Secure Communication through Switched-Current Chaotic Circuits

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

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 realization 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:

\[ x_i(n+1) = g(x_i(n)) + A_i(n) \]

\[ y_i(n+1) = h(x_i(n+1)) \]

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

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

where the first term computes the influence of the \( M \) neurons driving the \( i \)-th neuron, the second, the excitation from the \( N \) external input, \( I_j \); and \( \theta \) is the threshold of the \( i \)-th neuron.

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

\[ g(x) = k x - \alpha g(x) \]

where \( \alpha \) and \( k \) are the scaling and damping factors of refractoriness (residual effect of a neuron once fired), respectively, and \( g(x) \) is a hard sigmoid.
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 $-\epsilon$, greater than $\epsilon$, or comprised between both values. In the two first cases, the paths are routed to the same node and amplified by $k$, while if $x(n) \in [-\epsilon, \epsilon]$ the current is amplified by $-\delta$, where $\delta = \alpha/\epsilon - k$, according to (3) and (4). Current amplifiers can be implemented by properly ratioed bilateral current mirrors. Finally, if $h(*)$ 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,

$$
\begin{align*}
    x_1(n+1) &= f(x_1(n)) + y_0(n) + \theta_C \\
    x_2(n+1) &= g(x_2(n)) - \alpha x_3(n) + x_1(n+1) + \theta_M \\
    x_3(n+1) &= x_2(n) - \beta x_3(n)
\end{align*}
$$

(5)

where $\alpha$ and $\beta$ 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 $\theta_C$ 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 $\theta_M$ (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 $x_2(n)$ 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

$$
\begin{align*}
    x_1(n+1) &= x_2(n+1) - g(x_2(n)) + \alpha x_3(n) - \theta_M \\
    x_2(n+1) &= x_1(n) - \beta x_3(n) \\
    r(n) &= (x_2(n+1) - f(x_2(n)) - \theta_C) / \gamma
\end{align*}
$$

(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 $x_3(n)$ and $x_1(n)$ 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 $|\beta| < 1$, which 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.

EXPERIMENTAL RESULTS

The chaotic neuron of Fig. 2 has been fabricated in a double-metal, single-poly 1.6um 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 $I_B$ for the delay stages was set to 50µA. The total area occupation is 0.225mm².
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 \( \alpha = 0.1 \) and \( \beta = 0.2 \) 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 appearance 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.
REFERENCES


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).