Available online at www.sciencedirect.com
SCIENCE DIRECT®
C. R. Physique 5 (2004) 623–631
COMPTES RENDUS PHYSIQUE

Cryptography using optical chaos/Cryptographie par chaos optique

Fiberoptics setup for chaotic cryptographic communications

Valerio Annovazzi-Lodi *, Mauro Benedetti, Sabina Merlo, Michele Norgia

Dipartimento di Elettronica, Università di Pavia, Via Ferrata 1, 27100 Pavia, Italy

Presented by Guy Laval

Abstract

In this paper we present a fiberoptics setup which can be easily configured for different experiments on chaos generation, chaos synchronization and optical chaotic cryptography using semiconductor lasers. Long and short cavity, open and closed loop configurations are easily implemented with minor changes of the basic setup, allowing for a comparison of their performances using various encoding methods. Different transmission media, possibly including optical amplifiers, can be also tested. ***To cite this article: V. Annovazzi-Lodi et al., C. R. Physique 5 (2004).***

Résumé

Configuration expérimentale à base de fibre optique pour l'étude de la cryptographie par chaos. Nous présentons un montage expérimental réalisant un système de transmission crypté par chaos, à base de fibre optique. Ce montage peut être pratiquement configuré de différentes manières, selon qu'il s'agit d'étudier la génération de chaos, la synchronisation des lasers chaotiques, et bien sûr aussi la cryptographie optique par chaos. Moyennant des modifications mineures de montage, il est possible d'explorer des configurations de cavité de différentes longueurs, des schémas de synchronisation avec ou sans contre–réaction optique, ainsi que des effets spécifiques dus au milieu de propagation entre émetteur et récepteur et à la présence d'amplificateurs optiques sur la ligne de transmission. ***Pour citer cet article : V. Annovazzi-Lodi et al., C. R. Physique 5 (2004).***

Keywords: Chaos; Cryptography; Laser diode; Synchronization

Mots-clés : Chaos ; Cryptographie ; Laser à semi-conducteur ; Synchronisation

1. Introduction

The synchronization of chaotic semiconductor lasers has been proposed by several authors [1–4,6–9] in the last years as a means to implement secure data transmission on an optical network. Basically, this approach consists in hiding a message into a chaotic waveform generated by a laser driven to chaos, e.g., by delayed feedback from an external mirror [3,4,6–9] (Fig. 1(a)). A suitable method for encryption is the mere superposition of message and chaos, as in Fig. 2(b). The composite signal is then transmitted through the fiber link. At the receiver another laser is used, into which the composite waveform is injected. Under suitable operating conditions, the second laser synchronizes to the transmitter, which means that it generates almost exactly the same chaotic waveform. In this master/slave approach, the message is then extracted by making the difference between the received composite signal and the recovered chaotic waveform. However, synchronization is possible only if the parameters of

* Corresponding author.
E-mail address: valerio.annovazzi@unipv.it (V. Annovazzi-Lodi).

1631-0705/$ – see front matter
doi:10.1016/j.crhy.2004.03.005

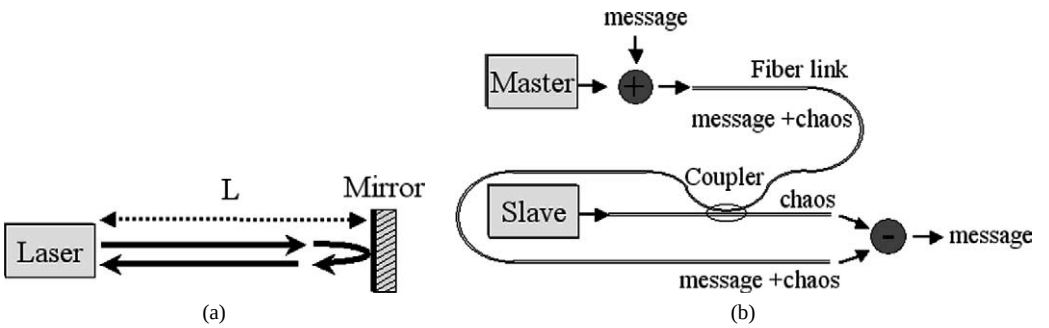

Fig. 1. (a) Delayed optical feedback on a laser from a remote mirror. (b) Basic ACM scheme: the master is a laser routed to chaos as in (a); the slave may be chaotic (closed loop) or not (open loop).

the two lasers are very close, which means, for example, that the lasers have been selected from the same wafer. The laser couple thus represents the (hardware) cryptographic key. This basic scheme is usually referred to as Additive Chaos Masking (ACM), and may be implemented by using a third laser modulated in amplitude by the message (an analog or digital signal), whose output is combined with the chaotic waveform. Other approaches are possible [6,9], such as Chaos Shift Keying (CSK), where the message directly modulates the transmitter laser pump current, and Chaos Modulation (CM), where the message is applied to the chaotic waveform by an external amplitude modulator. Much theoretical and numerical work has been performed on this topic, usually based on the well-known Lang–Kobayashi model [10]; more advanced detection methods have been also proposed, such as those based on the Kapitaniak approach [7]. Finally, chaos generation may use other schemes, such as a two-laser injection system [11]. However, delayed optical feedback for chaos generation, and direct injection of the master into the slave for synchronization, is by far much easier to implement than more sophisticated schemes, and have been used in most experimental implementations reported in the literature. In this framework, two main cases may be considered, since the slave may be intrinsically chaotic or, being stable alone, it may simply copy, because of injection, the master optical chaos. The first case is referred to as 'closed loop'; the second case is referred to as 'open loop'. Besides this topological distinction, another important difference is determined by the length L of the external laser cavity, defined by the distance between the laser facet and the external mirror (Fig. 1(a)). Such length is to be compared with distance l corresponding to the laser relaxation frequency f_r, i.e., $l = c/f_r$. If $L > l$ (but L is shorter than the coherence length of the source), the laser is working in the 'long cavity' regime; if $L < l$, it is working in the 'short cavity' regime. Both cases have been investigated in the literature, and they exhibit different properties. Both may be considered for cryptographic applications [4,5,11–13]. Experimental studies on cryptography based on chaotic lasers require to test several laser couples, as well as different encryption methods and detection schemes. Doing that in a standard bulk optics setup is possible, but relatively difficult and time consuming, mainly due to the optical alignment procedures. For this reason, we have developed a suitable fiberoptics setup which can be easily specialized with minor changes to implement open and closed loop schemes with long and short cavities. Also, CSK, CM, ACM experiments, as well as transmission through fibers of different length (possibly including splices, connectors, and optical amplifiers), can be performed simply by inserting or removing connectorized components. This system has been used for extensive testing of different laser models and several laser couples with various cryptographic schemes and transmission fiber links. In the following we present our fiberoptics setup, and show some results that we have obtained for the case of a short cavity, which represents a very promising approach for the practical implementation of optical chaos cryptography, because of its compactness, stability, high allowable data rate.

2. The fiberoptics setup

The fiberoptics setup is shown in Fig. 2. It includes two lasers in a master/slave configuration; an optical isolator is inserted in the fiber trunk connecting the two lasers to ensure one-way injection. As required in our experiments, polarizers have been included in front of each laser to work in the so-called 'coherent injection' regime, which means that all injected radiation is polarized along the direction of the laser emission. Incoherent injection [14] effects could be also studied by proper setup modifications. A fraction of the emission of each laser is detected by an amplified photodiode (PD1, PD2), for both d.c. current detection (to be observed during alignment) and RF modulation detection. The integrated indium phosphide photodiode/amplifier that we have selected (Optospeed HRXC10B, bandwidth $B = 8$ GHz) comes on a chip carrier, and is suitable to be used also as a partial mirror, which allows us to greatly simplify the setup. Indeed, it has been found that the reflected power from the gold contacts and mass plane surrounding the photodiode is sufficient to drive the laser to chaos; also, the feedback level can be easily varied by acting on the alignment. Thus, the setup can be specialized to study both the long cavity and the short cavity regimes, in open and closed loop configurations, by a suitable selection of the shape of each fiber

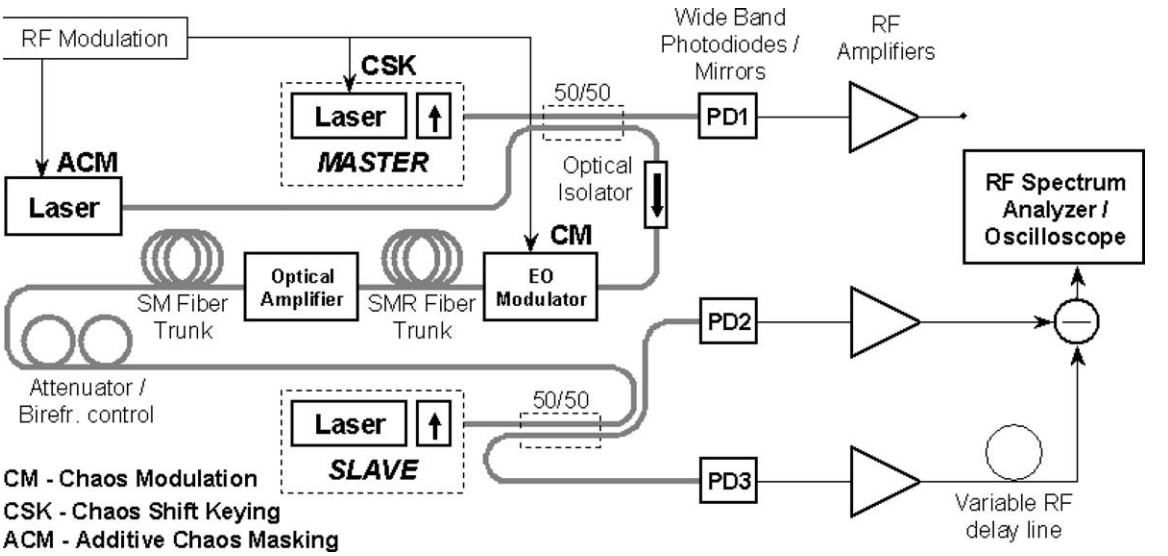

Fig. 2. The fiber optics setup for experiments on chaos cryptography.

tip, and of the alignment of the photodiodes. For example, if the fiber end next to the master laser is angled, and photodiode PD1 is aligned, the master laser is driven to chaos with the long cavity defined by the laser facet and PD1. On the other hand, if the fiber end next to the master laser is aligned, the fiber end next to the photodiode is angled, and the photodiode PD1 is tilted to avoid backreflection, the master laser is made chaotic with the short cavity (in the air) defined by the laser facet and the fiber tip next to it. In the first case, if in addition the fiber from the slave laser to photodiode PD2 is angled at both ends, and if PD2 is tilted, the solitary slave laser is unperturbed, and a long cavity, open loop, synchronization scheme is implemented. If instead the fiber termination next to photodiode PD2 is straight, and the photodiode is aligned, the solitary slave is chaotic, and thus the experimental setup implements a long cavity, closed loop synchronization scheme. Similarly, short cavity open loop and closed loop synchronization experiments can be performed. In our setup, the fiber tips are held by ferrules and their position is controlled by motorized 3-axis micropositioners with a resolution of 50 nm. This allows for an accurate control of the fiber-laser distance, as required especially in short cavity experiments, where subwavelength variations of such distance may strongly affect the laser regime [13]. The lasers are mounted on suitable holders, and their temperature is controlled within 0.01 K by standard Peltier modules. Synchronization between master and slave lasers can be evaluated either in the time or in the frequency domain by using a fast oscilloscope or a RF spectrum analyzer. Though photodiode PD1 could be used to monitor the master RF output, it is preferable to use it only for alignment, and monitor the master regime from a suitable port of the slave coupler (photodiode PD3). In this way, we work in a configuration which is much similar to that encountered in a real transmission system, where the output of the master photodiode (PD1) is not available at the receiver side. Moreover, this choice allows for studying synchronization when a long fiber trunk is inserted between master and slave, without the requirement of compensating a large transmission delay. Indeed, a variable RF delay line is used in the setup, as shown in Fig. 2, to compensate only the relatively small differential delay between the emission of the master and that of the slave, which is equivalent to twice the optical path between the slave coupler and the slave laser itself. The outputs of PD3, PD2 can be directly viewed and compared at a fast real-time oscilloscope. Then, the correlation between the chaotic waveforms is calculated by processing the traces after acquisition. Alternatively, one may observe the difference between the RF amplifier outputs, obtained, e.g., by passive sum of the two signals after inverting one of them by a supplementary amplifier. In this case, a RF spectrum analyzer gives a fast way of testing the synchronization quality over the whole chaos bandwidth, so that an expensive state-of-the art real time oscilloscope or streak camera is not required. Different fiber lengths and types may be inserted in the path between the two lasers, as well as fused splices and connectors to simulate a point-to-point connection. The effect of optical amplifiers, both Erbium doped (EDFA) and semiconductor types, can be also tested. The fiber birefringence control shown in Fig. 2 is used to compensate for the birefringence of the fiber trunks; together with the polarizer positioned in front of the slave, it also plays the role of an attenuator, and is used to control the intensity of injection from one laser to the other. Finally, it is shown in Fig. 2 how different encoding schemes (ACM, CSK and CM) can be tested in the fiberoptics setup. In our laboratory, the whole system has been built on an optical table with pneumatic quenching. A special effort has been devoted to obtain two almost identical external cavities. As already stated, a very accurate control of length L is required especially in short cavity experiments. To this purpose, an improvement to the basic setup consists in adding a built-in interferometric measurement of the

laser-fiber distance on both master and slave. This feature is added, without increasing the setup complexity, by using the lasers themselves as the optical sources of two interferometers. To this end, each laser source is operated in a non-chaotic regime (this may be obtained, e.g., by changing the supply current or by reducing backreflection by a small translation of the fiber tip in a direction orthogonal to its axis). The obtained configuration is the so-called feedback interferometer [15], which is suitable for measurement of distance and vibration amplitude on small targets, such as MEMS [16]. This configuration is compact and it does not need a reference arm. Its operating principle is based on the perturbation that the back-injected field from the target induces in the laser. The interferometric signal is obtained from the photodetected current at a monitor photodiode, and, in the low injection regime, has the form [15]:

$$I = I_0 + I_m \cos \Phi, \tag{1}$$

where I_0, I_m are constants,

$$\Phi = \frac{4\pi}{\lambda} L \tag{2}$$

is the inteferometric phase and λ is the laser wavelength. A straightforward approach to measure the target movement, when high resolution is not required, is fringe counting. Other more accurate methods may be also used [16]. When injection increases, the modulation of I is no longer harmonic, but becomes distorted; however, by suitable processing, the target movement can still be measured [15]. In our case, since an absolute distance measurement is required on a standing target, a sweep in wavelength is given to the laser in order to develop fringes [15]. For a small wavelength variation $\Delta\lambda$, the interferometric phase change $\Delta\Phi$ can be approximated from Eq. (2) as:

$$\Delta\Phi = -\frac{4\pi}{\lambda^2} L \Delta\lambda \tag{3}$$

from which the value of L can be inferred. The laser wavelength variation is obtained by giving the laser a slow linear variation of temperature. In practical cases, where L is of the order of 30 mm, the distance is measured with a precision of the order of 50 µm. When a built-in photodiode is not available, the interferometric signal may be extracted everywhere along the optical path. A convenient solution is to use a Glan cube as the polarizer in front of each laser. By slightly tilting the device, a small portion of the laser emission may be extracted and then detected by a photodiode. Such method effectively speeds up and improves matching of the cavity lengths.

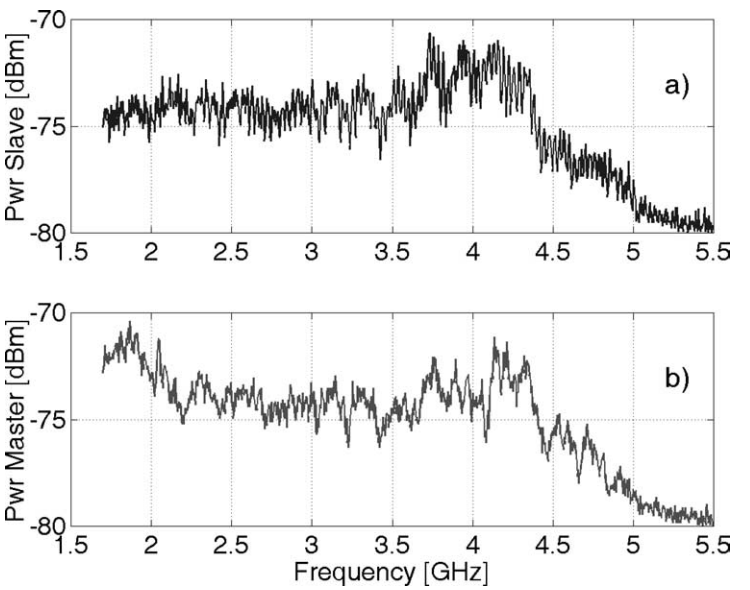

Fig. 3. Typical short cavity ($L = 30$ mm) RF spectra for two synchronized chaotic DFB laser at $\lambda = 1550$ nm in the closed loop configuration ((a) master, (b) slave).

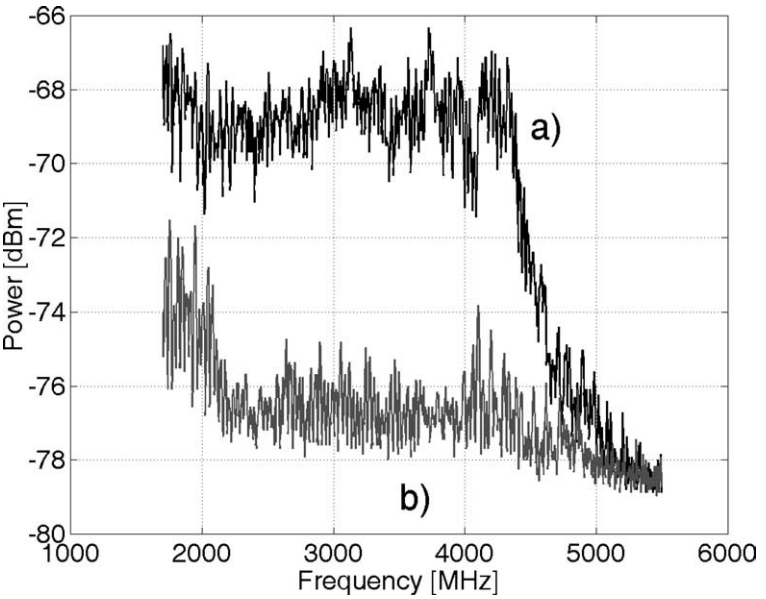

Fig. 4. Spectra of sum (a) and difference (b) of master and slave outputs showing synchronization in the frequency domain.

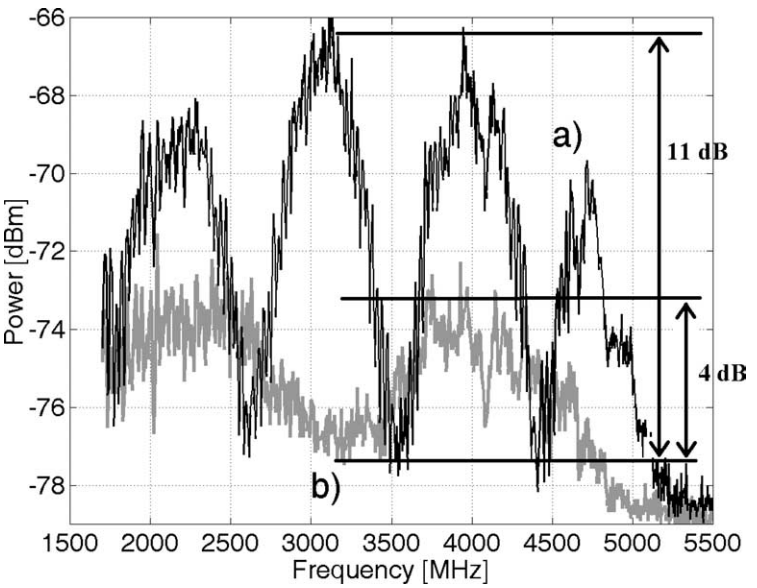

Fig. 5. Comparison of (a) a closed loop and (b) an open loop synchronization in the frequency domain.

3. Synchronization experiments

The setup described in the previous section has been used for experiments with different lasers and various configurations. In this section, we show experimental results obtained on a couple of Optospeed LCSH1550-DFB. Such devices are standard DFB telecommunication lasers working at a wavelength $\lambda = 1550$ nm. They were operated at a current $I = 7$–30 mA, for a maximum output power P of about 7 mW. The two lasers were selected among devices built in close proximity on the same wafer, and, after being tuned at the same wavelength by temperature, they exhibited only 1% difference both in the threshold current I_{th} and in the differential efficiency $\mathrm{d}P/\mathrm{d}I$. In the following, we focus on the short cavity, closed loop configuration, which gave the best performances, and exhibits better stability and compactness. The alignment of the setup was made in different steps. First, the laser-fiber distance was trimmed for the maximum chaos amplitude of the master, since, as it is well known, the effect

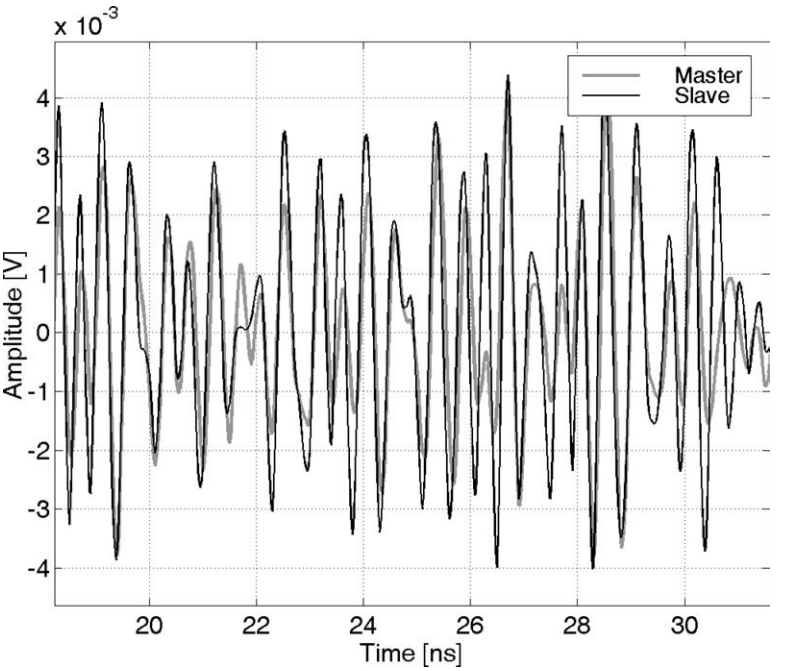

Fig. 6. Time series showing master/slave synchronization in the time domain.

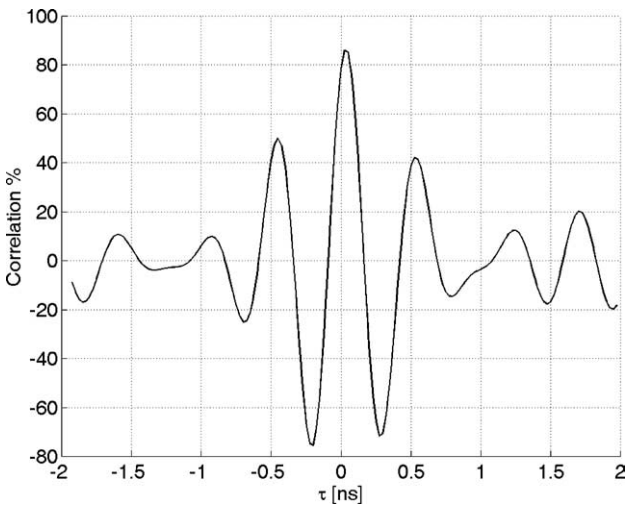

Fig. 7. Correlation diagram of synchronized master and slave.

strongly depends on the optical phase [13] and may even disappear for certain phase values. Then, accurate trimming of the phase of the slave was performed, since the synchronization quality is extremely sensitive to the relative phase of the laser cavities [4,5]. Finally, the injection level of the master into the slave was optimized. The fiber path connecting the two lasers has been progressively increased in length, starting from the 2 m of single-mode reduced-core (SMR) fiber of the isolator and coupler pigtails, then adding a piece of 500 m of SMR, and finally a 1300 m reel (radius $R = 10$ cm) of single mode fiber (SM). The last one introduced a significant attenuation due to bending and to the core radius mismatch with respect to the SMR fiber. Some fiber pieces were directly fusion spliced to each other, others were joined after splicing to connectorized patch cables. We also introduced two additional low-quality splices (0.3 dB loss). Finally an EDFA amplifier was included to compensate for the overall loss introduced by the passive components. All added devices were positioned after the optical isolator, as clearly shown in Fig. 2, to avoid unwanted back-injection. Figs. 3–7 illustrate the synchronization quality of master and slave with the above described fiber connection, for a cavity length $L = 30$ mm. It is interesting to observe that the performance was essentially the

same as in the back to back experiments (pigtails only), as long as the optical amplification compensated for the fiber losses. The synchronization quality could be even improved when optical amplification increased the injection level from the master into the slave. Similar results were found by substituting the EDFA with a semiconductor optical amplifier. Fig. 3 shows a comparison of master and slave RF spectra in optimized conditions. It must be pointed out that synchronization quality cannot be directly inferred from these diagrams, because it is not difficult to obtain almost identical spectra from similar lasers even if they are not optically connected. For this reason, it is important to consider the difference between the chaotic waveforms, and in Fig. 4 we show its spectrum (lower curve), along with the spectrum of the sum, for comparison (upper curve). From this figure, a separation of about 10 dB between the two diagrams demonstrates the good synchronization quality. As already stated, the chaos difference may be obtained by changing the sign of the amplification of one of the channels following PD2 or PD3. Alternatively, if the spectrum is not fractionally too large (or if we focus on a relatively small portion of spectrum), it is possible to change the length of the delay line in order to get a phase difference π between the two signals, i.e., a path difference of half the wavelength of the central frequency of the RF waveform. An interesting possibility, for fast trimming of the setup, is to select the length of the delay line so as to work with a relatively large differential path. In this case, different portions of the two chaos spectra have different relative phase difference, and the spectrum of their combination exhibits several maxima and minima, as shown in Fig. 5. Thus the system can be trimmed by maximizing the depth of the spectrum 'valleys', which is far easier than observing the sum and the difference at different times. In Fig. 5 a comparison is made between the open loop and the closed loop configuration (short cavity) for the same experimental conditions. It appears that the closed loop gives better synchronization performances; it requires, however, a more accurate trimming. Synchronization quality can be also appreciated by a direct comparison of portions of the chaotic waveforms of master and slave in the time domain, as shown in Fig. 6. As it appears from the figure, synchronization is not complete, as it usually happens in practical cases. From the time series, the master-slave correlation has been also computed as a function of the differential delay τ, and the result is plotted in Fig. 7. A correlation of more than 80% was measured for zero differential delay, and is reduced as τ increases, showing a quasi-periodical trend; this was to be expected, as chaos, differently from white noise, has a non-zero correlation time.

4. Transmission experiments

Transmission tests have been performed with the different methods shown in Fig. 2, namely, CSK, ACM, CM. The first scheme was implemented by modulating the pump current of the laser; the second by using a third laser at the same wavelength as the master/slave couple (to prevent an eavesdropper from extracting the message by optical filtering); the third by a pigtailed Lithium Niobate amplitude modulator, inserted after the optical isolator. In all cases, the fiber link between the master and the slave was the same as in synchronization experiments, including the optical amplifier. The different methods for signal encoding

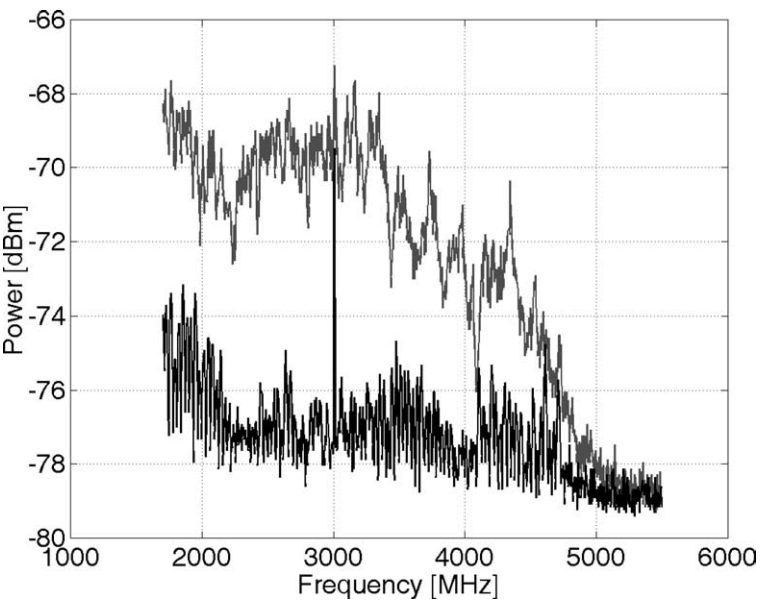

Fig. 8. Example of signal transmission and detection in the frequency domain: CSK scheme. Upper trace: master with hidden message; lower trace: master/slave difference with extracted message.

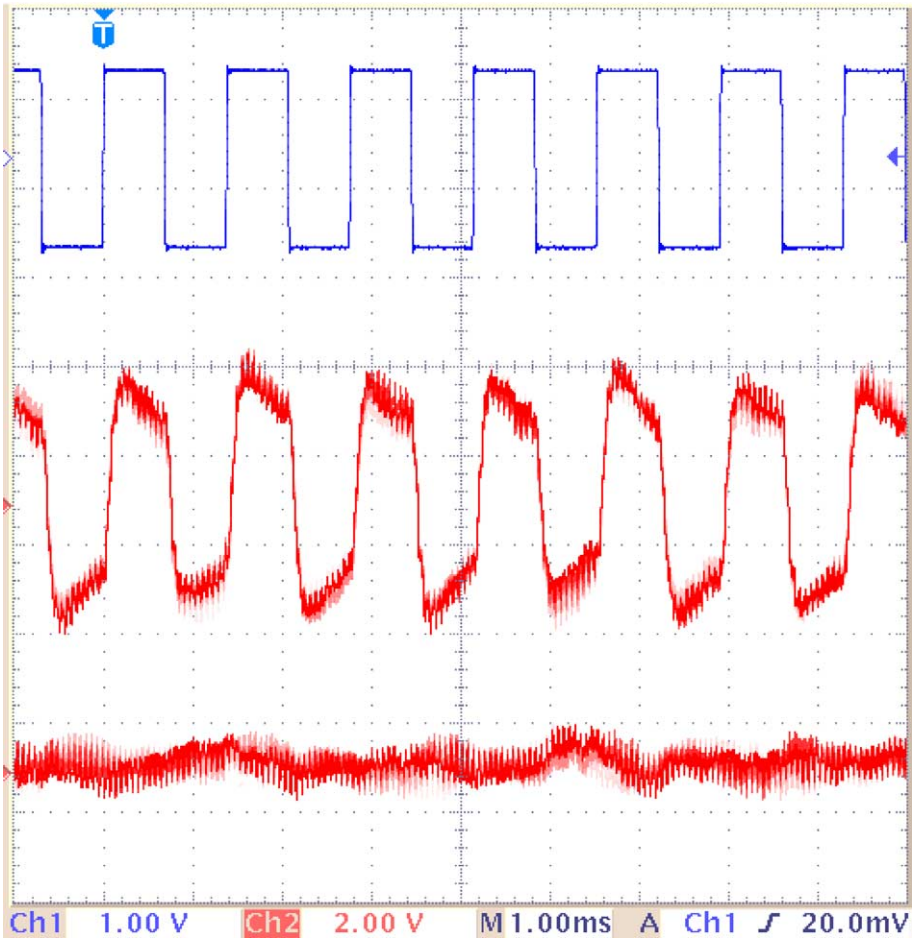

Fig. 9. Example of signal transmission and detection in the time domain: low frequency PM scheme. Transmitted signal (upper trace) can be detected from master-slave difference (middle trace); signal cannot be detected from master alone (lower trace).

have been studied theoretically and numerically and their peculiarities and performances have been pointed out [9]. From the experimental point of view a major issue determining the performances of all methods is chaos amplitude, which put a limit to the signal amplitude which may be safely masked, and, thus, to the obtainable S/N ratio after detection. For example, an ACM transmission experiment is shown in Fig. 8: a sinusoidal signal is hidden within the master chaos (upper trace); the signal is then recovered by making the difference between the master and the synchronized slave outputs (lower trace).

Very similar diagrams have been obtained in our setup with the other two encoding methods, since the maximum allowable amplitude, before the signal may be spotted by inspection of the composite spectrum, is the same. Still another possibility, which has not been shown in Fig. 2 for simplicity, is phase modulation (PM) of chaos. This approach exploits the well known dependence of chaos on the optical phase. It has been observed [4,5] that small variations of the external cavity length, around a suitable bias point, hardly affect the RF spectrum of chaos, so that an eavesdropper cannot detect a message which modulates the optical phase. However, the correlation degree between master and slave strongly depends on the relative phase; thus, their difference varies in amplitude allowing the listener to extract the hidden signal at the receiver. To exploit such principle a scheme was proposed where a relatively large digital signal switches the master/slave system from synchronization to de-synchronization (ON–OFF Chaos Phase Shift Keying [4,5]). Alternatively, transmission of a small analog signal may be considered. The PM scheme has been implemented in our setup by inserting two Lithium Tantalate electro-optical crystals between each laser and its fiber. The crystals were $1 \times 2 \times 10$ mm in length, they had a ARC treatment, and their refractive index variation, for a voltage change of about 750 V, corresponded to a modulation of the cavity length of half a wavelength. Only the crystal of the master was actuated, that of the slave being inserted just to work with identical external cavities at rest. An example of application of such scheme is shown in Fig. 9 for a low amplitude, low frequency (700 Hz) square-wave. The upper trace represents the transmitted signal. The trace at the middle is the output of an envelop detector fed by the difference

of the synchronized master and slave outputs. For comparison, the lower trace represents the output of the envelop detector fed by the master output only, from which the signal cannot be extracted.

5. Conclusions

We have presented a fiber optics setup for experiments on chaos generation, chaos synchronization and optical chaotic cryptography. Some experimental results have been presented for the short cavity, closed loop configuration.

Acknowledgements

This work was supported by the European Community under Contract IST 2000 29683 (OCCULT Project). The authors wish to thank Optospeed (CH) for supplying the selected laser couples, the amplified photodetectors and the semiconductor optical amplifier.

References

[1] S. Donati, C.R. Mirasso, IEEE J. Quantum Electron. 38 (2002) 1138.
[2] J.-P. Goedgebuer, P. Levy, L. Larger, C.-C. Chen, W.T. Rhodes, IEEE J. Quantum Electron. 38 (2002) 1178.
[3] S. Sivaprakasam, P.S. Spencer, P. Rees, K.A. Shore, IEEE J. Quantum Electron. 38 (2002) 1155.
[4] T. Heil, J. Mulet, I. Fisher, C.R. Mirasso, M. Peil, P. Colet, W. Elsasser, IEEE J. Quantum Electron. 38 (2002) 1162.
[5] M. Peil, T. Heil, I. Fischer, W. Elsässer, Phys. Rev. Lett. 88 (2002) 174101.
[6] J. Ohtsubo, IEEE J. Quantum Electron. 38 (2002) 1141.
[7] V. Annovazzi-Lodi, S. Donati, A. Sciré, IEEE J. Quantum Electron. 33 (1997) 1449.
[8] C. Mirasso, P. Colet, P. Garcia-Fernandez, IEEE Phot. Technol. Lett. 8 (1996) 299.
[9] J. Liu, H. Chen, S. Tang, IEEE J. Quantum Electron. 38 (2002) 1184.
[10] R. Lang, K. Kobayashi, IEEE J. Quantum Electron. 16 (1980) 347.
[11] V. Annovazzi-Lodi, S. Donati, A. Sciré, IEEE J. Quantum Electron. 32 (1996) 953.
[12] V. Annovazzi-Lodi, S. Donati, A. Sciré, IEEE J. Quantum Electron. 38 (2002) 1171.
[13] T. Heil, I. Fisher, W. Elsasser, A. Gavrielides, Phys. Rev. Lett. 87 (2001) 243901.
[14] J. Houdian, G. Huyet, J.G. McInerney, Opt. Comm. 199 (2001) 175.
[15] S. Donati, S. Merlo, J. Optics 29 (1998) 156.
[16] V. Annovazzi-Lodi, S. Merlo, M. Norgia, IEEE Trans. Mechatron. 6 (2001) 1.