Generation of True Random Numbers and Built-in-Self-Test of Mixed-Mode Analog Circuits: Is There Something in Common?

Gianluca Setti

Department of Engineering, University of Ferrara and Advanced Research Center on Electronics Systems, University of Bologna

Gianluca Setti received a Dr. Eng. degree (with honors) in Electronic Engineering and a Ph.D. degree in Electronic Engineering and Computer Science from the University of Bologna, Bologna in 1992 and in 1997, respectively, for his contribution to the study of neural networks and chaotic systems. From May 1994 to July 1995 he was with the Laboratory of Nonlinear Systems (LANOS) of the Swiss Federal Institute of Technology in Lausanne (EPFL) as visiting researcher. Since 1997 he has been with the School of Engineering at the University of Ferrara, Italy, where he is currently a Professor of Circuit Theory and Analog Electronics. He held several visiting position at Visiting Professor/Scientist at EPFL (2002, 2005), UCSD (2004), IBM T. J. Watson Laboratories (2004, 2007) and at the University of Washington in Seattle (2008, 2010) and is also a permanent faculty member of ARCES, University of Bologna. His research interests include nonlinear circuits, recurrent neural networks, implementation and application of chaotic circuits and systems, statistical signal processing, electromagnetic compatibility, wireless communications and sensor networks. Dr. Setti received the 1998 Caianiello prize for the best Italian Ph.D. thesis on Neural Networks and he is co-recipient of the 2004 IEEE CAS Society Darlington Award, as well as of the best paper award at ECCTD2005 and the best student paper award at EMCZurich2005. He served as an Associate Editor for the IEEE Transactions on Circuits and Systems - Part I (1999-2002 and 2002-2004) and for the IEEE Transactions on Circuits and Systems - Part II (2004-2007), the Deputy-Editor-in-Chief, for the IEEE Circuits and Systems Magazine (2004-2007) and as the Editor-in-Chief for the IEEE Transactions on Circuits and Systems - Part II (2006-2007) and of the IEEE Transactions on Circuits and Systems - Part I (2008-2009). He was the 2004 Chair of the Technical Committee on Nonlinear Circuits and Systems of the of the IEEE CAS Society, a Distinguished Lecturer (2004-2005), a member of the Board of Governors (2005-2008), and served as the 2010 President of the same society. Dr. Setti was also the Technical Program Co-Chair of NDES2000 (Catania) the Track Chair for Nonlinear Circuits and Systems of ISCAS2004 (Vancouver), the Special Sessions Co-Chair of ISCAS2005 (Kobe) and ISCAS2006 (Kos), the Technical Program Co-Chair of ISCAS2007 (New Orleans) and ISCAS2008 (Seattle), as well as the General Co-Chair of NOLTA2006 (Bologna). He is co-editor of the book Chaotic Electronics in Telecommunications (CRC Press, Boca Raton, 2000), Circuits and Systems for Future Generation of Wireless Communications (Springer, 2009) and Design and Analysis of Biomolecular Circuits (Springer, 2011), as well as one of the guest editors of the May 2002 special issue of the IEEE Proceedings on “Applications of Non-linear Dynamics to Electronic and Information Engineering”. He is a Fellow of the IEEE.

Abstract

During the last decade it has been widely highlighted that discrete-time chaotic dynamics can be thoroughly tackled by exploiting a statistical approach [1]-[5]. In this case, in fact, critical dependence on initial condition, probably the widest known feature of chaotic behavior, prevents the study of single trajectories from giving information which are globally valid. On the contrary,
a highly regular behaviour exists for the distribution of the points describing the evolution of a set of trajectories at each iteration step. This has been formalized by introducing a theoretical framework that is based on the classical Perron-Frobenius Operator (PFO) [1], which accounts for the evolution of the probability densities describing the distribution of the system state variable at each iteration step. Furthermore, by focusing on a particularly class of maps, namely Piecewise Affine Markov (PWAM) maps, and by specializing the set of theoretical tools for their study [3]-[4], one may show how such maps can be considered as easily implementable, stochastic processes generators with tunable statistical features.

Such a well-developed theoretical framework has been applied to obtain important improvements in several areas of ICT. These range from DS-CDMA in AWGN channels [6]-[13], tackling the problem of performance improvements for spreading sequences acquisition [14]-[17] and in presence of multipath [21]-[21], or including the effect of real pulses for information bearing waveforms [22]-[26], to UWB [27] and advanced CDMA communication [28], to coding theory [29] and electromagnetic interference reduction [30]-[35].

We will here show how such a well-developed set of theoretical tools allow to devise methodology, based on nonlinear dynamics, for implementing True Random Number Generators (TRNG) which closes the gap with the throughputs and the easiness of implementation of pseudo-RNGs [36]-[44]. More specifically, we will first prove that nonlinear maps exist that behave as TRNGs in an ideal setting and that robustly maintain such property with respect to implementation errors, and, furthermore, that such maps can be practically realized out of pipeline analog-to-digital converters (ADC) parts which are now ubiquitous in any mixed mode systems. With this, one can devise an architecture such as the one shown in Figure 1 to easily reuse design expertise and even analog Intellectual-Property (IP) blocks to quickly embed true random sources in SOCs and specialized apparatuses.

A chaos-based TRNG based on this approach has been implemented in 0.35um and 0.18um CMOS technology. Experimental results showed that the designed nonlinear-dynamics-based TRNGs:

- operate at a throughput of approximately 10Mbits/s, i.e. faster than current state-of-the-art TRNG [38],[42];
- in presence of implementation errors, behave in a completely satisfactory way when validated against two standard randomness test suites proposed by NIST (FIPS 140.2 and SP800-22) and it is therefore perfectly suitable for cryptographic applications [39],[42];
- are robust with respect to tampering attacks [41].

Interesting enough, by reversing the approach used to devise the chaos-based TRNG architecture, one can arrive to a very promising new technique for testing analog and mixed-mode integrated circuits, called Complex Oscillation Based Test (COBT). This methodology allows to overcome the limitations Oscillation Based Testing (OBT) which relies on forcing the circuits under test into some periodic (self)oscillatory mode whose amplitude and frequency allows to infer if the behavior of the circuit itself is correct: its advantage is the absence of external components in the validation phase,
given that the (self)oscillations can be obtained as simply as placing into a feedback loop the circuit under test, while its main disadvantage is that the plain measurement of frequency deviations with respect to nominal values can offer coverage of only a limited amount of faults.

The key idea is that the OBT procedure can be improved by substituting a wide band behavior (chaotic oscillation) for the periodic one. This offers many potential advantages given that:

- a wide band signals enables a more comprehensive test with regards to the operating characteristics to be tested
- a chaotic system can show great sensitivity to parameter variation, a feature that can represent a great advantage in testing since it enables even small fault to have very evident consequences.
- parametric testing is allowed since one may link the statistical properties of the generated chaotic signals to the parameters of the circuits under test.

We will show that this completely new approach allows very common analog circuit blocks such as switched capacitor filters [46]-[48] or ADC converters [45] to be easily tested. In fact, for instance for the latter case, a simple feedback connection including a complementary DAC conversion and a few simple additional components, as in Fig. 2, can turn the converter into a chaotic system based on a piecewise affine Markov map, for which a complete statistical characterization of the generated processes is possible.

![Figure 2: Scheme for testing an ADC using COBT.](image)

References


