Chapter 6
Recent Advances in Secure Transmission with Chaotic Carriers

Silvano Donati and Valerio Annovazzi-Lodi

Abstract After an outline of optical chaos generation and synchronization in semiconductor lasers, we discuss the fundamentals of optical secure transmission of data using chaotic carriers, based on different schemes, such as CM (Chaos masking) and CSK (Chaos Shift Keying). We present different versions of such schemes, which have been numerically evaluated and/or experimentally tested with discrete components or with a PIC (Photonic Integrated Circuit) realization of the crypto-systems. Finally, we outline some recent developments of the chaos secure transmission technique.

6.1 Introduction

Chaos is a quite interdisciplinary subject of research, with founding contributions coming from mathematics and physics [1], and with applications being developed almost everywhere in applied science. Indeed, chaos is the novel phenomenon we first encounter when the level of system complexity [2, 3]—the number of individual entities or number of differential equations and of nonlinearities in the system—departs markedly from the ground level of the Lagrangian system of the nineteenth century. Because of the added complexity, classical reductionism fails, and the pseudo-random—or chaos—evolution of the system unveils new conceptual phenomena unpredictable with the lower level description, as well as it opens a new ground of applications for development.

In optics, Haken [4, 5] has been the first to point out that the Maxwell-Block equations describing the laser [5, 6] can be brought to coincide with the Lorenz equations describing convective flow in the atmosphere, a well known paradigm for chaos. Since then, the rate equations in three variables for the laser are known as

S. Donati (✉) · V. Annovazzi-Lodi
Department of Electrical, Computer and Biomedical Engineering,
University of Pavia, Pavia, Italy
e-mail: silvano.donati@unipv.it

V. Annovazzi-Lodi
e-mail: valerio.annovazzi@unipv.it

O. Shulika, I. Sukhoivanov (eds.), *Advanced Lasers,*
Springer Series in Optical Sciences 193, DOI 10.1007/978-94-017-9481-7_6

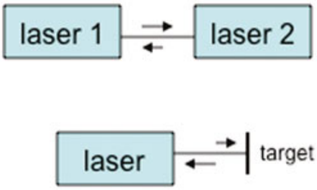


Fig. 6.1 Coupled-lasers: *top*, mutual (can be symmetrical or asymmetrical) *bottom*, self-coupling

Lorenz-Haken (L-H) equations, and they were soon shown by Arecchi [6] to be the base to identify classes of stable and unstable lasers.

Actually, semiconductor lasers belong to class B [6], and are stable unless a new term is added into the L-H equations, such as external injection from another laser or the feedback from a remote mirror. With this term, the L-H set become the well known Lang and Kobayashi equations [7] (or, Lamb's equations when excitation is decoupled from electric field) and system may experience chaos when driven heavily enough into feedback—a favourable condition because it allows easy control of the desired working regime.

6.2 Chaos in Lasers

The basic scheme to study the high-complexity dynamical regimes is that of Fig. 6.1, where we can have either a double-source arrangement (either in the mutual, symmetrical or asymmetrical, or in the unidirectional case) or a single-source subject to back-reflection from an external target (the so called delayed feedback or self-mixing case).

Self-mixing has two distinct applications at two different levels of injection:

1. at weak injection (when the return is barely 10^{-8} to $10^{-3}$of emitted power) perturbations of the laser field are frequency and amplitude (AM and FM) modulations of the cavity field, depending on external amplitude and phase of the return, and the system can be used in instrumentation for measurements of the external path-length (the self-mixing interferometer [8]) or as an optical radar detecting weak echoes [9, 10], also known as a coherent injection detector [9];
2. at moderate/large coupling (10^{-3} to a few10^{-2}) the system enters a more complex dynamical regime and starts generating periodic and multiperiodic oscillations and chaos, opening new avenues in communications and information technology.

An exhaustive literature is available on optical chaos and its applications, and recently ample reviews have appeared on the physics principles [11] and on the application repertoire [12] of chaos and related phenomena, to which we direct the interested reader.

About the analytical approach to study the new chaos phenomena, the Lang-Kobayashi equations [7], provide a powerful tool [12, 13, 14, 15, 16, 17], well confirmed by experimental evidence, also considering the effect of noise [18]. Using these equations to study the double-source unidirectional coupling case (Fig. 6.1,

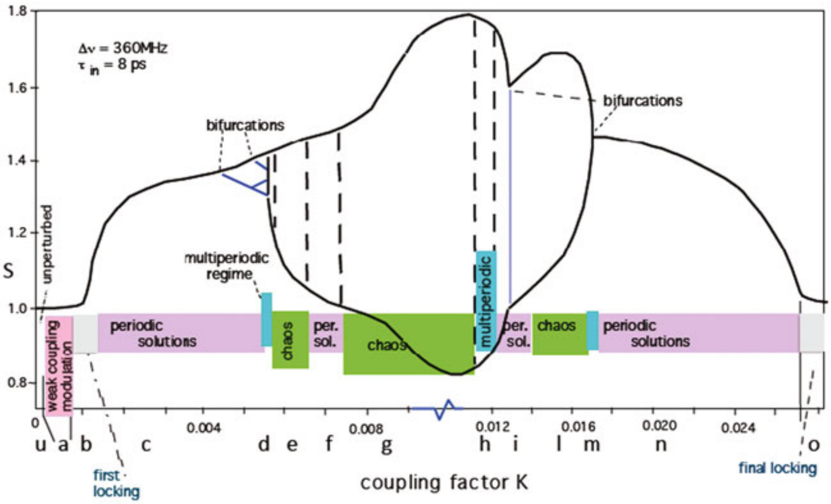


Fig. 6.2 Beating amplitude of master and slave oscillations of the coupled system, vs. the strength of coupling K, starting from the unperturbed regime (region *u*) and unveiling regimes of periodic solutions (regions *c,f,i,n*), multiperiodicity (*d,h,m*) and chaos (*e,g,l*), passing through first locking (*b*) to final locking (region *o*). (From Ref.[12])

top), the route to high dynamics behaviour and chaos is readily unveiled, as depicted in Fig. 6.2.

The parameter used to depict the system evolution is the beating amplitude $S = E_1 E_2^*$ of oscillations in laser 1 and 2 (master and slave arrangement), vs. the coupling strength K (fraction of field injected from laser 1 into laser 2) [18]. The regimes are identified based on three indicators: (i) the time series [or amplitude S(t)], (ii) the frequency spectrum S(f), and the state diagram, S vs dS/dt [5, 11].

In unperturbed conditions, the time series is a sinusoid, the spectrum is a single peak and the state diagram is a circle. Then, we encounter a locking state, and signal S disappears. But, at increased K, S reappears and now the time series has a distortion every other period, the spectrum carries sub-harmonics and the state diagram is a double loop figure, all indicative of the so-called period-1 oscillation regime. At even larger K, the sub-harmonics increase in number and amplitude, and the state diagram has multiple loops: it is the multiperiodic regime. Last, when harmonics accompany the sub-harmonics and broaden the spectrum widely, the time series is random-like looking, and the state diagram spread all over the available space of coordinates, we have chaos [12, 19]. As K is further increased, the system enters less complex regimes, including again periodic and multiperiodic solutions, and, after passing new chaotic regions, eventually reaches a new stable (locked) regime (Fig. 6.2, right end).

An example of the three diagrams for multiperiodic solutions and chaos is reported in Fig. 6.3.

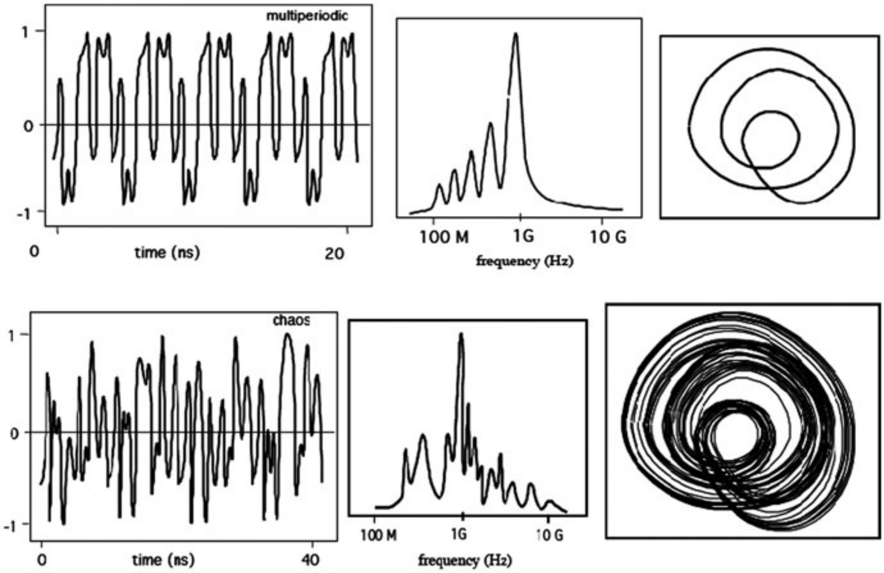


Fig. 6.3 Time series (*left*), frequency spectrum (*center*) and state diagram (*right*) of the beating signal S for the multiperiodic regime (regions *d,h,m* in Fig. 6.2) and *chaos* (*e,g,l*). (From Ref.[12])

6.3 Synchronizing Chaos

The waveforms generated by a chaotic laser can be thought as a sort of free-response or eigenfunctions of the complex system, similar to sinusoidal oscillations being the free response of a second-order system or oscillator. On this analogy, we may think of injecting from outside a chaos waveform into the system, in the conjecture that the system synchronizes, i.e, that it will adjust itself to follow the dynamical evolution of the injected signal. And, since to lock a linear second-order oscillator we need a frequency close to the free oscillation frequency, thus we expect that we need to stay close to the system free response to be able to synchronize the chaos generator.

The synchronization scheme of Fig. 6.4, with two identical coupled-lasers systems, system 1 with LD1 and LD2, and system 2 with LD3 and LD4 is considered in [20]. The output of system 1 (out 1) is connected to the sum node in system 2, at the input of LD4; in addition, the LD4 output is sent to the subtraction node in system 2. By this arrangement, when the LD2 and LD4 outputs differ, system 1 applies a correction to system 2 and brings it closer, until system 2 tracks the other, i.e., it is synchronized.

By using a modified L-K equation set [15] to model the synchronization scheme (Fig. 6.4), we find that output of system 2 reaches the steady-state solution irrespective of the arbitrary starting point, with an amplitude error (E2-E1)/E0 damping quickly to zero, after a few cycles of oscillation, with a small residual error, for all the different generated chaos waveforms.

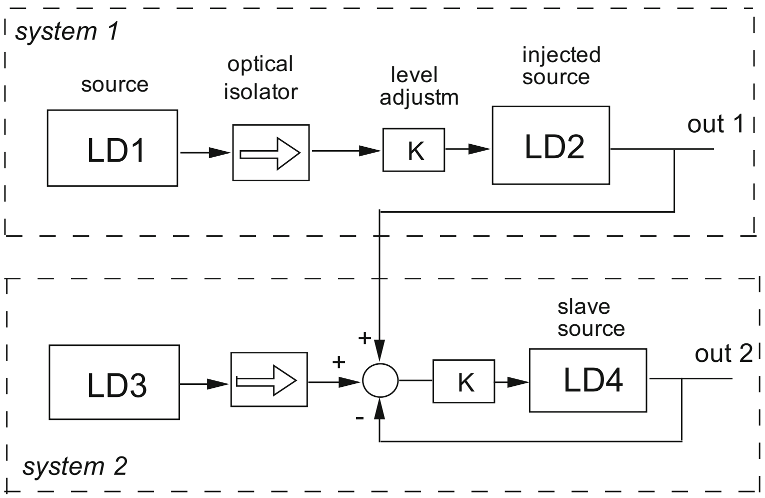


Fig. 6.4 Scheme of synchronization: two identical coupled-laser systems (*LD1/LD2* and *LD3/LD4*) are used. Out 1 is sent to the sum node at the input of slave laser *LD4* of *system 2*, and the output of *LD4* is sent back in subtraction, so that when *out 2* is equal to *out 1* (it is synchronized) no further correction is applied. (From Ref.[20])

One critical issue is sensitivity to system parameters: we find that small deviations from nominal values of the parameters are tolerated, whereas beyond a certain threshold (for example, 0.5 %) synchronization isn't achieved any longer. Dotted lines indicate this ideal condition (Fig. 6.5). For a real system, the error (E2-E1)/E0 is a function of the rms mismatch allowed for the parameters (Fig. 6.5, left); removing the effect of gain mismatch (of E2 and E1) we obtain the diagram of Fig. 6.5, right. Interesting to note, upon changing the laser parameters over a wide range of reasonable values doesn't affect the general trend of synchronization. And, for the error to be small, we need a parameter mismatch less than ~ 0.2 %, while error becomes large and synchronization is lost for a mismatch larger than ~ 0.8 %, typically. The sensitivity of chaos synchronization to system parameters is the key of secure transmission, usually referred to as Chaos Cryptography, as it will be shown in the next paragraph.

6.4 Using Chaos to Protect Data

A first scheme of cryptography, CM (Chaos Masking) readily follows from synchronization: summing (incoherently) to the generated chaos a small signal carrying the desired message will not impair synchronization of the slave because the (small) deterministic signal will be ignored (it is not a system eigenfunction), and upon subtracting the synchronized output (chaos) from the received signal (chaos + message) we will free out the message [20].

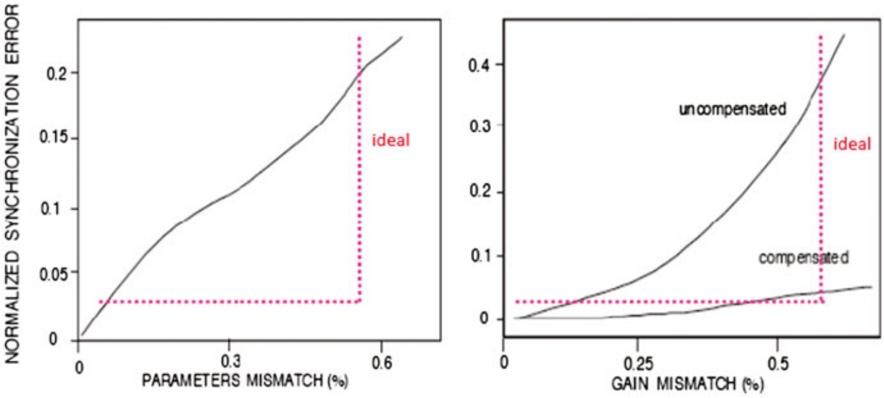


Fig. 6.5 Synchronization error vs. relative mismatch of system parameters (*left*) and vs. gain mismatch, in uncompensated and amplitude-normalized conditions (*right*). (From Ref.[20])

However, the CM scheme has some drawbacks. First, if the sum of signal to chaos is made at a slightly different λ, clever filtering could reveal the message. Second, the small amplitude of the message (e.g., 5 % of the transmitted power) makes the transmitted power mostly used by chaos rather than message, and thus SNR cannot be very high. So, the quest is on a method allowing for a message as large as the chaos.

The answer is chaos shift keying (CSK) [19]. In CSK, we encode the “0”s and “1”s bits of the digital message on different chaos waveforms (or, more correctly, on different orbits in the phase space), by acting on one of the several parameters governing the dynamical evolution of the system, e.g., the drive current of the laser [20].

Thus, each bit uses the entire chaos waveform and associated power, and we fully exploit the available photons (and increase SNR).

As shown in Fig. 6.6, at the transmitter 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, and we get a sequence of piece-wise chaos waveforms for the coded message. At the receiver end, two twin systems are set at bias J_0 (LD3/LD4) and J_1 (LD5/LD6). Injection of the received waveform synchronizes the designated bit, “0” for system LD3/LD4 and “1” for system LD5/LD6.

The CSK and CM cryptography schemes, however, are difficult to implement with the two-laser structure of the basic coupled-system cell, which is not minimum part-count. To go to a practical system, we need a simpler scheme, and this is indeed possible with the self-mixing (also called DOF—Delayed Optical Feedback) chaos cell (Fig. 6.7).

In a typical all-fiber DOF setup (Fig. 6.8 top), the laser diode is conjugated through a lens to a single-mode fiber, whose end-face is angled (8–12 deg. typ.) to avoid back-reflection. The fiber ends on a mirror, partially reflecting back the outgoing signal. By varying the distance of fiber tip to the mirror we can adjust the level K of feedback. In this case a so-called long-cavity system is realized. The message can be added to chaos by an external amplitude modulator.

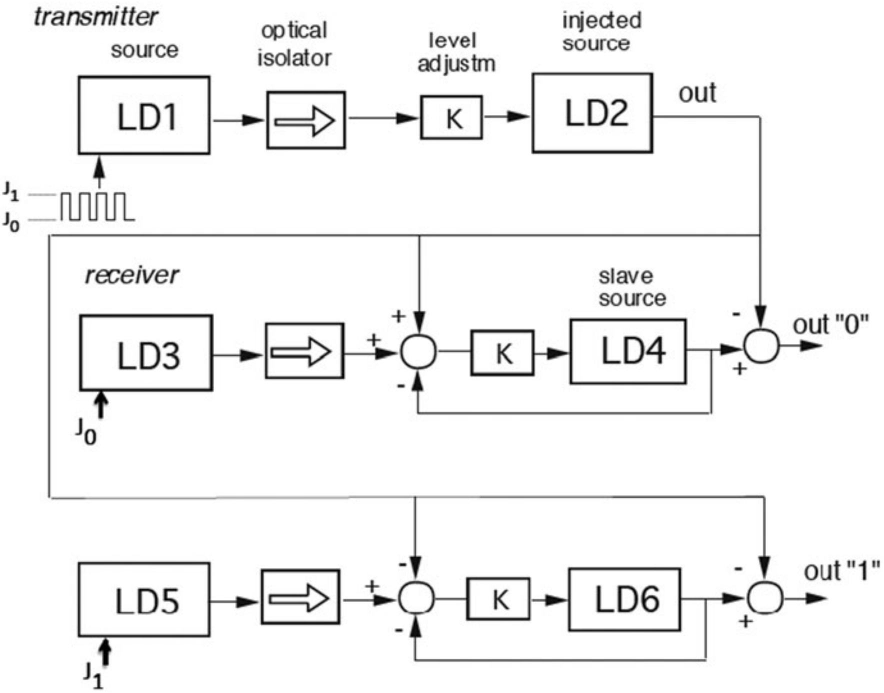


Fig. 6.6 CSK cryptography: the binary message modulates levels J_0 and J_1 of the bias current, and lasers *LD1/LD2* generate a sequence of chaos waveforms, for the "0" and "1" of the message. At the receiver end two twin systems are biased at J_0 (*LD3*) and J_1(*LD5*) and injection of transmitted waveform makes them synchronize on its designated bit, "0" for system *LD3/LD4* and "1" for *LD5/LD6*. (From Ref.[20])

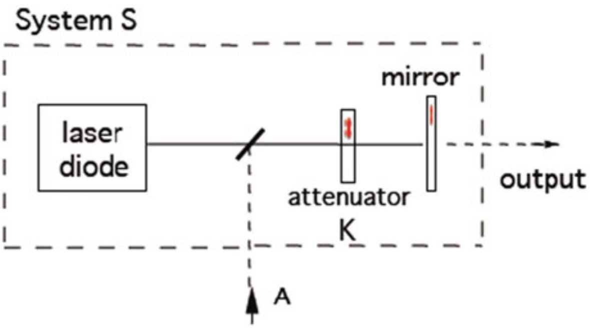
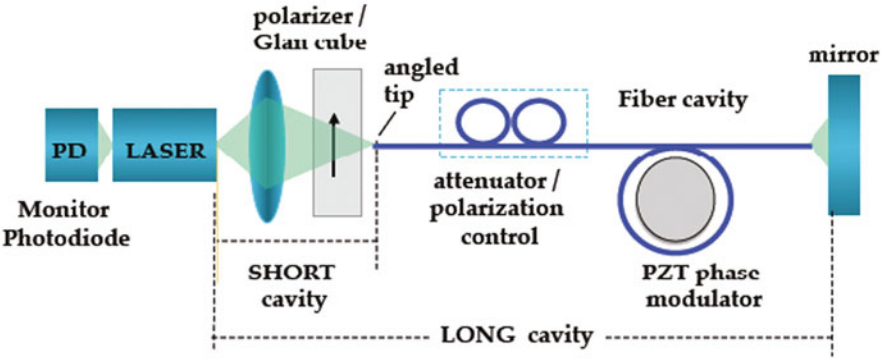


Fig. 6.7 DOF (delayed optical feedback) chaos generator: the laser is subject to a self-injection-coupling regime from the mirror. The beamsplitter injects an external signal for synchronization

We can also implement the DOF cell by an integrated optics technology (Fig. 6.8 bottom and Fig. 6.9), incorporating in a single photonic integrated circuit (PIC) the active source (a DFB laser), an active waveguide for amplitude and/or phase modulation, and the retro-reflector (the mirror-like cleaved facet of the chip). This solution offers a more stable short-cavity system [21]; also, the integrated optics



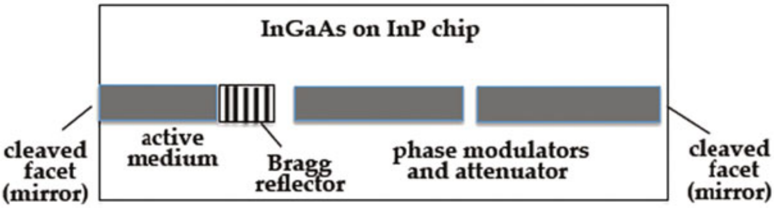


Fig. 6.8 Technologies for implementing the DOF scheme: all-fiber (*top*) and integrated optics (*bottom*)

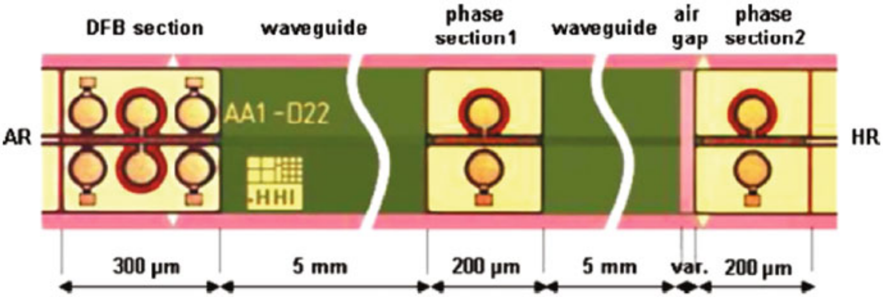


Fig. 6.9 A DOF short-cavity PIC-chip, fabricated by InGaAs waveguides on a InP substrate, and incorporating a DFB laser, two 5-mm waveguides and two phase modulators, to realize an integrated crypto-system. (From Ref.[22])

approach offers the possibility of developing more advanced chaos generators, which would be difficult to implement in bulk or micro-optics [22].

Practical solutions of CM and CSK schemes are available in the literature. An example of a CSK-PM system is reported in Fig. 6.10 [23], using a short-cavity DOF generator and a $LiTaO_3$ phase modulator to impress the message as a phase $\Delta\psi_{in}$ added to the optical pathlength 2 ks. As the short-cavity DOF is sensitive to the external cavity phase, the chaos waveform is somehow coded by phase $\Delta\psi_{in}$.

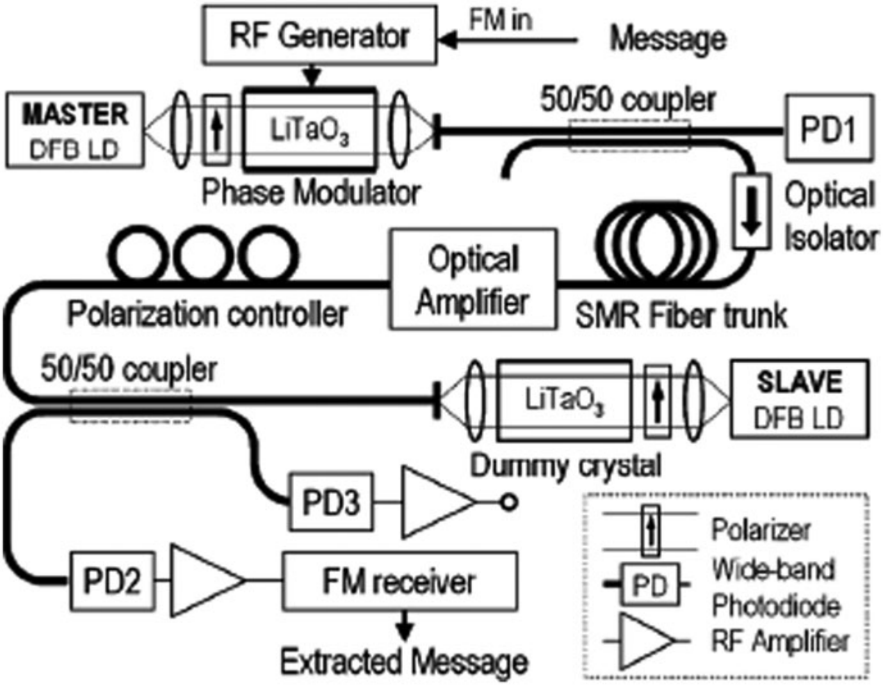


Fig. 6.10 A short-cavity DOF-CSK system, uses a $LiTaO_3$ phase modulator to impress the message as a phase variation in the cavity and hence in the chaos waveform generated by the DOF. At the receiver, a dummy modulator synchronizes only when phase is zero. Photodetector and an FM receiver act as phase-to-amplitude converter, thus extracting the message. (From Ref.[23])

At the receiver end, an identical DOF generator has the phase modulator set at zero voltage. Thus, the receiver is synchronized only for zero input message or phase $\Delta\psi_{in}$ Correlation of receiver and transmitter chaos waveforms progressively decreases at the increase of the phase difference, and this process is a sort of phase-to-amplitude conversion. With photodetection followed by a PM conversion we get a signal proportional to $\Delta\psi_{in}$ and hence to input signal.

In all the proposed solutions for secure transmission using chaos, security is based on synchronization sensitivity to laser parameters. The two users must share a 'twin' laser pair, i.e., two lasers of very similar parameters (selected from the same wafer). Thus, for an eavesdropper, it is very difficult to find a laser compatible with the twin pair, to synchronize chaos and decode the message.

With the standard two-laser system, chaotic transmission of digital signals in the GHz range has been demonstrated on the metropolitan network of Athens [24]. Also, transmission of RF analog signals has been experimentally proven (Fig. 6.11.) [25]. Several basic building blocks for future long-distance transmission have been already proposed, such as a chaotic wavelength converter for WDM transmission [26], and a chaotic repeater [27]. Moreover, dual-channel operation [28], chaotic multiplexing

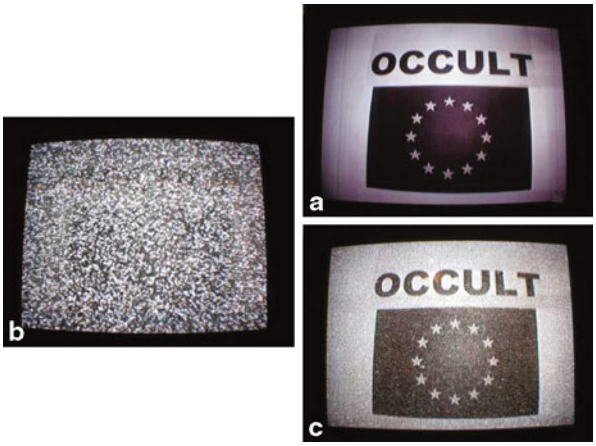


Fig. 6.11 Experiment of transmission of a video signal: **a** plaintext message, **b** message hidden in chaos, **c** recovered message. (From Ref. [25])

[29] and coding solutions for a more efficient signal protection have been studied [30, 31].

Alternative solutions based on the electro-optical feedback have been also proposed [32]. In the basic scheme, chaos is generated by using a nonlinear modulator fed by an auxiliary laser, the output of which is applied to the electrical input of the transmitter laser, after photodetection. The feedback loop is closed, by applying the photodetected laser output signal to the modulator electrical input. The message is added to chaos at the transmitter laser input node.

At the receiver, the optical signal (chaos + message), is photodetected and applied to the same modulator/laser combination, but working at open loop, to extract chaos by nonlinear filtering. The message is finally recovered by subtraction, from the received signal, of photodetected chaos.

This approach avoids optical injection and laser alignment procedures, and does not require the integrated optics technology for a practical in field implementation, since a compact and stable micro-optics realization is possible. On the other hand, its security relies on matched nonlinear modulators, instead on the more challenging (for an eavesdropper) matched lasers.

6.5 Recent Achievements

In addition to the basic two-laser scheme, open or close loop [33], more advanced setups have been developed, which offers a better synchronization quality to the authorized subscribers, who share the matched laser pair, as well as a better security against an eavesdropper attack. Both results are based on such schemes being symmetrical (differently from the basic two-laser solution), since both Tx and Rx lasers are injected by a third (possibly unmatched) chaotic laser (called the driver Drv).

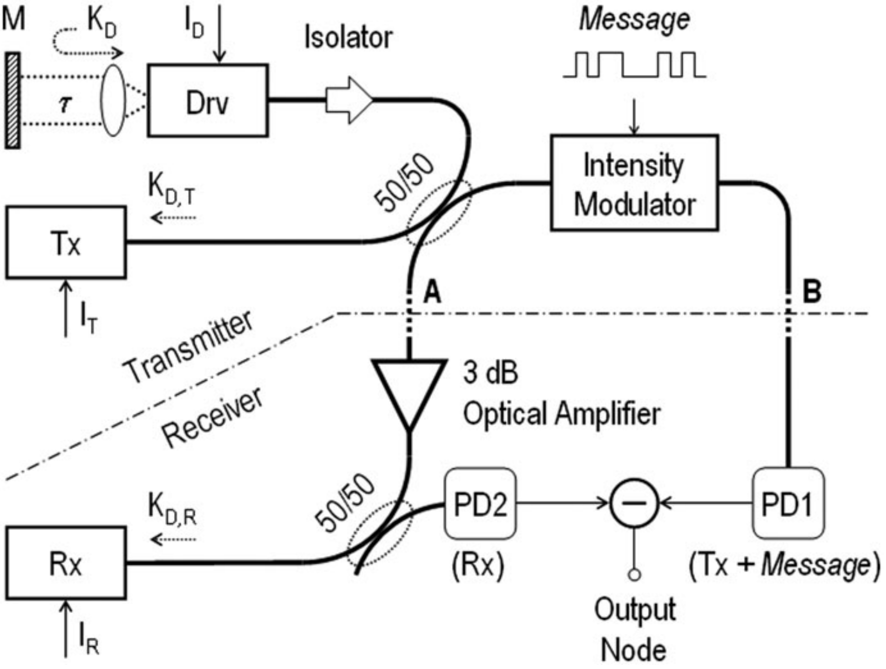


Fig. 6.12 A three-laser CM crypto-system uses a common source driver (*Drv*) to route into chaos and synchronise a pair of twin lasers (*Tx* and *Rx*). The message is recovered as in the basic scheme by chaos cancellation at the receiver. (From Ref. [34])

A CM implementation setup of such three-laser scheme [34] is shown in Fig. 6.12. In this case, the Drv laser is routed to chaos by delayed optical feedback, while Rx and Tx may have no feedback, or may experience a weak local optical feedback by a mirror. Numerical results for RF power spectra of Drv, Tx and Rx, and their difference are in Fig. 6.13. In Fig. 6.14, transmission of a 5 Gb/s message is simulated, with the RF spectra of the plaintext message, of the same message hidden in chaos, and of the recovered message after chaos subtraction. The eye-diagram of the recovered message is also shown.

In experiments, the high cancellation levels of Fig. 6.13 cannot be achieved. However, the advantage of the three-laser over the two-laser scheme has been confirmed. The requirement of using a supplementary laser is not really a drawback, since in a network the same Drv can be used to assist several interconnections between couples of users.

The three-laser scheme can be easily modified for use in free space propagation. The recent interest in FSOLs (Free Space Optical Links), especially for countries rapidly expanding their communication infrastructure, also requires a careful design for security, since the open optical beams can be easily intercepted by an eavesdropper.

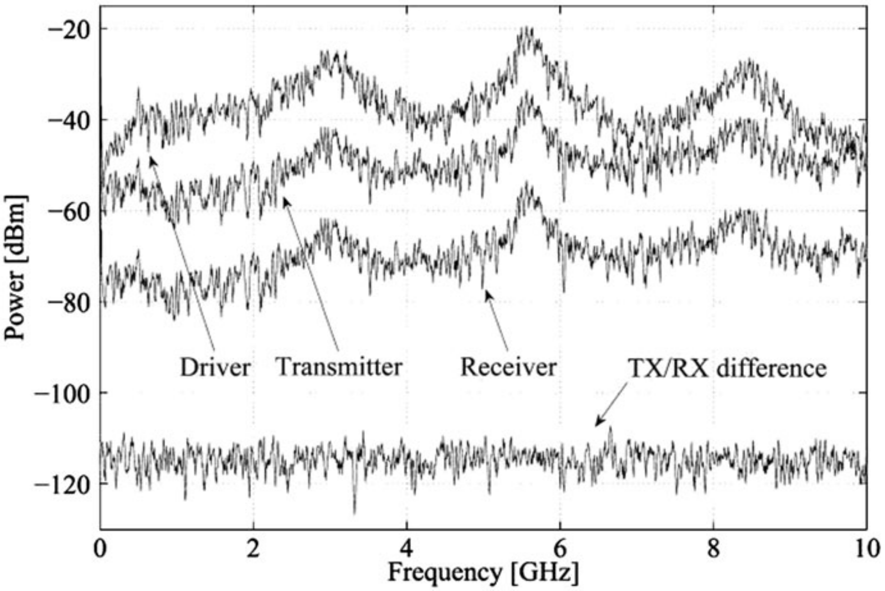


Fig. 6.13 Numerical RF power spectra for *Drv*, *Tx* and *Rx* in the scheme of Fig. 6.10. For better visualization, the traces of *Drv* and *Rx* have been shifted upwards by 20 dB and downwards by 20 dB, respectively. The difference signal is also shown. (From Ref.[34])

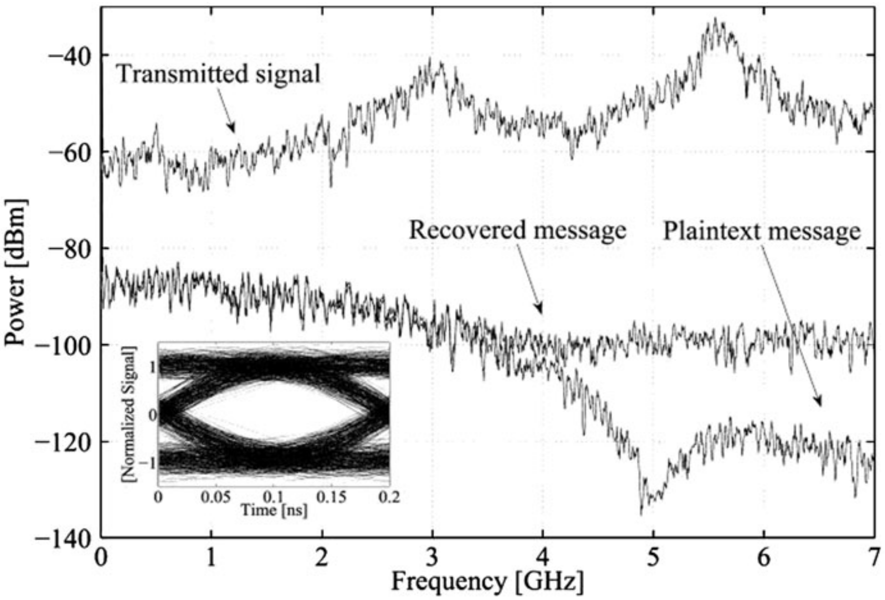


Fig. 6.14 Numerical RF spectra for CM transmission of a 5 Gb/s digital message with the scheme of Fig. 6.10. The eye diagram of the recovered message is shown in the inset. (From Ref.[34])

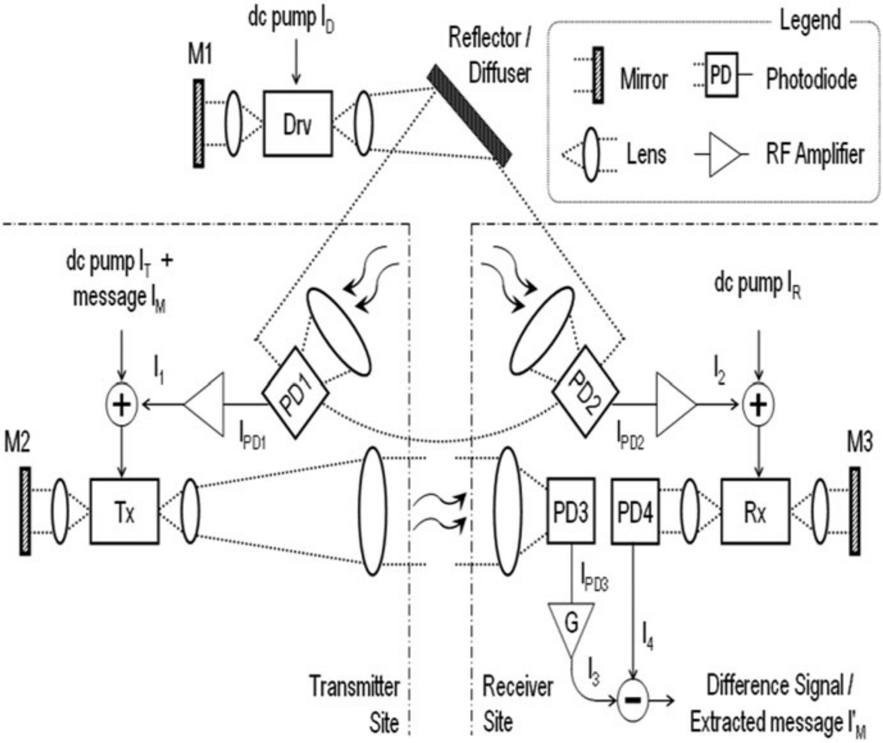


Fig. 6.15 Configuration for secure data transmission in free-space. Due to high channel attenuation, the optical emission of the Drv is photodetected and amplified before injection into *Rx* and *Tx*. The same is done for *Tx* to *Rx* injection. (From Ref.[35])

A suitable three-laser scheme [35] for such application, where attenuation is usually high, is proposed in Fig. 6.15.

The optical emission of Drv is photodetected and amplified before injection into Rx and Tx. The same is done for Tx to Rx injection. Electrical amplification is a convenient solution, with respect to optical amplification, and results in a lower cost, easier to align system. This scheme offers a viable solution also for indoor secure transmission, in a room or on a train or airplane, where many users share the same diffused channel, as well as the Drv, which can be installed, e.g., on the ceiling.

Another evolution of the standard setup has been in the direction of providing a real multi-user network protected by chaos.

All the schemes considered so far are practically restricted to transmission between two specific users, sharing a twin laser pair. However, in most cases, it is required to organize a network of several users that can freely transmit data to one-another in a secure way. In practice, it is difficult to find more than a few matched devices on a wafer, which can all synchronize efficiently to one another, and thus multi-user transmission would require that each user holds a laser (of a twin pair) for each

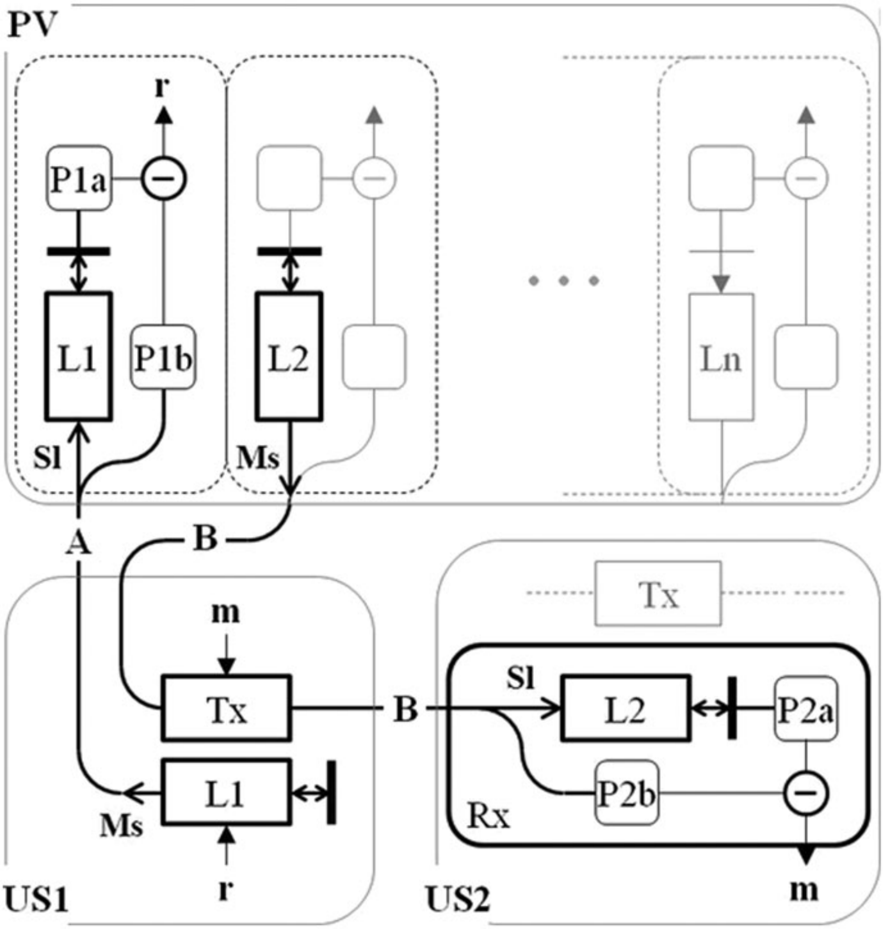


Fig. 6.16 Multi-user network configuration for secure data transmission. Path A is the connection between the provider (*PV*) and the first user (*US1*), while *B* is the connection between the two users (*US1* and *US2*). *Tx* is a modulator to introduce message m and Pij are photodiodes. (From Ref.[36])

potential partner. This is clearly unpractical. Alternatively, one could increase the message amplitude, so that a lower synchronization level can be tolerated, but in this case the security level would be poor.

A possible solution has been recently proposed [36], derived from the well-known public-key cryptography.

With this new approach, it is possible to exchange data between any couple of subscribers in a network. This can be done by introducing a provider, who is responsible of the network security, as shown in Fig. 6.16. For each subscriber, a couple of twin chaotic lasers is required, one being held by the provider and the other by the subscriber himself. The basic two-laser (or the three-laser) scheme of chaotic transmission is then used for secure data exchange, both between a subscriber (US) and the provider (PV), and between two subscribers (US1, US2).

With reference to Fig. 6.16, when subscriber US1 wants to send a message m to US2, it first sends a request to PV (message r). This is done in a protected way, by using lasers L1, i.e., the twin pair common to the provider PV and to US1. As a response to the request of US1, the provider routes the chaotic carrier generated by laser L2 to US1. User US1 can now transmit message m to US2 by modulating this carrier, implementing, for example, CSK (Chaos Shift Keying) or CM (Chaos modulation). Only user US2 can retrieve the message, since he is the only one to hold the corresponding twin laser. Other users, or an eavesdropper, cannot extract the message.

Several arrangements can be considered, based on this architecture. Extra security can be offered by protecting path B, since, in principle, an eavesdropper could intercept this carrier between PV and US1 and use it to send a message to US2, pretending it comes from an authorized subscriber. To tackle this problem, a possible solution is to hide the transmission carrier in chaos on its turn. The same laser pair L1, already used to send the request r from US1 to PV, can be used to this end, by implementing for example a two-laser scheme, where the roles of Ms and Sl subsystems (Fig. 6.16) are now interchanged, and the 'message' in this case is the chaotic carrier of L2.

References

1. see for example International Journal of Bifurcation and Chaos, 23, 2013. WSP (Singapore) ISSN: 0218–1274
2. see for example: Journal of Complexity, 29, 2013. Elsevier B.V.(Amsterdam) ISSN: 0885–064X
3. Tsoukas, H.: Chaos, complexity and organization theory. Organ. **5**, 291–313 (1998)
4. Haken, H.: Analogy between higher instabilities in fluids and lasers. Phys. Lett. A. **53**, 77–78 (1975)
5. Ohtsubo, K.: Semiconductor Lasers: Stability, Instability and Chaos, 2nd edn. (Springer Series Optical Sciences 111). Springer, New York (2009)
6. Arecchi, F.T., Puccioni, G.L., Tredicce J.R.: Deterministic chaos in laser with injected signal. Optics Commun. **51**, 308–314 (1984)
7. Lang, R., Kobayashi, K.: External optical feedback effects on semiconductor injection laser properties. IEEE J. Quant. Electron. QE-**16**, 347–355 (1980)
8. Donati, S.: Developing self-mixing interferometry for instrumentation and measurements. Laser Photon. Rev. **6**, 393–417 (2012)
9. Donati, S.: Responsivity and noise of self-mixing photodetection schemes", IEEE J. Quantum Electron. **47**, 1428–1433 (2011)
10. Donati, S.: "Photodetectors", Prentice Hall, Upper Saddle River (2000), see Sect. 8.4.
11. Soriano, M.C., Garcia-Ojalvo, J., Mirasso, C., Fischer, I.: complex photonics: dynamics and applications of delay-coupled semiconductors Lasers. Rev. Mod. Phys. **85**, 421–470 (2013)
12. S. Donati, S.-K. Hwang: Chaos and high-level dynamics in coupled lasers and their applications. Prog. Quantum Electron. **36**(2–3), 293–341 (2012)
13. Donati, S., Mirasso, C. (eds.): Optical chaotic cryptography. Feature Issue of: IEEE. J. Quantum Electron. QE-**38,** 1138–1184 (2002)

14. Larger, L., Goedgebuer, J.-P. (eds): Special Number on Criptography using Optical Chaos, Comptes Rendus de l'Academie des Sciences-Dossier de Physique, vol. 6, n. 5 (2004)
15. Ohtsubo, J.: Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback. IEEE J. Quantum Electron. **38**(9), 1141–1154 (2002)
16. Annovazzi-Lodi, V., Donati, S., Manna, M.: Chaos and locking in a semiconductor laser due to external injection. IEEE J Quantum Electron. QE-**30**, 1537–1541 (1994)
17. Mirasso, C.R., et al: Synchronization properties of chaotic semiconductor lasers and applications to encryption. C. R. Phys. **5**, 613–622 (2004)
18. Ju, R., Spencer, P.S., Shore, K.A.: The relative intensity noise of a semiconductor laser subject to strong coherent optical feedback. J. Opt. B-Quantum Semiclass Opt. **6**(8), S775–S779 (2004)
19. Annovazzi-Lodi, V., Donati, S., Scirè, A.: Synchronization of chaotic injected-laser systems and its application to optical cryptography. IEEE J. Quantum Electron. QE-**32**, 953–959 (1996)
20. Annovazzi-Lodi, V., Donati, S., Scirè, A.: Synchronization of chaotic lasers by optical feedback for cryptographic applications. IEEE J. Quantum Electron. QE-**33**, 1449–1454 (1997)
21. Syvridis, D., Argiris, A., Bogris, A., Hamacher, M., Giles, I.: Integrated devices for optical chaos generation and communications applications. IEEE J. Quantum Electron. **45**(11), 1421–1428 (2009)
22. Tronciu, V.Z., Mirasso, C., Colet, P., Hamacher, M., Benedetti, M., Vercesi, V., Annovazzi-Lodi, V.: Chaos generation and synchronization using an integrated source with an air gap. IEEE J. Quantum Electron. **46**(12), 1840–1846 (2010)
23. Annovazzi-Lodi, V., Benedetti, M., Merlo, S., Perez, T., Colet, P., Mirasso, C.: Message encryption by phase modulation of a chaotic optical carrier. IEEE Photon. Technol. Lett. **19**, 76–78 (2007)
24. Argyris, A., Syvridis, D., Larger, L., Annovazzi-Lodi, V., Colet, P., Fischer, I., Garcia-Ojalvo, J., Mirasso, C., Pasquera, L., Shore, K.A.: Chaos-based communication link at high bit rate using commercial fiberoptic link. Nat. Lett. **438**, 343–346 (2005)
25. Annovazzi-Lodi, V., Benedetti, M., Merlo, S., Norgia, M., Provinzano, B.: Optical chaos masking of video signals. IEEE Photon. Technol. Lett. **17**, 1995–1997 (2005)
26. Annovazzi-Lodi, V., Aromataris, G., Benedetti, M., Cristiani, I., Merlo, S., Minzioni, P.: All-optical wavelength conversion of a chaos masked signal, IEEE Photon. Technol. Lett. **19**, 1783–1785 (2007)
27. Matsuura, T., Uchida, A., Yoshimori, S.: Chaotic wavelength division multiplexing for optical communication. Opt. Lett. **29**, 2731–2733 (2004)
28. Paul, J., Sivaprakasam, S., Shore, K.A.: Dual-channel chaotic optical communications using external–cavity semiconductor lasers. J. Opt. Soc. Am. B. **21**, 514–521 (2004)
29. Lee, M.W., Shore, K.A.: Demonstration of a chaotic optical message relay using DFB laser diode. IEEE Photon. Technol. Lett. **18**, 169–171 (2006)
30. Ursini, L., Santagiustina, M., Annovazzi-Lodi, V.: Enhancing chaotic communication performances by manchester coding. IEEE Photon. Technol. Lett. **20**, 401–403 (2008)
31. Bogris, A., Chlouverakis, K.E., Argyris, A., Syvridis, D.: Enhancement of the encryption efficiency of chaotic communications based on all-optical feedback chaos generation by means of subcarriers modulation. In: Proceedings CLEO-Europe/IQEC, 2007, paper CH4-MON
32. Goedgebuer, J.P., Larger, l., Porte, H.: Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laserdiode. Phys. Rev. Lett. **80**, 2249–2252 (2008)
33. Vicente, R., Perez, T., Mirasso, C.: Open-versus closed-loop performance of synchronized chaotic external-cavity semiconductor lasers. IEEE J. Quantum Electron. **38**(9), 1197–1204 (2002)
34. Annovazzi-Lodi, V., Aromataris, G., Benedetti, M., Merlo, S.: Private message transmission by common driving of two chaotic lasers, IEEE J. Quantum Electron. **46**, 258–264 (2010)
35. Annovazzi-Lodi, V., Aromataris, G., Benedetti, M., Merlo, S.: Secure optical transmission on a free space optics data link IEEE J. Quantum Electron. **44**, 1089–1095 (2008)
36. Annovazzi-Lodi, V., Aromataris, G., Benedetti, M.: Multi-user private transmission with chaotic lasers. IEEE J. Quantum Electron. **48**, 1095–1101 (2012)