APPLICATION OF PIECEWISE-LINEAR SWITCHED-CAPACITOR CIRCUITS FOR RANDOM NUMBER GENERATION

Servando Espejo-Meana, Juan D. Martín-Gómez, Angel Rodríguez-Vázquez and José L. Huertas

Departamento de Electrónica y Electromagnetismo, Universidad de Sevilla, 41012-Sevilla, SPAIN

Abstract

An unconventional application of switched-capacitor (SC) circuits is discussed in this communication. A systematic method is given for the design of piecewise-linear (PL) parasitic-insensitive SC chaotic discrete maps. A very simple circuit is reported which generates a random one-bit digital sequence. Simulation results show that the random behavior is not significatively altered by large (about 5%) variations in the values of the design parameters, which makes monolithic implementations feasible. Simulation results and layout for a 2µm double metal CMOS prototype are included.

Introduction

Continuous progress in integrated circuit technology makes it possible to design complete signal processing systems (analog plus digital) in a single chip. Switched-Capacitor (SC) circuits have been demonstrated to be very efficient for building these complex chips [1-3]. As a matter of fact, SC techniques have been successfully applied to the design of a lot of signal processing basic operators, either linear or nonlinear. In particular signal generation (sinusoidal, triangular, square ...) via SC circuits have attracted big attention in technical literature [4-6].

Previous work about SC signal generators has concentrated on *periodic* waveforms. However, in other contexts, it has been shown that very simple nonlinear SC circuits can exhibit very complicated chaotic behaviors [7]. It suggests the possibility of applying SC techniques for the generation of *aperiodic, ergodic* signals. Thus, on-chip *random number generation* would be possible with potential applications in SC-based instrumentation and communication chips.

In this paper we first present a systematic technique for the design of parasitic-insensitive SC chaotic generators based on piecewise-linear (PL) *discrete maps,*

$$x(n+1)=f[x(n)], \qquad n=0,1,2,3,... \tag{1}$$

f(•) being a PL function, and then give simulation results and layout for a SC random number generator IC prototype based on a two-pieces discontinuous PL map.

Design of Parasitics-insensitive PL discrete maps

Let us consider an interval $[E_o, E_N]$, a partition $\Delta=\{E_0, E_1, ...E_N\}$ and the following PL function,

$$f(x) = \begin{array}{ll} M_0x+P_0 & , E_0<x<E_1 \\ M_1x+P_1 & , E_1<x<E_2 \\ .... & .... \\ M_ix+P_i & , E_i<x<E_{i+1} \\ .... & .... \\ M_{N-1}x+P_{N-1} & , E_{N-1}<x<E_N \end{array} \tag{2}$$

A more compact expression for this function can be obtained by using what we call here the *regionalizer operator*, as follows,

$$f(x)= \sum_{i=0}^{N-1} rgn(x,E_i,E_{i+1})[M_ix+P_i] \tag{3a}$$

where we define,

$$rgn(x,A,B)= \begin{array}{ll} 1 & , A<x<B \\ 0 & , otherwise \end{array} \tag{3b}$$

Fig.1a shows a conceptual block diagram for a parasitic-insensitive SC implementation of eq.(3a). Each term in this equation contributes during the *n-th* odd clock phase a charge Δq_i^o to the negative input terminal of the opamp, thus giving,

$$v^o(n) = \sum_{i=0}^{N-1} \frac{\Delta q_i(n)}{C_u} \tag{4}$$

The implementation of the *i-th* charge component in Fig.1a can be made as is shown in Fig.1b, where we define,

$$W_{iR}^o \doteq \begin{array}{ll} 1_D & , E_i<x<E_{i+1} \\ 0_D & , otherwise \end{array} \tag{5}$$

and where 1_D and 0_D respectively denote the one and zero in the binary number system.

The clocking conditions for the input switches in Fig.1b have to be selected taking into account the signs of parameters M_i and P_i, respectively. For positive parameters the phases in parenthesis should be used, the other applying for negative ones.

By analyzing Fig.1b with (5) and using the correct clocking for the input switches, it can be concluded that

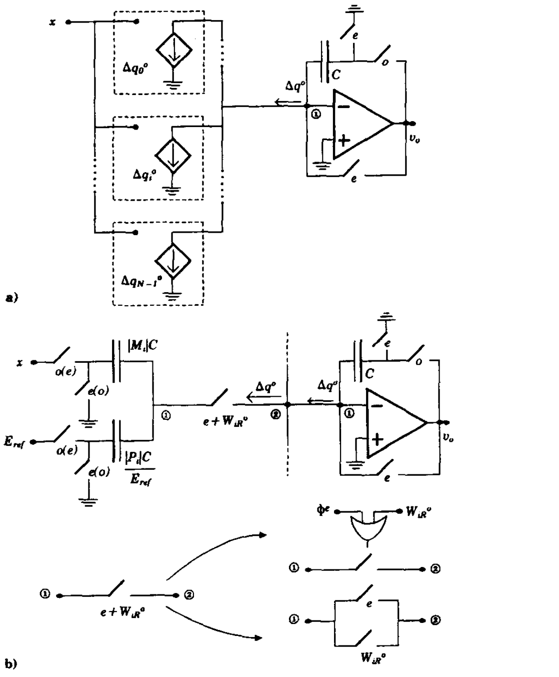

Figure 1

89CH2785-4/90/0000-0960$01.00 © 1990 IEEE

Fig.1a actually implements the PL transfer function characteristics, $v_0(n)=f(x)$, given in (3). Fig.2 shows the general circuit architecture of a SC PL function generator using the above methodology. The signals W_{iR}^{o} that control the transfer of charge to the virtual ground of the opamp can be implemented by using dynamic comparators as it is shown in Fig.3.

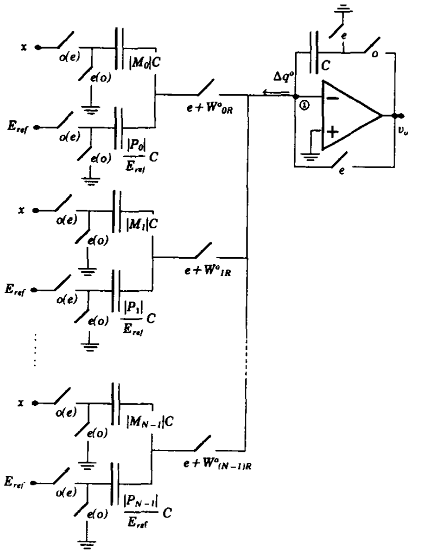

Figure 2

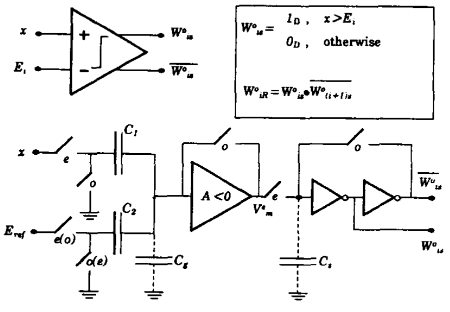

Figure 3

Simplifications in the SC PL generator

Fig.2 is a general scheme that can be simplified in case the PL function exhibits some kind of regularities. For instance, Fig.4a illustrates how to eliminate one capacitor and corresponding switches in case two slopes are equal, $M_k=M_l$. The case in which two ordinates at the origin are equal can be handled in a similar way. On the other hand, Fig.4b illustrates a simplification in the case of having two pieces with opposite slopes, $M_k=-M_l$.

A discontinuous PL map for random number generation

Fig.5 shows an SC circuit diagram for the following two pieces PL function,

$$f(x)=\begin{cases}-A+Bx & ,\ x>0\\ A+Bx & ,\ otherwise\end{cases}\qquad(6)$$

where different simplifications have been made according to the techniques in the above paragraph. In the next section this function is used as a basic building block for random number generation.

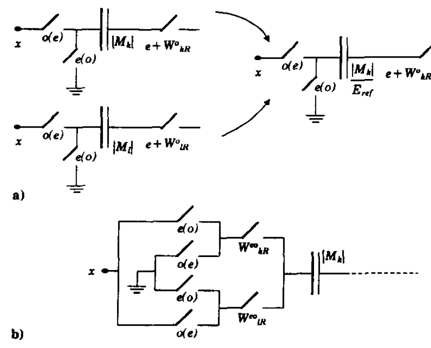

Figure 4

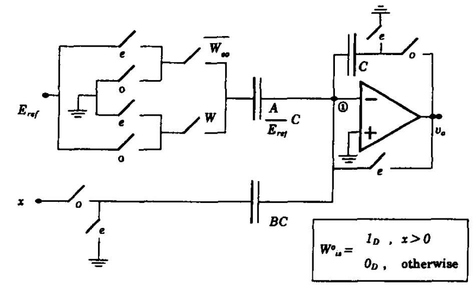

Figure 5

Architectures for PL discrete maps

Fig.6a shows the conceptual block diagram for a discrete map based on a parasitic-insensitive PL function generator. Since the output of the function generator is only valid during odd time instances, two half-a-period delay stages are required to guarantee proper timing of both positive and negative input signals of the generator. Fig.6b shows a parasitic-insentive implementation for the delay stages in Fig.6a [8].

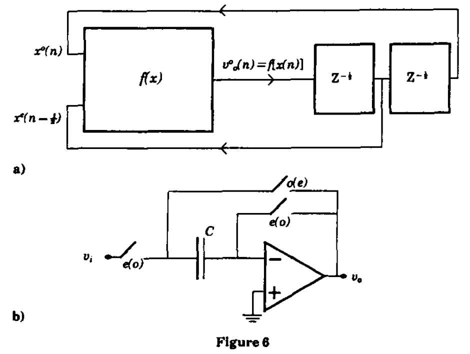

Figure 6

Fig.7 shows the concept for a random number generator based on a PL discrete map. The output signal $x(n)$ of the discrete map is compared with a reference level E, thus resulting in the following digital signal at the output of the comparator,

$$d(n)=\begin{cases}1_D & ,\ x(n)>E\\ 0_D & ,\ otherwise\end{cases}\qquad(7)$$

providing $x(n)$ is chaotic, this digital signal may be expected to exhibit random characteristics.

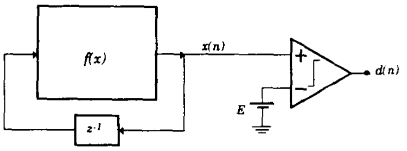

Figure 7

Design of a random number generator prototype

For the process of generation of $d(n)$ via Fig.7 to be a random process the following conditions must be fulfilled:

1. The underlying analog signal $x(n)$ has to be chaotic.
2. The process has to be ergodic (both regular and stationary).
3. Every possible result $\{d(n)=1$ and $d(n)=0\}$ must exhibit the same probability.
4. Probability of any result is not dependent on either past or future results.

Analysis of the discrete map of (6) shows that for $1<B<2$ the signal $x(n)$ cannot escape from the interval $[-A,\ A]$ also being chaotic in it. Furthermore, for $B>(\simeq 1.45)$, the full interval is visited in the time evolution of the signal. Values of B larger than 1.45 should then be used. Parameter A has to be chosen to prevent the SC circuit implementation of the map to be locked at parasitic stable points caused by the opamp voltage saturation characteristics. It is guaranteed by fulfilling the following conditions,

$$A<V_{dd}<\frac{A}{B-1} \tag{8}$$

$$\frac{A}{1-B}<V_{ss}<-A$$

where V_{DD} and V_{SS} are the positive and negative power supply voltages, respectively.

For a 5volts CMOS digital technology ($V_{DD}=2.5v$, $V_{SS}=-2.5v$) an appropriate choice owing to previous considerations should be $A=2.1v$, $B=1.76$. This guarantees that a discrete map implementation based on Fig.5 will, in response to the power-on transient, self-start to generate a chaotic signal $x(n)$ whose values are comprised in a interval $[-2.1v,\ 2.1v]$. Besides, they also guarantee that the sequence will return to this interval for any disturbance eventually driving $x(n)$ outside it.

Fig.8 shows the measured probability distribution and density functions for the map of (6) with $A=2.1v$ and $B=1.76$. As it can be seen, the probability density function is symmetrical around the point $x=0v$. It means that the subintervals $[-A,\ 0]$ and $[0,\ A]$ are equally probable. Hence, it is possible to design Fig.7 in such a way that every result exhibits the same probability. It can be achieved via the discrete map of (6) with $A=2.1v$, $B=1.76$ and $E=0v$.

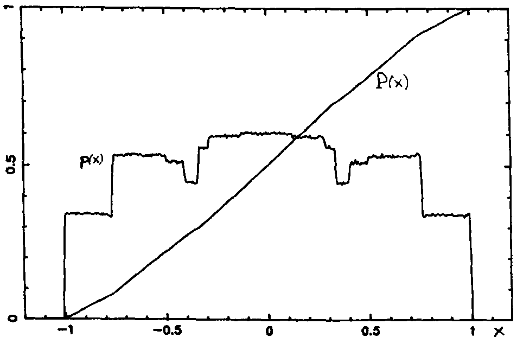

Figure 8

Fig.9 shows the circuit diagram of the herein proposed SC random number generator. The robustness of this circuits has been examined in detail by making a large number of simulations where A and B are randomly modified within typical tolerance margins around the nominal design values. The different simulations showed stationary, regular and ergodic behavior, thus demonstrating the viability of an IC prototype.

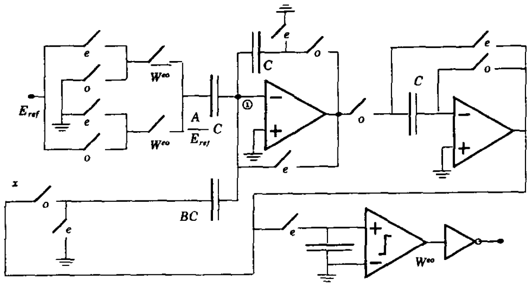

Figure 9

Fig.10 shows a layout of a 2µm CMOS monolithic prototype. Samples are now in progress. HSPICE device level simulations (including parasitics capacitors and resistors) have been performed demonstrating the correct operation of the proposed circuit. Typical process tolerances have been also considered in the simulations.

Conclusions

A systematic method is presented for the design of parasitic-insensitive SC PL function generators and chaotic discrete maps. A two-pieces PL map is reported leading to a probability density function that is symmetrical around the point $x=0$. Simulation results at the functional level demonstrate the feasibility of a SC random number generator based on this map. The corresponding random process exhibits regularity and stationarity properties, being also tolerant to typical deviations in the design parameters. Device level simulation results for a 2µm CMOS monolithic prototype are in accordance to both functional simulations and theoretical analysis.

References

[1] R. Gregorian and G.C. Temes: "*Analog MOS Integrated Circuits for Signal Processing*". John Wiley 1986.

[2] K. Nakayama and Y. Kuraishi: "Present and Future Applications of Switched-Capacitor Circuits". *IEEE Circuits and Devices Magazine*, Vol. 3, pp 10-21, Sept. 1987.

[3] Y. Solomon: "Switched-Capacitor Filters: Precise, Compact and inexpensive". *IEEE Spectrum*, Vol. 25, pp. 28-32, June 1988.

[4] B.J. Hosticka et al. "Design of Nonlinear Analog Switched-Capacitor Circuits using Building Blocks". *IEEE Trans. Circuits and Systems*, Vol. CAS-31, pp 354-368, Apr 1984.

[5] W.B. Mikhael and S. Tu: Continuous and Switched-Capacitor Multiphase Oscilators". *IEEE Trans. Circuits and Systems*, Vol. CAS-31, pp 280-293, March 1984.

[6] P.E. Fleischer et al.: "A Switched-Capacitor Oscilator with Precision Amplitude Control and Guaranteed Start-up". *IEEE J. Solid-State Circuits*, Vol. SC-20, pp 641-647, Apr 1985.

[7] A. Rodríguez-Vázquez et al. "Chaos from Switched-Capacitor Circuits: Discrete Maps". *Proceedings of the IEEE*, Vol. 75, pp 1090-1106, Aug. 1987.

[8] R. Gregorian: "High Resolution Switched-Capacitor D/A Converters". *Microelectronic Journal*. Vol. 12, pp. 10-13, 1981.

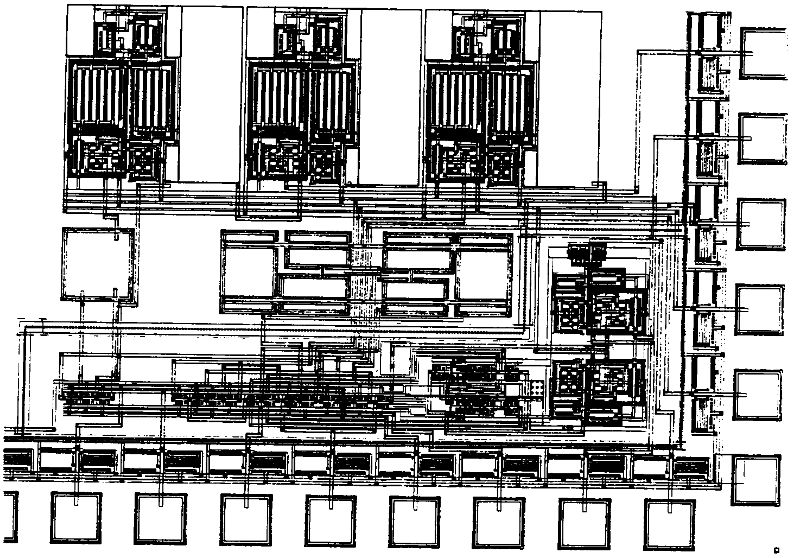

Figure 10