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

Résumé. Dans cet article sont présentés nos résultats d'investigations d'un système de cryptographie physique dédié aux télécommunications optiques sécurisées à haut débits. Ce système est composé d'un émetteur et d'un récepteur du même type — clé cryptographique physique secrète — mettant à profit les propriétés des systèmes chaotiques continus, afin de sécuriser en temps réel des transmissions de données optiques par chaos. L'émetteur en question est un oscillateur optoélectronique à double retard, dont le fonctionnement s'appuie sur une dynamique non linéaire à délais ; il permet pratiquement de générer d'une manière contrôlée un chaos d'une grande complexité sur la variable intensité optique. L'élément clé de décodage réside dans la capacité du système récepteur à reproduire le plus fidèlement possible les oscillations chaotiques de l'émetteur, autrement dit la *synchronisation* entre chaos, en vue de restituer avec une bonne qualité l'information utile noyée par modulation chaotique au niveau de l'émetteur.

Abstract. We report on the study of a physical cryptographic system intended for high speed optical telecommunications. This system consists of a transmitter and a receiver of the same type — secret physical cryptographic key — using the advantage of the chaotic systems properties in order to secure optical data transmission. The transmitter under study is a double delay line optoelectronic oscillator. This allows to produce high complexity chaotic signals in a controlled way, using the variable optical intensity. The decoding key issue is the capability of the receiving system to reconstruct chaotic oscillations of the transmitter : an efficient synchronization between distant chaos allows to reconstruct with a high quality the useful information, which is hidden by chaotic modulation at the transmitter.

1 Introduction

Depuis le travail fondateur de synchronisation du chaos déterministe de Pecora et Carroll [1], les travaux sur la cryptographie physique par chaos n'ont cessé de se développer, en particulier dans le domaine des télécommunications optiques [2,3,4] : 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. De manière antagoniste, la sécurité dépend de la complexité des transformations dynamiques qui mènent au chaos, mais malheureusement cette complexité rend aussi l'opération de synchronisation plus délicate d'un point de vue expérimental.

Le système dynamique proposé ici pour la génération de chaos appartient à la catégorie des systèmes d'Ikeda [5]. Il est construit à l'aide d'un composant électro-optique spécifique réalisant une non linéarité bi-dimensionnelle (2D), adaptée 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 du chaos généré, sur le principe d'une dynamique non linéaire à double retard.

Dans cet article, nous donnerons d'abord une brève description du dispositif expérimental permettant de produire les signaux chaotiques, puis sa mise en équation afin de le simuler et de l'explorer numériquement. Ensuite, nous présentons les premiers résultats obtenus d'une architecture émetteur-récepteur, et de ses performances en terme de synchronisation. Le codage et décodage d'une information binaire sera analysé pour ce type d'architecture, avec laquelle nous espérons pouvoir atteindre des débits multi-Gigabit.

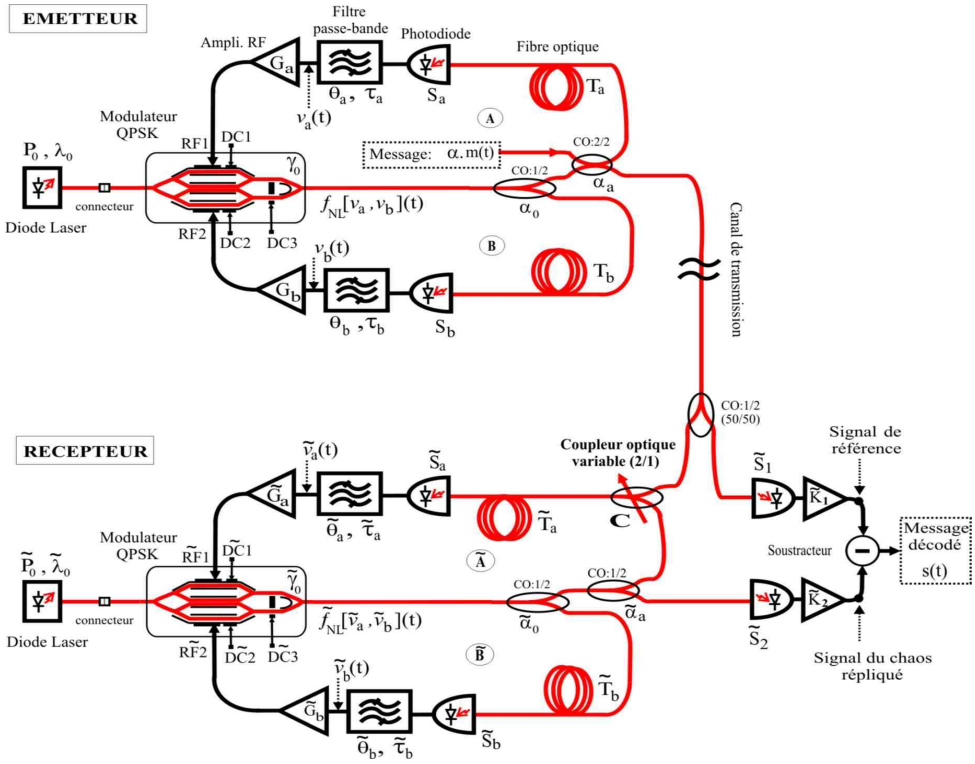


Fig. 1. *Schéma de principe du système cryptographique par chaos complet.*

2 Émetteur : générateur de chaos à modulateur QPSK

2.1 Description

Le schéma de la figure 1 illustre le système cryptographique physique complet pour la transmission unidirectionnelle de données optiques ; il est composé de deux sous-systèmes : un émetteur et un récepteur (le symbole « *tilda* » dénote tous les paramètres du récepteur).

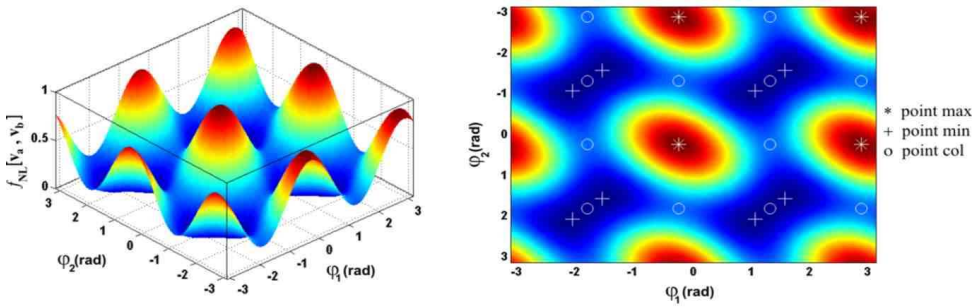
L'émetteur est un oscillateur opto-électronique chaotique [6], basé sur le principe d'une dynamique non linéaire à double retard. Cet oscillateur présente l'originalité d'avoir 2 boucles de contre-réaction électro-optiques non linéaires, impliquant chacune un élément retardant, une photodiode de conversion optique / électrique, un filtre électronique large bande, et un élément amplificateur. La non linéarité est réalisée par le modulateur télécom QPSK, considéré ici comme le cœur de ce générateur de chaos, et qui sert à transporter les oscillations micro-ondes à travers ses électrodes de modulation RF1 et RF2 sur la porteuse optique. Ce modulateur réalise un interféromètre à 4 ondes, dont la condition d'interférence statique est accordable par l'intermédiaire des 3 tensions continues V_{DC_m} $(m = 1, 2, 3)$ appliquées sur ses électrodes DCm. Comme le montre un exemple sur la figure 2, la fonction de transfert bi-dimensionnelle de modulation, notée $f_{NL}[v_a, v_b]$, est potentiellement fortement non linéaire, selon les amplitudes des tensions de modulation appliquées aux électrodes RF. Son expression est donnée par [6] :

$$f_{NL}[v_a, v_b](t) = \frac{1}{4}\left\{ \cos(\psi_3)\Big[\cos(\psi_3) + 2\cos\big(\psi_1 + \psi_2\big)\cos\big(\psi_2 + \psi_3 - \psi_1\big)\Big] + \cos^2\big(\psi_2 + \psi_3 - \psi_1\big)\right\} \quad (1)$$

avec :

$$\psi_{1,2} = \frac{\varphi_{1,2}(t)}{2}; \qquad \psi_3 = \frac{\phi_3}{2};$$

où les termes $\varphi_{1,2}(t) = \pi(v_{a,b}(t)/V_{\pi RF_{1,2}}) + \phi_{1,2}$ sont des déphasages variables ; ils sont dus à l'application sur les électrodes RF1 et RF2 des tensions de modulations variable $v_{a,b}(t)$. Les déphasages



(a) Vue en 3D (b) Vue de dessus

Fig. 2. *La fonction non linéaire bi-dimensionnelle réalisée par le modulateur QPSK.*

$\phi_m = \pi(V_{DC_m}/V_{\pi DC_m})$ sont statiques ; ils déterminent la condition d'interférence au point de repos du modulateur QPSK.

2.2 Mise en équations de l'émetteur et résultats expérimentaux

Les oscillations de l'émetteur peuvent se résumer à un modèle théorique de deux équations intégro–différentielles, excitées par un terme non linéaire retardé qui est fonction des deux variables couplées :

$$\frac{1}{\theta_i}\int_{t_0}^{t} x_i(\xi)\,\mathrm{d}\xi + \tau_i \frac{\mathrm{d}x_i}{\mathrm{d}t}(t) + x_i(t) = \beta_i \cdot f_{\mathrm{NL}}\left[x_a(t-T_i), x_b(t-T_i)\right] \tag{2}$$

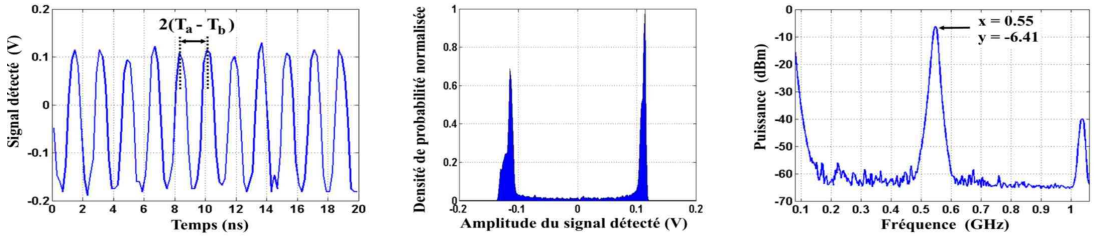
où $(i = a, b)$ selon la boucle de rétroaction concernée, et $x_i(t) = v_i(t)/(2V_{\pi RFi})$ représentent les variables normalisées. θ_i et τ_i sont les constantes de temps caractéristiques des filtres électroniques passe-bandes. $\beta_i = (\pi P_0 \gamma_0 G_i S_i \alpha_0 \alpha_i)/(2V_{\pi RFi})$ est le gain global normalisé de la boucle de rétroaction, avec : P_0 la puissance optique à l'entrée du modulateur QPSK ; γ_0 le coefficient des pertes optiques du modulateur ; G_i le gain de l'amplificateur de puissance RF ; S_i la sensibilité du photodétecteur ; α_0 le coefficient de couplage du couleur optique (1×2). Le paramètre α_i est le coefficient de couplage du coupleur optique (2×2) (qui n'apparaît pas pour la boucle (B)).

Tab.1. Paramètres expérimentaux du générateur de chaos à modulateur QPSK.

	Boucle (A)			**Boucle (B)**		
Paramètre	symbole	valeur	unité	symbole	valeur	unité
retard temporel	T_a	61	ns	T_b	60	ns
fréquence de coupure haute	f_{c1a}	13	GHz	f_{c1b}	13	GHz
fréquence de coupure basse	f_{c2a}	50	kHz	f_{c2b}	30	kHz
constante de temps rapide	$\tau_a = \frac{1}{2\pi f_{c1a}}$	12,2	ps	$\tau_b = \frac{1}{2\pi f_{c1b}}$	12,2	ps
constante de temps lente	$\theta_a = \frac{1}{2\pi f_{c2a}}$	3,18	μs	$\theta_b = \frac{1}{2\pi f_{c2b}}$	5,30	μs
Paramètres de la non linéarité bi-dimensionnelle						
tension demi-onde dynamique	$V_{\pi RF1}$	5,84	V	$V_{\pi RF2}$	6,08	V
tensions demi-onde statiques	$V_{\pi DC1}$	7,40	V	$V_{\pi DC2}$	7,14	V
	$V_{\pi DC3}$	14,24	V			
déphasages statiques	ϕ_1	1,2	rad	ϕ_2	0,7	rad
	ϕ_3	-0,2	rad			

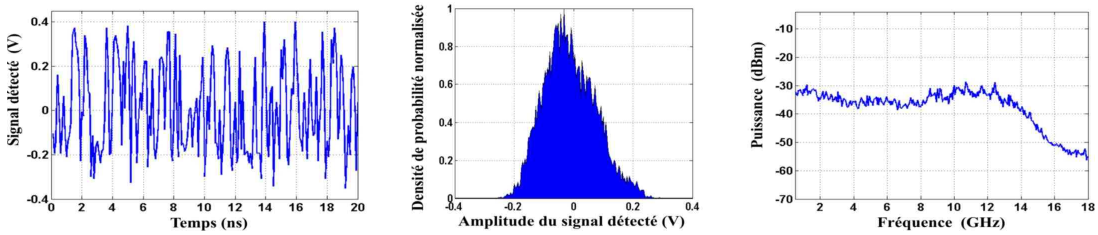
Avec les valeurs numériques indiquées au tableau 1 et selon les gains de rétroaction du système, le dispositif expérimental est capable de générer une multitude de régimes dynamiques, depuis le point fixe stable

jusqu'aux régimes chaotiques entièrement développés. À titre d'exemples, la figure 3 illustre un régime périodique, de période fonction des deux délais du système, correspondant à des gains de rétroaction considérés comme des gains modérés ($\beta_a \sim 1,2$; $\beta_b \sim 0,4$). En augmentant suffisamment et seulement un seul gain de rétroaction ($\beta_a \sim 5$), un régime chaotique entièrement développé est observé (figure 4). Ce régime possède les propriétés d'un bruit blanc gaussien (certes spectralement délimité par la bande passante d'environ 13 GHz du système).



(a) Trace temporelle (b) Profil statistique (c) Spectre de puissance

Fig. 3. *Régime périodique observé expérimentalement.* ($\beta_a \sim 1,2$; $\beta_b \sim 0,4$);



(a) Trace temporelle (b) Profil statistique (c) Spectre de puissance

Fig. 4. *Régime chaotique entièrement développé.* ($\beta_a \sim 5$; $\beta_b \sim 0,4$);

3 Synchronisation du système implémenté

Même si l'architecture du récepteur est très proche de celle de l'émetteur par certains aspects (mêmes blocs fonctionnels, mêmes composants), il n'en reste pas moins différent : le signal chaotique masquant le message est traité par deux voies différentes (voire la figure 1). En effet, grâce à un coupleur optique (1 entrée /2 sorties), le signal chaotique reçu est divisé en 2 signaux optiques. Le premier est directement détecté et converti en électrique par une photodiode rapide, puis amplifié pour fournir à la fin **le signal de référence** (noté par : X). Le second signal optique est combiné avec la contre-réaction de la boucle ($\tilde{A}$) à l'aide d'un coupleur optique variable (2 entrées/1 sortie), qui se caractérise par *un taux de couplage variable* C. Le signal optique ainsi combiné parcourt les mêmes éléments que le signal de contre-réaction de la boucle (A) de l'émetteur. La récupération du signal à la sortie du récepteur s'effectue à l'aide d'un autre coupleur optique (1 entrée /2 sorties) *via* la boucle ($\tilde{A}$). Ainsi, après une conversion optique / électrique et une amplification RF, ce signal représente **le signal du chaos répliqué** (noté par : Y).

3.1 Condition de couplage

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 "clés" (secrets) du récepteur et de l'émetteur. Lorsque ces éléments sont identiques, l'estimation de l'erreur de synchronisation peut déterminer les conditions de couplage, pour lesquelles l'émetteur (maître) pilote les oscillations du récepteur (esclave). Cette erreur est calculée à partir de la valeur quadratique moyenne normalisée (3), où le nombre d'échantillons N des traces temporelles

est pris assez grand, loin des transitoires, afin de s'assurer que l'ensemble des fréquences, des plus rapides aux plus lentes, soient présentes dans l'évaluation de l'erreur.

$$\varepsilon_{synchro}(C) = 100 \cdot \left(\frac{1}{N} \sum_{n=1}^{N} (Y - X)^2 \right)^{\frac{1}{2}} \cdot \left(\frac{1}{N} \sum_{n=1}^{N} X^2 \right)^{-\frac{1}{2}} \qquad (\%) \tag{3}$$

Lorsque l'appariement parfait des deux sous-systèmes est réalisé, la figure 5a montre que cette erreur de synchronisation dépend à la fois du taux de couplage C et du gain global de l'une des boucles du système (ici β_b). Globalement, la synchronisation s'établit lorsque l'asservissement du récepteur tend vers le couplage total ($C = 1$: la boucle $(\tilde{A})$ est ouverte) et l'un des gains de boucle est faible. Dans le cas contraire, à cause de la sensibilité du système aux conditions initiales et de l'influence de la modulation chaotique de l'information, le récepteur est capable de générer ses propres oscillations indépendamment de l'émetteur ; il devient dans ce cas un oscillateur chaotique désynchronisé.

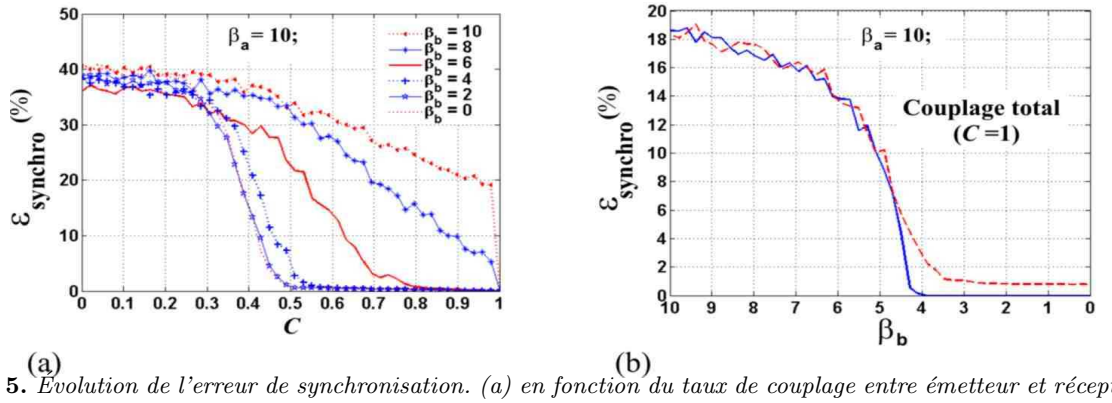


Fig. 5. *Évolution de l'erreur de synchronisation. (a) en fonction du taux de couplage entre émetteur et récepteur. (b) en fonction du paramètre de bifurcation β_b en couplage total.*

En adoptant le couplage total comme solution de pilotage du récepteur par l'émetteur, la figure 5b illustre l'estimation de l'erreur en fonction de l'un des gains de boucle. La courbe en trait continu représente l'évolution de celle-ci, lorsque son origine est due essentiellement à la différence des états initiaux de fonctionnement. À partir de cette courbe, on déduit que le système se synchronise dans un certain intervalle du paramètre de bifurcation ($\beta_b \leq 4$). Mais comme le montre l'autre courbe en trait pointillé, cet intervalle se réduit légèrement lorsque s'ajoute aux conditions de différence précédentes les conditions les plus probables de fonctionnement du système physique, à savoir des désaccords de paramètres entre l'émetteur et le récepteur. Dans le cas étudié, les paramètres en question sont les gains de boucle et les bandes passantes des filtres, et le désaccord est de ± 1%.

3.2 Codage/décodage d'une information numérique

Lorsque le système est considéré totalement synchronisé (le temps nécessaire à la synchronisation correspond grossièrement à la durée des régimes transitoires estimée à $6\,\theta_b = 31,8\,\mu$s), avec la mise en application des conclusions de la section 3.1, nous avons inséré au niveau de l'émetteur un message binaire codé NRZ (Non Return to Zero). Ce message est une séquence numérique générée aléatoirement (figure 6a), dont la durée d'un bit est de 300 ps (débit binaire $\approx 3,3$ Gbit/s). La restitution de l'information en clair (décodage) s'effectue au niveau du récepteur par une opération de soustraction entre les deux signaux de référence et du chaos répliqué. Cette restitution peut être formalisée par :

$$s(t) = \underbrace{\widetilde{k}_1 \cdot \left[f_{NL}\left[x_a, x_b\right](t - T_a) + \alpha \cdot m(t) \right]}_{X} - \underbrace{\widetilde{k}_2 \cdot \widetilde{f}_{NL}\left[\widetilde{x}_a, \widetilde{x}_b\right](t - \widetilde{T}_a)}_{Y} \tag{4}$$

où $s(t)$ est le signal décodé dépendant fortement de la similarité des deux non linéarités 2D réalisées ; $\widetilde{k}_1$ et $\widetilde{k}_2$ sont des gains d'amplification ; $m(t)$ est le message utile ; α est un taux de masquage, défini comme étant le rapport entre l'amplitude du message et l'amplitude du signal chaotique. Comme le montre les résultats numériques des figures 6b et 6c, ce taux de masquage joue un rôle déterminant par rapport à la qualité de masquage de l'information. La sécurité de la transmission se trouve renforcée par un taux faible au détriment de la qualité de synchronisation.

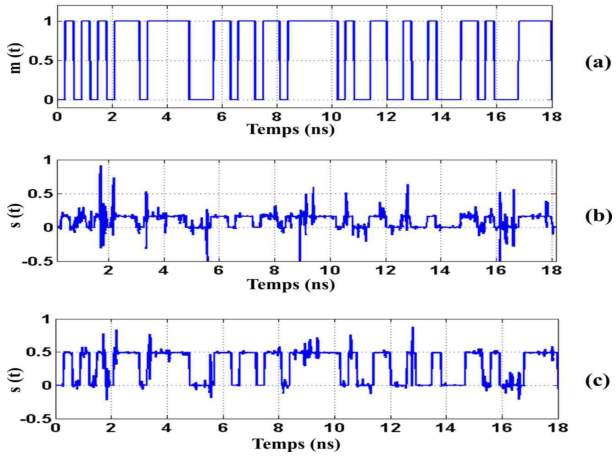


Fig. 6. *Cryptage/décryptage d'un message binaire codé NRZ avec couplage total* ($C = 1$); $\beta_a = 10$; $\beta_b = 2,2$; (*a*) *Message utile en clair.* (*b*) *Message décodé à* $\alpha = 3$ *%.* (*c*) *Message décodé à* $\alpha = 15$ *%.*

4 Conclusion

Nous avons présenté un système optoélectronique de cryptage/décryptage physique en temps réel de données optiques sécurisées par chaos sur la variable intensité optique. Ce système basé sur une dynamique non linéaire à retard est original par son architecture reconfigurable de double boucle, robuste par le nombre de paramètres physiques de sa clé cryptographique, et compatible avec les télécommunications optiques haut débit.

Le travail va désormais se concentrer sur la cryptanalyse du chaos produit, et sur l'estimation des performances expérimentales du système global, en termes de qualité de la réplication du chaos, de celle du masquage et du taux d'erreur binaire.

Références

1. L. M. Pecora, T. L. Carroll, Synchronization in chaotic systems, *Physical Review Letters*, **64** (8), 821-824 (1990).
2. G. VanWiggeren, and R. Roy, Optical communication with chaotic waveforms, *Physical Review Letters*, **81**(16), 3547-3550 (1998).
3. L. Larger, J. P. Geoddgebuer, and V. Udaltsov, Ikeda-based nonlenear delayed dynamics for application to secure optical transmission systems using chaos, *Comptes-Rendus de l'Académie des Sciences* (Physique), **5**, 669-681 (2004).
4. R. Lavrov, M. Peil, M. Jacquot, L. Larger, V. Udaltsov, and J. Dudley, Electro-optic delay oscillator with nonlocal nonlinearity : Optical phase dynamics, chaos and synchronization, *Physical Review E*, **80**, 026207(1-9) (2009).
5. K. Ikeda, Multiple-valued stationary state and its instability of the transmitted light by a ring cavity system, *Optics Communications*, **30** (2), 257-261 (1979).
6. M. Nourine, M. Peil, and L. Larger, Chaos généré par une non linéarité 2D et une dynamique à retard, *Comptes-Rendus de la* 12*ème Rencontre du Non Linéaire*, 149-154 (2009).