
©20xx IEEE. Personal use of this material is permitted. However, permission to reprint/republish this material for advertising or promotional purposes or for creating new collective works for resale or redistribution to servers or lists, or to reuse any copyrighted component of this work in other works must be obtained from the IEEE.
A Very Fast and Low-power Time-Discrete Spread-Spectrum Signal Generator

A. Cabrini, A. Carbonini, I. Galdi, F. Maloberti
Department of Electronics
University of Pavia
Via Ferrata 1, 27100, Pavia, Italy
[alessandro.cabrini, alessandro.carbonini, ivano.galdi, franco.maloberti]@unipv.it

Abstract— A non-linear circuit that obtains a logistic-like response with very low current levels suitable for generating of spread-spectrum signals is presented. This circuit obtains the non-linear transfer function by using only four cross-coupled transistors and may operate as a discrete-time spread-spectrum generator thus providing sequences of quasi-random numbers. The circuit was designed and simulated in 0.18-µm CMOS process and operates with nominal 1.2 V power supply. The power consumption of the non-linear block is about 80 µW with a data throughput of the output binary stream of 100 MB/s.

I. INTRODUCTION

Security issues are becoming even more widespread as an increasing number of embedded and distributed systems demand for safe and assured data transmission. Nowadays, security is crucial not only to high-end systems, such as firewalls, network routers, gateways, storage and web servers, but also to low-end systems such as wireless handsets, sensor networks, portable storage devices, and smartcards. In embedded systems the sophisticated methods of cryptography are needed for authentication, electronic certification, copyright protection, and information security [1].

Cryptography in embedded systems exploits random numbers in several ways [2], [3]. In general, the security provided by means of a deterministic algorithm is proportional to the complexity of the algorithm. Complex but deterministic encryption algorithms can be broken by means of massive network computing. On contrary, non-deterministic methods, where truly random numbers are generated from intrinsically random physical processes, provide the ultimate level of security. A possible implementation requires the use of a non-linear deterministic system, which allows the transition to chaotic (or quasi-random) evolution to be easily generated.

Typically, the realization of chaotic integrated circuits requires the integration of additional area and power hungry analog functions [4]. As a result, embedded cryptosystems designed under strict power and area constraints usually relies on relatively simple deterministic algorithms implemented with software routines, which are not adequate for high security applications.

In this work, we designed a fully-integrated non-linear circuit for the generation of chaotic signals by using a pseudo-quadratic map. The non-linear transfer function is implemented by means of only four cross-connected MOS transistors and a current source. Its use to generate discrete-time pseudo random sequences of numbers requires using a suitable sample and hold (S/H) circuit and a comparator. Simulation results showed the effectiveness of the proposed circuit as generator of deterministic chaos.

Figure 1: Implementation of a time-discrete chaotic generator with a non-linear transfer block and a suitable S/H.

The simulated power consumption of each four-transistors block is below 40 µW at 1.2 V power supply while the overall power consumption (including control and peripheral circuits) is approximately 80 µW. The estimated area occupation is few hundred of µm² for the four-transistors elementary cell and the associated circuitry. The sampling frequency of the system is as high as 100 MHz.
The paper is organized as follows. Next section describes the basic elementary cell conceived for generating the pseudo-logistic transfer function. In Section III the time-discrete generator is presented and, finally, Section IV shows simulation results that validate the effectiveness of the proposed solution.

II. NON LINEAR CELL

A method to obtain a time-discrete chaotic sequence of numbers foresees the use of a non-linear circuit (i.e. a circuit with a non-linear input/output transfer characteristic) which, for each time step $t_k$, is iteratively excited at the input node with the voltage provided at the output node at time $t_{k-1}$. The method is shown in Fig. 1 where the non-linear block $f(x)$ is feed back through a sample and hold which store the output of the system at time $t_k - 1$ and provide the input node, at time $t_{k+1}$, with the previously held signal. In general, the time evolution of the system is given by:

$$x_{k+1} = f(x_k) \quad (1)$$

where $x_k$ is the state of the system at time $t_k$ and $f(x_k)$ represents the so called ‘map’ of the system. Several maps are reported in literature [6] the most know being the ‘logistic’ map. When a logistic map is used, the evolution of the system can be defined as:

$$x_{k+1} = f(x_k) = r x_k (1 - x_k) \quad (2)$$

where $r$ is a positive real number which control the evolution of the system and the complexity of the output sequence.

A logistic-like transfer function often requires complicated circuits that use significant area and power consumption. This paper proposes the new scheme shown in Figure 2 that even if it uses few transistors achieves a high quality transfer function.

A. Circuit Operation

The non-linear transfer function $f(x)$ of the scheme of Fig. 2 requires using a differential input with a suitable common mode (in our case equal to $V_{DD}/2$). The cross-coupled control of the 4 transistors makes the structure symmetrical and, consequently even the response is symmetrical. For large signals one of the transistors of the series is off and the large signal resistance of the four elements is infinite. For small input signals the transistors are likely in the triode region and the four elements establish a given resistance. The non-linear cell is biased with a suitable current $I_{bias}$ to transform the resistance into a voltage $V_{OUT}$ at node OUT. The maximum output voltage $V_{OUT,max}$ is obtained with zero differential input signal $V_{IN+} - V_{IN-}$. In particular, assuming $V_{IN+} = V_{IN-} = V_{DD}/2$ and transistors $M_1$, $M_2$, $M_3$ and $M_4$ equally sized and working in their triode region, $V_{OUT,max}$ is given by:

$$V_{OUT,max} = V_{DD} - \frac{L I_{bias}}{\mu_p C_{ox} W \left( \frac{V_{DD}}{2} - V_{th,p} \right)} \quad (3)$$

where $L$ and $W$ are the transistor channel length and width, respectively, and $C_{ox}$ is the oxide capacitance while $\mu_p$ the carrier mobility. Analogously, the minimum output voltage $V_{OUT,min}$ (equal to 0 V) is obtained for a differential signal.
suitably referred to respectively. This way, the differential input signal must be equal to:
\[ V_{IN}^+ - V_{IN}^- = V_{DD} - 2V_{th, p} \]  
(4)

In particular, we can solve the system by considering the following relations:
\[ I_1 = k\left(V_{DD} - V_{IN}^+ - V_{th, p}\right)V_{DD} - V_1 \]
\[ I_1 = k\left(V_1 - V_{IN}^- - V_{th, p}\right)VOUT - V_1 \]
\[ I_2 = k\left(V_{DD} - V_{IN}^- - V_{th, p}\right)V_{DD} - V_2 \]
\[ I_2 = k\left(V_2 - V_{IN}^+ - V_{th, p}\right)VOUT - V_2 \]
\[ I_{bias} = I_1 + I_2 \]

where, as it can be seen from Fig. 2, \( I_1 \) and \( I_2 \) are the current of the two branches, \( V_1 \) and \( V_2 \) are the source voltages of \( M_1 \) and \( M_2 \), respectively and \( V_{th, p} \) is the transistor threshold voltage.

III. TIME-DISCRETE CHAOS GENERATOR

In order to use the proposed cell as time-discrete chaos generator we conceived the structure schematically depicted in Fig. 3a and 3b. At any time \( t_k \), the output voltage \( V_{OUT} \) of the non-linear cell is sampled through two suitable digital signals \( \Phi_1 \) and \( \Phi_2 \) operating at the frequency \( f_s \). The circuit operation is as follows. During the first operating phase (i.e., \( \Phi_1 \) high and \( \Phi_2 \) low), \( V_{OUT} \) is sampled on \( C_3 \) and \( C_4 \). The size of these capacitors is chosen in such a way that \( V_{OUT} \) is reduced by factor \( \gamma \). In second phase (i.e., \( \Phi_1 \) low and \( \Phi_2 \) high), top plate of \( C_1 \) is connected to the input and bottom plate of \( C_1 \) is connected to \( V_{ref} \) thus leading to an input voltage equal to \( V_{ref} + \gamma V_{OUT} \). Actually if we set \( V_{ref} \) to \( V_{ref, IN} \), we obtain the voltage \( V_{IN} \) given by (7). To notice that operation of \( C_1 \) and \( C_2 \) during the first phase (second phase) is the same as \( C_3 \) and \( C_4 \) during the second (first). This is required to properly drive the input node of the non-linear element during each time step \( t_k \). The operation of the inverting sampling channel used to provide \( V_{IN} \) is similar to the previous one except for the use of \( C_4 \) and \( C_2 \). The reference voltage \( V_{ref} \) is now set to \( V_{IN}^- \). On the other, the voltage drop across \( C_4 \) and \( C_2 \) is used differing from the case of sampling channel \( IN^- \). In fact, instead of connecting the top plate to the input node of non-linear cell, capacitor \( C_4 \) (\( C_2 \)) is now reversed thus leading to an output voltage equal to \( V_{IN}^- - \gamma V_{OUT} \).

\[
\gamma = \frac{V_{OUT}^+ - V_{OUT}^-}{V_{OUT}^M - V_{OUT}^m} 
\]
(6)

where \( V_{OUT}^m \) and \( V_{OUT}^M \) are the output voltage of the non-linear cell for a differential input signal equal to \( V_{ref, IN}^+ - V_{ref, IN}^- \) and \( 0 \) respectively. From above considerations it follows:
\[
\begin{align*}
V_{IN}^+(t_{k+1}) &= V_{ref, IN}^+ - \gamma V_{OUT}(t_k) \\
V_{IN}^-(t_{k+1}) &= V_{ref, IN}^- + \gamma V_{OUT}(t_k)
\end{align*}
\]
(7)

Which gives the relation that must be used to properly feedback the output voltage \( V_{OUT} \) to the input nodes \( IN^- \) and \( I \). Let us consider for example, the acquisition and generation of the input voltages \( V_{IN} \). To this end, we refers to the schematic given in Fig. 3b. The structure is controlled by means of two suitable digital signals \( \Phi_1 \) and \( \Phi_2 \) operating at the frequency \( f_s \).
digital domain by using a suitable analog-to-digital converter. In our case, to reduce power consumption, we used a simple comparator thus giving the required chaotic sequence of 0 and 1 at frequency equal to the sampling frequency $f_s$.

IV. SIMULATION RESULTS

The proposed solution has been designed and simulated in a 180 nm CMOS technology with a power supply $V_{DD}$ equal to 1.2 V. The non-linear cell has been designed having $M_1$, $M_2$, $M_3$ and $M_4$ equally sized with a biasing current of 30 $\mu$A.

The simulated transfer characteristic of non-linear cell is shown in Fig. 5 where, on the $x$-axis the time is reported since, the simulation was performed having as input signal $IN^+$ and $IN^-$ two square wave with rise and fall time, respectively, of 1 $\mu$s. The maximum of the input/output transfer characteristic was obtained for $IN^+ = IN^- = 600$ mV with an input voltage range ($V_{ref,IN^-} - V_{ref,IN^+}$) of about 350 mV. The maximum operating frequency of the non-linear (unloaded) cell was measured to be larger than 300 MHz.

Fig. 6 and Fig. 7 show, the spectrum and the autocorrelation function of the output signal. In this case we set $\gamma = 0.3$ $V_{ref,IN^-} = 450$ mV and $V_{ref,IN} = 750$ mV. The operating frequency $f_s$ of phases $\Phi_1$ and $\Phi_2$ was set equal to 100 MHz. Finally, in Fig. 8 the cumulative density function of $V_{OUT}$ is shown for two different output sequences of $10^5$ samples.

V. CONCLUSION

In this paper an integrated circuit for the generation of time-discrete chaotic signals has been presented. The main advantage of the proposed solution is based on the physical implementation of the non-linear cell. In fact, the transfer function is realized by only using four cross-coupled MOS transistors thus allowing power consumption and silicon area to be significantly reduced. The simulated power consumption of the non-linear cell is about 40 $\mu$W with a data throughput of the output binary stream of 100 MB/s. The proposed circuit provides a wide spectrum output signal with a power and area overhead smaller with respect to the implementation of simpler and less secure deterministic cryptography techniques.

VI. REFERENCES