Design Considerations for Integrated Continuous-Time Chaotic Oscillators

Manuel Delgado-Restituto, *Member, IEEE,* and Angel Rodríguez-Vázquez, *Fellow, IEEE*

***Abstract*— This paper presents an optimization procedure to choose the chaotic state equation which is best suited for implementation using Gm-C integrated circuit techniques. The paper also presents an analysis of the most significant hardware nonidealities of Gm-C circuits on the chaotic operation—the basis to design robust integrated circuits with reproducible and easily controllable behavior. The techniques in the paper are illustrated through a circuit fabricated in 2.4-μm double-poly technology.**

***Index Terms*— Analog and mixed analog/digital circuits, nonlinear circuit design.**

I. Introduction

DURING the last several years, there has been an ever-increasing interest in the application of chaotic modulation for data encryption in communication systems. This has been supported by a number of remarkable theoretical developments [1], and demonstrated through circuit implementation with wired links [2]–[7] and with RF links [8]. Some attempts have also been made to realize the chaotic modulation/demodulation units using monolithic integrated circuits—prompted by the convenience to reduce the size and the power consumption of chaotic communication systems.

A few chaotic chips have been reported during the last six years [9]–[13]. Most of them use discrete-time circuits to generate random signals with white or colored spectra [9]–[11], or to emulate the behavior of chaotic neurons [12], [13]. The circuits presented in [14] and [15] use electrically controllable continuous-time circuits to generate a bifurcation sequence to chaos, including several well-known attractors (Rössler, Chua's double-scroll, etc.). The circuit in [14] and the chaotic neurons have also been demonstrated for chaotic modulation with wired links [13], [16].

These chips have been basically aimed at demonstrating the possibility to generate chaotic behaviors, in some cases using additional off-chip components [15]. Thus, their design has been focused on the realization of well-known chaotic state equations, with no assessment of the adequacy of these equations for their implementation using integrated circuits. Neither detailed analysis of the integrated circuits hardware nonidealities nor their influence on the chaotic operation have been reported. Consequently, we can state that the basic tools needed to synthesize robust chaotic IC's with predictable behavior are lacking. This paper intends to overcome this drawback by addressing the optimum realization of a chaotic circuit for the vector field modulation data encryption system [1], and the study of the influence of their hardware nonidealities. We will focus on the realization of modulator/demodulator IC units which can be expressed in Lur'e form with a scalar time-invariant nonlinearity [17]–[19]. The reason is simply the wide repertoire of nonlinear dynamical phenomena, including all kinds of bifurcations and routes to chaos, which has been identified within this family, as well as its demonstrated applications to data encryption [6]–[8].

Section II first proposes an optimization procedure for the synthesis of chaos generators described in Lur'e form. We hence propose using the state-variable synthesis method to define the system level topology, and using transconductors and capacitors (Gm-C techniques) as basic elements for the circuit level realization. Several advantages support this choice. For instance, it allows a direct conversion from the state equations to the Gm-C circuit. It only requires grounded capacitors in the active realization, thus precluding the disturbing influence caused by the bottom-plate parasitics of integrated capacitors. The purpose of the optimization is, given a particular chaotic behavior, to obtain the most robust possible Gm-C monolithic implementation able to synthesize it. The presented procedure is general, although in the paper it is illustrated with the vector field modulation scheme. Section III proposes an IC-oriented design able to reproduce the well-known double-scroll attractor, as an example of application of the algorithm. Section IV proposes a classification of the error sources which affect the functionality of the integrated chaos generator. Analysis of these errors is essential to determine the accuracy requirements of the blocks composing the oscillator. Then, three of the most relevant sources of error are discussed, namely, the effect of nonideal integrators, nonlinear static deviations of transconductors, and mismatch errors on the circuit elements. In doing so, the optimized Gm-C circuit devised in Section III is used as a benchmark. Section V presents experimental results to illustrate the performance of a fabricated prototype of this circuit for chaotic modulation, and Section VI gives some concluding remarks.

Manuscript received February 5, 1997; revised June 18, 1997. This work was supported by the Spanish CICYT (Project TIC 96-1392-CO2-2) and the CEE (Project INSPECT). This paper was recommended by Associate Editor M. Ogorzalek.

The authors are with the Instituto de Microelectrónica de Sevilla, CNM, Edificio CICA, 41012-Sevilla, Spain (e-mail: angel@cnm.us.es).

Publisher Item Identifier S 1057-7122(98)02105-9.

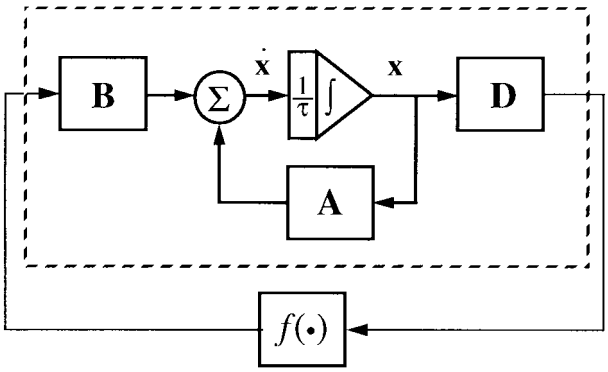

Fig. 1. Block diagram of a chaotic generator in Lur'e form.

II. High-Level Synthesis of Gm-C Chaotic Oscillators

A. A Gm-C State-Variable Architecture for Lur'e form Chaotic Oscillators

Members of the Lur'e family, denoted hereafter by L_n, are described by the continuous-time nonlinear state equation

$$\tau \frac{d}{dt}\boldsymbol{x}(t) = \boldsymbol{F}[\boldsymbol{x}(t)] = \boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B}f[\boldsymbol{D}^{\dagger}\boldsymbol{x}(t)] \tag{1}$$

which can be mapped onto the analog computer concept of Fig. 1. It consists of a forward path containing a linear time-invariant subsystem (included in the dashed box of Fig. 1) and a feedback path with a memoryless nonlinearity. In the above equation, τ represents the time-integration constant; $\boldsymbol{x}(t) \in \mathbb{R}^n$ is the state-space vector; $\boldsymbol{A} = [a_{ij}] \in \mathbb{R}^{n\times n}$ is a real invertible square matrix; $\boldsymbol{B} = [b_i] \in \mathbb{R}^n$ and $\boldsymbol{D} = [d_i] \in \mathbb{R}^n$ are real vectors; and the nonlinear map $f(\cdot)$ is a real-valued function, which is assumed continuous.

Fig. 2(a) shows a conceptual, generic Gm-C state-variable architecture for an nth-order Lur'e form of the type in (1). In this diagram, state variables are translated into capacitor voltages, the linear transconductors are assumed to perform as ideal VCCS's [see Fig. 2(b)], and the scalar function $f(\cdot)$ is determined by the nonlinear transfer characteristics of the nonlinear transconductors at the right hand side of the figure. According to Fig. 2(c), the output currents supplied by the nonlinear transconductors are given by

$$I_{qj} = g_{mbj} f(\boldsymbol{D}^{\dagger}\boldsymbol{x}). \tag{2}$$

Assuming for simplicity that all the integrating capacitances C_i take the same value C, transconductances g_{mij}, g_{mbi}, and g_{mdi} of Fig. 2(a) can be explicitly calculated from the elements of matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$ in (1), as follows:

$$\begin{aligned} g_{mij} &= a_{ij}C/\tau \\ g_{mbi} &= b_i C/\tau \\ g_{mdi} &= d_i g_{mr} \end{aligned} \tag{3}$$

where $i, j = 1, 2, \cdots, n$, and g_{mr} is a reference transconductance.

Because of the property of *topological conjugacy* [20], the same qualitative dynamics can be achieved by using different values of the transconductances g_{mij}, g_{mbi}, and g_{mdi} [equivalently, matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$ in (1)] in Fig. 2. Based on that, an algorithm can be defined to obtain the optimum set of values for integrated circuit implementation. Two main steps are identified in this algorithm: first, it must systematically generate a large enough set of topologically conjugate systems (definition of the design space); second, it must be able to select the optimum configuration according to some criteria (evaluation of candidates and selection). Both steps will be respectively discussed in this and the next section.

Based on a fundamental theorem about topological conjugacy of vector fields [19], it can be shown that the family L_n can be partitioned into topologically conjugate equivalence classes, each characterized by two characteristic polynomials (equivalently, by their associated eigenvalues). Thus, given a particular nonlinear continuous function $f(\cdot)$, the members of an equivalence class in L_n are formed by those vector fields whose matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$ satisfy

$$\chi(\boldsymbol{A} + \boldsymbol{B}\boldsymbol{D}^{\dagger}) = s^n + p_{n-1}s^{n-1} + \cdots + p_1 s + p_0 \tag{4}$$

and

$$\chi(\boldsymbol{A}) = s^n + q_{n-1}s^{n-1} + \cdots + q_1 s + q_0 \tag{5}$$

where the set of coefficients $(p_0, \cdots, p_{n-1};\ q_0, \cdots, q_{n-1})$ define the class and $\chi(\ )$: $\mathbb{R}^{n\times n} \rightarrow \mathbb{R}$ is the operator which transforms a square matrix into its characteristic polynomial.

Note that while the number of parameters of the matrices in L_n are $n^2 + 2n$, the equivalence classes are defined by only $2n$ coefficients. Thus, there exists infinitely many solutions to (4) and (5). In order to define the space for the optimization procedure, only a finite set formed by the canonical systems in the family L_n will be taken into account.

For our purposes, canonical systems are those vector fields with a minimum number of different nonzero entries in $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$ whose symbolic representation can be found in every equivalence class of L_n, except for a set of zero measure[1] [19]–[22]. Consequently, they can realize almost every prescribed set of coefficients $(p_0, \cdots, p_{n-1};\ q_0, \cdots, q_{n-1})$, and hence, synthesize almost every possible qualitative dynamics in L_n. Because any nonzero matrix entry has to be realized by means of a transconductor in Fig. 2(a), canonical systems are *a priori* the most advantageous in terms of system complexity. On the other hand, because the equivalence classes are defined by $2n$ coefficients, canonical systems are characterized by $2n+1$ different nonzero entries in the matrices (we can assign a value to one of the parameters and solve for the rest).

Not all the templates for matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$ with $2n+1$ different nonzero entries are valid symbolic representations of canonical systems, but the following conditions must be met [19]:

- system must be observable [17]; this excludes, for instance, the case $\boldsymbol{D} = \boldsymbol{0}$;
- system must remain in closed loop; this excludes the case $\boldsymbol{B} = \boldsymbol{0}$;
- system cannot be decomposed into independent subsystems; and
- equations (4) and (5) must be solvable.

[1] Note that some coefficients may appear at different entries of matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$.

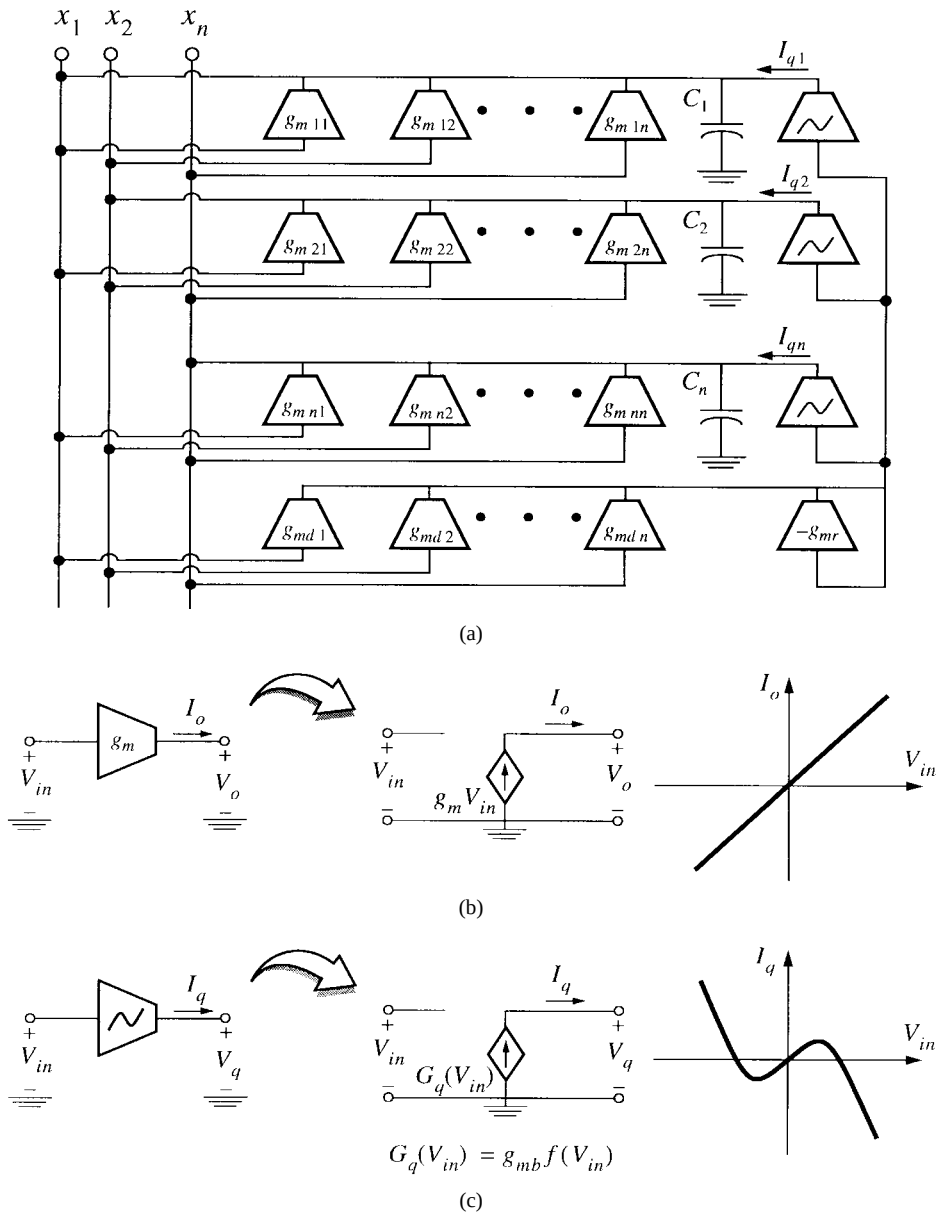

Fig. 2. (a) G_m-C realization of the block diagram in Fig. 1 based on the state-variable approach. (b) Ideal model for the linear transconductors. (c) Ideal model for the nonlinear transconductors.

We have written a computer routine which takes into account the above constraints to sequentially generate all the canonical systems of a given order within the family L_n. At the same time, the routine takes some prescribed coefficients $(p_0, \cdots, p_{n-1};\ q_0, \cdots, q_{n-1})$ as input, and gives the corresponding numerical values of matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$, and, consequently, the transconductance ratios in the generic architecture of Fig. 2(a).

B. High-Level Optimization

Once the design space has been defined, we are in the position to perform the selection process according to some evaluation criteria. In the following, it is assumed that the set of coefficients $(p_0, \cdots, p_{n-1};\ q_0, \cdots, q_{n-1})$ corresponds to some chaotic behavior of interest. The different evaluation criteria are described below.

1) Asymptotic Synchronization: There are two possible ways of using the block diagram of Fig. 1 in a chaotic vector field modulation scheme [23], depending on whether the coding process at the modulator is applied in the forward linear [6] [Fig. 3(a)] or the feedback nonlinear path [24] [Fig. 3(b)]. In both cases, message recovery is achieved by ensuring that the state vector of the demodulator $\boldsymbol{y}(t)$ tends asymptotically to that of the modulator $\boldsymbol{x}(t)$. This is equivalent to saying that the origin of the error system obtained by substracting the state equations of the modulator and demodulator is asymptotically stable. If this occurs, $\boldsymbol{y}_\rho \rightarrow \boldsymbol{x}_\rho$ and thus $d\{\boldsymbol{y}_\rho, c[\boldsymbol{x}_\rho, s(t)]\} = r(t) \approx s(t)$ as $t \rightarrow \infty$ by continuity of $d(\cdot)$. It can be shown that to guarantee the asymptotic synchronization of the encoder/decoder pairs in Fig. 3, matrix $\boldsymbol{A}'$ must have all its eigenvalues in the left complex-half plane [18], [23]. Thus, if the Lur'e form is given by (1), there must

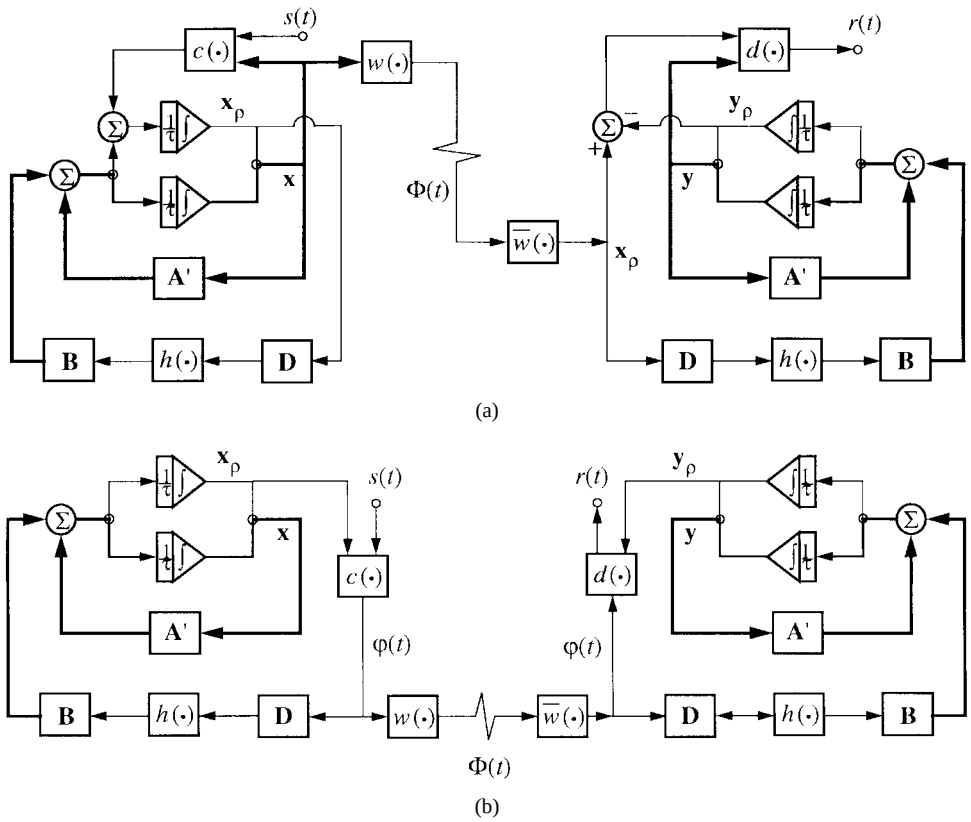

Fig. 3. Encoder/decoder pairs of a vector field modulation scheme using chaotic generators in Lur'e form. (a) Coding function in the forward path. (b) Coding function in the feedback path. $\Phi(t)$ is the transmitted signal; $s(t)$ is an information-bearing signal; $r(t)$ is the recovered message; $\boldsymbol{x}(t)$ and $\boldsymbol{y}(t)$ are, respectively, the state vectors of the transmitter and the receiver; $\boldsymbol{x}_\rho(t)$ and $\boldsymbol{y}_\rho(t)$ are subvectors of $\boldsymbol{x}(t)$ and $\boldsymbol{y}(t)$ formed by all the state variables involved in the nonlinear paths of the transmitter and the receiver, respectively; $c(\ )$ is a continuous function which codifies $s(t)$ with the signal $\boldsymbol{x}(t)$ in (a) [alternatively $\boldsymbol{x}_\rho(t)$ in (b)]; $d(\ )$ is a decoding function, continuous in $\boldsymbol{x}(t)$ for (a) such that $d\{\boldsymbol{x},\ c[\boldsymbol{x},\ s(t)]\} = s(t)$ [alternatively, $d(\ )$ is continuous in $\boldsymbol{x}_\rho(t)$ for (b), and verifies $d\{\boldsymbol{x}_\rho,\ c[\boldsymbol{x}_\rho,\ s(t)]\} - s(t)$]; and functions $w(\ )$ and $\overline{w}(\ )$ are such that $\boldsymbol{x}_\rho = \overline{w}[w(\boldsymbol{x})]$ in (a) and $\varphi = \overline{w}[w(\varphi)]$ in (b).

be a real number p such that matrix $\boldsymbol{A}$ can be decomposed as $\boldsymbol{A} = \boldsymbol{A}' + p\boldsymbol{B}\boldsymbol{D}^\dagger$, with $\boldsymbol{A}'$ verifying the above requirement. As a result, the nonlinearity $h(\cdot)$ in Fig. 3 takes the form $h(z) = f(z) + pz$. Obviously, this is a necessary condition for the selection of a Lur'e form but, unfortunately, not sufficient. Usefulness of a chaotic generator for vector field modulation schemes can only be verified after statistical simulations of the communication link accounting channel imperfections and parameter mismatch. If none of the elements of the design space passes this robustness test, the model defined by $(p_0, \cdots, p_{n-1};\ q_0, \cdots, q_{n-1})$ must be rejected for data encryption purposes.

2) Reduced Complexity: Because system parameters must be mapped into physical devices, those models having a maximum number of zero entries are *a priori* the best suited in terms of area and power consumption. Among the set of templates satisfying this requirement, there are cases especially appealing for integration, for instance, those having a unitary $\boldsymbol{D}$ vector[2] (component $d_\rho = 1$ for some integer $\rho \in [1, n]$, and 0 otherwise). In these configurations, the row of transconductors at the bottom of Fig. 2(a) can be replaced by a simple wire connecting the x_ρ line to the input nodes of the nonlinear blocks, thus saving $n + 1$ linear transconductors. Also, the transmitted signal $\Phi(t)$ in the chaotic modulation schemes of Fig. 3 becomes a scalar quantity, which notably simplifies the communication link.

Other systems advantageous for integration purposes are those with a minimum number of nonlinear blocks. This is because nonlinear transconductors are usually the most area- and power-intensive blocks in the diagram of Fig. 2(a). Thus, templates with $\boldsymbol{B}$ proportional to a unitary vector are also preferred options for monolithic synthesis.

3) Optimum Dynamic Range: Physical implementations of the circuit in Fig. 2(a) suffer from limitations on the dynamic range, because of the internal noise and deviations from the ideal transfer characteristics of real transconductors. The dynamic range must be made as large as possible for a reliable modulation/demodulation of the information signal.

One way to improve the dynamic range of the circuit of Fig. 2(a) is scaling [25], [26]. The purpose of scaling is to make the signal levels of all the state variables equal, so that there is not a single node in the circuit that limits the maximal level of the injected information signal. Let $V_{\max}$ be the maximal input voltage amplitude which can be handled by the transconductors of Fig. 2(a), and let $\boldsymbol{x}_m$ be the vector of the maximal amplitudes reached by the state variables within the chaotic attractor. Scaling is achieved through the linear transformation

$$\boldsymbol{y} = \boldsymbol{K}\boldsymbol{x} \tag{6}$$

[2]This is always possible because we can assign a value to some of the parameters (in this case, the nonnull component of $\boldsymbol{D}$) and solve for the rest.

where $\boldsymbol{y}$ is the state vector of the scaled oscillator; $\boldsymbol{x}$ is the state vector of the original nonlinear system; and $\boldsymbol{K}$ is a nonsingular diagonal matrix defined by

$$\boldsymbol{K} = \begin{bmatrix} k_1 & 0 & \cdots & 0 \\ 0 & k_2 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & k_n \end{bmatrix} \tag{7}$$

where $k_i = V_{\max}/x_{mi}$, $i = 1, 2, \cdots, n$. With this transformation, the scaled equation reads as

$$\tau \frac{d}{dt}\boldsymbol{y}(t) = \boldsymbol{A}_s\boldsymbol{y}(t) + \boldsymbol{B}_s f[\boldsymbol{D}_s^{\dagger}\boldsymbol{y}(t)] \tag{8}$$

where $\boldsymbol{A}_s = \boldsymbol{K}\boldsymbol{A}\boldsymbol{K}^{-1}$, $\boldsymbol{B}_s = \boldsymbol{K}\boldsymbol{B}$, and $\boldsymbol{D}_s^{\dagger} = \boldsymbol{D}^{\dagger}\boldsymbol{K}^{-1}$. Since $\boldsymbol{K}$ defines a similarity transformation, we have

$$\begin{aligned} \chi(\boldsymbol{A}_s) &= \chi(\boldsymbol{K}\boldsymbol{A}\boldsymbol{K}^{-1}) = \chi(\boldsymbol{A}) \\ \chi(\boldsymbol{A}_s + \boldsymbol{B}_s\boldsymbol{D}_s^{\dagger}) &= \chi[\boldsymbol{K}(\boldsymbol{A} + \boldsymbol{B}\boldsymbol{D}^{\dagger})\boldsymbol{K}^{-1}] = \chi(\boldsymbol{A} + \boldsymbol{B}\boldsymbol{D}^{\dagger}) \end{aligned} \tag{9}$$

which means that the scaled system is described by the same set of coefficients $(p_0, \cdots, p_{n-1};\ q_0, \cdots, q_{n-1})$ as the original—it reproduces the same qualitative dynamics. It is worth pointing out that scaling does not affect the system architecture (null entries to matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$ remain unaltered after scaling), but the canonical property of the original system may be lost, i.e., system parameters, initially with identical magnitude, turn to be different after scaling. Thus, the price to pay for improving the dynamic range is a possible increase on the system complexity. In the following steps of the optimization procedure, the design space will be augmented to include the scaled systems.

4) Low Sensitivity to Parameter Variations: Sensitivity analysis [27], [28] is essential to evaluate the tolerance of the chaotic oscillations against parameter deviations, and select those canonical systems which minimize the influence of such variations on the dynamic performance. Since the dynamic behavior of the elements in L_n is governed by the set of coefficients $(p_0, \cdots, p_{n-1};\ q_0, \cdots, q_{n-1})$, it must be known how these values are affected by the variations of the components of matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$. For convenience, let us gather the set of coefficients into the vector

$$\boldsymbol{C} = [p_0 \cdots p_{n-1} \quad q_0 \cdots q_{n-1}]^{\dagger} \tag{10}$$

and define $\boldsymbol{P}$ as the column vector formed by all the entries of matrices $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{D}$

$$\boldsymbol{P} = [\boldsymbol{e}_1^{\dagger}\boldsymbol{A} \quad \boldsymbol{e}_2^{\dagger}\boldsymbol{A} \quad \boldsymbol{e}_3^{\dagger}\boldsymbol{A} \quad \boldsymbol{B}^{\dagger} \quad \boldsymbol{D}^{\dagger}]^{\dagger}. \tag{11}$$

The deviation in the coefficient c_i caused by the variations of the parameter vector $\boldsymbol{P}$ around a nominal point $\boldsymbol{P}_Q$ can be first-order approximated by using a truncated Taylor expansion, which results in

$$\delta c_i = \sum_j \left.\frac{\partial c_i}{\partial p_j}\right|_{\boldsymbol{P}_Q} \cdot \delta p_j = c_i \sum_j \left.\left(\frac{p_j}{c_i}\frac{\partial c_i}{\partial p_j}\right)\right|_{\boldsymbol{P}_Q} \cdot \frac{\delta p_j}{p_{jQ}} \tag{12}$$

where $i = 1, \cdots, 2n$ and $j = 1, \cdots, n^2{+}2n$. Normalizing δc_i with respect to c_i at the nominal point results in the variability or relative change of c_i with respect to $\boldsymbol{P}$

$$\frac{\delta c_i}{c_i} = \sum_j S_{p_j}^{c_i} \cdot \frac{\delta p_j}{p_{jQ}} \tag{13}$$

where the quantity

$$S_{p_j}^{c_i} \equiv \left.\left(\frac{p_j}{c_i}\frac{\partial c_i}{\partial p_j}\right)\right|_{\boldsymbol{P}_Q} = \left.\frac{\partial(\ln c_i)}{\partial(\ln p_j)}\right|_{\boldsymbol{P}_Q} \tag{14}$$

is the sensitivity of c_i to parameter p_j. Defining the stability matrix as $\boldsymbol{S}_{\boldsymbol{P}}^{\boldsymbol{C}} = [S_{p_j}^{c_i}]$, and the variability vectors of $\boldsymbol{C}$ and $\boldsymbol{P}$, respectively, as $\boldsymbol{V}_{\boldsymbol{C}} = [\delta c_i/c_i]$ and $\boldsymbol{V}_{\boldsymbol{P}} = [\delta p_j/p_j]$, (13) can be written in matrix form as

$$\boldsymbol{V}_{\boldsymbol{C}} = \boldsymbol{S}_{\boldsymbol{P}}^{\boldsymbol{C}}\boldsymbol{V}_{\boldsymbol{P}}. \tag{15}$$

It is worth noting that the sensitivity matrix is invariant to the scaling of parameters. Thus, the dynamic range optimization detailed in Section II-B-3 does not affect the matrix $\boldsymbol{S}_{\boldsymbol{P}}^{\boldsymbol{C}}$.

In order to compare the sensitivity performance of the different candidates, matrix $\boldsymbol{S}_{\boldsymbol{P}}^{\boldsymbol{C}}$ gives poor insight. Rather, the worst-case deviations of the coefficients and their respective variances will be used as figures of merit [28]. The worst-case deviations of the coefficients can be obtained by taking the magnitudes on the right-hand side of (15)

$$\boldsymbol{V}_{\boldsymbol{C}}|_{\text{worst-case}} = |\boldsymbol{S}_{\boldsymbol{P}}^{\boldsymbol{C}}||\boldsymbol{V}_{\boldsymbol{P}}| \tag{16}$$

and the variance of the deviations of the coefficients c_i can be obtained by the expression

$$\text{var}(\boldsymbol{V}_{\boldsymbol{C}}) = \boldsymbol{S}_{\boldsymbol{P}}^{\boldsymbol{C}}\,\text{cov}(\boldsymbol{V}_{\boldsymbol{P}})(\boldsymbol{S}_{\boldsymbol{P}}^{\boldsymbol{C}})^{\dagger} \tag{17}$$

where $\text{cov}(\boldsymbol{V}_{\boldsymbol{P}})$ is the square matrix with elements

$$\text{cov}_{jk} = \text{cov}\left\{\frac{\delta p_j}{p_j},\ \frac{\delta p_k}{p_k}\right\} \tag{18}$$

and $\text{cov}(\cdot, \cdot)$ denotes the covariance between two random variables. In evaluating (17), the same matrix $\text{cov}(\boldsymbol{V}_{\boldsymbol{P}})$ is assumed for all the elements of the design space.

5) Reduced Mismatch: Matching properties are largely favored if circuit elements are built by replicating a given unitary device [29]. Thus, if system parameters are related by integer ratios, the circuit will gain in accuracy and, at the layout level, in modularity and integration density. Certainly, this property is always guaranteed whenever the coefficients $(p_0, \cdots, p_{n-1};\ q_0, \cdots, q_{n-1})$ are rational numbers. On the other hand, if the ratio of the largest to the smallest magnitude of the nonzero parameters is very high, the number of unit elements required to implement the oscillator increases, and consequently the area and the power consumption will increase as well [29]. Thus, replication only results efficiently whenever the spread of system parameters is low.[3]

[3]The spread of the system parameters can be minimized with a proper similarity transformation of the state variables. The new system will also reproduce the same qualitative dynamics, but the circuit architecture and sensitivity performance may change.

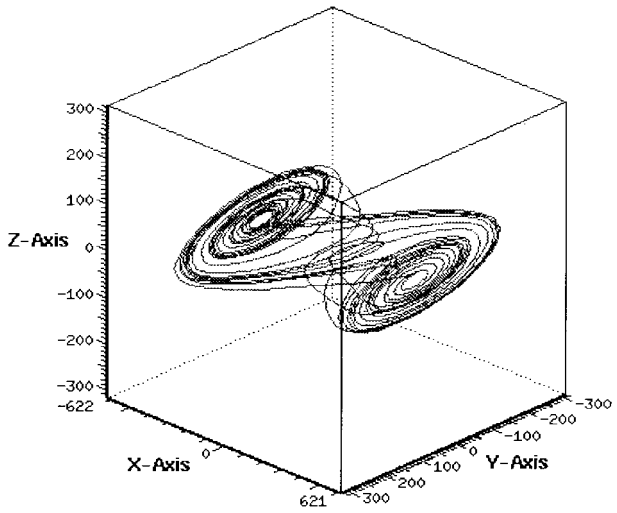

Fig. 4. The double-scroll chaotic attractor.

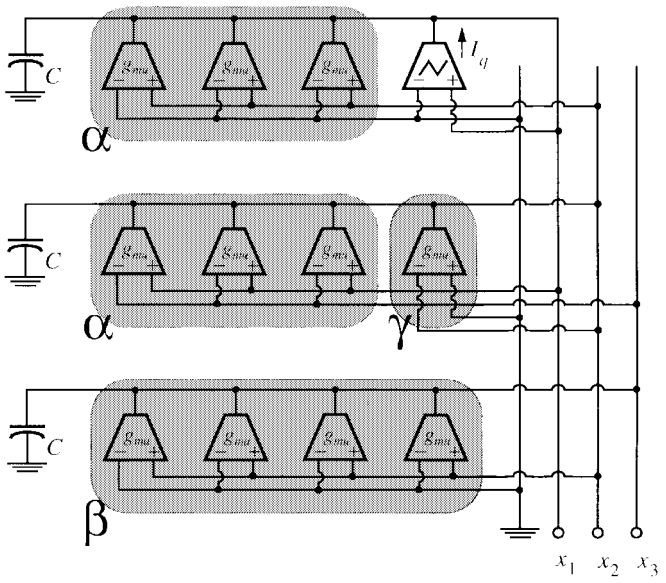

Fig. 5. Optimized G_m-C realization of the Chua's model.

III. Gm-C Design of Chua's Circuit

The above optimization procedure has been applied to the synthesis of an IC-oriented Chua's circuit [30]. As is well known, Chua's circuit is a third-order autonomous system belonging to L_3, with a real-valued continuous PWL nonlinear function given by

$$f[\boldsymbol{D}^\dagger \boldsymbol{x}(t)] = \tfrac{1}{2}\{|\boldsymbol{D}^\dagger \boldsymbol{x}(t) + B_p| - |\boldsymbol{D}^\dagger \boldsymbol{x}(t) - B_p|\} \tag{19}$$

where B_p is a real scale factor. Function $f(\cdot)$ divides $\mathbb{R}^3$ into an inner region D_0 containing the origin, and two outer regions D_{+1} and D_{-1}, such that, $\boldsymbol{F}(\boldsymbol{x}) = -\boldsymbol{F}(-\boldsymbol{x})$. According to (19), the two parallel boundary planes separating D_0 from the outer regions D_{+1} and D_{-1} are given, respectively, by

$$\begin{aligned} U_{+1} &= \{\boldsymbol{x} \in \mathbb{R}^3 | \boldsymbol{D}^\dagger \boldsymbol{x} = B_p\} \\ U_{-1} &= \{\boldsymbol{x} \in \mathbb{R}^3 | \boldsymbol{D}^\dagger \boldsymbol{x} = -B_p\}. \end{aligned} \tag{20}$$

Chua's circuit exhibits a wide variety of bifurcation and chaotic phenomena. Among them, it generates the double-scroll Chua's chaotic attractor (shown in Fig. 4), whose dynamic can be qualitatively defined by the set of characteristic coefficients [30]

$$\begin{aligned} &(p_1, p_2, p_3;\ q_1, q_2, q_3) \\ &\quad = (-0.094,\ 0.429,\ -0.648;\ 1.168,\ 0.847,\ 1.295). \end{aligned} \tag{21}$$

High-level optimization among the canonical members of L_3 described by the above set of coefficients has led to the following system parameters:

$$\boldsymbol{A} = \begin{bmatrix} m_1 & \alpha & 0 \\ \alpha & -\gamma & -\alpha \\ 0 & \beta & 0 \end{bmatrix} \quad \boldsymbol{B} = \begin{bmatrix} m_0 - m_1 \\ 0 \\ 0 \end{bmatrix} \quad \boldsymbol{D} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \tag{22}$$

where

$$(\alpha, \beta, \gamma, m_0, m_1) = (3, 4, 1, 1, -2). \tag{23}$$

The system defined by (22) and (23) verifies most of the criteria defined in the high-level optimization procedure: vector $\boldsymbol{D}$ is unitary, all the parameters have integer values, and their spread is very low (the largest ratio among nonzero parameters is four). Additionally, this configuration is found to exhibit a fairly good sensitivity performance against parameter deviations, and also satisfy the asymptomatic synchronization constraint. Regarding this last point, a convenient value for the parameter p defined in Section II-B1 is $p = m_1/(m_0 - m_1)$—this ensures the necessary condition for asymptotic synchronization of the encoder/decoder pairs of Fig. 3. Statistical simulations of these communication schemes using the system (22), (23) demonstrate a much more robust synchronization ability of Fig. 3(a) than that of Fig. 3(b). Thus, the encoder/decoder pair in Fig. 3(a) will be assumed in the following.

Fig. 5 shows a simplified $G_m - C$ realization of the system (22), (23) based on the general architecture of Fig. 2(a) and using differential-input transconductors. As stated in (3), all the integrating capacitors are assumed identical. Linear transconductors have been implemented by building a unitary block with gain g_{mu} and connecting in parallel as many of such units as indicated by the values of α, β, and γ in (23). On the other hand, the nonlinear transconductor has been designed so that its output current can be expressed as

$$\begin{aligned} I_q &= g_{mu} b_1 [f(x_1) + p x_1] \\ &= g_{mu} \left\{ m_1 x_1 + \frac{m_0 - m_1}{2} \{|x_1 + B_p| - |x_1 - B_p|\} \right\} \end{aligned} \tag{24}$$

according to the encoder/decoder requirements on asymptotic synchronization. Fig. 6 shows two different alternatives for the implementation of the nonlinear transconductor. In both

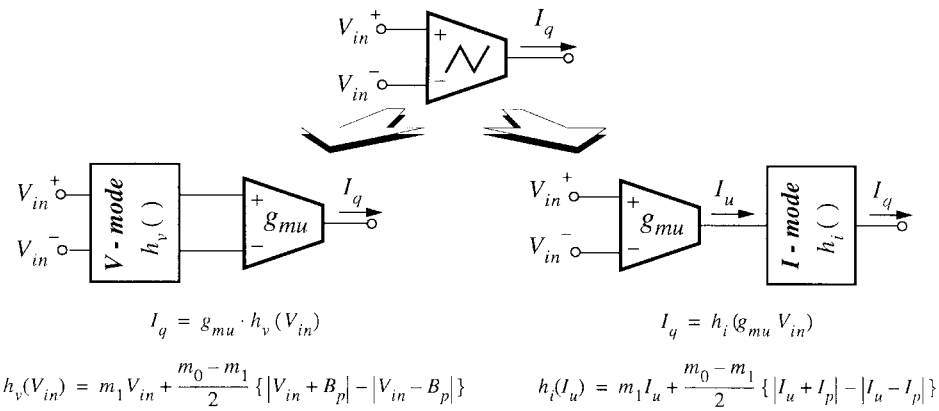

Fig. 6. Alternatives for the physical realization of the nonlinear transconductor.

cases, the PWL transfer function is obtained by shaping the characteristic of a linear transconductor. In Fig. 6(a), shaping is realized in voltage-mode at the front of the unit transconductance element, while in Fig. 6(b) shaping is done in current mode. Equivalence of both alternatives is guaranteed whenever $I_p = g_{mu}B_p$. Subsequent analyzes will use any of these representations as dictated by convenience although, in practice, we have adopted the current shaping approach for the realization of the PWL transconductor.

Two further circuit-level considerations must be taken into account in the design of the schematic of Fig. 5. One is that all the integration nodes are affected by the parasitics present at the input stages of the transconductors. To ensure that all the integration nodes exhibit the same capacitance C_t by construction, an extended approach is to add dummy devices [31]. Following this strategy, the global time constant of the circuit τ is given by

$$\tau = C_t/g_{mu} \tag{25}$$

where C_t is the total capacitance at the state variable nodes. Since parasitics are nonlinear and depend on the operating point of the circuit, it is largely recommended that more than 80% of the total capacitance be contributed by the nominal integrating capacitance C. Note that by adding dummy elements, Fig. 5 can be seen as an array of unit integrators ($g_{mu} - C_t$ structures) grouped by state variables, and loaded by a nonlinear transconductor.

A second consideration is that integrated components suffer severely from uncontrollable process variations (which may be around 30% of the absolute nominal values) due to the statistical deviations in technological parameters, temperature variations, and aging. Because such deviations are intolerable for the synchronization of the encoder/decoder pair of Fig. 3(a), a tuning mechanism [28], [32] must be incorporated to the general system architecture (not shown in Fig. 5). Absolute accuracies of about 1–2% are attainable with such a mechanism [16]—enough to guarantee correct operation of the analog encryption system.

IV. Error Sources and Block Requirements

Hardware nonidealities make any physical realization of the schematic in Fig. 5 deviate from the intended dynamics defined by (22), (23) and may even preclude the appearance of chaotic behavior. Error sources may be dynamic or static. The former are caused by the reactive behavior of the building blocks. Many of these errors can be grouped as integrator nonidealities, and have a large influence on the characteristic coefficients of the system. Another dynamic error source is due to the nonlinear transconductor, which can produce delays and ripples in the state variable x_1 when it crosses from one piece of the characteristics to another.

Static deviations are those observable from the DC characteristics of the building blocks and also have a large influence on the dynamic behavior of the system. For instance, real transconductors deviate from the linear behavior shown in Fig. 2(b), and this gives harmonic distortion, intermodulation, and makes the time constant of the circuit to be a function of the state variables. Another static error source is due to the gradual transition between the segments of the PWL characteristics in a real implementation of the nonlinear transconductor.

From a different perspective, error sources may be classified as deterministic or random. All the error sources referred to so far are deterministic. Attenuation of deterministic errors on the system performance does not require, in general, large device areas, but proper circuit topologies and strategies. Also, these deviations can be easily included as modifications to the mathematical model of the system, and hence, compensations could be developed if required. On the other hand, mismatch errors are strongly dependent on the area of the devices, and there is no reduction technique other than proper sizing. Their effects can be summarized as system parameter deviations, offset terms in the state equations, and time constant variation. Random errors are of crucial importance during the synthesis route, and their effects are in many cases the limiting factor on the accuracy of the system.

In the following, we will discuss three of the most relevant errors on the implementation of the schematic in Fig. 5: the effect of nonideal integrators, the influence of nonlinear static deviations in real transconductors, and the influence of mismatch between circuit components.

A. Effect of Nonideal Integrators

Their influence is better understood by resorting to frequency-domain analysis. Fig. 7 shows a Laplace domain

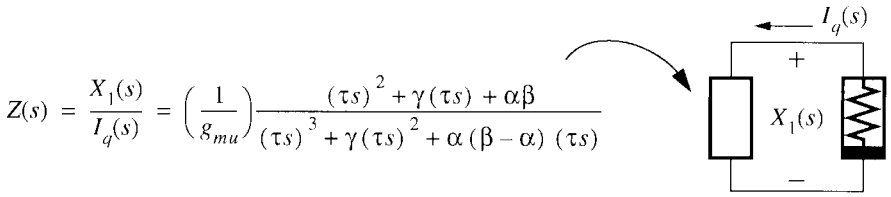

Fig. 7. Laplace domain representation of the optimized Chua's circuit.

representation of Fig. 5, assuming that linear transconductors are ideally modeled as shown in Fig. 2(b). It consists of a linear dynamic one-port terminated in a nonlinear resistor. The linear one-port is described by the impedance rational function $Z(s)$ shown in Fig. 7, and the transfer characteristic of the nonlinear resistor is given by (24). By KVL,

$$\begin{aligned} Z(s) - (g_{mu}m_0)^{-1} &= 0 \qquad x_1 \in D_0 \\ Z(s) - (g_{mu}m_1)^{-1} &= 0 \qquad x_1 \in D_1,\, D_{-1} \end{aligned} \tag{26}$$

which can be expressed in a unified manner as

$$(\tau s)^3 + (\gamma - m)(\tau s)^2 + (\alpha\beta - \gamma m - \alpha^2)\tau s - m\alpha\beta = 0 \tag{27}$$

where $m = m_0$ in the inner region D_0, and $m = m_1$ in the outer regions D_1 and D_{-1}. Solutions of (27) are the natural frequencies of the system. It is worth noting that the product of these frequencies by the time constant τ coincides with the eigenvalues of the dimensionless oscillator model, i.e., the roots of the equations $\chi(\boldsymbol{A} + \boldsymbol{B}\boldsymbol{D}^{\dagger}) = 0$ and $\chi(\boldsymbol{A}) = 0$, with the left hand side terms given by (4) and (5), respectively. Thus, (27) is inherent to the equivalence class defined by (21).

Fig. 8(a) shows a macromodel valid both for the linear and the PWL differential input transconductors used in Fig. 5. It includes the following second-order effects [33]: 1) finite input and output impedance; 2) frequency-dependent transconductance; and 3) output current saturation. Usually, the input conductance is very low and R_{in} can be disregarded with minor problems. Capacitances C_{in} and C_0 (alternatively, C_q for the PWL transconductor) are the parasitics associated to the input and output nodes, respectively. R_0 (alternatively, R_q for the PWL transconductor) represents the output resistance. The internal reactive behavior of the transconductor is modeled by $Z_r(s)$. For angular frequencies up to $\approx 0.2/\tau_2$, this impedance can be approximated as

$$Z_r(s) = 1 - \tau_2 s \tag{28}$$

where τ_2 is a time constant. Finally, function $G(v_{\mathrm{in}})$ in Fig. 8(b) [alternatively, $G_q(v_{\mathrm{in}})$ in Fig. 8(c) for the PWL transconductor] models the output current saturation observed for input voltage larger than E_l. Note that the nonlinear transconductor exhibits the same input impedance and reactive behavior as the linear transconductors, since we have assumed a current shaping approach in its implementation.

Taking into account Fig. 8, the transfer function of the unit integrators in Fig. 5 can no longer be represented by its ideal

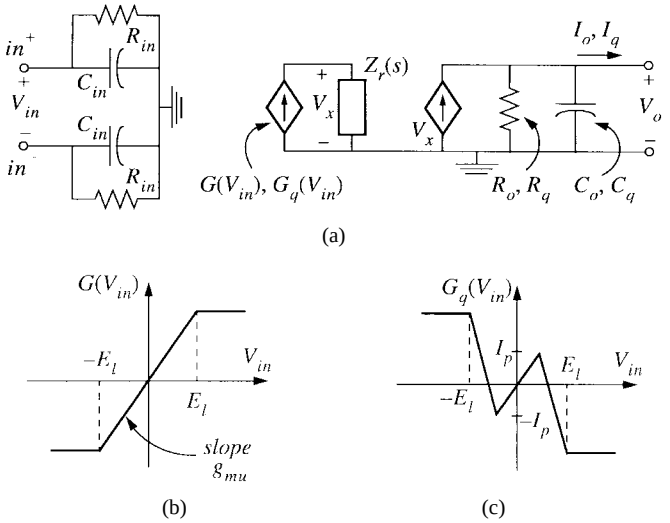

Fig. 8. Second-order effects of real transconductors: (a) macromodel schematic; transfer characteristic of (b) the linear transconductors in Fig. 5, $G(V_{\mathrm{in}}) = (g_{mu}/2)(|V_{\mathrm{in}} + E_l| - |V_{\mathrm{in}} - E_l|)$, and (c) the nonlinear transconductor in Fig. 5, $G_q(V_{\mathrm{in}}) = h_i[G(V_{\mathrm{in}})]$.

characteristic

$$H_{id}(s) = \frac{1}{\tau s} \tag{29}$$

but instead, by the following rational function [34],

$$H_{ni}(s) = A_0 \frac{1 - \tau_2 s}{1 + \tau_1 s} \tag{30}$$

where A_0 is the finite DC gain given by $A_0 = g_{mu}R_t$,[4] and τ_1 is the time constant associated to the resistive component of the impedance at the integration nodes, i.e., $\tau_1 = C_t R_t = A_0\tau$.

Now to examine the effect of the nonideal integrators on the characteristic coefficients of the system, we can use the method proposed in [34], which consists of two steps. First, (27) must be recast into the equivalent form

$$\begin{aligned} 1 + (\gamma - m)H_{id}(s) + (\alpha\beta - \gamma m - \alpha^2)H_{id}^2(s) \\ - (m\alpha\beta)H_{id}^3(s) = 0 \end{aligned} \tag{31}$$

derived from (29). Next, $H_{id}(s)$ must be replaced by $H_{ni}(s)$ in (31) without changing the coefficients of the polynomial. After some algebra, this gives the following modified characteristic

[4]The dummy device approach referred to in Section III can be extended to achieve the same resistive behavior at all the integration nodes. We will represent such a resistance by R_t.

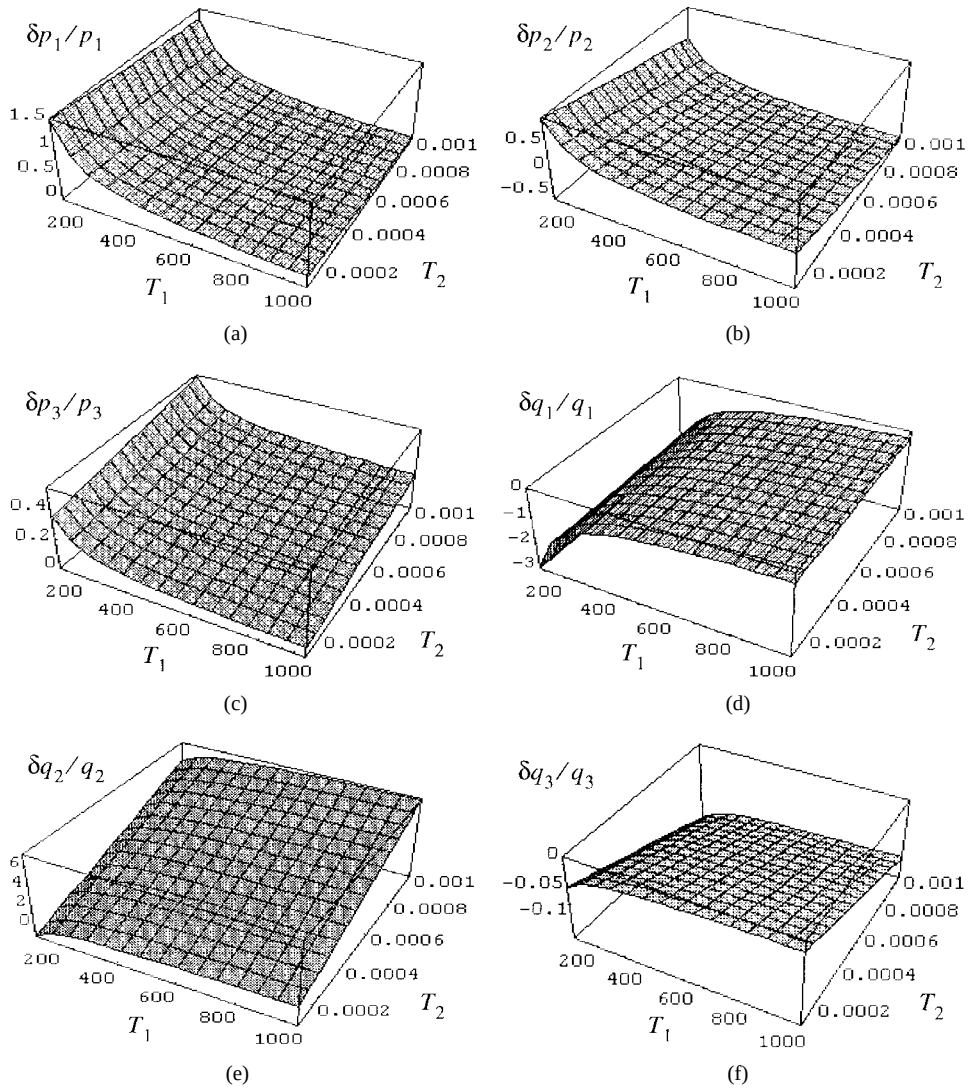

Fig. 9. Influence of nonideal transconductors on the characteristic coefficients.

equation:

$$(\tau s)^3[1-(\gamma-m)T_2+(\alpha\beta-\gamma m-\alpha^2)T_2^2+m\alpha\beta T_2^3] + (\tau s)^2\left[\gamma-m+\frac{3}{T_1}-2\left(\alpha\beta-\gamma m-\alpha^2-\frac{\gamma-m}{T_1}\right)T_2 + \left(-3m\alpha\beta+\frac{\alpha\beta-\gamma m-\alpha^2}{T_1}\right)T_2^2\right] + (\tau s)^1\left[\alpha\beta-\gamma m-\alpha^2-\frac{2(\gamma-m)}{T_1}+\frac{3}{T_1^2} - \left(-3m\alpha\beta+\frac{2(\alpha\beta-\gamma m-\alpha^2)}{T_1}+\frac{\gamma-m}{T_1^2}\right)T_2\right] + (\tau s)^0\left[-m\alpha\beta+\frac{\alpha\beta-\gamma m-\alpha^2}{T_1} + \frac{(\gamma-m)}{T_1^2}+\frac{1}{T_1^3}\right]=0 \tag{32}$$

where T_1 and T_2 are, respectively, the time constants τ_1 and τ_2 normalized with respect to τ:

$$T_1=\frac{\tau_1}{\tau}=A_0 \quad \text{and} \quad T_2=\frac{\tau_2}{\tau}=\frac{A_0}{\tau_1}\tau_2. \tag{33}$$

Note that every member of the equivalence class defined by (21) will show the same dependence on the integrator nonidealities, since (32) has been obtained regardless of the particular system topology used [recall that (27), and hence (31), are inherent to the family of Chua's circuits]. Of course, this is true whenever identical unit integrators are considered, and the nonlinear transconductors exhibit the same reactive behavior as the linear ones.

Fig. 9 shows the percentual variabilities of the coefficients $(p_1, p_2, p_3;\ q_1, q_2, q_3)$ with respect to parameters T_1 and T_2, from where circuit requirements for the transconductance amplifiers can be inferred.

Parameters T_1 and T_2 have a large influence on the dynamic performance of the oscillator (as they modify its natural frequencies) and may even preclude the appearance of chaotic behavior. Obviously this situation is undesirable for data encryption purposes and must be avoided. Thus, it is necessary to obtain a quantitative estimation of parameters T_1 and T_2 that ensure the existence of chaotic motion on the monolithic design. This can be done in a very simple manner using the method proposed by Ogorzalek, which has been successfully

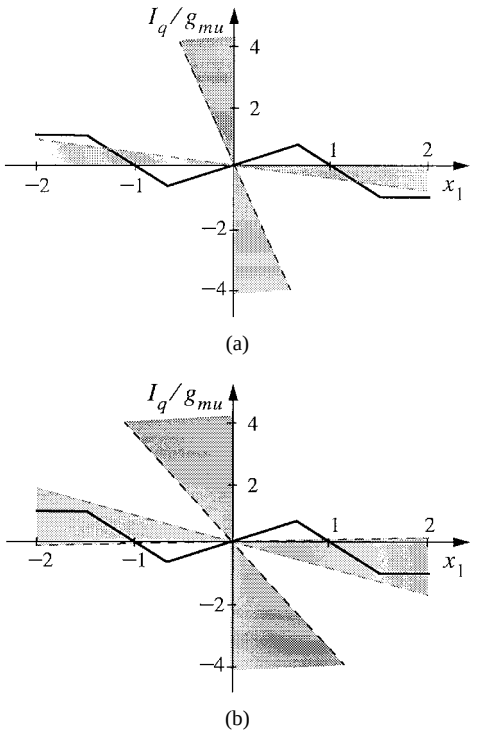

Fig. 10. Effect of the finite gain of the integrators on the stability sectors of the linearized system: (a) infinite gain and (b) gain $T_1 = 5$.

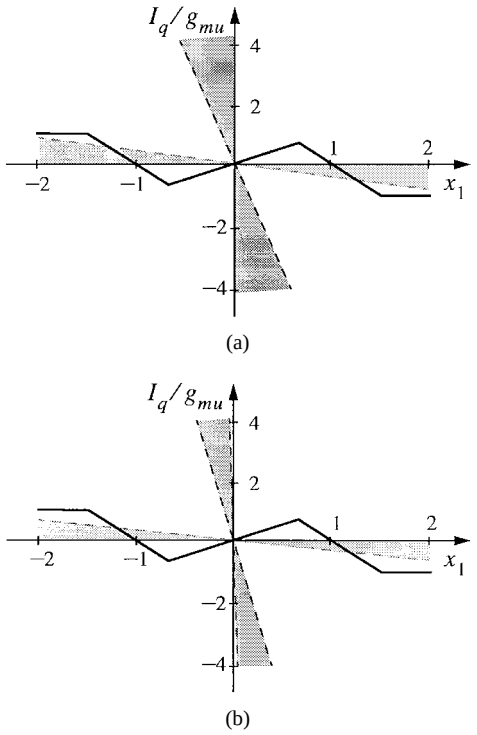

Fig. 11. Effect of the nondominant pole of the integrators on the stability sectors of the linearized system: (a) zero excess phase and (b) $T_2 = 0.01$.

applied to the Chua's circuit [35].[5] Let us consider the linearized system obtained by replacing the nonlinear resistor in Fig. 7 by a linear one of value $(g_{mu}m)^{-1}$ for some real number m, and let us obtain the absolute stability sectors [17] of this linearized system in terms of m. Let us draw these sectors on the driving point characteristic of the nonlinear resistor ($I_q - x_1$ plane). Suppose that the system parameters are such that there exist two disjoint absolute stability (or Hurwitz) sectors separated by unstable regions. Under these circumstances, a necessary condition for the existence of chaotic behavior is that the central piece of the nonlinear resistor DP characteristic lies in a unstable region, while the outer pieces cross over stability sectors.

First assume that $T_2 = 0$, so that, only the effect of T_1 is observed. Taking into account (32) and using the Routh–Hurwitz criterion, the stability sectors of the linearized system are defined by the inequalities:

$$m < \gamma + \frac{3}{T_1} \tag{34}$$

$$m^2\left(\gamma + \frac{2}{T_1}\right) - m\left(\gamma^2 - \alpha^2 + \frac{6\gamma}{T_1} + \frac{8}{T_1^2}\right) + \left(\gamma + \frac{2}{T_1}\right)\left(\alpha\beta - \alpha^2 + \frac{2\gamma}{T_1} + \frac{4}{T_1^2}\right) > 0 \tag{35}$$

$$m < \frac{T_1^2(\alpha\beta - \alpha^2) + T_1\gamma + 1}{T_1^3(\alpha\beta) + T_1^2\gamma + T_1}. \tag{36}$$

Fig. 10(a) shows the stability sectors (shaded areas) drawn in the nonlinearity plane for the ideal case $T_1 \to \infty$, as well as the DP characteristic of the nonlinear resistor [see (24)] for $B_p = 0.75$ V. As can be seen, there are two different Hurwitz sectors; the central piece of the nonlinearity lies in a unstable region; and the outer pieces intersect one of the Hurwitz sectors and pass from the region containing the central piece to the other unstable sector. Thus, the necessary conditions for the appearance of chaotic behavior are met.

Fig. 10(b) shows the effect of the finite gain of the integrators on the stability sectors of the linearized system. It manifests as an expansion of the Hurwitz regions. For low enough gain, both regions merge into a single stability sector, thus precluding the existence of chaos. This occurs for approximately $T_1 = 1.55$. Fig. 10(b) illustrates the case $T_1 = 5$. Note that the outer pieces of the PWL characteristic do not completely cross the stability sector because of the current saturation shown by the nonlinear resistor [see Fig. 8(c)]. As a consequence, no chaotic behavior arises. This observation allows us to characterize the set of suitable DP characteristics which can exhibit the nonlinear resistor to assure chaotic behavior. The slope of the central piece of the characteristic can take any positive value larger than that obtained from (36). On the other hand, the slope of the outer pieces must be negative enough so that the breakpoints originated by the saturation of the characteristic lie on the unstable sectors as shown in Fig. 10(a). Clearly, the range of values for the outer slopes of the characteristic increases as the position of the breakpoints B_p tends to the origin, and conversely, as the saturation points E_l are as far as possible from zero. Thus, parameter B_p, which has been contemplated so far as a mere scale factor on the system dynamics, is shown to play an important role when considering the limitations of real circuits.

[5] This approach, based on control theory, gives necessary conditions for the onset of chaotic oscillations, and hence, only provide lower limits for the parameters T_1 and T_2. Much more accurate results can be obtained using bifurcation analysis at the expense of an enormous computational effort.

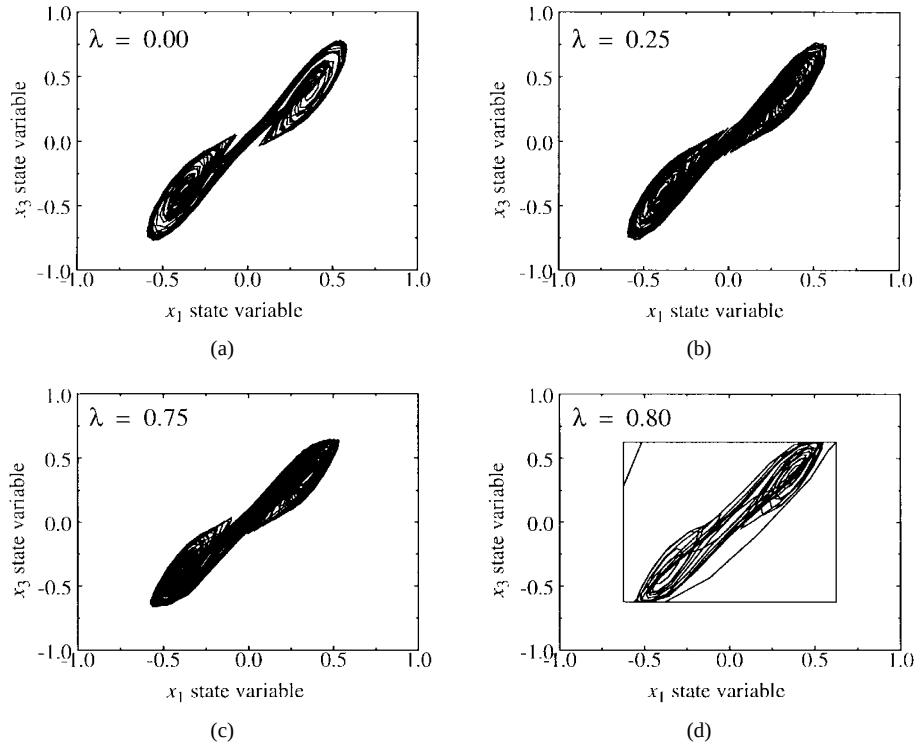

Fig. 12. $x_1 - x_3$ projections of the chaotic attractor for different values of λ.

Let us now consider the effect of T_2 on the chaotic region, assuming infinite gain for the integrators. Again, taking into account (32) and using the Routh–Hurwitz criterion, the stability sectors of the linearized system are given by

$$m > -\frac{1-\gamma T_2+(\alpha\beta-\alpha^2)T_2^2}{T_2-\gamma T_2^2+\alpha\beta T_2^3} \tag{37}$$

$$m < \frac{\gamma-2(\alpha\beta-\alpha^2)T_2}{1-2\gamma T_2+3\alpha\beta T_2^2} \tag{38}$$

$$\begin{aligned} m^2&(\gamma-2\alpha\beta T_2)(1-2\gamma T_2+4\alpha\beta T_2^2)\\ &-m^1[\gamma(\gamma-2\alpha\beta T_2)-\alpha^2-4(\alpha\beta-\alpha^2)\\ &\cdot(\gamma-2\alpha\beta T_2)T_2]\\ &+m^0(\alpha\beta-\alpha^2)[\gamma-2(\alpha\beta-\alpha^2)T_2]>0 \end{aligned} \tag{39}$$

$$m<0. \tag{40}$$

Fig. 11(a) and (b) shows, respectively, the stability sectors (shaded areas) associated to the cases $T_2 = 0$ and $T_2 = 0.01$ for the parameters given in (23). Contrary to the finite gain influence, the effect of the excess phase in the integrators is a shrinking of the Hurwitz regions. Consequently, the chaotic region increases because of the influence of the nondominant poles. However, this advantageous aspect must be seen with caution. For large enough excess phase, the stability sector defined by (37) and (39) reduces to a single line and then disappears, thus precluding the existence of chaos. This occurs for approximately $T_2 = 0.03$ which puts an upper limit on the allowed excess phase.

B. Nonlinear Static Deviations of Transconductors

In practice, the transfer gain of real transconductors varies continuously with the input signal level. Accordingly, the input–output characteristic of the unit transconductors in Fig. 5 must be expressed as $I_0 = G_n(V_{\mathbf{in}})$, where $G_n(\cdot)$ is a continuous, differentiable function [characteristic $G(\cdot)$ in Fig. 8(b) must be regarded as a first-order PWL approximation to $G_n(\cdot)$]. We will further assume that $G_n(\cdot)$ is monotonically increasing and odd-symmetric, so that transconductors are free from systematic offset errors. As an example, if transconductors are built upon basic differential pairs in the saturation region, function $G_n(\cdot)$ is given by

$$G_n(V_{\mathbf{in}}) = \begin{cases} g_{mu}V_{\mathbf{in}}\sqrt{1-(\lambda V_{\mathbf{in}})^2}, & |V_{\mathbf{in}}| \le E_l \\ \dfrac{g_{mu}}{2\lambda}\operatorname{sgn}(V_{\mathbf{in}}), & \text{otherwise} \end{cases} \tag{41}$$

where $E_l = 1/(\sqrt{2}\lambda)$ and λ is a positive real parameter which controls the shape of the characteristic. Observe that for $\lambda = 0$, the ideal characteristic in Fig. 2(b) is recovered.

Using this model for $G_n(\cdot)$ and assuming that the nonlinear transconductor is implemented as in Fig. 6(b), the state equations of the system in Fig. 5 can be written as

$$\begin{aligned} \frac{d}{dt}x_1(t) &= h_i[G_n(x_1)] + \alpha G_n(x_2)\\ \frac{d}{dt}x_2(t) &= \alpha[G_n(x_1) - G_n(x_3)] - \gamma G_n(x_2)\\ \frac{d}{dt}x_3(t) &= \beta G_n(x_2). \end{aligned} \tag{42}$$

Note that in the most general case, $\lambda \neq 0$, this vector field is piecewise continuous, not piecewise linear, which notably complicates its analysis. For this reason, we will exclusively resort to computer simulations.

Fig. 12 illustrates the influence of the shaping parameter λ on the trajectories generated by (42). In all cases, system parameters were those of (23); breakpoint position was $B_p =$

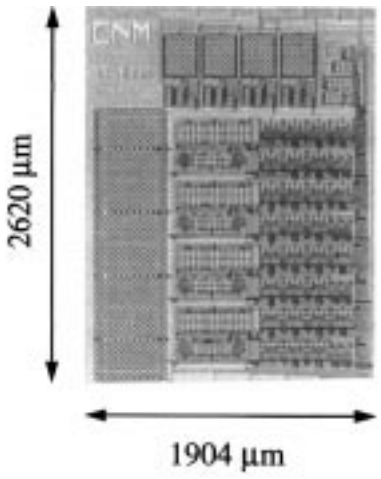

Fig. 13. Chip microphotograph.

0.25; and numerical integrations started at the same initial conditions. Fig. 12(a) shows the $x_1 - x_3$ projection of the chaotic attractor generated by (42) for the ideal case $\lambda = 0$. As parameter λ increases, the shape of the attractor varies, as Fig. 12(b) and (c) shows. For $\lambda = 0.80$, saturation of the transconductance amplifiers causes the trajectory of (42) to become locked, after some transient, at a stable limit cycle. This confirms that the static nonlinear deviations of the transconductors may have dramatic consequences on the dynamic behavior of the system, and must be considered on the realization of the monolithic design.

C. Mismatch Errors on the Circuit Elements

In the following, we will assume that none of the above deterministic error sources is present, and only consider the influence of random deviations on the circuit elements. Assume that every unit transconductance stage in Fig. 5 has a gain deviation and an output offset current. That is, while the ideal characteristic is given by [see Fig. 2(b)]

$$I_0 = g_{mu} V_{\text{in}} \tag{43}$$

we have, in practice,

$$I_0 = (g_{mu} + \delta g_{mu}) V_{\text{in}} + \delta I_{\text{off},\,u} \tag{44}$$

where both δg_{mu} and $\delta i_{\text{off},\,u}$ are stochastic variables, assumed statistically independent with zero mean. Similarly, assume that the currents delivered to the integrating capacitors have a gain slightly different from unity, $A_{FC} = 1 + \delta A_{FC}$, and include an offset term $\delta i_{\text{off},\,FC}$, where again the deviations δA_{FC} and $\delta i_{\text{off},\,FC}$ are statistically independent random variables with zero mean.[6] Finally, assume that the state variable capacitances in Fig. 5 are affected by random variations so that

$$C_i = C + \delta C \tag{45}$$

where C is the nominal value of the three capacitances C_i, and the variations δC are assumed statistically independent with zero mean. Using the above models for the different building blocks in Fig. 5, and considering that the piecewise linear function $h_v(x_1)$, defined in Fig. 6(a), is free from random variations,[7] we have

$$\begin{aligned}
&\frac{(C+\delta C)\,\dfrac{d}{dt}\,x_1(t) - \delta i_{\text{off},\,FC}}{1+\delta A_{FC}} \\
&\quad = [h_v(x_1) + \alpha x_2](g_{mu} + \delta g_{mu}) + \delta i_{\text{off},\,g} \\
&\frac{(C+\delta C)\,\dfrac{d}{dt}\,x_2(t) - \delta i_{\text{off},\,FC}}{1+\delta A_{FC}} \\
&\quad = [\alpha(x_1 - x_3) - \gamma x_2](g_{mu} + \delta g_{mu}) + \delta i_{\text{off},\,g} \\
&\frac{(C+\delta C)\,\dfrac{d}{dt}\,x_3(t) - \delta i_{\text{off},\,FC}}{1+\delta A_{FC}} \\
&\quad = [\beta x_2](g_{mu} + \delta g_{mu}) + \delta i_{\text{off},\,g}
\end{aligned} \tag{46}$$

where $\delta i_{\text{off},\,g}$ is given by

$$\delta i_{\text{off},\,g} = \beta \delta i_{\text{off},\,u} \tag{47}$$

since the value of β defines the maximum number of unit transconductances in the array of Fig. 5. Neglecting the terms containing products of random variables, (46) can be rewritten in the following form:

$$\begin{aligned}
&\frac{(C+\delta C)}{g_{mu}}\,\frac{d}{dt}\,x_1(t) \\
&\quad = [h_v(x_1) + \alpha x_2]\left(1 + \delta A_{FC} + \frac{\delta g_{mu}}{g_{mu}}\right) + \frac{\delta i_{\text{off},\,t}}{g_{mu}} \\
&\frac{(C+\delta C)}{g_{mu}}\,\frac{d}{dt}\,x_2(t) \\
&\quad = [\alpha(x_1 - x_3) - \gamma x_2]\left(1 + \delta A_{FC} + \frac{\delta g_{mu}}{g_{mu}}\right) + \frac{\delta i_{\text{off},\,t}}{g_{mu}} \\
&\frac{(C+\delta C)}{g_{mu}}\,\frac{d}{dt}\,x_3(t) \\
&\quad = [\beta x_2]\left(1 + \delta A_{FC} + \frac{\delta g_{mu}}{g_{mu}}\right) + \frac{\delta i_{\text{off},\,t}}{g_{mu}}
\end{aligned} \tag{48}$$

where

$$\delta i_{\text{off},\,t} = \delta i_{\text{off},\,g} + \delta i_{\text{off},\,FC} \tag{49}$$

or, equivalently, as

$$\begin{aligned}
(\tau + \delta\tau)\,\frac{d}{dt}\,\boldsymbol{x}(t) = &\{\boldsymbol{A}\boldsymbol{x}(t) + \boldsymbol{B} f[\boldsymbol{D}^{\dagger}\boldsymbol{x}(t)]\} \\
&\cdot \left(1 + \delta A_{FC} + \frac{\delta g_{mu}}{g_{mu}}\right) + \frac{\delta i_{\text{off},\,t}}{g_{mu}}
\end{aligned} \tag{50}$$

with matrices $\boldsymbol{A}, \boldsymbol{B}$, and $\boldsymbol{D}$ defined by (22). Observe that all the state equations of the system are affected in the same manner by mismatches—a consequence of the decomposition in unitary elements applied in the schematic of Fig. 5. Note from (50) that the effect of mismatch between the integrating capacitors is to perturb the time constant of the system by $\delta\tau = \delta C / g_{mu}$. On the other hand, the mismatch between

[6] These deviations arise in practice because of the nonideal output stages of the transconductance amplifiers. Adopting the dummy device approach for the realization of Fig. 5, we can assume that all the integrating capacitances are affected in the same way by these deviations.

[7] This assumption can be accepted if the parameters of the nonlinear characteristic are externally controlled with ideally infinite accuracy.

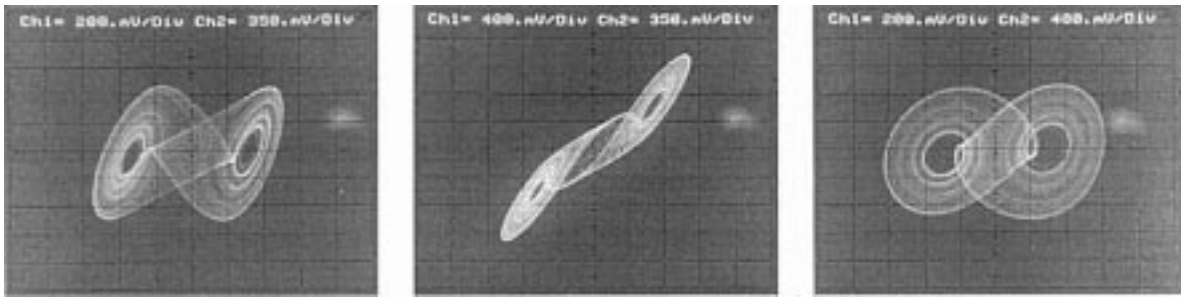

Fig. 14. Measured double-scroll Chua's attractor.

transconductors introduces two different kinds of error contributions. Some of them are time-invariant and have been grouped into the global offset term $\delta i_{\text{off},\,t}/g_{mu}$. The rest of the errors are time-variant since they depend on the state variables.

The consequences of all these variations on the functionality of the network can be evaluated by Monte Carlo analysis. A general theoretical development has not been reported yet, and hence, it is difficult to establish the form and the error levels which can be tolerated. Among the many possible criteria, we have chosen a measure which can be translated to the individual building blocks, with the intention of optimizing their implementation.

Assuming that the magnitudes of the state variables are always below the clamping voltage, E_l of the transconductors, the maximum nominal current which can be delivered at any time instant by the transconductors is found to be

$$\max\{I(t)\} = E_l \cdot [\beta g_{mu}]. \tag{51}$$

Now, for the output stages of the transconductors, we request that the current gain error be bounded by

$$|\delta A_{FC}| \leq \frac{\varepsilon}{4} \tag{52}$$

and that the offset error, relative to the maximum output current coming from the unit transconductance elements given by (51), be bounded by

$$\left|\frac{\delta i_{\text{off},\,FC}}{\max\{I(t)\}}\right| \leq \frac{\varepsilon}{4}. \tag{53}$$

Similarly, for every individual differential input stage implementing a transconductance g_{mu} and driven by a signal x_i,[8] we request that the relative transconductance error be bounded by

$$\left|\frac{\delta g_{mu}}{g_{mu}}\right| \leq \frac{\varepsilon}{4} \tag{54}$$

and that the offset error, relative to the maximum output signal of the transconductor $E_l g_{mu}$, be bounded by

$$\left|\frac{\delta i_{\text{off},\,u}}{E_l g_{mu}}\right| \leq \frac{\varepsilon}{4}. \tag{55}$$

Note that this is equivalent to establishing the same bound for the input-referred offset error $\delta i_{\text{off},\,t}/g_{mu}$, relative to the maximum input signal level E_l.

[8] Here, x_i denotes a state variable. The errors are due to the circuit elements, and not to the signals, which are assumed exact in every case.

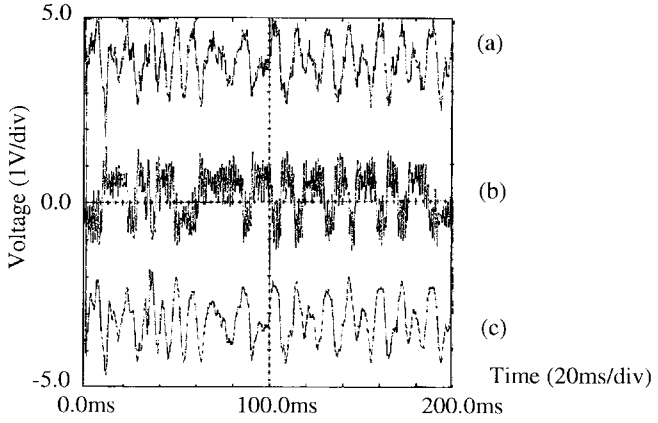

Fig. 15. Audio data transmission.

Conditions (52)–(55), applied on corresponding building blocks in the cell, allow the obtention of a bound for the error δI of the integrand $I(t)$ of every state equation. The bound of this error can be calculated as follows:

$$\begin{aligned}|\delta I| &= \left|\beta g_{mu} E_l \left(\delta A_{FC} + \frac{\delta g_{mu}}{g_{mu}}\right) + \delta i_{\text{off},\,t}\right| \\ &\leq \beta g_{mu} E_l \left[|\delta A_{FC}| + \frac{|\delta g_{mu}|}{g_{mu}} + \frac{1}{\beta}\frac{|\delta i_{\text{off},\,t}|}{E_l g_{mu}}\right] \\ &\leq \beta g_{mu} E_l \left[|\delta A_{FC}| + \frac{\delta g_{mu}|}{g_{mu}} + \frac{|\delta i_{\text{off},\,u}|}{E_l g_{mu}} + \frac{|\delta i_{\text{off},\,FC}|}{E_l \beta g_{mu}}\right] \\ &\leq \varepsilon \cdot \beta g_{mu} E_l = \varepsilon \cdot \max\{I(t)\}. \end{aligned} \tag{56}$$

Hence, the random error on any of the integrands is, at any time instant, less than a fraction of its maximum possible nominal value. In addition, since the relative errors on the weights are individually bounded, it can be expected that, for sufficiently low values of ε, the behavior of the system will be similar to the nominal one.

V. Circuit Design and Experimental Results

Taking into account the influence of the error sources discussed in the previous section, we have designed a monolithic circuit based on the schematic of Fig. 5, suitable for data encryption using the vector field modulation scheme of Fig. 3(a). All parameters in this circuit are electrically controllable to serve as cryptographic key in the audio transmission scheme.

Fig. 13 shows a microphotograph of the chaotic modulator/demodulator unit, which includes an on-chip tuning

scheme, and other auxiliary circuitry for biasing and measurement purposes. The dimensions of the circuit (developed in a 2.4 μm double-poly double-metal CMOS technology) have been also indicated in Fig. 13. Power dissipation is less than 1.8 mW for a symmetrical biasing of ± 2.5 V. Further details of the prototype are given in [36]. Because of their optimum design, the fabricated prototype is able to reproduce the whole bifurcation sequence toward the double-scroll Chua's attractor in a robust and reproducible manner.

Fig. 14 shows the projections of the double-scroll featured by the circuit. Fig. 15 illustrates the performance of the whole audio encryption scheme using the vector filed modulation scheme of Fig. 3(a) with $\boldsymbol{x}_\rho = x_1$; the coding function is a simple addition. Input signal [Fig. 15(a)] consists of a segment of speech. The worst-case signal-to-noise ratio of the recovered signal [Fig. 15(b)] is greater than $+40$ dB (this occurs at very low frequencies) with less than -0.2 dB loss of the input signal power. At higher frequencies, the signal-to-noise ratio rises up to $+60$ dB, while retaining similar losses at the receiver. As can be seen from Fig. 15, the transmitted signal [Fig. 15(c)] bears no resemblance to the information content.

VI. Conclusions

Every monolithic implementation encompasses several design considerations both at the system and at the circuit levels. System-level considerations center on the actual architecture of the nonlinear oscillator. Since there is a large variety of synthesis methods to realize a given electronic system, these criteria must determine which architecture provides the best compromise between complexity and performance. Important factors in the choice of a synthesis method are dynamic range properties and sensitivity to parameter variations. At the circuit level, the designer has to deal with the limitations imposed by the technological process, as well as the desired operating frequency, and the required tunability range. Additionally, there are topological demands coming from the system level, such as the number of inputs and outputs of the building blocks, and the specifications of the block requirements. Depending on the above considerations, designers have to decide which active elements are used to construct the building blocks defined at the system level, or the convenience of using balanced topologies, among other things. Other important constraints at the circuit level are chip area and power dissipation. These considerations are used in this paper for optimum choice of the chaotic state equation which is the best suited for implementation using Gm-C integrated circuit techniques.

References

[1] M. Hasler, "Engineering chaos for encryption and broadband communication," *Philos. Trans. R. Soc. Lond. A*, vol. 353, pp. 115–126, Oct. 1995.

[2] U. Parlitz, L. O. Chua, L. Kocarev, K. S. Halle, and A. Shang, "Transmission of digital signals by chaotic synchronization," *Int. J. Bifurc. Chaos*, vol. 2, no. 4, pp. 973–977, 1992.

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

[4] H. Dedieu, M. P. Kennedy, and M. Hasler, "Chaos shift keying: Modulation and demodulation of a chaotic carrier using self-synchronizing Chua's circuits," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 634–642, Oct. 1993.

[5] K. M. Cuomo and A. V. Oppenheim, "Circuit implementation of synchronized Chaos with applications to communications," *Phys. Rev. Lett.*, vol. 71, no. 1, pp. 65–68, July 1993.

[6] K. S. Halle, C. W. Wu, M. Itoh, and L. O. Chua, "Spread spectrum communication through modulation of chaos," *Int. J. Bifurc. Chaos*, vol. 3, no. 2, pp. 469–477, 1993.

[7] F. Böhme and W. Schwarz, "The chaotizer–dechaotizer channel," *IEEE Trans. Circuits Syst. I*, Mar. 1996.

[8] A. I. Panas, A. S. Dmitriev, L. Z. Kuzmin, and S. O. Starkov, "RF-band communications using chaos," in *Proc. NDES'96*, June 1996, pp. 167–171.

[9] A. Rodríguez-Vázquez, M. Delgado-Restituto, S. Espejo, and J. L. Huertas, "Switched capacitor broadband noise generator for CMOS VLSI," *Electron. Lett.*, vol. 27, no. 21, pp. 1913–1915, Oct. 1991.

[10] M. Delgado-Restituto, F. Medeiro, and A. Rodríguez-Vázquez, "Nonlinear switched-current CMOS IC for random signal generation," *Electron. Lett.*, vol. 29, no. 25, pp. 2190–2191, Dec. 1993.

[11] A. Rodríguez-Vázquez and M. Delgado-Restituto, "Generation of chaotic signals using current-mode techniques," *J. Intell. Fuzzy Syst.*, vol. 2, no. 1, pp. 15–37, Jan. 1994.

[12] M. Delgado-Restituto and A. Rodríguez-Vázquez, "Switched-current chaotic neurons," *Electron. Lett.*, vol. 30, no. 5, pp. 429–430, Mar. 1994.

[13] H. Horio and K. Suyama, "Experimental verification of signal transmission using synchronized SC chaotic neural networks," *IEEE Trans. Circuits Syst. I*, vol. 42, pp. 393–395, July 1995.

[14] A. Rodríguez-Vázquez, and M. Delgado-Restituto, "CMOS design of chaotic oscillators using state variables: A monolithic Chua's circuit," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 596–613, Oct. 1993.

[15] J. M. Cruz and L. O. Chua, "An IC chip of Chua's circuit," *IEEE Trans. Circuits Syst. II*, vol. 40, pp. 614–625, Oct. 1993.

[16] M. Delgado-Restituto, A. Rodríguez-Vázquez, R. L. Ahumada, and M. Liñán, "Experimental verification of secure communication using monolithic chaotic circuits," in *Proc. ECCTD'95*, Aug. 1995, vol. I, pp. 471–474.

[17] M. Vidyasagar, *Nonlinear Systems Analysis*, 2nd ed. Englewood Cliffs, NJ: Prentice-Hall, 1993.

[18] U. Feldmann, M. Hasler, and W. Schwarz, "Communication by chaotic signals: The inverse systems approach," *Int. J. Circuit Theory Appl.*, vol. 24, no. 5, pp. 551–579, Sept. 1996.

[19] C. W. Wu and L. O. Chua, "On the generality of the unfolded Chua's circuit," Memo. UCB/ERL M95/62, Aug. 1995.

[20] S. Wiggins, "Global bifurcations and chaos. Analytical methods," *Applied Mathematical Series 73.* New York: Springer-Verlag, 1988.

[21] L. O. Chua and G. N. Lin, "Canonical realization of Chua's circuit family," *IEEE Trans. Circuits Syst.*, vol. 37, pp. 885–902, July 1990.

[22] L. O. Chua, "Global unfolding of Chua's circuit," *IEICE Trans. Fundamentals*, vol. E-76-A, no. 5, pp. 704–734, May 1993.

[23] C. W. Wu and L. O. Chua, "A unified framework for synchronization and control of dynamical systems," *Int. J. Bifurcation Chaos*, vol. 4, no. 4, pp. 979–998, 1994.

[24] ———, "A simple way to synchronize chaotic systems with applications to secure communication systems," *Int. J. Bifurcation Chaos*, vol. 3, no. 4, pp. 1619–1627, 1993.

[25] R. Gregorian and G. C. Temes, *Analog MOS Integrated Circuits for Signal Processing.* New York: Wiley, 1986.

[26] G. Groenewold, "The design of high dynamic range continuous-time integratable bandpass filters," *IEEE Trans. Circuits Syst.*, vol. 38, pp. 838–852, Aug. 1991.

[27] A. S. Sedra and P. O. Brackett, *Filter Theory and Design: Active and Passive.* Portland, OR: Matrix, 1978.

[28] R. Schaumann, M. S. Ghausi, and K. R. Laker, *Design of Analog Filters. Passive, Active RC, and Switched Capacitor.* Englewood Cliffs, NJ: Prentice-Hall, 1990.

[29] E. A. Vittoz, "The design of high performance analog circuits on digital CMOS chips," *IEEE J. Solid-State Circuits*, vol. SC-20, pp. 657–665, June 1985.

[30] R. N. Madan, Ed., *Chua's Circuit: A Paradigm for Chaos.* Singapore: World Scientific, 1993.

[31] J. E. Kardontchik, *Introduction to the Design of Transconductor-Capacitor Filters.* Boston, MA: Kluwer, 1992.

[32] Y. P. Tsividis and J. O. Voorman, Eds., *Integrated Continuous-Time Filters.* New York: IEEE Press, 1993.

[33] A. Rodríguez-Vázquez, B. Linares-Barranco, J. L. Huertas, and E. Sánchez-Sinencio, "On the design of voltage-controlled sinusoidal oscillators using OTAs," *IEEE Trans. Circuits Syst.*, vol. 37, pp. 198–211, Feb. 1990.

[34] W. J. A. de Heij, E. Seevinck, and K. Hoen, "Practical formulation of the relation between filter specifications and the requirements for integrator circuits," *IEEE Trans. Circuits Syst.*, vol. 36, pp. 1124–1128, Aug. 1989.
[35] M. J. Ogorzalek, "Chaotic regions from double scroll," *IEEE Trans. Circuits Syst.*, vol. 34, pp. 201–203, Feb. 1987.
[36] M. Delgado-Restituto, M. Liñán, J. Ceballos, and A. Rodríguez-Vázquez, "Bifurcations and synchronization using an integrated programmable chaotic circuit," *Int. J. Bifurcation Chaos*, accepted for publication.

Manuel Delgado-Restituto (M'96) was born in Seville, Spain. He received the Bachelor's degree in physics in 1988, and the Ph.D. degree in physics in 1996, both from the University of Sevilla, Spain.

Since 1990, he has been working at the Analog Design Department of the Spanish Microelectronics Center, Sevilla, Spain, as a member of the research staff. His research interests include analog and mixed-mode integrated circuit design for nonlinear signal processing using neuro-fuzzy controllers and chaotic circuits. He is also interested in the design of radio frequency integrated circuits for wireless communication.

Angel Rodríguez-Vázquez (M'80–SM'96–F'96) received the degree of Doctor en Ciencias Físicas from the University of Sevilla, Spain, in 1983.

Since 1978 he has been with the Department of Electronics and Electromagnetism at the University of Sevilla, where he is currently a Professor of Electronics. In 1989, he joined the research staff of the Department of Analog Circuit Design of the Spanish Microelectronics Center. He has research interests in the design of analog and mixed-signal VLSI circuits for nonlinear signal processing, including vision chips, neuro-fuzzy controllers, and chaotic circuits. His work in these areas has resulted in systematic design methodologies to design these kinds of chips. He also has an interest in the design and modeling of data converters with an emphasis on $\Sigma\Delta$ techniques, symbolic analysis of analog integrated circuits, and optimization of analog integrated circuits. He has authored or coauthored more than 150 publications.

Dr. Rodríguez-Vázquez was co-recipient of the 1995 Guillemin–Cauer award of the IEEE Circuits and Systems Society, and the best paper award of the 1995 European Conference on Circuit Theory and Design. He has been a member of different Technical Program Committees and has served as an Associate Editor and Guest Editor for the IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS—PART II: ANALOG AND DIGITAL SIGNAL PROCESSING and the IEEE Press.