Review

Chaos and high-level dynamics in coupled lasers and their applications

Silvano Donati[a,b,*], Sheng-Kwang Hwang[b,c]

[a]*Department of Electronics, University of Pavia, Pavia, Italy*
[b]*Department of Photonics, National Cheng Kung University, Tainan, Taiwan*
[c]*Advanced Optoelectronic Technology Center, National Cheng Kung University, Tainan, Taiwan*

Abstract

In this paper, we first introduce mutual and self-coupling and related phenomena in laser diodes, and discuss how the chaos paradigm has been unveiled as a refinement of classical Adler's locking equation describing coupling. Then, we take the ICL (injected coupled laser) system as a reference and illustrate the newly found regimes of injection modulations, labile locking, periodicity and multiperiodicity, chaos, opening and closing bifurcations, up to the final locking of the system. Analysis is carried out by Lamb and Kobayashi equations, in good agreement with experiments. The concept of synchronization is then developed and schemes devised to implement it on an ICL system are discussed. We then show that two cryptography schemes easily follow from synchronization, namely CM (chaos masking) and CSK (chaos shift keying), and describe some implementations of them as well as the results of a sensitivity analysis. After that, we broaden the range of applicability of coupled phenomena showing they are robust against change of parameters and configurations. As a preferred, minimum part-count scheme useful for engineering implementation, we then introduce and evaluate the DOF (delayed optical feedback) configuration, basically a self-mixing scheme operating at a high level of (self-)coupling. For the DOF system, we run through the paradigm of high level dynamics, synchronization and cryptography variants (CM and CSK) again, and find that this system is well suited to all application criteria. We describe practical and in-field implementation of cryptography schemes, CM as well as the PIC (photonics integrated circuit) devices reported so far. A system analysis is then presented, with a summary of experiments on variants of basic cryptography scheme, and some general considerations about cryptography codes and robustness. Finally, we briefly digress to illustrate the recent field of non-cryptography applications of optical chaos systems, such as random number generation, distance measurement, and microwave photonics.
© 2012 Elsevier Ltd. All rights reserved.

*Corresponding author at: Department of Electronics, University of Pavia, v. Ferrata 1 27100 Pavia, Italy.
Tel.: +39 0382 985204; fax: +39 0382 422583.
E-mail address: silvano.donati@ieee.org (S. Donati).

Contents

1. Introduction

High-level dynamics in coupled lasers provides a rich phenomenology and a wealth of applications, ranging from cryptography to microwave photonics and instrumentation. A *coupling regime* is found whenever a laser source injects part of the emitted field into another laser, or back into its own cavity. Coupling gives rise to a rich variety of phenomena, conceptually interesting as they unveil new and unexpected behavior of the optical system, but is also important to engineering for the many applications enabled.

For example, at the weak level of interaction, self-coupled lasers are the starting point for self-mixing interferometry, a new method for measurements of optical phase shift as well as of field amplitude—the subject of a recently published review [1].

At the high level of interaction, the coupled-laser system displays a number of new interesting regimes of operation, ranging from induced modulation, to locking and unlocking,

to periodic and multi-periodic oscillations and to chaos, featuring alternate switching between regimes and opening and closing bifurcations, until, at still higher levels of injection, the coupled system reaches the final locking stage.

This is the subject of this review, which focuses on diode lasers as the specific source because they are best suited to applications, though the very general nature of coupling phenomena makes most of the findings and conclusions also applicable to other laser types and to non-optical oscillators as well.

In general, we obtain *coupling* when a small fraction of the field is injected into the laser cavity, either from a physically different laser or from a delayed portion of the laser field itself, as shown in Fig. 1.

Coupling phenomena have attracted interest since the early days of laser discovery, the first to study them being the Nobel Prize laureate H. Lamb, Jr. and M.B. Spencer, who published in 1972 two seminal papers describing both the three-mirror laser (or self-injection) [2] and the mutual (two sources) injection case [3].

They carried out an analysis based on the slowly varying approximation of field amplitude E and phase ϕ of the oscillating field, what we call today the Lamb's equations of the laser. Lamb's equations are well suited to Class A lasers (see Ref. [4], and below) such as gas and crystal lasers, in which E and ϕ are decoupled from the density of state N, whereas in a semiconductor laser (class B) we shall add a third equation to describe N (the carrier concentration) and its dependence on E and ϕ, yielding the modified Lamb equations also known as the Lang and Kobayashi (L–K) equations [5]. Despite the difference, interestingly the main results found with Lamb's equations at weak injection still hold and correctly describe low-level coupling phenomena for Class B lasers, including the semiconductor laser diode.

A first classification of coupled systems is based on the type of coupling, either *mutual*-coupled or *self*-coupled (Fig. 1). Mutual-coupled systems are the paradigm of oscillator synchronization and may be *symmetrical* (same coupling in both directions) or *asymmetrical* (different coupling, and a master/slave system when an optical isolator is inserted between sources).

Another classification is in according to the *strength* of coupling. We say coupling is *weak*, when the perturbing field brought back into the laser cavity is a fraction, say, down to about 10^{-9} and up to 10^{-2}, of the pre-existing field power. The 10^{-9} level tells us that coupling schemes are very sensitive to even minute retro-reflections of externally injected fields. This is well known practice in experiments with, e.g., frequency-stabilized lasers or optical-fiber communication transmitters, where we need to defend the laser from returns with a high-performance optical isolator to avoid spoiling the frequency stability or corrupting the amplitude with excess noise. Analysis shows that the sensitivity of
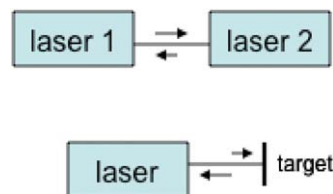

Fig. 1. Schematic of coupled lasers. Top: mutual coupling (can be symmetrical or asymmetrical); bottom: self-coupling.

mutual- and *self*-coupled oscillators to external injection—in the sense of minimum signal detectable or affecting performance—is down to the level of *quantum noise* associated with the power P of the oscillating field, both in amplitude (power $p_{min} = [2h\nu BP]^{1/2}$) and phase ($\phi_{min} = [P/2h\nu B]^{1/2}$), see Refs. [7,8]. This is because the process of interaction with the in-cavity field is coherent, similarly to *homo-* or *hetero*-dyne detection [8].

In the *weak* regime of *self-coupling*, the main phenomenon observed is amplitude (AM) and frequency (FM) modulation of the oscillating field. The driving term (or modulation index) is the product of the fraction of the returned field and the cosine (or sine) of the optical phase shift $2ks$ (k=wave vector, s=distance) external to the perturbed laser. This is the case first studied by Spencer and Lamb [2], the configuration that has opened the way to the development of self-mixing applications like interferometers and very sensitive echo-sensors [1].

Self-mixing modulations are easily explained as the result of a rotating-vector addition, shown in Fig. 2. Let E_0 be the unperturbed cavity field, and $aE_0 \, exp \, i2ks$ the field back from the target, a being the (field) attenuation and $2ks$ the phase delay of propagation. As known from communication theory, rotating vector addition generates an AM modulation driven by the in-phase component of the modulating term, that is $aE_0 \cos 2ks$, and an FM driven by the in-quadrature component, or $aE_0 \sin 2ks$. One point is that, while the AM signal is readily available from the power detected by a photodiode, FM is difficult to retrieve because it is impressed on the optical frequency (and we need a frequency down-conversion to detect it, see e.g. Ref. [1]).

Also in the *weak* regime of *mutual-coupling* we find AM and FM in the field of each of the two interacting lasers, and the driving terms are now the ratio of amplitudes and the frequency difference [6]. The coupled system can then be regarded as a special coherent detector receiver, also known as an *injection* detector [7].

Weak coupling phenomena are observed in all laser sources, including class A lasers [4], that do not exhibit chaos. As a consequence, while applications to measurements of amplitude and phase are feasible and have been demonstrated in a variety of class A and B lasers [1], chaos and high-level dynamics applications will require a class B laser (e.g., a semiconductor diode laser). Class C lasers are already chaotic on their own, but are poorly controllable.

Semiconductor diode lasers are intrinsically stable when operating in a stand-alone, unperturbed condition, but will become chaotic when coupled or self-coupled with sufficient strength. The coupling factor is thus the very convenient parameter to control the behavior of the system at a high level. And, from the practical point of view, semiconductor diode lasers are the preferred choice because of their well-known advantages of small size, low power consumption, batch fabrication, and match of parameters.
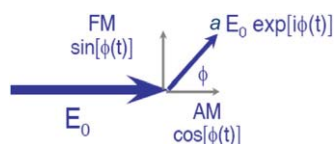

Fig. 2. Describing self-coupling with the aid of the rotating-vector model, it is easy to see that the in-phase component is responsible for AM, and is proportional to $\cos 2ks$, whereas the in-quadrature component is responsible for FM and is proportional to $\sin 2ks$.

Going back to classification, we say coupling is *strong* when the exchange is a fraction up to a few percent of the pre-existing oscillation power. Even at this apparently modest level of injection, the AM and FM modulations become so strong that they drive the laser out of a reproducible regime of oscillation, and the system enters a non-linear high-level dynamic regime, both in mutual- self-coupling cases, characterized by new and unexpected behaviors such as bifurcations, multi-periodicity and chaos in mutual-coupled systems, and relaxation oscillations, bi-stability, multi-stability, and chaos in self-coupled systems.

This regime is special in the sense that its evolution cannot be predicted by knowledge of the constitutive equations and initial conditions — the system ceases to be deterministic in a strict sense, and exhibits multiple solutions and a pseudo-random behavior of its state variables.

This is just the incipit of a paradigm heralding a *complex* system, in which evolution is determined by new laws specific to a higher level of organization whereas the lower-level laws cease to be significant [9,10].

Yet, the high-level dynamics can still be described by a small-perturbation analysis around the quiescent point of the unperturbed state, because the level of coupling (or, the factor multiplying the new perturbation terms in the constitutive equations) is small, about a few percent (or less) as mentioned above. Thus, fortunately, the L–K equations still apply under strong level conditions and become the appropriate tool to describe the observed complexity and chaos regimes [11,12].

The regimes of strong coupling and the development of new techniques like optical chaos generators, chaos masking, synchronization, and chaos-cryptography systems are the subjects covered in this paper, which is organized as follows. In the next Section, we introduce basic ideas underlying strong coupling dynamics and summarize the methods to analyze it. In Section 3, we develop the applications of chaos-based systems to a variety of cryptography systems. In Section 4, we describe experiments and in-field evaluations of prototype chaos communication systems, and the development of integrated photonics chips for chaos generators. In the final Section, we summarize the dawning applications to communications and signal processing, and finally we draw some conclusions.

2. Laser injection dynamics

The *laser injection* scheme reported in Fig. 3 is perhaps the simplest system representative of the high-level dynamics paradigm and the first studied since the 1980s to unveil chaos phenomena in lasers [13].
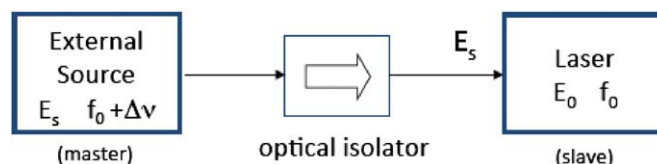

Fig. 3. The paradigm of high-level dynamics is unveiled by the basic scheme of injection, a particular case of mutual coupling becoming asymmetrical with the interposition of an isolator between the external source (master) and the receiving source (slave). When oscillators are electronics and the signal *E* is a scalar, we obtain the case studied by Adler which leads to the locking theory. With laser oscillators, the system is a prototype for optical chaos generation.

Also known as an ICL (injected coupled laser), it is a mutual asymmetric coupling scheme, consisting of a master and a slave oscillator, with an optical isolator to allow signal transfer in the direction from the master to the slave, and with the master source slightly offset by Δv in frequency with respect to the slave. The strength of coupling is defined by the ratio $E_s/E_0 = K$ of the injected (master) to unperturbed (slave) fields. To study the regime, we will let K vary from the unperturbed condition (very small K) up to the largest value of interest, corresponding to the final event of locking the slave laser to the master oscillator frequency.

2.1. The paradigm of high-level coupling phenomena in injected coupled lasers (ICL)

Actually, up until about the 1970s, the injection scheme (Fig. 3) was the reference to study locking and frequency attraction phenomena in conventional oscillators—those employed in radio engineering and made up of an active electronic component and a narrow-band resonator arranged in a regenerative feedback loop, so that when the circuit breaks into oscillations, the frequency is tuned to the resonator response.

Describing the oscillator by a second order differential equation and analyzing injection under a small-signal perturbation assumption, Adler found in 1946 [14] the well-known equation governing the phase of the slave oscillator (see also Appendix A1). Results are expressed in terms of the reduced phase ϕ of the complex signal, written as $E_0 \exp i\Phi$, where $\Phi = 2\pi f_0 + \phi$ is the total phase. The equation is as follows:

$$d\phi/dt = A + B\sin[\phi - \phi_s]. \qquad (1)$$

Here, A is the unperturbed frequency difference (Δv in our notation, the steady-state frequency $d\phi/dt$ of the unperturbed system), $B = \gamma E_s/E_0$ is the injection-induced perturbation, γ is the rate of coupling, and ϕ_s is the phase added to E_s in the injection process.

Solutions of Adler's Eq. (1) are the well-known milestones of oscillator injection theory, and they bring about:

(i) *frequency attraction* at small or moderate coupling strength [i.e., $d\phi/dt = (A^2 - B^2)^{1/2}$];
(ii) *injection modulations* in frequency (see Ref. [15] for expressions of FM);
(iii) *frequency locking* at $B \geq A$ [with $d\phi/dt = 0$ and phase pinned at $\phi = \arcsin(-A/B) + \phi_s$]. Also, solutions hint at:

(iv) *injection detection*, because the modulation components generated by injection are larger than the input signal (with a gain $\frac{1}{2}(B/A)^2 E_s/E_0$, see Refs. [7,8]).

Interestingly, Adler's Eq. (1) also holds for class A laser oscillators in the Lamb's equations approximation, as derived in Ref. [15], and is easily adapted through minor variants to the other case of mutual coupling, that is, symmetrical coupling [15]. In addition, both in the 3-mirror model and in the L–K approximation, it is shown to apply for the total phase $\Phi = \omega t$ also in the case of self-injection (or self-mixing scheme); see Eq. (4d) of Ref. [1].

Thus, up through the 1980s, all we knew from the Adler theory was that, at increasing coupling strength, modulations of the slave oscillator first appear in amplitude and frequency, with some frequency attraction, and then an inexorable final locking of the slave oscillator that follows at a certain level of coupling.

In subsequent years, it was found that, for some electronic oscillators as well as for class B lasers, the injection scheme does not have just a single locking. After the first locking, increasing the coupling strength de-locks the slave oscillator and begins generating sub-harmonic frequency waveforms, passes through bifurcations, followed by the chaotic regime, then back to sub-harmonics alternating between chaos and bifurcations until, at a much larger coupling strength than the initial, the final locking is reached.

Study of injection scheme dynamics is carried out with the L–K equations [16] for amplitude E, phase ϕ and the density of states N of the slave laser, in the injected scheme with input field E_s and (initial) frequency difference Δv. They are written in the following form [17]:

$$dE/dt = \tfrac{1}{2}[G_N(N-N_0)-1/\tau_p]E + (\kappa/\tau)E_s(t)\cos[2\pi\Delta vt + \phi(t)-\phi_s(t)]$$
$$d\phi/dt = \tfrac{1}{2}\,\alpha\{G_N(N-N_{thr})-1/\tau_p\} + (\kappa/\tau)E_s(t)/E(t)\sin[2\pi\Delta vt + \phi(t)-\phi_s(t)]$$
$$dN/dt = J\eta/ed-N/\tau_r-G_N(N-N_0)E^2(t) \tag{2}$$

where (with typical values noted) G_N is the modal gain $= 8.1 \times 10^{-13}$ m^3 s^{-1}, κ the fraction of field E_s coupled into the oscillating mode, N the carrier concentration (m^{-3}), N_{thr} the carrier concentration at threshold $= 2.5 \times 10^{24}$ m^{-3}, N_0 the carrier concentration at inversion $= 1.2 \times 10^{24}$ m^{-3}, τ the round trip time of slave laser cavity $= 2nL/c = 5$ ps, τ_p the photon lifetime in cavity $= 2$ ps, τ_r the carrier lifetime $= 5$ ns, α the linewidth enhancement factor $= 3$–6, J the pumping current density, η the internal quantum efficiency, and d the active layer thickness.

The L–K equations are point-independent equations describing the active material. Though quite different from other system-based equations describing the oscillator, they yield all the results found with other approaches, including Adler's equation [1]. When compared to experiments, the L–K equations are found to provide remarkably accurate modeling of both weak-level self-mixing phenomena and high-level chaos-related dynamics. The only deviation is a larger than predicted linewidth of oscillation, reconciled with experiment, as first proposed by Henry [18], with the introduction of an *a-posteriori* linewidth enhancement factor α in the L–K equations, on the second line of Eq. (2), with typical values between 1.1 and 6 [19].

Concerning the structure of the L–K equations, we see that nonlinearities are already present for $\kappa = 0$ (unperturbed laser) with terms of saturation $G_N NE$ and depletion of states $G_N(N-N_0)E^2$. Yet, these terms are not sufficiently strong to promote chaos, and, indeed, the semiconductor (single mode) laser is a class B laser inherently stable in standalone condition. It is when κ becomes large enough that the new term $E_s\cos\phi$ drives the laser out of the deterministic regime, into chaos oscillation.

Indeed, the laser constitutive equations are similar to the equations of atmospheric turbulence found by Lorenz, as originally pointed out by Haken in 1975 (see the discussion of Ohtsubo in Ref. [11]).

From Eq. (2), the quantities E, ϕ and N are computed numerically, using the standard Runge–Kutta method to integrate the time derivatives on a sufficiently small time interval step. The parameters governing system evolution are the coupling coefficient $K = E_s/E_0$, and the frequency offset Δv. In a typical simulation [17], we may start with 0.01-ps steps and assume initially a constant value for Δv (e.g., 360 MHz), while K is varied from 0 to 0.1.

As the characteristic quantity describing the system behavior, we take the beating signal S

$$S = E_s E_0 \cos(2\pi\Delta vt + \phi) \tag{3}$$

observed at a photodetector that receives the superposition of E_0 and E_s. [In fact, the photodetected current is $S = \sigma P$ in terms of the average optical power P and of the spectral sensitivity σ; as $P = A \langle |E_s + E_0|^2 \rangle / Z_0$, where A is the detector area and Z_0 is the vacuum impedence. On developing the square modulus, we find $S = (\sigma A / Z_0)[E_s^2 + E_0^2 + 2E_s E_0 \cos(2\pi \Delta v t + \phi)]$ whence Eq. (3) follows when the constant terms E_s^2 and E_0^2 are dropped].

Four representations are commonly used to visualize the trend of signal S:

  (i) the *amplitude portrait*, i.e., the modulus ISI of the beating signal versus coupling the strength K;
 (ii) the *time series*, that is, the time-dependent waveform of $S(t)$;
(iii) the (electrical) *frequency spectrum* of signal S;
(iv) the *state diagram*, that is the graph of S versus dS/dt.

Now let us illustrate the results of simulations [17] of the injection system (Fig. 3) predicted by the L–K equations (Eq. (2)).

The amplitude portrait is shown in Fig. 4, after normalization to the unperturbed value. First, there are changes of amplitude from the unperturbed condition to that of high K. Second and specific to strong coupling, we notice *bifurcations* at certain values of K, where the amplitude may undergo either an increasing or a decreasing evolution. The choice of which path is followed critically depends on the initial values of the variables, with a fine intermixing on the decimal places of variables deciding the result of evolution. Regime is here periodic or multiperiodic, with creation of sub-harmonics of the beating frequency Δv.

At even larger K's, we see that amplitude can vary widely, the sign of chaotic behavior. Chaos and multiperiodicity will alternate for a range of K values, until the system goes through closing bifurcations and reaches a final locking.
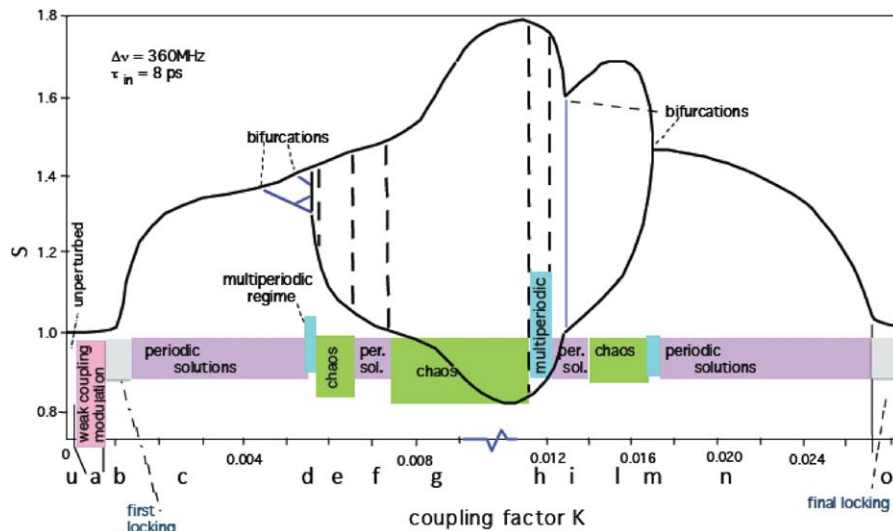

Fig. 4. Evolution of the amplitude of the beating waveform $E_s E_0$ as a function of the coupling strength K. Several regimes are encountered between the first locking at $K = 0.0006$ and the final locking at $K = 0.027$: periodic and multiperiodic solutions and chaos, as well as opening and closing bifurcations. Waveforms, frequency spectra and state diagrams for each regime are reported in Figs. 5–10.

We can illustrate the regimes at increasing K, looking at the corresponding time series, frequency spectrum and state diagram:

– at $K=0$ to 0.0001 (interval u in Fig. 4), the regime of *unperturbed* oscillations, the time series is a sinusoid, the frequency spectrum is a line at the detuning frequency Δv, and the state diagram is a circle (Lissajous curve for $x=\cos 2\pi\Delta vt$ and $y=\sin 2\pi\Delta vt$), see Fig. 5.

– at $K=0.0001$ to 0.0006 (interval a in Fig. 4), see Fig. 6, interaction with the injection signal produces a *weak modulation* regime [15] characterized by distortion of the beating waveform. The waveform becomes increasingly peaked, with the production of integer harmonics ($n=2,3,4...$) of the beating frequency Δv; the state diagram accordingly becomes distorted, but remains a single loop curve [15]. This regime is common to He–Ne (class A) as well to semiconductor diode (class B) lasers. Experiments match very well with theory [15] (see also below).

– at $K\approx0.0006$ to 0.0014 (b in Fig. 4), we reach the *first locking*. The beating waveform disappears (Fig. 7). But, different from plain oscillator theory, we have not reached the final stage of the evolution, because then,

– at $K=0.0014$ to 0.0051 (c in Fig. 4), the system exits from the locking condition, and it generates a *periodic waveform*, peculiar of the high-level dynamics because its signal now contains a sub-harmonic ($n=1/2$) of the beating frequency. This is visible in the time series (Fig. 8) and, more clearly, in the frequency spectrum; the state diagram has now a characteristic double loop.

– at $K=0.0043$, we observe a *first bifurcation* and at $K=0.0051$, a *second bifurcation*.

– at $K=0.0051$ to 0.0058 (d in Fig. 4), we obtain the *multiperiodic state*, with more subharmonics ($n=1/2, 1/3, 1/4,...$) with respect to the point c case, and more loops in the state diagram (Fig. 9). Creation of sub-harmonics is highly characteristic of the complex system, or chaos regime, because no (memoryless) nonlinearity in amplitude can generate them - ordinary distortion produces harmonics, not sub-harmonics.

– at $K=0.0058$ to 0.0066 (e in Fig. 4), we finally find the *chaos regime*. The time series waveform is erratic, the frequency spectrum is rich with integer and sub-harmonics, and a state diagram that nearly fills all the available E,E' space (see Fig. 10). The dotted vertical lines marking the e region in Fig. 4 indicate the range of the values taken by the beating amplitude.
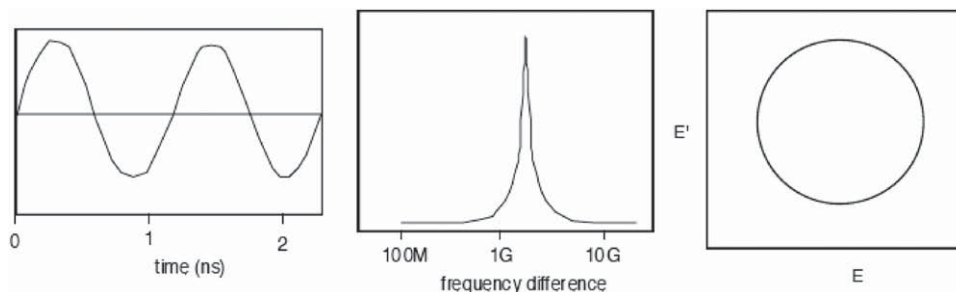

Fig. 5. Time series (left), frequency spectrum (center) and state diagram (right) of the beating signal at very small K (0 to 0.0001) or, in unperturbed conditions (point u in Fig. 4).
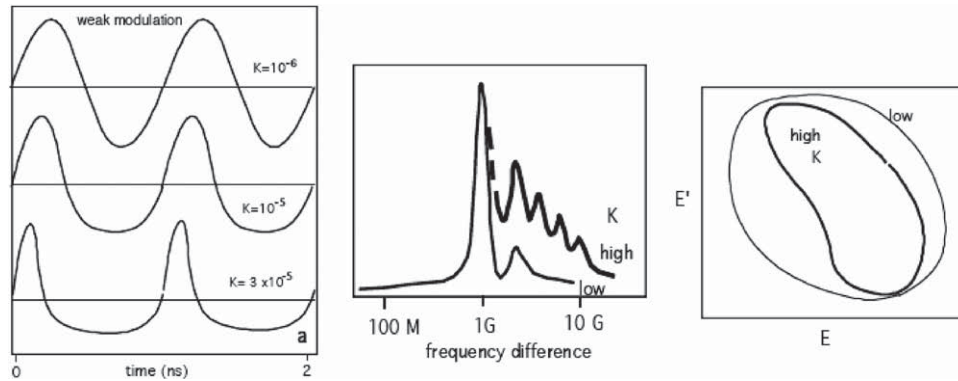
Fig. 6. Time series (left), frequency spectrum (center) and state diagram (right) of the beating signal at small $K=0.0001$ to 0.0006, in the weak coupling modulation regime (point a in Fig. 4). The beating waveform is progressively distorted at increasing coupling, and several integer harmonics show up in the frequency spectrum; the state diagram shape is a deformed single loop.
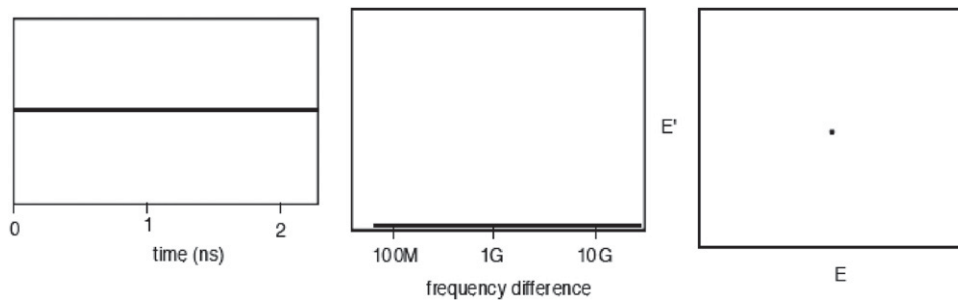

Fig. 7. Time series (left), frequency spectrum (center) and state diagram (right) of the beating signal at $K=0.0006$ up to 0.0014 (point b in Fig. 4), when system locks on the external injection and the beating signal disappears.
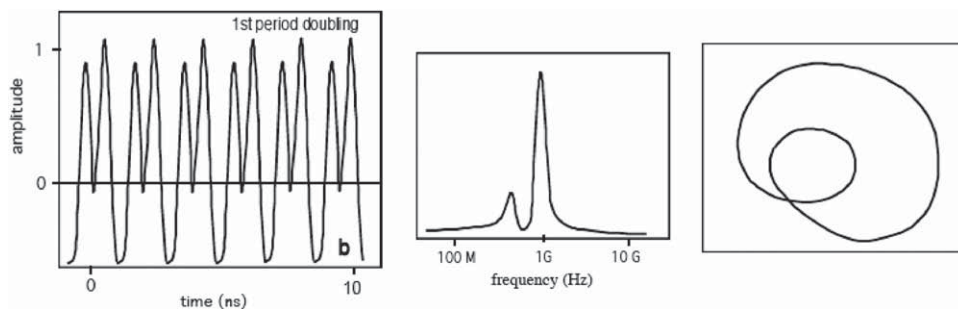

Fig. 8. Time series (left), frequency spectrum (center) and state diagram (right) of the beating signal at $K=0.0014$ to 0.0051 (point c in Fig. 4). This is the regime of *periodic solutions*, with the characteristic feature of sub-harmonics of the frequency detuning Δv, and the double loop in the state diagram. The system moves away from this regime at increased K, but later returns to it three times, in the intervals (points f, i and n in Fig. 4) $K=0.0066$ to 0.0074, $K=0.0124$ to 0.0140 and $K=0.0174$ to 0.027.
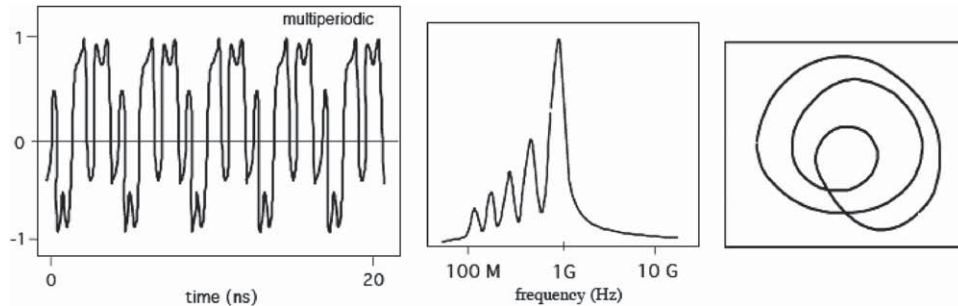
Fig. 9. Time series (left), frequency spectrum (center) and state diagram (right) of the beating signal at $K=0.0051$ to 0.0058: the injected signal locks the slave oscillator (point d in Fig.4). This is the regime of *multi-periodic solutions*, with the characteristic feature of several sub-harmonics of the frequency detuning Δv, and the multiple loops in the state diagram. The system moves away from this regime at increased K but it will later return back to it twice, in the intervals (points h and m in Fig.4) $K=0.0116$ to 0.0124 and $K=0.0165$ to 0.0174.
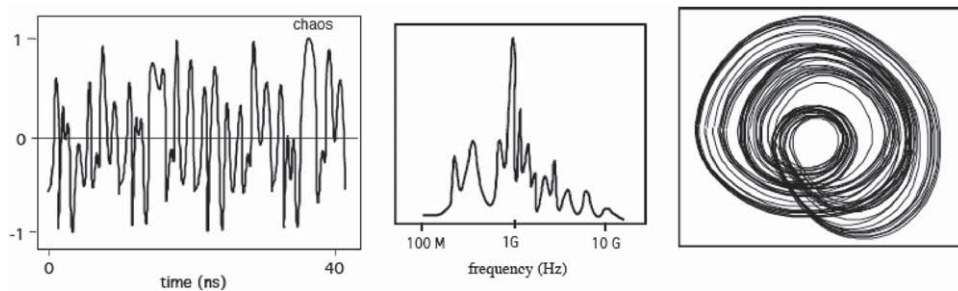

Fig. 10. Time series (left), frequency spectrum (center) and state diagram (right) of the beating signal at $K=0.0058$ and up to 0.0066 (point e in Fig. 4). This is the regime of *chaos*, with the characteristic feature of several harmonics and sub-harmonics of the frequency detuning Δv, and a lot of loops nearly filling all the space available in the state diagram. The system moves away from this regime at larger K, but it will later return back to it twice, in the intervals (points g and l in Fig. 4) $K=0.0074$ to 0.0116 and $K=0.0140$ to 0.0165.

After the chaos regime, unexpectedly,

– at $K=0.0066$ to 0.0074 (f in Fig. 4), system returns to a *periodic* regime, and the description of Fig. 8 still applies,
– at $K=0.0074$ to 0.0116 (g in Fig. 4), system goes back to the *chaos* regime, and the description of Fig. 10 still applies,
– at $K=0.0116$ to 0.0124 (h in Fig. 4), system enters the *multiperiodic* regime, and the description of Fig. 9 still applies.
– at $K=0.0124$ to 0.0140 (i in Fig. 4), we return to a *periodic* regime, and the description of Fig. 8 still applies,
– at $K=0.0140$ to 0.0165 (l in Fig. 4), we find again the *chaos* regime, and the description of Fig. 10 still applies,
– at $K=0.0165$ to 0.0174 (m in Fig. 4), we again enter a *multiperiodic* regime, and the description of Fig. 9 still applies,
– at $K=0.0174$ we find a closing bifurcation,

– at $K=0.0174$ to 0.027 (n in Fig. 4), we go back to a *periodic* regime, and the description of Fig. 8 still applies,

– at $K \approx 0.027$ (o in Fig. 4), we obtain the *final locking* and the beating waveform vanishes again as in Fig. 7.

Summarizing the evolution of the ICL system, we find two locking regions, one *labile* at a very small level of coupling, $K=0.0006$–0.0014, and one strong and *final* locking region at $K>0.027$. Below labile locking, there exists an injection modulation regime. Sandwiched between labile and strong locking we have found regimes of periodicity (P), multiperiodicity (M) and chaos (C) which occur in turn repeatedly (in the sequence PMCPCMPCMP for the chosen set of parameters), with three chaos intervals in the range $K=0.0058$–0.027.

Note that we have described regimes in terms of $K=E_s/E_0$, the ratio of *field* amplitudes. Correspondingly, the range of fractional powers involved is K^2. Thus, the first locking is found at $P_s=0.4$–$2 \times 10^{-6} P_0$, the final locking is reached at an injected power of $P_s=0.73 \times 10^{-3} P_0$ (much higher than labile locking), and chaos is generated in the three ranges of injected power levels of $P_s=3.3$–$4.3 \times 10^{-5} P_0$, 5.5–$13.4 \times 10^{-5} P_0$, and 1.9–$2.7 \times 10^{-4} P_0$ (the last being the preferred because it is the widest), etc.

With regard to the effect of detuning Δv, it was known since the times of Adler's equation that the coupling strength K_{lock} required for locking is proportional to Δv because the locking condition is $B=A$ (see Eq. (1) and ff), and in our notation $A=\Delta v \; B=K\kappa/\tau$, whence $K_{lock}=\tau \Delta v/\kappa$.

Of course, detuning Δv has also influence on the chaos dynamics. Already in the early papers [17,11] it was verified that some features of the dynamics may actually change with Δv, like the number of periods of the P–M–C sequence, but basically always with the same character and distinctive features of each P–M–C regime, as expected from a fundamental perspective. However, to design a chaos-based system, we need to know more concerning the effect of Δv on the system.

A detailed map of the high level behavior of the ICL system, in the coupling-detuning plane (K-Δv), has been computed in [20], by numerical solution of the L–K equations (as described above, for $\Delta v=360$ MHz), on a grid of values so as to fill the plane of parameters. Results are illustrated in Fig. 11, and indicate that, for all combinations of K and Δv values, the dynamics of the P–M–C and locking regions is, indeed, a complete description of the injection phenomena, because: (i) no new regime is found, (ii) each regime fills a connected area of the K-Δv diagram with a continuous contour, and finally, (iii) the general trend found for the single Δv value is also followed by other combinations of parameters.

These theoretical predictions are confirmed by the experimental evidence provided by the measurements by Troger et al. [21], reported in Fig. 12. They used an injection scheme like that of Fig. 3 yet with fiber-guided propagation, with two identical DFB lasers emitting ≈ 2.5 mW at $\lambda=1.3$ μm, and a 70-dB optical isolator between master and slave lasers.

In another region, that of injection modulation region below first locking, experimental results [8,15] obtained with a He–Ne dual-mode laser were found to be in excellent agreement with theory (see Fig. 13).

Several authors have also published experimental results about frequency spectra and time-series of periodic, multiperiodic, and chaos regimes, and the interested reader can find abundant literature on the subject. See, for example, Refs. [11,12,22]. All the results show
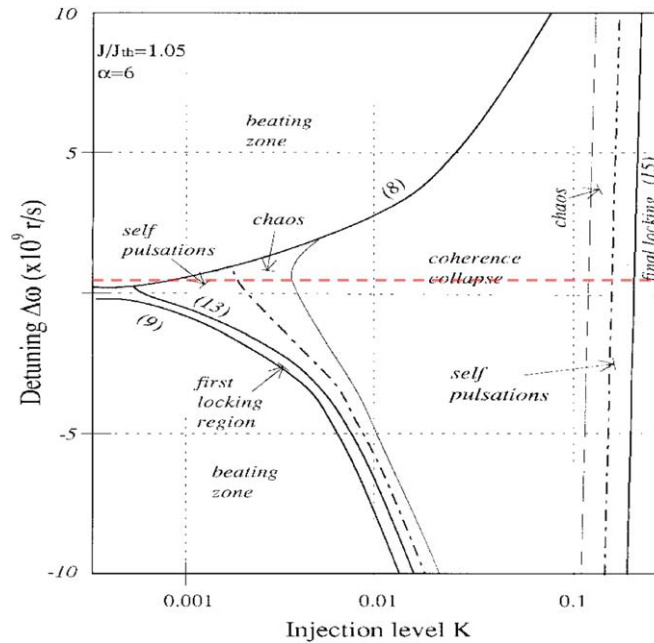
Fig. 11. Calculated regimes of injection system in the K-Δv plane of coupling factor versus detuning of injected frequency with respect to unperturbed oscillator frequency. Dotted line is for the results described in the text and waveforms of Figs. 4–10. (Adapted from Ref. [20], courtesy of IEEE).

a very good agreement of the calculated and experimental values of waveforms and spectra (or, at least, of their trends), even on a wide range of values of system parameters. Thus, we may safely conclude that the L–K equations provide an adequate framework and an accurate description of injection phenomena.

The only deviation from the L–K linear theory predictions occurs when the power density in the laser is large enough to excite nonlinear effects in the master and slave fields. In particular, Brillouin scattering can enhance components close to the central frequency of the slave laser and widen the line, whereas Raman scattering provides gain at frequencies far away from the central frequency and can be neglected (but a loss will be incurred).

Four-wave mixing can produce cross-products of the master and slave fields and their harmonics and sub-harmonics, thus considerably crowding the frequency spectrum. However, since the power internal to a typical semiconductor laser is below, say, 20 mW, nonlinear effects will produce small deviations from linear theory, and can be usually neglected.

Lastly, it is worth reporting that a *mutual-coupling*, *symmetrical* injection scheme, the one we can obtain by removing the optical isolator in the scheme of Fig. 3, exhibits virtually the same dynamical behaviour as that described above for the asymmetrical case.

Indeed, for a symmetrical-injection, we should duplicate the equations for the two fields E_1 and E_2 by re-writing Eq. (2) twice, with E_2 and ϕ_2 as the forcing terms in the E_1 and ϕ_1 set of equations, and vice versa for the other set. At small K, the perturbation is small and the amplitude of the forcing term is nearly constant, thus it is no surprise that solutions are very close to, and basically share the same trend of, the asymmetrical case of injection.
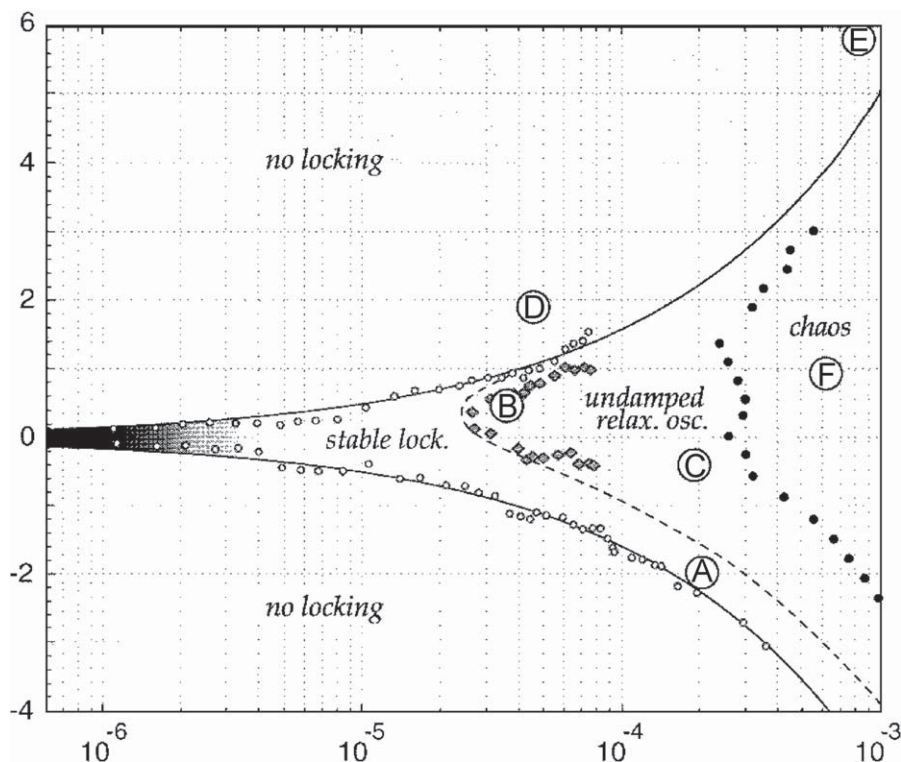
Fig. 12. Experimental results (points) about the injection system regimes in the K-Δv plane of coupling factor versus detuning. The horizontal scale is for $K=P_s/P_0$, and the vertical scale is for frequency detuning in GHz. Agreement of the trend with the results predicted by L–K equations (Fig. 11 and lines) is quite good. (Adapted from [21], courtesy of IEEE).

2.2. Interpreting the states of an injected coupled laser (ICL) system

The waveforms generated in the injection process lead to a rich variety of new dynamical regimes, such as injection modulation, periodic, multi-periodic and chaos, and they can be thought as a kind of *eigenfunctions* of the complex system (our injected coupled laser ICL), not significantly different from sinusoidal oscillations being the free response of an oscillator based on a second-order resonance.

A question then follows: what if we *inject* from the external laser the beating waveform into the ICL? The conjecture is that the system should react by adjusting itself to follow the dynamical evolution represented by the injected signal, or *become synchronized*.

Drawing a parallel, we need a frequency not too far from the free oscillation frequency when attempting to lock a linear second-order (RLC) oscillator. Thus, turning to ICL, it is reasonable to expect that we need a waveform *not too far* from the free response generated by the system to be able to synchronize the ICL, complex system.

2.3. Synchronization of injected coupled lasers (ICL)

ICL synchronization was introduced almost simultaneously by Annovazzi et al. [23] and Mirasso et al. [24], with papers submitted only a few days apart.
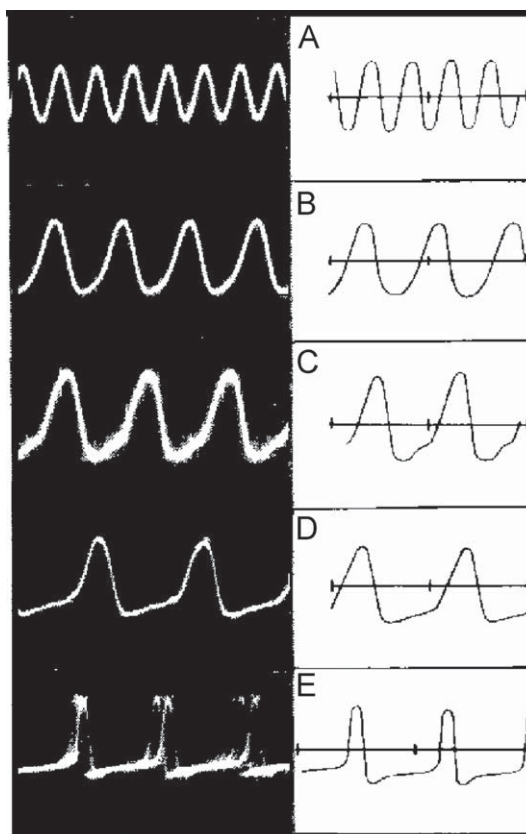
Fig. 13. Experimental (weak) injection-modulation waveforms in a dual-mode He–Ne laser and the corresponding theoretical results calculated (top to bottom) for $K/K_{lock} = 0.3$, 0.7, 0.85, 0.90 and 0.97 (Adapted from [15], courtesy of the IEEE).

To study synchronization [23], let us consider the scheme of Fig. 14, with two identical ICL systems, system 1 with LD1 and LD2, and system 2 with LD3 and LD4. Both systems have an isolator for the injection of the master into the slave. The output of system 1 (out 1) is connected to the summation node in system 2, at the input of slave laser LD4. Furthermore, the output of LD4 is sent in subtraction to the node in system 2. By this arrangement, when the outputs of LD2 and LD4 differ, system 1 will apply a correction to system 2 to bring it closer, and when equality is reached (out 2 equal to out 1), no further correction is applied, and system 2 is thus synchronized and can evolve freely.

To the scheme of Fig. 14, we can apply the L–K equations and compute the evolution of the output E_2 of system 2, starting from an arbitrary quiescent point up to a steady-state solution. In this way, we obtain the diagram of Fig. 15 where the amplitude error $(E_2 - E_1)/E_0$ is plotted versus time [23], showing that after a few cycles of oscillation, synchronization is achieved with a small residual error. Data in Fig. 15 are for a set of parameters that generate chaos (see Fig. 15 inset) and have $K = 0.006$. System 2 has also $K = 0.006$ but starts from an initial condition E_2 far from E_1. This was chosen as the most difficult case for synchronization; for
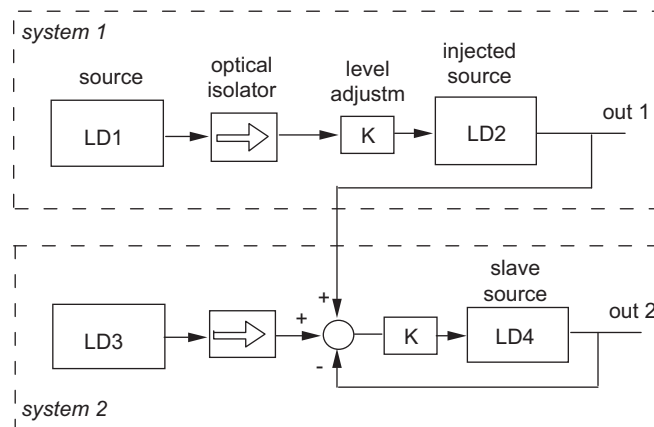
Fig. 14. Scheme for testing synchronization: two identical ICL systems (LD1/LD2 and LD3/LD4) are used. The output of system 1 (out 1) is sent to the summation node at the input of slave laser LD4 of system 2. The output of LD4 is sent to the node in subtraction, so that when out 2 is equal to out 1 no further correction is applied (From [23], courtesy of the IEEE).
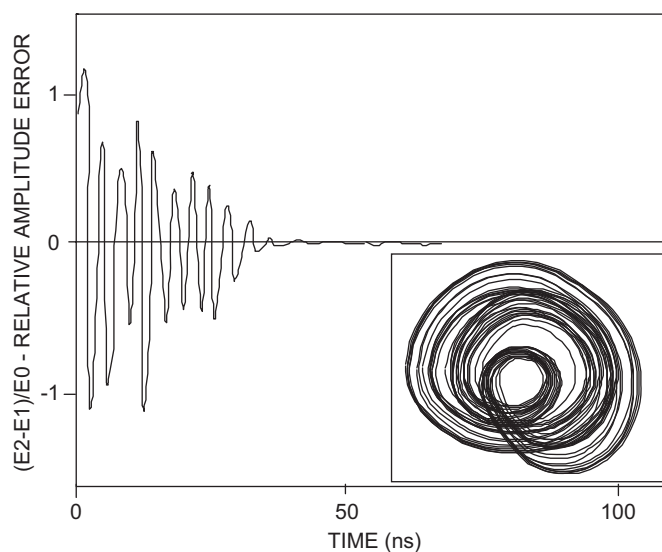

Fig. 15. Synchronization error $(E_2-E_1)/E_0$ of the slave (system 2 of Fig. 14) with respect to the master (system 1 of Fig.14) as a function of time. Inset shows the state diagram indicating that systems are in a choas regime. (Adapted from [23], courtesy of the IEEE).

other regimes (periodic, multiperiodic), the error was found to be smaller and to damp out even faster.

One critical issue is the *sensitivity to system parameters*. Ideally, in any synchronization scheme directed to a cryptographic application, small deviations from nominal values of the parameters (of the laser and of the injection source) should be tolerated, whereas when a certain threshold for mismatch (for example, 0.5%) is exceeded, synchronization should

not be achieved any longer, and the error $(E_2 - E_1)/E_0$ should become the largest possible. This is the ideal condition represented by the red dotted lines in Fig. 16. For the real system, the diagram of synchronization error $(E_2 - E_1)/E_0$ is calculated as a function of the rms error allowed for the parameters used in the L–K equations, and the result is plotted in Fig. 16 (at left). The effect of gain mismatch (affecting E_2 and E_1) can also be considered, as well as its reduction when removed by amplitude trimming or ACG (automatic gain control), see Fig. 16 (at right).

Changing the injection parameters $(K, \Delta v)$ or the laser parameters $(G_N, N_0, J, \eta, \alpha, \tau_r,$ etc.) over a range of reasonable values will affect the curve of Fig. 16, but not drastically its general trend. As an average of cases, we find that a low synchronization error requires a parameter mismatch less than ∼0.2%. On the other end of parameter space, the error is large and synchronization is lost for a mismatch larger than ∼0.8%.

Another special parameter affecting synchronization is the distance of the (master) injected field E_1 from the free-running state in the slave system E_2. Inside the chaos region, the distance can be expressed in terms of the corresponding K values. Then, numerical simulations show that, up to $|K_1 - K_2| \sim 0.2\%$, we obtain a good synchronization (<5% relative error of field amplitudes), while for $|K_1 - K_2| > 1.0\%$, the error becomes unacceptably large (no synchronization).

With regard to the nomenclature currently used in the literature [11,12], authors identify the scheme with the slave receiving injection only from the master system (our ICL) as an *open-loop* configuration, while if the slave also receives self-injection from a remote reflector (the case of DOF, see Section 3), the configuration is known as *closed-loop*. But, as open and closed loop are terms of control theory with quite different meanings, it is advisable that the terms mutual- coupling (or ICL) and self-coupling (or ODF) system are used instead.

2.4. Chaos cryptography with injected coupled lasers (ICLs)

A first scheme of cryptography directly follows from the synchronization results of Section 2.3. The key point is that a high-level dynamics waveform can synchronize a system tuned not much differently from it, whereas a deterministic signal will be ignored by
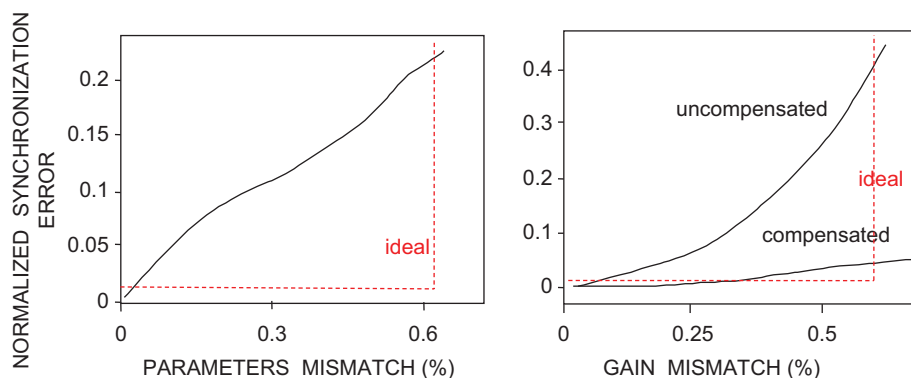

Fig. 16. Synchronization error versus (relative) mismatch of system parameters (left) and versus the bare gain mismatch (right), in uncompensated (normal) and compensated (amplitude-normalized) conditions (Adapted from [23], courtesy of the IEEE).

the system because it is far away from the system free response. Thus, we can devise a *chaotic masking* (CM) scheme of cryptography.

In the implementation of CM with ICL (Fig. 17), first proposed by Annovazzi et al. [23], a transmitter ICL is used to generate optical power with a chaos waveform. At the output node of the transmitter, we sum (incoherently) a small useful signal, a square wave (message in Fig. 17) to the chaos waveform.

The resultant sum signal out of this node is unintelligible (Fig. 18, left) because the square wave is *masked* by a much larger random-looking chaos waveform, both in the time domain and the frequency spectrum.

The sum signal is then sent down the transmission line (typically an optical fiber) to the receiver. At the receiver, we use the sum signal to synchronize an ICL identical to the transmitter (as in Fig. 14). Only the chaos component is effective in synchronizing the slave at the receiver, and, thus, we obtain a replica of transmitted chaos at the receiver output. By subtracting this replica from the received (sum) signal, we are able to recover (or decrypt) the message.

The result is shown in Fig. 18, where we can see the time series and the frequency spectrum of the sum signal (message cannot be detected in them), as well as the result of the decrypted message [23]. There is some residual ripple due to incomplete cancellation of the chaos because of synchronization errors, but the quality of reconstruction is adequate for most application purposes.

The CM scheme actually works, but some drawbacks are readily apparent. First, the incoherent sum at the output of transmitter node will, in practice, be made using slightly different wavelengths for the chaos and the message. This opens a door to the eavesdropper, who can crack the message by fine λ-filtering. Using the same wavelength is also not advisable, because of the resulting optical interference between chaos and message fields.

A second drawback is about amplitudes: if message has to be concealed in the chaos, and do not disturb the synchronization of the receiver, its amplitude shall be small enough. So we may require that message amplitude is not more than 1–5% of the chaos amplitude.

This brings about a power-efficiency issue: namely, most of the photons available from the transmitter laser are used, or better, wasted, in producing the chaos rather than carrying useful information of the message, and this spoils the SNR of the link.
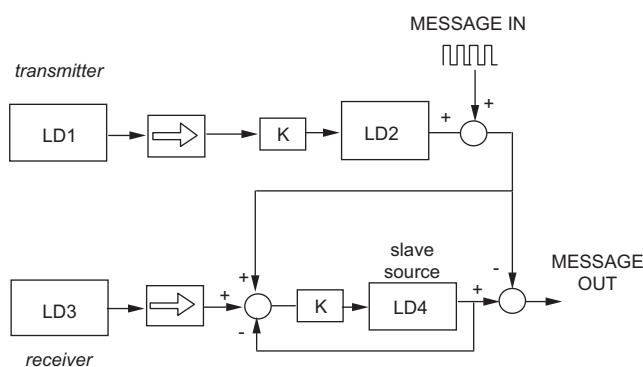

Fig. 17. Chaos Masking (CM) cryptography: chaos is generated by an ICL at the transmitter and the optical emitted power is summed to the optical power of the message. This constitutes the signal sent down the transmission line. At the receiver, an ICL identical to the transmitter receives the signal as in the scheme of Fig. 14. Only the chaos component is effective in synchronizing the slave at the receiver. Resulting difference frees out the message. (From [23], courtesy of the IEEE).
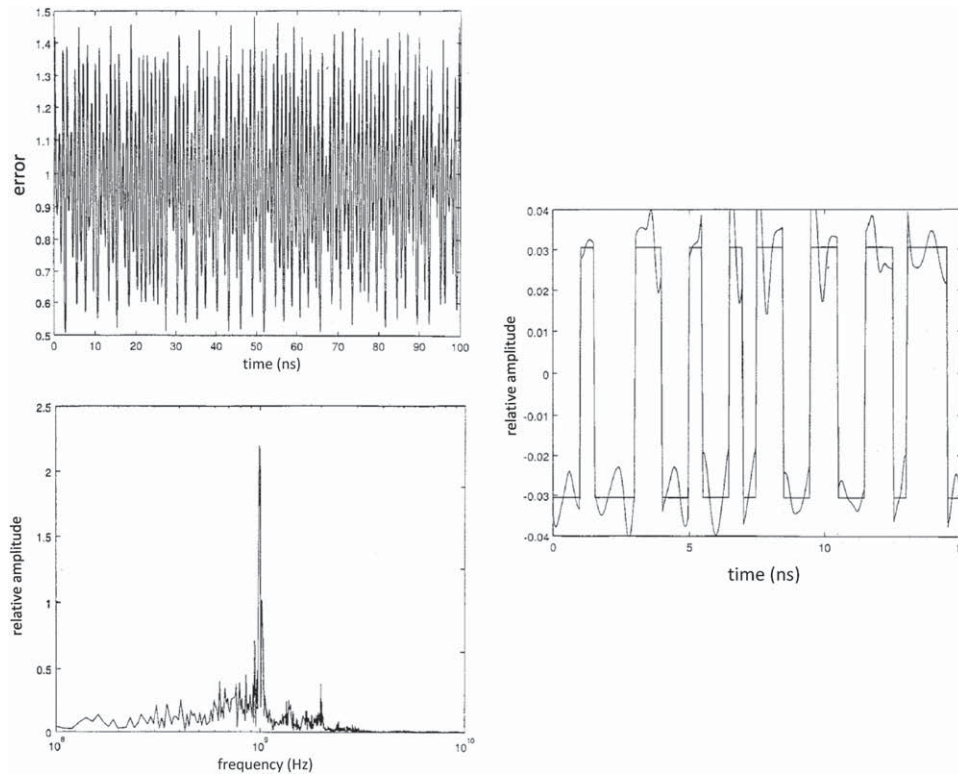
Fig. 18. Signals in the CM (chaos masking) system. Left: the sum signal (chaos+message) time series (top) and frequency spectrum (bottom); right: the reconstructed message resulting from the subtraction of the sum signal and the synchronized chaos. (Adapted from [23], courtesy of the IEEE).

The question is now, how about a scheme in which the signal is of same amplitude as that of the chaos? The answer is chaos shift keying (CSK), a scheme first proposed for ICL by Annovazzi et al. [23]. In CSK, we simply code the bits of a digital message to be transmitted, the "0"s and "1"s, with a different chaos waveform.

As each transmitted bit of the message is associated with the entire chaos waveform, we now fully exploit the available photons, and the SNR is that of a full amplitude message.

Of course, we need a way to generate chaotic waveforms that are undistinguishable to the eavesdropper, yet well recognized at the receiver end. As we will decode the bits through the synchronization process, the issue is on generating waveforms that are mutually orthogonal with respect to synchronization.

This condition can be satisfied by acting on one of the several parameters governing the dynamical evolution of the system, the easiest to access being probably the drive current of the laser (affecting G_N).

Thus, the CSK scheme of cryptography can be implemented as shown in Fig. 19 [23]. At the transmitter LD1/LD2, the drive current of laser LD1 is switched from J_0 to J_1, to code the bit "0" and bit "1" of the message. Current J affects G_N and hence E. Thus, the chaos evolution is different for the two bits. We then obtain a sequence of piece-wise chaos waveforms for the coded message.
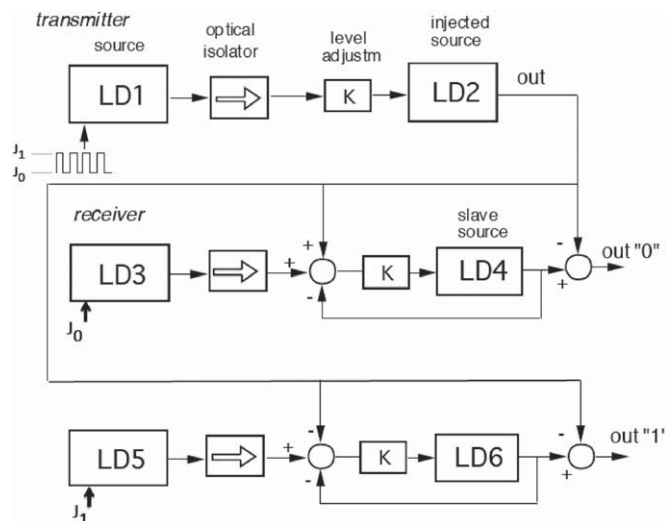
Fig. 19. Chaos Shift Keying (CSK) cryptography: transmitter LD1/LD2 generates a sequence of piece-wise chaos waveforms, representing the bit "0" and bit "1" of the message, by changing the drive current of the laser LD1, from J_0 to J_1. At the receiver end two twin systems are biased at J_0 (LD3) and J_1(LD5) and upon injection of the transmitted waveform, they synchronize on its designated bit, "0" for system LD3/LD4 and "1" for system LD5/LD6. (Adapted from [23], courtesy of the IEEE).

At the receiver end, two twin ICL systems are set at bias J_0 (LD3/LD4) and bias J_1 (LD5/LD6), so that upon injection of the received coded waveform, they synchronize on the designated bit, "0" for system LD3/LD4 and "1" for system LD5/LD6.

As we can see in Fig. 20, the CSK coded waveform doesn't show any trace of the message in the time domain or in the frequency spectrum, but synchronization extracts the sequence of bits of the message at the two outputs of the receiver [23].

The CSK cryptography scheme works well in all the simulations, but when scrutinized from the point of view of engineering and the suitability for implementation, it becomes evident that the two-laser structure of the basic ICL scheme is the weak point. We can actually realize it, but at the expense of added difficulty, because matched pairs of lasers (LD1/LD2, etc. in Fig. 19) are costly and challenging to obtain.

Thus, on the way of transferring chaos cryptography into the world of products, it would really help to have a simpler, possibly the simplest, configuration.

3. Self-coupling systems (or DOF, delayed optical feedback)

The minimum part-count configuration we may consider as the best candidate for a chaos generator is a laser subjected to *delayed optical feedback* (DOF). The DOF is simply the *self-coupled* scheme (Fig. 1) already mentioned in Section 1, also known as the *self-mixing* scheme and one that is widely used, at the weak level of interaction, as a method for measurements of phase and coherent injection detection of remote returns [1].

As shown in Fig. 21, the DOF system comprises a laser, a remote reflector, and an attenuator to adjust the level of feedback to a factor K in field amplitude [25]. A beam splitter conceptually allows us to enter the system with an external signal for the purpose of synchronization. The DOF is simpler than the ICL, and the system can be readily
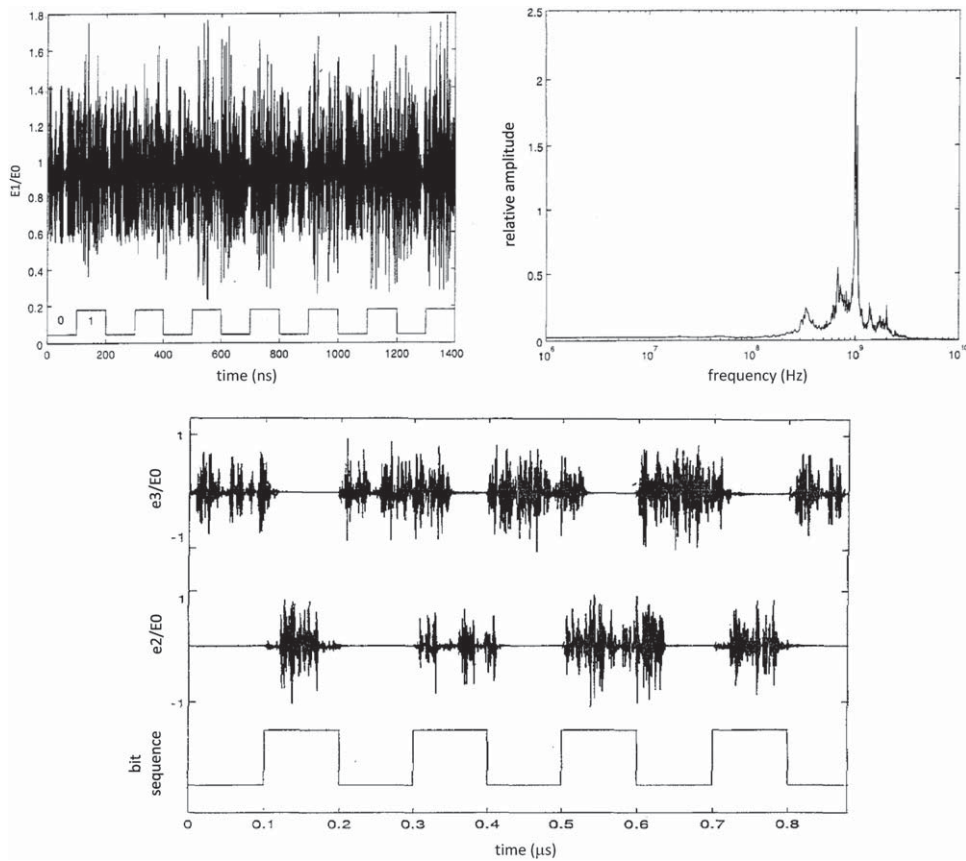
Fig. 20. Signals in the CSK system. Top: time series (left) and frequency spectrum (right), bottom: the sequence of bits separately available at out"0" and out"1" of Fig. 19, along with the message waveform (Adapted from [23], courtesy of the IEEE).

implemented in a compact device by means of well-known technologies such as *all-fiber* and *integrated optics* (Fig. 22).

In a typical all-fiber (AF) setup (Fig. 22 top), the laser diode is butt-coupled or conjugated through a lens to a single-mode optical fiber pigtail. The fiber end-face in front of the chip is angled (at 8–12° typically) so as to avoid back-reflection. The fiber may be a few meters long and terminates at a mirror reflecting back the outgoing end.

By varying the distance between the fiber output tip and the mirror we can easily adjust the level K of feedback. A polarizer and/or a polarization controller are used to inject into the laser light with the same state of polarization as the emitted field (i.e. horizontal polarization, in the plane of the diode junction), and a phase modulator serves to add the phase-coded message.

With a fiber a few meters in length, this DOF scheme would be classified as a *long-cavity* DOF. A long cavity is one for which the total external optical path-length $2s$ is larger than $L_2 = c/2\omega_2$, the length-equivalent of the high-frequency modulation cutoff $f_2 = \omega_2/2\pi$ of the diode laser.
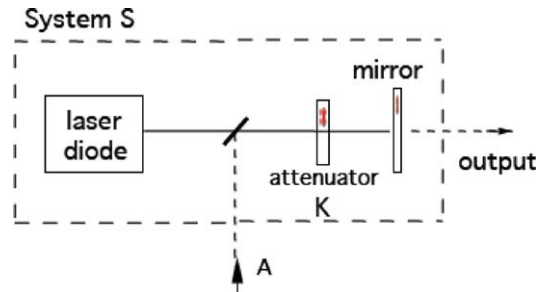
Fig. 21. Scheme for a DOF (delayed optical feedback) chaos generator: the laser is subjected to a self-injection-coupling, or self-mixing regime. The mirror reflects the outgoing beam back into the cavity, and an attenuator is used to adjust the level of feedback. The 45°-oriented beamsplitter serves to inject an external signal for synchronization. (Adapted from [25], courtesy of the IEEE).
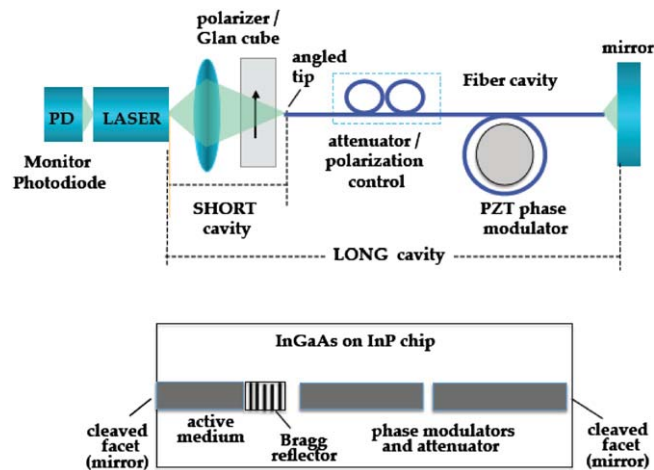

Fig. 22. Technologies for implementing the DOF scheme: all-fiber (top) and integrated optics (bottom).

In the opposite case, if the length is shorter than L_2 (typically a few centimeters), we are in the case of a *short-cavity* DOF, and the feedback reflection will come from the fiber end-face in front of the chip (in this case, the fiber serves to carry the optical signal to a transmission line).

The main differences of the two cases are: (i) the frequency spectrum of the generated chaos is a sequence of lines for a long cavity and a continuous distribution for a short cavity, and (ii) the system (and its generated chaos) is sensitive to the phase of the retro-reflected field (short cavity) or is not, depending only on the intensity (long cavity).

Another variant that we can realize and experiment with AF is that of *coherent* or *incoherent* feedback. When the return to the cavity involves an optical path-length $2s$ shorter than the coherence length of the source at hand, or $2s < L_c$, then the feedback is coherent, whereas if $2s > L_c$ or, another possibility, we re-enter the cavity with a state of polarization orthogonal to the oscillating mode, we obtain incoherent feedback [28]. With

the polarization control of the AF setup, it is straightforward to rotate the returning linear polarization by 90° and be able to experiment with incoherent DOF also with a short fiber.

In the integrated-optics (IO) version, we start with a planar optical waveguide structure, and arrange along the propagation path all of the functions necessary to our system. In the example of Fig. 22 (bottom), we may integrate the laser active region and its Bragg reflector, and two modulators working in push-pull with opposite-sign drives, so that we can introduce a controlled attenuation in the signal reflected back from the (cleaved) end-face, as well as a phase modulation input for the signal. Of course, given the small chip size, the IO lends itself to a short-cavity DOF (see also Section 4.3).

Going back to the system aspects, since the 1980s DOF (and, generally, semiconductor lasers subjected to optical feedback) have been reported to exhibit a number of dynamic phenomena. Such effects were initially described by Tkach and Chraplyvy [26] and later investigated by Petermann [27].

The diagram of feedback strength versus the distance for retro-reflection (Fig. 23) includes five regions associated with specific behavior, such as weak modulation, linewidth narrowing and broadening, coherence collapse, and the external cavity mode (Fig. 23). In the diagram, we add the regions of operation for measurement purposes (self-mixing) and chaos generation.
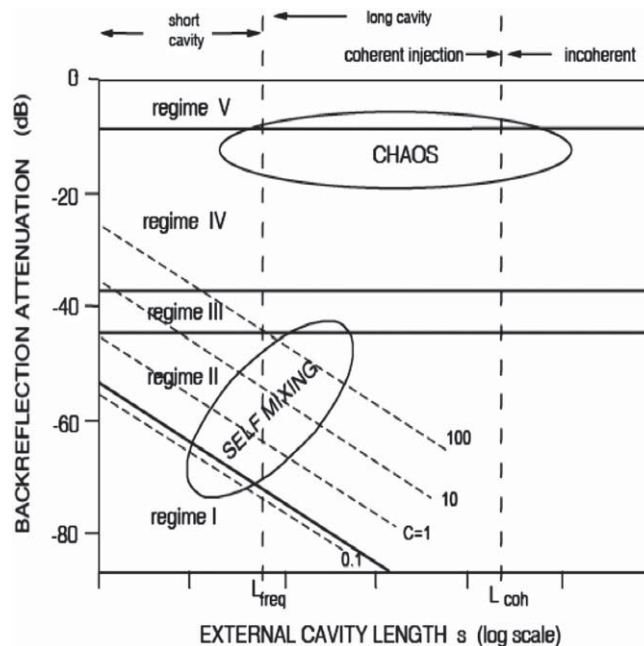

Fig. 23. Diagram of coupling-strength vs. external cavity length: In the original description [26], region I corresponds to linewidth narrowing/broadening (depending on the phase of feedback), II to line splitting and mode-hopping, III to return to single-mode narrow-line operation, IV to coherence collapse, V to external cavity mode. Dotted lines represent constant C for a typical laser diode. L_{freq} is the relaxation length and L_c the coherence length of the laser. Preferred regions of operation for measurements (self-mixing) and chaos cryptography are indicated.

3.1. Paradigm of high-level coupling in DOF

To study DOF operation, we return to the L–K equations (Eq. (3)) and alter them for the case at hand, letting $E_S = E(t-\tau)$ and $\phi_S = 2ks$ for the (self)-injection term, in which $k = 2\pi/\lambda$ is the wavevector, s is the distance to the remote reflector, $\tau = 2L/c$ is the external time delay to the retroreflector, and $\kappa = K$ is the coupling factor.

So we write, with the same symbols (and typical values) as in Eq. (3):

$$dE/dt = \tfrac{1}{2}[G_N(N-N_0)-1/\tau_p]E + (\kappa/\tau_{in})E(t-\tau)\cos[\phi_S + \phi(t)-\phi(t-\tau)]$$

$$d\phi/dt = \tfrac{1}{2}\,\alpha\{G_N(N-N_{thr})-1/\tau_p\} + (\kappa/\tau_{in})E(t-\tau)/E(t)\sin[\phi_S + \phi(t)-\phi(t-\tau)]$$

$$dN/dt = J\eta/ed - N/\tau_r - G_N(N-N_0)E^2(t) - \kappa_{incoh}(N-N_0)E^2(t-\tau) \qquad (4)$$

In the third line of Eq. (4), the last term accounts for incoherent feedback [28]. In this case, we let $\kappa = 0$ and the external perturbation enters in the L–K equations through the decrease of state density due to the delayed field $E(t-\tau)$. For pure coherent feedback, we let $\kappa_{incoh} = 0$ in Eq. (4).

The κ factor in Eq. (4) is the product of $A^{1/2}$, for the power attenuation A associated with propagation to the external mirror and back, the external reflector (field) reflectivity r_{ext}, the mode superposition factor η, and the mirror transmission factor $(1-r^2)/r$, where r is the laser output mirror (field) reflectivity [1,11,12].

From the second line of Eq. (4), we derive again Adler's equation as

$$d\phi/dt = 2\pi v_0 t + C\sin(\phi + \phi_S), \qquad (5)$$

where v_0 is the unperturbed frequency, $C = [1+\alpha^2]^{1/2}\kappa(\tau/\tau_{in})$ is the coupling parameter (or C-factor), and τ_{in} is the laser cavity roundtrip time [1].

Results of simulations of the DOF system with typical values for parameters (the same as in the list of Eq. (3)) show that the evolution of the system follows much the same pattern as that of the ICL system.

There are some important differences, however. The main parameters affecting the dynamics are the coupling factor K (as for injection), and the reflector distance s (in place of Δv). The main description of the system is provided by the field amplitude E (in place of the beating), and with regard to frequency, the high frequency cutoff of the laser f_2 takes the place of Δv.

Self-pulsation, periodicity and chaos are again found for all setup variants (coherent vs. incoherent, short vs. long cavity). The high dynamic regimes lie between an initial region of moderate perturbation heralded by mode hopping due to the external-cavity added phaseshift, and a final state of oscillation and bistability on the external cavity.

Typical results of simulation for E vs. K (for the coherent, short cavity case) are shown in Fig. 24. Concerning the evolution of the dynamic state, we find:

– at very low K ($<10^{-4}$), the system is unperturbed.
– at weak K (<0.002), the system exhibits self-coupling modulations, in amplitude ($\cos 2ks$) and frequency ($\sin 2ks$) with sensitivity to the external phaseshift $2ks$—this is the regime of the self-mixing interferometer [1] and corresponds to the regime of weak injection modulation of the system.
– at moderate K (0.002 to 0.005), the system starts switching in amplitude and frequency due to coupling with external cavity modes (ECMs).
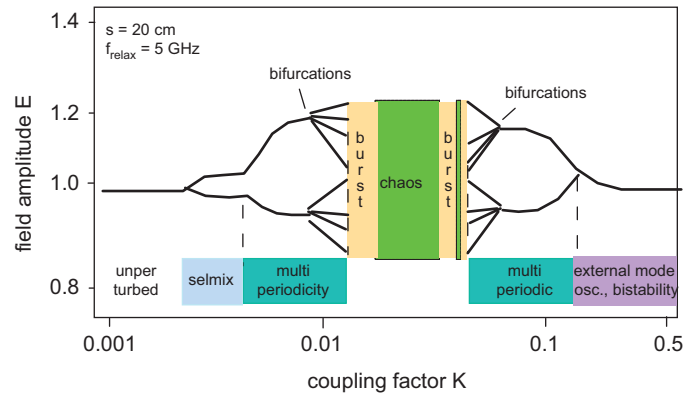
Fig. 24. In the *E* vs. *K* diagram of DOF or self-coupled system, we find alternating regimes of chaos, burst and multiperiodicity, sandwiched between an initial weak modulations (the self-mixing regime) and a final condition of external mode oscillation, much the same character as for the injected system of Fig. 4.

- at larger *K* (0.005 to 0.015), the system enters a periodic/multiperiodic regime.
- at even larger *K* (≈ 0.015), the system breaks into chaotic pulsations.
- self-pulsation and chaos alternate a few times until the system oscillates or becomes locked on the external cavity (at $K \approx 0.04$).
- at still higher *K* values, the system ends up with steady oscillation, or bistability, on the external cavity.

The time series and spectrum for periodic and multiperiodic, burst and chaos regimes of a DOF short cavity coherent system have been calculated from Eq. (4) assuming the standard set of laser parameters (cf. Eq. (2)). The results are reported in Fig. 25. Data are representative of findings for a wide range of parameters, i.e., coupling factor $K = 0.001$ to 0.7, external reflector distance $s = 7.5$ to 30 mm, α-factor varied from 3 to 6, and phaseshift $2ks$ (mod. 2π) varied from $-\pi$ to π. The pattern of transition boundaries from an unperturbed regime to chaos finely depends on the particular set at hand, yet waveforms found in any island have much the same character for a wide combination of parameters. The trend of transition boundaries is moving to decreasing values of *K* as the distance *s* is increased, much the same as reported by Jones et al. [28]. The passage from short to long cavity is located [11] at $L_2 = c/2\omega_2 = 30$ mm for our set of parameters.

An important difference between short and long cavities revolves around the frequency spectrum of the field amplitude in the chaos regime. As shown in Fig. 26, the short cavity DOF gives a continuous spectrum, and amplitude changes with the interferometric phase of the external path $2ks$. The long cavity DOF yields a spike-like spectrum but is insensitive to external phase.

Long cavity DOF has been extensively studied and numerical simulations were confirmed by experimental measurements, basically using the all-fiber setup of Fig. 22. Annovazzi et al. [29] found that, with an external fiber of 0.875 to 9.375 m long, chaos develops over a wide range of bias current (from 10 to 18 mA) and *K* factor (0.05 to 0.2) combinations. The electrical spectra evolves from a few-lines centered at $f = f_2$ (about 4 GHz in Fig. 27) at low *K*, to a wide many-line spectrum, filling the interval of 1.75 to over
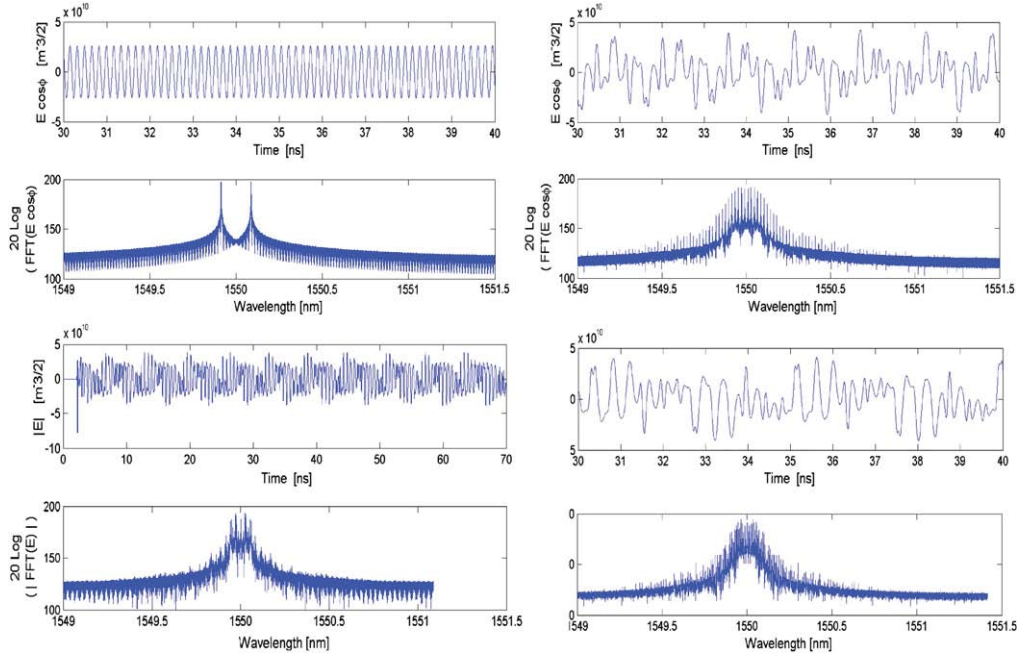
Fig. 25. Time series (top) and optical spectrum (bottom) pairs for a DOF system at different levels of K (0.01 to 0.1), showing the regimes of periodic solution (top left), multi-periodic solution (top right), burst regime (bottom left), and chaos (bottom right).
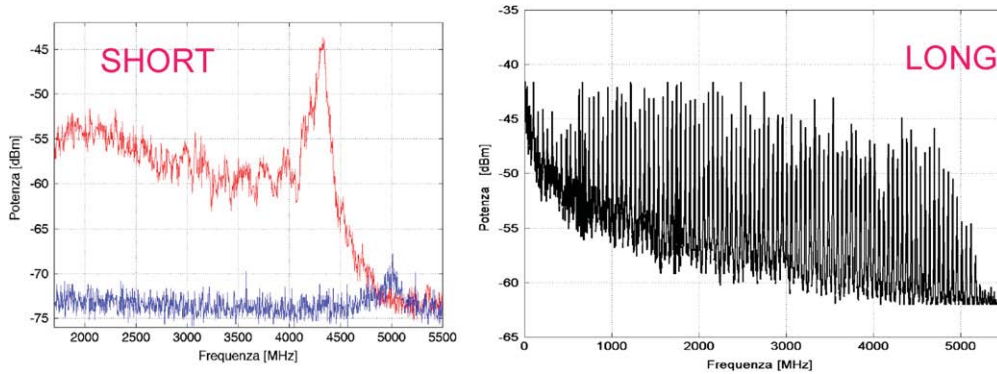

Fig. 26. Frequency spectrum of chaos generated by a short cavity DOF (left), and of a long cavity DOF (right). In the first case the spectrum is continuous and sensitive to external path phaseshift $2ks$, while it is independent from $2ks$ and is made of discrete lines in the second case. (Adapted from [29], courtesy of the IEEE).

5.5 GHz at higher K (Fig. 27). The frequency spacing of the lines is $\Delta f = c/2s$, or 150 MHz for the $s = 72$ cm distance of system in Fig. 22. Consistently, when $s < c/2\Delta f$ ($=3$ cm for $\Delta f = 5$ GHz), the line spacing occupies the entire frequency span and we obtain the continuous spectrum of the short cavity (Fig. 26, left).
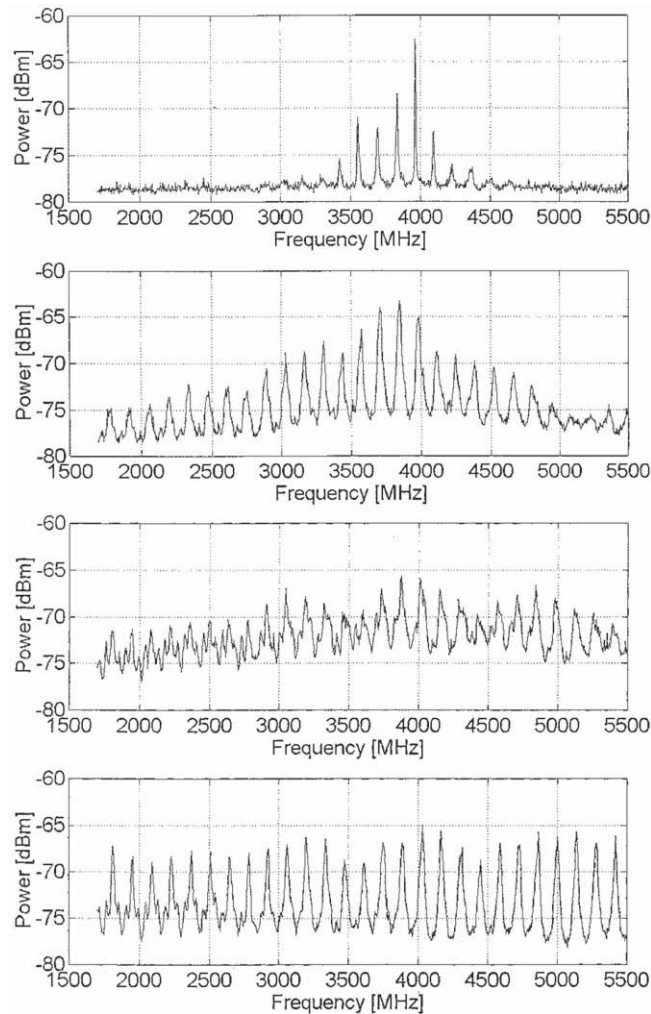
Fig. 27. A long cavity DOF system exhibits a large interval of chaos generation, in current and coupling factor. At increasing K (top to bottom in figure), system evolves from the periodic regime to chaos, and the electrical spectrum spreads from the initial relaxation frequency f_2 (about 4 GHz) to nearly zero and up to $1.5f_2$ and more. (From [29], courtesy of the IEEE).

Incoherent DOF is the case most frequently found in practice when the laser cavity is affected by an unintentional return by the transmission line (even scattering from the fiber) or a stray back-reflection. Only one equation (the third line in Eq. (4)) provides the nonlinear coupling of variables, through the last term delayed by τ, which describes the propagation to the remote backscattering source of disturbance. As the re-injected term decreases N and hence E, the burst regime is enhanced in particular, with delayed and inverted polarity damped oscillation trains, as reported by Ju and Spencer [30]. The usual chaos and periodicity regimes are also found in incoherent DOF, but both are different from the other regimes, the threshold bias current of the laser is not affected by feedback, and chaos is found at a higher level of coupling strength [11,12]. Using a ring external cavity to rotate the polarization of the

returning field by 90°, Ju and Spencer [30] found, at increasing remote mirror reflectivity r, a stable regime for $r < 0.27$, chaos for $0.27 < r < 0.55$, burst relaxation oscillations for $0.55 < r < 0.8$, and a two-state regime for $r > 0.8$ in which the laser switches between on and off states, which are triggered by the delayed reflection.

Among the possible variants of the DOF chaos schemes, the coherent short cavity looks to be the most attractive for cryptographic applications because: (i) it is compact and amenable to integration and batch production; (ii) the range of parameters for chaos generation is wide; and (iii) the coherent dependence on external reflector optical path $2ks$ adds one extra variable to the security of transmission.

3.2. Synchronization of DOF system

Much in the same way as for ICL (cf Section 2.3), synchronization of a DOF can be performed by applying, at the slave system input, the difference of the master (or synchronizing) system S1 and of the output of S2, as shown in Fig. 28 (top), so that when the condition $E_2 = E_1$ is reached, the slave system is allowed to evolve freely [25]. The speed at which synchronization takes place varies with the initial conditions of the slave system and the state of the master, or, type of waveform injected in the slave. A typical result representative of the average speed obtained is shown in Fig. 28 (bottom). The synchronization error, defined as $\sigma = (E_2 - E_1)/E_0$, where E_0 is the unperturbed amplitude, damps out in a few cycles of the relaxation frequency f_2 of the laser, down to a small residual ripple (typically $\sigma = 4 \times 10^{-4}$) left over in the steady state—quite an acceptable (small) error from the engineering point of view.

About sensitivity to parameters of the synchronization error, exhaustive numerical simulations have been carried out [25], and results can be summarized as follows: at an above-threshold current $J/J_0 = 1.1$ to 1.4, the steady-state error σ keeps below 10^{-3} in the K range of chaos generation (1.3 to 10×10^{-4}). With respect to the mismatch of internal laser parameters (i.e., G_N, N_{thr}, N_0, τ_p, τ_r, α, ω_0, η, and d in Eq. (2)), the DOF error follows the same trend of the injected-system data of Fig. 16.

3.3. Chaos cryptography with DOF system

Using the synchronization method described in Section 3.2, it is straightforward to adapt the CSK (Chaos Shift Keying) to DOF, and the resulting scheme is reported in Fig. 29. System S1 generates a sequence of chaotic waveform samples, coded by the binary bits "0" and "1" of the message, which enter the system as the values K_0 and K_1 of the DOF generator. At the receiver end, two receivers R1 and R2 are tuned onto the K_0 and K_1 chaos waveforms, and thus separately synchronize on the sequence of "0" and "1" found in the message. By combining the outputs of R1 and R2 bits we are able to reconstruct the message [25].

In Fig. 29, we report an example of waveforms obtained by the DOF system with CSK coding: upon transmitting a square wave, the output S_{out2} damps to zero at each received "0" bit, whereas S_{out2} will do the same for the "1" bit.

4. Experiments

In recent years, extensive developmental activity has been carried out to demonstrate the feasibility of chaos-based cryptography. Several groups pursued an engineering effort to
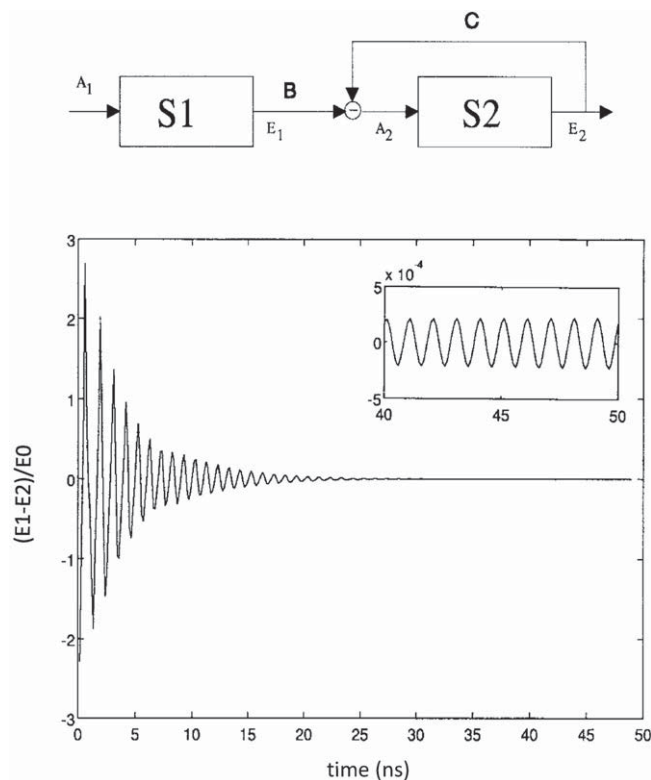
Fig. 28. (Top) Scheme for synchronization of DOF: at the input node of S2, the master output E_1 is added and the E_2 output subtracted, in a way similar to the configuration of Fig. 14; (bottom) the synchronization error $(E_2-E_1)/E_0$ relative to unperturbed value E_0, as a function of time, for a chaos regime of S1. Error damps out fast though a minute residue (see inset, about 4×10^{-4} peak-to-peak) is observed at long times. (Adapted from [25], courtesy of the IEEE).

develop a chaos cryptography system, also thanks to the support of two European programs, Occult and Picasso [31].

Experiments have included Chaos Masking and Chaos Shift Keying generated by DOF systems, initially in discrete micro-optics configuration, and later on in integrated-optics technology. A few experiments have been also conducted with apparatus deployed in the field.

4.1. Chaos masking experiments

Experiments have been first performed according to the CM (Chaos Masking) approach described in Section 3.2.

Annovazzi et al. [32] have used a 1.55-μm DFB laser with a short-cavity DOF to generate the chaos waveform masking the message. The message was a weak optical signal, superposed in intensity with chaos at a wavelength close to 1.55-μm (Fig. 30). At the receiver end, a second laser tuned on the transmitter parameters synchronizes with the chaos contained in the line received waveform. A balanced detector subtracts the chaos waveform from the received waveform and recovers the message.
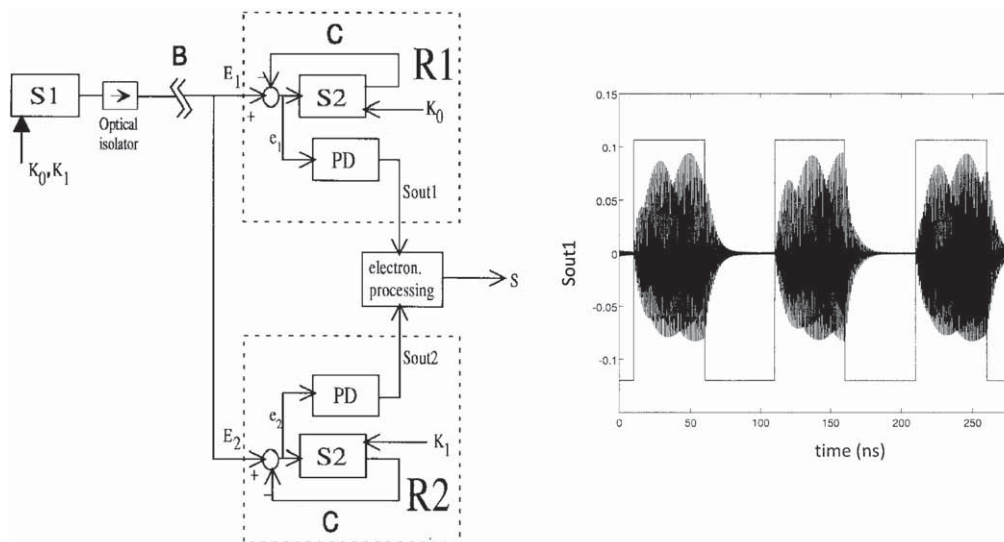
Fig. 29. (Left): scheme of CSK cryptography with the DOF generator S1 in transmission followed, after the line B, by receivers R1 and R2 tuned onto the "0" and "1" chaos waveforms generated by K_0 and K_1. (Right): output of receiver R1 showing the synchronization on the "0" bits in the message. (Adapted from [25], courtesy of the IEEE).

Fig. 31 shows the performance of the CM-DOF system: the time-domain series of chaos at the transmitter and receiver ends are very close, and the frequency spectrum of the transmitted signal (chaos plus message) does not show any intelligible features, while the difference between the received signal and recovered chaos has a clear signal peak at 3 GHz with a CNR (carrier-to-noise ratio) of >5 dB [32]. Another result, shown in Fig. 32, is about the transmission of an audio tone and a video image, both modulated with the 3-GHz carrier. The reconstructed signals are of good quality in both cases. These results were obtained for a back-to-back CM-DOF, that is without any intervening attenuation nor any line noise adding degradation of the transmitted signal, like that experienced on a real fiber trunk.

An experiment on an installed 120-km trunk of monomode G-652 3rd-window fiber then followed [33]. Conducted by Argyris et al., this study was carried out in the Athen's metropolitan network (Fig. 33, left) [33]. As we can see in Fig. 33 (right), the message cannot be recognised in the chaos masked waveform, whereas the signal closely approaches the transmitted signal when decoded by the receiver, so that the BER (bit error rate) is reasonable, even for transmission rates in the Gb/s range. The eye diagram of the CM-DOF system, for a 1.5 GHz transmission, is shown in Fig. 34 [33].

4.2. Chaos shift keying experiments

An improvement of CNR is offered by CSK with respect to CM (cf. Section 2.4), because with CSK it is not necessary to keep the amplitude of message small with respect to that of the chaos masking waveform, as in CM.

On the other hand, the weak point of the CSK basic scheme (Figs. 19 and 29) is the subtraction, at the input node, of output signal E_{out} and synchronizing signal E_{syn}. This operation shall be performed on the field amplitudes, and thus it requires a phase-sensitive
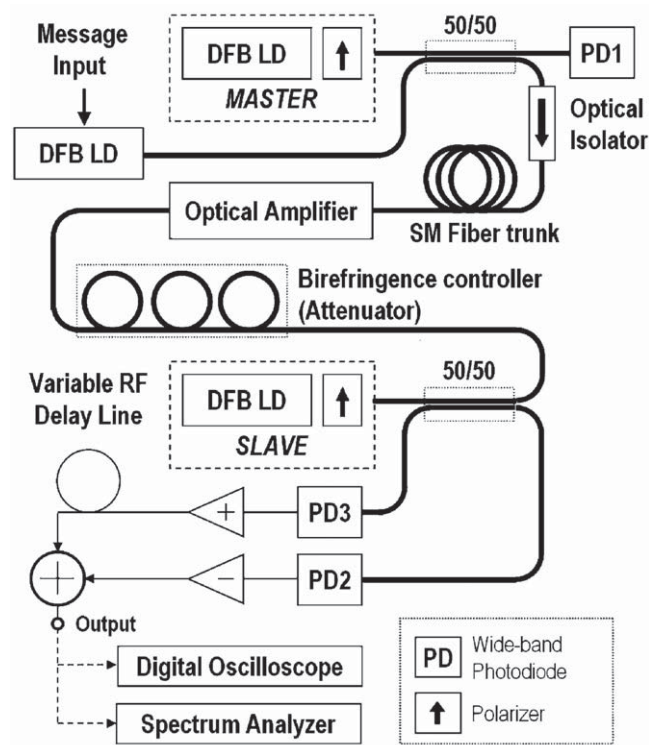
Fig. 30. Chaos Masking experiment with a DOF chaos generator: the MASTER DFB laser is the chaos DOF source, and its output is superposed with the 50/50 fused-fiber coupler to the message, by another DFB laser at a wavelength close to the master. After propagation, the received signal is amplified and adjusted in polarization state and comes to synchronize the SLAVE DFB chaos DOF. The balanced detector (PD2 and PD3 plus fiber coupler) serves to inject the received signal and to make the difference of it and the synchronized chaos. (From [32], courtesy of the IEEE).

adjustment to keep the fields E_{out} and E_{syn} out of phase by π, (or, opposition) a condition critical to be mantained in a practical implementation.

A solution to make a practicable CSK is offered by the DOF system reported by Annovazzi et al. [34]. They used a short-cavity DOF generator and incorporated a phase modulator in the external cavity (Fig. 35). The message enters as the voltage drive ΔV_{in} of the LiTaO$_3$ phase modulator, introducing a phase $\Delta\psi_{in}$ added to the optical pathlength $2ks$. As a short cavity DOF is sensitive to the phase of the external cavity, the generated chaos waveform carries a trace of the message impressed with phase $\Delta\psi_{in}$. At the receiver end, an identical DOF generator has the phase modulator set at zero voltage drive. Thus, the receiver is synchronized only for zero input message or phase $\Delta\psi_{in}$, and the correlation between the receiver and the transmitter chaos waveforms progressively decreases at the increase of the phase difference $\Delta\psi_{in}$. This process is a sort of phase-to-amplitude conversion, and therefore direct photodetection of the receiver chaos optical signal followed by an FM detection supplies a signal proportional to $\Delta\psi_{in}$ and hence to ΔV_{in} [34]. In Fig. 36, we can see the electrical power spectrum of chaos (master) with a message
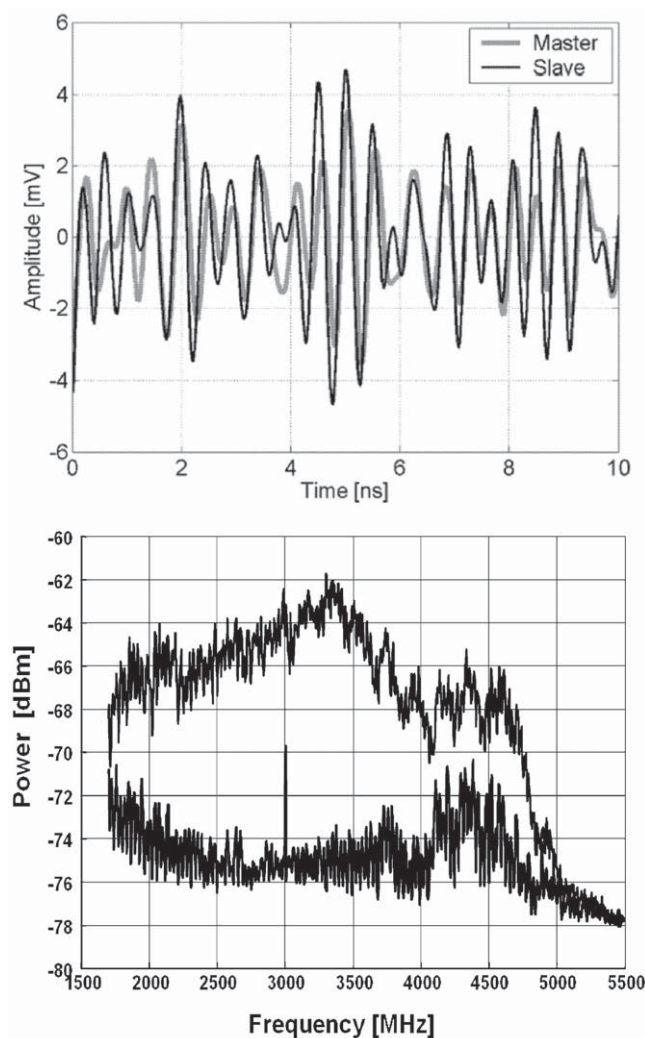
Fig. 31. Performance of the CM-DOF cryptography: the time-domain waveform of the chaotic amplitude (upper figure, gray for master and black for slave) does not show any trace of a message; (bottom): the frequency spectrum of transmitted signal (top trace) and the difference between master and slave (bottom trace) revealing the peak of extracted carrier at 3 GHz (Adapted from [32], courtesy of the IEEE).

hidden in it, and that of the extracted message, the 100-MHz note, now with a good CNR of ≈ 12 dB.

4.3. Integrated optics technology for cryptography

Integrating the functions of a chaos-based system into an IO (Integrated Optics) or PIC (Photonic Integrated Circuit) chip is crucial to demonstrate that high-level dynamics systems not only can work in principle, but are ready to be engineered and to become viable products.
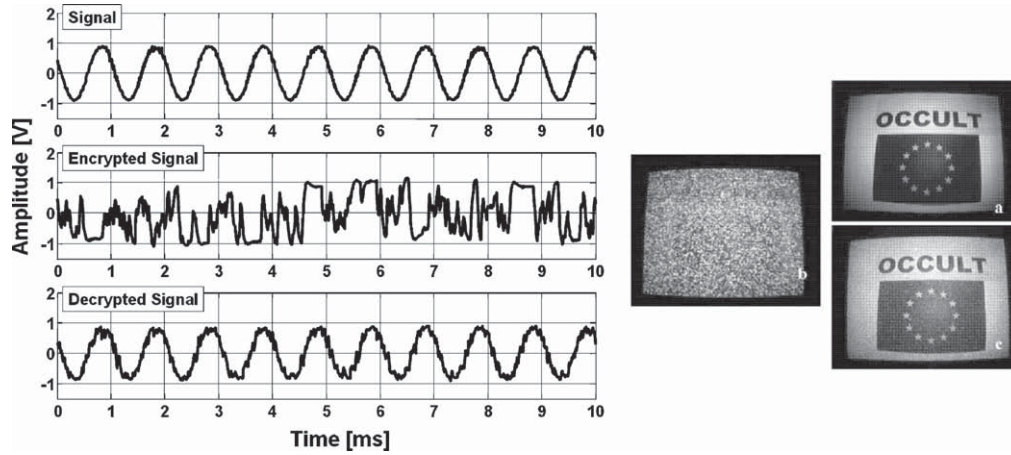
Fig. 32. Signals from the CM-DOF of Fig. 30: a tone at 3 kHz (left) at the input (top), masked by chaos (middle), and reconstructed (bottom); a TV image at 5 MHz video bandwidth, chaos coded (left) and at the input (top right) and output (bottom right) (Adapted from [32], courtesy of the IEEE).
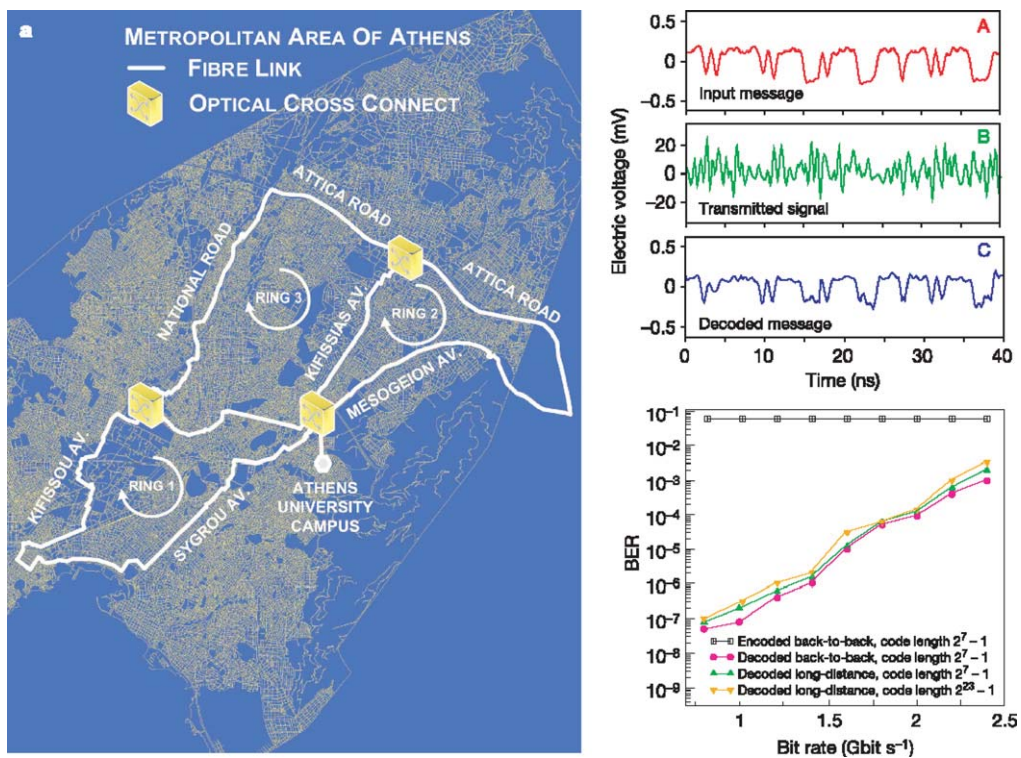

Fig. 33. Path of the 120-km trunk of single mode G-652 3rd window fiber of the Athen's metropolitan network for the transmission experiment with a CM-DOF system (left); right, from top to bottom: message, chaos encoded message, reconstructed message, and bit error rate (Adapted from [33], courtesy of Nature Photonics Letters, London).
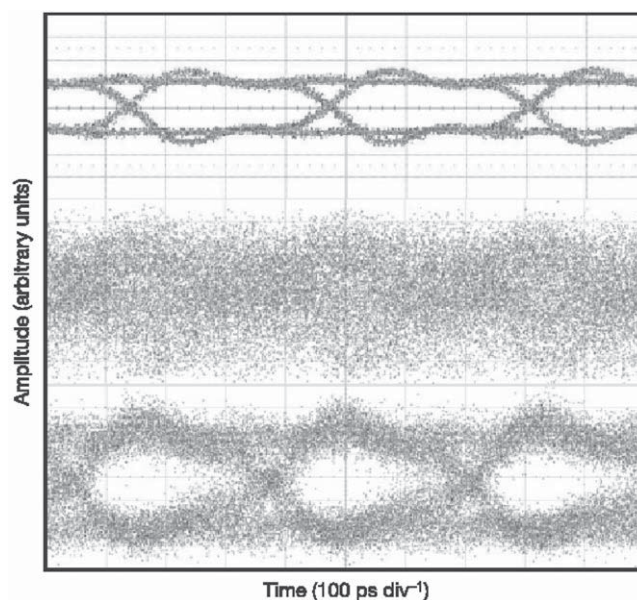
Fig. 34. Eye diagram of the data transmission with the CM-DOF system. Top: input message at 1.5 GHz bit rate; middle: chaos-coded waveform; bottom: waveform reconstructed after a 120-km propagation in single mode, 3rd window, installed fiber (From [33], courtesy of Nature Photonics Letters, London).

Several prototypes or demonstrators have been developed recently [35–38] in the frame of EEC programs [31] as well as of other national (Japan, US) efforts.

Argyris et al. [35] first reported a PIC chip based on indium phosphide technology, that incorporates all the desirable functions to make a versatile chaos generator or chaos-based transmitter based on a short-cavity DOF system. The chip works at 1560 nm, in the third window of optical fibers, and employs a standard InP technology based on ridge waveguide and a multi quantum well InGaAs active layer. The chip includes four basic sections (Fig. 37): (i) a DFB laser of standard design, with a Bragg reflector on one side, and a cleaved facet on the other side (the left-chip edge) where the optical beam is emitted; (ii) a gain/absorption section (GAS) to trim the K factor of re-injection; (iii) a phase section (PS) to finely control the external cavity length $2ks$, at the interferometric level; and (iv) a very long (10-mm) drift section, a passive waveguide going to the right-side chip edge where a high reflective coating is applied. The rings visible in the micrograph (Fig. 37, bottom) are the access contact to the sections, brought out to external connectors by micro striplines. To electrically isolate sections biased at different voltages, a back-to-back doped island can be used, whereas the intermixing process could allow for the reduction of absorption and losses in the passive waveguide zone.

By trimming the bias current to the GAS section, Argyris et al. [35] were able to generate the regimes of unperturbed, periodic and multiperiodic, and chaos, dependent on phase (i.e. current to the PS), at low bias. When the GAS is driven hard by a high current so as to become an SOA (semiconductor optical amplifier), a fully chaotic regime independent of phase is developed. Also interesting is the emergence, at certain intermediate bias levels, of intense peaks at 3.3 and 6.6 GHz [35].
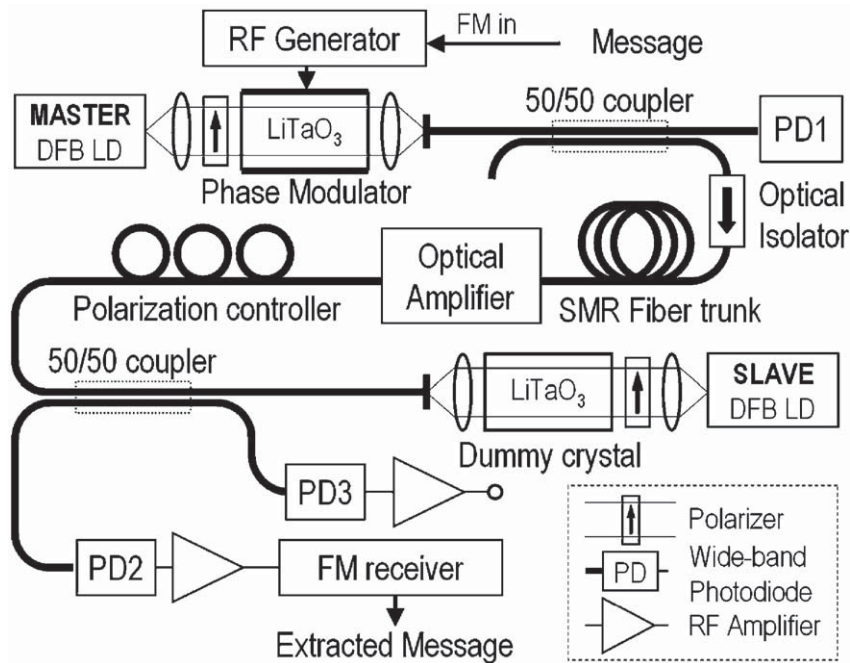
Fig. 35. A short-cavity DOF- CSK system, implemented in hybrid (micro-optics-and-fiber) technology, uses a lithium tantalate phase modulator to impress the message as a phase variation $\Delta\psi_{in}$ in the cavity and hence in the chaos waveform generated by the phase-sensitive DOF. At the receiver, a dummy modulator set at zero synchronizes only when $\Delta\psi_{in}=0$ and its waveform deviates from the input the more $\Delta\psi_{in}$ increases. Photodetection by PD2 and an FM demodulation of signal act as phase-to-amplitude converter, thus extracting the message (From [34], by courtesy of the IEEE).

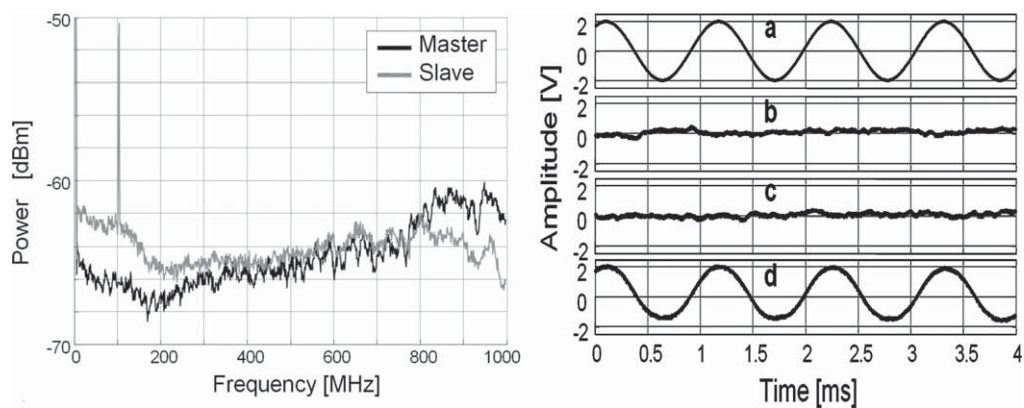
Fig. 36. Left: electrical frequency spectrum of chaos of the master DOF (black curve) with the FM signal hidden in chaos, and of the slave DOF with the extracted signal, the 100-MHz carrier tone (gray curve). Right: sine wave signal transmitted over the carrier (a), with master and slave off (b), with master on and slave off (c), and recovered (d). (Adapted from [34], by courtesy of the IEEE).
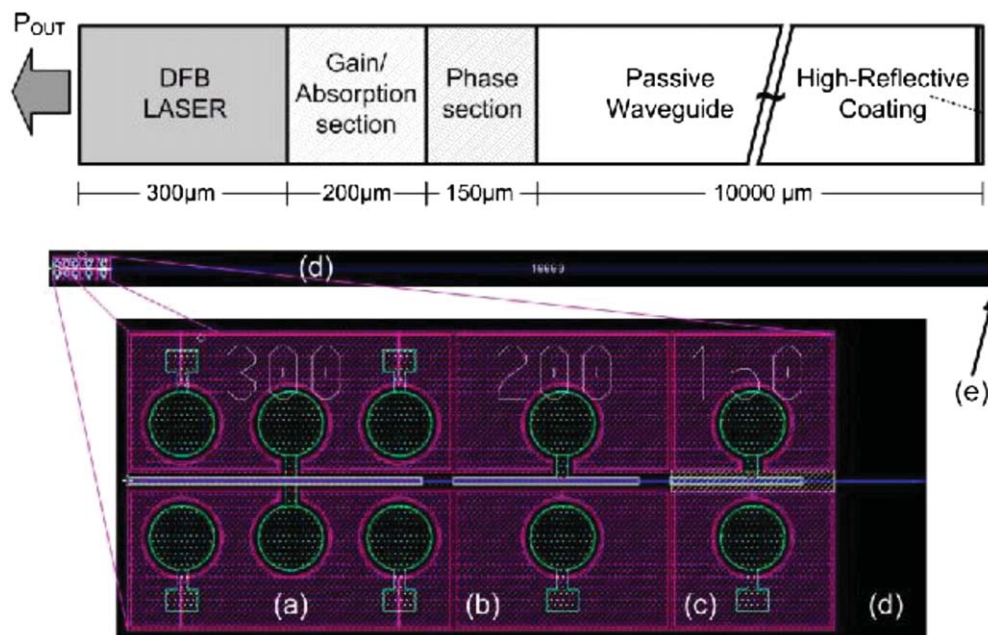
Fig. 37. PIC (Photonics Integrated Circuit) chip implementing the functions of a short cavity DOF. Top: the functional blocks, including a DFB 1.55-μm laser, gain and phase control sections, and a long (1-cm) passive waveguide running up to the reflective end-facet. Bottom: micrograph of the chip (Adapted from [35], courtesy of the American Physical Society).

In later work [36], Argyris et al. reported an interesting experiment of secure data communication, on a 100-km trunk of dispersion-compensated fiber, using their PIC [35] for the transmitter and receiver of a CM system (Fig. 38). The only extra component needed was a Mach–Zehnder modulator, placed at the transmitter output, to amplitude modulate the message (in OOK format) by taking advantage of the dc power pedestal of the chaos waveform available at the transmitter.

In another implementation of the DOF short-cavity generator (Fig. 39), also based on InGaAs waveguides fabricated in an InP substrate, Tronciu et al. [37] described a PIC chip incorporating a DFB laser, two 5-mm long waveguides and two phase modulators, that realizes the phase-coded scheme of transmission of Fig. 35. For a 1 Gb/s transmission rate of a binary NRZ sequence, they reported a wide open eye diagram and a BER better than 10^{-4} at the receiver decoded output, while the error was larger than 10^{-1} for the masked signal [37].

For a quite different structure (Fig. 40), a ring oscillator made by a passive waveguide fed by a DFB laser and boosted by two side SOA amplifiers, and with in-line photodiode for signal conversion to electrical output, Sunada et al. [38] have reported a good control of periodic and chaos regimes througout all the range of currents to the different sections. As the ring structure minimizes the losses, and the SOAs can provide gain, the structure is unique because it can work at very high K, approaching unity or even >1.
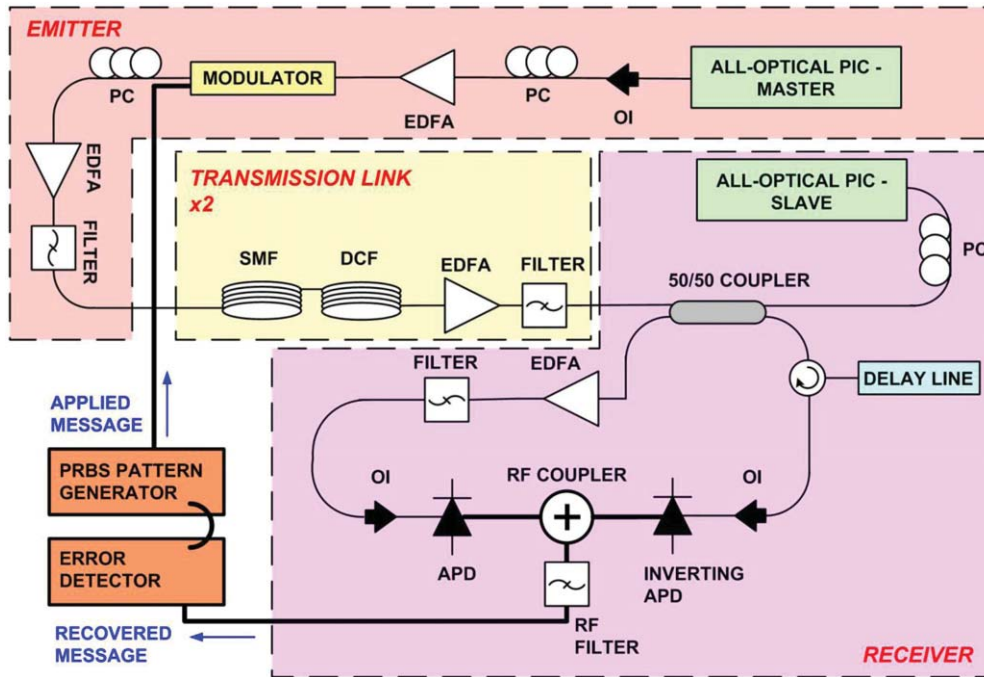
Fig. 38. Experiment of chaos secure transmission based on CM (Chaos Masking) cryptography using as transmitter and receiver the PIC chip of Fig. 37. Message is added by a Mach-Zehnder modulator at the transmitter output (From [36], courtesy of the Optical Society of America).
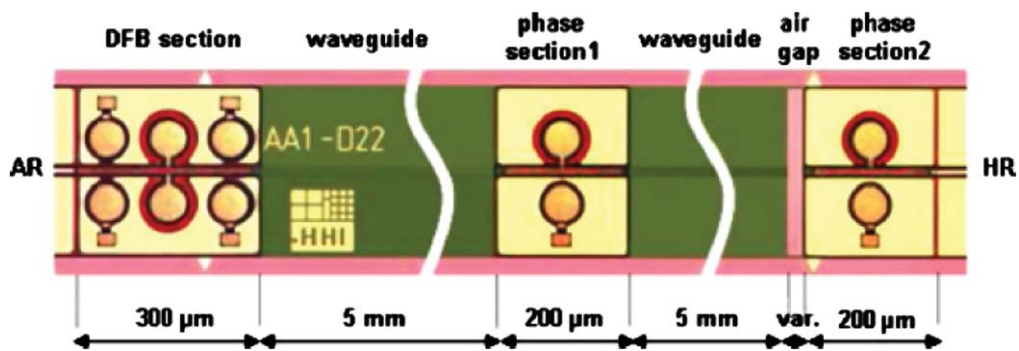
Fig. 39. Another implementation of a DOF short-cavity PIC chip, fabricated by InGaAs waveguides on a InP substrate, and incorporating a DFB laser, two 5-mm waveguides and two phase modulators, to realize the phase-coded scheme of transmission of Fig. 35. (From [37], courtesy of the IEEE).

4.4. Development aspects of chaos cryptography

System aspects are an important check in the development of a new technology like chaos cryptography, and in particular (i) compatibility to existing methods, (ii) retrofit of

Fig. 40. A ring structure chaos generator PIC (top), featuring a 3.5×3.5-mm chip in InP with a passive waveguide closing a ring path around a DFB laser and a pair of SOA. 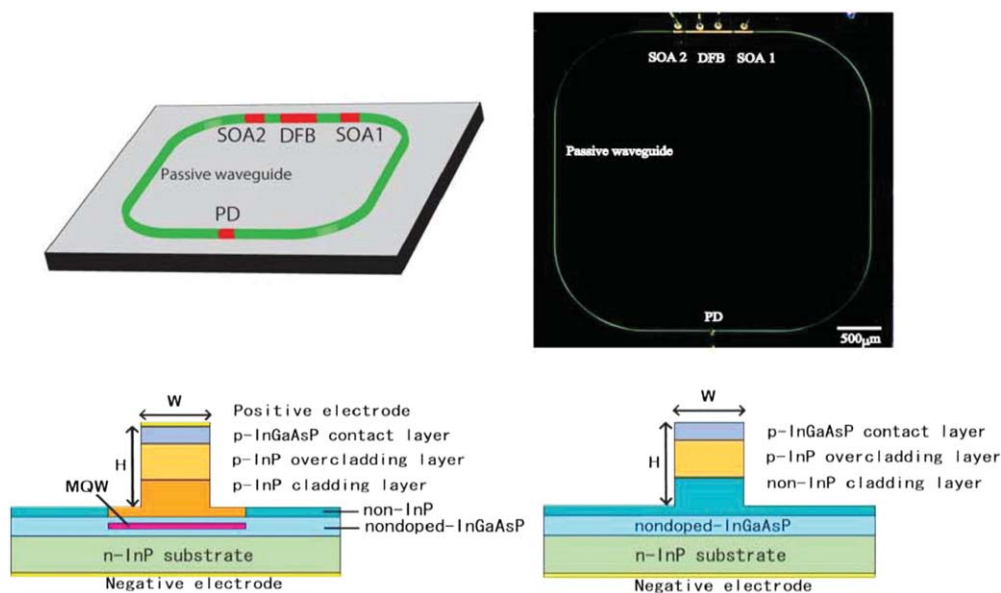Bottom: active (left) and passive (right) guide structure (Adapted from [38], courtesy of the Optical Society of America).

previous approaches, and (iii) flexibility of reconfiguration are key aspects that may be crucial for the success of the new idea.

In this view, several extensions as well as issues about interfacing with classical TLC (Telecommunication) methodologies have been studied and discussed recently for the chaos cryptography system.

First of all, several authors have tested optical chaos cryptography signals for robustness to attenuation in long fiber transmission and to added noise of optical amplifier line regeneration [11,12,33]. These studies found that the effects of dispersion and nonlinearity of the fiber do not impact the chaos-coded signals differently from a normal telecommunication data transmission.

Annovazzi et al. [39] have tested the robustness of the chaos cryptography message to wavelength conversion, an operation that optical streams undergo in modern network, all-optical dispatching. Based on four-wave mixing in an SOA, they demonstrated a transfer of message from one wavelength to another shifted by 2 nm with -10 dB conversion efficiency and little SNR penalty, as well as with a 20-nm potential conversion shift.

Ursini et al. [40] considered NRZ (Non-Return to Zero) and Manchester modulation formats for digital transmission with a CM system, and found that the shift from baseband to higher frequency with Manchester coding effectively improves the masking and recovery process, resulting in a final gain of several dB in the Q-factor (the generalised SNR) of the transmission link.

In a different context of optical communications, that of a Free Space Optical Link (FSOL), Annovazzi et al. [41] have successfully demonstrated the applicability of a CSK system, based on a slightly modified synchronization method. They use electrical injection in transmitter Tx and receiver Rx lasers, biasing them with the electrical signal generated

by a third (master-chaos) laser, photodetected to supply the bias drive. When Tx and Rx are well matched, the system can withstand a -30 dB propagation loss with no penalty, up to the high frequency cutoff of the multipath diffuse propagation.

Other concepts extending classical approaches such as CM and CSK, and proposing new variants have been developed. For example, Pisarkis and Ruiz-Oliveras [42] proposed a complete synchronization scheme that improves transmission quality and de-sensitizes CM to the influence of parameters, up to 5 GHz, close to the laser upper frequency response, while Buldu et al. [43] showed that two modes of a multimode laser driven to chaos can be de-multiplexed and used to synchronize two separate monomode lasers, hinting at channel multiplexing in chaotic transmission. Other papers have considered combining the actions of delayed optical feedback and chaos electrical drive of bias [44] to generate high-dimensionality chaos—or hyperchaos [45]. Also, many other contributions are available in the literature that we cannot mention because of space limitations.

In conclusion, beyond their intrinsic value, all these works basically attest to the fact that chaos cryptography stands on very solid roots, and that it can be easily re-adapted to exploit new concepts, most of which differ little from the point of view of necessary hardware, yet significantly deviate conceptually from the basic ideas.

4.5. Cryptography security and system issues

Establishing a secure communication against malicious adversaries has been a target since the times of Romans, and the *cypher* used by Julius Caesar to communicate with his generals is perhaps the first working example of cryptography. It was based on moving by two (or more) places forward in the alphabet each letter of a message, e.g. "oqtpkpi cvvaem" for "morning attack"—an easy and efficient cypher whose embryonic key is the number of moves of the cypher.

In the Middle Ages and the Renaissance, cyphers based on letter transposition and/or substitution were improved by contributions of scholars like Leon B. Alberti (Rome), inventor of the polialphabetic cypher disk, G. Cardano (Pavia), G.B. Della Porta (Naples) and Blaise de Vigenère (France), inventor of polyalphabetic table, a cypher considered unbreakable for two centuries, until in mid 1800, the Prussian lieutenant F. Kansiski published the method to force it.

Whatever the cryptography method, the rules for correct use were investigated in 1863 by Kerckhoffs, who found that the security of a cryptography does not reside in the *algorithm* (or cypher method) but in the *key* (or secret word to operate the algorithm), and obviously, in keeping the key secret.

Indeed, if the cypher method (e.g., transposition of letters) becomes known to a third party (or eavesdropper), the code will be easily broken by repeated attempts. Only if the key is sufficiently large (or complicated), attempts to break the encrypted message will require too much time.

Shannon [46] found in 1949 the conditions for a cryptography code to be theoretically unbreakable: the key must be a one-time pad (not re-used), its length shall be equal to or greater than the message, and the encrypted message shall be randomised. With the exception of a one-time pad, most cryptography codes can be broken by a brute force attack if enough computational time is available, but the effort needed may be increasing exponentially with the key size. So, a cryptography may be theoretically breakable but *computationall*y secure.

In the computer era, much more complex cyphers became possible, based on the binary format for representation and encryption of any kind of data. Cypher algorithms have been developed which demand limited resources (speed, memory and CPU capability) while the breaking attempt requires increasingly large computational time and resources, so as to be impractical and effectively impossible.

Algorithms derived from intractable mathematical problems, such as, prime number factorization, discrete logarithm and elliptic-curves, have increased substantially the difficulty of brute-force attacks.

Thus, in the last few decades, the applications of *computer-enabled* cryptography have entered everyday life with, e.g., ATM cards, computer passwords, e-commerce, digital signature, etc.

In the era of *photonics*, it is quite possible that the paradigm of cryptography makes a new turn, and takes advantage of the parallelism of information flux and of the much larger bandwidth potentially available in the optical region. The rich variety of wave-forms generated by high-level chaos dynamics, and also the unique features of entangled photons – exploited by quantum cryptography – are two additional strong points favouring applications of the new *photonic-enabled* technology.

Secrecy of the key used to operate the algorithm is an issue even more critical than code breaking. Each pair of communicators require a different key and, with an increasing number of communicators, there is a problem of key management to keep all the keys secret. The problem of distributing a secret key, when a secure channel is not already there, is a chicken-and-egg problem, a practical obstacle for cryptography in the real world.

So while traditional methods were based on *symmetrical* cryptography (one key to encrypt and another to decrypt, both to be secret), a groundbreaking step was the invention, by Diffie and Hellman [47], of the public-key or *asymmetrical* cryptography (one key public, one key secret).

In the public-key scheme, Bob sends to Alice a *public key* (openly available) to encrypt her message, and upon receiving it, uses a *secret key* to decrypt it. Both keys are generated secretly as an interrelated pair, though the private key is computationally infeasible from the public key.

Secret key cryptography is the core of today's widely known encryption technology, with products such as RSA encryption, PGP, Schnorr, etc. Their security properties have been generally tested using empirical methods and ad-hoc reasoning and, more recently, by techniques called *provable security*, that evaluates the computational difficulty needed to crack security aspect of the encryption [48].

As asymmetrical cryptography is rather slow in dispatching large amount of data, frequently it is used just to exchange first the crucial information—the symmetrical key—and then crypted communication continues using the faster and simpler symmetrical cryptography.

All the above considerations, belonging to classical "computer science" cryptography, should now be somehow confronted to our optical chaos-based approach—at least in the present status of DOF CM or CSK, or derived schemes.

First of all, ours is a symmetrical cryptography scheme. The keys are in part hardware, that is, a pair of matched semiconductor lasers, and in part software or numerical, that is, are the values of the working parameters. The algorithm (cypher method) is chaos synchronization—and as such, we shall assume it is known or easy-to-discover to the eavesdropper.

From the foregoing discussion, our cryptography is a breakable one, in the sense that malicious Eve can intercept a chaos-crypted message going from Bob to Alice, and try to synchronize herself with a fake laser diode emulating the true key laser of Alice.

One issue still open and deserving experimental analysis to be verified or falsified is whether a general-purpose, commercially available laser, can be used as Alice's laser in place of the true hardware key. Assuming conservatively that this can be done at some added complexity, we are then left with a cryptography whose robustness resides in the numerical key.

A relatively simple and effective index of robustness is the number of possible cases facing Alice who is trying to decript the message by chance.

Considering a typical chaos cryptography system, such as a short-cavity P-CSK (phase-coded CSK, as in Section 4.3) implemented by Tx/Rx chips of the same wafer, we may estimate the following number of different choices for each parameter affecting the generated chaos:

- K value (adjusted to $\approx 10\%$ steps)　　　　　　　　10 cases
- cavity length s (gross adjustment to $\approx 20\%$ steps)　5 cases
- cavity length $2ks$ excess to nλ (adjust to $\lambda/50$)　50 cases
- drive current J (1mA steps in 15–35 mA)　　　　20 cases
- α-factor (step of 1 in a 2–6 range)　　　　　　　　4 cases
- wavelength range (or chip temperature)　　　　　10 cases
- time delay synchronism (adjusted to 5%)　　　　　20 cases

The total of these cases rises to $N = 4 \times 10^7$. Being a rule-of-thumb evaluation, the estimate has a wide uncertainty, yet it indicates that chaos cryptography may not offer the desirable large N.

In contrast to chaos, quantum cryptography based on entangled states has virtually infinite N, or–the method is *computationally secure*.

Chaos cryptography is not computationally secure but has the advantages of exploiting all the available bandwidth of the laser (GHz) and has no constraint on the quantum efficiency of the detectors and the attenuation of the fiber, whereas quantum cryptography requires one-photon-at-a-time transmission (reducing bandwidth) and close to unity detector efficiency and limited medium loss.

The limit of N can be overcome by reinforcing the system with *over-encryption*, which consists in superposing different methods simultaneously. In fact, the eavesdropper is defeated if just one of the algorithms used to encrypt is missed out, even if a low-N one.

In conclusion, chaos-based cryptography is a new promising approach, yet further research is necessary to exploit its full potentiality. New configurations should be developed to increase factor N, and an effort is advisable to be able to translate into optical chaos systems the concept of *asymmetrical* or public-key cryptography.

5. Applications of chaos to high frequency and instrumentation

5.1. Interferometer measurements

Self-mixing interferometry (SMI) is a measurement method based on the DOF scheme at weak levels of interaction, in contrast to the high level considered in Section 3 which gives rise to chaos-based applications.

In a recently published review [1], the reader can find the details of operation of SMI as well as the discussion of SMI applications to distance-related measurements and other physical parameters.

In this section, we wish to only add that, also at the high-level of self-coupling, an interferometric measurement can be carried out by the SMI scheme.

Indeed, as the chaos waveform of a short-cavity DOF scheme is sensitive to the optical pathlength of the external reflector (cf. Section 3.1), then by inspection of the chaos waveform $c(t)$, we can have a signal proportional to $\cos 2ks$ (where $k = 2\pi/\lambda$ is the wavevector), like that supplied by a normal interferometer.

Measuring the amplitude of the chaos waveform $c(t)$ at the relatively high frequency (around the f_2 of the laser) is unwieldy. Instead, we can take advantage of the lucky circumstance that the time-average $\langle c(t) \rangle$ of the chaos waveform is not zero (as positive and negative semiperiods do not cancel out) but is proportional to the peak-to-peak amplitude, that is $\langle c(t) \rangle \approx \cos 2ks$, the desired signal, now at low-frequency.

In Fig. 41, we report the waveforms for an SMI measurement [49] performed at increasing levels of coupling: from weak ($C = 0.01$ corresponding to $K = 3 \times 10^{-5}$) to moderate ($C = 2$) to strong ($C = 60$, $K = 0.18$) coupling. In the last case, the laser is driven deep in the chaos regime. In Fig. 41 (bottom trace), the chaos waveform at $\approx f_2$ is unnoticed because it is beyond the high-frequency cutoff of the SMI circuit and yet the SMI signal is present because of the non-vanishing average.

However, as can be seen in Fig. 41, the SNR of the SMI signal is not as good as weak or moderate coupling, and thus preference is to the low C range for best operation.

5.2. Telemetry

When driven in the chaos regime, a laser can be employed as the optical source to make a correlation-based rangefinder (that is, a distance-measuring instrument), as first demonstrated by an experiment of Myneni et al. [50].

They used a commercial 850-nm laser diode, and coupled back in the cavity a few percent of the output field by means of a mirror placed at $s = 22$ cm, and tilted in angle to adjust the K and obtain a wideband choatic source. The optical spectrum of the DOF laser was broadened up to about $\Delta\nu \approx 50$ GHz from the ≈ 10 MHz unperturbed value.

Correspondingly, the autocorrelation of the optical field became a spike-like distribution with a duration of ≈ 50 ps (or 15-mm in equivalent length). The principle of measurement, then, is as follows: we make a correlation of a delayed replica $S(t-T)$ of the transmitted $S(t)$ waveform and the received $S(t-2L/c)$ returning from the remote target at distance L. Using an adjustable delay line to match the $S(t-2L/c)$ and $S(t-T)$ waveforms so that their correlation is maximized, we obtain $T = 2L/c$ from the experiment and determine L. With a 3-GHz bandpass of the electronic circuitry, resolution of the measurement was a few millimiters (corresponding to a few ps of correlation maximum localization).

In another contribution, Lin and Liu [51] discussed the use of a chaos-driven ICL source in combination with a correlation measurement on the signal, converted to electrical for Tx/Rx by microwave antennas. They considered a proof-of-concept scheme using an ICL system that generates wideband chaos. By photodetection, the optical spectrum is converted into an electrical multi-GHz quasi-white noise signal. The signal is transmitted and received back by antennas, so as to sense the external target by correlating the received waveform to the transmitted one. Simulations were backed by an experiment with
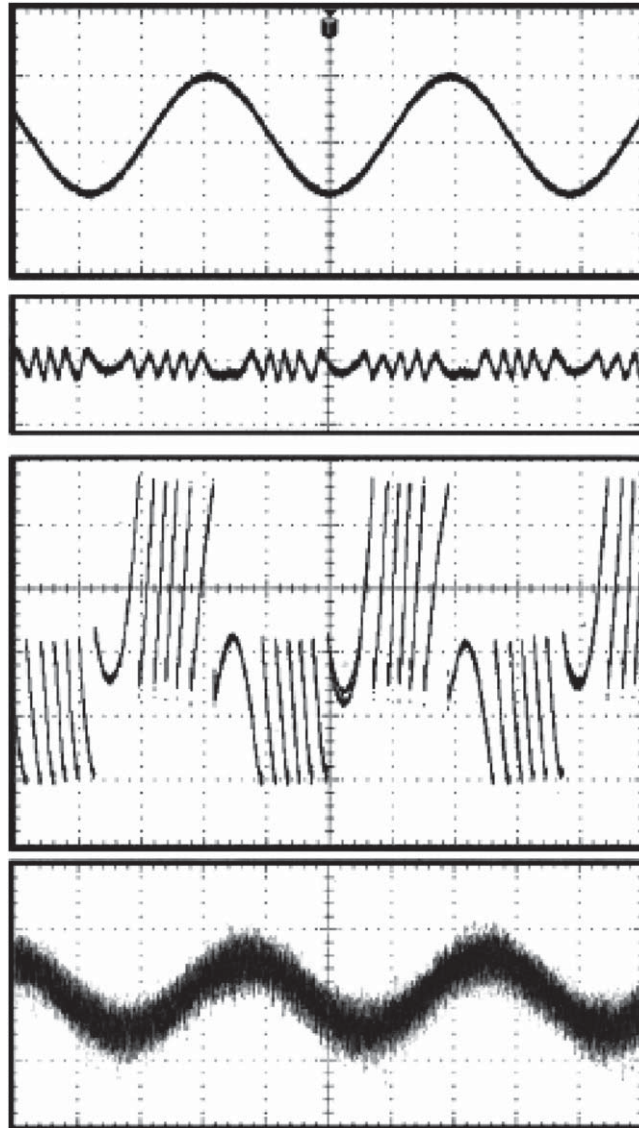
Fig. 41. Waveforms obtained with a DOF scheme used as an SMI. Top to bottom: the drive signal of distance s(t) to the remote reflector; the SMI signals for weak return ($C=0.01$), moderate return ($C=2$) and strong return ($C=60$). (From [50], courtesy of the SPIE, Bellington).

a 1300-nm laser, providing a flat-spectrum microwave signal in the range from 1.5 to 3 GHz, from which the measured resolution was 9 cm.

In a later paper [52], Lin and Liu used directly the optical output of the ICL to sense the remote target and made the correlation measurement. The reported resolution was 3 cm with sub-cm accuracy.

5.3. Random number generation

Driven into the chaos regime, an ICL or DOF system supplies a waveforms that are much similar to random noise. Though generated by a deterministic process, chaos waveforms may have (see, for example, Fig. 26) a power spectrum nearly flat from zero frequency to an upper frequency f_2, of the order of magnitude of the cutoff frequency of modulation (or even larger because of feedback). Thus, the spectrum is similar to that of white noise. In addition, f_2 may be in the range of several to a few tens of GHz, so chaos generation is competitive with other technques for high-frequency random number generation.

Sunada et al. have reported [38] on a ring-cavity DOF chaos generator chip, a PIC integrated in InP technology, that, when subjected to several randomness tests (NIST, Diehard, K–S), showed excellent compliance to the tight specifications of the standards. The autocorrelation of the generated waveform damps to zero in less than 100 ps, and the power spectrum is nearly flat (± 5 dB) from 0 to 10 GHz.

Moreover, with digital processing after sampling the analogue waveform, random bit streams with bit-rates as high as 140 Gb/s have been demonstrated with the PIC chip.

A similar result has been reported also by Argyris et al. [53], using a DFB laser integrated on a PIC chip with a 1-cm reflector DOF, generating a random bit sequence up to 140 Gb/s.

5.4. Microwave generation

When the ICL system is driven into the self-pulsation region through strong coupling (at $K \approx 0.2$–0.4 in Fig. 11), the output intensity of the slave laser undergoes high-speed single-period oscillation, also known as *period-one* (P1) oscillation.

The frequency of P1 oscillation can be continuously tuned from a few to hundreds of GHz by simply adjusting the level and frequency of the optical injection [54].

Broadly tunable microwave generation with constant microwave power has been demonstrated by Chan et al. [55] through such an all-optical scheme, which circumvents restrictions imposed by microwave electronics and electrical parasitics.

Further, an optoelectronic feedback approach has been proposed [56] to reduce the linewdith of the generated microwave, from tens of MHz down to tens of kHz, thus eliminating the need of an external reference microwave source for such a purpose.

Since the P1 oscillation frequency depends strongly on the level of the optical injection, amplitude modulation of the optical injection leads to frequency modulation of the generated microwave, thus carrying out signal conversion from optical AM to microwave FM [57].

P1 oscillations originate from the beating between light injected by the master laser and light emitted around the shifted cavity-resonance of the slave laser [58]. The optical spectrum, consisting of discrete lines equally separated by the P1 oscillation frequency, is thus dominated by these two frequencies. Such a feature of optical single-sideband modulation is advantageous for radio-over-fiber applications, in order to mitigate microwave fading due to fiber chromatic dispersion [55].

By taking advantage of the discrete spectral lines under P1 oscillation, Hwang et al. have proposed [59] using ICL as an all-optical frequency converter. Simultaneous frequency down-, no-, and up-conversion are feasible, and modulation format transparency is achieved, which

was only possible previously through four-wave mixing, without the need of any pump or probe as in other converters. Since the intensity and the frequency of spectral lines depend strongly on the injection frequency and amplitude, frequency modulation of the optical injection leads to amplitude modulation of spectral lines, and vice versa, a hint to modulation format conversion between optical AM and optical FM.

6. Conclusions

In this paper, we have presented an overview of chaos and chaos-related basic phenomena and their applications. We have tried to systematize the field of chaos and high-level dynamics, discussing several versions of coupling phenomena in laser diodes, such as injection coupled and delayed optical feedback, which represent different classes of systems and lead to different performance.

The examples reported in this paper inevitably reflect the scientific interest of the authors, and yet they, hopefully, are representative of the basic ideas and tools we can deploy in research and applications.

In particular, rather than citing a long list of contributions, we have tried to show the guiding principles underpinning the applications, and underline how methods and options from different disciplines (electronics, communications, control theory, etc.) can cross fertilize the chaos-related concept, the principle that really makes chaos cryptography an effective and sophisticated approach.

Chaos dynamics is still far from being fully exploited, and we think that, in the years to come, it will continue to offer an excellent opportunity for young researchers and a field in which to make the most of his/her creativity and talent.

Appendix A1. Derivation of Adler's equation

Injection of a signal into an electronic oscillator can be modeled by the scheme shown in Fig. A1, that is, with an amplifier with gain G (that includes saturation), a frequency selective element (an LCR group in the original Adler's derivation), and a feedback loop. Of course, gain and selective functions can also be distributed rather than lumped. Let E_0 be the amplitude of the free running oscillator and E_s the injected signal. Inside the loop, a characteristic time τ describes the relaxation (or decay) of E_0 (usually τ is the larger between propagation time of the feedback loop and inverse of high frequency cutoff gain). We represent the signals by rotating vectors, as:

$$E_0 = E_0 \exp\ i\Phi \ \ \text{and} \ \ E_s = E_s \exp i\Phi_S,$$

and write the injected phase as: $\Phi_s = 2\pi\Delta vt + \phi_s$, where Δv is the detuning from unperturbed frequency, and ϕ_s the phase shift collected at the coupling (or injection) node C (cf. Ref. [8], p. 261 for details). At the coupling node the following equation holds:

$$dE_0/dt = (1/\tau)E_s \tag{A1}$$

By developing the time differentiation, we get:

$$[dE_0/dt + E_0 i\ d\Phi/dt]\exp\ i\Phi = (1/\tau)E_s \exp\ i\Phi_s, \tag{A1a}$$

This equation can be satisfied by equating real and imaginary parts separately, obtaining:

$$dE_0/dt = (E_s/t)\cos(\Phi_s - \Phi) \tag{A2a}$$

$$d\Phi/dt = (E_s/\tau E_0)\sin(\Phi_s - \Phi) \tag{A2b}$$

Now, what we actually observe in the experiment is the phase difference of the oscillator with respect to the injected frequency, $\phi = \Phi - 2\pi\Delta vt$. Introducing this quantity in Eq. (A2b), so that $d\Phi/dt = d\phi/dt + 2\pi\Delta v$ and $\Phi_s - \Phi = \phi_s - \phi$ we can rewrite it as:

$$d\phi/dt = -2\pi\Delta v - (E_s/\tau E_0)\sin(\phi - \phi_s) \tag{A3a}$$

Finally, we insert $K = E_s/E_0$ for the coupling factor and obtain:

$$d\phi/dt = -2\pi\Delta v - (K/\tau)\sin(\phi - \phi_s) \tag{A3b}$$

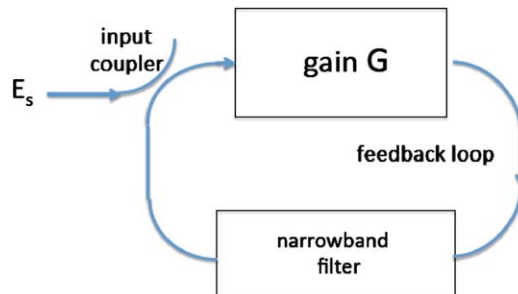which is coincident with Eq. (1) of the text with $A = -2\pi\Delta v$ and $B = -K/\tau$.

Fig. A1. Model of a generic oscillator used to derive Adler's equation.

Note that also Eq. (A2b) is another formulation of Adler equation. By expressing the total phase as $\Phi = 2\pi\phi t + \phi$, we put it in the form:

$$d\phi/dt = -2\pi f_0 + (K/\tau)\sin(\phi_s + 2\pi\Delta vt - \phi) \tag{A4a}$$

or, we have the unperturbed frequency f_0 and, impressed on it, a frequency modulation carried by the last term containing Δv—the injection modulation.

In the original Adler formulation, Eq. (A3a) was deduced for the voltage V in an LCR-tuned electronic oscillator, and τ was the damping time constant, $\tau = Q/2\omega_0$, $Q = \omega_0 L/R$ being the quality factor of the resonator and $\omega_0 = (LC)^{-1/2}$ the resonant frequency.

A few comments are in order about this derivation.

– first, Eq. (A2b) is basically the same as the second line of Eq. (2), the one describing $d\phi/dt$, in both Lamb [3] and Lang and Kobayashi [5] derivations for a laser oscillator in the injection regime. Also, Eq. (A2a) is similar to the amplitude equation, the one describing dE/dt, in both Lamb and L–K equations.

As such, Adler's equation not only explains frequency locking reached at coupling $A = B$ (or $\Delta v = K/\tau$) also frequency attraction and AM/FM injection modulations described in the text. These features are common to *every* kind of oscillator working in the injection regime.

– second, the stationary gain condition tacitly assumed in our derivation can be easily removed by considering a second-order differential equation for the oscillator of the type

$$E'' + (\Gamma - p)E'' + (2\pi f_0)^2 E = 0 \tag{A5}$$

where Γ and $p = 1/\tau_p$ are the gain and loss rates of the oscillator loop, respectively. The gain can further be assumed of the form $\Gamma = G_0(1 - E/E_{00})^2$ to describe saturation taking place (with quadratic dependence) at value E_{00}. Repeating the calculation for $E = E_0 \exp i\Phi$, and ignoring terms higher than the first order, it is easy to obtain

$$dE_0/dt = [G_0(1 - E/E_{00})^2 - p]E_0 + (E_s/\tau E_0)\cos \Delta vt + \phi_s \tag{A5a}$$

a form coincident with the complete Lamb or L–K for amplitude rate equation.

Comment about Adler's equation and chaos

When Adler's equations, in the form of Eqs. (A3) and (A5a), are tested by extensive numerical simulations, we find that they always contain frequency locking and injection modulations for any combination of the parameters, but *do not* go to any chaos nor to other high-level regime.

Now, as Lamb's equations are basically the same structure of Eqs. (A3) and (A4a), we obtain as a consequence that Class A lasers (for example, the He–Ne) *do not* go to chaos, neither in normal nor in injected regimes. Nor any enhancement of gain nonlinearity by saturation [term $(E/E_{00})^2$] will help to drive systems to chaos.

To attain chaotic regime, we have to add more complexity into Adler's or Lamb's equations. One way already there is the third equation of the L–K set (Eq.(2)), in which product NE^2 is the main source of increased nonlinearity. This will drive the injected system to chaos at a large enough K value.

In conclusion, class B lasers (like the semiconductor diode) can go into high-level and chaos regimes when in a DOF or ICL scheme, because of the 3-equation L–K set.

Opposite to this, in a Class A laser, the equation about pumping levels like the last of the L–K set (Eq. (2)) should certainly apply, but in it we have normally $J\eta/ed \approx N/\tau_r$, so that the nonlinear term $G_N(N-N_0)\,E^2$ is negligible, and the equation is decoupled from the first two for E and ϕ.

References

[1] S. Donati, Laser and Photonics Review 6 (2012) 393–417, http://dx.doi.org/10.1002/lpor.201100002.
[2] M.B. Spencer, W.E. Lamb, Physical Review A 5 (1972) 884–891.
[3] M.B. Spencer, W.E. Lamb, Physical Review A 5 (1972) 891–897.
[4] F.T. Arecchi, G.L. Puccioni, J.R. Tredicce, Optics Communications 51 (1984) 308–314.
[5] R. Lang, K. Kobayashi, IEEE Journal of Quantum Electronics 16 (1980) 347–355.
[6] S. Donati, Electro-Optical Instrumentation, Prentice Hall, Upper Saddle River, N.J., 2004 see Sect. 4.5.2.
[7] S. Donati, IEEE Journal Quantum Electronics 47 (2011) 1428–1433.
[8] S. Donati, Photodetectors, Prentice Hall, Upper Saddle River, N.J., 2000, see Sect.8.4.
[9] S.A. Kauffman, At Home in the Universe: The Search for Laws of Self-Organization and Complexity, Oxford University Press, New York, 1995.
[10] H. Tsoukas, Organization 5 (1998) 291–313.
[11] K. Ohtsubo, Semiconductor Lasers: Stability, Instability and Chaos 2nd edition, Springer Series Optical Sciences, 111, Springer-Verlag, New York, 2009.
[12] D.M.K. Kane, K.A. Shore, Unlocking Dynamic Diversity-Optical Feedback effects on Semiconductor Lasers, Wiley & Sons ltd, London, 2008.
[13] C.J. Buczek, R.J. Freiberg, M.L. Skolnick, Proceedings IEEE 61 (1973) 1411–1431.
[14] R. Adler, IRE Proceedings of Waves and Electrons 34 (1946) 351–357.
[15] V. Annovazzi Lodi, S. Donati, IEEE Journal of Quantum Electronics 16 (1980) 859–865.
[16] R. Lang, K. Kobayashi, IEEE Journal of Quantum Electronics 16 (1980) 347–355.
[17] V. Annovazzi Lodi, S. Donati, M. Manna, IEEE Journal of Quantum Electronics 30 (1994) 1537–1541.
[18] C.H. Henry, IEEE Journal Lightwave Technology 4 (1986) 288–1297; see also IEEE Journal of Quantum Electronics QE-23 (1986) 9–27.
[19] Y. Yu, G. Giuliani, S. Donati, IEEE Photonics Technology Letters 14 (2004) 900–902.
[20] V. Annovazzi Lodi, A. Scirè, M. Sorel, S. Donati, IEEE Journal of Quantum Electronics 34 (1998) 2350–2356.
[21] J. Troger, P.A. Nicati, L. Thevenaz, P.A. Robert, IEEE Journal of Quantum Electronics 35 (1999) 32–38.
[22] S. Donati, C. Mirasso, Feature Issue of IEEE Journal of Quantum Electronics 38 (2002), 1138–1184.
[23] V. Annovazzi Lodi, S. Donati, A. Sciré, IEEE Journal of Quantum Electronics 32 (1996) 953–959; see also S. Donati, V. Annovazzi Lodi: Crittografia Ottica Caotica, Proceedings Conference Fotonica'95, Sorrento, May 1–4, 1995, pp. 463–466.
[24] C.R. Mirasso, P. Colet, P. Garcia-Fernandez, IEEE Photonics Technology Letters 8 (1996) 299–301.
[25] V. Annovazzi Lodi, S. Donati, A. Scirè, IEEE Journal of Quantum Electronics 33 (1997) 1449–1454.
[26] R.W. Tkach, A.R. Chraplyvy, IEEE Journal of Lightwave Technology 4 (1986) 1655–1661.
[27] K. Petermann, Laser Diode Modulation and Noise, Kluwer Academic Publication, Dodrecht, 1991.
[28] R.J. Jones, P.S. Spencer, J. Lawrence, D.M. Kane, IEE Proceedings part J, Optoelectronics 148 (2001) 7–12.
[29] V. Annovazzi Lodi, S. Merlo, M. Norgia, A. Scire, IEEE Journal of Quantum Electronics 38 (2002) 1171–1177.
[30] R. Ju, P.S. Spencer, IEEE Journal of Lightwave Technology 23 (2005) 2513–2523.
[31] EEC Program OCCULT and PICASSO, see URL: ⟨http://cordis.europa.eu/fetch?CALLER=PROJ_ICT&ACTION=D&CAT=PROJ&RCN=xxxxx⟩, specialize with xxxxx=57468, 80185, and 24846.
[32] V. Annovazzi Lodi, M. Benedetti, S. Merlo, M. Norgia, B. Provinzano, IEEE Photonic Technology Letters 17 (2005) 1995–1997.
[33] A. Argyris, D. Syvridis, L. Larger, V. Annovazzi, P. Colet, I. Fischer, J. Garcia-Ojalvo, C. Mirasso, L. Pasquera, K.A. Shore, Nature Letters (2005) 343–346.
[34] V. Annovazzi-Lodi, M. Benedetti, S. Merlo, T. Perez, P. Colet, C. Mirasso, IEEE Photonic Technology Letters 19 (2007) 76–78.
[35] A. Argyris, M. Hamacher, K.E. Chlouverakis, A. Bogris, D. Syvridis, Physical Review Letters 100 (2008) DOI 194101.

[36] A. Argyris, E. Grivas, M. Hamacher, A. Bogris, D. Syvridis, Optics Express 18 (2010) 5188–5196.

[37] V.Z. Tronciu, C. Mirasso, P. Colet, M. Hamacher, M. Benedetti, V. Vercesi, V. Annovazzi Lodi, IEEE Journal of Quantum Electronics 46 (2010) 1840–1846.

[38] S. Sunada, T. Harayama, K. Arai, K. Yoshimura, P. Davis, K. Tsuzuki, A. Uchida, Optics Express 19 (2011) 5713–5724.

[39] V. Annovazzi-Lodi, G. Aromataris, M. Benedetti, I. Cristiani, S. Merlo, P. Minzioni, IEEE Photonic Technology Letters 19 (2007) 1783–1785.

[40] L. Ursini, M. Santagiustina, V. Annovazzi Lodi, IEEE Photonics Technology Letters 20 (2008) 401–403.

[41] V. Annovazzi Lodi, G. Aromataris, M. Benedetti, S. Merlo, IEEE Journal of Quantum Electronics 44 (2008) 1089–1095.

[42] A.N. Pisarkis, F.R. Ruiz-Oliveras, IEEE Journal of Quantum Electronics 46 (2010) 279–284.

[43] J.M. Buldu, J. Garcia-Ojalvo, M.C. Torrent, IEEE Journal of Quantum Electronics 41 (2005) 164–170.

[44] J. Hizanidis, S. Deligiannidis, A. Bogris, D. Syvridis, IEEE Journal of Quantum Electronics 46 (2010) 1642–1648.

[45] O.E. Rössler, Physics Letters A 71 (1979) 155–157.

[46] C. Shannon, W. Weaver, The Mathematical Theory of Communication, University of Illinois Press, ISBN 0-252-72548-4, 1963.

[47] W. Diffie, M. Hellman, Proceedings of the AFIPS 45 (1976) 109–112.

[48] B. Schneier, Applied Cryptography, 2nd ed., John Wiley & Sons, Chichester, ISBN 0-471-11709-9, 1996.

[49] G. Giuliani, S. Donati, M. Passerini, T. Bosch, Optical Engineering 40 (2001) 95–99.

[50] K. Myneni, T.A. Bar, B.R. Reed, S.D. Petel, N.J. Corron, Applied Physics Letters 78 (2001) 1496–1499.

[51] F.Y. Lin, J.M. Liu, IEEE Journal of Quantum Electronics 40 (2004) 815–820.

[52] F.Y. Lin, J.M. Liu, IEEE Journal of Selected Topics in Quantum Electronics 10 (2004) 991–997.

[53] A. Argyris, S. Deligiannidis, E. Pikasis, A. Bogris, D. Syvridis, Optics Express 18 (2010) 18763–18768.

[54] S.K. Hwang, J.M. Liu, J.K. White, IEEE Journal of Selected Topics in Quantum Electronics 10 (2004) 974–981.

[55] S.C. Chan, S.K. Hwang, J.M. Liu, Optics Express 15 (2007) 14921–14935.

[56] S.C. Chan, J.M. Liu, IEEE Journal of Selected Topics in Quantum Electronics 10 (2004) 1025–1032.

[57] S.C. Chan, S.K. Hwang, J.M. Liu, Optics Letters 31 (2006) 2254–2256.

[58] S.C. Chan, IEEE Journal of Quantum Electronics 46 (2010) 421–428.

[59] S.K. Hwang, H.F. Chen, C.Y. Lin, Optics Letters 34 (2009) 812–814.