An IC Random Number Generator Based on Chaos

V. Tavas[1], A. S. Demirkol[1], S. Ozoguz[1], S. Kilinc[2], A. Toker[1], A. Zeki[1]
[1]Istanbul Technical University, Faculty of Electrical-Electronics Engineering,
Maslak, 34469, Istanbul, Turkey
[2] Dokuz Eylul University, Faculty of Engineering,
Alsancak, Izmir, Turkey
E-mail : tavas@itu.edu.tr, demirkola@itu.edu.tr, ozoguz@itu.edu.tr, selcuk.kilinc@deu.edu.tr,
tokeral@itu.edu.tr, zekia@itu.edu.tr

Abstract
In this work, an integrated random number generator based on oscillator sampling method is presented. The random number generator exploits a continuous-time chaotic circuit as the entropy source. A source-coupled multivibrator is used to transform the generated chaotic signal into jittered oscillations required in the oscillator sampling method. The random number generator circuit is fabricated using 0.35µm CMOS process. The circuit is supplied with ±1.65V and occupies an area of 0.25mm^2. The throughput of the RNG is 2Mbit/s and its average power consumption is measured as 35mW at its typical throughput. It is shown that experimental binary data obtained from the fabricated IC pass the four tests of FIPS-140-1 test suite.

INTRODUCTION

As a result of new design challenges arising due to the rapid advances in IC technology, electronic circuits are to be redesigned so that they are compatible with state-of-the-art integration technology. To be specific, IC compatible circuits of today have to operate at low voltages with low power dissipation, while offering an acceptable high-frequency operation performance. On the other hand, random number generators (RNG) are generally used in different cryptosystems where true randomness is needed to produce secret keys. Some works in the decade premise a new type of RNGs suitable for IC technology based on continuous-time chaos (see [1-4] and the references cited therein).

In this paper, the design of a RNG based on continuous-time chaos is described which is completely suitable for integration. The random number generator is based on oscillator sampling method [5] and uses a continuous time chaotic oscillator as the entropy source. The details of the chaos oscillator were recently presented in [3], [6].

Post layout simulation results of the designed circuit, experimental results of the fabricated IC and random number test results of the fabricated chip verifying the proper operation of the chip are also provided. Statistical quality of the random bits generated from the fabricated RNG is verified using the well-known FIPS-140-1 statistical test [7].

OVERVIEW OF THE RANDOM NUMBER GENERATION METHOD

In the design of the proposed RNG, oscillator sampling method described in Fig. 1 is used [5]. In this architecture, there are two free running oscillators, one oscillating at much higher frequencies than the other. Random bits are generated by sampling the fast oscillator at the rising edge of the slow oscillations via a D-type flip-flop. The randomness of this scheme is mainly due to the jitter noise of the slow oscillator. Numerical analyses of this architecture show that, if the standard deviation in the slow oscillator period due to the time jitter is greater than the fast oscillator period, two sequential samplings can be assumed uncorrelated [8]. However, any practical circuit implementation of this scheme is known to offer a limited statistical quality since jitter level of a typical slow oscillator is not large enough to generate enough unpredictability [8]. This drawback is solved by increasing deliberately the jitter level of the slow oscillations by using an entropy source such as chaotic signals [3], [10] or physical noise [8], [9]. Both of these approaches lead to acceptable statistical quality of the random bits at the architecture output.

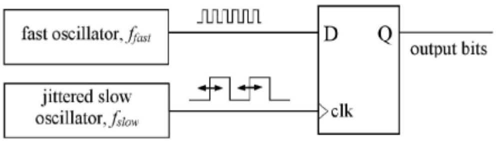

fast oscillator, f_{fast}
jittered slow oscillator, f_{slow}
D
Q
clk
output bits

Fig. 1: Oscillator sampling method.

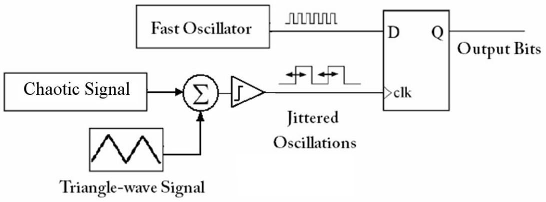
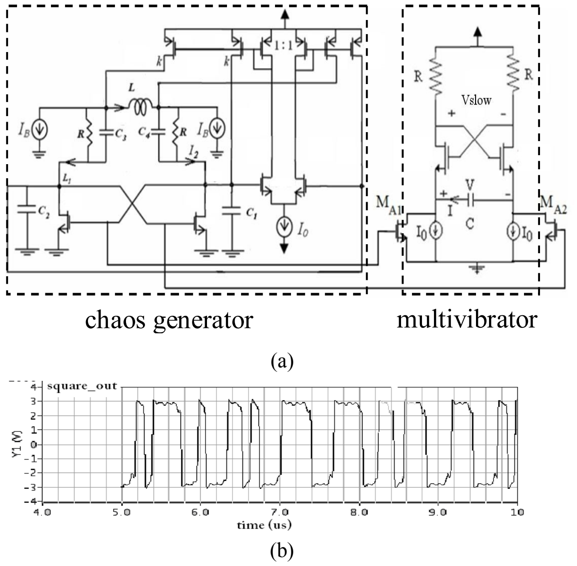


Fig. 2: Architecture used to implement oscillator sampling method.

Adopting the chaos-based approach to improve entropy, we used the architecture depicted in Fig. 2 [3], [10] the details of which are given in the sequel.

SIMULATION RESULTS OF THE HARDWARE RNG



(a)

(b)

Fig. 3: a) Circuit used to generate jittered slow oscillator. b) Typical waveform for the jittered slow oscillator output with a mean frequency of 2MHz.

In the adopted scheme of Fig. 2, the jittered oscillation is obtained by applying a hard-limiting nonlinearity (realized using a comparator) to the sum of the chaotic signal and the triangle wave signal [3]. An alternative implementation of the subcircuit consisting of the chaos and the triangle-wave generators, the summing block and the comparator is designed as shown in Fig. 3a. This structure which considerably simplifies the circuit implementation can be used to substitute the subcircuit mentioned above owing to the judicious interconnection of the chaos generator and the multivibrator. To be specific, the multivibrator performs a twofold function: it generates the triangle-wave signal (indeed, the voltage *V* across the capacitor *C* is a triangle-wave signal) and it provides the required hard-limiting function (the nonlinear differential voltage transfer between V_{slow} and V is a hard-limiting type nonlinearity). On the other hand, the summation operation is realized at the nodes *A* and *B* in current-mode, where triangle-wave current *I* and the drain currents of M_{A1} and M_{A2} are added owing to the Kirchhoff's Laws. Frequency of square wave is controlled via biasing current I_0; hence via the current passing through the capacitor. By changing this current flowing through the capacitor by adding drain currents of M_{A1} and M_{A2}, which are, in turn, chaotic signals, jittered square wave is generated. Typical waveforms obtained at the voltage output V_{slow} is given in Fig. 3b. It should be noted that the details of the chaotic circuit shown within the dashed box were given in [3] and [6]. Post-layout simulations of the circuit using Cadence Design Tools indicated that loading effects of the successive stages may lead to seriously deformed signals at the outputs of the circuit in Fig. 3(a); hence an additional inverter is connected at the multivibrator output to reduce this deterioration (not shown for the sake of simplicity).

Preliminary numerical analysis of the RNG architecture in Fig. 2 indicated that four parameters mainly affect RNG performance: (i) Ratio of the slow oscillator mean period and the fast oscillation period, which is advised to be no less than 50 [3]. (ii) Power ratio of the chaotic signal and triangle wave signal. When this ratio is increased, the standard deviation of the modulated slow oscillator period, σ_{slow}, increases. According to the numerical simulations of RNG, the system performance improves when σ_{slow} increases. For an acceptable randomness quality, σ_{slow} is suggested to span 6–10 high-frequency periods [3]. (iii) Ratio of the chaotic signal bandwidth and the slow oscillator average frequency. Note that this parameter gives the upper limit for the RNG throughput, since throughput is the mean frequency of the slow oscillator. This parameter will be denoted by $f_{0,chaos}/f_{slow}$ where $f_{0,chaos}$ is the peak frequency in the frequency spectrum of the chaotic signal, a quantity that is used here to quantify the chaotic signal bandwidth [3]. (iv) Another important parameter is the mark space ratio of the fast oscillator which should be close to unity to achieve an unbiased output [3], [8], [9].

In our design, the passive component values were taken as R=10kΩ, C=12pF, the aspect ratios of the cross coupled and differential pair transistors were 25μm/1μm and 15μm/1μm, respectively, while the dimensions of M_{A1} and M_{A2} were both kept at 3μm/1μm. With these settings, a typical waveform of the slow oscillator is shown in Fig. 3(b), where the mean frequency is measured as 2MHz. From the simulations, the standard deviation of the slow oscillator period, σ_{slow} is found to be approximately 60ns. In order to implement the fast oscillator, a ring oscillator is designed oscillating at 150MHz which is as large as 75 times of jittered slow oscillator frequency, meeting the corresponding design criterion given above. It should be noted that, with this frequency value, standard deviation of the slow oscillator period spans 10 high frequency periods, which is consistent with the RNG design criterion (refer to the discussion above) [3]. Simulation results indicated that for larger oscillating frequencies, particularly over 200MHz, mark space ratio of the ring oscillator considerably diverges from unity; hence causing an unacceptable bias at the RNG output.

The sampling of the slow oscillator is realized using a parallel system composed of D-type and T-type flip-flops as shown in Fig. 4. In this circuit, D-type and T-type flip-flops operate as shift registers and frequency dividers, respectively. With this circuit, RNG output bits are retrieved at the fourth rising side of the clock signal, thus the data is retrieved at a rate of 0.5Mbit/s, much lower than the RNG actual throughput.

Therefore, any possible problems that could arise during the data reading operation due to the limitation of the data acquisition speed of the test system are avoided. The waveforms at the flip-flop outputs of the digital part are shown in Fig. 5.

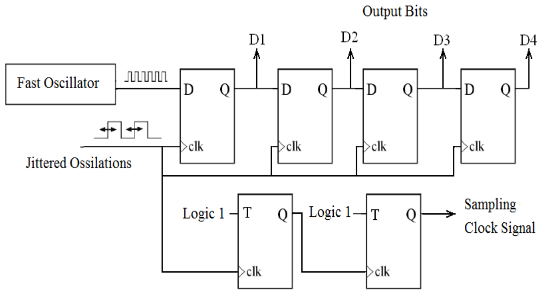


Fig. 4: Circuit schematic of the digital circuitry of the RNG.

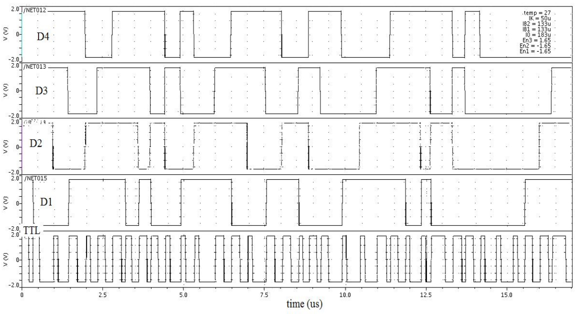


Fig. 5: The output waveforms of the D-type flip-flops (D_1-D_4) and the T-type flip-flop (last row) in Fig. 4.

EXPERIMENTAL RESULTS AND EVALUATION OF RNG PERFORMANCE

The circuit described in the previous section is fabricated using AMS 0.35 CMOS process and the chip photo of fabricated RNG is given in Fig. 6. The circuit is supplied with ±1.65V and occupies an area of 0.25mm^2.

The chaotic attractor observed from the fabricated chip is shown in Fig. 7, which verifies the proper operation of the entropy source of the RNG. The jittered oscillations observed at the output of the multivibrator (refer to Fig. 3) are shown in Fig. 8(a). The mean oscillation frequency of the slow oscillator was 2.2MHz, which is in perfect agreement with the simulation results. On the other hand, the standard deviation of the slow oscillation period, σ_{slow} was measured as 45ns, slightly lower than the value expected from the simulations. However, assuming that the fast oscillator properly operates at 150MHz, σ_{slow} spans 6-7 fast oscillator periods; thus being consistent with the design criterion of the RNG.

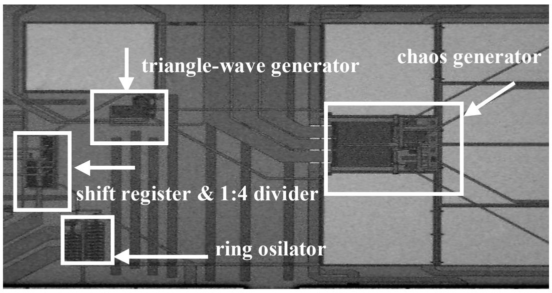


Fig. 6: Layout of the fabricated RNG.

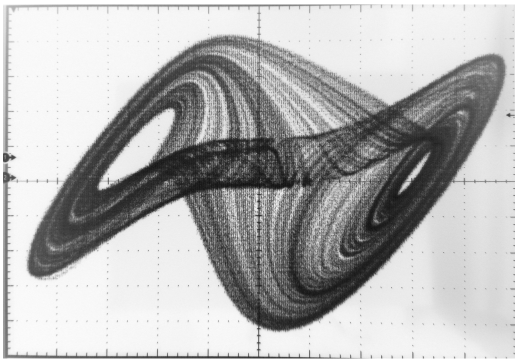


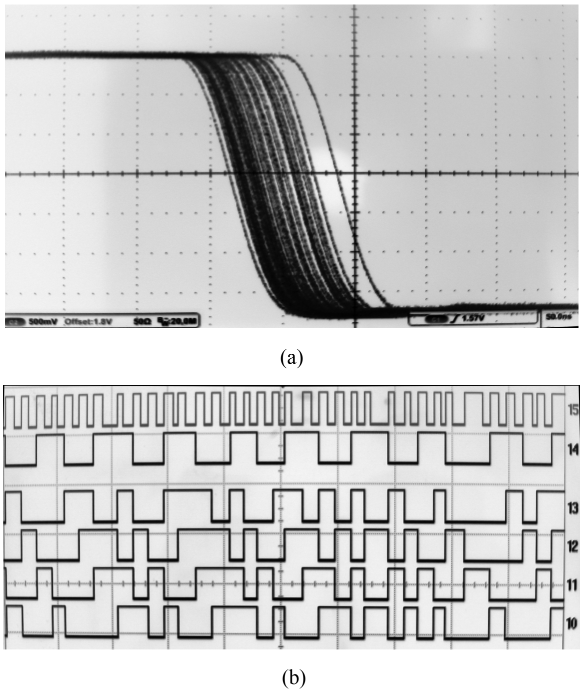
Fig. 7: The observed chaotic attractor (X-axis=500mV/div, Y-axis=200mV/div).

In order to verify the proper operation of the RNG digital part consisting of the D-type and T-type flip-flops, corresponding flip-flop outputs are probed via a logic analyzer and the measured timing diagrams are investigated. In Fig. 8(b), the jittered slow oscillation at the T flip-flop output is shown in the first row, while the outputs of four D-type flip-flops are shown in the third-sixth rows. From these diagrams, proper operation of the RNG digital circuitry can readily be verified.

In order to evaluate the RNG performance of the fabricated chip, the following metric is used as a figure of merit:

$$\Phi = \left[\frac{2^m}{k}\sum_{i=1}^{2^m} n^2(i)\right] - k \qquad (1)$$

where output bit sequence is divided into k non-overlapping sub-sequences of length m and $n(i)$ is the number of occurrences of the ith type of sequence with i=1,…,2m. To verify randomness of the output bits, a bit sequence of 20Mbits was acquired using a high-speed data acquisition card and the data was grouped into 1000 blocks, each having a length of 20,000 bits. The figure of merit in (1) is calculated for each block for m=4 and k=5000, which correspond to poker test in the FIPS-140-1 test suite [7]. The histogram of the calculated values is illustrated in Fig. 9 where the distribution of the Φ-metric can be considered. From these results, the maximum of the calculated values is found as 46.17, which is smaller than the maximum allowed value of Φ=57 in FIPS-140-1 test suite [7]. On the other hand, we have verified that all the data blocks passed the four tests (i.e. monobit, poker, runs, longest runs) of the test suite without applying any post-processing.



(a)

(b)

Fig. 8 a) Jittered slow oscillations observed at the slow oscillator output of the fabricated chip. b) Mesured waveforms at the flip-flop outputs.

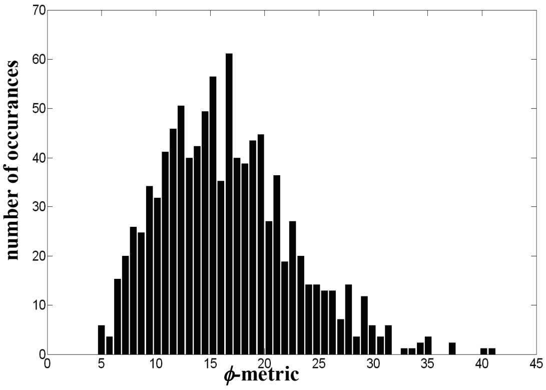


Fig. 9: Measured Φ metric at the output of the fabricated RNG.

CONCLUSION

An IC random number generator based on oscillator sampling method is presented in this paper. Proposed method utilizes a continuous time chaotic circuit as an entropy source to increase the randomness of the output bit sequence. Throughput of the system is 2Mbits/s and randomness quality of the RNG is verified using standard random number test FIPS-140-1 which the output sequence passes all the tests.

REFERENCES

[1] Gonzales O. A., Han G., De Gyvez P., and Sinencio E.S.: 'Lorenz-based chaotic cryptosystem: a monolithic implementation', IEEE Trans. Circuits Syst. I, 2000, 47, pp. 1243-1247.

[2] Ozoguz S., Elwakil A.S., Ergun S.: 'Cross coupled chaotic oscillators and application to random bit generation', IEE Proc. Circuits, Devices & Systems, 2006, 153, pp. 506-510.

[3] Tavas, V., Demirkol, A.S., Ozoguz, S., Zeki, A., Toker, A., "An integrated cross-coupled chaos oscillator applied to random number generation", IET Circuits, Devices & Systems, Vol:3 pp. 1-11, 2009.

[4] Callegari S., Rovatti R., Setti G., "Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos", IEEE Trans. Signal Process., 2005, 53, pp. 793–805.

[5] Fairfield, R. C., Mortenson, R. L., Coulthart, K.B., "An LSI random number generator", Proc. Advances in Cryptolgy Conf. (CRYPTO '84), pp. 203-230, 1984.

[6] Tavas, V., Ozoguz, S., ve Toker, A., "A new IC chaotic circuit (in Turkish)", Elektrik-Elektronik-Bilgisayar-Biyomedikal Muh. 12. Ulusal Kongresi Bildiriler Kitabi, pp. 253-256, 2007.

[7] National Institute of Standard and Technology, "Security requirements for cryptographic Modules", FIPS PUB 140-1, 1994.

[8] Petrie, C. S., Connelly, J. A., "A noise based IC random number generator for applications in cryptography", IEEE Trans. Circuit & Systems, Vol: 47, No: 5, pp. 615-621, 2000.

[9] Bucci, M., Germani L., Luzzi R., Trifiletti A., and Varanonuovo M., "A high-speed oscillator-based truly random number source for cryptographic applications on a smart card IC", IEEE Transaction on computer, Vol: 52, No: 4, pp. 403- 409, 2003.

[10] Ergun S., Ozoguz S., "Truly random number generators based on non-autonomous continuous-time chaos", Int. J Cir. Theory Appl., 38, 1, pp. 1-24.