Optical Cryptosystem Based on Synchronization of Hyperchaos Generated by a Delayed Feedback Tunable Laser Diode

Jean-Pierre Goedgebuer,* Laurent Larger,* and Henri Porte*

GTL-CNRS Telecom, UMR CNRS 6603, Georgia Tech Lorraine, 2-3 rue Marconi, 57070 Metz, France

(Received 22 August 1997)

We propose a method for encrypting a signal within the high dimensional chaotic fluctuations of the wavelength from a delayed feedback tunable laser diode. Decoding is performed remotely by using a slave laser diode fully synchronized with the master one. No additional synchronization channel is required. [S0031-9007(98)05424-6]

PACS numbers: 89.70.+c, 05.45.+b

Secure communications based on chaos have been investigated for some years, especially in the area of radiofrequency transmissions. Signal encoding and decoding is achieved using a carrier whose amplitude fluctuates chaotically. Compared with conventional data encryption techniques in which the key is a pseudorandom binary number that controls the encryption algorithm, but which is slow, chaos is used as a coding key embodied directly in the structure of the carrier. At least two classical methods have been demonstrated for communicating with chaos [1]. The first method due to Ott, Grebogi, and Yorke [1] utilizes controlling chaos. The dynamics of a chaotic oscillator is made to follow prescribed orbits in the attractor by using small perturbations, thus allowing a message to be encoded in the chaotic wave form. A very different concept developed by Pecora and Carroll [1] uses the idea of synchronized chaos for secure communications. In this case, a small information-bearing signal is masked by a large chaotic signal. The chaotic code-generating system is divided in two subsystems, namely, the master and the slave. The slave is replicated at the receiver. The master subsystem is used to synchronize the two slave subsystems. The message signal is added to the chaotic signal generated by the slave subsystem at the transmitter and this composite signal is transmitted to the receiver. When the two subsystems are synchronized, the message can be reproduced by subtracting the chaotic part of the composite signal. So far most of the studies were implemented with electrical circuits featuring low dimensional attractors, such as the double scroll or Chua's attractor that has a single positive Lyapunov exponent [2]. The simple chaotic processes thus obtained can, however, be defeated by an eavesdropper without the synchronized receiver, using unmasking signal processing techniques which work well for simple chaotic systems [3]. One way to solve this security problem is by using hyperchaotic systems with multiple positive Lyapunov exponents to mask the message. A recent theoretical work [4] indicates the possibility of synchronizing hyperchaotic chaos with just one transmitted signal. Practical realizations remain, however, to be developed. The question of optical synchronization of chaos has also been studied in optics, but results deal mostly with numerical simulations [5] except some unique demonstrations of control of laser chaos and digital encoded transmission [6]. When talking about chaos in optics, it looks natural to look for nonlinearities induced by optical power. It is probably the reason why implementing optical chaotic cryptosystems poses severe problems which often require an accurate control of the instabilities and of the power-induced nonlinearities. Our objective is the effective implementation of a high dimensional chaotic system for optically encoded communications. It is achieved with a delayed feedback chaotic generator which is known to produce high dimensional chaos [7]. Since there is no rigorous analysis for synchronization of delay-differential equations, we used a way which is different from Pecora and Carroll. We also show that we can use advantageously the wavelength, rather than the power, to produce an optical chaos whose parameters can be controlled very easily both at the transmitter and at the receiver. The latter is used to obtain a chaos replication without a synchronization channel, in a way which seems specific to delayed feedback systems. We were surprised by the quality and robustness of the chaos replication thus attained. The method was checked with chaotic signals with a dimension estimated to be of the order of 5×10^2.

Chaos replication—We assume the transmitter to be a delayed feedback chaotic system ruled at time t by a difference-differential equation of the form

$$x(t) + \tau\, dx(t)/dt = \beta F[x(t - T)] + f(t)\,, \quad (1)$$

where β is the bifurcation parameter, F is a nonlinear feedback function with a time retardation T, and τ the time response of the system. We take $f(t)$ in the form $f(t) = A[s(t) + \tau\, ds/dt]$, with $s(t)$ the message to be encrypted and A an attenuation parameter. Let the receiver equation be written in the form of Eq. (1), except that the variable in the nonlinear function F is taken to be $x(t)$:

$$y(t) + \tau\, dy(t)/dt = \beta F[x(t - T)]\,. \quad (2)$$

From Eqs. (1) and (2), we obtain $x(t) - y(t) = As(t)$, meaning that we have the recovery of the message $s(t)$, and, as $s(t) = 0$, we can have chaos replication. The time required for chaos replication can be evaluated by considering small deviations of $y(t)$ from $x(t)$, i.e.,

$$y(t) = x(t) + \delta y(t)\,. \tag{3}$$

From Eq. (2), we have

$$\delta y(t) + \tau\, d\delta y(t)/dt = 0 \tag{4}$$

thus giving

$$\lim_{t\to\infty}[y(t) - x(t)] = \lim_{t\to\infty}[\exp(-t/\tau)] = 0\,. \tag{5}$$

We observe asymptotically the occurrence of synchronization; practically the time required to have synchronism is of the order of τ. We note in Eq. (1) that the message $s(t)$ is embedded via $f(t)$ in the trajectories of $x(t)$. This method of synchronization seems to be specific to delayed feedback systems. We think that this encoding should improve security compared with methods where $s(t)$ is directly added to a chaotic carrier.

The question is whether this method can be realized in practice. In what follows, we describe the implementation of Eqs. (1) and (2) using wavelength-induced nonlinearities. We also show that using the wavelength rather than the power allows a large range of values for the bifurcation parameter β.

Principle of implementation—Assume that we have an optical component that features a nonlinearity in wavelength, i.e., its response is a nonlinear function F of wavelength Λ. When operating this nonlinear element with a feedback signal, we have a bistable device with steady states that are fixed wavelengths. On the other hand, as the feedback signal features a time retardation T large compared to the time response τ of the device, one knows that high dimensional chaos ruled by a delayed-differential equation can occur. In our case, one gets a light beam with a constant optical power, but with chaotic fluctuations of its wavelength. The equivalent in radiofrequency would be a chaotic frequency modulation that can be used as a spread-spectrum carrier. The advantages of wavelength over intensity as used so far [7] rely not only on an easy control of the nonlinear parameters but also on the possibility to have large bifurcation parameters β. It was shown that $\beta > 15$ ensures a chaotic process with a Gaussian probability density law [8]. This feature, combined with the dimension of chaos which increases linearly with β, improves security by giving rise to more complex dynamics. Then, the strategy for signal encryption and chaos replication is as follows. First the message $s(t)$ is injected in the feedback loop of the transmitter to drive a wavelength tunable laser diode which is in cascade with a wavelength nonlinear element. The wavelength thus emitted exhibits high dimensional chaotic fluctuations $x(t)$. The receiver is a replica of the first chaotic oscillator (in the sense that it is formed by the same elements), but with its feedback loop open. The transmitted signal $x(t)$ is sent into the receiver at the correct point, namely, into the nonlinear element to generate a signal $F[x(t - T)]$. The receiver then operates as a nonautonomous device producing chaotic fluctuations $y(t)$ of wavelength. A subtraction of the input chaos $x(t)$ from the output chaos $y(t)$ results in the recovery of the message $s(t)$. Any separate channel for transmitting synchronizing data is not needed.

The core of the transmitter and receiver is the wavelength tunable laser diode with its nonlinear element used to generate the nonlinear function F. The nonlinear element is, in the system described hereafter, a birefringent plate. When placed between two crossed (or parallel) polarizers, a birefringent plate exhibits a spectral transmission curve that is a $\sin^2$ function vs wavelength. For the transmitter to operate as a chaotic oscillator it is known that the F function should exhibit at least one minimum or one maximum. This condition can be easily met with a suitable choice of the optical path difference (OPD) of the plate.

Experimental setup—Figure 1 shows the cryptosystem. The *transmitter* has already been treated as a generator of chaos in wavelength [9], and we simply give some brief recallings, pointing out the main differences as it is used to encrypt a message $s(t)$. It is formed by a Distributed Bragg Reflector (DBR) two-section tunable laser diode (tuning rate α, optical power P_0) with a feedback loop containing a birefringent plate (BP) with an optical path-difference D (OPD D), a photodetector (PD) (gain η), and a delay line (T). The time response of the feedback loop driving the laser diode is τ. The spectral transmission curve of BP is the F function:

$$F(\Lambda) = \sin^2(\pi D/\Lambda)\,, \tag{6}$$

where Λ is the wavelength emitted by the laser diode. The wavelength Λ can be varied continuously around a center wavelength $\Lambda_0 = 1550$ nm by the injection

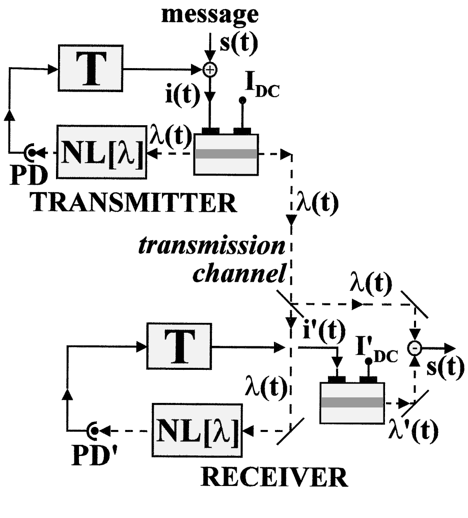

FIG. 1. Schematic diagram of the cryptosystem. NL stands for the nonlinear function $F(\Lambda)$.

current i of the tunable laser diode: $\Lambda(t) = \Lambda_0 + \lambda(t)$, where $\lambda(t) = \alpha i(t)$ is the modulation of the wavelength around Λ_0 generated by the modulation current $i(t)$. The message $s(t)$ to be encrypted is introduced in the feedback loop in such a way that the modulation current $i(t)$ is formed by the addition of $s(t)$ and the time-delayed signal provided by PD. It can then be shown [9] that chaotic fluctuations occur in the wavelength $\lambda(t)$ emitted by the laser diode, which obeys the difference differential equation (1) with

$$x(t) = \pi D\lambda(t)/\Lambda_0^2, \qquad \beta = \pi\alpha\eta P_0 D/\Lambda_0^2,$$
$$F[x(t)] = \sin^2[x(t) - \phi_0] \quad \text{and} \quad \phi_0 = \pi D/\Lambda_0. \tag{7}$$

We observe that a high value of the OPD D ensures a large bifurcation parameter β. The theoretical limitation, which is set by the spectral resolution of the device, i.e., the laser linewidth, is high ($\beta \sim 10^4$) and thus offers a wide range of possibilities [9].

The *receiver* is a replica of the transmitter, except that the feedback loop is open and fed directly with the transmitted light beam which features the chaotic wavelength fluctuations $x(t)$. This beam is directed into the nonlinear birefringent plate BP$'$, which exhibits the same spectral transfer function as in Eq. (6). It can then be shown that the laser diode emits light with chaotic fluctuations $\lambda'(t)$ of its wavelength, which obeys Eq. (2) with

$$y(t) = \pi D\lambda'(t)/\Lambda_0^2.$$

The message $s(t)$ is recovered by subtraction of the output wavelength $y(t)$ from the input $x(t)$. This can be carried out using a spectral filter working at an inflection point of its spectral transmission curve.

Experimental verifications—They were conducted with the following parameters: $\Lambda_0 = 1550$ nm, $\alpha = 0.2$ nm/mA, $P_0 = 5$ mW, $D = 11$ mm, $T = 0.51$ ms, $\tau = 8.6$ μs, and $\eta = 1.5$ A/W. These parameters yield a bifurcation parameter $\beta \sim 22$. This value is 7 times higher than that obtained with the delayed feedback systems reported so far, and is beyond the minimum limit of $\beta = 15$ required to have Gaussian chaos [8]. An estimate of the dimension d of the chaos is given by the relation $d \sim 0.4\,\beta T/\tau$, yielding $d \sim 5 \times 10^2$ for the system used (that corresponds approximately to 250 zero or positive Lyapunov exponents). Note that d can also be expressed in terms of the normalized variance $\sigma^2 = \langle x^2(t)\rangle/\langle x(t)\rangle^2$ of the fluctuations of $x(t)$: $d \sim \beta^2\sigma^2 T/\tau$, meaning a variance of about 1.5 for the system used [8]. Figure 2 shows how chaos replication is obtained at the receiver output as there is no message [$s(t) = 0$]. The time needed for chaos replication at the beginning of the process is the loading time T of the receiver. Then chaos replication occurs and the cyptosystem can operate. Figure 3(a) shows decoding of a 2 kHz sine signal which was injected in the feedback loop of the transmitter -7 dB below the level of the photocurrent. The signal-to-noise ratio of the message recovered after decoding at the receiver output was then measured to be 15 dB. These first results were obtained using free-space propagation with a distance of 2 m between the transmitter and the receiver. The amount of excursion of the wavelength of the light was about 1.5 nm (200 GHz). Propagation losses were compensated at the receiver to obtain the same value of the bifurcation parameter β as that in the transmitter by adjusting the gain of the photodetector in the receiver loop of the receiver. We have made no great effort to optimize the values of the parameters associated with the transmission and detection processes. We have checked that this scheme works when the transmitter and the receiver lasers have slightly mismatched parameters (the laser chips were chosen from two different wafers). The most critical parameter was noticed to be the OPD of the birefringent plates which governs ϕ_0 and the bifurcation parameter β. A β mismatch introduces decoding noise at the received output that can be evaluated from Eqs. (1) and (2). In Fig. 3(a), the β mismatch is estimated to be about 1%. We then introduced voluntarily a β mismatch of 3% and 5%. Figures 3(b) and 3(c) show the decoding noise thus obtained. This will be discussed quantitatively in terms of rms noise, along with the requirement for an efficient masking of the message within chaos, in a longer article.

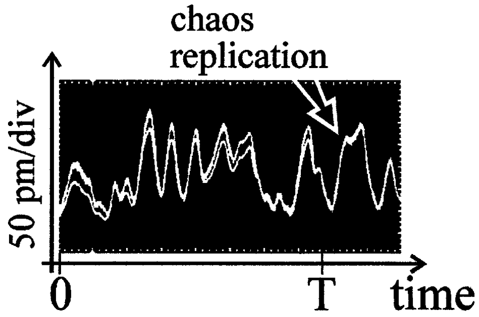

FIG. 2. Evolution to the synchronization of the two chaos $\lambda(t)$ and $\lambda'(t)$ at the receiver output. At time T, the two traces are superimposed (vertical axis is the wavelength).

We conclude with some comments concerning the scope, application, and significance of the method:

(1) The transmitter and receiver are simple and efficient (complex chaotic behavior occurs in simple systems). *Strong* wavelength-induced nonlinearities yielding large bifurcation parameters can be easily achieved using large OPDs, while operating with a low level of energy. This results in chaotic regimes with a wide range of complicated trajectories. The entropy of the chaotic carrier in which the message is embedded, which can be evaluated by calculating the Lyapunov exponents, can be very high.

(2) Experiments have shown that wavelength-induced nonlinearities are very robust to instabilities and allow

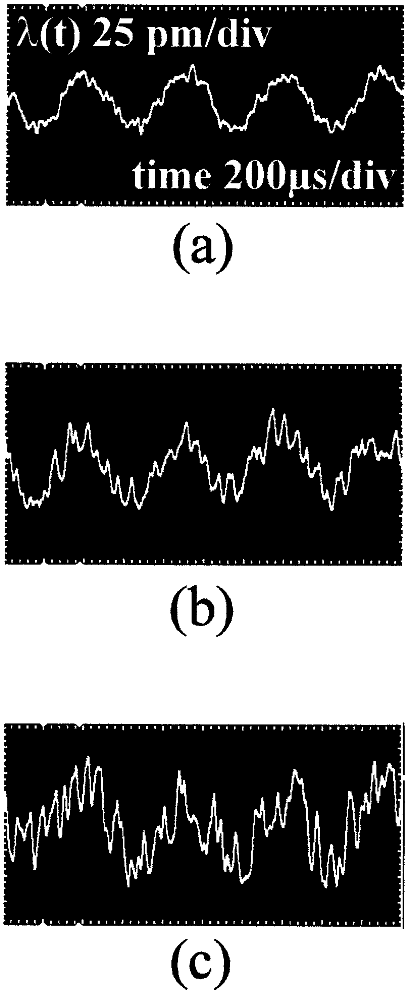

FIG. 3. Decoding of a sine wave form with a β mismatch of (a) 1%, (b) 3%, and (c) 5% (vertical axis is the wavelength).

a good chaos replication to be obtained. In particular, pertaining to the application to communication, we have addressed the issue of chaos replication with no external synchronization channel.

(3) Breaking the encryption key (which is defined in our system by the parameters β, τ, and T) was demonstrated [3] in the case of the Chua's circuit which features a single positive Lyapunov exponent. The situation is different here for two reasons: (i) The large value of the dimension of chaos, which can be 10^2-10^3 higher than in the delayed feedback systems reported so far; (ii) the possibility to generate more complicated nonlinear functions by using other spectral filters, thus increasing the key complexity. Specifically, chaotic regimes produced by nonanalytical nonlinear functions seem to be still unsolved mathematically. We believe that the cryptoanalysis of such systems can become a very difficult task.

(4) A point which also remains to be clarified is the influence of the chromatic dispersion of optical fibers used as the transmission channel. Present day 1550 nm dispersion-shifted fibers feature low dispersion (typically 10 (ps/nm)/km). However, a limitation of the transmission span and of the bit rate can be expected. We are now developing a more practical cryptosystem for applications in fiber encoded transmissions and operating with a higher bit rate.

(5) There has been much work on optical nonlinear chaotic systems, and we speculate that the generation of chaos using controlled wavelength-induced nonlinearities may be extended to all-optical devices. This should open a large body of research about the dynamics and the degree of confidentiality for secure communications.

The support of France Telecom is gratefully acknowledged (Contract No. 931B0190).

*Permanent address: Laboratoire d'Optique P. M. Duffieux, UMR CNRS 6603, Université de Franche-Comté, 25030 Besançon Cedex, France.

[1] E. Ott, C. Grebogi, and J. A. Yorke, Phys. Rev. Lett. **64**, 1196 (1990); S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993); L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990); K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

[2] T. Matsumoto, L. O. Chua, and M. Komura, IEEE Trans. Circuits Syst. **32**, 798 (1985).

[3] T. Beth, D. E. Lazic, and A. Mathias, *Lecture Notes in Computer Science* (Springer-Verlag, Berlin, 1994), Vol. 839, pp. 318–331.

[4] J. H. Peng, E. J. Ding, M. Ding, and W. Yand, Phys. Rev. Lett. **76**, 904 (1996).

[5] V. Annovazzi-Lodi, S. Donati, and A. Scire, IEEE J. Quantum Electron. **32**, 953 (1996); C. R. Mirasso, P. Colet, and P. Garcia-Fernandez, IEEE Photonics Technol. Lett. **8**, 299 (1996); R. Daisy and B. Fischer, Opt. Commun. **133**, 282 (1997); Y. Liu and J. Ohtsubo, IEEE J. Quantum Electron. **33**, 1163 (1997).

[6] R. Roy, T. W. Murphy, T. D. Maier, Z. Gills, and E. R. Hunt, Phys. Rev. Lett. **68**, 1259 (1992); S. Bielawski, D. Derozier, and P. Glorieux, Phys. Rev. A **47**, R2492 (1993); P. Crolet and R. Roy, Opt. Lett. **19**, 2056 (1994).

[7] K. Ikeda, K. Kondo, and O. Akimoto, Phys. Rev. Lett. **49**, 1467 (1982); R. Vallée and C. Delisle, Phys. Rev. A **31**, 2390 (1985); Y. Liu and J. Ohtsubo, IEEE J. Quantum Electron. **30**, 334 (1994).

[8] B. Dorizzi, B. Grammaticos, M. Leberre, Y. Pomeau, R. Ressayre, and A. Tallet, Phys. Rev. A **35**, 328 (1987).

[9] J. P. Goedgebuer, L. Larger, and H. Porte, Phys. Rev. E (to be published); L. Larger, J. P. Goedgebuer, H. Porte, and F. Delorme, IEEE J. Quantum Electron. (to be published).