# Chaos Shift Keying: Modulation and Demodulation of a Chaotic Carrier Using Self-Synchronizing Chua's Circuits

Hervé Dedieu, *Member, IEEE,* Michael Peter Kennedy, *Member, IEEE,* and Martin Hasler, *Fellow, IEEE*

***Abstract*— We describe a technique for transmitting digital information using a chaotic carrier. Each symbol to be transmitted is coded as an attractor in Chua's circuit. The symbols are detected at the receiver by cascaded self-synchronizing Chua's circuit subsystems. A proof of the synchronization effect is demonstrated using weak assumptions on the statistical behavior of the chaotic carrier to be transmitted. Furthermore a bound for the average time of synchronization is given. Results of both practical experimentation and simulations are presented which verify our approach.**

## I. Introduction

### A. Background

It HAS BEEN REPORTED in very recent studies [1]–[4] that it is possible to design synchronizing systems driven by chaotic signals. Although the concept of chaotic systems 'seems to defy synchronization' since two identical chaotic systems started at nearly the same initial conditions have trajectories which quickly become uncorrelated, Pecora and Carroll [1]–[4] have theoretically and experimentally shown that it is possible to create chaotic systems in such a way that

- a first (chaotic) system called the driving system transmits some of its state variables (called the driving signals) to a second system called the response system. This forces the state variables of the response system to synchronize with the other state variables not passed to the response system.
- A necessary and sufficient condition for the synchronization given by Pecora and Carroll is that all the conditional Lyapunov exponents associated with some variational equation be negative. The term "conditional" comes from the fact that the Lyapunov exponents depend on the driving signals.

The importance of the discovery by Pecora and Carroll has been quickly highlighted in the signal processing and circuits and systems communities. Oppenheim *et al.* [5] have reported some applications of what they have called "chaotic switching" and "chaotic masking and modulation." In particular, they showed how the concept of synchronization can be used to mask information by adding a chaotic signal to a speech signal to be transmitted. The chaotic signal used as a noise-like signal is recovered by the receiver using the synchronization effect. The speech signal is simply obtained by subtraction. More recently Kocarev *et al.* [6] have also applied the ideas of Pecora and Carroll in the context of chaotic masking ("secure communications"). They used a Chua's circuit as a simple generator of chaotic signals. They experimentally showed the synchronization effect in an application very similar to the one described in [5] in which the information signal is buried in the chaotic signal. It should be noted that in the two approaches the power level of the information signal must be significantly lower than the power of the chaotic signal in order for synchronization to be possible.

### B. Motivation

In the context of chaotic masking, the addition of a chaotic signal to an information signal suffers from certain disadvantages. Principal among these is the requirement that the level of the information signal be lowered to at least 30 dB below the level of the chaotic signal. The consequence is that it is difficult to ensure a correct detection if a noise of the same power level as the information signal corrupts the chaotic signal. Instead of adding a chaotic noise to an information signal, a rather different point of view is taken in this paper in which the chaotic signal itself directly bears the information. In taking from the work of Kocarev *et al.* [6], we use a Chua's circuit to develop a shift keying technique for the coding/decoding of binary signals where the carrier signal is chaotic. The main points we address in this paper are the following.

- We propose a simple architecture for the implementation of modulation with an analog chaotic carrier.
- We prove the synchronization effect. We do not use the computation of the conditional Lyapunov exponents and use instead weak assumptions on the driving signal.
- We explain how to compute a bound for the average time of synchronization.
- We verify our approach by simulation and experiment.

## II. Modulation and Demodulation of Chaotic Signals Using Chua's Circuit

The transmitter is based on a Chua's circuit (see Fig. 2) whose chaotic behavior has been widely studied [8]–[11]. It

Manuscript received June 4, 1993; revised June 17, 1993. This paper was recommended by Guest Editor L. O. Chua.

H. Dedieu and M. Hasler are with the Department of Electrical Engineering, Swiss Federal Institute of Technology, Lausanne, Switzerland.

M. P. Kennedy is with the Department of Electronic and Electrical Engineering, University College Dublin, Belfield, Dublin, Ireland.

IEEE Log Number 9211621.

consists of a single nonlinear resistor (see Fig. 1) and four linear circuit elements: two capacitors, an inductor and a resistor. Details of the synthesis of the nonlinear resistor can be found in [7]. The modulation device runs as follows. A binary data stream (the signal to be transmitted) "modulates" the chaotic carrier $v_{C1}(t)$. If an input bit $+1$ has to be transmitted the switch of Fig. 2 is kept open for a time interval $T$. If the next bit to be transmitted is $-1$, the switch is closed connecting in parallel the resistor $r$ with the nonlinear negative resistor. During the transmission of the $-1$ bit, the device can be seen as a Chua's circuit with a three-segment piecewise-linear resistor having a slope $G_0' = G_0 + \frac{1}{r}$ in the central region and a slope $G_1' = G_1 + \frac{1}{r}$ in the outer region. The breakpoints $B_p$ remain unchanged. The following three equations describe the dynamics of the modulation system:

$$C_1 \frac{dv_{C1}(t)}{dt} = \frac{1}{R}(v_{C2}(t) - v_{C1}(t)) - h_{\pm}(v_{C1}(t)) \quad (1)$$

$$C_2 \frac{dv_{C2}(t)}{dt} = -\frac{1}{R}(v_{C2}(t) - v_{C1}(t)) + i_{L1}(t) \quad (2)$$

$$L \frac{di_{L1}(t)}{dt} = -v_{C2}(t). \quad (3)$$

The function $h_{\pm}$ in (1) has the following meaning; during a bit 1 transmission $h_{\pm} = h_{+}$, where $h_{+}$ is the three-segment piecewise-linear function with slopes $G_0$, $G_1$ and breakpoints $-B_p$ and $+B_p$; during a bit $-1$ transmission $h_{\pm} = h_{-}$ where $h_{-}$ is the three-segment piecewise-linear function with slopes $G_0'$, $G_1'$ and breakpoints $-B_p$ and $+B_p$. We suppose that the signal $v_{C1}(t)$ is transmitted to the receiver without any alteration. The receiver is made of three subsystems (See Figs. 3–5). The goal of the first subsystem is to create as close as possible a copy of the signal $v_{C2}(t)$, this signal will be referred to as $v_{C21}(t)$. The first subsystem is governed by the two following equations:

$$C_2 \frac{dv_{C21}(t)}{dt} = \frac{1}{R}(v_{C1}(t) - v_{C21}(t)) + i_{L2}(t) \quad (4)$$

$$L \frac{di_{L2}(t)}{dt} = -v_{C21}(t). \quad (5)$$

The second and the third subsystem are designed to produce the signals $v_{C12}(t)$ and $v_{C12}'(t)$. As it will be shown in the theoretical part $v_{C12}(t)$ converges to $v_{C1}(t)$ during the transmission of $+1$ bit while $v_{C12}'(t)$ converges to $v_{C1}(t)$ during the transmission of $-1$ bit. Equation (6) governs the second subsystem while (7) governs the third subsystem.

$$C_1 \frac{dv_{C12}(t)}{dt} = \frac{1}{R}(v_{C21}(t) - v_{C12}(t)) - h_{+}(v_{C12}(t)) \quad (6)$$

$$C_1 \frac{dv_{C12}'(t)}{dt} = \frac{1}{R}(v_{C21}(t) - v_{C12}') - h_{-}(v_{C12}'(t)). \quad (7)$$

Additional elements for the circuits of Figs. 3–5 remain to be designed for the synchronization detectors.

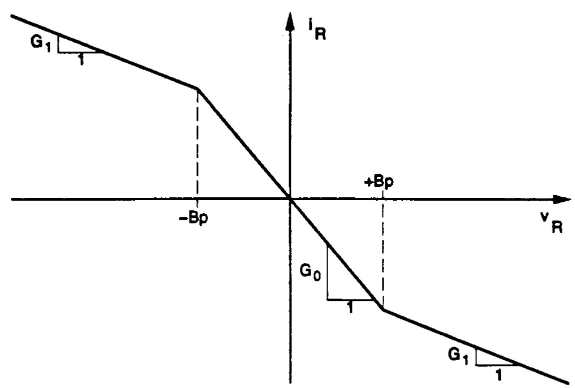



Fig. 1. Three-segment piecewise-linear function. The inner region has slope $G_0$; the outer regions have slopes $G_1$.

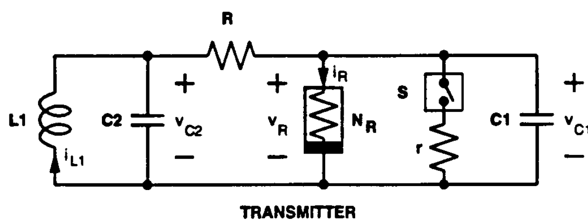



Fig. 2. Transmitter for binary CSK using Chua's circuit. Chaotic signal $v_{C_1}$ is transmitted. The Chua diode $N_R$ is defined by (35).

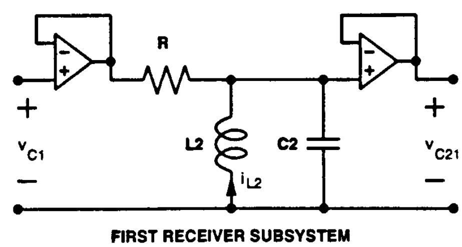



Fig. 3. Receiver: First subsystem.

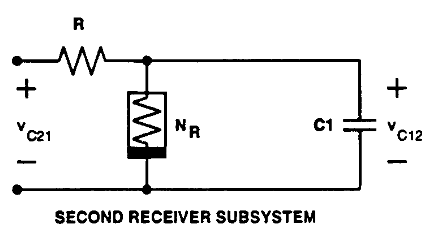



Fig. 4. Receiver: Second subsystem.

## III. THEORY

We suppose here that a bit $+1$ is transmitted during a time interval $T$ that is very large compared to the circuit time constants in order to give asymptotic convergence results on the difference between $v_{C1}(t)$ and $v_{C12}(t)$. Two questions of interest have to be solved: Can we ensure asymptotic convergence of $v_{C12}(t)$ to $v_{C1}(t)$ (i.e., $\lim_{t\to\infty}(v_{C1}(t) - v_{C12}(t)) = 0$) independent of the initial values of voltages and currents of the receiver? Can we give an approximate value

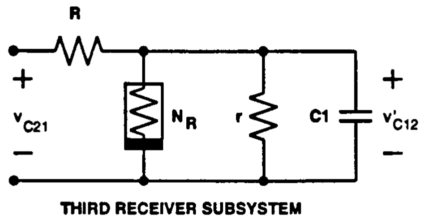



Fig. 5. Receiver: Third subsystem.

of the time $T$ of bit transmission that ensures no intersymbol interference if one wants to design a synchronization detector?

### A. Synchronization of $v_{C2}(t)$ and $v_{C21}(t)$ when a $+1$ is Transmitted

The first question is how close are the signals $v_{C2}(t)$ and $v_{C21}(t)$ during the transmission and what should be the transmission duration in order that $v_{C2}(t)$ and $v_{C21}(t)$ be as arbitrarily close as we want?

Let $\epsilon_2(t)$ be defined as follows:

$$\epsilon_2(t) = v_{C21}(t) - v_{C2}(t). \tag{8}$$

Let $\Delta i_L(0)$ and $\Delta v_{C2}(0)$ be the differences in initial conditions, i.e.,

$$\Delta v_{C2}(0) = v_{C21}(0) - v_{C2}(0) \quad \Delta i_L(0) = i_{L2}(0) - i_{L1}(0). \tag{9}$$

Looking at (2)–(5) it is straightforward to show that

$$\epsilon_2(t) = \frac{\Delta i_L(0)}{C_2\omega_0} e^{-\frac{t}{\tau_2}} \sin(\omega_0 t) + \Delta v_{C2}(0) e^{-\frac{t}{\tau_2}} \left[\cos(\omega_0 t) - \frac{1}{\tau_2\omega_0}\sin(\omega_0 t)\right]. \tag{10}$$

With $\tau_2$ and $\omega_0$ defined as

$$\tau_2 = 2RC_2 \tag{11}$$

$$\omega_0 = \sqrt{\frac{1}{LC_2} - \frac{1}{4R^2C_2^2}}. \tag{12}$$

As $v_{C2}(t)$ and $v_{C21}(t)$ result from the excitation of two identical asymptotically stable linear systems with the same driving signal $v_{C1}(t)$, it is obvious that the difference between the two signals decreases exponentially to zero as shown by (10). The time constant $\tau_2$ of the exponential gives us a first parameter to assess the value of $T$.

### B. Synchronization of $v_{C1}(t)$ and $v_{C12}(t)$ When a Bit $+1$ Is Transmitted

As a simplification we suppose that $v_{C21}(t) = v_{C2}(t)$ (i.e., $\epsilon_2(t) = 0$), this is not a restrictive assumption since we have seen that $v_{C21}(t)$ converges exponentially towards $v_{C2}(t)$. For notational convenience, let us define $\epsilon_1(t)$ as follows:

$$\epsilon_1(t) = v_{C12}(t) - v_{C1}(t). \tag{13}$$

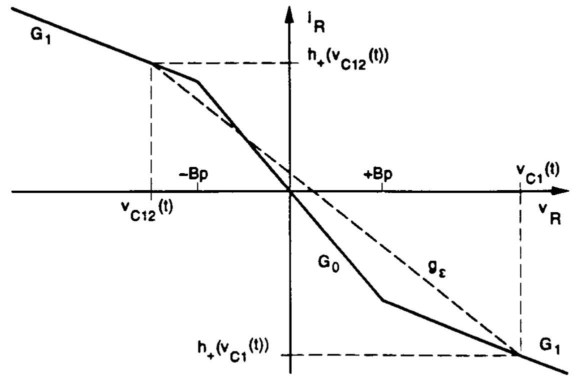



Fig. 6. $g_\epsilon(t)$ is the slope of the dashed line.

Let us replace $\frac{1}{R}$ by $G$, from (1) and (6) we get

$$C_1\frac{d\epsilon_1(t)}{dt} = -G\epsilon_1(t) - \left[\frac{h_+(v_{C12}(t)) - h_+(v_{C1}(t))}{v_{C12}(t) - v_{C1}(t)}\right]\epsilon_1(t). \tag{14}$$

It is obvious that the term inside the brackets in (14) is the slope of the straight line which joins the two points $(v_{C12}(t), h_+(v_{C12}(t))$ and $(v_{C1}(t), h_+(v_{C1}(t))$ (see Fig. 6). Let $g_\epsilon(t)$ denote this slope and let us define the function $h_\epsilon(t)$ such that

$$h_\epsilon(t) = G + g_\epsilon(t). \tag{15}$$

Note that for all $t$

$$G + G_0 \le h_\epsilon(t) \le G + G_1. \tag{16}$$

Equation (14) can be written in the following compact form

$$C_1\frac{d\epsilon_1(t)}{dt} = -h_\epsilon(t)\epsilon_1(t). \tag{17}$$

Clearly, (17) has an equilibrium point at $\epsilon_1(t) \equiv 0$, i.e., when $v_{C12}(t) \equiv v_{C1}(t)$. We will show in addition that this equilibrium point is *stable*. The solution of (17) is given by

$$\epsilon_1(t) = \epsilon_1(0)e^{-\frac{1}{C_1}\int_0^t h_\epsilon(\tau)\,d\tau}. \tag{18}$$

*Property 1:* The difference $\epsilon_1(t)$ for any time $t$ has the same sign as $\epsilon_1(0)$.

This property is obvious from (18). Consider now the domain $\mathcal{D}$ of Fig. 7 defined by

$$\mathcal{D} = (-\infty, u_-] \cup [u_+, +\infty) \tag{19}$$

with $u_-$ and $u_+$ defined as follows:

$$u_- = \frac{(G_0 - G_1) + (G_0 - G_2)}{G_1 - G_2}B_p, \qquad u_+ = -u_- \tag{20}$$

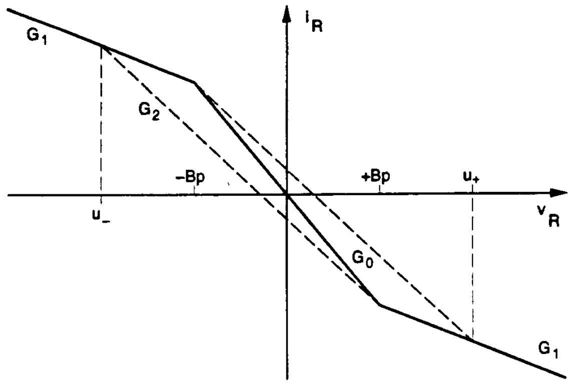



Fig. 7. Definition of $u_-$ and $u_+$; the slope of the two dashed oblique lines is $G_2$ with $-G < G_2 < G_1$.

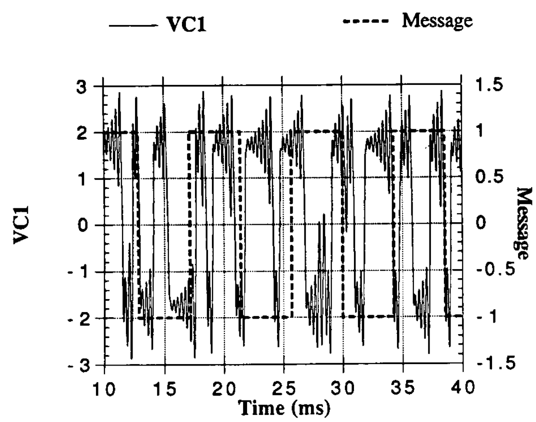



Fig. 8. Behavior of the chaotic signal $v_{C1}(t)$ and of the binary message.

and $G_2$ in (20) chosen in such a way that

$$-G < G_2 < G_1. \tag{21}$$

*Property 2:* A sufficient condition for the variable $h_\epsilon(t)$ to be positive is that at least one of the two signals $v_{C1}(t)$ or $v_{C21}(t)$ be in the domain $\mathcal{D}$.

The proof of property 2 is obvious. Since one of the two signals is at least in $\mathcal{D}$ we have $G_2 \le g_\epsilon(t) \le G_1$. From (16) and (21), it is clear that $h_\epsilon(t) \ge G_2 + G > 0$.

*Property 3:* a) In the case where $\epsilon_1(0)$ is negative, a sufficient condition for the variable $h_\epsilon(t)$ to be positive is that $v_{C1}(t)$ be in the domain $\mathcal{D}_1 = (-\infty, -B_p] \cup [u_+, +\infty)$. b) In the case where $\epsilon_1(0)$ is positive, a sufficient condition for the variable $h_\epsilon(t)$ to be positive is that $v_{C1}(t)$ be in the domain $\mathcal{D}_2 = (-\infty, u_-] \cup [B_p, +\infty)$.

The proof follows from properties 1 and 2. Suppose that $\epsilon_1(0)$ is negative.

From property 1 we have that $v_{C1}(t) > v_{C12}(t)$ for any time $t$, thus if $v_{C1}(t)$ is in $(-\infty, -B_p]$ then $v_{C12}(t)$ is also in $(-\infty, -B_p]$. For $v_{C1}(t)$ in $(-\infty, -B_p]$, $h_\epsilon(t) = G + G_1$ that is a positive quantity from (21).

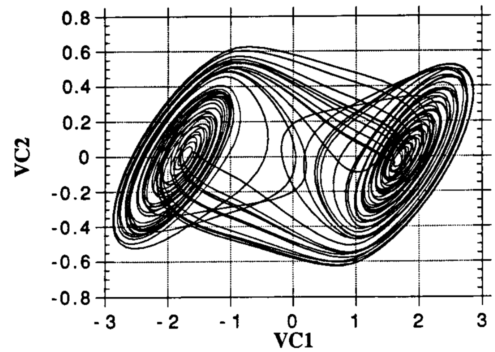



Fig. 9. Double scroll attractor in the phase plane $v_{C1}(t)$, $v_{C2}(t)$ during modulation.

From property 2, we know that a sufficient condition for $h_\epsilon(t)$ to be positive is that $v_{C1}(t)$ be in $\mathcal{D}$. As a result if $\epsilon_1(0)$ is negative, a sufficient condition for $h_\epsilon(t)$ to be positive is that $v_{C1}(t)$ be in $\mathcal{D} \cup (-\infty, -B_p] = \mathcal{D}_1$. A similar proof can be shown for case b) of property 3.

Let us now consider the relative duration time of $v_{C1}(t)$ in the region $(-B_p, u_+)$, this relative duration time will be referred to as $\alpha(t)$. Let us define an index variable $I_\alpha(\tau)$ which has the following meaning

$$I_\alpha(\tau) = \begin{cases} 1, & \text{if } v_{C1}(\tau) \in (-B_p, u_+), \\ 0, & \text{if } v_{C1}(\tau) \notin (-B_p, u_+). \end{cases} \tag{22}$$

The relative duration time of $v_{C1}(t)$ in the area $(-B_p, u_+)$ is then defined as

$$\alpha(t) = \frac{1}{t}\int_0^t I_\alpha(\tau)\, d\tau. \tag{23}$$

In a similar fashion we define an index variable $I_\beta(\tau)$ which has the following meaning

$$I_\beta(\tau) = \begin{cases} 1, & \text{if } v_{C1}(\tau) \in (-\infty, -B_p], \\ 0, & \text{if } v_{C1}(\tau) \notin (-\infty, -B_p]. \end{cases} \tag{24}$$

The relative duration time of $v_{C1}(t)$ in the area $(-\infty, -B_p]$ is then defined as

$$\beta(t) = \frac{1}{t}\int_0^t I_\beta(\tau)\, d\tau. \tag{25}$$

Let $\alpha_\infty$ and $\beta_\infty$ be the two variables defined as follows:

$$\alpha_\infty = \lim_{t\to\infty}\alpha(t), \qquad \beta_\infty = \lim_{t\to\infty}\beta(t). \tag{26}$$

For simplicity we assume that these limits exist, but the subsequent arguments could be adapted to limsup for $\alpha_\infty$ and liminf for $\beta_\infty$.

*Property 4:* If there exists a constant $G_2$ such that

a) $-G < G_2 < G_1$

b) and that the maximum relative duration times $\alpha_\infty$ and

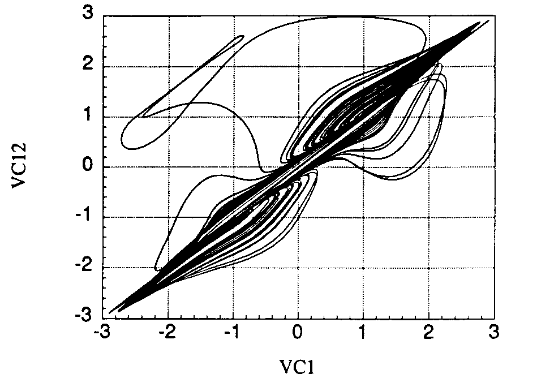



Fig. 10. $v_{C12}(t)$ as function of $v_{C1}(t)$ during the transmission of several bits $+1$, $-1$.

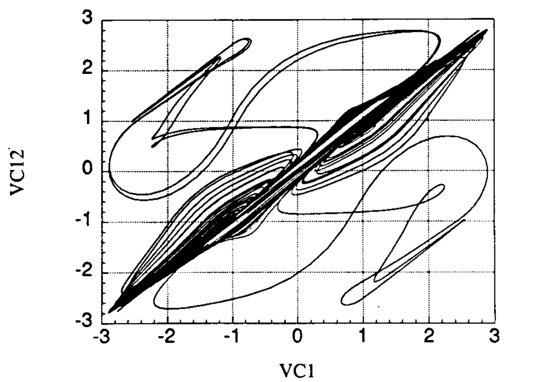



Fig. 11. $v'_{C12}(t)$ as a function of $v_{C1}(t)$ during the transmission of several bits $+1$, $-1$.

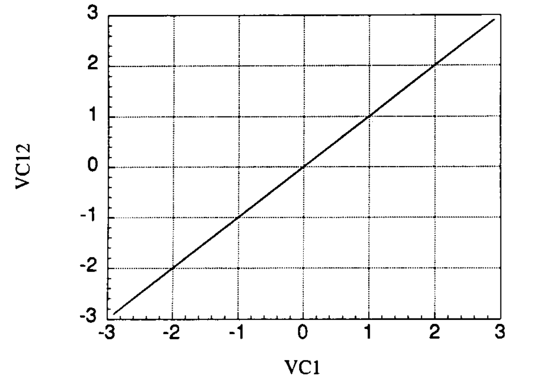



Fig. 12. $v_{C12}(t)$ as a function of $v_{C1}(t)$ during the transmission of several bits $+1$.

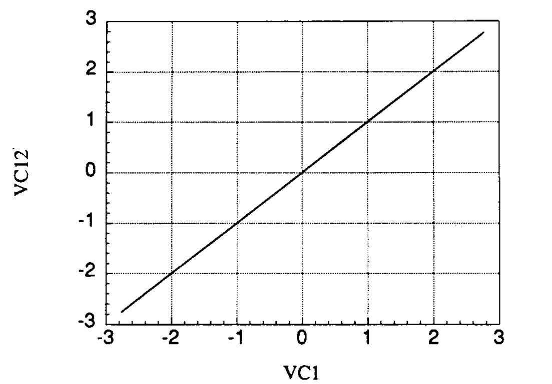



Fig. 13. $v_{C12}(t)$ as a function of $v_{C1}(t)$ during the transmission of several bits $-1$.

$\beta_\infty$ obeys

$$G_0\alpha_\infty + G_1\beta_\infty + G_2(1-\alpha_\infty-\beta_\infty) > -G, \quad (27)$$

then $\epsilon_1$ converges exponentially towards zero with a time constant which is at least

$$\tau_1 = \frac{C_1}{G + G_0\alpha_\infty + G_1\beta_\infty + G_2(1-\alpha_\infty-\beta_\infty)}. \quad (28)$$

*Proof:* Assume that $\epsilon_1(0)$ is negative, by symmetry a similar proof can be given if $\epsilon_1(0)$ is positive.

We can write

$$\int_0^t h_\epsilon(\tau)\,d\tau = \int_0^t I_\alpha(\tau)h_\epsilon(\tau)\,d\tau + \int_0^t I_\beta(\tau)h_\epsilon(\tau)\,d\tau + \int_0^t [1 - I_\alpha(\tau) - I_\beta(\tau)]h_\epsilon(\tau)\,d\tau. \quad (29)$$

Observe that from the definition of $I_\alpha(\tau)$ and $I_\beta(\tau)$ we have

$$\begin{cases} I_\alpha(\tau)h_\epsilon(\tau) \geq (G+G_0)I_\alpha(\tau), \\ I_\beta(\tau)h_\epsilon(\tau) = (G+G_1)I_\alpha(\tau), \\ (1-I_\alpha(\tau)-I_\beta(\tau))h_\epsilon(\tau) \geq (G+G_2)[1-I_\alpha(\tau)-I_\beta(\tau)]. \end{cases} \quad (30)$$

From (29), (30), (23), and (25), it follows that

$$\int_0^t h_\epsilon(\tau)\,d\tau \geq \Big[(G+G_0)\alpha(t) + (G+G_1)\beta(t) + (G+G_2)[1-\alpha(t)-\beta(t)]\Big]t. \quad (31)$$

From (26), the limit of (31) becomes

$$\lim_{t\to\infty}\int_0^t h_\epsilon(\tau)\,d\tau \geq \lim_{t\to\infty}[G + G_0\alpha_\infty + G_1\beta_\infty + G_2(1-\alpha_\infty-\beta_\infty)]t. \quad (32)$$

Equations (18) and (32) show that if

$$G + G_0\alpha_\infty + G_1\beta_\infty + G_2(1-\alpha_\infty-\beta_\infty) > 0$$

then

$$\lim_{t\to\infty}\epsilon_1(t) = 0. \quad (33)$$

Property 4 allows the computation of the average duration time of synchronization if one knows the relative duration times $\alpha_\infty$ and $\beta_\infty$. These relative duration times have to be assessed via simulation. Observe that $\alpha_\infty$ has to be evaluated for different values of $G_2$ in order to find the best bound for the exponential factor $\tau_1$.

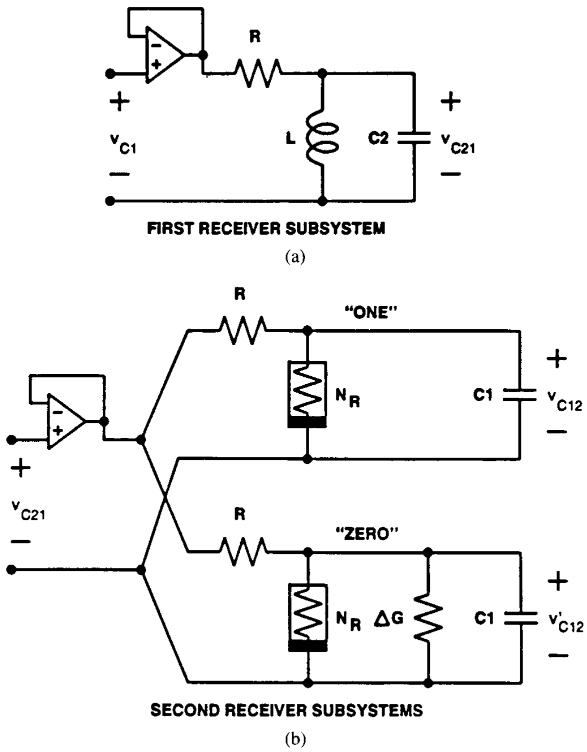



Fig. 14. Receiver for binary CSK using the transmitter in Fig. 2. (a) The first subsystem restores $v_{C_2} (= v_{C_{21}})$ from $v_{C_1}$. (b) The second subsystems, which are "tuned" to $+1$ and $-1$, produce signals $v_{C_{12}}$ and $v'_{C_{12}}$. When a $+1$ is transmitted, $v_{C_{12}}$ synchronizes with $v_{C_1}$; when a $-1$ is transmitted, $v'_{C_{12}}$ synchronizes with $v_{c_1}$.

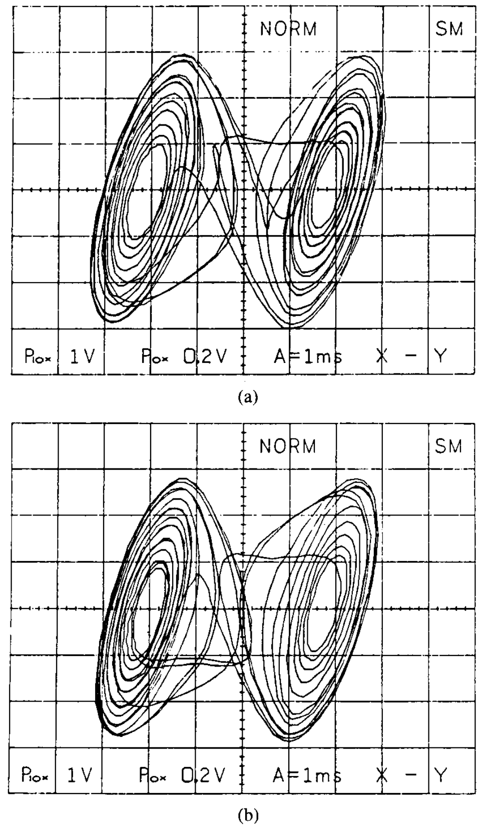



Fig. 15. Attractors in the transmitter corresponding to the $P_{+1}(+1)$ and $P_{-1}(-1)$ parameter sets: (a) $+1$; (b) $-1$. In both cases, the horizontal and vertical axes are $v_{C_1}$ and $v_{C_2}$, respectively.

### *C. Desynchronization of $v_{C1}(t)$ and $v_{C12}(t)$ When a Bit $-1$ Is Transmitted*

In this subsection, we show that $v_{C1}(t)$ and $v_{C12}(t)$ desynchronize when a bit$-1$ is transmitted.

As before, we define $\epsilon_1(t) = v_{C12}(t) - v_{C1}(t)$. When a $-1$ is transmitted, we now have

$$C_1 \frac{d\epsilon_1(t)}{dt} = -G\epsilon_1(t) - [h_+(v_{C12}(t)) - h_-(v_{C1}(t))]. \quad (34)$$

If $v_{C1}(t)$ and $v_{C12}(t)$ are to remain synchronized, then $\epsilon_1(t) \equiv 0$ must be a stable fixed point of (34). Substituting $\frac{d\epsilon_1(t)}{dt} = 0$ and $\epsilon_1(t) = 0$ into (34), we get $h_+(v_{C21}(t)) = h_-(v_{C1}(t))$ or equivalently,

$$h_+(v(t)) \equiv h_-(v(t)),$$

which is not true. Thus, we have proven by contradiction that $v_{C1}(t) = v_{C12}(t)$ is not a solution when a $-1$ is transmitted.

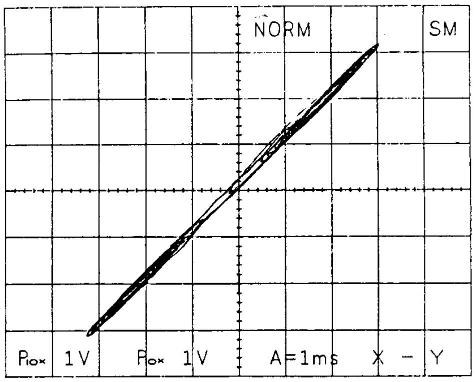
## IV. Example for Evaluating a Lower Bound on $T$

Consider Chua's circuit shown in Fig. 2 the component values of which are given in Table I. For differents values of $G_2$ such that $-G < G_2 < G_1$, we show in Table II the corresponding value of $u_+$ calculated from (20). The relative duration times $\alpha_\infty$ and $\beta_\infty$ were evaluated over a total duration of 1 s. Table II shows that $\tau_1$ is at least 411 $\mu$s while $\tau_2$ is 336 $\mu$s. This shows in this particular case that $\tau_1 + \tau_2$ will fix the bit duration $T$. In order to have a decrease of 99% in $\epsilon_1(0)$, $T$ should be at least 3.5 ms.

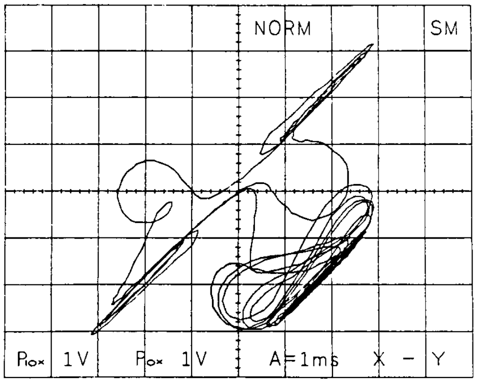
## V. Simulations

We present here simulations using the subsystems described from Figs. 2 and 5. The value of $r$ was chosen in order that $G'_0$ and $G'_1$ exhibit variations of 1% with respect to $G_0$ and $G_1$. The other values were chosen according to Table II. The value of $T$ was 4.65 ms.

Fig. 8 shows the chaotic message from time 10 ms to time 40 ms and the corresponding binary message. Fig. 9 shows the double scroll attractor in the phase-plane $(v_{C1}(t), v_{C2}(t))$ during the transmission of the binary message presented in Fig. 8. Fig. 10 shows the relationship between $v_{C12}(t)$ and $v_{C1}(t)$ during the transmission of 120 bits which were alternatively $+1$, $-1$ while Fig. 11 displays the relationship between $v'_{C12}(t)$ and $v_{C1}(t)$ during the same transmission. Obviously the receiver subsystems are not synchronized during the whole transmission (it is hoped that the receiver not matched to receive the right bit exhibits a desynchronized behavior). Finally, Fig. 12 shows the relationship between $v_{C12}(t)$ and $v_{C1}(t)$ during the transmission of sixty nonconsecutive $+1$

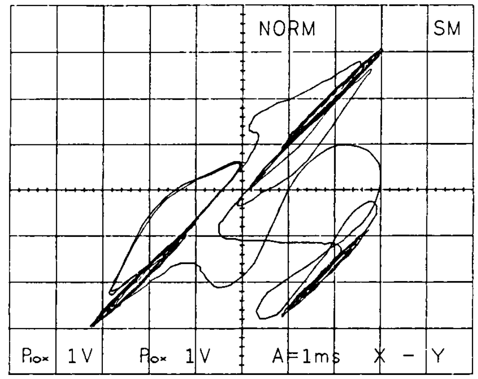



(a)

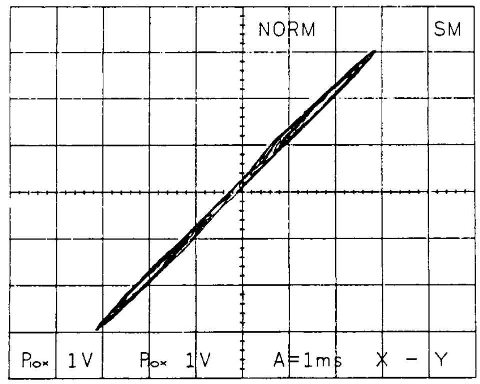



(b)

Fig. 16. Phase portrait for the receiver's $+1$ subsystem: (a) $+1$ transmitted (synchronization); (b) $-1$ transmitted (no synchronization). In both cases, the horizontal and vertical axes are $v_{C_1}$ and $v_{C_{12}}$, respectively.




(a)




(b)

Fig. 17. Phase portrait for the receiver's $-1$ subsystem: (a) $+1$ transmitted (no synchronization); (b) $-1$ transmitted (synchronization). In both cases, the horizontal and vertical axes are $v_{C_1}$ and $v'_{C_{12}}$, respectively.

TABLE I
VALUES OF THE ELEMENTS OF THE CHUA'S CIRCUIT

| $R(\Omega)$ | $L$ (mH) | $C_1$ (nF) | $C_2$ (nF) | $G_0$ ($\mu$ S) | $G_1$ ($\mu$ S) | $B_p$ (V) |
|---|---|---|---|---|---|---|
| 1680 | 18 | 10 | 100 | −753 | −396 | 1 |

TABLE II
$u_+$, $\alpha_\infty$, $\tau_1$ AS A FUNCTION OF $G_2$, $\beta_\infty$ AND $\tau_2$

| $G_2$ ($\mu$ S) | $u_+$ (V) | $\alpha_\infty$ | $\beta_\infty$ | $\tau_1$ ($\mu$ s) | $\tau_2$ ($\mu$ s) |
|---|---|---|---|---|---|
| −595 | 2.59 | 0.5351 | 0.435 | 411 | 336 |
| −594 | 2.61 | 0.5379 | 0.435 | 473 | 336 |
| −592 | 2.64 | 0.5416 | 0.435 | 748 | 336 |
| −591 | 2.66 | 0.5451 | 0.435 | 1500 | 336 |
| −589 | 2.69 | 0.5484 | 0.435 | 4272 | 336 |

bits. The signals were sampled during the last half duration of each bit in order to avoid transients. Fig. 13 is the alter ego figure of Fig. 12; it shows the relationship between $v'_{C12}(t)$ and $v_{C1}(t)$ during the transmission of sixty nonconsecutive $-1$ bits.

## VI. EXPERIMENTAL RESULTS

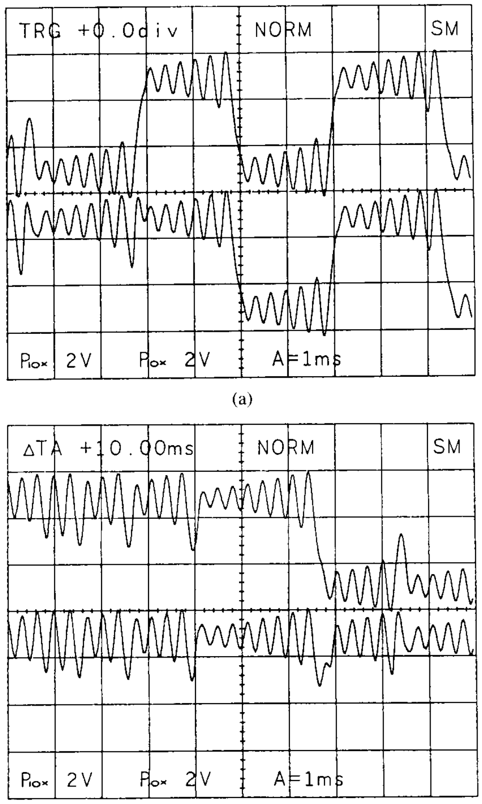
In our demonstration of binary CSK, the transmitter and receiver consist of a Chua's circuit and matched Chua's circuit subsystems (see Figs. 2 and 14). The transmitter is switched between two parameter sets $P_{+1}$ and $P_{-1}$—and their associated chaotic attractors (Fig. 15)—corresponding to $+1$ and $-1$ respectively, by switching a resistor $r$ in parallel with the Chua diode $N_R$ [7]. The chaotic voltage across capacitor $C_1$ is sent from the transmitter to the receiver, where it first synchronizes with $v_{C_{21}}$ and then with either $v_{C_{12}}$ or $v'_{C_{12}}$, depending on whether a $+1$ or a $-1$ has been transmitted.

The component values for the linear parts of the transmitter and receiver were as follows: $L = 18$ mH (TOKO 10RB), $C_2 = 100$ nF, $C_1 = 10$ nF and $R = 1730\ \Omega$ (all components were measured with $\pm 1\%$ accuracy). The Chua diode is defined by its driving-point characteristic:

$$i_R = G_1 v_R + \frac{1}{2}(G_0 - G_1)(|v_R + B_p| - |v_R - B_p|) \quad (35)$$

where $G_0 = -0.753$ mS, $G_1 = -0.396$ mS, and $B_p = 1$ V; the analog switch $S$ is a Siliconix DG308 and $r = 150$ k$\Omega$. The subsystems of the receiver were matched to those of the transmitter. Explicitly, the parameter sets corresponding to $+1$ and $-1$ are

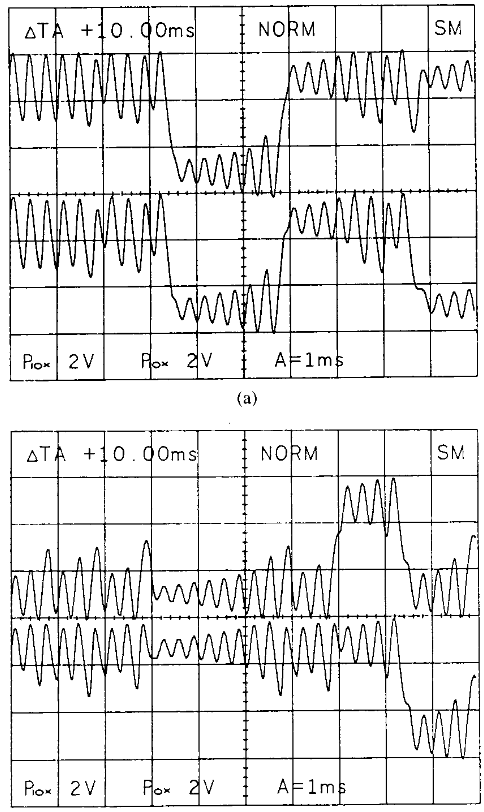
$$P_{+1} = \{L, C_2, R, G_0, G_1, B_p, C_1\},\ P_{-1} = \{L, C_2, R, G_0 + 1/r, G_1 + 1/r, B_p, C_1\}.$$




(a)

(b)

Fig. 18. Experimentally recorded time waveforms for the receiver's +1 subsystem: (a) +1 transmitted (synchronization occurs within 10 ms); (b) −1 transmitted (loss of synchronization within 10 ms). Upper trace: $v_{C_1}$; lower trace: $v_{C_{12}}$. Horizontal axis: time (1 ms per division).




(a)

(b)

Fig. 19. Experimentally recorded time waveforms for the receiver's −1 subsystem: (a) +1 transmitted (loss of synchronization within 10 ms); (b) −1 transmitted (synchronization occurs within 10 ms). Upper trace: $v_{C_1}$; lower trace: $v'_{C_{12}}$. Horizontal axis: time (1 ms per division).

### A. Static Performance

We first verified that the receiver subsystems synchronized with the appropriate transmitted signal. When the signal corresponding to a +1 attractor was transmitted, the receiver's +1 subsystem synchronized with the received signal; when a −1 was transmitted, it did not (see Fig. 16). Similarly, when the resistor $r$ was connected across the Chua diode in the transmitter circuit and a −1 thus transmitted, the receiver's −1 subsystem synchronized with the incoming signal; when a +1 was transmitted, it did not (see Fig. 17).

### B. Dynamic Performance

In order to evaluate the dynamic performance of our binary CSK system based on Chua's circuit, we transmitted a repetitive 50 Hz plus-one-minus-one sequence by applying a square wave to the gate of the analog switch $S$. This switched the transmitter signal back and forth between the +1 and −1 attractors.

Typical receiver waveforms are shown in Figs. 18 and 19. In each case, full synchronization and desynchronization occur within 10 ms.

## VII. Conclusion

We have proposed a simple architecture for chaotic shift keying modulation and demodulation. A proof has been given for the synchronization effect. As in the work of Pecora and Carroll [1]–[4] we needed some a priori information on the driving signal to prove the synchronization effect. In the general case treated by Pecora and Carroll this *a priori* information is computed via the conditional Lyapunov exponents. In the particular case we dealt with here we used a Chua's circuit in which it was simpler to make assumptions on the relative duration times of the driving signal in two areas of the piecewise-linear characteristic of the Chua's diode. Furthermore this simpler approach leads to reasonable lower bound for the average time of synchronization which is of prime importance to ensure correct bit transmission. Simulations have been carried out in accordance with the theory. We built a binary CSK system using Chua's circuits and verified our theoretical predictions and simulations. Despite the fact that the values of the components at the transmitter and the receiver were not exactly matched, the circuit behaved in close accordance with the simulations.

## ACKNOWLEDGMENT

The authors would like to thank A. Flanagan for fruitful comments and support during the work.


## REFERENCES


[1] L. M. Pecora and T. L. Carroll, "Synchronization in chaotic systems," *Physical Rev. Lett.*, vol. 64, no. 8, pp. 821–824, Feb. 1990.

[2] ——, "Driving systems with chaotic signals," *Physical Rev. A.*, vol. 44, no. 4, pp. 821–824, Aug. 1991.

[3] T. L. Carroll and L. M. Pecora, "Synchronizating chaotic circuits," *IEEE Trans. Circuits Syst.*, vol. 38, no. 4, pp. 453–456, Apr. 1991.

[4] L. M. Pecora and T. L. Carroll, "Synchronized chaotic signal and systems," in *Proc. 1992 IEEE ICASSP*.

[5] A. V. Oppenheim, G. W. Wornell, S. H. Isabelle, and K. M. Cuomo, "Signal processing in the context of chaotic signals," in *Proc. IEEE ICASSP*, pp. IV-117–IV-120, 1992.

[6] L. Kocarev, K. S. Halle, K. Eckert, L. O. Chua, and U. Parlitz, "Experimental demonstration of secure communications via chaotic synchronization," *Int. J. Bifurcation and Chaos*, vol. 2, no. 3, pp. 709–713, Sept. 1992.

[7] M. P. Kennedy, "Robust op amp implementation of Chua's circuit," *Frequenz*, vol. 46, pp. 66–80, Mar.–Apr. 1992.

[8] T. Matsumoto, "A chaotic attractor from Chua's circuit," *IEEE Trans. Circuits Syst.*, vol. 31, no. 12, pp. 1055–1508, Dec. 1984.

[9] R. N. Madan (Guest Editor), "Chua's circuit: A paradigm for Chaos," *J. Circuits, Syst. and Comput.—Part I*, vol. 3, no. 1, Mar. 1993; Part II, vol. 3, no. 2, 1993.

[10] M. J. Ogorzalek, "Chaotic regions from double scroll," *IEEE Trans. Circuits Syst.*, vol. 34, no. 2, pp. 1055–1508, Feb. 1987.

[11] L. O. Chua, M. Komuro, and T. Matsumoto, "The double scroll family. Parts I and II," *IEEE Trans. Circuits Syst.*, vol. 33, no. 11, pp. 1072–1118, Nov. 1986.


**Hervé Dedieu** (M'92) received the Ph.D. degree from the Institut National Polytechnique de Toulouse, France, in 1988.

From 1984 to 1988, he worked with the Signal Processing Laboratory of the Ecole Nationale Supérieure d'Electronique, d'Electrotechnique et d'Hydraulique de Toulouse where his research was concentrated on adaptive filtering. During the same period, he also worked for the French National Spacial Agency (CNES) on different projects for satellite attitude restitution and studies of architectures of fast digital modulators/demodulators for synthetic aperture radar. In 1989, he joined the Circuits and Systems group of the Swiss Federal Institute of Technology where his research interests include filter theory (broadband matching), adaptive filter theory and nonlinear prediction of time series. He is also involved in a speech recognition project as a partner of a european Esprit project.

**Michael Peter Kennedy** (M'92) was born in Dublin, Ireland, on April 25, 1963. He received the bachelor of engineering (electronics) degree with first class honors from University College Dublin (UCD) in 1984. He received the M.S. and Ph.D. degrees in electrical engineering from the University of California 1987 and 1991, respectively.

After receiving the Ph.D. degree, he worked as a Postdoctural Research Fellow at the Electronics Research Laboratory, Berkeley, and as a visiting professor in the Chair of Circuits and Systems at the Ecole Polytechnique Fédérale de Lausanne, Switzerland. He returned to UCD in 1992 as a College Lecturer in the Department of Electrical and Electronic Engineering , where he teaches electronic circuits and computer-aided circuits and systems analysis. He also directs the undergraduate electronics laboratory. His current research interests are in simulation, design, analysis, synchronization, and control of nonlinear dynamical systems. His work on electronic instrumentation, computer-aided circuit analysis, neural networks, forced oscillators, piecewise-linear circuit theory, nonlinear dynamics, and signal processing has appeared in *Procedings of the IEE*, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS, *Artificial Neural Networks: Paradigms, Applications, and Hardware Implementations* (New York: IEEE), *International Journal of Circuit Theory and Applications*, *Frequenz*, and *Journal of Circuits, Systems, and Computers*.

Dr. Kennedy received UCD Scholarships from 1981–1983, the Best Bachelor's Thesis in Electronic Engineering Award in 1984, the National University of Ireland's Bursary in Electrical and Electronic Engineering in 1984, and the Scholarship Exchange Board Travelling Scholarship in 1985. While studying at the University of California at Berkeley, he was awarded a Semiconductor Research Corporation Scholarship and held the Wilson and Albert M. Flagg and Earle C. Anthony Scholarships. For his service to the international community at Berkeley, he received the International Volunteer Award. He received the 1991 Best Paper Award from the *International Journal of Circuit Theory and Applications* for his paper with L. Chua entitled "Hysteresis in Electronic Circuits: A Circuit Theorist's Perspective." In 1993, he was appointed Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—I: FUNDAMENTAL THEORY AND APPLICATIONS

**Martin Hasler** (SM'90–F'93) received the Diploma in 1969 and the Ph.D. degree in 1973 from the Swiss Federal Institute of Technology, Zurich, both in physics.

He continued research in mathematical physics at Bedford College, University of London, from 1973 to 1974. At the end of 1974, he joined the Circuits and Systems group of the Swiss Federal Institute of Technology, Lausanne, where he was given the title of a Professor in 1984. During the 70's, his research was concentrated on filter theory and design, in particular active and switched capacitor filters. In 1979, he started with nonlinear circuit theory, a new field for his institution. The main concern in the beginning was qualitative analysis of dynamic, and later also of resistive circuits. In this context, he got interested in chaotic behavior of electric circuits. Later, he also became interested in artificial neural networks, as a special class of nonlinear circuits. Finally, he started research on modeling of nonlinear circuits and systems, as a complement to nonlinear circuit and system analysis.

Dr. Hasler is the author and coauthor of more than 80 research papers and 4 books, among them: M. Hasler and J. Neirynck, *Nonlinear Circuits* (Artech House, Boston, 1986) and Y. Kamp and M. Hasler, *Recursive Neural Networks for Associative Memory* (Wiley and Sons, London, 1990). He has won the best paper award of the *International Journal of Circuit Theory and Applications* for 1986. He currently is on the editorial board of this journal, as well as of the *Annales des Télécommunications*. He was an Associate Editor of the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS from 1991 to 1993 and currently he is the Editor of Part I of this journal. He was the chairman of the Technical Committee on Nonlinear Circuits and Systems of the IEEE CAS Society from 1990 to 1993.