On the Short-Term Predictability of Fully Digital Chaotic Oscillators for Pseudo-Random Number Generation

Ahmed G. Radwan[1], Abhinav S. Mansingka[2], Mohammed A. Zidan[2], Khaled N. Salama[2]
[1]Engineering Mathematics Department, Faculty of Engineering, Cairo University, Giza, Egypt
[2]Electrical Engineering Program, King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia
E-mail: agradwan@ieee.org, khaled.salama@kaust.edu.sa

Abstract— This paper presents a digital implementation of a 3rd order chaotic system using the Euler approximation. Short-term predictability is studied in relation to system precision, Euler step size and attractor size and optimal parameters for maximum performance are derived. Defective bits from the native chaotic output are neglected and the remaining pass the NIST SP. 800-22 tests without post-processing. The resulting optimized pseudo-random number generator has throughput up to 17.60 Gbits/s for a 64-bit design experimentally verified on a Xilinx Virtex 4 FPGA with logic utilization less than 1.85%.

***Keywords*— Chaos; nonlinear systems; digital circuits; pseudo random number generator (PRNG); NIST.**

I. INTRODUCTION

Good hardware pseudo-random number generators (PRNGs) remain critical for applications [1] and should necessarily have high throughput and low area with good statistical properties and unpredictability. Chaos theory is thus considered attractive for many recent applications and especially PRNG implementations due to the high sensitivities within system dynamics [1]-[16]. The digital realizations of the 1D discrete chaotic maps presented in [2],[3] are slow and large due to multiplication and have only one dimensional output. Numerically solved multidimensional continuous-time chaotic systems [4], [5] eliminate such drawbacks, provide multiple outputs and also have multiplier-free architectures.

This paper introduces the digital implementation of a known 3rd order chaotic system introduced in [6] and studies the dependence of the short-term predictability on the system precision, Euler step size and attractor size. Optimum parameters are derived that exhibit short-term predictability are minimized. High-significance statistically defective bits are discarded and the resulting PRNG is experimentally verified with logic utilization of less than 1.85% on a Xilinx Virtex 4 FPGA and 138 bits that pass all NIST SP.800-22 tests [7] without post-processing.

This paper is organized as follows: Section II illustrates the digital realization of the chaotic generator, and the short-term predictability is presented in section III. The details of the optimal hardware implementation and the experimental results are discussed in section IV and V, then the conclusion.

II. FULLY DIGITAL CHAOS GENERATOR

A. Digital Realization

The 3rd order chaotic system is described as follows:

$$\dot{Z} = \ddot{Y} = \dddot{X} = J(X, Y, Z) \quad (1a)$$

$$J(X, Y, Z) = -0.25Z - 0.5Y + 0.25|X| - D \quad (1b)$$

where D controls attractor size [3]. The Euler approximation (with step size $h = 2^{-k}$) is applied:

$$X_{t+h} = X_t + hY_t \quad (2a)$$

$$Y_{t+h} = Y_t + hZ_t \quad (2b)$$

$$Z_{t+h} = Z_t + hJ(X_t, Y_t, Z_t) \quad (2c)$$

The circuit schematic of the resulting pipelined structure is shown in Fig. 1. A fixed point two's complement format with a bus width of N_B bits for each of $\{X, Y, Z\}$ is used with N_I-bits allocated to the sign and integer part and the remaining N_F-bits to the fractional part. The function $|X|$ represents the absolute value of X and is realized by using an adder/subtractor with the most-significant bit as the carry-in. X is subtracted from D if X is positive and added otherwise to follow the ODE in (1).

B. Chaotic Response

The attractors of the output of the proposed circuit are shown in Fig.2(a)-(c). Fixed-point arithmetic and a numerical solution of the ODE cause the output to follow pseudo-chaotic trajectories [8] and verified by the positive maximum Lyapunov exponent (MLE) using [9]. The MLE was found to be $0.0519, 0.0409, 0.0396, 0.0363$ *and* 0.0331 for $N_B = 32, 40, 48, 56, 64$ with $N_F = 29, 37, 45, 53, 61$ respectively with $h = 2^{-5}$ and $D = 0.5$. The MLE is independent of D [6] and decreases with decreasing Euler step size [10] but remains positive.

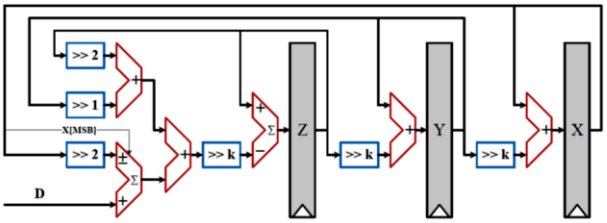

Fig. 1. Circuit diagram of the fully digital 3rd order ODE-based chaos generator with absolute value nonlinearity in X.

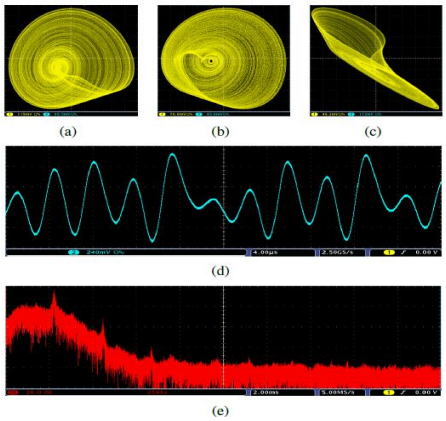

Fig. 2. Oscilloscope trace from a *Xilinx FPGA* of (a) $-Y$, (b) $Y-Z$ and (c) $Z-X$ attractors from the digital chaos generator, (d) time series of the X-variable and (e) frequency spectrum (FFT) of the X-variable.

III. DIGITAL SHORT-TERM PREDICTABILITY

The attractor shape indicates that only a subset of the digital phase space is used by the chaotic system. Furthermore, short-term predictability is clearly apparent through the output time waveforms in Fig. 2(d) and the non-uniform spectrum in Fig. 2(e). In the digital domain, short-term predictability presents statistical defects in the high-significance bits of the output as illustrated in Fig. 3.

It is dependent on N_I, the Euler step size h and the attractor size (through D). If the chaotic output is to be implemented as a PRNG, defective bits need to be discarded [4]. Defects are assessed by testing the output bits through the NIST SP. 800-22 suite. The set of high-significance bits in each of $\{X, Y, Z\}$ that fails the tests are judged defective.

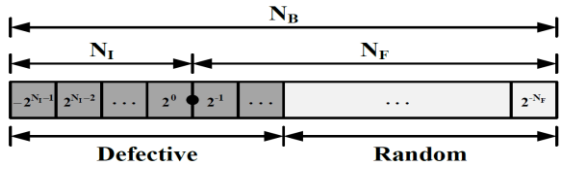

Fig. 3. Defective Bits due to short-term predictability in $\{X, Y, Z\}$

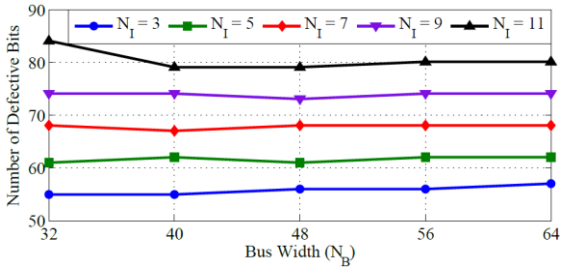

Fig. 4. No. of defective bits v/s N_B with $D = 0.5$ and $h = 2^{-5}$.

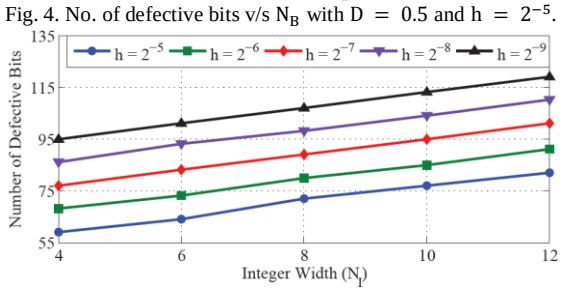

Fig. 5. Number of defective bits versus bus width for different integer widths N_I with $D = 0.5$ and h from 2^{-5} to 2^{-9}

A. *Number of Integer Bits*

Fig. 4 illustrates the number of defective bits versus N_B for different number N_I with $D = 0.5$ and $h = 2^{-5}$. For a given N_I, the number of defective bits is independent of N_F and for a given N_B, an increase in N_I correspondingly decreases N_F, increasing in the number of defective bits. The resulting design principle suggests minimizing NI to maximize the number of fast-moving low significance bits.

B. *Euler Step Size*

The Euler step size h has an upper bound such that the numerical solution accurately models the behavior of the ODE [10]. Furthermore, $h = 2^{-k}$ is required for hardware optimization. Fig. 5 shows number of defective bits versus N_I for different values of h with $N_B = 64$ and $D = 0.5$. Analysis indicates that higher Euler step sizes correspond to fewer defective bits simply because there are more truncation nonlinearities and thus greater randomness. Furthermore, the effect of different N_I and the Euler step size h are independent as shown in Fig. 4 and Fig. 5.

C. *Size of the Attractor*

The parameter D controls attractor size and has a minimum value necessary for chaos [6]. In this case, the lower bound is $D \approx 0.22$. The upper bound is limited by the size of the available phase space (specified by N_I). The effect of different D is shown in Fig. 6 (a)-(c) where the $X-Y$ attractor increases in size for increasing D. Fig. 7 plots max $(|X|, |Y|, |Z|)$ versus D that result in a linear relationship:

$$\max(|X|, |Y|, |Z|) \approx 10.45D \quad (3)$$

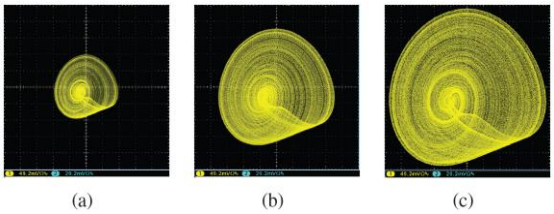

Fig. 6. Same scale oscilloscope trace from a Xilinx FPGA of $X-Y$ attractors with (a) $D = 1.375$, (b) $D = 2.5$ and (c) $D = 3.375$.

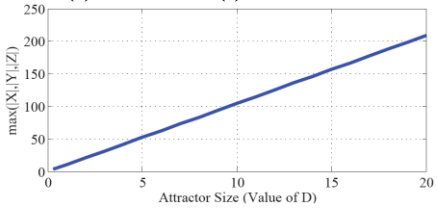

Fig. 7. Maximum absolute value of $\{X, Y, Z\}$ for D from 0.3 to 20.

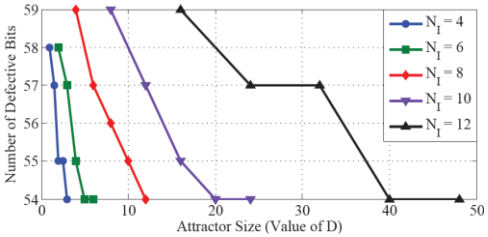

Fig. 8. Number of defective bits versus value of D for different N_I with $N_B = 32$ and $h = 2^{-5}$. D is valued such that the resulting attractor is guaranteed to be bounded within the phase space defined by each N_I.

Fig. 8 shows the number of defective bits against the value of D for different N_I with $N_B = 32$ and $h = 2^{-5}$, indicating that the best result is achieved with a value of D that maximizes the use of phase space, irrespective of the integer width. Therefore, this parameter should be optimized in conjunction with the integer width such that true optimality can be attained from (4) for a given integer width N_I,:

$$D_{opt} \approx \frac{2^{N_I-1}}{10.45} \tag{4}$$

Note that the value D should be rounded to the available precision of the fixed-point implementation and should always be kept lower than the optimal value to ensure the absence of arithmetic overflow.

IV. OPTIMAL HARDWARE IMPLEMENTATION

Based on the analysis, minimizing short-term predictability requires: (a) The highest possible Euler step size and (b) optimizing attractor size to fully utilize the phase space. This maximizes PRNG throughput of a given chaotic system by minimizing defective bits. In such cases, the integer width should simply be minimized such that phase space utilization is maximized. For this particular system, the resulting optimal values are $N_I = 3, h = 2^{-5}$ and $D = 0.37510 = 0.0112$ for which the top 18 bits in each of $\{X, Y, Z\}$ are defective.

Note that $D_{opt} \approx 0.383$ but the implemented value is lower to avoid overflow and is finite in binary. Determining N_B requires accounting for the hardware and performance. Using a Xilinx Virtex 4 XC4VSX3 FPGA (30,720 LUTs and 30,720 FFs), a simple figure of merit (FOM) is defined as:

$$\text{FOM} = \frac{\text{Throughput}}{\text{Area}} = \frac{N_{PRNG} \times f_{CLK}}{8 \times (\text{LUT} + \text{FF})} \tag{5}$$

where the throughput of the PRNG is the product of the clock frequency f_{CLK} (in MHz) and the number of PRNG bits N_{PRNG}. The denominator approximates a gate count using the number of look-up-tables (LUTs) and flip-flops (FFs) utilized on the FPGA. For the given parameters, the figure of merit is shown against the bus width in Fig. 9, wherein the optimal bus width N_B is found to be 64 bits. The sensitivity to initial conditions is a well-known phenomenon in chaos [6] exampled by a positive MLE, thus $\{X0, Y0, Z0\}$ are the PRNG seed values and cannot be the equilibrium points:

$$\dot{Z} = \dot{Y} = \dot{X} = 0 \tag{6a}$$

$$X^* = \pm 4D, Y^* = 0, Z^* = 0 \tag{6b}$$

Given the parameters of the optimized chaos generator, if $(X, Y, Z) = (\pm 1.5, 0, 0)$, the PRNG would be stationary at those points and thus should specifically be excluded. Furthermore, the sensitivity is dictated by the Euler step size, wherein the different between two initial conditions must be sufficiently large to overcome truncation error. Any changes in the 5 least significant bits may be suppressed and thus only the top 59-bits should be considered. Therefore, the seed value for the optimum generator is 177-bits wide.

TABLE I: STATISTICS OF THE ABSOLUTE VALUE OF CROSS-CORRELATION COEFFICIENTS BETWEEN INDIVIDUAL PRNG BITS

Maximum	Minimum	Mean	Median	Std. Deviation
0.0073	1.34×10^{-8}	0.0011	0.0010	0.0009

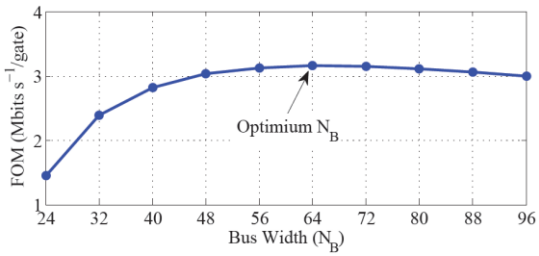

Fig. 9. Figure of merit as a function of bus width. $N_B = 64$ is optimal.

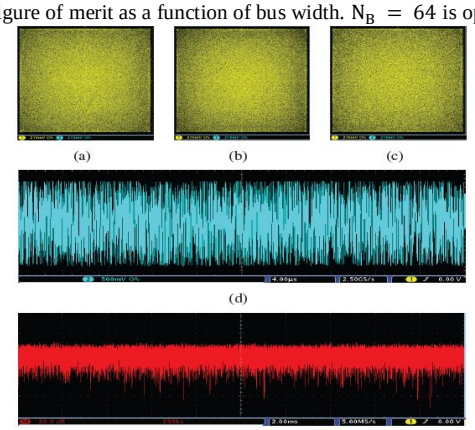

Fig. 10. Experimental results of (a) $X - Y$, (b) $Y - Z$ and (c) $Z - X$ attractors, (d) time series of the X-variable and (e) frequency spectrum (FFT) of the X-variable after truncating statistically defective bits.

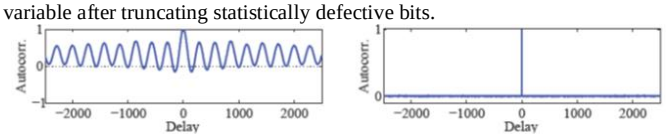

Fig. 11. Autocorrelation functions before and after truncation of defective bits for X.

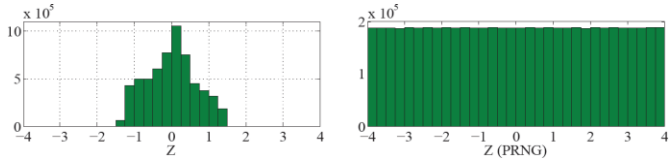

Fig. 12. Histograms of Z variable before and after the truncation of defective bits.

V. EXPERIMENTAL RESULTS

The chaotic system is implemented using the optimized parameters, the 18 most-significant bits from each of $\{X, Y, Z\}$ are discarded and the remaining are concatenated together to form a PRNG. Fig. 10 depicts the $X - Y - Z$ phase plots after truncation of defective bits in which values are seen to be uniformly distributed unlike the output time series and spectrum of X from Fig. 2.

This is also reflected in the autocorrelation functions of each of the output Z shown before and after truncation in Fig. 11. The high correlation in the native chaos is suppressed to give a favorable delta-like autocorrelation function necessary for good PRNGs. Furthermore, Table I summarizes the statistical results of the absolute value of cross-correlation coefficient for each bit with every other bit after truncation of defective bits.

The cross-correlations do not exceed 0.0073, indicating that the bits are reasonably uncorrelated. Statistical improvements are further expressed through the histograms of each of the three outputs before and after truncation, shown in Fig. 12. The

truncation effectively suppresses biases that inherent to the chaotic attractor and gives desirable uniformly distributed output. The $NIST\ SP.800-22$ test [13] results in Table II utilize 6,000,000 iterations of the native output from the 64-bit system and the corresponding truncated output. Each output bit is individually assessed for statistical properties. Given that all the output bit-streams are reasonably uncorrelated from Table I, the full 138 bits $PRNG$ bits can be used. The short-term predictability can be detected from the NIST data as shown in Table II. Statistical properties are enhanced after eliminating defective bits with full passage of all tests. The experimental results on a Xilinx Virtex 4 FPGA are also provided in Table II, indicating logic utilization less than 1.85%, flip-flop utilization less than 0.63% and PRNG throughput up to 17.60 Gbits/s. Table III compares this work against other chaos-based PRNGs using $Gc = 8 \times (LUT + FF)$ for our work as with the FOM. Minimization of defective bits enables high efficiency PRNG throughput, surpassing previous work. Furthermore, an ASIC implementation should give much better performance than this FPGA implementation.

VI. CONCLUSION

This paper discussed the short-term predictability of a 3rd order chaotic system against system precision, Euler step size and attractor size to maximize performance. In general, the maximum possible Euler step size with the minimum possible integer width maximizes phase space utilization. This system-independent optimization technique can be easily applied to other digital chaotic systems. The optimal PRNG from a 64-bit implementation is obtained by truncating the defective high-significance bits, yielding a 138-bit PRNG that passes the NIST $SP.800-22$ tests without post-processing with throughput up to 17.60 Gbits/s, logic utilization less than 1.85% and flip-flop utilization less than 0.63% experimentally verified on a Xilinx Virtex 4 FPGA. This provides throughput 3x greater than the best previous chaos-based PRNG at roughly half the area.

TABLE II : NIST SP. 800-22 TEST RESULTS AND EXPERIMENTAL RESULTS ON A XILINX VIRTEX 4 FPGA FOR THE NATIVE 64 –BIT SYSTEM AND CORRESPONDING TRUNCATED OUTPUT AS PRNG

NIST SP. 800-22 Results				
	Original		**PRNG**	
	PV	**PP**	**PV**	**PP**
Monobits	×	**0.73**	√	**0.99**
Block Frequency	×	**0.74**	√	**0.99**
Cumulative Sums	×	**0.74**	√	**0.99**
Runs	×	**0.74**	√	**0.99**
Longest Run	×	**0.71**	√	**0.98**
Rank	×	**0.74**	√	**0.99**
Fast Fourier Transform	×	**0.72**	√	**0.96**
Non-Overlapping Template	×	**0.72**	√	**0.99**
Overlapping Template	×	**0.72**	√	**1.00**
Universal	×	**0.72**	√	**0.99**
Approximate Entropy	×	**0.69**	√	**0.96**
Random Excursions	√	**0.99**	√	**0.99**
Random Excursions Variant	√	**1.00**	√	**1.00**
Serial	×	**0.70**	√	**0.97**
Linear Complexity	×	**0.74**	√	**0.99**
Experimental Results on the Xilinx Virtex 4 FPGA				
Total LUTs (out of 30,720)	**505**		**505**	
Total FFs (out of 30,720)	**192**		**192**	
Bits/Cycle	**192**		**138**	
Frequency [MHz]	**127.52**		**127.52**	
Throughput [Gbits/s]	**24.48**		**17.60**	

TABLE III : COMPARISON WITH PREVIOUSLY REPORTED PRNGS

System		**Area (Gc)**	**Thr. (Mb/s)**	**FOM**	**NIST**
Addabbo,2007[3]	Renyi Map	3988	200	0.05	Pass
Chen, 2010 [14]	Log. Map	9622	200	0.02	Pass
Li, 2010 [15]	Log. Map	9136	200	0.02	Pass
Chen, 2010 [17]	Log. Map	31655	3200	0.10	Pass
Zidan, 2011 [4]	ODE	2464	1180	0.48	Pass
Li, 2012 [2]	Log. Map	11903	6400	0.54	Pass
This Work	**ODE**	**5576**	**17598**	**3.16**	**Pass**

REFERENCES

[1] M. Delgado-Restituto and A. Rodriguez-Vazquez, "Integrated chaos generator," Proc. IEEE, 2002, 90, (5), pp. 747–767.

[2] C.-Y. Li, Y.-H. Chen, T.-Y. Chang, L.-Y. Deng, and K. To, "Period extension and randomness enhancement using high-throughput reseeding-mixing PRNG," IEEE Trans. Very Large Scale Integr. (VLSI) Syst., 2012, 20, (2), pp. 385–389.

[3] T. Addabbo, M. Alioto, A. Fort, A. Pasini, S. Rocchi, and V. Vignoli, "A class of maximum-period nonlinear congenital generators derived from the Renyi chaotic map," IEEE Trans. Circuits Syst. I: Reg. Papers, 2007, 54, (4), pp. 816–828.

[4] M. A. Zidan, A. G. Radwan, and K. N. Salama, "Random number generation based on digital differential chaos," Proc. IEEE Int. Midwest Symp. Circuits Syst. (MWSCAS), 2011, pp. 1–4.

[5] M. A. Zidan, A. G. Radwan, and K. N. Salama, "The effect of numerical techniques on differential equation based chaotic generators," Proc. Int. Conf. Microelectronics (ICM), 2011, pp. 1–4.

[6] J. C. Sprott, "A new class of chaotic circuit," Physics Lett. A, 2000, (266), pp. 19–23.

[7] A. Rukhin, J. Soto, M. Smid, E. Barker, S. Leigh, M. Levenson,M. Vangel, D. Banks, A. Heckert, J. Dray, S. Vo, and L. E. Bassham, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST Special Publication 800-22, 2010.

[8] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of piecewise linear chaotic maps," Int. J. Bifurcation Chaos, 2005, 15,(10), pp. 3119–3151.

[9] A. S. Mansingka, A. G. Radwan, M. A. Zidan, and K. N. Salama, "Analysis of bus width and delay on a fully digital signum nonlinearity chaotic oscillator," Proc. IEEE Int. Midwest Symp. Circuits Syst. (MWSCAS), 2011, pp.1–4.

[10] A. S. Mansingka, A. G. Radwan, and K. N. Salama, "Design, implementation and analysis of fully digital 1-D controllable multiscroll chaos," Proc. Int. Conf. Microelectronics (ICM), 2011, pp. 1 – 4.

[11] M. A. Zidan, A. G. Radwan, and K. N. Salama: 'Controllable v-shape multiscroll butterfly attractor: system and circuit implementation', Int. J. Bifurcation Chaos, 2012, 22, (6), pp. 1250143-1250156

[12] M. L. Barakat, A. G. Radwan, and K. N. Salama: 'Hardware realization of chaos-based block cipher for image encryption', Proc. Int. Conf. Microelectronics (ICM), 2011, pp. 1 – 4.

[13] B. M. Gammel, R. Gottfert, and O. Kniffler, "An nlfsr-based stream cipher," Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), 2006, pp. 2917–2920.

[14] S.-L. Chen, T. Hwang, and W.-W. Lin, "Randomness enhancement using digitalized modified logistic map," IEEE Trans. Circuits Syst. II: Exp. Briefs, 2010, 57, (12), pp. 996–1000.

[15] C.-Y. Li, T.-Y. Chang, and C.-C. Huang, "A nonlinear PRNG using digitized logistic map with self-reseeding method," Proc. IEEE Int. Symp. VLSI Design, Automation Test (VLSI-DAT), 2010, pp. 108–111.

[16] A. S. Mansingka, M. A. Zidan, M. L. Barakat, A. G. Radwan, K. N. Salama, "Fully Digital Jerk-Based Chaotic Oscillators for High Throughput Pseudo Random Number Generators up to 8.77 Gbits/s," Microelectronics Journal, 2013

[17] S.-L. Chen, T. Hwang, S.-M. Chang, and W.-W. Lin, "A fast digital chaotic generator for secure communication," Int. J. Bifurcation and Chaos, 2010, 20, (12), pp. 1–19.