References

1 NOBLES, P., ASHWORTH, D., and HALSHALL, F.: 'Indoor radiowave propagation measurements at frequencies up to 20GHz'. IEEE Vehicular Technology Conf. Proc., 1994, **2**, pp. 873–877

2 DAVIES, R., BEACH, M.A., and MCGEEHAN, J.P.: 'Wireless propagation measurements in indoor multipath environments at 1.7GHz and 60 GHz for small cell systems'. IEEE Vehicular Technology Conf. Proc., May 1991, pp. 589–593

3 RAPPAPORT, T.S., and HAWBAKER, D.A.: 'Effects of circular and linear polarized antennas on wideband propagation parameters in indoor radio channels'. IEEE GLOBECOM'91 Proc., 1991, pp. 1287–1291

4 HIPERLAN, ETSI RES-10

5 WONG, M.T., and LAW, C.L.: 'Wideband impulse response of indoor channel at 2GHz using directive patch antennae'. IEEE SICON/ICIE '95 Proc., July 1995, pp. 532–536

CMOS 2.4μm chaotic oscillator: experimental verification of chaotic encryption of audio

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

Indexing terms: Chaos, Oscillators, Audio signals

The Letter reports the first experimental verification of chaotic encryption of audio using custom monolithic chaotic oscillators. We use G_m–C techniques to realise a chaotic modulator/demodulator 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. Measurements demonstrate how to exploit the synchronisation between two of these ICs for encrypted transmission.

Introduction: Different studies have shown that chaotic synchronisation can be used for data encryption [1]. 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 synchronisation property to recover the data. Fig. 1 shows a block diagram for the realisation 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, indecipherable. However, this transmitted signal still contains the information related to $s(t)$, which can be recovered at the receiver side by using a demodulator unit which synchronises to the modulation used in the transmitter.

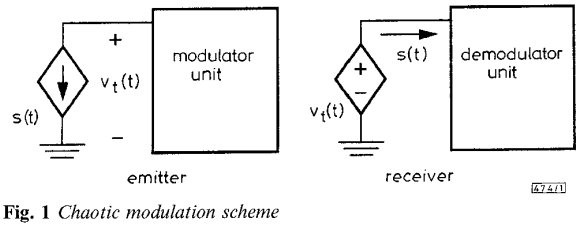

Fig. 1 *Chaotic modulation scheme*

An interesting feature of chaotic encryption is the simplicity of the required hardware. It opens new vistas for innovative application of analogue integrated circuits, based on nonlinear signal processing concepts. However, proper design of this kind of circuit involves a strict compromise between the robustness against parameter variations of the chaotic synchronisation, needed to decode the encrypted signal, and the security of the communication. Although some groups have realised chaotic encryption using discrete circuits, the above difficulties have precluded their realisation using monolithic units. This Letter reports the first experimental verification of continuous-time chaotic encryption of audio signals using a dedicated monolithic chaotic modulator/demodulator unit.

Circuit behaviour and diagram: The modulator/demodulator unit is represented by a third order nonlinear state equation,

$$\frac{d}{dt}\mathbf{x}(t) = \mathbf{A}\mathbf{x}(t) + \mathbf{B}f[\mathbf{D}^T\mathbf{x}(t)] \qquad (1)$$

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

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

Data encryption can be realised using many different sets of parameter values. The issue is to identify those which are the best suited for monolithic implementation. It involves searching in the parameter space to find the optimum values owing to considerations on mismatching, loading, etc. This, together with the use of on-chip tuning, can provide accuracies of ~1–2% in the pole frequency — enough to guarantee synchronisation. With these targets in mind we have done an exhaustive search in the parameter space of eqn. 1, to determine the optimum configuration. This obtains:

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

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

$$(\alpha, \beta, \gamma, s_0, s_1) = (3, 4, 1, 1, -2) \qquad (4)$$

Monte Carlo analysis with uncorrelated relative variations of up to 7% from the nominal values in eqn. 4 show that 100% of the obtained trajectories evolve towards a chaotic attractor — required for chaotic encryption.

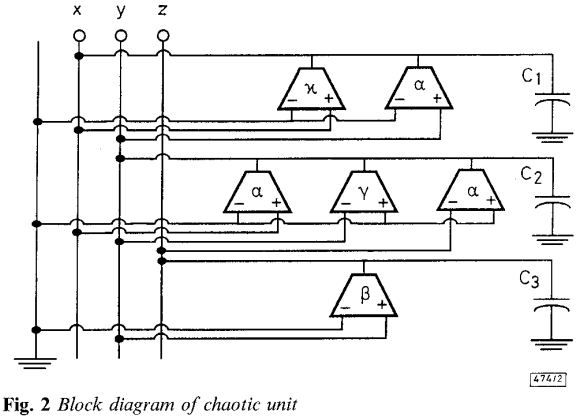

Fig. 2 *Block diagram of chaotic unit*

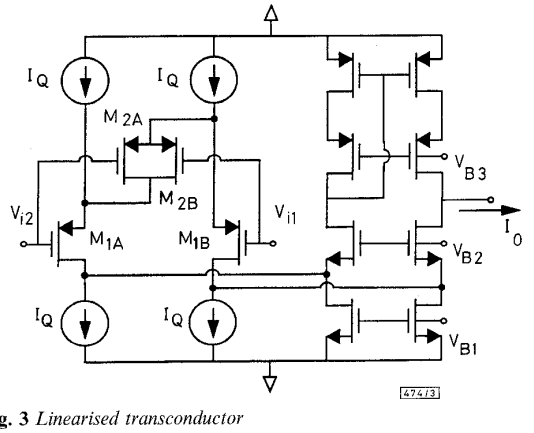

Fig. 3 *Linearised transconductor*

Fig. 2 shows a block diagram to realise eqn. 3 using G_m–C techniques. This includes quasi-linear and piecewise-linear transconductors. Fig. 3 shows the schematics used for the linear, which includes a source-degeneration scheme for linearisation [4]. Fig. 4 shows the circuit used for the PWL function consisting of a front-

end transconductor and a nonlinear circuit that operates in the current domain based on the high-accurate rectification mechanism proposed by the authors in [5]. All parameters in these nonlinear characteristics have been made electrically controllable to serve as a cryptographic key in the audio transmission scheme.

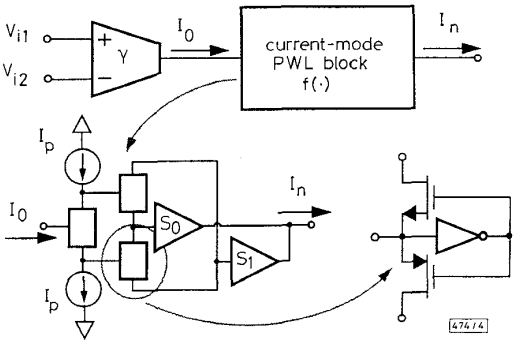

Fig. 4 *PWL function circuit*

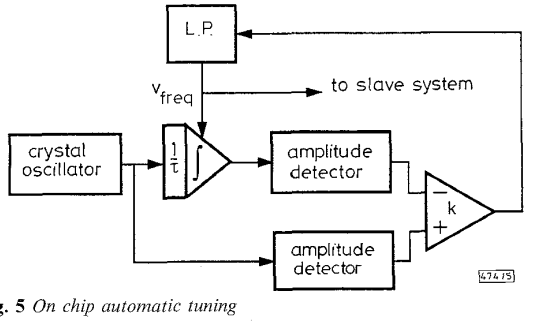

Fig. 5 *On chip automatic tuning*

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.

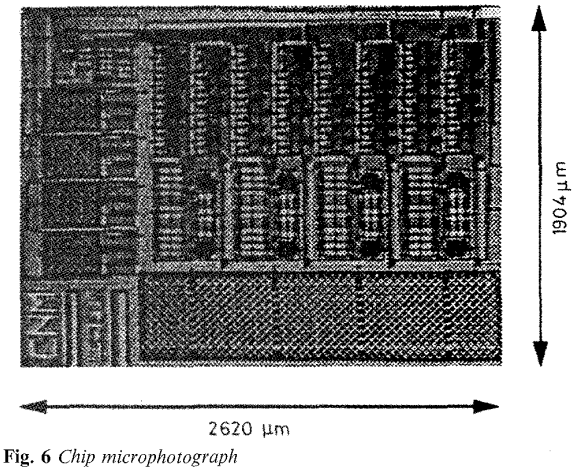

Fig. 6 *Chip microphotograph*

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 2.4µm double-poly double-metal CMOS technology) have also been indicated in Fig. 6. Power dissipation is <1.8mW for a symmetrical biasing of ±2.5V. 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, creating attractors. The fabricated prototype is able to reproduce the whole bifurcation sequence leading to these attractors.

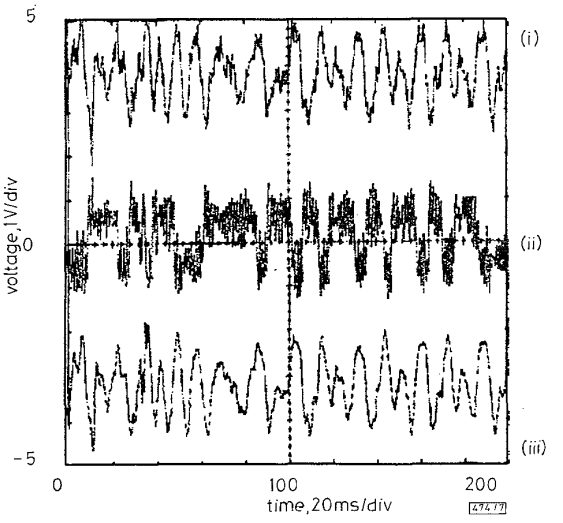

Fig. 7 *Audio data transmission*

Fig. 7 illustrates the performance of the whole audio encryption scheme. Input signal (Fig. 7(i)) consists of a segment of speech. The worst-case signal/noise ratio of the recovered signal (Fig. 7(ii)) is >+40dB (this occurs at very low frequencies) with <–0.2dB loss of the input signal power. At higher frequencies, the signal/noise ratio rises to +60dB while retaining similar losses at the receiver. As can be seen from Fig. 7, the transmitted signal (Fig. 7(iii)) keeps no resemblance to the information content.

22 February 1996
Electronics Letters Online No: 19960552

M. Delgado-Restituto, M. Liñán and A. Rodríguez-Vázquez (*Department of Analog and Mixed-Signal Circuit Design, Centro Nacional de Microelectrónica - Universidad de Sevilla, Edificio CICA, C/Tarfia s/n, 41012 Sevilla, Spain*)

References

1 OGORZALEK, M.J.: 'Taming chaos – Part I: Synchronization', *IEEE Trans, Circuits Syst. I: Fundam. Theory Appl.*, 1993, **40**, (10), pp. 693–699
2 HASLER, M.: 'Synchronization principles and applications'. Proc. Int. Symp. on Circuit and Systems, 1994, Tutorial 6.2, pp. 314–327
3 HALLE, K.S., WU, C.W., ITOH, M., and CHUA, L.O.: 'Spread spectrum communication through modulation of chaos', *Int. J. Bifurcation Chaos*, 1993, **3**, (2), pp. 469–477
4 KRUMMENACHER, F., and JOEHL, N.: 'A 4MHz CMOS continuous-time filter with on-chip automatic tuning', *IEEE J. Solid-State Circuits*, 1988, **SC-23**, pp. 750–758
5 DELGADO-RESTITUTO, M., and RODRÍGUEZ-VÁZQUEZ, A.: 'Switched-current chaotic neurons', *Electron. Lett.*, 1994, **30**, pp. 429–430

Current monitoring technique for testing embedded analogue functions in mixed signal ICs

M. Robson and G. Russell

Indexing terms: Mixed analogue-digital integrated circuits, Built-in self-test

The authors demonstrate how *M*-sequences and current monitoring can be combined to produce a system level technique for testing analogue circuits, much of the test hardware being obtained from reconfigured digital system hardware.

Theory: The *M*-sequence test method is derived from the impulse response technique used in control theory (Towill [1]), in which a