Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Physique 5 (2004) 609–611
COMPTES RENDUS PHYSIQUE

Cryptography using optical chaos/Cryptographie par chaos optique

Encryption using chaotic dynamics for optical telecommunications

Laurent Larger [a,b,*], Jean-Pierre Goedgebuer [a,b]

[a] *GTL-CNRS Telecom/UMR FEMTO-ST 6174, 2–3, rue Marconi, 57070 Metz cedex, France*
[b] *FEMTO/Optics Department, UMR CNRS 6174, université de Franche-Comté, 16, route de Gray, 25030 Besançon cedex, France*

Presented by Guy Laval

Abstract

Chaos-based encryption appeared recently in the early 1990s as an original application of nonlinear dynamics in the chaotic regime. While the first experimental realizations were made in Electronics, the Optics community rapidly showed a strong interest in this new scientific application due to the well-known feature of Optics in the area of nonlinear phenomena. Numerous optical demonstrations have been performed, involving chaotic dynamics with particularly interesting properties in terms of chaos complexity, and also in terms of bandwidth i.e., encryption speed. This special issue gives a review of most of the current works on optical chaos dedicated to encryption. ***To cite this article: L. Larger, J.-P. Goedgebuer, C. R. Physique 5 (2004).***

Résumé

Dynamiques Chaotiques Appliquées à la cryptographie pour les télécommunications optiques. La cryptographie par chaos est apparue récemment au début des années 90, comme une application originale des dynamiques non linéaires en régime chaotique. Alors que les premières réalisations ont été mises en œuvre à partir de circuits électroniques, l'optique s'est rapidement intéressée au sujet. Grâce à des propriétés physiques particulières et familières dans le domaine de l'Optique, de nombreux démonstrateurs originaux et variés ont été développés, fonctionnant avec des dynamiques chaotiques aux propriétés attractives, tant en terme de complexité des régimes chaotiques, qu'en terme de bande passante, et donc de vitesse de codage. Ce numéro spécial passe en revue la plupart des travaux actuels sur les systèmes cryptographiques par chaos en optique. ***Pour citer cet article : L. Larger, J.-P. Goedgebuer, C. R. Physique 5 (2004).***

Keywords: Optical telecommunication; Chaos; Encryption

Mots-clés : Télécommunications optiques ; Chaos ; Cryptographie

With the advent of world wide networks and digital communication techniques, cryptography was brutally transfered from a very restricted area i.e., the military domain, diplomacy, state affairs, to a very broad area covering, at the same time, the previous domains, but also private companies, medical and bank information, electronic payment on the internet, etc. Security and secrecy are becoming fundamental requirements for everyone, in the present day communication society, thus justifying the number of current research activities on new and/or alternate encryption methods. Within this research domain, and apart from the most general encryption techniques based on software algorithms, two original cryptographic methods based on physical

* Corresponding author.
E-mail address: laurent.larger@georgiatech-metz.fr (L. Larger).

1631-0705/$ – see front matter
doi:10.1016/j.crhy.2004.05.004

principles have appeared as physically and technologically feasible during the last two decades: quantum cryptography, and chaos cryptography. The first is mainly dedicated to absolute security secret key distribution, in which the key can then be used to transmit securely information by conventional algorithm based encryption. The second method is also involved at the level of the physical layer in transmission systems, with the advantage of allowing potentially a very high encryption speed (up to several tens of Gb/s, unlike algorithm-based encryption softwares that is typically limited to a few hundreds of Mb/s).

The genesis of encryption using chaos started with the demonstration of the synchronization of two coupled chaotic trajectories [1]. The synchronization property for such waveforms was thought initially to be non realistic, due to the intrinsic natural tendency of two quasi-identical chaotic dynamics to diverge one from another, due to the so-called Sensitivity to Initial Conditions, popularly called the 'Butterfly effect'.

In communication theory, the possibility of synchronization of a given waveform, sinusoidal or not, means generally that the waveform can be used as an information carrier in a transmission system; the synchronization is then used at the receiver to retrieve the carried information. Moreover, when the waveform features a pseudo-random character, a privacy property of the communication can be expected, together with the carrier capability: this is typically the case for the well-known digital transmission technique, the Code Division Multiple Access or CDMA, used in the Global Positioning System (GPS), and for the third mobile phone generation. Briefly, CDMA involves long pseudo-random bit sequences as a carrier waveform for each user channel, whose carrier is consequently broadband due to the pseudo-random character. The sequence acts as a code, without which the decoding and the retrieving of the encoded information can not be performed, and the transmission is made secure through the use of this pseudo-random carrier. Similarly, it was assumed in the early 1990s that chaotic waveforms could be used as an information carrier signal, and at the same time as a means to protect the carried information due to its pseudo-random and broadband character. The intrinsic determinism of the chaotic dynamics i.e., the mathematical law ruling their trajectories, is, of course, the milestone of the synchronization technique.

The first experimental demonstration of information transmission using a chaotic carrier followed quite rapidly that of the synchronization principle in 1993 [2]. The chaos generator of concern was an electronic circuit generating a Lorenz type chaotic oscillation embedded in a 3-Dimensional phase space. The first cryptanalysis of such a system followed even faster [3], highlighting that a low chaos complexity was definitively a weakness of the cryptosystem. Nonlinear dynamics in Optics (laser dynamics, large delay optical or optoelectronic cavities) were well known for their ability to produce high complexity dynamics. Different groups revisited independently various such optical systems for application to chaos encryption systems, from the theoretical point of view [4] (external cavity semiconductor laser), and from the experimental point of view as well [5] (synchronization of chaotic external cavity semiconductor lasers; [6], encryption/decryption with chaotic Erbium doped fiber lasers; [7], encryption/decryption with chaotic laser wavelength; [8], synchronized chaos in microchip lasers; [9], GHz synchronization between external cavity semiconductor lasers). All of these results were obtained with optical systems, due to the following reasons:

- these systems are, of course, intrinsically dedicated to modern communication systems using optical fibers;
- the dynamical processes involved in optical systems can be fast, thus resulting in another interesting feature of chaos-based optical cryptosystems, their potentially very high encryption speed;
- high complexity chaotic dynamics are obtained, whether due to intrinsic complex nonlinear coupling between light and matter interactions in lasers, or due to the presence of a large delay feedback cavity enabling dynamics with large number of degrees of freedom.

Cryptanalysis of such optical chaos cryptosystems has been so far more difficult to implemente than that of the first electronic set-ups. Only Erbium fiber laser chaotic dynamics was shown to be analyzed with enough detail, with the disadvantage that the chaos thus generated can be broken and the message easily retrieved. The lack of complexity inherent to the weak nonlinearity attached to the fiber laser dynamics is responsible for the success of the cryptanalysis attack [10]. Cryptanalysis of the other chaos encryption systems are still under progress, but they are much more oriented towards techniques usually devoted to nonlinear dynamics analysis, the linear techniques being definitively not sufficient to retrieve enough information from the chaotic time series masking the message.

The optical chaos-based cryptosystems reported in this special issue exhibit most of the above mentioned characteristics. However, the set-ups of interest are described by different nonlinear dynamical models, whose fundamental relevance in terms of confidentiality and transmission quality is still one of the remaining open questions in the field. Among these set-ups, the dynamics of the external cavity lasers (see Fig. 1, upper left) involve linear feedback delay terms, whereas the nonlinear operation consists in a coupling in the rate equations between the optical field amplitude and the inversion population density. The situation is different for optoelectronic encryption systems, for which the delayed feedback has two particularities: it is nonlinear, and it is optical phase insensitive due to the electronic nature of the feedback. The latter situation is, however, explored in two distinct schemes. In the first one (Fig. 1, upper right), the differential process still originates from the laser rate equations, in which the nonlinear coupling between the population inversion density and the optical field amplitude involves a

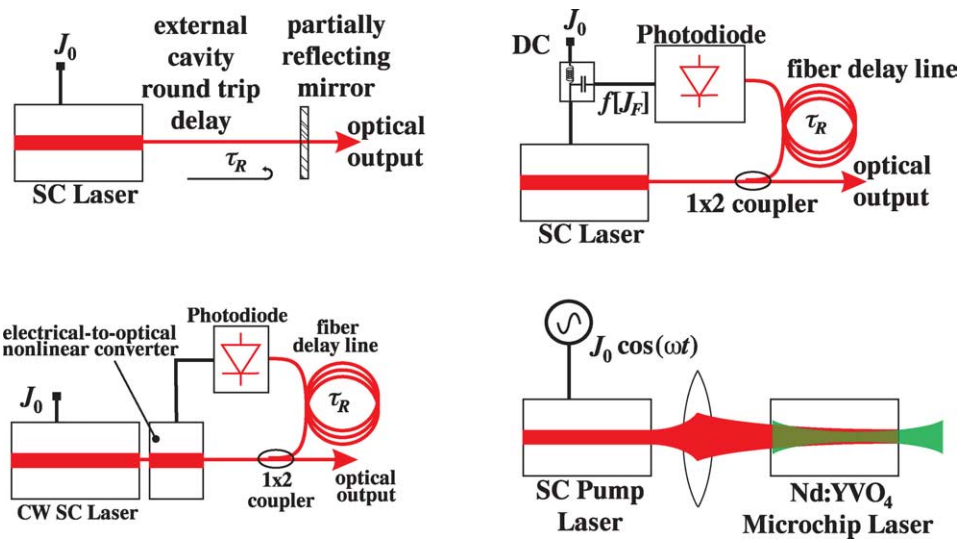

Fig. 1. Four sub-class of nonlinear dynamics in Optics mostly involved in optical chaos generation for encryption.

delay term originating from the feedback signal acting on the electronic pumping strength. In contrast, in the other optoelectronic feedback scheme (Fig. 1, lower left), the differential process is determined by the linear filtering performed by the electronic part of the oscillator feedback; this filtering is applied to a scalar nonlinear feedback transformation. Finally, the fourth setup (Fig. 1, lower right) involves nonlinear coupled rate equations in a solid state laser between population inversion and the optical electric field, when the population inversion is driven by an externally modulated pump laser. The security (synchronization capability) of the chaos communication schemes using the previous optical chaos generators relies essentially on the extreme synchronization sensitivity with respect to the physical parameters and exact operating conditions, these latter constituting the key of the encryption method. Without the exact knowledge of the chaos generator set-up used at the emitter, it is highly difficult for an unauthorized receiver to reproduce the right chaotic waveform which can synchronize with the one transmitted, thus enabling the message recovery.

Such a diversity in the experimental optical chaos generator is very positive for the definition of the optimal architecture, as well as for competition within the scientific community involved in chaos-based encryption systems. Work is still under progress to explore the best configuration, and also new configurations, that could be implemented in the future at the physical layer of a multi-Gbits/s fiber network.

References

[1] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821.
[2] K.M. Cuomo, A.V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65.
[3] Th. Beth, D.E. Lazic, A. Mathias, Lect. Notes in Comput. Sci. 839 (1993) 318.
[4] C. Mirasso, P. Colet, P. Garcia-Fernandez, IEEE Phot. Techn. Lett. 8 (1996) 299.
[5] V. Annovazzi-Lodi, S. Donati, A. Scire', IEEE J. Quantum Electron. 33 (1997) 1449.
[6] G.D. VanWiggeren, R. Roy, Science 279 (1998) 1198.
[7] J.-P. Goedgebuer, L. Larger, H. Porte, Phys. Rev. Lett. 80 (1998) 2249.
[8] A. Uchida, M. Shinozuka, T. Ogawa, F. Kannari, Opt. Lett. 24 (1999) 890–892.
[9] I. Fischer, Y. Liu, P. Davis, Phys. Rev. A 62 (2000) 011801(R).
[10] J.B. Geddes, K.M. Short, K. Black, Phys. Rev. Lett. 83 (1999) 5389.