Optical encryption system using hyperchaos generated by an optoelectronic wavelength oscillator

Laurent Larger,[1,*] Jean-Pierre Goedgebuer,[1,*] and Franck Delorme[2]
[1]GTL-CNRS Telecom, UMR CNRS 6603, Georgia Tech Lorraine, 2-3 rue Marconi, 57070 Metz, France
[2]France Telecom CNET, 196 Avenue H. Ravera, Boîte Postale 107, 92225 Bagneux Cedex, France

(Received 4 September 1997)

An optical encryption system using chaos in which a signal can be masked is reported. The particular design of the chaotic oscillator and the use of wavelength as the dynamical variable provides an accurate control of chaos and a potential number of encryption keys. Experimental results are reported and discussed. [S1063-651X(98)13606-1]

PACS number(s): 05.45.+b

I. INTRODUCTION

Data encryption using chaos was reported in the early 1990s [1,2] as a new approach for signal encoding that differs from the classical methods that use numerical algorithms as the encryption keys. A chaotic signal is intrinsically dedicated to encryption. Firstly, the dynamics is similar to that of a white noise, which can be used to mask data and to protect communication signals from eavesdroppers. Secondly, chaotic systems are deterministic, and in some cases, their complicated dynamics can be governed by a quite simple nonlinear differential equation, which can also be used at the decoding process to extract the original information encrypted in chaos. The general scheme for an encrypted transmission system based on chaos is depicted in Fig. 1. The transmitter consists of two main elements, a master generator of chaos, and an encryption device for encoding an information-bearing signal in chaos. The receiver is also formed by two subsystems, a slave generator of chaos, which should be able to replicate the chaotic signal generated at the transmitter (it usually consists of the same elements used in the transmitter to generate chaos), and a decoding device whose role is to extract the original signal from chaos.

Much work has been devoted to such chaotic systems suitable for data encryption. Pecora *et al.* [1] reported a system in which the generator of chaos is formed by a stable and an unstable subsystem. The same stable subsystem is used at the receiver to generate a chaos synchronized on the original one, and which can be subtracted from the transmitted chaotic signal to recover the information. Another approach consists in coding the information into unstable periodic orbits (UPOs) attached to chaos in its phase space [2]. This encryption method involves that each UPO can be addressed separately by the information signal. This is achieved by the so-called OGY (Ott, Grebogi, Yorke [3]) method which addresses chaotic oscillations to any of its UPOs. Decoding is achieved in a reciprocal way. The OGY method is attractive potentially, but needs a processing time that seems to be relatively high to induce the small perturbations required to address each of the trajectories. Analog and faster methods were also studied, using analog feedback in the chaotic oscillator loop [4,5].

The demonstrators mostly reported up to the present have been successfully realized using electronic circuits to generate the encoding chaotic dynamics [6–9]. The family of these dynamics is generally described by a three- or four-dimensional nonlinear differential system. The complexity of chaotic dynamics (which also determines the key complexity in terms of cryptography) can be expressed by the attractor dimension [10,11], which is calculated to be between 2 and 3, or 3 and 4 for the systems reported in Refs. [6–9]. Since complexity is related to the degree of confidentiality of the encryption method, the fractal dimension should be as high as possible. As the dimension exceeds 3, the system is termed hyperchaotic.

Recent works [12–14] have proposed optoelectronic systems for data encryption using chaotic fluctuations of optical power generated by laser diodes with an optical feedback. Such chaos in optical power can exhibit a high complexity (hyperchaos), and fast intensity fluctuations with a wide bandwidth, which is well suited to the high bit rate and high encoding rate that are expected in future fiber communication networks. However, generating chaos in power implies the physical parameters of the laser diodes, such as its nonlinear behavior in power, to be controlled very accurately and with a high reliability. This probably explains why experimental demonstrations in optics have been relatively limited so far.

We report here a different approach, in which chaos in wavelength rather than chaos in intensity, is used to encrypt a signal. The advantages are in the high accuracy and high reliability of chaos control—and hence, of the encryption and decoding process. Generating chaos in wavelength for signal encryption relies on the wavelength agility of a laser diode with a feedback loop and a nonlinear element in wavelength. At the receiver side, decoding is achieved using a nonautonomous generator of chaos in wavelength. We

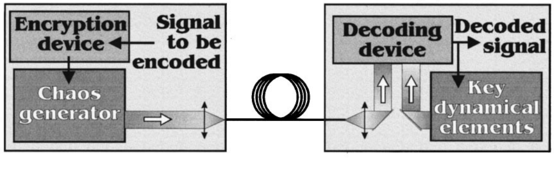

FIG. 1. Principle of encryption using chaos.

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

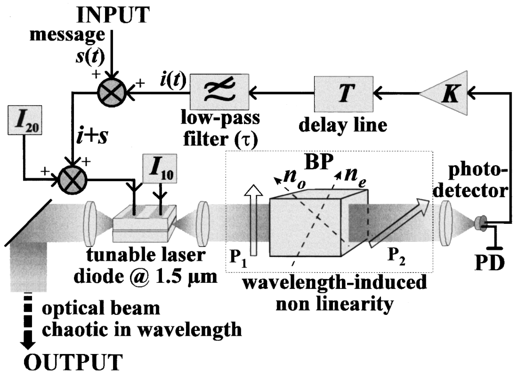

FIG. 2. Chaos generator used as the transmitter. The transmitter is formed by a DBR two-section wavelength tunable laser diode with a delayed nonlinear feedback loop. The input message $s(t)$ is encrypted within chaotic fluctuations of the wavelength emitted by the laser diode.

present an effective experimental demonstration in which optically generated chaos is used for signal encryption.

The article is organized as follows. Section II describes the generator of chaos, which produces controlled chaotic fluctuations of the wavelength of a laser diode. In Sec. III, we consider how such a generator of chaos can be used as a transmitter to mask a signal. The decoding process at the receiver is also discussed with considerations on the decoding errors. Section IV describes the experimental realization of the receiver. Finally the first experimental results are reported in Sec. V.

II. THE CHAOTIC WAVELENGTH GENERATOR

The generator of the chaotic wavelength beam that is used to encrypt the information is depicted in Fig. 2. Its mode of operation has already been discussed in other circumstances [15]. It consists of an electrically tunable DBR multielectrode laser diode with a feedback loop formed by a delay line and an optical device whose peculiarity is to exhibit a nonlinearity in wavelength. Under some conditions, it turns out that the wavelength emitted by the laser diode fluctuates chaotically around its center wavelength Λ_0. More precisely, the chaotic oscillator in Fig. 2 consists of the following.

(i) A tunable double electrode DBR laser diode whose center wavelength is set at Λ_0 by means of a dc injection current I_{20}. The wavelength can be tuned continuously around Λ_0, i.e., without mode hopping, with a modulation current i superimposed to I_{20}. Then the emitted wavelength Λ is proportional to i: $\Lambda=\Lambda_0+\lambda$ with $\lambda=Si$, where S is the tuning rate of the laser diode. The optical power P_0 is wavelength independent and is adjustable by means of an injection current I_{10}.

(ii) A spectral filter operating as a wavelength nonlinear element, formed by a birefringent plate BP set between two crossed polarizers P_1 and P_2. The fast and slow axes of BP are oriented at 45° to the polarizing directions of P_1 and P_2. The power spectrum density of light at the output of P_2 is a channeled spectrum, i.e., a function F_{NL} of wavelength Λ, which can be expressed as

$$F_{\mathrm{NL}}[\Lambda]=\sin^2\left(\frac{\pi D}{\Lambda}\right), \tag{1}$$

where D is the optical path difference (OPD) of BP. The tuning range of the laser diode being much smaller than the center wavelength Λ_0, Eq. (1) can be approximated as

$$F_{\mathrm{NL}}[\lambda]=\sin^2\left(\frac{\pi D}{\Lambda_0^2}\,\lambda-\Phi_0\right), \tag{2}$$

with $\Phi_0=\pi D/\Lambda_0$, and where $\lambda=\Lambda-\Lambda_0=Si$ is the wavelength deviation from the center wavelength Λ_0 as the laser diode is tuned with a current i around bias current I_{20}. Equations (1) and (2) also indicate that the function $F_{\mathrm{NL}}[\Lambda]$ exhibits sinusoidal lobes inside the tuning range of the laser diode, spaced in wavelength by a free spectral range equal to Λ_0^2/D: (i) a photodetector PD providing a linear conversion of the optical power into a photocurrent with a conversion factor K; (ii) a delay line that introduces a time delay T longer than the response time τ of the loop; (iii) the time constant τ of the system is theoretically limited by the wavelength switching time of the laser diode (typically 10 ns). Practically, the time constant τ is related to the photodetector and its amplifier, as described in the experimental part.

Then the output wavelength of the system is ruled by a differential difference equation, also termed Ikeda's equation [16]:

$$\lambda(t)+\tau\,\frac{d\lambda}{dt}\,(t)=\beta_\lambda\sin^2\left[\frac{\pi D}{\Lambda_0^2}\,\lambda(t-T)-\Phi_0\right], \tag{3}$$

with $\beta_\lambda=KP_0S$ and $\Phi_0=\pi D/\Lambda_0$, where $\lambda(t)$ is the wavelength deviation from the center wavelength Λ_0, β_λ is the bifurcation parameter in λ units, D is the optical path difference of the birefringent plate, Λ_0 is the center wavelength of the tunable DBR laser, adjustable with I_{20}, τ is the time constant of the feedback loop, K is the adjustable photodetector gain (A/W), P_0 is the optical power of the tunable laser DBR (W), S is the wavelength–DBR-current tuning rate of the laser (m/A). We refer the reader to Ref. [15] for a detailed description of the system and considerations on routes to chaos in wavelength. The regime of oscillations in wavelength depends on the value of the bifurcation parameter β_λ, which can be adjusted through the gain K of the photodetector. As the bifurcation parameter is increased from zero to a maximum value $\beta_{\lambda\ \max}$, the dynamics of the device is characterized first by the well-known period doubling cascade, which converges to the so-called accumulation point β_λ^*, and then to full chaos for higher values of the bifurcation parameter as described in [15].

In the following, the bifurcation parameter is set in order to operate in the full chaos regime. Under these conditions, the wavelength $\lambda(t)$ emitted by the laser diode fluctuates chaotically. The power spectrum of the fluctuations of wavelength thus obtained is similar to that of a white noise spectrum with a bandwidth limited approximately to $1/(2\pi\tau)$. Note that other chaotic behaviors could also be obtained as well, using other spectral filters in the feedback loop to induce nonlinear functions and to generate different encryption keys that can be used, for instance, to encode different data channels.

The dynamical properties (such as the attractor dimension, the Lyapounov dimension, or the Lyapounov exponents [11]), and the statistical properties of chaos attached to Eq.

(3) have been calculated by Dorizzi *et al.* [17]. They found that nonlinear time-delayed differential systems with a $\sin^2$ feedback exhibit a very complex behavior characterized by an attractor dimension that can be larger than 10, and a probability density function, which tends asymptotically to be Gaussian when the bifurcation parameter is much greater than the free spectral range of the spectral filter. The high degree of complexity of the dynamics thus obtained [18] makes such systems good candidates for signal encryption. Moreover, the simple expression of the dynamical law expressed by Eq. (3) should be favorable for a highly reliable and easy control of the dynamics, which is required to decrypt the information at the receiver as explained in the following.

III. ENCRYPTION-DECRYPTION METHOD

A. Encrypting

The encryption method that is used consists in superimposing electrically the information signal to the chaotic signal propagating in the feedback loop (Fig. 2). It should be noticed here that the information signal is injected inside the chaotic oscillator loop, unlike the technique of an external addition sometimes used in other works [1,14]. In other words, the information participates directly to the chaotic dynamics ruled by Eq. (3). Moreover, this in-loop addition technique provides an easy decoding method as will be demonstrated later.

Let $s(t)$ be the signal to be encrypted and β_λ the bifurcation parameter of the generator in Fig. 2 operating in a chaotic regime. Encrypting $s(t)$ in chaos is carried out by superimposing electrically $s(t)$ to the injection current $i(t)$ produced by the feedback loop. The wavelength $\lambda_e(t)$ thus emitted is chaotic and can be expressed as

$$\lambda_e(t)=S[i(t)+s(t)]=\lambda_c(t)+\lambda_s(t). \tag{4}$$

The chaotic part $\lambda_c(t)$ of the transmitted wavelength $\lambda_e(t)$ results from the feedback current $i(t)$, which obeys the following dynamical law (see Fig. 2)

$$i(t)+\tau\frac{di}{dt}(t)=\frac{\beta_\lambda}{S}\sin^2\left[\frac{\pi D}{\Lambda_0^2}\lambda_e(t-T)-\Phi_0\right]. \tag{5}$$

Then $\lambda_c(t)=Si(t)$ is ruled by

$$\lambda_c(t)+\tau\frac{d\lambda_c}{dt}(t)=\beta_\lambda\sin^2\left[\frac{\pi D}{\Lambda_0}[\lambda_c(t-T)+\lambda_s(t-T)]-\Phi_0\right]. \tag{6}$$

Hence, the emitted wavelength around Λ_0 is the sum of $\lambda_c(t)$, and of a small wavelength deviation $\lambda_s(t)=Ss(t)$ corresponding to the information to be masked in the chaotic part $\lambda_c(t)$.

A key point is that the amplitude of the message is much smaller than the fluctuations of chaos, i.e., $s(t)\ll i(t)$, or $\lambda_s(t)\ll\lambda_c(t)$, in order to realize so-called chaos masking. A high masking efficiency requires a signal-to-chaos ratio ρ_{SC} much smaller than 1 for encoding a signal. Then, the interceptor can only detect chaotic fluctuations of the wavelength, without being able to extract the small amplitude information signal, which is superimposed to chaos. From the Fourier analysis viewpoint, the spectrum of $s(t)$ should be narrower and with a level much below that of chaos, so that information cannot be extracted by a simple filtering process. The principle of this encryption method is similar to the Vernam-cipher method [19], which is well known in cryptography and which was proven to be absolutely secure by Shannon [20] provided that the noise has maximal entropy. In the case discussed here, the spectrum of chaos is similar to that of a white noise over a bandwidth that is of the order of $1/(2\pi\tau)$, τ being the response time of the slowest component forming the generator of chaos as defined in the previous section. Entropy here is used in its statistical meaning and is expressed as

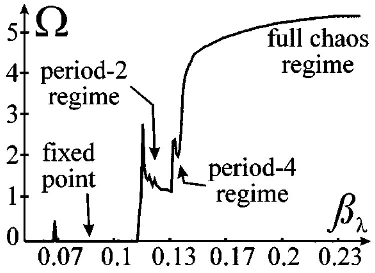

FIG. 3. Entropy Ω vs bifurcation parameter β_λ, for $\Phi_0=0.3$ and $T/\tau=60$.

$$\Omega=\sum_i p_i\ln(p_i),$$

where p_i is the probability for the wavelength λ_i to appear in the chaotic regime. The entropy was calculated for $T/\tau=60$ from numerical simulations of Eq. (3) for different values of the bifurcation parameter β_λ, and from the wavelength statistics attached to each regime. The result is plotted in Fig. 3, which represents the evolution of entropy versus the bifurcation parameter β_λ. It clearly shows that a high value of the bifurcation parameter ensures a high entropy. A detailed analysis of the degree of confidentiality thus obtained remains to be carried out and is beyond the scope of this paper (see also Ref. [21]).

B. Decoding

Let us now come back to the dynamics expressed by Eq. (3). The chaotic evolution of the wavelength emitted by the generator is a particular solution with well-defined initial conditions. To define entirely such a solution (also called a trajectory in the phase space of the system), the initial conditions should be known over the time interval T. Normally, they have to be defined with an infinite accuracy for describing a particular solution, due to the well-known high sensitivity of chaotic systems to initial conditions; a negligibly small difference between two neighbor initial conditions grows exponentially, due to the positive Lyapounov exponents [11] of chaotic systems, and the two corresponding trajectories diverge from each other very rapidly.

In order to achieve the decoding process, the local chaotic oscillator at the receiver should be able to recognize any of the possible trajectories generated by the transmitter. Hence,

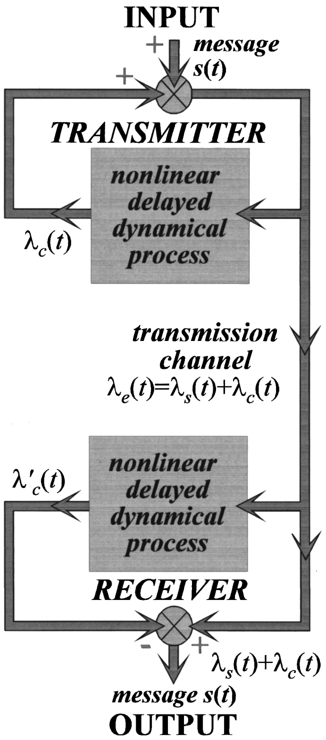
INPUT
+
message
$s(t)$
+
TRANSMITTER
nonlinear delayed dynamical process
$\lambda_c(t)$
transmission channel
$\lambda_e(t)=\lambda_s(t)+\lambda_c(t)$
$\lambda'_c(t)$
nonlinear delayed dynamical process
RECEIVER
-
+
$\lambda_s(t)+\lambda_c(t)$
message $s(t)$
OUTPUT

FIG. 4. Principle of operation of the cryptosystem.

the generator of chaos used as the receiver should be identical to that used at the transmitter and should operate with initial conditions identical to those used at the transmitter. Then, ideally, the receiver should generate chaos in wavelength synchronized with that produced by the transmitter. Applying a message in the feedback loop of the transmitter yields a synchronization error at the receiver, and we can expect to retrieve the message. However, as the receiver is an independent generator of chaos (without external synchronization), synchronization is rapidly lost due to at least three different reasons: (i) information decoding is performed through a ‘‘desynchronization’’ process; (ii) the initial conditions cannot be exactly the same between the transmitter and the receiver (due to channel noise, for instance); (iii) the devices forming the chaotic oscillator at the receiver cannot duplicate perfectly those used at the transmitter for technological reasons. This results in a dramatic desynchronization between trajectories defined by slightly different dynamical laws. This is also the reason why much work has been devoted to chaos synchronization. The method we use is different and operates without external synchronization.

The decoding method used is actually performed by updating continuously the initial conditions, including the message-induced perturbations, and by using a self-synchronized dynamical process at the receiver (no input implies no output). The principle of operation of the encrypting-decrypting system is depicted in Fig. 4 in which the transmitter and receiver are schemed as two blocks. At the transmitter the information-bearing signal $s(t)$ is added to the feedback signal as explained before, and the emitted wavelength $\lambda_e(t)$ is expressed by Eq. (4). The message is encoded as a time-dependent wavelength modulation of the carrier, which is chaotic in wavelength as explained earlier. A part of it is used to operate as a feedback signal for the nonlinear device in the transmitter, while the other part is directed to the receiver. At the receiver, the input signal is routed to the nonlinear device, which is identical to that used in the transmitter, and which produces a chaotic regime identical to that of the first laser. Then the encoded signal is recovered by subtracting the output wavelength from the input wavelength.

Let us first consider a chaotic oscillation without information encoding, i.e., $s(t)=0$ and $\lambda_e(t)=\lambda_c(t)$ at the transmitter. In Fig. 4, the box at the transmitter stands for the nonlinear delayed dynamical process (NLDDP). Its input is a set of continuous wavelengths $\lambda_e(t)$ on a time interval $[t-T,t]$, that are the initial conditions. Starting from this initial state, the NLDDP generates at the box output another set of continuous wavelengths $\lambda_e(t)$ on the time interval $[t,t+T]$. These values are fed back to the box input as new initial conditions $\lambda_e(t)=\lambda_c(t)$ to reinitiate the process. The transmitter operates as an autonomous chaotic oscillator, since it generates a chaotic wavelength $\lambda_e(t)$ without the need of any external signal. This chaotic wavelength obeys the dynamical law expressed by Eq. (6).

The working conditions of the receiver are different. In contrast, it works as a nonautonomous chaotic system. The wavelength values generated during the successive time intervals $[t+(n-1)T,t+nT]$ by the transmitter are used by the nonautonomous receiver as external initial conditions, to produce with a delay T other wavelength values $\lambda_c'(t)$ on successive time intervals $[t+nT,t+(n+1)T]$. In Fig. 4, the receiver box is schemed as a nonautonomous generator whose dynamics is ruled by

$$\lambda_c'(t)+\tau'\,\frac{d\lambda_c'}{dt}\,(t)=\beta_\lambda'\sin^2\!\left[\frac{\pi D'}{(\Lambda_0)^2}\,\lambda_e(t-T')-\Phi_0'\right]. \tag{7}$$

Its experimental realization is described later. As the dynamical process of the receiver is identical to that of the transmitter, i.e., $\tau'=\tau$, $D'=D$, $T'=T$, $\Phi_0'=\Phi_0$, the chaotic wavelength values calculated at the receiver are identical to those generated by the transmitter, since they operate with the same initial conditions: $\lambda_e(t)=\lambda_c'(t)$.

Let us now consider the case of a message $s(t)$ applied to the transmitter at time t. Then the wavelength at the receiver input is $\lambda_e(t)=\lambda_c(t)+\lambda_s(t)$ [see Eq. (4)], while the wavelength $\lambda_c'(t)$ at the receiver output is ruled by Eq. (7), which can be written as

$$\lambda_c'(t)+\tau'\,\frac{d\lambda_c'}{dt}\,(t)$$
$$=\beta_\lambda'\sin^2\!\left[\frac{\pi D'}{(\Lambda_0)^2}\,[\lambda_c(t-T')+\lambda_s(t-T')]-\Phi_0'\right]. \tag{8}$$

Setting $\beta_\lambda=\beta_\lambda'$, $\tau=\tau'$, $D=D'$, $\Phi_0=\Phi_0'$, and comparing Eq. (8) with Eq. (7), we have obviously $\lambda_c'(t)=\lambda_c(t)$. The information $s(t)$ is then recovered at the receiver by subtracting the output wavelength from the input: $\lambda_s'(t)=\lambda_e(t)-\lambda_c'(t)$. As the transmitter and receiver are assumed to be identical, and assuming no noise is introduced by the transmission link, the information is recovered without any distortion.

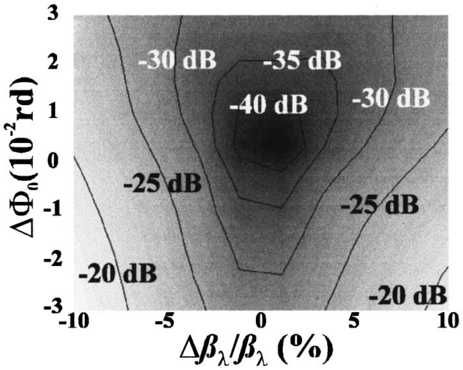

FIG. 5. Decoding error in dB vs parameter mismatch $(\Delta\Phi_0, \Delta\beta_\lambda/\beta_\lambda)$.

C. Decoding errors

As the transmitter and receiver are not identical, the recovered signal is altered by a decoding error. This decoding error can be evaluated, calculating the difference between the receiver input and output wavelengths $\lambda_c'(t)-\lambda_c(t)=\varepsilon(t)$. In an ideal system, this difference is equal to zero as no message is applied to the transmitter. Practically, the components forming the transmitter and the receiver have to be adjusted carefully. The most critical adjustments are on the Φ_0 and β_λ parameters. Considering the following parameter deviations $\Delta\beta_\lambda=\beta_\lambda'-\beta_\lambda$ and $\Delta\Phi_0=\Phi_0'-\Phi_0$ between the transmitter and receiver, the error dynamics $\varepsilon(t)$ is ruled by the following equation, which is obtained by subtracting Eq. (8) from Eq. (6):

$$\varepsilon(t)+\tau\frac{d\varepsilon}{dt}(t)=\frac{\Delta\beta_\lambda}{2}-\beta_\lambda\Delta\Phi_0 \times\cos\{2[\lambda_e(t-T)-\Phi_0+\alpha]\} \qquad (9)$$

with $\tan(2\alpha)=2\beta_\lambda\Delta\Phi_0/\Delta\beta_\lambda$.

By integrating numerically Eq. (6) and Eq. (9), we evaluated the root-mean-square (rms) error decoding noise $\sigma=\langle\varepsilon^2(t)\rangle$ of $\varepsilon(t)$ due to parameter mismatch. The calculated value $\sigma_{\beta,\Phi}(\Delta\beta_\lambda,\Delta\Phi_0)$ is represented in Fig. 5 for a particular dynamical regime of the chaotic oscillator defined by $\beta_\lambda=0.2$ nm and $\Phi_0=0.3$, and as a function of the deviation of the Φ_0 and β_λ parameters. The rms decoding noise is expressed in dB units as $(\sigma)_{\mathrm{dB}}=10\log_{10}[\sigma]$ in the $(\Delta\beta_\lambda,\Delta\Phi_0)$ plane. The 0 dB reference level is arbitrary taken as the rms level of the chaotic signal computed from Eq. (3). For $\Delta\beta_\lambda=\Delta\Phi_0=0$, the transmitter and receiver devices are perfectly duplicated, and the decoding noise is zero ($-\infty$ in dB). When increasing the Φ_0 and β_λ mismatch, the rms decoding noise is increased. As an illustration, for $\Delta\Phi_0=0$ and $\Delta\beta_\lambda/\beta_\lambda=5\%$, we obtain an rms decoding of about -30 dB. The latter determines the minimum theoretical ρ_{SC} of the information-bearing signal $s(t)$ masked originally in chaos. Here, the message $s(t)$ can be -30 dB $[(\rho_{SC})_{\mathrm{dB}}=-30$ dB] below the masking chaos for the theoretical limit of a signal-to-noise ratio (ρ_{SN}) equal to 1 at the receiver output. More generally, the ρ_{SC} of $s(t)$ in the masking chaos can be expressed in dB units as

$$(\rho_{SC})_{\mathrm{dB}}=(\sigma)_{\mathrm{dB}}+(\rho_{SN})_{\mathrm{dB}}, \qquad (10)$$

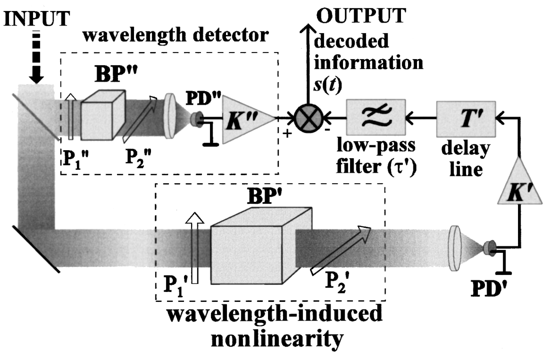

FIG. 6. Receiver. The receiver is a replica of the transmitter, without the laser diode. The input is the output light beam of the transmitter in which the message is encrypted. A part of it is directed into a delayed nonlinear subsystem formed by elements identical to those used in the transmitter. The signal thus obtained is subtracted from the input, yielding the recovery of the message at the output.

where σ is related to the decoding noise due to the transmitter and receiver mismatch, and ρ_{SN} refers to the signal-to-noise ratio required at the receiver output. For instance, coming back to the case of a 5% β_λ mismatch, and assuming the signal $s(t)$ is recovered at the receiver output with a signal-to-noise ratio $\rho_{SN}=20$ dB, $s(t)$ is masked within chaos with a signal-to-chaos ratio $\rho_{SC}=-10$ dB. This does not consider the influence of other parameters, such as the detection noise or the channel noise.

IV. THE RECEIVER USED FOR SIGNAL DECODING

The receiver is depicted in Fig. 6. The same components as those forming the transmitter are used, except the laser diode, which is removed. The NLDDP is performed using a birefringent plate BP$'$ set between crossed polarizers P_1' and P_2' a photodetector PD$'$ with an amplification gain K', and a delay line with a time delay $T'=T$. Due to propagation losses in the transmission fiber, the photocurrent detected by PD$'$ should be amplified with K' adjusted such that the bifurcation parameters in the transmitter and the receiver be the same. The time constant of the system is $\tau'=\tau$. It can be adjusted using a low pass filter as shown in Fig. 6.

The birefringent plate BP$'$ behaves as a spectral filter with a nonlinear spectral curve $F_{\mathrm{NL}}'[\Lambda]$. It is chosen to exhibit the same OPD as that used in the transmitter, $D'=D$. Then we have $F_{\mathrm{NL}}'[\Lambda]=F_{\mathrm{NL}}[\Lambda]$. The light beam is routed to the birefringent plate and converted into a time-delayed electrical signal by the photodetector and the delay line T. The subtraction process is performed on the output photocurrent generated by the NLDDP, and the signal provided by a wavelength detector which converts linearly the input wavelength into an electric current. The wavelength detector used is formed by a spectral filter realized by a birefringent plate BP$''$ set between crossed polarizers P_1'' and P_2'' and operating at the inflection point of its spectral transmission curve. Finally, the original message is recovered at the output of the receiver.

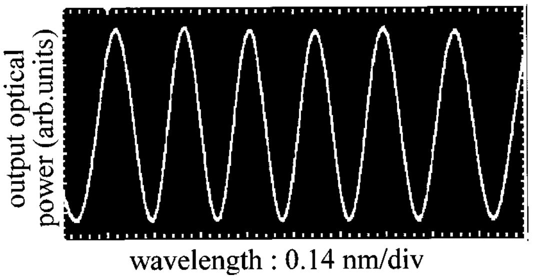

FIG. 7. Nonlinear function: channeled spectrum.

V. EXPERIMENTAL IMPLEMENTATION AND RESULTS

Experimental verifications were conducted with a two electrode $In_{1-x}Ga_xAs_yP_{1-y}$ DBR laser diode operating at a center wavelength $\Lambda_0 = 1550$ nm, as the current I_{20} was 9 mA. Its wavelength tunability and continuous tuning range were $S = 0.25$ nm/mA and $\delta\lambda = 1.5$ nm, respectively. The laser threshold was $I_{10\text{th}} = 8$ mA, and the operating power was $P_0 = 5$ mW, which was obtained for $I_{10} = 20$ mA. The birefringent plate BP used in the transmitter feedback loop was a 7 cm long calcite slab. Its OPD was $D = (n_e - n_o)\ l = 11$ mm, with $n_e - n_o = 0.157$ for calcite at $\Lambda_0 = 1.55\ \mu$m wavelength. The polarizers P_1 and P_2 were Glan polarizers oriented at 45° to the fast and slow axes of BP. Antireflection coatings were necessary to minimize unwanted interferences from the multiple reflected beams. The nonlinear function F_{NL} induced by the birefringent plate was checked, tuning the wavelength of the laser diode. Figure 7 shows the channeled spectrum thus obtained. Seven oscillations can be seen inside the tuning range of the laser diode, with a free spectral range FSR that was measured to be 0.21 nm, as expected from Eq. (2). The delay line was formed by a charge-coupled device memory component (first in first out) of 512 analog capacitive memories. The delay T was $T = 0.51$ ms. The constant time of the transmitter was adjusted at $\tau = 8.6\ \mu$s using a low-pass filter. This value was voluntarily chosen to be large enough due to the electronic equipment available at the laboratory. The detector in the transmitter feedback loop was a $0.9A/W$ $In_xGa_{1-x}As/InP$ photodiode followed by a transimpedance amplifier whose gain K was adjusted such that the value of the bifurcation parameter was $\beta_\lambda = 0.2$ nm. Then the wavelength emitted by the transmitter was a chaotic signal $\lambda_e(t)$. Its spectrum, which is shown in Fig. 8, was obtained using a fast Fourier transform (FFT) spectrum analyzer. The spectrum thus obtained is similar to that of a white noise whose bandwidth is $1/(2\pi\tau) = 18$ kHz. The message $s(t)$ to be encrypted was added to the current in the feedback loop, and the encoded chaotic signal was routed in free space to the receiver.

The operating mode of the receiver was checked using a birefringent plate BP′, a photodetector and a delay line identical to those in the transmitter. As mentioned earlier, signal decoding requires the receiver to be closely matched to the transmitter. The first condition $\Phi_0' = \Phi_0$ was achieved by comparing the channeled spectra produced by BP and BP′, and rotating BP′ around one of its axes in order to adjustate accurately its OPD to that of BP. A fine tuning of the rotation angle allowed the two channeled spectra to be superimposed exactly. The second condition on the bifurcation parameter $\beta_\lambda' = \beta_\lambda$ was easily fulfilled by adjusting the receiver gain K' as there is no message $(s=0)$, such that the signal at the receiver output is zero (practically, the decoder output is altered by a slight noise, probably due to unavoidable deviations in the characteristics of the electronic devices used). The adjustment of the other parameters, such as the delay T and the response time τ, was found to be much less critical.

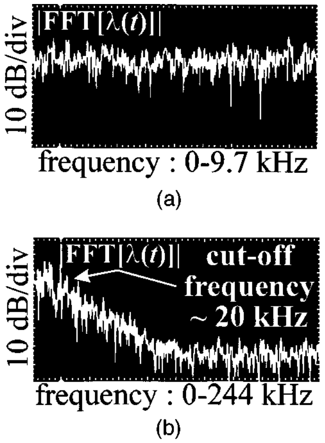

FIG. 8. Experimental FFT spectrum of the chaotic fluctuations of wavelength ($\beta_\lambda = 0.23$, $\Phi_0 = 0.3$, $T/\tau = 60$).

First the system was tested with no message driving the transmitter $[s(t)=0]$. Figure 9(a) shows the chaotic carrier obtained at the receiver output as the photodetector PD′ was switched off, and its FFT which shows a continuous broad spectrum. The -3 dB cutoff frequency was measured to be 20 kHz (see Fig. 8).

Then we turned PD′ on to obtain the decoding error $\varepsilon(t)$ as shown in Fig. 9(b). Its rms as defined in the previous section was measured to be -22 dB.

A 2 kHz sine signal $s(t)$ was then applied to the transmitter. Its level was adjusted -7 dB below the masking chaotic carrier. This was carried out by comparing chaos and the message amplitude at the receiver output. The chaos level was first measured with no message applied to the transmitter, and with PD′ off. Then the chaotic carrier was suppressed by opening the feedback loop in the transmitter, and the level of $s(t)$ was adjusted at the receiver output, still maintaining PD′ off, to be about 0.4 that of the chaotic wave. Figure 10 shows the chaotic encrypted signal $\lambda_e(t)$ thus obtained. The sine wave $s(t)$ was not recognizable in the spectrum of $\lambda_e(t)$. Finally, the cryptosystem was oper-

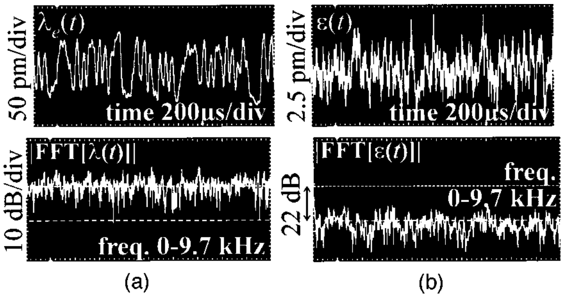

FIG. 9. No message is applied to the transmitter $[s(t)=0]$. (a) Chaotic carrier $\lambda_c(t)$ (top trace) and its FFT spectrum (bottom trace). (b) Noise $\varepsilon(t)$ at the receiver output [top trace] and its FFT spectrum (bottom trace). The level of noise $\varepsilon(t)$ is -22 dB below that of the chaotic carrier $\lambda_c(t)$.

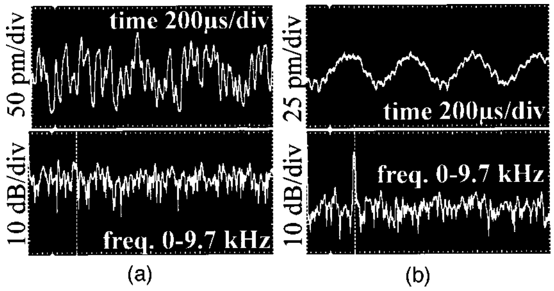

FIG. 10. The message $s(t)$ is a 2 kHz sine wave form. (a) Chaotic encrypted wavelength $\lambda_e(t)$ emitted by the transmitter (top trace) and its FFT spectrum (bottom trace). The message $s(t)$ is masked with a -7 dB signal-to-chaos ratio. (b) Decoded signal at the receiver output (top trace) and its FFT spectrum (bottom trace) showing a strong peak at 2 kHz frequency, with a signal-to-noise ratio of 15 dB.

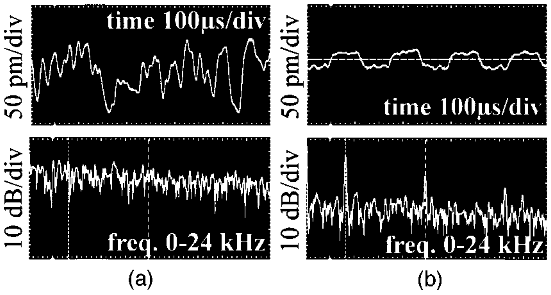

FIG. 11. The message $s(t)$ is a 4 kHz square wave form. (a) Chaotic encrypted wavelength $\lambda_e(t)$ emitted by the transmitter (top trace) and its FFT spectrum (bottom trace). The message $s(t)$ is masked with a -10 dB signal-to-chaos ratio. (b) Decoded signal at the receiver output (top trace) and its FFT spectrum (bottom trace) showing the fundamental and the harmonics. The signal-to-noise ratio is 12 dB.

ated, and $s(t)$ was obtained at the receiver output with a $(\rho_{SN})_{\mathrm{dB}}$ of the order of 15 dB [Fig. 10(b)], that was in good accordance with theoretical predictions in Eq. (10). Figure 11 gives other illustrations obtained as $s(t)$ was a 4 kHz square signal encrypted using similar working conditions.

VI. CONCLUSION

An experimental optical encryption system was reported in the audio frequency domain. Its originality relies on the use of wavelength-agile laser diodes to generate a masking chaotic carrier. The use of wavelength to generate the required nonlinearities allows an easy control of the chaotic dynamics both at the transmitter and at the receiver. Moreover, this provides potentially a number of encryption keys simply by changing the nonlinear element involved in the differential delayed dynamical process. The limits of the encoding efficiency were shown to be related to the decoding parameters that can be easily matched to those used in the transmitter. This experimental issue is physically inherent to wavelength. This indeed offers a high flexibility compared to other optical systems with power-induced nonlinearities and that have been mostly plagued by optical instabilities and the difficulty to duplicate two optical chaos. Future work will deal with improving the system performance in view of applications to encrypt signals with high bit rates as well as with a better understanding of the confidentiality attached to hyperchaos.

ACKNOWLEDGMENT

We thank France Telecom for the financial support of this research project (Contract No. 931B0190).

[1] L. M. Pecora and T. L. Carroll, Phys. Rev. Lett. **64**, 821 (1990).

[2] E. Ott, C. Grebogi, and J. A. Yorke, Phys. Rev. Lett. **64**, 1196 (1990); see also T. Shinbrot, E. Ott, C. Grebogi, and J. A. Yorke, *ibid.* **65**, 3215–3218 (1991).

[3] S. Hayes, C. Grebogi, and E. Ott, Phys. Rev. Lett. **70**, 3031 (1993).

[4] E. R. Hunt, Phys. Rev. Lett. **67**, 1953 (1991).

[5] K. Piragas, Phys. Rev. A **170**, 421 (1992).

[6] T. L. Carroll, IEEE Trans. Circuits Syst. **42**, 105 (1995).

[7] U. Feldmann, M. Hasler, and W. Schwarz, Int. J. Circ. Theory Appl. **24**, 551 (1996).

[8] K. M. Cuomo and A. V. Oppenheim, Phys. Rev. Lett. **71**, 65 (1993).

[9] U. Parlitz, L. O. Chua, Lj. Kocarev, K. S. Halle, and A. Shang, Int. J. Bifurcation Chaos Appl. Sci. Eng. **2**, 973 (1992); see also recent work on chaos synchronization using electrical circuits, for example, A. Tamaševicius, A. Cenys, G. Mykolaitis, A. Namajunas, and E. Lindberg, Electron. Lett. **33**, 2025 (1997).

[10] J. D. Farmer, E. Ott, and J. A. Yorke, Physica D **7**, 153 (1983).

[11] J.-P. Eckmann and D. Ruelle, Rev. Mod. Phys. **57**, 617 (1985).

[12] P. Colet and R. Roy, Opt. Lett. **19**, 2056 (1994); and see also R. Roy, T. W. Murphy, T. D. Mayer, and Z. Gills, Phys. Rev. Lett. **68**, 1259 (1992).

[13] C. R. Mirasso, P. Colet, and P. García-Fernández, IEEE Photonics Technol. Lett. **8**, 299 (1996).

[14] R. Daisy and B. Fischer, Opt. Commun. **133**, 282 (1997); see also P. Celka, IEEE Trans. Circuits Syst. **42**, 1 (1995).

[15] L. Larger, J.-P. Goedgebuer, and J. M. Merolla, IEEE J. Quantum Electron. **34**, 594 (1998).

[16] K. Ikeda and K. Matsumoto, Physica D **29**, 223 (1987).

[17] B. Dorizzy, B. Grammaticos, M. Le Berre, Y. Pomeau, E. Ressayre, and A. Tallet, Phys. Rev. A **35**, 328 (1986).

[18] M. Le Berre, E. Ressayre, A. Tallet, and H. M. Gibbs, Phys. Rev. Lett. **56**, 274 (1986).

[19] G. S. Vernam, J. Am. Inst. Electr. Eng. **55**, 109 (1926).

[20] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).

[21] J. P. Goedgebuer, L. Larger, H. Porte, Phys. Rev. Lett. **80**, 2249 (1998).