Cryptage par chaos haut-débit sur réseau optique installé

Laurent Larger, Roman Lavrov & Maxime Jacquot

Département d'Optique P.M. Duffieux, Institut FEMTO–ST, UMR CNRS 6174, Université de Franche–Comté, 25030 Besançon Cedex, France.
laurent.larger@univ-fcomte.fr

Nous présentons les derniers résultats d'un domaine d'application particulier des comportements chaotiques, celui de la cryptographie par chaos. Depuis la démonstration du principe de synchronisation entre chaos en 1990[1], les télécommunications optiques sont apparus dans ce contexte comme le mode de transmission présentant le plus de potentiel, tant en termes applicatifs qu'en termes de performances[2]. Cette nouvelle approche de la sécurisation des données intervient au niveau de la couche physique des systèmes de transmission, en noyant les signaux intelligibles (typiquement les successions de 0 et de 1 des données binaires), dans un comportement chaotique contrôlé, et surtout synchronisable au niveau d'un récepteur autorisé. L'optique, outre ses formidables propriétés largement exploitées dans les réseaux fibrés actuels, offre aussi l'avantage de permettre une réalisation relativement aisée de systèmes dynamiques à comportements chaotiques de grande complexité, grâce au principe des dynamiques à retard. Après avoir exploré plusieurs pistes de réalisation pratique de systèmes de communications sécurisés par chaos [3,4], nos derniers résultats ont permis de mettre au point une nouvelle architecture[6] avec laquelle des performances inégalées ont pu être atteintes. Une transmission de données binaires masquées par un onde lumineuse dont la phase optique présente des fluctuations chaotiques ultra-rapides, a pu être réalisées jusqu'à 10Gb/s, non seulement en laboratoire, mais également sur des réseaux à fibre optique installés. Des tests sur le réseau "Lumière" de la ville de Besançon, et sur le réseau métropolitain d'Athènes ont été accomplis avec succès.

Au delà de l'efficacité obtenue dans le cadre des communications optiques par chaos, l'architectures présentées de chaos en phase électro–optique semble également être un excellent candidat pour d'autres applications, comme la génération de séquences aléatoires à très haut débit[7], ou encore pour la mise en œuvre de calculateurs analogiques d'un nouveau type, le "Reservoir Computing" aussi appelé "Liquid State Machine"[8].

Références

1. L. M. Pecora, T. L. Carroll, Synchronization in chaotic systems, *Phys. Rev. Lett.*, **64** (8), 821–824 (1990).
2. G. VanWiggeren and R. Roy, Communicating with chaotic lasers, *Science*, **279**(3), 1198–1200 (1998).
3. J. P. Goedgebuer, L. Larger, and H. Porte,, Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laserdiode, *Phys. Rev. Lett.*, **80**, 2249–225 (1998).
4. A. Argyris *et al.*, Chaos–based communications at high bit rates using commercial fiber–optic links, *Nature*, **438**, 343–346 (2005).
5. L. Larger, J.-P. Gordegbuer and V.S Udalsov, Ikeda–based nonlinear delayed dynamics for application to secure optical transmission systems using chaos, *C.R. de Physique 4* **5** (6), 669–681 (2004).
6. R. Lavrov *et al.*, Electro–optic delay oscillator with non–local non linearity : optical phase dynamics, chaos, and synchronization, *Phys. Rev. E*, **80**, 026207 (2009).
7. A. Uchida *et al.*, Fast physical random bit generation with chaotic semiconductor lasers, *Nature Photonics*, **2**, 728–732 (2008).
8. W. Maass, Th. Natschläger and H. Markam, Real–Time Computing Without Stable States : A New Framework for Neural Computation Based on Perturbations *Neural Comput.*, **14** (11), 2531–2560 (2002).