

Générateur de chaos opto-électronique à double retard pour les télécommunications optiques sécurisées à haut débits

Mourad Nourine, Laurent Larger, Yanne Kouomou Chembo, Kirill Volyanskiy, & Michael Peil

Département d'Optique, Institut FEMTO-ST, UMR CNRS 6174, Université de Franche-Comté, 25030 Besançon Cedex, France.

`mourad.nourine@univ-fcomte.fr`

Depuis que Pecora et Carroll [1] ont réussi à démontrer la possibilité de synchronisation du chaos déterministe, les travaux sur la cryptographie physique par chaos n'ont cessé de se développer, en particulier dans le domaine des télécommunications optiques [2] : améliorations des systèmes pour augmenter la qualité et le débit de transmission, mais aussi diversifications des architectures de génération de chaos afin d'en augmenter la complexité, et donc la sécurité. La qualité de la transmission est liée à la qualité de la synchronisation entre chaos. Dans la configuration des systèmes auto-synchronisants, cette qualité de synchronisation dépend fortement du degré d'appariement entre les éléments "clé" (secrets) du récepteur et de l'émetteur. De manière antagoniste, la sécurité dépend de la complexité des transformations dynamiques qui mènent au chaos ; cette complexité rend cependant l'opération de synchronisation plus délicate d'un point de vue expérimental.

Le système dynamique étudié pour la génération de chaos appartient à la catégorie des systèmes d'Ikeda [3]. Il est construit à l'aide d'un composant électro-optique spécifique réalisant une non linéarité bi-dimensionnelle, adapté aux télécommunications haut débits. Ce composant est un interféromètre à ondes multiples, réalisé en optique intégré (LiNbO_3), et disposant de 2 électrodes de modulation indépendantes : un modulateur QPSK (Quadrature Phase Shift Keying). Le but de cette architecture est d'augmenter la complexité[4] du chaos généré, sur le principe d'une dynamique non linéaire à double retard.

Nous présentons les premières simulations numériques d'une architecture émetteur-récepteur, et de ses performances en terme de synchronisation. Le codage et décodage d'une information binaire est analysé pour ce type d'architecture, avec laquelle nous espérons pouvoir atteindre des débits d'au moins 3 Gbit/s.

Références

1. L. M. PECORA, AND T. L. CARROLL, Synchronization in chaotic systems, *Phys. Rev. Lett.*, **64**(8), 821–824 (1990).
2. L. LARGER, J. P. GEODDGEBUER, AND V. UDALTSOV, Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos, *C. R. Physique*, **5**, 669-681 (2004).
3. K. IKEDA, Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system, *Optics Communications*, **30**, 257-261 (1979).
4. M. NOURINE, M. PEIL, AND L. LARGER, Chaos généré par une non linéarité 2D et une dynamique à retard, *C. R. 12èmes Rencontres du Non Linéaire*, 149-154 (2009).