Experimental Verification of Chaotic Encryption of Audio using Monolithic Chaotic Modulators

M. Delgado-Restituto, A. Rodríguez-Vázquez and M. Liñán

Dept. of Analog Design, CNM
Edificio CICA, C/ Tarfia sn, 41012-Sevilla, SPAIN
Phone #34 5 4623811, FAX #34 5 4624506

ABSTRACT

This paper reports the first experimental verification of chaotic encryption of audio signals using integrated circuits. It is based on a g_m-C modulator/demodulator analog CMOS IC that implements a 3rd-order nonlinear differential equation. This has been fabricated in 2.4μm double-poly technology and includes on-chip tuning circuitry based on amplitude detection. It is capable of generating controllable continuous-time chaotic signals. Also, measurements demonstrate how to exploit the synchronization between two of them for encrypted transmission. In these experiments, the worst-case signal to noise ratio of the recovered signal is greater than +40dB (at the low corner of the audio spectrum) with less than -0.2dB loss of the input signal power. At higher frequencies, the signal-to-noise ratio rises up to +60dB, while retaining similar losses at the receiver.

KEYWORDS: Chaotic Circuits, Chaotic Encryption, Nonlinear Microelectronics, Analog Integrated Circuits

1. INTRODUCTION

In the last years, many experimental results have confirmed that the cells in a network of chaotic oscillators may evolve in phase, in spite of their intrinsically irregular behavior and sensitivity to initial conditions [1]. This nontrivial fact has drawn considerable interest, not only at a theoretical level (giving rise to an increasing number of papers about the phenomenon), but also due to the potential engineering applications based on so-called *chaotic synchronization.*

One of the most promising applications refers to the *encryption* of data. The basic idea is to exploit the noise-like appearance of a chaotic carrier to hide an information-bearing signal, and make use of the synchronization property to recover the data. Fig.1 shows a block diagram for the realization of this idea based on *chaotic modulation* [2,3]. At the emitter side the information bearing signal, represented by the current $s(t)$, is injected into a chaotic oscillator (modulator unit), thereby modifying its dynamics. If the power of the chaotic signal is large as compared to that of the information signal, the transmitted signal $v_t(t)$remains chaotic and, thus, undecipherable. However, this transmitted signal still contain the information related to $s(t)$, which can be recovered at the receiver side by using a demodulator unit which synchronizes to the modulation used in the transmitter.

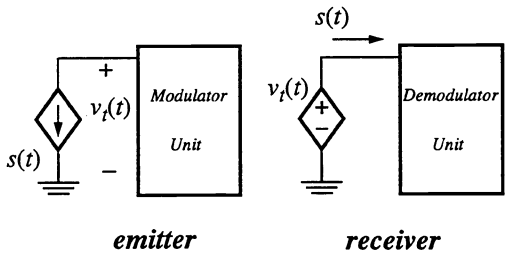

Fig. 1: Chaotic Modulation Scheme.

This conceptually simple encryption mechanism open new vistas for innovative application of analog integrated circuits, based on nonlinear signal processing concepts. However, proper design of this kind of circuits involve a strict compromise between the *robustness* against parameter variations of the chaotic synchronization, needed to decode the encrypted signal, and the *security* of the communication, so that an intruder cannot intercept the information content. Although some groups have realized chaotic encryption using discrete circuits, the above difficulties have precluded their realization using monolithic modulator/demodulator units. This paper reports the first experimental verification of chaotic encryption of audio signals using integrated circuits.

2. MATHEMATICAL MODEL AND CIRCUIT DESIGN

It is represented by a third order continuous-time nonlinear state equation,

0-8194-1976-1/95/$6.00

$$\frac{d}{dt}\mathbf{x}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}\, f\left[\mathbf{D}^{\mathrm{T}}\mathbf{x}(t)\right] \tag{1}$$

where $\mathbf{x}(t) = [x(t), y(t), z(t)]^{\mathrm{T}}$ is the state vector; $\mathbf{A}=[\, a_{ij}\,]$ is a real matrix which defines the linear part of the system; $\mathbf{B}=[\, b_i\,]$ and $\mathbf{D}=[\, d_i\,]$ are real vectors; and $f(\bullet)$ is a real-valued odd symmetric piecewise-linear (PWL) function,

$$f(\mu) = s_1\mu + \frac{s_0 - s_1}{2}\{|\mu + B_p| - |\mu - B_p|\} \tag{2}$$

Smoother approximations to this PWL function also qualify for data encryption purposes.

State equations (1) can be mapped onto a g_m–C circuit where state variables are represented by the capacitor voltages. Fig.2 shows a block diagram where a_{ij} equals g_{mij}/C_i, b_i equals g_{mbi}/C_i, and the components of $\mathbf{D}$ are implemented via finite gain voltage amplifiers.

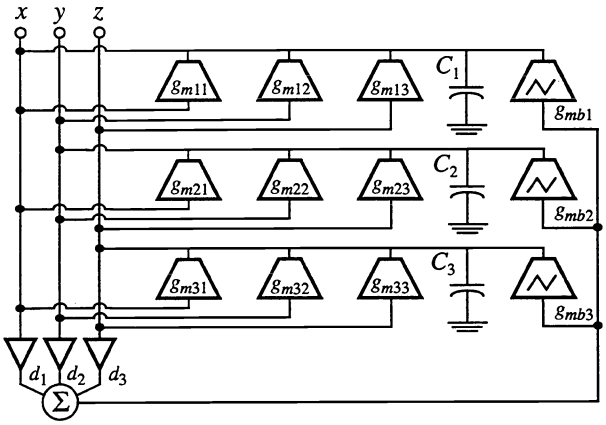

Fig. 2: Chaotic Unit Block Diagram.

The intended application of data encryption can be realized using many different set of parameter values. The point is to identify those which are the best suited for monolithic implementation. It involves searching in the parameter space to find the optimum solution owing to considerations on mismatching, loading, etc. In particular, loading considerations recommend to equalize the capacitors, i.e. $C \equiv C_1 = C_2 = C_3$, and to keep each capacitor loaded by the same number of transconductors. On the other hand, matching of the transconductors is improved by enforcing the following rules:

- Transconductances must be integer multiples of a given unit element g_{mu}. Thus, non-integer n/m ratios can be realized by separately grouping n and m unit transconductors. Application of this criterium significantly simplifies the design of the circuit, since only one transconductor need be designed to reproduce all the rest.

- Spread of transconductances should be minimized.

This, together with the use of on-chip tuning, provide accuracies of about 1-2% in the pole frequency -- enough to guarantee synchronization of the emitter (modulator) and the receiver (demodulator) units. With these rules in mind we have done an exhaustive search in the parameter space of (1), to determine the optimum configuration. The resulting model is described by the following set of equations:

$$\frac{dx}{dt} = f(x) + \alpha y \qquad \frac{dy}{dt} = \alpha(x - z) - y \qquad \frac{dz}{dt} = \beta y \tag{3}$$

where $f(\bullet)$ is given by (2), and the parameter values are:

$$(\alpha, \beta, s_0, s_1) = (3, 4, -2, 2) \quad (4)$$

Monte Carlo analysis with uncorrelated relative variations of up to 7% from the nominal values in (4), show that 100% of the obtained trajectories evolve towards a chaotic attractor.

The preliminary considerations for the design are completed by the choice of the time constant, $\tau = 2\pi C/g_{mu}$. Our purpose in this experimental prototype is the signal transmission in the voice-band, which, after several behavioral trials, has led to the following nominal values, $C = 30$pF and $g_{mu} = 1.0$ μA/v.

Fig.3 shows the schematics used for the transconductor, which includes a source-degeneration scheme for linearization [4]. Fig.4 shows the circuit used for the PWL function consisting of a front-end transconductor and a nonlinear circuit that operates in current domain based on the high-accurate rectification mechanism proposed by the authors in [5]. All parameters in this nonlinear characteristics have been made externally controllable to serve as cryptographic key in the audio transmission scheme.

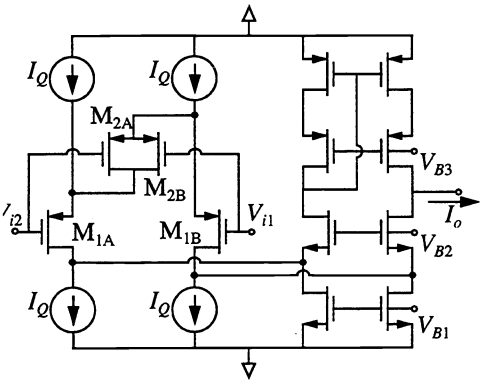

Fig. 3: Linearized transconductor.

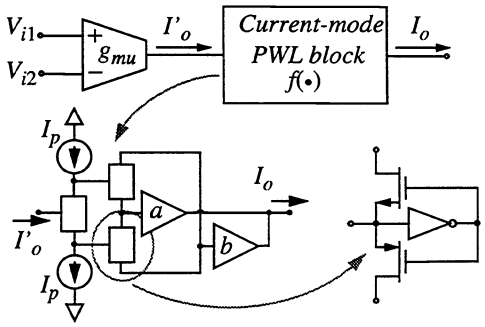

Fig. 4: PWL Function Circuit.

Fig.5 shows the block diagram of the circuit used for on-chip tuning, based on amplitude detection. Here, a reference sinusoidal signal passes through an integrator and the changes in the output amplitude, if the signal frequency changes, are detected and used to tune the system.

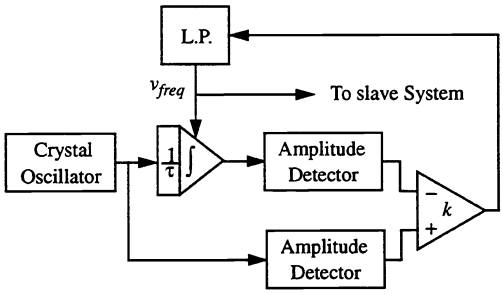

Fig. 5: On-chip Automatic Tuning.

3. EXPERIMENTAL RESULTS

Fig.6 shows a microphotograph of the chaotic modulator/demodulator unit, which includes the 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) has been also indicated in Fig.6. Power dissipation is less than 1.8mW for a symmetrical biasing of ±2.5v.

For the previously cited design parameters the oscillator generates fully *aperiodic, ergodic* waveforms at *x(t), y(t),* and *z(t).* Despite their aperiodicity, these trajectories remain confined to regions of regular, characteristic shape within the state space, cre-

ating *attractors*. Fig.7 shows the *double-scroll* Chua's attractor [3], measured from the fabricated prototype. The picture represents the Lissajous projection onto the (x, z) plane of the state space (horizontal axis 250mV/div, vertical axis 350mV/div). Results are in full accordance with the theory and simulations.

Fig.8 illustrates the performance of the whole secure communication scheme. Input signal (Fig.8(a)) consists of a segment of speech. The worst-case signal to noise ratio of the recovered signal (Fig.8(b)) is greater than +40dB (this occurs at very low frequencies) with less than -0.2dB loss of the input signal power. At higher frequencies, the signal-to-noise ratio rises up to +60dB, while retaining similar losses at the receiver. As can be seen from Fig.8, the transmitted signal (Fig.8(c)) keeps no resemblance to the information content.

4. ACKNOWLEDGMENTS

This research has been supported partially by ESPRIT IV Project 8795 AMFIS.

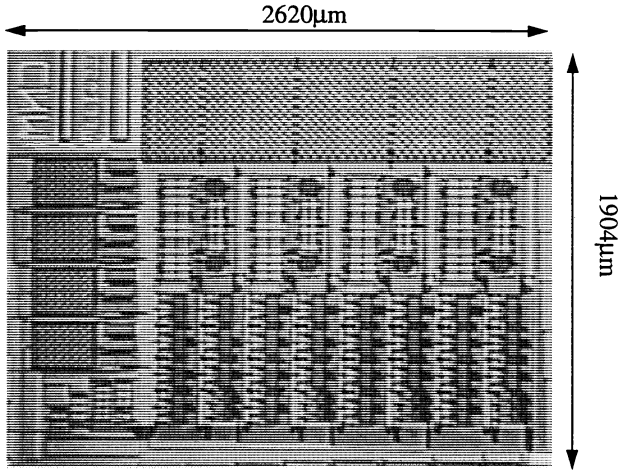

Fig. 6: Chip Microphotograph.

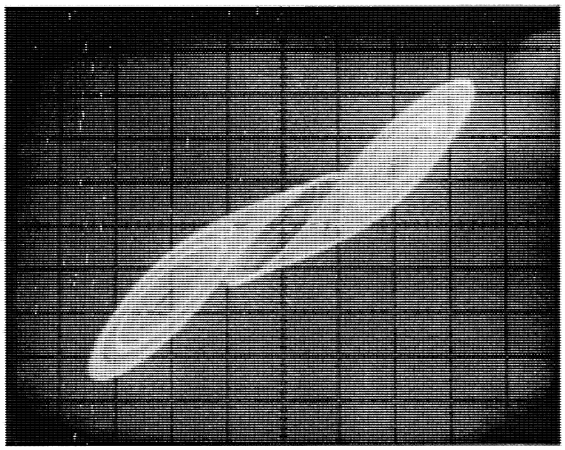

Fig. 7: Measured Chaotic Attractor.

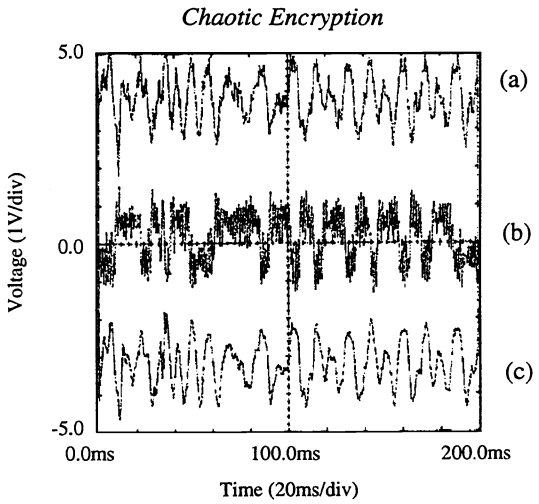

Fig. 8: Audio Data Transmission.

5. REFERENCES

1. M. J. Ogorzalek: "Taming Chaos--Part I: Synchronization". *IEEE Transactions on Circuits and Systems* - I: *Fundamental*

Theory and Applications, Vol.40, No.10, pp. 693-699, Oct. 1993.

2. M. Hasler: "Synchronization Principles and Applications". *Proc. of the Int. Symp. on Circuit and Systems*, Tutorial 6.2, pp. 314-327, 1994.

3. K.S. Halle, C.W. Wu, M. Itoh, L.O. Chua: "Spread Spectrum Communication through Modulation of Chaos". *Int. J. Bifurcation and Chaos*, Vol.3, No.2, pp. 469-477, 1993.

4. F. Krummenacher and N. Joehl: "A 4MHz CMOS Continuous-Time Filter with On-Chip Automatic Tuning". *IEEE J. Solid-State Circuits* SC-23, pp. 750-758, Jun. 1988.

5. M. Delgado-Restituto and A. Rodríguez-Vázquez: "Switched-Current Chaotic Neurons". *Electronics Letters*, Vol.30, No.5, pp. 429-430, Mar. 1994.