Message Encryption by Phase Modulation of a Chaotic Optical Carrier

Valerio Annovazzi-Lodi, *Senior Member, IEEE*, Mauro Benedetti, *Member, IEEE*,
Sabina Merlo, *Senior Member, IEEE*, Toni Perez, Pere Colet, and Claudio R. Mirasso

***Abstract*—We present a numerical and experimental evaluation of message encryption by phase modulation, using a chaotic optical carrier generated by a laser subject to delayed optical feedback. This method offers better security than the conventional amplitude masking, where the signal is simply added to the chaotic waveform.**

***Index Terms*—Chaos, communication systems, cryptography, phase modulation.**

I. Introduction

OPTICAL chaotic cryptography is a hardware technique for secure transmission which makes use of a couple of lasers operating in the chaotic regime [1]–[9]. Chaos-based encryption uses a chaotic laser [“master” laser (ML)] at the transmitter side to hide the information to be transmitted (the message); another laser [“slave” laser (SL)], at the receiver, allows for message recovery. The extraction of the hidden message from chaos is based on synchronization between ML and SL, i.e., on the generation of the same chaotic waveform at both ends of the channel. Synchronization can be only obtained under suitable conditions, by injecting part of the ML output into the SL, and relies on two lasers being closely matched, which ensures security. The cryptographic key consists in the set of parameters of the two matched lasers. In the basic scheme (“chaotic masking”), chaos is simply added to the message [1], [2], [4], [6], and transmission of real signals has been recently demonstrated [4].

Another approach, first proposed in [5], exploits the strong dependence of synchronization on the relative phase between the external cavities of ML and SL. Indeed, a phase variation of the ML external cavity, which is small enough to be undetectable by observation of the chaotic waveform or of its spectrum, can substantially affect the correlation between the two laser outputs [8]. Thus, if the ML phase is modulated by a message, the latter can be extracted by transferring the induced variation of the correlation coefficient into amplitude modulation. This can be easily done by taking the difference between the phase-modulated (PM) chaotic waveform coming from the transmitter and the chaotic waveform from the receiver, as in the standard masking scheme [3], [4]. Moreover, the system must operate at a suitable bias point, which, for analog signal transmission, is halfway between maximum and minimum correlation level for best linearity. An important characteristic of this method is that it requires a “closed loop” scheme for detection, i.e., the SL must be routed to chaos by an external cavity identical to that of the master. On the other hand, with chaos masking, the message can be extracted (with a lower signal-to-noise (S/N) ratio) also by the less critical “open loop” scheme, where the SL has no feedback and can be less strictly matched to the ML [2].

Though phase modulation cryptography has been already studied theoretically, it has been demonstrated experimentally only in the quasi-static regime [5]. One problem in working with real signals is that signal detection by waveform difference results in a relatively complex setup, which is more critical to align than in the case of standard masking; an accurate delay compensation is required between the ML and SL chaotic waveforms to get the true difference [3]. To that purpose, an RF delay line may be used on either ML or SL photodetected signal, as in [3] and [4]. In this letter we show, however, that under suitable operating conditions, the message can be detected simply by direct observation of the output of the SL, by using a single photodetector and RF amplifier, which requires neither delay trimming or matching of amplifiers and RF lines. With this more manageable scheme, secure transmission of a frequency-modulated (FM) carrier has been demonstrated.

II. Numerical Analysis and Experiments

The arrangement for the phase modulation experiment is shown in Fig. 1, and consists of a typical master/slave configuration. Each laser is driven to chaos by back-reflection from the fiber tip positioned in front of its launching lens [4], which defines an external cavity of about 10 cm. This short-cavity scheme is compact and mechanically stable, as required for low phase drift. A $LiTaO_3$ crystal is included in the master cavity and is used as a phase modulator to insert the message; the crystal in the slave cavity only keeps symmetry, as required for efficient synchronization. To simplify the numerical analysis, the laser and external cavity parameters were taken to be identical for both ML and SL. The equations for the complex

Manuscript received July 6, 2006; revised November 9, 2006. This work was supported in part by MIUR (COFIN 2005), in part by the Spanish MCyT and Feder under Projects TEC2005-07799-C02-01 and FIS2004-00953, and in part by EU Project PICASSO IST-2005-34551.

V. Annovazzi-Lodi, M. Benedetti, and S. Merlo are with the Dipartimento di Elettronica, Universita' di Pavia, I-27100 Pavia, Italy (e-mail: valerio.annovazzi@unipv.it).

T. Pérez, P. Colet, and C. R. Mirasso are with the Departament de Física, Universitat de les Illes Balears and Instituto Mediterráneo de Estudios Avanzados, CSIC-UIB, Campus UIB 07122 Palma de Mallorca, Spain (e-mail: claudio@galiota.uib.es).

Digital Object Identifier 10.1109/LPT.2006.888968

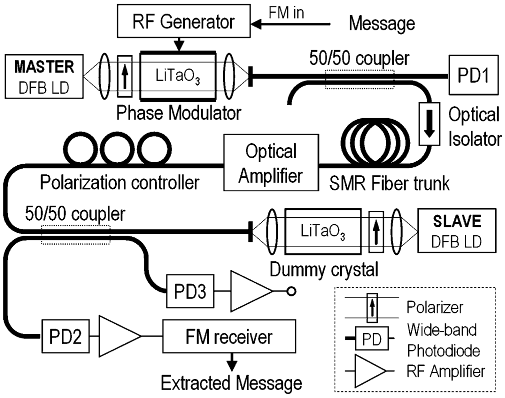

Fig. 1. Transmission setup.

slowly varying electric field E_M of transmitter (ML) and E_S of receiver (SL) are [5]

$$\dot{E}_M(t) = \frac{(1+i\alpha)}{2}\left[G(t) - \frac{1}{\tau_{\text{ph}}}\right]E_M(t) + k_f E_M(t-\tau_f)e^{-i\phi_f(t)} \tag{1}$$

$$\dot{E}_S(t) = \frac{(1+i\alpha)}{2}\left[G(t) - \frac{1}{\tau_{\text{ph}}}\right]E_S(t) + k_f E_S(t-\tau_f)e^{-i\phi_0} + k_c E_M(t-T)e^{-i\phi_c}. \tag{2}$$

Equations (1) and (2) describe the lasers by the linewidth enhancement factor $\alpha = 5.0$, the photon lifetime $\tau_{\text{ph}} = 2.5$ ps, and the modal gain $G = g(N - N_0))/(1 + \sigma|E|^2)$, where $g = 1.8 \times 10^{-8}$ ps^{-1} is the differential gain, $N_0 = 1.0 \times 10^8$ is the carrier concentration at transparency, $\sigma = 1.5 \times 10^{-7}$ is the saturation parameter. The external cavities are modeled by the second terms: $\tau_f = 200$ ps is the feedback delay time, $k_f = 25$ ns^{-1} is the feedback strength, and ϕ is the optical phase, which is constant ($\phi_0 = 3.17$ for our partameter values) for the SL while it is modulated (ϕ_f) in the ML. The last term of the SL equation models the injection from the ML: T, ϕ_c are the propagation time and phase ($\phi_c = T = 0$ in the simulations, as in a back-to-back experiment), $k_c = 70$ ns^{-1} is the coupling coefficient. The equation for carriers N can be found in [5].

Applied phase modulation had the general form $\phi_f = \phi_{0m} + \phi_m \cos(2\pi[f_0 + \Delta f \cos(2\pi f_m t)]t)$, where f_0 is a carrier frequency and f_m is the message frequency, assumed to be of sinusoidal form. As it was observed experimentally, this FM-over-PM scheme is robust to additive noise, consisting mainly of residual chaos at the slave output, which, instead, strongly affects message detection when the chaotic carrier is directly modulated in phase. Numerical results have shown the viability of detection by direct observation of the slave output. Indeed, we have found that, by selecting suitable values of message and carrier amplitude, the FM signal can be efficiently hidden in the ML spectrum, while it is clearly detectable at the SL output.

Typical results obtained in optimized conditions are shown in Figs. 2 and 3. Parameter $\phi_m = 5$, $f_0 = 100$ MHz, $\Delta f = 100$ Hz, and $f_m = 1$ kHz were selected to match the experimental values (see below). In Fig. 2, the master RF spectrum, with the hidden modulated carrier, shows no visible signal. However, the carrier is evident in the SL spectrum of Fig. 3, with its FM modulation (at 1 kHz) highlighted in the inset. The small second-harmonic component may be easily filtered out.

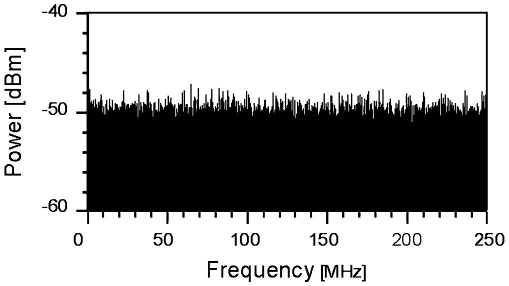

Fig. 2. Simulated master RF spectrum with hidden FM modulated carrier.

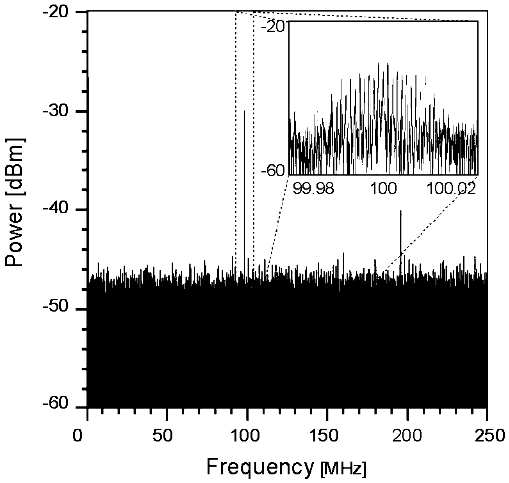

Fig. 3. Simulated slave RF spectrum with the recovered signal (zooming around the carrier frequency is shown in the inset).

Experiments were performed on the setup of Fig. 1. The path between transmitter and receiver was ≈1.2 km of standard telecommunication fiber and, besides splitters, couplers, and joints, it included also a semiconductor optical amplifier, to increase the maximum injection level from master into slave. The optical isolator in Fig. 1 ensures unidirectional injection. Polarizers in front of the lasers select, for both feedback and injection, the same polarization as that of the laser emission. Moreover, the polarizer in the slave was used, together with the polarization controller, to trim the injection level. The laser pair consisted of standard 1-mW distributed feedback telecommunication devices ($\lambda = 1550$ nm), which were selected between first neighbors of the same wafer. Their difference of threshold and differential efficiency were lower than 1%, and their wavelengths were matched within 100 pm by temperature tuning. The characteristics of the chaotic regime of the lasers depend on the operating conditions, such as injection current and feedback level.

Master/slave synchronization was obtained by adjusting the injection current (≈50% above threshold), the alignment, and the temperature of both lasers, as well as the injection level,

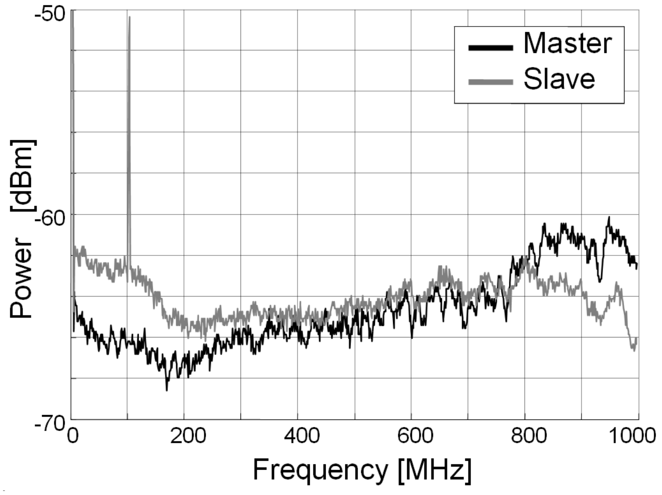

Fig. 4. RF chaos spectra: ML with hidden carrier (black) and SL with extracted carrier (gray). The traces have been separated by a 3-dB attenuator for a better comparison of their shape.

which was of the same order of the feedback level ($10^{-2} - 10^{-3}$ of the laser output power). The two external cavities were also carefully matched. The regimes of the two lasers were compared by observing the outputs of photodiodes PD1 and PD2 by an RF spectrum analyzer. The synchronization level was checked, as explained in [3], by observing (with no delay compensation) the spectrum of the difference of ML (at PD3) and SL (at PD2) outputs.

When the setup was aligned at best, the correlation coefficient between master and slave outputs was ≈ 0.9, in the absence of modulation. The chaos bandwidth was ≈ 5 GHz, limited by the photodiode and amplifier speeds. Transmission experiments were performed by modulating the input voltage of the master $LiTaO_3$ crystal, giving rise to a 100-MHz carrier, modulated on its turn by a 1-kHz message. At the slave output, the carrier was fed to an FM receiver to get the message.

In Fig. 4, the master and slave RF spectra are shown. The FM carrier is not visible in ML spectrum (black line) since it is embedded in chaos; after proper alignment of the setup, however, the recovered carrier becomes clearly visible in the SL spectrum (gray line). In the figure, synchronization was optimized in the 0- to 200-MHz working range and the two traces were separated for easier comparison.

In Fig. 5, the message without encryption (a) can be compared with the recovered message (d) obtained with both ML and SL switched ON, and with the setup properly aligned. Fig. 5(b) (ML and SL OFF) represents the channel noise; Fig. 5(c) (ML ON and SL OFF) is the message as it would be detected by an eavesdropper tapping the fiber. The carrier and the message amplitude were adjusted to reach a compromise between low signal distortion and good S/N ratio; the maximum phase modulation was a small variation ($<2\pi$) around the phase bias ϕ_{0m}, which was also trimmed for the best quality of the recovered message.

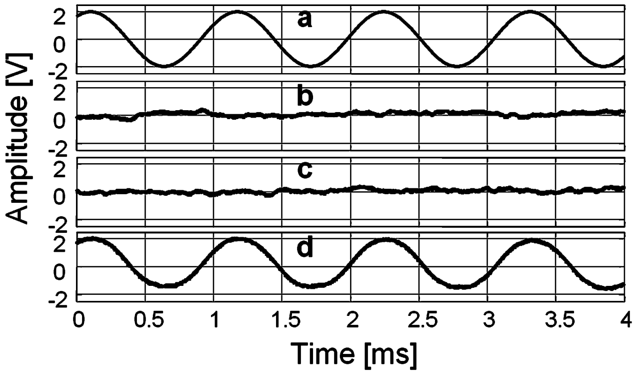

Fig. 5. (a) Sinusoidal message modulating the carrier of Fig. 4; (b) system output with ML and SL OFF; (c) system output with ML ON and SL OFF; (d) recovered message with both ML and SL ON and aligned.

As expected [5], the optimum value of ϕ_{0m} gave partial chaos correlation with no carrier, while trimming for both maximum and minimum chaos correlation resulted into message fading.

In conclusion, we have shown that phase modulation of a chaotic carrier is a viable method for secure transmission in the RF range. Message detection by direct observation of the slave output results in a much more manageable experimental setup. Both the carrier and the modulation frequency of our experiments were determined by the availability of suitable modulators and receivers. Further investigations will be devoted to the evaluation of the intrinsic speed limit (which is expected to be related to the synchronization delay), as well as to the extension of this method to higher frequency signals (including digital signals in baseband).

REFERENCES

[1] S. Donati and C. Mirasso, Eds., “Feature section on optical chaos and applications to cryptography,” *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1138–1196, Sep. 2002.

[2] J. Ohtsubo, “Chaos synchronization and chaotic signal masking in semiconductor lasers with optical feedback,” *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1141–1154, Sep. 2002.

[3] V. Annovazzi-Lodi, M. Benedetti, S. Merlo, and M. Norgia, “Fiberoptics setup for chaotic cryptographic comunications,” *Comptes Rendus de l'Academie des Sciences-Dossier de Physique*, vol. 6, no. 5, pp. 623–631, 2004.

[4] V. Annovazzi-Lodi, M. Benedetti, S. Merlo, M. Norgia, and B. Provinzano, “Optical chaos masking of video signals,” *IEEE Photon. Technol. Lett.*, vol. 17, no. 9, pp. 1995–1197, Sep. 2005.

[5] T. Heil, J. Mulet, I. Fischer, C. R. Mirasso, M. Peil, P. Colet, and W. Elsasser, “ON/OFF phase shift keying for chaos-encrypted communication using external-cavity sermiconductor lasers,” *IEEE J. Quantum Electron.*, vol. 38, no. 9, pp. 1162–1170, Sep. 2002.

[6] L. Larger and J.-P. Goedgebuer, Eds., “Special Issue on Criptography Using Optical Chaos,” *Comptes rendus de l’Academie des Sciences-Dossier de Physique*, vol. 5, pp. 609–681, 2004.

[7] A. Argyris *et al.*, “Chaos-based communications at high bit rates using commercial fiber-optic links,” *Nature*, vol. 438, pp. 343–346, 2005.

[8] M. Peil, T. Heil, I. Fischer, and W. Elsäßer, “Synchronization of chaotic semiconductor laser systems: A vectorial coupling-dependent scenario,” *Phys. Rev. Lett.*, vol. 88, pp. 174101–04, 2002.

[9] S. Peters-Flynn, P. S. Spencer, S. Sivaprakasam, I. Pierce, and K. A. Shore, “Identification of the optimum time-delay for chaos synchronization regimes of semiconductor lasers,” *IEEE J. Quantum Electron.*, vol. 42, no. 4, pp. 427–434, Apr. 2007.