



ELSEVIER

Available online at www.sciencedirect.com

SCIENCE @ DIRECT®

Physics Letters A 308 (2003) 54–60

PHYSICS LETTERS A

www.elsevier.com/locate/pla

Cracking chaos-based encryption systems ruled by nonlinear time delay differential equations

Vladimir S. Udaltsov^{a,b,*}, Jean-Pierre Goedgebuer^{a,b}, Laurent Larger^{a,b},
Jean-Baptiste Cuenot^{a,b}, Pascal Levy^{a,b}, William T. Rhodes^{a,b}

^a *GTL-CNRS TELECOM, UMR CNRS 6603, Georgia Tech Lorraine, 57070 Metz, France*

^b *Laboratoire d'Optique PM Duffieux, UMR 6603, Université de Franche-Comté, 25030 Besançon cedex, France*

Received 5 July 2002; accepted 18 December 2002

Communicated by A.P. Fordy

Abstract

We report that signal encoding with high-dimensional chaos produced by delayed feedback systems with a strong nonlinearity can be broken. We describe the procedure and illustrate the method with chaotic waveforms obtained from a strongly nonlinear optical system that we used previously to demonstrate signal encryption/decryption with chaos in wavelength. The method can be extended to any systems ruled by nonlinear time-delayed differential equations.

© 2003 Elsevier Science B.V. All rights reserved.

PACS: 05.45.-a

Keywords: Chaotic cryptanalysis; Nonlinear dynamical forecasting; Chaos; Hyperchaos

1. Introduction

Since it was found that chaotic waveforms can be used to encrypt signals for secure communications [1], many attempts to break the key of chaotic cryptosystems and to retrieve the information have been reported. A wide class of breaking methods is based on phase space reconstruction of the emitter dynamics through the return map analysis or the use of nonlinear dynamical forecasting (NLDF) [2,3]. Most of those methods have been applied for breaking com-

munication schemes of low dimensionality, ruled by Lorenz and Rossler equations [2,4]. If primarily it was thought that chaotic waveforms with a high dimensionality (hyperchaos) could make it more difficult to extract the message [5], Short and Parker have shown later that increasing the dimension does not necessarily achieve a significant improvement in the security of the system [4].

This Letter considers a specific class of chaotic systems, the delayed nonlinear feedback (DNLF) systems, i.e., systems ruled by nonlinear time-delay differential equation (DDE) whose dynamics can exhibit high-dimensional attractors with many positive Lyapunov exponents. Those few last years, researchers have focused on the use of synchronized chaos to

* Corresponding author.

E-mail address: vladimir.oudaltsov@georgiatech-metz.fr
(V.S. Udaltsov).

achieve secure communication systems. In these systems, identical laser transmitter and receiver chaotic setups are self-synchronized by sending a chaotic-encrypted message signal from the transmitter to the receiver. These systems may represent a significant breakthrough for secure communications since they can provide signal encryption rates that are greater than 1 GHz.

One such laser system was developed in our group, using a wavelength tunable laser diode with a nonlinear feedback and a specific open-loop receiver [6]. This experiment was novel in two important aspects: the dynamics appeared to be of high dimensionality (~ 500) and the feedback function was highly nonlinear (with up to 5 extrema) with the hope of enhancing the privacy of the transmission. The same features were also used in another system we reported later in the radiofrequency domain [7,8] to enhance the security level. However security of these systems is still an open issue although chaotic communications based on simpler encryption schemes have been shown to be susceptible to be cracked mainly in two cases: (i) it was shown that the information transmitted by a DNLF-system with a weak nonlinearity introduced by an erbium optical amplifier in the feedback loop [9] could be successfully unmasked by considering the chaotic waveform as a convolution of the original laser pulses with an “echo”-function associated with the delayed feedback loop [10]; (ii) a second type of attacks was proposed from time-series analysis in the case of Mackey–Glass systems, which feature a nonlinear function with only one extremum [11–13]. In this Letter we report on our investigations of the security features of systems that exhibit a stronger nonlinearity and a more complex encryption process. In order to evaluate the security we used experimental data sets obtained from the setup reported in [6].

2. The method used

A delay feedback system representative of those of concern and used in the experiments reported in [6] is shown in Fig. 1. The transmitter consists of a source (a wavelength tunable laser diode with center wavelength $\Lambda_0 = 1550$ nm), a nonlinear element (a birefringent plate with an optical path-difference $D = 11$ mm between its ordinary and extraordinary

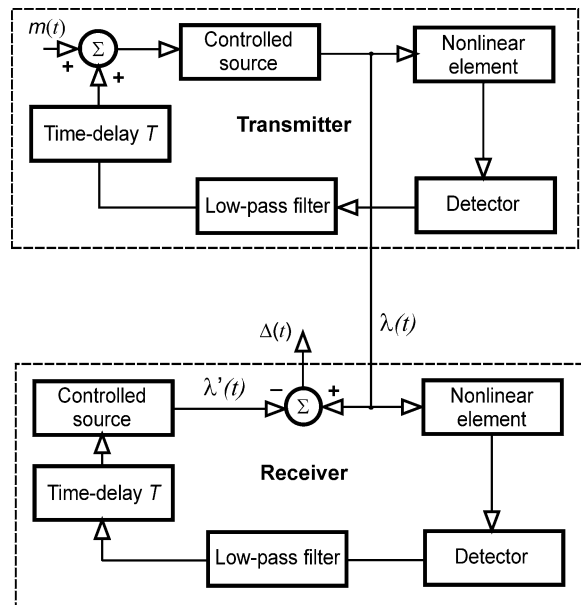


Fig. 1. The block-diagram of the communication DNLF-system.

axes), a detector with a time response $\tau = 8.6$ μ s (the latter being schemed as a low-pass filter in Fig. 1) and a feedback loop with a delay time $T = 510$ μ s. The message signal $m(t)$ is added to the feedback signal in the transmitter to produce the chaotic transmitted signal, which takes the form of chaos in wavelength. The wavelength fluctuations $\lambda(t)$ around Λ_0 in the transmitted beam can be expressed in the general form [14]:

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

with the output signal $x(t) = K\lambda(t)$, $K = \pi D/\Lambda_0^2$. The coefficient β is the bifurcation parameter, $F(x) = \sin^2[x(t) - \Phi]$ is the feedback nonlinear function (with multiple extrema) attached to the birefringent plate, with $\Phi = \pi D/\Lambda_0$. The message $m(t)$ is embedded in the trajectories of $x(t)$ via the function $f(t) = \gamma[m(t) + \tau dm(t)/dt]$ with $\gamma = 10^{-2}$ being an attenuation parameter related to the transmitter. The message is mixed with the chaotic signal inside the feedback loop, and not just added outside the transmitter to the chaotic carrier. The message $m(t)$ changes the dynamics of the entire transmitter; thus the transmitted signal $x(t)$ represents more than simply the superposition of a chaotic signal and the message. Because of this situ-

ation, a high degree of security may be expected. The receiver consists of elements identical to those in the transmitter. The laser diode at the receiver emits light with chaotic fluctuations $\lambda'(t)$ of its wavelength, ruled by [6]

$$y(t) + \tau_R \frac{dy(t)}{dt} = \beta_R F_R[x(t - T_R)] \quad (2)$$

with $y(t) = K\lambda'(t)$. For the authorized receiver, proper delay time $T_R = T$, response time $\tau_R = \tau$, bifurcation parameter $\beta_R = \beta$, and nonlinear function $F_R = F$ allow recovery of the message by subtracting $y(t)$ from $x(t)$, yielding a difference signal

$$\Delta(t) = x(t) - y(t) = m(t). \quad (3)$$

This is the algorithm we adopted in our experiments [6–8]. In contrast, for an unauthorized receiver, the difference signal $\Delta(t)$ is a chaotic error signal, which can be expressed as

$$\begin{aligned} \Delta(t) = & \beta F[x(t - T)] - \beta_R F_R[x(t - T_R)] \\ & + \tau_R \frac{dy}{dt} - \tau \frac{dx}{dt} + f(t), \end{aligned} \quad (4)$$

and direct access to $m(t)$ is clearly impossible without knowing τ , T and the nonlinear function $\beta F[\cdot]$.

Let us now consider an intruder tapping the transmission line. The wavelength fluctuations detected by the eavesdropper in the transmitted light beam are expressed by Eq. (1). Estimates of the dimensionality of the wavelength dynamics have been made, suggesting a Lyapunov dimension of 500 in previous experiments. The encryption scheme described by Eq. (1) has been suspected to produce secure encryption compared with methods where the message is directly added to the chaotic carrier [15], because the message and the chaotic signal couple with each other through a more sophisticated process and a strongly nonlinear function. Assuming, however, that the eavesdropper knows that our encryption algorithm relies on a DDE, then only τ , T and the nonlinear function $\beta F[\cdot]$ are required at most to recover the message from the transmitted signal (note that changing the nonlinear function $F[\cdot]$ used in [6] can be easily put in practice by using an electro-optic crystal instead of a birefringent plate).

To test the breaking method that will be explained hereafter, we adopted a message $m(t)$ formed by the sum of two sine-signals with frequencies of 8 and

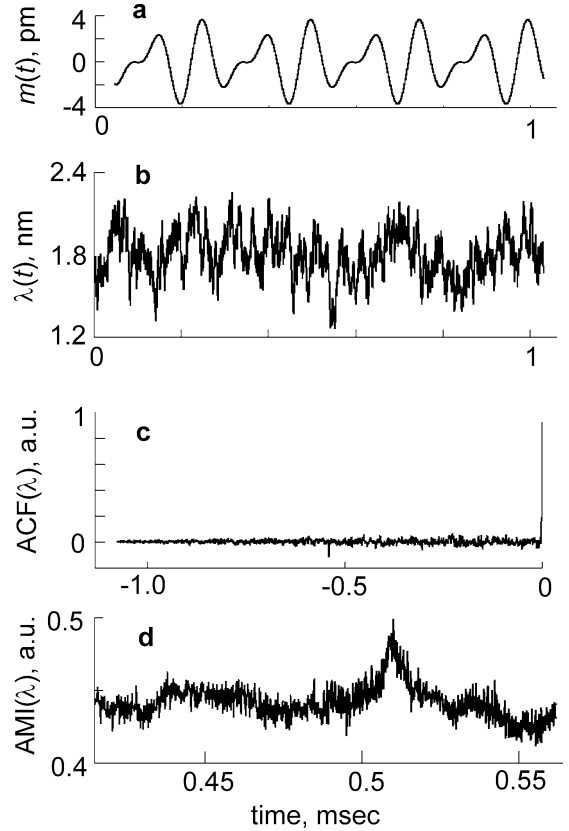


Fig. 2. Examples of signals: (a) the message signal $m(t)$, (b) the transmitted signal $\lambda(t)$, (c) the ACF of transmitted signal, (d) the AMI of transmitted signal.

12 kHz (Fig. 2(a)). The amplitude of this composite message signal was equal approximately to 0.5% of that of the chaotic signal in the feedback loop in order to have a high masking efficiency. The output transmitter signal thus obtained and that we used in our simulations, is shown in Fig. 2(b). It was approximately 1 ms in duration and was sampled at 86 ns intervals to yield $N = 12000$ points.

We start with the assumption that parameters τ and T can be recovered relatively easily. The value of the time response τ can be estimated by analyzing the spectrum of the tapped signal $x(t)$ and measuring its bandwidth (for example, using the least-squares method), which is inversely proportional to τ . Previous results obtained in our experiments have shown that the mismatch of τ in the transmitter and the receiver can reach the value of 4–5% without incurring

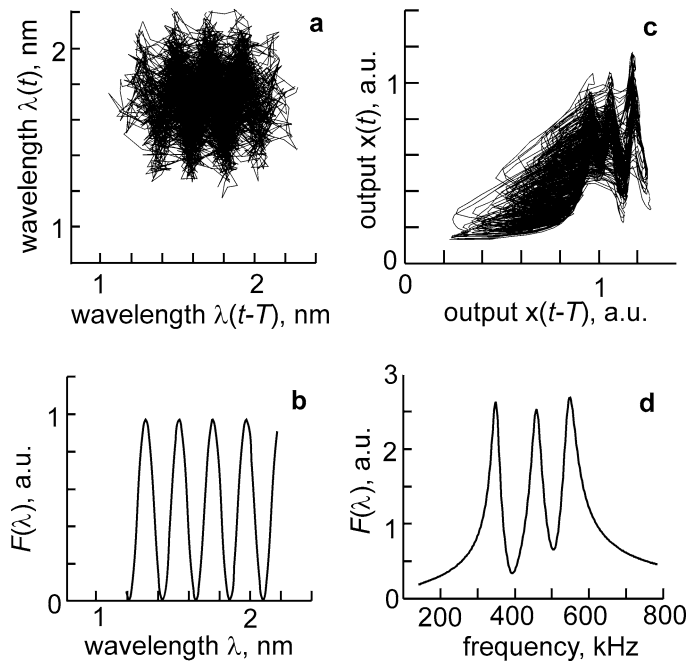


Fig. 3. Examples of the return maps and the nonlinear function F . (a), (c) The return maps; (b), (d) the nonlinear functions F ; (a), (b) for the system [6]; and (c), (d) for the system [7].

dramatic problems in the recovery of the message signal at the receiver, so the value of τ can be known with an accuracy of the order of a few percents. By analyzing the spectrum of the tapped signal $x(t)$, we found $\tau = 9 \mu\text{s}$, a value which is in agreement with the original one within a 5% accuracy. A value of the time-delay T can be also obtained. A few methods can be applied here: (i) the analysis of the autocorrelation function (ACF) of the time series $x(t)$; (ii) the average mutual information technique (AMI) [16]; (iii) the 3D-reconstruction of the derivative of $x(t)$ [13]; (iv) the reconstruction of the return map of $x(t)$ [17]. The example of the calculated ACF of $x(t)$ is shown in Fig. 2(c). A narrow peak can be obtained if the sampling step is small enough (for our setup it must be less than $0.001 T$); the location of the peak gives the value of the time-delay T , with an accuracy that is higher as the sampling step is smaller. The peak corresponding to the time-delay T can be found also observing the AMI of $x(t)$ (Fig. 2(d)). The value of T was found to be $T = 514 \mu\text{s}$ with an accuracy higher than 1% (see also, for example, [13]).

Recovering the type of nonlinearity used in the transmitter is more difficult and can pose problems

when the nonlinear function $F[\cdot]$ features a high complexity such as a high number of extrema. This can be understood from Fig. 3. The return map of the transmitter output $\lambda(t)$ vs. $\lambda(t - T)$ was plotted in Fig. 3(a) to be compared with the nonlinear function F used in the feedback, shown in Fig. 3(b). (As another example, we also show in Fig. 3(c) and (d) the return map and the nonlinear function of the radiofrequency transmitter reported in [7] where the nonlinearity was formed by a set of three oscillating resonant circuits.) It can be seen that only a rough prediction of the type of the nonlinearity used in the transmitter can be obtained using data in Fig. 3(a) and (c). Another method is thus required to extract the information on the nonlinearity used in the transmitter, as we explain below.

The usual operating condition of the chaos-based transmitter is that the amplitude of the message signal is much smaller than the amplitude of the chaotic carrier oscillations, i.e., $m(t) \ll x(t)$ to ensure a high masking efficiency. We also assume that $|dx(t)/dt| \gg |dm(t)/dt|$, that is usually fulfilled in practice, and assume that the dynamics of the variable $x(t)$ can then

be approximately described by the expression

$$x(t) + \tau \frac{dx(t)}{dt} \approx \beta F[x(t - T)]. \quad (5)$$

Eq. (5) is similar to Eq. (1) when the message signal is not injected in the feedback loop [$f(t) = 0$], i.e., this approximation means physically that the local dynamics of the system (during a short time interval less than τ) with and without a message are assumed to be the same. That assumption allows one to apply the analysis of the local dynamics described by Eq. (5) for recovering of Eq. (1). We applied F -forecasting within very small neighborhood $\{x^i\}$ of every point x^i of the transmitted signal by analyzing the dynamics exhibited by the neighboring points. (If the size of $\{x^i\}$ is not small enough the trajectories of the systems described by Eqs. (1) and (5) become significantly different with the time evolution of the message.) Therefore having the series of the sampled signal $x(t)$ and delayed signal $x(t - T)$, one can calculate the function $X(t) = x(t) + \tau dx(t)/dt$, and finally, estimate a forecasting of the function F that can be reconstructed using, for example, an expansion in polynomials (up to degree 2 in [4]) with the least-squares minimization.

Practically the procedure for key breaking that we applied includes the following steps:

(1) We choose the arbitrary series of the sampled output signal $x(t)$ over a time interval approximately a few T -cycles, and the corresponding series of the delayed signal $x(t - T)$.

(2) We calculate the derivative of the transmitted signal at every point x^i as a vector $dx^i/dt = (x^{i+1} - x^{i-1})/2h$, where h is the sampling step, and next the vector $X^i = x^i + \tau dx^i/dt$. It is obvious that the sampling step must be at least a few times smaller than τ .

(3) For a more accurate approximation we choose the points of the series $x_T = x(t - T)$ surrounded by the set of neighbor points $\{x_T^i\}$ that represents small monotonic (in the time domain) pieces. The size of $\{x_T^i\}$ is arbitrary chosen equal to 5% from the value of the difference: $\max(x_T) - \min(x_T)$, where $\max(x_T)$ and $\min(x_T)$ stand for the maximum and minimum values of the series of x_T . In our case the number of points in the neighborhood is typically between 3 and 5.

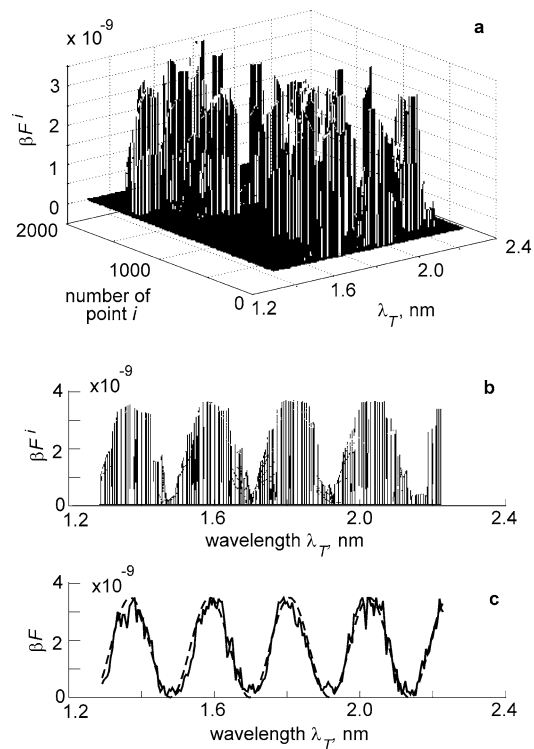


Fig. 4. The reconstruction of the function $\beta F(\lambda)$. (a) The spline cubic approximation as a matrix $\beta F^i(\lambda_T^i)$, (b) the projection of $\beta F^i(\lambda_T^i)$ on the plane $\{\beta F^i, \lambda_T(t)\}$, (c) the averaged values of the βF^i (the dashed curve is the original function describing the nonlinearity involved in the experimental feedback loop).

(4) Next we estimate the interpolation of the function βF^i at every chosen point x_T^i surrounded by a monotonic set $\{x_T^i\}$, using the equation $X^i = \beta F^i(x_T^i)$. Doing that we applied three types of a data interpolation: a spline linear interpolation, a spline parabolic interpolation, and a spline cubic interpolation. An example of the latter interpolation, corresponding to a 2000-point sampled series of $\lambda_T = \lambda(t - T)$, is shown in Fig. 4(a). The projections of βF^i on the plane $\{\beta F^i, \lambda_T\}$ are shown in Fig. 4(b). After averaging a number of time series λ_T we get the forecast of $\beta F(\lambda)$ shown in Fig. 4(c) (solid curve) with the original function $\beta F(\lambda)$ (dashed curve). We obtained qualitatively similar results applying the other noted types of interpolations.

(5) However the results of $[\beta F(\cdot)]$ -forecasting shown in Fig. 4(c) cannot be introduced directly in Eq. (1) to recover the message, due to the resulting

errors that reach 25% of the original values of $\beta F(\cdot)$. The attempts to use these results lead to a chaotic error signal $\Delta(t)$ expressed by Eq. (4), with an amplitude at least 3 times higher than of the message signal. A possible way to overcome that problem is to analyze the signal through a series with much longer duration, but it would take hours of calculations using a PC. We used a faster way to recover the message. The data represented in Fig. 4(b) and (c) show qualitatively that the function $\beta F(\lambda)$ is a periodic function of the $\sin^2(\cdot)$ -type. We then assume that $\beta F(\lambda)$ can be approximated by the expression: $\beta F(\lambda) \approx A \sin^2(B\lambda + C)$, where A , B , and C are the parameters that have to be determined. Then we calculate the 3D-matrix of the fitting error:

$$E_{i,j,k} = \sum_{l=1}^N [\beta F_l - A_i \sin^2(B_j \lambda^l + C_k)]^2, \quad (6)$$

where N is the number of points in Fig. 4(c) used for $[\beta F(\lambda)]$ -forecasting. The matrix is calculated for values within a volume $\{A_i, B_j, C_k\}$ centered on the expected values A , B , and C of the parameters. These values can be obtained in advance using the data shown in Fig. 4(b) and (c). Next we determine the minimum of the error matrix $E_{i,j,k}$. Finally we obtain: $A = 3.44 \text{ nm}$, $B = 14.2 \text{ nm}^{-1}$, and $C = 0.78\pi + n\pi$ (the corresponding values for the parameters of Eq. (1) are: $\beta = 3.5 \text{ nm}$, $K = \pi D/\Lambda_0^2 = 14.4 \text{ nm}^{-1}$, $\Phi_0 = \pi D/\Lambda_0 = 2.43$). Eq. (1) is then reconstructed.

The existence of the minimum of the 3D-matrix $E_{i,j,k}$ is illustrated in Fig. 5. Fig. 5(a) and (b) show a 2D-section $E_{i,k}$, and the corresponding lines of the equal potentials of the surface $E_{i,k}$, respectively. The surface $E_{i,k}$ shown in Fig. 5(a) is calculated within a wide range of the parameters A , B , and C . For example, the parameter C is varied from 0 to π . Having the data shown in Fig. 4(b) and (c), the error-matrix $E_{i,j,k}$ is calculated within a small volume of parameters $\{A_i, B_j, C_k\}$ surrounding the point of the minimum. Practically it takes only a few minutes of calculation.

(6) As the last step the numerical modeling of the receiver can be applied for message recovery. We solved Eq. (2) for the receiver with the obtained values of the parameters A , B , and C . Then we calculated the difference signal $\Delta(t)$ using Eq. (3). The difference signal $\Delta(t)$ thus obtained is shown in Fig. 6(a). It

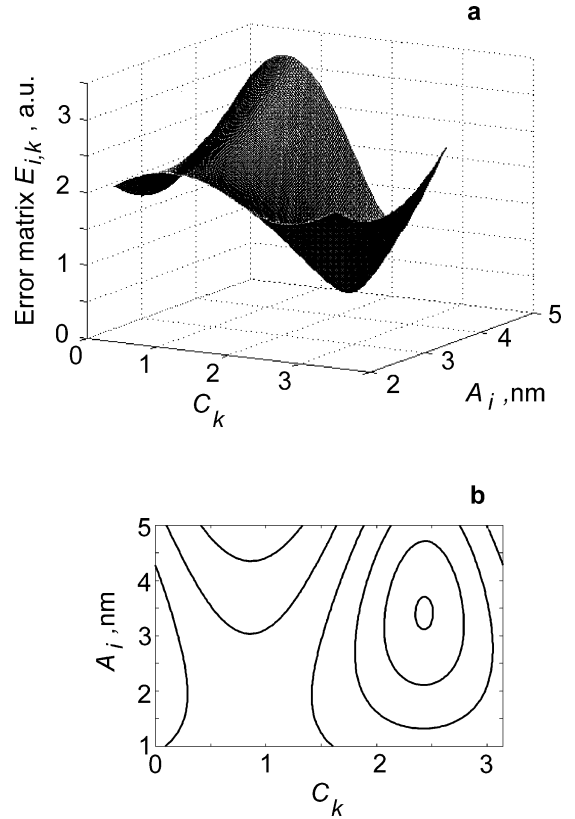


Fig. 5. Minimization of the error matrix $E_{i,j,k}$. (a) The section $E_{i,k}$ of the matrix $E_{i,j,k}$ and (b) the projection of the lines of an equal potential of the surface $E_{i,k}$ on the horizontal plane.

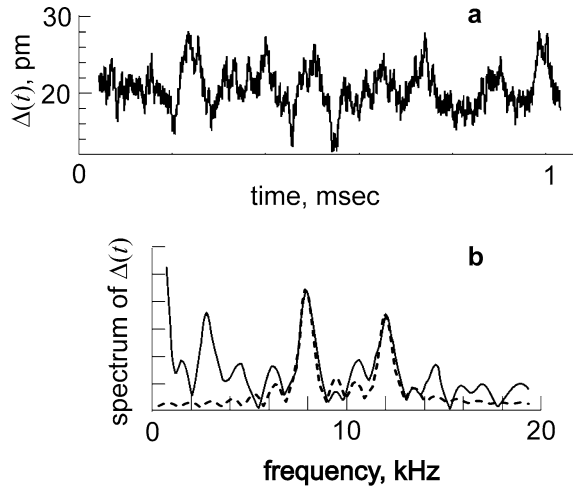


Fig. 6. Recovery of the information signal. (a) The difference signal $\Delta(t)$ and (b) the spectrum of $\Delta(t)$. The dashed line is the spectrum of the original message signal $m(t)$ shown in Fig. 2(a).

can be compared with the original message signal (Fig. 2(a)). The spectrum of $\Delta(t)$ is also shown in Fig. 6(b). One can see the peaks corresponding to the two components of the original transmitted message, showing that the encrypted message is recovered.

3. Conclusion

Finally we have shown that our DNLF-system is not completely safe. The key represented by the five parameters of the system can be broken despite of the very high dimensionality of the chaotic carrier, of the strong nonlinearity involved in the feedback loop, and also despite that, in the experimental method used, the message participates to the chaotic dynamics of the transmitter through a complicated encoding scheme. In the example presented here, we made however explicit use of some a priori knowledge of the \sin^2 -type of nonlinearity used experimentally. This had the result of recovering the message through a fitting method, with three parameters (A , B and C) only to be calculated, but we should comment that the procedure would be much more complex and would take hours of computing if the analytical function describing the nonlinearity was completely unknown by the intruder. This situation is not unrealistic in the experiments on chaos in wavelength [6] since the birefringent plate used can be replaced by a spectral filter featuring any spectral transmission curve nonlinear in wavelength. In that case, the number of parameters to be calculated can be much greater than 3. A more complicated situation can be met if the nonlinear function cannot be expressed analytically since chaotic regimes produced by nonanalytical nonlinear functions are still unsolved mathematically. From that point of view, the possibility to generate more complicated nonlinear functions by using random (and, for example, dynam-

ical) spectral filters in the feedback loop might be a solution to increase key complexity and to make cryptanalysis of such systems extremely difficult.

Acknowledgements

The participation of V.S. Udaltsov was supported by the Centre National de la Recherche Scientifique (CNRS), France.

This work was funded by the EEC (Contract IST-2000-29683, OCCULT).

References

- [1] K.M. Cuomo, A.V. Oppenheim, *Phys. Rev. Lett.* 71 (1993) 65.
- [2] G. Pérez, H.A. Cedeira, *Phys. Rev. Lett.* 74 (1995) 1970.
- [3] K.M. Short, *Int. J. Bifur. Chaos Appl. Sci. Engrg.* 6 (1996) 367.
- [4] K.M. Short, A.T. Parker, *Phys. Rev. E* 58 (1998) 1159.
- [5] L. Kocarev, U. Parlitz, T. Stojanovski, *Phys. Lett. A* 217 (1996) 280.
- [6] J.P. Goedgebuer, L. Larger, H. Porte, *Phys. Rev. Lett.* 80 (1998) 2249.
- [7] L. Larger, V.S. Udaltsov, J.P. Goedgebuer, W.T. Rhodes, *Electron. Lett.* 36 (2000) 199.
- [8] L. Larger, J.P. Goedgebuer, V.S. Udaltsov, W.T. Rhodes, *Electron. Lett.* 37 (2001) 594.
- [9] G.D. VanWiggeren, R. Roy, *Science* 279 (1998) 1198.
- [10] J.B. Geddes, K.M. Short, K. Black, *Phys. Rev. Lett.* 83 (1999) 5389.
- [11] B. Mensour, A. Longtin, *Phys. Lett. A* 244 (1998) 59.
- [12] M.J. Brüner, Th. Meyer, A. Kittel, J. Parisi, *Phys. Rev. E* 56 (1997) 5083.
- [13] Ch. Zhou, C.-H. Lai, *Phys. Rev. E* 60 (1999) 320.
- [14] V.S. Udaltsov, J.P. Goedgebuer, L. Larger, W.T. Rhodes, *Phys. Rev. Lett.* 86 (2001) 1892.
- [15] L.M. Pecora, T.L. Carroll, *Phys. Rev. Lett.* 64 (1990) 821.
- [16] A. Fraser, H. Swinney, *Phys. Rev. A* 33 (1986) 1134.
- [17] R. Hegger, M.J. Brüner, H. Kantz, A. Giaquinta, *Phys. Rev. Lett.* 81 (1998) 558.