MODELING AND ANALYSIS OF CHAOS-MODULATED DUAL OSCILLATOR-BASED RANDOM NUMBER GENERATORS

Salih Ergün

TÜBİTAK-National Research Institute of Electronics and Cryptology
PO Box 74, 41470, Gebze, Kocaeli, Turkey
phone: + (90) 262 6481370, fax: + (90) 262 6481100, email: salih@uekae.tubitak.gov.tr
web: www.uekae.tubitak.gov.tr

ABSTRACT

This paper introduces a numerical model for the simulation of chaos-modulated dual oscillator-based random number generators. Random number generation method based on dual oscillator architecture is described. Developed model allows the estimation of the output entropy and bias as a function of design parameters, thus provides determination of these parameters for a continuous-time chaotic source appropriately. Numerical simulations are performed in order to address important design issues and simulation results, verifying the feasibility and the correct operation of the model, are presented. High-performance random number generators can be realized in the light of the numerical model.

1. INTRODUCTION

Nowadays, because of the increasing demand of electronic official and financial transactions, the need for information secrecy has raised. Therefore, random number generators (RNGs) which have been used for only military cryptographic applications in the past got expanding usage for a typical digital communication equipment.

Almost all cryptographic systems require unpredictable values, therefore RNG is a fundamental component for cryptographic mechanisms. Generation of public/private key-pairs for asymmetric algorithms and keys for symmetric and hybrid crypto systems require random numbers. The one-time pad, challenges, nonces, padding bytes and blinding values are created by using truly random number generators (TRNGs) [1]. Pseudo-random number generators (PRNGs) generate bits in a deterministic manner. In order that pseudo-random sequences appear to be generated by a TRNG, PRNGs must be seeded by a shorter truly random sequence [2]. Random numbers are also used during the authentication procedure between two crypto equipments and initial value randomization of a crypto module that realizes an algorithm.

Even if TRNG design is known, any useful prediction about the output can not be made. To fulfill the requirements for secrecy of one-time pad, key generation and any other cryptographic applications, the TRNG must satisfy the following properties: The output bit stream of the TRNG must pass all the statistical tests of randomness; the next random bit must be unpredictable; the same output bit stream of the TRNG must not be able to reproduced [3]. The best way to generate truly random numbers is to exploit the natural randomness of the real world by finding a random event that happens regularly [3]. Examples of such usable event include elapsed time during radioactive decay, thermal and shot noise, oscillator jitter and the amount of charge of a semiconductor capacitor [2].

There are few integrated circuit (IC) TRNG designs reported in the literature; however fundamentally four different techniques were mentioned for generating random numbers: amplification of a noise source [4, 5] dual oscillator architecture [1, 6, 7], discrete-time chaotic maps [8, 9, 10] and continuous-time chaotic oscillators [11, 12]. In spite of the fact that, the use of discrete-time chaotic maps in the realization of TRNG is well-known for some time, it was only recently shown that continuous-time chaotic oscillators can be used to realize TRNGs also. Following up in this direction, we investigated the usefulness of the developed numerical model to analyze continuous-time chaos & dual oscillator based TRNG designs.

External interference is a major concern in TRNG design since interfered and random signals have comparable levels. To solve this problem in [7], a TRNG which mixes three of the four mentioned TRNG techniques except for the continuous-time chaos method was presented. Similar to this approach, a TRNG design which uses the dual oscillator architecture with continuous-time chaotic oscillator was proposed in [12]. In this design [12] random bit sequences were generated by sampling the output of a fast oscillator at the rising edges of a slower clock, frequency of which was modulated by a chaotic signal.

In [12], chaos-modulated dual oscillator architecture was not analyzed in detail. It was only experimentally verified that, proposed structure pass the statistical tests for randomness without any further post-processing for much higher throughput rates.

This paper introduces a numerical model for the simulation of chaos-modulated dual oscillator-based TRNGs and states important design issues. Developed model allows the estimation of the output entropy and bias as a function of the design parameters, thus provides determination of these parameters for a continuous-time chaotic source appropriately.

2. DUAL OSCILLATOR ARCHITECTURE

Dual oscillator architecture is a popular method used for deriving a random source. In this method, dual free-running oscillators one being fast and one being slower are used. There are TRNG studies in the literature indicating their investigation that typical levels of oscillator jitter are not nearly sufficient to produce statistical randomness [7].

Consequently, two processes have been adopted to further randomize the output of a classical dual oscillator based TRNG: Postprocessing techniques, compromising the unpredictability of the TRNG, are added [13] which will decrease the throughput; or a noise source is used to modulate the frequency of the slower clock [1, 14], where fast clock is sampled with the rising edge of noise-modulated slower clock. In this case, drift between the two clocks provides the source of random binary digits. Similar to amplification of a noise source technique, the noise must be amplified to a level where it can be used to modulate the frequency of the slower clock.

Throughput of the slower clock, which determines the throughput data rate of TRNG, is basically limited by the bandwidth of the noise signal used as the core of the TRNG, caused by the bandwidth of the amplifier. As a result of the limitation indicated above, highest speed TRNG based on classical dual oscillator architecture has been presented in [14] with throughput rate of $10Mbps$.

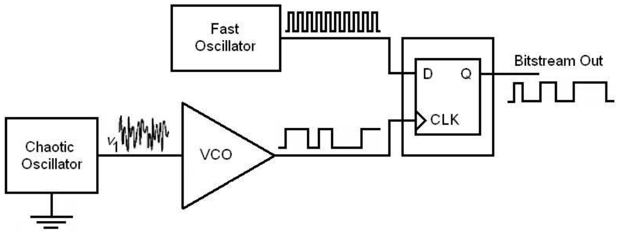

Figure 1: Chaos-modulated dual oscillator architecture.

Dual oscillator architecture was improved in [12], developing the idea to mix a few TRNG techniques and as a novelty including continuous time chaos method. In this new structure which is shown in Fig. 1, output of a fast oscillator is sampled on the rising edge of the chaos-modulated slower clock using a D flip-flop.

A voltage-controlled oscillator (VCO) is used to implement the modulation of the slower clock frequency with the chaotic oscillator output signal. Center frequency of the VCO determines the center frequency of the slower clock. Drift between the two oscillators provides random bit generation to be more robust. Because of the nonlinear aliasing phenomenon associated with sampling, the dual oscillator architecture achieves increased output throughput and higher statistical quality [7].

In the previous designs [12, 15, 16], chaotic signals were converted into binary sequences by using a comparator, which is basically analog to digital convertion in two bit quanta. However dual oscillator architecture provides most of the frequency components of input signal to affect the output. High deviation level achieved by chaos-modulated oscillator was reported in [12], where the measured minimum period and the maximum period feature a deviation much greater than the fast oscillator period thus provides uncorrelated random bit stream.

It was experimentally verified in [12] that, in order to remove the biasing of the output bit sequence, fast oscillator should have a balanced duty cycle. To get a satisfactory result, fast oscillator was implemented in [12] by dividing the frequency of a low jitter crystal oscillator by a certain number, which provides a fast oscillator with a duty cycle very close to 50%.

The slow and fast oscillators used in [1] and [14] have center frequency ratios in the order of 1 : 100. Similarly, experimental results were successful in [15], when the slower clock frequency is adjusted up to 170 KHz for a center frequency ratio of 1 : 111.

On the contrary to classical noise-based dual oscillator architecture, chaos-modulated dual oscillator architecture exploits the chaotic signal, which is in the order of a few volts with a center operation frequency (f_0) in the GHz range, without using any amplifier. In this architecture, f_0 basically determines the theoretical limit of the throughput rate (f_{rng}) which results in the order of a few ten times f_0. Such data rates, which are substantially higher than the throughput of TRNGs available on the market and in the literature, may render proposed TRNGs exploiting continuous-time chaos attractive when compared to their counterparts based on the other common techniques.

It should be noted that, doubts about the previous dual oscillator architectures concern the choice of design parameters. Their values depend on experimental data and this is a drawback of the previous designs. For the purpose of addressing this issue an effective model, which provides appropriately chosen design parameters, is developed in this paper.

3. MODELING OF DUAL OSCILLATOR ARCHITECTURE

Due to their extreme sensitivity to initial conditions, having a positive Lyapunov exponent and a noise-like power spectrum, which make them unpredictable [17], chaotic systems lend themselves to be exploited for random number generation.

In order to obtain random bit sequences from a continuous-time chaotic oscillator by using dual oscillator architecture, only one of the state variables of the chaotic system is exploited. This method relies on generating non-invertible data from the waveform of the chaotic oscillator and it should be noted that non-invertibility is a key feature for generating PRNGs [18]. Although n-dimensional trajectories in the state plane is invertible, one may obtain a non-invertible section by considering only the values corresponding to one of the states, say x.

Developed numerical model will allow the estimation of the output bit entropy and bias as a function of the design parameters, thus will adapt dual oscillator architecture for a continuous-time chaotic source by determining appropriate design parameters. For a constant VCO modulation signal x, the frequency of the slower clock f_{slow} can be calculated according to the following equation:

$$f_{slow} = f_{slow\ center}(K_1 + K_2 x + K_3 x^2) \qquad (1)$$

where $f_{slow\ center}$ is the center frequency of the slower clock, corresponding to VCO, determines the throughput data rate (f_{rng}). Herein, K_1, K_2 and K_3 are the model parameters which can be determined by applying a curve fitting method to approximate the nonlinear transfer function of the given VCO module. For $-x_{max} < x < x_{max}$, VCO converts the chaotic signal x via the nonlinear relationship into a frequency signal and the related period values, distributed about the mean period $1/f_{slow\ center}$.

If the fast and the slower clock frequencies are known as well as the starting phase difference ΔT, the output of the fast oscillator, sampled at the rising edge of the chaos-modulated slower clock, can be predicted as illustrated in Fig. 2. It can be shown that the binary data $S_{(dual\ oscillator)i}$ is the inverse of least significant bit of the ratio between the total periods of the slower clock and period of the fast clock:

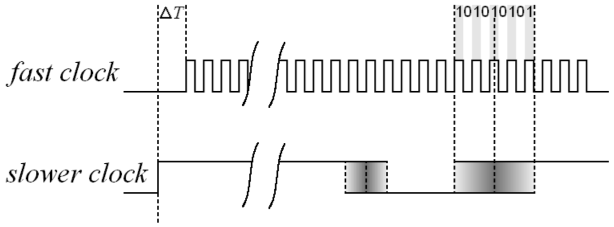

Figure 2: Fast and the slower clock output signals.

$$S_{(dual\ oscillator)i} = ((\lfloor \frac{(\sum_{j=1}^{i} T_{slow\ j}) - \Delta T}{T_{fast}/2} \rfloor mod 2)/(2d_{fast}))' \tag{2}$$

where $T_{fast} = \frac{1}{f_{fast}}$, f_{fast} and d_{fast} are the period, frequency and the duty cycle of the fast clock, respectively. In practice, center frequency of the slower clock is assigned at least a hundred times the center operation frequency of the chaotic oscillator (f_0). Hence, in T_{slow} time, x can be considered as a constant signal but in order to simulate the modulation of the VCO by a continuous-time chaotic signal more accurately, average of x is used instead of discrete time samples and the periods of the slower clock $T_{slow\ j}$ are obtained at times satisfying:

$$T_{slow\ j} = \frac{1}{f_{slow\ center}(K_1 + K_2 Avr(x) + K_3 (Avr(x))^2)} \tag{3}$$

where $Avr(x)$ is the average of x calculated from $t = t'$ to $t = t' + T_{slow\ j}$. We have numerically verified that, for high $\frac{f_{fast}}{f_{slow\ center}}$ ratios, the effect of ΔT becomes negligible and the mean value (m_{output}) of the output sequence $S_{dual\ oscillator}$ approaches the fast clock duty cycle d_{fast}.

In order to choose the design parameters such as $\frac{f_{fast}}{f_{slow\ center}}$, f_0 and f_{rng} appropriately, the concept of approximate entropy $(ApEn)$ [19] was employed as a measure of sequential irregularity or randomness. $ApEn$ is an essential tool which has been introduced for this purpose [20, 21], and based on the frequencies of repeating patterns in the output sequence. The approximate entropy $ApEn$ of order m, $(m \geq 1)$ is defined as:

$$\begin{aligned} ApEn(m) &= \Phi^{(m)} - \Phi^{(m+1)} \\ \Phi^{(m)} &= \sum_{\ell=1}^{2^m} \pi_\ell log \pi_\ell \end{aligned} \tag{4}$$

where m is the block length, 2^m is the number of all possible patterns and π_ℓ is the relative frequency of pattern $\ell = (i_1, ..., i_m)$ in the output sequence. Thus, sequences with large $ApEn$ values imply substantial irregularity, or randomness [20].

On the contrary to classical statistical tests, $ApEn$ provides a rigorous metric for proximity to randomness of a single finite sequence, particularly a very short sequence, without considering its underlying source [21]. This useful capability makes the utilization of $ApEn$ ideal for the numerical model of the proposed design. Shannon Entropy could be also used in the given model, however it should be noted that accurate calculation of Shannon Entropy requires the sequence to be infinite. The use of $ApEn$ is more appropriate for the developed model where numerical binary sequences are finite.

4. IMPLEMENTATION OF NUMERICAL MODEL

In order to verify the feasibility and the correct operation of the developed model, topology given in Fig. 1 was implemented numerically. A double-scroll attractor was used in the numerical model as the core of the RNG. Exploited chaotic attractor was obtained from a simple model given in [22] and is expressed by the Equation 5. It should be noted that when the nonlinearity is replaced by a continuous nonlinearity, the system is qualitatively similar to Chua's oscillator.

$$\begin{aligned} \dot{x} &= f_0 y \\ \dot{y} &= f_0 z \\ \dot{z} &= f_0(-ax - ay - az + sgn(x)) \end{aligned} \tag{5}$$

where f_0 corresponds to center operation frequency of the chaotic oscillator. The equations in 5 generate chaos for different set of parameters. For example, the chaotic attractor shown in Fig. 3 is obtained from the numerical analysis of the system with $a = 0.666$ using a 4^{th}-order Runge-Kutta algorithm with an adaptive step size.

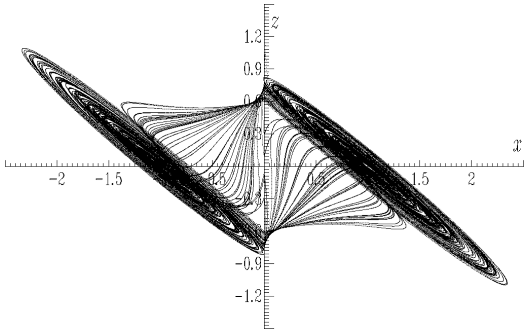

Figure 3: Results of the numerical analysis of the chaotic oscillator.

In order to address important design issues, numerical simulations were performed by sweeping the corresponding model parameters. Using the given Equation 2, output sequences have been obtained with the corresponding m_{output} and $ApEn$ values, of order 8 for a sequence length of 20000 bit, for different values of $\frac{f_{fast}}{f_{slow\ center}}$, f_0, f_{rng}, d_{fast} and ΔT where $f_{rng} = f_{slow\ center}$.

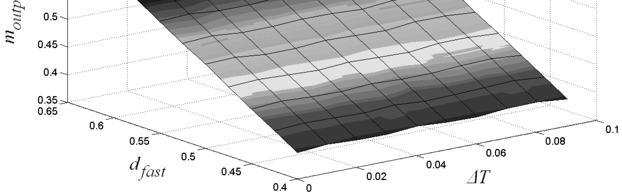

Figure 4: Mean value of $S_{dual\ oscillator}$ sequence with respect to d_{fast} and ΔT.

The mean value of $S_{dual\ oscillator}$ sequence m_{output} is plotted in Fig. 4 as a function of d_{fast} and ΔT for $d_{fast} \in$

$[0.4, 0.6]$. The mean values for higher $\frac{f_{fast}}{f_{slow\ center}}$ ratios are also shown in Fig. 5 for $d_{fast} = 0.5$. It should be noted from the given graphs that, m_{output} is sensitive to starting phase difference ΔT for $\frac{f_{fast}}{f_{slow\ center}} < 20$ while the effect of ΔT becomes negligible for high $\frac{f_{fast}}{f_{slow\ center}}$ ratios, and the mean value of the output sequence approaches the fast clock duty cycle d_{fast}. As a consequence, to provide unbiased output sequence, fast oscillator should have a balanced duty cycle and its frequency should be increased.

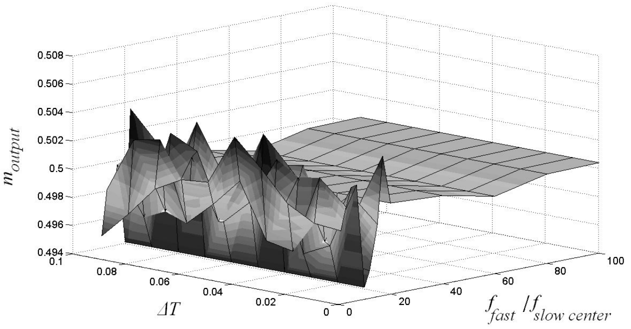

Figure 5: Mean value of $S_{dual\ oscillator}$ sequence with respect to $f_{fast}/f_{slow\ center}$ and ΔT.

In implementation, model parameters belong to nonlinear transfer function of the VCO, given in Equation 1, were assigned as $C_1 = 0.5$, $C_2 = 1$ and $C_3 = -0.08$ where, $K_1 = \frac{C_1 + 2x_{max}}{2x_{max}}$, $K_2 = C_2/(2x_{max})$ and $K_3 = C_3/(2x_{max})$. These model parameters are realistic values based on 74HCT4046A VCO integrated circuit module and determined by a curve fitting method.

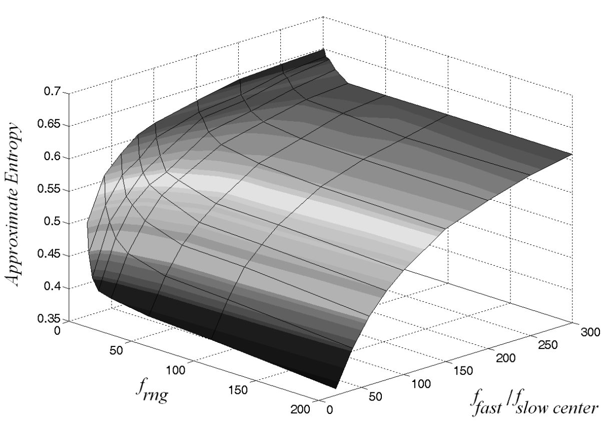

Figure 6: Approximate entropy of $S_{dual\ oscillator}$ sequence with respect to $f_{fast}/f_{slow\ center}$ and f_{rng}.

As shown in Fig. 6, $ApEn$ of the output bit sequence decreases as the f_{rng} increases and along with the increase in $\frac{f_{fast}}{f_{slow\ center}}$, $ApEn$ increases as well. In Fig. 7 how $ApEn$ of the output sequence, can come close the maximum information entropy ($ln2$) which might be possible for a perfect TRNG is shown as a function of $\frac{f_{fast}}{f_{slow\ center}}$ and f_0. Throughput data rate (f_{rng}) is basically limited by the f_0 and an increase either in f_0 or $\frac{f_{fast}}{f_{slow\ center}}$ results in an increase in $ApEn$ making much higher data rates possible.

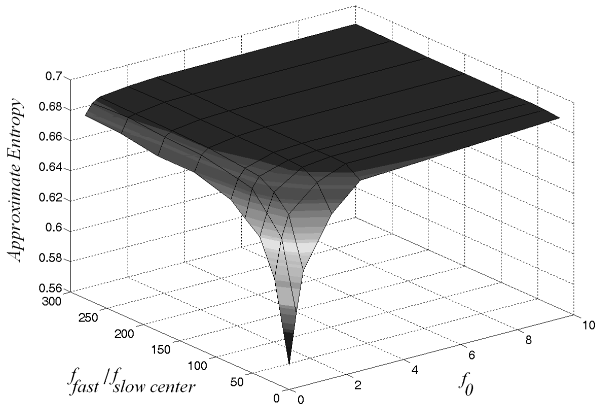

Figure 7: Approximate entropy of $S_{dual\ oscillator}$ sequence with respect to $f_{fast}/f_{slow\ center}$ and f_0.

Although, it has been numerically verified that bit sequence $S_{dual\ oscillator}$ passed the test suite of FIPS-140-2 [23] without post-processing, down to $\frac{f_{fast}}{f_{slow\ center}} = 40$, 200 is an optimum value for the given ratio after which $ApEn$ stays steady. In accordance with the practical limitations, in order to obtain perfectly uncorrelated binary sequences with maximum entropy, f_{fast} should be increased by considering a balanced duty cycle.

In order to compare robustness of double-scroll attractor based TRNGs against external interference, approximate entropy values of the binary sequences generated by different techniques [15, 16] in the presence of sinusoidal signal interference are calculated by using numerical models. In Fig. 8, corresponding $ApEn$ values of order 8 for a sequence length of 20000 bit are given versus m, where m is the ratio of interfering sinusoidal signal amplitude to chaotic signal (x) amplitude.

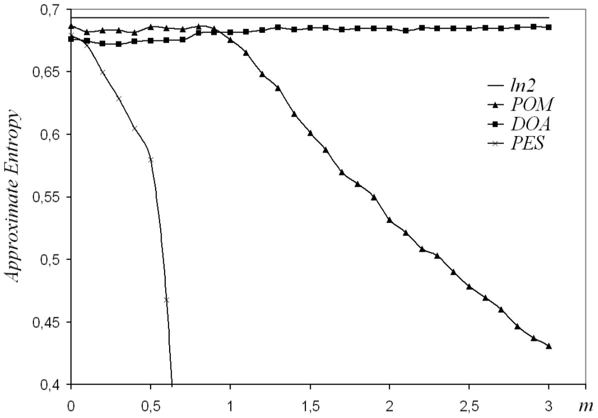

Figure 8: Comparison between the robustness of double-scroll attractor based TRNGs in the presence of sinusoidal signal interference.

As shown in Fig. 8, chaos-modulated dual oscillator architecture, *DOA* is not sensitive to non-random influences coupling into the source while the other methods are. Additionally, numerical results demonstrate that, in comparison with *PES* [16] where random sequences are generated by periodically sampling one of the state, TRNG denoted by *POM* [15] which uses Poincaré map of the chaotic system is more robust against sinusoidal signal interference. However, sinusoidal signal amplitude must be smaller than the chaotic signal amplitude for the *POM* to remain unaffected. In the given graph that, *ln*2 is the maximum information entropy which might be possible for a perfect TRNG. It is noteworthy that, chaos-modulated dual oscillator architecture not only offers much higher throughput rates but also provides more robustness against external interference.

5. CONCLUSIONS

An effective and accurate model of chaos-modulated dual oscillator-based random number generators was developed. The model allows the assessment of the output randomness as a function of design parameters, thus provides an essential tool to help resolve important design issues. Numerical results demonstrate that, chaos-modulated dual oscillator architecture is more robust against external non-random interference. Model can adapt dual oscillator architecture for any chaotic oscillator existing in the literature, by determining appropriate design parameters. In conclusion, numerical results presented in this paper not only verify the feasibility of the developed model, but also encourage its use for the realization of a high-performance random number generator circuit as well.

REFERENCES

[1] B. Jun and P. Kocher, "The Intel Random Number Generator,"*Cryptography Research, Inc.* white paper prepared for Inter Corp. Apr. 1999 http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf.

[2] A. Menezes, P.van Oorschot, and S.Vanstone, *Handbook of Applied Cryptology*. CRC Press, 1996.

[3] B. Schneier, *Applied Cryptography*. 2^{nd} ed. John Wiley & Sons, 1996.

[4] W.T. Holman, J.A. Connelly, and A.B. Downlatabadi, "An Integrated Analog/Digital Random Noise Source," *IEEE Trans. Circuits and Systems I*, vol. 44, no. 6, pp. 521-528, June 1997.

[5] V. Bagini and M. Bucci, "A Design of Reliable True Random Number Generator for Cryptographic Applications," in *Proc. CHES 1999*, Workshop Cryptographic Hardware and Embedded Systems, pp. 204-218, 1999.

[6] M. Dichtl and N. Janssen, "A High Quality Physical Random Number Generator," in *Proc. SAME 2000*, Proc. Sophia Antipolis Forum Microelectronics, pp. 48-53, 2000.

[7] C.S. Petrie and J.A. Connelly, "A Noise-Based IC Random Number Generator for Applications in Cryptography," *IEEE Trans. Circuits and Systems I*, vol. 47, no. 5, pp. 615-621, May 2000.

[8] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-Based Random Number Generators-Part II: Practical Realization," *IEEE Trans. Circuits and Systems I*, vol. 48, no. 3, pp. 382-385, Mar. 2001.

[9] S. Callegari, R. Rovatti, G. Setti, "Embeddable ADC-Based True Random Number Generator for Cryptographic Applications Exploiting Nonlinear Signal Processing and Chaos", *IEEE Transactions on Signal Processing*, vol. 53, pp. 793-805, n. 2, Feb. 2005.

[10] M. Delgado-Restituto, F. Medeiro, and A. Rodriguez-Vazquez., "Nonlinear Switched-current CMOS IC for Random Signal Generation", *Electron. Lett.*, 29, (25), pp. 2190-2191, 1993.

[11] M.E. Yalçın, J.A.K. Suykens, and J. Vandewalle "True Random Bit Generation from a Double Scroll Attractor", *IEEE Trans. Circuits and Systems I*, vol. 51, (7), pp. 1395-1404, 2004.

[12] S. Ergün, S. Özoğuz, "Truly Random Number Generators Based on a Non-Autonomous Chaotic Oscillator," *Int. J. Electron. Commun.*, vol. 61, pp. 235-242, 2007.

[13] B. Sunar, W.J. Martin and D.R. Stinson, "A Provably Secure True Random Number Generator with Built-In Tolerance to Active Attacks," *IEEE Trans. Comput.*, vol. 56, no. 1, pp. 109-119, Jan. 2007.

[14] M. Bucci, L. Germani, R. Luzzi, A. Trifiletti, and M. Varanonuovo, "A High Speed Oscillator-based Truly Random Number Source for Cryptographic Applications on a SmartCard IC", *IEEE Trans. Comput.*, vol. 52, pp. 403-409, Apr. 2003.

[15] S. Ergün, S. Özoğuz, "Truly Random Number Generators Based On a Double-Scroll Attractor," in *Proc. MWSCAS 2006*, IEEE Int. Midwest Symposium on Circuits and Systems, pp. 322-326, Aug. 2006.

[16] S. Ergün, S. Özoğuz, "Compensated True Random Number Generator Based On a Double-Scroll Attractor," in *Proc.NOLTA 2006*, Int. Symposium on Nonlinear Theory and its Applications, pp. 391-394, Sep. 2006.

[17] R. Devaney, *An introduction to Chaotic Dynamical Systems*. 2^{nd} ed. Reading, MA: Addison-Wesley, 1989.

[18] A.Shamir, "On The Generation of Cryptographically Strong Pseudorandom Sequences", *ACM Transactions on Computer systems*, vol. 1(1):38-44, 1983.

[19] 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, Available at http://csrc.nist.gov/rng/SP800-22b.pdf

[20] S. Pincus, and B.H. Singer, "Randomness and degrees of irregularity," *Proc. Natl. Acad. Sci. USA.*, Mar. 1996; vol. 93, pp. 2083-2088.

[21] S. Pincus, and R.E. Kalman, "Not all (possibly) "random" sequences are created equal," *Proc. Natl. Acad. Sci. USA.*, Apr. 1997; vol. 94, pp. 3513-3518.

[22] A. S. Elwakil, K. N. Salama, and M. P. Kennedy, "An equation for generating chaos and its monolithic implementation," *Int. J. Bifurcation Chaos*, vol. 12, no. 12, pp. 2885-2896, 2002.

[23] National Institute of Standard and Technology, "Security Requirements for Cryptographic Modules," NIST, Boulder, CO, Jan. 1994.