A Novel Dual Entropy Core True Random Number Generator

İhsan Çiçek[1,2], Ali Emre Pusane[2], Günhan Dündar[2]

[1] Informatics and Information Security Research Center, TUBITAK BILGEM, 41470, Kocaeli, Turkey
ihsan.cicek@tubitak.gov.tr
[2] Department of Electrical and Electronics Engineering, Bogazici University, Istanbul, Turkey
ali.pusane@boun.edu.tr, dundar@boun.edu.tr

Abstract

True random number generators based on 1D chaotic maps have limited entropy generation capability due to their finite number of *Lyapunov* exponent(s). In this work, we introduce a novel dual entropy core discrete time chaos based true random number generator architecture that can enhance the randomness of the bitstream using hardware redundancy. We develop a custom mathematical model of the proposed TRNG architecture for numerical simulations and, show that the entropy generated by the proposed architecture is higher than that of a single entropy core counterpart. We calculate the entropy of the generated bitstream using a practical information metric: T-entropy. T-entropy calculations reveal that the proposed architecture is capable of generating high entropy for a wide range of parameter values. As a proof of concept, we implemented the proposed architecture on a field programmable analog array integrated circuit. Acquired random numbers successfully passed all NIST 800.22 statistical tests without any post-processing. To the very best of our knowledge this is the first hardware implementation of a dual entropy core true random number generator in the literature.

1. Introduction

True Random Number Generators (TRNGs) are accepted to be the most critical component of any cryptographic system, since no deterministic cryptographic function is capable of generating more entropy at the output than what is available at the inputs [1]. Hence, the unpredictability and the security of the cryptographic system depend heavily on the TRNG, portraying it as the most critical and crucial component of the system. Traditional TRNG design methods based on the sampling of amplified electrical noise cannot satisfy the specific requirements of contemporary lightweight cryptographic applications due to limited bandwidth of the entropy source [2]. Multiple oscillator sampling based TRNGs consume considerable amounts of power and area for fast generation of random bits [3, 4]. Design resources required for achieving a certain level of randomness are quite large and usually unacceptable from a lightweight cryptography point of view.

A dynamic system operating in chaotic regime can act as an information source according to ergodic theory [6]. Exponentially divergent and aperiodic behaviour of a chaotic system is characterized and driven by the underlying positive *Lyapunov* exponent(s), making them extremely sensitive to variations in the initial conditions. Small deviations in the initial conditions are transformed into huge variations throughout the spatio-temporal evolution of the chaotic trajectories. While the non-linear dynamics of chaotic systems are defined in deterministic terms, their high sensitivity to small perturbations in the initial conditions render them practically unpredictable. Continuous wandering of the initial conditions caused by the existing electrical noise in physical implementations makes it impossible to determine the initial conditions exactly, due to finite measurement precision, hence providing the desired unpredictability. Chaos based TRNGs use chaotic signals as the entropy source. Continuous time chaos based TRNG implementations usually occupy large area and consume high power as a result of large analog components, such as OPAMPs, oscillators, OTAs, and, inductors, required to implement the differential equations defining the dynamic system [7, 8]. On the contrary, discrete time chaos based TRNGs can be realized using much less design resources, thus yielding compact and efficient building blocks for lightweight-cryptographic systems [9, 10, 11]. Consequently, discrete time chaos based TRNGs are considered to be more compatible with all-digitally implemented cryptographic systems using standard CMOS processes since they do not need any large area occupying components unlike their counterparts. Conventional discrete time chaos based TRNGs in the literature use a single endomorphic map as the entropy source [9]. In this approach, a chaotic signal is compared to a threshold for random bit generation. Primary disadvantage of this approach is that the implemented system exhibits sensitive dependence to variations of parameters and this has a direct impact on the maximum achievable entropy and statistical properties. For instance, any variation in chaos control parameter(s) can adversely affect the available entropy while deviation of the bit extraction threshold introduces statistical bias to the generated bitstream.

In this work, we propose a novel dual entropy core discrete time chaos based true random number generator architecture employing hardware redundancy to generate higher entropy random bits with less sensitivity to chaos control parameter variations when compared to its conventional single entropy core counterpart. To the very best of our knowledge this is the first hardware implementation of a dual entropy core true random number generator in the literature. The paper is organized as follows: In Section II, we outline the custom mathematical model of the proposed architecture for numerical simulations and we evaluate the randomness performance using a practical information measure, T-entropy, as the randomness metric. Section III provides a brief description of the design of a proof of concept circuit implementing the proposed architecture on a field programmable analog array chip along with associated measurement and statistical test results.

2. Mathematical Model of The Proposed TRNG

A conventional single entropy core discrete time chaos based TRNG architecture can be portrayed as shown in Fig. 1, in which the non-linear function block implements the chaotic map function, and the sample and hold block drives the chaotic dynamics to form the entropy core. The comparator, together with a threshold generator, compose the extractor, which generates random bits depending on the spatio-temporal location of chaotic trajectory in the partitioned phase space. The threshold generator capable of tracking the chaotic signal and dynamically dividing the phase space is required to generate random bits.

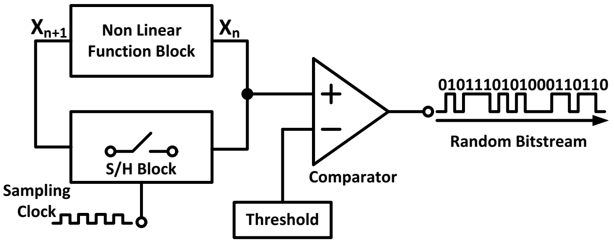


Figure 1. Conventional single entropy core discrete time chaos based TRNG architecture.

The entropy of the generated bitstream is a strong function of the chaos control parameter, since it directly affects the *Lyapunov* exponent(s) and the chaotic behaviour. Maximum entropy that can be generated by a single entropy core discrete time chaos based TRNG is fundamentally limited by its finite number of *Lyapunov* exponent(s) according to Pesin's Theorem [12]. For the single entropy core TRNG system presented in Fig. 1, any deviation in the comparison threshold will be translated into statistical bias at the output bitstream, which needs to be addressed by a post-processor at the expense of reduced throughput. Furthermore, any deviation in the chaos control parameter manifests itself as reduced entropy, which is unacceptable from a security point of view.

The basic idea behind our novel dual entropy core TRNG architecture presented in Fig. 2 is to generate high entropy random bits by comparing uncorrelated and independent state variables of two chaotic systems having uniform invariant measures. We use entropy core redundancy to increase maximum achievable entropy, which is fundamentally limited by the *Lyapunov* exponent in the single entropy core architecture. For the ease of calculation and implementation, we used the same map in both entropy cores. While, in principle, all endomorphic maps exhibiting chaotic behaviour with uniform invariant measure can be used as entropy sources, we have chosen the *Bernoulli* map, presented in Fig. 3, as the entropy source in our studies for its simplicity and uniform invariant measure.

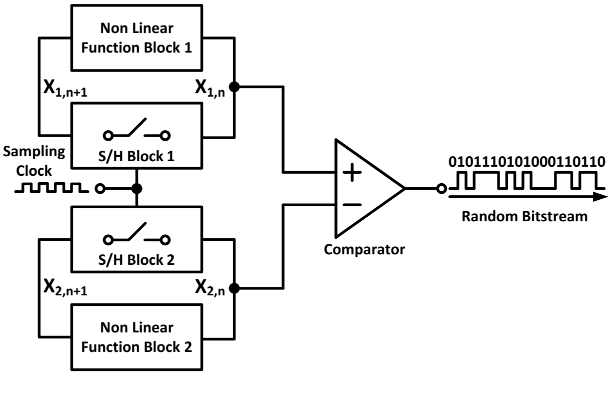


Figure 2. Proposed dual entropy core discrete time chaos based TRNG architecture.

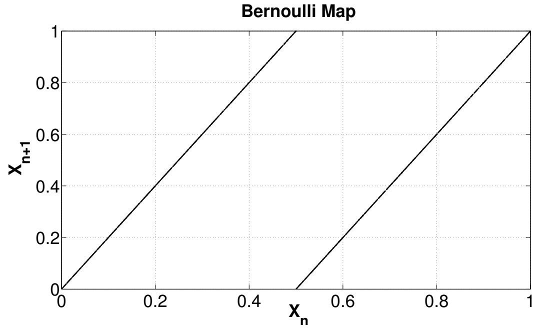


Figure 3. Bernoulli map function.

In mathematical terms, *Bernoulli* map can be expressed as

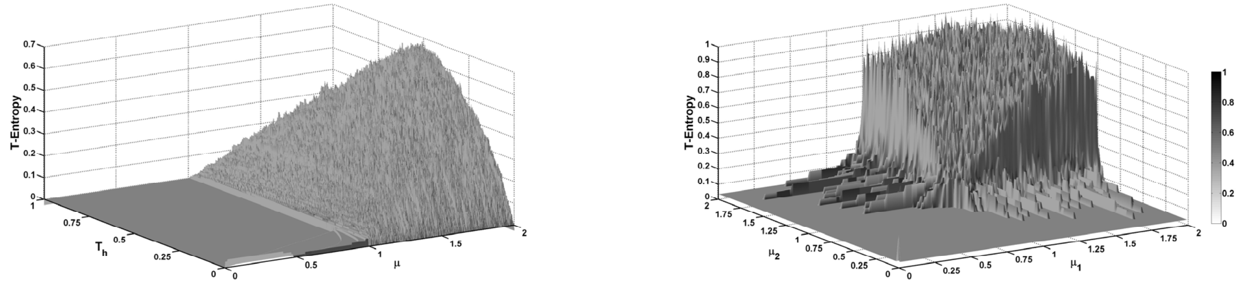
$$x_{n+1} = \left\{ \begin{array}{llcll} \mu x_n, & 0 & \leq & x_n & < 0.5 \\ \mu x_n - 1, & 0.5 & \leq & x_n & \leq 1, \end{array} \right. \quad (1)$$

where μ is the chaos control parameter setting both the dynamic and statistical properties of the map. Assume that we have two uncorrelated and uncoupled *Bernoulli* maps that are guaranteed to start from different initial conditions with independent chaos control parameters μ_1 and μ_2. Then, we can define a bit extractor function,

$$b_n = B(x_{1,n}, x_{2,n}) = \left\{ \begin{array}{lccc} 0, & x_{1,n} & \leq & x_{2,n} \\ 1, & x_{2,n} & < & x_{1,n}, \end{array} \right. \quad (2)$$

where $x_{i,n}, \quad i = 1, 2, ...$ corresponds to the chaotic time series generated by the i^{th} core. We construct the dual entropy core discrete time chaos based TRNG model presented in Fig. 2 using (1) and (2). Our dual entropy core TRNG model is based on symbolic dynamics that translates generated chaotic time series into symbolic binary strings of ones and zeros using the relation between chaotic samples from different entropy cores. The mathematical model implemented in MATLAB generates one random bit per map iteration, corresponding to at speed sampling in practice.

In order to evaluate the randomness performance of the proposed architecture, an entropy metric is required, since pass-fail type statistical tests do not provide a fine resolution metric for evaluation of the entropy of generated finite bitstream. A vocabulary based information measure, called T-entropy, is used to calculate the entropy of the generated finite bitstream [13]. T-entropy calculation is based on a recursive hierarchical pattern copying (RHPC) algorithm, called T-decomposition, which parses the bitstream in terms of bit patterns, while accounting for consecutive repetitions of each pattern. Recursive bit pattern identification approach enables the algorithm to detect any existing long range dependencies and structures in patterning. T-entropy of a finite bitstream is calculated based on the complexity of the RHPC algorithm [14]. We calculated the T-entropy of the bitstreams generated by both single and dual entropy core



(a) T-entropy of the bitstream generated by single entropy core TRNG.

(b) T-entropy of the bitstream generated by dual entropy core TRNG.

Figure 4. 3D T-entropy of Single and dual entropy core TRNG generated bitstream comparison.

TRNG models, covering all possible values of parameters affecting statistical properties. 3D projections of calculated T-Entropies are constructed as shown in Fig. 4(a) and 4(b). Note that in both cases, T-entropy increases as the chaos control parameter(s) μ approach to the ideal value of 2. In single entropy core case, any deviation in the T_h parameter reduces the maximum achievable entropy level of 0.693 drastically as shown in Fig. 4(a). On the contrary, in the dual entropy core case presented in Fig. 4(b), both the maximum achievable entropy level and the associated parameter interval are large, which enables generation of high entropy bits for a wide range of parameter values. Our proposed architecture stands out with its maximum achievable entropy level exceeding 0.9 for a wide range of chaos control parameters, thus surpassing its highly parameter sensitive counterpart. The dual entropy core TRNG architecture is less sensitive to deviations in the chaos control parameters, which creates an advantage over singe entropy core counterpart from an implementation point of view at the expense of hardware redundancy. Moreover, it does not require a comparison threshold generator.

3. FPAA Implementation and Measurement Results

Field programmable analog array (FPAA) is a cost effective reconfigurable platform for fast prototyping of analog circuits. For each entropy core, a non-linear function block and a sample-hold block are required, which can be built using the resources found in the computational analog blocks (CABs) of the FPAA chip. In addition, the bit extractor function (2) can be implemented by using the comparator component within the available CABs as shown in Fig. 5. We have used a switched capacitor based FPAA chip (AN231E04) as the implementation platform for the proof of concept design of the proposed architecture, since it allows realization of discrete time systems [15]. The chip is powered by 3.3V DC and driven by a 16MHz master clock, which is used to synthesize CAB component clocks. The non-linear dynamics of dual *Bernoulli* map based TRNG is driven by sample-hold circuits operating at 2MHz. An average throughput in the excess of 1.5Mbps is achieved as shown in Fig. 6. The throughput is limited by the switched capacitor implementation technology of the FPAA. An off the shelf available FPGA development board is used to acquire and transfer a dataset of 400 Mbits to computer for statistical tests. Even though no set of statistical tests can absolutely qualify a TRNG, they are useful in determining the statistical performance for

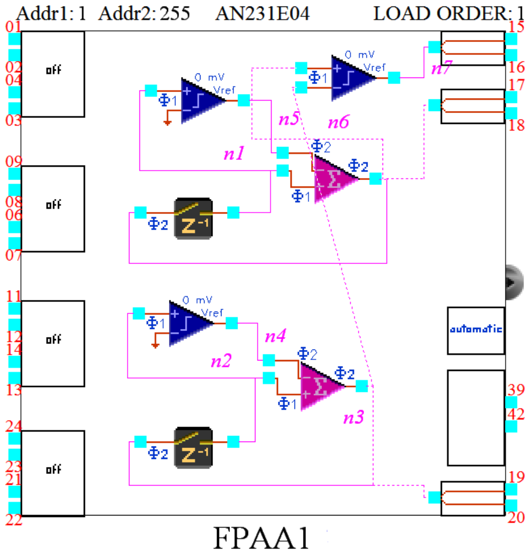


Figure 5. FPAA implementation of dual *Bernoulli* map based TRNG.

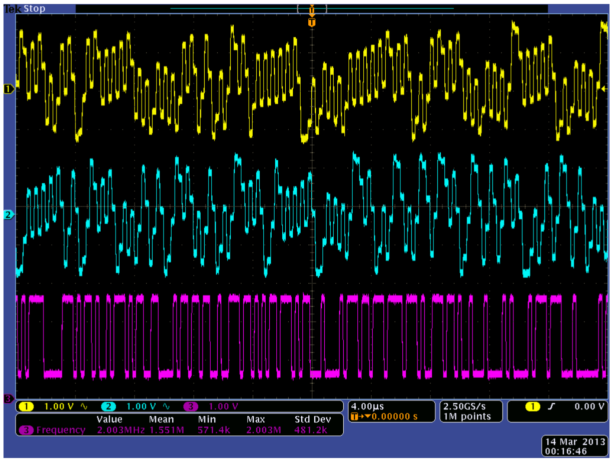


Figure 6. Measurement results of dual *Bernoulli* map based TRNG implemented on FPAA.

cryptographic applications. NIST statistical test suite v2.0 is used for evaluating the statistical performance of the acquired bitstream as presented in Table 1. Each p-value corresponding to a particular test describes the probability of the bitstream generated by an ideal TRNG [16]. NIST statistical test suite divides the raw bitstream into 1 Mbit blocks and applies the tests. Proportion column in Table 1 shows the ratio of 1 Mbit sequences passing the particular NIST test. According to the results in Table-1, the acquired bitstream successfully passes all NIST statistical tests.

Table 1. NIST STS v2.0 Test Results

Test	P-Value	Proportion
Frequency	0.904708	0.9975
Block Frequency	0.783973	0.9900
Cumulative Sums	0.549331	0.9850
Runs	0.605916	0.9800
Longest-Run	0.432672	0.9950
Rank	0.783973	0.9900
FFT	0.366918	0.9900
Universal	0.319084	0.9800
Apen	0.585209	0.9975
Serial	0.968128	0.9925
Linear-Complexity	0.978072	0.9875

4. Conclusion

In this work, we introduce a novel dual entropy core discrete time chaos based true random number generator architecture, which can enhance the randomness of the generated bitstream using hardware redundancy. We have chosen the *Bernoulli* map as the entropy core, which has limited entropy due to its single *Lyapunov* exponent. We developed a mathematical model of dual entropy core TRNG architecture. Using numerical simulations and a practical information metric, we show that the dual entropy core TRNG can generate more randomness than a single entropy core counterpart for a wide range of the chaos control parameter set. A proof of concept dual entropy core TRNG is designed and implemented on a switched capacitor technology based FPAA integrated circuit. Acquired bitstream successfully passed all NIST 800.22 statistical tests. Proposed architecture can be used to improve the randomness performance of 1D chaotic map based TRNGs.

5. References

[1] H. Bock, M. Bucci, and R. Luzzi, “An offset-compensated oscillator-based random bit source for security applications,” in *Cryptographic Hardware and Embedded Systems - CHES 2004*, vol. 3156, pp. 27–83, Springer Berlin / Heidelberg, 2004.

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

[3] M. Jessa and M. Jaworski “Enhancing the Randomness of a Combined True Random Number Generator Based on the Ring Oscillator Sampling Method,” *Proceedings of the 2011 International Conference on Reconfigurable Computing and FPGAs (RECONFIG ’11)*,IEEE Computer Society, Washington, DC, USA, pp.274–279, 2011.

[4] J. P. Murphy, “Field-programmable true random number generator,” *Electronics Letters,* vol.48, no.10, pp.565–566, May 10 2012.

[5] Markettos, A.T., Moore, S.W. “The Frequency Injection Attack on Ring-Oscillator-Based True Random Number Generators.” *In: Clavier, C., Gaj, K. (eds.) CHES 2009. LNCS*, vol. 5747, pp. 317–331. Springer, Heidelberg (2009).

[6] J. P. Eckmann and D. Ruelle, “Ergodic theory of chaos and strange attractors”, *Reviews of Modern Physics*, 57 (3, part 1): pp. 617–656, 1985.

[7] M.E. Yalcin, J. A. K. Suykens and J. Vandewalle, “True random bit generation from a double-scroll attractor,” *IEEE Transactions on Circuits and Systems I,* vol. 51, no. 7, pp. 1395–1404, 2004.

[8] V. Tavas *et al.*, “Integrated cross-coupled chaos oscillator applied to random number generation,” *IET Circuits Devices Syst.* vol. 3, no. 1, pp. 1–11, 2009.

[9] T. Stojanovski, J. Pihl and L. Kocarev,“Chaos-based random number generators. Part II: practical realization,” *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,* vol. 48, no. 3, pp. 382–385, 2001.

[10] F. Pareschi, G.S. and R. Rovatti,“A Fast Chaos-based True Random Number Generator for Cryptographic Applications” in *Proc. IEEE 32nd European Solid-State Circuits Conference, ESSCIRC 2006* pp. 130-133, Sep. 2006

[11] O. Katz, D. A. Ramon and I. A. Wagner,“A Robust Random Number Generator Based on a Differential Current-Mode Chaos,” *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on,* vol.16, no.12, pp.1677-1686, Dec. 2008

[12] Y. B. Pesin, “Characteristic Lyapunov exponents and smooth ergodic theory,” *Russian Math. Surveys* 32 (4): 55–114, 1977.

[13] M. R. Titchener, “Deterministic computation of complexity, information and entropy,” *Proceedings of 1998 IEEE International Symposium on Information Theory*, pp.326, 1998.

[14] R. Steuer, W. B. Ebeling and M. R. Titchener, “Partition based entropies of dynamic and stochastic maps,” *Stochastics and Dynamics*, vol. 1, no. 1, pp. 45–61, 2001.

[15] Anadigm, “The AN231E04 dpASP Dynamically Reconfigurable Analog Signal Processor,” AN231E04 Datasheet, Rev. 1.1

[16] A. Rukhin. et. al., “A statistical test suite for random and pseudo random number generators for cryptographic applications,” http://csrc.nist.gov/rng/SP800-22b.pdf, May 2001, nIST 800-22.