True Random Number Generation Based on Double-Scroll Chaotic System

Selcuk Kilinc , Serdar Ozoguz, Koray Ozdemir

Faculty of Electrical and Electronics Eng'g
Istanbul Technical University, 34469
Istanbul, Turkey

***Abstract* – A new random number generator design from a double-scroll chaos is presented. The structure is based on the well-known oscillator sampling technique where the chaotic signal is employed as the entropy source. The proposed random number generator is realized in the laboratory and the generated bits are subjected to standard random number tests. Using full NIST-800-22 test suite, it is shown that the generated binary sequences have good statistical properties.**

INTRODUCTION

True random number generators (RNGs) have been widely employed in cryptographic systems or spread spectrum applications to generate unpredictable bit streams. According to [1], IC RNG designs reported in the literature are basically grouped into three main categories: i) direct amplification of a noise generated from a noise source [2], [3] ii) using dual oscillator structure which relies on sampling of a high frequency oscillator with a jittered low frequency oscillator [4], [5] iii) using discrete-time chaotic maps such as Bernoulli shift which is known to generate uniformly distributed numbers [6]. According to the first and second approaches, physical noise sources such as thermal or shot noise are employed, while the third approach exploits deterministic chaos as the entropy source in RNG. However, in integrated circuit environment, physical noises are generally corrupted and poorly uncorrelated signals, since the noise are often masked by deterministic disturbances such as substrate noise and power supply noise. Moreover, the amplitudes of physical noises are too small, and they need to be amplified with a large amplification factor over a wide range of frequencies before to be used in any RNGs. This entails the use of a costly well-designed high-gain electronic amplifier that is expected to function through a wide-bandwidth. This fact limits the speed of these RNGs. All these concerns may favor the use of chaos in the implementation of robust IC RNG. A perfect review of the above mentioned methods can be found in [1].

On the other hand, recent works give promising results on the implementation of RNGs using continuous-time chaotic oscillators [7, 8]. In [7], an RNG design using a double-scroll chaotic attractor is presented which is based on partitioning the state-space of the double-scroll attractor into three non-overlapping subspaces whose boundaries are determined by two thresholds. The evaluation of this RNG performance using standard random number tests revealed that the performance of the RNG is very sensitive to the values of the thresholds. Also, this circuit generates highly biased output streams, thus requires a post-processing block which eliminates the bias in the output bits. For this purpose, the authors propose to use of Von Neumann's post-processing technique [9] which considerably limits the RNG throughput.

In [8], a chaos based RNG architecture inspired from the classical dual oscillator architecture, is presented [10, 11]. In this structure, unlike the classical approach where the jittered low frequency oscillation is generated from a noise driven voltage controlled oscillator (VCO), the jittered low frequency oscillations are obtained from the output of a chaos driven VCO. Although the performance of this RNG is justified by standard random number tests, the resulting circuit has usually more complicated structure than classical noise-based dual oscillator architecture, due to the complicated structure of the involved chaotic circuit and the VCO.

In this paper, in order to simplify circuit implementation of the structure in [8], we propose a new RNG where the use of VCO is not required. Moreover, unlike to the circuit in [7], our technique does not require post-processing; hence the RNG throughput is much higher.

In order to verify the feasibility of the RNG, the whole system is built using discrete components. The generated random numbers has passed all the tests in the NIST-800-22 test suite.

DOUBLE-SCROLL CHAOTIC ATTRACTOR SYSTEM

Let us consider the following chaotic system proposed in [12]:

$$\dot{x} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -a & -a & -a \end{bmatrix} x + \begin{bmatrix} 0 \\ 0 \\ a \end{bmatrix} f(x_1), \quad f(x_1) = \begin{cases} 1 & x_1 \geq 0 \\ -1 & x_1 \geq 0 \end{cases} \quad (1)$$

Numerical analysis of the system showed that this model exhibits a double-scroll chaotic attractor for $a \in (0.5, 1)$.

Fig. 1 shows one possible circuit realization of the model in (1). The core of the circuit is implemented using current-feedback operational amplifiers (CFOAs). For $R_1=R_2=aR_3=R$, $C_1=C_2=C_3=C$, and using the normalized quantities $t_n=t/RC$, $x_1=I_{R1}$, $x_2=I_{C1}$, $x_3=I_{C3}$, it can be verified that the circuit realizes system equations in (1).

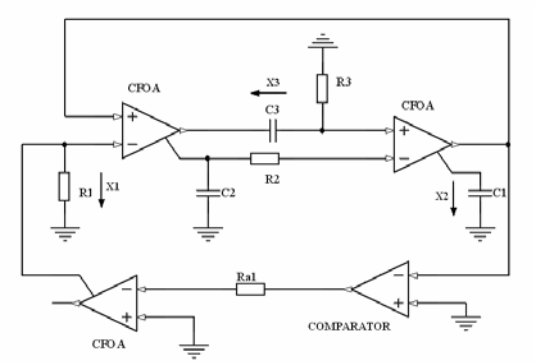

Fig. 1. A circuit realization of the chaotic system.

The circuit in Fig. 1 is verified experimentally using the commercial CFOA, Analog Devices' AD844, supplied under ±5V and LM311 type comparators. The passive component values have been chosen as $R_1=R_2=1k\Omega$, $R_3=1.9k\Omega$ (corresponding to $a=0.53$), $R_{a1}=15k\Omega$, $C_1=C_2=C_3=1nF$. The observed projection of the double-scroll chaotic attractor shown in Fig. 2 verifies the feasibility of the circuit.

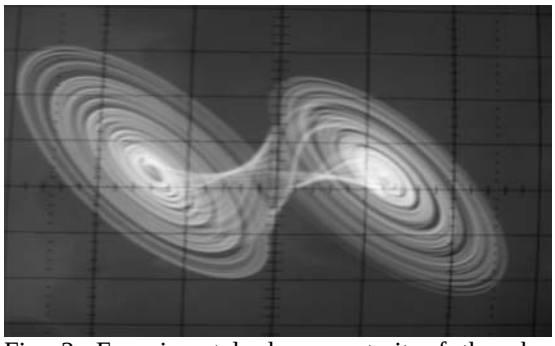

Fig. 2. Experimental phase portrait of the chaotic system.

RANDOM NUMBER GENERATION

Let us consider the well-known structure in Fig. 3, which employs oscillator sampling technique that makes use of oscillator phase noise to produce randomness [1]. In this design, the output of a fast oscillator is sampled on the rising edge of a jittered slower oscillator using a D flip-flop. The main limitation of this technique is that typical levels of the slow oscillator jitter are not sufficient to produce statistical randomness. The usual way to tackle this limitation is using a VCO driven by physical noise [10]. In this section, we experimentally show that continuous-time chaos can also be used to improve the level of slow oscillator jitter.

For this purpose, the jittered slow oscillator is realized using the structure in Fig. 4. In this circuit, the mean frequency of the jittered oscillator is determined by the frequency of the triangle-wave signal whereas the level of jitter is determined by the chaotic signal. Since the levels of chaotic signal is very large compared to the typical noise levels obtained from any physical noise source, it is not necessary to employ an amplifier or a VCO to

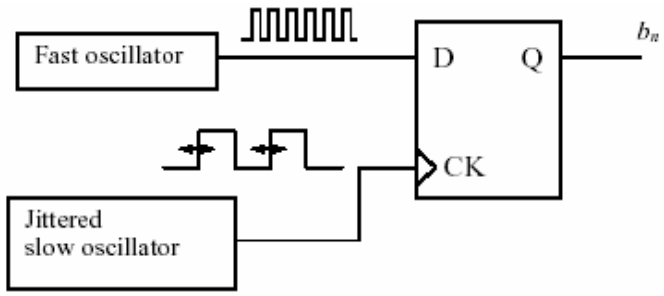

Fig. 3. Conventional RNG architecture based on oscillator sampling method.

increase the levels of jitter in Fig. 4 as in the RNG architectures in [10, 11].

On the other hand, it is obvious that chaotic signals are usually unevenly distributed and slightly correlated signals, unlike physical noise. However, the results of the standard random number tests presented in the sequel show that the effects of all these imperfections are compensated thanks to the mixing operation which exists inherently in the oscillator sampling technique.

In order to asses the quality of the RNG depicted in Figs. 3 and 4, this circuit is built using discrete components. The double-scroll chaotic system shown in Fig. 1 is employed as the entropy source of the RNG. The amplitude of the triangle-wave signal is chosen equal to the peak value of the chaotic signal. The frequency of the fast oscillator is kept at 100 kHz, while that of the triangle-wave signal is chosen as 1.5 kHz. Note that this latter frequency determines the RNG throughput. Experimental results indicated that when the frequency of the triangle-wave signal is increased larger than 1.5KHz, output bit streams fails in random number tests. For this setting, experimental waveform of the jittered oscillation is shown in Fig. 5. Mean value of the period of the slow oscillation is measured as 647.4μs whereas its standard deviation is 176.3μs.

The RNG system is also implemented on the computer to make numerical simulation. The aim for this is to find the proper value for the parameter a that gives a high-quality set of random numbers. For this purpose, the system is simulated with different a values and the corresponding outputs of the poker test which takes part in FIPS–140–1 test suite [13] are examined.

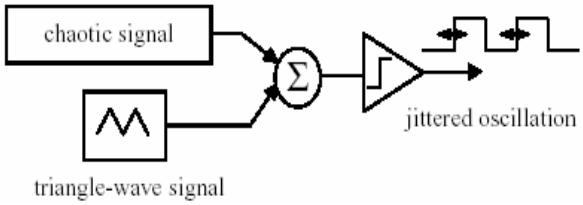

Fig. 4. Realization of the jittered slow oscillator in Fig. 3.

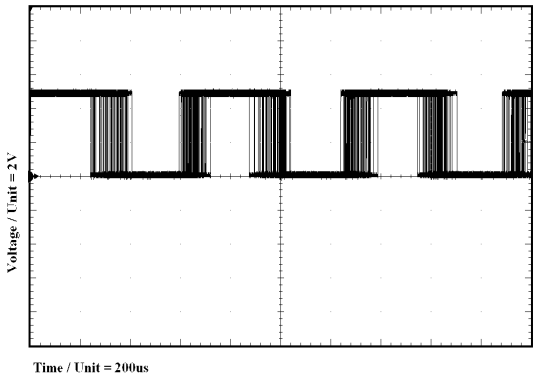

Fig. 5. Experimental waveform of jittered oscillation.

The output of poker test p, is a standard χ-squared test on the distribution of 20,000 bits examined in four-bit groups. The output of the test is found according to $p = \frac{2^4}{k}\left(\sum_{i=1}^{16} n_i^{\,2}\right) - k$ where test n_i, ($0 \le i \le 2^4$) is the number of occurrences of the ith bit-group. Unless the value of p satisfies $2.16<p<46.17$, the produced bit sequence can not be evaluated as random.

Fig. 6 shows the results of the above described procedure when the parameter a of the involved chaotic oscillator is varied from 0.5 to 1. From this graph, it can be deduced that for a is between 0.5 and 0.8, the RNG outputs fullfill poker test. On the other hand, an interesting property of the chaotic system is that maximum Lyapunov exponent is almost linearly dependent to a. This fact can also be seen from Fig. 6 where maximum Lyapunov exponent is calculated from the numerical solution of (1) and plotted against a. Therefore, the results depicted in Fig. 6 indicate that the performance of the proposed RNG is not sensitive to the Lyapunov exponent, hence to the quality of the involved chaotic oscillator. This fact shows the robustness of the proposed RNG.

For comparison purpose, the RNG system in [7] is also implemented on the computer. In the numerical simulation of this system, one of the threshold values are kept at -1 (c_1=-1) as in [7], while the other one (c_2) is varied between -0.1 and -2.2. The variation of poker test result with c_2 is given in Fig. 7. As it is seen from the figure, the output bitstreams fulfill poker test in a very narrow range of parameter c_2 which strongly depends on the parameter a, hence to the lyapunov exponent of the involved chaotic oscillator. It should be noted that this is a very strict condition that it may cause the RNG to fail very easily when an unwanted small variation or shift in the value of a and c_2 occurs. Moreover, as it is stated earlier, the system in [7] requires de-skewing (Von Neumann technique) [9] as a post-processing block. The proposed RNG and the RNGs in [7] are simulated numerically for the duration of 10,000 normalised unit time. During this period, the proposed RNG produces 701 binary numbers, whereas the one in [7] generates 64 bits. This means our RNG, which employs the same

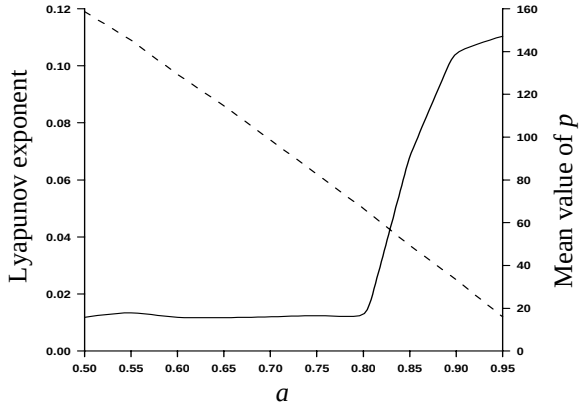

Fig. 6. Results of the numerical simulation.

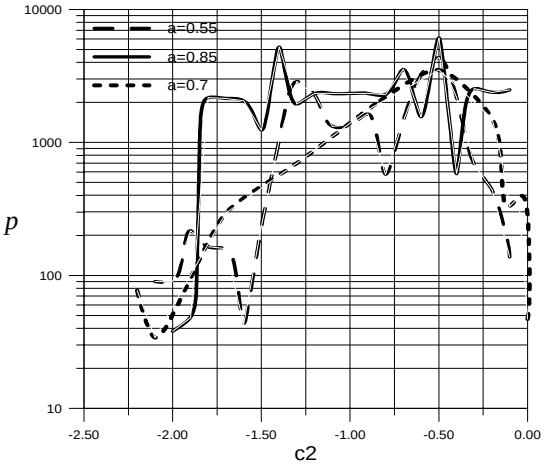

Fig. 7. Variation of poker test result with c_2 for the RNG method in [7].

chaotic system in [7], is about eleven times faster than the other one.

The candidate random numbers generated by the RNG described in Figs. 3 and 4 are uploaded to the computer using a data-acquisition card and are examined using the full random number test suites of NIST documented in NIST-800-22 [14]. A bit sequence of 70 million was acquired to the computer. The data was grouped into 700 blocks, each having a length of 100,000 bits and subjected to the full NIST test suite. For this data, the results of the NIST random number tests are tabulated in Table 1. The name of the test is given in the first column. One test is applied to each of the 700 blocks and for each test, 700 p-values corresponding to these blocks are obtained.

The data pass the test if i) an acceptable proportion of the p-values is larger than 0.01, ii) the distribution of the p-values is close to the uniform distribution. The proportion of the number of blocks, whose p-values are larger than 0.01, is reported in the last column. The value given in the second column of Table 1 corresponds to the goodness-of-fit of the distribution of p-values to uniform distribution. It should be also noted that the nonperiodic-templates, random-excursions and random-excursions (variant) tests are actually a series of 176 tests. For these three tests, we have given only the results with minimum

TABLE 1 Typical results of the NIST test suite.

Statistical test	Uniformity of the p-values	Proportion of passing blocks
Block-frequency	0.004581	0.9800
Linear-complexity	0.176657	0.9862
Runs	0.853761	0.9843
Fft	0.020724	0.9862
Apen	0.005193	0.9829
Serial	0.739918	0.9871
Serial	0.138408	0.9971
Cumulative-sums	0.839261	0.9957
Cumulative-sums	0.690492	0.9986
Longest-run	0.009535	0.9814
Frequency	0.453247	0.9957
Rank	0.364541	0.9929
Universal	0.061841	0.9875
Overlapping-templates	0.002700	0.9786
Nonperiodic-templates	0.030515	0.9757

pass rates. From the results given in Table 1, it can be deduced that the prototype RNG showed no significant signs of nonrandom behavior [14].

CONCLUSION

We present a continuous-time chaotic oscillator based RNG. A simple double-scroll attractor system is chosen as the entropy source because of its simplicity. The chaotic signal, after summed with triangle-wave, is used to produce the jittered slow oscillation in the dual-oscillator based RNG. The presented approach eliminates the necessity of any wide bandwidth amplifier and VCO. The RNG presented in this work does not require post-processing and is found to be about eleven times faster than the RNG in [7]. The randomness quality of the RNG is verified using full NIST800-22 test suite.

Acknowledgement: This work is granted by The Scientific and Technical Research Council of Turkey (TUBITAK) under the project 106E093.

REFERENCES

[1] C.S. Petrie, J.A. Connelly, "A noise-based IC random number generator for applications in cryptography", *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications*, vol. 47, no. 5, pp. 615-621, May 2000.

[2] W. T. Holman, J. A. Connelly, and A. Dowlatabadi, "An integrated analog/digital random noise source," *IEEE Trans. Circuits Syst. I*, vol. 44, June 1997.

[3] W. T. Penzhorn, "The design of a truly random monolithic noise generator," *Microelectron. J.*, vol. 15, no. 4, pp. 29–40, 1984.

[4] L. Letham, D. Hoff, and A. Folmsbee, "A 128K EPROM using encryption of pseudorandom numbers to enable read Access," *IEEE J. Solid-State Circuits*, vol. 21, pp. 881–889, Oct. 1986.

[5] R. C. Fairfield, R. L. Mortenson, and K. B. Coulthart, "An LSI random number generator," in *Proc. CRYPTO'84*, 1984, pp. 203–230.

[6] M. Delgado-Restituto, F. Medeiro, and A. Rodriguez-Vazquez, "Nonlinear switched-current CMOS IC for random signal generation," *Electron. Lett.*, vol. 29, no. 25, pp. 2190–2191, Dec. 9, 1993.

[7] M.E. Yalçın, J.A.K. Suykens, J. Vandewalle, "True random bit generation from a double scroll attractor", *IEEE Trans. Circ. Syst. I*, vol. 51, no.7, pp.1395-404, July 2004.

[8] S. Ergün, S. Özoğuz, "Truly random number generators based on a non-autonomous chaotic oscillator", *Int. J Electron. Commun. (AEÜ)*, vol. 61, no. 4, pp. 235-242, April 2007.

[9] J. Von Neumann, "Various techniques used in connection with random digits", *Applied Math Series, G. E. Forsythe, Ed. Boulder, CO: National Bureau of Standards*, 1951, vol. 12, pp. 36–38.

[10] B. Jun, P. Kocher, "The Intel random number generator", *white paper prepared for Intel Corporation, Cryptography Research Inc.*, April 1999 http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf.

[11] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, M. Varanonuovo, "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC", *IEEE Trans. Comp.*, vol. 52, no. 4, pp. 403-409, April 2003.

[12] A.S. Elwakil, K.N. Salama, M.P. Kennedy, "A system for chaos generation and its implementation in monolithic form", *IEEE Int. Symp. Circ. Syst. (ISCAS)*, vol. 5, pp. 217-220, May 2000.

[13] Federal Information Processing Standards Publication, "Security Requirements For Cryptographic Modules", FIPS PUB 140-1, 1994 January 11. http://csrc.nist.gov/publications/fips/fips1401.htm.

[14] National Institute of Standard and Technology, "A statistical test suite for random and pseudo random number generators for cryptographic applications", NIST–800–22, May 2001. http://csrc.nist.gov/publications/nistpubs/800-22/sp-800-22-051501.pdf.