A Letters Journal Exploring
the Frontiers of Physics

OFFPRINT

Experimental demonstration of bidirectional chaotic communication by means of isochronal synchronization

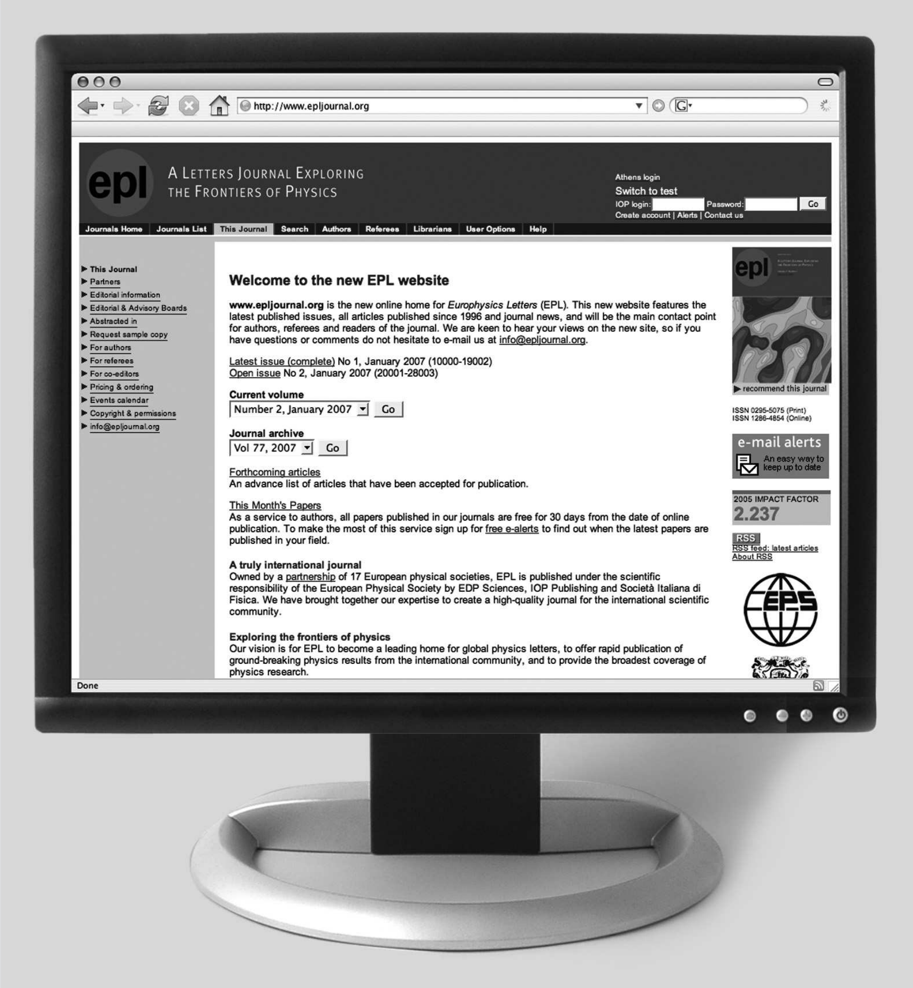
A. Wagemakers, J. M. Buldú and M. A. F. Sanjuán

EPL, **81** (2008) 40005

TAKE A LOOK AT THE NEW EPL

Europhysics Letters (EPL) has a new online home at

www.epljournal.org



Welcome to the new EPL website

www.epljournal.org is the new online home for *Europhysics Letters* (EPL). This new website features the latest published issues, all articles published since 1996 and journal news, and will be the main contact point for authors, referees and readers of the journal. We are keen to hear your views on the new site, so if you have questions or comments do not hesitate to e-mail us at info@epljournal.org.

Latest issue (complete) No 1, January 2007 (10000-19002)
Open issue No 2, January 2007 (20001-28003)

Current volume
Number 2, January 2007 Go

Journal archive
Vol 77, 2007 Go

Forthcoming articles
An advance list of articles that have been accepted for publication.

This Month's Papers
As a service to authors, all papers published in our journals are free for 30 days from the date of online publication. To make the most of this service sign up for free e-alerts to find out when the latest papers are published in your field.

A truly international journal
Owned by a partnership of 17 European physical societies, EPL is published under the scientific responsibility of the European Physical Society by EDP Sciences, IOP Publishing and Società Italiana di Fisica. We have brought together our expertise to create a high-quality journal for the international scientific community.

Exploring the frontiers of physics
Our vision is for EPL to become a leading home for global physics letters, to offer rapid publication of ground-breaking physics results from the international community, and to provide the broadest coverage of physics research.

ISSN 0295-5075 (Print)
ISSN 1286-4854 (Online)

Take a look for the latest journal news and information on:

- reading the latest articles, free!
- receiving free e-mail alerts
- submitting your work to EPL

www.epljournal.org

A Letters Journal Exploring the Frontiers of Physics

February 2008

EPL, **81** (2008) 40005 www.epljournal.org
doi: 10.1209/0295-5075/81/40005

Experimental demonstration of bidirectional chaotic communication by means of isochronal synchronization

A. Wagemakers[(a)], J. M. Buldú and M. A. F. Sanjuán[(b)]

Nonlinear Dynamics and Chaos Group, Departamento de Física, Universidad Rey Juan Carlos
Tulipán s/n, 28933 Móstoles, Madrid, Spain

received 17 September 2007; accepted in final form 17 December 2007
published online 21 January 2008

PACS 05.45.Xt – Synchronization; coupled oscillators
PACS 42.55.Px – Semiconductor lasers; laser diodes
PACS 42.65.Sf – Dynamics of nonlinear optical systems; optical instabilities, optical chaos and complexity, and optical spatio-temporal dynamics

Abstract – We give the first experimental demonstration of simultaneous bidirectional communication through chaotic carriers thanks to the phenomenon of isochronal synchronization. Two Mackey-Glass electronic circuits with chaotic behaviour exchange their signals through a coupling line with delay. When the internal feedback of the circuits and the coupling are accurately matched, isochronal synchronization arises. Under this dynamical regime, we introduce a binary message at both outputs and recover it at the opposite circuit. Finally, we discuss the security of this kind of communication system by analyzing the message recovered by a potential eavesdropper.

Introduction. – Probably, one of the most promising application of the synchronization of chaotic systems is its use in secure communications. First proposed by Pecora and Carroll in their seminal paper about chaos synchronization [1], the transmission/recovery of an encrypted message using chaotic systems was experimentally demonstrated by Kocarev *et al.* two years later [2]. The message recovery process relies on the chaos-pass filtering properties of the synchronized chaotic systems, *i.e.*, when a message is introduced in the chaotic carrier output of the transmitter system, the receiver synchronizes only with the chaotic part of its input signal and the message can be recovered after a straightforward signal treatment. Therefore, synchronization between chaotic systems is a necessary requirement in communications with chaotic carriers, nevertheless synchronization can have many faces [3]. If we assume a certain delay in the coupling line, which would correspond to the case of real applications, it would be possible to define different kinds of synchronization by taking into account the delay between the synchronized systems. In the most general case, the receiver follows the transmitter output with a lag equal to the coupling time, in what is usually called achronal synchronization [4]. However, if the internal parameters of the coupled systems are adequately tuned, it is possible to obtain anticipated synchronization [5,6], where the receiver system advances in time the dynamics of the transmitter. The intermediate case is known as isochronal synchronization [7] (also called zero-lag synchronization) and corresponds to the situation where both chaotic systems have the same dynamics at exactly the same moment, despite the time lost in the transmission line. Isochronal synchronization has been observed in the dynamics of interconnected cortical areas of the brain [8–10] and it has been recently reproduced in small arrays of coupled chaotic lasers [11,12] and electronic circuits [13] where bidirectional coupling was introduced. It is within the framework of lasers that isochronal synchronization has been proposed as a technique to bidirectionally encrypt/decrypt a message. Two recent works [14,15] have shown by means of numerical simulations that it is possible to establish bidirectional secure communication between two independent chaotic lasers and, in addition, messages can be sent simultaneously (*i.e.*, both lasers sending/receiving messages at the same time). More recently, unidirectional message transmission in the framework of isochronal synchronization has been shown experimentally in semiconductor lasers with opto-electronic feedback [16].

[(a)] E-mail: alexandre.wagemakers@urjc.es
[(b)] E-mail: miguel.sanjuan@urjc.es

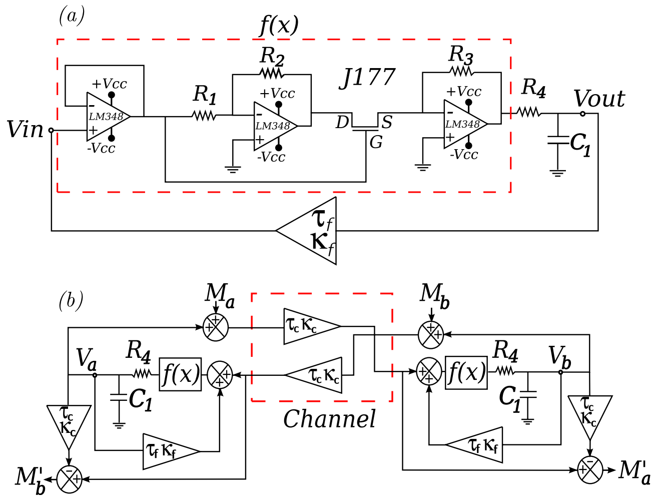


Fig. 1: (Colour on-line) In (a) a single Mackey-Glass circuit is represented. The circuit is composed of a nonlinear function $f(x)$ outlined in the dashed box. At the output of the nonlinear function a simple RC circuit, composed of R_4 and C_1, integrates the voltage V_{out}. V_{out} is further introduced into a delayed feedback loop, represented by a triangle. The symbols τ_f and κ_f correspond to the feedback delay and feedback strength, respectively. Parameter values are: $R_1 = 1\,\text{k}\Omega$, $R_2 = 0.5\,\text{k}\Omega$, $R_3 = 4\,\text{k}\Omega$, $R_4 = 1\,\text{k}\Omega$, $C_1 = 1\,\mu\text{F}$, J177 is a JFET transistor and LM348 is an operational amplifier. In (b) we plot the schematic setup of the experiment corresponding to the transmission of a message with chaotic masking. The outputs of two identical Mackey-Glass circuits are coupled through a digital delay line and then they are added to the feedback signal of the opposite circuit.

In this letter we present, to the best of our knowledge, the first experimental demonstration of simultaneous bidirectional communication between two chaotic systems by means of isochronal synchronization. First, we synchronize two Mackey-Glass electronic circuits with time-delayed feedback, where, a delay is also introduced in the coupling line. Both systems are coupled bidirectionally and isochronal synchronization arises when feedback and coupling parameters are accurately matched. Then an encrypted message is introduced in both chaotic outputs and recovered at the opposite system. Finally we show how this encryption technique is suitable to negotiate an encryption key between both systems, even in the case that an eventual eavesdropper has access to both transmitted signals.

Experimental setup. – We have chosen a Mackey-Glass electronic circuit [17–19] as the chaotic system to encrypt/decrypt the transmitted messages. The electronic circuit, based on the Mackey-Glass model, is shown in fig. 1(a) and consists in a nonlinear oscillator whose oscillations are induced by the feedback loop with delay. Three basics elements can be distinguished. First of all, a nonlinear function $f(x)$, which processes the signal V_{in}, so that it feeds the analog integrator with the voltage $f(V_{in})$. This integrator is the second element of the system and it is composed of a simple RC circuit, represented by R_4 and C_1. The voltage at the capacitor C_1 is the dynamical variable V_{out}, which is sent in turn to the third element, a digital delay line represented by a triangle in fig. 1(a). Along the delay line, a gain κ_f and a delay τ_f is applied to the voltage V_{out}, so that the voltage $V_{in}(t)$ at the output of the delay line is $V_{in}(t) = \kappa_f V_{out}(t - \tau_f)$.

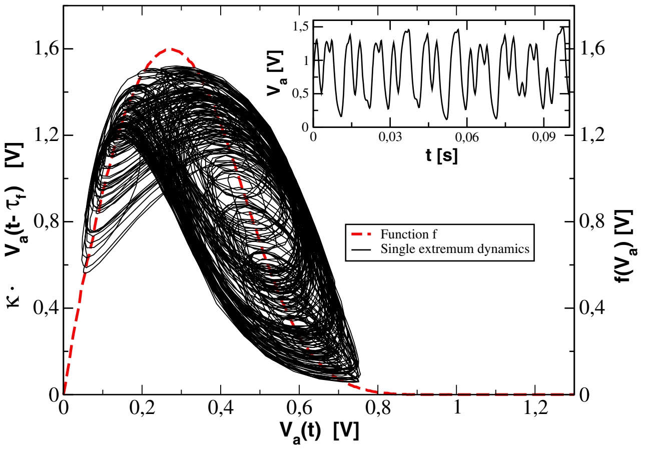


Fig. 2: (Colour on-line) Chaotic attractor of the system in the phase space given by $[V_a,\ V_a(t - \tau_f)]$ and the corresponding time series (inset) for an uncoupled Mackey-Glass circuit. The overall aspect of the attractor reflects the nonlinear function f (dashed line). The maximum value of this function is $V_{max} = 1.605\,\text{V}$ which scales the dynamics of the circuit. The feedback parameters of the system for this experiment are: $\tau_f = 8\,\text{ms}$, $\kappa_f = 1$. The threshold for the feedback strength which undergoes a Hopf bifurcation is $\kappa_f = 0.55$, below this value the system does not oscillate. However, this threshold depends on the delay τ_f of the feedback loop.

The differential equations that represent this circuit are quite similar to the Mackey-Glass model. The form of the nonlinearity differs slightly with the original Mackey-Glass model [17] and it can be seen in fig. 2 (dashed line). However, these differences do not change the main characteristics of the system. Equations corresponding to the circuit of fig. 1(a) can be easily deduced by circuit analysis. We obtain the differential equation:

$$R_4 C_1 \frac{\mathrm{d}V_{out}}{\mathrm{d}t} = -V_{out} + f(\kappa_f V_{out}(t - \tau)), \qquad (1)$$

where the nonlinear function $f(\kappa_f V_{out}(t - \tau))$ depends on a p-channel JFET (Junction Field Effect Transistor).

Now we describe the communication setup which consists in a coupling line with delay that connects two identical Mackey-Glass electronic circuits (see fig. 1(b)). Both circuits are coupled to each other (bidirectionally) by adding the output signals V_{out} to the variables V_{in} of the opposite circuit. The variable V_{out} of each circuit is sent through a digital coupling line with a certain delay and gain. The equations of the coupled system represented in the fig. 1(b) are:

$$R_4C_1\frac{\mathrm{d}V_a}{\mathrm{d}t} = -V_a + f(\kappa_f V_a^{\tau_f} + \kappa_c(V_b^{\tau_c} + M_b^{\tau_c})), \qquad (2)$$

$$R_4C_1\frac{\mathrm{d}V_b}{\mathrm{d}t} = -V_b + f(\kappa_f V_b^{\tau_f} + \kappa_c(V_a^{\tau_c} + M_a^{\tau_c})), \qquad (3)$$

where variables V_a and V_b correspond to the output variable of each circuit, and the superscript τ_c means the delayed variable, *i.e.*, $V_a^{\tau_f} = V_a(t-\tau_f)$. The encrypted messages are M_a and M_b and they are introduced at V_a and V_b, respectively, by means of a voltage adder, in a classical chaos masking encryption way. A parallel method of introducing the message through the feedback loop has been recently proposed [20], however, a third dynamical unit is required in this case.

The digital delay line is composed of an autonomous microcontroller with on-board memory and DAC (Digital-to-Analog Converter) and ADC (Analog-to-Digital Converter) converters. The signal is first converted to a digital signal and then stored into a FIFO buffer and after a number of clock ticks, the signal is then converted back into analog. The gains κ_f and κ_c and the delay τ_c of each channel can be adjusted by software, so that we can make automated measurement for several gains and delays. The delay ranges from 0 to 20 ms. The gains κ_f and κ_c have values in the interval [0, 1].

Finally, the output signals of both circuits are sampled with an ADC sampling board connected to a computer and signals are later analyzed with Matlab software. More details of the experimental setup can be found in ref. [13].

Isochronal synchronization. – Figure 2 shows the dynamics of one of the circuits in the absence of coupling, which behaves chaotically for a sufficient feedback and delay. The output voltage V_a exhibits a single extremum dynamics when plotted in the phase space defined by $[V_a, V_a(t-\tau_f)]$, which reflects its chaotic behaviour. Both circuits behave similarly, since the only difference between them is introduced by the tolerance of their electronic components.

At this point, we couple together both circuits through a delay line of gain κ_c and delay τ_c. When the bidirectional coupling is introduced different scenarios arise, as it can be observed in the bifurcation diagram of fig. 3 (left inset). From low to moderate coupling strengths, both circuits behave chaotically, although windows of N-period oscillations arise for intermediate and high couplings.

Since we are interested in communicating through chaotic masking, we set the coupling strength to $\kappa_c = 0.3$ which sets the system to lie within the chaotic region. Figure 3 shows the outputs of both circuits corresponding to the mentioned value of κ_c and a coupling delay time of $\tau_c = 18$ ms. We can observe how the system is highly synchronized without a delay between both outputs, despite the time lost in the transmission line. This is the typical signature of isochronal synchronization.

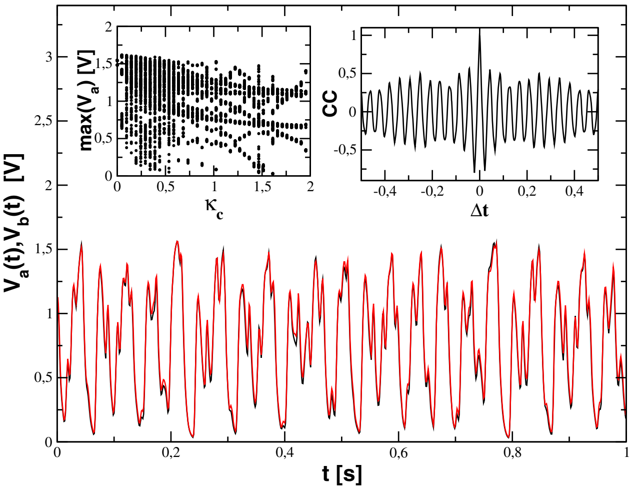


Fig. 3: (Colour on-line) Time series of both circuit outputs V_a (black line) and V_b (red line) under isochronal synchronization ($\kappa_c = 0.3$). Inset on the left shows the bifurcation diagram of the coupled system as a function of the coupling strength κ_c with a fixed coupling delay of $\tau_c = 18$ ms. The right inset shows the cross-correlation function under isochronal synchronization. A maximum of 0.99 is observed at $\Delta t = 0$, which indicates that there is no delay between both outputs. Time series and cross-correlation function plotted here are obtained for $\kappa_c = 0.3$. The time window used for the computation of the cross-correlation is 1.3 s. Feedback parameters (equal for both circuits) are $\tau_f = 18$ ms and $\kappa_f = 0.4$. The rest of the internal parameters are those given in fig. 1.

In order to characterize the quality of the synchronization and to evaluate the delay between the output of both circuits we compute the Cross-Correlation function (CC) between the V_a and V_b. The CC function is defined as:

$$C(\Delta t) = \frac{\langle (V_a(t) - \langle V_a\rangle)(V_b(t+\Delta t) - \langle V_b\rangle)\rangle}{\sqrt{\langle (V_a(t) - \langle V_a\rangle)^2\rangle\langle (V_b(t) - \langle V_b\rangle)^2\rangle}},$$

where the brackets indicate time averaging. In this way we compute the correlation between time series for different shifts in the time axis, obtaining the quality of the synchronization $(-1 < C(\Delta t) < 1)$ and the delay between the time series, indicated by the position of the maximum of the CC function.

In the right inset of fig. 3, we plot the CC function, which confirms that we are dealing with isochronal synchronization since: a) The maximum of the CC (~ 0.99) function has a value close to unity, indicating the synchronized behaviour and b) the maximum is placed at $\Delta t = 0$, which reflects that there is no delay between both outputs despite the time taken in the transmission line. Note that similar to ref. [12], the bidirectional coupling and the inclusion of the feedback loops lead to a stable zero-lag synchronization, *i.e.*, leader-laggard alternation between both outputs is not observed.

We have repeated the experiment for different values of κ_c and τ_c, obtaining similar results. The only requirement to obtain isochronal synchronization with high

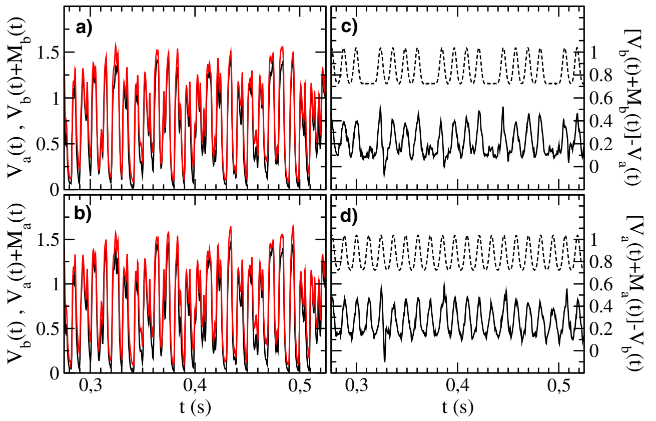


Fig. 4: (Colour on-line) (a) and (b) show the input and output signals of circuit a and b, respectively. The message can be recovered by subtraction of both signals. Plots (c) and (d) show the transmitted (dashed line) and recovered (solid line) message at both circuits.

cross-correlation values is to accurately match the feedback and the coupling delay, *i.e.*, $\tau_c = \tau_f$, as previously reported in [12].

Bidirectional communication. – Since the synchronization is a necessary condition to communicate by means of chaotic masking, the next step is the evaluation of the ability of the system to encrypt/decrypt a message.

We introduce a binary message with a bit rate of 80 b/s. In the frequency domain, the message is hidden by the broad spectrum of the circuit dynamics, which has a peak at ~ 120 Hz. The transition between the 0/1 state has been filtered since we have observed that drastic jumps worsen synchronization. The amplitude of the message must be as low as possible to guarantee a good encryption, but it is also limited by the amplitude of the intrinsic noise of the system, which hinders the message recovery for low values of the message amplitude. Taking into account both restrictions, we have selected a message amplitude of 0.4 V for the clarity of the results. It corresponds to a 25% of the RMS value of the circuit output.

Figures 4(a), (b) show the input and output signals of both circuits, where a message has been already added to both chaotic signals. A message $M_b(t)$ is encrypted by chaos masking with the $V_b(t)$ signal, while at the opposite circuit a message $M_a(t)$ is masked by $V_a(t)$. In order to recover the message, the input signal has been shifted a time τ_c, since it is the time taken by the output signal to arrive at the opposite circuit. We can observe how, by subtracting the output to the input signal, it is possible to decrypt the transmitted message, whose quality can be improved further by filtering and reshaping. Note that thanks to the bidirectional coupling both systems are sending/receiving a message simultaneously, something that cannot be achieved in unidirectional communication.

It is worth to distinguish from two similar but different bit-recovery scenarios. When both circuits are sending and receiving the same bit, we obtain identical synchronization, which can be analytically demonstrated by substituting $V_a = V_b$ and $M_a = M_b$ in eqs. (2), (3). Intuitively, we can argue that if both outputs are synchronized, and the same signal ($M_a = M_b$) is perturbing both inputs, we are helping to synchronize both outputs thanks to a common external signal (*i.e.*, the message). A different, but also efficient, bit-recovery process occurs when circuits are sending different bits. In this case, the added message, whose amplitude should be low enough to be hidden by the chaotic signal, is treated by the receiving circuit as additive noise, which is filtered due to the chaos-pass filtering properties of the synchronized system [14]. In both cases, the intrinsic noise of the electronic circuits, and the tolerance of the electronic components, lead to the appearance of noisy fluctuations at the recovered message, which translates into a similar quality in the recovered bit. However, an appropriate filtering together with a threshold-passing treatment lead to a satisfactory recovery of the message.

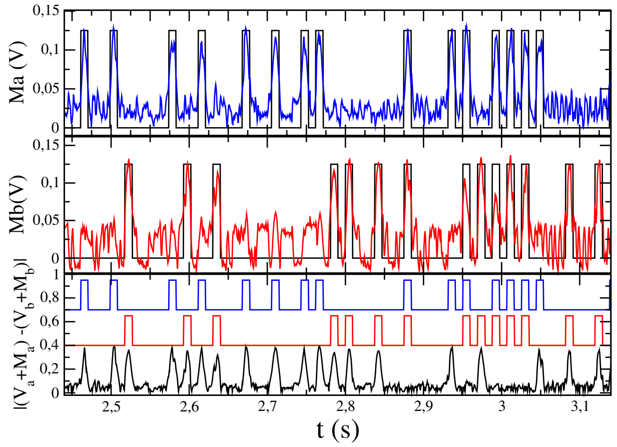


Fig. 5: (Colour on-line) Transmitted bits (solid lines) and recovered signals at circuit a (blue lines) and b (red lines). The bottom figure corresponds to the absolute value of the signal recovered by an eavesdropper. We can observe that only when two bits do not coincide, the transmitted signal can be recovered by an eavesdropper.

Arriving at this point it is worth discussing the security of this kind of transmission. Since the signal of both circuits is accessible to a potential eavesdropper, it would be reasonable to think that the eavesdropper could be able to recover the encrypted messages by subtracting both signals (note that in unidirectional communication only one signal is accessible). Nevertheless, as it has been proposed in refs. [14,15], it is a suitable technique to negotiate a secret key between the users. Figure 5 shows the message recovered by a possible eavesdropper (bottom time series) when both users are communicating. We can observe that when a bit "1" (or "0") is sent by the two systems at the same time, the eavesdropper do not detect its presence, since the bit is suppressed when doing the signal subtraction. Only when two bits do not coincide the eavesdropper recovers the bit. In this way both users could send a certain number of bits randomly distributed and take the first N bits that coincide as the secret key to communicate. Note that each receiver system knows which are the right bits by simply comparing the received signal with the sent signal.

Conclusions. – We have shown that two bidirectionally coupled Mackey-Glass electronic circuits can exhibit isochronal synchronization despite the delay existing in the transmission line. Isochronal synchronization appears for a wide range of coupling time and is robust against the intrinsic noise of the electronic systems. We have used the isochronal synchronization in order to transmit, bidirectionally and simultaneously, an encrypted message. Finally, we have shown the ability of this kind of communication to negotiate secret keys between users. When a potential eavesdropper has access to both transmitted signals he/she is not able to recover the whole chain of transmitted bits, since bits that coincide are not detected. Despite this type of secure communication has been recently proposed, we give here the first experimental implementation.

***

Financial support from the Ministry of Education and Science (Spain) under Project No. FIS2006-08525 is acknowledged.

REFERENCES

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

[2] Kocarev L., Halle K. S., Eckert K., Chua L. O. and Parlitz U., *Int. J. Bifurcat. Chaos*, **2** (1992) 709.

[3] Pikovsky A. S., Rosenblum M. G. and Kurths J., *Synchronization: A universal concept in nonlinear sciences* (Cambridge University Press) 2004.

[4] Heil T., Fischer I., Elsässer W., Mulet J. and Mirasso C. R., *Phys. Rev. Lett.*, **86** (2001) 795.

[5] Voss H. U., *Phys. Rev. E*, **61** (2000) 5115.

[6] Masoller C., *Phys. Rev. Lett.*, **86** (2001) 2782.

[7] Schwarz I. B. and Shaw L., *Phys. Rev. E*, **75** (2007) 046207.

[8] Engel A. K., König P., Kreiter A. K. and Singer W., *Science*, **252** (1991) 1177.

[9] Roelfsema P. R., Engel A. K., König P. and Singer W., *Nature*, **385** (1997) 157.

[10] Chawla D., Friston K. J. and Lumer E. D., *Neural Netw.*, **14** (2001) 727.

[11] Fischer I., Vicente R., Buldú J. M., Peil M., Mirasso C. R., Torrent M. C. and García-Ojalvo J., *Phys. Rev. Lett.*, **97** (2006) 123902.

[12] Klein E., Gross N., Rosenbluh M., Kinzel W., Khaykovich L. and Kanter I., *Phys. Rev. E*, **73** (2006) 066214.

[13] Wagemakers A., Buldú J. M. and Sanjuán M. A. F., *Chaos*, **17** (2007) 023128.

[14] Klein E., Gross N., Rosenbluh M., Kinzel W., Khaykovich L. and Kanter I., *Phys. Rev. E*, **74** (2006) 046201.

[15] Vicente R., Mirasso C. R. and Fischer I., *Opt. Lett.*, **32** (2007) 403.

[16] Peil M., Larger L. and Fischer I., *Phys. Rev. E*, **76** (2007) 045201.

[17] Mackey M. C. and Glass L., *Science*, **197** (1977) 287.

[18] Kim M.-Y., Sramek C., Uchida A. and Roy R., *Phys. Rev. E*, **74** (2006) 016211.

[19] Namajunas A., Pyragas K. and Tamasevicius A., *Phys. Lett. A*, **201** (1995) 42.

[20] Zhou B. and Roy R., *Phys. Rev. E*, **75** (2007) 026205.