Chaos Shift-Keying Encryption in Chaotic External-Cavity Semiconductor Lasers Using a Single-Receiver Scheme

Claudio R. Mirasso, Josep Mulet, and Cristina Masoller

***Abstract*—In this letter, we numerically show that chaos shift-keying (CSK) encryption can be achieved by using a single receiver, thus providing a better performance when comparing with the traditional CSK scheme based on two receivers. We analyze the rate equation model for two unidirectionally coupled single-mode external-cavity semiconductor lasers operating in a chaotic regime. The message is encoded in the emitter by slightly varying its injection current. We find that under appropriate conditions, the receiver laser synchronizes to the chaotic emitter, filtering the encoded message and allowing message extraction.**

***Index Terms*—Injection-locked oscillator, nonlinear optics, semiconductor lasers (dynamics).**

I. Introduction

THE ISSUE of enhancing the privacy in transmitted data has attracted the attention of many researchers in the last years. Historically, software encryption has been used since a long time ago. However, in the last decade it has been proposed that a complementary technique to improve privacy could be implemented by codifying at hardware level. This new technique requires the use of devices (emitters and receivers) operating in a chaotic regime [1]. Different chaotic synchronization schemes and their applications to encoded communications have been proposed using electronic circuits, solid state lasers, fiber ring lasers, semiconductor lasers [2]–[14], and microchip lasers [16]. Recent experiments with semiconductor lasers, [3]–[6], have shown the feasibility of synchronizing the so-called hyper-chaos, i.e., attractors with a very large number of degrees of freedom. This fact opens the possibility of using such schemes for information encryption at hardware level.

Different communication schemes have been proposed for encoding the message: chaos masking (CMA), chaos modulation (CMO), chaos shift keying (CSK), and ON–OFF shift keying (OOSK). In the CMA scheme, the message is not really encoded on the carrier signal but just added to it, while in the CMO scheme [2], [8], the carrier is modulated by the message. On the other hand, the CSK scheme [9] is based on the definition of two clearly separated states for bits "1" and "0," while in the OOSK the system synchronized either to a bit "1" or "0" being unsynchronized for the other bit [10], [11]. In all these methods, the intensity of the message has to be small enough to avoid detection in the time or frequency domains. To the best of our knowledge, in the proposed CSK schemes the decoder consist of two replicas of the transmitting systems, each one configured for detecting either a bit "1" or "0" [9]. Although more secure, this scheme becomes more complicated to implement than the CMA and CMO schemes, and also the bit rate is smaller because the period of modulation can not be smaller than the time needed to entrain each of the states at the receiver, as it would also happen in the OOSK scheme. In this work, we show that CSK encryption can also be implemented with a single receiver and that a high degree of synchronization can be achieved for both bits "1" and "0" under this condition. Moreover, we show that the message can be decoded and the bit rate can be increased up to the gigabits rates, thus, significantly improving the performance of the communication system.

Manuscript received October 1, 2001; revised December 10, 2001. This work was supported by the Spanish MCyT under Project CONOCE BFM2000-1108 and the European Commission under Project OCCULT IST-2000-29683. C. Masoller was supported in part by PEDECIBA, in part by CSIC (URUGUAY), and in part by the Universitat de les Illes Balears.

C. R. Mirasso is with the Departament de Física, Universitat de les Illes Balears, E-07071 Palma de Mallorca, Spain (e-mail: claudio@imedea.uib.es).

J. Mulet is with the Instituto Mediterráneo de Estudios Avanzados, E-07071 Palma de Mallorca, Spain.

C. Masoller is with the Instituto de Física, Facultad de Ciencias, Universidad de la República, Igua 4225, Montevideo 11400, Uruguay.

Publisher Item Identifier S 1041-1135(02)01863-3.

II. The Model

For our analysis, we use as the carrier the chaotic output of a single-mode semiconductor laser subjected to an external optical feedback [Master Laser (ML)]. The digital message is encoded by a small variation of its injection current around a bias value. The receiver [Slave Laser (SL)] operates under the same conditions except that its injection current takes a constant value. The transmitter and receiver lasers are consider as identical. The mirrors are positioned such that the external cavity length is the same for both lasers. The output of the transmitter laser is unidirectionally injected into the receiver laser via an optical isolator. We model both ML and SL by using the rate equations for the complex slowly varying amplitude of the electrical field E and minority carriers inside the cavity N, that read [2]

$$\dot{E}_{t,r}(t) = \frac{1}{2}(1+j\alpha_{t,r})\left(G_{t,r} - \frac{1}{\tau_{t,r}}\right)E_{t,r} + F_{E_{t,r}}(t) + \gamma E_{t,r}(t-\tau)e^{-j\omega\tau} + \kappa_r E_t(t-\tau_c)e^{-j\omega\tau_c} \quad (1)$$

$$\dot{N}_{t,r}(t) = \frac{I_{t,r}(t)}{e} - \frac{1}{\tau_{n_{t,r}}}N_{t,r} - G_{t,r}|E_{t,r}|^2 \quad (2)$$

$$G_{t,r}(t) = \frac{g(N_{t,r} - N_{o_{t,r}})}{1 + s|E_{t,r}(t)|^2} \quad (3)$$

with $I_t(t) = I_b + I_m B(t)$ where $B(t) = 1/2\ (-1/2)$ for a "1" ("0") bit and $I_r(t) = I_b$. By modulating the current with the function $B(t)$, we do not have two different chaotic attractors, as is the case of conventional CSK encryption, but two states of the same attractor associated to the two levels of the transmitter injection current. The term $\kappa_r E_t(t-\tau_c)e^{-j\omega\tau_c}$ in (1) exists only for the slave laser, and accounts for the light injected from the master laser. For simplicity, we assume that both lasers operate at the same wavelength and have the same internal parameters. The effect of a mismatch between laser parameters has been already considered and it has been shown that for slightly differences the lasers still synchronize [8] , [9], [12]. The parameters are $g = 1.5 \times 10^{-8}$ ps^{-1} is the differential gain, $s = 5 \times 10^{-7}$ is the gain saturation coefficient, $\alpha = 5$ is the linewidth enhancement factor, $e = 1.602 \times 10^{-19}$ C is the electronic charge, $\tau_n = 2$ ns is the carrier lifetime, $\tau_t = 2$ ps is the photon lifetime. The photon lifetime of the receiver is $\tau_r = 1.91$ ps, slightly smaller to compensate for the injected power. $N_o = 1.5 \times 10^8$ is the carrier number at transparency, $\gamma = 30$ ns^{-1} is the feedback rate, $\kappa_r = (1 - r_o^2)\xi/(\tau_{\text{in}} r_o) = 80$ ns^{-1} is the coupling rate, $r_o = 0.556$ is the field reflectivity at the laser facet, $\tau_{\text{in}} = 8$ ps is the laser round-trip time, and $\xi = 0.51$ account for additional losses; $\tau = 0.3$ ns is the external cavity round-trip time and $\tau_c = 1$ ns is the time that the light takes to go from the ML to the SL. The bias current is $I_b = 44$ mA (the threshold current is $I_{\text{th}} \approx 15$ mA) and $\omega = 1.2 \times 10^3$ ps^{-1} is the free-running emission frequency. Equations (1)–(3) are written in the reference frame where the free-running emission frequencies at threshold are zero when neglecting spontaneous emission. $F_{E_{t,r}}(t)$ are Langevin noise sources that describe spontaneous emission processes. They have zero mean and correlation $\langle F_{E_i}(t) F^*_{E_j}(t')\rangle = 4\beta N_{t,r}\delta_{i,j}\delta(t-t')$, $\beta = 10^{-7}$ ns^{-1} being the spontaneous emission rate.

III. Results

A pseudorandom sequence of input bits in the nonreturn-to-zero scheme is superimposed on the bias current of the ML. As a first example in Fig. 1, we plot the output power of the ML without (panel a) and with (panel b) the input message. The output power of the SL is shown in panel (c), while the 2-Gb/s digital message with an amplitude of 2 mA is shown in panel (d) together with the recovered message (after being filtered). The output of the SL synchronizes with the output of the ML lagged in time, with a lag time $-\tau_c$ which in all figures is compensated for. By simply subtracting the input and output of the SL, and after using a standard filtering process, the message is clearly recovered.

In Fig. 2, we plot the synchronization diagram, i.e., the output power of the SL versus the output power of the ML. When no message is included [panel (a)] the synchronization is almost perfect and a clear 45° straight line is obtained. When the message is added to the ML [panel (b)] the line becomes broaden although maintaining a reasonably small width. This broadening comes from the fact that the ML current changes from $I_b + I_m/2$ to $I_b - I_m/2$ giving rise to two slightly separated parallel straight lines that for this small modulation amplitude are indistinguishable. We also show in Fig. 2(c) and (d) the synchronization diagram when a 6 and 10 mA amplitude message is added to the SL. In these cases, it can be seen how the synchronization degrades associated with the appearance of two parallel lines. We will discuss this point with more detail below. In Fig. 3, we plot the message and its recovery counterpart, after being filtered, for three different modulation frequencies. It can be seen that the message is always very well recovered allowing a clear distinction between bits "1" and "0." Panel (c) displays the case of a bit rate of 3 Gb/s. Although this frequency is high (the relaxation oscillation frequency for a laser with these parameters is ~4 GHz) the message can still be recovered. However, we have to stress that for these parameters this is the maximum bit rate for which we can extract a clear message.

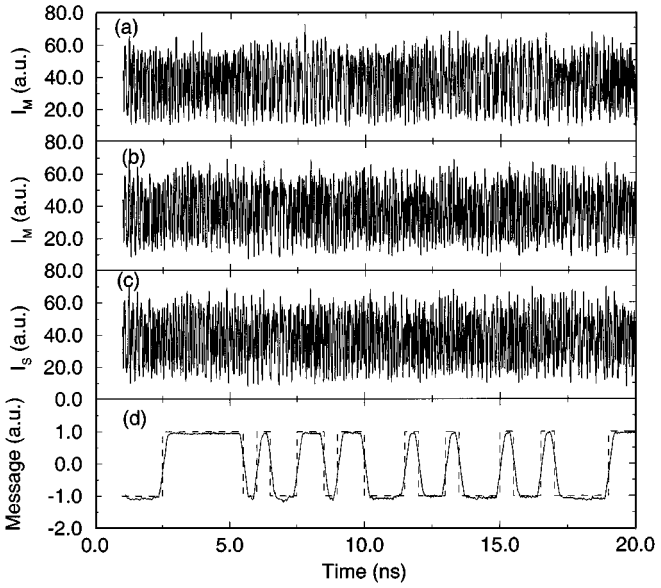

Fig. 1. Panels (a)–(c) output power of ML and SL versus time. (a) ML without message. (b) ML power with a 2-Gb/s message encoded. (c) SL power output. Panel (d) 2-Gb/s message. Dashed line: Original message. Solid line: Recovered message after filtering process.

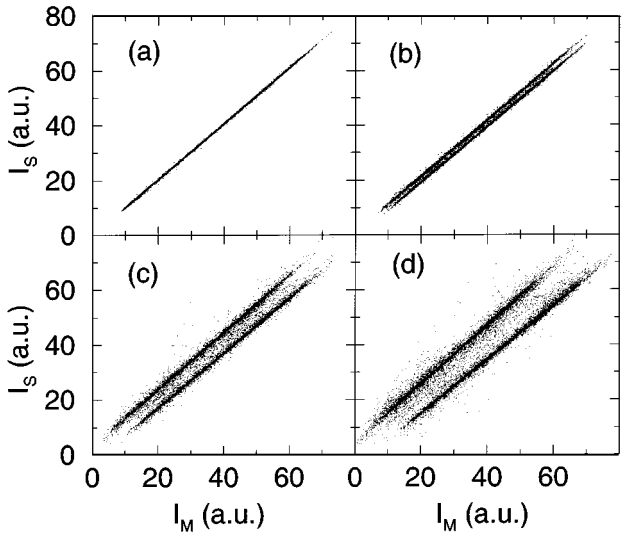

Fig. 2. Synchronization diagram, i.e., the output power of ML versus SL. Both ML and SL operate with constant current (a), a 2-Gb/s message, with $I_m = 2$ mA in (b), $I_m = 6$ mA in (c), and $I_m = 10$ mA in (d) is encoded through a time variation of the injection current of the ML.

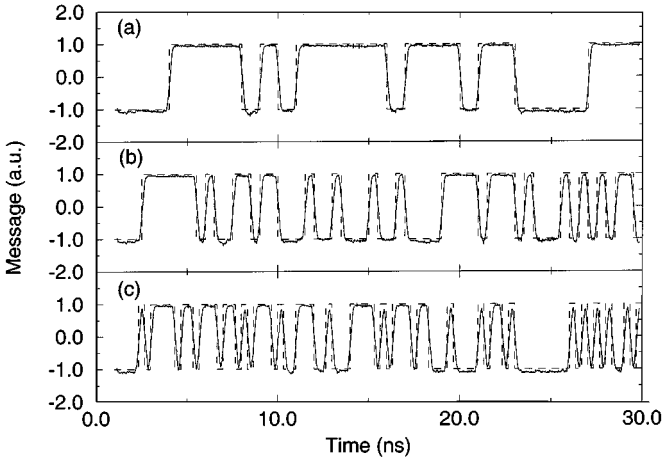

Fig. 3. Recovered message with amplitude $I_m = 2$ mA for different bit rates: (a) 1 Gb/s, (b) 2 Gb/s, and (c) 3 Gb/s. Dashed line: Original message. Solid line: Recovered message after filtering.

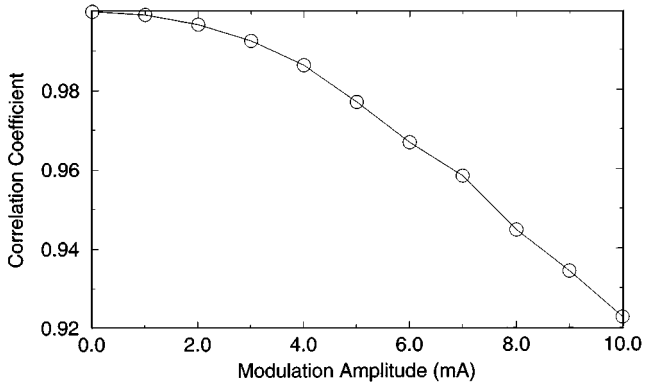

Fig. 4. Correlation coefficient versus modulation amplitude for a bit rate of 2 Gb/s.

As was already anticipated, the fact that we modulate the ML injection current between two values gives rise to two lines in the synchronization diagram. If the amplitude is small enough (for our parameter values $\lesssim$2 mA) these two lines cannot be resolved in the synchronization plot. However, as the modulation amplitude is increased the two lines become more separated and the synchronization degrades. Moreover, for large amplitudes it is already possible to recognize the message on the top of the chaotic carrier. In Fig. 4, we plot the correlation coefficient between the ML and SL intensities, which is a measure of the degree of synchronization. It can be seen that the correlation coefficient is larger than 0.92 even for modulation amplitude of 10 mA. This is due to the large value of the optical coupling used, while for lower values of κ_r the quality of the synchronization degrades. Frequent bursts of desynchronization occur which lead to a lower correlation coefficient and to a lower quality of message recovery.

IV. Conclusion

We have numerically demonstrated that it is possible to encrypt a message in a chaotic output of a single-mode external-cavity semiconductor laser within the CSK scheme using a single receiver. When the injection current of the emitter slightly modulated (with an amplitude $\lesssim$5% of the bias current) we are able to encode/decode a digital message. It is important to maintain the modulation amplitude below the limit in order to prevent decryption of the message by filtering processes. The message can be simply recovered by subtracting the input and output of the receiver and using a standard filtering technique. This scheme allows for a robust and fast encoding of the message, being the largest bit rate for robust message decoding (3 Gb/s for our parameter values) below (but of the order of) the relaxation frequency of the emitter.

References

[1] L. M. Pecora and T. L. Carroll, "Driving systems with chaotic signals," *Phys. Rev. A*, vol. 44, pp. 2374–2383, 1991.
[2] C. R. Mirasso, P. Colet, and P. García-Fernández, "Synchronization of chaotic semiconductor lasers: Application to encoded communications," *IEEE Photon. Technol. Lett.*, vol. 8, pp. 299–301, Feb. 1996.
[3] J. P. Goedgebuer, L. Larger, and H. Porte, "Optical cryptosystem based on synchronization of hyperchaos generated by a delayed feedback tunable laser diode," *Phys. Rev. Lett.*, vol. 80, pp. 2249–2252, 1998.
[4] P. Spencer, C. R. Mirasso, P. Colet, and A. Shore, "Modeling of optical synchronization of chaotic external-cavity VCSELs," *IEEE J. Quantum Electron.*, vol. 34, pp. 1673–1679, Sept. 1998.
[5] I. Fischer, Y. Liu, and P. Davis, "Synchronization of chaotic semiconductor laser dynamics on sub-ns timescales and its potential for chaos communication," *Phys. Rev. A*, vol. 62, 011 801(R), 2000.
[6] H. Fujino and J. Ohtsubo, "Experimental synchronization of chaotic oscillation in external cavity semiconductor lasers," *Opt. Lett.*, vol. 25, pp. 625–627, 2000.
[7] A. Sánchez-Díaz, C. Mirasso, P. Colet, and P. García-Fernández, "Encoded Gbit/s digital communications with synchronized chaotic semiconductor lasers," *IEEE J. Quantum Electron.*, vol. 35, pp. 292–297, Mar. 1999.
[8] V. Annovazzi-Lodi, S. Donati, and A. Scire, "Synchronization of chaotic injected-laser systems and its application to optical cryptography," *IEEE J. Quantum Electron.*, vol. 32, pp. 953–959, June 1996.
[9] J. K. White and J. V. Moloney, "Multichannel communication using an infinite dimensional spatiotemporal chaotic system," *Phys. Rev. A*, vol. 59, pp. 2422–2426, 1999.
[10] L. Rogister, A. Locquet, D. Pieroux, P. Mégret, O. Deparis, and M. Blondel, "Cryptographic scheme using chaotic laser diodes subject to incoherent optical feedback," *Proc. SPIE*, vol. 4283, pp. 379–389, 2001.
[11] C. Mirasso, "Applications of semiconductor Lasers to secure communications," in *Fundamental Issue of Non-Linear Dynamics*, B. Krauskof and D. Lenstra, Eds: American Institute of Physics, 2000.
[12] A. Locquet, F. Rogister, M. Sciamanna, P. Mégret, and M. Blondel, "Two types of synchronization in unidirectionally coupled chaotic external-cavity semiconductor lasers," *Phys. Rev. E*, vol. 64, 045 203(R), 2001.
[13] L. Rahman, G. Li, and F. Tian, "Remote synchronization of high-frequency chaotic signals in semiconductor lasers for secure communications," *Opt. Commun.*, vol. 138, pp. 91–94, 1997.
[14] H. F. Chen and J. M. Liu, "Open-loop chaotic synchronization of injection-locked semiconductor lasers with gigahertz range modulation," *IEEE J. Quantum Electron.*, vol. 36, pp. 27–34, Jan. 2000.
[15] A. Uchida, M. Shinozuka, T. Ogawa, and F. Kannari, "Experiments on chaos synchronization in two separate microchip lasers," *Opt. Lett.*, vol. 24, pp. 890–892, 1999.
[16] P. Spencer and C. R. Mirasso, "Analysis of optical chaos synchronization in frequency-detuned external cavity VCSELs," *IEEE J. Quantum Electron.*, vol. 35, pp. 803–809, May 1999.
[17] S. Sivaprakasam and K. A. Shore, "Message encoding and decoding using chaotic external-cavity diode lasers," *IEEE J. Quantum Electron.*, vol. 36, pp. 35–39, Jan. 2000.