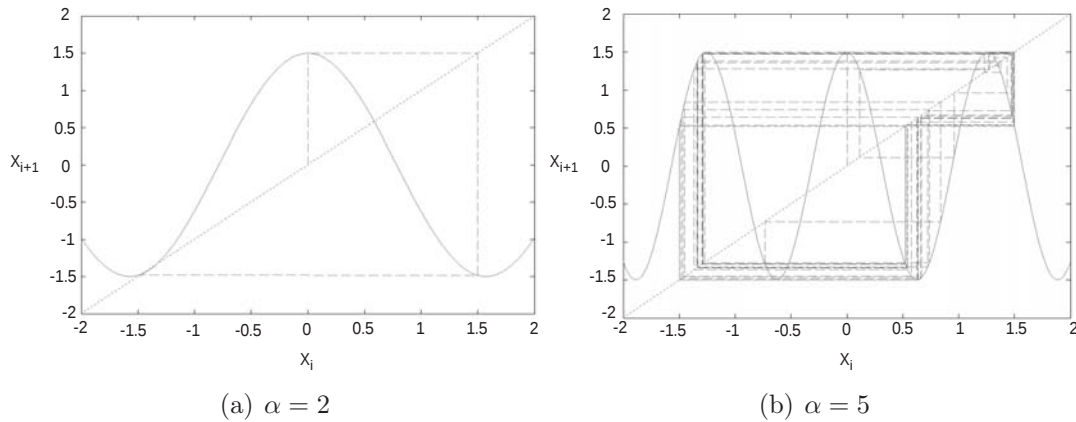


FIG. 1.16 – Comportement itératif pour différentes non-linéarités

En s'inspirant de l'équation (1.19), la figure (1.16) montre la fonction non linéaire pour le même déphasage et la même amplitude mais pour un facteur multiplicatif α différent

apparition d'une solution cyclique

de façon à augmenter ou diminuer le nombre d'extrema de la fonction non linéaire dans la fenêtre visualisée. Le point initial des itérations est également le même ($X_0 = 0$). La plage de variation est très différente suivant la valeur de α . Intuitivement, on peut comprendre qu'un plus grand nombre d'extrema augmente la complexité, car une même valeur peut avoir beaucoup plus d'antécédents possibles.

Du temps discret au temps continu

Comme nous avons pu le voir dans la partie décrivant l'influence de la fonction non linéaire, l'évolution de la trajectoire au niveau de l'élément non linéaire est traduit par une fonction itérative qui peut être schématiquement représentée par la figure 1.17(a).

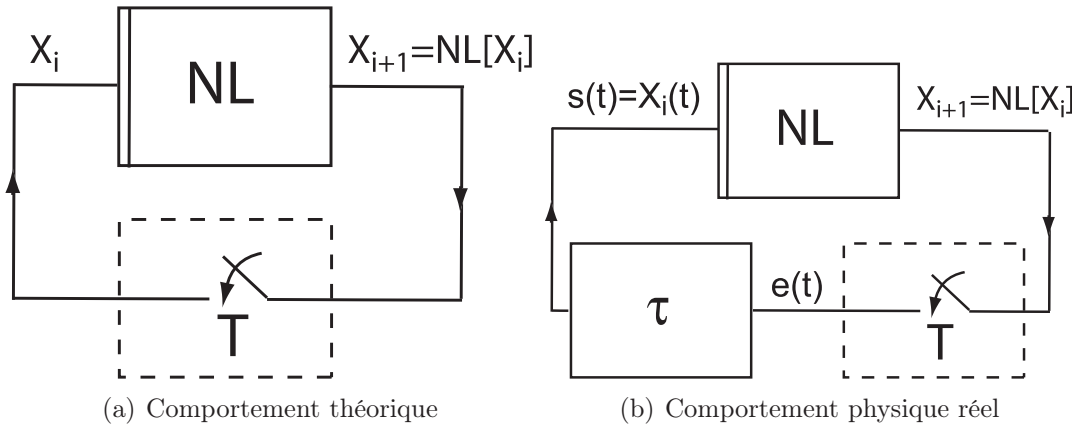


FIG. 1.17 – Modélisation de la boucle itérative

Cependant, il faut savoir que la boucle, en réalité, possède des éléments avec une bande passante limitée (contrairement à la non linéarité par exemple, qui est amnésique et instantanée). Il est donc nécessaire d'introduire une bande passante (fig.1.17(b)) dont la constante de temps τ aura une influence sur la dynamique de transition des X_i observés (fig.1.18, passage de X_i à X_{i+1}).

Suivant le type de filtrage effectué, l'évolution chaotique aura des caractéristiques différentes. Voici les équations différentielles permettant de caractériser deux types de filtres : un filtre passe-bas (1.20) et un filtre passe-bande (1.21).

$$\tau \frac{ds}{dt}(t) + s(t) = e(t) \quad (1.20)$$

Dans l'ensemble des applications qui suivent, c'est un filtre passe-bande qui sera utilisé pour la modélisation du fonctionnement du système.

$$\tau_1 \cdot \tau_2 \cdot \frac{d^2s}{dt^2}(t) + (\tau_1 + \tau_2) \frac{ds}{dt}(t) + s(t) = (\tau_1 + \tau_2) \frac{de}{dt}(t) \quad (1.21)$$

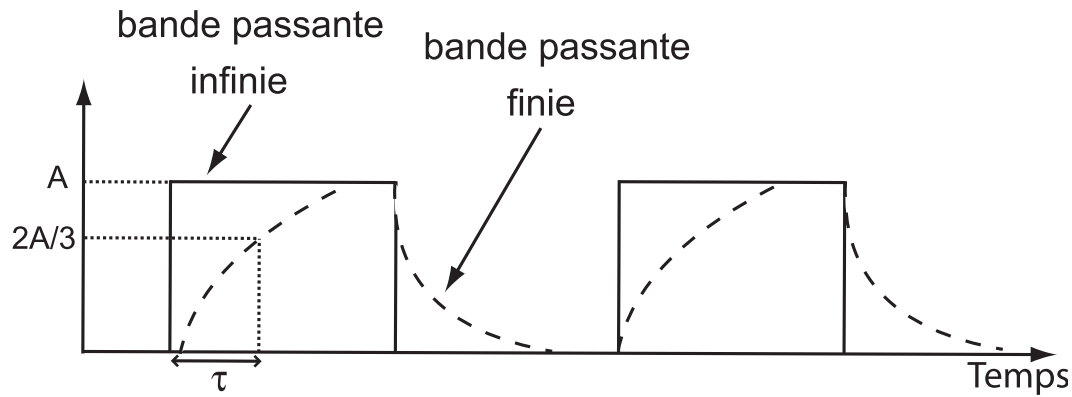


FIG. 1.18 – Evolution avec et sans constante de temps dans le système

Les constantes de temps haute et basse du système ont une grande influence sur la dimension du chaos généré. Ces valeurs sont liées à la valeur du retard décrit par la suite. En effet, l'oscillateur chaotique fonctionnera correctement si l'ensemble des conditions suivantes sont respectées :

- Une non-linéarité ayant un nombre d'extrema et une amplitude suffisante
- une boucle de rétroaction permettant l'auto-entretien des oscillations (périodiques ou chaotiques)
- Un retard temporel supérieur à la constante de temps la plus rapide du système ($T \gg \tau$). Il est toutefois nécessaire de remarquer que cette condition n'est pas indispensable dans le sens où, si $T < \tau$, le système pourrait quand même osciller pour des valeurs de gains très importantes et seulement dans certains cas particulier [14, 15].

1.4 Outils et techniques de caractérisation de comportements non linéaires

A partir d'un système dynamique non linéaire, nous avons pour objectif d'obtenir un comportement chaotique de qualité, robuste, et capable de masquer correctement une information à transmettre. L'identification de ces propriétés requiert un certain nombre d'outils à même de les mesurer, à partir de l'observation d'un comportement de l'oscillateur non linéaire. Ce sont ces outils que nous allons tenter de décrire maintenant. Certains sont déjà bien connus en traitement du signal (analyse statistique, analyse fréquentielle), et d'autres seront plus spécifiquement issus du domaine des dynamiques non linéaires (espace des phases, diagrammes de bifurcation, exposants de Lyapunov).

1.4.1 Analyse statistique : quelques définitions

Il existe des modèles statistiques qui caractérisent bien les signaux aléatoires et de ce fait les signaux pseudo-aléatoires. Les signaux chaotiques que nous cherchons à obtenir devront préférentiellement présenter une signature statistique aussi proche que possible de celle d'un vrai bruit. Dans cet ordre d'idée, nous pouvons remarquer que les signaux Gaussiens, encore appelés signaux de Laplace-Gauss ou signaux normaux, sont probablement les plus importants d'un point de vue théorique et surtout d'un point de vue pratique, puisque de nombreuses applications justifient l'utilisation de cette distribution dans les phénomènes physiques [16].

le modèle Gaussien

En probabilité, le théorème de la limite centrale est un ensemble de résultats sur la convergence faible d'une suite de variables aléatoires. Intuitivement, d'après ces résultats, toute somme de variables aléatoires indépendantes et identiquement distribuées tend vers une certaine variable aléatoire. Le résultat le plus connu et le plus important est simplement appelé *théorème de la limite centrale*, d'après lequel, si la somme d'un grand nombre de variables aléatoires a une variance finie, alors elle suivra une loi normale. Comme la plupart des phénomènes physiques ont une variance finie, celle-ci est largement applicable et appliquée dans la réalité. Disposer d'une dynamique chaotique dont la statistique est de type Gaussienne (ou quasi-Gaussienne), pourra donc être considéré comme une caractéristique attractive pour les communications chaotiques sécurisées : l'analyse de la distribution statistique du chaos par un espion ne pourra donc pas lui donner d'information pertinente sur l'origine déterministe de ce chaos.

Par définition, on dit qu'une variable aléatoire f est Gaussienne ou normale, si sa densité de probabilité vaut :

$$p(f) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp \left\{ -\frac{(f - f_0)^2}{2\sigma^2} \right\} \quad (1.22)$$

où σ^2 est la variance et f_0 la valeur moyenne. Un exemple d'une variable Gaussienne est représenté sur la figure 1.19 dans le cas théorique d'une variable statistique correspondant à une fréquence autour de 1 GHz, avec différents écarts types.

En l'absence de modulation, la seule fréquence émise est la fréquence centrale correspondant à f_0 . La fréquence centrale d'émission est la valeur pour laquelle est obtenue $p'(f) = 0$ puisqu'il s'agit de la valeur maximum du modèle Gaussien.

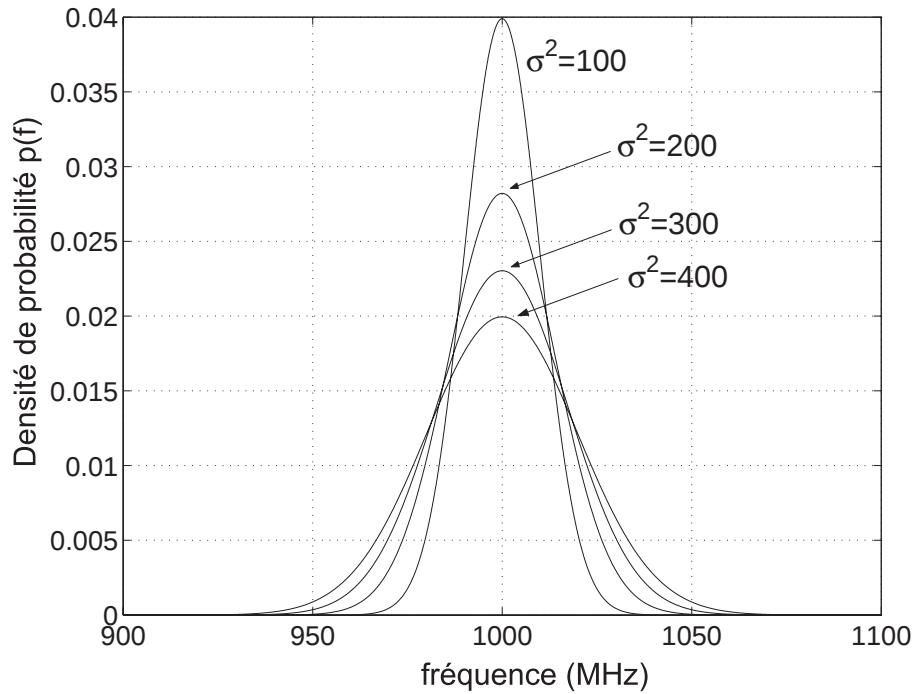


FIG. 1.19 – Modèle statistique gaussien pour $f_0 = 1 \text{ GHz}$, $100 < \sigma^2 < 400$

Représentation graphique dans les cas pratiques : l'histogramme

Il est important d'effectuer un petit rappel sur ce type de représentation graphique et comment celle-ci est obtenue. Les appareils de mesure et les résultats issus des simulations numériques utilisent le même procédé, car les valeurs de la variable statistique sont considérées dans la pratique comme appartenant à des intervalles en nombre fini, et non à une distribution continue comme dans (1.22).

Mathématiquement, nous pouvons définir une partition en m intervalles de I :

$$(I_1 = [b_1, b_2], \dots, I_j = [b_j, b_{j+1}], \dots, I_m = [b_m, b_{m+1}]) = I_j \quad (1.23)$$

avec $1 \leq j \leq m$. L'indice j est la classe permettant de désigner les valeurs appartenant à I_j . Elle est caractérisée par son amplitude $a_j = b_{j+1} - b_j$, le nombre d'observations n_j appartenant à cette classe, et la fréquence relative $f_j = n_j/n$.

De manière pratique, l'histogramme est obtenu en juxtaposant des rectangles dont la base est égale à l'intervalle de fréquence de la classe et dont la surface est égale à l'amplitude statistique de la classe. Nous pouvons donc facilement comprendre que l'interprétation visuelle est sensible à la surface du rectangle. Ainsi, le choix de la partition conduit à une représentation plus ou moins informative. L'histogramme pour deux valeurs d'échantillonnage différentes ($m = 50$ et $m = 1000$) est représenté sur la figure 1.20. L'am-

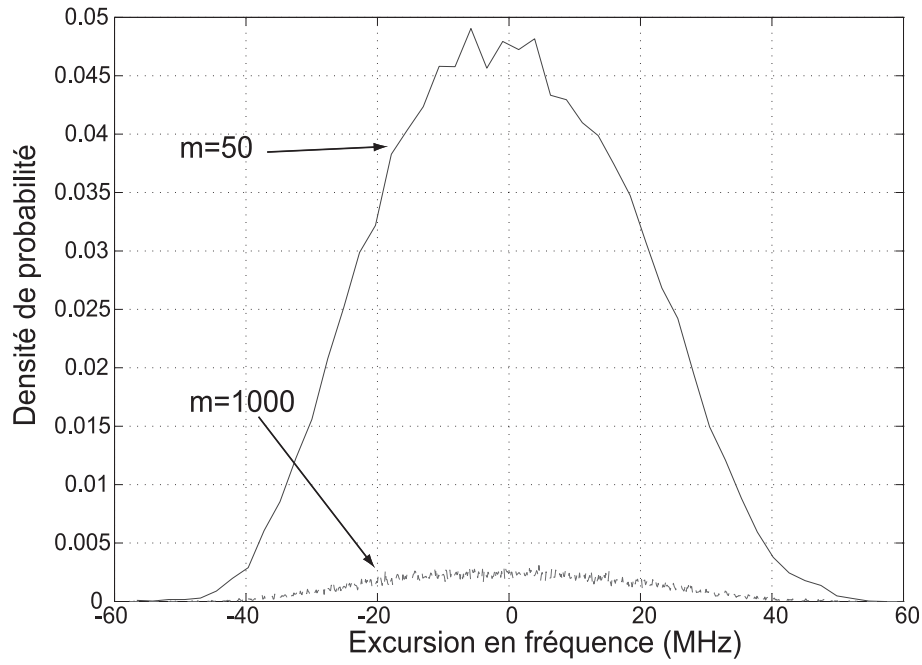


FIG. 1.20 – Histogramme pour 2 valeurs d'échantillonnage différentes ($m = 50$ et $m = 1000$)

plitude de chaque rectangle donnée par la relation f_j/a_j a une importance significative. Pour l'ensemble des mesures ou des simulations numériques qui suivront, cette valeur sera normalisée pour transformer le nombre d'échantillons en une densité spectrale.

1.4.2 Analyse dans le domaine fréquentiel

Un autre outil de caractérisation très classique en traitement du signal, et qui serait inévitablement utilisé par un espion pour l'analyse de la porteuse chaotique, concerne l'analyse spectrale. Cette méthode est utile pour caractériser tout type de signaux qu'ils soient d'origine linéaire ou non linéaire, de type périodique, quasi-périodique, pseudo-aléatoire ou encore complètement aléatoire (bruit blanc par exemple).

Analyse de Fourier

Le spectre en fréquence va nous permettre d'observer la manière dont se comporte une série temporelle [17]. En effet, le spectre d'un signal périodique ou quasi-périodique est constitué de raies discrètes correspondant aux fréquences et sous-harmoniques du système. En revanche, dans le cas d'un signal chaotique, on obtient un spectre continu. Ce spectre chaotique continu peut être de plus ou moins bonne qualité en terme de porteuse chaotique pour le cryptage, en fonction de la présence ou non de fréquences prépondérantes. L'identification de ces fréquences par un espion lors d'une analyse spectrale, peut

potentiellement constituer un trou de sécurité. Il est alors intéressant de travailler avec des porteuses chaotiques à équi-répartition des composantes spectrales.

Une technique fondamentale pour la représentation en fréquence consiste à décomposer le signal en une superposition de différentes fonctions. Pour un signal périodique, il s'agit d'une superposition d'ondes sinusoïdales de fréquences discrètes et multiples d'un même fondamental, que l'on peut reconstituer en connaissant les coefficients de Fourier :

$$x(t) = \frac{a_0}{2} + \sum_{n=1}^{+\infty} (a_n \cos n\omega t + b_n \sin n\omega t), \quad (1.24)$$

où a_0 , a_n et b_n sont les coefficients de Fourier calculables par une intégration du signal temporel sur une période.

Pour les phénomènes non-périodiques, il est nécessaire d'avoir recours à la transformée de Fourier. Cette méthode consiste à représenter le signal par une superposition d'ondes sinusoïdales dont les fréquences sont continûment distribuées. L'amplitude associée à chacune de ces fréquences forment alors une fonction complexe de la fréquence f appelée «spectre continu des fréquences du signal». Sa définition est donnée par :

$$X(\omega) = \int_{-\infty}^{+\infty} x(t) e^{-j\omega t} dt \quad (1.25)$$

Dans les cas pratiques, on se limite souvent à une version discrétisée de cette transformée de Fourier, dans l'espace des fréquences. On parle de transformée de Fourier discrète (1.26), que l'on obtient à partir d'une version échantillonnée avec un pas T_e $x_j | x_j = x(t = j T_e)_{j=1 \dots n}$, du signal d'origine en temps continu $x(t)$. Tous les appareils d'acquisition numérique des signaux fournissent, en général, ce spectre discrétisé, par l'intermédiaire d'un algorithme de calcul dit FFT (Fast Fourier Transform).

$$X \left(\omega = 2\pi \frac{k}{n T_e} \right) = X_k = \frac{1}{n} \sum_{j=1}^n x_j \cdot \exp \left[-i \frac{2\pi j k}{n} \right] \quad \text{avec } k = 1, \dots, n \quad (1.26)$$

L'analyse de Fourier, bien que très utilisée, présente quelques inconvénients. En effet, cette analyse donne une information globale et non locale dans le temps, ce qui présente un problème pour l'étude des signaux non stationnaires. Cette analyse ne permet pas de savoir à quels instants les fréquences ont été émises. De plus, l'étude des signaux dont la fréquence varie dans le temps nécessite la mise en place d'une analyse temps/fréquence qui permettra une localisation des périodicités dans le temps, et indiquera donc si la période varie d'une façon continue, ou si elle apparaît puis disparaît par la suite.

Rapprochement statistique : la densité spectrale

Un problème important dans de nombreuses applications est l'étude de la répartition en fréquences d'un signal aléatoire. En effet, le signal $x(t)$ a une transformée de Fourier $X(\omega)$ qu'on ne peut théoriquement pas calculer mais dont on peut trouver une estimation. On cherche à calculer la répartition de l'énergie du signal en fonction de la fréquence.

La densité spectrale de puissance d'un signal est la transformée de Fourier de la fonction d'autocorrélation (théorème de Wiener-Kintchine) [18] :

$$\phi_{xx}(f) = \sum_{n=-\infty}^{+\infty} R_{xx}(n) e^{-i.2\pi.n.f} \quad (1.27)$$

La fonction d'autocorrélation d'un signal aléatoire échantillonné x_i est :

$$R_{xx}(n) = E(x(i).x^*(i+n)) \quad (1.28)$$

Dans le cas de l'analyse d'un signal réel (par exemple échantillonné), la durée d'observation est nécessairement limitée et correspond à la plus grande possible (fonction de la mémoire disponible), de façon à prendre le plus de variations possibles du signal. La notion de densité spectrale d'un signal réel peut alors être remplacée par celle de la moyenne des densités spectrales obtenues sur plusieurs intervalles finis d'observations.

1.4.3 Espace des phases et types d'attracteurs

Un système dynamique non linéaire est potentiellement capable de donner lieu un grand nombre de solutions différentes, en fonction des valeurs des paramètres, ou encore des conditions initiales. L'espace des phases, encore appelé espace des états, est un outil permettant d'étudier qualitativement le type de solution obtenu. On observe alors l'évolution de l'état du système dans cet espace, dont chaque point correspond à un état unique. Par exemple, une solution qui passe deux fois par le même état correspond nécessairement un comportement périodique. La succession des états du système pour une solution donnée est appelée trajectoire.

Un attracteur dans cet espace est un objet géométrique vers lequel tendent un ensemble de trajectoires des points de l'espace des phases, c'est à dire une situation ou un ensemble de situations vers lesquelles évolue un système dynamique, pour un ensemble de conditions initiales. Le bassin d'attraction d'un attracteur est l'ensemble des points de l'espace des phases qui donnent une trajectoire évoluant vers l'attracteur considéré. On peut donc avoir plusieurs attracteurs dans un même espace des phases. Il existe deux types d'attracteurs : les attracteurs réguliers et les attracteurs étranges chaotiques. En effet, les attracteurs réguliers décrivent l'évolution de solutions non-chaotiques. Il s'agit par exemple de points fixes, de cycles limites ou encore de tores.

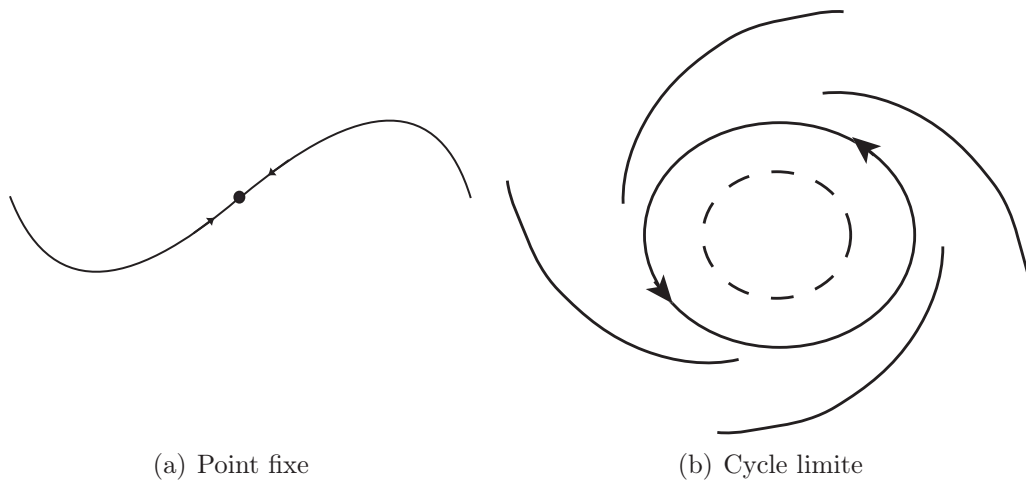


FIG. 1.21 – Deux exemples d'attracteurs réguliers dans un espace des phases 2D

Pour un point fixe stable, un écartement de sa position initiale dû à une quelconque perturbation n'aura aucune influence (fig.1.21(a)). Le système étant en général dissipatif, le mouvement perturbé s'atténuera pour faire revenir l'état du système à sa position initiale.

Le cycle limite sera caractéristique d'un mouvement périodique entretenu (apport d'énergie extérieure pour compenser la dissipation). Le système ne revient pas à une position initiale mais y repassera après avoir parcouru le cycle. Sa représentation graphique dans l'espace des phases (fig.1.21(b)) est une courbe fermée.

Les attracteurs étranges sont caractéristiques de l'évolution des systèmes chaotiques : au bout d'un certain temps, tous les points de l'espace des phases appartenant au bassin d'attraction de l'attracteur, donnent des trajectoires qui tendent à former l'attracteur étrange. A grande échelle, un attracteur étrange n'est pas une surface lisse, mais une surface repliée plusieurs fois sur elle-même. Les trajectoires de deux points voisins divergent rapidement sur un attracteur chaotique, mais comme l'attracteur a des dimensions finies (évolution bornée dans l'espace des phases), l'attracteur, donc l'ensemble de ses trajectoires, doit se replier sur lui-même. Ce processus caractéristique, appelé étirement-repliement se répète à l'infini et fait apparaître un nombre infini de plis imbriqués les uns dans les autres qui ne se recoupent jamais et qui permettent à un nombre infini de trajectoires de former le même attracteur. Ainsi, deux points très proches au départ (conditions initiales) peuvent se retrouver au bout d'un temps fini à deux extrémités opposées de l'attracteur.

L'interprétation graphique à partir des représentations des attracteurs de Hénon, Lorenz et Rössler dans l'espace des phases (fig.1.22) reste très parlant étant donnée la dimension très faible du chaos généré. Des structures étranges mais bien identifiées apparaissent

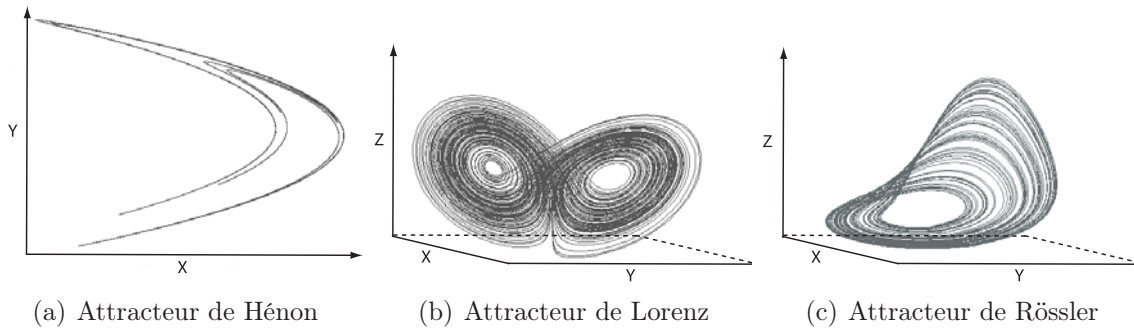


FIG. 1.22 – Attracteurs chaotiques « célèbres » dans leur espace des phases de basses dimensions (2D et 3D)

dans l'espace des phases.

Dans les systèmes hyperchaotiques dont la dimension de l'attracteur étrange est grande ($D \gg 3$), la représentation de l'espace des phases peut s'avérer extrêmement difficile, et un espion qui tenterait ce type d'analyse ne pourrait très probablement pas avoir accès à des informations pertinentes sur l'origine du chaos, si celui-ci est très complexe. Nous mettons ici en évidence l'intérêt de travailler dans un espace des phases de grandes dimensions, et dans lequel la trajectoire chaotique est très dense (grande complexité, faible structuration de l'attracteur).

1.4.4 Notions de bifurcation

Une dynamique non linéaire est, comme nous en avons déjà parlé, capable d'engendrer différents types de solution, en fonction de la valeur des paramètres, et ou de celles des conditions initiales. Lorsqu'on fait varier continûment un paramètre, il est possible d'observer une transition entre deux types de solution, en une valeur bien précise du paramètre. Cette valeur caractérise un point de bifurcation dans l'espace des paramètres. Une bifurcation correspond à un changement qualitatif du type de solution observé (et pas uniquement quantitatif).

Stabilité du point fixe

Par définition, la stabilité est le caractère de ce qui tend à demeurer dans le même état malgré de petites perturbations. Rapportée aux systèmes dynamiques, il s'agit de la solution du modèle mathématique du système. Lorsque le système non linéaire est soumis à une légère perturbation, celui-ci est confronté à deux situations : soit il revient vers son état initial, que l'on suppose être ici un point fixe, soit il le quitte pour rejoindre un autre régime dynamique.

Illustrons simplement l'influence d'une légère perturbation dans le cas d'un système

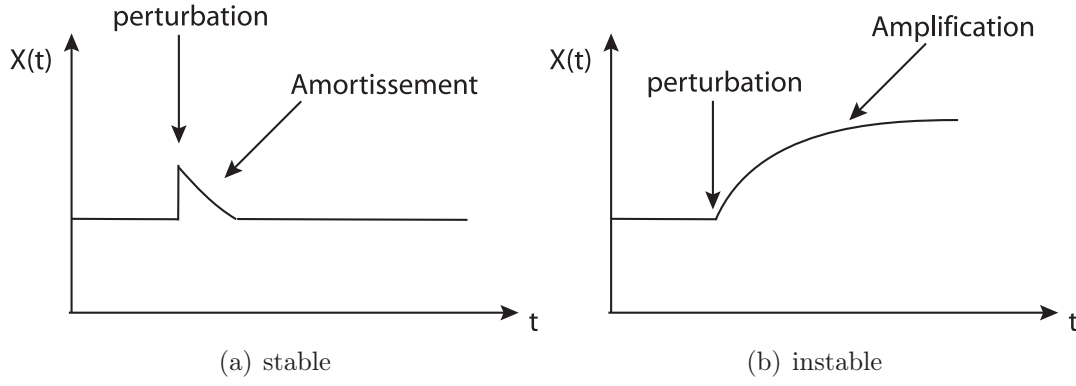


FIG. 1.23 – Type de points fixes

non linéaire à temps continu, à deux variables d'état (dimension 2), qui peut être décrit par deux équations couplées en X et Y :

$$\begin{cases} \frac{dX}{dt} = f(X, Y) \\ \frac{dY}{dt} = g(X, Y) \end{cases} \quad (1.29)$$

l'état stationnaire (X_s, Y_s) considéré ici est un point fixe, observé avant la perturbation (fig.1.23), et répondant à la condition suivante :

$$\begin{cases} \frac{dX_s}{dt} = f(X_s, Y_s) = 0 \\ \frac{dY_s}{dt} = g(X_s, Y_s) = 0 \end{cases} \quad (1.30)$$

Si cet état stationnaire est soumis à une légère perturbation telle que $X = X_s + x$ avec $x \ll X_s$ et $Y = Y_s + y$ avec $y \ll Y_s$, les fonctions non linéaires $f(X_s, Y_s)$ et $g(X_s, Y_s)$, peuvent être linéarisées à l'aide d'un développement de Taylor dont les termes d'ordre supérieur ou égal à 2 sont négligés :

$$\begin{cases} \frac{dX}{dt} = f(X, Y) = f(X_s, Y_s) + \left(\frac{\partial f}{\partial X} \right)_s x + \left(\frac{\partial f}{\partial Y} \right)_s y \\ \frac{dY}{dt} = g(X, Y) = g(X_s, Y_s) + \left(\frac{\partial g}{\partial X} \right)_s x + \left(\frac{\partial g}{\partial Y} \right)_s y \end{cases} \quad (1.31)$$

Ainsi, la matrice jacobienne J du système dynamique linéaire autour de $(X_s, Y_s) = M_s$ peut être définie par :

$$J = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \quad (1.32)$$

avec

$$a_{11} = \left(\frac{\partial f}{\partial X} \right)_{M_s}, \quad a_{12} = \left(\frac{\partial f}{\partial Y} \right)_{M_s}, \quad a_{21} = \left(\frac{\partial g}{\partial X} \right)_{M_s}, \quad a_{22} = \left(\frac{\partial g}{\partial Y} \right)_{M_s}$$

Le problème a donc été rapporté à un système dynamique linéaire classique, à deux dimensions. La stabilité se déduit tout aussi classiquement en cherchant les valeurs propres de la matrice jacobienne. Celles-ci peuvent être complexes. Alors, suivant la valeur positive ou négative de la partie réelle, on identifiera respectivement un point fixe instable ou stable. Le signe de la partie réelle dépend des paramètres du système dynamique. On comprend alors comment une bifurcation par perte de stabilité peut être induite lors de la variation d'un paramètre de bifurcation, qui correspond précisément à une valeur propre coupant l'axe imaginaire pour une valeur précise d'un paramètre. Lorsque le point fixe n'est plus stable, la solution dynamique observée change de nature, par exemple en devenant un cycle limite.

Le type de bifurcation décrit précédemment est un cas particulier puisque celui-ci concerne la perte de stabilité d'un point fixe caractéristique. Ce paragraphe a toutefois l'avantage de rappeler l'intérêt du calcul des exposants (valeurs propres de la matrice jacobienne) permettant d'observer l'écart ou le rapprochement des trajectoires après une perturbation. Ce calcul est également à la base du principe développé plus en détail dans la partie concernant les exposants de Lyapunov (paragraphe 1.4.6).

1.4.5 Les types de bifurcation et ses diagrammes

La variation de l'un des paramètres du système peut changer le type de régime dynamique observé. Le diagramme de bifurcation va permettre d'observer l'évolution de la solution dynamique en fonction de la valeur d'un paramètre du système sur une grande plage de variation. Un tel diagramme permet d'avoir une vision plus globale de la succession de plusieurs bifurcations.

Pour mieux comprendre ce procédé d'observation des solutions dynamiques, nous proposons de l'illustrer par un exemple d'un système dynamique en temps discret, l'application logistique :

$$x_{n+1} = g_a(x_n) = a x_n (1 - x_n) \quad (1.33)$$

Partant d'un point fixe stable (pour une valeur faible du paramètre de bifurcation a), la première bifurcation est dite de Hopf supercritique. Elle est caractérisée par une perte de stabilité du point fixe, et l'apparition d'un cycle limite stable en $a = 3$ (fig.1.24).

Cette première bifurcation rencontrée lorsqu'on augmente a à partir de 0 apparaît en $a_0 = 3$ (fig.1.24(a)). Graphiquement, on observe l'arrêt de la courbe du point fixe, et l'émergence d'un cycle en ce même point avec une amplitude du cycle augmentant en

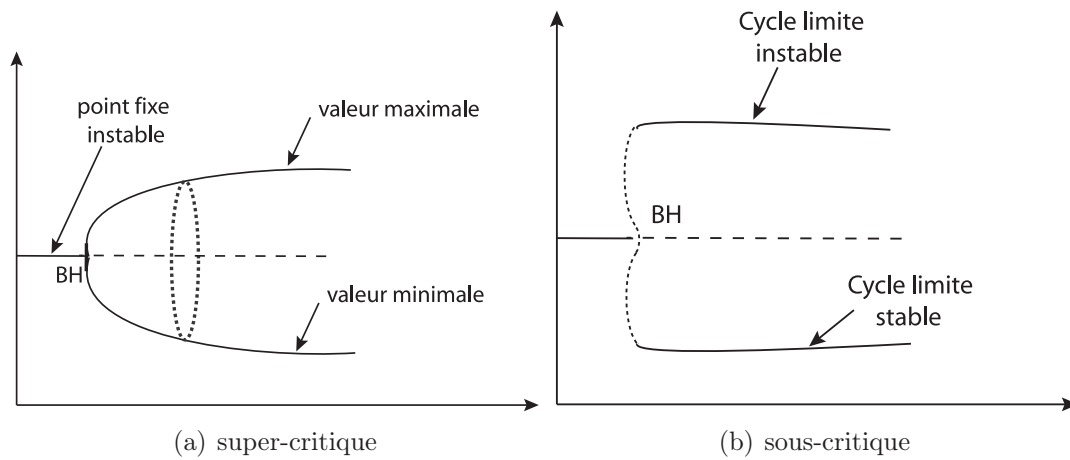


FIG. 1.24 – Type de bifurcation

$\sqrt{a - a_0}$. D'autres types de bifurcation peuvent, par exemple, être observées dépendant de la forme locale de l'itération $x_{n+1} = f(x_n)$, comme la bifurcation de Hopf sous-critique : le cycle limite qui apparaît est instable, et il est situé du côté stable de la branche du point fixe (fig.1.24(b)). Ce cycle instable est en général connecté à un cycle stable de grande amplitude, ce qui a pour conséquence une discontinuité dans le diagramme de bifurcation : à gauche du point de bifurcation, le régime stable observé est un point fixe, alors qu'à droite, il y a un cycle limite de grande amplitude.

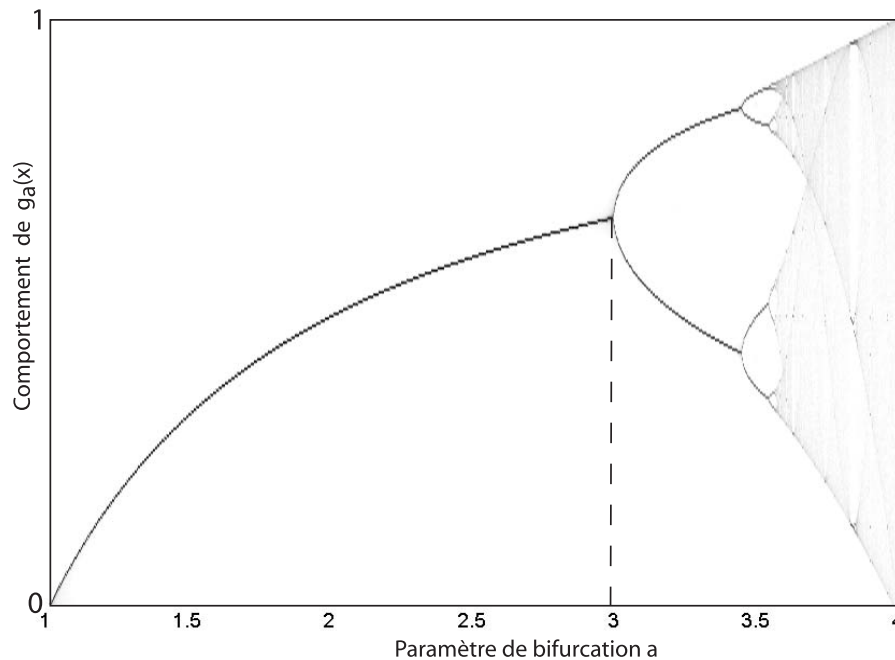


FIG. 1.25 – Exemple d'un diagramme de bifurcation

Si nous revenons au cas de l'application logistique $[x_{n+1} = g(x_n)]$ (fig.1.25), le diagramme de bifurcation pour $a > 3$ présente tout une succession de bifurcations de cycles d'ordre 2^n , qui perdent leur stabilité alors qu'un cycle stable d'ordre 2^{n+1} apparaît. Cette séquence de bifurcation est appelée cascade de dédoublements de période, et elle se poursuit en théorie jusqu'à des cycles d'ordre infini en 2^n . Mais les cycles d'ordre de plus en plus grand se produisent de plus en plus rapprochés sur l'axe des a , et c'est pour une valeur finie de a que l'on atteint la limite des cycles d'ordre infini : c'est le point d'accumulation a^* [19]. Au delà, pour $a > a^*$, les premiers régimes chaotiques apparaissent. Ainsi, on appelle aussi cette évolution du diagramme de bifurcation «route vers le chaos» (mais il existe aussi d'autres «routes vers le chaos» que la cascade de dédoublements). Notons aussi le mode particulier de représentation choisie pour chaque régime dynamique à une valeur donnée de a : sur une verticale, les valeurs atteintes sont colorées en niveau de gris, en fonction de la probabilité d'apparition de chaque point pour un régime dynamique donné (a donné). C'est également ce mode de représentation que l'on obtiendra expérimentalement, grâce aux effets de persistance des affichages à l'oscilloscope (une valeur très probable sera plus «lumineuse» du fait de la persistance, et représentera alors la densité de probabilité de cette valeur).

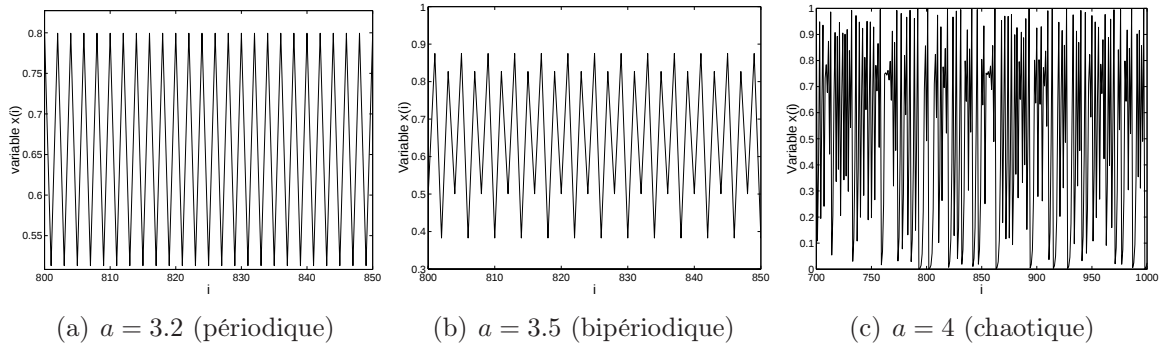


FIG. 1.26 – Type d'évolution de la dynamique de l'application logistique

Densité de probabilité

Une variable aléatoire X est caractérisée par sa fonction de répartition F_X .

Soit X une variable aléatoire de fonction de répartition F_X ; alors il existe une fonction numérique d'une variable réelle telle que :

$$F_X(x) = \int_{-\infty}^x f(\xi) d\xi \quad (1.34)$$

f est la densité de probabilité de la variable aléatoire X . Cette densité de probabilité permet de déterminer la fonction de répartition F_X :

$$P(X \in [a, b]) = F_X(b) - F_X(a) = \int_a^b f(x)dx \quad (1.35)$$

Une densité de probabilité possède deux propriétés importantes :

$$\begin{cases} f(x) \geq 0 \\ \int_{-\infty}^{+\infty} f(x) = 1 \end{cases} \quad (1.36)$$

Cette densité de probabilité permet d'obtenir de nombreuses informations dans les diagrammes de bifurcation (fig.1.25). Le lien est facilement fait avec le tracé des histogrammes permettant d'observer la densité de probabilité.

1.4.6 Exposants de Lyapunov

Le calcul de la stabilité d'un système à deux variables dans la partie 1.4.4 est un cas particulier. Pour un système à n dimensions, les calculs s'avèrent beaucoup plus compliqués. De plus, ce cas particulier de la partie 1.4.4 s'applique uniquement lorsque l'état initial se retrouve ultérieurement (point fixe ou cycle). Lorsque la solution étudiée est chaotique, il n'est plus question d'utiliser un développement linéaire autour d'une trajectoire périodique, ou de type point fixe. Il est toutefois possible de décrire, pour des portions de l'attracteur, les directions principales de l'espace des phases dans lesquelles des petites perturbations initiales de cet attracteur s'amplifient (exposants positifs) ou s'atténuent (exposants négatifs). C'est alors la moyenne de ces exposants sur l'ensemble des portions de l'attracteur, qui va nous permettre de définir les exposants de Lyapunov. Chacun d'entre eux mesure le taux de divergence ou de convergence suivant l'un des axes proposés de l'espace des phases local, de sorte qu'en moyenne un hyper-volume initial A_0 évolue selon une loi de type :

$$A = A_0 \cdot \exp((\lambda_1 + \lambda_2 + \dots + \lambda_n) \cdot t), \quad (1.37)$$

où les λ_i sont les différents exposants de Lyapunov. Dans le cas d'un système dynamique $\vec{x}(t) = f(\vec{x})$ où $f(\vec{x})$ est un champ de vecteurs, et si $\vec{x}_t$ et $\vec{x}'_t$ sont deux solutions voisines de ce système dynamique, l'évolution de leur écart, dans la limite des petits écarts, suivra la loi :

$$\frac{d(\vec{x}_t - \vec{x}'_t)}{dt} = \frac{d \delta \vec{x}_t}{dt} \quad (1.38)$$

où $\mathcal{D}^t f(x_t)$ est la matrice jacobienne de l'application f en x_t . Si cette matrice est diagonalisable, il existe une matrice inversible P^t telle que :

$$D^t = P_t^{-1} \mathcal{D}^t f P_t$$

où D_t est une matrice diagonalisable contenant les valeurs propres de $\mathcal{D}^t f$. Etant donné que le jacobien $\mathcal{D}^t f$ est isomorphe à D^t et que par conséquent les applications linéaires qu'elles définissent sont linéairement conjuguées, l'évolution de la divergence peut être étudiée de manière équivalente à l'aide de D^t . Soit Λ_i^t avec $i = 1, 2, 3, \dots, n$ les valeurs propres de la matrice jacobienne $\mathcal{D}^t$, l'équation suivante définit les n exposants de Lyapunov tout au long des différents points de l'attracteur :

$$\lambda_i = \lim_{t \rightarrow \infty} \frac{1}{t} \ln[\Lambda_i^t] \quad (1.39)$$

Il est nécessaire, si l'on a à faire à un système dissipatif, que la somme des exposants soit négative. En effet, dans le cas contraire, le volume initial finirait par remplir tout l'espace dans lequel il est immergé. Les valeurs positives de λ_i sont la signature d'une divergence des trajectoires initialement voisines sur l'attracteur. A titre d'exemple, le type d'attracteur associé au nombre d'exposants de Lyapunov positifs (noté +), nuls (noté 0) ou négatifs (noté -) en dimension 3 est donné au tableau 1.2 :

Type d'attracteur	Signe des exposants
point fixe	(-, -, -)
cycle limite	(0, -, -)
tore T^2	(0, 0, -)
attracteur étrange	(+, 0, -)

TAB. 1.2 – Type d'attracteur et exposants de Lyapunov

Une valeur peut être attribuée à la dimension de l'attracteur chaotique. Cette dimension peut être approchée grâce à la conjecture de Kaplan-Yorke [20] à partir de la connaissance du spectre de Lyapunov. La conjecture de Kaplan et Yorke définit une dimension selon la relation suivante :

$$D_{KY} = j + \frac{\sum_{i=1}^j \lambda_i}{|\lambda_{j+1}|} \quad (1.40)$$

où les λ_i sont les exposants de Lyapunov, et j l'entier le plus grand pour lequel :

$$\lambda_1 + \dots + \lambda_j \geq 0 \quad (1.41)$$

L'étude du spectre de Lyapunov constitue donc, quand elle est possible, un outil intéressant de quantification du degré de complexité d'un attracteur. Selon (1.40), plus on aura un nombre important d'exposants de Lyapunov supérieurs à 0, plus l'attracteur chaotique est complexe, et sera donc intéressant à priori pour la cryptographie par chaos.

1.5 Applications des différents types d'oscillateurs

Nous allons maintenant recentrer nos propos autour de l'application particulière qui est visée dans le cadre de ce travail, les télécommunications. Cette section a pour objet, de souligner l'utilisation vaste des systèmes dynamiques non linéaires dans ce domaine, en général pour fabriquer des comportements périodiques, mais parfois aussi pseudo-aléatoires.

1.5.1 Télécommunications à porteuse harmonique

Au cours du développement des dispositifs de télécommunication, il est apparu indispensable de coder l'information à transmettre pour adapter l'information au canal de transmission. L'une des formes de codage de l'information parmi les plus simples et les plus anciennes consiste à effectuer une translation en fréquence du signal informatif. Ce type de codage est appelé modulation harmonique. Il est d'usage de distinguer trois types de modulation analogique :

- La modulation d'amplitude (AM)
- La modulation de fréquence (FM)
- La modulation de phase (PM)

Le fonctionnement de ces trois modulations repose sur la modification d'une des caractéristiques (amplitude, fréquence ou phase) d'un signal sinusoïdal au rythme du signal informatif. En l'absence d'un signal informatif, ce signal prend la dénomination de porteuse et sa fréquence est appelée fréquence porteuse.

Des techniques de modulation analogique, la modulation d'amplitude fut la première employée car elle se caractérise par une grande simplicité de mise en œuvre. Cependant, l'utilisation de l'une des modulations se justifie par les caractéristiques qui la définissent (influence du bruit, bande de fréquence, complexité de mise en œuvre...).

Pour cela, effectuons une comparaison des différents types de modulation. Pouvoir quantifier la qualité du signal d'information après sa transmission et sa démodulation, est l'un des points essentiels des télécommunications. Il est relativement intuitif de comprendre que le signal reçu après une transmission à longue distance va être considérablement atténué, et dégradé par la superposition de bruit. Enfin, le signal subit différents traitements qui vont globalement entraîner des déformations. Il est d'usage de caractériser le bruit par sa puissance. De ce fait, l'influence du bruit sur un signal est caractérisée par son rapport signal/bruit. Plus ce rapport est élevé, meilleure est la qualité du message d'information. La mesure de déformation d'un signal est donnée par son taux de distortion harmonique total. Nous reviendrons ultérieurement sur ce type de mesure et par conséquent sur la détermination des performances liées à un type de modulation. D'un

point de vue générale, retenons uniquement les points essentiels de chacun des types de modulation (TAB.1.3) notamment en fonction du paramètre δ correspond à l'indice de modulation.

Modulation	Bande de fréquence	complexité de mise en oeuvre	Améliorations après démodulation	sensibilité aux perturbations
AM	$2 f_m$	minime	jamais en détection crête	importante
FM	$2 N(\delta) f_m$	complexe	si $\delta > 0.475$	faible
ϕ M	$2 N(\delta) f_m$	complexe	si $\delta > 0.775$	faible

TAB. 1.3 – Différences entre les types de modulation

Dans ces trois modes de modulation harmonique, on fait bien évidemment appel à des oscillateurs, la plupart du temps très faiblement non linéaires, et qui ont pour but de générer une oscillation harmonique correspondant à la fréquence porteuse. C'est ainsi une oscillation purement harmonique, à une seule composante fréquentielle, qui est utilisée dans ce mode de transmission de l'information. Cette condition de pureté spectrale de la porteuse n'est toutefois nullement nécessaire pour une porteuse d'information, comme nous allons le voir.

1.5.2 Télécommunications à étalement de spectre

Au début des années 20, Goldsmith utilise la FM pour étaler le spectre d'une modulation AM afin de réduire l'effet du bruit et des trajets multiples sur une communication. Dès les années 1940, Wiener et Shannon ont développé des théories de traitement du signal dans le but d'utiliser la technique d'étalement de spectre à des fins de cryptographie dévolue aux transmissions militaires. L'utilisation de cette technique dans la radio-localisation (GPS) lui permet d'entrer enfin dans le domaine public. A la fin des années 90, l'étalement de spectre apparaît comme une solution de multiplexage d'avenir qui permet d'envisager les radiocommunications numériques de masse.

Le principe de la modulation à étalement de spectre (Spread Spectrum) consiste à étaler l'information sur une bande de fréquences beaucoup plus large que la bande nécessaire, dans le but de combattre les signaux interférents et les distorsions liées à la propagation : le signal se confond avec le bruit. Le signal est codé au départ, un code est assigné à chacun des usagers afin de permettre le décodage à l'arrivée. L'étalement est assuré par un signal pseudo-aléatoire appelé code d'étalement. A la réception, le signal est perçu comme du bruit si le récepteur n'a pas le code. La modulation avec étalement de spectre est ainsi optimisée pour lutter contre le bruit, dont elle limite mieux les effets.

Un spectre étalé est donc obtenu en modulant le signal avec une séquence connue sous le nom de séquence pseudo-aléatoire ayant une apparence de bruit. Le signal étalé (spec-

tralement) doit apparaître comme un bruit, en particulier pour les autres transmissions éventuelles utilisant le même spectre étalé.

La modulation CDMA

La modulation CDMA est une modulation à étalement de spectre signifiant Accès Multiple à Répartition par Code. Celui-ci se développe actuellement pour la téléphonie mobile et/ou le wireless. Les avantages du CDMA se retrouvent dans la protection (sécurité) des communications, la qualité, la faible consommation, la flexibilité de l'allocation. . .

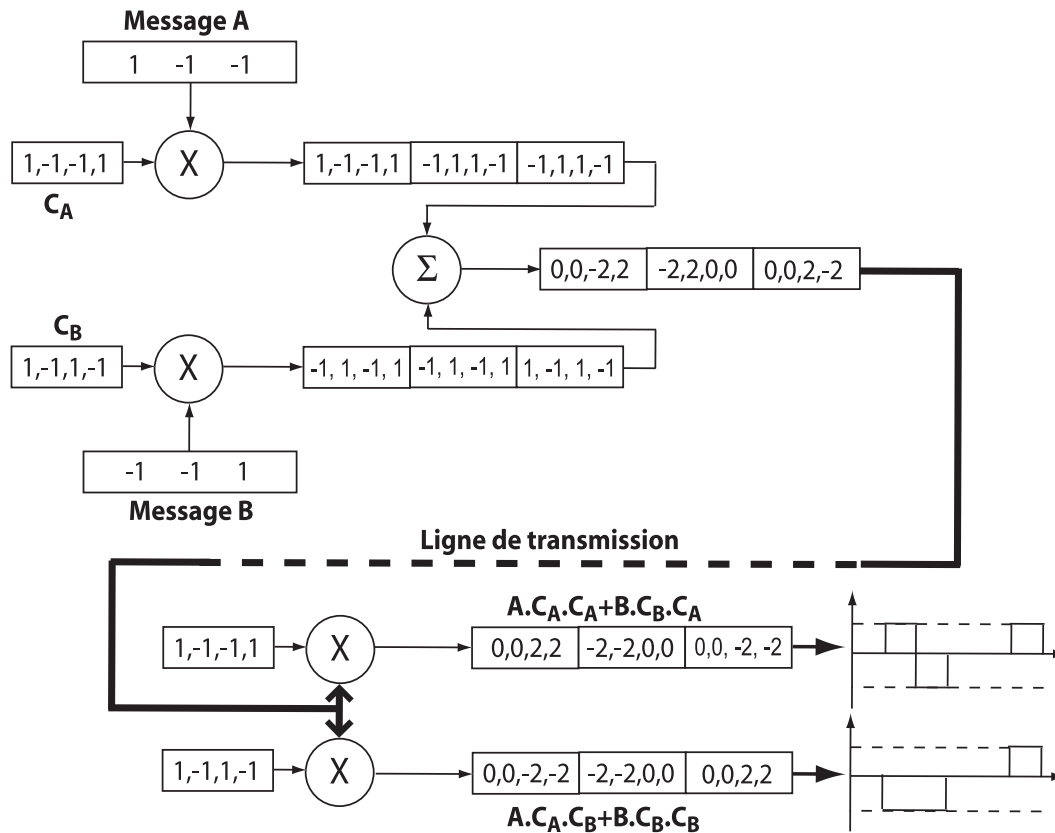


FIG. 1.27 – Principe du CDMA

La technique CDMA consiste à faire partager un même canal de transmission (bande de fréquence) au même moment par des utilisateurs qui sont caractérisés par des codes différents ayant des propriétés d'autocorrélation et d'intercorrélation permettant au niveau de la réception de séparer les messages des différents utilisateurs.

Le principe de l'accès multiples avec codes donne lieu à plusieurs variantes dont nous allons décrire l'étalement par séquence directe (DSSS⁴) (fig.1.27) qui est un principe gé-

⁴Discrete Sequence Spectrum Spreading

néral du CDMA.

- Le message A de l'émetteur A , représenté par une séquence de $+1$ et -1 traduisant la séquence linéaire de bits 1 et 0 logiques, est multiplié par un code (C_A). Ce code est une séquence de $+1$ et -1 («les chips») judicieusement choisie et dont les transitions sont m fois plus fréquentes. Le même processus est utilisé pour le message B .
- Les séquences produits $A C_A$ et $B C_B$ sont ajoutées puis transmises.
- A la réception, le destinataire du message A multiplie la séquence reçue par le code C_A et le destinataire du message B par le code C_B .

Si les codes sont bien choisis sur la durée d'un bit (donc de m «les chips»), la moyenne en réception du message A de $C_A C_A$ sera égale à $m/2$, tandis que $C_A C_B$ aura une moyenne nulle. Les codes C_A et C_B sont dits orthogonaux puisque la somme des produits des éléments correspondants est quasi nulle.

Communications par chaos

La mise au point de systèmes de transmissions sécurisés de l'information fait l'objet d'un intérêt croissant dans le domaine militaire comme dans le domaine civil. Dans ce contexte, les transmissions analogiques comme numériques sur porteuse chaotique ont été introduites comme alternative possible aux techniques d'étalement de spectre classique. La porteuse générée par un oscillateur non linéaire instable donne au signal émis l'apparence d'un bruit et le rend ainsi difficilement détectable par l'observateur ne connaissant pas les paramètres de l'émetteur. La complexité des circuits est, de plus, largement réduite puisque l'oscillateur chaotique délivre naturellement un signal à spectre étalé.

Les oscillateurs chaotiques utilisés à l'émission réalisent simultanément deux fonctions : ils étalent le spectre du signal tout en assurant une forme de cryptage. Ainsi, la transmission du message est difficilement déchiffrable et il est quasiment impossible de retrouver les symboles d'information pour l'observateur qui ne connaît pas les paramètres de l'émetteur. Un atout majeur des systèmes chaotiques est leur simplicité de réalisation au niveau circuit.

1.5.3 Cryptographie par chaos

La synchronisation entre l'oscillateur et le système esclave

La synchronisation de signaux chaotiques a été découverte par Carroll et Pecora lorsqu'ils ont réussi à reproduire à l'identique un signal électrique chaotique et à le mettre en phase avec le signal original [21].

Les communications sécurisées s'inspirent de cette découverte pour réaliser un système de chiffrement par chaos ; le signal chaotique peut être reconstitué s'il traverse les mêmes éléments qui l'ont formé. Ce principe va permettre de générer un signal chaotique

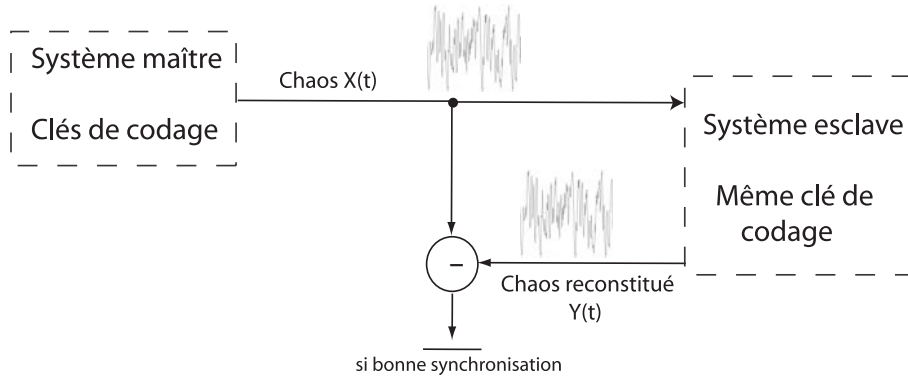


FIG. 1.28 – Synoptique de synchronisation entre deux systèmes

masquant une information. Ce signal transmis est à la base de la reconstitution de la dynamique chaotique pour extraire l'information [22].

Un système de cryptage par chaos est composé de deux parties : le brouilleur et le décrypteur. Ceux-ci sont strictement identiques pour assurer de façon optimale le respect des conditions initiales. La synchronisation des dispositifs est établie en amorçant le chaos dans le système de réception que nous nommerons dans un premier temps le système esclave étant donné sa nature à être commandé. C'est dans ce dernier système qu'est injectée la dynamique chaotique issue du système maître. Cet ensemble constitue un cryptosystème à clés symétriques secrètes. Le système maître et le système esclave possèdent les mêmes clés. La synchronisation représente la phase critique de l'opération de décryptage. Du fait de la nature complexe du comportement du signal brouilleur, le moindre écart lors du décodage va entraîner un parasite sur le signal nul (dans le cas d'une synchronisation parfaite) comme représenté sur la figure 1.28 qui est couramment appelé bruit de déchiffrement ou bruit de décodage.

La limitation du bruit de déchiffrement et la complexité de la clé sont dépendantes. En effet, en utilisant une clé moins complexe permettant ainsi de générer un signal chaotique de dimension moins élevée, le bruit de décodage sera moins important. Cependant, la dimension moins élevée du chaos engendrera une perte de la qualité de masquage.

Les systèmes hyperchaotiques constitués par des boucles non linéaires à retard génère un signal chaotique d'une dimension très importante, et de là s'instaure une difficulté supplémentaire pour la synchronisation. Soit $x(t)$ le signal généré et $y(t)$ le signal reconstitué, nous pourrions définir l'erreur de synchronisation instantanée entre $x(t)$ et $y(t)$:

$$\epsilon(t) = y(t) - x(t) \quad (1.42)$$

Influence de l'insertion de l'information sur la dynamique chaotique

Il existe plusieurs méthodes pour insérer le signal d'information dans le signal chaotique. Une première méthode consiste à simplement masquer le signal d'information en l'additionnant au signal chaotique à l'extérieur de la boucle d'oscillation chaotique (fig.1.29).

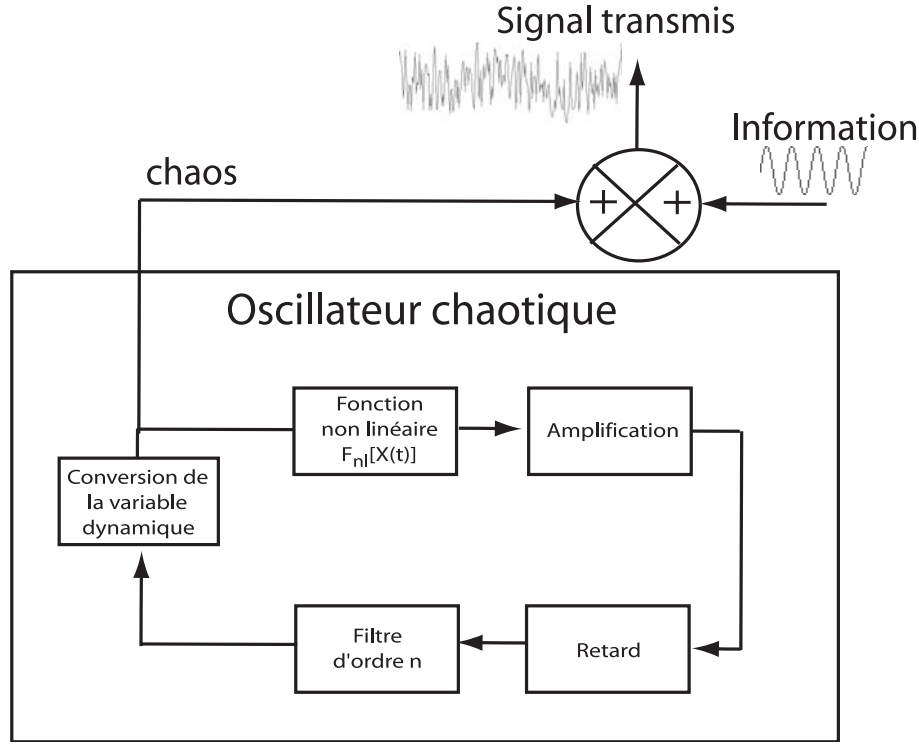


FIG. 1.29 – Méthode de masquage

Cette technique est appelée «masquage par chaos». Cette technique présente certains désavantages. En effet, l'insertion d'un signal d'information va changer l'évolution du chaos et cette méthode d'insertion est effectuée à l'extérieure de la boucle. Par conséquent, pour que le récepteur puisse se synchroniser sur l'émetteur et ainsi décoder le signal d'information, celui-ci doit avoir une amplitude A_{info} relativement faible par rapport au signal chaotique A_{chaos} :

$$A_{\text{info}} \ll A_{\text{chaos}} \quad (1.43)$$

Dans le cas contraire, le masquage ne serait pas efficace. Ce type de masquage présente également un inconvénient au niveau de la faible amplitude du signal d'information pour que celui-ci puisse être correctement crypté. En effet, dans un environnement particulièrement bruité comme une transmission hertzienne, le signal d'information ne pourrait pas se différencier du bruit de transmission [23] car tous les deux sont extérieures à l'oscillateur.

Une seconde méthode s'avère meilleure dans le cas de la cryptographie. Le signal d'information est directement inséré dans la boucle qui génère le signal chaotique (fig.1.30).

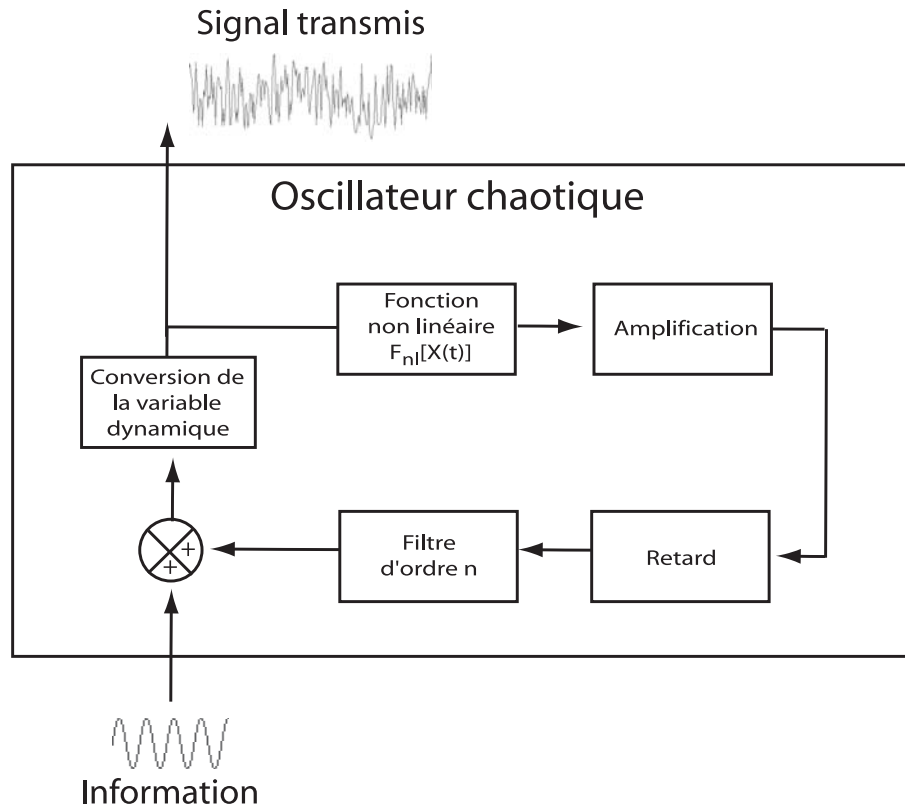


FIG. 1.30 – Modulation du chaos par l'information

Ainsi, le message a une influence directe sur la dynamique chaotique, ce qui potentiellement augmentera la complexité du chaos généré [24]. De ce fait la communication sera mieux sécurisée. L'amplitude du signal qui transporte l'information a peu d'influence sur la synchronisation avec le récepteur. Le bruit de transmission et l'erreur d'accordabilité seront les deux sources d'erreur de décodage [25].

L'insertion de l'information sera faite de la même manière qu'à la figure 1.30. Cependant, il est important de savoir que l'endroit d'insertion de l'information a une influence notable sur l'architecture du récepteur permettant le décodage [26].

Nous allons, dans la suite de ce chapitre, présenter divers systèmes opto-électroniques de cryptographie par chaos qui ont été réalisés au laboratoire, sur la base des architectures des figures 1.29 et 1.30.

Cryptographie par chaos en longueur d'onde

Le premier système optique concernant la cryptographie par chaos a été réalisé au sein du laboratoire d'Optique PMD [27] ; l'ensemble du système est basé sur une dynamique

non linéaire à retard permettant de générer un chaos de grande dimension.

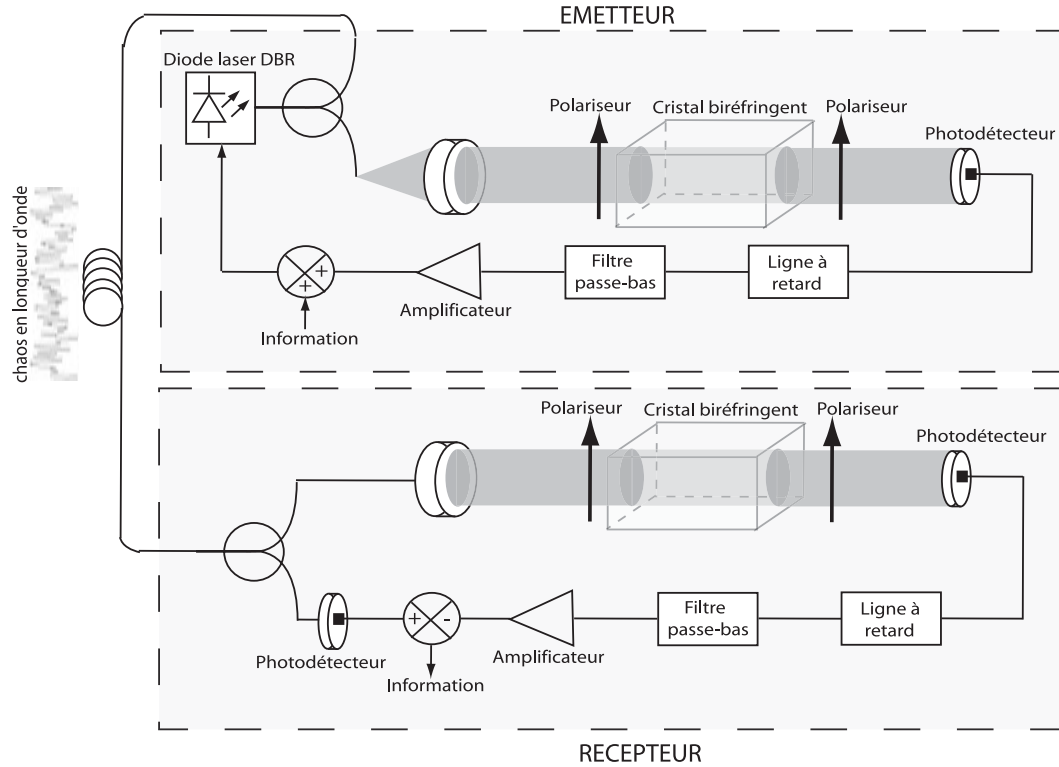


FIG. 1.31 – Système de cryptage par chaos en longueur d'onde

Les différentes fonctions qui constituent l'oscillateur chaotique sont placées en boucle fermée, dans laquelle l'information aura un rôle actif sur la dynamique chaotique. Du côté du récepteur, les mêmes éléments sont utilisés de manière à constituer les mêmes clés que celles utilisées à l'émetteur-codeur. La différence entre l'émetteur et le récepteur réside dans l'association de ces éléments qui sont, contrairement à l'oscillateur autonome de l'émetteur, placés en boucle ouverte au récepteur. Le premier système de ce type conçu au laboratoire est un système non linéaire à retard permettant de générer un signal optique dont la longueur d'onde présente des variations chaotiques. C'est le premier système hyperchaotique lié au cryptage de l'information (fig.1.31). La lame biréfringente va permettre d'obtenir des variations non linéaires de l'intensité optique en fonction de la longueur d'onde. L'intensité optique peut ensuite être détectée puis rebouclée sur la diode laser après certaines fonctions électroniques linéaires (filtrage, amplification, détection du message, retard).

La diode laser DBR permettrait de réaliser la source commandée en courant pour pouvoir générer un signal optique de puissance constante mais de longueur d'onde variable. Cette diode accordable en longueur d'onde possède une caractéristique particulière avec la présence de sauts de mode qui peuvent entraîner des effets non linéaires supplémentaires

dans la boucle d'oscillation. Ce type de problème doit être éliminé afin de contrôler au mieux les effets non linéaires. Nous verrons que des problèmes similaires sont susceptibles d'apparaître dans les systèmes électroniques capables de générer un chaos en fréquence.

Générateur de chaos sur la phase optique

Ce générateur n'a pas pu être utilisé pour la conception d'un système de masquage des informations [28]. En effet, la sensibilité de la phase optique aux perturbations extérieures est trop importante pour avoir pu envisager la synchronisation entre deux systèmes.

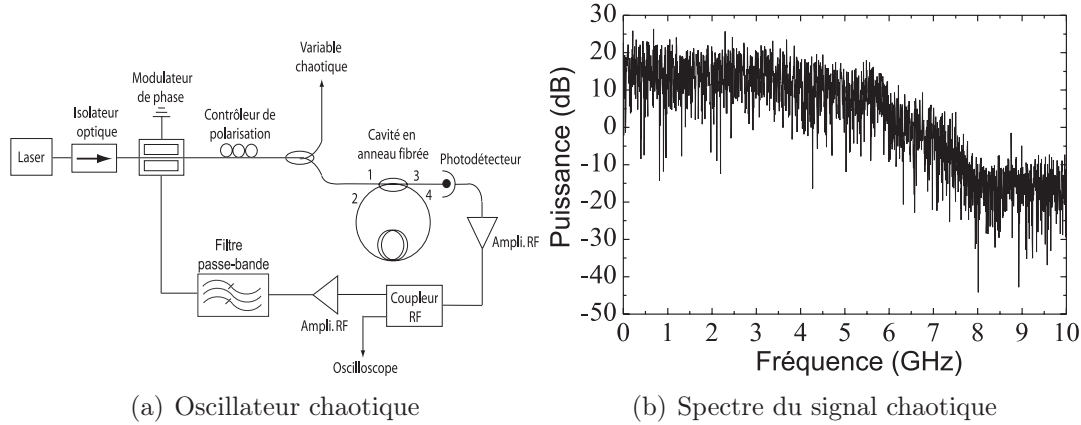


FIG. 1.32 – Caractéristique du générateur de chaos en «phase optique»

Pour cette raison, seul le générateur de chaos a été réalisé (fig.1.32(a)). Toutefois, cet oscillateur a été capable de générer un chaos possédant un très large spectre, s'étalant sur plusieurs GHz (fig.1.32(b)). La non-linéarité de transformation de la phase en intensité, est réalisée par une cavité en anneau fibrée. Son fonctionnement est similaire à celui d'un interféromètre de Fabry-Pérot, donc un interféromètre à ondes multiples. La différence notable entre les deux types d'interféromètres est leur courbe de transmission. En effet, au lieu d'avoir des pics de résonance, la cavité en anneau fibré sera caractérisée par ses trous dits d'antirésonance [29].

Système de cryptographie à très haut débit par chaos en intensité

Pour effectuer des applications pour les télécommunications très large bande, c'est à dire capables de crypter des signaux à très haut débit, il est important de s'affranchir de tout type de sensibilité excessive par rapport à certains paramètres physiques (longueur d'onde, phase optique). Le montage précédent a permis de produire un signal chaotique très large bande, mais il n'a pu donner lieu à la réalisation viable d'un ensemble émetteur/récepteur chaotique synchronisé, précisément pour des problèmes de stabilité : le succès de l'opération de synchronisation tient à la réalisation d'un accord aussi parfait

que possible entre les éléments de l'émetteur et du récepteur, cet accord étant d'autant plus délicat pour une dynamique chaotique de grande largeur spectrale [30].

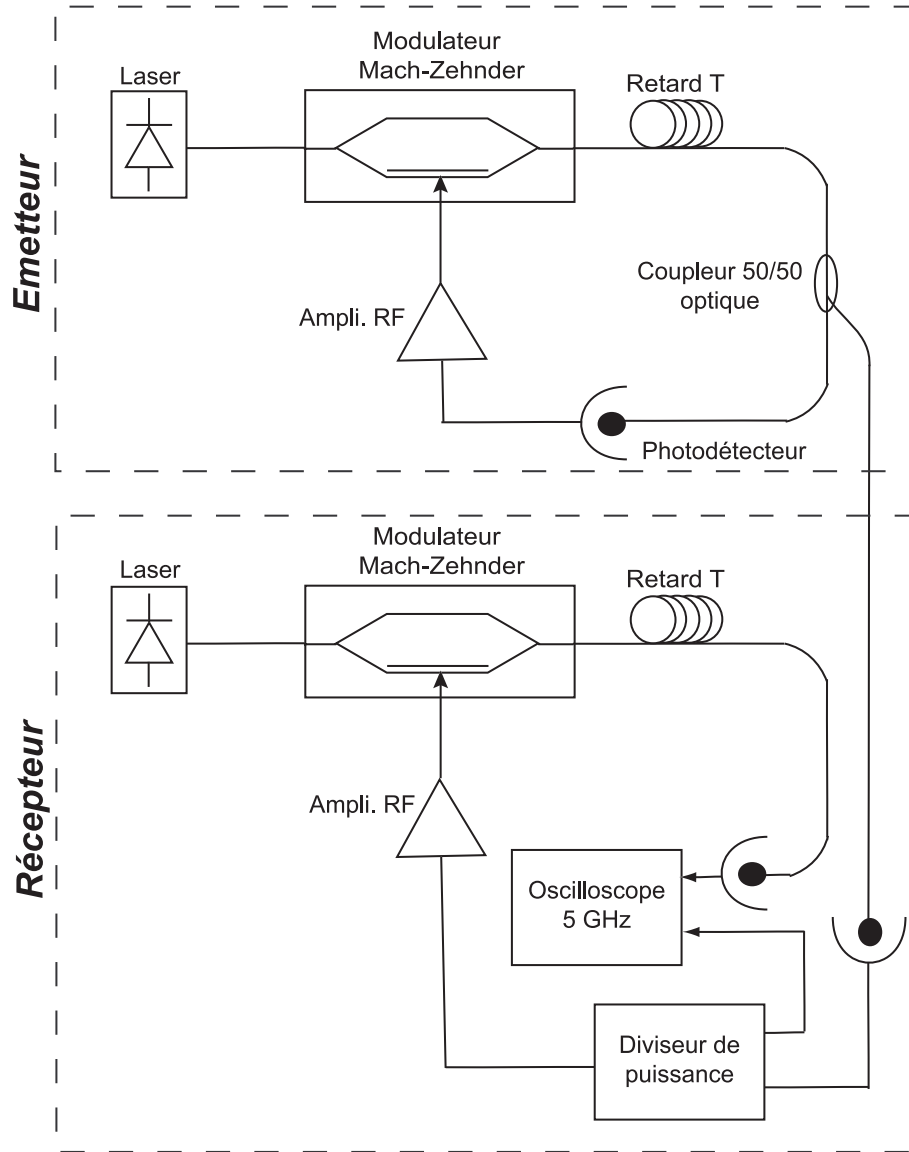


FIG. 1.33 – Système de cryptage haut débit

Le montage expérimental qui a permis pratiquement de vaincre ces contraintes est représenté sur la figure 1.33. Il fait intervenir un oscillateur électro-optique non linéaire à retard, constitué de composants standards des télécommunications hauts débits. La variable chaotique est l'intensité optique. La non-linéarité est réalisée par la fonction de modulation d'un interféromètre de Mach-Zehnder en optique intégré. Les résultats expérimentaux montrent qu'un débit de 3 GHz peut être atteint, pour un taux d'erreur binaire de $7 \cdot 10^{-9}$ [31].

Tous ces démonstrateurs opto-électroniques de cryptage par chaos, ont été développés

dans le contexte des télécommunications optiques. Leurs principes, exposées aux figures 1.29 et 1.30, sont toutefois a priori généraux, et notre objectif consiste à les appliquer au domaine des communications radiofréquences. C'est ce que nous allons reporter dans la suite, à l'aide des différentes notions présentées dans ce premier chapitre.

Notes du lecteur

Chapitre 2

La cryptographie par chaos en fréquence

*Un savant, c'est quelqu'un
qui est à peu près certain,*

Jules Renard

*Ce qui est affirmé sans preuve
peut être nié sans preuve,*

Euclide de Mégare

2.1 Introduction

La cryptographie par chaos est une application issue de la possible synchronisation entre deux oscillateurs chaotiques distants [32, 33]. Les systèmes hyperchaotiques tels que ceux décrits par les dynamiques non linéaires à retard, sont susceptibles de générer un signal chaotique de grande dimension, qui, de ce fait, rendra le cryptage de l'information plus sûr. En effet, l'analyse du chaos masquant l'information sera d'autant plus difficile dans le cas de signaux chaotiques de grande dimension. Plusieurs démonstrateurs ont été présentés dans le domaine des transmissions optiques, sur la base précisément des dynamiques non linéaires à retard.

Actuellement, la modulation de fréquence est largement utilisée dans les systèmes de télécommunications, notamment dans les télécommunications hertziennes. En effet, les transmissions sans fil ont pris le pas sur les transmissions filaires, car ce type de transmission est très avantageux financièrement puisqu'il évite de relier deux points éloignés difficiles d'accès.

La modulation d'amplitude est également un type de modulation adopté pour les transmissions hertziennes. Cependant, la synchronisation est très sensible aux bruits. Le bruit intrinsèque au système de cryptographie, mais aussi le bruit engendré par la transmission doivent être les plus petits possibles afin de pouvoir limiter le bruit de décodage

au minimum.

Nous détaillerons, au cours de ce chapitre, les caractéristiques d'une modulation de fréquence et les effets du bruit pouvant affecter le signal transmis. Nous analyserons les systèmes de démodulation. Les applications au cryptage par chaos seront ensuite exposées avec la réalisation du premier système de cryptographie par chaos en fréquence. Nous étudierons ce premier système en mettant en avant les résultats expérimentaux obtenus. La bande passante limitée de ce prototype nous poussera à énoncer les perspectives pour pouvoir générer une porteuse de plusieurs centaines de MHz. Enfin, dans une dernière partie, nous expliquerons la solution choisie pour mettre en œuvre un système de cryptographie par chaos UHF. Constitué à partir de la même structure que le système électronique, certaines de ces fonctions sont réalisées d'une manière différente afin de s'adapter aux contraintes technologiques propres à la mise en œuvre d'une forte non linéarité en haute fréquence.

2.2 Les transmissions hertziennes : la modulation de fréquence

2.2.1 Quelques rappels sur les radiofréquences et les hyperfréquences en télécommunication

Il existe de nombreux types de modulation dans les télécommunications avec pour chacun d'eux les avantages et les défauts liés à l'environnement dans lequel ils évoluent mais aussi le débit d'information qu'ils sont capables de transmettre.

Les transmissions hertziennes sont effectuées dans un espace libre où tous les types de bruit (ou presque) susceptibles d'affecter le signal de transmission sont présents. C'est pourquoi le choix de la modulation est primordiale afin de limiter l'influence du bruit de transmission.

Il est, avant toute chose, nécessaire de rappeler les valeurs du spectre électromagnétique et ses applications dans les télécommunications. Dans le tableau 2.1 se trouvent le type de chaque spectre (LF¹, MF², HF³, VHF⁴, UHF⁵, SHF⁶...) ses valeurs limites et ses applications dans les transmissions actuelles.

Les radiofréquences, les hyperfréquences, et l'optique ont tous des avantages et des inconvénients dans les télécommunications. Il est bon de rappeler pourquoi les transmis-

¹Low Frequency

²Middle Frequency

³High Frequency

⁴Very High Frequency

⁵Ultra High Frequency

⁶Supra High Frequency

LF : 30 kHz /300 kHz MF : 300 kHz /3 MHz	Diffusion AM longue portée, ondes de surfaces terrestres et propagation ionosphérique (couche D)
HF : 3/30 MHz	propagation ionosphérique (D, E, F), communications militaires
VHF : 30/300 MHz UHF : 300 MHz /3 GHz	Ondes planes, radio FM et télévision, couverture dans l'horizon radio
SHF : 3/30 GHz	Communications satellites, faisceaux hertziens, radars, téléphonie mobile, télévision par satellite
Optique $\lambda = 1.3/1.55\mu m$	communications terrestres très hauts débits

TAB. 2.1 – Occupation du spectre électromagnétique

sions hyperfréquences restent le type de fréquences privilégié pour les communications hertziennes.

La longueur d'onde associée aux signaux de basses fréquences est importante. Cette longueur d'onde importante va limiter l'atténuation atmosphérique en espace libre. Cependant, l'utilisation d'antennes directives n'est pas possible et la taille des antennes reste très grande. Les services associés aux porteuses de basses fréquences sont les communications maritimes et les services fixes sur de longues distances, la radiodiffusion et la radio navigation.

Les signaux hyperfréquences réalisent le meilleur compromis entre l'atténuation et la directivité des antennes. Ces fréquences trouvent de nombreuses applications avec les communications mobiles, les liaisons terre-satellites et intersatellites et les communications locales, car elles permettent d'avoir un très haut débit.

Les signaux optiques permettent aux transmissions d'atteindre des débits record. Cependant, les distances de transmissions sans amplification ou régénération⁷ restent faibles car l'atténuation engendrée par ce type de signal est relativement élevée pour des transmissions assez longues ($> 1000 km$). L'atténuation caractérise l'affaiblissement du signal au cours de la propagation. Dans le cas d'une fibre optique, l'atténuation se traduit par une décroissance exponentielle de la puissance en fonction de la longueur de fibre. Soient P_0 et P_L les puissances à l'entrée et à la sortie d'une fibre de longueur L , celles-ci sont reliées par la relation suivante :

$$P_L = P_0 \exp(-\alpha L) \quad (2.1)$$

où α est le coefficient d'atténuation exprimé en dB/km . Celui-ci est proche de $0.2dB/km$

⁷dans la pratique, les liaisons longues distances à fibre optique font usage d'amplificateurs optiques tous les 70/80 km

pour une longueur d'onde optique $\lambda = 1550 \text{ nm}$. Dans le cas des transmissions en espace libre, l'atténuation de l'onde électromagnétique est exprimée par la relation suivante :

$$L(dB) = 32.4 + 20 \log[F(MHz)] + 20 \log[d(km)] \quad (2.2)$$

où L sont les pertes, F la fréquence de la porteuse de transmission et d la distance de transmission. Il est toutefois important de préciser les pertes des autres types de câbles de transmission comme les câbles coaxiaux et les guides circulaires dont les pertes sont respectivement de 60 dB/km et de 2 dB/km .

La figure 2.1 répertorie le graphe des pertes en fonction de la distance de transmission et du support de transmission utilisé.

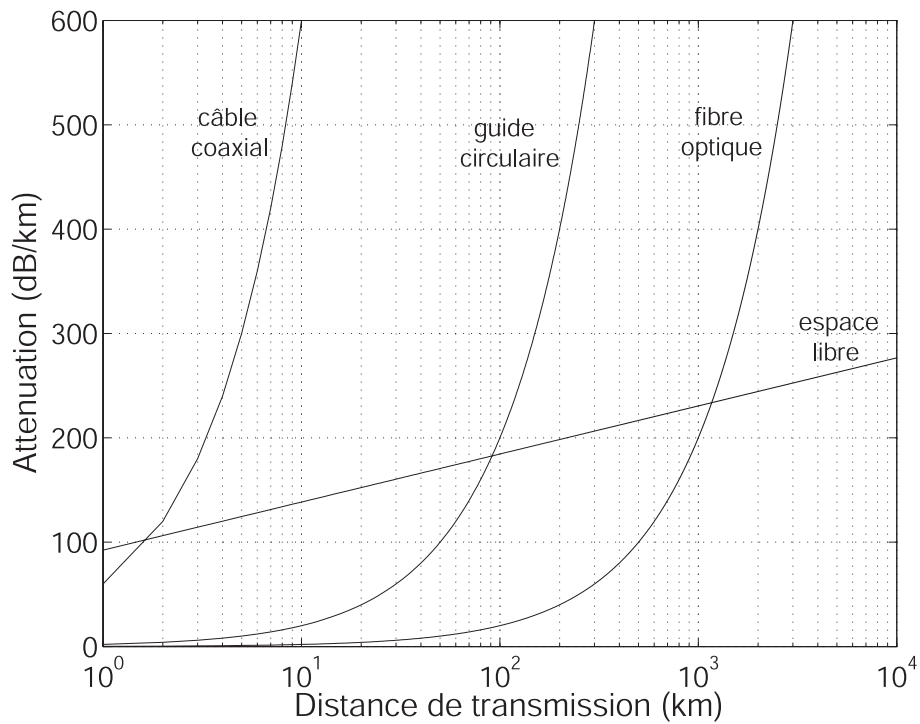


FIG. 2.1 – Atténuation typique pour quatre supports de transmission les plus utilisés

Nous remarquons que l'atténuation entre les deux supports majoritairement utilisés dans les télécommunications actuelles varie selon le type d'application pour lesquelles ceux-ci sont utilisés. En effet, le graphique nous montre qu'il est préférable d'utiliser les transmissions hertziennes dans le cas de longues distances. En revanche, les pertes engendrées par une fibre optique pour des liaisons inférieures à 1000 km sont moins importantes qu'une transmission en espace libre.

2.2.2 Rappels et définition de la modulation en fréquence

Le cryptage par chaos en fréquence se base sur la modulation de fréquence (2.3) majoritairement utilisée dans les transmissions hertziennes. Un signal modulé en fréquence s'écrit typiquement :

$$V(t) = A. \cos \left[\omega_0 t + k \int_0^t s(t) dt \right] \quad (2.3)$$

où $s(t)$ est le signal modulant. La porteuse de notre système est la variable chaotique définie comme telle :

$$\omega(t) = 2\pi f(t) = \omega_0 + \Delta\omega(t) \quad (2.4)$$

$\Delta\omega(t)$ a une évolution pseudo-aléatoire et sa valeur crête à crête peut être considérée comme l'excursion en fréquence de la modulation.

Pour discerner l'ensemble des points importants relatifs à la modulation chaotique en fréquence, nous allons remplacer le signal modulant chaotique par un signal modulant sinusoïdal ($\omega = \omega_0 + \Delta\omega \cos \Omega t$). Ainsi, le signal $V(t)$ de l'équation (2.3) devient :

$$V(t) = A. \cos \left[\omega_0 t + \frac{\Delta\omega}{\Omega} \sin(\Omega t) \right] \quad (2.5)$$

$\Delta\omega/\Omega$ est l'indice de modulation. En comparant ce signal sinusoïdal au signal chaotique modulant, Ω peut prendre une valeur quelconque comprise dans la bande de base du signal chaotique. La fréquence angulaire du signal modulant Ω et l'excursion en fréquence $\Delta f(t) = \Delta\omega(t)/2\pi$ vont définir l'indice de modulation. Bien entendu, la forme du signal modulant est relativement importante. Suivant la forme, périodique ou chaotique, du signal modulant, son analyse est différente.

2.2.3 Les techniques de démodulation de signaux FM

Il existe plusieurs techniques possibles pour démoduler un signal modulé en fréquence (FM) ; nous en analyserons uniquement deux :

- La démodulation par dérivation et par détection de phase
- La démodulation par l'utilisation d'une boucle à verrouillage de phase (PLL)

Démodulation par dérivation et détection de phase

Pour démoduler un signal FM, il est nécessaire de recourir à un dispositif dont la tension (ou le courant) de sortie varie linéairement avec la fréquence. De ce fait, l'opérateur mathématique permettant cette opération est la dérivation. Le signal FM $V(t)$ (2.3) deviendra par conséquent après sa dérivation :

$$\frac{dV}{dt}(t) = -A(\omega_0 + k s(t)) \sin \left[\omega_0 t + k \int_0^t s(t) dt \right] \quad (2.6)$$

Il s'agit donc d'un signal modulé en fréquence et en amplitude. La détection d'enveloppe permet de récupérer uniquement le signal modulé en amplitude sans tenir compte de la fréquence instantanée du signal dérivé.

En récupérant l'enveloppe du signal (redressement + filtrage), le signal modulant est reconstitué. Le synoptique suivant (fig.2.2) montre l'ensemble des étapes à respecter pour la démodulation du signal FM.

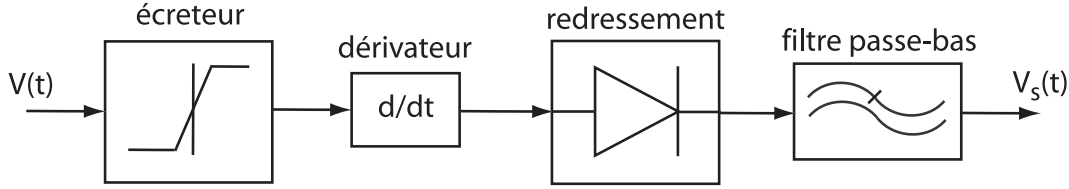


FIG. 2.2 – Dérivation et détection d'enveloppe

L'écreteur permet d'avoir des signaux d'amplitude constante avant le dérivateur et donc de s'affranchir des éventuelles variations du signal modulé (A n'est pas constant dans la pratique...). Il ne reste plus ensuite qu'à effectuer une détection crête.

La boucle à verrouillage de phase

La boucle à verrouillage de phase est un système de contrôle de la fréquence en boucle fermée. Son fonctionnement est basé sur la comparaison de la phase du signal d'entrée et du signal de sortie issu d'un oscillateur local commandé en tension (VCO). La PLL⁸ est donc, comme son nom l'indique, un système asservi en phase. Son principe de fonctionnement est illustré dans le domaine de Laplace par la figure 2.3.

La boucle à verrouillage de phase va permettre d'éliminer le bruit de phase en générant le signal $V_s(t)$ à partir du signal modulé en fréquence $F_e(t)$. Le signal $V_s(t)$ est égal au signal modulant $s(t)$ lorsque la PLL est verrouillée.

En 1932, un groupe de scientifique anglais mettait au point un système dépassant la réception superhétérodyne. En effet, cette dernière se compliquait davantage avec l'augmentation du nombre de sous-porteuses et l'apparition de spectre cannelé. C'est pourquoi, un nouveau type de récepteur appelé récepteur homodyne et par la suite renommé récepteur synchrodyne s'appuyant sur une boucle à verrouillage de phase est né [34].

Si l'écart de phase $\Delta\phi = \phi_e - \phi_s$ entre les signaux d'entrée et de sortie n'est pas constant, la tension d'entrée du VCO⁹ varie ce qui entraîne une variation de fréquence

⁸Phase Locked Loop

⁹Voltage Controlled Oscillator

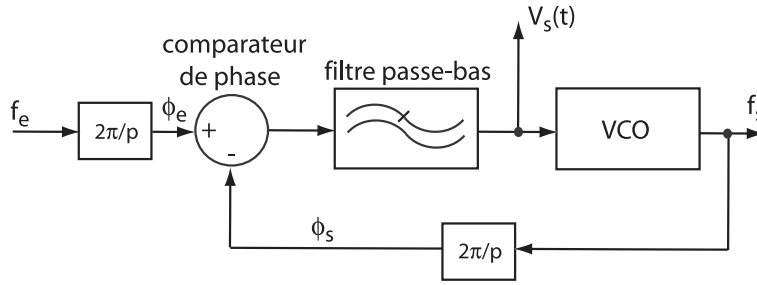


FIG. 2.3 – Principe d'une boucle à verrouillage de phase

du signal présent à la sortie de celui-ci. La fréquence du VCO ayant changée, la phase du signal de sortie peut «rattraper» celle du signal d'entrée. Pour un écart de phase $\Delta\phi$ constant :

$$\begin{cases} \frac{d(\phi_e - \phi_s)}{dt} = 0 \\ f_e - f_s = 0 \end{cases} \quad (2.7)$$

la fréquence instantanée du signal d'entrée est donc égale à la fréquence du signal délivré par le VCO. La fréquence instantanée du signal d'entrée de la PLL étant une fonction linéaire du signal modulant $s(t)$, le signal de commande du modulateur FM de la PLL suit exactement le signal $s(t)$.

L'avantage d'un tel système est de ne pas être tributaire de la forme des signaux. De plus, la théorie des systèmes asservis indique qu'un tel dispositif se comporte comme un filtre passe-bas. L'équation (2.8) est l'interprétation mathématique du comportement dynamique linéaire d'une PLL dans le domaine de Laplace :

$$H(p) = \frac{1}{1 + \frac{p}{2\pi K_{cp}\alpha_{vco}} + \frac{\tau p^2}{2\pi K_{cp}\alpha_{vco}}} \quad (2.8)$$

Chacun des paramètres influe sur les caractéristiques de fonctionnement de la PLL. K_{cp} la sensibilité du comparateur de phase, α_{vco} la sensibilité du VCO et τ la constante de temps du filtre passe-bas du premier ordre, ont chacun une influence sur la fréquence naturelle ω_n et le coefficient d'amortissement z du système en boucle fermée.

En étudiant l'influence des paramètres du comparateur de phase K_{cp} et de la fréquence de coupure du filtre passe-bas que l'on peut interpréter par sa constante de temps τ , le coefficient d'amortissement (2.10) et la fréquence naturelle (2.9) du système à verrouillage de phase ont une importance sur la stabilité du système de détection d'enveloppe :

$$\omega_n = \sqrt{\frac{2\pi K_{cp}\alpha_{vco}}{\tau}} \quad (2.9)$$

$$z = \frac{1}{2\sqrt{2\pi K_{cp} \alpha_{vco} \tau}} \quad (2.10)$$

Ainsi, on peut définir les limites de stabilité du système. En effet, celui-ci ne doit pas être résonant pour éviter tout décrochage de la boucle. Il doit également avoir une fréquence de coupure (τ petit) assez haute pour avoir un débit de transmission le plus grand possible.

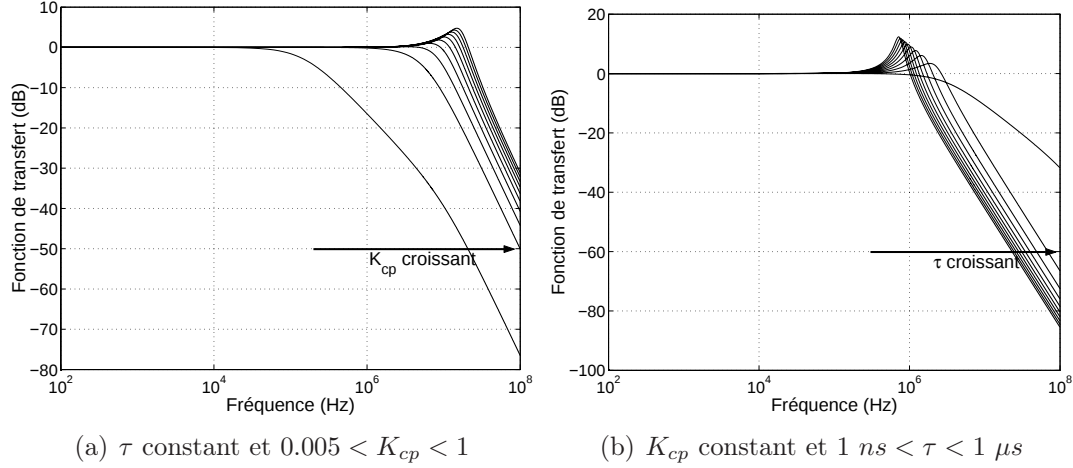


FIG. 2.4 – Fonction de transfert de la PLL pour différents paramètres

Le comparateur de phase peut pratiquement se réaliser de deux manières, soit analogique, soit numérique. Le phasemètre par produit, le pont de phase et le modulateur en anneau sont des systèmes analogiques alors que les phasemètres à bascule RS ou à OU-exclusif sont de type numérique.

- Le phasemètre par produit est le montage le plus simple mais son gros désavantage est sa dépendance aux amplitudes des signaux d'entrée
- Le pont de phase, comme le modulateur en anneau, met en œuvre un ou deux transformateurs, ce qui permet d'avoir une isolation galvanique entre les entrées et la sortie du comparateur de phase (application à l'électronique de puissance).
- Les phasemètres numériques sont les plus utilisés. Ils n'ont pas les inconvénients des phasemètres analogiques mais il existe une différence entre le phasemètre à bascule RS et le phasemètre à OU-exclusif. Le premier fournit une différence de phase absolue variant entre 0 et 2π rad (fig.2.5(a)), alors que la pente change de signe entre $0/\pi$ rad et $\pi/2\pi$ rad (fig.2.5(b)) pour le OU-exclusif.

Il est important de souligner que ces phasemètres ont une réponse non linéaire [35, 36] comme la figure 2.5(b) peut le montrer. Ainsi, en boucle fermée, il est possible pour certaines conditions de générer un signal chaotique [37]. De nombreuses études ont déjà porté sur la réalisation d'oscillateurs chaotiques à base d'une PLL. Le chaos issu de ce

type de montage est toutefois de basse dimension.

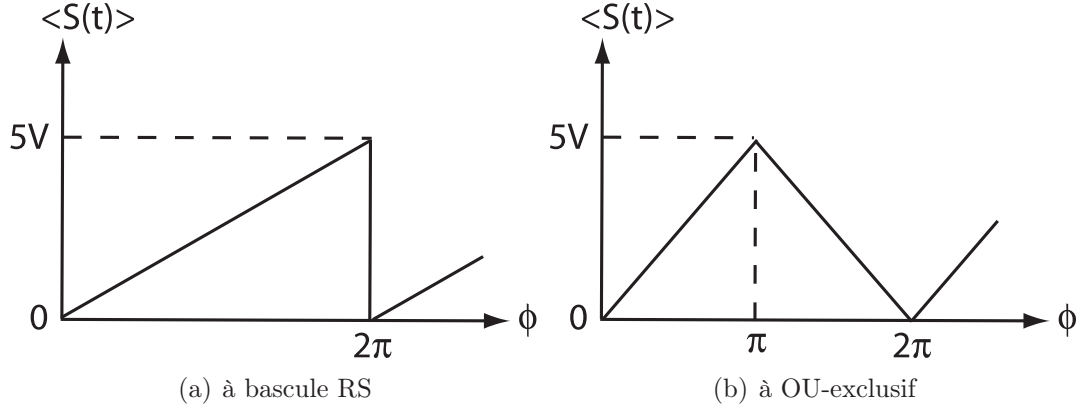


FIG. 2.5 – Différents phasemètres numériques

Pour les comparateurs de phase numériques, la zone de capture¹⁰ est plus petite que la zone de maintien¹¹. Cependant, il existe certains composants pour lesquels les deux zones sont confondues. Leur fonctionnement s'inspire de bascules JK. Pour cela, il est nécessaire que, lors d'un changement brutal de la fréquence de référence, le comparateur de phase fournisse un signal dont le signe ne dépende d'abord que de l'écart de fréquence, puis lorsqu'elles sont devenues égales, il joue son rôle habituel de comparateur de phase. C'est le principe du comparateur de phase/fréquence [38].

Dans la conception du démodulateur chaotique, une PLL sera utilisée. Les performances du démodulateur sont liées aux qualités de la PLL qui viennent d'être évoquées.

2.2.4 Les antennes de transmission

Les antennes de transmission permettent la propagation électromagnétique en milieu libre d'un point à un autre, sans la présence d'un câble. Les transmissions hertziennes peuvent être définies comme l'exploitation du spectre électromagnétique en champ libre pour effectuer de la transmission d'informations (cryptée ou non). De nombreuses applications trouvent leur compte dans cette méthode de transmission comme la diffusion (TV, radiophonie, signalisation...), la liaison point à point (ponts radio, liaisons satellites), l'accès fixe (la boucle locale -radio ou satellite-), les radio mobiles (radio taxi, médecins...), les réseaux cellulaires (la téléphonie mobile, les réseaux radio).

C'est en 1887 que le physicien allemand Hertz observe les ondes électromagnétiques prédites par l'anglais Maxwell. A partir de 1890, l'italien Marconi s'intéressa à la télégraphie sans fil, et, dès 1895, utilisant l'oscillateur de Hertz, le cohéreur de Branly et

¹⁰zone dans laquelle les phases d'entrée et de sortie passent d'un état désynchronisé en un état synchronisé

¹¹zone dans laquelle les phases sont maintenues synchronisées

l'antenne de Popov, il construisit un émetteur capable de transmettre un signal radio à quelques kilomètres de distance [39].

Les antennes sont des éléments transformant un signal électrique en une onde électromagnétique (émission) ou le contraire (réception). Il est important de connaître leur impédance, leur gain et leur directivité.

Un conducteur électrique fournit de l'énergie sous forme de chaleur (chauffage), ou de lumière (lampe). De même il fournit un champ magnétique (principe du transformateur) et électrique (principe du condensateur, du tube cathodique). Le principe de l'antenne d'émission est de faire en sorte que le champ électromagnétique soit important, sans chauffer ni s'illuminer. Ce champ se propage en milieu libre, c'est alors une onde électromagnétique non guidée.

Pour mieux comprendre le fonctionnement d'une antenne, nous allons décrire plusieurs types d'antenne qui ont des particularités différentes.

Différents types d'antenne

Plusieurs types d'antenne existent suivant les applications pour lesquelles elles seront utilisées [40].

L'antenne la plus connue est de type dipôle demie onde. C'est une ligne de transmission terminée par un circuit ouvert dont la longueur est égale au quart de la longueur d'onde de la porteuse (fig.2.6(a)). Lorsque cette ligne est dépliée, elle mesure alors une demie longueur d'onde.

Un autre type d'antenne est l'antenne «ground plane» (fig.2.6(b)). C'est l'antenne précédente dont un des deux brins est le sol. C'est une antenne verticale.

Enfin, un troisième type d'antenne est l'antenne Yaggi (fig.2.6(c)). Il s'agit de l'antenne la plus courante en Ultra Haute Fréquence (UHF). Elle est constituée d'un dipôle 1/2 onde, d'un ou plusieurs directeurs et d'un réflecteur. Le tout est maintenu par un isolant. Sa directivité dépend du nombre de directeurs.

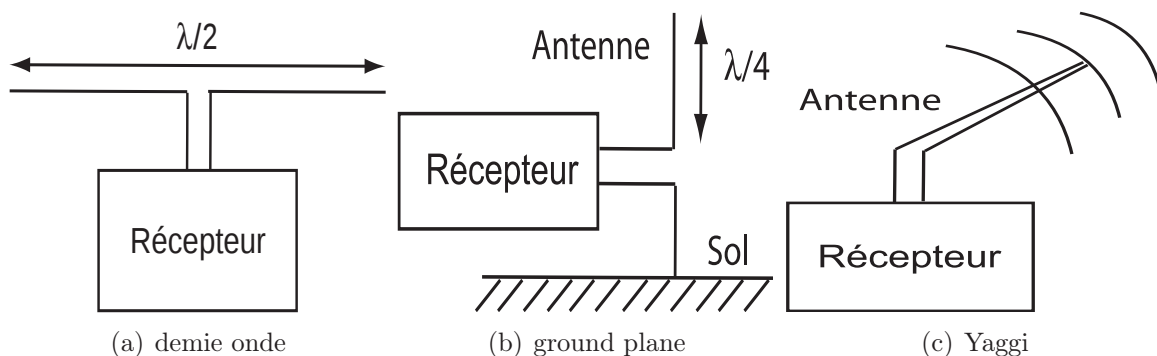


FIG. 2.6 – Différents types d'antenne

Selon la puissance d'émission et la puissance de réception désirées, on peut calculer une portée théorique en onde directe. Malheureusement, l'onde est réfléchiée par le sol, les murs. Cette réflexion peut entraîner de la diffraction [41]. Pour tout cela, la théorie n'est valable qu'à 60% près. En dépit de propriétés bien particulières à chacun des types présentés, les différentes antennes n'échappent guère à cette règle simple selon laquelle la directivité est d'autant plus élevée que leurs dimensions sont grandes par rapport à la longueur d'onde.

Le champ électromagnétique, rayonné à grande distance r , dans la direction $\vec{u}$, par une antenne s'exprime en fonction de la caractéristique vectorielle du rayonnement $\vec{F}$, liée à la structure de l'antenne. Ce champ décroît comme l'inverse de la distance r en champ lointain. En régime harmonique, cela s'écrit :

$$\vec{E}(r, \vec{u}) = \frac{\exp(j(\omega t - kr))}{r} \vec{F}(\vec{u}) = \frac{\exp(j(\omega t - \frac{r}{c}))}{r} \vec{F}(\vec{u}) \quad (2.11)$$

Ce rayonnement est constitué par le champ électromagnétique qui se propage dans l'espace par le biais de l'inductance et de la capacité de l'espace libre. En supposant l'émission ponctuelle et l'antenne totalement omnidirectionnelle, on peut supposer que le rayonnement se propage de manière identique dans toutes les directions. Pour donner une image cela ressemble à un ballon que l'on gonfle et qui voit son diamètre augmenter. Comme la puissance émise est constante, que la surface occupée par le rayonnement ne fait que croître, la densité de puissance diminue au fur et à mesure que l'on s'éloigne de la source d'émission. C'est ce que l'on appelle l'atténuation en espace libre qui est en d^{-2} , où d est la distance de transmission. Cette atténuation est cependant moins importante que les autres modes de transmission pour de longues distances (voir figure 2.1 page 54).

Pour une longueur donnée, vérifiant $l \ll \lambda$ (approximation du doublet de Hertz) et en utilisant la loi de Biot et Savart, le champ à grande distance d'un élément de courant $i = I_0 \exp(j\omega t)$ pour les conventions des coordonnées sphériques (θ : colatitude et ϕ : longitude) est le suivant :

$$\begin{cases} \vec{E} = \frac{\eta I_0 l \sin \theta}{2 \lambda r} \exp(j\omega (t - r/c)) \vec{u}_\theta \\ \vec{H} = \frac{I_0 l \sin \theta}{2 \lambda r} \exp(j\omega (t - r/c)) \vec{u}_\phi \end{cases} \quad (2.12)$$

Nous remarquons que les champs sont proportionnelles à $1/\lambda$ et par conséquent à la fréquence f . La puissance rayonnée est donc proportionnelle à f^2 ou ω^2 . Ceci explique que les lignes, et en particulier les lignes ouvertes, soient limitées en fréquence d'utilisation à cause de la perte d'énergie par rayonnement.

Les calculs ne sont pas d'un intérêt fondamental pour la compréhension de cette partie

c'est pourquoi nous n'allons pas revenir sur ceux-ci.

Les deux systèmes, électronique et optoélectronique, mis en œuvre concernant la cryptographie par chaos en fréquence, ont des applications aux transmissions hertziennes. L'un des avantages pratiques de l'augmentation des fréquences de transmission est la réduction de la taille des antennes. En effet, les antennes $\lambda/2$ que nous utilisons ont une taille moyenne de 30 m, 15 cm et 10 cm pour des fréquences de transmission respectives de 5 MHz, 1 GHz et 1.5 GHz. Esthétiquement parlant, nous observons l'importance de ce changement de fréquence dans la téléphonie mobile notamment.

2.3 Système électronique de cryptographie par chaos

Un premier système de cryptographie par chaos en fréquence a été conçu au laboratoire [42, 43]. Il s'agit d'un système électronique. Une partie du travail de thèse a permis d'optimiser le fonctionnement de ce dernier système pour pouvoir développer plus facilement un système fonctionnant pour des hautes fréquences.

Inspiré des systèmes optoélectroniques non linéaires à retard décrits précédemment, ce premier oscillateur chaotique en fréquence possède uniquement des fonctions électroniques qui lui permettent d'émettre un signal chaotique en fréquence d'une grande stabilité (fig.2.7) permettant de masquer l'information.

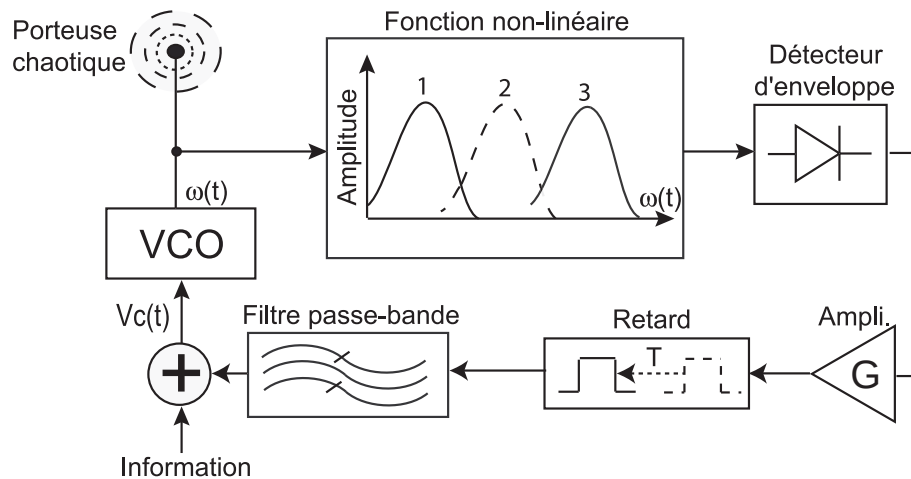


FIG. 2.7 – Oscillateur chaotique en fréquence

D'un point de vue physique, sa réalisation est basée sur des fonctions électroniques relativement simples. Cependant, le signal issu de l'oscillateur est complexe. Il est déterministe, et peut être mathématiquement décrit par la relation suivante, dans le cas d'un filtre sélectif passe-bande dans la chaîne d'oscillation :

$$\tau_1 \cdot \tau_2 \cdot \frac{d^2 \Delta \omega}{dt^2}(t) + (\tau_1 + \tau_2) \frac{d \Delta \omega}{dt}(t) + \Delta \omega(t) = \tau_1 \cdot \beta \frac{dF_{nl}[\Delta \omega(t - T)]}{dt} \quad (2.13)$$

où T est le retard, F_{nl} une fonction non linéaire, τ_1 et τ_2 les constantes de temps basses et hautes du système introduites par le filtrage passe-bande, et β l'amplification normalisée.

Par la suite, nous allons décrire l'ensemble des fonctions qui constituent l'oscillateur chaotique : le retard, la fonction non linéaire, le convertisseur U/f , et le type de filtrage.

2.3.1 Conversion de la dynamique chaotique

La conversion du chaos en bande de base en un signal chaotique en fréquence est effectuée par un oscillateur dont la fréquence est contrôlée en tension.

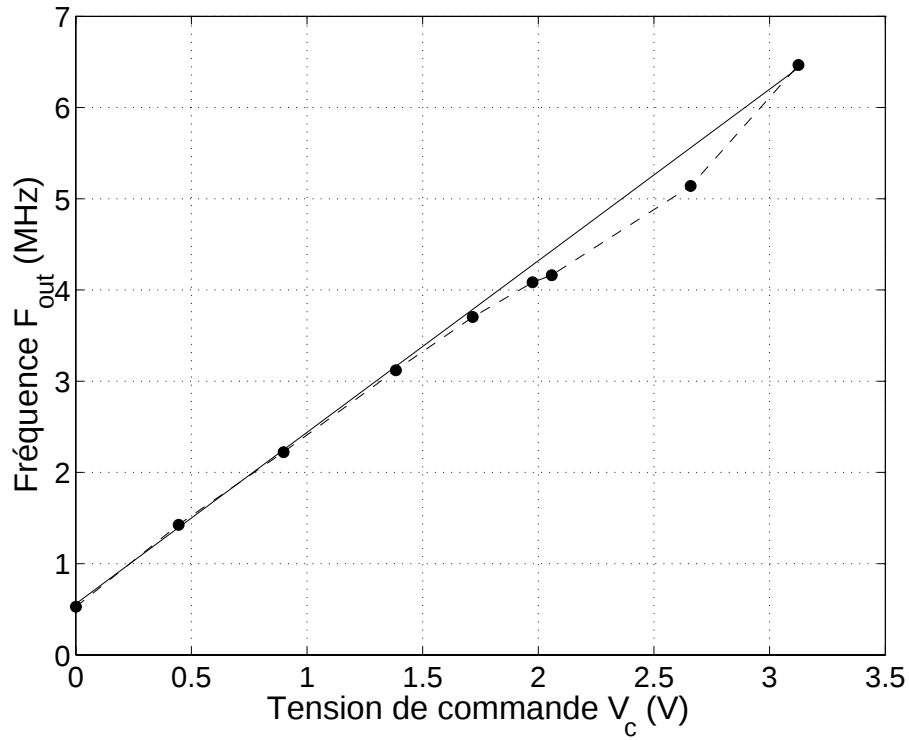


FIG. 2.8 – Sensibilité du VCO

Une régression linéaire à partir du relevé de la caractéristique expérimentale (fig.2.8) donne la fonction qui régit la conversion linéaire du VCO (2.14).

$$f_{out}(\text{MHz}) = 1.8(\text{MHz/V}) V_c(\text{V}) + 0.56(\text{MHz}) \quad (2.14)$$

Le VCO joue le rôle de convertisseur entre le chaos en bande de base V_c et le chaos en fréquence f_{out} avec une efficacité de conversion $S = 1.8 \text{ MHz/V}$, et une fréquence centrale $f_0 = 0.56 \text{ MHz}$. Dans l'ensemble des mesures suivantes c'est le chaos en bande de base

qui sera observé. En effet, celui-ci est relié à la dynamique chaotique (fréquence) par la sensibilité du VCO. Nous verrons par la suite l'influence de la PLL qui, utilisant le même VCO, va permettre de compenser les dérives en fréquence du récepteur sur l'émetteur.

La fréquence issue du VCO va être injectée dans la fonction non linéaire. Ainsi, l'excursion en fréquence est fonction du gain de la boucle d'oscillation. Celle-ci est typiquement comprise entre 500 kHz et 1 MHz.

2.3.2 La fonction non linéaire

La fonction non linéaire $F_{nl}[\omega]$ est réalisée par trois filtres passe-bande résonants actifs (dans la gamme de fréquence correspondant à celle du signal de sortie du VCO) dont la contre-réaction est effectuée avec une inductance, une capacité et une résistance (filtres RLC¹² parallèle) comme représentés sur la figure 2.9. Il est difficile de parler de fonctionnement non linéaire lorsque sont concernés des filtres qui sont à la base des systèmes linéaires. En effet, si l'entrée d'un système linéaire est une sinusoïde alors sa sortie est une sinusoïde de même fréquence et d'amplitude plus ou moins grande. Dans notre cas, les variables concernées en entrée et en sortie sont respectivement la fréquence et l'amplitude (et non amplitude et amplitude comme dans l'approche classique des filtres).

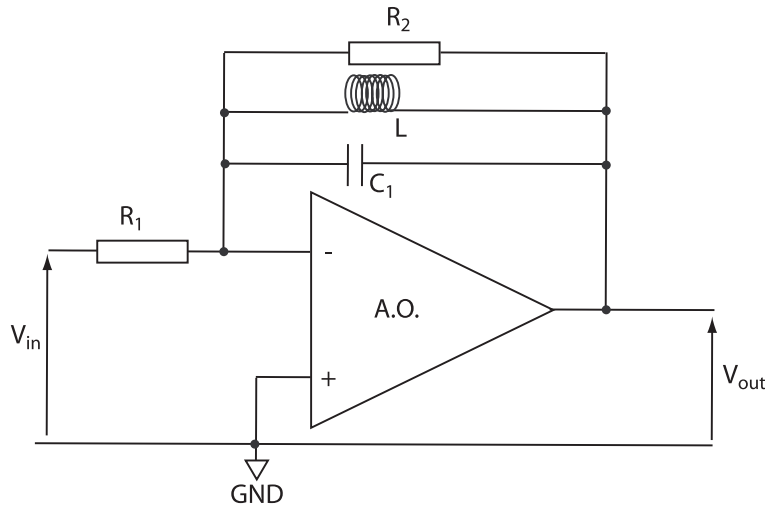


FIG. 2.9 – Circuit résonant pour un pic de la non linéarité

Après avoir traversé les filtres passe-bande résonants, la modulation de fréquence initiale générée par le VCO va présenter des variations non linéaires d'amplitude portées par la fréquence de modulation du VCO autour de 4 MHz. Ensuite, cette porteuse est éliminée à l'aide d'un démodulateur d'amplitude. L'entrée et la sortie de cet élément non linéaire est :

¹²Résistance-Inductance-Capacité

$$\mathcal{A}(t) = F_{nl}[f(t)] \quad (2.15)$$

où la fonction non linéaire F_{nl} représente le profil de filtrage des cellules RLC parallèles

La non linéarité, pour une variation linéaire de la fréquence de modulation, est représenté sur la figure (2.12) pour une fréquence centrale de modulation voisine de 4.3 MHz, et une excursion en fréquence linéaire $\Delta f = 500$ kHz.

La fonction non linéaire est décrite par la relation mathématique (2.16). Celle-ci est composée de fréquences de résonance f_i , de facteurs de qualité Q_i et de gains G_i dont l'indice i est la référence du pic résonant (1, 2 ou 3). Elle correspond à la superposition des différentes résonances.

$$F_{nl}[f(t)] = \left| \sum_{i=1}^3 \frac{g_i Q_i}{1 - jQ_i \left(\frac{f(t)}{f_i} - \frac{f_i}{f(t)} \right)} \right| \quad (2.16)$$

Démodulateur d'amplitude

Ce circuit est suivi d'une démodulation d'amplitude afin d'extraire l'enveloppe en éliminant la porteuse.

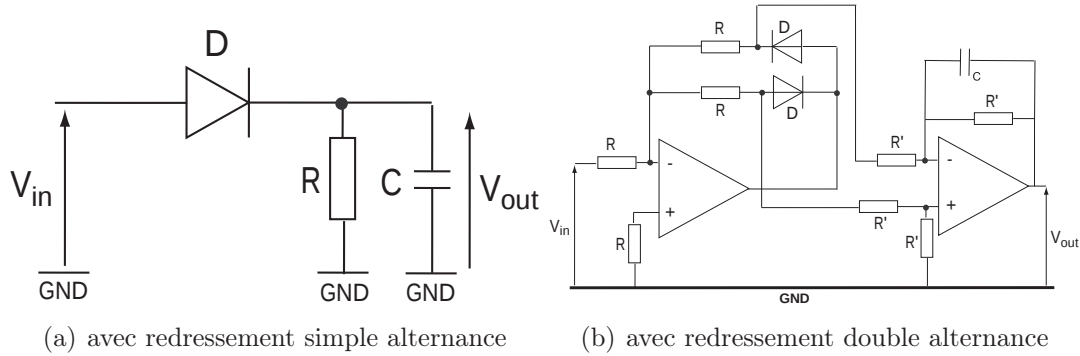


FIG. 2.10 – Systèmes de détection d'enveloppe

En effet, la figure 2.11(a) montre la non linéarité avant la détection d'enveloppe pour une modulation de fréquence linéaire. Le signal observé peut être comparé à une modulation d'amplitude à la différence près que la fréquence de la porteuse n'est pas constante. Le signal peut donc être défini par la relation suivante :

$$s(t) = A.(1 + m u(t)) \cos((\Delta\omega(t) + \omega_0) t) \quad (2.17)$$

Dans ce genre de modulation, et contrairement à la modulation d'amplitude standard, le signal modulant $u(t)$ et la fréquence de la porteuse $\omega(t) = \Delta\omega(t) + \omega_0$ sont dépendants. En effet, selon la valeur de $\omega(t)$, $u(t)$ aura une valeur différente. Il est nécessaire de

pouvoir supprimer cette porteuse pour ne conserver que l'enveloppe du signal. L'indice de modulation m est défini par la relation suivante :

$$m = \frac{\Delta s}{2A} \quad (2.18)$$

avec Δs l'excursion en amplitude et $2A$ l'amplitude lorsque $u(t) = 0$. Lorsque cet indice de modulation est inférieur à 1, la démodulation peut s'effectuer par détection d'enveloppe. Il s'agit d'une démodulation non cohérente ou asynchrone (fig.2.10).

Le problème du circuit utilisant un redressement simple alternance est de dimensionner au mieux le circuit RC pour que la tension de sortie s'approche au mieux de la forme de l'enveloppe. Lorsque l'écart entre la fréquence porteuse et la fréquence maximum du signal modulant (interférences) diminue, le comportement de la non-linéarité va changer : l'enveloppe dépend en effet de la vitesse de modulation de la fréquence. Nous reviendrons ultérieurement sur cet aspect critique de la non linéarité.

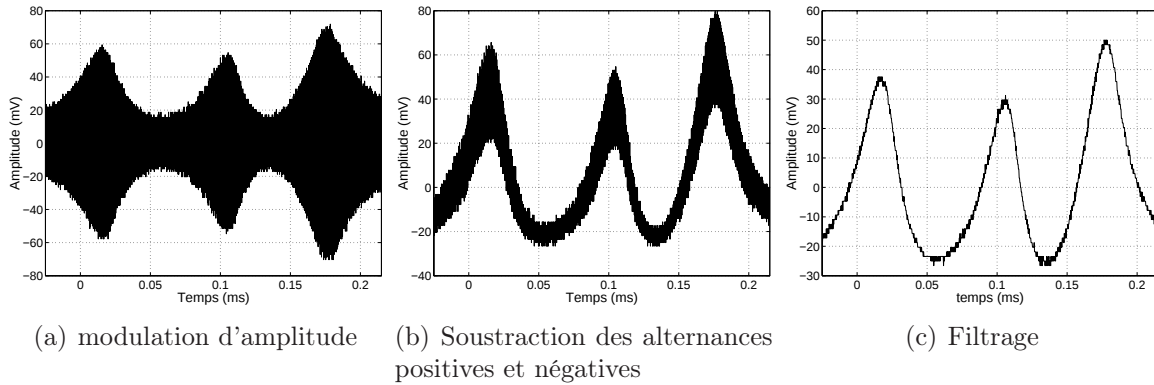


FIG. 2.11 – Détection d'enveloppe

Un amplificateur opérationnel avec des diodes montées tête-bêche en contre-réaction (fig.2.10(b)) va permettre d'extraire les alternances positives et négatives pour, ensuite, les soustraire l'une par rapport à l'autre (fig.2.11(b)). Pour éliminer complètement le signal haute fréquence, on utilise un filtre pour obtenir le signal représenté sur la figure 2.11(c). Ce filtre a une fréquence de coupure $f_c = 8$ kHz. Cette fréquence de coupure fixe la limite haute de la dynamique en bande de base.

Les acquisitions sont sensiblement différentes suivant les relevés expérimentaux (fig.2.12(b)) et théoriques (fig.2.12(a)). Les effets capacitifs et inductifs respectivement des inductances et des capacités qui sont nécessaires à la réalisation des circuits résonants, sont des composants très facilement perturbables (CEM, tolérance du composant...).

Intuitivement, ce genre de fonction non linéaire est réalisable de manière robuste et reproductible uniquement autour d'une gamme de fréquence faible (4 MHz dans notre

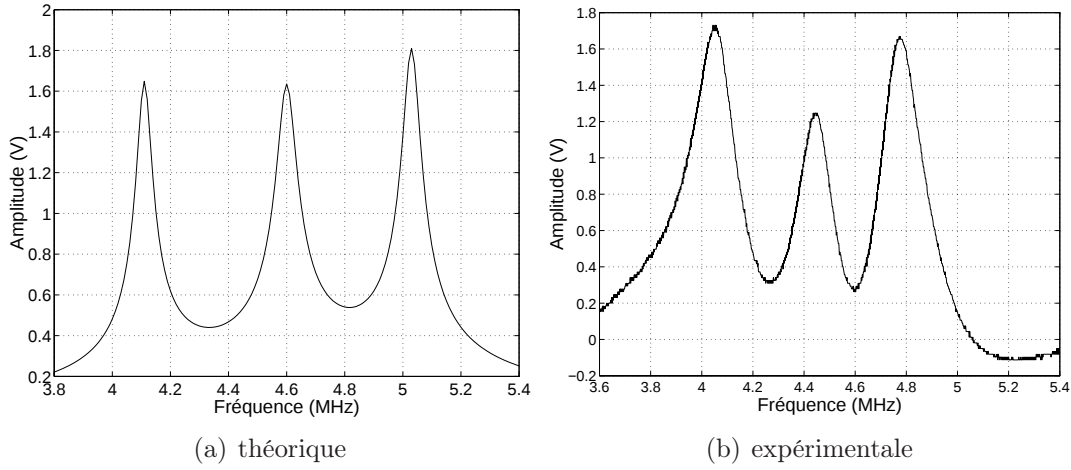


FIG. 2.12 – Non-linéarités

système). En effet, le facteur de qualité va sérieusement augmenter avec la fréquence de modulation ce qui va entraîner des problèmes de conception ; il y aura de plus d'autres problèmes de conception pour reproduire cette non linéarité à l'identique en vue d'une synchronisation pour une application à la cryptographie. Les caractéristiques des trois pics résonants de chacun des filtres RLC sont répertoriées dans le tableau 2.2.

	théorie			pratique		
pics de resonance	pic 1	pic 2	pic 3	pic 1	pic 2	pic 3
fréquence de résonance (MHz)	4.11	4.6	5.03	4.6	5.1	5.3
facteur de qualité	75	65	78	37	44	42.3
gain	0.1	0.11	0.105	1	1.5	1

TAB. 2.2 – Caractéristiques des filtres résonants

En reliant le facteur de qualité Q_i , le gain g_i et la fréquence de résonance f_i (2.16) au montage (fig.2.9), chacun des pics de résonance est défini par les composants électroniques suivants :

$$g = \frac{R_2}{R_1}, \quad f = \frac{1}{2\pi\sqrt{LC}}, \quad Q = R_2\sqrt{\frac{C}{L}} \quad (2.19)$$

2.3.3 Retard temporel

Le retard est réalisé en bande de base, ou basse fréquence, par une mémoire analogique CCD fonctionnant à une fréquence d'horloge de $F_h = 1$ MHz délivrée par un oscillateur à quartz. Cette ligne à retard par mémoire analogique CCD fonctionne comme un vecteur de $N = 1024$ éléments dont chaque charge représente un échantillon du signal à retarder. Un décalage d'échantillon dans la mémoire intervient toutes les deux périodes d'horloge.

Ainsi, le retard vaut $T = 2N/F_h$. Par conséquent, le retard temporel vaut théoriquement $T = 2.048$ ms.

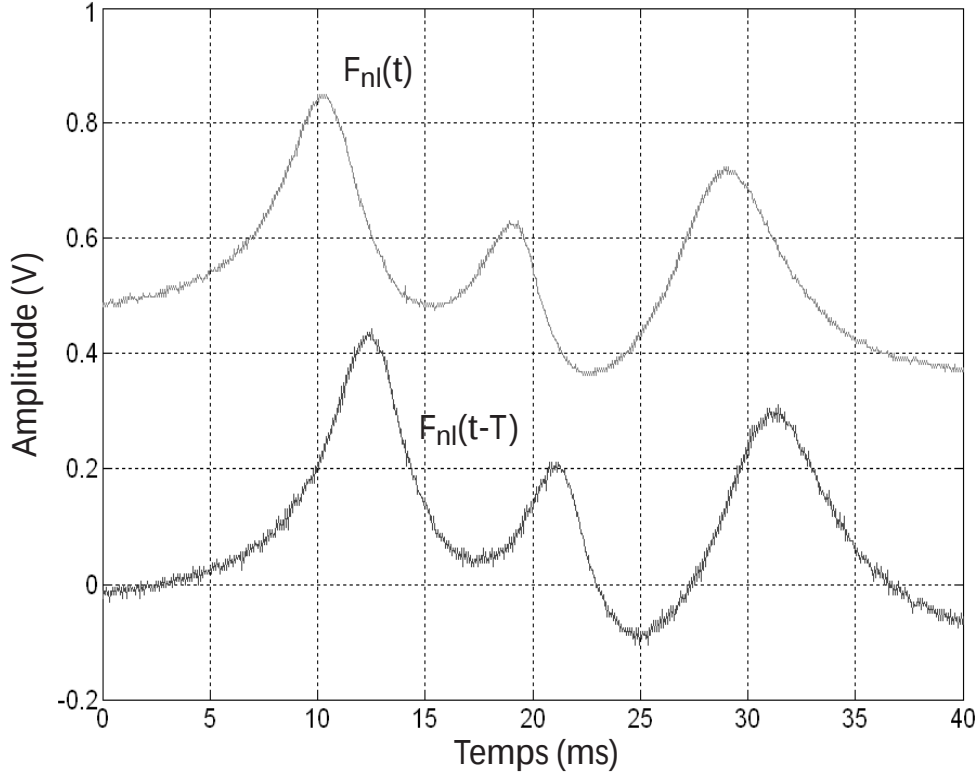


FIG. 2.13 – Retard temporel engendré par la mémoire analogique

La fréquence d'horloge délivrée par le quartz peut entraîner un bruit de décodage. En effet, les dérives à court terme - c'est à dire le bruit de phase ou de fréquence - de chaque oscillateur à quartz modifie très légèrement la valeur du retard temporel. Or, ce paramètre est la clé de codage la plus sensible [44]. En effet, une légère dérive rend très rapidement le décodage impossible. Il est cependant important de préciser la stabilité du résonateur à quartz compatible TTL dont la précision est 0.01% à 25°C , ce qui entraîne une différence maximale d'environ $0.2\mu\text{s}$ sur la valeur du retard ; cet écart sera pratiquement tout à fait négligeable (erreur relative de 10^{-4}).

2.3.4 Filtre assurant la dynamique limitante du système en bande de base

Ce filtre utilisé est un passe-bande dont les caractéristiques sont des fréquences de coupure basse et haute de $f_1 = 498$ Hz et $f_2 = 8.67$ kHz. Ce choix est arbitraire, et permet de fixer, à l'intérieur de la bande passante de la détection d'enveloppe, la bande de base dans laquelle un comportement chaotique est généré.

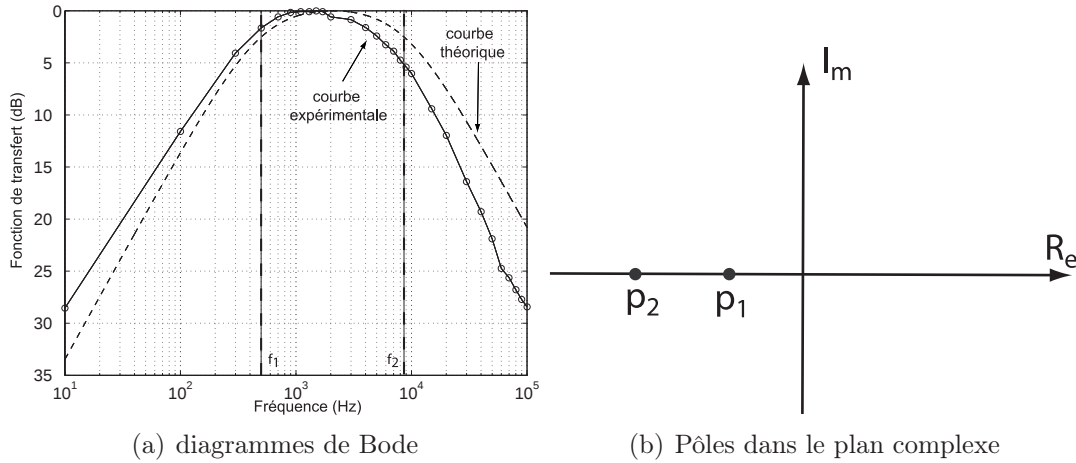


FIG. 2.14 – Caractéristiques du filtre passe-bande en bande de base

Un tel système peut être considéré comme la mise en cascade de deux systèmes du premier ordre passe-bas et passe-haut de constantes de temps respectives $\tau_1 = 2$ ms et $\tau_2 = 115$ μ s (2.20). En effet, il s'agit d'un système sur amorti dont le coefficient d'amortissement vaut $z > 1$. Ainsi, la réponse indicielle du filtre n'aura aucune oscillation, il s'agira d'une réponse apériodique. De ce fait, les pôles dans le plan complexe sont réels négatifs (fig.2.14(b)). Ainsi, la fonction de transfert dans le domaine de Laplace est définie par :

$$H(p) = \frac{U(p)}{V(p)} = \frac{G(\tau_1)p}{(1 + \tau_1 p)(1 + \tau_2 p)} \quad (2.20)$$

Si $V(p)$ et $U(p)$ sont respectivement les entrée et sortie de ce filtre, les règles de passage entre les domaines de Laplace et temporel nous permettent de dériver de ce filtre l'équation différentielle reliant $v(t)$ et $u(t)$:

$$u(t) + (\tau_1 + \tau_2) \frac{du}{dt}(t) + \tau_1 \tau_2 \frac{d^2u}{dt^2}(t) = G \tau_1 \frac{dv}{dt}(t) \quad (2.21)$$

En posant $S = \Delta\omega(t)/u(t)$, $\beta = SG$ et $v(t) = F_{nl}[\Delta\omega(t)]$, on montre ainsi que l'on retrouve bien la loi dynamique des fluctuations FM de l'oscillateur à retard donné dans l'équation (2.13).

Les diagrammes de Bode théorique et expérimental (fig.2.14(a)) sont légèrement différents (décalage de la fréquence centrale mais pente correcte). Les valeurs de cette dynamique limitante constituent une des clés de codage. Il s'avère donc nécessaire qu'elles soient identiques (ou très proches) entre l'émetteur et le récepteur, pour assurer une bonne synchronisation et, de ce fait, limiter le bruit de décodage de l'information.

2.3.5 Caractérisation du chaos en fréquence de l'oscillateur HF

L'oscillateur décrit par les éléments énoncés précédemment va générer une onde sinusoïdale de fréquence variable (signal FM). Cette fréquence sera la variable dynamique chaotique permettant de masquer l'information à l'intérieur de la porteuse. Nous décrirons le fonctionnement de l'oscillateur chaotique principalement par des mesures expérimentales. Nous verrons l'efficacité de cet oscillateur chaotique appliqué au cryptage de l'information, en transmettant et en décodant une information.

Analyse temporelle et spectrale

La porteuse chaotique est une porteuse haute fréquence (HF) puisque sa gamme de fréquence, bien que proche de la moyenne fréquence, est supérieure à 3 MHz.

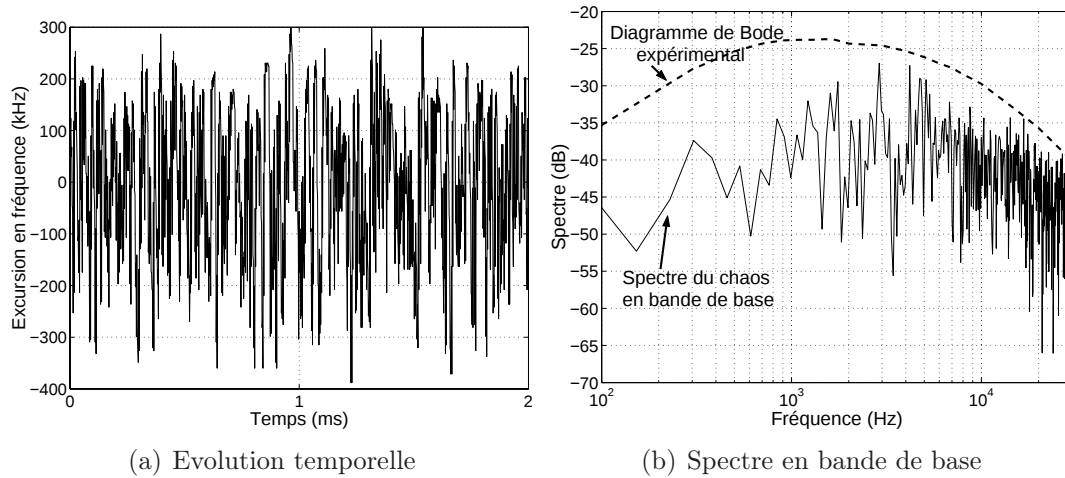


FIG. 2.15 – Evolution temporelle et spectrale du chaos en bande de base

La figure 2.15(a) montre que l'évolution chaotique possède bien l'apparence d'un signal bruité. Le spectre du chaos en bande de base (fig.2.15(b)) est large bande dans la bande passante qui est définie par les bornes du filtre de la dynamique limitante. Sur la base d'une analyse spectrale classique, nous constatons que la porteuse chaotique ne permet de révéler à un espion qu'une estimation grossière des seuls paramètres τ_1 et τ_2 du générateur de chaos (le retard et la non linéarité ne sont pas détectables à ce niveau).

Le spectre représenté sur la figure (2.16) correspond au signal FM chaotique (porteuse hertzienne) qui a l'apparence du spectre d'un bruit rose. Un bruit rose est un bruit blanc filtré. Il aura donc les propriétés d'un bruit blanc mais dans une bande limitée. Son spectre est relativement plat dans la bande de fréquence de la porteuse.

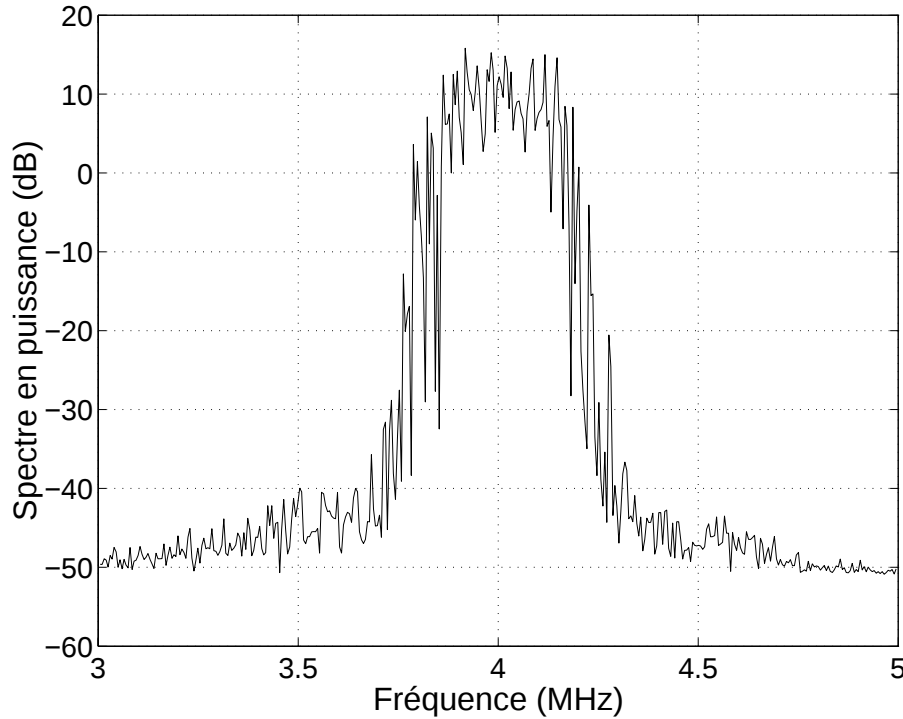


FIG. 2.16 – Spectre de la modulation de fréquence

L'analyse statistique qui va suivre étudie la densité de probabilité des fréquences apparaissant dans la porteuse FM.

Analyse statistique

L'analyse statistique peut s'effectuer de plusieurs manières différentes. Tout d'abord, nous avons déjà vu que les spectres représentés précédemment pouvaient être analysés via leur densité spectrale.

Cependant, en observant la densité de probabilité du chaos émis, nous pouvons remarquer que le type de régime chaotique est différent suivant la valeur de certains paramètres. L'influence du paramètre d'amplification A du générateur est représentée sur le diagramme de la figure 2.17(a) où l'on a repris la notation du chapitre 1 avec un paramètre de gain normalisé β dépendant linéairement du gain électronique A . Nous pouvons observer la succession de bifurcations que provoque l'augmentation progressive de A . La route vers le chaos est la même que celle décrite dans le chapitre 1. En effet, la densité de probabilité liée aux couleurs plus ou moins foncées du diagramme de bifurcation permet d'observer, pour

les faibles valeurs de β , les premiers dédoublements de période des régimes d'oscillation harmoniques ($\beta = 1$ à 2).

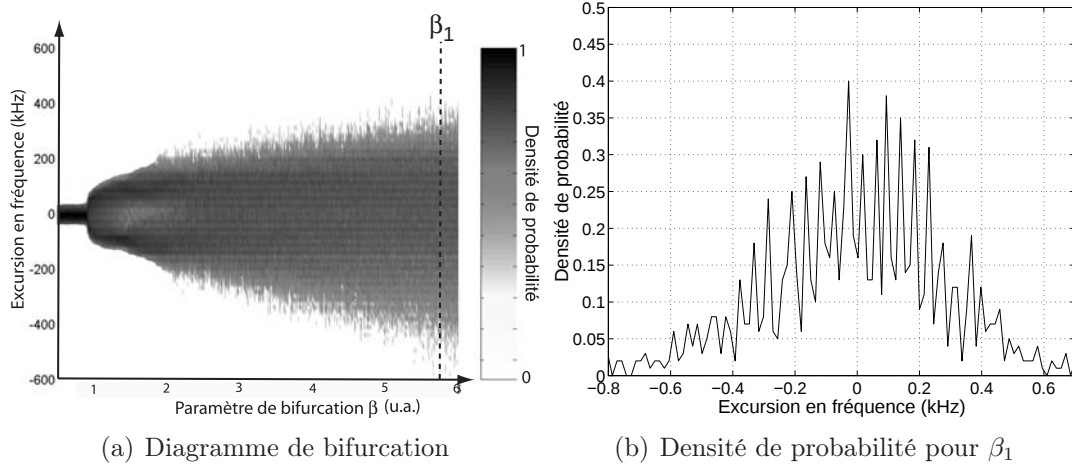


FIG. 2.17 – Diagramme de bifurcation pour $f_0 = 3.7$ MHz, $T = 2$ ms

Le diagramme de bifurcation est issu du calcul des histogrammes qui matérialise la densité de probabilité de chaque signal chaotique pour des amplifications A différentes. Par conséquent, la densité de probabilité a été tracée sur la figure 2.17(b) pour une valeur de gain β caractérisant l'un des nombreux régimes chaotiques. Ce régime peut être distingué sur le diagramme de bifurcation par le curseur noté β_1 .

2.3.6 Système de réception et de réplique du chaos

Ce système est composé des mêmes éléments que l'émetteur détaillé précédemment. Cependant, l'ensemble des fonctions que sont le retard, la non-linéarité, le filtre passe-bande, et la fréquence centrale de modulation qui caractérisent les clés de codage de l'information, sont organisées en boucle ouverte (fig.2.18).

Ces éléments en boucle ouverte vont pouvoir reconstituer localement le chaos en bande de base au récepteur. L'information contenue dans le chaos en fréquence peut être décrite à partir de l'équation différentielle non linéaire à retard (2.13), et en considérant l'insertion du message de manière additive avant le filtre :

$$\begin{cases} \tau_1 \cdot \tau_2 \cdot \frac{d^2 c}{dt^2}(t) + (\tau_1 + \tau_2) \frac{dc}{dt}(t) + c(t) = \tau_1 \cdot \beta \frac{dF_{nl}[\Delta\omega(t - T)]}{dt} \\ a(t) = c(t) + m(t), \Delta\omega(t) = 2\pi S a(t) \end{cases} \quad (2.22)$$

Le système d'équation (2.22) décrit l'évolution du chaos en fréquence contenant l'information. En traversant les mêmes éléments qui ont permis de coder l'information, le chaos $b(t)$ réobtenu au récepteur, en bande de base est décrit par une équation similaire

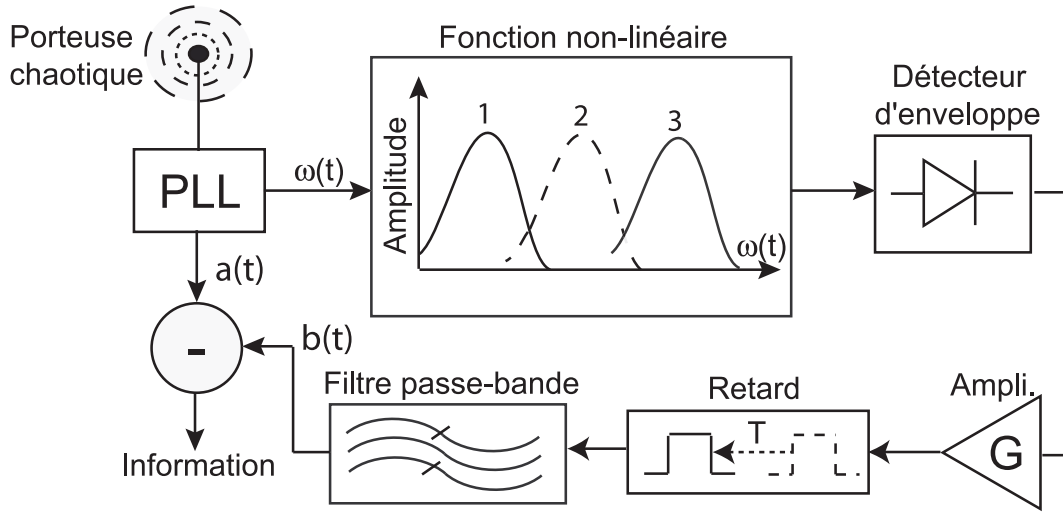


FIG. 2.18 – Synoptique du système de décryptage

à (2.13). Ce chaos répliqué en bande de base ne contient par contre pas l'information, comme on peut s'en apercevoir en écrivant sa loi d'évolution :

$$\tau'_1 \cdot \tau'_2 \cdot \frac{d^2 b}{dt^2}(t) + (\tau'_1 + \tau'_2) \frac{db}{dt}(t) + b(t) = \tau'_1 \cdot \beta' \frac{dF'_{nl}[\Delta\omega(t - T')]}{dt} \quad (2.23)$$

Dans cette dernière expression, $\Delta\omega$ est la modulation de fréquence reproduit par la PLL, et verrouillée sur celle qui est détectée par l'antenne et venant de l'émetteur. Comme décrit à l'équation (2.23), cette modulation de fréquence est directement obtenue par modulation du VCO de l'émetteur par le signal $a(t) = c(t) + m(t)$, c'est à dire $\Delta\omega = S a(t)$. Si les paramètres du récepteur (noté avec un $'$) sont identiques à ceux de l'émetteur, (2.23) est identique à l'équation différentielle de (2.22), et on doit donc avoir $b(t) = c(t)$.

La boucle à verrouillage de phase va permettre également d'extraire le chaos en bande de base $a(t)$ contenant l'information. La soustraction entre les deux signaux chaotiques avec et sans le message permet le décodage de l'information initiale.

La boucle à verrouillage de phase

Les caractéristiques principales d'une PLL se définissent expérimentalement par la bande de maintien et la bande de capture. Ces bandes sont très importantes puisque celles-ci sont notamment liées à l'excursion maximum en fréquence de la porteuse chaotique.

La plage de capture B_c et la plage de maintien B_m vont définir les bornes entre lesquelles la PLL pourra évoluer.

La figure 2.19 montre que la plage de maintien est amplement suffisante pour l'excursion en fréquence de la modulation valant $\Delta f < 1$ MHz. A noter qu'il s'agit d'une boucle à verrouillage de phase avec un comparateur de phase pour lequel $B_m > B_c$. En utilisant

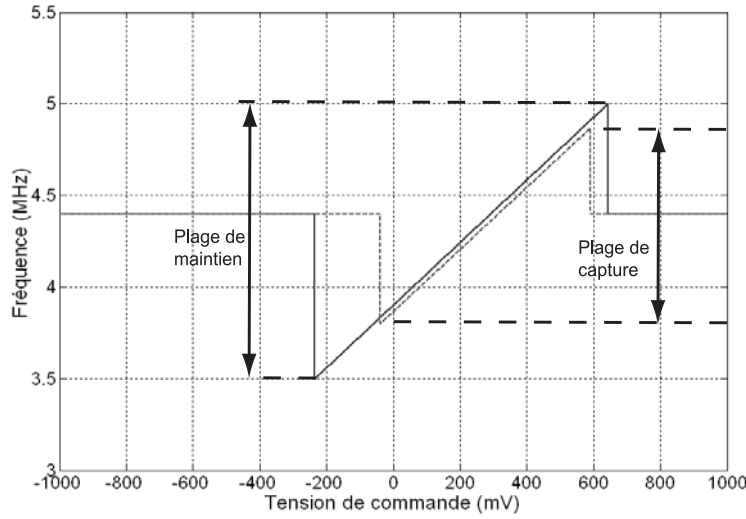


FIG. 2.19 – Plages de capture et de maintien de la PLL

un comparateur de phase/fréquence, la plage de capture augmente jusqu'à être égale à la plage de maintien. Voici quelques relevés expérimentaux permettant d'observer la réponse indicielle.

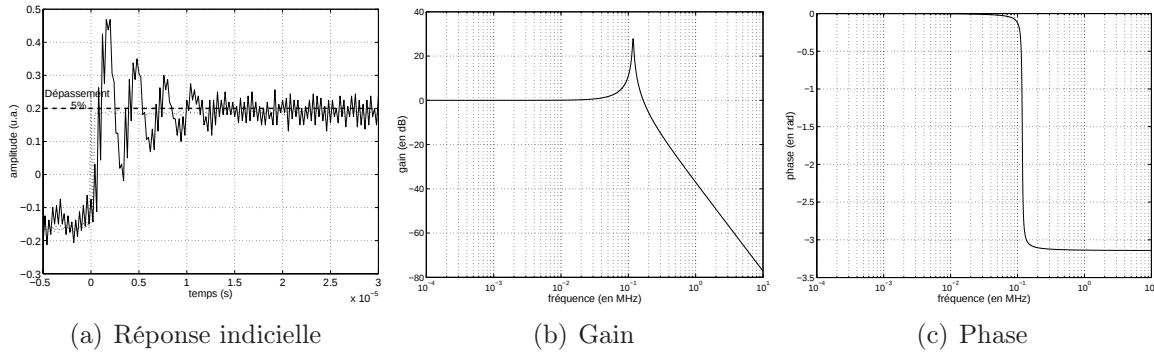


FIG. 2.20 – Caractérisation de la PLL

Les diagrammes de Bode théoriques (fig.2.20(b)) montrent que le circuit bouclé est résonant pour des fréquences de modulation supérieure à la bande passante initiale du chaos en bande de base. Le détecteur de phase est un composant numérique OU-exclusif peu sensible aux variations d'amplitude.

2.3.7 Synchronisation et extraction de l'information

La synchronisation entre les deux systèmes dépend des différences entre leurs paramètres respectifs : l'amplification, les fréquences de coupure du filtre passe-bande, le retard et la fonction non linéaire, qui doivent être les plus proches possibles.

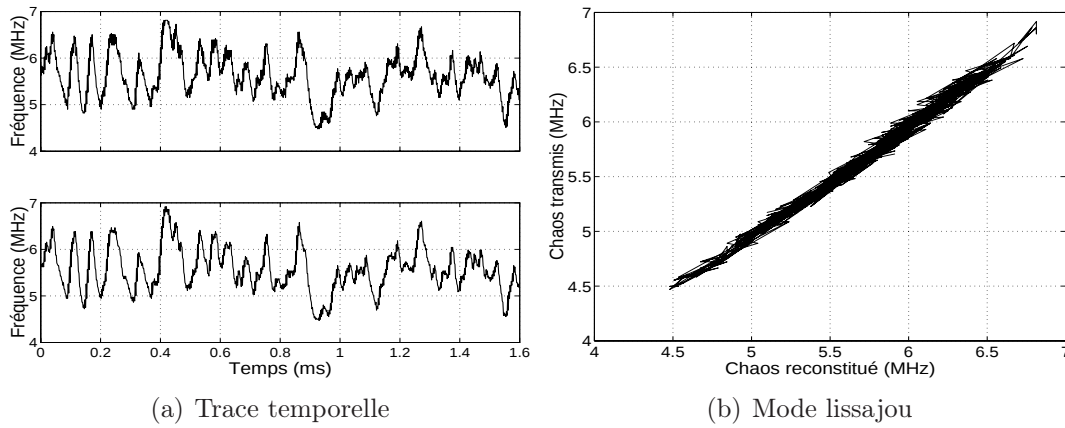


FIG. 2.21 – Synchronisation maître/esclave

Nous pouvons observer la qualité de synchronisation entre le chaos transmis et le chaos reconstitué du côté du récepteur. Deux types de représentations ont été effectuées. L'une décrit les évolutions temporelles du chaos émis et du chaos reconstitué. L'autre représentation a été réalisée pour bien mettre en évidence les propriétés de synchronisation entre l'émetteur et le récepteur. La représentation graphique en mode Lissajou permet d'observer rapidement les erreurs d'accordabilité entre les éléments. Dans le cas d'une synchronisation parfaite (et en l'absence d'information), le mode Lissajou également appelé mode XY doit correspondre à un segment. Dans le cas d'une perte de synchronisation, celui-ci s'élargit pour se transformer en une tache où les évolutions appartenant à chacun des signaux chaotiques s'entrecroisent.

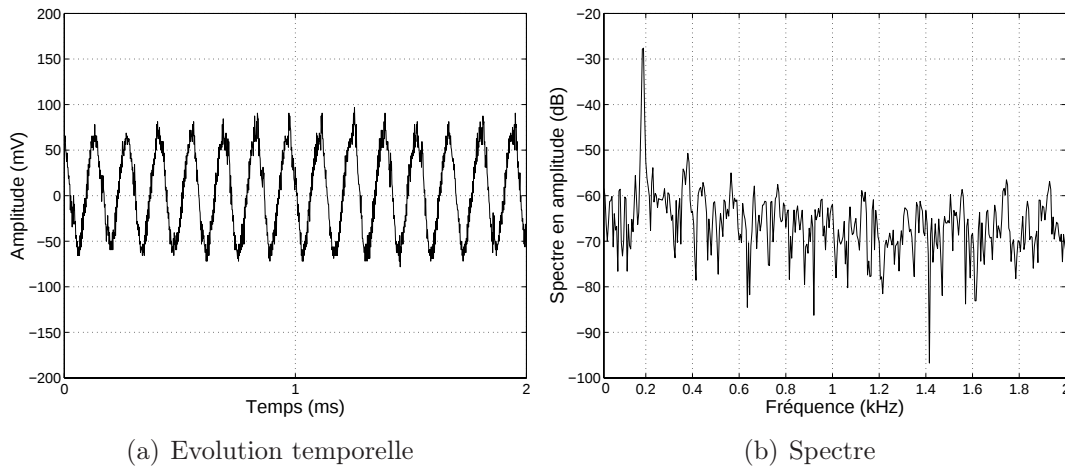


FIG. 2.22 – Message décrypté

Une fois la synchronisation atteinte, le décryptage est chose possible et la qualité de celui-ci peut être mis en avant par le rapport signal sur bruit (2.24). En effet, le rapport

signal sur bruit correspond à l'affaiblissement du signal d'information par rapport au niveau de bruit moyen. Le rapport signal/bruit indique l'écart de niveau qui existe entre un signal d'amplitude maximale (à la puissance RMS) et le bruit de fond généré par le circuit électronique de réception réalisant la synchronisation et le décryptage. En effet, au bruit du circuit s'ajoutera le bruit de décryptage dû à la synchronisation approximative.

En considérant le signal d'information $s(t) = m(t) + n(t)$ où $n(t)$ est le bruit engendré par la transmission et le bruit de décodage dû à une accordabilité approximative des clés de codage, le rapport signal/bruit est défini de la manière suivante :

$$SNR(dB) = 10 \log_{10} \left(\frac{P_m}{P_n} \right) \quad (2.24)$$

où P_m est la puissance efficace du signal $m(t)$ et P_n la puissance efficace du bruit. Dans notre cas, ce signal vaut pour le système électronique réalisé :

$$SNR \approx 31 \text{ dB}$$

Pour mieux observer l'influence du bruit sur un signal temporel (fig.2.22(a)), le SNR peut être tracé pour un signal d'information d'amplitude constante (0.5 V ou 1 V) mais pour une valeur moyenne du bruit qui varie (fig.2.23).

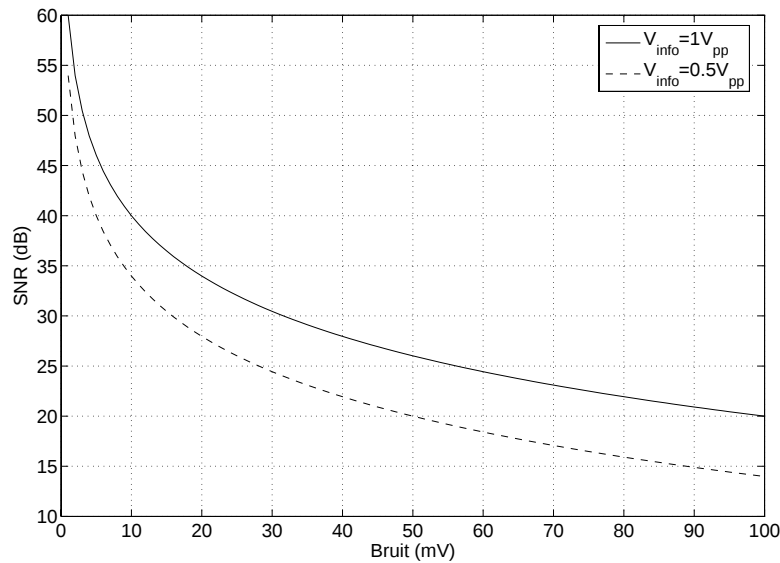


FIG. 2.23 – Rapport signal/bruit en fonction de l'amplitude de chacun des signaux

Nous pouvons simplement comprendre qu'en augmentant l'amplitude du signal d'information, nous allons naturellement augmenter le SNR. Cependant, si l'information a une amplitude trop grande, son masquage par la porteuse chaotique de même amplitude

sera moins efficace, et la sécurité du cryptage par chaos en sera diminuée. Le compromis des deux paramètres est nécessaire.

2.3.8 Perspectives d'adaptation aux fréquences UHF

Présentant de nombreux avantages, le système décrit précédemment possède aussi quelques inconvénients. La fréquence centrale de modulation est trop faible pour pouvoir proposer une transmission hertziennne dans les bandes de fréquences correspondant à l'utilisation actuelle du spectre électromagnétique. Ce problème est essentiellement lié à la réalisation de la non linéarité et de sa copie conforme pour la synchronisation du récepteur. Les effets capacitifs et inductifs des composants vont rendre très difficile le contrôle précis des caractéristiques des composants pour les hautes fréquences. Ainsi, la synchronisation entre le chaos généré par l'émetteur et le chaos reproduit du côté du récepteur sera difficile ou impossible à cause des problèmes de précision d'ajustement de la non linéarité.

Plusieurs solutions ont été mises en avant pour pouvoir translater la fréquence de quelques MHz au GHz, notamment par la multiplication de la fréquence de la porteuse, en utilisant un système électronique permettant de générer une porteuse aux fréquences désirées à partir du chaos en bande de base. Une autre solution était l'utilisation d'un changeur de fréquence à partir d'une boucle à verrouillage de phase.

Les solutions précédentes sont toutes très efficaces pour la conception d'un oscillateur UHF, mais deviennent plus délicates pour des applications à la cryptographie par chaos. Au bruit intrinsèque des composants et au bruit de transmission viennent s'ajouter les effets de stabilité de la fréquence centrale. Pour cette raison, nous avons préféré réaliser un nouvel oscillateur permettant de générer directement une dynamique chaotique aux fréquences désirées, en changeant certaines fonctions telles que la non linéarité et le retard.

2.4 La cryptographie par chaos UHF : système d'interférences RF

L'oscillateur chaotique en fréquence est une boucle non linéaire à retard capable d'émettre une porteuse chaotique en modulation de fréquence, comportement qui est obtenu pour un gain de boucle suffisant (fig.2.24).

L'oscillateur chaotique en fréquence est composé des éléments suivants :

- Une non linéarité réalisée à partir d'interférences RF utilisant des composants optoélectroniques
- Un retard temporel réalisé par une fibre optique d'une longueur de deux kilomètres.

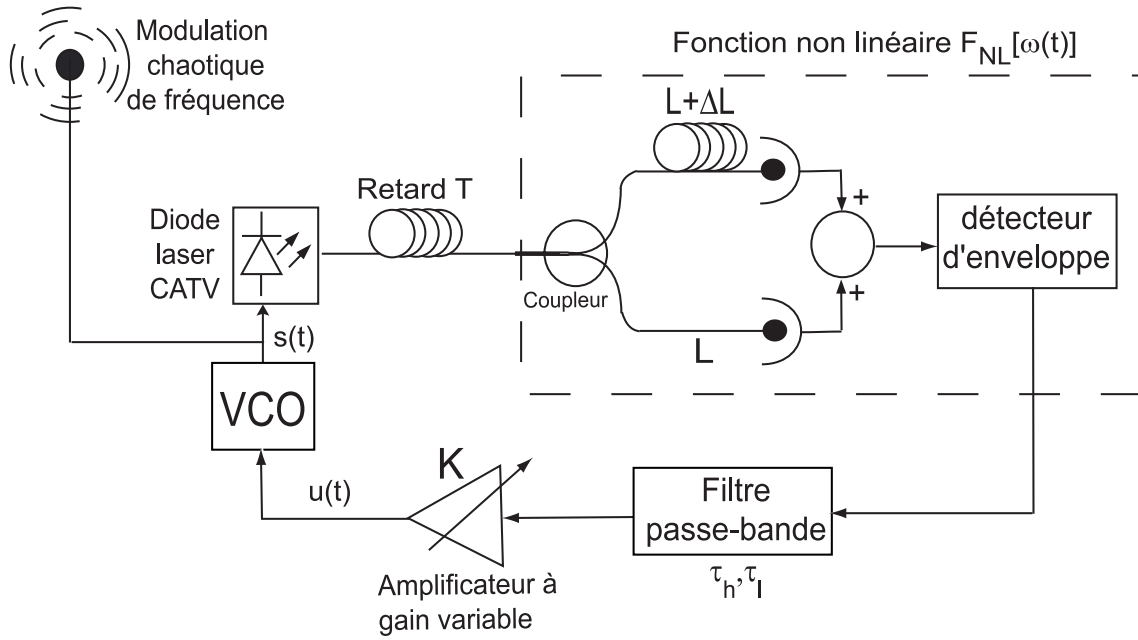


FIG. 2.24 – Oscillateur chaotique

- Un filtre passe-bande permettant de limiter la dynamique du chaos en bande de base.
- Un amplificateur à gain variable pour régler le régime d'oscillation (état stationnaire, périodique, pseudopériodique, pseudo-chaotique et chaotique).
- Un oscillateur commandé en tension (VCO) permettant de convertir le chaos en bande de base en un chaos en fréquence.

2.4.1 L'oscillateur commandé en tension

L'oscillateur commandé en tension (VCO) va générer un signal sinusoïdal modulé en fréquence. Cette modulation de fréquence va dépendre du signal de modulation $u(t)$. Cette modulation de fréquence idéale se traduit par l'expression mathématique suivante :

$$s(t) = V_0 \cdot \cos[2\pi \gamma_{vco} u(t) t + \omega_0] = V_0 \cos[\omega(t) t] \quad (2.25)$$

où γ_{vco} est la sensibilité linéaire du VCO en MHz/V et $u(t)$ le signal modulant. La fréquence instantanée du signal est définie par une composante continue f_0 et une composante dynamique $\Delta f(t)$:

$$f(t) = \underbrace{\Delta f(t)}_{v(t)} + \underbrace{f_0}_{v_0} \quad (2.26)$$

Dans l'équation (2.25), nous pouvons remplacer la variable fréquence par la variable

phase qui est définie de la manière suivante :

$$\varphi(t) = \int_0^t \omega(\theta) d\theta = 2\pi \gamma_{vco} \int_0^t u(\theta) d\theta \quad (2.27)$$

Cependant, dans les systèmes expérimentaux, les fluctuations de phase et d'amplitude ne peuvent pas être négligées. Ainsi, l'équation (2.25), en ajoutant les termes de fluctuation, devient :

$$s(t) = V_0[1 + A(t)] \cos[\omega(t)t + \phi(t)] \quad (2.28)$$

Initialement, dans notre oscillateur chaotique en fréquence, V_0 est une constante et $\omega(t)$, bien que présentant des variations pseudo-aléatoires, reste déterministe. Cependant, $A(t)$ et $\phi(t)$ qui représentent le bruit respectivement d'amplitude et de phase, peuvent engendrer des perturbations dans le fonctionnement de notre système. Le bruit de phase est largement utilisé pour décrire les fluctuations aléatoires de la fréquence. Dans les oscillateurs, il est causé par le bruit thermique et le bruit en $1/f$.

Le bruit en amplitude est typiquement inférieur de 20 dB au bruit de phase. C'est pourquoi, nous le négligerons en considérant que $A(t) \ll 1$. Il faut, cependant, savoir que, expérimentalement, le VCO présente des variations de l'amplitude du signal de sortie en fonction de la fréquence de modulation. La puissance de sortie diminue effectivement avec l'augmentation de la fréquence de modulation. Cette variation d'amplitude déterministe qui accompagne la modulation de fréquence a une incidence non négligeable sur les interférences RF. Nous reviendrons ultérieurement sur ce problème.

2.4.2 Principe de réalisation de la fonction non linéaire

Le principe utilisé pour mettre en œuvre une transformation non linéaire à partir d'une modulation de fréquence, est directement inspiré du système expérimental optique réalisant un chaos en longueur d'onde optique (voir 1.5.3 page 44). Il s'agit d'utiliser un montage interférométrique, dont la condition d'interférence est modulée par la variable dynamique d'entrée. On obtient alors une transformation non linéaire correspondant à la fonction d'interférence elle-même, en l'occurrence une fonction $\sin^2$ dans le cas d'une interférence à 2 ondes. La figure 2.25 rappelle la réalisation d'un tel montage en optique par une structure de type Mach-Zehnder déséquilibré.

L'onde est divisée en deux à l'entrée par une jonction Y dans le cas d'un interféromètre en optique intégrée, ou par une lame séparatrice en massif, ou encore par un polariseur à 45° dans le cas d'un montage à cristal biréfringent. Chacune de ces deux ondes suit alors un chemin optique différent au travers de deux guides de longueur différente, ou de deux trajets aériens différents en massif, ou encore le même chemin physique mais selon

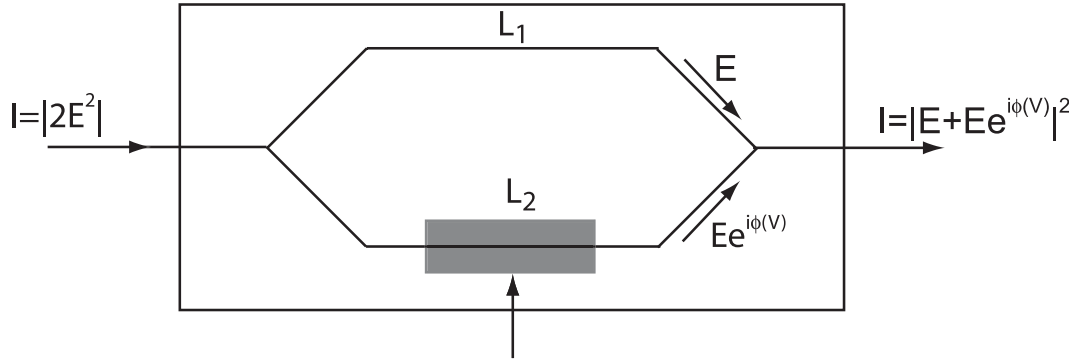


FIG. 2.25 – Principe de l'interféromètre de Mach-Zehnder déséquilibré

deux axes de polarisation dans le cas de l'interféromètre par lame biréfringente. En sortie de l'interféromètre, les deux ondes déphasées à cause de la différence de chemin optique, sont recombinaées par une autre jonction Y, un autre cube séparateur (re-combineur), ou encore un second polariseur à 45°. L'intensité alors détectée en sortie de l'interféromètre s'écrit :

$$I = I_0 \left[1 + \cos \left(2\pi \frac{\Delta}{\lambda} \right) \right] = I_0 \left[1 + \cos \left(2\pi \Delta \frac{\nu}{c} \right) \right] \quad (2.29)$$

où Δ est la différence de chemin optique ($n(L_1 - L_2)$ en optique intégrée ou en massif avec cubes séparateurs, ou $L(n_1 - n_2)$ dans le cas d'une lame biréfringente), ν est la fréquence (optique ici) de l'onde. Dans le cas du générateur de chaos en longueur d'onde, c'est la variation de cette dernière (où de la fréquence ν correspondante), qui fait varier la condition d'interférence. La «force» de la non linéarité peut alors être définie par le nombre d'arches de sinusoides pouvant être balayées dans la gamme de variation de la fréquence optique. Par exemple, une variation de 1 nm autour de 1,55 μm qui correspond à une variation de fréquence de 130 GHz autour de 200THz, permet d'avoir une non linéarité d'ordre 3 (3 arches de sinusoides balayées) si l'on a une différence de chemin optique de l'interféromètre de l'ordre de 2,5 mm. Expérimentalement, le générateur de chaos en longueur d'onde décrit au Chapitre 1, permet avec une différence de chemin optique de 10 mm, d'avoir une transformation non linéaire d'ordre 10 à 14, donc une non linéarité extrêmement forte.

Si l'on cherche maintenant à transposer ce principe dans le domaine des ondes hyperfréquences autour du GHz (ce qui est notre objectif), une non linéarité d'ordre 3 implique une différence de chemin hyperfréquence de l'ordre de la dizaine de mètres, sur la base d'une accordabilité réaliste de l'ordre de quelques 10 MHz pour un VCO à ces fréquences. L'utilisation de câbles radiofréquences pour ce type de réalisation devient vite un problème à la fois de poids, d'encombrement, et de pertes linéiques. C'est pourquoi nous

nous sommes orientés vers une tentative de réalisation optoélectronique de cette non linéarité, en utilisant une transposition de fréquence dans le domaine optique à l'aide de la modulation directe analogique d'une diode laser, et à l'aide de différences de chemins radiofréquences réalisés par voie optique (fig.2.26). De plus, dans le contexte des dynamiques chaotiques à grand retard, la fibre optique va pouvoir être utilisée pour réaliser aisément au travers d'une longueur de fibre supplémentaire de l'ordre du kilomètre, de très grands retards temporels T , qui sont peu dispersifs dans la gamme de modulation RF, et avec de très faibles pertes. Dans la partie «bras optique» de l'interféromètre RF (longueurs L et $L + \Delta L$) chaque bras déphasant les deux ondes RF, est terminé par une photodiode, afin de récupérer les deux ondes déphasées dans le domaine électrique, et de les faire interférer dans ce même domaine via un sommateur RF. Une détection d'enveloppe permet ensuite de récupérer un état d'interférence moyen. Après avoir présenté le principe de la non linéarité, nous allons maintenant décrire plus en détail les caractéristiques électriques et optiques des différents éléments constituant cette non linéarité optoélectronique par interférences radiofréquences.

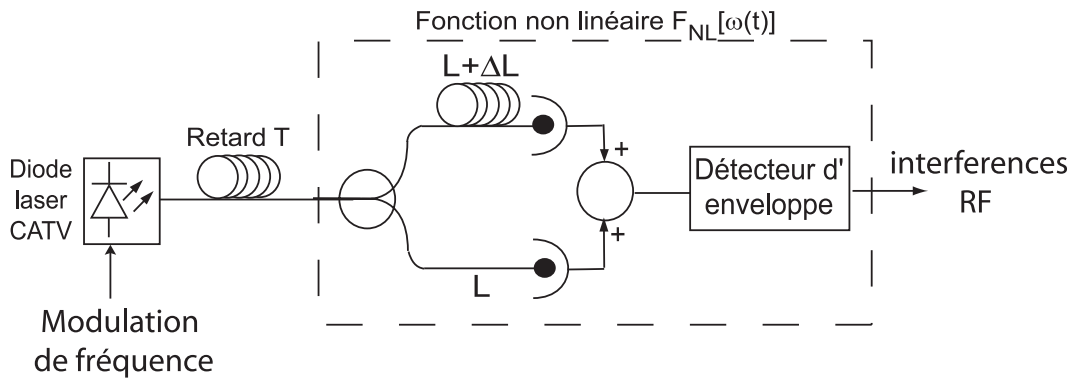


FIG. 2.26 – Non linéarité optoélectronique

La diode laser MQW-DFB CATV

Cette diode laser est une diode CATV de longueur d'onde 1310 nm capable de générer un faisceau de puissance maximale $P_{max} = 8 \text{ mW}$. CATV est l'abréviation de Cable TV qui trouve de nombreuses applications dans le domaine analogique.

Une diode laser à contre-réaction répartie (DFB) est une diode qui émet sur un seul mode longitudinal. Pour cela, un réseau de Bragg a été gravé en dessous (ou au dessus) de la couche active. Ainsi, le réseau gravé dans la même couche fournit au mode un indice effectif de réfraction périodique le long de l'axe de propagation : le couplage entre l'onde et le réseau est un couplage par indice. En effet, des variations périodiques d'indice dues au réseau vont être observées. Ces variations périodiques d'indice vont jouer le rôle de couches

diélectriques empilées d'indice alternativement haut et bas. Ce principe s'inspire des filtres optiques dichroïques¹³. Le principe de base s'appuie sur les variations de coefficient de réflexion en fonction de la longueur d'onde du faisceau optique. En effet, une couche mince diélectrique dont l'épaisseur variable est déposée à la surface d'un substrat, présente un coefficient de réflexion maximal pour toute longueur d'onde telle que l'épaisseur soit un multiple impair du quart de la longueur d'onde. Ce dispositif constitue un filtre qui présente un pic de réflexion à une longueur d'onde donnée [45].

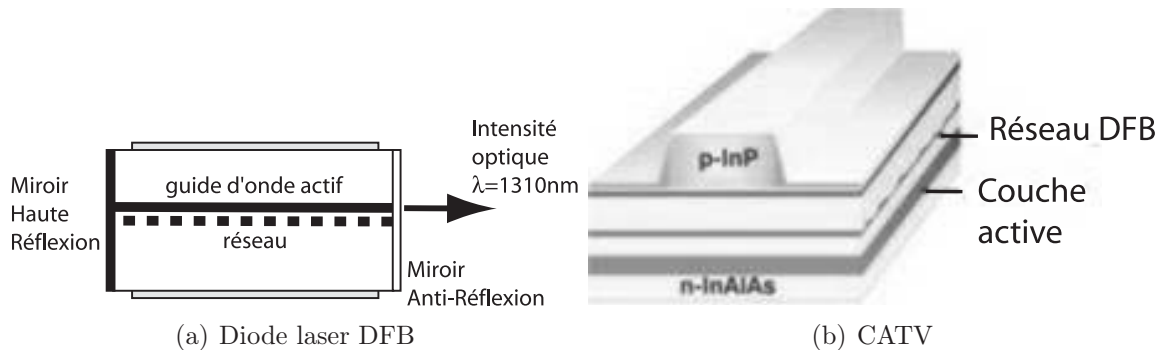


FIG. 2.27 – Laser à contre réaction répartie pour des applications analogiques

Une autre caractéristique importante de la diode laser DFB utilisée est sa structure «multiples puits quantiques» (MQW). Le type MQW est très répandue car il offre de significatifs avantages comme un courant de seuil très bas, une sensibilité plus importante, une réduction du bruit, une meilleure linéarité, et pour finir une meilleure stabilité thermique. Un laser MQW est une structure avec une couche très mince de matière semiconductrice comprise entre deux régions qui sont des bandes interdites. Cela limite le mouvement des électrons et des trous, et de ce fait force les énergies pour que le mouvement soit quantifié et se produise uniquement aux énergies discrètes.

Les lasers à semiconducteurs ont par nature une conversion électrique-optique linéaire. Cette caractéristique est essentielle pour les transmissions analogiques. Cependant, il est nécessaire de choisir une diode laser avec un bruit en intensité (RIN : Random Intensity Noise) le plus faible possible afin d'éviter des perturbations supplémentaires. De ce fait est apparue une classe de diode laser pour les transmissions analogiques appelées des diodes lasers CATV¹⁴.

Cette caractéristique de faible RIN va déterminer le rapport entre le niveau de la porteuse et le niveau de bruit du côté du récepteur avant un processus non linéaire introduit

¹³propriétés que possèdent certains corps ou substances de présenter une coloration différentes suivant la direction de l'observation

¹⁴Initialement, cette abréviation était communément utilisée pour les antennes de télévision et maintenant, ce terme fait typiquement référence aux câbles de télévision

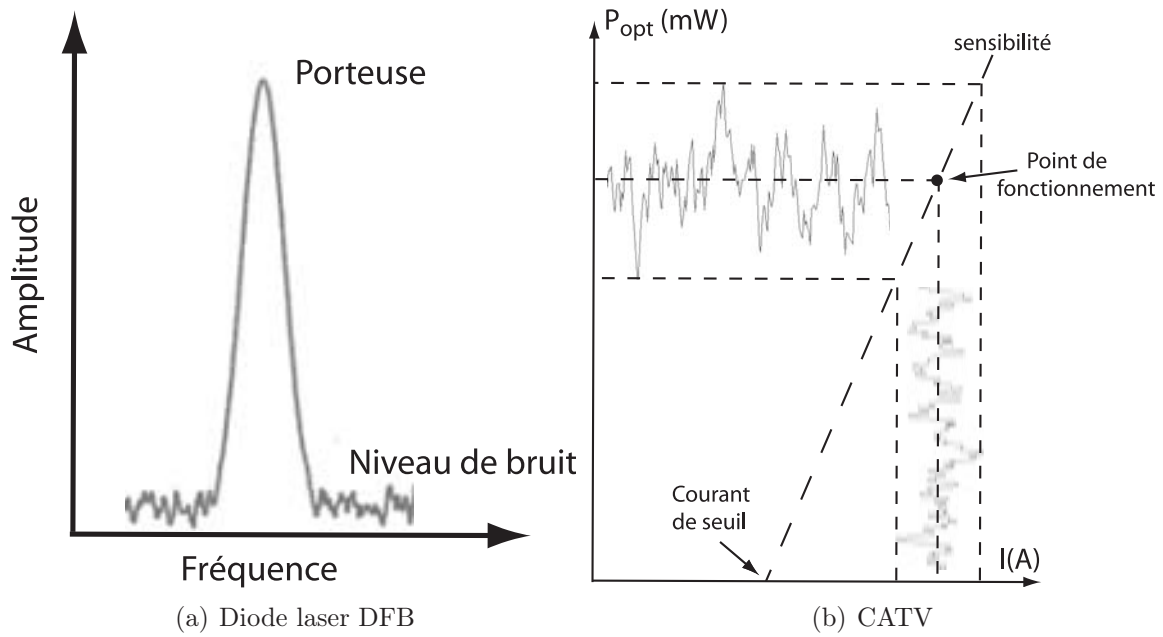


FIG. 2.28 – Caractéristiques d'une diode laser analogique

par la détection et l'éventuelle saturation d'amplitude (fig.2.28(a)). Cette mesure est appelée CNR pour Carrier to Noise Ratio. Elle s'exprime en dB/Hz et permet d'avoir une estimation du bruit introduit par la diode lors de la transmission optique sur le signal électrique analogique.

Dans notre montage (fig.2.26), cette diode laser va générer une onde lumineuse modulée en amplitude par le signal $s(t)$ issu du VCO. Le champ électromagnétique et l'intensité optique de l'onde lumineuse sont alors définis de la manière suivante :

$$\begin{cases} E(t, z) = \sqrt{I(t - kz/\omega)} \cos(\omega t - kz) \\ I(t) = I_0[1 + m s(t)] \end{cases} \quad (2.30)$$

I_0 est l'intensité optique moyenne liée au courant de polarisation de la diode (point de fonctionnement).

Cette onde va traverser une fibre optique de 2 km qui va réaliser un retard temporel de $10 \mu s$ indispensable dans la génération de dynamiques hyperchaotiques (voir partie 1.2.2). Cette onde optique va ensuite être séparée en deux ondes via un coupleur optique 50/50, qui vont chacune traverser deux longueurs de fibres différentes respectivement notées L et $L + \Delta L$ (fig.2.29) dans l'équation (2.31). L'onde lumineuse à l'entrée de chacun des photodétecteurs sera :

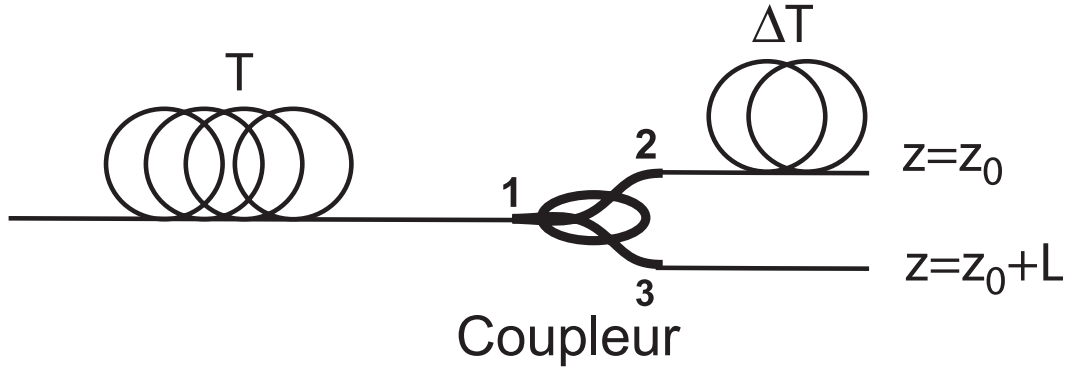


FIG. 2.29 – Partie optique de la non linéarité

$$\begin{cases} E_1(t, L + \Delta L) = \frac{1}{2}\alpha\sqrt{I(t - k(L + \Delta L)/\omega)} \cos[\omega t - k(L\Delta L)] \\ E_2(t, L) = \frac{1}{2}\sqrt{I(t - kL/\omega)} \cos[\omega t - kL] \end{cases} \quad (2.31)$$

$\alpha < 1$ correspond aux déséquilibres en puissance optique en les deux bras fibrés de l'interféromètre.

La photodétection et la sommation

Les photodétecteurs Les tensions $v_{ph1}(t)$ et $v_{ph2}(t)$ délivrées par les amplificateurs transimpédances des deux photodiodes seront respectivement :

$$\begin{cases} v_{ph1}(t) = K \langle E_1^2 \rangle = \frac{V_0 \kappa}{2} (1 + s(t - k(L + \Delta L)/\omega)) I_0 \\ v_{ph2}(t) = K \langle E_2^2 \rangle = \frac{V_0 \kappa}{2} \alpha (1 + s(t - kL/\omega)) I_0 \end{cases} \quad (2.32)$$

où κ représente la combinaison des pertes optiques, des sensibilités de conversion optoélectronique et électro-optique (voir figure 2.26). Le sommateur a une bande passante qui va couper le continu (comportement passe-bande). Ainsi, le signal électrique à sa sortie ne conservera que la modulation RF. Dans les relations précédentes, nous pouvons définir le retard $T = kL/\omega$ et la différence de temps $\Delta T = k\Delta L/\omega$ engendrée par la différence de longueur entre les deux fibres optiques réalisant les interférences RF.

La sommation La sommation est réalisée par l'intermédiaire d'un combineur de puissance qui va permettre d'additionner les deux signaux RF déphasés :

$$\sigma(t) = \frac{V_0 \kappa}{2} [\alpha s(t - T - \Delta T) + s(t - T)] \quad (2.33)$$

D'après l'équation (2.25) et quelques manipulations trigonométriques, le signal obtenu après la sommation des deux signaux RF, en considérant que la différence d'atténuation

entre les deux bras fibrés est nulle ($\alpha = 1$), est défini par :

$$A_1(t) = \frac{V_0 \kappa}{2} [\cos(\omega(t - T)(t - T)) + \cos(\omega(t - T - \Delta T)(t - T - \Delta T))] \quad (2.34)$$

La détection d'enveloppe La détection d'enveloppe dans le premier montage présenté à la partie 2.3.2 utilisait un circuit de redressement double alternance à l'aide de diodes et d'amplificateurs opérationnels. Ce type de montage pouvait convenir pour des basses fréquences, mais il n'est pas envisageable lorsqu'il s'agit d'un signal RF ayant une fréquence porteuse autour de 1GHz, dont on cherche à extraire l'amplitude au travers de son enveloppe. La solution qui a été adoptée consiste en l'utilisation de composants RF passifs tels que dans le schéma représenté à la figure 2.31. Un diviseur de puissance permet dans un premier temps de délivrer deux signaux identiques, à partir du signal d'entrée dont on cherche à détecter l'enveloppe.

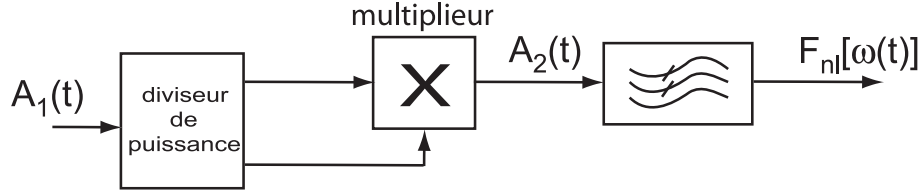


FIG. 2.30 – Détecteur d'enveloppe quadratique

Les deux signaux identiques sont ensuite recombinaés, mais au travers d'un mixeur, réalisant ainsi leur multiplication, et fournissant un signal de sortie correspondant au carré du signal d'entrée initial. La sortie s'exprime alors par :

$$A_2(t) = \frac{(V_0 \kappa)^2}{4} [\cos^2(\omega(t - T)(t - T)) + \cos^2(\omega(t - T - \Delta T)(t - T - \Delta T)) + \cos(\omega(t - T)(t - T)) \cos(\omega(t - T - \Delta T)(t - T - \Delta T))] \quad (2.35)$$

A la sortie du mixeur, il est nécessaire d'ajouter un filtre pour éliminer les composantes HF. Le but de ce filtre est de ne conserver que les variations d'amplitude lentes de la condition d'interférence liées à la modulation de fréquence, en supprimant la porteuse FM ($F_{nl}(t) = \langle A_2 \rangle_\tau$, où τ est la constante de temps du filtre). La fonction non linéaire est alors complètement définie par l'équation suivante :

$$F_{nl}[\omega(t)] = \frac{(V_0 \kappa)^2}{4} \cos\{\underbrace{[\omega(t - T) - \omega(t - T - \Delta T)]}_{g(t)} t + \omega(t - T - \Delta T) \Delta T\} \quad (2.36)$$

Dans le cas habituel des interférences, la fonction $g(t)$ est nulle, et on trouve alors la dépendance classique d'une figure d'interférence :

$$\omega \Delta T = 2\pi \frac{c}{\Lambda} \Delta T = 2\pi \frac{\Delta L}{\Lambda} \quad (2.37)$$

où ΔL est la différence de chemin «électromagnétique» réalisée par voie optique, et Λ est la longueur d'onde instantanée de la porteuse RF ($\Lambda = 20$ cm pour $f = 1.5$ GHz).

En réalité, $g(t)$ peut être un signal non négligeable dépendant des variations de fréquence, mais aussi du temps. Nous verrons par la suite l'effet de cet élément dans la section 2.6.3. En considérant la fréquence centrale du VCO (2.26), nous arrivons à la relation (2.38) fonction des fluctuations engendrées par l'excursion en fréquence angulaire $\Delta\omega(t) = \omega(t) - \omega_0$:

$$F_{nl}[\omega(t)] = \frac{(\kappa V_0)^2}{4} \cos[\Delta\omega(t - T - \Delta T) \Delta T + \phi_0] \quad (2.38)$$

avec $\phi_0 = \Delta T \omega_0$.

La figure 2.31 représente la non linéarité pour un terme temporel $g(t)$ nul ; nous vérifierons, par la suite, dans quelles mesures ce terme peut être considéré comme négligeable.

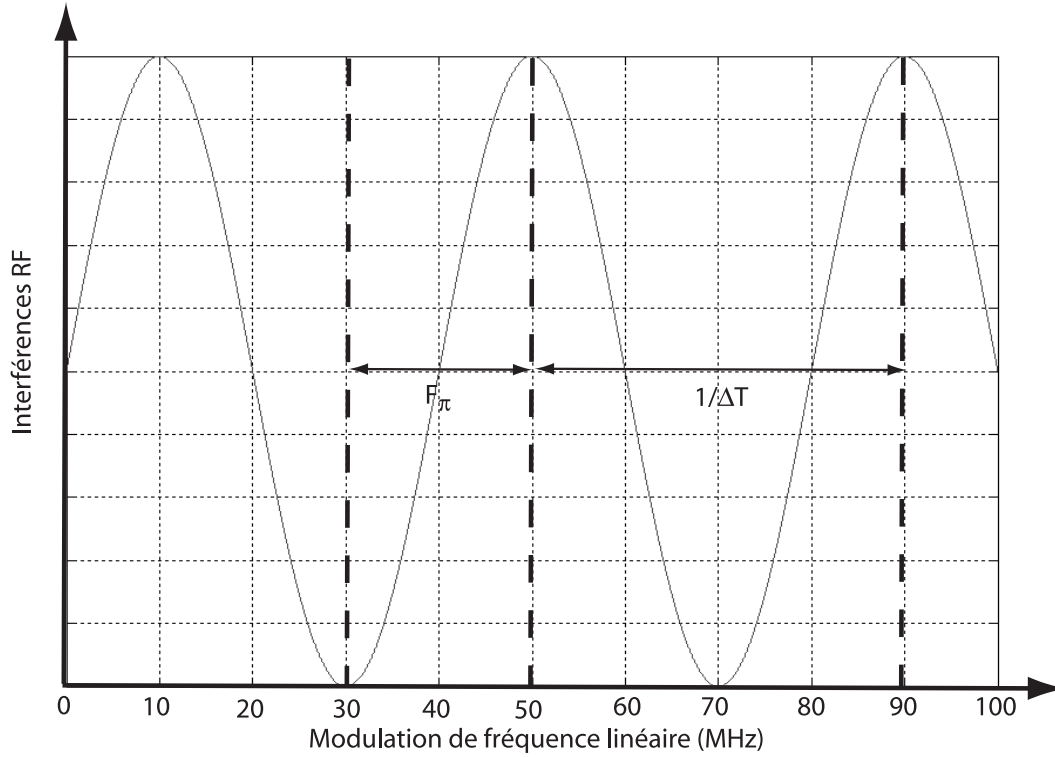


FIG. 2.31 – Non linéarité pour $\Delta T = 25$ ns, $f_0 = \omega_0 2\pi = 1.5$ GHz

La caractéristique non linéaire de notre système est donc une fonction dont le comportement est potentiellement très non linéaire, puisqu'avec une plage de variation de

100 MHz autour de 1.5 GHz, nous serons capables de balayer 5 extrema, ce qui correspond à un polynôme de degré 6.

2.4.3 Le retard temporel

Dans le cas des oscillateurs non linéaires à retard, l'emploi de décalages temporels importants est nécessaire à l'obtention de signaux hyperchaotiques (de grandes dimensions, donc difficiles à analyser). Il existe plusieurs façons de réaliser ce retard :

- une fibre optique
- un câble coaxial
- un système électronique à mémoire discrète

Le choix d'une réalisation électronique à mémoire discrète n'est pas possible étant donnée la bande passante requise. En effet, la mémoire analogique CCD utilisée dans le premier système de cryptographie par chaos en fréquence (voir la partie 2.3.3 page 67) possède une bande passante trop étroite (0 – 170 kHz). Une autre réalisation de ce type de retard est en cours de développement. Elle est constituée de convertisseurs numérique/analogique et analogique/numérique permettant de traiter numériquement le signal analogique. Le retard alors réalisé est en partie fixé par la taille d'une mémoire numérique FIFO¹⁵. Le but de ce circuit est d'augmenter la bande passante de cette fonction électronique. Cependant, la bande passante, bien que plus grande, reste encore trop modeste pour pouvoir analyser correctement l'oscillateur chaotique dont le chaos en bande de base peut atteindre une extension spectrale de 5 MHz.

Une autre solution est de réaliser le retard électriquement avec une longueur de câble coaxial, ou optiquement avec une longueur de fibre. Pour des raisons de sécurité de l'information transmise, il est important de pouvoir générer un chaos de grande dimension. Pour cela, le rapport entre le retard et la constante de temps définissant la dynamique limitante de la variable chaotique, doit être le plus grand possible. La constante de temps de notre chaos en bande de base est $\tau_1 = 1.6\mu s$ c'est pourquoi nous avons choisi une longueur de fibre de 2 km correspondant à un retard de 10 μs .

Dans les systèmes de cryptage, ce rapport peut atteindre 100 voire plus. Dans notre cas, ce rapport vaut :

$$T/\tau_1 = 6.25$$

Dans le cas d'une longueur de deux kilomètres, il est préférable de choisir un retard optique à un retard électronique. En effet, les pertes associées à un câble coaxial sont beaucoup plus importantes (fig.2.1). D'autre part, le poids de 2 km de câble coaxial est

¹⁵First In First Out

très élevé (plusieurs dizaine de kg) et son prix est également plus élevé (≈ 230 euros pour une fibre et ≈ 1000 euros pour un câble coaxial).

2.4.4 La dynamique limitante : modélisation et limitations expérimentales

La dynamique limitante est un élément important de notre oscillateur chaotique puisque celle-ci va déterminer les caractéristiques spectrales du chaos en bande de base.

L'équation (2.39) est en réalité un modèle assez simpliste du processus dynamique qui régit l'évolution temporelle de notre oscillateur. En effet, cette représentation temporelle différentielle de la loi d'évolution correspond au cas peu réaliste où la fonction du filtrage de la contre-réaction électronique est celle d'un passe-bande du second ordre seulement. Dans la réalité, plusieurs fréquences de coupure agissent effectivement, et compliquent notablement la loi différentielle, en faisant intervenir des dérivées d'ordre plus élevé. Pourtant, nous allons montrer qu'en présence de bruit, les effets «faible amplitude» des filtres d'ordre supérieur, sont a priori négligeables, à partir du moment où ces faibles amplitudes sont plus petites que le bruit. Les phénomènes dynamiques déterministes sont alors masqués par le bruit de fond. Ce principe est illustré sur la figure 2.32. En 2.32(a), on remarque qu'en présence de bruit, l'action du filtrage n'est effective que pour une bande de fréquence centrée sur la bande passante de la dynamique passe-bande. En 2.32(b), la courbe supérieure en pointillés montre la fonction de filtrage réellement mesurée en pratique. Celle-ci fait clairement apparaître une coupure d'ordre supérieure à 2 au delà de 90 MHz, liée au filtrage introduit par l'amplificateur et le sommateur. A cause du niveau de bruit non négligeable, on observe en fait la même caractéristique de filtrage avec bruit que dans le cas d'un second ordre pur avec bruit (fig.2.32(a)), car la bande de fréquence où l'on pourrait voir l'effet d'un ordre supérieur, est en fait masquée par le bruit. Ainsi, l'influence des comportements dynamiques d'ordre supérieur peut être négligée, et nous considérerons dans la suite que le modèle dynamique simpliste de l'équation (2.39) peut tout de même être utilisé pour simuler le comportement des solutions observées dans le système expérimental.

$$\tau_1 \tau_2 \frac{ds}{dt} + (\tau_1 + \tau_2) s(t) + \int_0^t s(u) du = (\tau_1 + \tau_2) e(t) \quad (2.39)$$

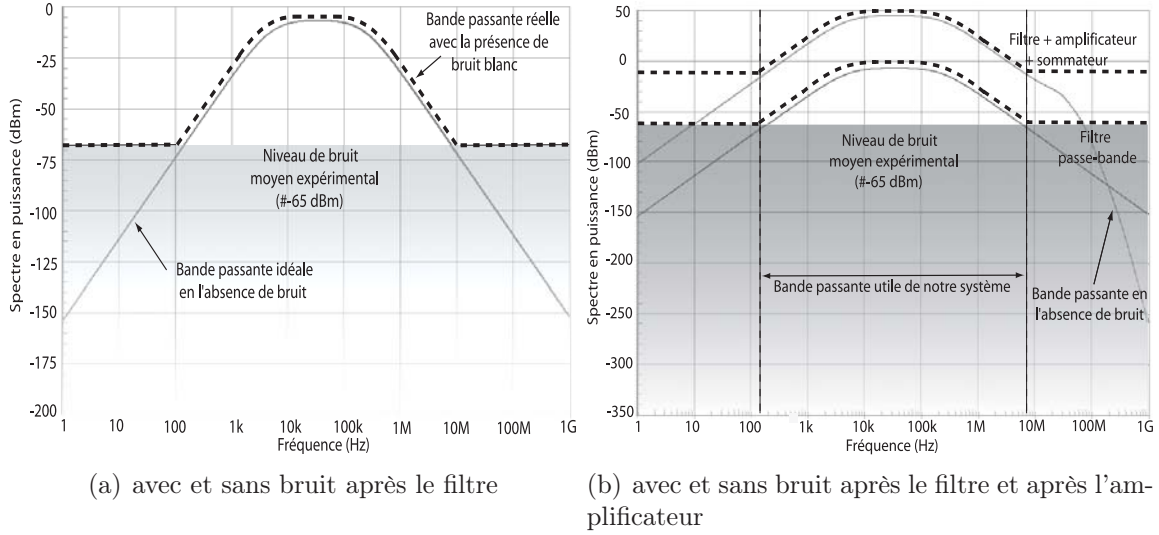


FIG. 2.32 – Bande passante de l'amplificateur et du filtre

2.5 Caractérisation de l'oscillateur chaotique

2.5.1 Définition du modèle mathématique

L'oscillateur chaotique, représenté figure 2.24, est l'association en boucle fermée de l'ensemble des éléments décrits précédemment. A partir de cette description, et en faisant abstraction du bruit, la dynamique du système mis en œuvre expérimentalement peut être modélisée de la manière suivante :

$$\tau_1 \tau_2 \frac{d^2 \Delta \omega}{dt^2}(t) + (\tau_1 + \tau_2) \frac{d \Delta \omega}{dt}(t) + \Delta \omega(t) = (\tau_1 + \tau_2) \beta_\omega \frac{dF_{nl}[\Delta T \Delta \omega(t - T) + \phi]}{dt} \quad (2.40)$$

où F_{nl} est la fonction non linéaire réalisée par des interférences RF (2.37), τ_1 et τ_2 sont les temps caractéristiques des coupures hautes et basses respectivement du modèle dynamique de type passe-bande du second ordre, ϕ est un paramètre qui correspond à un décalage le long de l'axe des fréquences de la fonction non linéaire, et β_ω est le poids, en unité de pulsation, de la transformation non linéaire au travers de la contre-réaction. Ces deux derniers paramètres dépendent de la manière suivante des grandeurs caractéristiques de l'oscillateur :

$$\beta_\omega = K \kappa^2 V_0^2 \gamma_{vco} = K \pi V_{det} \gamma_{vco} \Delta T \quad (2.41)$$

$$\phi = \frac{2n \Delta L \omega_0}{c} = \Delta T \cdot \omega_0 = \Delta T \cdot 2\pi f_0 \quad (2.42)$$

Dans ces deux expressions, on reconnaît les paramètres physiques et optiques suivants : V_{det} est l'amplitude de la non-linéarité à la sortie d'un démodulateur d'amplitude, K est

la gain de l'amplificateur, κ est le gain optoélectronique regroupant les pertes par transmission optique, la sensibilité des photodiodes et de la diode laser, V_0 est l'amplitude du signal sinusoïdal à la sortie du VCO, γ_{vco} est la sensibilité du VCO, n est l'indice de réfraction, c est la célérité d'une onde électromagnétique dans le vide, ΔL est la différence de longueur des fibres optiques réalisant la différence de marche de l'interférence RF, et ω_0 est la fréquence centrale de la modulation en fréquence. Pour permettre des raisonnements comparatifs avec d'autres générateurs de chaos à retard, et pour faire ressortir les paramètres pertinents dans la définition du comportement de l'oscillateur, il peut être judicieux de réécrire l'équation (2.40) à l'aide de variables normalisées sans dimension. Il apparaît alors un gain sans unité β qui correspond à β_ω normalisé par rapport à l'intervalle spectral libre de la fonction d'interférence RF. Ce critère de normalisation est celui classiquement utilisé dans le cas des précédents montages étudiés au laboratoire, et réalisant des dynamiques non linéaires à retard en longueur d'onde par exemple. Ce critère permet typiquement de donner un ordre de grandeur du nombre d'extrema de la fonction non linéaire qui participe effectivement au processus dynamique, c'est-à-dire qu'il donne une estimation du degré de la non linéarité impliquée dans la dynamique chaotique (donc une image de la complexité ; rappelons qu'un degré de 1 correspondant à une non linéarité parabolique, suffit à engendrer des solutions chaotiques). L'équation dynamique normalisée sans source de bruit devient donc :

$$\tau_1 \tau_2 \frac{d^2 x}{dt^2}(t) + (\tau_1 + \tau_2) \frac{dx}{dt}(t) + x(t) = (\tau_1 + \tau_2) \beta \frac{dF_{NL}}{dt}(t - T) \quad (2.43)$$

où $x = \Delta T \Delta \omega$ est une variable sans dimension et le gain β normalisé est :

$$\beta = \frac{\pi V_{det} \gamma_{vco} \Delta T}{2} \quad (2.44)$$

2.5.2 Simulations numériques des comportements dynamiques

Il existe plusieurs solutions pour résoudre l'équation différentielle à retard (EDR) de l'équation (2.43). La méthode d'Euler fut la première méthode numérique à être mise en œuvre pour résoudre les équations différentielles d'ordre quelconque. Ensuite, les méthodes de Runge-Kutta (du 2nd, 4^{ieme}, ... ordre) sont apparues de manière à optimiser les temps de calcul tout en obtenant une précision de calcul bien meilleure. Au cours de ce chapitre, nous allons effectuer un rappel de la méthode d'Euler pour ensuite expliquer la méthode de Runge-Kutta du quatrième ordre qui est la méthode choisie pour la résolution de l'EDR.

Rappels sur la méthode d'Euler

La méthode d'Euler est la plus simple mais également la moins précise. Pour illustrer la résolution numérique, nous allons partir de l'équation différentielle suivante :

$$\frac{dy}{dt} = f[y] \quad (2.45)$$

Cette méthode tronque le développement de Taylor après le second terme ($y(t_0 + h) \simeq y_0 + h y'_0(t_0)$) où la fonction f_0 a été évaluée par la pente prise au point initial (t_0, y_0) . Une valeur approchée de $y(t_0 + h)$ est donc $y(t_0 + h) \simeq y_0 + h f(t_0, y_0)$. Cette expression fournit une relation point par point pour laquelle une solution approchée de l'équation différentielle est obtenue par l'utilisation répétée de l'application récursive :

$$\begin{cases} y_{n+1} = y_n + h f(t_n, y_n) \\ t_n = t_0 + n h \\ y_n \simeq y(t_n) \end{cases} \quad (2.46)$$

Pour mieux comprendre la relation précédente, un schéma de la méthode d'intégration est représenté sur la figure 2.33(a).

La méthode d'Euler est donc une approche au premier ordre. L'erreur d'intégration à chaque étape est de l'ordre de h^2 . L'erreur cumulée sur une série d'étape est de l'ordre de h , h étant le pas d'intégration.

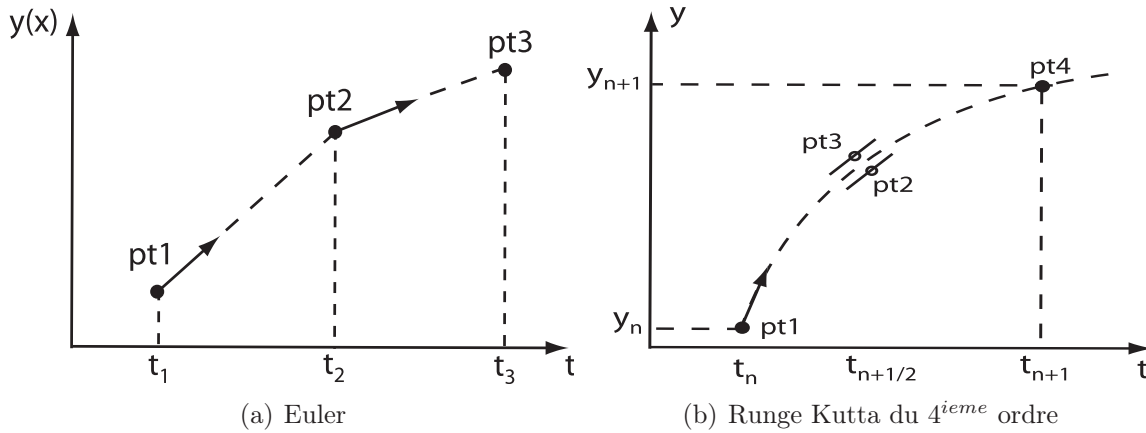


FIG. 2.33 – Différentes méthodes d'intégration numérique

Résolution par la méthode de Runge Kutta

Les méthodes de Runge-Kutta constituent une famille de procédure d'intégration numérique d'ordre croissant, dont la méthode d'Euler est le premier ordre.

Toutes les méthodes d'intégration consistent, en connaissant une valeur $y(t_n)$ à l'instant t_n de la fonction à déterminer, à calculer sa valeur voisine à l'instant ultérieur $t_n + h$ [46].

L'expression de la dérivée est approchée à l'aide de 4 valeurs pondérées entre deux points voisins en utilisant l'algorithme suivant :

$$\begin{cases} k_1 = h.f(t_n, y_n) \\ k_2 = h.f(t_n + \frac{h}{2}, y_n + \frac{k_1}{2}) \\ k_3 = h.f(t_n + \frac{h}{2}, y_n + \frac{k_2}{2}) \\ k_4 = h.f(t_n + h, y_n + k_3) \end{cases} \quad (2.47)$$

De cet algorithme est issue la moyenne pondérée permettant de définir la valeur de la solution $y(t)$ par des itérations successives :

$$\begin{cases} y_{n+1} = y_n + \frac{k_1 + k_4 + 2.(k_2 + k_3)}{6} \\ x_{n+1} = x_n + h \end{cases} \quad (2.48)$$

L'erreur de cet algorithme d'intégration est alors en h^4 où h est le pas d'intégration. Il s'agit d'une valeur à choisir de façon à optimiser le temps et la précision de calcul.

Le nombre de points est dépendant de la durée d'intégration $t_N - t_0$, et du pas d'échantillonnage h :

$$N = \frac{t_N - t_0}{h} \quad (2.49)$$

La méthode de Runge Kutta du quatrième ordre aura donc une erreur d'approximation plus petite que la méthode d'Euler. Bien que plus compliquée à mettre en œuvre, elle permet pour un même temps de calcul donné (soit le même pas d'intégration) d'avoir une meilleure précision de calcul.

De nombreuses applications devant résoudre des équations différentielles non linéaires utilisent la méthode de Runge-Kutta du quatrième ordre. Elle est souvent présentée comme étant le meilleur compromis entre le temps de calcul et la précision de celui-ci. Il existe toutefois une autre méthode qui mérite une étude concernant ses performances pour la simulation d'équation différentielle non linéaire à retard. Il s'agit de la méthode prédicteur/correcteur. Celle-ci ne sera par contre pas discutée ici.

2.5.3 Paramètres de l'oscillateur pour les simulations numériques

Il est important de pouvoir prévoir le comportement du système. Ainsi, il est nécessaire de réaliser un modèle mathématique (2.40). A partir de là, la méthode de Runge-Kutta du quatrième ordre explicitée dans la section précédente va permettre de résoudre l'équation (voir programme en annexe B).

Au travers des divers outils de caractérisation décrits dans le premier chapitre, nous pouvons faire des analyses qui porteront dans un premier temps uniquement sur le fonctionnement de l'oscillateur. Nous représenterons l'évolution temporelle de la dynamique

chaotique du système : la fréquence. Nous associerons les études spectrales du signal en bande de base, et celles de la porteuse de la modulation de fréquence.

Nous allons également tracer quelques diagrammes de bifurcation en faisant varier le gain, puis la phase, pour mettre en évidence leur influence sur le régime dynamique alors choisi par l'oscillateur. Nous calculerons, ensuite, la dimension de la dynamique chaotique dans l'espace des phases par l'intermédiaire des exposants de Lyapunov, eux-mêmes obtenus à partir d'une technique de calcul connue, spécialement développée pour les systèmes à retard de très grande dimension [47].

Nous allons rassembler l'ensemble des valeurs caractérisant le système expérimental (Tab.2.3). Ensuite, à partir de ces valeurs expérimentales, nous pourrions évaluer les bornes de variations du gain normalisé β et de la phase ϕ .

Paramètre	Notation	valeur
Constante de temps passe-bas	τ_1	$1.6 \mu s$ (100 kHz)
Constante de temps passe-haut	τ_2	$16 \mu s$ (10 kHz)
Sensibilité du VCO	γ_{vco}	30 MHz/V
Amplitude du signal de sortie du VCO	V_0	0.2 V
Gain optoélectronique	κ	3.3
Gain variable	K	$0.3 < K < 32$
Fréquence centrale de modulation	f_0	$950 \text{ MHz} < f_0 < 1.5 \text{ GHz}$
Ordre de l'interférence	$\Delta T, \Delta L$	25 ns, 5 m
Retard	T	$10 \mu s$

TAB. 2.3 – Paramètres utilisés pour les simulations numériques

D'après les équations (2.42) et (2.44), nous pouvons en déduire le facteur de proportionnalité de la phase ϕ en fonction de la fréquence centrale de la modulation et la plage de variation du gain normalisé β en fonction du gain variable K de l'amplificateur.

$$25.10^{-3} < \beta < 2.61 \text{ et } \phi = 25.10^{-9} 2 \pi f_0$$

La phase est définie à modulo 2π près pour une variation de la fréquence centrale de 40 MHz.

2.5.4 Analyse temporelle, spectrale et statistique

Suivant les valeurs du gain en boucle fermée β , nous pouvons obtenir des traces temporelles de différents types. Sur l'ensemble des figures suivantes, la variable dynamique observée est l'excursion en fréquence en sortie du VCO. Elle est déterminée à partir de la solution de l'équation (2.43) :

$$\Delta f(t) = \frac{x(t)}{2 \pi \Delta T} \quad (2.50)$$

Nous pouvons observer pour un gain faible, une évolution périodique (fig.2.34(a)). Pour un gain plus important, nous allons observer une évolution bipériodique (fig.2.34(b)) caractérisée par deux valeurs successives de l'amplitude crête de l'évolution temporelle. Ensuite, pour des gains plus élevés, le système va entrer dans un régime dynamique chaotique, où l'on peut distinguer un continuum d'amplitudes crêtes. Les régimes chaotiques obtenus sont de dimension plus ou moins grande suivant la valeur du gain. La figure 2.34(c) montre un régime chaotique de faible dimension (valeur modérée du gain β).

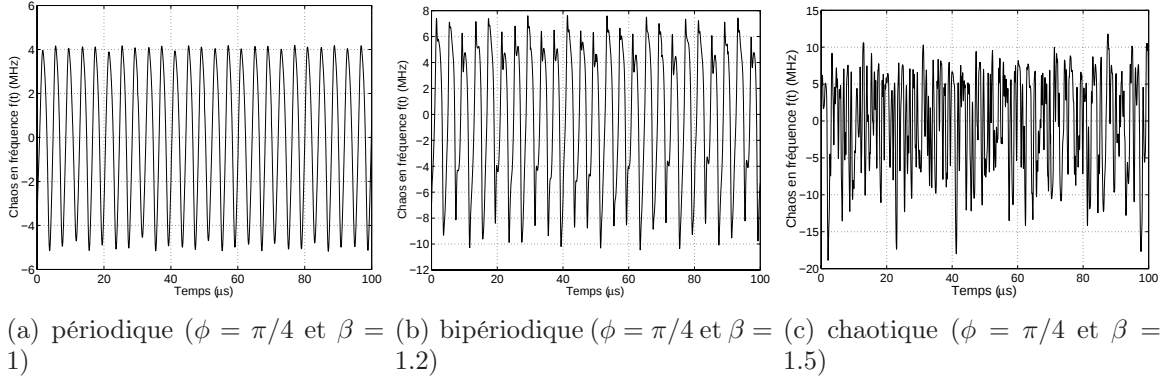


FIG. 2.34 – Evolutions temporelles pour différents gains β

Pour un régime chaotique beaucoup plus complexe que celui observé précédemment, nous allons montrer son spectre associé en bande de base (fig.2.35(b)).

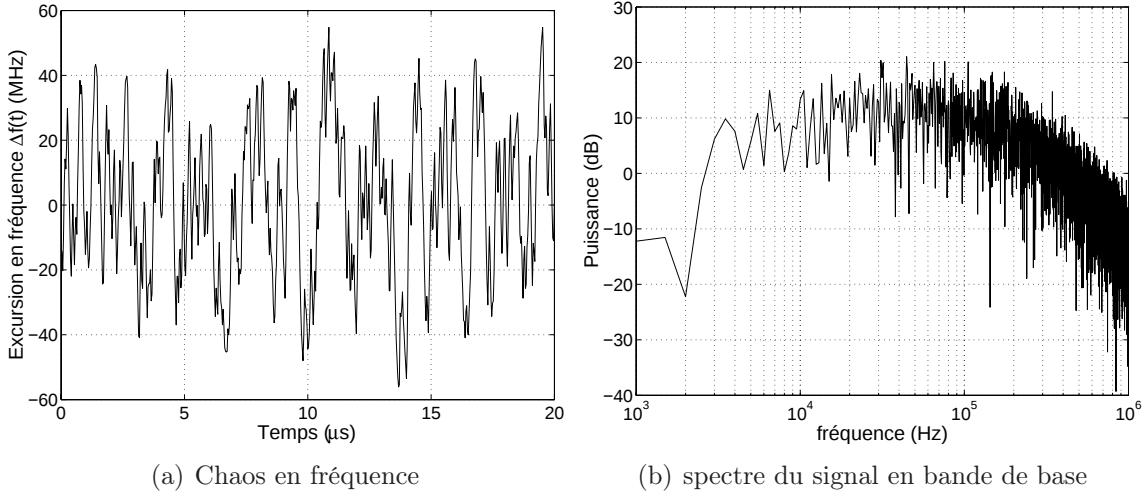


FIG. 2.35 – Evolutions temporelle et spectrale ($\phi = \pi/4$ rad, $\beta = 2.6$ et $T = 10 \mu s$)

Le spectre du chaos en bande de base possède un étalement compris entre 10 kHz et 100 kHz comme pour le système expérimental, en accord avec les fréquences de coupure de la dynamique limitante de type passe-bande. Cette bande spectrale est celle correspondant

au débit d'information qu'il est possible de transmettre avec le système de cryptographie par chaos en fréquence; le message d'information est effectivement inséré dans la partie basse fréquence de notre oscillateur (fig.2.52).

Comme nous pouvons le remarquer, La densité spectrale du chaos en bande de base est relativement uniforme dans la bande passante; aucune fréquence n'est vraiment prédominante dans la bande passante. Après la conversion linéaire tension/fréquence réalisée par le VCO, le spectre de la dynamique chaotique en bande de base se retrouve après modulation de fréquence, autour de la porteuse FM servant pour la transmission. Le spectre de la porteuse chaotique aura la même forme que le spectre en bande de base, mais son excursion en fréquence dépendra de l'amplitude du signal en bande de base, et sa fréquence centrale sera comprise entre 1 et 1.5 GHz.

Pour caractériser les régimes chaotiques susceptibles d'être générés par notre oscillateur, il est intéressant d'avoir une approche statistique en caractérisant la densité de probabilité de notre signal. Celle-ci peut facilement être obtenue par l'intermédiaire d'un histogramme dont le principe a été décrit dans le premier chapitre.

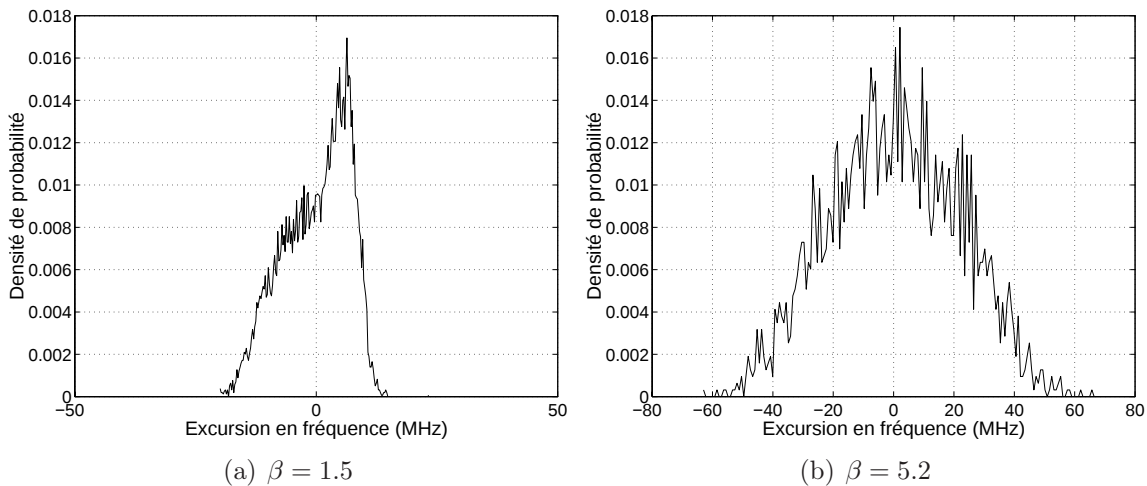


FIG. 2.36 – Densité de probabilité pour deux régimes différents ($\phi = \pi/4$ et $T = 10 \mu s$)

La figure 2.36 montre la densité de probabilité de deux régimes chaotiques pour des gains différents. Nous observons, tout d'abord, l'influence du gain sur le type de régime chaotique du signal. En effet, bien que les variations de la fréquence soient chaotiques, nous remarquons que l'analyse statistique montre une différence notable de densité de probabilité. Pour un gain trop faible, le régime est chaotique mais sa représentation statistique ne permet pas de le confondre avec un bruit Gaussien (fig.2.36(a)). Pour un gain plus important, le signal aura alors l'apparence d'un processus Gaussien quelconque. Dans cette situation, il sera supposé difficile d'identifier statistiquement l'origine déterministe du signal bruité utilisé pour masquer une information, car il sera difficile à distinguer par

rapport à un vrai bruit Gaussien aléatoire. La genèse du bruit Gaussien est relativement courante, puisqu'il correspond naturellement à la limite de la superposition d'un grand nombre de phénomènes aléatoires indépendants et possédant la même loi de probabilité ; selon le théorème de la limite centrale, la densité de probabilité aura une répartition Gaussienne (fig.2.36(b)). La condition nécessaire (mais toutefois pas suffisante) à la génération d'un signal d'apparence aléatoire, est donc un gain β suffisamment élevé (> 2 environ).

2.5.5 Diagrammes de bifurcation

Paramètre de bifurcation : le gain

L'ensemble des informations temporelles et statistiques du paragraphe précédent peuvent être réunies sous la forme d'un diagramme de bifurcation (fig.2.37). En effet, celui-ci permet de mettre en évidence le type d'évolution temporelle sous la forme d'une densité de probabilité codée en niveau de gris en fonction de la valeur du gain de l'oscillateur.

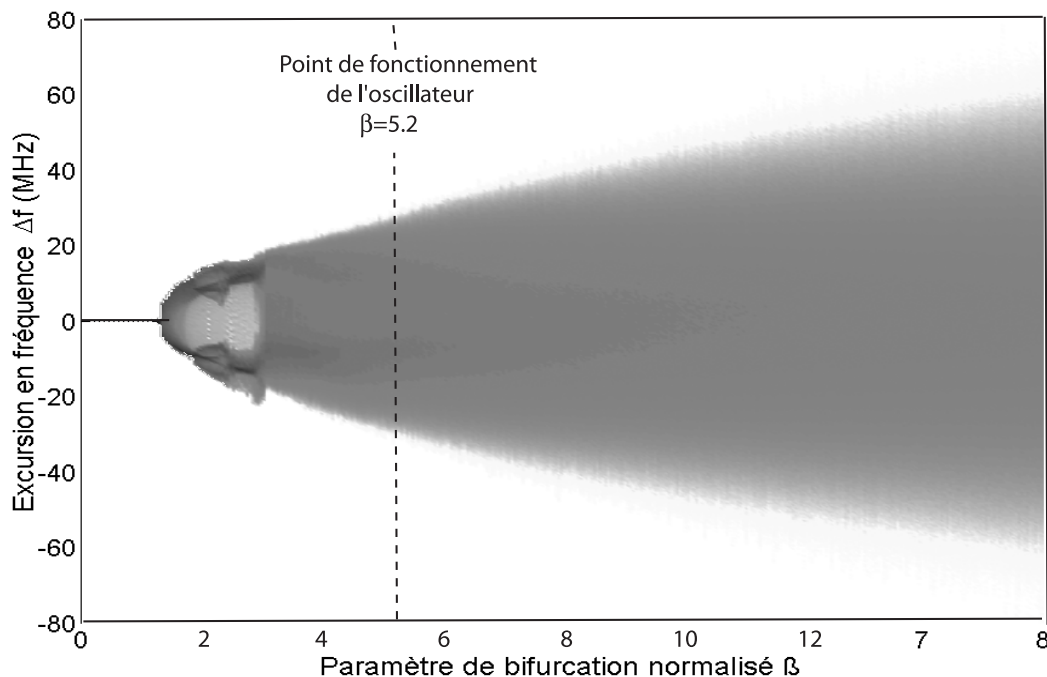


FIG. 2.37 – Diagramme de bifurcation ($T = 10 \mu s$ et $\phi = 2.1 \text{ rad}$)

Le diagramme de bifurcation (fig.2.37) a été tracé pour une valeur de la phase différente par rapport aux simulations précédentes. Le comportement reste toutefois comparable qualitativement dans l'évolution en fonction du gain β .

Ainsi, pour de faible valeur de ce gain, le régime reste stationnaire. Soumis à une perturbation, le système revient systématiquement au point fixe initial. Ensuite, une première bifurcation pour $\beta = 1.6$ va matérialiser un premier régime périodique (bifurcation

de Hopf). Pour $\beta > 2$, des bifurcations supplémentaires à l'origine de l'élargissement spectral, vont marquer la transition entre la périodicité du système vers une évolution chaotique. Les dédoublements de fréquence s'observent mieux dans le cas des systèmes passe-bas et pour des retards très grands devant τ_1 . Dans notre cas, nous ne pouvons pas parler significativement de dédoublements de fréquence mais plutôt d'un élargissement de spectre.

Pour $\beta > 4$, la densité de probabilité va permettre d'évaluer la nature plus ou moins Gaussienne de la statistique en régime chaotique.

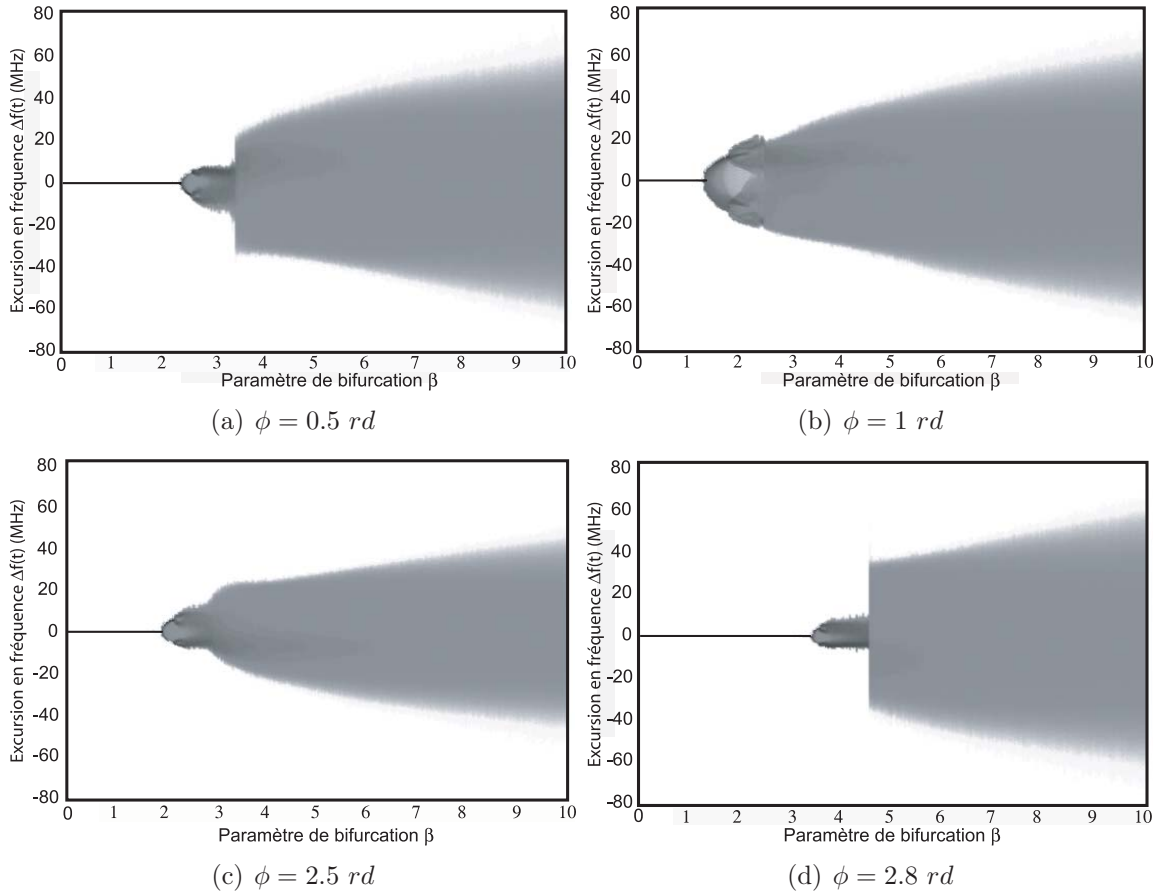


FIG. 2.38 – Diagrammes de bifurcation en fonction de β pour différents déphasages ($T = 10 \mu s$)

On remarque que les détails des différents diagrammes de bifurcation changent notablement en fonction du paramètre ϕ . Intuitivement, ceci s'explique par des arguments similaires à ceux développés dans le chapitre 1 (voir partie 1.3.4 page 19) concernant la dépendance de l'instabilité du point fixe par rapport à ce même paramètre. Ainsi, selon la valeur de la phase ϕ , on observera une route vers le chaos différente notamment visible dans les transitions périodiques/chaotiques (voir fig.2.38(a) et 2.38(b) ou fig.2.38(c) et

2.38(d)).

Paramètre de bifurcation : la phase

Comme nous venons de le souligner, la phase est également un paramètre dont les modifications engendrent des bifurcations. A titre d'illustration, les figures 2.39(a) et 2.39(b) représentent des diagrammes de bifurcation à β constant, et pour une phase ϕ variant continûment de 2 à 8 radians.

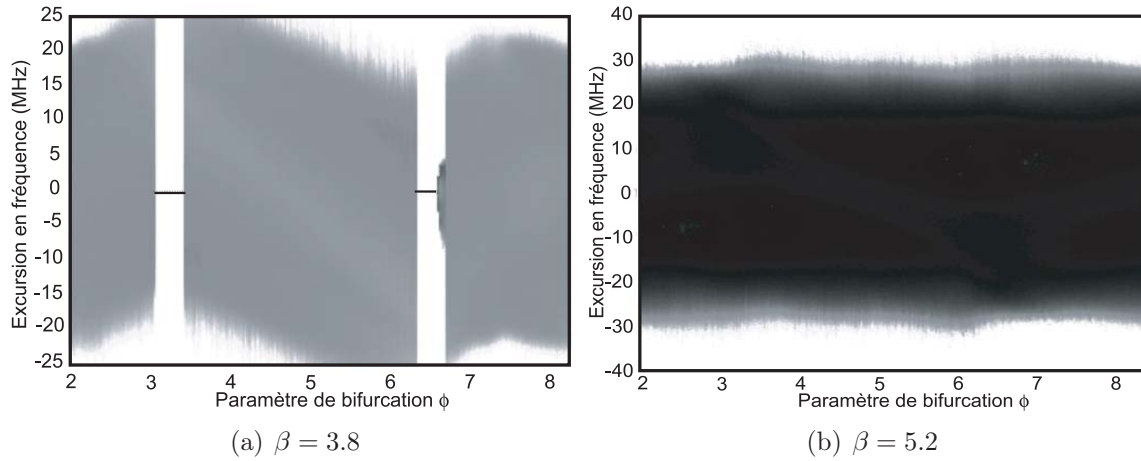


FIG. 2.39 – Diagrammes de bifurcation en fonction du déphasage ($T = 10 \mu s$ et $\Delta T = 25 ns$)

Pour un gain moyen ($\beta = 1.9$), on remarque qu'il existe des valeurs de ϕ permettant des régimes chaotiques et d'autres forçant un régime de point fixe stationnaire. Pour un gain plus élevé, la valeur de la phase a peu d'importance sur la statistique du régime chaotique.

En conclusion, si l'oscillateur est ajusté à un point de fonctionnement de faible gain, la valeur du déphasage devra être judicieusement choisie pour pouvoir obtenir un régime chaotique à même de masquer l'information à coder. Dans le cas contraire, on observerait un régime de point fixe ou périodique avec lequel le masquage d'une information ne peut être efficace.

Phénomène d'hystérésis

Les conditions initiales sont importantes dans l'évolution d'un signal chaotique [48]. En effet, la valeur de la condition initiale et les valeurs du gain β et de la phase ϕ de la fonction non linéaire vont déterminer le régime d'oscillation de notre boucle non linéaire (fig.2.37 et 2.39(a)).

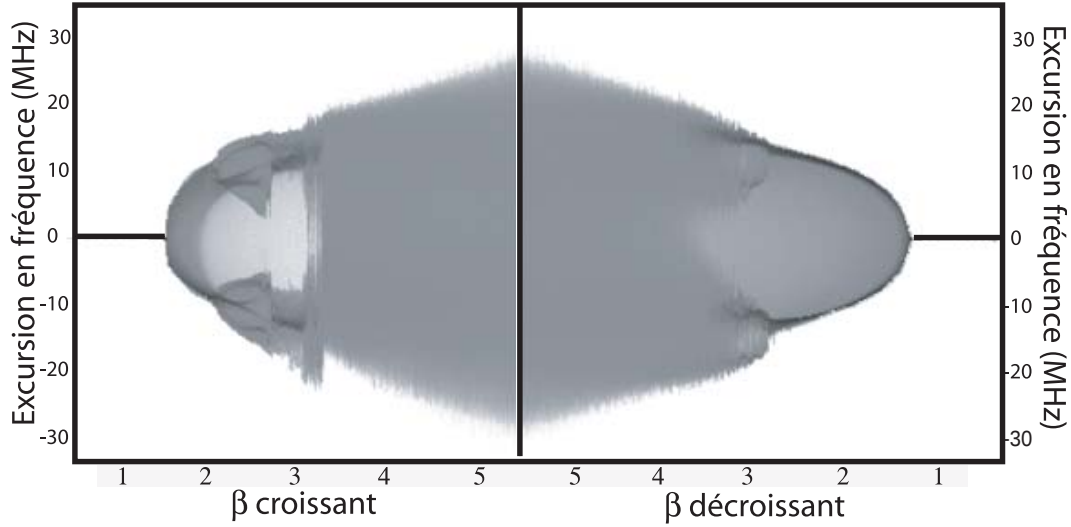


FIG. 2.40 – Diagrammes de bifurcation ($T = 10 \mu s$ et $\phi = 2.1 \text{ rad}$)

L'influence des conditions initiales et de la phase peut être mise en évidence dans un diagramme de bifurcation par un phénomène d'hystérèse [49]. L'évolution croissante ou décroissante du paramètre de bifurcation β conduit à un résultat différent (fig.2.40). La première explication qui peut être mise en avant est le changement d'attracteur étrange dans l'espace des phases. Ce changement d'attracteur pousse à une évolution différente dans le cas d'une évolution croissante ou décroissante du paramètre de bifurcation [50].

Intuitivement, nous pouvons comprendre que le type de régime dynamique fixé par le filtre (passe-bas ou passe-bande) présente une importance dans la visualisation de l'hystérèse dans les diagrammes de bifurcation. En effet, la composante continue du signal conservé dans le cas d'une dynamique passe-bas va permettre de décaler le point de fonctionnement de façon à ce que celui-ci se déplace sur la non linéarité pour ensuite changer le type de bifurcation. Cependant, dans le cas d'une dynamique passe-bande, l'explication devient plus compliquée. Dans le cas de notre système, ce phénomène ne présente pas vraiment d'importance dans le contexte de la cryptographie par chaos. En effet, l'hystérèse observé ne perturbera pas la synchronisation effectuée entre l'émetteur et le récepteur. Nous tenterons simplement, expérimentalement, de mettre en évidence cet hystérèse (voir 3.4.2 page 149).

2.5.6 Espace des phases

L'observation des divers régimes dynamiques possibles peut aussi se faire dans l'espace des phases. Dans le cas des dynamiques à retard, celui-ci est, a priori, infini, et ne peut être réellement utile pour une observation. A titre indicatif, nous avons quand même représenté ci-dessous trois exemples de régime dynamique dans un espace des phases reconstruit en

dimension finie par la méthode dite des retards ; les coordonnées de l'espace des phases correspondent à la variable dynamique retardée avec des valeurs différentes soient $\omega(t)$, $\omega(t - T_1)$ et $\omega(t - T_2)$ ($T_1 \neq T$, $T_2 \neq 2T$, T_1 et T_2 a priori quelconque).

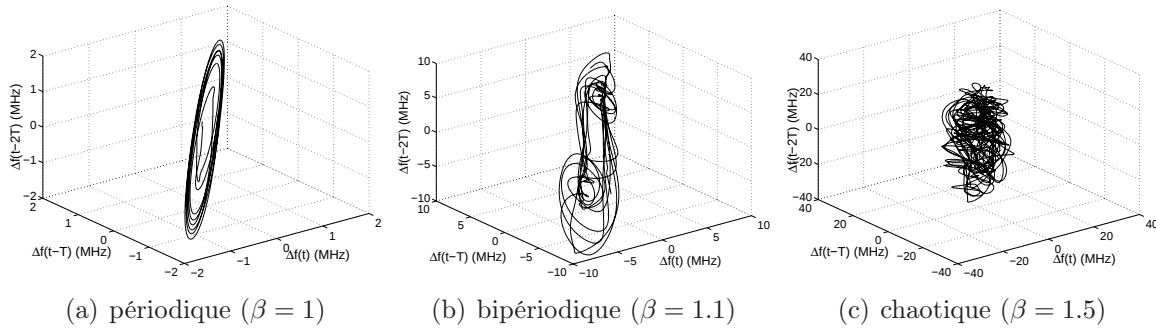


FIG. 2.41 – Trajectoires dans l'espace des phases pour différents gains β et $\phi = \pi/4 \text{ rad}$

On remarque bien sur ces figures que la trajectoire peut être identifiée dans le cas périodique sur la figure 2.41(a) (3 dimensions suffisent) ; mais dès les régimes faiblement chaotiques ($\beta = 1.5$), cette représentation ne suffit plus car la dynamique est trop complexe.

2.5.7 Exposants et dimension de Lyapunov

Nous avons vu, lors des paragraphes précédents, des méthodes statistiques et des représentations graphiques permettant d'observer les évolutions temporelles et spectrales pour différentes valeurs de paramètres. Aucune de ces méthodes ne peut nous donner une valeur reflétant la dimension de l'attracteur dans lequel évolue la variable dynamique. Il s'agit effectivement de méthodes qualitatives. Le diagramme de bifurcation va nous donner le type de régime dans lequel l'oscillateur évolue, le spectre de la porteuse chaotique va nous montrer l'extension en fréquence de la variable chaotique et le débit de transmission potentiel dans le cas d'un système de télécommunication. L'évolution temporelle permettra d'observer les variations chaotiques de notre porteuse, et enfin la fonction de densité de probabilité pouvant modéliser le signal pseudo-aléatoire en termes statistiques.

D'un point de vue plus quantitatif, nous pouvons classer par ordre de complexité les régimes chaotiques obtenus en calculant les exposants de Lyapunov. En effet, le calcul des exposants de Lyapunov (voir partie 1.4.6 page 36) peut nous permettre d'évaluer la dimension de l'attracteur étrange d'un régime chaotique considéré, grâce à la conjecture de Kaplan-Yorke.

A titre d'illustration, nous avons représenté les résultats de ces calculs pour un régime chaotique solution de l'équation (2.43), à la figure 2.42. Le spectre de Lyapunov indique

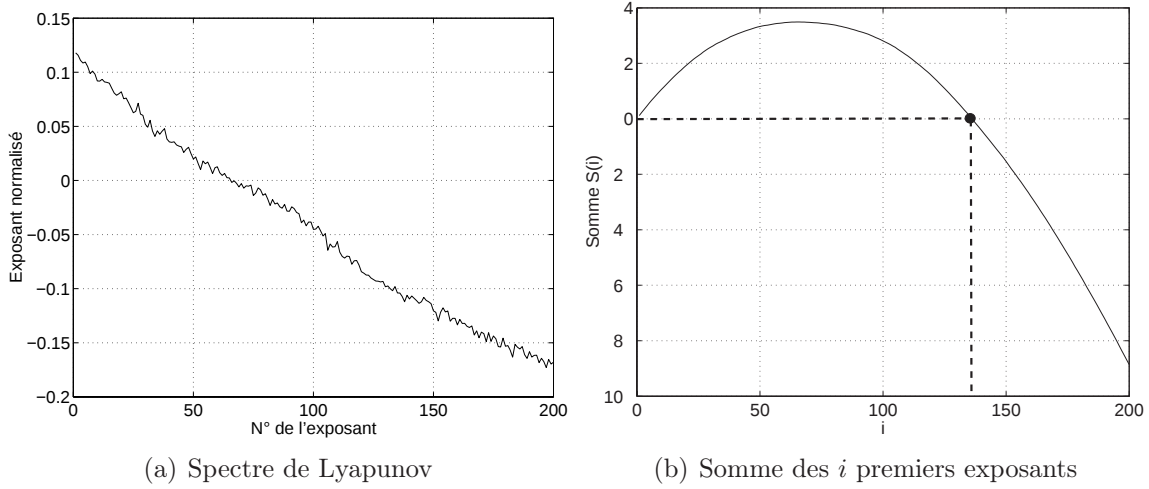


FIG. 2.42 – Exposants de Lyapunov ($\beta = 5.2$, $\phi = \pi/4$ et $T = 10 \mu s$)

la présence d'un grand nombre d'exposants positifs (fig.2.42(a)). A partir de ce spectre, on calcule son intégrale (fig.2.42(b)) afin d'identifier un passage par zéro, ce qui donne une estimation de la dimension de Kaplan-Yorke D_{KY} .

La dimension de l'attracteur chaotique par application de la conjecture de Kaplan-Yorke est :

$$D_{KY} \approx 136$$

Cet outil de caractérisation quantitatif d'un régime chaotique va maintenant être utilisé pour estimer la dépendance de la complexité des solutions chaotiques, en fonction de deux paramètres caractéristiques de notre oscillateur chaotique en fréquence.

Ces paramètres seront l'amplification normalisée β , et la différence de longueur des bras de l'interféromètre ΔL .

On remarque que ces deux paramètres ont le même effet sur la dynamique normalisée, même s'ils ont chacun une signification physique différente : β est un gain pur de la chaîne d'oscillation, alors que ΔL agit sur l'espacement des cannelures de la fonction d'interférence (ou intervalle spectrale libre en optique).

La phase, comme nous pouvons le voir sur la figure 2.44, n'a pas une grande influence sur la dimension du chaos en fréquence, à partir du moment où le chaos est suffisamment complexe ($\beta \geq 2$). En effet, pour une phase variant de 0 à 2π , nous remarquons que la dimension est approximativement la même. Ce résultat sera réutilisé dans le calcul de l'influence du paramètre ϕ sur la réplique du chaos (voir partie 2.6.2 page 107).

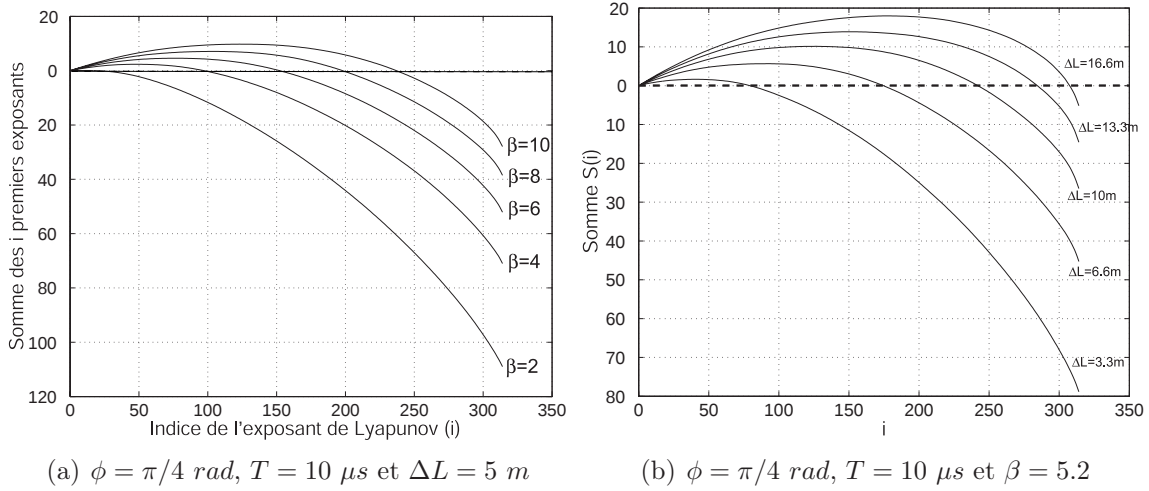
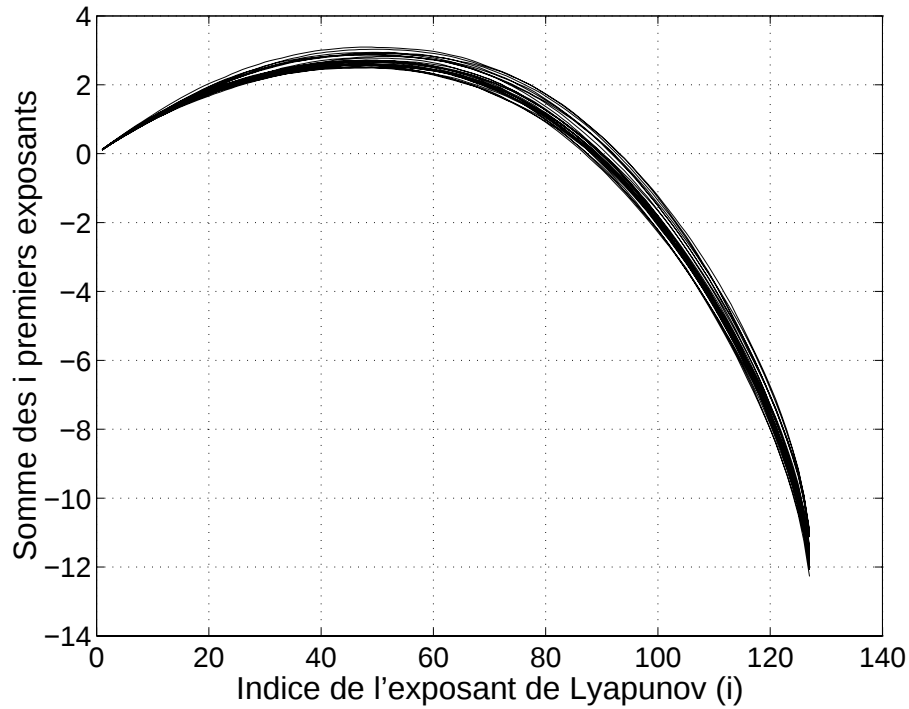


FIG. 2.43 – Somme des premiers exposants de Lyapunov pour différents paramètres

FIG. 2.44 – Somme des premiers exposants de Lyapunov pour différentes phases ϕ ($\beta = 4$, $\Delta L = 5 \text{ m}$, $T = 10 \mu s$)

2.6 Réception et réplique de la porteuse chaotique

Nous avons abordé, dans les précédentes sections, les conditions de génération d'une porteuse chaotique en fréquence. Celle-ci est destinée dans le cadre de ce travail, à effectuer le masquage d'une information.

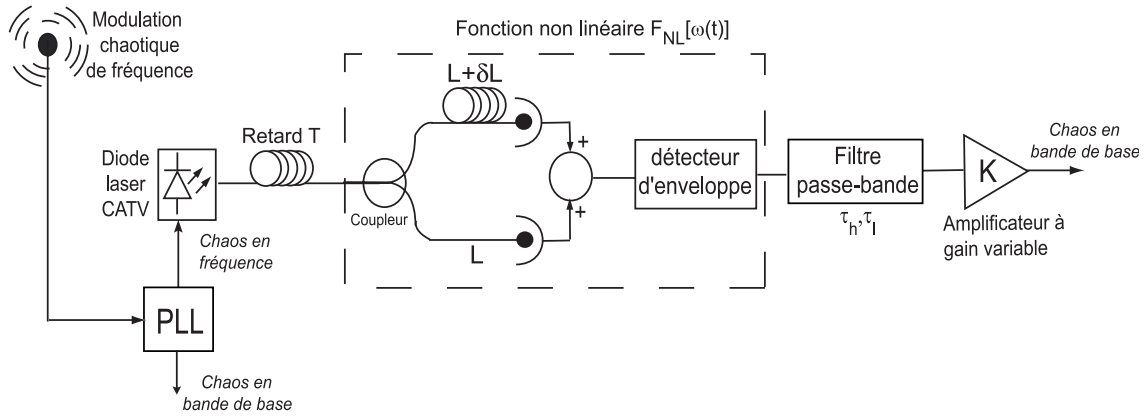


FIG. 2.45 – Synoptique du récepteur/décodeur

Les sections suivantes vont détailler les étapes nécessaires à l'émission et à la réception de ce message codé par chaos FM : nous expliquerons tout d'abord les opérations de détection/démodulation de la porteuse FM, puis de la réplication de chaos. Dans la section suivante, nous verrons les applications qu'il peut y avoir dans le codage/décodage du message à l'intérieur d'une porteuse chaotique.

Le récepteur possède une boucle ouverte formée par les mêmes fonctions que celles de l'émetteur, qui sont le retard, la non linéarité, l'amplification et le filtre passe-bande (fig.2.45). L'élément qui diffère de l'émetteur est lié au remplacement du VCO par une boucle à verrouillage de phase (PLL). Celle-ci va permettre de régénérer la porteuse chaotique en fréquence reçue en éliminant le bruit en amplitude accumulé pendant la transmission, mais aussi de reconstituer le chaos en bande de base.

Nous verrons, dans un premier temps, l'intérêt d'utiliser une boucle à verrouillage de phase, et quel est son principe de fonctionnement. Nous allons, dans un second temps, exposer le principe de réplication de chaos en l'absence de message. Nous verrons finalement comment ce même principe, lorsque le signal transmis est la porteuse chaotique FM combinée à un message, permet la récupération du seul message par suppression du chaos de masquage.

2.6.1 La boucle à verrouillage de phase : synchronisation

La PLL est utilisée lorsque les conditions de réception du signal FM sont trop difficiles, pour lesquelles le discriminateur ne se comporte plus de manière satisfaisante (cas des communications par satellites). Un préambule sur la boucle à verrouillage de phase et la manière de démoduler des signaux est disponible dans la partie 2.2.3 page 55.

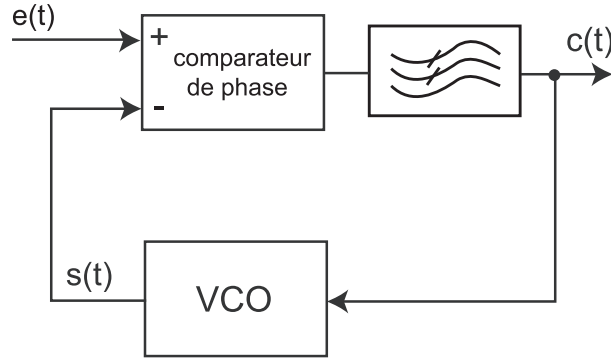


FIG. 2.46 – Synoptique d'une PLL

Une PLL (fig.2.46) est un système bouclé composé d'un comparateur de phase et d'un oscillateur commandé en tension (VCO). Les signaux haute fréquence en entrée et en sortie de la PLL sont respectivement :

$$\begin{cases} e(t) = A \cos[2\pi f_0 t + \varphi(t)] & \text{avec } \varphi(t) = 2\pi k_f \int_0^t m(u) du \\ s(t) = B \cos[2\pi f_0 t + \psi(t)] & \text{avec } \psi(t) = 2\pi k_0 \int_0^t y(u) du \end{cases} \quad (2.51)$$

$e(t)$ est le signal à démoduler et $s(t)$ est le signal en sortie du VCO qui constitue le signal de retour de la PLL. Le signal $c(t)$ délivré à la sortie du filtre, représente également la sortie de la PLL :

$$c(t) = S_{CP} [\varphi(t) - \psi(t)] = S_{CP} \left(2\pi k_f \int_0^t m(u) du - 2\pi k_0 \int_0^t y(u) du \right) \quad (2.52)$$

où S_{CP} est la sensibilité du comparateur de phase. Le filtre, dans le cas d'un comparateur de phase numérique, fait partie intégrante de cet élément. En effet, le comparateur de phase fonctionne comme un OU-exclusif permettant ainsi d'avoir un rapport cyclique proportionnel aux variations de la différence de phase. Ainsi, en conservant uniquement la composante continue, la tension en sortie du filtre sera proportionnelle aux variations $\varphi(t) - \psi(t)$.

Pratiquement, l'insertion du filtre va permettre de contrôler les performances de la boucle à verrouillage de phase en agissant sur son temps de réponse, son gain, son dépassement... La fréquence de coupure du filtre est une caractéristique de la PLL très importante. En effet, il est important de choisir cette fréquence de coupure supérieure à la bande passante du chaos en bande de base [51]. La fréquence de coupure associée à la pente d'atténuation (l'ordre du filtre) doit être choisies de manière à ne pas trop déformer une partie du spectre initial du chaos en bande de base (fig.2.47).

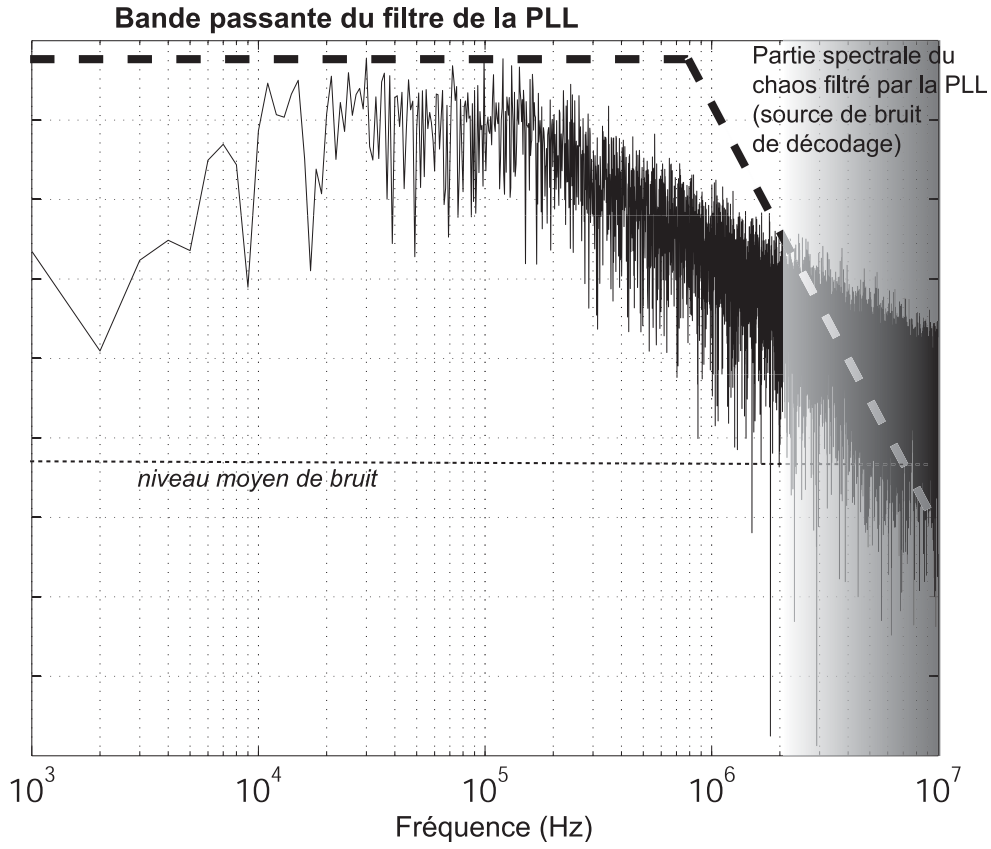


FIG. 2.47 – Influence de la bande passante d'une PLL sur le chaos

2.6.2 Réplication du chaos

La connaissance des clés de codage est nécessaire au décryptage de l'information. Cependant, une erreur somme toute négligeable entraînera une erreur de synchronisation qui fournira un bruit de décodage supplémentaire [30]. Pour étudier l'influence de ces clés, rappelons les équations pour l'émetteur (2.53) et le récepteur (2.54) régissant le principe de synchronisation :

$$x(t) + \frac{\tau_1 \tau_2}{\tau_1 + \tau_2} \frac{dx}{dt}(t) + \frac{1}{\tau_1 + \tau_2} \int_{t_0}^t x(\theta) d\theta = \beta (1 + \cos[\Delta T x(t - T) + \phi]) \quad (2.53)$$

$$y(t) + \frac{\tau'_1 \tau'_2}{\tau'_1 + \tau'_2} \frac{dy}{dt}(t) + \frac{1}{\tau'_1 + \tau'_2} \int_{t_0}^t y(\theta) d\theta = \beta' (1 + \cos[\Delta T' x(t - T') + \phi']) \quad (2.54)$$

Pour pouvoir effectuer une analogie correcte avec les mesures expérimentales, nous nous intéresserons uniquement aux erreurs introduites par des variations de β et ΔT . Les équations (2.53) et (2.54) permettent d'introduire l'équation régissant le comportement de l'erreur instantanée de synchronisation de la fréquence chaotique :

$$\epsilon_{\Delta p}(t) = y_{p'}(t) - x_p(t) \quad (2.55)$$

où $\Delta p = p' - p$ est l'erreur de réglage d'un paramètre entre l'émetteur et le récepteur. L'équation (2.40) va nous permettre de déduire l'erreur de synchronisation instantanée (2.55) en fonction de l'accordabilité d'un des paramètres de codage (ΔT , ϕ , β , T ou les constantes de temps τ_1 et τ_2). Nous choisirons de représenter l'erreur de synchronisation moyenne normalisée à l'amplitude efficace de l'oscillation chaotique :

$$\sigma_{\Delta p} = \sqrt{\frac{\langle \epsilon_{\Delta p}^2 \rangle}{\langle x_p^2 \rangle}} \quad (2.56)$$

Pour déterminer la solution homogène de l'équation (2.53), nous allons poser :

$$u(t) = \int_{t_0}^t x(s) ds \quad (2.57)$$

De ce fait, l'équation (2.53) peut être écrite comme une équation différentielle ordinaire du second ordre et linéaire avec la présence d'un second membre qui permettra de forcer la dynamique à un régime non linéaire chaotique.

$$\dot{u} + \frac{\tau_l \tau_h}{\tau_l + \tau_h} \ddot{u} + \frac{1}{\tau_l + \tau_h} u = \beta (1 + \cos[\Delta T x(t - T) + \phi]) \quad (2.58)$$

Les racines du polynôme caractéristique correspondent à la solution homogène :

$$r_{1,2} = \frac{1}{2(\tau_1 + \tau_2)} \left[-1 \pm \sqrt{1 - \frac{4\tau_1\tau_2}{\tau_1 + \tau_2}} \right] \quad (2.59)$$

Ainsi, la solution stationnaire pour x est donnée par la relation suivante :

$$x(t) = \beta \int_{t_0}^t U(s, t) \cos[\Delta T x(t - T) + \phi] ds \quad (2.60)$$

avec

$$U(s, t) = r_1 e^{(s-t)r_1} - r_2 e^{(s-t)r_2}$$

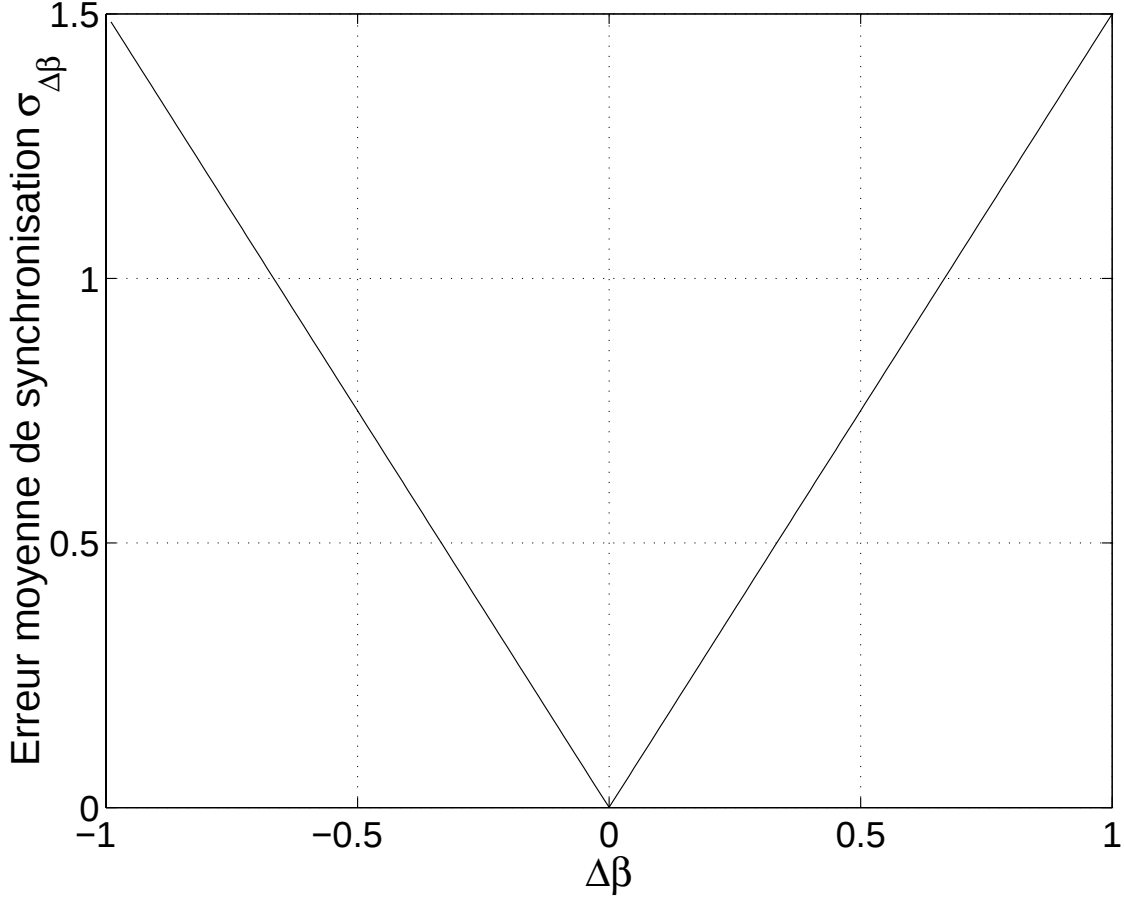
De la même manière, nous obtenons l'expression suivante pour le récepteur :

$$y(t) = \beta' \int_{t_0}^t U'(s, t) \cos[\Delta T' x(t - T') + \phi'] \quad (2.61)$$

Influence du gain normalisé β

En considérant (2.40), et en supposant pour le calcul que $T = T'$, $\phi = \phi'$, $\Delta T = \Delta T'$ et $U(s, t) = U'(s, t)$, nous pouvons en déduire l'équation qui permettra de calculer l'erreur instantanée introduite par un réglage approximatif du gain β (2.62).

$$\langle \epsilon_{\Delta\beta}^2 \rangle = (\beta' - \beta)^2 \left\langle \left[\int_{t_0}^t U(s, t) \cos[\Delta T x(t - T) + \phi] \right]^2 \right\rangle = \left(\frac{\beta' - \beta}{\beta} \right)^2 \langle x^2 \rangle \quad (2.62)$$

FIG. 2.48 – Influence du paramètre β sur la synchronisation

D'après l'équation (2.56), on en déduit la valeur moyenne de l'erreur de synchronisation :

$$\sigma_{\Delta\beta} = \left| \frac{\Delta\beta}{\beta} \right| \quad (2.63)$$

L'équation précédente montre que l'erreur est proportionnelle à la différence $\Delta\beta$. Ainsi, les simulations numériques montrent l'évolution linéaire de l'erreur en fonction de l'écart $\Delta\beta = \beta' - \beta$ mais aussi la symétrie par rapport l'axe qui définit une fonction d'amplification β identique entre l'émetteur et le récepteur (fig.2.48).

Influence de l'ordre de l'interférence ΔT

En s'inspirant de l'équation (2.62), nous pouvons aisément déduire la fonction qui permet de calculer l'influence de ΔT (2.65). Cependant, il est important de préciser que

le déphasage est également un paramètre qui dépend de ΔT .

L'équation régissant le comportement de l'erreur de synchronisation en supposant que l'ensemble des paramètres sont identiques excepté ΔT est :

$$\epsilon_{\Delta T}(t) = 2\beta \int_{t_0}^t U(s, t) \sin \left[\frac{\Delta T + \Delta T'}{2} x(s - T) + \frac{\phi + \phi'}{2} \right] \sin \left[\frac{\Delta T - \Delta T'}{2} x(s - T) + \frac{\phi - \phi'}{2} \right] ds \quad (2.64)$$

Dans un premier temps, pour pouvoir effectuer un calcul plus simple, nous allons supposer d'une part que $\Delta T \approx \Delta T'$, et d'autre part que la valeur de la fréquence centrale est très grande par rapport à l'excursion en fréquence. Ainsi, nous pourrions admettre que l'erreur de synchronisation est uniquement dépendante de $\Delta\phi = \phi' - \phi = (\Delta T' - \Delta T) x_0$, x_0 étant la fréquence centrale normalisée de modulation.

En considérant les approximations et de l'équation précédente, nous pouvons définir l'équation suivante :

$$\epsilon_{\Delta\phi}(t) = -2 \sin \left(\frac{\phi' - \phi}{2} \right) \int_{t_0}^t U(s, t) \cos \left[\Delta T x(t - T) + \phi + \frac{\Delta\phi}{2} - \frac{\pi}{2} \right] ds \quad (2.65)$$

Pour un gain β et un retard T assez grand, le nombre et la valeur des exposants de Lyapunov positifs sont pratiquement indépendants de la valeur du déphasage ϕ [52]. Dans le cas de notre système, cette affirmation est appuyée par le calcul des exposants de Lyapunov sur la figure 2.44. Ainsi, nous pouvons considérer que :

$$\left\langle \left[\int_{t_0}^t U(s, t) \cos[\Delta T x(s - T) + \phi] ds \right]^2 \right\rangle = \frac{\langle x^2 \rangle}{\beta^2} \quad (2.66)$$

Aux vues des approximations faites, le calcul revient à déterminer l'influence d'une erreur de phase sur la synchronisation. Ainsi, dans le cas où la différence entre ΔT et $\Delta T'$ est très faible, l'erreur de synchronisation moyenne suit la relation suivante :

$$\sigma_{\Delta T} = 2 \left| \sin \left(\frac{\Delta\phi}{2} \right) \right| = 2 \left| \sin \left(\frac{(\Delta T' - \Delta T) x_0}{2} \right) \right| \quad (2.67)$$

Rappelons que l'ordre d'interférence ΔT a une influence directe sur la variable dynamique normalisée puisque celle-ci est mise à l'échelle en fonction de ΔT . Cet ordre d'interférence a également une influence, comme nous venons de le voir, sur la phase ϕ . Le calcul permettant de démontrer l'évolution de l'erreur moyenne de synchronisation en fonction de l'erreur de réglage $\Delta T' - \Delta T$ est ainsi relativement complexe. Nous avons

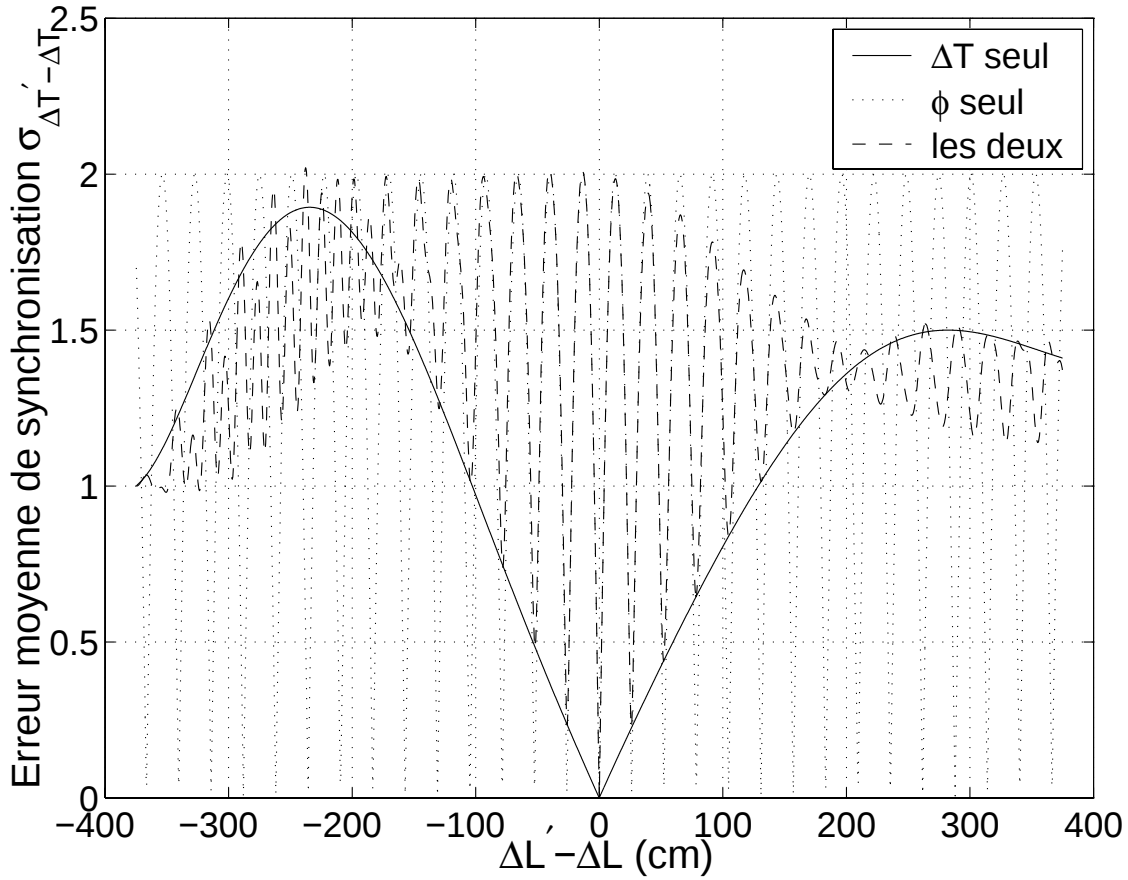


FIG. 2.49 – Influence de la différence de longueur des bras fibrés sur la synchronisation

donc effectué le calcul pour mettre en évidence l'erreur moyenne de synchronisation en fonction de la phase mais nous ne calculerons pas l'erreur totale engendrée par $\Delta T' - \Delta T$. Nous avons, cependant, tracé les différentes formes d'erreur sur la figure 2.49. Nous remarquons que pour une erreur de l'ordre d'interférence assez faible, la relation entre l'erreur moyenne de synchronisation et l'erreur de réglage du paramètre $\Delta T'$ est linéaire.

Influence des constantes de temps du signal en bande de base

Le calcul des erreurs engendrées par une différence entre la bande passante de l'émetteur et du récepteur va mettre en évidence d'une part la nécessité de connaître cette clé de codage en vue de décrypter l'information, mais aussi, cette partie peut permettre de faire le rapprochement avec la conception de la PLL.

En effet, comme nous le soulignons dans la partie 2.6.1, le choix de la constante de temps est très importante pour ne pas perturber la bande passante du chaos. Pour cela, il faut conserver les mêmes fréquences de coupure et le même ordre du filtre passe-bande utilisé sur l'émetteur pour la génération du chaos en fréquence.

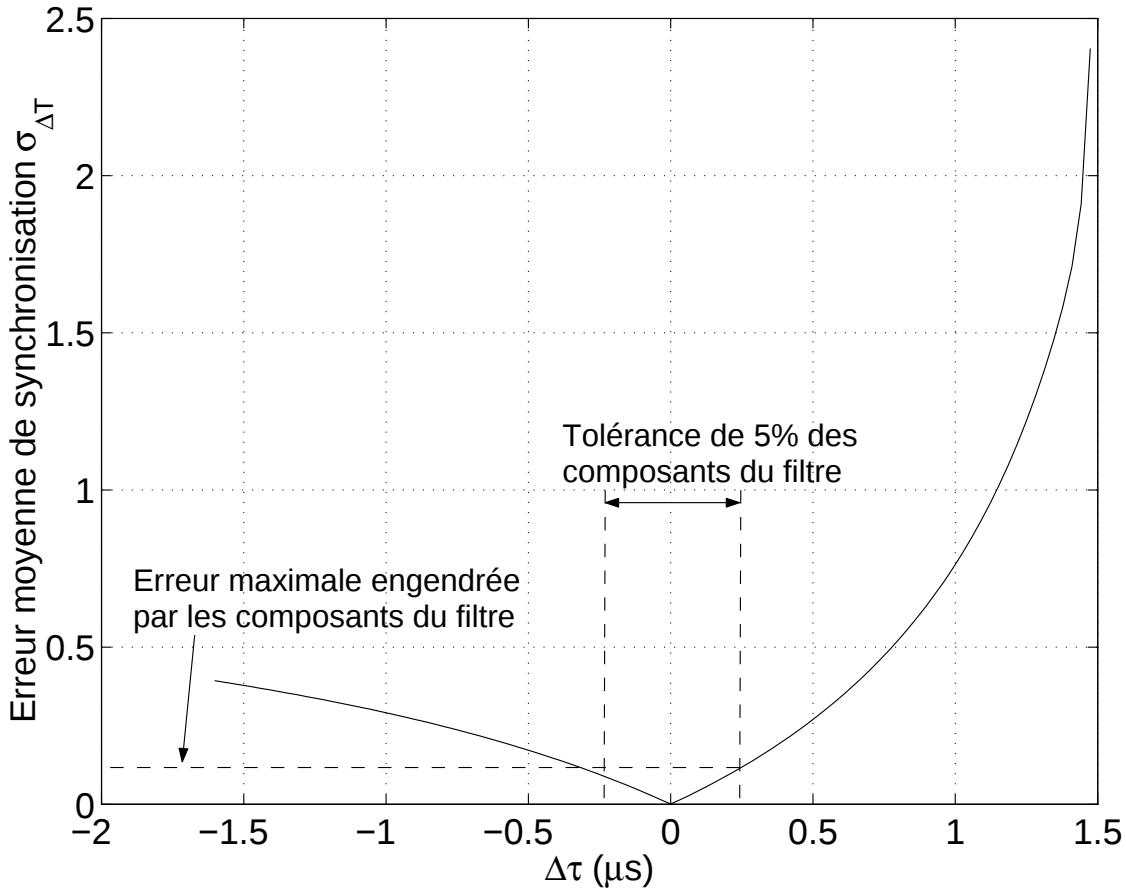


FIG. 2.50 – Influence de la différence de la fréquence de coupure haute sur la synchronisation

Expérimentalement, nous ne pouvons pas faire les mesures pour justifier les calculs. Cependant, la figure 2.50 montre très bien la nécessité de ne pas perturber le spectre chaotique pour ne pas engendrer un bruit supplémentaire de décodage.

En effet, chaque composant utilisé dans la réalisation de la fonction de filtrage, que ce soit la résistance ou la capacité sont susceptibles d'entraîner une variation de 120 ns par rapport à la valeur initiale. Ce filtre est conçu de la même manière du côté de l'émetteur, la tolérance de 5% des composants entraîne alors une erreur maximale de 240 ns sur la constante de temps basse. La fréquence de coupure associée est susceptible de varier de 22 kHz. D'après le calcul précédent, ce désaccord en fréquence de coupure peut entraîner un écart-type du bruit de décodage de l'ordre de 4 %.

2.6.3 Conditions de fonctionnement et de simulations

Nous allons maintenant revenir sur l'approximation qui a été faite à la section 2.4.1 lors de l'établissement du modèle de la transformation non linéaire obtenue par interfé-

rence RF. Cette approximation consiste à considérer que la condition d'interférence est instantanée par rapport aux fluctuations de fréquences qui sont donc supposées lentes. A titre de comparaison, cette approximation est évidente dans le cas du système chaotique en longueur d'onde optique, et n'a même pas été envisagée. Un rapide calcul d'ordre de grandeur, indique que pour une dynamique de la fréquence optique avec un temps caractéristique de l'ordre de $10\mu s$, l'interférence réalisée par le filtre biréfringent correspond à un décalage temporel des ondes optiques dû à la différence de marche de l'interféromètre (1cm environ), de l'ordre de 60ps ; pendant cet intervalle de temps, la fréquence optique n'a pas eu le temps de changer de manière significative, compte tenu de sa dynamique d'évolution de l'ordre de quelques μs . Dans le cas de l'interféromètre RF, d'une part la différence de marche est beaucoup plus importante (elle peut aller jusqu'à la centaine de mètres dans la pratique, donc un décalage temporel de l'ordre de la μs), et d'autre part le temps caractéristique de la dynamique de la fréquence RF est plus rapide (temps caractéristique allant de la μs à la centaine de ns). De ce fait, nous assistons à une interférence entre deux ondes RF qui n'ont pas nécessairement la même fréquence instantanée, donc une condition d'interférence, ou encore une transformation non linéaire, qui devient dynamique par rapport à la modulation FM entre deux instants de l'ordre de la μs . Cette condition doit a priori changer radicalement les propriétés dynamiques des ondes chaotiques obtenues. Nous allons, effectivement, essayer d'observer l'influence des paramètres ΔT et τ (respectivement l'ordre d'interférence et la constante de temps de notre système) sur la fonction non linéaire engendrée par les interférences RF.

$$F_{nl}[\omega(t)] = \frac{(V_0 \kappa)^2}{4} \cos\{\underbrace{[\omega(t-T) - \omega(t-T-\Delta T)]}_{g(t)} t + \omega(t-T-\Delta T) \Delta T\} \quad (2.68)$$

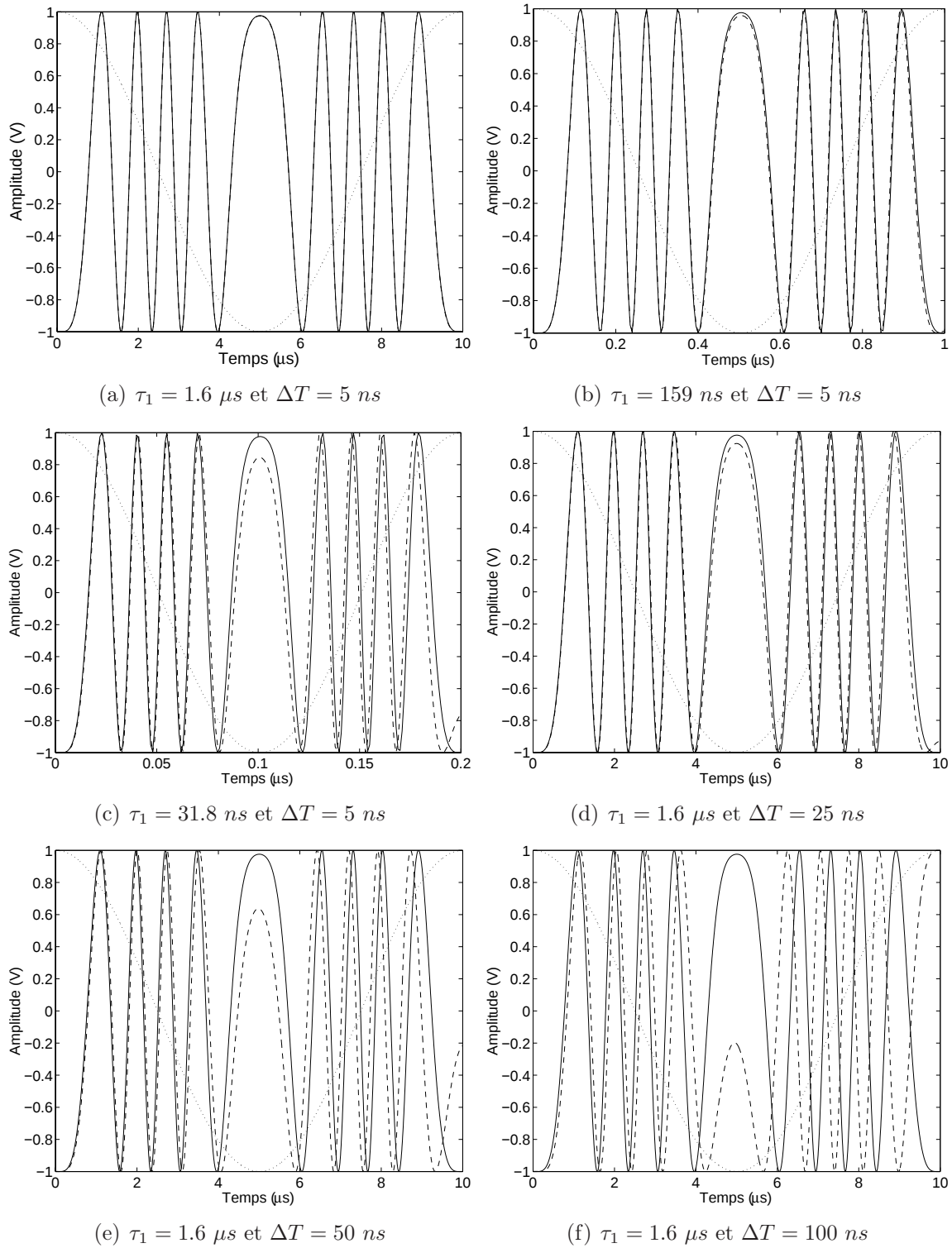
avec

$$\omega(t-T) = \Delta\omega(t-T) + \omega_0 \quad (2.69)$$

A partir de là, plusieurs observations peuvent être faites en considérant la valeur de la différence de fréquence $\omega(t-T) - \omega(t-T-\Delta T)$ due à la rapidité de variation de celle-ci. Intuitivement, la variation de cet élément dépendant du temps vient d'une part de la valeur de la constante de temps τ_1 , mais aussi de la différence de longueur des bras de l'interféromètre ΔT .

2.6.4 Les effets de la constante de temps sur la non linéarité

Pour évaluer qualitativement la nature dynamique de la fonction non linéaire, nous allons montrer que sa représentation graphique change effectivement en fonction des paramètres τ_1 et ΔT .

FIG. 2.51 – Fonction non linéaire pour différents τ_1 et ΔT

Sur la figure 2.51, nous pouvons voir sur un même graphique, en traits pleins la fonction non linéaire si l'approximation $\Delta\omega(t) \equiv \Delta\omega(t - \Delta T)$ est respectée ($g(t) \equiv 0$), et en traits

pointillés, la fonction non linéaire en considérant que l'approximation précédente n'est pas valable, et en traits pointillés fin le signal de modulation du VCO qui est une sinusoïde. Au final, nous pouvons observer l'influence des deux paramètres que sont la constante de temps haute τ_1 et l'ordre d'interférence ΔT sur laquelle nous pouvons agir en modifiant la différence de longueur des deux bras fibrés.

Les deux courbes avec et sans approximation sont confondues pour $\tau_1 \gg \Delta T$ qui représentent les conditions expérimentales que nous avons choisies. Pour les autres graphiques, l'un des deux paramètres varie, entraînant, de ce fait, des variations non linéaires supplémentaires en fonction du temps. Pour que les deux courbes soient confondues et pour pouvoir faire l'approximation $\Delta\omega(t) \equiv \Delta\omega(t - \Delta T)$, il est nécessaire de réaliser cette condition :

$$\tau_1 \gg \Delta T \quad (2.70)$$

Dans le cas où la condition (2.70) ne serait pas respectée, le fonctionnement du système de cryptographie ne serait pas modifié. Simplement, en vue d'une bonne réplique du chaos en bande de base du côté du récepteur, la fonction non linéaire doit être similaire à celle de l'oscillateur. En revanche, cette condition a une importance sur la modélisation du chaos en fréquence généré par notre oscillateur. En effet, dans le cas où le terme temporel $g(t)$ est considérée comme nul, l'interférence a bien une forme sinusoïdale. Dans le cas contraire, $g(t)$ introduira des variations supplémentaires permettant d'augmenter éventuellement l'ordre de notre non linéarité et de ce fait, pour un gain β identique, nous pouvons augmenter la dimension de notre chaos en fréquence.

2.7 Applications aux communications cryptées

De manière générale, les communications analogiques concernent les signaux de type parole en téléphonie, musique pour la radiodiffusion ou images pour la télévision. Il est important d'analyser la qualité de codage et de restitution de l'information afin d'estimer la qualité d'une liaison de communication.

Un point important dans le système de communication sécurisée par le masquage de l'information dans un chaos en fréquence, est l'introduction du message dans la boucle de l'oscillateur. Il est nécessaire de l'extraire dans la même partie de la boucle du côté du récepteur, sinon le message ne serait pas restitué correctement [25].

2.7.1 Analyse du signal chaotique contenant l'information

D'après l'équation (2.40), nous pouvons déduire l'évolution du signal chaotique contenant le message $m(t)$:

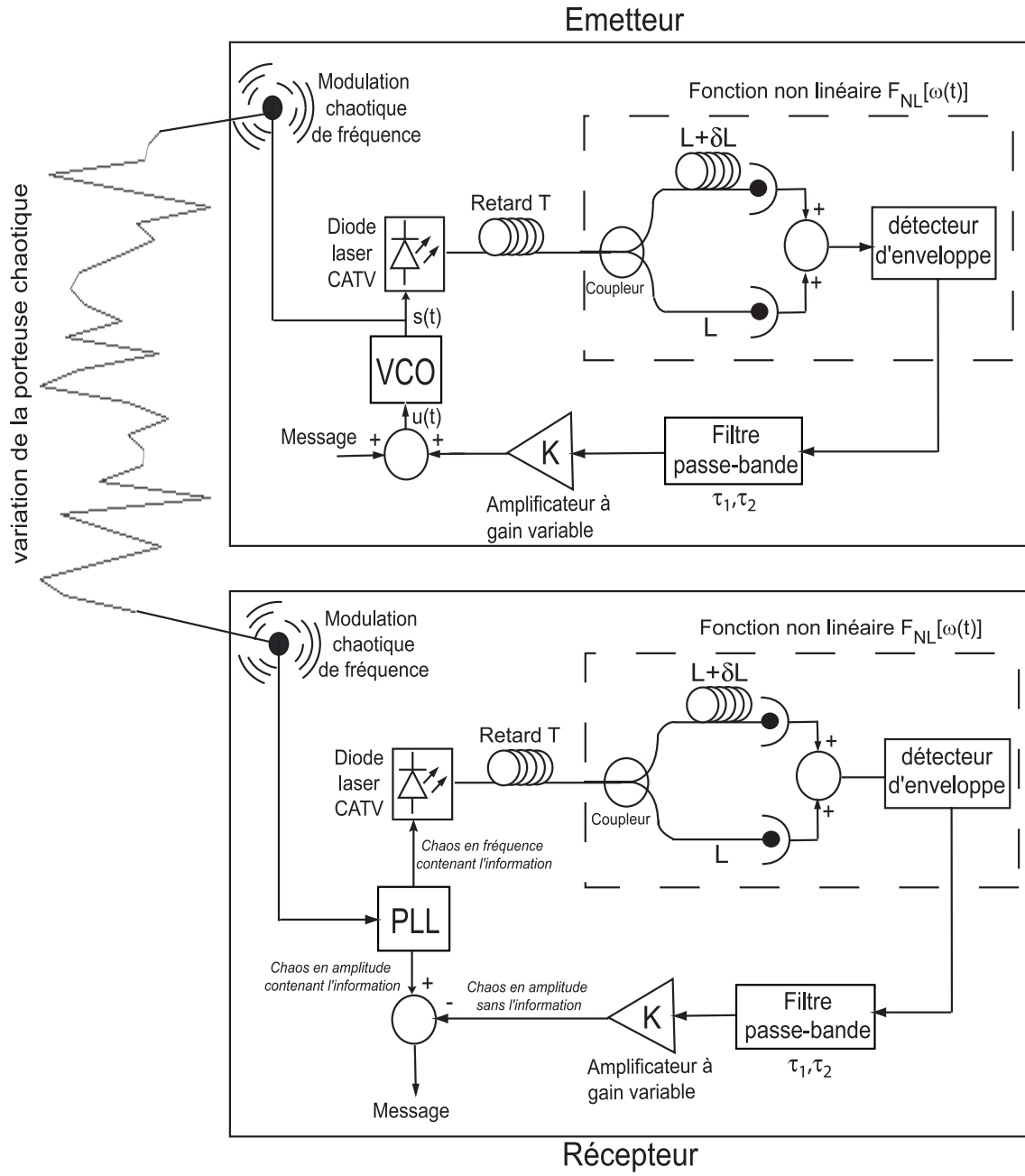


FIG. 2.52 – Système de communication cryptée par chaos en fréquence

$$\tau_1 \tau_2 \frac{d^2 \Delta \omega}{dt^2}(t) + (\tau_1 + \tau_2) \frac{d \Delta \omega}{dt}(t) + \Delta \omega(t) + \omega_0 + h(t) = (\tau_1 + \tau_2) \beta F_{NL}[\Delta T \Delta \omega(t - T) + \phi] \quad (2.71)$$

avec $h(t)$ l'équation différentielle du second ordre contenant le message $m(t)$:

$$h(t) = \gamma_{vco} \left[\tau_1 \tau_2 \frac{d^2 m}{dt^2}(t) + (\tau_1 + \tau_2) \frac{dm}{dt}(t) + m(t) \right] \quad (2.72)$$

Dans notre système comme dans la grande majorité des systèmes de transmission, le

signal porteur de l'information $m(t)$ à transmettre, subit une transposition de fréquence, processus connu sous le nom de modulation ($\omega(t) = \Delta\omega(t) + \omega_0$). Notre message a une bande passante comprise entre 10 kHz et 100 kHz. Ce message fait partie intégrante du signal FM porteur, dont la bande de fréquence est de 100 MHz autour de la fréquence centrale comprise entre 1 et 1.5 GHz. La seule condition pour obtenir une bonne qualité de masquage est que l'amplitude du signal d'information soit faible par rapport à l'amplitude du chaos en bande de base, sous peine de le voir directement (la composante chaotique apparaîtrait comme un bruit de fond, et non plus comme un bruit prédominant).

Comme dans l'ensemble des systèmes de communications, il est nécessaire de réduire au maximum le bruit accumulé pendant la transmission hertzienne, mais aussi le bruit de décryptage dû à des réglages approximatifs de certaines clés de codage. Les clés de codage, que ce soit le retard, l'ordre d'interférence ou la bande passante du chaos en bande de base, ont toute une sensibilité plus ou moins importante sur le décryptage.

L'importance du bruit de décryptage des signaux analogiques est caractérisé par le rapport signal sur bruit [53]. Ainsi, dans le cas d'une information matérialisée par un signal sinusoïdal, la raie spectrale correspondant à la fréquence du signal décodé sera plus ou moins prédominante suivant la valeur du niveau de bruit de décodage.

Un signal chaotique aura pour but de masquer complètement la fréquence de l'information pendant la transmission (fig.2.53). Le cryptage est visuellement de bonne qualité pour le point de fonctionnement qui sera adopté pendant les démonstrations expérimentales c'est à dire $T = 10 \mu s$, $\tau_1 = 1.6 \mu s$, $\Delta T = 25 ns$ et $\beta = 2.6$. En d'autres termes, le pic de fréquence du message aura une amplitude au plus égale au niveau du bruit chaotique.

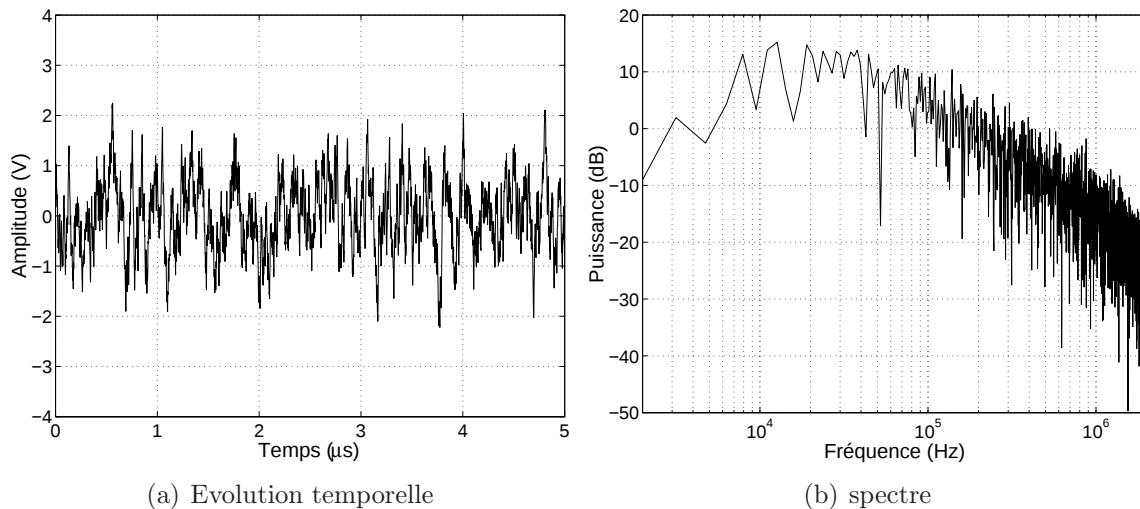


FIG. 2.53 – Chaos en bande de base et information

Nous pouvons maintenant représenter l'évolution temporelle des signaux décryptés,

erreur $\varepsilon_{\Delta T}$	SNR
0	70 dB
666 ps	40 dB
1.3 ns	32 dB

TAB. 2.4 – SNR en fonction de l’erreur de l’ordre d’interférence

en fonction de l’erreur d’accordabilité de l’ordre d’interférence $\varepsilon_{\Delta T}$ entre l’émetteur et le récepteur (fig.2.54). Le SNR¹⁶ obtenu pourra alors nous donner une indication sur la qualité du décodage. Le SNR est le rapport signal/bruit. Le signal correspond à l’amplitude de la raie spectrale et le bruit correspond au niveau moyen du spectre du bruit de décodage autour de cette raie. Le tableau suivant donne le SNR pour chacune des erreurs de l’ordre d’interférence.

Dans les télécommunications actuelles, lorsque le signal reçu d’un émetteur distant est faible, il est très sensible aux perturbations extérieures qui entraîneront une distorsion supplémentaire. D’autre part, dans notre système de cryptage analogique, le bruit de décodage est un facteur supplémentaire de perturbation.

Dans les transmissions actuelles, les mesures expérimentales montrent raisonnablement que la qualité de réception (après décryptage concernant notre système) est considérée bonne lorsque le rapport signal/bruit est supérieur à 40 dB [54]. Dans le cas des simulations numériques précédentes permettant d’extraire le SNR, le bruit engendré par la transmission hertzienne et par le bruit intrinsèque au système de réception (bruit de décodage dû essentiellement à l’imperfection d’accordabilité entre les clés) n’est pas pris en compte. Par conséquent, les simulations ne reflètent pas complètement le comportement expérimental.

En ce qui concerne la transmission d’un signal numérique, la qualité de transmission et de décodage est interprétée par le calcul du BER¹⁷. Celui-ci est caractérisé par le rapport du nombre de bits éronnés par le nombre de bits émis.

Après la transmission d’un signal numérique, nous obtenons un signal de réception déformé par rapport au signal émis (fig.2.55). Le signal perturbé a effectivement subi les altérations suivantes :

- distorsion d’amplitude : les fluctuations brutales du signal émis (transitions brusques générant des harmoniques jusque dans les hautes fréquences) ont été atténuées par un effet de filtrage du canal
- distorsion de phase : mis à part un retard pur, le signal émis a subi une distorsion de phase. On constate cette distorsion dans la déformation des impulsions. On pourrait augmenter cette distorsion jusqu’à ce que le signal reçu soit méconnaissable par

¹⁶Signal Noise Ratio

¹⁷Bit Error Rate

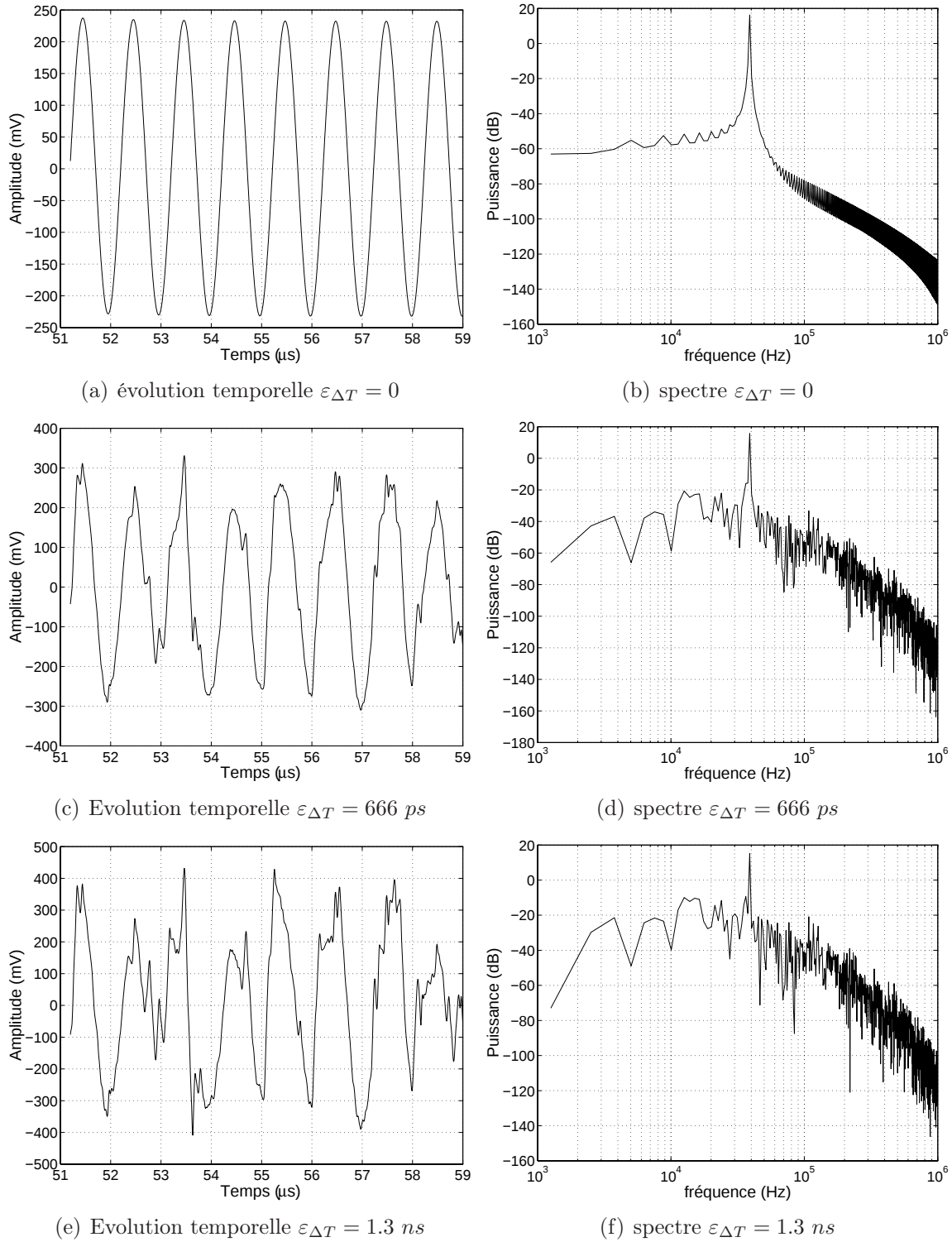


FIG. 2.54 – Evolution temporelle et spectre pour différentes erreurs d'accordabilité

rapport au signal émis.

- du bruit de fond s'est superposé au signal émis. Le bruit de fond peut altérer la reconnaissance d'un signal binaire (un "zéro" est reconnu comme un 1 ou vice versa)

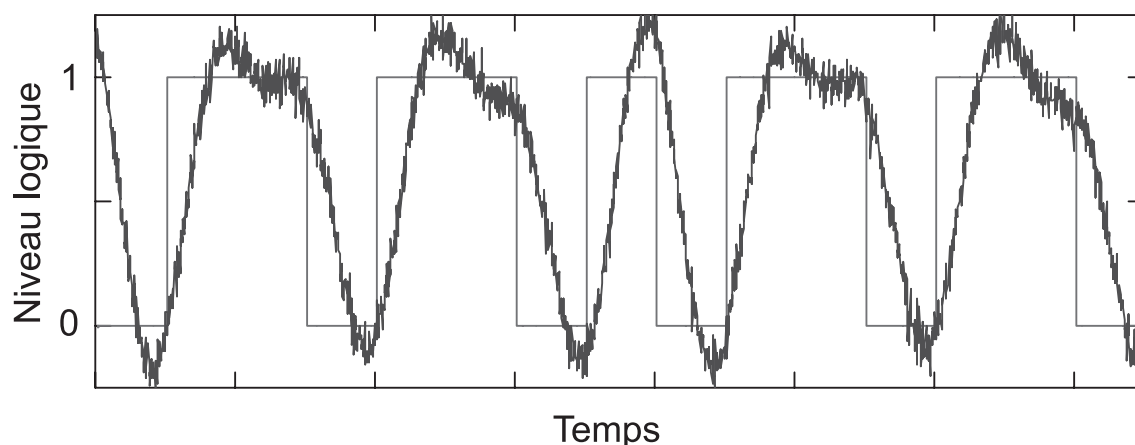


FIG. 2.55 – Exemple de l'influence de transmission sur un signal binaire

Une perturbation supplémentaire détériore le signal décodé dans le cas de notre système de codage analogique, il s'agit de la différence d'accordabilité entre les éléments de l'émetteur et ceux du récepteur.

Expérimentalement et qualitativement, le BER peut être observé en traçant un diagramme de l'œil qui, à partir d'un signal de modulation binaire et pseudo-aléatoire comme signal d'information, va permettre d'établir les propriétés de transmission.

Le diagramme de l'œil permet d'une manière très simple d'apprécier la qualité des signaux numériques reçus. Il s'agit d'une des mesures de base en transmission numérique.

L'«ouverture de l'œil» caractérise le bruit et les distorsions apportées par la chaîne de transmission. L'opération d'échantillonnage doit se produire à l'instant précis où l'œil est le plus ouvert. Un œil bien ouvert permettra au dispositif de démodulation de discerner aisément les symboles transmis. A l'opposé, un œil fermé se traduira inévitablement par de nombreuses erreurs de transmission.

La fermeture de l'œil est le résultat :

- soit du bruit : il faut alors s'efforcer d'améliorer la qualité du signal radio
- soit d'interférences intersymboles : les caractéristiques amplitude-fréquence et/ou phase-fréquence de la chaîne de transmission ne sont pas correctes (NB : ce type de défaut affecte également la qualité de transmission en télévision).

2.7.2 Conclusion

L'ensemble de ce chapitre nous a présenté un premier système électronique de cryptographie par chaos en fréquence, et un second système optoélectronique. Le premier système électronique permettait de transmettre des informations masquées par une porteuse

chaotique dont la fréquence centrale était d'environ 4 MHz. Les résultats expérimentaux ont démontré la possibilité de transmettre une information cryptée basse fréquence. Dans les systèmes de télécommunications actuelles, cette fréquence de transmission est trop faible pour espérer trouver des applications dans la téléphonie mobile, ou dans les communications spatiales. De ce fait, un nouveau système optoélectronique a été proposé, permettant de générer une porteuse de fréquence centrale comprise entre 1 et 1.5 GHz. Cet oscillateur non linéaire à retard génère un signal de fréquence chaotique à partir d'interférences radiofréquences. Ainsi, les applications à la cryptographie par chaos ont pu être démontrées à l'aide des simulations numériques présentées au cours de ce chapitre. Le chaos en fréquence est de grande dimension, et permet ainsi d'obtenir un masquage de l'information d'une plus grande confidentialité. Le chapitre suivant permettra ainsi de vérifier la validité de notre modèle théorique au travers de résultats expérimentaux.

Notes du lecteur

Chapitre 3

Résultats expérimentaux

*La pensée naît d'événements de l'expérience
vécue et elle doit leur demeurer liée comme
aux seuls guides propres à l'orienter*

Hannah Arendt

*La connaissance théorique est un trésor dont
la pratique est la clé,*

Th. Fuller

3.1 Introduction

Au cours de ce chapitre, nous allons exposer les résultats expérimentaux concernant la description des composants utilisés et l'analyse numérique des comportements de l'oscillateur chaotique. Enfin, nous vérifierons l'utilisation de ce système pour des applications à la cryptographie par chaos en fréquence, selon une architecture émetteur/récepteur déjà connue (voir partie 2.7 page 113).

L'oscillateur chaotique sera d'abord abordé par la mise en œuvre expérimentale et la caractérisation de ses fonctions élémentaires. La réalisation de ces fonctions dans un domaine RF a posé des problèmes particuliers liés aux hautes fréquences, qu'il s'agit de bien identifier et de maîtriser si l'on souhaite, au final, un ensemble ayant un comportement chaotique bien compris et contrôlé dans ses mécanismes dynamiques. Cette maîtrise et cette compréhension sont, bien sûr, indispensables au bon fonctionnement d'un système complet émetteur/récepteur capable de masquer et de décoder une information dans la porteuse chaotique FM.

L'analyse et la caractérisation des composants sont très utiles pour prévenir les éventuels défauts de fonctionnement en haute fréquence, notamment au niveau des pertes, les déphasages et les phénomènes non linéaires. Les caractérisations électriques détaillées des comportements hautes fréquences seront effectuées, en particulier pour ce qui concerne les composants intervenant dans la réalisation de la non linéarité. En effet, la totalité de ces

composants fonctionnent dans le domaine des hautes fréquences et sont susceptibles d'apporter des imperfections que nous ne considérons généralement pas dans les simulations numériques.

Nous tracerons les évolutions temporelles et spectrales pour illustrer qualitativement le régime chaotique qui peut être obtenu. Nous compléterons cette analyse en soulignant l'influence du gain β et de la phase ϕ de l'équation (2.43) page 90 sur le régime adopté par l'oscillateur, en traçant quelques diagrammes de bifurcation. Nous verrons, ensuite, l'influence de certains paramètres sur la qualité de réplication du signal chaotique. Ainsi, nous pourrions vérifier que les comportements observés sont conformes aux résultats issus des simulations numériques. Enfin, pour vérifier que le système complet peut fonctionner pour des applications aux télécommunications cryptées, nous coderons puis transmettrons, un message analogique et un message numérique, tout en observant la qualité du message décodé à la sortie du récepteur.

3.2 Analyse des composants de l'oscillateur

Les composants électroniques, optoélectroniques et optiques de notre système ont tous des caractéristiques importantes dans l'oscillateur chaotique. La bande passante, la phase et le gain de leur fonction de transfert vont influencer directement ses caractéristiques. La maîtrise globale de l'ensemble de ces caractéristiques sera particulièrement critique lors de la synchronisation avec un système de réception. En effet, des différences de caractéristiques entre deux composants de l'émetteur et du récepteur auront pour conséquence un bruit de décodage plus ou moins important suivant la nature et l'importance de cette différence ; nous allons donc décrire maintenant les principaux composants dont les caractéristiques en hautes fréquences sont les plus critiques pour le système de cryptographie.

3.2.1 Caractéristique de l'oscillateur commandé en tension

L'oscillateur commandé en tension va permettre de convertir le chaos en amplitude en un chaos en fréquence par wobulation. Sa caractéristique de conversion tension/fréquence sera souhaitée linéaire afin de ne pas introduire un phénomène non linéaire supplémentaire, et difficilement duplicable, par rapport à la fonction d'interférences RF dans notre oscillateur ; une bonne séparation des actions linéaires et non linéaires dans la chaîne d'oscillation sera plus favorable à l'obtention de bonnes conditions de synchronisation.

Le choix de ce composant (ROS-1500) se porte tout d'abord sur la bande passante du signal de modulation. Elle ne doit en aucun cas modifier l'allure du spectre de notre chaos en bande de base. La bande passante du VCO (100 MHz) est ainsi très supérieure à la bande passante du chaos en bande de base qui peut varier de 100 kHz à 5 MHz. Ensuite,

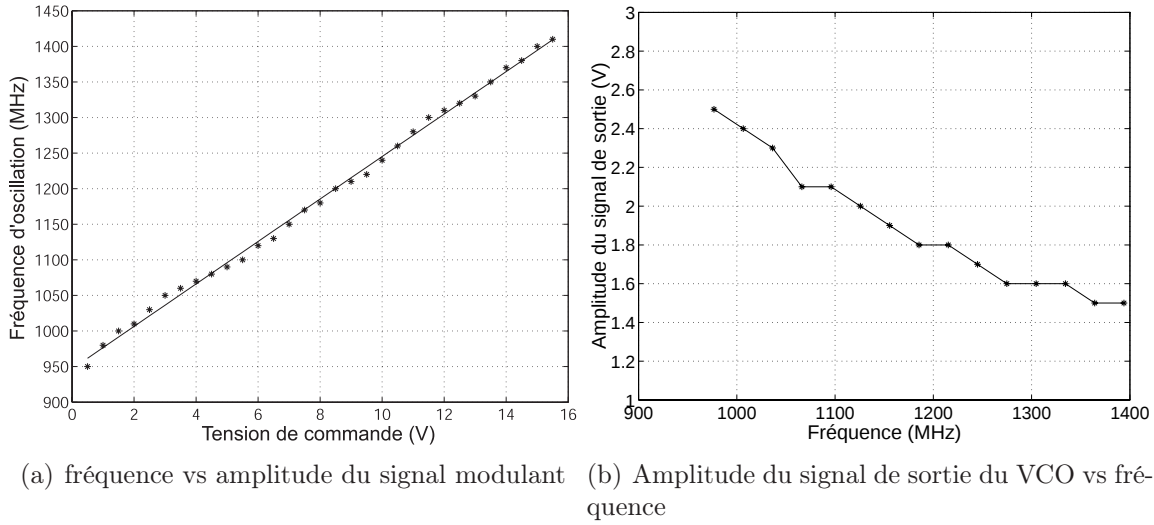


FIG. 3.1 – Caractéristique du VCO (minicircuits ROS-1500)

l'amplitude du signal en sortie (V_0) et la sensibilité γ_{vco} du VCO sont deux paramètres qui agissent sur la gain β de la boucle d'oscillation. Par conséquent, il est indispensable de trouver un composant dont le produit $V_0 \gamma_{vco}$ soit le plus important possible de manière à limiter le nombre d'amplificateurs dans l'oscillateur chaotique.

Les points de mesure permettant de définir précisément la sensibilité et la plage de fonctionnement du VCO suit la régression linéaire (fig.3.1(a)) caractérisée par la relation suivante :

$$F_m(MHz) = 28.9(MHz/V) V_c(V) + 947(MHz) = \gamma_{vco} V_c + f_0 \quad (3.1)$$

La conversion linéaire du VCO peut être cependant perturbée indirectement par des fluctuations de l'amplitude du signal de sortie qui n'est pas constante suivant la fréquence de modulation (fig.3.1(b)). Par la suite, nous pourrions montrer l'influence de cette amplitude variable en observant le type de régime (stationnaire, périodique ou chaotique) adopté par notre oscillateur, suivant les conditions de fonctionnement choisies. Le gain β dépend effectivement de l'amplitude du signal en sortie du VCO, et la prise en compte de ce phénomène modifie légèrement le modèle dynamique de l'oscillateur (changement de la fonction non linéaire, modulation du profil de cette dernière par la dépendance de l'amplitude).

Pratiquement, nous pouvons observer que le taux de distorsion harmonique (TDH) global du signal sinusoïdal en sortie du VCO est relativement important (fig.3.2). La valeur maximum de ce taux peut atteindre $TDH = 22\%$, ce qui signifie que le signal en sortie du VCO est très déformé. Pour conserver la validité du modèle théorique et réduire

la valeur de ce taux, nous allons placer un filtre SAW¹. Ainsi, le signal qui va moduler en puissance la diode laser CATV aura un meilleur taux de distorsion ($TDH = 3.5\%$ pour la valeur la plus haute).

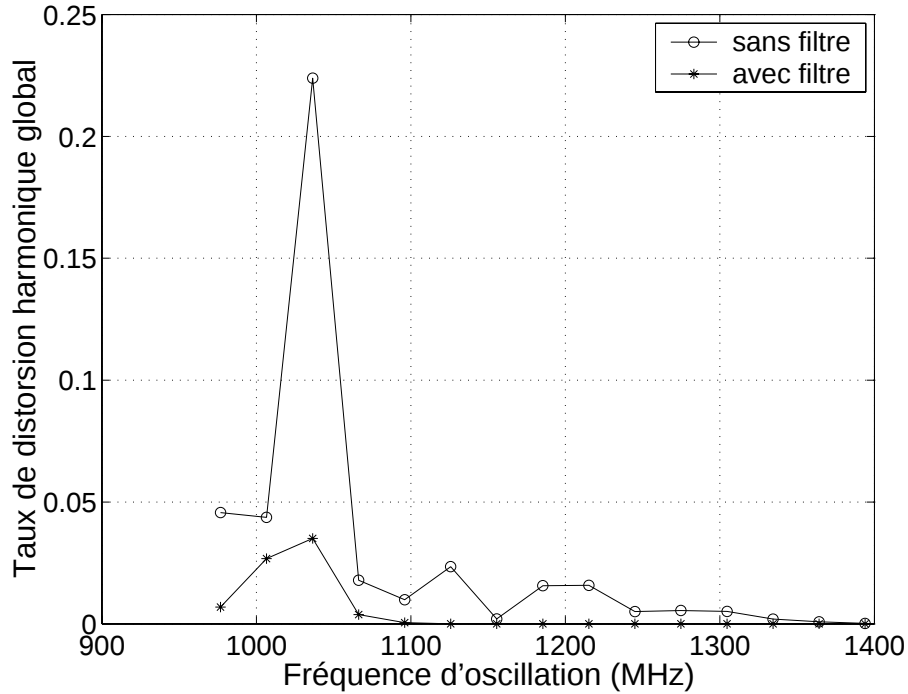


FIG. 3.2 – Taux de distorsion global du signal en sortie du VCO avec et sans filtre SAW

Le filtre SAW a une fréquence de coupure de 1.7 GHz et une pente d'atténuation importante supérieure 40 dB/dec au delà de sa fréquence de coupure. Un filtre dont la fréquence de coupure serait plus proche de 1.5 GHz, aurait été plus adapté. Il aurait encore diminué le taux de distorsion. Le taux de distorsion obtenu est cependant convenable avec l'insertion du filtre choisi.

3.2.2 La non linéarité

La non linéarité (fig.3.3) est la fonction la plus sensible à mettre en œuvre expérimentalement. Constituée de composants optiques, optoélectroniques, et électroniques, des imperfections supplémentaires liées à ces derniers peuvent altérer la fonction d'interférences, dépendant en principe uniquement de la différence de longueur entre les bras fibrés.

Les composants électroniques et optoélectroniques en haute fréquence possèdent des caractéristiques expérimentales effectives qui sont à l'origine de dysfonctionnements, comme

¹Surface Acoustic Wave

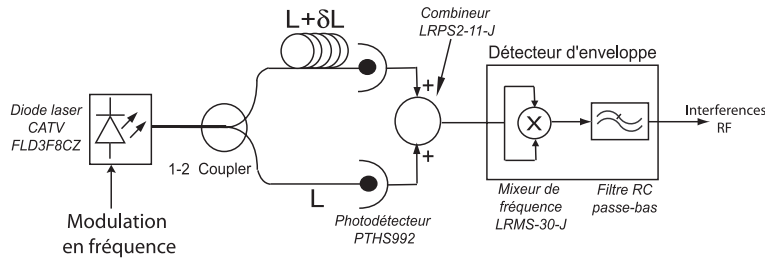


FIG. 3.3 – Réalisation expérimentale de la fonction non linéaire

l'écart de paramètres de certaines fonctions entre les éléments de l'émetteur et du récepteur. Ces caractéristiques expérimentales sont :

- une impédance d'entrée des composants qui n'est pas constante sur toute la plage de fréquence utile
- des paramètres S présentant des différences sensibles tant en module qu'en phase
- des effets capacitifs et inductifs dus à l'imperfection des pistes dans la conception des cartes électroniques

Pour pouvoir mesurer l'ensemble des paramètres utiles à une analyse pertinente, nous avons utilisé un analyseur de réseau vectoriel [55]. Il s'agit d'un appareil de mesure dont le fonctionnement est assez complexe. En pratique, il existe deux types d'analyseur de réseau : scalaire et vectoriel. L'analyseur de réseau scalaire mesure uniquement le module de transfert alors que l'analyseur de réseau vectoriel mesure également la phase. Par conséquent, l'analyseur de réseau vectoriel utilisé va permettre de mesurer les coefficients de réflexion en entrée et en sortie (S_{11} et S_{22}) et les coefficients de transmission direct et inverse (S_{21} et S_{12}).

Caractérisation des composants optoélectroniques

La caractérisation des composants optoélectroniques concerne la photodiode et la diode laser CATV. Nous allons mesurer les paramètres S_{11} et S_{21} caractérisant respectivement les paramètres de réflexion à l'entrée du composant, et les paramètres de transmission directe (voir figure 3.4, caractéristiques électriques de la liaison laser et photodiode).

Le quadripôle optoélectronique (fig.3.4) est composé de :

- la diode laser CATV fibrée (longueur de fibre ≈ 2.2 m)
- un coupleur 10/90 permettant d'atténuer d'une part la puissance optique de la diode laser, et d'observer d'autre part la modulation de l'intensité sans perturber l'oscillateur (longueur de fibre ≈ 5 m).
- un photodétecteur également fibré (longueur de fibre ≈ 1.1 m)

L'abaque de Smith sert, entre autres choses, à convertir le coefficient de réflexion à l'impédance de charge (et vice-versa). Son cadre d'utilisation est cependant bien plus

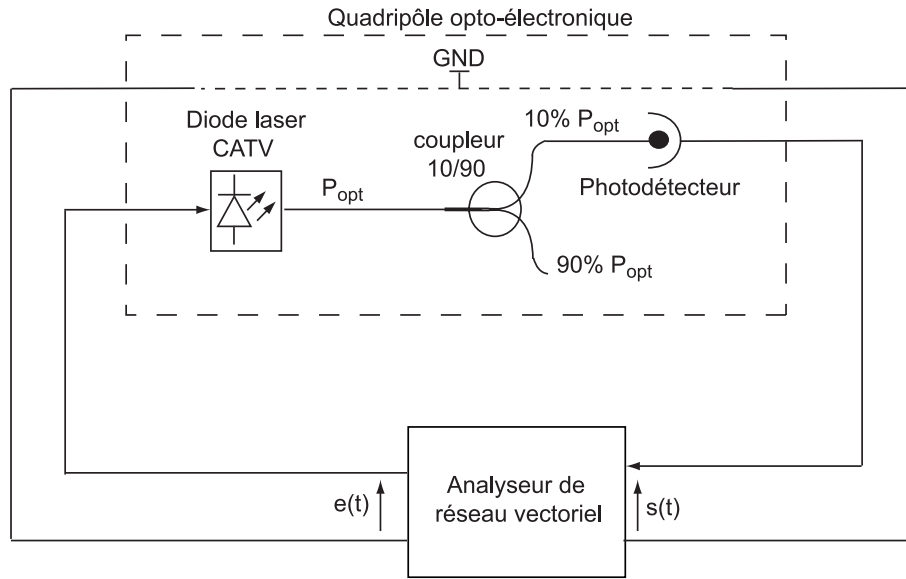


FIG. 3.4 – Constitution du quadripôle optoélectronique

large. Il est utilisé pour de nombreuses opérations de caractérisation des phénomènes ondulatoires des ondes électriques hautes fréquences qui mettent en jeu des décalages de longueur de conducteurs; par exemple, dans le plan des coefficients de réflexion, un décalage de l'onde électrique d'une distance x se traduit par un simple déphasage :

$$\Delta\phi = \frac{4\pi}{\lambda} x \quad (3.2)$$

Dans le cas de nos mesures, les longueurs de pistes mises en jeu sont négligeables par rapport à la longueur d'onde de notre signal électrique. Notre signal qui peut évoluer entre 950 MHz et 1.5 GHz correspond à une longueur d'onde minimale de 20 cm. En revanche, le déphasage du paramètre de réflexion provient des variations de la partie réelle et imaginaire de notre impédance d'entrée complexe. Pratiquement, un tour complet dans l'abaque correspond à un déphasage de 2π .

La figure 3.5 représente l'abaque de Smith du paramètre S_{11} . Les variations du coefficient de réflexion entraînent des pertes supplémentaires dans la transmission du signal. La plage de fonctionnement dans laquelle peut évoluer notre système (soit 950 MHz/1.5 GHz) est matérialisée par les points 1 et 2. Dans cet intervalle, nous remarquons que les variations du paramètre S_{11} suivent un cercle de rayon à peu près constant. Cela signifie que l'impédance complexe à l'entrée du composant possède une partie réelle de valeur constante. En revanche, sa partie imaginaire ne l'est pas.

Avec l'abaque de Smith relevé expérimentalement sur le quadripôle optoélectronique,

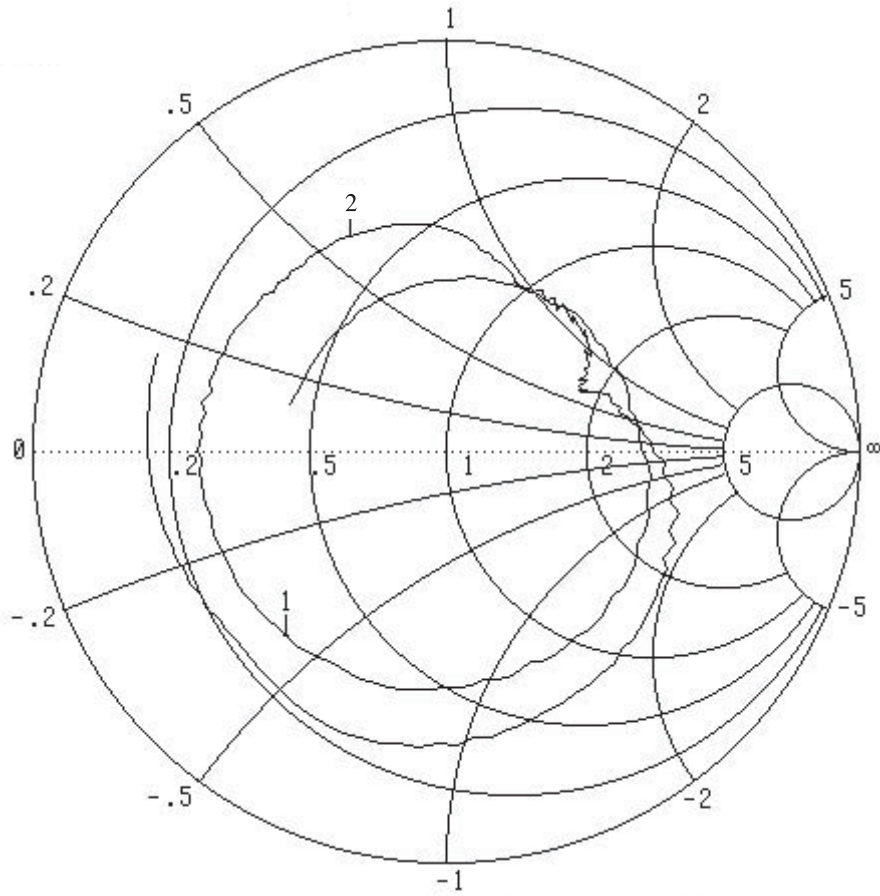


FIG. 3.5 – Paramètres S_{11} (réflexion à l'entrée) du quadripôle optoélectronique

nous pouvons définir dans la bande de fréquence nous concernant le TOS², ROS³ ou VSWR⁴. L'abaque de Smith (fig.3.5) n'est pas complet. L'abaque ne montre que les paramètres en échelle radiale, le TOS, les coefficients de réflexion et de transmission, (dB, P, V et I) ne sont pas indiqués.

Le VSWR de ce quadripôle est donc $\rho = 4.5$ et le coefficient de réflexion est $\Gamma = 0.63$. Le coefficient de réflexion est relativement important. Cependant, sa forte valeur ne présente pas un problème majeur si ce coefficient est le même du côté du récepteur.

Le paramètre S_{21} caractérise la transmission directe du composant. Elle est assimilable au tracé d'un diagramme de Bode (module et phase) et donne des informations très importantes sur le fonctionnement de l'élément optoélectronique.

Dans notre cas, nous pouvons observer des variations de phase très importantes. Pour sa caractérisation, l'élément optoélectronique complet est constitué de la diode laser fibrée,

²Taux d'Onde Stationnaire

³Rapport d'Onde Stationnaire

⁴Voltage Standing Wave Ratio

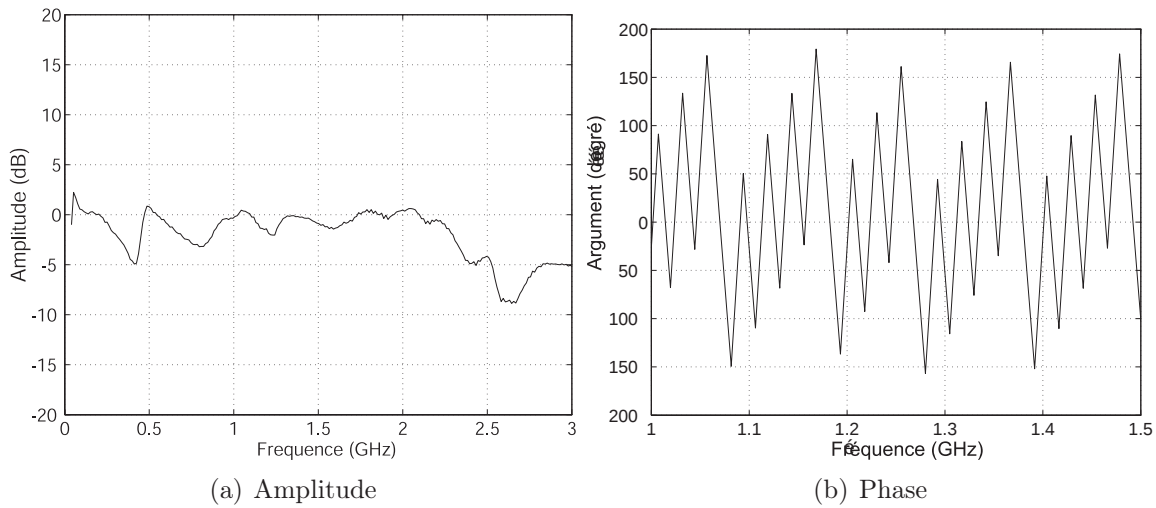


FIG. 3.6 – Paramètre de transmission S_{21} du quadripôle optoélectronique

et d'un coupleur 10/90 permettant d'atténuer la puissance optique pour le photodétecteur qui est le dernier composant. L'ensemble de ces composants introduit entre l'entrée et la sortie de l'analyseur vectoriel une longueur de fibre de 8.3 m. Cette longueur est assimilable à un retard tel qu'il est souhaité dans notre oscillateur chaotique. Cette analyse montre que le retard a une importance capitale sur notre oscillateur puisque celui-ci introduit, par exemple, un déphasage supplémentaire permettant de vérifier le critère de Barkhausen (voir 1.2.1 page 8) pour un grand nombre de fréquences dans notre boucle d'oscillation.

La périodicité du déphasage dépend approximativement de la longueur de fibre optique entre les deux composants optoélectroniques :

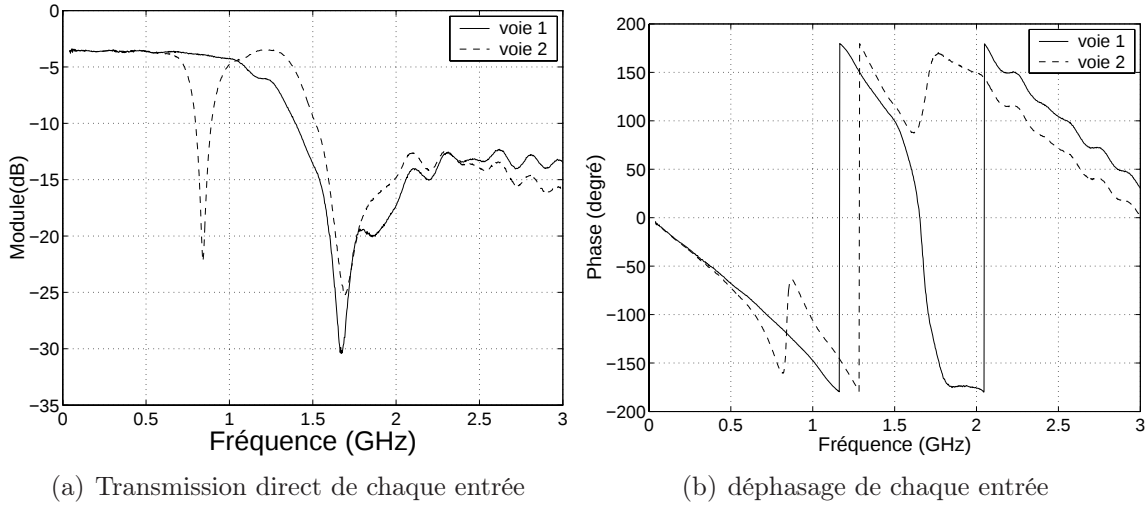
$$\phi = \frac{n L \omega}{c} \iff L = \frac{c \phi}{n \omega} \quad (3.3)$$

Dans notre cas, une variation de fréquence Δf de 25 MHz suffit à provoquer une variation de phase de 2π . La longueur physique mesurée est $L \approx 8.2$ m, ce qui correspond à une variation de fréquence Δf de 24.1 MHz. Par conséquent, nous pouvons en déduire que le retard introduit par la longueur de fibre optique explique très bien les variations importantes de déphasage observées.

Caractérisation du sommateur (Minicircuits LRPS-2-11J)

Le sommateur est réalisé à partir d'un combineur de puissance qui va ajouter (ou combiner) la puissance des signaux déphasés de chacune des entrées pour pouvoir obtenir des interférences RF.

Pratiquement, nous observons un déséquilibre entre les deux entrées (fig.3.7(a)). Ce déséquilibre va entraîner une pondération d'une entrée sur l'autre. En théorie, le signal

FIG. 3.7 – Paramètre de transmission S_{21}

issu du combineur devrait être $V_S = V_1 + V_2$ où V_1 et V_2 sont les tensions de chaque signal d'entrée. Le composant entraînera une pondération des signaux d'entrée sur le signal de sortie pour obtenir $V_S = \alpha V_1 + \gamma V_2$ où α et γ sont des coefficients d'atténuation.

Ce composant est bidirectionnel et est intégré dans un circuit électronique. Ainsi, Le composant situé après celui-ci aura une onde réfléchi qui deviendra, de ce fait, une onde incidente sur la sortie de notre combineur de puissance. Cette onde a un effet perturbateur supplémentaire dans la mise en cascade de quadripôles.

Le calcul des paramètres S de deux composants montés en série ne revient pas à la multiplication des matrices $[S]$ caractérisant chaque composant. En effet, celle-ci n'est pas chaînable. Nous ne détaillerons pas les calculs dans cette partie (voir annexe D pour le détail des calculs). Le résultat de la mise en cascade de deux quadripôles dont le premier (diode laser + photodétecteur) est unidirectionnel et le second bidirectionnel (sommateur) est le suivant :

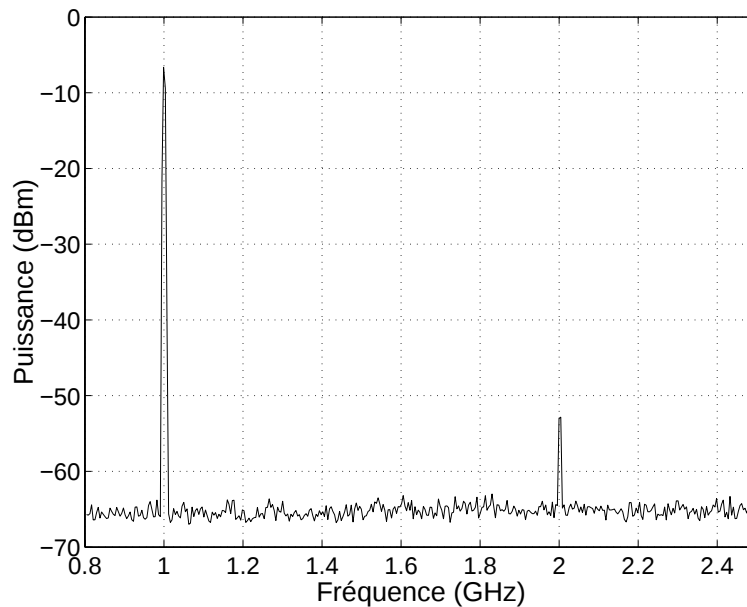
$$S = \begin{pmatrix} S'_{11} & 0 \\ S_{21} S'_{21} & \frac{S_{22} S'_{21}}{S'_{12}} \end{pmatrix} \quad (3.4)$$

où S'_{ab} correspondent aux paramètres de l'ensemble optoélectronique et S_{ab} aux paramètres du sommateur.

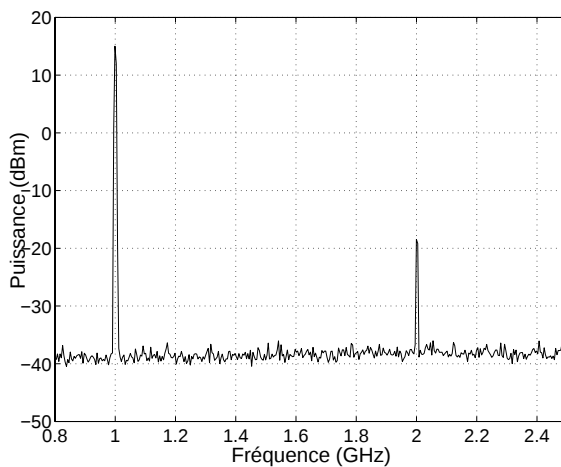
La matrice obtenue est facilement interprétable physiquement. En effet, le paramètre de réflexion dépend uniquement de la réflexion à l'entrée de la diode laser. Le paramètre de transmission inverse est logiquement nul. Le paramètre de transmission direct est le produit des paramètres de transmission de chacun des composants.

Caractérisation de l'amplificateur (Minicircuits ERA-8SM)

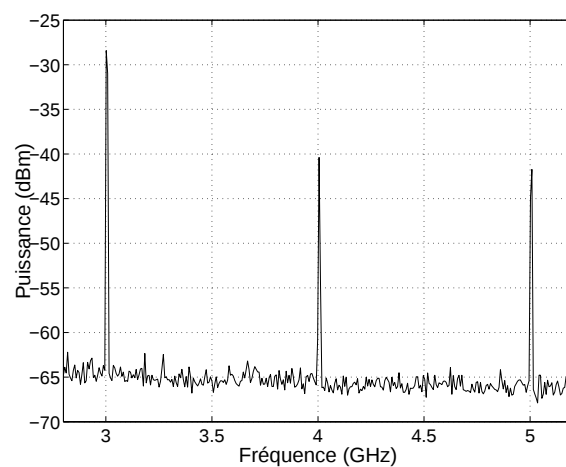
L'amplificateur est également un paramètre sensible en HF. En effet, celui-ci peut être à l'origine des non linéarités supplémentaires. La caractérisation de l'amplificateur avec les paramètres S ne permet pas de mettre en évidence le comportement non linéaire, qui est en général caractérisé par le taux de distorsion harmonique.



(a) Spectre du signal d'entrée



(b) Signal de sortie (fondamental et premier harmonique)



(c) Signal de sortie (autres harmoniques)

FIG. 3.8 – Amplification d'un signal sinusoïdal avec l'amplificateur ERA-8SM

L'amplification a été normalisée, c'est pour cela que celle-ci reste à 0 dB. Afin de ne pas détériorer le matériel, le signal de sortie de l'amplificateur est atténué par une fonction de l'analyseur vectoriel. Ce composant est très bien adapté. L'abaque de Smith

montre, en effet, que S_{11} (fig.3.2.2) s'éloigne très peu du centre de l'abaque synonyme d'une adaptation parfaite. En effet, le centre de l'abaque montre que l'impédance d'entrée du composant, pour la plage de variation de la fréquence du test (soit 40 MHz à 4 GHz), reste approximativement constante et proche de 50Ω .

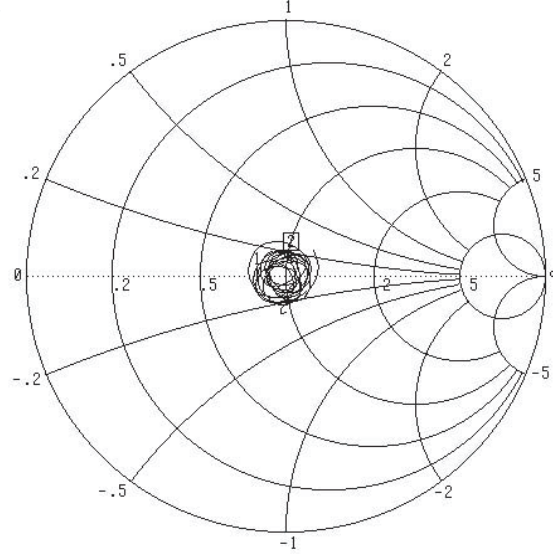


FIG. 3.9 – Paramètre de réflexion S_{11}

Le taux de distorsion harmonique est observable sur la figure 3.8. Nous souhaitons, en bout de chaîne RF, obtenir l'enveloppe d'un phénomène d'interférence entre 2 ondes RF purement sinusoïdales. La présence d'harmoniques, et la nature large bande de certains composants, sont susceptibles d'occasionner, en plus des interférences sur le fondamental, des interférences entre harmoniques. Pour s'affranchir de cela, nous pouvons voir que, lorsque l'ensemble des harmoniques du signal d'entrée sont négligeables (fig.3.8(a)), le signal de sortie possède des harmoniques beaucoup plus importants mais dont l'amplitude reste négligeable par rapport au fondamental (fig.3.8(b) et 3.8(c)). Le signal d'entrée, ajusté à une puissance de -10 dBm, correspond à $100 \mu\text{W}$. Le signal de sortie n'est donc pas saturé et ne peut pas introduire des harmoniques supplémentaires dus à un écrêtage. Le taux de distorsion harmonique mesuré a pour valeur :

$$THD = 0.7\%$$

Cette valeur a une influence largement négligeable sur le modèle adopté dans le chapitre précédent. Cependant, si celui-ci était plus important, ce phénomène non linéaire ne pourrait plus être considéré comme négligeable ($THD > 1\%$) et des déformations du signal seraient observables dans son évolution temporelle. Le modèle théorique caractérisant l'oscillateur devrait alors être modifié afin de pouvoir refléter plus fidèlement le

fonctionnement réel.

3.2.3 Relevé expérimental de la fonction d'interférence

Le déphasage introduit par la différence de longueur de chacun des bras fibrés va générer des interférences constructives et destructives pour obtenir une non linéarité de forme sinusoïdale. A la sortie du sommateur, nous avons une modulation d'amplitude créée par la modulation de fréquence du VCO. La figure 3.10 est obtenue en modulant le VCO par une rampe (évolution linéaire de la fréquence), et en détectant le signal RF à la sortie de l'amplificateur.

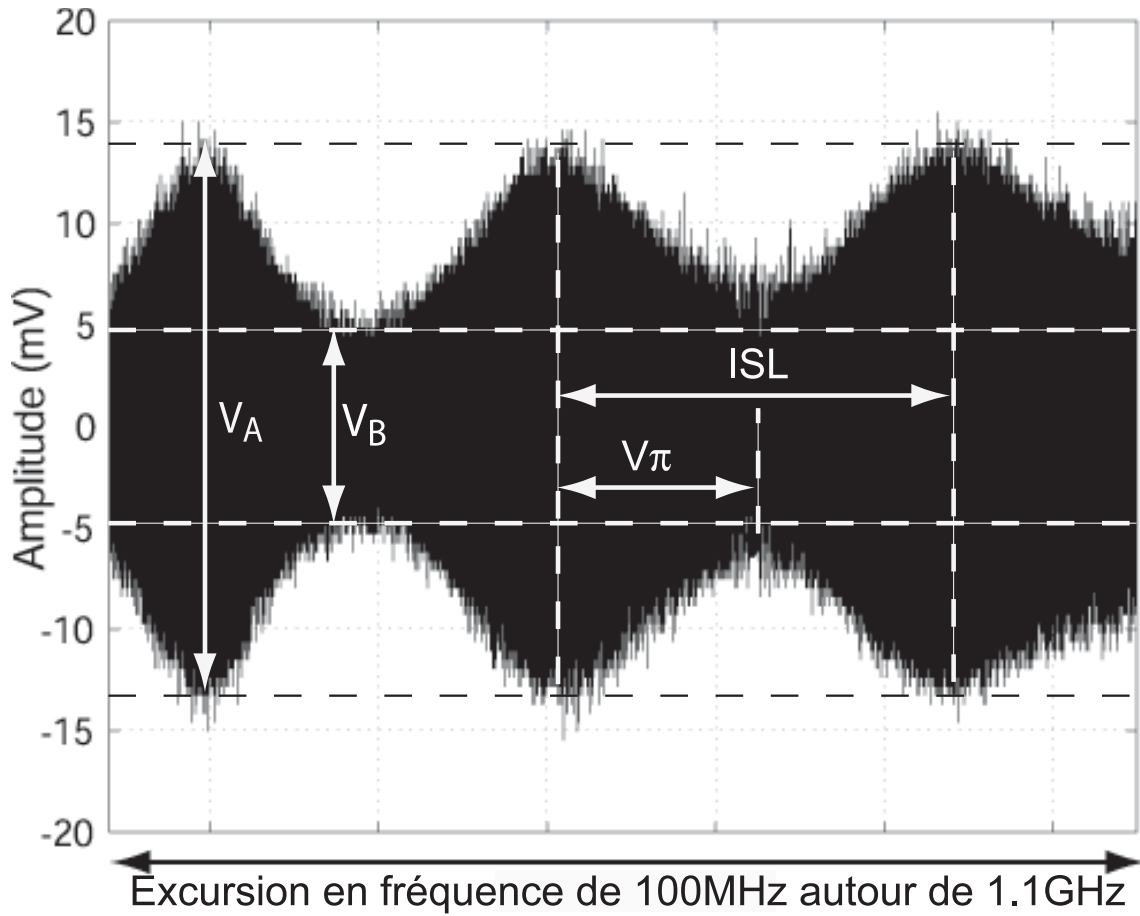


FIG. 3.10 – Interférences RF

Le comportement global de la fonction d'interférence est bien cohérent avec les mesures individuelles des composants RF faites précédemment. Le principe des oscillateurs chaotiques est basé sur leur fonctionnement non linéaire. Pour notre oscillateur chaotique en fréquence, il est nécessaire de pouvoir trouver un lien non linéaire entre la modulation en fréquence et la modulation en amplitude qui sera traitée en bande de base. C'est le rôle rempli par les interférences RF que nous venons de montrer expérimentalement.

En se référant à la figure 3.3 page 125, la sommation des deux porteuses RF après chacun des photodétecteurs, dans le cas d'une différence de longueur de fibre optique de 5 m soit $\Delta T = 25$ ns, pour une modulation de fréquence linéaire de 100 MHz, donne des variations d'amplitude en fonction de la porteuse représentées sur la figure 3.10. Une des données importantes de cette modulation est l'indice de modulation du signal obtenu. L'indice de modulation est donné par la relation suivante :

$$m = \frac{V_A - V_B}{V_A + V_B} \quad (3.5)$$

Dans le cas de notre système, cet indice de modulation a pour valeur $m = 47.4\%$. A présent, il faut éliminer la porteuse HF afin de conserver uniquement l'enveloppe. La qualité de la démodulation d'amplitude est fonction de la valeur de l'indice de modulation.

La détection d'enveloppe

La détection d'enveloppe est effectuée par un détecteur quadratique.

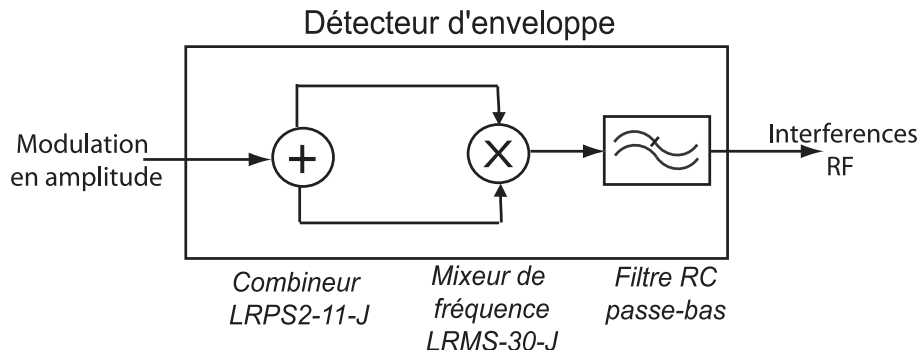


FIG. 3.11 – Constitution du détecteur d'enveloppe

Les caractéristiques hyperfréquences du combineur de puissance sont les mêmes que précédemment (mesurées pour le sommateur). A partir des deux signaux identiques fournis par le combineur, le mixeur va générer une composante spectrale à une fréquence nulle (élimination de la porteuse HF), et une autre correspondant à $2F$.

Seule la composante B.F. est utile dans la bande d'oscillation non linéaire. Celle-ci est conservée par un filtre passe-bas alors que la composante à $2F$ est rejetée. Un filtrage passe-haut, de fréquence de coupure très basse, est également mis en œuvre afin de ne pas avoir de composante continue dans le spectre chaotique en bande de base. La combinaison de ce passe-bas avec un passe-haut conduit à une dynamique limitante en bande de base de type passe-bande.

La réalisation de ce filtre a été faite à l'aide de dipôles R et C (fig. 3.13). Ceci nous permet de contrôler effectivement la dynamique limitante de type passe-bande de l'oscil-

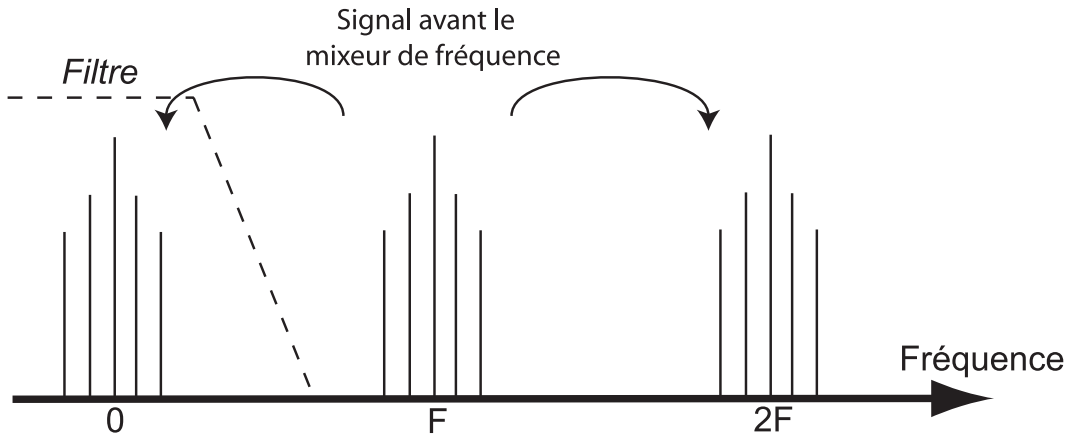


FIG. 3.12 – Principe de fonctionnement du détecteur d'enveloppe

lateur chaotique. Les valeurs des résistances et des condensateurs choisis ont conduit à un filtre passe-bande du second ordre, avec des coupures haute et basse de $f_l = 10$ kHz et $f_h = 100$ kHz respectivement.

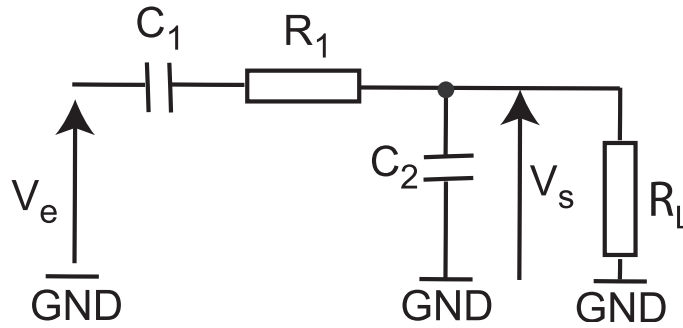


FIG. 3.13 – Filtre passe-bande

De manière plus précise, la fonction de transfert du filtre passe-bande est défini par :

$$H_{\text{filtre}}(p) = \frac{R_l C_1 p}{1 + (R_1 C_1 + R_l C_2 + R_l C_1) p + R_1 R_l C_1 C_2 p^2} \quad (3.6)$$

où R_l est la résistance de charge et $p = j \omega$.

Compte tenu des valeurs des fréquences de coupure très éloignées, et de la faible sélectivité du filtre (second ordre), la réponse du filtre est apériodique, et ne présentera aucune oscillation dans la réponse transitoire. Il s'agit effectivement d'un système sur-amorti (coefficient d'amortissement z supérieur à 1).

$$\left\{ \begin{array}{l} \omega_n = \frac{1}{\sqrt{R_1 R_l C_1 C_2}} \\ z = \frac{R_1 C_1 + R_l C_2 + R_l C_1}{2 \sqrt{R_1 R_l C_1 C_2}} \end{array} \right. \quad (3.7)$$

Connaissant la valeur de chacun des composants ($R_1 = 10 \Omega$, $R_t = 100 \Omega$, $C_1 = 100 \text{ nF}$ et $C_2 = 22 \text{ pF}$) nous pouvons, à partir du coefficient d'amortissement et de la pulsation naturelle, définir les fréquences de coupure de notre filtre (3.8).

$$\begin{cases} \tau_2 = \frac{1}{\omega_n (z - \sqrt{z^2 - 1})} \\ \tau_1 = \frac{1}{\omega_n (z + \sqrt{z^2 - 1})} \end{cases} \quad (3.8)$$

Ainsi, le coefficient d'amortissement, la fréquence naturelle, et les fréquences de coupure de notre système sont pratiquement calculés de manière précise avec les valeurs suivantes :

$$z = 4.45, f_n = 10.73 \text{ kHz}, f_2 = 12 \text{ kHz} \text{ et } f_1 = 95 \text{ kHz}$$

Pour vérifier l'appariement de la bande passante de notre système expérimental (émetteur et récepteur), nous avons tracé le diagramme de Bode de chacun d'eux (fig.3.14).

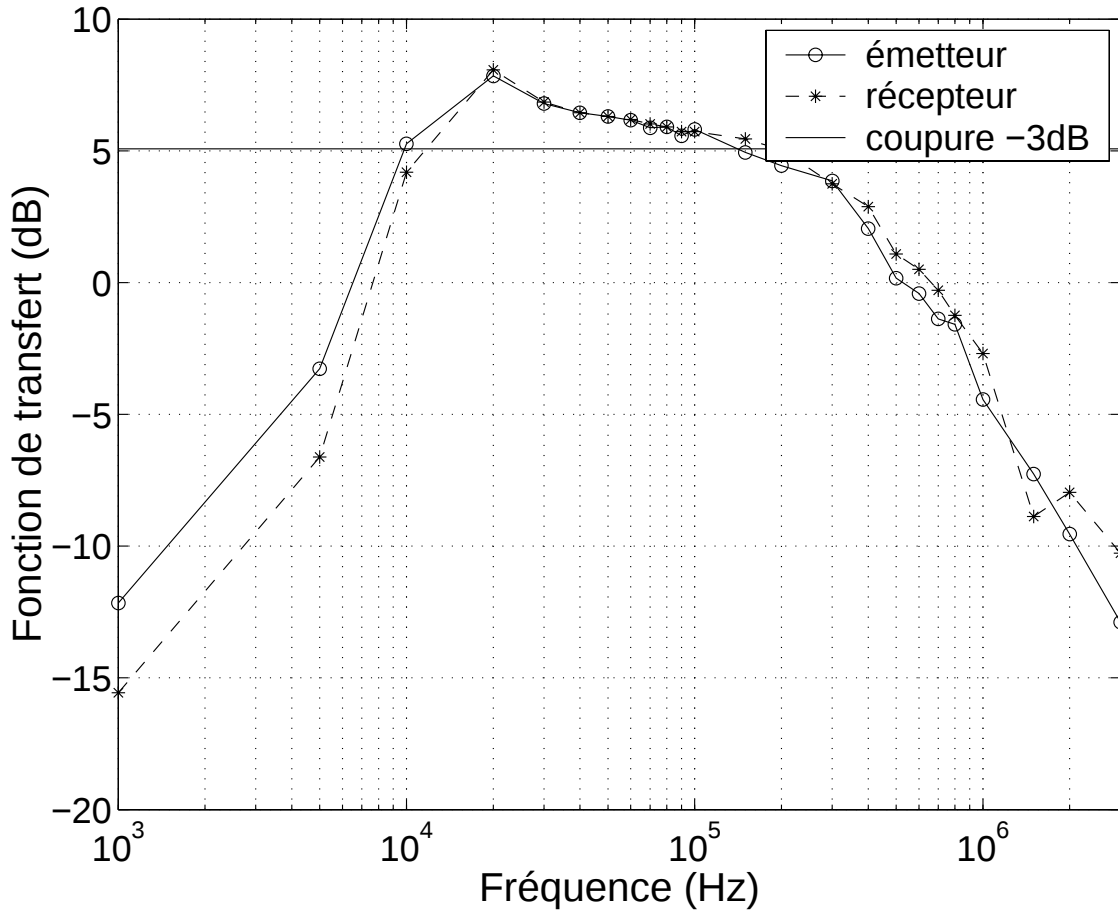


FIG. 3.14 – Diagramme de Bode des systèmes d'émission et de réception

La bande passante est approximativement respectée. La tolérance des composants peut être à l'origine de cette légère erreur. La pente d'atténuation correspond très bien à celle d'un filtre passe-bande du second ordre soit -20 dB/dec.

3.3 Analyse des interférences RF

Nous venons de voir comment réaliser une fonction non linéaire à partir d'interférences RF. Le principe de sa mise en œuvre reste simple, mais le phénomène d'interférence RF peut être assez complexe à analyser, suivant les paramètres expérimentaux choisis. Nous allons proposer une telle analyse dans différentes situations quantitatives telles que des variations de la différence de longueur entre les deux bras de l'interféromètre (voir la figure 3.3 page 125). Nous présenterons et interpréterons les résultats obtenus pour des faibles et des grandes différences de chemin RF, avant de proposer des critères de choix des paramètres de l'interféromètre RF pour notre oscillateur chaotique.

3.3.1 Faibles différences de chemin RF

Comme nous l'avons souligné tout au long de la partie 3.2.3 page 132, la non linéarité a été réalisée avec la génération d'interférences RF. Cette situation, d'un point de vue du principe, a déjà été explorée expérimentalement en optique. Cependant, nous allons tenter ici de montrer que le comportement dynamique des interférences en RF peut être qualitativement très différent de la situation rencontrée en optique.

Une différence de longueur $\Delta L = 1$ cm entre les deux bras de l'interféromètre RF représente, en optique, 6450λ (pour une longueur d'onde $\lambda_{opt} = 1.55 \mu m$ très courante en télécommunications). Cette même différence de longueur représente, en RF, pour une fréquence de modulation de 1 GHz (soit $\lambda_{elec} = 30$ cm) une longueur d'onde de $\lambda/30$. Deux valeurs significativement très différentes qui, sur le plan expérimental, ne se maîtrisent pas avec la même simplicité. Nous allons donner un exemple en calculant les valeurs numériques pour obtenir un ISL⁵ relatif équivalent en optique et en RF.

1. En optique, pour une différence de longueur $\Delta L = 1$ cm, l'excursion en longueur d'onde pour balayer l'ISL est d'environ $\Delta \lambda = 2 \text{ \AA}$. Le laser semiconducteur accordable pour les télécoms optiques permettent effectivement, et très facilement, de balayer cet ISL, et même beaucoup plus. Le montage optique (voir partie 1.5.3 page 44) permettra donc d'avoir accès expérimentalement à des non linéarités d'ordre très élevé (voir les explications liées à l'interféromètre de Mach-Zehnder de la partie 2.25 page 80 pour compléter cette explication), donc à des comportements chaotiques de très grande complexité.

⁵Intervalle Spectral Libre

2. En RF, pour une différence de longueur $\Delta L = 5$ m, l'excursion en fréquence pour balayer l'ISL est d'environ $\Delta f = 40$ MHz. L'obtention de comportements aux propriétés semblables à celles du montage optique, nécessitent donc en RF, pour $\Delta L = 5$ m, une source RF accordable sur plusieurs fois l'excursion de 40 MHz. Ceci fixe les contraintes sur la source à utiliser (par exemple, $f_0 = 1.5$ GHz, avec $\Delta f = 100$ MHz).

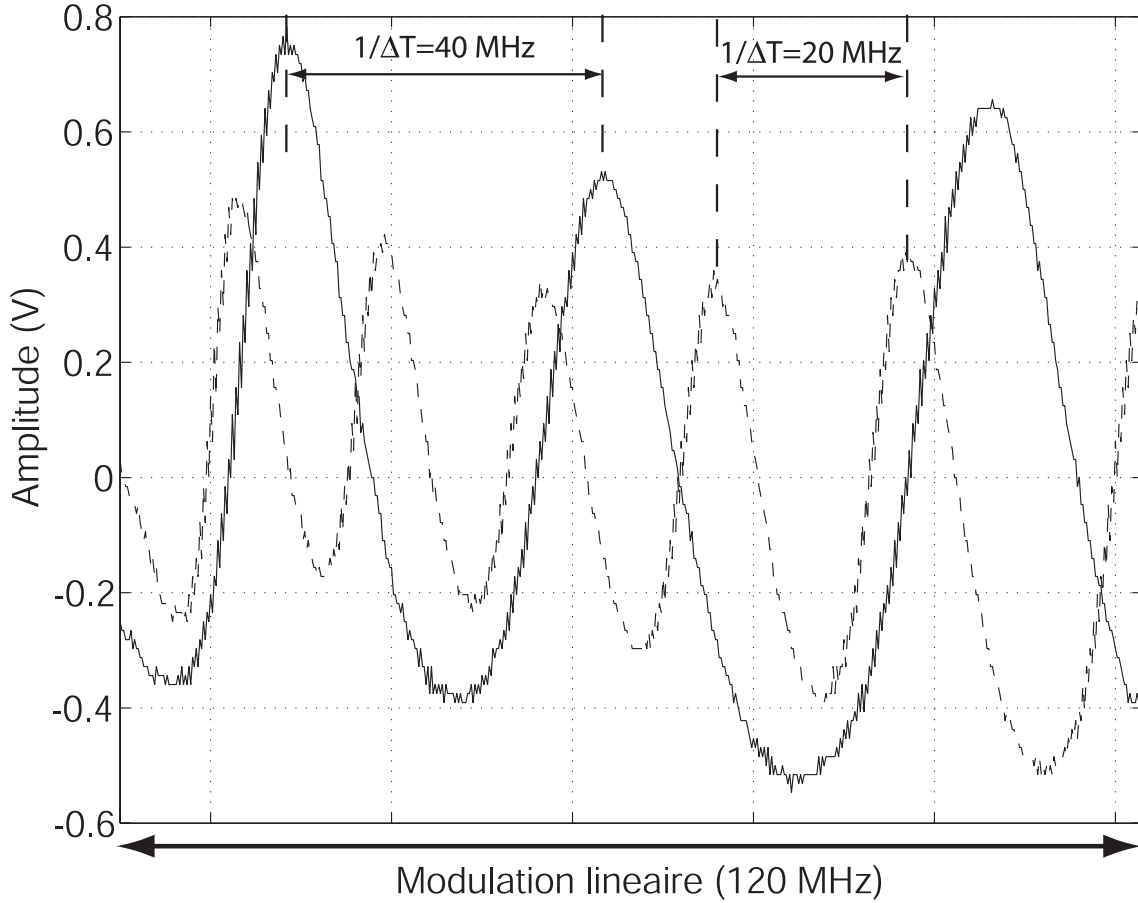


FIG. 3.15 – Non linéarité expérimentale pour $\Delta L = 5$ m et $\Delta L = 10$ m ($f_0 = 1.08$ GHz)

Inversement, si l'on se fixe la source accordable (donc la plage d'accordabilité en fréquence), et que l'on cherche la différence de chemin RF permettant de balayer un nombre donné d'ISL, on procède de la manière suivante : le nombre d'extrema est inversement proportionnel à la différence de longueur entre les deux bras fibrés. L'ISL de l'interférence est défini par :

$$ISL = \frac{1}{\Delta T} = \frac{c}{n \Delta L} \quad (3.9)$$

où c est la célérité dans le vide, n l'indice de réfraction de la fibre optique, et ΔL la

différence de longueur entre les deux bras. Ainsi, nous obtenons respectivement $ISL = 40$ MHz et $ISL = 20$ MHz, pour $\Delta L = 5$ m et $\Delta L = 10$ m.

Ce paramètre physique est, en effet, directement lié à l'ordre d'interférence comme le montre la figure 3.15.

3.3.2 Grandes différences de chemin RF

Le paramètre commun entre un montage interférométrique optique et RF est la célérité $c = 3 \cdot 10^8$ m/s. Pour une différence de longueur entre les bras du montage interférométrique de 5 m et 1 cm (valeur pour lesquelles nous avons calculé les excursions en fréquence et en longueur d'onde qui permettent de balayer les quelques ISL recherchés pour la complexité du comportement chaotique), nous avons respectivement $\Delta T = 25$ ns et $\Delta T = 50$ ps.

Ce sont ces valeurs de ΔT qui sont à l'origine de propriétés dynamiques fondamentalement différentes entre le montage optique et le montage RF, malgré un principe physique de base identique (cf. paragraphe précédent). Ces valeurs de ΔT sont à comparer, d'un point de vue dynamique, aux temps d'évolution caractéristiques de chacun des montages. Dans le cas optique (chaos en longueur d'onde) travaillant dans une gamme de fréquence audio, les temps caractéristiques sont de l'ordre de la dizaine de μs . Comparé aux 50 ps de ΔT , on explique très facilement que le processus d'interférence optique est nécessairement instantané. Au contraire, dans le montage RF, les 25 ns sont à comparer aux temps caractéristiques d'une dynamique de modulation RF de l'ordre du $1/10 \mu s$. Nous observons donc ici des temps de variation de la modulation RF non négligeables par rapport au temps de parcours de la différence de chemin RF. *Le phénomène d'interférence n'est alors plus instantané.*

Cette situation est illustrée à la figure 3.16 dans les conditions expérimentales extrêmes (pour un temps caractéristique de modulation $\tau_1 = 40$ ns, nous avons réalisé expérimentalement $\Delta L = 1$ km, soit $ISL = 200$ kHz et $\Delta T = 500$ ns à la figure 3.16(b) et $\Delta L = 500$ m, soit $ISL = 400$ kHz et $\Delta T = 250$ ns à la figure 3.16(c)).

Des cannelures caractéristiques apparaissent alors dans le spectre du signal RF de sortie de l'interféromètre. Ces cannelures s'expliquent théoriquement en écrivant l'expression du signal observé après le mixeur de fréquence qui réalise le détecteur d'enveloppe quadratique à la sortie de la non linéarité de notre système (3.10). On obtient l'expression suivante :

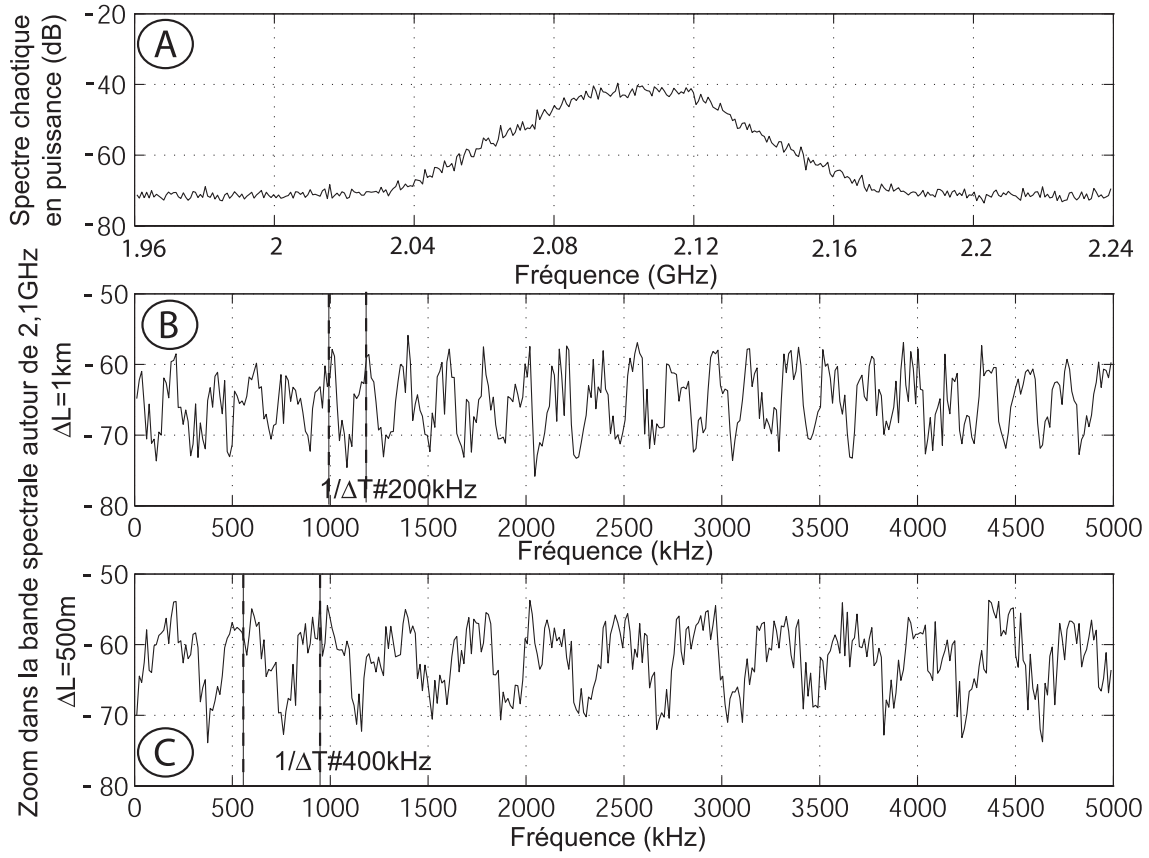


FIG. 3.16 – Cannelure dans le spectre chaotique

$$A_2(t) = \frac{(V_0 \kappa)^2}{4} \underbrace{\left[\cos^2(\omega(t-T)(t-T)) + \cos^2(\omega(t-T-\Delta T)(t-T-\Delta T)) + \right.}_{\text{termes d'interférence à } 2f} \underbrace{\left. \cos\{[\omega(t-T) - \omega(t-T-\Delta T)](t-T) + \omega(t-T-\Delta T)\Delta T\} \right]}_{\text{termes en BF}} \quad (3.10)$$

Les termes en $\cos^2$ sont à l'origine du signal à $2f$ observé spectralement. Ces deux termes, compte tenu de la variation pseudo-aléatoire de $\omega(t)$ avec des temps caractéristiques plus rapide que ΔT , génèrent des cannelures issues d'un phénomène d'interférence à $2f$. Le second terme de l'équation (3.10) représente la partie BF de la transformation non linéaire dynamique (et non instantanée) qui est effectivement utilisée dans la chaîne d'oscillation chaotique. Le spectre de cette composante BF est représenté à la figure 3.17 avec la même échelle horizontale que pour la composante à $2f$ (fig. 3.16(b) et 3.16(c)). On peut remarquer l'absence de cannelures dans ce spectre BF, ce qui est un point positif en termes de confidentialité (identification de la fonction non linéaire par le spectre BF impossible)

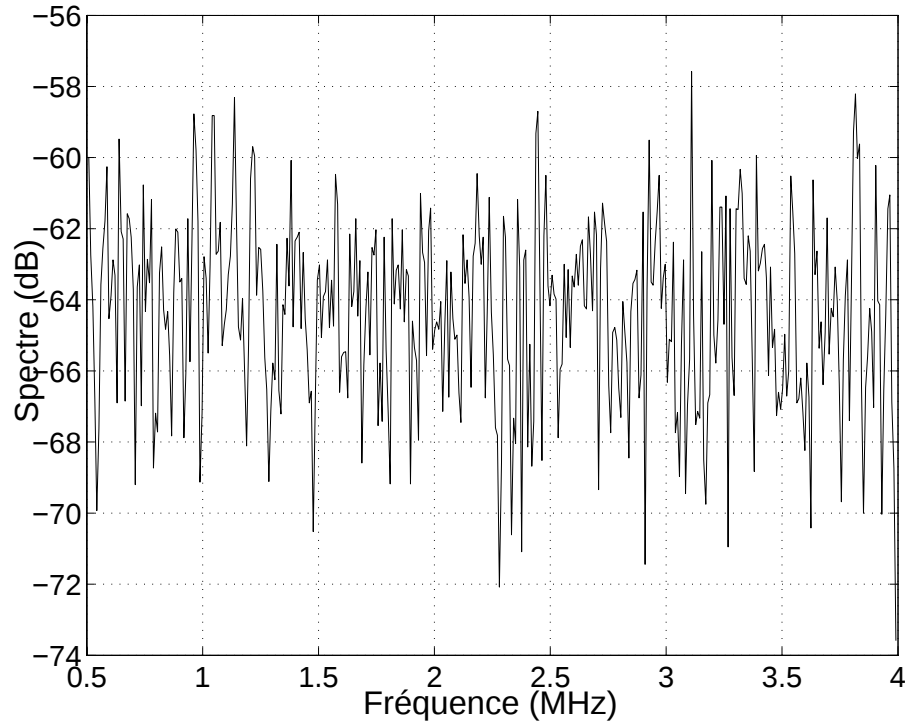


FIG. 3.17 – Spectre BF du signal à la sortie du mixeur de fréquence

3.3.3 Choix des paramètres de l'interféromètre RF

D'un point de vue pratique, nous venons donc de montrer que le montage RF, contrairement au montage optique, nous permet de mettre en œuvre deux types différents de générateur de chaos, en fonction des valeurs des paramètres dynamiques du système. Pour obtenir un montage RF du même type que le générateur optique, les simulations numériques ont montré que l'ordre d'interférence et la fréquence de coupure haute du système devait respecter la relation $\Delta T \ll \tau_1$, τ_1 étant la constante de temps liée à la fréquence de coupure haute. En effet, sans cette approximation, le terme temporel aurait une valeur non négligeable dans la relation non linéaire (3.10).

Si, par contre, nous souhaitons un générateur de chaos basé sur des interférences dynamiques, on choisira $\Delta T > \tau_1$. Pour illustrer ces deux types de générateur de chaos, nous avons effectué quelques mesures de la fonction d'interférence (sortie BF) pour deux constantes de temps différentes et pour des ordres d'interférences de valeurs successives 25 ns, 500 ns, 2.5 μ s et 5 μ s (fig.3.18). La représentation est réalisée de façon à observer pour un même ordre d'interférence, l'effet relatif de deux bandes passantes différentes ($\tau_1 = 1.6 \mu$ s et $\tau_1 = 40$ ns).

Pour ces relevés de la fonction d'interférence (sortie BF), nous avons choisi un signal modulant le VCO dont la fréquence vaut approximativement 10 kHz (à l'intérieur du filtre

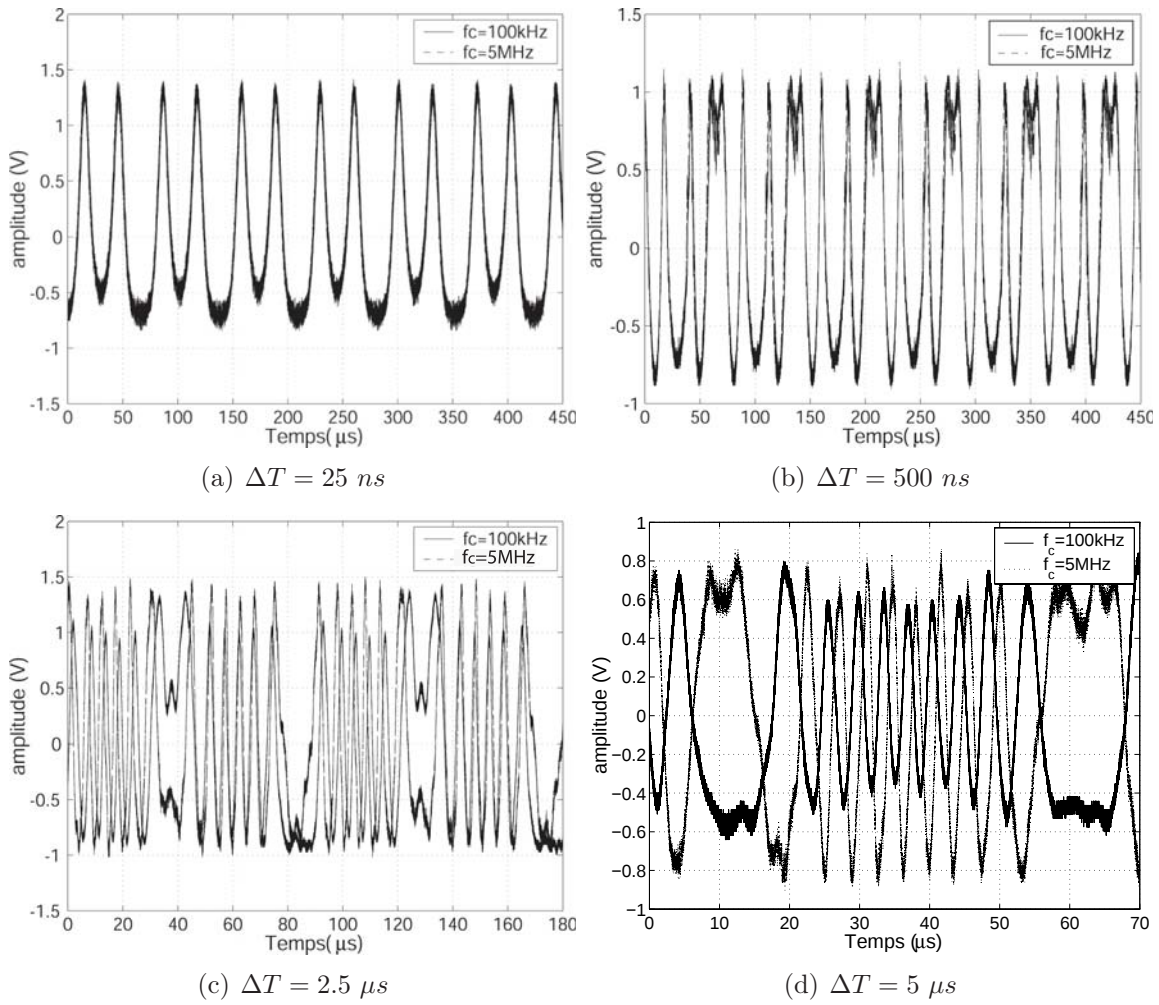


FIG. 3.18 – Dépendance de l'ordre d'interférence ΔT et de la fréquence de coupure haute f_1

sélectionnant la composante BF en sortie de la fonction d'interférence) et dont l'amplitude est ajustée suivant le nombre de cannelures que l'on souhaite balayer.

Plusieurs cas sont alors observés :

- figure 3.18(a) : pour deux constantes de temps τ_1 différentes et un ordre d'interférence similaire, nous obtenons respectivement des rapports $\Delta T/\tau_1$ de $16 \cdot 10^{-3}$ et 0.31 qui sont inférieurs à l'unité. L'ordre d'interférence reste trop petit par rapport à la constante de temps pour pouvoir donner lieu à des différences de formes des réponses non linéaires : l'interférence est dite «instantanée».
- figure 3.18(b) : un léger décalage est observable dû à des rapports $\Delta T/\tau_1$ qui augmentent : respectivement 0.31 et 6.3 ; on est dans une situation intermédiaire entre le cas instantané et le cas dynamique.
- figures 3.18(c) et 3.18(d) : les rapports $\Delta T/\tau_1$ deviennent importants (Tab.3.1). Le

comportement de la fonction d'interférence est clairement dynamique, puisque sa réponse à 2 filtres BF différents n'est pas la même.

	$\Delta T = 2.5 \mu s$	$\Delta T = 5 \mu s$
$\tau_1 = 1.6 \mu s$	1.56	3.125
$\tau_1 = 80 ns$	31.25	62.5

TAB. 3.1 – Rapports $\Delta T/\tau_1$

Dans la suite de ce travail, nous avons opté pour une configuration «classique» du générateur de chaos FM, pour laquelle la fonction d'interférence est instantanée. Ce choix a été motivé pour des contraintes de matériel disponible et de temps de mise en œuvre (ajustement émetteur/récepteur plus délicat dans le cas de grands retards). Néanmoins, il serait intéressant à l'avenir d'explorer également les possibilités de synchronisation d'un montage à base d'interférences RF dynamiques ainsi que d'étudier en détail les propriétés dynamiques des comportements chaotiques issus d'un tel montage.

3.4 Caractérisation de l'oscillateur chaotique

De la même manière que pour les simulations numériques, nous allons effectuer des mesures pour analyser les régimes dynamiques obtenus, et afin de vérifier la validité du modèle théorique (voir équation (2.43) page 90). Des relevés temporels, spectraux et statistiques, ainsi que les tracés de diagrammes de bifurcation nous ont permis de dégager des critères de conception et d'analyse de l'oscillateur, afin d'optimiser ses propriétés par rapport à une application à la cryptographie par chaos.

L'ensemble des éléments caractérisés précédemment constitue en grande partie notre oscillateur chaotique. Celui-ci est composé d'une partie optique, d'une partie optoélectronique et d'une partie électronique. La figure 3.19 montre la disposition des composants dont chaque encadré numéroté correspond respectivement :

1. aux cartes électroniques qui regroupent une partie optoélectronique avec la diode laser et les photodétecteurs utiles à la réalisation des interférences RF. La partie entre ces deux composants optoélectroniques est électronique. Elle réalise le traitement du signal chaotique en bande de base (filtrage, amplification, détection d'enveloppe).
2. à une bobine de fibre optique se situant après la diode laser (et un coupleur 10/90 permettant d'atténuer le signal optique). La longueur de cette fibre est de 2 km permettant ainsi de générer un retard T de $10 \mu s$.
3. à un coupleur 50/50 qui répartit le signal optique dans deux bras de longueur différente.



FIG. 3.19 – Photographie du montage expérimental de l'oscillateur chaotique

4. aux deux photodétecteurs fibrés ayant une longueur de fibre identique, et auxquels nous ajoutons une jarrettière optique d'une longueur de 5 m (soit $\Delta T = 25$ ns) pour réaliser le déséquilibre des bras de l'interféromètre RF.
5. aux appareils d'alimentation et de régulation qui sont nécessaires aux réglages de la fréquence centrale de modulation, et au contrôle en courant et en température du point de fonctionnement de la diode laser.

Une photographie de la carte électronique expérimentale est disponible en annexe E.5.1.

3.4.1 Evolution temporelle et spectrale

La représentation temporelle de l'évolution de la fréquence du signal sinusoïdal en sortie du VCO, montre que celle-ci est chaotique lorsque le gain de boucle est suffisamment élevé (fig.3.20(a)). Ensuite, il est nécessaire, à partir du calcul de son histogramme, d'observer si l'approximation gaussienne est respectée comme nous l'avons calculé dans le chapitre précédent (fig.3.20(b)).

Sur ce même graphique, nous avons tracé la courbe théorique Gaussienne qui se rapproche le plus de notre relevé expérimental. Le modèle gaussien correspond à un écart-type

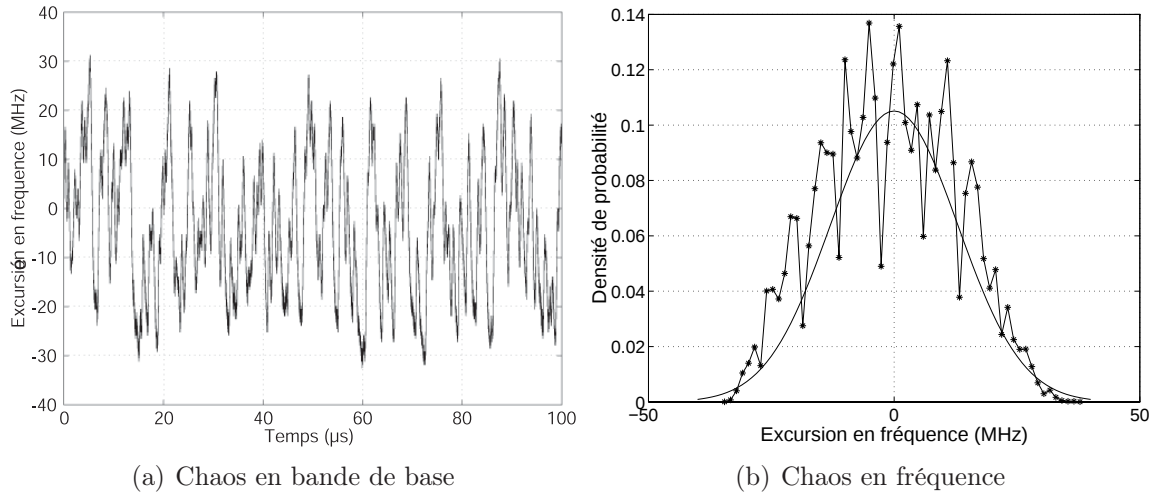


FIG. 3.20 – Evolution temporelle et comportement statistique ($\beta = 2.2$, $\Delta T = 25$ ns, $T = 10$ µs et $f_0 = 1.2$ GHz)

$\sigma = 13$ MHz.

Le spectre du chaos en bande de base (fig.3.21(a)) et celui de la porteuse chaotique (fig.3.21(b)) est relativement plat dans la bande passante, montrant ainsi une équirépartition «anonyme» des composantes spectrales du chaos. Celui-ci s'apparente ainsi à un bruit blanc filtré dans la bande de base du chaos. Ainsi, ce spectre ne délivre pas d'autre information pendant sa transmission que la bande de fréquence utile du chaos (pas de cannelure par exemple).

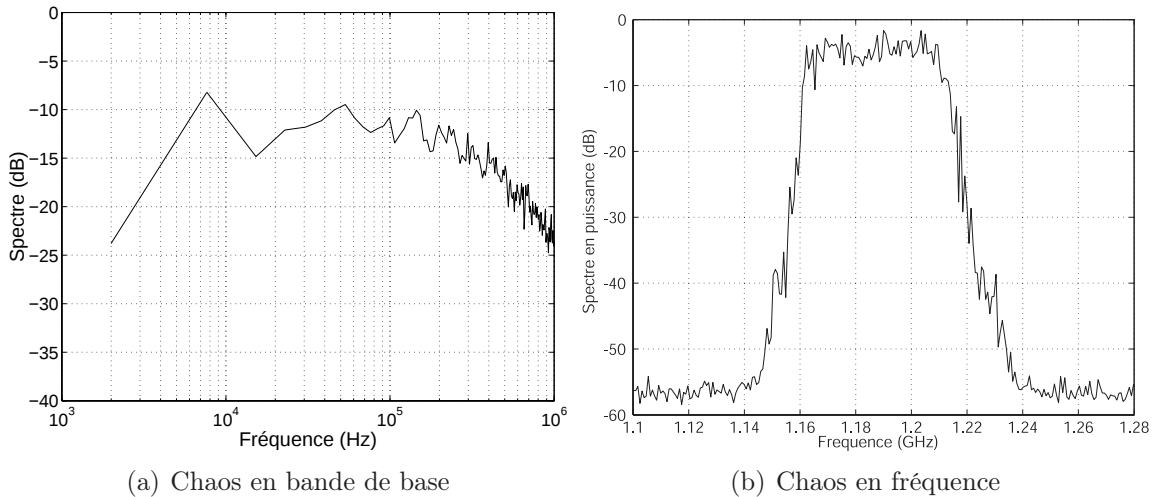


FIG. 3.21 – Spectre du chaos en bande de base et du chaos en fréquence ($f_0 = 1.2$ GHz, $\Delta T = 5$ m, $\beta = 2.2$, $\tau_1 = 10$ µs)

Le pirate peut avoir accès à l'ensemble des relevés précédents à partir du chaos en

modulation de fréquence, puisque ce dernier est disponible sur le canal hertzien public. En utilisant une PLL, il va pouvoir extraire le chaos en bande de base. Il aura ainsi une estimation de la bande passante des variations chaotiques de la fréquence. Le pirate connaît alors seulement le type de dynamique limitante utilisée dans notre système.

3.4.2 Diagramme de bifurcation

Un diagramme de bifurcation peut, comme nous avons pu le voir pour les simulations numériques, donner des informations tant au niveau statistique qu'au niveau expérimental en évaluant le gain suffisant pour atteindre un régime chaotique. Expérimentalement, nous avons tracé les diagrammes de bifurcation pour des évolutions successives du gain normalisé β puis du déphasage ϕ . Nous avons également essayé de mettre en évidence la notion d'hystérésis présente dans les diagrammes de bifurcation lorsqu'on impose une évolution croissante ou décroissante du gain pour le tracé de ces diagrammes.

Paramètre de bifurcation : le gain normalisé β

Les variations du gain de la boucle non linéaire à retard sont très significatives graphiquement, et à partir des différents régimes périodiques et chaotiques de l'oscillateur, elles mettent en évidence l'importance du gain pour obtenir un régime oscillatoire, qu'il soit périodique ou chaotique.

Comme nous pouvons le voir sur la figure 3.22, le tracé d'un diagramme de bifurcation en fonction des variations du gain β est fidèle au modèle théorique (voir 2.5.5 page 96).

Il se décompose en plusieurs parties :

1. $\beta < 1.3$: une perturbation n'entraînera pas le système dans une oscillation auto-entretenu. Le régime reste stationnaire, de type point fixe stable.
2. $1.3 < \beta < 1.5$: première évolution périodique (fig.3.24(a)). Il s'agit d'un signal carré dont les temps de montée sont liés à la constante rapide τ_1 de temps de la dynamique limitante, et les durées des plateaux correspondent au retard T .

Nous avons vu que la dynamique limitante de notre système était caractérisée par une réponse à un échelon apériodique (amortissement fort, voir page 134). Ce système peut donc être modélisé, en première approximation, par la mise en cascade de deux systèmes du premier ordre. Nous allons calculer la transformée de Laplace inverse du signal en sortie d'un filtre passe-bas dont la fréquence de coupure haute est similaire à celle de notre système expérimental ($f_1 \approx 150$ kHz). Le signal d'entrée étant un échelon :

$$v_s(t) = LP^{-1} \left[\frac{G}{p(1 + \tau_1 p)} \right] = G[1 - \exp(-t/\tau_1)] u(t) \quad (3.11)$$

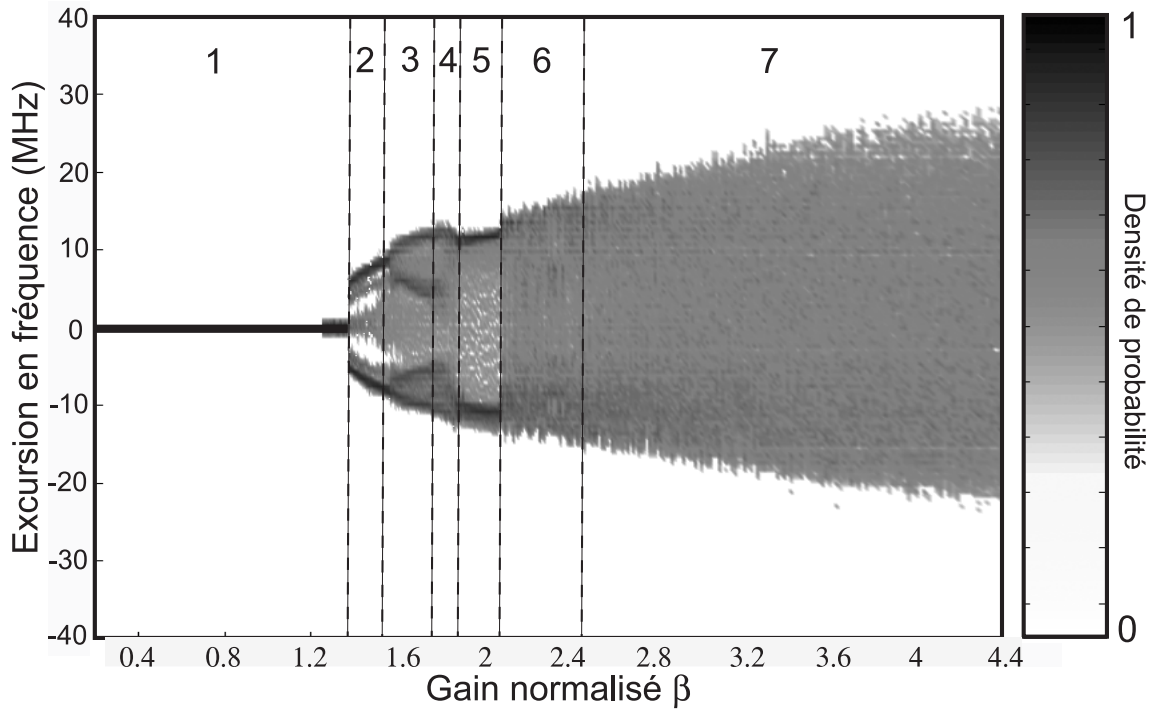
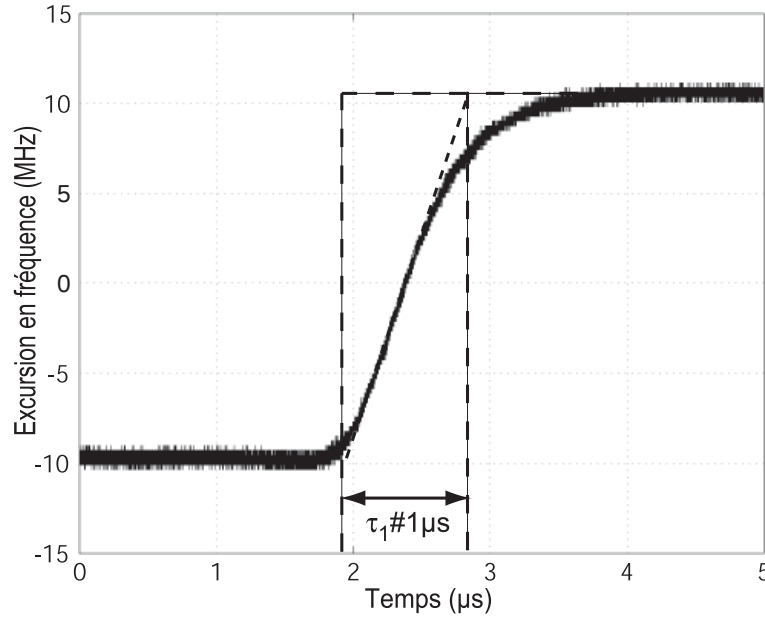
FIG. 3.22 – Diagramme de bifurcation pour $\phi = 2.1 \text{ rad}$ 

FIG. 3.23 – zoom sur le temps de montée de l'évolution périodique

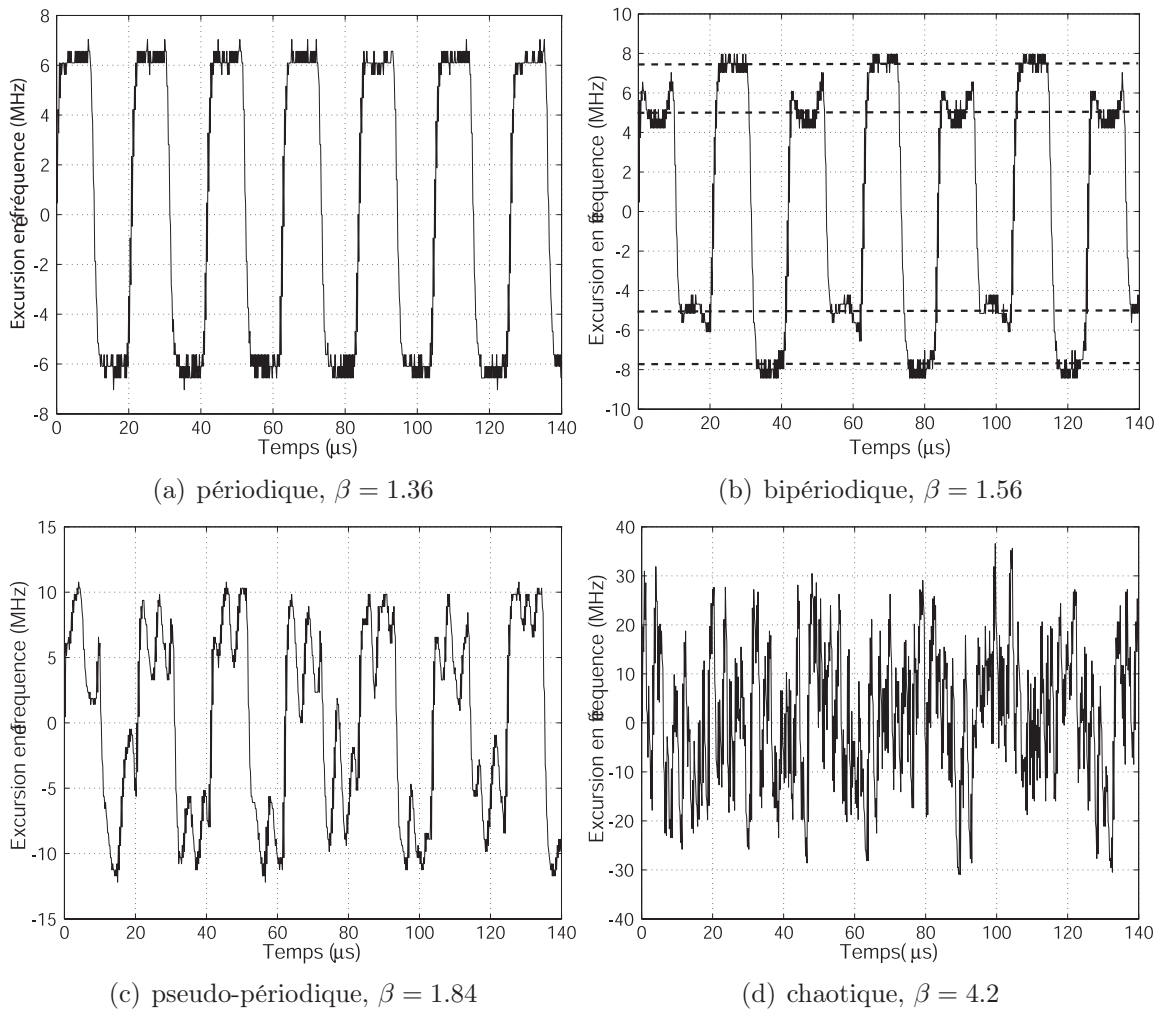
En adoptant cette approche pour l'analyse du temps de montée de l'oscillation périodique rectangulaire observée, la pente à l'origine est égale à K/τ_1 . La constante de temps alors liée au temps de montée (fig.3.23) est de $\tau_1 \approx 1.1 \mu s$; cette valeur confirme, en boucle fermée, la fréquence de coupure haute de notre dynamique.

3. $1.5 < \beta < 1.7$: le régime reste périodique mais le spectre s'élargit un peu plus avec un dédoublement de fréquence (fig.3.24(b)). Cette bifurcation à $\beta = 1.5$ ressemble à la transition période 2 vers période 4 observée dans de nombreux systèmes à retard de dynamique passe-bas, transition que l'on retrouve donc qualitativement ici dans le cas d'une dynamique passe-bande.
4. $1.7 < \beta < 1.9$: les dédoublements supplémentaires deviennent difficiles à observer. Nous pouvons simplement remarquer que la densité de probabilité est plus importante sur les cotés du diagramme. Ainsi, le régime périodique précédent se transforme en un régime pseudopériodique où les différents états sont difficilement observables (fig.3.24(c)).
5. $1.9 < \beta < 2.1$: avec l'augmentation du gain β , on pourrait s'attendre à observer une transition d'un régime pseudopériodique à un régime chaotique (comme c'est le cas pour d'autres dynamiques à retard, en particulier celles du type passe-bas). Cependant, nous pouvons remarquer que le système repasse par un régime périodique du même type que lorsque $1.3 < \beta < 1.5$ (fig.3.24(a)).
6. $2.1 < \beta < 2.5$: La structure périodique disparaît ou est fortement atténuée; on s'approche sans doute des comportements chaotiques, mais la densité de probabilité ne suit pas une loi Gaussienne. Les extrémités du diagramme de bifurcation sont plus sombres. Nous revenons à un cas pseudopériodique comme dans le cas (4).
7. $\beta > 2.5$: La loi devient quasi-gaussienne. Le régime est chaotique. En augmentant le gain, on augmente l'excursion en fréquence. Ainsi, un nombre plus important d'extrema de la non linéarité sera couvert par les variations de la fréquence porteuse. La dimension de l'attracteur étrange dans lequel évolue le chaos en fréquence augmente [56].

Ces différents régimes sont observables avec les évolutions temporelles associées au diagramme de bifurcation (fig.3.22) pour différents gains :

Le paramètre ϕ agit de manière significative sur la route vers le chaos. Les dédoublements de fréquence vont être plus ou moins observables suivant la valeur de ϕ qui est, pratiquement, proportionnelle à la fréquence centrale de modulation. Selon ϕ , le premier comportement oscillatoire ne débutera pas pour le même gain (fig.3.25(d)). Il existe également des transitions directes entre un régime stationnaire et chaotique, sans passer par des comportements périodiques (fig.3.25(b)).

L'influence de la phase sur le comportement chaotique est visible sur les diagrammes de bifurcation précédents, mais celle-ci est encore plus significative sur un diagramme de bifurcation dont le paramètre de bifurcation est la phase, comme nous allons le décrire maintenant.

FIG. 3.24 – Evolutions temporelles pour différents gains β

Paramètre de bifurcation : la phase ϕ

Ce diagramme de bifurcation n'a pas pour but de nous montrer les différents régimes que peut adopter notre oscillateur. Il met simplement en évidence, pour un faible gain comme c'est le cas dans notre système, l'importance du déphasage pour sa mise en oscillation.

Le diagramme de bifurcation (fig.3.26) montre les coupures des régimes chaotiques pour une évolution croissante de la fréquence centrale. Le paramètre $\phi = \omega_0 T$ est effectivement proportionnel à la fréquence centrale de modulation. L'alternance entre les régimes stationnaires, périodiques et chaotiques, est aussi provoquée par une variation résiduelle du gain du système, bien que celui-ci soit supposé fixé à environ 2.2; mais, pratiquement, les variations d'amplitude du signal en sortie du VCO avec f_0 (fig.3.1(b)) entraînent une légère variation du gain équivalent global β dans la boucle d'oscillation (pour un VCO parfait, l'amplitude de sortie est indépendante de f_0).

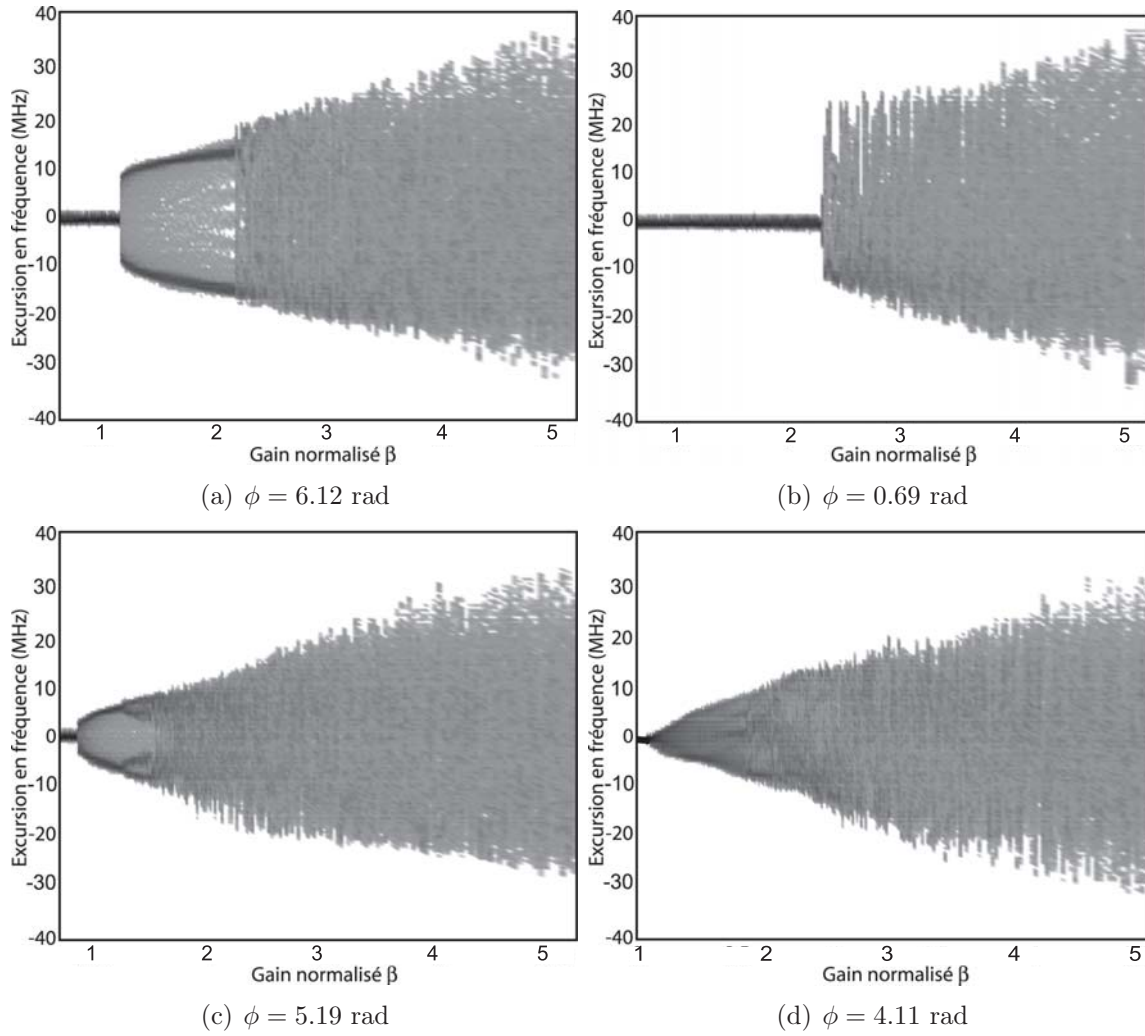


FIG. 3.25 – Influence de la phase ϕ ($\Delta T = 25$ ns et $T = 10$ μ s)

Les variations de la fréquence centrale (1040/1120 MHz) sur le diagramme de bifurcation correspondent à une variation de $\omega_0 T$ de 4π (théoriquement, les comportements dynamiques se retrouve pour une variation de 2π). Nous pouvons donc remarquer que, pour une variation de phase de 0 à 2π et de 2π à 4π , la densité de probabilité et les régimes adoptés par le système sont différents, très probablement à cause de cette variation d'amplitude de sortie du VCO avec la fréquence centrale f_0 . Ce problème est d'autant plus important que les fréquences centrales de modulation sont importantes, car elles correspondent des amplitudes de sortie du VCO de plus en plus faibles.

Hystérésis

Selon que le gain varie dans un sens croissant ou décroissant, il est possible de voir apparaître un phénomène d'hystérésis dans les deux diagrammes de bifurcation (fig.3.27).

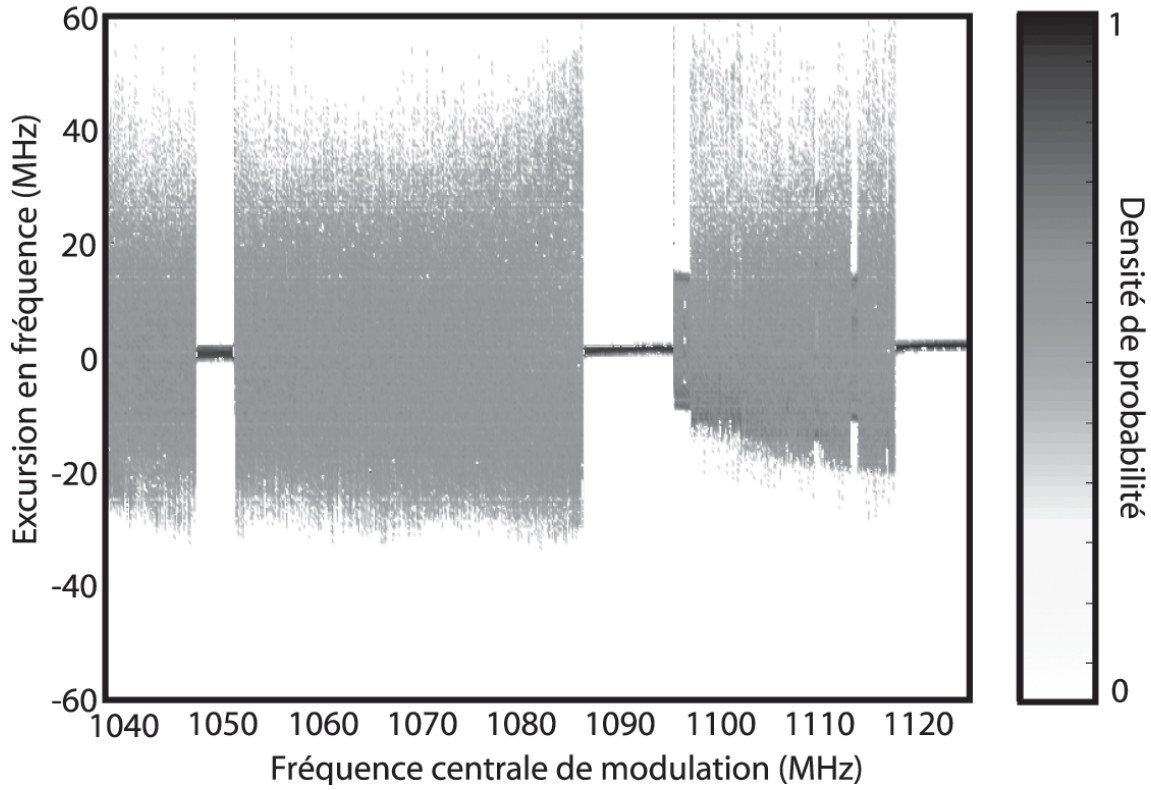


FIG. 3.26 – Diagramme de bifurcation pour $\beta = 4.4$, $T = 10 \mu s$ et $\Delta T = 25 ns$

Ce phénomène a été mis en évidence significativement dans les simulations numériques (voir 2.5.5 page 98).

Cependant, ces hystérésis ne s'observent que pour certaines plages de valeurs du paramètre ϕ , très probablement parce que la coexistence d'attracteurs à l'origine de l'hystérèse, n'existe effectivement que pour certaines valeurs de ϕ .

L'hystérèse dans les diagrammes de bifurcation ne suscite pas un grand intérêt dans l'analyse de notre système en vue d'une application à la cryptographie. Cependant, le phénomène physique mis en évidence expérimentalement et analytiquement dans nos simulations est un sujet de préoccupation au niveau plus fondamental de l'étude mathématique des dynamiques à retard passe-bande.

Nous avons vu dans la partie 1.3.4 page 19 et la partie précédente, que la phase ϕ a une influence importante sur la mise en oscillation du système. L'observation de l'hystérèse sur certains relevés expérimentaux montre que la route vers le chaos peut être très différente suivant la valeur de la phase ϕ . En effet, la figure 3.27(a) montre une grande différence entre une croissance ou une décroissance du paramètre de bifurcation β . Pour un gain croissant, le système ne passe pas d'un état stationnaire vers un état chaotique par l'intermédiaire de dédoublements de fréquence. Il s'agit d'un passage brutal du point

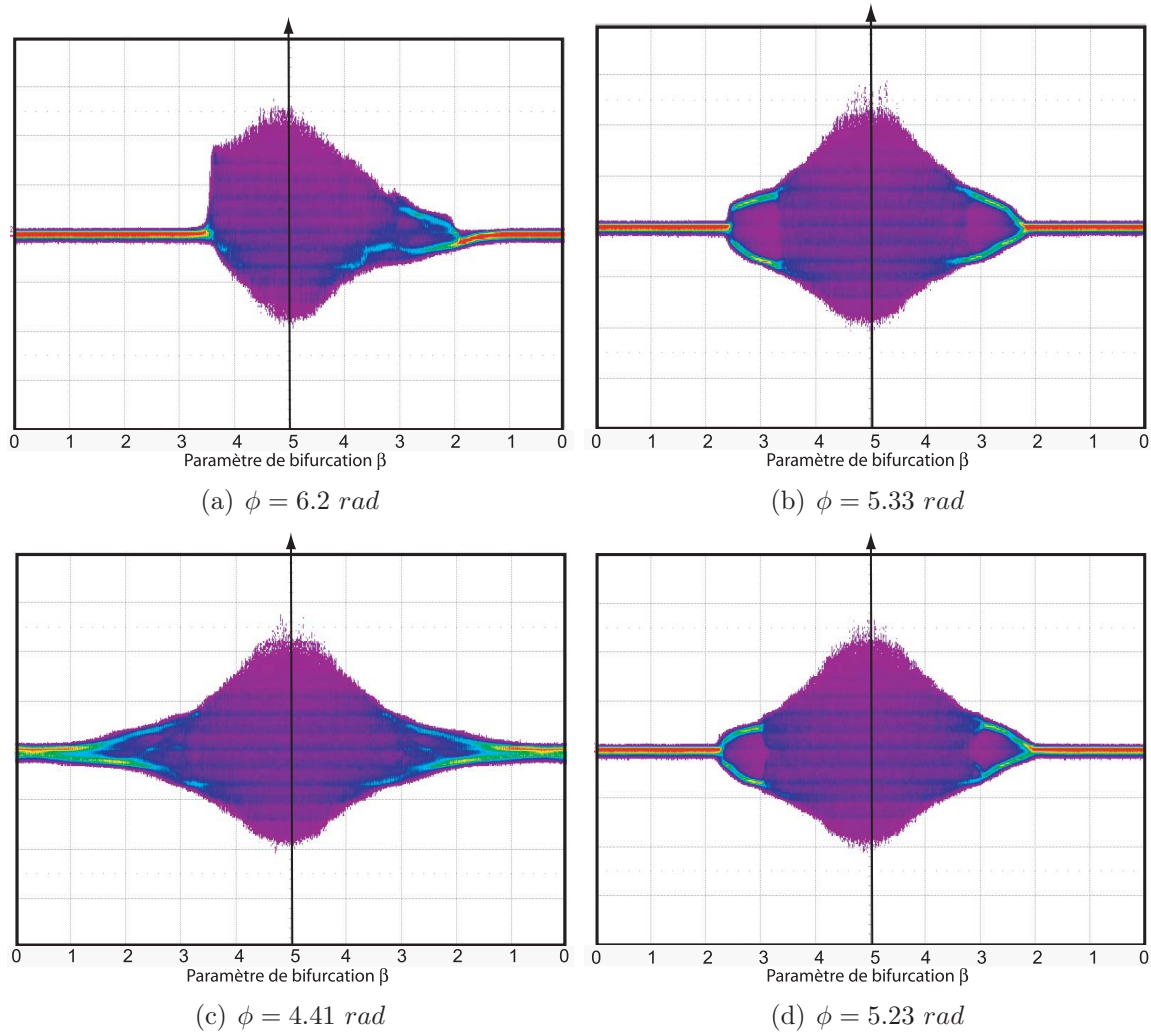


FIG. 3.27 – Hystérésis pour différentes valeurs de ϕ ($T = 10 \mu s$ et $\Delta T = 25 ns$)

fixe à un régime chaotique. Cependant, dans le cas d'un paramètre de bifurcation qui décroît, le régime chaotique, avant de revenir à son état initial, va traverser des régimes périodiques. Dans le cas de la figure 3.27(d), la route vers le chaos passe bien par des états périodiques qui, par plusieurs dédoublements de fréquences, atteindra un régime chaotique de grande dimension. Pour une variation décroissante de β , les dédoublements de fréquences s'observent plus facilement. Les différences de densité de probabilité montrent bien l'évolution temporelle «bipériodique» de quatre états (comme observé fig.3.24(b)).

Etant donné que ce problème est secondaire dans la conception du système, nous n'avons pas étudié plus en détails cette différence entre les simulations numériques et la pratique, mais nous espérons que ces constatations sur les comportements expérimentaux et numériques des diagrammes de bifurcation, pourront éveiller l'intérêt et la curiosité de certains lecteurs.

3.5 La réplication du chaos en fréquence

Après l'étude de l'oscillateur chaotique, nous allons aborder le récepteur et notamment sa capacité à réaliser une bonne synchronisation, sans laquelle il est impossible de décrypter un signal d'information noyé dans le chaos. Le récepteur est composé à partir des mêmes éléments que l'émetteur, mais ils sont assemblés de manière différente. Des éléments supplémentaires apparaissent en vue d'affiner l'ajustement de certaines clés de codage, ce qui permet de limiter au mieux le bruit de décryptage.

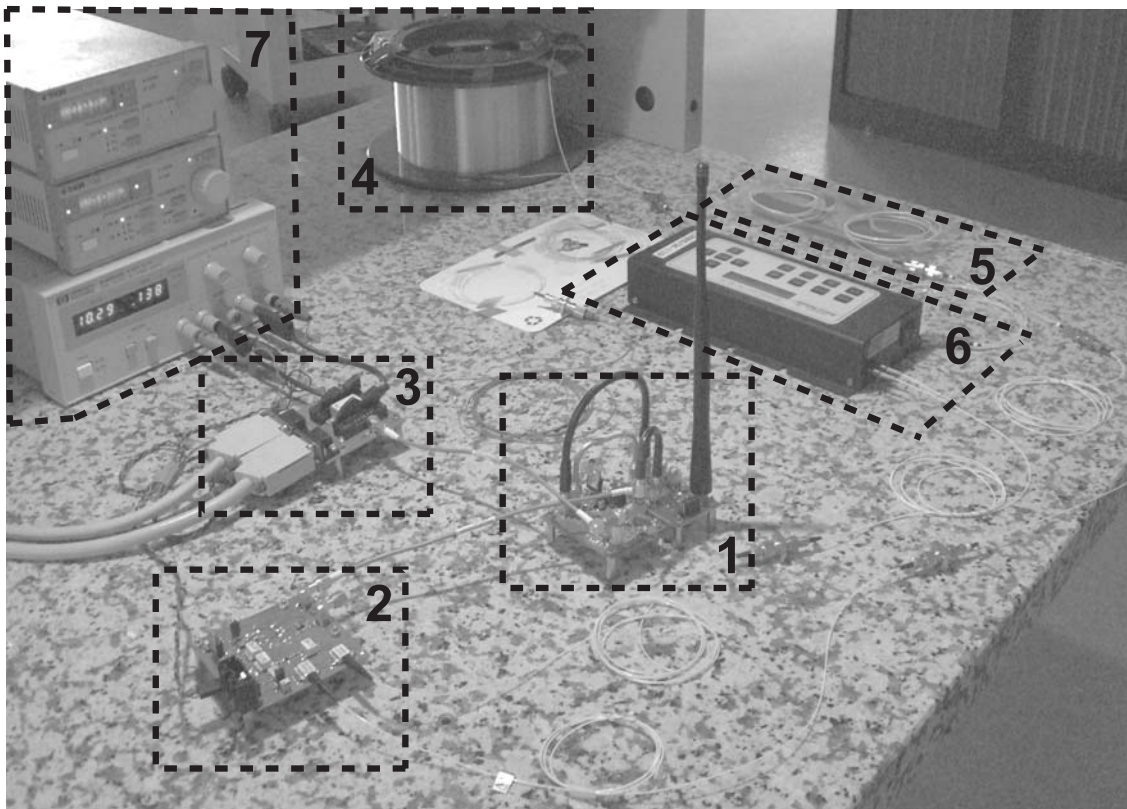


FIG. 3.28 – Montage expérimental du récepteur/décodeur

La figure 3.28 montre la conception expérimentale du système. Les composants du récepteur (numérotés de 1 à 7) sont respectivement :

1. La boucle à verrouillage de phase (PLL). Elle permet de restituer le chaos en fréquence (signal de modulation de la diode laser) et le chaos en amplitude (envoyé sur le circuit électronique du traitement du signal en bande de base) en s'affranchissant au mieux du bruit en amplitude rajouté par le canal.
2. Un circuit électronique dont une partie est la même que l'émetteur (partie opto-électronique et électronique de l'interféromètre RF, filtrage, amplificateur) et d'une autre partie permettant la soustraction du chaos en amplitude issu de la PLL et

du chaos récupéré en sortie de la boucle constituée par les mêmes composants que l'émetteur.

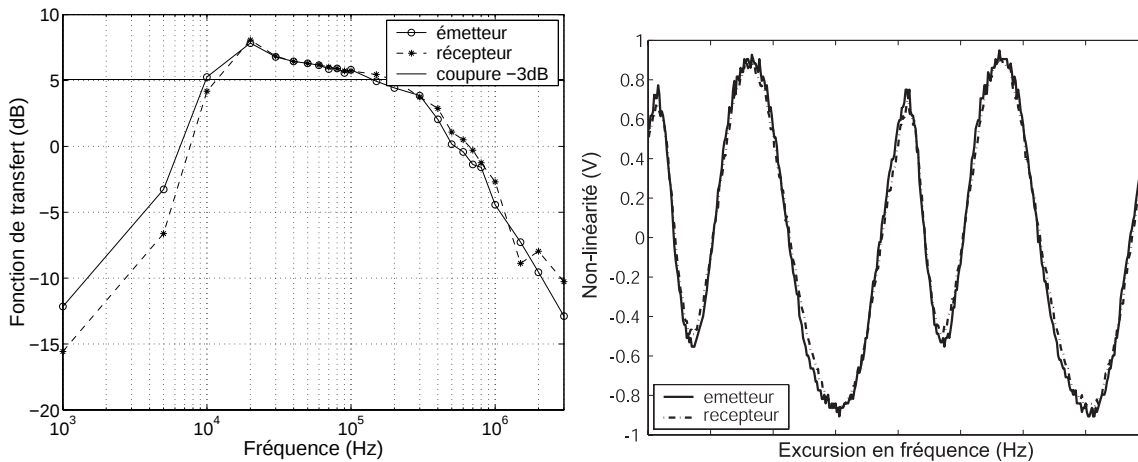
3. Une diode laser CATV.
4. Un retard optique.
5. Un coupleur 50/50 permettant d'orienter le signal dans les bras fibrés de l'interféromètre.
6. Une ligne à retard réglable dans le but d'obtenir avec une très bonne précision la même différence de longueur des bras de l'interféromètre. Le réglage de son retard varie entre 0 et 600 ps et sa précision est de 1 fs.
7. Des appareils d'alimentation et de régulation similaires à l'émetteur.

Une photographie de la carte électronique expérimentale est disponible en annexe E.5.2.

A noter que l'ensemble des éléments détaillés sur le récepteur sont, pour la plupart, les mêmes qu'à l'émetteur, mais placés, dans le cas du récepteur, en boucle ouverte (voir 2.45 page 103).

3.5.1 Accordabilité des fonctions de l'émetteur et du récepteur

Pour pouvoir synchroniser les signaux chaotiques obtenus en bande de base, il est nécessaire d'obtenir les mêmes fonctions constituant l'émetteur et le récepteur.



(a) Diagramme de Bode en amplitude des filtres passe-bande

(b) Fonctions non linéaires

FIG. 3.29 – Appariement de la dynamique en bande de base et des fonctions non linéaires

Les composants que nous avons décrits précédemment, doivent réaliser les fonctions de la transformation non linéaire, du processus dynamique limitant, du retard pur, et

d'amplification. Ces fonctions de base de l'architecture de générateur de chaos doivent être réalisées de la manière la plus identique possible entre l'émetteur et le récepteur afin de garantir la meilleure synchronisation possible. Grâce à la synchronisation, il sera possible de répliquer le signal chaotique en bande de base de la dynamique locale. Ce chaos répliqué est à comparer à celui restitué par la PLL de réception. Nous verrons par la suite que cette synchronisation est essentielle au fonctionnement du système de cryptographie, lorsqu'un message est inséré à l'émetteur.

Les figures 3.29(a) et 3.29(b) montrent respectivement la bande passante et la fonction non linéaire de l'émetteur et du récepteur. Elles ne sont pas idéalement superposées comme c'est le cas dans les simulations numériques pour une synchronisation parfaite. En effet, le bruit de décodage est essentiellement dû aux légères différences enregistrées entre les éléments de l'émetteur et du récepteur.

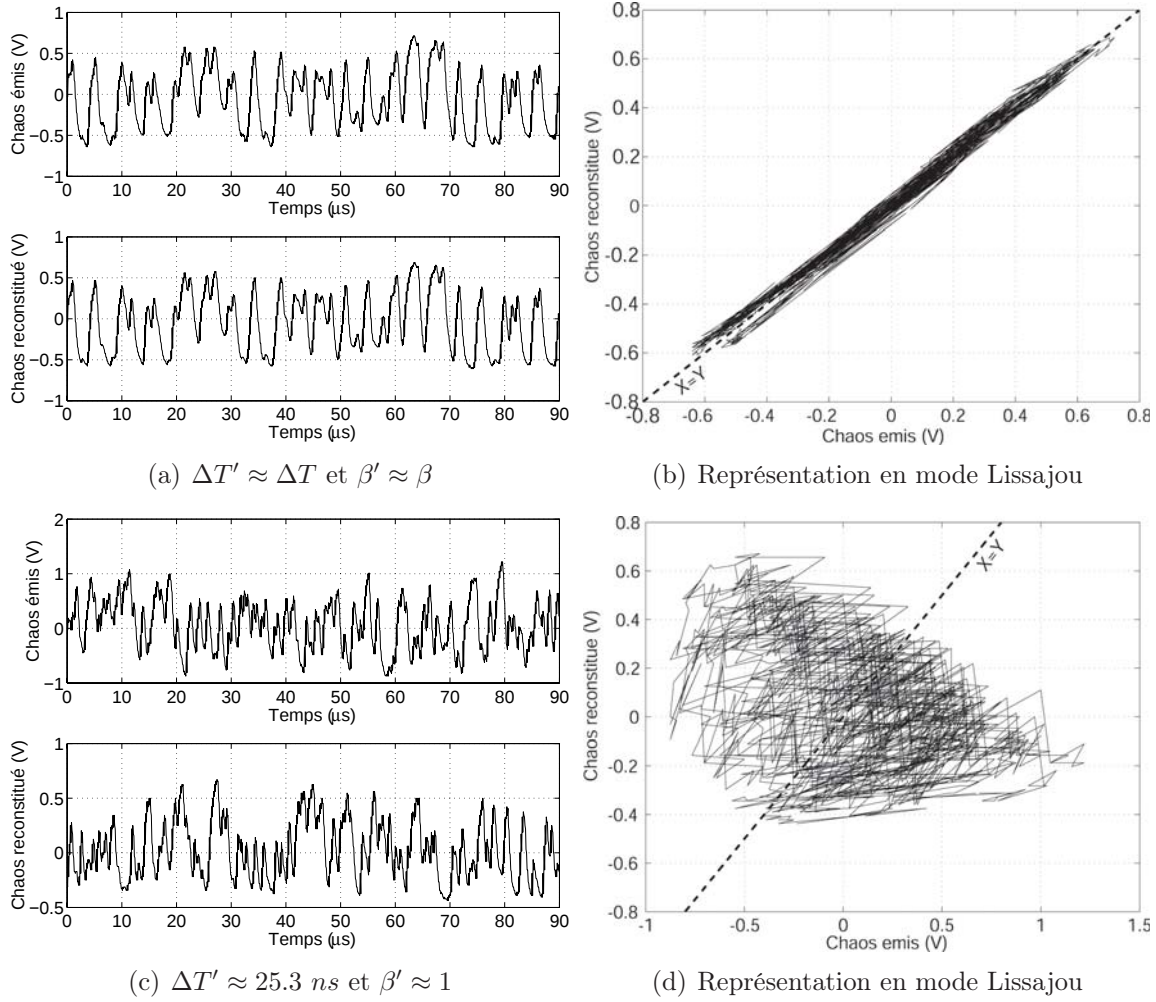
3.5.2 Synchronisation entre deux signaux chaotiques : les fonctions nécessaires à l'oscillation chaotique, et leurs paramètres caractéristiques

Sans la connaissance des clés de codage, il est supposé impossible, voire très difficile, de décrypter le signal. Pour étayer cette affirmation, nous allons représenter expérimentalement l'influence de certaines clés sur la synchronisation [25].

Dans un premier temps, pour vérifier le fonctionnement du système, il est possible de représenter la synchronisation entre le chaos généré par l'oscillateur et le chaos reconstruit du côté du récepteur avec le mode lissajou (ou mode XY) d'un oscilloscope enregistrant sur deux voies chacun des deux signaux chaotiques de l'émetteur et du récepteur.

Pour une bonne synchronisation (fig.3.30(a)), nous pouvons voir que les deux signaux en bande de base ont une évolution temporelle qualitativement comparable, cependant, il est difficile de visualiser efficacement les petites différences avec ce type d'observation. La synchronisation de ces deux signaux est plus facile à observer par une représentation en mode Lissajou (fig.3.30(b)). Cette représentation consiste dans le tracé de la courbe du chaos reçu, en fonction du chaos reconstruit. Une synchronisation parfaite est représentée par la bissectrice ($X=Y$) avec une épaisseur infiniment fine.

Dans notre système, la meilleure synchronisation possible suit la direction de la bissectrice, mais correspond à une trace plus épaisse qu'une droite. Cette épaisseur est due au bruit intrinsèque au système et aux défauts d'appariement entre les différentes fonctions. Dans le cas où les signaux issus de l'émetteur et du récepteur ne sont plus synchronisés (fig.3.30(c)), la représentation en mode XY prend la forme d'une trace remplissant uniformément un espace carré, indiquant que les deux signaux chaotiques n'ont plus rien en commun (fig.3.30(d)).

FIG. 3.30 – Représentation en mode lissajou ($\Delta T = 25 \text{ ns}$ et $\beta = 1.7$)

3.5.3 Influence de l'ordre d'interférence ΔT

L'ordre d'interférence de la non linéarité est un paramètre très sensible de notre système de cryptage. Celui-ci va, en effet, agir sur l'ISL de l'interférence mais aussi sur le paramètre «déphasage».

L'erreur de synchronisation, représentée sur la figure 3.31 est définie par le calcul de la valeur RMS de la différence entre la porteuse chaotique émise et le chaos reconstituée au récepteur. Ce calcul est défini par l'équation (2.56) page 106.

Les mesures effectuées, contrairement aux simulations numériques, prennent en compte le bruit intrinsèque aux systèmes d'émission et de réception, ainsi qu'un défaut d'appariement résiduel pour l'ensemble des paramètres du système. Cette différence de contexte entre expérience et simulation explique un écart-type de l'erreur non nul pour les mêmes valeurs de ΔT . Une explication tout à fait similaire peut être fournie pour les autres mesures (β en particulier) représentées à la figure 3.32 pour commenter l'erreur non nulle

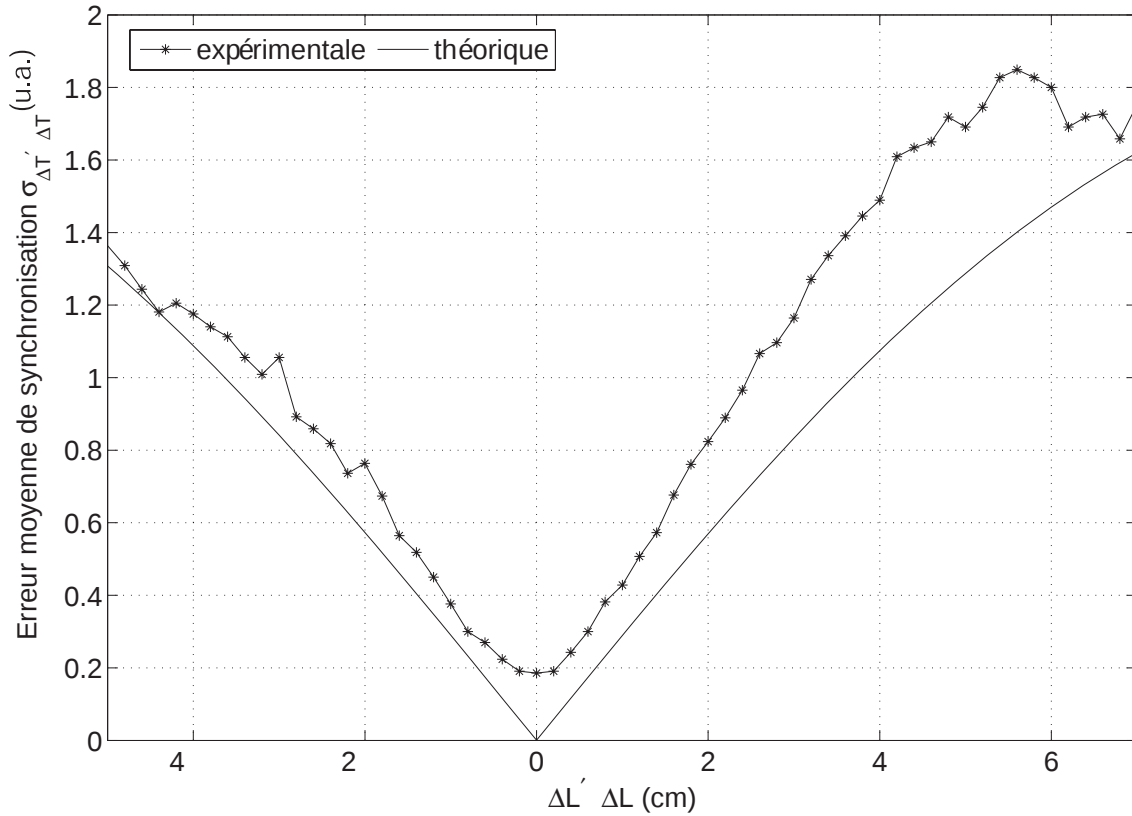


FIG. 3.31 – Influence de l'erreur sur la synchronisation pour $\beta = 3.8$, $T = 10 \mu s$

observée au minimum.

Le retard T est un paramètre également très sensible mais comme nous l'avons vu, l'influence de ce paramètre sur la synchronisation est également dépendant de la bande passante de l'oscillateur. Pratiquement, les lignes à retard réglables peuvent introduire une valeur de retard supplémentaire jusqu'à 600 ps équivalente à une longueur de fibre de 12 cm. Elle représente dans le cas de la différence de longueur ΔL une erreur relative maximale de 2.4%. En revanche, cette longueur est trop petite pour pouvoir introduire une différence de retard significative pour l'observation de l'erreur de synchronisation introduite par un appariement approximatif du retard temporel. Le rapport $T/\tau_1 = 6.25$ est ici beaucoup trop faible pour faire intervenir les problèmes évoqués dans la partie 3.3.3 page 140 . Une variation de longueur de retard de 12 cm entraînerait une erreur relative d'au plus de 6 ‰ dans le cas du retard temporel réalisé avec une fibre de 2 km.

3.5.4 Influence du gain normalisé β

Le gain normalisé β est un paramètre de codage et il peut, dans le cas d'un mauvais réglage, entraîner des perturbations supplémentaires sur la synchronisation.

Comme pour montrer l'influence de l'ordre d'interférence, nous avons tracé la courbe

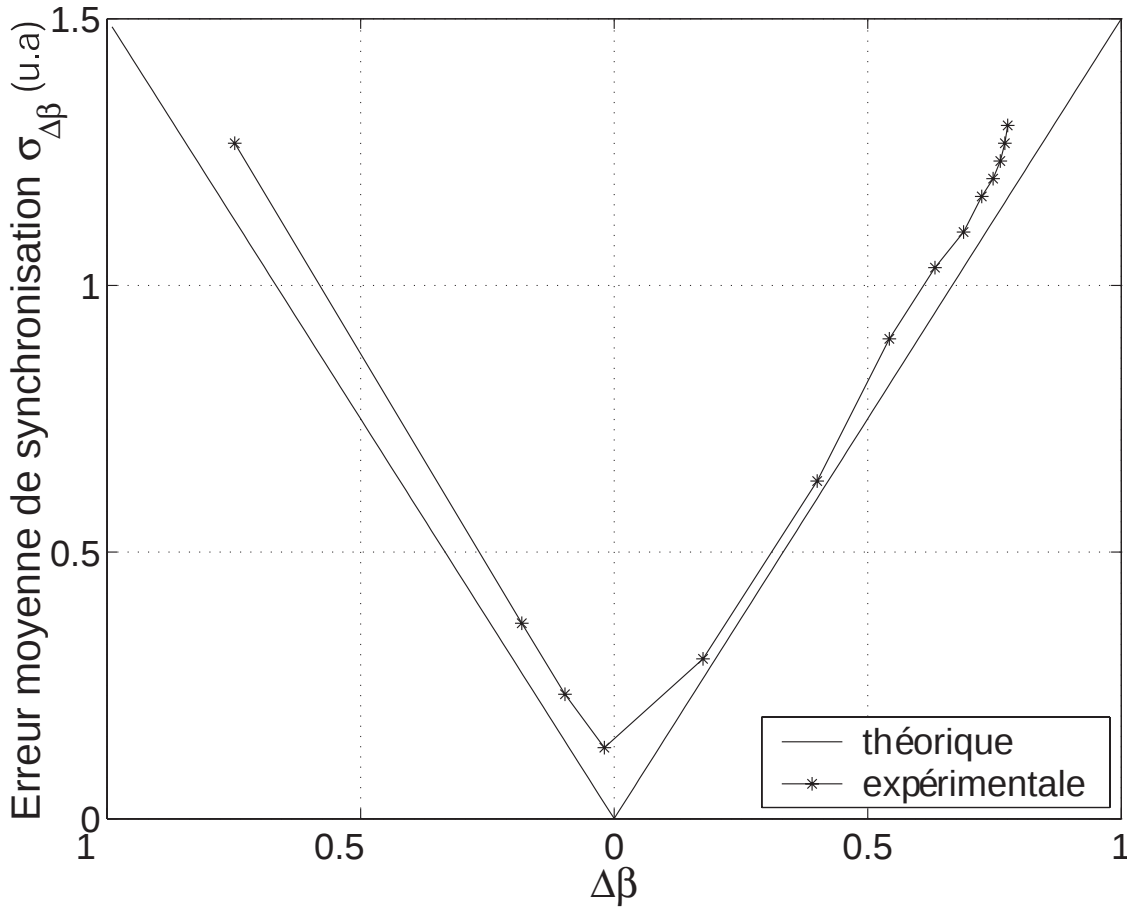


FIG. 3.32 – Influence de l'erreur sur la synchronisation pour $\Delta T = 25 \text{ ns}$, $T = 10 \mu s$

expérimentale et la courbe théorique pour une comparaison plus simple (fig.3.32). Les différences d'écart-type pour une erreur nulle sont également produites par le bruit de décodage de l'ensemble des autres éléments. Comme nous pouvons le remarquer, les points de mesures n'ont pas une répartition homogène sur l'intervalle de variation de l'amplification. En effet, l'amplificateur à gain variable avec lequel nous pouvons faire varier β , est linéaire en dB . Nous avons donc une commande de la forme suivante :

$$G_{dB} = S(dB/V) V_{commande} + G_0$$

Nous pouvons remarquer que l'influence du gain sur l'erreur en fréquence introduite dans la synchronisation, est symétrique par rapport à une erreur nulle. Les variations de l'écart-type sont linéaires comme nous avons pu le voir dans les simulations numériques avec l'équation (2.62) (voir page page 107).

3.6 Système de cryptographie

Dans le cas analogique, le principe de cryptage consiste à générer une porteuse chaotique dont l'étalement spectral couvre la totalité de celui de l'information analogique. Dans le cas du numérique, la largeur spectrale du chaos est liée au débit binaire, dont le spectre doit également pouvoir être masqué par la porteuse chaotique. En termes de qualité de la liaison cryptée, une transmission analogique mettra en avant le rapport signal sur bruit du décodage par synchronisation entre chaos. Une transmission numérique se réfère quant à elle à la valeur du BER⁶ après synchronisation et suppression de la porteuse chaotique par le récepteur. Pour avoir une image concrète sur la qualité du décodage d'une information numérique, nous tracerons un diagramme de l'oeil.

3.6.1 Codage d'un message analogique

Dans les systèmes de télécommunication actuels, la majorité des informations transmises est de type numérique. Cependant, certaines informations sont encore de types analogiques comme la télévision, la radio, mais aussi certaines applications des télécommunications BF.

Dans le cas d'un système analogique, il est nécessaire que le rapport signal/bruit (SNR) soit important. Actuellement, les mesures montrent qu'une image (pour un signal vidéo) est considérée de bonne qualité, lors de sa réception, quand son SNR⁷ est supérieur à 40 dB [57].

Le tableau 3.2 permet d'avoir une idée sur la qualité de l'image en fonction de son SNR.

SNR (dB)	qualité de l'image
60 dB	excellente, pas de bruit apparent
50 dB	petite quantité de bruit mais image de bonne qualité
40 dB	raisonnable mais pertes de quelques détails avec apparition de "neige"
30 dB	image pauvre avec une grande quantité de bruit
20 dB	image inutilisable

TAB. 3.2 – Qualité d'une image en fonction de son SNR

Dans le cas de notre liaison codée par chaos, la mesure du SNR nous donne :

$$SNR \approx 36 \text{ dB}$$

⁶Bit Error Rate

⁷Signal to Noise Ratio

Le SNR est relativement bon étant donnée la difficulté d'accordabilité des clés de codage du récepteur avec celles de l'émetteur et en prenant en compte le bruit intrinsèque du système.

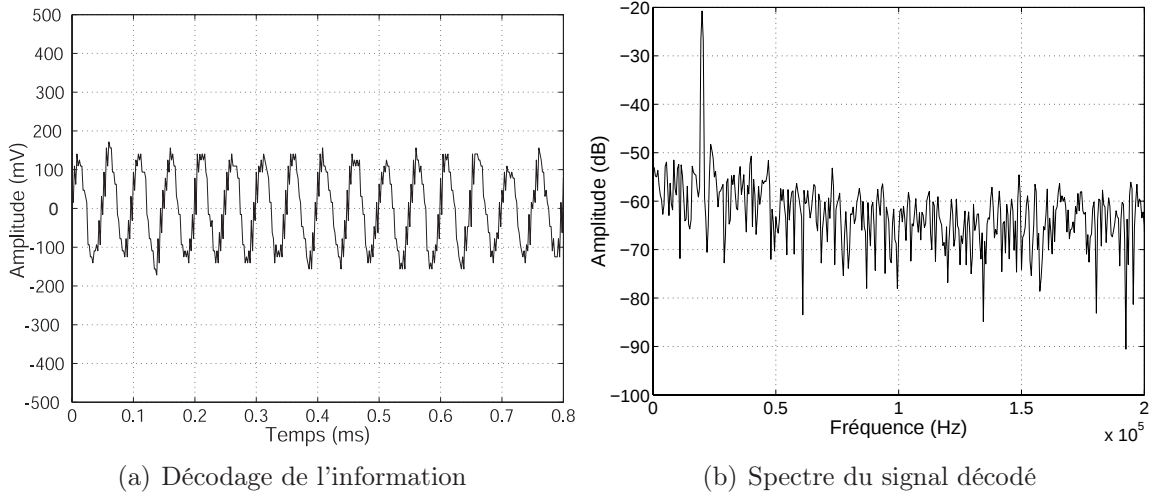


FIG. 3.33 – Signal d'information après son décryptage ($\phi = 1.82 \text{ rad}$, $\Delta T = 25 \text{ ns}$, $T = 10 \text{ } \mu\text{s}$ et $\beta = 2$)

3.6.2 Codage d'un message numérique

Dans le cas d'un signal d'information numérique, nous allons tracer un diagramme de l'œil (fig.3.35) permettant d'apprécier la qualité de décryptage des 0 et des 1 transmis.

Pour effectuer ce type de mesure, nous avons besoin d'un générateur de séquences binaires pseudo-aléatoires. Ce type de générateur est, dans son principe, un système très simple constitué de registre à décalage à n bascules D à entrée série, et d'une porte logique OU-exclusif placées en contre-réaction.

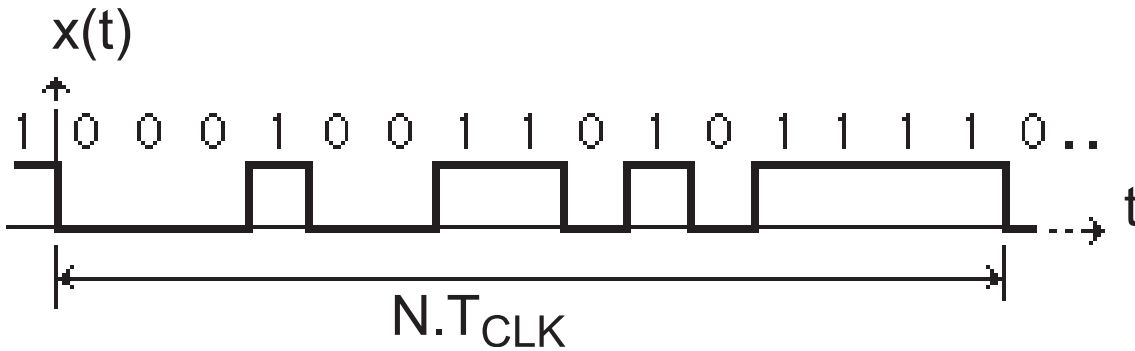


FIG. 3.34 – Exemple d'une séquence binaire pseudo-aléatoire

La séquence de longueur maximale dure $N T_{CLK}$, avec $N = 2^n - 1$. Si N est très grand, la succession de bits est d'apparence quelconque, mais si l'on attend une durée égale à $N T_{CLK}$, on recommence un cycle. Cela justifie le nom de pseudo-aléatoire (fig.3.34).

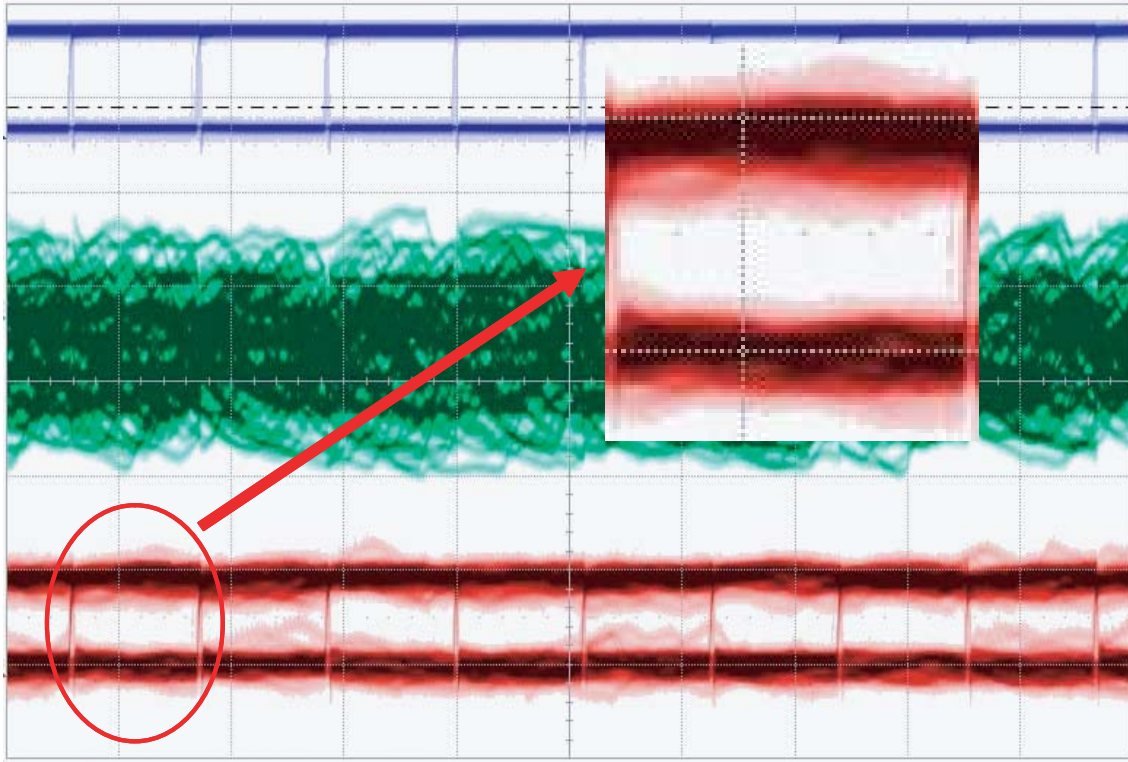


FIG. 3.35 – Diagramme de l'œil ($\phi = 1.82 \text{ rad}$, $\Delta T = 25 \text{ ns}$, $T = 10 \mu\text{s}$ et $\beta = 2$)

La figure 3.35 représente de haut en bas la trace du signal d'information binaire original [17], celle du signal crypté et enfin, celle du signal décrypté en sortie du système de réception.

Pendant sa transmission, le signal binaire est totalement masqué par le signal chaotique. Le diagramme de l'œil du signal binaire est totalement fermé. Les transitions d'un état haut vers un état bas ou l'inverse ne peuvent, en effet, pas être appréhendées, et le code binaire transmis est totalement invisible pour un espion qui observe le canal par une détection FM directe.

Le décodage, lors d'une synchronisation idéale, devrait permettre une restitution du même signal binaire d'origine. Le diagramme de l'œil est, en fait, un peu plus fermé à cause du bruit de décryptage. De la même manière que pour un signal analogique, des opérations supplémentaires de traitement du signal nous donnerait un signal d'information largement utilisable par les systèmes de communications actuels (par exemple par utilisation de codes correcteur d'erreur dans cette situation numérique).

3.7 Conclusion

Au cours de ce chapitre, nous avons pu mettre en œuvre le générateur de chaos RF et son récepteur pour l'appliquer à la transmission cryptée de signaux analogiques et numériques. Les résultats expérimentaux obtenus pour les différentes dynamiques de l'oscillateur sont compatibles avec nos attentes : les diagrammes de bifurcation ont les mêmes types d'évolution pour des gains et des paramètres ϕ identiques. Le spectre du chaos en fréquence qui est une donnée disponible pour l'espion (car elle est le spectre du signal transmis) est uniforme dans sa bande passante et, est conforme à un bruit rose (bruit blanc filtré). La bande passante du signal d'information disponible dans le spectre en bande de base est également compatible à nos attentes.

Nous avons pu, également, mettre en évidence la particularité de l'architecture RF par rapport à des interféromètres optiques. Bien que le principe de base sur la conception de l'interféromètre soit le même, la différence des fréquences a montré que l'analyse était très différente.

L'oscillateur chaotique et son récepteur constituent la première démonstration d'une liaison hertzienne à porteuse FM chaotique dans la bande GSM. Les informations transmises peuvent être numériques ou analogiques, s'adaptant ainsi à l'ensemble des systèmes actuelles de transmission d'informations.

3.8 Perspectives expérimentales

Nous avons pu mettre en évidence le fonctionnement du système de cryptage comme nous l'avions observé au cours des simulations numériques.

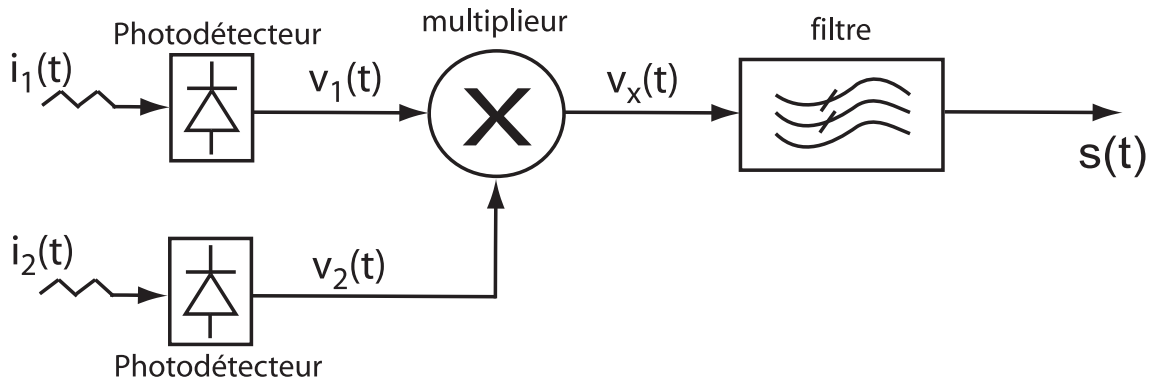


FIG. 3.36 – Optimisation de la non linéarité

La conception expérimentale réserve toutefois des problèmes supplémentaires comme des problèmes d'adaptation d'impédance, des problèmes de bruit intrinsèque au système

qui perturbe le fonctionnement global. La réduction du nombre de composants est une perspective d'amélioration importante.

A posteriori, la non linéarité aurait pu être, par exemple, conçue différemment. Ainsi, une nouvelle architecture permettrait d'éviter un déséquilibre en puissance entre les bras fibrés mais aussi de réduire les dimensions de la carte électronique. En effet, la non linéarité est composée d'un sommateur puis d'un détecteur quadratique permettant d'extraire l'enveloppe des interférences RF. Ce type de circuit peut se réduire à la simple multiplication des signaux à la sortie des photodétecteurs suivie d'un filtre permettant d'éliminer la composante HF (fig.3.36).

Notes du lecteur

Conclusion générale et perspectives

Ce travail de thèse a été consacré au développement de systèmes électroniques et opto-électroniques de transmissions Radio à base de porteuses chaotiques en modulation de fréquence. Ce domaine de recherche récent propose une alternative aux solutions algorithmiques actuelles à clé secrète, utilisées pour répondre aux problématiques de confidentialité rencontrées de plus en plus souvent dans tous les systèmes de communication. La solution proposée est de plus, potentiellement complémentaire aux solutions algorithmiques, dans le sens où elle intervient au niveau de la couche physique des systèmes de transmission de données numériques par porteuse radio.

Le débit et la souplesse des transmissions radio sont souvent liés à la gamme de fréquence de la porteuse. Dans la plupart des démonstrations de communication par chaos en électronique que l'on peut trouver dans la littérature, cette gamme de fréquence était en général limitée aux basses fréquences (quelques dizaines de kHz). Sur la base d'un savoir-faire expérimental en optique, nous avons étudié les possibles transpositions aux communications Radio, des techniques et principes démontrés avec succès à de très hauts débits en optique (3 Gb/s). Deux approches successives ont été menées, et ont conduit chacune à une réalisation de deux systèmes complets de transmission Radio cryptée par porteuse chaotique FM. La première version correspond à une réalisation à des fréquences intermédiaires, avec une porteuse chaotique FM de l'ordre de 5 MHz. Celle-ci, bien que ne pouvant pas satisfaire des contraintes plus ambitieuses en termes de débit de codage, a toutefois permis de développer, tester, et démontrer dans un premier temps, la possibilité de transposition des techniques initialement développées en optique. En particulier, nous avons démontré la possibilité de génération, dans le domaine des ondes radio et de l'électronique, d'oscillations chaotiques de grande complexité grâce un schéma de dynamique non linéaire à retard. Le principal verrou alors identifié pour la montée en fréquence de la porteuse électronique, concernait la réalisation d'une transformation fortement non linéaire en électronique, à des fréquences élevées, c'est à dire donc sans pouvoir faire intervenir des montages à amplificateurs opérationnels comme c'était le cas dans la première version. Ce travail de recherche a permis de trouver, une solution originale pour la réalisation de cette non linéarité, au travers de la mise en œuvre, par voie opto-électronique, d'un interféromètre à grande différence de chemin "radio-fréquence", avec des ondes ra-

dio dans la gamme GSM (1.5 GHz). Pour cette seconde version de générateur de chaos électronique, une nouvelle architecture de générateur de chaos radio-fréquence a ainsi été conçue, réalisée et intégrée, dans un système complet de transmission sans fil par porteuse radio à modulation de fréquence chaotique.

Le système réalisé en est encore au stade de démonstrateur de laboratoire, mais des performances déjà très encourageantes ont été obtenues. Un rapport signal sur bruit de 35 dB a été mesuré. Grâce à de nombreuses améliorations technologiques au niveau de la mise en œuvre des diverses fonctions électroniques et opto-électroniques, le système étudié pourrait sans doute, sans trop de problèmes, proposer des performances bien supérieures. En particulier la simplification de certaines fonctions de traitement du signal, par exemple la démodulation d'amplitude et la conversion en bande de base de la modulation FM et de la transformation non linéaire associée, demande encore à être perfectionnées, afin d'atteindre une meilleure reproductibilité de la chaîne d'oscillation entre émetteur et récepteur, ainsi qu'un meilleur rapport signal sur bruit global de la chaîne de décodage. La souplesse d'utilisation des fibres optiques pour la réalisation de différences de chemin RF à bras multiples, conférant alors un degré de liberté supplémentaire dans la manière de produire un comportement chaotique. Enfin, des perspectives à plus long terme pourraient concerner la mise en œuvre hybride "analogique et numérique" de la chaîne d'oscillation chaotique. Ce nouveau type d'architecture de générateur de chaos permettrait de disposer à la fois d'une source analogique chaotique dans le domaine RF, en même temps qu'une très grande souplesse et précision de réglage des conditions d'oscillations chaotiques, par un ajustement fin et précis de certains des paramètres numériques clé de l'oscillateur. Cette perspective s'inspire directement de travaux effectués en parallèle dans ce domaine par l'équipe de XLIM Brive dans le projet national Transchaos auquel nous avons également participé.

Enfin, sur un plan plus fondamental, l'étude du générateur de chaos FM par interférences Radio et ligne à retard, a permis de mettre à jour une nouvelle classe de dynamique non linéaire à retard. Dans certaines conditions particulières de fonctionnement, nous avons pu en effet observer un comportement de la transformation non linéaire par interférences RF, qui n'est plus instantané, mais dynamique. Les propriétés dynamiques de ce nouveau type d'oscillateur à retard sont encore peu connues, et leur portée effective dans diverses applications sont encore à découvrir. Toutefois, les méthodes et techniques de génération de porteuses électroniques large spectre sont encore en plein développement, et leur utilisation dans diverses applications en sont encore au stade prospectif (radars, générateurs de nombres aléatoires, communications par porteuses large bande, signaux de test pour les futurs équipements électroniques haute fréquence...). Ce travail espère pouvoir contribuer à ce domaine de recherche à la frontière entre les propriétés fondamentales

des dynamiques chaotiques, et leur utilisation dans des applications précises.

Cartes électroniques du chaos en fréquence (BF)

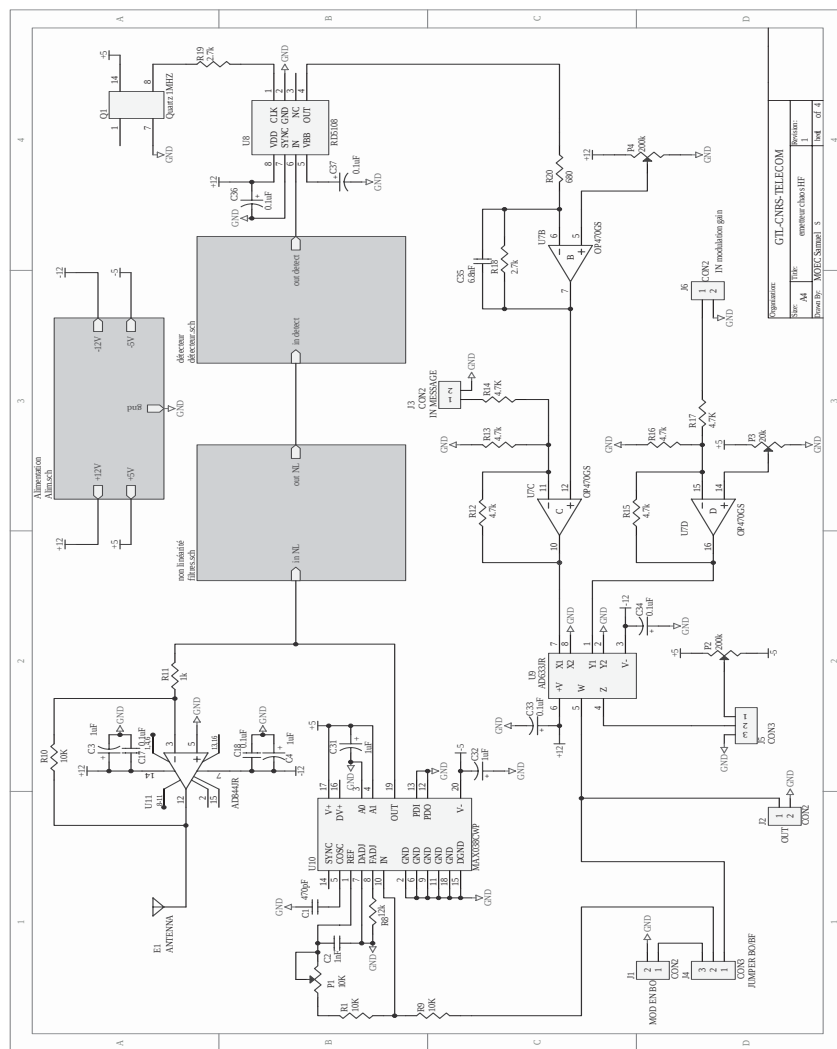


FIG. A.1 – Schéma du système d'émission

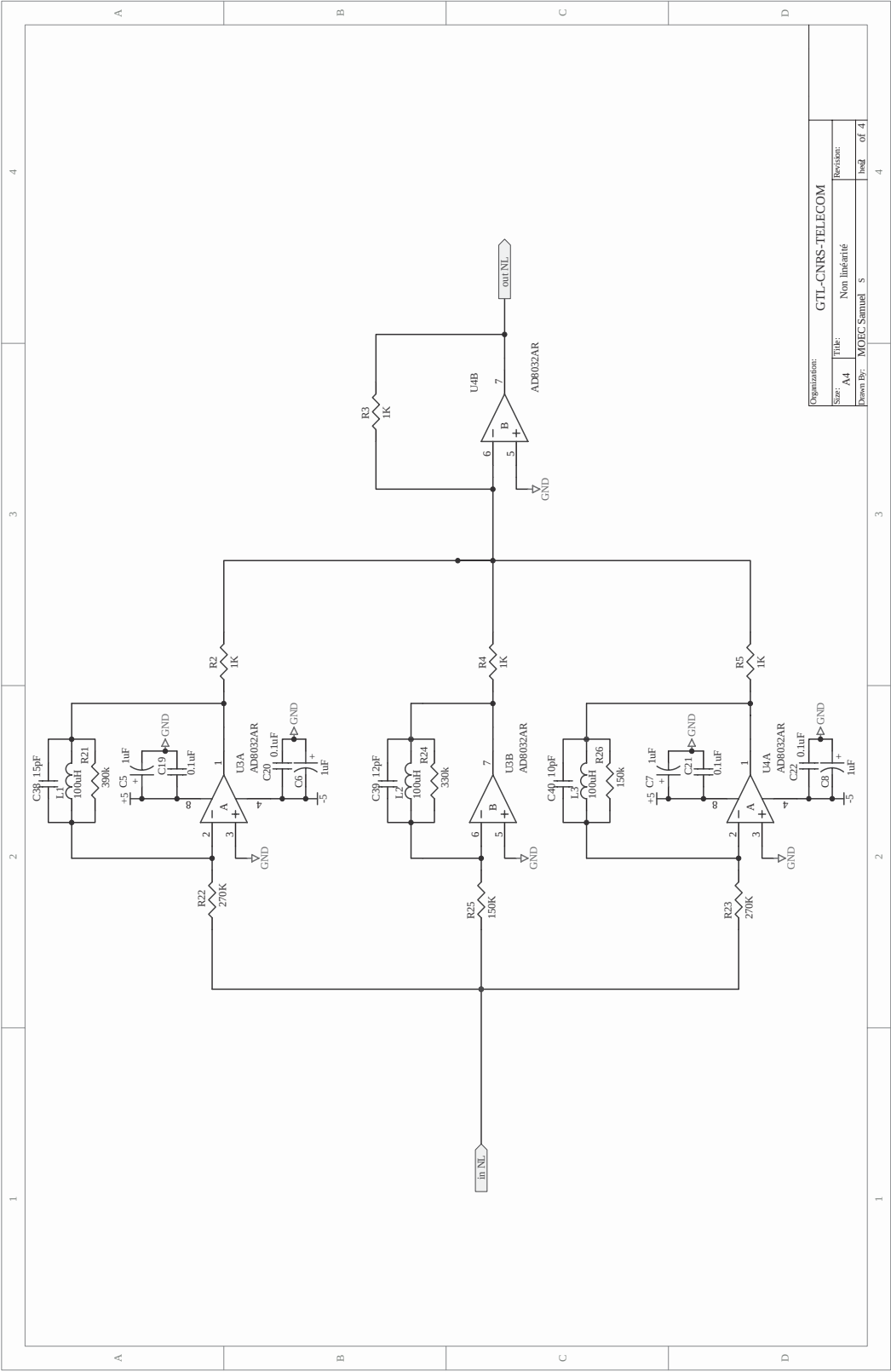


FIG. A.2 – Non-linéarité

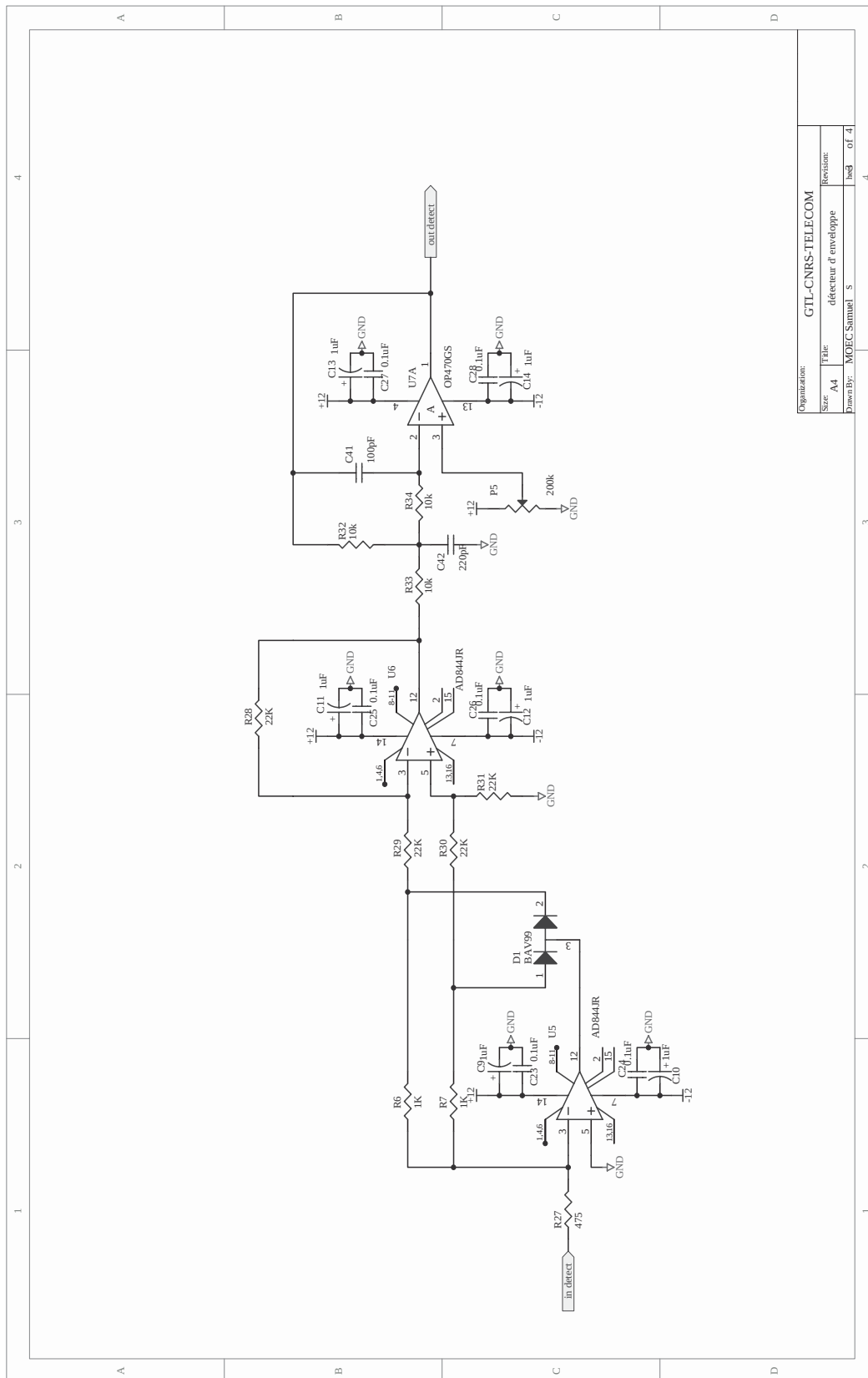


FIG. A.3 – Détecteur d'enveloppe

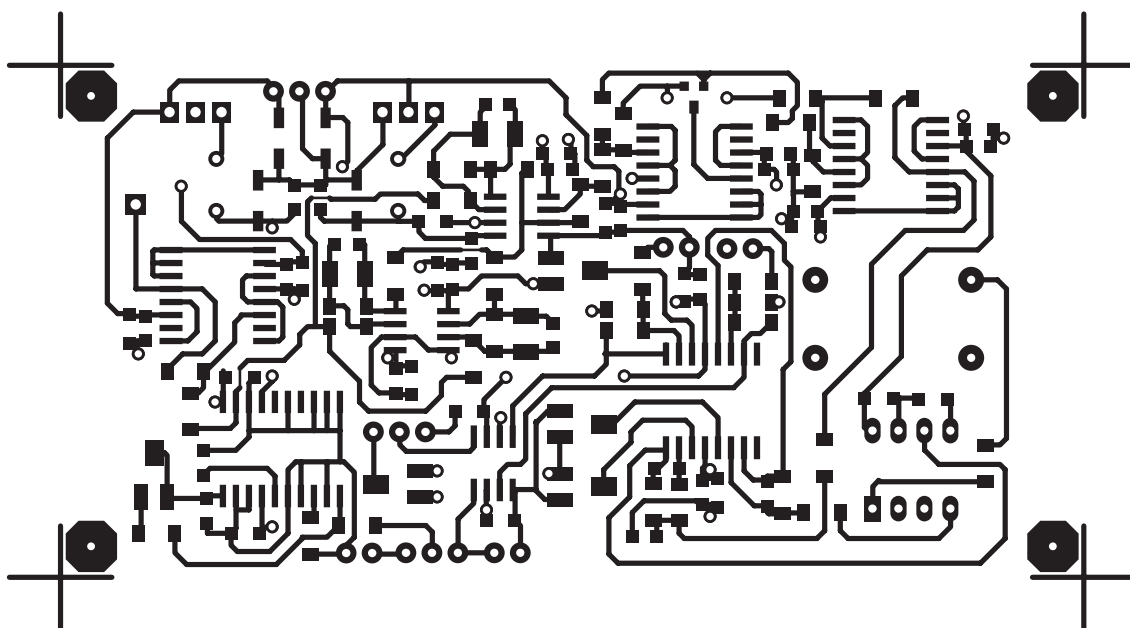


FIG. A.4 – Schéma du système de réception

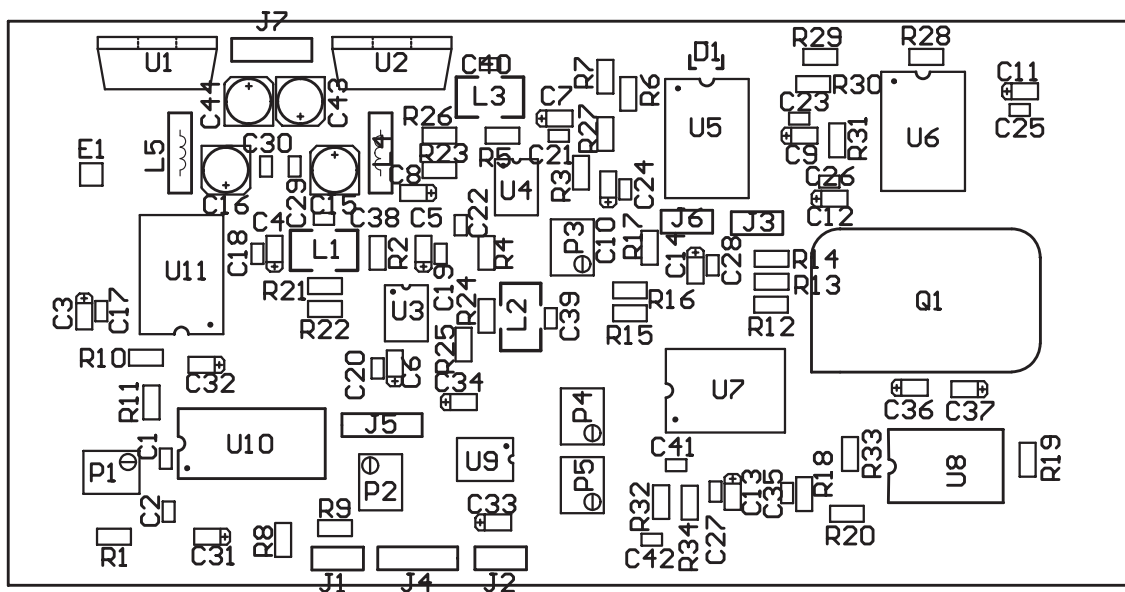


FIG. A.5 – Schéma du système de réception

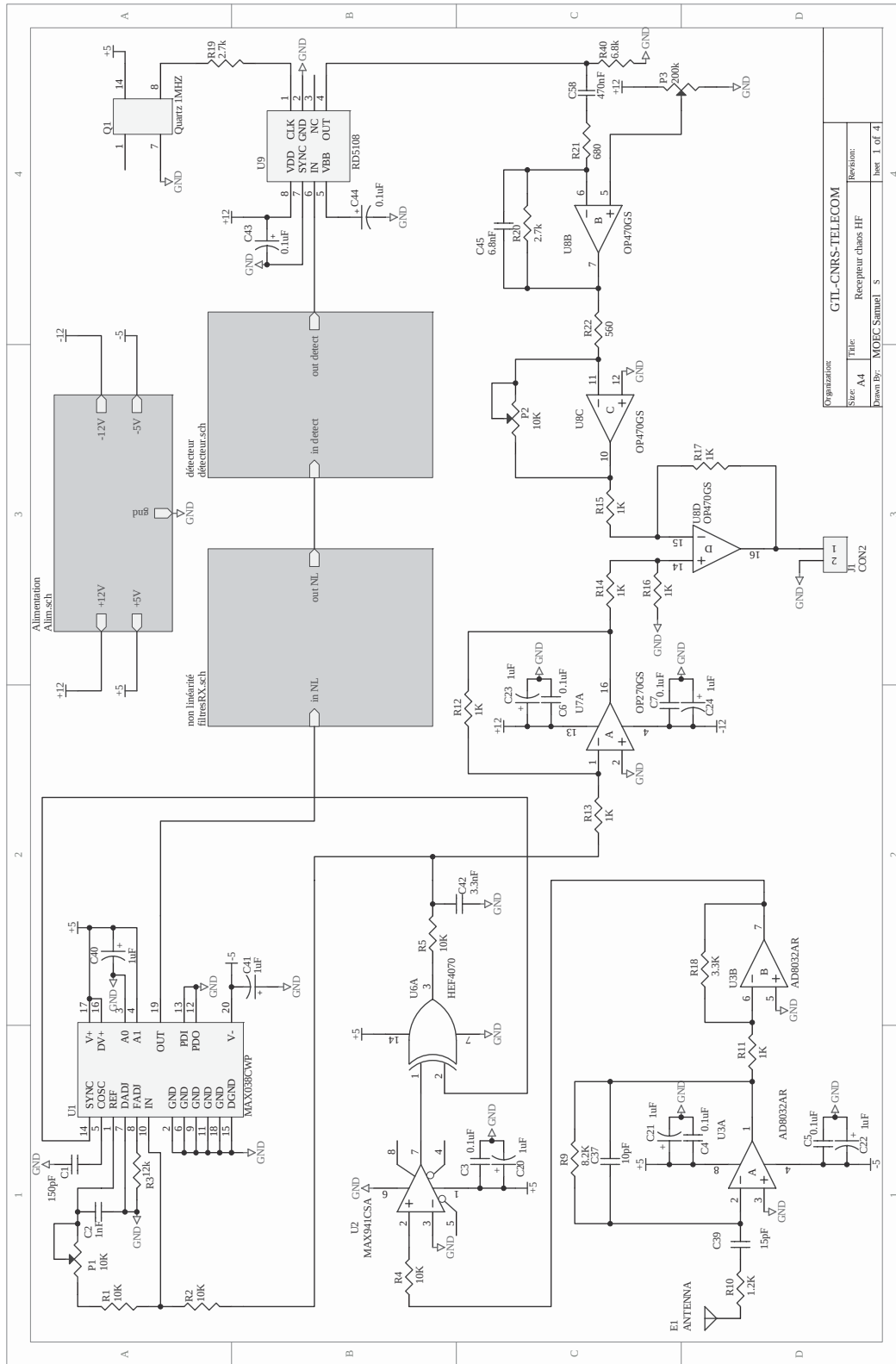


FIG. A.6 – Schéma du système de réception

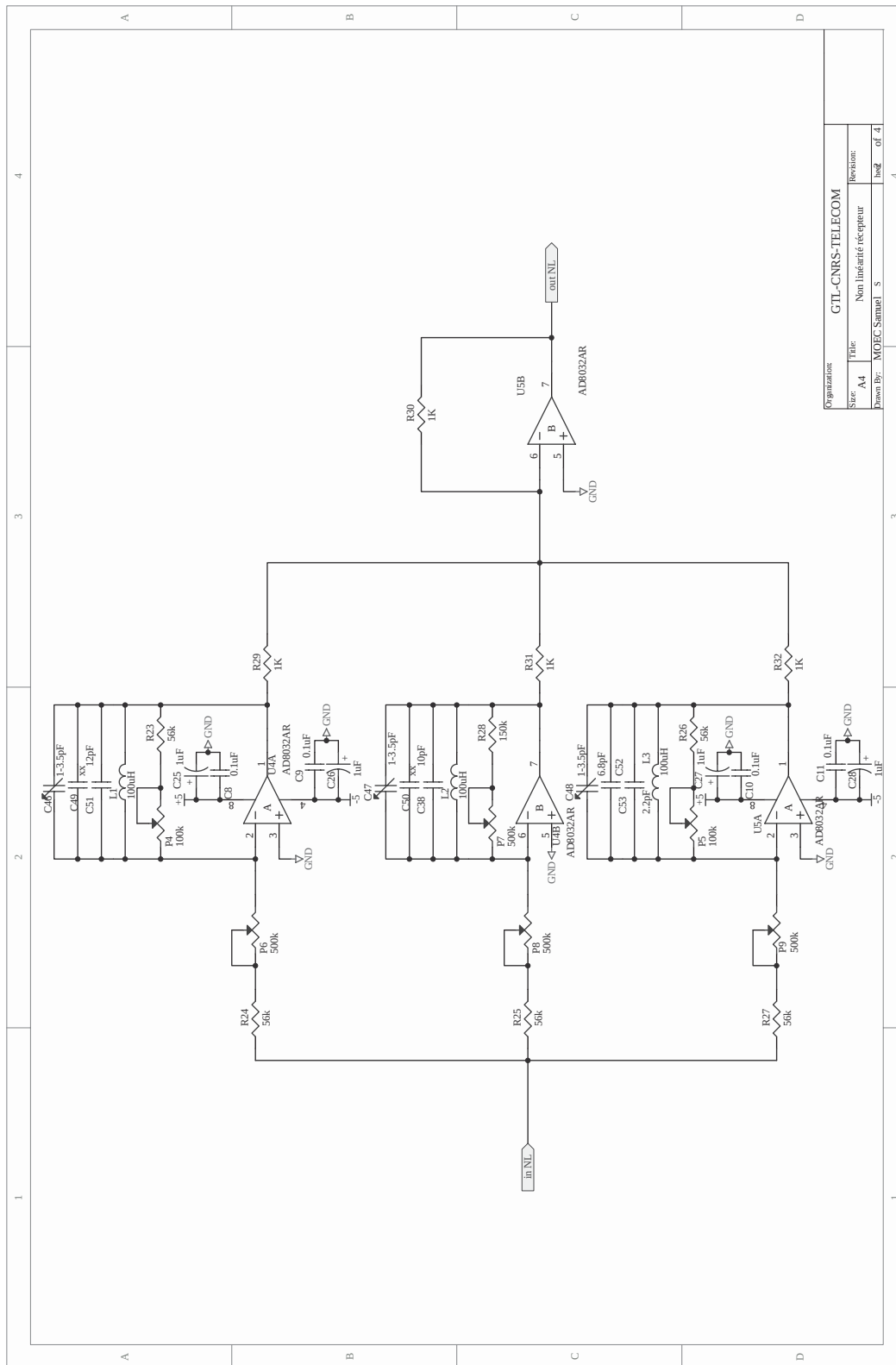


FIG. A.7 – Non-linéarité du récepteur

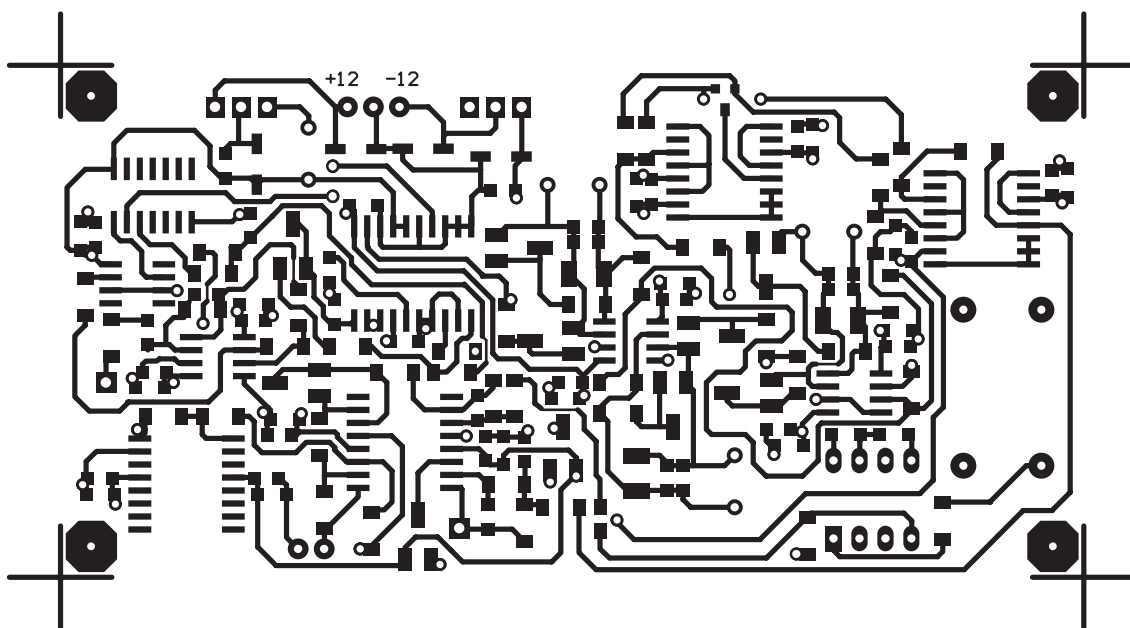
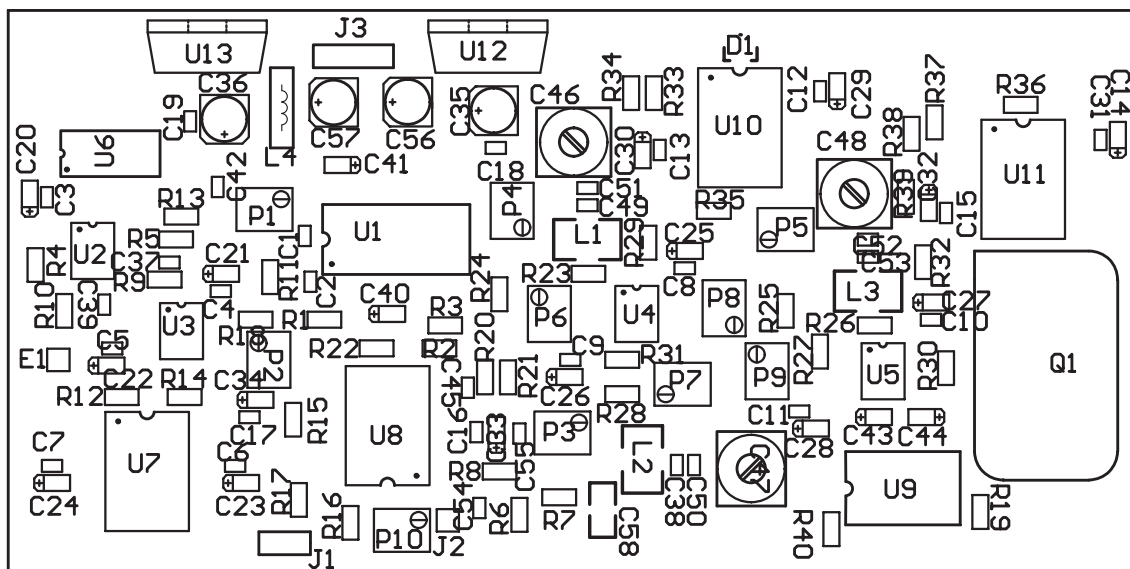


FIG. A.8 – Schéma du système de réception



Annexe B

Résolution de l'équation différentielle du second ordre par la méthode Runge-Kutta du quatrième ordre

Nous allons décrire le calcul de l'équation différentielle suivante :

$$\tau_1 \tau_2 \frac{d^2 s}{dt^2}(t) + (\tau_1 + \tau_2) \frac{ds}{dt} + s(t) = (\tau_1 + \tau_2) \frac{de}{dt}(t)$$

Pour qu'elle soit transformée en un système à deux équations. Cette équation différentielle peut, en intégrant chacun des termes, prendre la forme suivante :

$$\frac{\tau_1 \tau_2}{\tau_1 + \tau_2} \frac{ds}{dt} + s(t) + \frac{1}{\tau_1 + \tau_2} \int_{t_0}^t s(\theta) d\theta = e(t)$$

Nous retrouvons le système à deux équations suivant :

$$\begin{cases} (\tau_1 + \tau_2) \frac{dz}{dt}(t) = s(t) \\ \frac{\tau_1 \tau_2}{\tau_1 + \tau_2} \frac{ds}{dt}(t) = e(t) - s(t) - z(t) \end{cases}$$

En normalisant les équations par rapport à la constante de temps courte du système τ_1 .

$$\begin{cases} \frac{dz}{d\xi}(\xi) = \frac{\tau_1}{\tau_1 + \tau_2} s(\xi) \\ \frac{ds}{d\xi}(\xi) = - \left(1 + \frac{\tau_1}{\tau_2} \right) [e(\xi) - s(\xi) - z(\xi)] \end{cases}$$

Pour des simplifications d'écriture, nous noterons :

$$\begin{cases} \Upsilon = 1 + \frac{\tau_1}{\tau_2} \\ \psi = \frac{\tau_1}{\tau_1 + \tau_2} \end{cases}$$

Rappel de l'algorithme de Runge-Kutta du quatrième ordre

$$\frac{d\vec{X}}{d\xi} = f(\vec{X}, \vec{\xi})$$

$$X_{n+1} = X_n + \frac{K_1}{6} + \frac{K_2}{3} + \frac{K_2}{3} + \frac{K_4}{6} + O(h^5)$$

$$\begin{cases} K_1 = h f(X_n, \xi_n) = \begin{pmatrix} K_{1s} \\ K_{1z} \end{pmatrix} \\ K_2 = h f\left(X_n + \frac{K_1}{2}, \xi_n + \frac{h}{2}\right) = \begin{pmatrix} K_{2s} \\ K_{2z} \end{pmatrix} \\ K_3 = h f\left(X_n + \frac{K_2}{2}, \xi_n + \frac{h}{2}\right) = \begin{pmatrix} K_{3s} \\ K_{3z} \end{pmatrix} \\ K_4 = h f(X_n + K_3, \xi_n + h) = \begin{pmatrix} K_{4s} \\ K_{4z} \end{pmatrix} \end{cases}$$

Le pas d'intégration h est très important dans ce type de calcul car nous pouvons remarquer l'erreur d'approximation en dépend directement. Ainsi, plus celui-ci est petit, plus la précision du calcul est importante. Pour effectuer une bonne approximation, nous allons définir le pas d'échantillonnage égal à la constante de temps courte de l'oscillateur.

Application de l'algorithme à notre équation

nous considérons dans cet algorithme que :

$$e(\xi_n) = \beta f[s(\xi_n)]$$

En boucle fermée, la sortie $s(\xi_n)$ de l'équation différentielle est rebouclée sur l'entrée $e(\xi_n)$ par l'intermédiaire de la fonction non-linéaire f . N , que nous verrons apparaître dans la non-linéarité, est un pas matérialisant les différents points de calcul de la variable $s(\xi_n)$.

$$f(X_n, \xi_n) = \begin{bmatrix} -\Upsilon & -\Upsilon \\ \psi & 0 \end{bmatrix} \begin{bmatrix} s(\xi_n) \\ z(\xi_n) \end{bmatrix} + \begin{bmatrix} \Upsilon \\ 0 \end{bmatrix} \beta f(s(\xi_n + N))$$

$$f\left(X_n + \frac{K_1}{2}, \xi_n + \frac{h}{2}\right) = \begin{bmatrix} -\Upsilon & -\Upsilon \\ \psi & 0 \end{bmatrix} \begin{bmatrix} s(\xi_n) + K_{1s} \\ z(\xi_n) + K_{1z} \end{bmatrix} + \begin{bmatrix} \Upsilon \\ 0 \end{bmatrix} \beta f\left(\frac{1}{2}(s(\xi_n + N) + s(\xi_n + N + 1))\right)$$

En développant l'équation matricielle précédente, nous obtenons :

$$\begin{bmatrix} -\Upsilon(s(\xi_n) + z(\xi_n) + K_{1s} + K_{1z}) + \Upsilon \beta f\left(\frac{1}{2}(s(\xi_n + N) + s(\xi_n + N + 1))\right) \\ \psi(s(\xi_n) + K_{1s}) \end{bmatrix}$$

De la même manière, nous obtenons K_2 , K_3 et K_4 .

Programme permettant la résolution sur une période correspondant au retard T

$$f_{nl} = \beta f[s(\xi_n + N)]$$

$$dy0 = -\Upsilon(s(\xi_n) + z) + \Upsilon f_{nl}$$

$$dz0 = \psi s(\xi_n)$$

$$y05 = s(\xi_n) + \frac{1}{2\tau_1} dy0$$

$$z05 = z + \frac{1}{2\tau_1} dz0$$

$$f_{nl} = \beta f \left\{ \frac{1}{2} [s(\xi_n + N) + s(\xi_n + N + 1)] \right\}$$

$$dy05 = -\Upsilon(y05 + z05) + \Upsilon f_{nl}$$

$$dz05 = \psi y05$$

$$y05 = s(\xi_n) + \frac{1}{2\tau_1} dy05$$

$$z05 = z + \frac{1}{2\tau_1} dz05$$

$$dy05s = -\Upsilon(y05 + z05) + \Upsilon f_{nl}$$

$$dz05s = \psi y05$$

$$y1 = s(\xi_n) + \frac{dy05s}{\tau_1}$$

$$z1 = z + \frac{dz05s}{\tau_1}$$

$$f_{nl} = \beta f(s(\xi_n + N + 1))$$

$$dy1 = \Upsilon(y1 + z1) + \Upsilon f_{nl}$$

$$dz1 = \psi y1$$

$$s(\xi_{n+1}) = s(\xi_n) + [dy0 + dy1 + 2.0 * (dy05 + dy05s)] \tau_1 / 6$$

$$z = z + [dz0 + dz1 + 2.0 * (dz05 + dz05s)] \tau_1 / 6$$

Annexe C

Calcul de l'influence du compensateur d'erreur dans la matrice [S] obtenue

Dans ce calcul, nous allons définir les paramètres S_{ijM} mesurés sur les coupleurs parfaits que nous trouvons à l'intérieur de l'analyseur de réseau et les paramètres S_{ijA} du vrai quadripôle inconnu.

Nous pouvons que les paramètres mesurés sur les coupleurs parfaits sont alors fonction des paramètres du composants inconnu et des termes significatifs du compensateur d'erreur.

Il s'agit d'un système bien conditionné de quatre équations à quatre inconnues. Il admet une solution qui permet de remonter aux S_{ijA} grâce aux équations suivantes :

Paramètre de transmission direct

$$S_{21A} = \frac{1}{\Delta} \left(\frac{S_{21M} - e_{30}}{e_{10} e_{32}} \right) \left[1 + \left(\frac{S_{22M} - e'_{33}}{e'_{23} e'_{32}} \right) (e'_{22} - e_{22}) \right] \quad (C.1)$$

Paramètre réflexion en entrée

$$S_{11A} = \frac{1}{\Delta} \left(\frac{S_{11M} - e_{00}}{e_{10} e_{01}} \right) \left(1 + \frac{S_{22M} - e'_{33}}{e'_{23} e'_{32}} e'_{22} \right) \quad (C.2)$$

Paramètre de transmission inverse

$$S_{12A} = \frac{1}{\Delta} \left(\frac{S_{12M} - e'_{03}}{e'_{23} e'_{01}} \right) \left[1 + \left(\frac{S_{11M} - e_{00}}{e_{10} e_{01}} \right) (e_{11} - e'_{11}) \right] \quad (C.3)$$

Paramètre de réflexion en sortie

$$S_{22A} = \frac{1}{\Delta} \left(\frac{S_{22M} - e'_{33}}{e'_{23} e'_{32}} \right) \left(1 + \frac{S_{11M} - e_{00}}{e_{10} e_{01}} e_{11} \right) - \frac{e'_{11}}{\Delta} \left(\frac{S_{21M} - e_{30}}{e_{10} e_{32}} \right) \left(\frac{S_{12M} - e'_{03}}{e'_{23} e'_{01}} \right) \quad (C.4)$$

avec

$$\Delta = \left(1 + \frac{S_{11M} - e_{00}}{e_{10} e_{01}} e_{11}\right) \left(1 + \frac{S_{22M} - e'_{33}}{e'_{23} e'_{32}} e'_{22}\right) - \left(\frac{S_{21M} - e_{30}}{e_{10} e_{32}}\right) \left(\frac{S_{12M} - e'_{03}}{e'_{23} e'_{01}}\right) e_{22} e'_{11}$$

L'ensemble de ces équations sont lourdes mais nécessaires pour corriger les imperfections propres à l'analyseur de réseau vectoriel. Les douzes termes d'erreur de la matrice [e] sont déterminés avec la calibration. Si ceux-ci sont mal déterminés, la procédure de correction sera fausse et les S_{ijA} très éloignés des vraies valeurs.

Le but de la calibration est de déterminer pour chacune des fréquences à laquelle l'analyseur doit être calibré, les douzes termes d'erreur complexe. La procédure de calibration standard utilise alors des étalons de coefficients de réflexion (charge 50 Ω , court-circuit, circuit ouvert) que l'on connecte successivement à chacun des ports de l'analyseur de réseau. En pratique, il est toutefois impossible de réaliser un circuit ouvert parfait en très haute fréquence. Toute interruption de la ligne engendre une capacité d'extrémité qui rend le circuit ouvert non parfait. L'étalon *circuit ouvert* sera donc, en fait, une capacité de très faible valeur réalisée par l'interruption de l'âme d'un câble coaxial hyperfréquence mais pas du conducteur externe. Dans ces cas là, il existe des modèles très précis et valables de la capacité qui sont connus de l'analyseur de réseau et lui permettent de connaître à toute fréquence le déphasage β présenté en réflexion par cet étalon de coefficient de réflexion $\exp(-j\beta)$.

Voici la procédure de calibration et les coefficients de réflexion effectivement mesurés :

Type de mesure	étalon	expression mesurée
port 1, direct	charge 50 Ω	$S_{11M} = e_{00}$
port 1, direct	court-circuit	$S_{11M} = e_{00} + \frac{-e_{10} e_{01}}{1+e_{11}}$
port 1, direct	circuit ouvert	$S_{11M} = e_{00} + \frac{(e_{10} e_{01}) \exp(-j\beta)}{1-e_{11} \exp(-j\beta)}$
port 2, inverse	charge 50 Ω	$S_{22M} = e'_{33}$
port 2, inverse	court-circuit	$S_{22M} = e'_{33} + \frac{-e'_{23} e'_{32}}{1+e'_{22}}$
port 2, inverse	circuit ouvert	$S_{22M} = e'_{33} + \frac{e'_{23} e'_{32} \exp(-j\beta)}{1-e'_{22} \exp(-j\beta)}$
port 1 et 2, direct	charge 50 Ω	$S_{21M} = e_{30}$
port 1 et 2, direct	charge 50 Ω	$S_{21M} = e'_{03}$
port 1 et 2, direct	liaison directe	$S_{11M} = e_{00} + (e_{10} e_{01}) \frac{e_{22}}{1-e_{11} e_{22}}$
port 1 et 2, direct	liaison directe	$S_{21M} = e_{30} + (e_{10} e_{32}) \frac{e_{11}}{1-e_{11} e_{22}}$
port 1 et 2, inverse	liaison directe	$S_{22M} = e'_{33} + (e'_{23} e'_{32}) \frac{e'_{11}}{1-e'_{22} e'_{11}}$
port 1 et 2, inverse	liaison directe	$S_{12M} = e'_{03} + (e'_{23} e'_{01}) \frac{1}{1-e'_{22} e'_{11}}$

Annexe D

Calcul du chaînage de plusieurs quadripôles

Un multipôle d'ordre n de matrice $[S]$, de vecteur d'ondes incidentes (a) et de vecteur d'ondes réfléchies (b) est défini de la manière suivante :

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} S_{11} & \cdots & S_{1n} \\ \vdots & \ddots & \vdots \\ S_{n1} & \cdots & S_{nn} \end{pmatrix} \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \quad (\text{D.1})$$

Comme nous avons pu le voir, la mise en cascade deux quadripôles ne revient pas à la multiplication de chacune de ces matrices $[S]$ pour obtenir la matrice $[S]$ du système global. Pour résoudre ce problème, une nouvelle matrice $[T]$ est définie. Elle peut être chaînée entre plusieurs quadripôles en cascade.

$$S = \begin{pmatrix} b_1 \\ a_1 \end{pmatrix} = [T] \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} \quad (\text{D.2})$$

En résolvant le système linéaire constitué par les deux matrices précédentes définissant $[T]$ et $[S]$ à partir de a_n et b_n , nous trouvons la relation suivante :

$$T = \begin{pmatrix} -\frac{S_{11} S_{22} - S_{12} S_{21}}{S_{21}} & \frac{S_{11}}{S_{21}} \\ -\frac{S_{22}}{S_{12}} & \frac{1}{S_{21}} \end{pmatrix} \quad (\text{D.3})$$

Ainsi, si deux quadripôles A et B de matrices $[T_A]$ et $[T_B]$ sont mis en cascade, la matrice de l'ensemble est simplement $[T] = [T_A][T_B]$. La matrice $[S]$ de ce quadripôle pouvant être retrouvée par la relation inverse de la précédente

$$S = \begin{pmatrix} \frac{S_{11}}{S_{21}} & \frac{T_{11} T_{22} - T_{12} T_{21}}{T_{22}} \\ \frac{1}{T_{22}} & -\frac{T_{21}}{T_{22}} \end{pmatrix} \quad (\text{D.4})$$

Ainsi, dans le cas de l'association d'un quadripôle unidirectionnel (éléments opto-électroniques) et d'un quadripôle bidirectionnel (power splitter), les matrices $[T]$ sont respectivement définies comme suit :

$$T_A = \begin{pmatrix} -\frac{S'_{11} S'_{22} - S'_{12} S'_{21}}{S'_{21}} & \frac{S'_{11}}{S'_{21}} \\ -\frac{S'_{22}}{S'_{12}} & \frac{1}{S'_{21}} \end{pmatrix} = \begin{pmatrix} 0 & \frac{S'_{11}}{S'_{21}} \\ 0 & \frac{1}{S'_{21}} \end{pmatrix} \quad (\text{D.5})$$

$$T_B = \begin{pmatrix} -\frac{S_{11} S_{22} - S_{12} S_{21}}{S_{21}} & \frac{S_{11}}{S_{21}} \\ -\frac{S_{22}}{S_{12}} & \frac{1}{S_{21}} \end{pmatrix} \quad (\text{D.6})$$

Ainsi, le produit de ces deux matrices va nous donner la matrice $[T]$:

$$T = \begin{pmatrix} -\frac{S'_{11} S_{22}}{S'_{21} S_{12}} & \frac{S'_{11}}{S_{21} S'_{21}} \\ -\frac{S_{22}}{S_{12} S'_{21}} & \frac{1}{S_{21} S'_{21}} \end{pmatrix} \quad (\text{D.7})$$

La matrice $[S]$ caractérisant la mise en cascade de l'élément opto-électronique et du sommateur est la suivante :

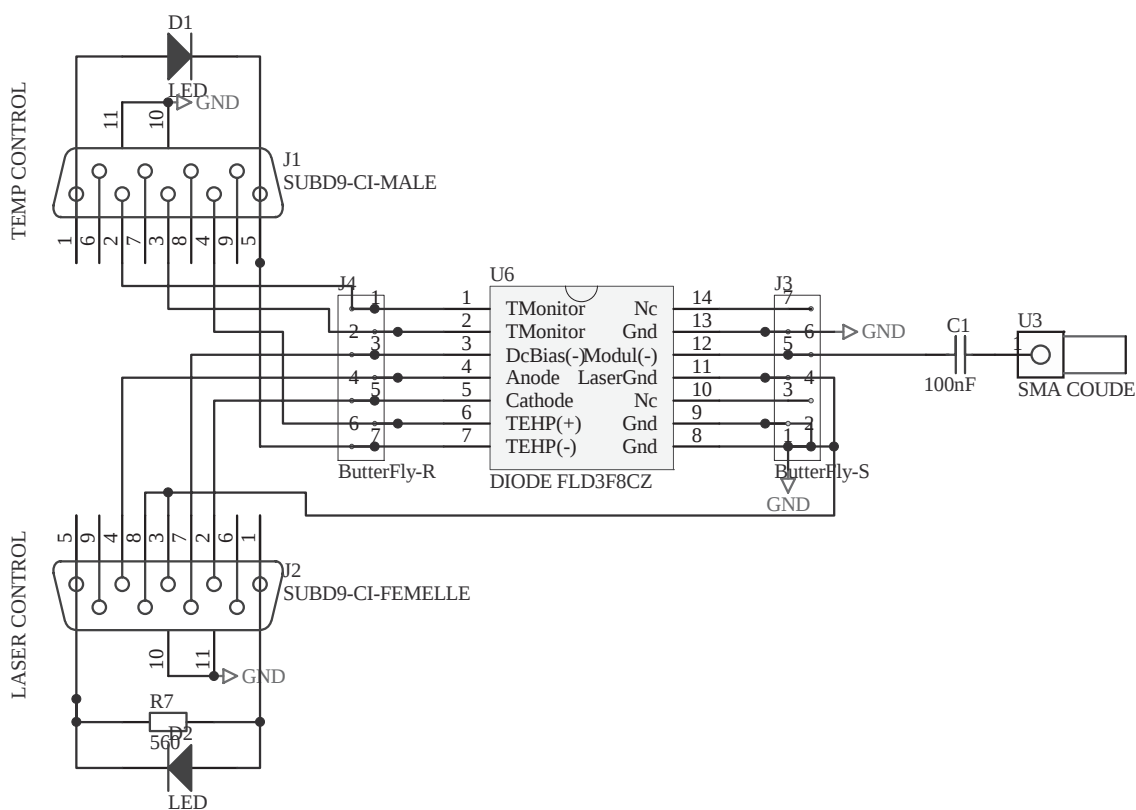
$$S = \begin{pmatrix} S'_{11} & 0 \\ S_{21} S'_{21} & \frac{S_{22} S_{21}}{S_{12}} \end{pmatrix} \quad (\text{D.8})$$

A noter que si les éléments n'étaient pas mis dans le même ordre ou s'il s'agissait de quadripôle n'ayant pas les mêmes caractéristiques (unidirectionnel ou bidirectionnel), la matrice $[S]$ correspondant au système global ne serait pas la même.

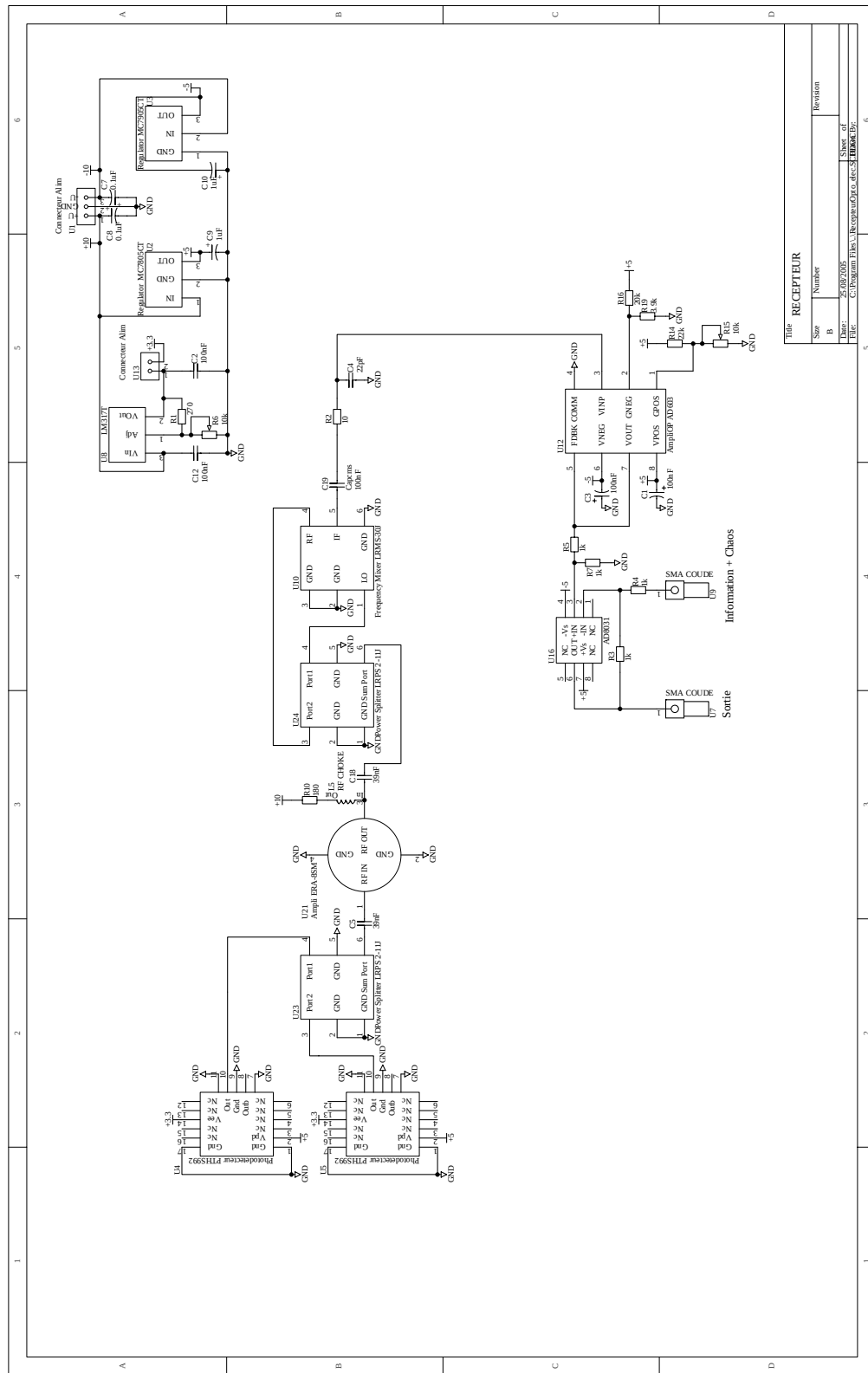
Annexe E

Schémas des cartes électroniques et opto-électroniques réalisées

E.1 Support de la diode laser CATV (modulation et alimentation)



E.3 Schéma électronique d'une partie du récepteur



E.4 Typon

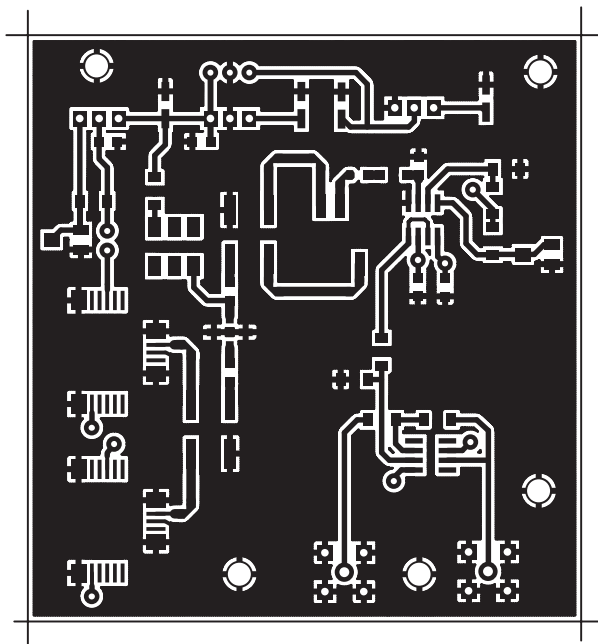


FIG. E.1 – Typon de la carte (Top Layer)

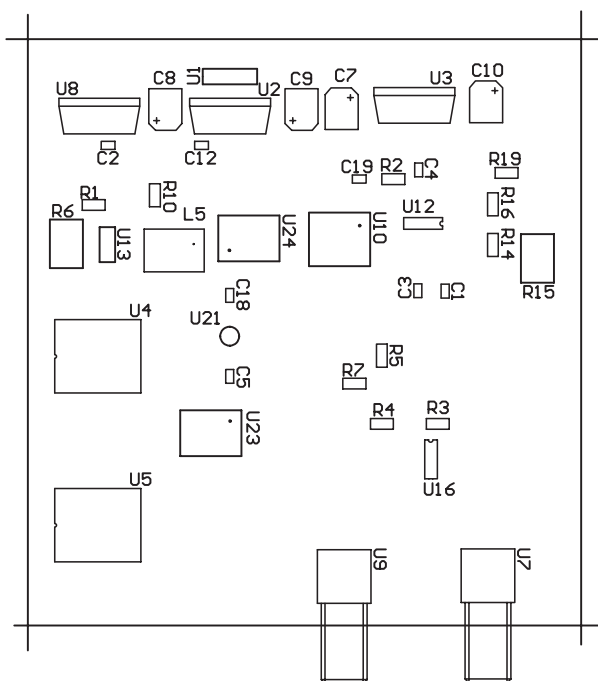


FIG. E.2 – position des composants sur la carte

E.5 Photographie des cartes électroniques de l'émetteur et du récepteur

E.5.1 Emetteur

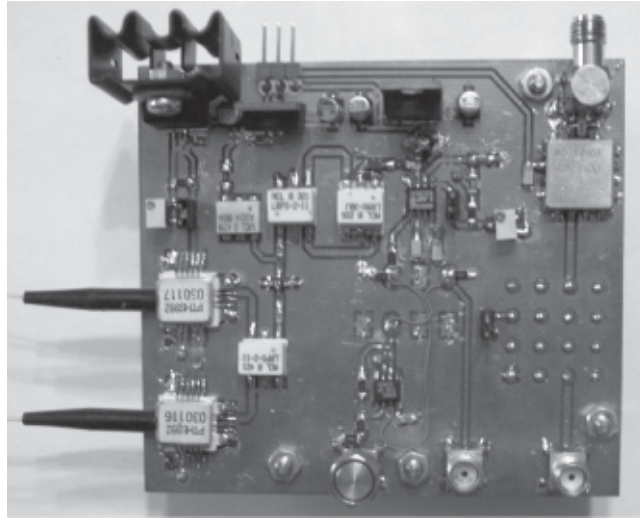


FIG. E.3 – Photographie de l'émetteur

E.5.2 Récepteur

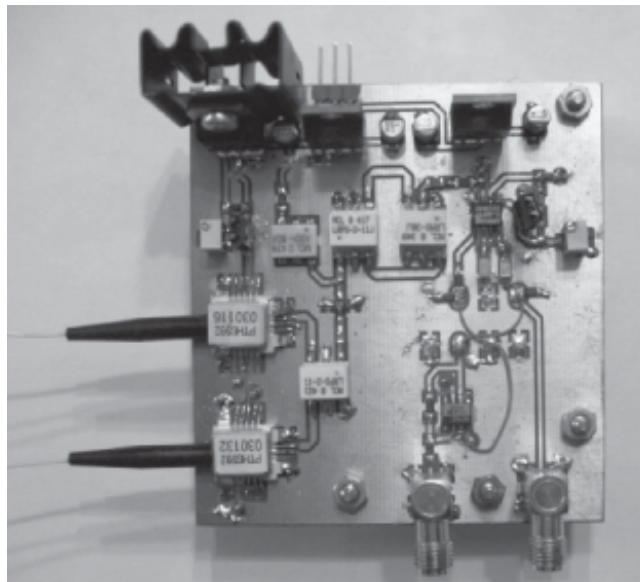


FIG. E.4 – Photographie du récepteur (sans la PLL)

E.5.3 Support de la diode laser

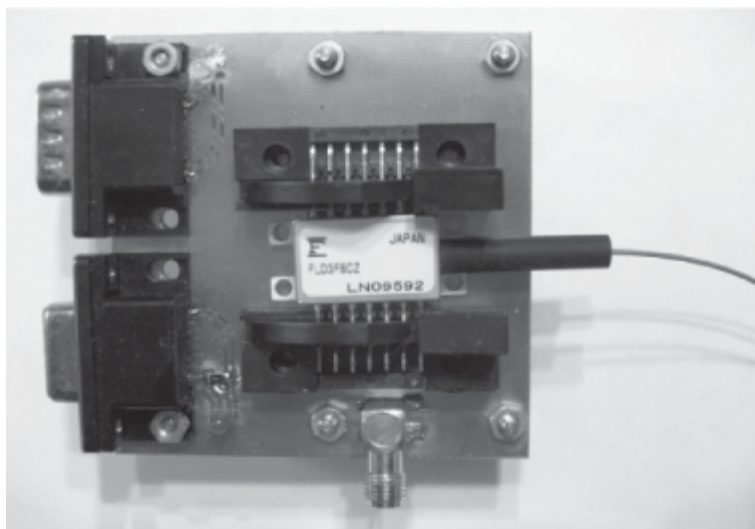


FIG. E.5 – Photographie du support de la diode laser connecté sur chacune des cartes précédentes

Bibliographie

- [1] F. Carmagnat, *Le téléphone public : cent ans d'usages et de techniques*. Collection technique et scientifique des télécommunications, 2003.
- [2] G. Brassard, *Cryptologie contemporaine*. Masson, 1992.
- [3] P. Bergé, Y. Pomeau, and C. Vidal, *L'ordre dans le chaos*. Hermann, 1992.
- [4] J. Gleick, *La Théorie du chaos*. Flammarion, 1991.
- [5] I. Prigogine, *Les lois du chaos*. Flammarion, 1997.
- [6] J. Mainguenaud, *Cours d'Automatique, chapitre 4 : systèmes asservis non-linéaires*. Collection de l'ingénieur-technicien, 1974.
- [7] T. Erneux, "Dynamique nonlinéaire à retard," *Compte Rendu de la 8ème Rencontre du Non Linéaire*, pp. 73–78, 2005.
- [8] A. Elwalkil and M. Kennedy, "Improved Implementation of Chua's Chaotic Oscillator Using Current Feedback Op Amp," *IEEE Transactions on Circuits and Systems*, vol. 47, pp. 76–79, january 2000.
- [9] L. Chua, "The Genesis of Chua's Circuit," *Archive für Elektronik und Übertragungstechnik*, vol. 46, pp. 250–257, 1992.
- [10] K. Ikeda, "Multipe-valued stationnary state and its instability of the transmitted light by a ring cavity system," *Optics Comm*, vol. 30, August 1979.
- [11] L. A. Aguirre, "Recovering map static nonlinearities from chaotic data using dynamical models," *Physica D*, pp. 41–57, 1997.
- [12] G. Elert, *The Chaos Hypertextbook : Mathematics in the Age of the Computer*. Learning in Motion, 2004.
- [13] M. Le Berre, A. S. Patrascu, E. Ressayre, and A. Tallet, "Localized structures in chaotic patterns from disorder to ordering," *Phisical Review A*, vol. 56, pp. 3150–3160, october 1997.
- [14] K. Ikeda and O. Akimoto, "Instability leading to periodic and chaotic self-pulsations in a bistable optical cavity," *Physical Review Letters*, vol. 48, pp. 617–620, march 1982.
- [15] F. Hopf, D. Kaplan, H. Gibbs, and R. Shoemaker, "Bifurcations to chaos in optical bistability," *Physical Review Letters*, vol. 25, pp. 2172–2182, April 1982.
- [16] B. Picinbono, *Signaux aléatoires : Fonctions aléatoires et modèles*. Dunod, 1994.

-
- [17] J. G. Proakis, *Digital communications*. McGraw-Hill, 4th ed., 2001.
 - [18] baher H., *Analog & Digital signal processing*. John Wiley & Son, 2001.
 - [19] K. T. Alligood, T. D. Sauer, and J. A. Yorke, *Chaos : an introduction to dynamical systems*. Springer, 1996.
 - [20] J. Kaplan and J. Yorke, *Functional Differential Equations and Approximation of Fixed Points*. Springer, 1979.
 - [21] L. M. Pecora and T. L. Carroll, "Synchronisation in chaotic systems," *Physical Review letters*, vol. 64, p. 821–824, February 1990.
 - [22] L. Pecora and T. carroll, "Driving systems with chaotic signals," *Physical Review A*, vol. 44, pp. 2374–2383, August 1991.
 - [23] T. Beth, D. E. Lazic, and A. Mathias, *Cryptanalysis of Cryptosystems based on Remote Chaos Replication*. Springer-Verlag Berlin Heidelberg, 1994.
 - [24] S. Tang, H. F. Chen, S. K. Hwang, and J. M. Liu, "Message encoding and decoding through chaos modulation in chaotic optical communications," *IEEE Transactions on Circuits and Systems*, vol. 49, pp. 163–169, February 2002.
 - [25] L. Larger, J.-P. Goedgebuer, and F. Delorme, "Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator," *Physical Review E*, vol. 57, pp. 6618–6624, june 98.
 - [26] V. S. Udaltsov, J.-P. Goedgebuer, L. Larger, and W. T. Rhodes, "Communicating with optical hyperchaos : Information encryption and decryption in delayed nonlinear feedback systems," *Physical Review Letters*, vol. 86, pp. 1892–1895, February 2001.
 - [27] L. Larger, *Cryptage de signaux par chaos en longueur d'onde*. PhD thesis, UFR des Sciences et Techniques de l'Université de Franche-Comté, Janvier 1997.
 - [28] E. Genin, L. Larger, J.-P. Goedgebuer, M. W. Lee, R. Ferrière, and X. Bavard, "Chaotic oscillations of the optical phase for multigigahertz-bandwidth secure communications," *IEEE J. Quantum Electron.*, vol. 40, pp. 294–298, march 2004.
 - [29] E. Genin, *Etude et réalisation d'un générateur de chaos optoélectronique sur la phase optique pour les télécommunications cryptées au débit*. PhD thesis, U.F.R. des Sciences et Techniques de l'Université de Franche-Comté, 2003.
 - [30] Y. C. Kouomou, P. Colet, N. Gastaud, and L. Larger, "Effect of parameter mismatch on the synchronization of chaotic semiconductor lasers with electro-optical feedback," *Physical Review E*, vol. 69, 2004.
 - [31] N. Gastaud, S. Poinot, L. Larger, J.-M. Merolla, M. Hanna, J.-P. Goedgebuer, and F. Malassenet, "Electro-optical chaos for multi-10Gb/s optical transmissions," *Electronics Letters*, vol. 40, july 2004.
 - [32] M. J. Bünner and W. Just, "Synchronisation of time-delay systems," *Phys. Rev. E*, vol. 58, pp. 4072–4075, october 1999.

-
- [33] A. Tamasevicius, A. Cenys, A. Namajunas, and G. Mykolaitis, "Synchronising hyper-chaos in infinite-dimensional dynamical systems," *Chaos, Solitons & Fractals*, vol. 9, no. 8, pp. 1403–1408, 1998.
 - [34] J. Encinas, *Systèmes à verrouillage de phase (P.L.L.) : Réalisations et applications*. Masson, 1990.
 - [35] B. A. Harb and A. M. Harb, "Chaos and bifurcation in third-order phase locked loop," *Chaos, Solitons and Fractals*, vol. 19, pp. 667–672, 2004.
 - [36] H.-A. Tanaka, S. Oishi, and K. Horiuchi, "Chaos from orbit-flip homoclinic orbits generated in real systems," *IEEE Symposium on Circuits and Systems*, vol. 1, pp. 263–266, 1995.
 - [37] T. Endo and L. O. Chua, "Bifurcation diagrams and fractal basin boundaries of phase-locked loop circuits," *IEEE Transactions on Circuits and Systems*, vol. 37, pp. 534–540, April 1990.
 - [38] J. Smith, *modern communication circuits*. McGraw-Hill, 1986.
 - [39] J. Montagné, *Le Siècle de la Radio*. les cahiers de j.-c. montagné (n^o 1) ed., 2001.
 - [40] J. Kraus and R. Marhelka, *Antennas for all applications*. Mc Graw Hill, 2002.
 - [41] J. Bolomey, *Antennes*. Encyclopedia Universalis, 1986.
 - [42] L. Larger, J.-P. Goedgebuer, V. S. Udaltsov, and W. T. Rhodes, "Radio transmission system using fm high dimensional chaotic oscillator," *Electronics Letters*, vol. 37, pp. 594–595, April 2001.
 - [43] L. Larger, V. S. Udaltsov, J.-P. Goedgebuer, and W. T. Rhodes, "Chaotic dynamics of oscillators based on circuits with VCO and nonlinear delayed feedback," *Electronics letters*, vol. 36, pp. 199–200, February 2000.
 - [44] J.-B. Cuenot, *Système optoélectronique de communication sécurisé par chaos en longueur d'onde*. PhD thesis, Université de Franche-Comté, 2001.
 - [45] I. et M. Joindot, *Les télécommunications par fibres optiques*. Dunod, 1996.
 - [46] W. H. Press, S. A. Teukolsky, W. T. Vetterling, and B. P. Flannery, *Numerical Recipes in C, The Art of Scientific Computing*. Cambridge University Press, second ed., 1992.
 - [47] J. D. Farmer, "Chaotic attractors of infinite-dimensional dynamical system," *Physica 4D*, pp. 366–393, 1982.
 - [48] I. P. Smirnov, A. L. Virovlyansky, and G. M. Zaslavsky, "Ray chaos, travel time modulation, and sensitivity to the initial conditions," *The Journal of the Acoustical Society of America*, vol. 117, pp. 1595–1606, March 2005.
 - [49] C. Tresser, P. Coulet, and A. Arneodo, "On the existence of hysteresis in a transition to chaos after a single bifurcation," *Journal de Physique (Paris)*, vol. 41, pp. 243–246, May 1980.
 - [50] A. Prasad, L. D. Iasemidis, S. Sabesan, and K. Tsakalis, "Dynamical hysteresis and spatial synchronisation in coupled non-identical chaotic oscillators," *Pranama - journal of Physics*, vol. 64, pp. 513–523, April 2005.

- [51] X. Bavard, *Numérisation du Chaos et Applications aux Systèmes de Communication Sécurisés par Chaos en Longueur d'Onde*. PhD thesis, Université de Franche-Comté, ST, 2004.
- [52] B. Dorizzi, B. Grammaticos, M. Le Berre, Y. Pomeau, E. Ressayre, and A. Tallet, “Statistics and dimension of chaos in differential delay systems,” *Physical Review Letters A*, vol. 35, pp. 328–339, january 1987.
- [53] S. Haykin, *Communication Systems*. John Wiley & Sons, 1996.
- [54] P. H. Young, *Electronic Communication Techniques*. Prentice Hall, 1999.
- [55] Hewlett-Packard, *Exposé de formation : Calibration de l'analyseur de réseau*. Technical report, 1985.
- [56] A. Balanov, N. Janson, and E. Scholl, “Delayed feedback control of chaos : Bifurcation analysis,” *Physical Review E*, vol. 71, january 2005.
- [57] P. H. Young, *Electronic Communication Techniques*. Prentice Hall, 1999.