Journées PARISTIC

ACI SI

Novembre 2005

LABRI Bordeaux

TRANSCHAOS

ACI SI 2003-06

Danièle Fournier-Prunaret, LESIA - INSA, Toulouse

Laurent Larger, FEMTO-ST Besançon

Raymond Quéré, XLIM/IRCOM, Brive / Limoges

PLAN

- **Principes**
- **Etat de l'art**
- **Objectifs du projet**
- **Equipes et compétences**
- **Avancées du projet**
- **Résultats obtenus**
- **Travail à venir**

Mots clés : chaos, transmission, cryptographie, système non linéaire, synchronisation, système optoélectronique

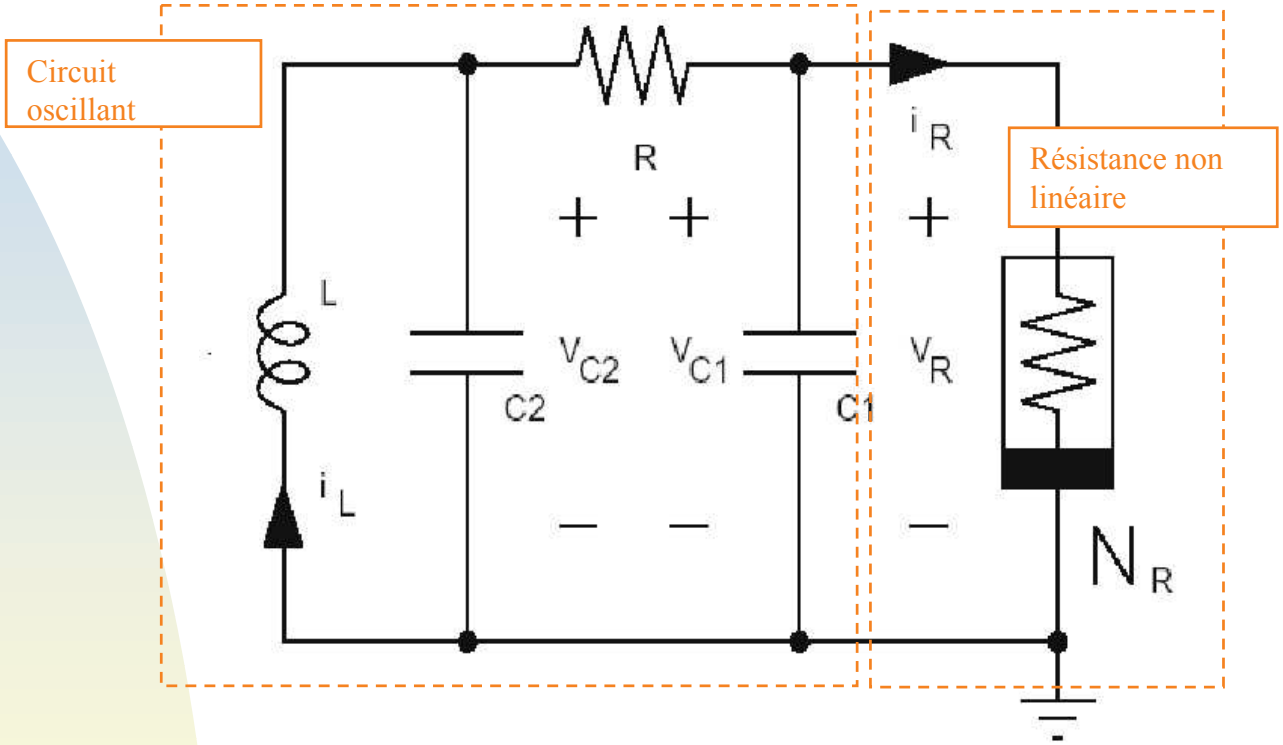
PRINCIPES

- Utiliser les **Dynamiques non linéaires et le Chaos**
  - Régime chaotique : Masquage
  - Déterminisme : Décodage
- Sécuriser les **TRANSMISSIONS**
  - Nouveaux algorithmes de Cryptographie
  - Sécurisation possible au niveau physique
  - Potentiel Multi-Utilisateurs (CDMA)

ETAT DE L'ART

- **Transmissions** par chaos
  - Synchronisation : Pecora & Caroll (1990)
  - Circuits électroniques analogiques (modèles de dimension 3)
- **Cryptographie** par chaos
  - Génération de nombres pseudo-aléatoires par chaos
- **Problèmes** :
  - Faible complexité, faibles non-linéarités, faibles dimensions $\Rightarrow$ **systèmes faciles à attaquer**
  - Format de modulation « non standard » $\Rightarrow$ **compatibilité** avec les communications numériques ?

ETAT DE L'ART : CIRCUIT DE CHUA



- Emission, réception, synchronisation

OBJECTIFS DU PROJET

- Travailler avec des **systèmes de grande complexité**
  - Attaques cryptographiques plus difficiles
- Explorer des **mises en œuvre expérimentales** compatibles avec les communications numériques
  - Communications radio
  - Liaisons par fibre optique
- **Analyse comparative** des propriétés de complexité en temps discret / temps continu

EQUIPES

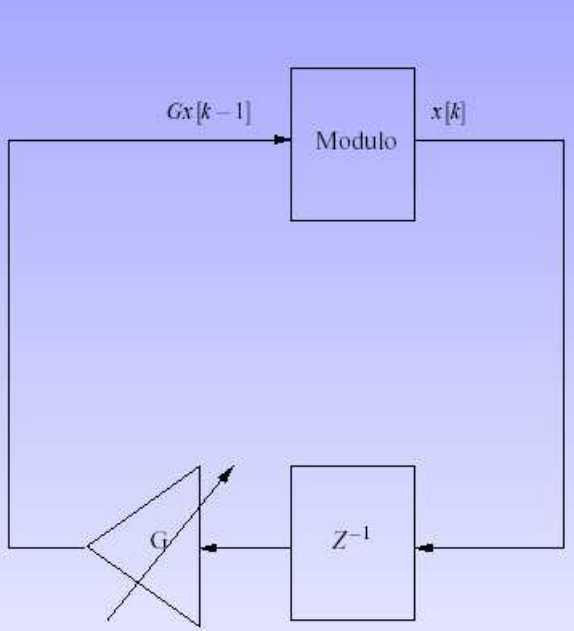
- **LESIA**
  - Systèmes dynamiques non linéaires discrets et continus, aspects théoriques
  - Cryptographie par courbes elliptiques
- **XLIM/IRCOM**
  - Transmissions radio par sauts de fréquence discrets et chaotiques,
  - Systèmes RF non linéaires
- **FEMTO-ST**
  - Systèmes optoélectroniques, chaos échantillonné par impulsions optiques
  - Systèmes dynamiques optiques et optoélectroniques non linéaires

AVANCEES DU PROJET

- **Système RF, systèmes optoélectroniques**
  - Modèle dynamique (études en cours)
  - Architecture des démonstrateurs
  - Choix de réalisation (en cours)
- **Cryptosystème numérique**
  - Simulation sur DSP
  - **Cryptanalyse** (en cours)
    - Estimation des paramètres du système

RESULTATS OBTENUS

- **Démonstrateur RF**
  - Études des diagrammes de stabilité et des espaces de paramètres
  - Études des comportements chaotiques obtenus



Processus itératif de la fonction modulo

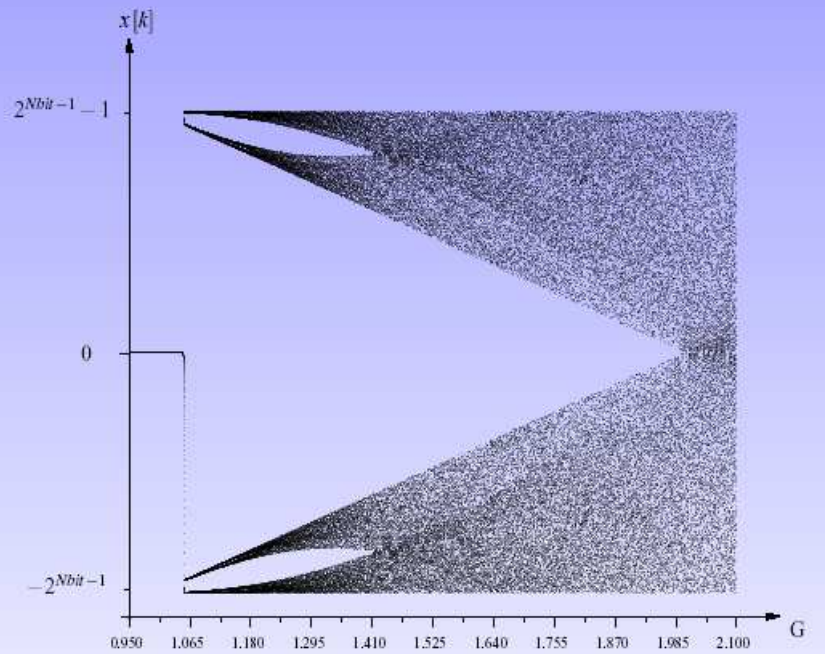
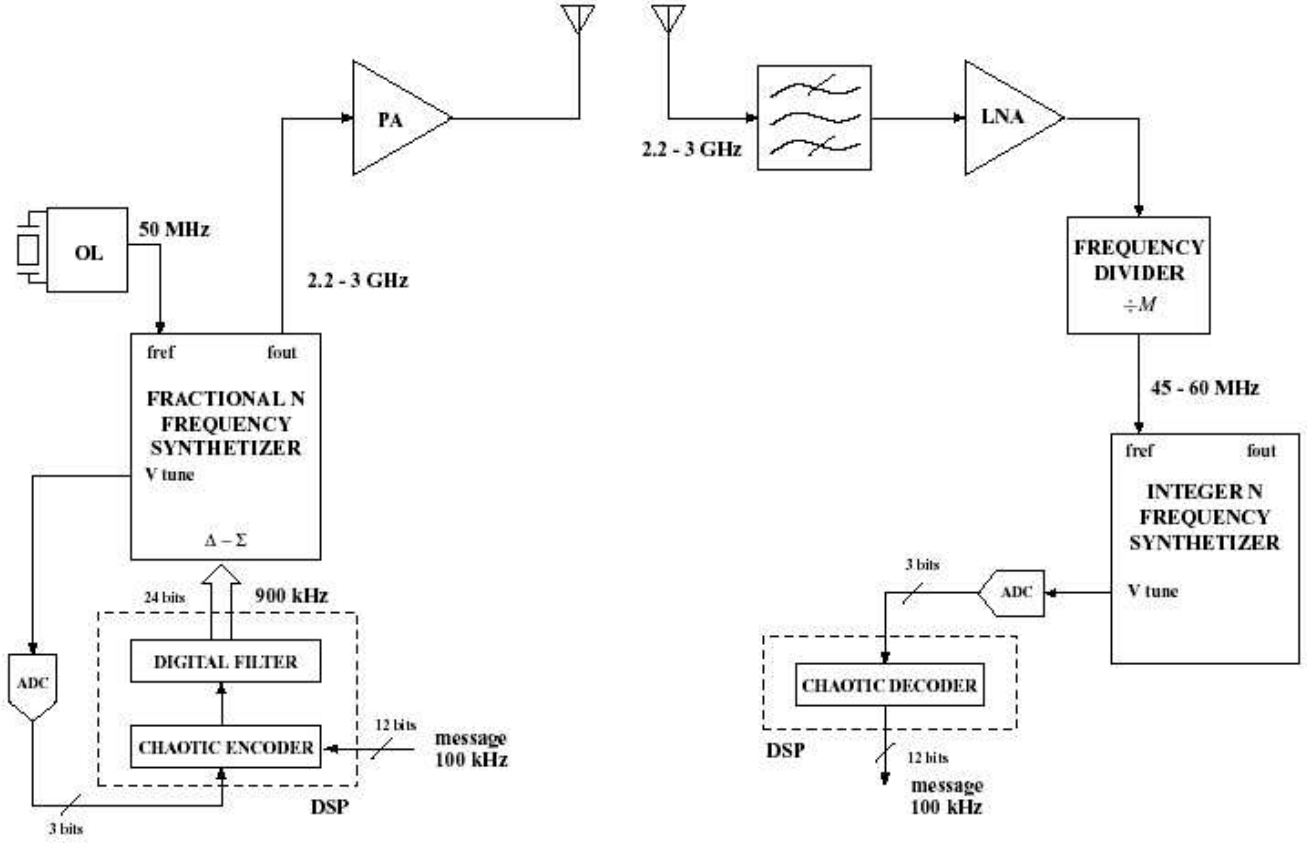


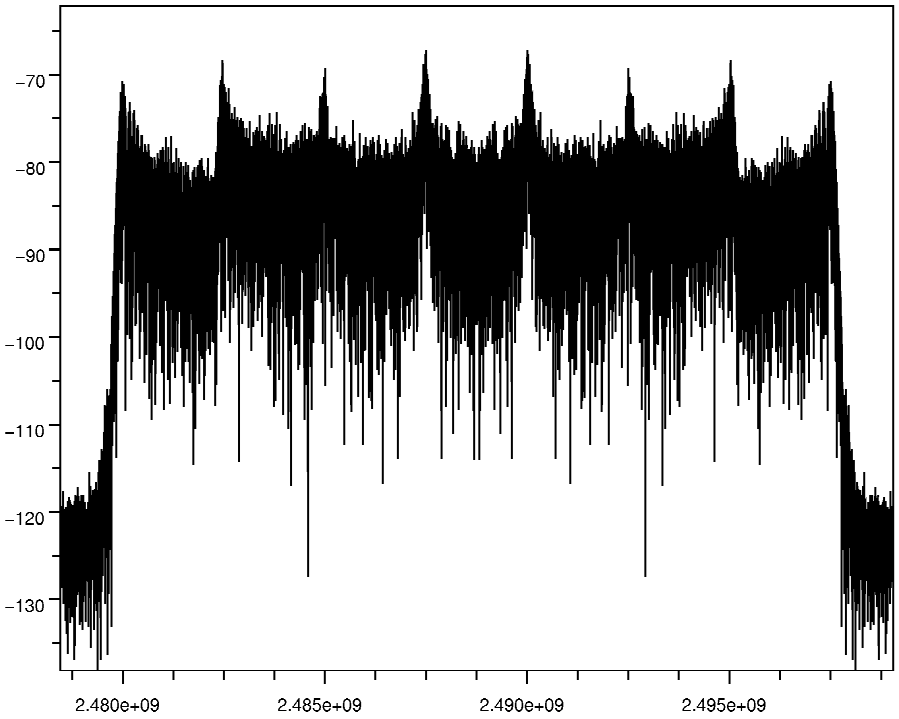
Diagramme de bifurcation

RESULTATS OBTENUS

- **Démonstrateur RF**
  - Simulation de l'architecture émetteur-récepteur



RESULTATS OBTENUS



Spectre de sortie de l'émetteur

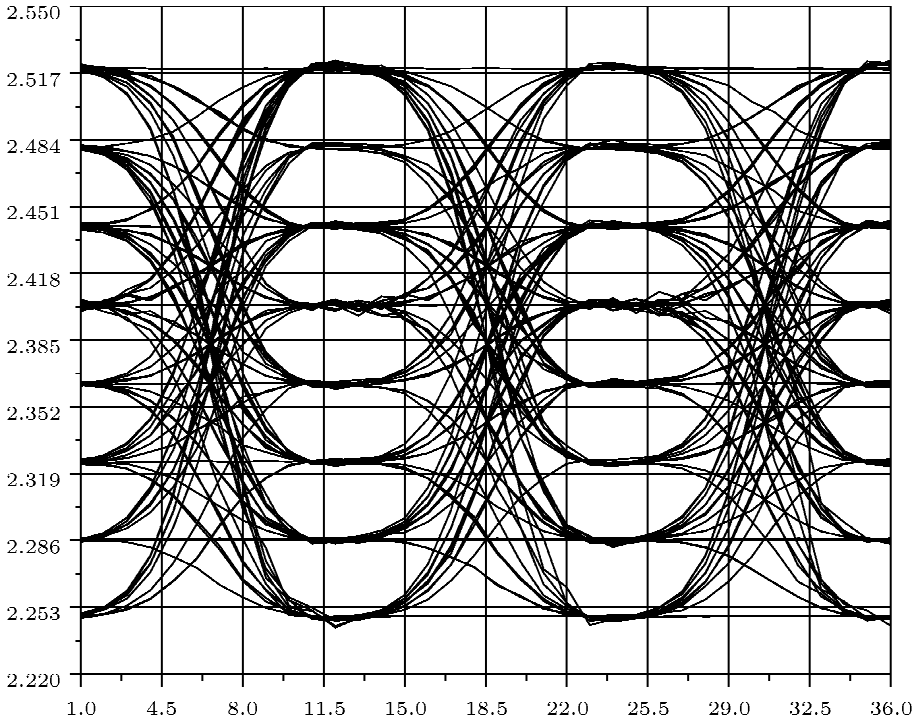
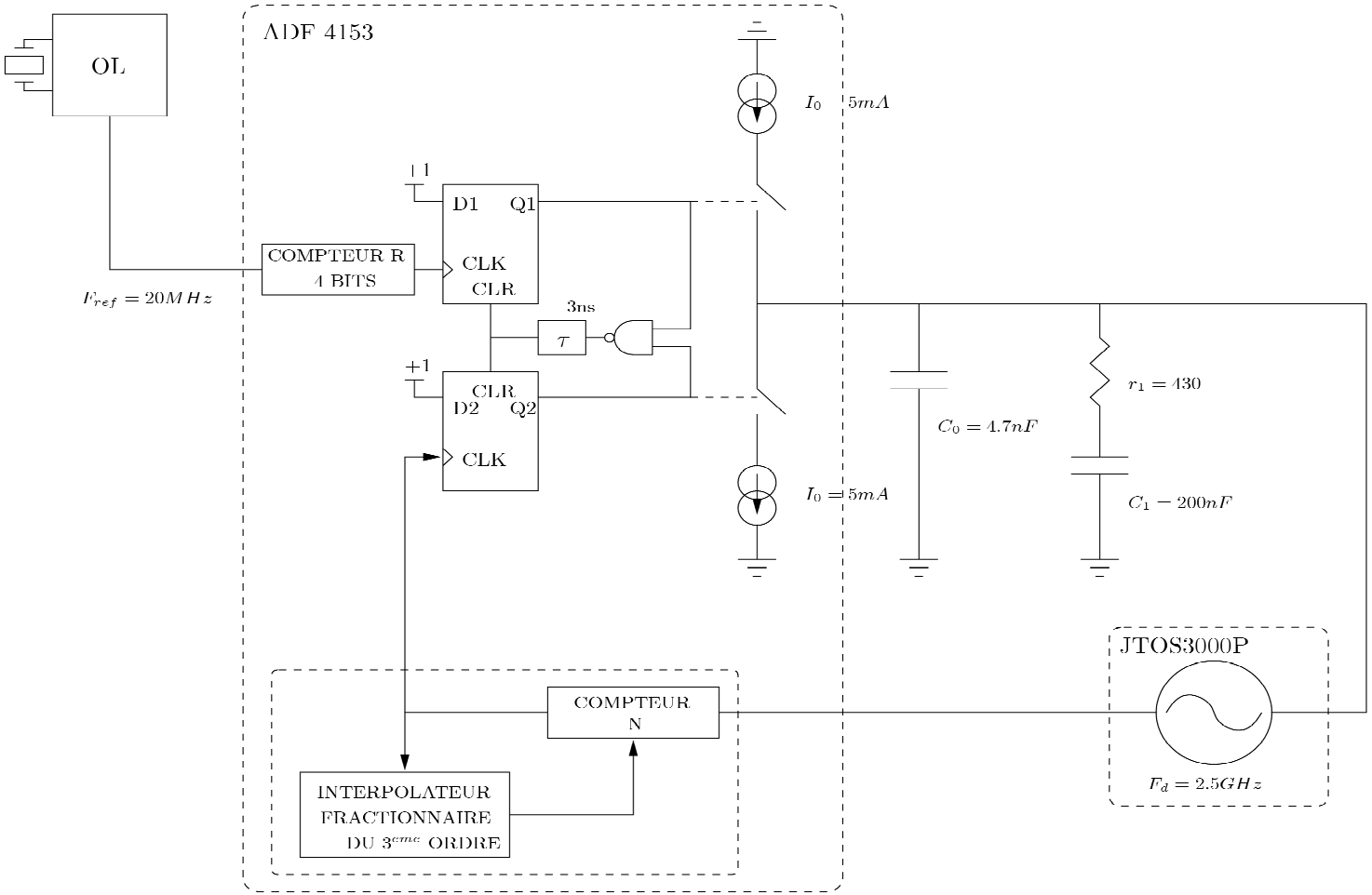


Diagramme de l'oeil en réception

- Résultats de simulation

RESULTATS OBTENUS

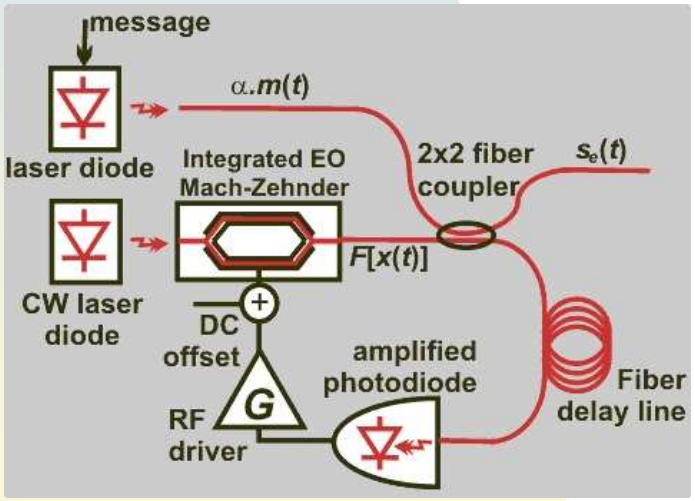
- **Démonstrateur RF** : réalisation expérimentale de la partie émetteur



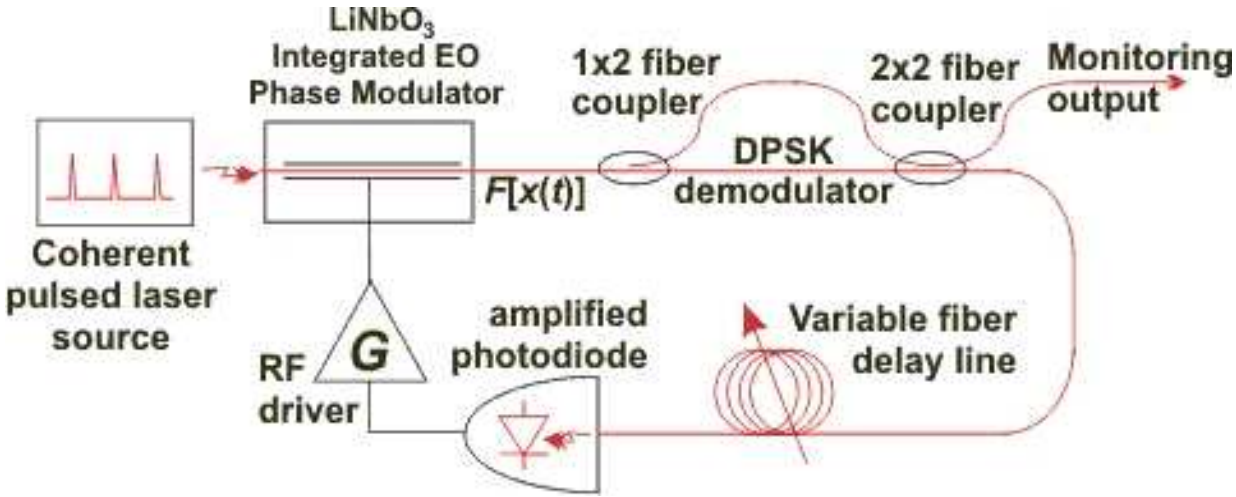
RESULTATS OBTENUS

- **Démonstrateurs optiques**
  - Réalisation de deux **générateurs de chaos**

en intensité



en phase optique

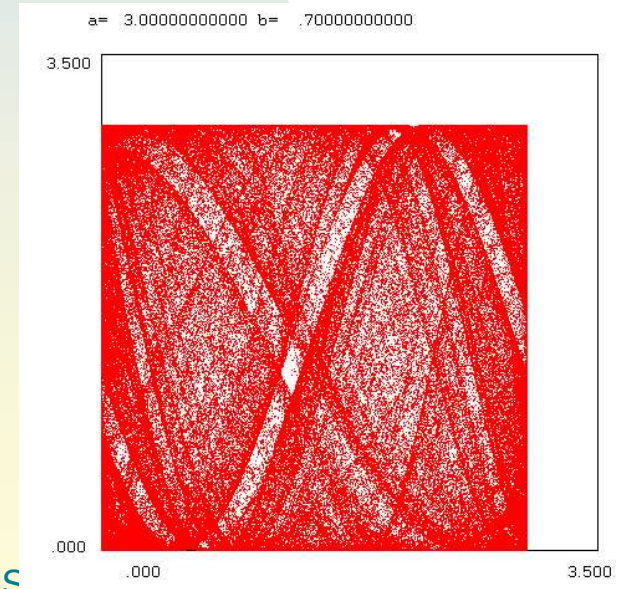


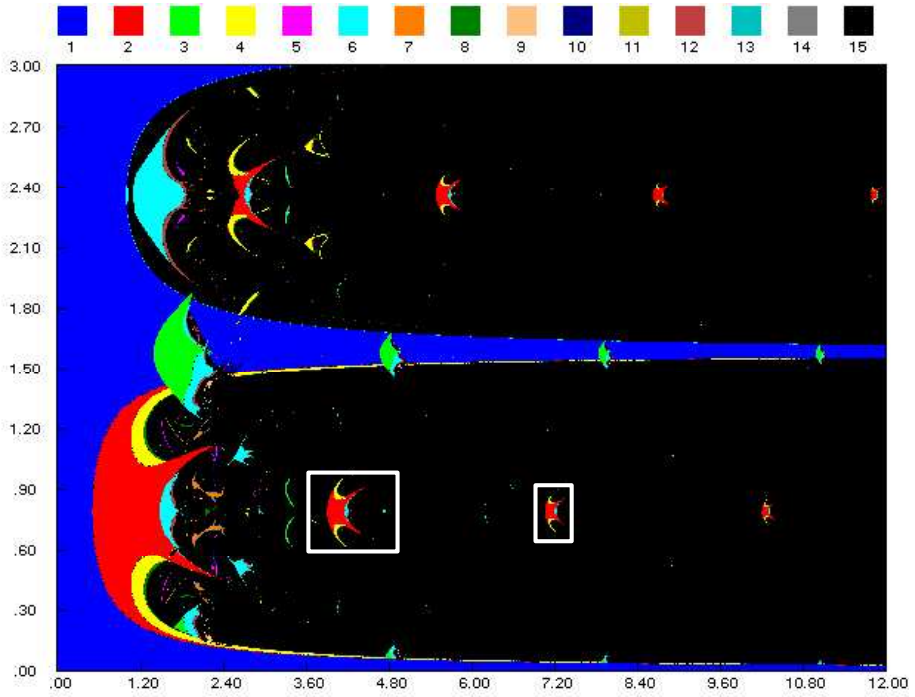
RESULTATS OBTENUS

- **Démonstrateurs optiques**
  - Étude théorique d'un **modèle itératif** pour le générateur en phase optique

$$\varphi_n = a.\sin^2[\varphi_{n-P} - \varphi_{n-P-N} + c]$$

a , c paramètres du système optique, $P=N=1$





RESULTATS OBTENUS

- **Démonstrateurs optiques**
  - **Mise en œuvre expérimentale** des générateurs de chaos
  - Étude numérique et expérimentale des comportements chaotiques
  - Choix de l'architecture (codage/décodage en temps continu à 3Gb/s)

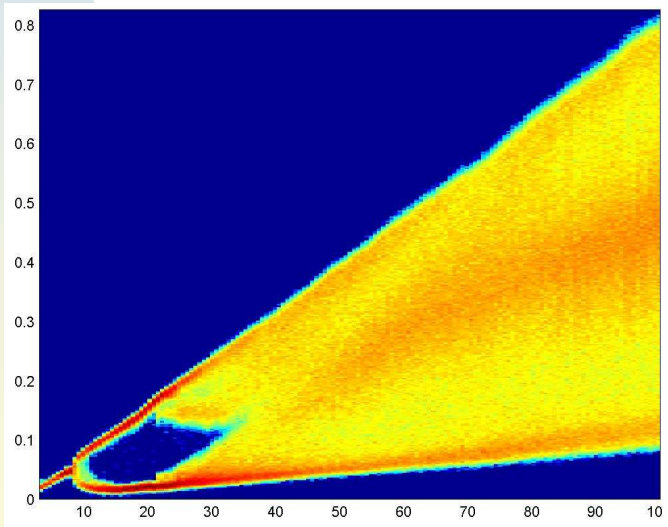


Diagramme de bifurcations
Taux de répétition: 10 GHz

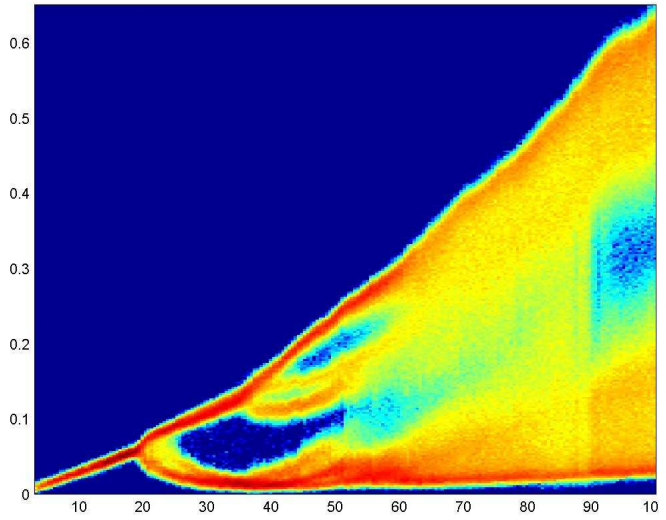


Diagramme de bifurcations
Taux de répétition: 7.5 GHz

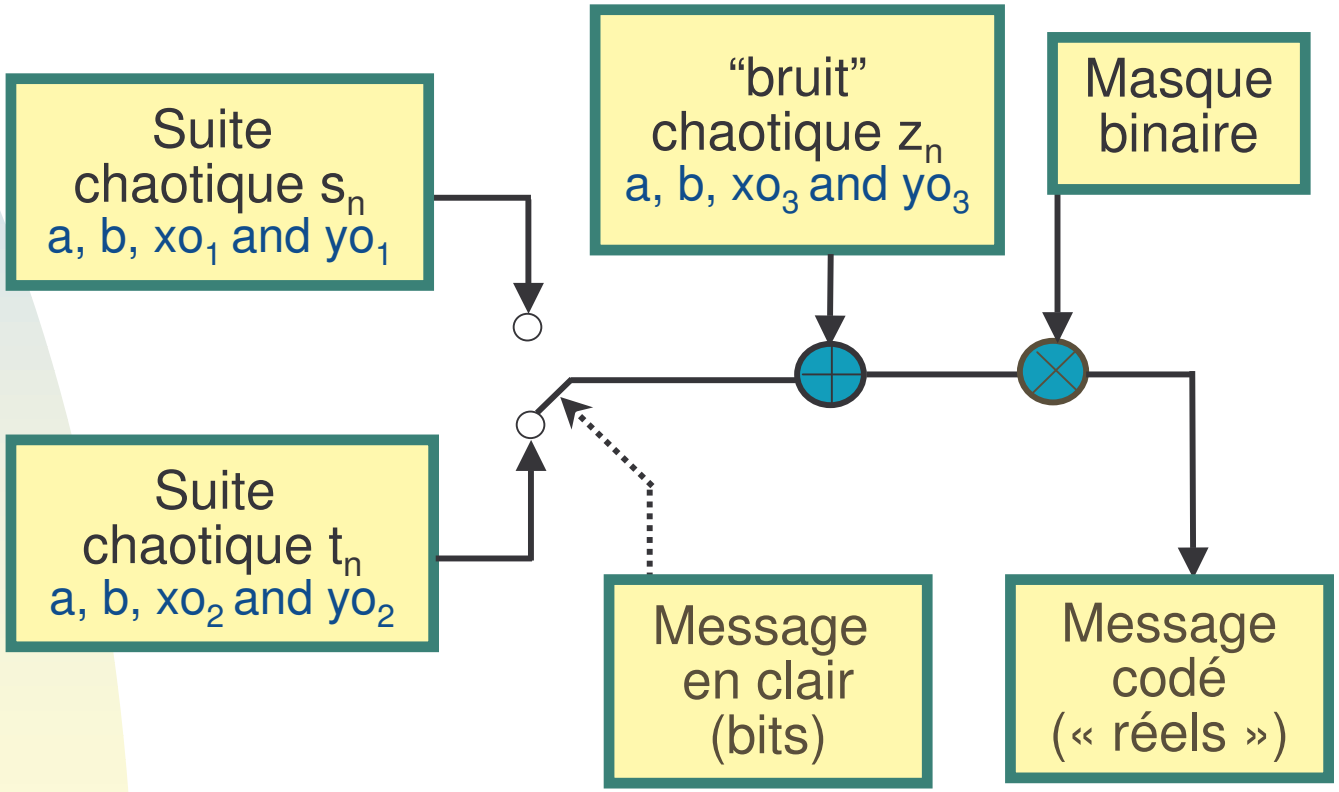
RESULTATS OBTENUS

- **Cryptosystème numérique**
  - Etude de la robustesse d'un cryptosystème basé sur le principe du « Chaos Shift Keying »
    - **2 séquences chaotiques différentes**
      - $\{ s_n \} = F^n(s_0)$
      - $\{ t_n \} = F^n(t_0)$
    - **N-ième valeur cryptée c_n**

      $c_n = s_n$ si $p_n = 0$; $c_n = t_n$ si $p_n = 1$
    - **Bruit, masque**
  - Estimation des paramètres ….

RESULTATS OBTENUS

- **Cryptosystème numérique**



Clé : **conditions initiales, paramètres, masque**

RESULTATS OBTENUS

- **Cryptanalyse**
  - Système supposé connu
    - **Retard** connu ou non
    - **Conditions initiales** connues ou non
  - Estimation des paramètres inconnus
    - Liée à la **dimension** du modèle
    - **Difficile** pour un attaquant

RESULTATS OBTENUS

- Mise en ligne sur le site ACI Transchaos et sur le site de l'IRCOM d'outils flexibles de modélisation et de simulation de systèmes chaotiques sous SCICOS/SCILAB

http://www.lesia.insa-toulouse.fr/nouveau/transchaos/ACI-TRANSCHAOS.html

TRAVAIL A VENIR

- **Synchronisation**, codage/décodage en temps discret
- **Cryptanalyse**
- **Modélisation** des dynamiques non linéaires
  - Système optoélectronique
  - Système RF $\Rightarrow$ système hybride
- **Analyse** de complexité, comparaison temps discret – temps continu

EN RESUME

- Quelques idées clés :
  - **Retard**
    - **Dimension élevée** du système
    - Meilleure **sécurisation**
  - **Masque**
    - Transmission **plus rapide**
    - Meilleure **sécurisation**
  - Mixer les aspects **numérique - analogique**
    - Système « hybride »
    - Espace d'état **infini**