Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Physique 5 (2004) 669–681
COMPTES RENDUS PHYSIQUE

Cryptography using optical chaos/Cryptographie par chaos optique

Ikeda-based nonlinear delayed dynamics for application to secure optical transmission systems using chaos

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

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

Presented by Guy Laval

Abstract

The pionneering work of Ikeda initiated the investigation in Optics of dynamical systems described by nonlinear delayed differential equations (NLDDEs). Our group has developed in optoelectronics similar dynamical systems intended for practical implementation of chaos-based encryption demonstrators. Different set-ups have been implemented making use of various optical variables, such as the wavelength, the intensity, the optical path difference or the optical phase, each of them exhibiting different advantages (chaos complexity, encryption speed, masking efficiency, encryption key size). A general architecture of NLDDE chaos generators and some of their related dynamical properties are reported, as well as the implementation in practical encryption systems using chaotic dynamics. Security issues, performance, and future developments of those systems are also addressed. ***To cite this article: L. Larger et al., C. R. Physique 5 (2004).***

Résumé

Dynamiques non linéaires à retard d'Ikeda appliquées à un système de transmission optique sécurisé par chaos. Les travaux précurseurs d'Ikeda ont marqué le début de l'exploration en optique des systèmes dynamiques décrits par des équations différentielles non linéaires à retard (EDNLR). Notre groupe s'est inspiré de ces travaux pour mettre au point en optoélectronique des démonstrateurs de systèmes cryptographiques par chaos. Plusieurs montages expérimentaux ont été mis au point à partir de variables dynamiques physiques différentes, comme la longueur d'onde, l'intensité, la différence de chemin optique, ou encore la phase optique, chacune d'elles présentant des propriétés particulières (la complexité du chaos, la vitesse de codage, l'efficacité de masquage, ou encore la taille de la clé de cryptage). Une architecture générale de réalisation d'EDNLR est présentée, ainsi que son principe d'implémentation dans un système complet de cryptographie par chaos pour les télécommunications optiques. Les problèmes de sécurité, les performances, et les développements à venir de ce type de systèmes sont évoqués. ***Pour citer cet article : L. Larger et al., C. R. Physique 5 (2004).***

Keywords: Optoelectronic oscillator; Delayed nonlinear dynamics; Chaos; Encryption using chaos

Mots-clés : Oscillateur optoélectronique ; Dynamique non linéaire à retard ; Chaos ; Cryptographie par chaos

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

1631-0705/$ – see front matter
doi:10.1016/j.crhy.2004.05.003

1. Introduction

Nonlinear delay differential dynamics have known a growing interest in the last 25 years in Optics, through numerous theoretical, numerical, and experimental investigations [1–4]. These dynamics were explored at the early beginning mainly for fundamental interests [5,6]. Such an interest is due to, among other reasons, an amazing feature: these dynamical systems exhibit extremely complex chaotic behaviour (with arbitrarily high attractor dimension), although their mathematical description can be as simple as a scalar first order differential equation:

$$y(t) + \tau \cdot \frac{\mathrm{d}y}{\mathrm{d}t}(t) = \beta \cdot f\big[y(t - \tau_R)\big]. \tag{1}$$

A rapid analysis of Eq. (1) highlights some of the most important properties of such dynamics. The left-hand side is typical of a stable linear first order dynamics, with a characteristic response time τ; its role is only to limit the fastest oscillations time scale. The right-hand side contains a nonlinear function $f[\cdot]$ applied to the delayed dynamical variable $y(t - \tau_R)$; the nonlinear function is practically bounded for physical reasons. The delay forces the natural dynamic phase space to be infinite dimensional: instead of a single initial condition $y(t_0)$ as usually required for a first order differential equation to determine a solution uniquely, an infinite number of values is needed to define the necessary functional $y(t)$ over the time interval $[t_0 - \tau_R; t_0]$. The importance of the role of the nonlinear transformation in the high complexity chaotic behavior [6] is determined by two main factors (see Fig. 1):

- its strength, through the amplitude of the magnification factor β (usually considered as the bifurcation parameter); this parameter can be considered as a weight of the nonlinear delayed feedback terms in the dynamical process, thus influencing the amplitude Δy of the dynamical variable; the role of β is typically the stretching operation usually of concern in chaotic dynamics;
- the number of extrema of $f[\cdot]$ concerned by the fluctuation interval Δy; in that interval, $f[\cdot]$ can be approximated by a polynomial function of order N, where N could be a measure of the actual nonlinear function complexity concerned by a given dynamical regime; the role of the extrema is typically the folding operation, which is also required in chaotic dynamics, together with the stretching operation; for $N = 2$ (the equivalent polynomial function is a parabola), one could find many similar behaviors in the solutions of Eq. (1), with respect to the well known logistic map [9].

Both of these, the nonlinear transformation (magnified by a factor β, bounded, and at least with one extremum), and the delay (usually much greater than τ) are the key elements in the generation of a high dimensional chaotic process. They play a major role for the security when encryption using chaos is of concern. A major advantage of Optics, is their easy experimental implementation.

Independently of the interest in time delay dynamics initiated in 1979 in Optics, a particular application of nonlinear dynamic appeared in the early 1990s [7,8]: secure communications using chaotic waveforms. The feasibility was demonstrated using electronic circuits, which were used for the generation of chaotic dynamics modeled by 'standard' nonlinear ordinary differential equations. Although the demonstration was successful, these electronic set-ups were plagued by a low dynamical complexity, which consisted in a weakness in terms of encryption efficiency. Due to their extreme intrinsic complexity, as well as their attractive feature in view of modern high speed optical telecommunications, delay systems in Optics became very interesting candidates for exploring encryption using chaos [10–17]. This article reviews the research activities on chaos based communications developed by our group, making use of the particular Ikeda–type nonlinear delay dynamics to generate chaos.

After a first analysis of the physical principles and some of the mechanisms involved in the precursor setup of the Ikeda ring cavity, a general architecture is deduced for generating experimentally nonlinear delay differential dynamics. Using these

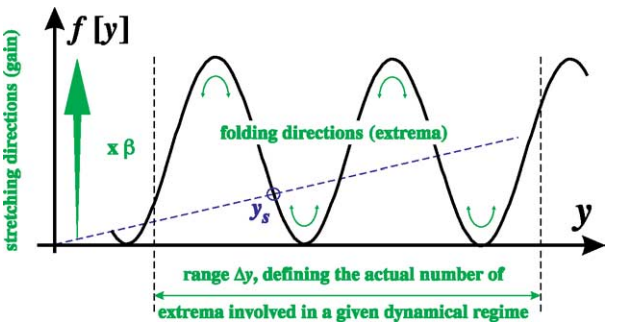

Fig. 1. Important properties of the nonlinear function acting on the delayed variable in Eq. (1).

chaos generators, a particular concept for implementing a chaos-based encryption system is reported. Illustrations are given through different optoelectronic setups and experimental characterizations, in terms of nonlinear dynamics, and also in terms of chaotic secure communication. Security issues and future developments of the Ikeda setups for chaotic secure communication are developed in the last section.

2. From the Ikeda ring cavity to chaos-based communication

2.1. The Ikeda setup, its dynamics and complexity

The brain experiment imagined by Kensuke Ikeda in 1979 is depicted in Fig. 2(a). It consists in:

- An input laser beam with constant optical intensity I_0; this quantity is an important parameter for the tuning of a given dynamical regime observed at the system output. The coherence of the laser light ensures the existence of interferences between the input light beam, and the one fed back by the cavity after one round trip.
- A ring cavity comprising two partial reflecting mirrors, one for the input and one for the output. The length L of the cavity determines a round trip time of the light beam, which defines the delay $\tau_R = L/c$ (where c is the velocity of light). Intensity and/or phase modulation observed at the cavity output is thus fed back to the cavity input with a delay τ_R.
- A 2-level atomic cell, in which light–matter interaction occurs. In a simplified model, only the Kerr effect is considered. Under these conditions, the phase of the light beam propagating through the cell is changed proportionally to its intensity $I_{\text{in}}(t)$. This phase change is expressed as $2\pi\, n_2\, I_{\text{in}}(t)\, l/\lambda$, where l is the medium length, λ is the laser wavelength, and n_2 is the Kerr refractive index coefficient. Notice also that the dynamics of this light–matter interaction is extremely fast since it is determined by the level lifetime τ of the atomic cell, thus leading to dynamical fluctuations much faster than the round trip time τ_R.
- At the atomic cell input, a two-wave interference occurs between the constant intensity cavity input beam, and the intra-cavity feedback beam, whose phase is determined by the τ_R-previous intensity interference through the Kerr effect in the atomic cell.

The dynamics of the cavity output intensity $I(t, I_0)$ can then be described by the nonlinear delay differential equation in Eq. (1), in which the nonlinear function corresponds to the transformation law of the input phase into an output intensity (the intensity of a two-wave interference figure, typically the $\sin^2$-curve shown in Fig. 1).

According to this description, the physical setup appears as an oscillator, with a feedback loop comprising a strong nonlinearity ($\beta\, f(x)$), and a delay (τ_R). This delay is large compared to the characteristic response time (τ) of the limiting dynamics. A block diagram can then be used to generalize this oscillation principle, as depicted in Fig. 2(b). The linear tuning is representative of the optical phase change rate with respect to the optical intensity through the Kerr effect. The nonlinear transformation $f(x)$ is physically generated by the interference after the optical feedback at the cavity input. The cavity length determines the delay τ_R, and the dynamics limitation is fixed by the atomic cell level lifetime τ.

A first and simple approach to the oscillator dynamics in the case of large delays ($\tau_R \gg \tau \simeq 0$) usually involves the adiabatic approximation. It consists in neglecting the derivative term in Eq. (1). The continuous time dynamics is then expressed as discrete time dynamics, for which the time evolution is a sequence of discrete values of the dynamical variable y over the time interval τ_R. Labelling each τ_R–time interval with an integer n, the dynamics are reduced to a 1D-mapping $y_{n+1} = \beta \cdot f(y_n)$ (where f is similar to the plot in Fig. 1). The oscillator feedback is then equivalent to an iteration process, returning the vertical axis value y_{n+1} onto the horizontal axis. This operation can be represented graphically with the first bisector straightline, which intersects the nonlinear function at the steady states values (defined as the solutions of $y_s = \beta\, f(y_s)$). The stability of these steady states can be determined by a first order analysis, leading to the following result: the steady state is stable if the absolute

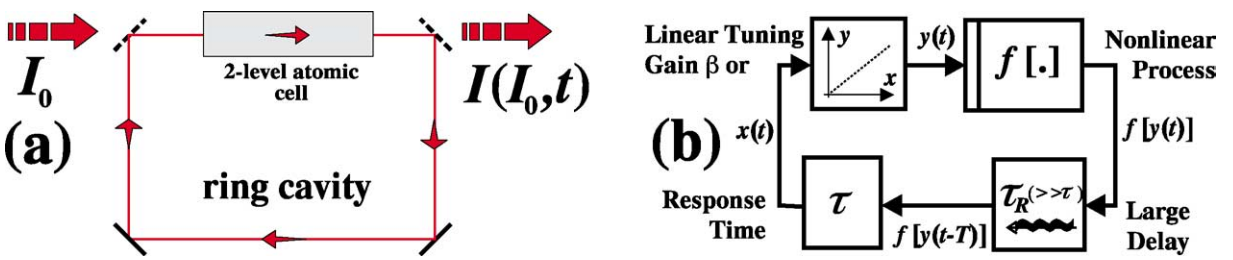

Fig. 2. The Ikeda ring cavity: (a) the experiment; (b) a block diagram interpretation.

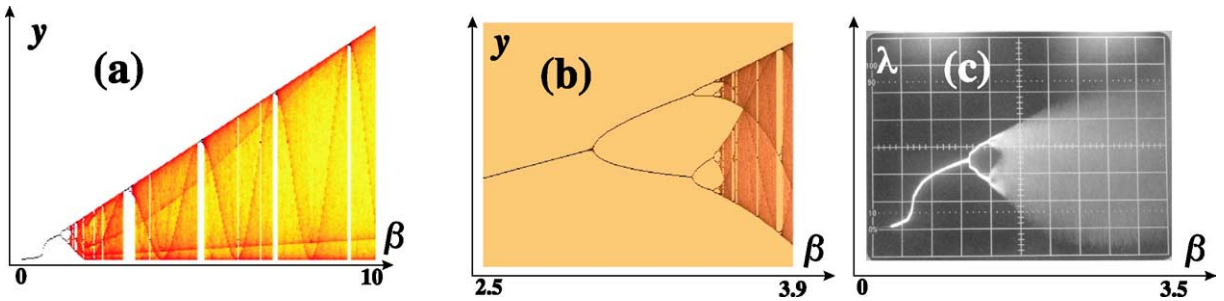

Fig. 3. Bifurcation diagrams for (a) the $\sin^2$-map; (b) the logistic map; and (c) experimental $\sin^2$-delay differential dynamics.

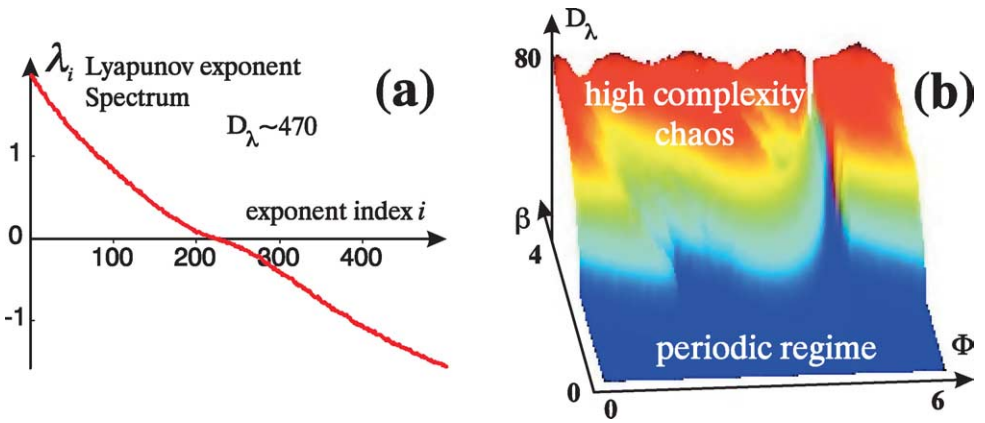

Fig. 4. Lyapunov exponents and dimension calculation from the Ikeda dynamical model: (a) Lyapunov spectrum in the chaotic regime with $\beta = 20.5$, $\Phi = 2.1$ and $\tau_R/\tau = 60$; (b) Lyapunov dimension calculation in the (β, Φ)-plane.

value of the slope $|f'(y_s)|$ is lower than 1, otherwise it is unstable. Increasing the feedback gain β (or the slope of the linear tuning element in Fig. 2(b)) changes the number of the steady states, as well as the slope, at these positions. This is the reason why β is usually considered as a bifurcation parameter of the system. For low values of β, a single steady state exists and is necessarily stable. When increasing β, the steady states loses their stability and periodic regimes are observed. For sufficiently large values of β, high complexity chaotic regimes are observed. They are the regimes of interest for chaos encryption (see the bifurcation diagram in Fig. 3(a)). Between the low and high β-values, a period doubling route to chaos is observed when increasing β, in a way similar to that of the well-known logistic map (Fig. 3(b)) [9].

When comparing the two first bifurcation diagrams, it can be qualitatively noticed that the multiple extrema nonlinear function allows a broad range of values for the bifurcation parameter, and high complexity chaotic dynamics are obtained. On the other hand, the parabola has a very limited range of chaotic regime due to the single extremum. This property is related both to the unbounded character of the parabola and to the single extremum character. The case of a delay dynamical system involving a bounded nonlinear function with a single extremum has been intensively studied in the literature; it is referred as the Mackey–Glass model in Medicine, which describes hematological disorder [18]. It was shown that a limited complexity only can be obtained for high values of the bifurcation parameter β, unlike the Ikeda model, which differs by the single extremum nature of the nonlinear function ($f(y) = y/(1 + y^{10})$). This result confirms that the Ikeda model with its multiple extrema nonlinear function is a good candidate for chaos generation dedicated to encryption.

The actual dynamics complexity of the Ikeda model is even better when considering a non–zero response time τ. The dynamics is thus no longer a discrete mapping, it has to fluctuate continuously in time according to Eq. (1). An experimental bifurcation diagram of such a continuous time delay dynamics is represented in Fig. 3(c). The qualitative profile of the bifurcation diagram is not dramatically changed compared to the discrete time case (Fig. 3(a)), however the dynamics complexity is strongly improved. The phase space dimension of the dynamical system is indeed increased from 1 to infinity. The definition and the measure of the actual complexity of such nonlinear delayed systems is not yet a solved problem. However, there exists a computation method intended to evaluate this complexity in terms of the finite attractor dimension [5]. When applied to the Ikeda dynamics [6], this method gives the Lyapunov spectrum of a given chaotic regime in a reconstructed phase space of finite dimension. Such a spectrum is represented in Fig. 4(a) for parameter values related to a real experimental

situation. The spectrum plots the Lyapunov exponents arranged in decreasing order. Each exponent is representative of an expanding (if it is positive) or contracting (if it is negative) direction along the chaotic trajectory in the reconstructed phase space. From this spectrum, one can calculate a Lyapunov dimension, which is conjectured to be equal to the information dimension of the chaotic regime [19]. For the example represented in Fig. 4(a), the numerous positive exponents lead to a Lyapunov dimension as high as 470, thus indicating a high complexity for the chaotic regime. A 3D Lyapunov dimension calculation is also given in Fig. 4(b) for the same dynamics, in the (β, Φ) parameter plane. It shows the wide parameter range for which high complexity chaos can be obtained (dimensions greater than 50, even for small β-values).

The Lyapunov dimension is an interesting parameter to consider in terms of chaos complexity. However, its linear dependence with the ratio τ_R/τ ([6]) reveals a default of relevance, since the increase of the delay does not implies an increase of the number of parameters needed to define the dynamics (only the value of the delay is modified); a larger delay increases the required number of initial conditions needed to determine a given solution of the dynamics, thus measuring the 'memory size' of the delayed dynamics. The Lyapunov dimension, however, also increases linearly with the feedback gain β in the case of a multiple extrema nonlinear function. This situation, in the contrary of the delay dependence, represents an actual increase of complexity. The exact shape of the additional extrema contributing to the dynamics, is indeed required to determine exactly the dynamics corresponding to a larger β. To distinguish this fundamental difference between the delay dependence and the feedback gain dependence, the Lyapunov entropy appears to be a much better indicator than the Lyapunov dimension. The entropy saturates with the increase of the delay above a certain value, whereas it increases linearly with β, as long as the β increase implies an increase of the number of extrema participating to the chaotic dynamic (and hence the number of folding dynamical processes); typically the entropy also saturates in β with the Mackey–Glass dynamics, which involves a single extremum nonlinear function, even for high values of β.

For the previous fundamental reasons, Ikeda-based dynamics dedicated to chaos encryption must involve a nonlinear function $f(y)$ with a high number of extrema, as far as security aspects are related to chaos complexity. Such a situation is effectively met with the Ikeda dynamics for high β-values (typically > 5).

2.2. Encoding and decoding technique

The complex chaotic regimes required for chaos communication are generated using nonlinear delay dynamics as described in the previous section. In order to present the encoding and decoding technique typically used in our experiments, we will use first an open loop chain representation as depicted in Fig. 5(left). The different elements required for a nonlinear delayed dynamics are gathered into a single block labelled as NLDDP, standing for nonlinear delayed dynamical process.

When the NLDDP output is fed back to its input as done at the emitter side, we obtain the nonlinear delayed oscillator that generates the chaotic waveform (see Fig. 5(right)). To mix a message $m(t)$ within the chaotic carrier, we add it inside the oscillation loop. The message thus participates to the chaotic oscillation, with an influence depending on its relative weight with respect to the chaos. The relative amplitude of the message with respect to that of the chaos determines the so–called masking efficiency. A high masking efficiency corresponds to a well hidden message inside the chaos, and at the same time a weakly perturbed chaos. The sum (chaos + message) is fed back to the input of the NLDDP, and also serves as the transmitted signal. Notice that there exists practically several encoding configurations by simply changing the message mixing point [20] with respect to the different elements constituting the NLDDP. For sake of simplicity, only the additive dynamical variable case is explained and illustrated in Fig. 5.

On the receiver side, the NLDDP is reproduced physically, but in an open loop configuration. Its input corresponds to the received signal i.e. the message masked by the chaos. According to the analogy between the emitter and receiver architectures, the output of the receiver NLDDP replicates the same chaotic waveform as that in the emitter. This is sometimes also called 'chaos synchronization', although 'chaos replication' reflects better the phenomenon, since the open loop receiver cannot generate any chaotic waveform without its input signal. Subtracting the replicated chaos from the received signal allows one to recover the information message.

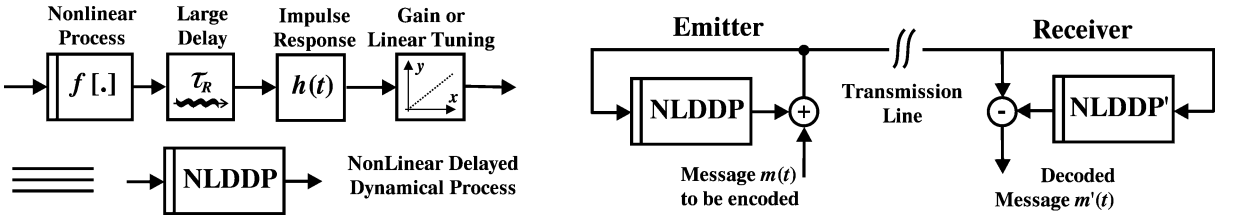

Fig. 5. Encoding and decoding. Left: open loop system approach defining a global nonlinear delayed dynamical process, right: message encryption and extraction schemes.

To demonstrate the decoding, the input / output transfer function of the NLDDP is written here in the time domain using an integral representation of the dynamics, instead of the differential one as in Eq. (1). This involves the impulse response $h(t)$ of the corresponding linear differential operator. In the case of a first order differential process, $\mathrm{Id} + \tau(\mathrm{d}/\mathrm{d}t)$ corresponds to $h(t) = \mathrm{e}^{-t/\tau}u(t)$, where $u(t)$ is the Heaviside function. For a realistic higher order linear dynamical process, $h(t)$ takes a more complicated form. The integral representation allows one to express the instantaneous dynamical variable $y(t)$ as the result of a convolution product of its delayed nonlinear transformation $f[y(t-\tau_R)]$ with the impulse response $h(t)$ of the linear feedback filtering process. The transmitted encrypted signal $s(t)$ is then written as follows:

$$s(t) = \beta\big[h_\theta \star f(s_{\theta-\tau_R})\big] + m(t) = \beta \int_{t_0}^{t} h(t-\theta) f\big[x(\theta-\tau_R)\big]\,\mathrm{d}\theta + m(t) = y(t) + m(t). \tag{2}$$

The chaotic signal generated at the receiver can be similarly written as:

$$y'(t) = \beta'\big[h'_\theta \star f'(s_{\theta-\tau'_R})\big] = \beta' \int_{t_0}^{t} h'(t-\theta) f'\big[s(\theta-\tau'_R)\big]\,\mathrm{d}\theta. \tag{3}$$

For perfect matching conditions between the emitter and receiver elements ($h = h'$, $f = f'$, $\beta = \beta'$ and $\tau_R = \tau'_R$), it is easy to see from Eqs. (2) and (3) that the receiver is able to replicate exactly the chaotic oscillations of the emitter. The message $m(t)$ is obtained straightforwardly when subtracting the generated chaos $y'(t)$ from the received one $s(t)$. In more realistic situations, any parameter mismatch between the emitter and receiver leads to an unavoidable decoding noise, which limits the decoding quality of the extracted message. For a given minimum required decoding quality, one finds a corresponding maximum threshold of the masking efficiency at the emitter (relative amplitudes of the message and of the chaotic carrier).

Experimental realizations of the previously defined chaos generator architecture, and encoding–decoding schemes, will be described in the next section.

3. Optoelectronics set-ups, experimental results

The main drawback for an experimental implementation of the Ikeda ring cavity for encryption by chaos, is the low tuning efficiency of the interference condition due to the Kerr effect. A large variation of the interference condition would require high optical energy levels, which are not usually met in optical telecommunication systems. Following the same idea to perform the nonlinear function through a tunable interference condition, we have:

$$f[y] = \sin^2(\pi\Delta/\lambda), \tag{4}$$

where y represents the dynamical variable used to change the interference condition, which can be either related to the optical path difference Δ, or to the laser wavelength λ. In the Ikeda setup, the dynamical variable is $\Delta(I) = (n_0 + n_2 I)L$, and it varies linearly with an optical intensity through the Kerr refractive index coefficient n_2. In the wavelength chaos generator depicted in Fig. 6, the interference is varied using small wavelength variations, $\lambda(t) = \lambda_0 + \delta\lambda(t)$.

A DBR double electrode wavelength tunable semiconductor laser is used in order to adjust the laser wavelength within a few nm around $\lambda_0 = 1.55$ µm, according to $\delta\lambda = S_\lambda i_{\mathrm{DBR}}$. As depicted in Fig. 6, a 6 cm-long calcite slab ($\Delta \simeq 1$ cm)

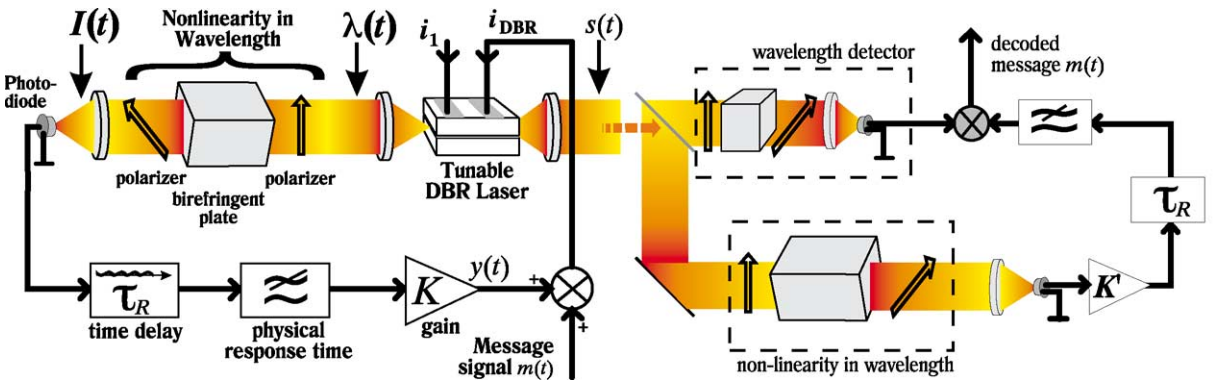

Fig. 6. Emitter–encoder and receiver–decoder using a wavelength chaos generator.

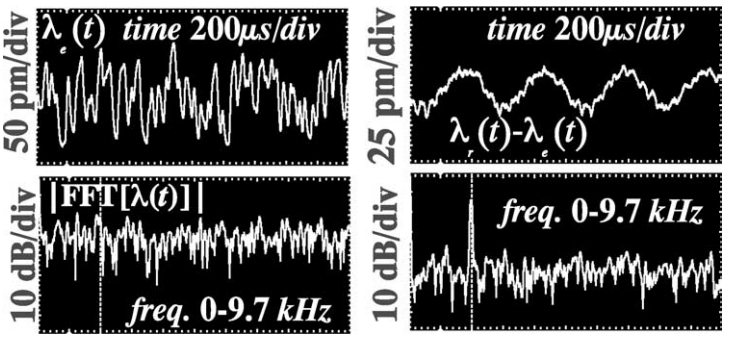

Fig. 7. Encoded and decoded signals with wavelength chaos. Upper: time traces, lower: corresponding spectra.

placed between two crossed polarizers is used as a birefringent interferometer, whose output interference is scanned according to the laser wavelength. Notice that any other spectral filtering (e.g. a more complex multiple wave interference filter like a Fabry-Pérot) can be used to perform the nonlinear transformation, as long as the filter profile exhibits extrema within the wavelength tuning range of the laser. The 1.5 nm continuous range allows one to scan more than 12 extrema of a nonlinear function as depicted in Fig. 1. The resulting intensity is detected by a photodiode, from which the electrical signal is delayed by $\tau_R = 512$ μs with an electronic delay line. After amplification and filtering with an electronic first order low pass filter of cut-off frequency $f_c = 1/2\pi\tau = 18$ kHz, the resulting signal serves as the input current for the laser wavelength tuning. An electronic adder allows one to hide a small amplitude message i_{m} into the large amplitude chaotic feedback current i_{fb}. The output signal consists of a chaotically wavelength modulated laser beam masking a small message, which is transmitted to the receiver. The decoder consists in two branches. One is dedicated to a linear wavelength detection (e.g. a spectral filter operating within its linear part), thus providing at the output of a photodiode an electronic signal proportional to the chaotic fluctuations hiding the message. The other branch replicates the same NLDDP as in the emitter, thus reproducing the same chaotic fluctuations without the message. A subtraction is used to extract the message.

Due to the unavoidable mismatch between the emitter and receiver parameters, a chaotic decoding noise is observed at the receiver. The fine parameter tuning is important, firstly to recover the message, and secondly to improve the quality of the recovered signal. Matching the delay τ_R at the emitter and receiver is well known to be a very sensitive operation, since in some cases, only a 0.1% relative error on the parameter adjustment at the receiver can induce a decoding error large enough to make the message recovery impossible. Typical analogue encoded and decoded sine waveforms are reported in Fig. 7. The transmitted signal (left traces) has noise-like temporal fluctuations (upper), and a nice flat spectrum (lower) that does not reveal the hidden message frequency (whose position is indicated by the cursor). The decoded message (right traces) shows clearly the original sine waveform in the time domain, with a slight noise superimposed to it. The corresponding spectrum shows a signal-to-noise ratio of about 20 dB in the decoding process.

Due to technological and physical reasons, the wavelength setup does not offer an attractive potential for the multi-Gbit/s optical communications. The wavelength tuning speed is indeed limited to less than 150 MHz, and the large wavelength fluctuations would also cause transmission quality degradation due to dispersion effects. Thus, other experimental situations have been explored following the same principles, but seeking for faster dynamical processes. The idea is still based on an Ikeda-type dynamics for the chaos generation, and the same encoding and decoding scheme as in Fig. 5(b). Instead of using wavelength modulation, a faster process based on electro–optic effects was chosen to modulate the optical path difference Δ in Eq. (4).

The most straightforward way to modulate electro-optically an optical interference is to choose a component widely used in ultra fast fiber telecommunication systems, the electro-optic Mach–Zehnder modulator. Such integrated optics components in lithium niobate ($LiNbO_3$) are commercially available for bit rate up to 40 Gb/s. Those devices are usually operating in a weak nonlinear operation, since the applied voltage is typically intended to encode bits 0 and 1 through the switching between destructive and constructive interference conditions. The corresponding voltage switching amplitude is called V_π; it can be practically as low as a few Volts for integrated optics components. However, operating with a larger voltage swing enables one to scan practically at least 2 to 3 extrema of the interference transfer function, thus performing a highly nonlinear transformation suitable for high complexity dynamics in a time delay system. An intensity chaos generator can be constructed similarly to the wavelength chaos generator. The setup is actually known for more than 20 years and has been used as an electro-optic demonstrator for the Ikeda ring cavity instabilities [21]. We revisited the setup as depicted in Fig. 8 for the demonstration of chaos encoding and decoding of optical information for ultra-high bit rate fiber transmission systems. Previous unsuccessful attempts [22] or performance limited realizations [23] with a similar electro-optic setup brought us to the following setup modification: the message is added optically to the chaotic carrier at the output of the Mach–Zehnder modulator. This characteristic has important consequences:

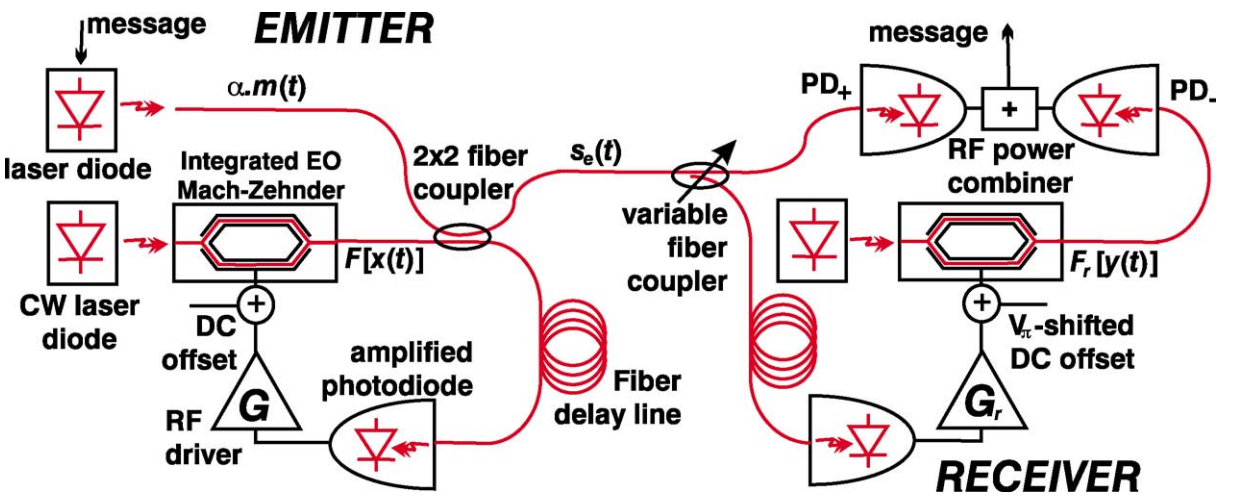

Fig. 8. Multi-Gbits/s intensity chaos encoder and decoder.

(i) Note that the optical chaotic carrier produced by the Mach–Zehnder interferometer features an RF spectrum much larger than the 6 GHz-electrical RF spectrum observed for the voltage at the Mach–Zehnder input electrode. This is explained by the multiple extrema nonlinearity actually scanned in large amplitude chaotic regime. This spreading can be easily observed directly on the optical spectrum, and is measured to be greater than 30 GHz. This allows several 10 Gb/s masking capability for the setup in Fig. 8.

(ii) The message bandwidth is intrinsically independent of the chaos generator bandwidth due to the all-optical mixing in the fiber coupler. In order to mask properly the message, the chaotic carrier spectrum has however to be at least as wide as the message spectrum, which defines a limit on the actual efficient message encoding speed, depending on the chaos bandwidth.

(iii) Under these conditions and assuming emitter/receiver matching is achieved, the encoding/decoding bandwidth capability of the system is limited by the photodiodes bandwidth PD_+ and PD_-, and of the power combiner bandwidth only, meaning that the encryption bandwidth can be much larger than that of the electro-optic modulator used. This is a great advantage in view of high speed encryption systems. Also notice that subtraction between the detected 'chaos + message' signal ($s_e(t)$) and the receiver generated chaotic signal is performed experimentally through an adequate biasing of the Mach–Zehnder, such that the receiver nonlinear function corresponds to the opposite of that in the emitter. The subtraction is obtained at the power combiner output (electric adder).

According to the previous remarks, the modeling of the intensity chaos encoder and decoder is slightly modified with respect to Eqs. (2) and (3). The emitter and receiver equations should, in this case, be changed into:

$$x(t) = \beta\left\{h_\theta \star \left[f(x_{\theta-\tau_R}) + \alpha m(\theta)\right]\right\} = \beta[h \star s](t), \tag{5}$$

where $s(t) = f[x(t-\tau_R)] + \alpha m(t)$ is the transmitted signal from the emitter. At the receiver side, the locally generated chaos, without the message is

$$s'(t) = f'\left[y'(t-\tau'_R)\right] \quad \text{with} \quad y'(t) = \beta'[h' \star s](t). \tag{6}$$

Decoding is performed by adding electronically $s(t)$ and $s'(t)$, and for a proper tuning of the Mach–Zehnder bias so that $f'[\cdot] = C - f[\cdot]$. Since the detectors PD_- and PD_+ are not DC sensitive, the output signal is directly proportional to the message $m(t)$.

The main feature of the device compared with the wavelength chaos generator and the Ikeda model, consists in the large bandpass nature of the dynamical process. Usually in most of the ultra wide band communication systems, the low frequencies are filtered out by the electronic feedback, thus yielding a bandpass dynamical behavior. The process involved in the nonlinear feedback is therefore fundamentally different, as well as the dynamical trajectories that can be observed on the bifurcation diagram in Fig. 9(c) (to compare with Fig. 3(c)). The fundamental properties of such bandpass nonlinear delayed dynamics are not widely known yet, although they should reveal very interesting phenomena. From our encryption point of view, first numerical calculations tend to show that for an equal bandwidth, the bandpass systems exhibit greater Lyapunov dimension than the low pass ones. The chaos encryption system in Fig. 8 also takes advantage of this situation.

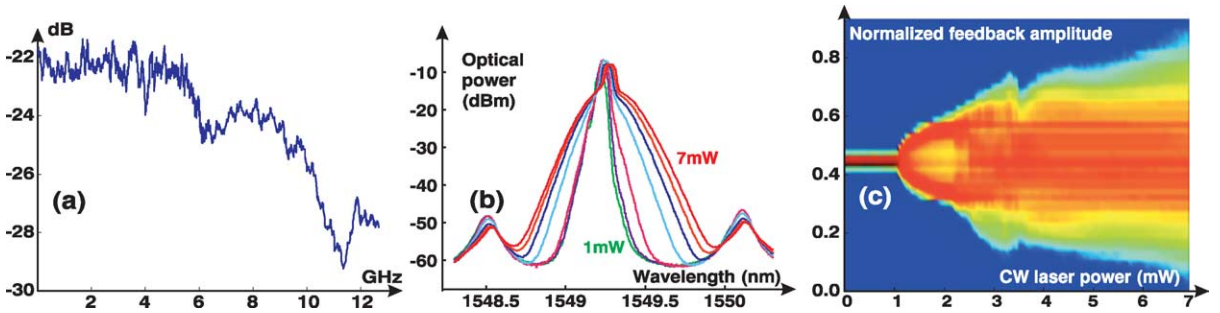

Fig. 9. Dynamical properties of the intensity chaos setup: (a) RF spectrum of the chaotic optical carrier spread by the nonlinear function and filtered by a 10 GHz photodiode; (b) optical spectrum for increasing CW laser power, from 1 mW to 7 mW with 1 mW step; (c) experimental bifurcation diagram recorded with a 5 GHz oscilloscope.

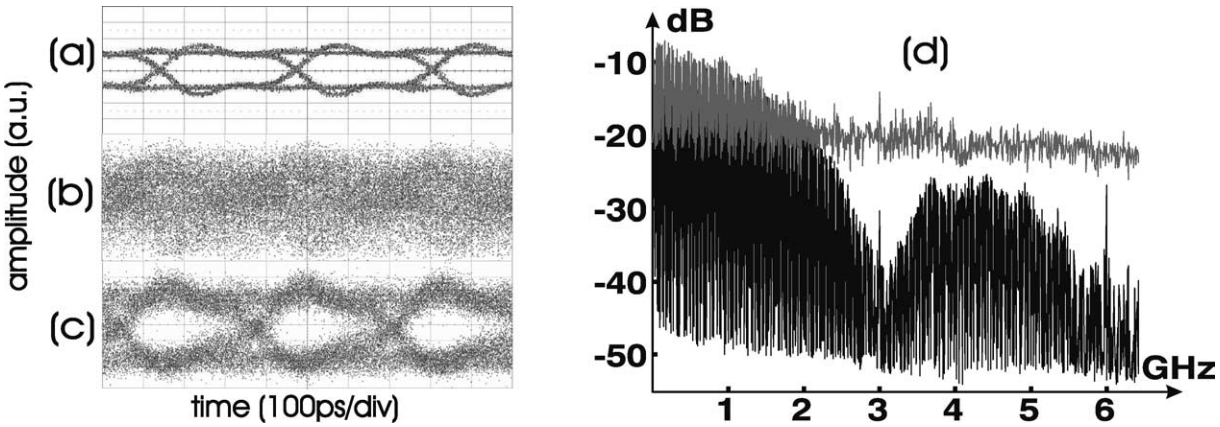

Fig. 10. Bit Error Rate (BER) test with binary pseudo random sequence (length $2^7 - 1$) at 3 Gb/s: (a) eye diagram for the direct transmission without chaos encryption (BER $< 10^{-12}$); (b) eye diagram for the direct detection by an eavesdropper of the chaos encoded message (BER $> 10^{-2}$); (c) eye diagram of the recovered bits corresponding to Bit Error Rate of 7×10^{-9}; and (d) RF spectra of the original binary message (black), and the encoded one (spectral masking, grey trace).

Typical experimental encoding and decoding results at 3 Gb/s are depicted in Fig. 10. The message is obtained through a direct laser diode modulation with a $2^7 - 1$ binary pseudo random sequence. The masking efficiency is determined by adjusting the relative message to chaos optical power, thus varying the parameter α in Eq. (5). For $\alpha > 1.7$, it was found that the chaotic carrier was not strong enough to prevent eavesdropping from direct detection of the transmitted signal, leading to a measurable BER (in the order of 10^{-2}). Fig. 10 was obtained with $\alpha = 1.4$, thus preventing bit recovery from direct detection, but also leading to an acceptable BER for the authorized receiver of 7×10^{-9}. To the best of our knowledge, this setup currently achieves the best results in terms of masking efficiency, decoding quality, and bit rate.

As already explained, security is here viewed as a compromise to be done between the masking efficiency and the BER i.e., the decoding quality (or BER quality). However, deeper investigations are still needed to have a better understanding of the correct confidentiality level that can be expected from this chaos-based encryption scheme. The next section is intended to give directions to solve this problem.

4. Security issues and future developments

The points we already explored concerning the problem of confidentiality are divided into two classes. On the one hand, we investigated new physical situations to implement the chaos encryption principles described earlier; this concerns the combination of coherence modulation principles together with a time delayed electro-optic chaos generator, and it also concerns the exploration of new chaos generator architectures. On the other hand, we explored the possibility of extracting from the transmitted signal – the one available to an eavesdropper – any determinism attached to the chaos generation process. If the determinism of the chaos generator can thus be recovered, the eavesdropper would be able to construct his own decoder and recover the message.

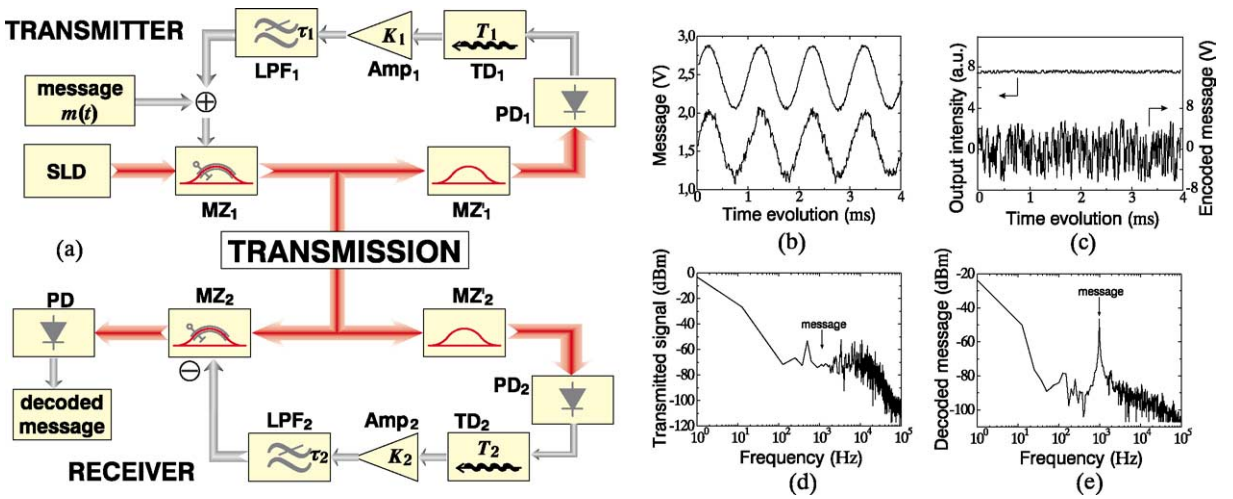

Fig. 11. Chaotic encoding with coherence modulation. (a): experimental setup, (b): original and recevered sine waveform, (c): transmitted intensity fluctuations and chaotic coherence modulated carrier, (d) spectrum of the transmitted intensity encoding the sine waveform, (e): spectrum of the recovered sine signal.

4.1. Encoding chaotic architectures with enhanced security

Coherence modulation has been found to be a possible way to add a second security level at the physical layer of the transmission system, complementary to the chaos encoding principle. This unusual optical modulation technique has been known for a long time, but is not used in conventional fiber telecommunication systems. A typical coherence modulation transmitter consists of (see Fig. 11(a)):

– A broadband optical emitter, such as a super luminescent diode, or amplified spontaneous emission, instead of highly coherent laser light.
– An unbalanced electro-optic interferometer e.g., a Mach–Zehnder modulator, whose static optical path difference (OPD) is greater than the light source coherence length. Due to this, no detectable intensity modulation occurs in the presence of an electro-optic modulation, although a phase modulation is present in the transmitted light beam. Virtually, the broadband source can be viewed as a set of incoherent wavepackets, whose spatial extension is of the order of the source coherence length. An unbalanced interferometer divides the input wavepackets into two at the output, the latter being separated by a distance greater than the coherence length (thus preventing from any detectable interference).

The coherence demodulator consists of a second unbalanced interferometer, whose static OPD is adjusted to that of the modulator: the OPD acts as an encoding key, without which demodulation cannot be performed. The demodulator interferometer duplicates a second time the two input wavepackets, leading at its output to four wavepackets, two of them being separated by twice the OPD, but the two others are superimposed, giving rise to an interference between them. If an electro-optic voltage is applied to the modulator, the interference at the demodulator is scanned according to the modulator voltage amplitude with respect to the half wave voltage electro-optic device.

Combining the modulator and the demodulator in a single emitter with an electro-optic feedback and a time delay as shown in Fig. 11 yields a chaotically coherent modulated light beam at the modulator output. The emitter and receiver setup is depicted in Fig. 11(a) [24], and the corresponding encoding and decoding signals and spectra are shown in Fig. 11(b)–(e). Besides the dual security level proposed by the coherence modulation combined with the chaotic encoding, the main advantages of the setup are:

– its extremely good matching capability between the emitter and receiver components, thus leading to an excellent decoding quality (typical signal-to-noise better than 40 dB);
– its all-optical subtraction capability to extract the message, due to the intrinsic physical properties of the coherence demodulation principles;
– its multiplexing capability due to coherence modulation properties (different channels corresponding to different static OPDs).

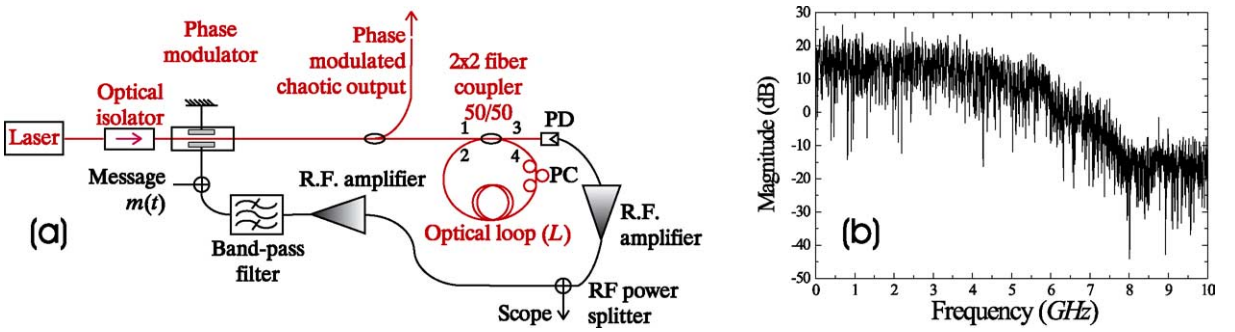

Fig. 12. High dimensional, high speed, phase chaos: (a) experimental setup; (b) RF spectrum of the electronic feedback signal.

Unfortunately, a high bandwidth requires the use of nonconventional optical components for telecommunication, such as high power broadband optical source, and high speed unbalanced integrated Mach–Zehnder modulators.

The advantage of this approach is its high flexibility for testing new chaotic processes involving nonlinear delay systems derived from the general scheme in Fig. 2(b). Such an approach is reported in [25], when two feedback loops comprising two different time delays and two different nonlinear functions are considered. The aim is to enhance the chaotic carrier complexity, thus making more difficult any kind of time series analysis that might be use by an eavesdropper. Using a standard Lyapunov dimension algorithm adapted for the multiple nonlinear delayed feedback loop, we obtained greater attractor dimensions as compared to the single feedback loop.

The Ikeda–type nonlinear dynamical system represents the simplest version for nonlinear delayed dynamics: its model corresponds to a scalar first order delay differential equation. Vectorial models and more complex, but still deterministic, dynamics could offer a higher degree of security. This issue has motivated recent investigations [26] on fiber cavity based optoelectronic oscillators, as depicted in Fig. 12(a). At first sight, the setup seems very similar to Ikeda setup, since it consists of an all-optical (fiber) ring cavity, and the phase modulation (electro-optically) is changed at each cavity round trip of the beam. However, the physical phenomena ruling the dynamical behavior exhibit a great difference: the phase modulation is performed at the input of the cavity, and not inside.

In order to observe instabilities in this oscillator, the typical time scale fluctuations needs to be faster than the cavity round trip time i.e., the cut-off frequency of the phase modulator has to be higher than the cavity free spectral range.

The mathematical model can be written in the same way as the previous nonlinear delay oscillator. The dynamical process is supposed to be ruled by the impulse response of the electronic feedback, convolved by the detected optical intensity fluctuation $p_3(t)$ at the input of the electronic feedback (the photodiode).

$$\phi(t) = \beta[h \star p_3](t), \quad \text{where } p_3(t) = \rho p_0\left[\kappa + (1-\kappa)\gamma\frac{p_{4_{\tau_R}}}{p_0} - 2\sqrt{\gamma\kappa(1-\kappa)\frac{p_{4_{\tau_R}}}{p_0}}\sin\left[\varphi_{4_{\tau_R}} + \phi_L - \phi(t)\right]\right]. \tag{7}$$

The last expression for $p_3(t)$ reflects the interference observed at port 3 of the fiber coupler. The two interfering beams are formed by the cavity input light with a modulated phase $\phi(t)$ and a constant power p_0, and the delayed cavity feedback having a power $p_{4_{\tau_R}} = p_4(t-\tau_R)$ and a phase $\varphi_{4_{\tau_R}} = \varphi_4(t-\tau_R)$. The latter two quantities are ruled by a 2D-mapping describing the sequence of interferences inside the fiber cavity, thus distinguishing this chaotic phase dynamics as from Ikeda dynamics:

$$\begin{aligned} p_4(t) &= \rho p_0\left[1-\kappa+\gamma\kappa\frac{p_{4_{\tau_R}}}{p_0} + 2\sqrt{\gamma\kappa(1-\kappa)\frac{p_{4_{\tau_R}}}{p_0}}\sin\left(\phi_L - \phi(t) + \varphi_{4_{\tau_R}}\right)\right], \\ \varphi_4(t) &= \phi(t) + \frac{\pi}{2} - \arctan\left\{\frac{\sqrt{\kappa\gamma p_{4_{\tau_R}}}\cos[\phi_L - \phi(t) + \varphi_{4_{\tau_R}}]}{\sqrt{(1-\kappa)p_0} + \sqrt{\kappa\gamma p_{4_{\tau_R}}}\sin[\phi_L - \phi(t) + \varphi_{4_{\tau_R}}]}\right\}. \end{aligned} \tag{8}$$

The numerical results obtained with this dynamical model show a very good qualitative agreement with the experimental observations.

Besides enhancing security through greater dynamical complexity, we also started to investigate the confidentiality of chaos based encryption systems using a cryptanalytic approach.

4.2. *Cryptanalysis directions*

Following the cryptanalysis approach, we assume that the system architecture is known (for example determined by a scalar nonlinear delay differential dynamics as in Eq. (1)), and the n parameter settings used to generate the chaotic oscillations are

unknown to the eavesdropper. One way for the eavesdropper to intervene is to perform an exhaustive search of all the exact values $(p_i)_{i=1\text{to}n}$. This task is done within a volume of the parameter space; this volume corresponds to all the achievable chaotic regimes:

$$V = \int_{\text{Chaos}} \mathrm{d}^n p_i \,. \tag{9}$$

A finite precision (δp_i) is practically attached to each parameter p_i, that precision being determined by the minimum parameter matching allowing a sufficient decoding quality. This approach leads to an equivalent number of necessary bits quantifying the key space size:

$$N = \sum_i \log_2 \frac{V}{\prod_i \delta p_i}. \tag{10}$$

For experimental systems, this calculation leads to a key size between 20 and 25 bits, which is relatively small as compared with the several hundreds bits key size used in algorithm based encryption techniques. However, this rough approach gives only a minimum equivalent key size, which is not realistic due to the physical nature of chaos. A more realistic approach should consider the following:

- The physical signal has to be analyzed in the analogue world, since we are dealing with very fast analogue signals, which are difficult to process numerically (a multi GHz signal sampling is required, thus also introducing noise in the data).
- The nonlinear function, as already stated, can be chosen from a huge set of possibilities, which is not considered by the previous cryptanalytic approach, since this function is assumed to be fixed. Considering a system governed by Eq. (7) and (8) would significantly increase the complexity of the required computation.
- The assumption of scalar nonlinear delay dynamics does not match the most recent ultra fast chaos generators now used in effective experimental demonstrators. Multiple delays and multiple feedback loops should be considered, which makes also the analysis much more difficult.

To the best of our knowledge, no efficient cryptanalysis method has been found yet, but only a few papers have reported such analyses. Among these papers, successful results were obtained under quite restricted situations, such as low dimensional dynamics [27], or low nonlinear process authorizing linear approaches [28].

However, an interesting direction should be investigated more deeply, using nonlinear time series analysis techniques in order to recover the dynamics determinism [29]. These analysis tools have been used to investigate single extremum nonlinear delay dynamics so far. They begin to be used to break multiple extrema systems, as well as for multiple delay and multiple nonlinear function delay dynamics, but so far those methods have failed (although they were successfully used to break low complexity systems with a single extremum).

5. Conclusions

A generalized nonlinear delayed differential dynamics based on the Ikeda ring cavity principle has been described, together with its application to secure communications using a chaotic carrier for optical telecommunications. Practical implementations and performance of the whole encryption system have been reported through different experimental situations involving different dynamical variables (wavelength, intensity, coherence modulation, optical phase) and different performances (encoding speed, decoding quality, masking capability, dynamics complexity). The architecture based on an electro-optical nonlinearity performed by $LiNbO_3$ integrated optics components succeeded in demonstrating a record encryption speed for a digital pseudo random sequence at 3 Gb/s. Improvements are in progress in view of several 10 s of Gb/s. Enhanced architectures for chaos generation have also been proposed, in order to improve complexity and confidentiality. One of the open problems that remains partly unsolved is the evaluation of the security level, which is extremely high in the various cases discussed previously. This problem has been addressed, giving directions for solving that important issue.

Acknowledgements

This work was supported by the European community in the frame of the OCCULT project (IST-2000-29683).

References

[1] K. Ikeda, Opt. Comm. 30 (1979) 257.
[2] H.M. Gibbs, F.A. Hopf, D.L. Kaplan, R.L. Schoemacker, Phys. Rev. Lett. 46 (1981) 474.
[3] F. Arecchi, W. Gadomski, R. Meucci, Phys. Rev. A 34 (1986) 1617.
[4] T. Aida, P. Davis, IEEE J. Quant. Electron. 28 (1992) 686.
[5] J.D. Farmer, Physica D 4 (1982) 366.
[6] B. Dorizzi, B. Grammaticos, M. Le Berre, Y. Pomeau, É. Ressayres, A. Tallet, Phys. Rev. A 35 (1987) 328.
[7] L.M. Pecora, T.L. Carroll, Phys. Rev. Lett. 64 (1990) 821.
[8] K.M. Cuomo, A.V. Oppenheim, Phys. Rev. Lett. 71 (1993) 65.
[9] C. Tresser, P. Coullet, C. R. Acad. Sci. Paris, Sér. A 287 (1978) 577;
M. Feigenbaum, J. Stat. Phys. 19 (1978) 25.
[10] C. Mirasso, P. Colet, P. Garcia-Fernandez, IEEE Phot. Techn. Lett. 8 (1996) 299.
[11] V. Annovazzi-Lodi, S. Donati, A. Scire', IEEE J. Quantum Electron. 32 (1996) 953.
[12] G.D. VanWiggeren, R. Roy, Science 279 (1998) 1198.
[13] J.-P. Goedgebuer, L. Larger, H. Porte, Phys. Rev. Lett. 80 (1998) 2249.
[14] I. Fischer, Y. Liu, P. Davis, Phys. Rev. A 62 (2000) 011801(R).
[15] S. Sivaprakasam, K.A. Shore, IEEE J. Quantum Electron. 36 (2000) 35.
[16] A. Uchida, S. Yoshimori, M. Shinozuka, T. Ogawa, F. Kannari, Opt. Lett. 26 (2001) 866.
[17] S. Tang, J.M. Liu, Opt. Lett. 26 (2001) 1843.
[18] M.C. Mackey, L. Glass, Science 197 (1977) 287.
[19] J.P. Eckmann, D. Ruelle, Rev. Mod. Phys. 57 (1985) 617.
[20] V.S. Udaltsov, J.-P. Goedgebuer, L. Larger, W. Rhodes, Phys. Rev. Lett. 86 (2001) 1892.
[21] A. Neyer, E. Voges, IEEE J. Quantum Electron. 18 (1982) 2009.
[22] P. Celka, IEEE Trans. Circuits Syst. I 42 (1995) 455.
[23] J.-P. Goedgebuer, P. Levy, L. Larger, C.-C. Chen, W.T. Rhodes, IEEE J. Quantum Electron. 38 (2002) 1178.
[24] M.W. Lee, L. Larger, J.-P. Goedgebuer, IEEE J. Quantum Electron. 39 (2003) 931.
[25] M.W. Lee, L. Larger, V. Udaltsov, É Genin, J.-P. Goedgebuer, Opt. Lett. 29 (2004) 325.
[26] É. Genin, L. Larger, J.-P. Goedgebuer, M.W. Lee, R. Ferrière, X. Bavard, IEEE J. Quantum Electron. 40 (2004) 294.
[27] Th. Beth, D.E. Lazic, A. Mathias, Lect. Notes in Comput. Sci. 839 (1993) 318.
[28] J.B. Geddes, K.M. Short, K. Black, Phys. Rev. Lett. 83 (1999) 5389.
[29] R. Hegger, M.J. Bünner, H. Kantz, Phys. Rev. Lett. 81 (1998) 558.