

## Interféromètre radio-fréquence réalisé en optoélectronique, application aux communications sécurisées par chaos

A. Pallavisini, L. Larger, V. Udaltsov  
GTL-CNRS Telecom / UMR FEMTO-ST 6174  
2-3, rue Marconi  
57070 Metz  
apallavi@georgiatech-metz.fr

### Résumé

Les premiers systèmes de cryptographie par chaos en électronique étaient pénalisés en termes de niveau de confidentialité par la faible dimension de la dynamique chaotique utilisée : une réalisation électronique du système de Lorenz. Des systèmes optiques ont ensuite permis un renouveau de cette application originale, grâce à l'utilisation de dynamiques non linéaires à retard, dont les dimensions d'attracteur étrange peuvent atteindre plusieurs centaines. Nous proposons une transposition originale dans le domaine des radio-fréquences, de ces dynamiques optiques à retard appliquée à la cryptographie par chaos.

### Abstract

*The first chaos based cryptographic systems suffered in terms of security from the low dimensional chaos initially involved: a Lorenz-type electronic oscillator. Later, optical demonstrators gave a second impulse to the field of chaos secure communications through the use of nonlinear delay dynamics to provide chaotic oscillations; chaotic attractor dimensions of several hundreds were achieved. We propose an original transposition of the same principles in the field of radio-communication systems.*

## 1 Introduction

Une dynamique non linéaire à retard peut être assez simplement réalisée en organisant quelques éléments clés en boucle d'oscillation : une transformation non linéaire, un retard temporel en général grand devant le temps caractéristique de la dynamique limitante (e.g. un filtre linéaire), et un amplificateur rebouclé sur la fonction non linéaire. Dans la perspective d'une réalisation expérimentale, le principal problème réside en général dans la manière de mettre en œuvre la transformation non linéaire. Une solution élégante et efficace retenue dans de nombreux montages optiques consiste en l'utilisation d'un interféromètre accordable par voie électro-optique [1], ou optoélectronique [2]. Dans le cas le plus simple d'un interféromètre à deux ondes, nous obtenons une fonction non linéaire périodique de type *sinus*. De plus l'utilisation, d'une fibre optique permet très facilement de réaliser un retard temporel correspondant au temps de propagation dans la longueur de la fibre. Nous avons cherché à appliquer ces mêmes principes au domaine de l'électronique radio-fréquence (RF). Le but final est de montrer la faisabilité d'un système de communication radio à base d'une porteuse chaotique de très grande dimension, grâce à l'utilisation d'une dynamique à retard réalisée dans le domaine RF.

Toutefois, le passage de l'optique à l'électronique RF n'est pas immédiat, du fait de la grande différence des ordres de grandeur mis en jeu lors d'un phénomène d'interférence. Là où une distance physique de l'ordre du micron suffit à faire passer la

condition d'interférence de destructif à constructif dans le domaine optique (fréquences de l'ordre 200 THz), plusieurs dizaines de centimètres sont nécessaires dans le domaine radio (si  $f = \omega/(2\pi) \simeq 1$  GHz, comme dans le cas qui nous concerne). La méthode de balayage dynamique de cette interférence —typiquement en  $\sin^2(\omega\Delta/c)$  où  $\Delta$  est la différence de marche entre les deux chemins de l'interféromètre— doit également être adaptée par rapport à la situation optique (pour laquelle des phénomènes électro-optiques sont utilisés pour agir sur  $\Delta$ ). Il sera en effet plus judicieux d'agir sur la fréquence RF  $f = \omega/(2\pi)$  pour balayer la fonction *sinus*: la fréquence devenant une variable dynamique, nous serons amenés à réaliser une dynamique chaotique en modulation RF de fréquence (FM).

## 2 Description de l'oscillateur chaotique en fréquence

Dans le domaine des applications domestiques, la majorité des transmissions hertziennes sont effectuées pour des fréquences égales à 433 MHz; elles sont entre 900 MHz et 2 GHz pour la téléphonie mobile, et à des fréquences beaucoup plus importantes pour des transmissions par satellites. Nous nous sommes attachés à la réalisation d'un oscillateur chaotique FM dans une gamme de fréquences entre 1 GHz et 1.5 GHz, donc a priori utilisable dans le cas de la téléphonie mobile.

### 2.1 Synoptique de l'ensemble de l'oscillateur

Le générateur de chaos en fréquence représenté à la figure 1(a) est constitué d'une fonction non-linéaire, d'un retard temporel, d'un filtre passe-bande, d'un amplificateur à gain variable, et d'un convertisseur tension / fréquence (VCO sur la figure) permettant d'obtenir la variable dynamique (la fréquence) à partir d'une tension issue de la chaîne d'oscillation électronique. Ces fonctions sont organisées en une boucle fermée formant ainsi un oscillateur, avec lequel nous espérons atteindre des régimes chaotiques lorsque le gain de la boucle d'oscillation est suffisamment élevé (excitation d'une plage suffisamment non linéaire de la fonction d'interférence).

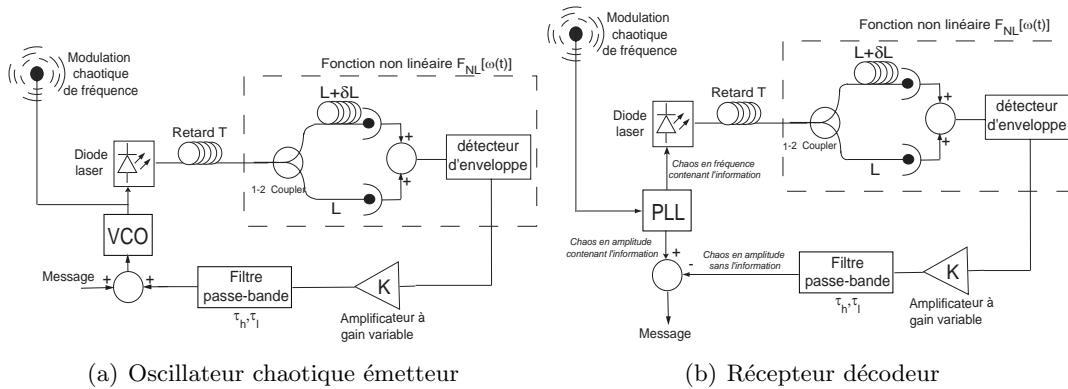


FIG. 1 – Synoptique du système de communication radio sécurisé par chaos

### 2.2 Interférences RF opto-électroniques

Les interférences RF réalisent la fonction non-linéaire  $v(t) = F[\omega(t)]$ , où  $\omega$  est la pulsation RF fournie par le VCO (correspondant à des fréquences de l'ordre de 1.5 GHz),

et  $v$  est une tension issue de la détection d'une valeur moyenne de l'interférence. Comme déjà indiqué, la condition d'interférence est modifiée en modulant la fréquence RF. L'amplitude de cette modulation est limitée avec les composants utilisés à une centaine de MHz, et cette limite conjuguée à la contrainte de pouvoir balayer plusieurs extrema de la fonction d'interférence en *sinus*, impose la géométrie de l'interféromètre en termes de différence  $\delta L$  de longueur de bras de l'interféromètre. Avec les valeurs numériques données ( $f_0 = \omega_0/(2\pi) \simeq 1.5$  GHz et  $\Delta f = \Delta\omega/(2\pi) \simeq 100$  MHz), il est nécessaire d'avoir environ 5 m de différence de marche entre les 2 bras de l'interféromètre. Ces bras sont pratiquement réalisés par des coupleurs optiques fibrés et des fibres optiques. L'extrémité de chaque bras est terminée par une photodiode afin de récupérer la modulation RF de l'onde optique, qui provient initialement du signal RF (sortie FM du VCO) appliqué en modulation directe d'une diode laser (voir la figure 1(a)). À la sortie des photodiodes, le moyennage des interférences RF est réalisé par un détecteur d'enveloppe quadratique, qui gomme la porteuse RF pour ne conserver pratiquement que les composantes fréquentielles dite "de la bande de base", et liées à la vitesse de la modulation FM.

La fonction non linéaire  $F[\omega]$  est finalement de la forme :

$$F[\omega] = \frac{\kappa^2 V_0^2}{4} \left\{ 1 + \cos \left[ \frac{2n \delta L}{c} \cdot \omega \right] \right\} = \frac{\kappa^2 V_0^2}{4} \left\{ 1 + \cos \left[ \frac{2n \delta L}{c} \cdot \Delta\omega + \phi \right] \right\}, \quad (1)$$

où  $\kappa$  est un gain opto-électronique prenant en compte les divers coefficients de conversion entre l'électronique et optique à l'entrée et à la sortie de la partie optique de l'interféromètre. La fréquence angulaire instantanée du signal FM produit par le VCO est notée  $\omega(t) = \Delta\omega(t) + \omega_0$ , où  $\omega_0$  est la pulsation RF centrale et  $\Delta\omega(t)$  est la déviation. Le paramètre  $\phi = 2n \delta L \omega_0 / c$  est un déphasage réglable par l'intermédiaire de la fréquence centrale du VCO.

### 2.3 Définition des paramètres temporels et de l'amplification du système

L'extension spectrale du signal en "bande de base" de l'oscillateur (le spectre des variations de fréquences), est typiquement déterminé par deux éléments : d'une part il y a la dynamique limitante de la chaîne d'oscillation, c'est-à-dire le filtre passe-bande dont le rôle est d'atténuer toutes les composantes spectrales en dehors de sa bande ; et d'autre part, il y a le gain de la boucle d'oscillation qui, au contraire, a pour but d'amplifier toutes les fréquences présentes dans la boucle, en leur donnant une amplitude suffisante pour exciter au travers des effets non linéaires de la fonction d'interférence, de nouvelles composantes spectrales en dehors de la bande passante du filtre. Plus le gain est élevé, plus le spectre d'une dynamique chaotique est étendu, résultat de la compétition entre le filtrage "dissipatif" de fréquences élevées, et la non linéarité génératrice de fréquences harmoniques. La dynamique limitante correspond pratiquement à un filtre électronique passe-bande du second ordre, dont les fréquences de coupure basse et haute sont respectivement  $(2\pi\tau_1)^{-1} = 10$  kHz et  $(2\pi\tau_2)^{-1} = 5$  MHz.

Le retard temporel  $T$  quant à lui, a un rôle qui peut être interprété de diverses manières. C'est tout d'abord une mémoire intrinsèque de l'oscillateur, qui lui confère son caractère de dynamique à espace des phases infini. Il doit être grand devant le temps caractéristique  $\tau_2$  correspondant à la coupure haute de la dynamique limitante passe-bande, de manière à pouvoir contenir un nombre important d'oscillations élémentaires de durée  $\tau_2$ . C'est aussi un retard, qui lorsqu'il est grand devant  $\tau_2$ , définit un grand nombre

de modes propres d'oscillation (un retard est linéairement déphasant, et si  $T \gg \tau_2$ , il y a un grand nombre de fréquences qui peuvent être en phase après un tour dans la boucle d'oscillation). Ce retard est réalisé dans la partie optique du montage, à l'aide d'une fibre optique de 2 km permettant d'obtenir un retard  $T = 10 \mu\text{s} \gg \tau_2 = 30 \text{ ns}$ .

## 2.4 Modèle dynamique de l'oscillateur

L'ensemble des éléments décrits précédemment est placé en boucle fermée. Le système est ainsi caractérisé par une équation différentielle non-linéaire à retard de la forme :

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

où  $\beta$  est un gain normalisé comprenant les différents facteurs de conversion (bande de base, FM, optique, électrique, ...) et les différents gains électroniques. Par l'intermédiaire d'un amplificateur à gain variable dans la boucle d'oscillation, il est possible de contrôler linéairement ce gain normalisé, et ainsi d'explorer les différents régimes dynamiques possibles en fonction de gain.

## 3 Comportements dynamiques

### 3.1 Diagrammes de bifurcation

Afin d'éprouver la validité du modèle dynamique relativement simple de l'équation (2), nous avons relevé des diagrammes de bifurcation expérimentaux en fonction du paramètre  $\beta$  "gain de la boucle", et pour deux valeurs différentes du paramètre  $\phi$ .

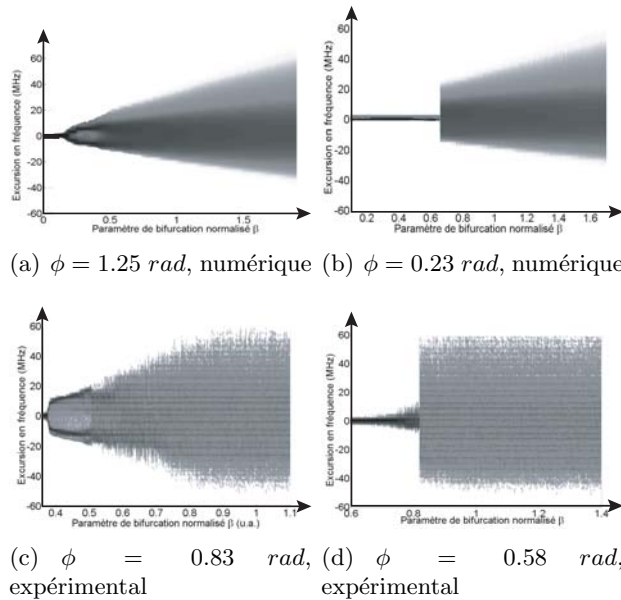


FIG. 2 – Diagramme de bifurcation pour différentes valeurs de déphasage

Nous avons ensuite calculé ces mêmes diagrammes dans des conditions paramétriques similaires, à partir de l'intégration numérique du modèle (méthode de Runge–Kutta d'ordre 4 à pas constant d'environ  $0.02 \times \tau_2$ ). La méthode de représentation de ces diagrammes n'est pas académique puisqu'elle ne fait pas intervenir de coupe de Poincaré. La raison

est liée au fait que le système développe des chaos extrêmement complexes de grande dimension, pour lesquels nous n'avons pas pu établir de section adaptée. Lors du tracé du diagramme, la signature considérée pour un régime dynamique donné est alors constituée par la densité de probabilité de la variable dynamique (ici la fréquence instantanée du signal FM). Cette densité de probabilité est codée en échelle de gris, et évaluée pour chaque échantillonnage du paramètre de bifurcation en abscisse. Les résultats sont représentés à la figure 2. Ils montrent une correspondance qualitative et quantitative satisfaisante, permettant d'espérer en une bonne adéquation entre modèle théorique et système expérimental. Il est à noter que ce système répond à un type particulier de dynamique à retard du fait de la présence du filtrage passe-bande. Cette particularité est soupçonnée conférer à ce type de dynamique un certain nombre de propriétés particulières non présentes dans les systèmes à retard plus classiques, en général décrits par des dynamiques limitantes de type passe-bas. Par exemple, la transition du point fixe s'effectue assez souvent directement vers un régime chaotique, sans nécessairement passer par des cycles limites. En particulier, des transitions en crise sont observées, pour lesquels le point fixe perd sa stabilité au profit d'un régime chaotique de forte amplitude. Des études théoriques plus détaillées sont en cours pour explorer ces transitions.

Il y a toutefois une caractéristique commune avec les dynamiques à retard passe-bas, qui concerne l'obtention pour les fortes valeurs du gain, de régimes chaotiques de grande complexité. Ce sont ces régimes qui sont plus particulièrement visés dans le contexte de l'application aux communications sécurisées par chaos.

### 3.2 Régimes chaotiques pour la sécurisation

La figure 3 représente différents relevés expérimentaux de trajectoires chaotiques du système dynamique, pour deux couples de valeurs des paramètres  $\beta$  et  $\phi$ .

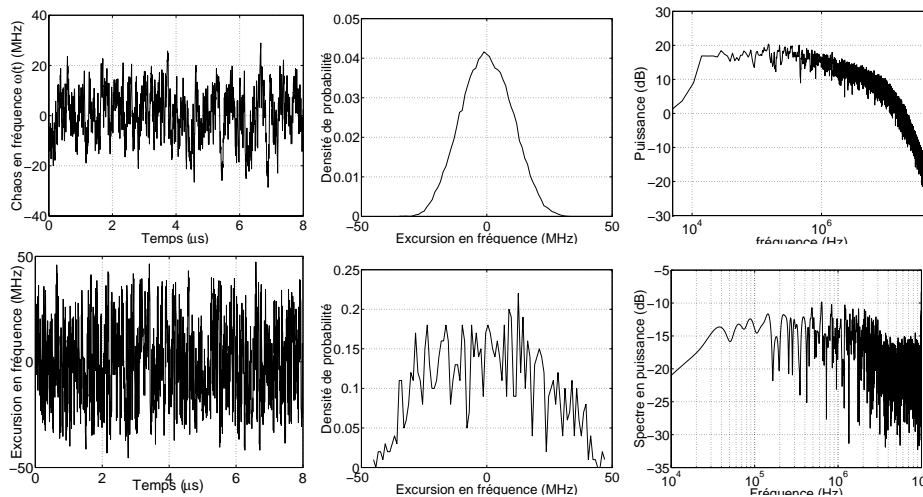


FIG. 3 – Signatures temporelle (gauche), statistique (milieu) et spectrale (droit). En haut :  $\phi = 0.41$  rad et  $\beta = 2.371$ , numériques ; en bas :  $\phi = 0.83$  rad et  $\beta = 1.8$ , expérimentales

Les relevés de gauches correspondent à des traces temporelles du signal en bande base ; on remarque que l'aspect temporel apparaît bien comme bruité. Les graphes situés au centre sont des histogrammes représentant la statistique de la déviation de fréquence

par rapport à la fréquence centrale du VCO ; on remarque également, pour les deux conditions paramétriques, des distributions relativement quelconque sans trace particulière de déterminisme. Enfin, les graphiques de droite sont les spectres des mêmes trajectoires, relevés en bande de base (correspondant par exemple à la tension de commande du VCO). Ces spectres ont une allure relativement constante sur l'ensemble de la bande passante de 10 kHz à 5 MHz environ. C'est à l'intérieur de ce pseudo bruit rose que l'on cherchera à noyer le spectre d'une information à coder sur la porteuse chaotique.

## 4 Conclusion et perspectives

Nous avons présenté les premiers résultats d'un nouveau générateur de chaos basé sur une dynamique non linéaire à retard impliquant un processus dynamique passe-bande. Le système opto-électronique proposé est capable de produire un signal radio-fréquence à modulation de fréquence chaotique. Il implique une transformation non linéaire originale consistant en un interféromètre radio-fréquence, dont la condition d'interférence est modulée par la variation de la fréquence de la porteuse RF. Les signaux obtenus ont montré un bon caractère aléatoire et bruité, qui semble les rendre apte à masquer correctement une information. La prochaine étape du travail consistera à apparier les éléments d'un récepteur / décodeur de signal sécurisé par chaos, avec une architecture du type de celle représentée à la figure 1(b). Une fois le récepteur apparié, un processus de réplication de chaos [3, 4] devra permettre de reproduire au niveau du récepteur, la porteuse chaotique sans le message ; ensuite, une simple soustraction entre le signal chaotique local et celui détecté et venant de l'émetteur aboutira à la restitution de l'information codée par chaos.

## Références

- [1] H. M. Gibbs, F. A. Hopf, D. L. Kaplan, and R. L. Schoemaker, *Observation of chaos in optical bistability*, Phys. Rev. Lett., **46**, 474 (1981).
- [2] L. Larger, J.-P. Goedgebuer, J.-M. Merolla, *Chaotic Oscillator in Wavelength: A New Setup for Investigating Differential Difference Equations Describing Nonlinear Dynamics*, IEEE J. of Quantum Electron., **34**, 594 (1998).
- [3] L. M. Pecora and T. L. Carroll, *Synchronisation in Chaotic Systems* Phys. Rev. Lett., **64**, (1990)
- [4] J.-P. Goedgebuer, L. Larger, H. Porte, *Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode*, Phys. Rev. Lett., **80**, 2249 (1998).

Les auteurs remercient la Communauté Economique Européenne pour le soutien de cette activité de recherche dans le cadre du contrat FET-IST-2000-29683 "OCCULT".