ACI SI

Décembre 2003

IRISA, Rennes

TRANSCHAOS

Le chaos pour la sécurité des transmissions

Danièle Fournier-Prunaret, LESIA - INSA, Toulouse

Laurent Larger, GTL-CNRS Telecom, Metz / LOPMD Besançon

Raymond Quéré, IRCOM – CNRS, Brive / Limoges

TRANSCHAOS

- Utiliser les dynamiques non linéaires
  - Régime chaotique : Masquage
  - Déterminisme : Décodage
- Sécuriser les TRANSMISSIONS
  - Méthode alternative de Cryptographie
  - Sécurisation au niveau physique
  - Potentiel Multi-Utilisateurs (CDMA)

PLAN

- Principes
- Equipe du projet
- Objectifs
- Calendrier

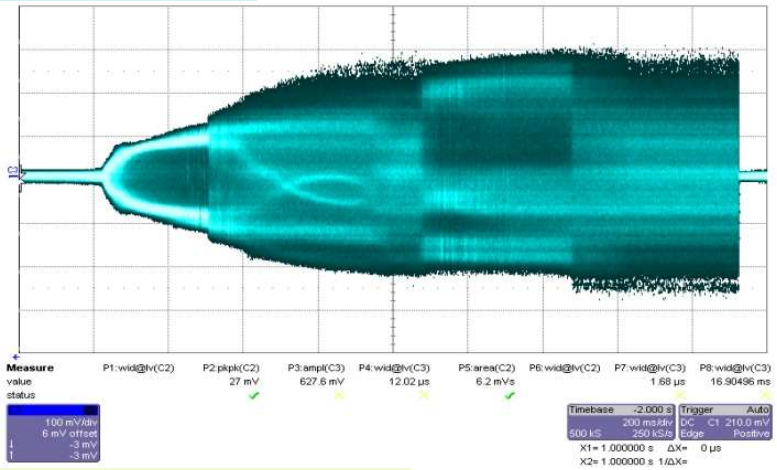
Mots clés : chaos, transmission, cryptographie, CDMA, système non linéaire, synchronisation

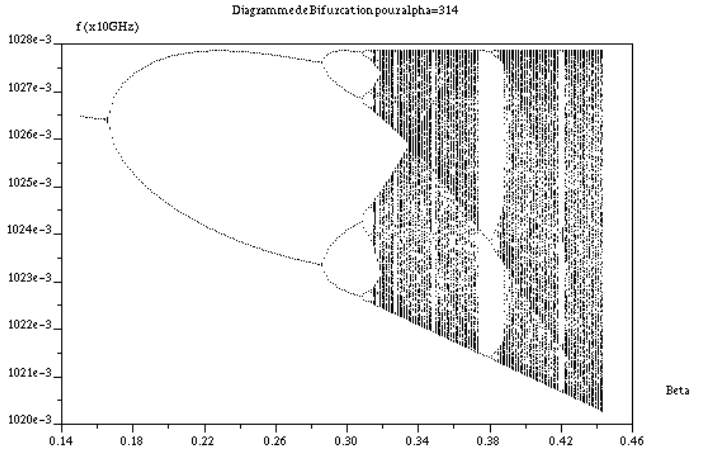
PRINCIPES

- Génération de dynamique chaotiques
  - Système non linéaire, déterministe
  - Système physique
    - Analogique (temps discret/temps continu)
    - Couche physique d'une transmission
  - Modélisation
    - Numérique
    - DSP dédié

PRINCIPES

- Route vers le chaos
- Diagrammes de bifurcation



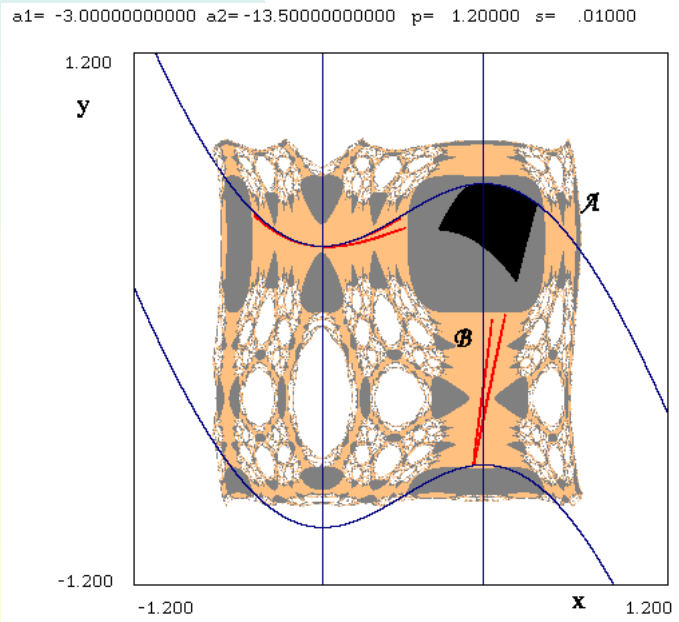


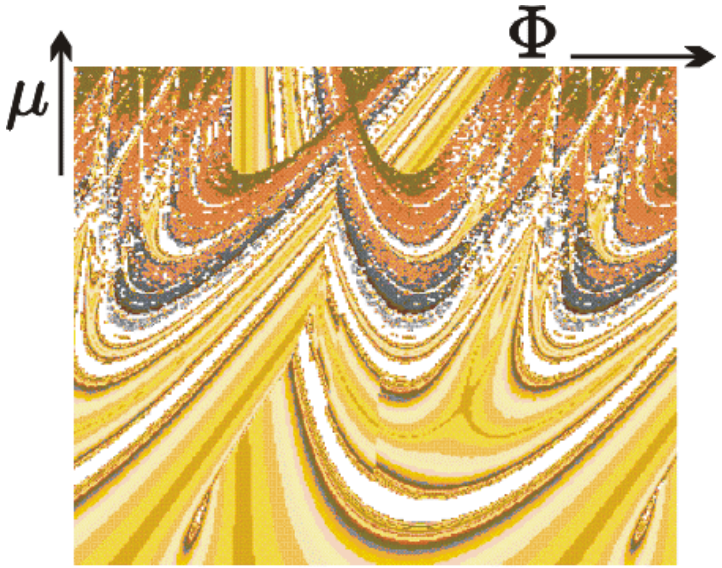
Système optoélectronique

circuit micro-ondes

PRINCIPES

- Dynamiques dans l'espace des paramètres
  - Sensibilité aux conditions initiales (SCI)
  - Régimes de fonctionnement : Bassins, frontières
  - Mesure de la complexité : Exposants de Lyapunov, dimensions fractales

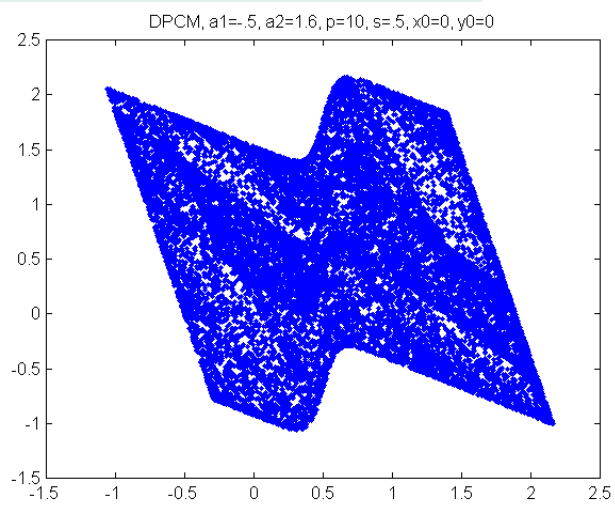


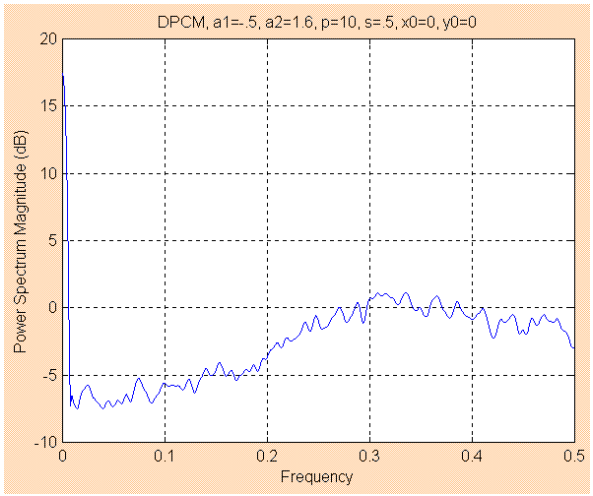


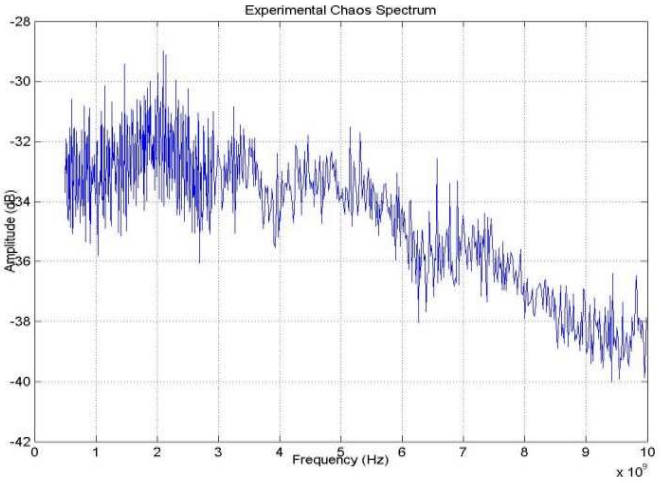
Exposants de Lyapunov
(modèle discret)

PRINCIPES

- En régime chaotique :
  - attracteur chaotique dans un espace des phases
  - représentation spectrale







Equipe du projet TRANSCHAOS

- Constitution de l'équipe du projet ACI : Action spécifique CNRS Non linéaire, Signal et Composants (AS03 2002)
  - LESIA Toulouse
  - LOPMD GTL-CNRS Telecom Metz et Besançon
  - IRCOM Limoges

Equipe du projet TRANSCHAOS

- LESIA
  - Systèmes dynamiques non linéaires discrets et continus depuis 1980
    - Attracteurs chaotiques
    - Bassins et frontières fractales
    - Bifurcations → route vers le chaos
  - Cryptographie
    - Courbes elliptiques (depuis 1995)
    - Cryptographie chaotique (depuis 2000)
      - Réalisation sur DSP

Equipe du projet TRANSCHAOS

- Personnes impliquées
  - Danièle FOURNIER-PRUNARET, Professeur
  - Véronique GUGLIELMI, MCF
  - Pierre PINEL, MCF
  - AbdelKaddous TAHA, enseignant
  - Pascal CHARGE, MCF
- Publications
  - Int. J. Bifurcation & Chaos, IEEE TCS,…
  - Conférences : NDES, NOLTA, ECCTD…

Equipe du projet TRANSCHAOS

- LOPMD
  - Systèmes Optoélectroniques ou électroniques
    - Cryptographie par chaos depuis 1994
    - Systèmes non linéaires à retard
    - Quatre démonstrateurs analogiques réalisés
  - Synchronisation par chaos

Equipe du projet TRANSCHAOS

- Personnes impliquées
  - Laurent LARGER, MCF
  - Pierre-Ambroise LACOURT postdoc CNRS
  - Marc HANNA, CR
  - Jean-Marc MEROLLA, CR

Equipe du projet TRANSCHAOS

- **IRCOM**
  - Circuits micro-ondes non linéaires
    - Stabilité
    - Analyse des comportements chaotiques
  - Transmission CDMA (Code Division Multiple Access)
    - Ondes chaotiques

Equipe du projet TRANSCHAOS

- Personnes impliquées
  - Raymond QUERE, Professeur
  - Jacques GUITTARD, PRAG
  - Jean-Christophe NALLATAMBY, MCF
  - Alan LAYEC, Doctorant

OBJECTIFS

- Etudes théoriques des signaux chaotiques discrets dans le contexte de la cryptographie par chaos
  - Systèmes de faible dimension avec fortes non-linéarités (LESIA)
  - Systèmes de dimension élevée
    - Systèmes actuels à temps continu
    - Discrétisation de systèmes continus (LESIA-LOPMD-IRCOM)
    - Ouverture vers de nouveaux schémas de synchronisation

OBJECTIFS

- Cryptographie chaotique
  - Système de transmission de signaux analogiques/numériques (LOPMD)
    - Impulsions optiques (solitons)
    - Système mixte (IRCOM - LESIA)
  - Système tout numérique
    - Conservation des propriétés après discrétisation (LESIA)

OBJECTIFS

- Synchronisation
  - Nouvelles architectures
    - Combiner boucle ouverte/fermée (LOPMD - IRCOM - LESIA)
    - Combiner système émission/réception RF et modulation numérique (IRCOM - LESIA)
  - Schéma de crypto par chaos à clé publique/privée

CALENDRIER

- Réunions trimestrielles
  - 21 janvier à Toulouse
- Etudes théoriques : 2003-2004
- Etudes expérimentales : 2004-2005
  - Système optoélectronique
  - Système analogique-numérique
  - Système numérique