Secure Communication through Switched-Current Chaotic Circuits

Manuel Delgado-Restituto, Rafael López de Ahumada and Angel Rodríguez-Vázquez

Departament of Analog Design

Centro Nacional de Microelectronica, c/Tarfia sn, 41012-Sevilla, Spain

ABSTRACT

This paper presents the use of analog integrated circuits for secure communication based on chaos synchronization. The phenomenon is demonstrated through experimental measurements realized on silicon prototypes in a double-metal, single-poly 1.6μm CMOS technology. The circuits operate in current-mode domain and were designed following switched-current circuit techniques. The proposed circuit can be reduced to the interconnection of elementary units similar to that encountered in the emulation through artificial neural networks of chaotic phenomena observed in nerve tissues.

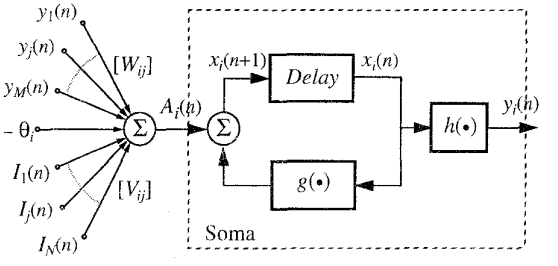

Fig. 1 Analog computer concept for the chaotic neuron circuit.

INTRODUCTION

Secure communication refers to the encryption of signals to be transmitted through a communication channel, such that the signal information content cannot be deciphered by intruders. Recent studies suggest that secure communication can be realized by exploiting the *synchronization* properties of coupled chaotic oscillators [1], [2]. Different practical schemes have been reported based on either nonlinear differential equations [2][3][4] or nonlinear difference equations [5], and demonstrated through experimental prototypes built using discrete components [2][3][4][6].

This paper reports the first experimental verification of secure communication using *monolithic* chaotic oscillators. It is based on the synchronization between two sets of nonlinear finite difference equations, implemented using analog sampled-data current-mode techniques based on current mirrors. It enables fabrication of the prototypes in conventional VLSI technologies, requiring no specialized primitive components.

A remarkable feature of the proposed circuits is that they can be reduced to the interconnection of *elementary* processing units, whose responses emulate the chaotic responses observed in some simple living beings. It follows the proposal of a chaotic artificial neuron model made by Aihara, Takabe and Toyoda [7] based on the observation of chaos and phase-locking in normal squid axons [8], which open new vistas in the comprehension of living neurons [9], and support important engineering applications to solve difficult optimization problems [10] and for dynamical associative memories [11]. In this sense, the experimental verification of secure communication herein presented contributes to enrich these vistas, while its practical realisation through monolithic circuits serves as motivation to further explore their practical usage in future advanced information processing engines.

THE ELEMENTARY PROCESSING UNIT

The proposed secure communication scheme is based on the interconnection of processing units described by the chaotic artificial neuron model of Aihara, Takabe and Toyoda. Fig. 1 shows its schematic, defined by the following finite-difference equations:

$$\begin{aligned} x_i(n+1) &= g(x_i(n)) + A_i(n) \\ y_i(n+1) &= h(x_i(n+1)) \end{aligned} \quad , \; n = 0, 1, \ldots \tag{1}$$

where $x_i(n+1)$ and $y_i(n+1)$ are the internal state and output of the ith chaotic neuron at the discrete time $n+1$, respectively; and $A_i(n)$ is the input excitation at the instant n, given by

$$A_i(n) = \sum_{j=1}^{M} W_{ij} y_j(n) + \sum_{j=1}^{N} V_{ij} I_j(n) - \theta_i \tag{2}$$

where the first term computes the influence of the M neurons driving the ith neuron; the second, the excitation from the N external input, I_j; and θ_i is the threshold of the ith neuron.

The activation function of the neuron, $g(\bullet)$, exhibits an N-shaped characteristics that can be modelled as,

$$g(x) = kx - \alpha f(x) \tag{3}$$

where α and k are the scaling and damping factors of refractoriness (residual effect of a neuron once fired), respectively; and $f(\bullet)$ is a hard sigmoid,

0-7803-2570-2/95 $4.00 ©1995 IEEE

$$f(x) = \frac{|x+\varepsilon| - |x-\varepsilon|}{2\varepsilon} \tag{4}$$

with ε, a positive number defining the steepness of the function.

With regards to the output function, $h(\bullet)$, even though it is made to coincide with $f(\bullet)$ in the original model, for our purposes, it represents the identity function.

CMOS Implementation of the Processing Unit

Fig. 2 shows the conceptual schematic for a switched-current implementation of the processing unit. Summation is easily realized exploiting KCL. The delay operation can be realized as a cascade of two track-and-hold switched-current stages, as proposed by Hughes et al. [12]. The nonlinear activation function has been achieved using a novel, highly accurate CMOS circuit strategy to realize piecewise-linear characteristics in current-mode domain. It is based on the rectifying characteristics of the current switch [13], which provides very high resolution and virtually zero current offset, uninfluenced by transistor mismatches (indeed, minimum size transistors were used in the prototype). The current switches, together with the current sources, are used to discriminate the input current into three paths depending on whether $x(n)$ is lower than -ε, greater than ε, or comprised between both values. In the two first cases, the paths are routed to the same node and amplified by k, while if $x(n) \in [-\varepsilon, \varepsilon]$ the current is amplified by $-\delta$, where $\delta = \alpha/\varepsilon - k$, according to (3) and (4). Current amplifiers can be implemented by properly ratioed bilateral current mirrors. Finally, if $h(\bullet)$ is assumed to be the identity function, the output of the neuron is easily obtained by replicating the output of the delay stage.

SECURE COMMUNICATION SCHEME

Fig.3 shows the block diagram of the secure communication system based on chaotic neurons. The transmitter is described by the following discrete-time dynamics,

$$\begin{aligned} x_1(n+1) &= f(x_1(n)) + \gamma s(n) + \theta_C \\ x_2(n+1) &= g(x_2(n)) - \alpha x_3(n) + x_1(n+1) + \theta_M \\ x_3(n+1) &= x_2(n) - \beta x_3(n) \end{aligned} \tag{5}$$

where α and β are scaling factors. Note that the transmitting system encompasses two major steps [6]. First, the neuron labeled soma 1 in Fig. 3, is driven by the information bearing signal $s(n)$ to generate the state variable $x_1(n)$. The nonlinear characteristics of such neuron has been vertically shifted by θ_C to ensure chaotic behavior. This process is called *chaotic coding*. For correct coding, the amplitude of the incoming signal to the neuron must be low enough, so that $x_1(n)$ bears no resemblance to $s(n)$. Next, the coded signal, $x_1(n+1)$, is taken as the input for a set of two coupled finite-difference equations. One equation results from a second chaotic neuron with threshold θ_M (soma 2 in Fig. 3), involving the state variable $x_2(n)$. The other equation is linear and comes from the subsystem formed by a delay stage with state variable $x_3(n)$ and a linear amplifier with gain $-\beta$. Both subsystems generate the transmitting signal, $x_2(n+1)$, to be sent through the channel. This process constitutes the *chaotic modulation*.

The equations involved in the receiving system are

$$\begin{aligned} x_4(n+1) &= x_2(n+1) - g(x_2(n)) + \alpha x_5(n) - \theta_M \\ x_5(n+1) &= x_2(n) - \beta x_5(n) \\ r(n) &= (x_4(n+1) - f(x_4(n)) - \theta_C)/\gamma \end{aligned} \tag{6}$$

and can be considered as the reverse of those in the transmitter, sequentially comprising a demodulation and decoding process. Obviously, the success in recovering the information signal depends on the ability to synchronize the state variables $x_5(n)$ and $x_3(n)$, in the receiver and transmitter, respectively. It has been shown that this is possible whenever the conditional Lyapunov exponents of the subsystem $x_3(n)$ are all negatives, assuming close matching between the corresponding parameters at both sites of the secure communication scheme [5]. In our case, this condition is equivalent to the requirement that $|\beta| < 1$, what implies that the recovered signal $r(n)$ tends to $s(n)$ for large n [6]. This last observation imposes that the maximum frequency component of the information signal $s(n)$ must be much lower than the sampling frequency of the system, so that convergence occurs in spite of different initial conditions.

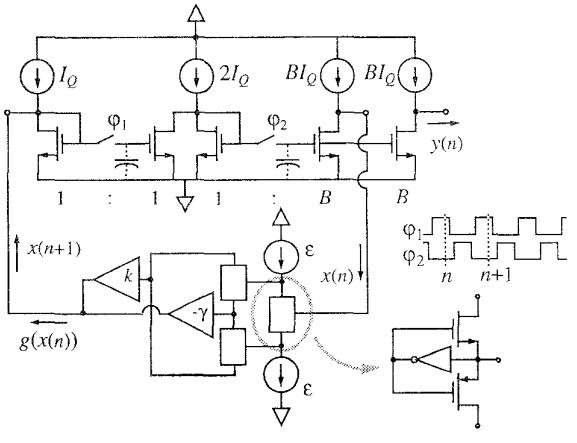

Fig. 2 Schematics of the switched-current chaotic neuron.

EXPERIMENTAL RESULTS

The chaotic neuron of Fig. 2 has been fabricated in a double-metal, single-poly 1.6μm CMOS technology. Fig. 4 shows the corresponding microphotograph. Some extra miscellaneous circuitry has been added to both circuits to enable testing the output current and to either open or close the feedback loop. Dummy switches were also added to reduce the influence of clock feedthrough. All current amplifiers were binary-weighted for programmability. Bias current I_Q for the delay stages was set to 50μA. The total area occupation is 0.225mm^2.

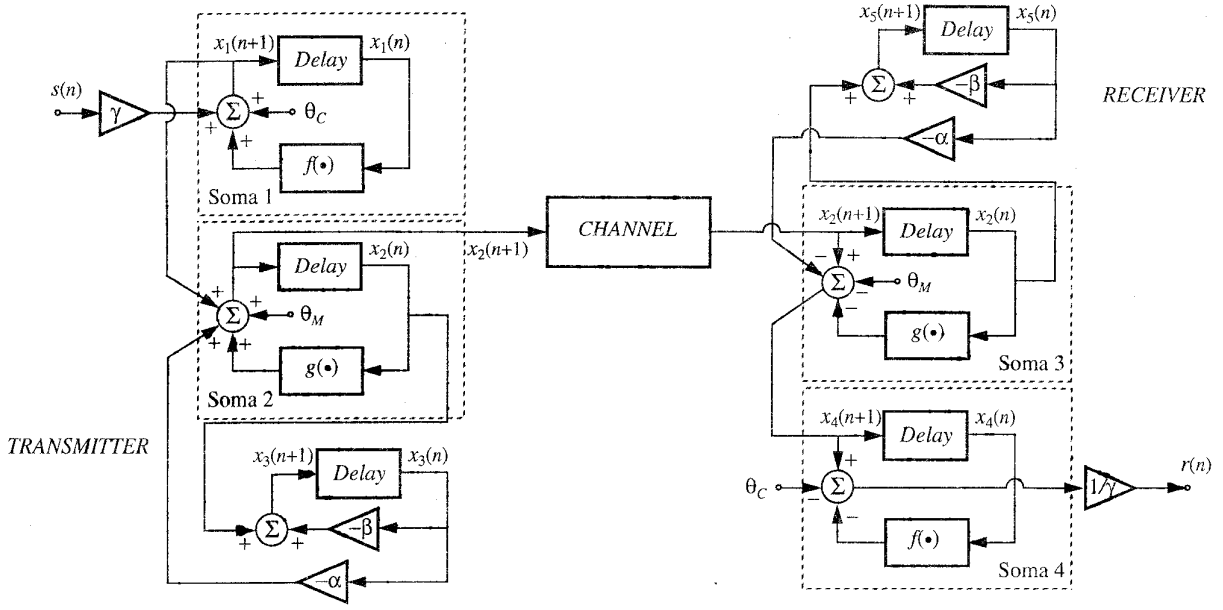

Fig. 3 Block diagram of the secure communication system.

Fig. 5 shows the experimental bifurcation tree of the neuron for $k = 0.75$, $\varepsilon = 1.4\mu A$ and $\delta = 10$ and taking neuron excitation A as the bifurcation parameter. Fig. 5 also shows the simulated bifurcation diagram corresponding to the same set of parameter values. Full accordance between experimental and theoretical results is clear.

We transmitted a sine wave of 150mv p-p and 1kHz to test the secure communication system. Clock frequency was 50kHz. Scaling factors were set to α=0.1 and β=0.2 through off-the-chip current amplifiers. All the nonlinearities in Fig. 3 were identical, with parameters $\varepsilon = 2.0\mu A$, $\delta = 10$ and k slightly less than 1.0. The threshold values were $\theta_C = 12\mu A$ and $\theta_M = -8\mu A$, which ensured chaotic behavior in all the neurons. Fig. 6 shows both the waveforms and the spectra for the signals, $s(n)$, $x_2(n+1)$ and $r(n)$. Note that the system can recover the transmitted tone with more than 25dB SNR, with only -0.43dB loss of the input signal power, in spite of the noise-like apperance of the transmitted signal. Also, we have determined experimentally that only 1% variation in a single slope of one neuron's activation function, results in a complete loss of the information signal is completely loss, thus confirming the security of the system.

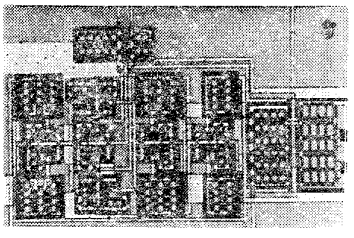

Fig. 4 Microphotograph of the prototype.

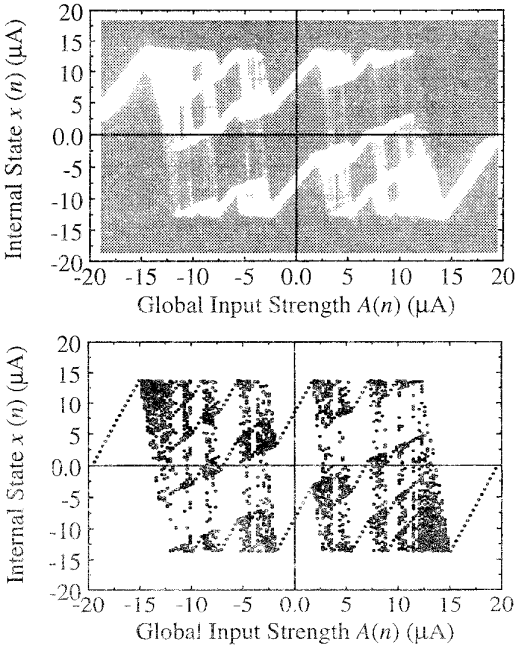

Fig. 5 Experimental versus simulated bifurcation diagram for the chaotic neuron.

RERERENCES

[1] M. Hasler: "Synchronization Principles and Applications". *Tutorial 6.2 in the Proc. of the Int. Symp. on Circuits and Systems*, pp. 314-327, 1994.

[2] A. V. Oppenheim, G. W. Wornell, S. H. Isabelle and K. M. Cuomo: "Signal Processing in the Context of Chaotic Signals". *Proc. of the* 1992 *IEEE Int. Conf. on Acoustics, Speech and Signal Processing* IV, pp. 117-120, Mar. 1992.

[3] 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. on Circuits and Systems* II, Vol.40, pp. 634-642, Oct. 1993.

[4] T. Carroll and L. M. Pecora: "Synchronizing Chaotic Signals". *IEEE Trans. on Circuits and Systems* Vol. CAS-38, pp. 453-456, Apr. 1991.

[5] M. Itoh and H. Murakami: "Chaos Synchronization in Discrete-Time Dynamical Systems and Secure Communications". *Proc. of the European Conf. on Circuit Theory and Design*, pp. 611-614, 1993.

[6] M. Itoh, H. Murakami and L. O. Chua: "Performance of Yamakawa's Chaotic Chips and Chua's Circuits for Secure Communications". *Proc. of the Int. Symp. on Circuits and Systems*, pp. 105-108, 1994.

[7] K. Aihara, T. Takabe and M. Toyoda: "Chaotic Neural Networks". *Phys. Lett. A*, Vol. 144, pp. 333-340, Mar. 1990.

[8] G. Matsumoto, K. Aihara, Y. Hanyu, N. Takahashi, S. Yoshizawa and J. Nagumo: "Chaos and Phase Locking in Normal Squid Axons". *Physics Letters A*, Vol. 123 pp. 162-166, Aug. 1987.

[9] C.A. Skarda and W.J. Freeman: "How Brains make chaos in order to make sense of the world". *Brain and Behavioral Science*, Vol. 10, pp. 161-195, 1987.

[10] T. Yamada, K. Aihara and M. Kotani: "Chaotic Neural Networks and the Travelling Salesman Problem". *Int. Joint Conf. on Neural Networks*, Vol.II, pp. 1549-1552, 1993.

[11] M. Adachi, K. Aihara and M. Kotani: "Nonlinear Associative Dynamics in a Chaotic Neural Network". *Proc. of the 2nd International Conference on Fuzzy Logic & Neural Networks*, pp. 947-950, Jul. 1992.

[12] J. B. Hughes, I. C. Macbeth and D. M. Patullo: "Switched Currents Filters". *IEE Proceedings*, Vol. 137, Pt. G, No. 2, pp. 156-162, April 1990.

[13] A. Rodríguez-Vázquez, R. Domínguez-Castro, F. Medeiro and M. Delgado-Restituto: "High-Resolution CMOS Current Comparators: Design and Applications to Current-Mode Function Generation". *Analog Integrated Circuits and Signal Processing,* special issue on Current-Mode Circuits, 1995 (to appear).

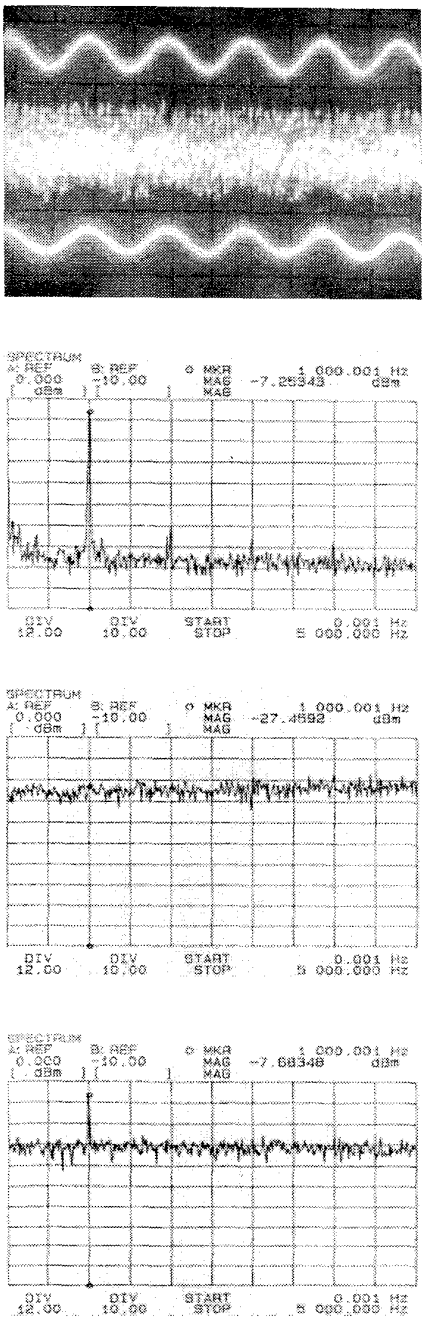

Fig. 6 Performance of the secure communication prototype. (a) From top to bottom, the waveforms represent the information, transmitted, and recovered signals (vertical scales: 300mv/div, 1v/div, 200mv/div); (b) (c) and (d) show their respective power density spectrums (vertical scale, 12dB/div).