Cryptographie par chaos à l'aide des dynamiques non linéaires à retard

Mémoire en vue de l'obtention d'une Habilitation à Diriger des Recherches

Laurent Larger
Laboratoire d'Optique P.M. Duffieux, UMR CNRS 6603
Université de Franche–Comté - 25030 Besançon Cedex -

Table des matières

1 Curriculum Vitæ

État civil

LARGER Laurent
né le 04/05/1968 à Colmar (Haut–Rhin).
Domicile : 64, rue des Granges – 25000 Besançon
Téléphone : (33) (0)3 81 61 98 05
Bureau : Laboratoire d'Optique Pierre Michel Duffieux, UMR CNRS 6603,
Université de Franche–Comté, 16 route de Gray – 25030 Besançon Cedex
Tél. : (33) (0)3 81 66 64 68, Fax. : (33) (0)3 81 66 64 23
e-mail : laurent.larger@univ-fcomte.fr

Études Supérieures et expériences professionnelles

- 06/86 – 09/88 : 06/86, Baccalauréat série C à Besançon, mention B. 86 – 88, mathématiques supérieures, et spéciales P' à Strasbourg.
- 09/88 – 09/92 : Élève à l'**École Normale Supérieure de Cachan** en section Physique Appliquée.
  88/89, Licence EEA mention B, (Paris XI Orsay). 89/90, Maîtrise EEA mention TB (Paris XI Orsay).
  90/91, Agrégation de Sciences Physiques option Physique Appliquée ($9^{\text{ème}}$ rang).
  91/92, DEA Systèmes Électroniques et Photoniques mention B (Strasbourg I) ; le stage de recherche portait sur l'étude du comportement spectral d'une diode laser à cavité externe réalisée par un réseau de diffraction en configuration de Littrow.
- 09/92 – 12/93 : **Service National** en tant que VSNE en Allemagne pour des activités de **Recherche et Développement industriel** dans le domaine de la métrologie optique de distance par interférométrie, et de la rugosimétrie sans contact par champ proche acoustique. Travaux effectués à l'Institut Fraunhofer de Fribourg (RFA) dans le cadre d'un contrat de recherche avec l'entreprise Hommelwerke GmbH.
- 01/94 – 01/97 : Travail de **Thèse** au laboratoire d'Optique Pierre–Michel Duffieux, sur le thème "Cryptage de signaux par chaos en longueur d'onde". Enseignant en tant que moniteur à l'Université de Franche–Comté.
- 01/97 – 09/97 : Enseignant chercheur contractuel à l'Université de Franche–Comté, laboratoire d'Optique, sur un demi–poste **ATER**.
- 09/97 – 09/98 : **PRAG** de Physique à l'IUT de Nîmes, département Sciences et Génie des Matériaux (en création, seconde année). Mise de tous les enseignements de Physique en seconde, et participation aux enseignements de Mathématiques.
- 09/98 → : Recrutement sur un poste de **Maître de Conférence** à l'Université de Franche–Comté, laboratoire d'Optique. Titularisation en Septembre 1999.

Langues étrangères : **anglais**, lu écrit et parlé ; **allemand**, lu écrit et parlé.

2 Synthèse des activités de recherche

Les activités de recherche ont été effectuées principalement à l'Université de Franche–Comté, au Laboratoire d'Optique Pierre–Michel Duffieux, UMR CNRS 6603, dans l'équipe Opto-Électronique, et sous la direction du Professeur Jean–Pierre Goedgebuer. Le travail de thèse s'est déroulé sur le site de Besançon à l'UFR des Sciences et Techniques. Après le recrutement à l'Université de Franche–Comté sur un poste de Maître de Conférence, les recherches se sont poursuivies à Besançon, mais une partie a été aussi effectuée au sein du nouveau site de l'UMR 6603 à Metz, le GTL–CNRS Télécom, alors récemment créé en collaboration avec l'Université d'Atlanta (Georgia Institute of Technology).

2.1 Présentation et situation du thème de recherche

La sécurisation des informations est un thème de recherche pour lequel on assiste actuellement à un fort regain d'intérêt, principalement pour deux raisons. C'est d'une part une conséquence du formidable développement des télécommunications dans les 30 dernières années. Mais il est clair que la sécurisation est aussi naturellement apparue, du fait de la vulgarisation des échanges d'information à caractère confidentiel. En effet, la notion de confidentialité s'est largement étendue, à partir d'un domaine qui ne concernait initialement que la diplomatie, l'armée ou les gouvernements. Cette confidentialité est aujourd'hui devenue nécessaire à chaque individu, au travers de la banalisation des échanges d'information sur des grands réseaux de communication publiques internationaux (comme l'Internet). Ces échanges d'informations privées concernent par exemple des transactions financières suite à des achats électroniques, ou bien encore la transmission de données médicales confidentielles.

La technique de sécurisation actuellement le plus répandue est basée sur des algorithmes de codage, qui effectuent l'opération de cryptage par des moyens logiciels, c'est–à–dire à l'aide de calculs numériques. Les problématiques posées par cette technique sont les suivantes : il y a bien sûr en premier lieu le niveau de confidentialité, mais il y aussi la vitesse de codage, nécessairement limitée par le temps des calculs requis par les algorithmes. La puissance croissante des calculateurs numériques permet d'améliorer la vitesse de codage, mais elle permet aussi de rendre plus performantes les attaques de ce type de cryptage, et donc de diminuer le niveau de confidentialité initialement proposé.

Des solutions alternatives, complètement différentes de ces techniques numériques, présentent dans ce contexte un intérêt de recherche évident : cela a été, et est toujours, le cas de la cryptographie par chaos. Il s'agit en effet d'une méthode matérielle et non logicielle, donc potentiellement beaucoup plus rapide, qui s'appuie sur des principes très différents, principes issus de la théorie du chaos. C'est donc assez naturellement qu'en 1994, ce thème de recherche a démarré dans l'équipe opto–électronique du laboratoire d'Optique de Besançon, dans le contexte des télécommunications optiques bien sûr, et avec le soutien d'un grand opérateur des télécommunications, France Télécom.

2.2 Bref historique et état de l'art de la cryptographie par chaos

La cryptographie par chaos est un domaine de recherche assez récent, puisqu'elle trouve son origine en 1990. Elle a démarré avec les travaux de Louis Pecora et Thomas Carroll qui ont démontré théoriquement et expérimentalement la possibilité de synchronisation entre deux oscillateurs chaotiques. Cette capacité de synchronisation semblait *a priori* impossible à imaginer pour deux évolutions chaotiques, à cause de la propriété très connue de sensibilité aux conditions initiales.
La sécurisation d'information par chaos est ensuite rapidement apparue comme la première application concrète de cette possibilité de synchronisation. En y regardant de plus près, et en faisant appel à des notions élémentaires de théorie de l'information, ce passage de la théorie du chaos vers

la cryptographie n'est en fait pas si surprenant.
En effet, dans le contexte général des systèmes de transmission d'informations, on utilise d'abord un oscillateur qui sert de porteuse à l'information, après une modulation par cette dernière du signal de l'oscillateur. La porteuse, comme son nom l'indique, transporte alors l'information le long d'une ligne de transmission en faisant appel aux propriétés physiques des ondes. Au niveau d'un récepteur, un système de détection et de démodulation permet d'extraire l'information transportée par l'onde, pour la reconvertir en un signal, aussi similaire que possible à celui présent à l'émetteur, avant l'opération de modulation. Cette étape de démodulation utilise généralement un procédé de synchronisation. Ceci constitue un premier lien direct entre les dynamiques chaotiques capable de se synchroniser, et les systèmes de communication.
L'aspect sécurisation apparaît comme un second lien à l'évocation de la nature pseudo–aléatoire de la porteuse chaotique. En effet, dans la plupart des systèmes de communication, c'est une porteuse sinusoïdale qui est généralement utilisée, mais rien n'interdit *a priori* l'utilisation d'autres types d'oscillation, même si elles ne sont pas périodiques comme dans le cas des dynamiques chaotiques. Un contre–exemple typique à l'utilisation des porteuses harmoniques, est donné par une technique originale de modulation utilisant des codes binaires pseudo–aléatoires : il s'agit du CDMA, ou Code Division Multiple Access. Le CDMA est une technique de modulation numérique relativement récente, de plus en plus utilisée dans les télécommunications modernes. Son succès est dû à ses propriétés particulières qui sont :

⋆ la résistance de la démodulation par rapport aux chemins multiples (réflexions parasites sur des bâtiments par exemple, ce qui est fréquent en téléphonie mobile) ;

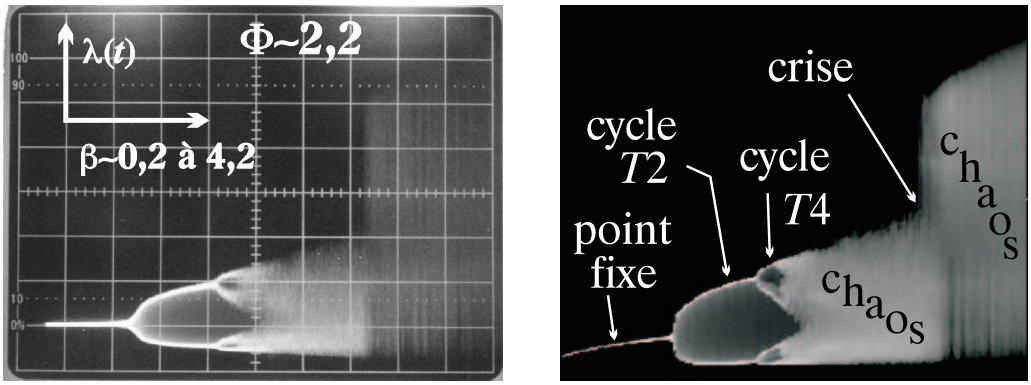
⋆ et une sécurisation intrinsèque des informations binaires transportées, sécurisation liée précisément à l'utilisation de codes pseudo–aléatoires. En effet, seule la connaissance de ce code peut permettre l'opération de démodulation.

Au travers de cette dernière propriété, l'avênement de la cryptographie par chaos nous apparaît bien moins fortuite, ou autrement dit, bien plus évidente. Et ce sont même des propriétés assez voisines qui caractérisent la sécurisation par chaos et le CDMA dans le contexte des télécommunications. Ces propriétés sont par exemple l'étalement spectral opéré par la porteuse, ou encore la nature critique de la démodulation sans une connaissance précise des conditions de modulation.

Après la découverte de la possibilité de synchronisation, et l'énoncé du principe de la cryptographie par chaos en 1990, la première démonstration expérimentale de cryptage par chaos est apparue en 1993. L'architecture du générateur de chaos alors mis en œuvre était basée sur un circuit électronique à plusieurs boucles d'oscillations imbriquées, dont l'une est non linéaire, afin de permettre un comportement chaotique. Le modèle théorique de ce type d'oscillateur chaotique s'apparente à celui que Lorenz avait développé dans ses travaux de modélisation des dynamiques climatiques, c'est–à–dire une dynamique vectorielle du premier ordre à 3 variables couplées de manière non linéaire. La dimension fractale de l'attracteur étrange correspondant est alors légèrement supérieure à 2, ce qui hélas indique clairement une dynamique de faible complexité. Cette faiblesse a été évidemment exploitée quelques années plus tard, dans la publication de la première tentative de crypto-analyse des systèmes sécurisés par chaos. L'aspect faible dimension n'étant pas une limite de principe, d'autres techniques de cryptographie par chaos ont ensuite été publiées. Et c'est principalement la richesse des dynamiques chaotiques qui a ouvert un vaste champ d'exploration des méthodes cryptographiques basées sur l'utilisation du chaos. Les principes essentiels de ce type de cryptage commencent à peine à être cernés de manière plus globale, notamment en termes de confidentialité et de performances. C'est dans ce contexte que ce sont inscrits les travaux de recherche rapportés dans ce manuscrit.

2.2.1 Résumé du travail de thèse

Le cryptage par chaos constitue, comme nous venons de le présenter, une des applications récentes des dynamiques chaotiques. Ce type de dynamique possède par nature deux aspects es-



(a) Relevé expérimental

(b) Par intégration numérique

FIG. 1 – Diagrammes de bifurcation (chaos en longueur d'onde, éq.(1), $\beta = 0,2$ à 4.2, et $\Phi = 2,2$)

sentiels au codage d'une information :

⋆ l'évolution dans le temps est bruitée (spectre large de type " bruit blanc " permettant de noyer une information dont l'amplitude est plus faible que celle du chaos), et elle peut alors permettre de brouiller, ou encore de masquer une information.

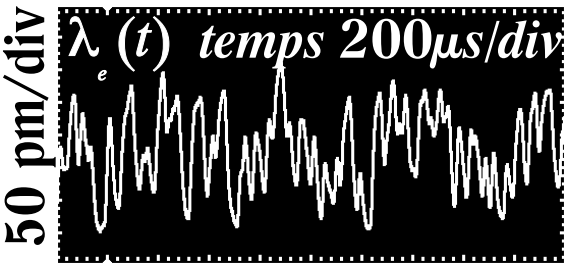
⋆ Mais ces dynamiques possèdent aussi un déterminisme local (loi d'évolution dynamique, équation différentielle d'évolution dans le temps) qui permet une reproduction, ou synchronisation, du même pseudo-bruit au niveau d'un récepteur, rendant ainsi possible le décodage.

Le travail de thèse a consisté dans un premier temps à maîtriser et à comprendre certaines des propriétés complexes de la dynamique chaotique choisie (hyperchaos généré par une équation différentielle non linéaire à retard). Cette compréhension a été accompagnée par la réalisation expérimentale d'un oscillateur opto–électronique fortement non linéaire, utilisant la variable dynamique original "longueur d'onde"λ. L'évolution temporelle de cette dernière est régie par une loi dynamique scalaire (une seule variable dynamique $\lambda(t)$), non linéaire (fonction F), et à retard (durée T) :

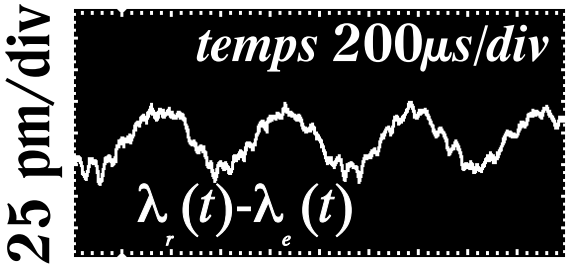
$$\tau \frac{\mathrm{d}\lambda}{\mathrm{d}t} + \lambda(t) = F[\beta, \lambda(t-T)] = \beta \sin^2[\lambda(t-T) + \Phi] \tag{1}$$

L'analyse des différentes solutions $\lambda(t)$ de l'éq.(1), ou autrement dit l'analyse des différents régimes dynamiques, en fonction des paramètres β et Φ de la fonction non linéaire F, a permis de mettre en évidence une vaste plage de valeurs de ces paramètres (β, Φ, T) adaptés à une application de cryptage (régime chaotique suffisamment complexe, attracteur chaotique de très grande dimension, supérieure à plusieurs dizaines et même plusieurs centaines). Le bon fonctionnement de l'oscillateur a été vérifié expérimentalement en visitant les nombreux régimes dynamiques accessibles pour différentes valeurs du couple (β, Φ) ; nous avons pu en particulier observer la fameuse route vers le chaos selon une cascade de bifurcations par dédoublement de période. Des tracés expérimentaux du diagramme de bifurcation ont été effectués, ils ont pu être comparés avec ceux obtenus numériquement par calcul des solutions de l'équation (1). Le très bon accord observé (Figure 1) a permis de conclure d'une part à la validité du modèle dynamique adopté, et d'autre part à la bonne maîtrise expérimentale du générateur de chaos. Ce dernier point est fondamental dans le contexte de la cryptographie par chaos, où il est nécessaire de pouvoir synchroniser avec une précision aussi bonne que possible deux oscillateurs chaotiques, l'un à l'émetteur, l'autre au récepteur.

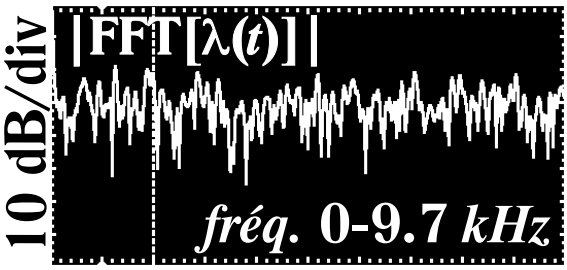
Dans un deuxième temps, la bonne connaissance de la dynamique de notre oscillateur nous a



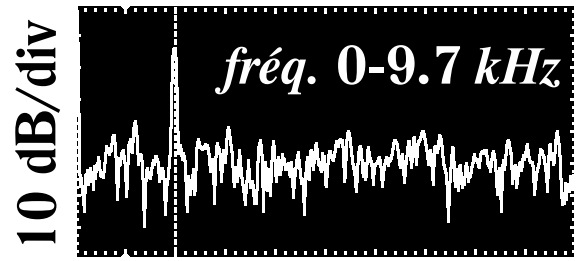
(a) Chaos transmis portant une sinusoïde



(b) Sinusoïde décodée



(c) Spectre du chaos transmis



(d) Spectre du résultat de décodage

FIG. 2 – Résultats expérimentaux de la cryptographie par chaos en longueur d'onde

permis de développer une technique de codage / décodage. Cette technique s'appuie sur des principes de synchronisation entre l'émetteur–codeur et l'oscillateur local de réception. Après avoir montré et évalué numériquement les performances de la méthode de codage / décodage, un démonstrateur a été réalisé, ce qui a constitué une première scientifique dans le domaine du cryptage par chaos en télécommunications optiques. Les résultats expérimentaux du système complet de cryptage ont (Figure 2), eux aussi, été en très bon accord avec les simulations numériques qui tenaient compte d'écarts inévitables dans l'appariement entre émetteur et récepteur.

Ces résultats ont présenté un intérêt suffisant aux yeux de notre partenaire de recherche France Télécom, pour décider le dépôt d'un brevet (Janvier 96) étendu au domaine international (USA, GB, Allemagne, Janvier 1997).

Liste des publications : Compte tenu du caractère confidentiel du travail effectué, les publications n'ont pu être faites avant le dépôt officiel des brevets protégeant les intérêts de notre partenaire industriel (France Télécom). Un **brevet** [B1] étendu au domaine international constitue la valorisation principale de la thèse avant la soutenance.

2.2.2 Contributions au domaine de recherche

Les points forts scientifiques des résultats obtenus se situent principalement sur deux plans :

1. D'un point de vue fondamental, les études menées dans le but de réaliser un générateur de chaos expérimental, ont permis d'ouvrir de nouvelles voies d'investigation des dynamiques non linéaires à retard généralisées [P1,P3]. Ces dynamiques particulières sont en effet encore relativement peu étudiées malgré leur grande richesse de comportements dynamiques, même dans le cas de formulations aussi simples que celle de l'équation (1). Lorsqu'elle sont étudiées,

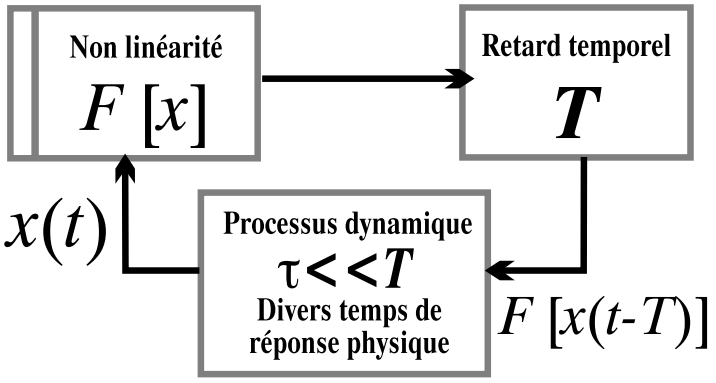
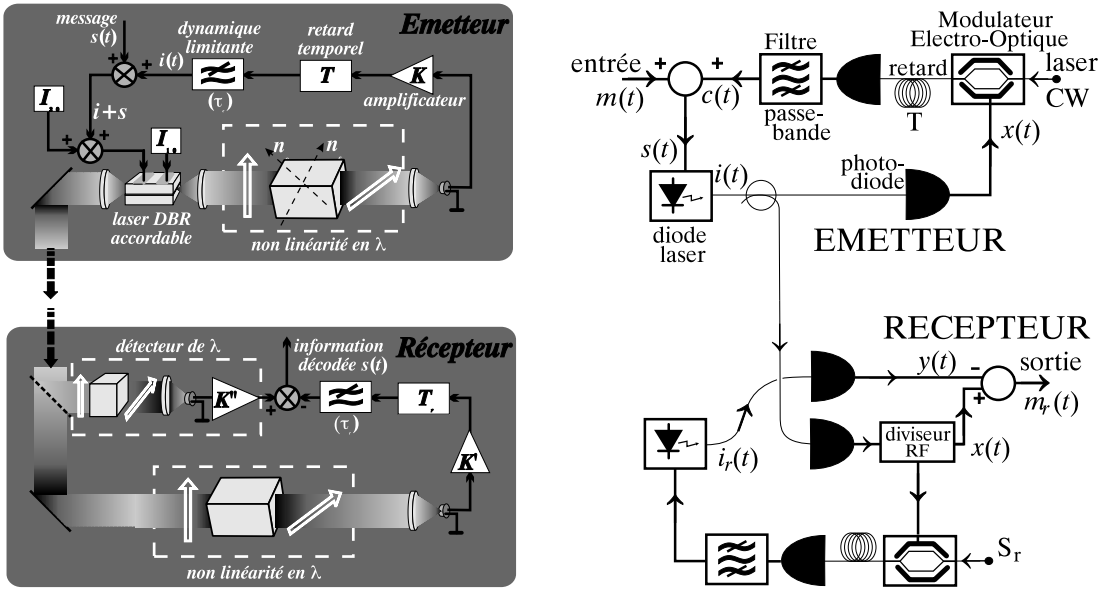


FIG. 3 – Architecture générale d'une dynamique non linéaire à retard

ces équations concernent des phénomènes physiques (gîte d'un navire soumis à un système de stabilisation, cavité optique non linéaire en anneau d'Ikeda) ou de sciences du vivant (évolution de populations animales dans un schéma proie-prédateur, production désordonnée de cellule du sang dans certains cas de leucémie selon le modèle de Mackey–Glass), phénomènes qui sont relativement complexes à analyser, mais dont on arrive à rendre compte à l'aide d'un simple modèle dynamique non linéaire à retard. L'expérience réalisée dans le contexte de la cryptographie optique a permis de dégager une architecture générale (représentée à la figure 3) de mise en œuvre expérimentale des dynamiques à retard. Ainsi, grâce à cette architecture, il est en principe possible de réaliser n'importe quelle dynamique modélisée par une équation de la forme (1). Un profil non linéaire quelconque de la fonction F est en effet rendu possible expérimentalement grâce à l'utilisation de la variable longueur d'onde, pour laquelle la fonction non linéaire correspond physiquement à un filtre spectral. Il est même possible en principe d'aborder selon cette même méthode les comportements d'une classe généralisée des dynamiques non linéaires à retard, comme celle décrite par n'importe quelle équation du type (2), incluant un ordre N élevé de la dynamique, avec plusieurs transformations non linéaires F_p de forme quelconque, et comprenant plusieurs retards temporels T_p. Cette exploration expérimentale des dynamiques non linéaires est particulièrement intéressante si l'on considère les difficultés numériques qui apparaissent lors de la simulation de tels systèmes (temps de calcul nécessaire, stabilité des procédures d'intégration numérique pour des ordres élevés, incertitude des résultats numériques du fait de l'incontournable sensibilité aux conditions initiales).

$$\sum_{n=1}^{N}\left(\prod_{k=1}^{n}\tau_k\right)\frac{\mathrm{d}^n\lambda}{\mathrm{d}t^n}+\lambda(t)=\sum_{p}F_p[\lambda(t-T_p)] \tag{2}$$

2. Mais aussi sur le plan appliqué, et dans le contexte de la cryptographie par chaos, les résultats obtenus ont permis de démontrer pour la première fois la faisabilité d'une telle cryptographie dans le domaine de l'optique [B1,P2,P4]. Le système qui a été réalisé (figure 4(a)) se démarque également des travaux antérieurs par les caractéristiques suivantes : il s'agit bien sûr d'un système opto–électronique dédié aux télécommunications optiques. La variable dynamique est originale, puisqu'il s'agit de longueur d'onde d'un laser semi-conducteur accordable, au lieu de la variable plus classique "intensité optique". Le type même de générateur de chaos utilisé, décrit par une équation différentielle non linéaire à retard, a permis pour la première fois d'obtenir des propriétés dynamiques idéales dans le contexte de la cryptographie par chaos :
   – La porteuse chaotique pseudo-aléatoire ne présente quasiment aucune signature fréquentielle susceptible d'être utilisée à des fins de crypto–analyse spectrale (spectre de type



(a) Chaos en longueur d'onde

(b) Chaos en intensité

FIG. 4 – Démonstrateurs optiques de cryptage par chaos

"bruit blanc").

- L'auto–corrélation temporelle présente une allure en forme de Dirac, ce qui témoigne également de l'absence de signature temporelle du déterminisme à l'origine du chaos.
- La distribution statistique du signal chaotique tend asymptotiquement vers un profil gaussien, ce qui rend ce signal semblable, du point de vue statistique, à celui provenant d'un vrai bruit, généré par exemple par le mélange d'un grand nombre de processus aléatoires indépendants (théorème de limite centrale).
- La dimension effective de l'attracteur étrange correspondant à la dynamique chaotique, peut atteindre plusieurs centaines, ce qui présuppose d'une grande complexité de comportement (et donc d'un niveau de confidentialité bien meilleur que les systèmes à base de chaos de faible dimension, typiquement de quelques unités). En d'autres termes, il est difficile par exemple d'identifier cet attracteur à l'aide des méthodes conventionnelles.
- Il existe pratiquement un grand nombre de possibilités dans le réglage des paramètres physiques qui permettent d'obtenir un comportement chaotique complexe, dont les propriétés physiques classiques (spectrale et statistique) sont toutes les mêmes. Ceci correspond en termes cryptographiques à une taille importante de la clé de codage, et donc à un bon niveau de confidentialité.

Des propriétés particulières du système de décryptage ont également été mises en évidence [P4]. La technique de synchronisation adoptée, dite en boucle ouverte, est inconditionnellement stable et permet un recouvrement exact de l'information masquée, à la condition d'une identité rigoureuse entre les paramètres dynamiques de l'émetteur et du récepteur. Nous avons quantifié expérimentalement et numériquement dans ce contexte l'influence des écarts entre ces paramètres, inévitables dans un système physique réel. Nous avons également énoncé, dans les conditions réalistes d'écarts de paramètres, le principe de compromis à réaliser entre la qualité de masquage de l'information sur la ligne de transmission, et la qualité du décodage.

2.3 Recherches effectuées après la thèse

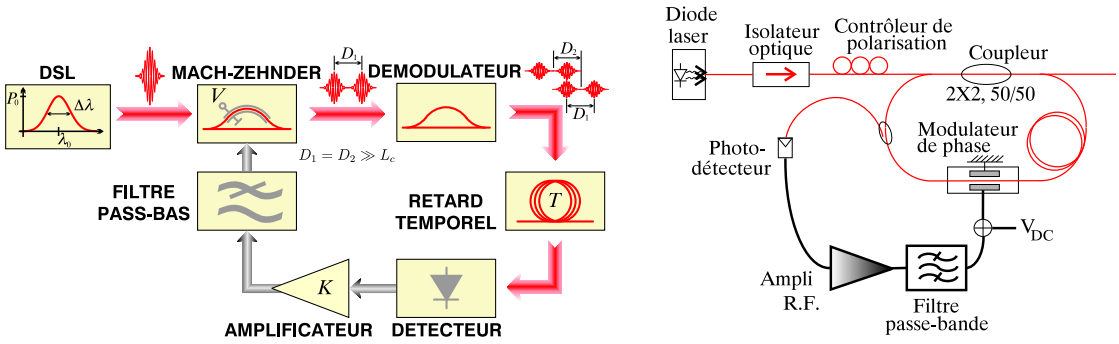
La cryptographie par chaos étant, encore actuellement, un domaine de recherche en constant développement, c'est principalement sur les bases du travail doctoral que se sont poursuivies les activités de recherche après la thèse. Le travail qui va être présenté a par ailleurs suivi de manière assez fidèle le programme de recherche qui avait été proposé lors de ma candidature au recrutement sur un poste CNRS sur lequel j'ai été initialement retenu avant d'opter pour un poste de maître de conférence en 97/98.

Au cours de ces quatre dernières années, les travaux de recherche ont été effectués dans le cadre de sept thèses co–encadrées au laboratoire d'Optique (Besançon et Metz), dont deux sont soutenues et une troisième est quasi–achevée dans sa rédaction. Ces travaux se sont également déroulés en collaboration avec Vladimir Udaltsov de l'Institut de Physique de Saint–Petersbourg (directeur de recherche, chercheur invité à GTL–CNRS Télécom), et Thomas Erneux directeur de recherche dans le Groupe d'Optique Théorique Non Linéaire à l'Université Libre de Bruxelles. Ces recherches ont obtenu le soutien financier de l'ANVAR (Sept.98–Mai 00) et de la CEE (Sept.01–), et ont constitué un des thèmes centraux d'une Action Spécifique (AS03 Sept.01) demandée par le département STIC du CNRS. L'ensemble a été principalement valorisé par 11 publications dans des revues à comité de lecture (dont 4 étaient principalement issues des travaux de thèse, mais sont parues après la thèse pour des raisons de confidentialité liées au dépôt d'un premier brevet), 2 brevets supplémentaires et 28 communications à des congrès internationaux.

2.3.1 Diversification des variables dynamiques

Le travail de thèse concerne l'utilisation d'un générateur opto–électronique de fluctuations chaotiques de la longueur d'onde d'un laser accordable. Cette variable longueur d'onde a démontré son intérêt par sa souplesse de fonctionnement au niveau expérimental. Néanmoins, il était intéressant de vérifier dans le cas d'autres variables dynamiques optiques, ou électroniques, la généralité des principes physiques mis évidence avec la variable longueur d'onde. Le problème physique à résoudre consiste alors à déterminer une configuration expérimentale qui permette de réaliser l'analogue des fonctions utilisées dans le cas de la longueur d'onde, dont la plus importante est la transformation non linéaire. Les variables dynamiques impliquées dans ces nouveaux systèmes cryptographiques sont alors susceptibles de présenter des intérêts propres à leur nature physique.

Chaos en intensité. Dans le cas de la variable "intensité optique", il s'agit de bénéficier des larges bandes passantes accessibles par les modulateurs de lumière actuels, et donc de permettre des débits de codage par chaos beaucoup plus élevés que ceux accessibles dans le cas de la longueur d'onde (dont la rapidité d'accordabilité est actuellement limitée technologiquement à une bande passante de l'ordre de quelques $100MHz$). La fonction non linéaire de ce chaos en intensité est alors réalisée par un interféromètre électro–optique de Mach–Zehnder intégré sur $LiNbO_3$. Cette non linéarité agit pratiquement entre les variables physiques "tension électro–optique" d'entrée du modulateur et "intensité optique" en sortie de l'interférence. Ce thème de recherche fait l'objet de deux thèses sur le site de Metz, dont une est quasiment achevée dans sa rédaction, et a permis de démontrer un codage à $100Mbits/s$ (montage expérimental représenté à la figure 4(b), [P12,B2,C8]). Une autre thèse vient de débuter, avec pour objectif un débit de $10Gbits/s$ (ce qui correspond à la limite des installations actuelles en télécommunication optique, mais sans l'opération de sécurisation). Une particularité du chaos en intensité ainsi généré, consiste en l'utilisation d'une dynamique d'ordre plus élevé, car la dynamique du générateur de chaos fait intervenir des filtres passe–bande à coupure très raide. Dans le cas de filtre passe–bande, la route vers le chaos est alors beaucoup plus directe (on ne passe plus forcément par les régimes périodiques de cascade de bifurcations par dédoublement de période), et la complexité obtenue en terme de dimension de Lyapunov, à largeur de bande égale, est plus élevée que pour un système passe–bas du premier



(a) Schéma basé sur le principe de la modulation de cohérence

(b) Schéma basé sur une cavité en anneau type "Ikeda"

FIG. 5 – Générateur de chaos

ordre [P11].

Modulation de cohérence chaotique. Dans le cas de la variable plus originale "différence de chemin optique", le travail s'est inspiré de recherches antérieures du laboratoire, dans le domaine d'une technique originale en télécommunication optique, la modulation de cohérence. Cette technique utilise une configuration particulière, dans laquelle une source de lumière de faible cohérence est modulée par un interféromètre électro–optique, dont la différence de marche est supérieure à la longueur de cohérence de la source (figure 5(a)). Ainsi, aucune modulation d'intensité n'est produite en sortie du Mach–Zehnder ; l'information de modulation électro–optique est toujours présente, mais elle se retrouve codée par une différence de chemin optique entre les paquets d'onde constituant le faisceau lumineux de sortie. Dans cette configuration, la fonction non linéaire est obtenue par un étage dit "de démodulation de cohérence", modélisé mathématiquement par une fonction d'interférence à deux ondes de contraste 1/2, modulée par une enveloppe de cohérence. La nature particulière de cette fonction non linéaire, a permis de mettre en évidence une route vers le chaos originale, dite en œil [P9], dont l'origine a pu être démontrée analytiquement. D'un point de vue physique, les variables dynamiques impliquées dans cette fonction non linéaire "tout optique", sont la différence de chemin optique avant l'étage de démodulation de cohérence, et la puissance optique de sortie de cet étage. Outre la bande passante des interféromètres électro–optiques également mis en jeu, la configuration particulière liée à la modulation de cohérence a permis d'améliorer le niveau de masquage de l'information cryptée [P13], en noyant cette information à plus de $70dB$ en dessous du niveau de signal disponible sur la ligne de transmission. Une autre particularité de ce démonstrateur de cryptage par chaos en modulation de cohérence concerne le récepteur, dans lequel l'opération de décodage est effectuée pour la première fois de manière tout optique [P13,Ca10,Ca11], grâce à une démodulation de cohérence électro-optique (le démodulateur d'un système de modulation de cohérence classique est habituellement constitué d'un interféromètre passif, comme celui utilisé à l'émetteur dans le générateur de chaos).

Chaos en phase optique. Ces travaux sur la variable différence de chemin optique sont en partie à l'origine d'un autre montage expérimental [Ca14], qui met en œuvre une variable dynamique similaire, puisqu'il s'agit de la phase optique (c'est donc un chemin optique et non plus une différence de chemin optique qui est modulée chaotiquement). À la grande différence du montage à base de la modulation de cohérence, ce nouveau générateur de chaos en phase optique fonctionne en régime extrêmement cohérent, puisqu'il utilise un laser DFB à fibre ultra stable, de très grande longueur de cohérence (très faible largeur de raie), et surtout aussi de très grande stabilité de la longueur d'onde centrale. Le schéma du générateur de chaos en phase optique est représenté à la

figure 5(b), il est en fait constitué d'un laser DFB à fibre, qui illumine d'abord un modulateur de phase, dont la sortie est injectée dans un anneau fibré réalisant à la fois la fonction retard optique (anneau de 1 à 2 *mètres* de long), et la non linéarité (interféromètre en anneau, réalisant un filtrage spectral complémentaire par rapport à la traditionnelle fonction d'Airy d'un Fabry-Pérot). On peut remarquer qu'il s'agit toujours d'une boucle de contre réaction opto–électronique, mais il y a en fait à la fois un retour tout optique (anneau fibré), et un retour opto–électronique. Ce dernier est constitué par un coupleur placé avant la sortie de l'anneau, et un photo–détecteur, dont le signal électrique, après amplification, est appliqué sur le modulateur de phase. Ainsi, le modulateur de phase agit sur la condition d'interférence de l'anneau, avec des temps caractéristiques inférieurs au temps de parcours (retard T) de l'anneau. En d'autres termes, la fonction de filtrage de l'anneau est en permanence en régime transitoire, puisqu'elle est sans cesse modulée chaotiquement par la phase optique imposée par la modulateur.

Fréquence électronique. Enfin, nous avons également cherché à appliquer les principes généraux du système cryptographique par chaos à une architecture purement électronique, en faisant un parallèle entre les variables optiques, et leur pendant électronique. La longueur d'onde issue d'une source laser accordable est ainsi devenue une fréquence électronique d'un oscillateur contrôlé en tension. Le filtre de longueur d'onde a été remplacé par un filtre de fréquences électroniques suivi d'un démodulateur d'amplitude, réalisant ainsi une non linéarité entre les variables "fréquence électronique" et amplitude démodulée en sortie du filtre. Ce montage a permis pour la première, la réalisation d'un générateur de chaos de très grande dimension en électronique [P5], à partir duquel un système complet de cryptage par chaos destiné aux transmissions hertziennes a pu être développé [P7,B3]. En effet, de part sa structure même, le générateur de chaos produit une signal modulé en fréquence de manière chaotique, ce signal FM pouvant directement servir de porteuse, déjà modulée par une information, dans une transmission hertzienne.

2.3.2 Nouvelles techniques de cryptage par chaos

Cryptage par commutation de clé. L'exploration de nouvelles techniques cryptographiques se poursuit actuellement sous divers aspects. Ce travail est effectué à la fois d'un point de vue théorique, et d'un point de vue expérimental. Dans ce dernier cas, nous avons mis à profit l'existence du système opérationnel de cryptage par chaos en longueur d'onde pour mener à bien les investigations (le développement d'un nouveau montage expérimental de cryptage par chaos pouvant constituer à lui seul un travail assez vaste pour un sujet de thèse à part entière).
En cryptographie par chaos, la technique de CSK (pour Chaos Shift Keying) est en fait connue dans son principe, mais elle avait surtout été appliquée sur des systèmes cryptographiques électroniques de faible dimension. Le CSK consiste pratiquement à envoyer un signal provenant d'un oscillateur en régime chaotique, dont un des paramètres est modulé en fonction d'une information binaire. C'est donc une technique essentiellement destinée à la sécurisation de données numériques. L'utilisation dans le générateur de chaos de deux valeurs voisines d'un paramètre, correspond physiquement à la génération de deux signaux chaotiques différents dans leur déterminsime, mais globalement très semblables (au sens statistique ou spectral par exemple). Il donc difficile à partir de l'observation du signal transmis de détecter les instants commutations correspondants à l'information binaire cryptée par CSK. Comme de nombreux paramètres sont pratiquement disponibles, un des enjeux de ce travail est de déterminer s'il existe certains paramètres plus adaptés que d'autres pour disposer d'une confidentialité aussi bonne que possible. Un des résultats importants (mais attendu) de ce travail [P8,C8], est que le paramètre T présente le meilleur compromis afin d'avoir à la fois un très bon niveau de masquage, et un très bon niveau de décodage.

Point d'insertion du message et point d'émission de la porteuse chaotique. Une autre façon de d'expliquer ce que signifie "technique" de cryptage par chaos, serait de parler de la manière employée pour mélanger une information dans un signal chaotique. Cet aspect a été

abordé numériquement et théoriquement par V. Udaltsov [P6]. Son étude a porté sur l'analyse des différents points d'insertion d'un message dans l'émetteur, en relation avec les différents points à partir desquels on transmet le message crypté vers le récepteur. Une des conclusions de cette étude est que le point d'insertion est *a priori* indépendant, mais qu'il implique la mise en œuvre d'une technique de démodulation (ou décodage) plus ou moins complexe.

2.3.3 Cryptographie très haut débit

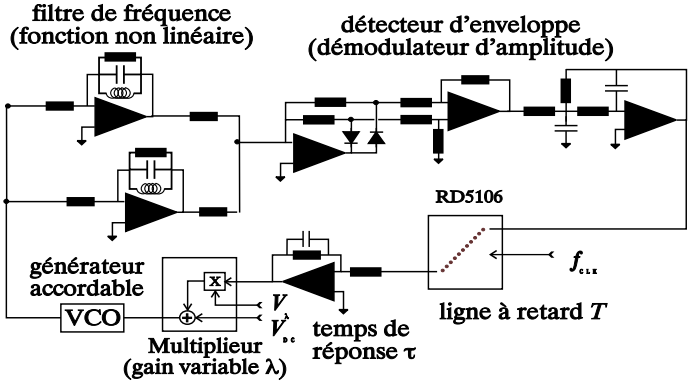
Chaos en intensité utilisant des Mach–Zehnder large bande. La limite de la vitesse de codage a été évoquée dans le cadre de la mise en œuvre d'un système cryptographique par chaos en intensité (partie 2.3.1). Grâce à l'utilisation de la variable intensité optique, et grâce aux très grandes vitesses de modulation des Mach–Zehnder en optique intégrée, nous avons discuté l'avantage en terme de débit maximum de codage que présentaient de tels systèmes cryptographiques opto–électroniques. Dans le cadre d'un premier démonstrateur, un débit de $100 Mbits/s$ a été obtenu. Le projet européen OCCULT en cours de réalisation a pour but l'obtention d'un système de cryptage par chaos autorisant un débit de minimum de $1 Gbits/s$. Cet objectif semble pouvoir être atteint dans notre équipe par une approche "système" très originale par rapport aux autres partenaires du projet (qui sont tous orientés vers une réalisation à base de diode laser à cavité externe, dont l'approche pourrait être qualifiée plutôt par le terme "composant").

Anneau fibré à modulation de phase rapide. Le démonstrateur de cryptographie par chaos en modulation de cohérence, qui utilise également des modulateurs électro–optiques intégrés de Mach–Zehnder, est en principe aussi susceptible de permettre des grands débits de codage. Pour des problèmes technologiques, il est toutefois pratiquement difficile d'atteindre des débits supérieurs à quelques $100 Mbits/s$. La raison à cela est liée principalement aux pertes dans les modulateurs de lumière impliqués, qui sont à grande différence de chemin optique ; ces composants sont en fait "exotiques", et impossibles à trouver sur le marché avec les performances nécessaires. C'est dans ce contexte que nous nous sommes tournés vers l'architecture à base de cavité en anneau fibrée, et de modulateur de phase [Ca14] (figure 5(b), voir aussi la partie 2.3.1). Compte tenu des éléments impliqués dans ce montage, la bande passante accessible est d'au moins $10 GHz$. Si l'on réussit à mettre en œuvre une structure "émetteur / récepteur" appariée, et ainsi à obtenir la synchronisation entre chaos sur l'ensemble de la bande de fréquence concernée, il sera possible d'effectuer un cryptage par chaos à un débit encore non atteint jusqu'à présent.

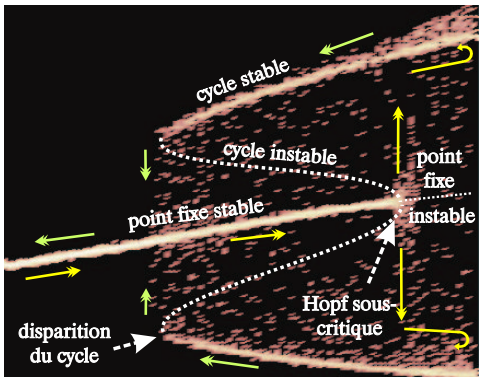
2.3.4 Étude des dynamiques non linéaires à retard et crypto-analyse

Une des originalités importantes nos systèmes de cryptage par chaos repose sur l'utilisation des dynamiques à retard. Ces dynamiques particulières sont en fait globalement assez peu étudiées d'un point de vue fondamental, même si l'on observe depuis quelques années un net regain d'intérêt pour ces systèmes très particuliers (qui interviennent dans un certain nombre de systèmes physiques, comme la dynamique de production de cellules du sang, l'évolution des populations animales dans un contexte proie–prédateur, la gîte des navires possédant un système de stabilisation, les cavités optiques non linéaires en anneau, les diodes laser à cavité externe, etc ... , les systèmes de cryptographie par chaos).

Bifurcations de Hopf des systèmes à retard. Dans ce contexte, nous avons étudié un certain nombre de comportements dynamiques observés expérimentalement. Dans le cadre d'un travail de collaboration avec Thomas Erneux du groupe d'Optique Théorique Non Linéaire de l'Université Libre de Bruxelles, il est apparu que des phénomènes observés même relativement simples, n'étaient pas encore très clairement expliqués dans le cas des dynamiques non linéaires scalaires à retard. C'est ainsi que nous nous sommes intéressés à une bifurcation très classique et très documentée



(a) Montage expérimental basé sur le principe du chaos électronique en fréquence



(b) Diagramme de bifurcation expérimental et son hystérésis caractéristique au voisinage du point de Hopf

FIG. 6 – Démonstration de la bifurcation de Hopf sous–critique dans un système à retard

en dynamique non linéaire, la bifurcation de Hopf. Elle se caractérise pratiquement, lors de la variation d'un paramètre de la dynamique, par l'apparition locale d'un cycle lors du changement de stabilité d'un point fixe (voir le diagramme de bifurcation "type" de la figure 1(b)). En termes de valeurs propres de la dynamique linéarisée au voisinage du point fixe, cela correspond dans le plan complexe au croisement de l'axe imaginaire par une valeur propre lors de la variation du paramètre (la partie réelle de la valeur propre visite des valeurs positives puis négatives en passant par zéro, d'où le changement de stabilité du point fixe ; et donc la valeur propre passe par une valeur imaginaire pure, d'où l'existence du cycle). Il existe alors deux situations possibles pour une bifurcation de Hopf,

⋆ soit le cycle est stable, et il coexiste avec la branche instable du point fixe (la bifurcation est alors dite super–critique),

⋆ soit le cycle est instable, et il coexiste alors avec la branche stable du point fixe (il s'agit du cas sous–critique).

Dans toutes les expériences physiques ou numériques portées à notre connaissance, seul le cas super–critique apparaît. Une curiosité naturelle nous a donc poussé à rechercher une explication à cette absence surprenante. Au travers d'une étude perturbative de la bifurcation de Hopf dans les dynamiques à retard du type de l'équation (1), nous avons pu établir des conditions sous lesquelles le cas sous–critique devait apparaître, conditions qui ne semblaient être remplies dans aucune des expériences connues. Nous avons ensuite aussi imaginé un montage expérimental remplissant ces conditions, et nous avons obtenu le diagramme de bifurcation de la figure 6(b), où un comportement en hystérésis a été observé, comportement caractéristique de la situation cas sous–critique [P14,Ca13,Ca16].

Ce travail nous a également appris que, dans le cas des dynamiques non linéaires à retard, les études analytiques en sont seulement au stade de l'exploration des régimes de faible complexité, et qu'elles sont pour l'instant loin de pouvoir décrire les régimes chaotiques de grande complexité utilisés en cryptographie par chaos.

Dynamiques non linéaires à faible retard. Un autre problème encore non complètement décrit dans la littérature a été abordé dans le cadre d'un travail avec V. Udaltsov. Il s'agit de l'influence du retard temporel dans les dynamiques à retard. Il est connu que c'est précisément ce retard qui est à l'origine de la grande complexité des régimes chaotiques obtenus. La dimension infinie de l'espace des phases des dynamiques à retard, trouve son origine dans les conditions initiales nécessaires pour définir de manière unique une solution quelconque de ces dynamiques :

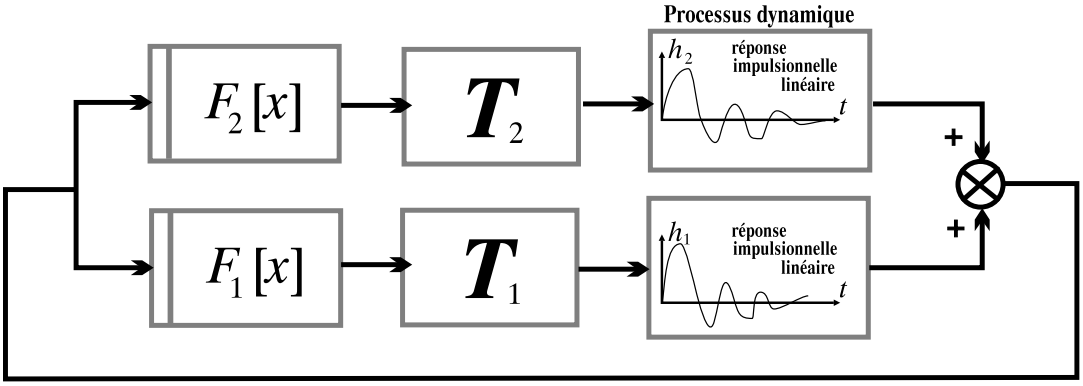
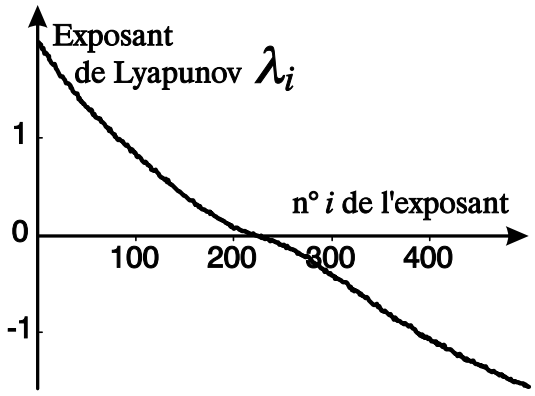


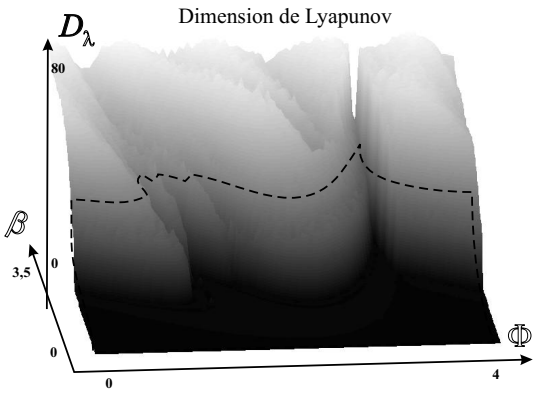
FIG. 7 – Principe d'un générateur de chaos amélioré, proposant une meilleure robustesse face à la crypto–analyse

ces conditions initiales sont en effet de taille infinie, puisque outre les valeurs initiales liées aux termes différentiels ($x(t=0)$ pour une dynamique du premier ordre en $\dot{x}$), il est aussi nécessaire de fournir une infinité de valeurs $x(t),\ t \in [-T, 0[$, pour remplir la "mémoire initiale" du système. Pratiquement, les informations nécessaires pour définir "correctement" une solution d'un système à retard, ne sont pas de taille "aussi infinie" que l'affirme la rigueur mathématique. En effet, l'action du temps de réponse physique τ revient à gommer ou atténuer l'effet de variations trop rapides de la mémoire. Toutes les façons de remplir la mémoire par une fonction $x(t),\ t \in [-T, 0]$ ne sont donc pas indépendantes, et il en résulte pratiquement une dimension fractale grande mais finie, des attracteurs chaotiques. Très logiquement, la valeur de cette dimension est liée au nombre de constantes de temps τ que l'on peut mettre dans la mémoire de durée T. Nous avons bien sûr pris soin de choisir dans la plupart des situations expérimentales développées, des valeur T/τ relativement élevées, afin d'obtenir des régimes chaotiques très complexes (dimension d'attracteur de plusieurs dizaines, à plusieurs centaines).
Une question alors posée au cours de nos réflexions a concerné le problème de la limite inférieure de la valeur de T/τ, en dessous de laquelle les régimes chaotiques ne sont plus possibles. Dans ces premiers travaux, Ikeda préconisait une valeur de l'ordre de deux. Nous avons en fait observé numériquement des solutions chaotiques même pour des valeurs de 1/10 [P10]. Ces études numériques ont certes montré que les chaos alors générés possèdent une structure très faiblement complexe (quasi-périodicité), mais nous avons également pu observer que les régimes chaotiques semblent toujours accessibles, même pour des valeurs très faibles du rapport T/τ, à conditions de disposer d'un poids extrêmement important de la fonction non linéaire (gain β de l'ordre de $(T/\tau)^{-1}$ dans la boucle de contre réaction).

Évolution de la dimension de Lyapunov dans différents types de systèmes à retard. Pour explorer les régimes chaotiques de grande complexité que nous recherchons en cryptographie par chaos, nous avons commencé à développer un savoir–faire (connu dans la littérature) basé sur des algorithmes d'analyse de séries temporelles chaotiques, et d'analyse de dynamiques définies par leur équation différentielle. La trame de fond à laquelle est rattachée cet axe de recherche est la crypto–analyse, dont le but pour nous est de dégager les points faibles en terme de sécurité des systèmes que nous avons développés, et par la suite d'imaginer de nouvelles architectures de générateur de chaos (figure 7), capables de combler les failles de sécurité qui auront été trouvées. Ces outils numériques ont pour but par exemple d'évaluer le spectre de Lyapunov pour ensuite en déduire la dimension de Lyapunov de l'attracteur, d'effectuer un calcul de spectre, d'auto–corrélation ou encore d'information mutuelle moyenne, afin de rechercher les traces dans les séries temporelles, donc dans le signal transmis, des paramètres "clé". Ces paramètres, s'ils peuvent être obtenus à partir de l'observation du signal chaotique, sont ensuite susceptibles d'être utilisés par un espion,



(a) Exemple de spectre de Lyapunov ; chaque valeur positive indique une direction de contraction de l'espace des phases



(b) Dimension de Lyapunov en 3 dimensions pour le chaos en longueur d'onde, en fonction des paramètres β et Φ

FIG. 8 – Résultat de calculs permettant d'estimer la dimension fractale des attracteurs chaotiques

pour construire un récepteur capable d'effectuer le décodage. Une des principales conclusions de ces premières études, est que la dynamique non linéaire scalaire n'est pas suffisante pour garantir une bonne sécurité. Mais nous nous sommes également aperçus que des dynamiques vectorielles [P11] à plusieurs non linéarités, plusieurs retards temporels, et plusieurs processus dynamiques (éq.(2)) semblent très bien contrecarrer ce défaut de cuirasse des premières dynamiques utilisées. Les dynamiques scalaires à retard constituent en fait l'expression la plus simple d'un générateur de chaos de grande complexité (voir figures 8), qu'il est donc très facile de modifier légèrement pour obtenir des dynamiques chaotiques plus robustes aux outils d'analyse actuels.

2.3.5 Dynamiques chaotiques et communications numériques

Codes CDMA générés par chaos. Un travail actuellement en cours, en collaboration avec V. Udaltsov, concerne l'application des dynamiques chaotiques générées par des systèmes non linéaires à retard, en vue de la génération de codes pseudo–aléatoires pour le CDMA. Le but de cette étude concerne le remplacement des codes de Gold utilisés et brevetés dans les communications par étalement de spectre. Des premières études ont confirmés des résultats publiés récemment par d'autres groupes, consistant à dire que les codes CDMA générés par dynamiques chaotiques seraient plus performants, entre autre en termes d'inter-corrélation (ce qui correspond pratiquement à la diaphonie entre canaux), et en termes de nombre maximum d'utilisateurs simultanés. Les recherches se poursuivent actuellement pour développer un schéma efficace de synchronisation de code chaotique.

Numérisation de la porteuse chaotique. Une autre aspect pratique lié aux transmissions numériques est actuellement à l'étude. Il s'agit de l'influence d'une numérisation du chaos [Ca15] utilisé en transmissions cryptées, sur le recouvrement de l'information après une conversion inverse numérique vers analogique. Cet aspect de la transmission cryptée par chaos est relié aux problèmes de bruits introduits sur le canal de transmission, problème qui est encore relativement peu abordé dans la littérature.

2.4 Encadrement de la recherche

Cette section regroupe les encadrements et co–encadrements d'étudiants de troisième cycle.

2.4.1 Stages de DEA

- 96/97, *Non linéarité de type fonction d'Airy pour la génération d'une dynamique non linéaire à retard sur la variable longueur d'onde* (J.-B. Cuenot).
  Ce premier stage de DEA a été co–encadré pendant mon année d'A.T.E.R. Le but était de démontrer la possibilité d'agir sur la clé de codage en changeant le type de fonction non linéaire. Dans le contexte de la cryptographie par chaos en longueur d'onde, changer cette fonction revenait à changer le profil du filtre spectral utilisé. Au lieu du filtre biréfringent utilisé pendant la thèse, c'est–à–dire un filtre interférentiel à deux ondes, il était proposé de mettre en évidence les spécificités rattachées à l'utilisation d'un filtre Fabry–Pérot, donc un filtre interférentiel à n ondes.
- 99/00, *Transmission en format binaire d'un signal crypté par chaos* (R. Gémayel).
  Ce sujet de recherche est en fait très vaste, et d'un grand intérêt pour la cryptographie par chaos. L'idée consiste à exprimer le fait qu'une des principales faiblesses de ce type de cryptage, réside dans la mise à disposition sur la ligne de transmission de l'ensemble de la dynamique chaotique à l'origine du codage. L'espion a alors la possibilité d'effectuer une analyse complète de ce signal chaotique pour essayer d'en extraire le déterminisme, et ensuite tenter le décodage. Une solution pour limiter ce pouvoir d'analyse, consisterait à limiter l'information disponible sur la ligne de transmission, à une forme minimale qui permettent encore le décodage à partir de la connaissance des paramètres clé du générateur de chaos, mais qui rende très difficile une quelconque analyse dynamique du signal transmis. Les résultats de ce stage ont permis d'apporter des réponses encourageantes, mais encore insuffisantes à ce problème crucial. Des travaux ultérieurs sur ce même sujet sont prévus.
- 00/01 *Stabilisation d'un grand chemin optique constitué par une fibre, par asservissement d'une condition d'interférence* (A. Ab Chaala).
  Dans le contexte d'une non linéarité optique obtenue grâce à des phénomènes de cohérence, il est nécessaire de contrôler précisément la phase optique. Ce contrôle est souvent implicite dans des interféromètres classiques, mais dans le cas d'un montage fibré à grand chemin optique, la phase absolue peut être amenée à fluctuer de manière très sensible, du fait de perturbation extérieur. Cette situation est rencontrée dans le montage expérimental de la thèse d'Éric Genin, et il a été envisagé de mettre en œuvre un contrôle actif de la longueur optique d'une grande longueur physique de fibre optique. Pour cela, il existe un certain nombre de techniques, dont une consiste à agir sur un cylindre piézo–électrique, autour duquel est enroulée la fibre en question.
- 00/01 Participation à l'encadrement d'un stagiaire de DEA en Mathématiques, Olivier Éveilleau, *Comportement des solutions d'une équation différentielle à retard utilisée en optronique*, encadré par Jacky Cresson du Laboratoire de Mathématiques de Besançon.
  Le sujet portait sur les théorèmes fondateurs dans l'étude des propriétés des solutions des dynamiques non linéaires scalaires à retard. Le sujet de ce stage de DEA est issu de discussions et de séminaires donnés en commun au laboratoire d'Optique et au laboratoire de Mathématiques à Besançon. Il est apparu au cours de ces discussions, que les fondements mathématiques qui permettent de décrire les systèmes différentiels non linéaires à retard, ne sont fait pas complètement maîtriser pour décrire correctement toutes les solutions observées dans la pratique.
- 01/02 *Caractérisation de la limite du débit de codage d'un générateur de chaos en longueur d'onde* (A. Pallavisini).
  L'origine de ce sujet se trouve dans l'exploration des limites de rapidité de la cryptographie par chaos en longueur d'onde. Cette limite est supposée se située, dans le générateur de chaos en longueur d'onde, au niveau de la diode laser DBR multi–électrode accordable.

La bande passante de l'accordabilité de ces composants est en effet limitée pour des raisons technologiques et physiques à quelques centaines de *MHz*. Le sujet de stage consiste à explorer cette limite, et à tenter de profiter des effets de dynamique fortement non linéaire pour générer des harmoniques de fréquence. On espère alors pouvoir élargir à environ $1GHz$, la largeur spectrale de la dynamique chaotique en intensité, qui est une image non linéaire de celle en longueur d'onde (limitée à quelques $100MHz$).

2.4.2 Doctorants

Les thèmes de recherche cités dans cette section, dans le cadre des thèses encadrées, ou en cours d'encadrement, ne sont pas détaillés. Ces informations ont en effet déjà été développées dans la partie 2.3 traitant des axes de recherche explorés après le doctorat.

1. *"Système opto-électronique de sécurisation par chaos en longueur d'onde"*, par Jean-Baptiste Cuenot à l'UMR 6603 GTL–CNRS Telecom Metz. Septembre 1997 – Mars 2002.
2. *"Transmission cryptée par chaos en intensité"* par Pascal Lévy à l'UMR 6603 GTL–CNRS Telecom Metz. Avril 1998, soutenance prévue fin 2002.
3. *"Transmission optique cryptée par chaos en modulation de cohérence"*, par Min Won Lee à l'UMR 6603 de Besançon. Octobre 1998 – Mars 2002.
4. *"Étude de la sensibilité au bruit d'une transmission cryptée par chaos"*, par Xavier Bavard à l'UMR 6603 GTL–CNRS Telecom Metz. Septembre 2000 –.
5. *"Générateur de chaos fibré à boucle de contre–réaction tout optique pour la génération de chaos de très forte dimension et large bande passante"* par Éric Genin, à l'UMR 6603 de Besançon. Octobre 2000 –.
6. *"Cryptographie par chaos très haut débit"* par Nicolas Gastaud à l'UMR 6603 GTL–CNRS Telecom Metz. Octobre 2001–
7. *"Crypto–analyse d'un système de transmission sécurisé par chaos"* par Alexandre Locquet à l'UMR 6603 GTL–CNRS Telecom Metz. Octobre 2001–

2.4.3 Jurys de thèse

J'ai bien sûr fait partie des jurys de thèse de **Jean–Baptiste Cuenot** (Mars 2002) et **Min Won Lee** que j'ai encadré *à Metz et Besançon*. J'ai également été sollicité pour être dans la jury de la thèse de **Stéphane Penaud** *à l'IRCOM Limoges*, en Avril 2001, et dont le sujet consistait en l'étude des performances de codes CDMA à partir d'oscillateurs chaotiques réalisant des dynamiques non linéaires à retard.

2.5 Participations à la vie de la communauté scientifique

J'ai eu la charge de "*référer*" plusieurs articles dans les revues scientifiques suivantes :

- Physics Letters A
- Electronics Letters
- Physical Review Letters
- European Physics Journal D
- Optics Letters
- Photonics Technology Letters

J'ai également participé à l'animation de diverses rencontres scientifiques, dans un but de diffusion, de promotion et de prospection de la recherche (Groupement de Recherche "Systèmes à retard", Action Spécifique AS03, "Physiques et signaux non linéaires", rencontres de travail du projet européen OCCULT, École de Physique des Houches).

2.6 Perspectives de recherche

Les thèmes de recherche dans le domaine de la cryptographie par chaos sont encore en plein développement, et de nouveaux axes apparaissent chaque année dans la littérature. Néanmoins, les axes principaux que nous souhaitons aborder dans les années à venir peuvent se résumer de la manière suivante.

La **crypto–analyse** est bien sûr un point essentiel qu'il est nécessaire de continuer à développer, afin de bien évaluer le degré de confidentialité que peut proposer les nouveaux systèmes de cryptographie par chaos. À titre d'exemples concrets, nous proposons des analyses systématiques de dimensions d'attracteur de manière comparative entre les différentes architectures des générateurs de chaos imaginés jusqu'ici. Une approche originale est également envisagée en vue de l'analyse des séries temporelles, elle concerne une utilisation des ondelettes dans l'étude des séries temporelles.

Le développement de nouvelles **techniques de synchronisation entre chaos** est également un point clé du développement des dynamiques chaotiques dans les systèmes de télécommunication (pour la sécurisation, mais aussi pour pour le CDMA). Une technique de synchronisation optimale devrait permettre d'améliorer la qualité du décodage, ainsi que la sensibilité de cette qualité par rapport au bruit transmis par le canal.

L'**influence du canal de transmission**, et plus généralement une approche des communications sécurisées par chaos au travers du formalisme de la théorie de l'information (en termes de capacité de canal, de quantité d'information minimum nécessaire à la synchronisation, etc ...) devrait permettre d'établir un certain nombre de fondements quantitatifs des différentes propriétés de la cryptographie par chaos.

Enfin, l'extension de la cryptographie par chaos au domaine des **signaux entièrement numériques** (implémentation des générateurs de chaos dans des DSP) devrait permettre de s'affranchir des problèmes actuels de limitation de la qualité de décodage, du fait des inévitables désaccords entre les paramètres de l'émetteur et du récepteur. Mais ce travail pourrait aussi permettre un rapprochement bénéfique entre la cryptographie algorithmique traditionnelle, et la cryptographie par chaos.

3 Synthèse des activités d'enseignement

3.1 Natures disciplinaires des enseignements

Les diverses disciplines enseignées couvrent à la fois les sciences de l'ingénieur, et la physique générale. J'ai en effet eu la chance d'avoir à faire des enseignements très variés, tant du point de vue des domaines visités (optique géométrique et physique, Physique générale du CAPES Physique–Chimie, électronique et électro–cinétique, traitement numérique du signal, télécommunications optiques, physique ondulatoire), que du niveau des enseignements (DEUG STU-SV, STPI, SM, licence EEA, Physique, Sciences Physiques, CAPES Physique–Chimie, maîtrise EEA et de Sciences Physiques, DEA filière Optique).

Tous ces enseignements, outre l'apport humain, ont bien sûr permis d'acquerrir aussi un certain recul dans les activités de recherche, par rapport aux connaissances de base en Physique générale et Sciences pour l'Ingénieur.

3.2 Créations de documents pour l'enseignement

L'enseignement effectué ne s'est bien sûr pas limité à la reproduction d'enseignements pré–existants. Un apport personnel peut être évalué au travers de divers documents réalisés, à partir de documentations et réflexions personnelles sur les sujets abordés en cours, TD, et TD.

- Polycopié de cours sur les bases théoriques de traitement du signal (Maîtrise EEA), disponible sur le serveur "Corpus" du réseau interne de l'université.
- Polycopié de cours en Télécommunications Optiques (Maîtrise EEA, aspects physiques des guides d'onde optique, et en cours d'élaboration, généralités technologiques sur les transmissions par fibre optique)
- Textes de TP d'Optique (Licence EEA, Maîtrise de Sciences Physiques, anciens texte de la filière physique, actualisés et adapté à la filière EEA)
- Textes de TP d'Électronique (DEUG STPI) crées ou actualisés, et adaptés à certaines filières (en libre accès sur serveur "Corpus" également)

L'enseignement traditionnel s'est accompagné aussi d'une volonté d'encadrement plus rapproché des étudiants, dans le cadre de projets ou de stages. Outre l'intérêt humain, ce type d'enseignement a permis dans certains cas de favoriser la venue d'étudiant au laboratoire, dans le cadre de poursuites d'étude en troisième cycle. L'encadrement d'étudiants en projet ou stage est réellement apparu comme un moyen d'attirer des candidats en DEA puis en thèse.

3.3 Encadrement de projets

Licence EEA :

98/99, Système électronique de simulation du phénomène d'interférence (Bourgeat/Didiot). Ce projet a donné lieu à la création d'un nouveau TP destiné aux étudiants de licence EEA, et permettant d'aborder la plupart des notions intervenant dans le phénomène d'interférence (excepté la cohérence spatiale). Le principe consiste à montrer le phénomène d'interférence, non pas comme une intensité moyenne (visible) de l'amplitude résultant de la superposition de deux ondes lumineuse monochromatiques (invisibles), mais comme le résultat d'une chaîne de traitement du signal qui réalise les opérations de base de l'interférence sur un signal électronique temporel (division d'un signal, décalage relatif dans le temps, re-combinaison de ces signaux, mise au carré pour en extraire une image énergétique, puis filtrage par un passe–bas pour récupérer la valeur moyenne de l'énergie). Cette approche électronique ou encore "signal", du phénomène physique d'interférence, est supposée plus adaptée au public des filières EEA. D'un point de vue plus global, elle permet aussi pour un plus large public d'étudiants en physique, d'observer temporellement les opérations

mathématiques intervenant dans le calcul d'un phénomène physique d'interférence. Ce TP a par ailleurs fait l'objet d'un développement "pré–série" dans une nouvelle société (SARL Dida Concept, Pascal Ney) proposant des TP "clé en main" dans le secondaire et le supérieur.
98/99, Le Photo-détecteur (Molnar/Bonnemaille)
99/00,Étage transimpédance large bande en composants discrets pour détection de lumière par photo-diode PIN (Vuillemin/Dubois), Compensation des imperfections d'une ligne à retard analogique (Lemercier/Voisard)

Maîtrise EEA :

99/00, Système de comptage du nombre de passage en phase entre 2 signaux décalés en fréquence par effet Doppler (Gillet/Bourgeois).
99/00, Cryptage par chaos numérique sur des EPLD (Bourgeat/Didiot).
00/01, Détection et mesure d'extrema sur un signal électronique pseudo-aléatoire (Nkondjo/Pong Tchoffo).
01/02 Réalisation d'une liaison optique de transmission numérique de données (Hamnache/Martins).

Licence de Physique :

00/01, Caractéristiques statiques d'un laser YAG pompé par diode (Moreira/Moingeon), Étude théorique et expérimentale des traitements optiques par couches minces diélectriques (Ligier)

Maîtrise de Physique :

99/00, (co-encadrement) Système d'acquisition par caméra CCD pour l'étude de la cohérence spatiale d'une source lumineuse (Alnaboulsi/Bendoula).
00/01, (co-encadrement) principe et réalisation de mesure optique par ellipsométrie (Coda)

3.4 Encadrement de stages

- 99/00, *Conception et réalisation d'un module laser accordable en fréquences optiques permettant de faire du multiplexage en longueur d'onde* (É. Genin, ENSP Strasbourg, stage de 2$^{\text{ème}}$ année d'école d'ingénieur). Éric Genin est actuellement en thèse sous ma responsabilité. Le module laser réalisé a permis de disposer au laboratoire d'une source laser semi-conductrice fibrée, mono-mode, et accordable, puisqu'il s'agit d'un laser DBR multi-électrode comme celui utilisé dans l'expérience de cryptage par chaos en longueur d'onde. Ce laser a pu servir ensuite dans des expériences de cryptage quantique, de caractérisation d'impulsion optique par mélange quatre ondes dans des fibres, ainsi dans une expérience destinée à réaliser une source hyperfréquence ultra–stable accordable, à partir d'un oscillateur opto-électronique.
- 00/01, *Dépendance de l'hystérésis d'une bifurcation de Hopf sous–critique d'un système non linéaire à retard, vis–à–vis des paramètres dynamiques* (R. Fischer, ENS Paris, stage de 2$^{\text{ème}}$ année de Magistère). Ce stage expérimental était destiné à explorer de manière systématique les bifurcations par perte de stabilité d'un point fixe dans un oscillateur électronique non linéaire à retard, qui avait été initialement mis au point pour démontrer expérimentalement l'existence du cas de la bifurcation de Hopf sous–critique dans un tel système dynamique.

3.5 Responsabilités administratives dans l'enseignement

Les principales responsabilités d'enseignement sont détaillées ci-dessous.

Responsable de la salle de travaux pratiques d'Optique : gestion de l'occupation de la salle, planification de la ré–organisation de ces salles lors des travaux de rénovation en 2001 ; gestion du matériel pédagogique ; achat de matériels d'enseignement.

Secrétaire adjoint de la commission de Physique (1998–2002) de l'UFR Sciences et Techniques, mise en place d'un tableau de gestion des services d'enseignement en Physique.

4 Administration de la recherche

Bien que l'administration de la recherche soit *a priori* un frein aux activités "brutes" de recherche, elles sont rapidement et de manière assez évidente apparues nécessaires et profitables, afin de disposer de moyens de recherche. Ce besoin de "moyens" est à Besançon une réelle nécessité, compte tenu de la tradition du laboratoire de produire des travaux de recherche appuyés de manière aussi systématique que possible par des résultats expérimentaux.

4.1 Gestion et prospection de contrats de recherche

Pendant la thèse, le contrat de recherche dans le cadre de l'appel d'offre "Fonctions Optiques Nouvelles pour les Télécommunication" a été honoré par la réalisation du démonstrateur de cryptage par chaos en longueur d'onde, et par la rédaction de 3 rapport intermédiaires, et un rapport final.

Je me suis occupé de la gestion scientifique d'un contrat ANVAR sur la période 98/00 ($200k$F), concernant la réalisation d'un système de cryptage par chaos pour les télécommunications hertziennes hyper–fréquence. Outre la réalisation d'un démonstrateur, un rapport final a été rédigé.

J'ai participé à l'élaboration d'un projet de contrat européen qui a débuté en Septembre 2001, sur 3 années (montant total : $1.35M$€ dont $300k$€ pour l'UMR 6603). Ce contrat est actuellement en cours, j'ai effectué deux présentations lors des deux premières réunions de travail semestrielles, je me suis également occupé de la rédaction des rapports correspondants.

4.2 Animation de la vie interne du laboratoire

Une importante et régulière participation a été prise lors des campagnes d'achat de matériel de laboratoire à usage général et particulier, sur les sites de Besançon, et de Metz. Ce travail, exigeant en temps et en effort (définition des spécifications techniques du matériel, prospection et mise en concurrence, négociations des tarifs sur plusieurs semaines, ...), s'est révélé très payant, surtout dans un laboratoire très orienté vers les réalisations expérimentales. À titre d'exemple, citons le matériel suivant concerné par ces campagnes d'achat : matériel d'usage général, composants électroniques, alimentations diverses, modulateurs et détecteurs opto-électroniques large bande, appareils de mesure haut de gamme (oscilloscope $4GHz$, compteur de taux d'erreur, analyseur de spectre optique), pour un montant global de l'ordre de $100k$€ par an sur ces 4 dernières années.

J'ai participé à l'animation et à l'**organisation de mini-séminaires** inter–disciplinaires sur le thème très général "Systèmes Mathématiques et Physiques" (Novembre-Décembre 2000) dans le cadre de l'Institut des Micro-techniques et de la collaboration avec le laboratoire de Mathématiques de Besançon.

Enfin, je suis actuellement **membre élu du Conseil de Laboratoire**.

4.3 Diffusion des recherches en direction du public

Pour participer à la connaissance des activités du laboratoire à l'extérieur, citons deux actions particulières :

- Une conférence a été donnée auprès des étudiants de l'Université, au sein du Projet Aurore de l'Université de Franche-Comté. Elle était intitulée "Applications des dynamiques chaotiques à la sécurisation de l'information" (Avril 2001).
- Il nous a été demandé la rédaction d'un article de vulgarisation afin d'expliquer à un public d'opticiens du monde de la recherche et de l'industrie, les principes de la cryptographie par

chaos qui ont été développés au laboratoire. Cet article a été publié dans le premier numéro (Mars 2001) de la nouvelle revue de la Société Française d'Optique, "Photonique".

- Une **vidéo** a été réalisée (Juillet 96) afin d'illustrer de manière parlante et vivante, d'une part les phénomènes de bifurcations et de route vers le chaos observés avec le générateur de chaos en longueur d'onde, et d'autre part le fonctionnement pratique sur un signal musical de la cryptographie optique par chaos en longueur d'onde. Cette vidéo a participé en 1998 au concours CNRS du film scientifique.

5 Liste des publications

5.1 Articles dans des revues à comité de Lecture

P1 L. Larger, J.-P. Goedgebuer, J.M. Mérolla, "Chaotic oscillator in wavelength : a new set-up for investigating differential difference equations describing non linear dynamics", IEEE Journal of Quantum Electronics, Vol.34, n°4, pp. 594–601 (April 1998)

P2 J.-P. Goedgebuer, L. Larger, H. Porte, "An optical cryptosystem based on replication of hyperchaos and wavelength-induced nonlinearities", Physical Review Letters, Vol.80, n°10, pp. 2249–2252 (March 1998)

P3 J.-P. Goedgebuer, L. Larger, H. Porte, F. Delorme, "Chaos in wavelength in a tunable feedback laser diode", Physical Review E, Vol.57, n°3, pp. 2795–2798 (March 1998)

P4 L. Larger, J.-P. Goedgebuer, F. Delorme, "An optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator", Physical Review E, Vol.57, n°6, pp. 6618–6624 (June 1998)

P5 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, n°3, pp. 199–200 (February 2000)

P6 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, n°9, pp. 1892–1895 (February 2001)

P7 L. Larger, V.S. Udaltsov, J.-P. Goedgebuer and W.T. Rhodes, "Radio transmission system using FM-high dimensional chaotic oscillator", Electronics Letters, Vol.37, n°9, pp. 594-595 (April 2001)

P8 J.-B. Cuenot, L. Larger, J.-P. Goedgebuer and W. T. Rhodes, "Chaos Shift Keying with an optoelectronic encryption system using chaos in wavelength", IEEE Journal of Quantum Electronics, Vol.37, n°7, pp. 849–855 (July 2001)

P9 L. Larger, M. W. Lee, J.-P. Goedgebuer, T. Erneux and W. Elflein, "Chaos in coherence modulation : bifurcations of an oscillator generating optical delay fluctuations", JOSA B, Vol.18, n°8, pp. 1063–1068 (August 2001)

P10 V.S. Udaltsov, J.-P. Goedgebuer, L. Larger and W.T. Rhodes, "Dynamics of nonlinear feedback systems with short time delays", Optics Communications, Vol.195, pp. 187–196 (August 2001)

P11 V.S. Udaltsov, L. Larger, J.-P. Goedgebuer, W.T. Rhodes, M. W. Lee and É. Genin, "Chaotic bandpass communication system", IEEE Trans. On Circuits And Systems (à paraître, Juillet 2002)

P12 J.-P. Goedgebuer, P. Levy, L. Larger, C.C. Chen and W.T. Rhodes , "High bandwidth chaotic encryption system", IEEE Journal of Quantum Electronics, Special Issue on Optical Chaotic Cryptography (accepté, 2002)

P13 M.W. Lee, L. Larger and J.-P. Goedgebuer, "Encryption system using chaotic delays between lightwaves", Physical Review Letters, (soumis, Mars 2002)

P14 L. Larger, T. Erneux and J.-P. Goedgebuer, "Experimental and analytical investigation of sub–critical Hopf bifurcation in time delayed dynamics", Physical Review E, (soumis, Août 2002)

5.2 Brevets

B1 L. Larger, J.-P. Goedgebuer, H. Porte, P.-L. François, "Système de transmission optique mettant en oeuvre un cryptage par chaos déterministe", Brevet FR 2743459 (Janvier 96, France Telecom), Brevet étendu à DE, UK et USA.

B2 J.-P. Goedgebuer , L. Larger, J.-M. Mérolla "Dispositif de cryptage de signaux par hyperchaos pour la sécurisation de l'information dans les réseaux optiques", Brevet n°9806892 (Juin 98, France Telecom). Brevet étendu à DE, UK et USA.

B3 V. Udaltsov, L. Larger, J.-P. Goedgebuer, "Dispositif de codage de signaux pour les radiocommunications", Brevet n°9907831 (Juillet 99, France Telecom). Brevet étendu à DE, UK et USA.

5.3 Communications avec actes

Ca1 J.-P. Goedgebuer, L. Larger, "Secure optical telecommunication using chaos for signal transmission", Proc. 1st International Conference on Theory and Apllication of Cryptology, PRAGOCRYPT, Prague (CTU Publishing House, pp.II.1-II.9, Octobre 96) – ***Conférence invitée***

Ca2 J.-P. Goedgebuer, L. Larger, H. Porte, "Signal encryption using optical hyperchaos" , EQEC' 98, Technical Digest, pp. 35-37 Glasgow (Septembre 98) – ***Conférence invitée***

Ca3 J.-P. Goedgebuer, L. Larger, W.T. Rhodes, "Chaos begins to communicate" , 6^{th} Latin American Meeting on Optics, Lasers and their Applications, SPIE, Cartagène, Colombie (Octobre 98) – ***Conférence invitée***

Ca4 J.-P. Goedgebuer, L. Larger, J.-B. Cuenot, "Fiber telecommunication using chaos for secure signal transmission", Actes du $15^{\text{ème}}$ Colloque Optique Hertzienne et Diélectrique (OHD'99), pp.C17–C20 (Septembre 99) – ***Conférence invitée***

Ca5 J.-P. Goedgebuer, V. Udaltsov, L. Larger, W.T. Rhodes, "Communication using synchronized hyperchaos" , Proc. 12^{th} IEEE LEOS Annual Meeting (LEOS'99) San Francisco (Novembre 99), vol.2, pp.441–442 – ***Conférence invitée***

Ca6 L. Larger, J.-P. Goedgebuer, "Cryptage de signaux par chaos en longueur d'onde", $3^{\text{ème}}$ Rencontres du Non Linéaire, Institut Poincaré, Paris, (9–10 Mars 2000), ISBN 2-87800-154-0, pp. 1–6 – ***Conférence invitée***

Ca7 M. W. Lee, L. Larger, J.-P. Goedgebuer and W. Elflein, "Dynamique chaotique sur un retard optique dans un schéma de modulation de cohérence", $3^{\text{ème}}$ Rencontres du Non Linéaire, Institut Poincaré, Paris, (9–10 Mars 2000), ISBN 2-87800-154-0, pp.117–122

Ca8 J.-P. Goedgebuer, L. Larger, "Chaos in wavelength", Technical Digest of the annual OSA Meeting 2000, Providence, USA – ***Conférence invitée***

Ca8 L. Larger, T. Erneux, M. W. Lee, and J.-P. Goedgebuer, "Super and sub-critical Hopf bifurcation leading to chaos : theory and experiments", CLEO/Europe-IQEC 2000, Nice, France, ISBN 0-7803-6318-3, p.148 (September 2000)

Ca9 L. Larger, T. Erneux, M.W. Lee, J.-P. Goedgebuer "Bifurcations de Hopf super- et sous-critique des systèmes dynamiques non linéaires à retard : expériences et analyse perturbative ", $4^{\text{ème}}$ Rencontres du Non Linéaire, Institut Poincaré, Paris, (15-16 Mars 2001), pp.153–158

Ca10 M.W. Lee, L. Larger, J.-P. Goedgebuer "Dynamique non linéaire à deux retards temporels", $4^{\text{ème}}$ Rencontres du Non Linéaire, Institut Poincaré, Paris, (15–16 Mars 2001), pp.159–164

Ca11 M.W. Lee, L. Larger, J.-P. Goedgebuer "New non-linear dynamical system with 2 time delays", Focus Meeting 2001 CLEO/Europe–IQEC, p.241, Munich, Allemagne, (Juin 2001)

Ca12 M.W. Lee, L. Larger, J.-P. Goedgebuer "Secure optical communication using chaotic coherence modulation", Focus Meeting 2001 CLEO/Europe–IQEC, p.184, Munich, Allemagne (Juin 2001)

Ca13 L. Larger, T. Erneux, J.-P. Goedgebuer "Démonstration expérimentale d'une bifurcation de Hopf sous–critique dans un système à retard", $5^{\text{ème}}$ Rencontres du Non Linéaire, Institut Poincaré, Paris, (14–15 Mars 2002), pp.113–118

Ca14 É. Genin, L. Larger, J.-P Goedgebuer "Générateur de chaos optoélectronique dans une cavité en anneau fibrée", 5ème Rencontres du Non Linéaire, Institut Poincaré, Paris, (14–15 Mars 2002), pp.91–96

Ca15 X. Bavard, L. Larger, J.-P. Goedgebuer "Influence de la numérisation sur la synchronisation de données dans un système de transmission sécutisé par chaos", 5ème Rencontres du Non Linéaire, Institut Poincaré, Paris, (14–15 Mars 2002), pp.13–18

Ca16 L. Larger, J.-P. Goedgebuer, T. Erneux "Sub–critical Hopf bifurcation in a time–delayed differential dynamic", 7th Experimental Chaos Conference, San Diego, Californie USA (25–29 Août 2002)

5.4 Communications sans acte

C1 A. Fischer, J.-P. Goedgebuer, L Larger, "Demonstration of multistability in wavelength in tunable laser diodes", Proc. European Quantum Electronics Conference, EQEC 94, Amsterdam, (Août 1994)

C2 J.-P. Goedgebuer, L. Larger, "Optical chaos in wavelength for secure communication", 3rd International Conference on Correlation Optics, State University of Chernovtsi, Ukraine (20-23 Mai 97) – ***Conférence invitée***

C3 L. Larger, J.-P. Goedgebuer, F. Delorme, "First demonstration of optical cryptography using chaos in wavelength", Annual Meeting OSA'97, Long Beach, Californie, USA (12-17 Octobre 97)

C4 C. C. Chen, H. Porte, L. Larger, J.-P. Goedgebuer, "Polarization independant LiNbO3 Mach-Zehnder modulator using TE-TM phase trimming by laser ablation " , Annual Meeting OSA'97, Long Beach, Californie, USA (12-17 Octobre 97)

C5 J.-P. Goedgebuer, L. Larger, H. Porte, "Signal encryption using chaos in wavelength", French–UK Meeting on Optoelectronics, Lille (Octobre 97) – ***Conférence invitée***

C6 J.-P. Goedgebuer, L. Larger, "Synchronization of hyperchaotic laser devices", dans 10th Conference on Laser Optics, St-Petersbourg, Russie (Juin 98)

C7 J.-P. Goedgebuer, L. Larger, "Optical cryptography using chaos in wavelength", XXVIth INAOE, Puebla, Mexique, (Novembre 98) – ***Conférence invitée***

C8 J.-B. Cuenot, P. Levy, L. Larger and J.-P. Goedgebuer, "Transmission de signaux par chaos sur fibre optique", 19ème JNOG, Limoges, Décembre 1999

C9 J.-P. Goedgebuer, V. Udaltsov, L. Larger, "Chaos for communicating", dans 11th Conference on Laser Optics, St-Petersbourg, Russie (Juin 2000) – ***Conférence invitée***

C10 J.-P. Goedgebuer, L. Larger, "chaos in Optics", Xth National Meeting on Optics, Armenia, Colombie (Septembre 2000) – ***Conférence invitée***

C11 V. Udaltsov, J.-P. Goedgebuer, L. Larger, "Nonlinear chaotic systems with short time delays", Optics for the Next Millenium, St–Petersbourg, Russie (Octobre 2000) – ***Conférence invitée***

C12 M.W. Lee, L. Larger, J.P. Goedgebuer "Mise en œuvre à des fins de cryptage d'un générateur de retard optique chaotique", 20ème JNOG Toulouse, (Octobre 2000)

C13 J.-P. Goedgebuer and L. Larger, "Chaos in systems governed by difference-differential equations, or how it is possible to encrypt data for optical and wireless telecommunication", From Gama Ray Optics to Semiconductor Laser Dynamics, Bruxelles, 6–7 Avril 2001 – ***Conférence invitée***

C14 L. Larger, J.-P. Goedgebuer, "Experimental and numerical investigations of time delayed optoelectronic oscillators : dynamics and application to secure optical telecommunication", International SIAM conference on dynamical system DS01, Snowbird, Utah, USA (20-24 Mai 2001), mini-symposium on Delay Differential Equations in Non-Linear Optics – ***Conférence invitée***

C15 J.-P. Goedgebuer, L. Larger, P. Levy, "Optical cryptosystem for high bit rate telecommunications", Photonic West SPIE Conference, San Jose, California, (Janvier 2002) – ***Conférence invitée***

5.5 Séminaires

S1 J.-P. Goedgebuer, L. Larger, "Controlled chaos for secure optical communications", Université de Nuremberg-Erlangen, Allemagne (Mai 96)

S2 J.-P. Goedgebuer, L. Larger, "Du chaos aux télécommunications cryptées", Laboratoire de Photonique Quantique et Moléculaire, ENS Cachan (Janvier 97) – ***Séminaire invité***

S3 J.P. Goedgebuer, L. Larger, A. Fischer, " Commutation en longueur d'onde pour le routage et le cryptage de signaux ", dans Réunion France Telecom "Nouvelles Fonctions Optiques" CNET Lannion (Juin 97)

S4 J.P. Goedgebuer, L. Larger, "Cryptage de signaux par chaos en longueur d'onde", au CNET Bagneux (Octobre 97) – ***Séminaire invité***

S5 J.P. Goedgebuer, L. Larger, "A new approach to chaos for secure communication", Georgia Tech University, Atlanta, USA (Décembre 98)

S6 L. Larger, J.P. Goedgebuer, "Cryptage optique par chaos en longueur d'onde", Séminaire laboratoire de photophysique moléculaire, Univ. Paris XI, Orsay (26 Mai 2000) – ***Séminaire invité***

S7 L. Larger, J.P. Goedgebuer, J.-B. Cuenot, P. Levy, M. W. Lee, "Dynamiques non linéaires à retard en régime chaotique : application aux télécommunications cryptées", GdR Automatique, Systèmes à Retard, ENSAM Paris (19 Octobre 2000) – ***Séminaire invité***

S8 L. Larger, J.P. Goedgebuer, "Applications des dynamiques chaotiques à la sécurisation de l'information", Projet Aurore, conférence de vulgarisation des travaux de recherche au sein de l'université de Franche-Comté, 5 Avril 2001, Faculté de Médecine de Besançon

5.6 Article de vulgarisation

L. Larger, J.-P. Goedgebuer, "Dynamiques chaotiques appliquées à la cryptographie", *Photoniques* (revue de la Société Française d'Optique), n°1, 1er trimestre 2001, pp. 20–23

L. Larger, J.-P. Goedgebuer, "Le chaos chiffrant", *Pour La Science* (hors série sur la cryptographie), à paraître, Août 2002

5.7 Support de diffusion de la recherche

Film vidéo "Les télécommunications optiques cryptées par chaos", (12 *min.*), largement diffusé dans de nombreuses conférences internationales, et déposée en 1998 au concours CNRS du film Scientifiques. Cette vidéo est actuellement (Mai 2002) en cours de numérisation et de montage pour la réalisation d'un document multimédia.

6 Annexes

Publications dans des revues à comité de lecture

Brevets