

# Generalized Hardware Post-processing Technique for Chaos-Based Pseudorandom Number Generators

Mohamed L. Barakat, Abhinav S. Mansingka, Ahmed G. Radwan, and Khaled N. Salama

This paper presents a generalized post-processing technique for enhancing the pseudorandomness of digital chaotic oscillators through a nonlinear XOR-based operation with rotation and feedback. The technique allows full utilization of the chaotic output as pseudorandom number generators and improves throughput without a significant area penalty. Digital design of a third-order chaotic system with maximum function nonlinearity is presented with verified chaotic dynamics. The proposed post-processing technique eliminates statistical degradation in all output bits, thus maximizing throughput compared to other processing techniques. Furthermore, the technique is applied to several fully digital chaotic oscillators with performance surpassing previously reported systems in the literature. The enhancement in the randomness is further examined in a simple image encryption application resulting in a better security performance. The system is verified through experiment on a Xilinx Virtex 4 FPGA with throughput up to 15.44 Gbit/s and logic utilization less than 0.84% for 32-bit implementations.

**Keywords:** Chaos, pseudorandom number generator, post-processing, FPGA.

Manuscript received Oct. 5, 2012; revised Nov. 30, 2012; accepted Dec. 10, 2012.

Mohamed L. Barakat (phone: +20 11 1300 2330, mohamed.barakat@kaust.edu.sa), Abhinav S. Mansingka (abhinav.mansingka@kaust.edu.sa), and Khaled N. Salama (khaled.salama@kaust.edu.sa) are with the Electrical Engineering Program, King Abdullah University of Science and Technology, Thuwal, Kingdom of Saudi Arabia.

Ahmed G. Radwan (corresponding author, agradwan@ieee.org) is with the Department of Engineering Mathematics, Cairo University, Giza, Egypt, and also with the Nanoelectronics Integrated Systems Center (NISC), Nile University, Egypt.

<http://dx.doi.org/10.4218/etrij.13.0112.0677>

## I. Introduction

Pseudorandom number generators (PRNGs) have increasingly become crucial components in communication systems, cryptography, and stochastic simulations [1]-[4]. With a deterministic yet unpredictable nature, chaos-based PRNGs (CB-PRNGs) implement a chaotic equation that produces randomized symbols when initialized by a seed. Many CB-PRNGs have been digitally realized using chaotic maps [5]-[8] and recently using the numerical solution of differential equations [9], [10], while other chaos-based true random bit generators have also been proposed [11]. Digital design provides several benefits over analog implementation in terms of area efficiency, repeatability, portability, power consumption, and integrability with IC technology [12]. The performance of PRNGs is evaluated on the basis of period length, unpredictability, and other statistical properties. Digital CB-PRNGs suffer from serious dynamical degradations due to quantization errors and finite representation of system states, including loss of ergodicity and shorter pseudo-orbits [13].

Nevertheless, digital implementation of CB-PRNGs, area efficiency, and high throughput strongly motivate researchers to create an effective post-processing technique to overcome statistical flaws in the output. The Von Neumann technique [14], XOR correctors [15], [16], truncation of defective bits [10], hash-function post-processing [12], [17], and linear code correctors [18], [19] are examples of well-known solutions that overcome bias and enhance random properties of PRNGs. While most previous solutions can solve statistical defects, none of them preserve the raw RNG throughput and some

incur a huge hardware overhead.

This paper introduces the first digital implementation of a third-order jerk chaotic system with maximum function nonlinearity, previously realized in an analog form in [20]. A positive maximum Lyapunov exponent (MLE) of 0.1362 confirms chaotic dynamics. A generic nonlinear XOR-based post-processing technique with rotation and feedback is introduced to suppress short-term predictability and maximize RNG throughput from the proposed chaotic system with low hardware cost. The new technique is evaluated against known techniques and shows superior performance, enabling full utilization of all output bits as a CB-PRNG, successfully passing all NIST SP. 800-22 tests. Furthermore, the technique is applied to four different chaotic oscillators to prove its generalized effect, resulting in the same enhancement of randomness. The maximum nonlinearity system is verified on a Xilinx Virtex 4 FPGA, and the processed CB-PRNG output is applied in a simple image encryption system and shows improved security results compared to the native chaos.

## II. Fully Digital Chaos Generator

### 1. Digital Realization

Although hardware implementation of low-complexity chaotic maps is simple [21], [22], multiplier-free differential equation-based chaotic systems can achieve higher throughput while occupying the lower hardware area. The third-order chaotic system adopted in this work employs the max comparison function as the primary nonlinear function and is described by the following set of first-order ordinary differential equations (ODEs) [20]:

$$\dot{X} = Y, \quad \dot{Y} = Z, \quad \dot{Z} = -0.5Z - Y - 8\max(X, 0) + 0.5. \quad (1)$$

The equilibrium point of the system is determined at  $(\dot{X}, \dot{Y}, \dot{Z}) = (0, 0, 0)$ . This produces  $Y=0$ ,  $Z=0$ , and  $8\max(X, 0)=0.5$ , giving the equilibrium point at  $(X^*, Y^*, Z^*) = (0.0625, 0, 0)$ . The Jacobian ( $J$ ) and its trace (sum of the diagonal terms) at the equilibrium point are given as

$$J = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -8 & -1 & -0.5 \end{bmatrix}, \quad \text{trace}(J) = -0.5. \quad (2)$$

A negative trace indicates a dissipative chaotic flow, while the eigenvalues of the chaotic system at the equilibrium point are the roots of the characteristic equation derived from  $J$ :

$$s^3 + 0.5s^2 + s + 8 = 0 \Rightarrow s = \left(-2, \frac{3 \pm i\sqrt{55}}{4}\right). \quad (3)$$

One negative real eigenvalue and a complex conjugate pair

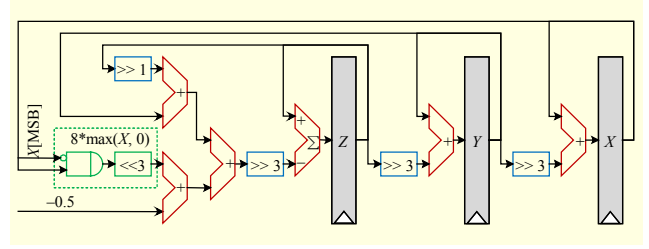


Fig. 1. Circuit diagram of fully digital third-order ODE-based chaos generator with maximum function nonlinearity in  $X$ .

of eigenvalues with a positive real part indicate a *saddle point of index 2*, suggesting a chaotic attractor [23]. The seed  $\{X_0, Y_0, Z_0\}$  can be arbitrarily chosen so long as  $\{0.0625, 0, 0\}$  is avoided. This system is digitally implemented on hardware for the first time by realizing the numerical solution of the ODE. The Euler, Runge-Kutta, and midpoint methods are well-known numerical techniques for solving ODEs. The Euler approximation is adopted in this work, as it produces the best chaotic response, occupies the lowest area, and provides the highest throughput [24]. The step size is fixed to be  $h=2^{-3}$ , the highest possible value to provide the greatest nonlinearity [25], resulting in a nonlinear feedback pipeline [26]:

$$X_{t+h} = X_t + hY_t, \quad Y_{t+h} = Y_t + hZ_t, \quad Z_{t+h} = Z_t + hJ(X_t, Y_t, Z_t). \quad (4)$$

The circuit schematic of the numerical solution is shown in Fig. 1. A fixed point two's complement format is used with 5 bits allocated to the sign and integer part and the remaining to the fractional part. As shown in (1), all constants and the Euler step size have been optimized to powers of 2 to simplify scalar multiplications to arithmetic shifts. The function  $\max(X, 0)$  is calculated by performing a bitwise AND operation on every bit of  $X$  with the inverse of the most significant bit (MSB). This in effect yields the output as zero whenever  $X$  is negative and  $X$  otherwise, thus giving the appropriate functionality. For an  $N$ -bit implementation, the total component requirement is 5  $N$ -bit adders, 1  $N$ -bit subtractor, 3  $N$ -bit registers, and  $N$  2-input AND gates. The system has three outputs  $\{X, Y, Z\}$ , each of which is  $N$ -bit wide, constituting a total of  $3N$  output bits.

### 2. Chaotic Response

The attractors ( $X$ - $Y$ - $Z$  phase plots) of the proposed circuit output are depicted in Fig. 2, showing excellent correspondence with the analog attractor in [20]. Phase space boundedness is a necessary but insufficient condition to indicate chaos. Chaotic attractors in general are full of periodic trajectories [27]; however, they are unstable and the probability to completely trace a periodic orbit is zero. Nevertheless, finite fixed point representations adopted in a digital realization of chaotic systems cause the output to always follow effectively periodic

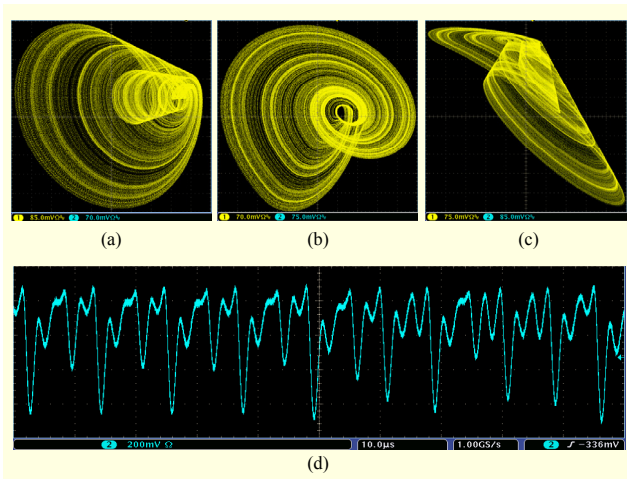


Fig. 2. Experimentally obtained attractors (a)  $X$ - $Y$ , (b)  $Y$ - $Z$ , and (c)  $Z$ - $X$ , from digital chaos generator. (d) Time series output of  $X$ . Results are drawn on oscilloscope from Xilinx Virtex 4 FPGA.

trajectories that are pseudochaotic [13] and approximate the true chaotic trajectories of the ODE.

However, a positive MLE for the output time series indicates the presence of chaotic dynamics. Given an arbitrary change in initial conditions, the MLE theoretically approximates the long-term divergence in the solution by  $\delta S(t) \approx e^{\lambda t} S(\delta t)$ , with a positive MLE confirming the existence of chaos. While this technique only applies to chaotic systems defined over continuous phase spaces, the software package developed in [28] enables the calculation of the MLE from a time series of discrete data and thus treats the digital output as if it were sampled from a truly chaotic source. Using a 32-bit implementation, the MLE is found to be 0.1362. While it has been shown that the MLE of such systems decreases with increasing system precision due to lower truncation nonlinearities [26], it remains positive and is thus sufficient to indicate chaos.

### III. Nonlinear Post-processor

The MSBs are the primary contributors in constructing the attractor shape illustrated in Fig. 2. Consequently, they have slower transition rates compared to the least significant bits (LSBs) and thus cause short-term predictability to be apparent in all chaotic systems [29]. In the digital context, this creates an uneven distribution of pseudorandomness across the output bits. The MSBs are not only biased but also highly correlated, while the LSBs show desirable statistical randomness. This makes a strong case for efficient post-processing to correct the flaws and ensure that the entire output has statistically random properties. XOR-based correctors are efficient solutions to remove statistical bias with a controllable hardware cost, according to

the following [30]:

$$E(X \oplus Y) \approx \frac{1}{2} - 2(\mu - \frac{1}{2})(\nu - \frac{1}{2}) - \frac{1}{2}\rho, \quad (5)$$

where  $X$  and  $Y$  are independent random variables with  $E(X)=\mu$  and  $E(Y)=\nu$  denoting expectation values and  $\rho$  denoting the correlation between  $X$  and  $Y$ . Assuming that  $X$  represents an ideal random variable ( $\mu=0.5$ ) and  $Y$  is a variable loaded with bias ( $\nu \neq 0.5$ ), the expression indicates that the XOR operation gives a result with lower bias ( $E(X \oplus Y) \approx 0.5$ ), provided that the correlation is low ( $\rho \approx 0$ ).

### 1. Proposed Technique

The proposed post-processor uses a subset of the random bits (low significance) to suppress the bias in the nonrandom bits (high significance) through a nonlinear XOR operation with rotation and feedback. Such random bits are statistically independent by the nature of the chaotic dynamics similar to noise. Compared to the solution of the ODE, adding noise to the MSBs creates large deviations, which emulate the instability in the original chaotic trajectories, resulting in a random walk process in the discrete time [31]. The post-processing steps are described below.

**Detection of Random Bits.** The NIST SP. 800-22 test suite [32] is used as a reference to assess statistical characteristics of the output bitstreams, each of which is isolated and examined. Bitstreams that fail NIST tests are judged to be generated at defective bit locations. From a digital implementation perspective, the number of defective bits in a bus of width  $N$  depends on the following: 1) the number of integer bits in the fixed point representation, 2) the Euler step size, and 3) the system characteristics, all of which are held constant here. As expected, a set of highly significant bits in the  $X$ ,  $Y$ , and  $Z$  outputs of the generator is verified to be statistically defective.

**Bit Location Permutation.** Assume that output branches  $\{X, Y, Z\}$  are corrected to the corresponding outputs, that is,  $\{U, V, W\}$ , respectively, after applying the post-processing. Within a single branch, let the number of statistically defective highly significant bits be  $\beta$ , and let the total bus width be  $N$ . In the

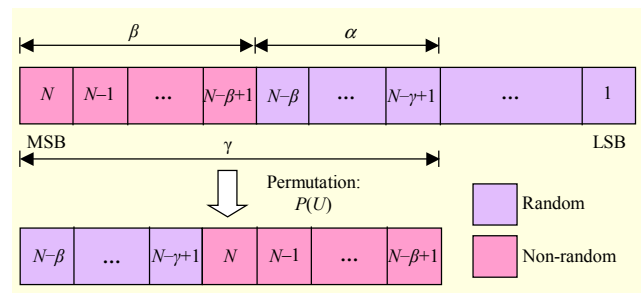


Fig. 3. Representation of proposed bit location permutation.

proposed technique, the defective bits are overlapped, partially or fully, with  $\alpha$  statistically random bits from the same branch. The resulting bus of width  $\gamma=\alpha+\beta$  is rotated right by  $\beta$ , creating a permutation  $P$ . This operation is illustrated in Fig. 3 and is described as follows, where  $B$  is bit position and  $U$  represents a bus of width  $N$ :

$$P(U[B]) = \begin{cases} U[B-\beta], & B \in (N-\alpha, N), \\ U[B-\alpha], & B \in (N-\gamma, N-\alpha). \end{cases} \quad (6)$$

**Feedback and XORing.** The output  $U$  is delayed one cycle, permuted, fed back, and bitwise XORed with the corresponding un-rotated bits of the native output from the current cycle, described as follows:

$$U_i[B] = \begin{cases} X_i \oplus P(U_{i-1}[B]), & B \in (N-\gamma, N), \\ X_i[B], & B \in (1, N-\gamma), \end{cases} \quad (7)$$

where  $\{X_i\}$  represents the  $N$ -bit native chaotic output,  $\{U_i\}$  represents the  $N$ -bit post-processed output,  $P(U_{i-1})$  represents the permutation described in (6) and Fig. 3,  $B$  represents the bit position, and  $i$  denotes the iteration number. The resultant output bitstream from each defective bit location is linearly independent from bits constituting the operation due to the delay and feedback.

**Choosing Overlap Width.** The proposed post-processing utilizes  $\alpha$  statistically random bits to reduce the bias in the most significant  $\beta$  bits of each output branch. The correlation value  $\rho$  described in (5) is inversely proportional to the size of  $\alpha$  given the high correlation initially depicted in the MSBs of the native output. Thus, the width of  $\alpha$  is tuned such that  $\varepsilon \leq \alpha \leq \beta$ , where  $\alpha$  is the minimum number of random bits required for effective bias reduction (given  $\varepsilon \geq 1$ ). The lower bound  $\alpha$  is dependent on the following: 1) the severity of the correlation  $\rho$  in the top  $\beta$  bits, 2) system characteristics, and 3) implementation parameters. In this work, it is experimentally determined. Hardware efficiency motivates the upper bound for  $\varepsilon \leq \alpha \leq \beta$  wherein XOR operations between statistically random bits are avoided.

## 2. Circuit Implementation

The circuit schematic of the proposed technique is shown in

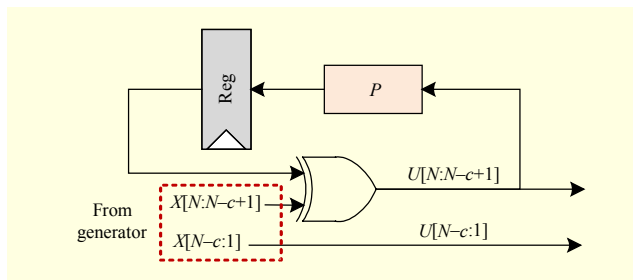


Fig. 4. Schematic of proposed post-processing circuit.

Fig. 4, where  $P$  represents (6). The permutation is implemented through a simple reordering of bit locations and requires no hardware. Total hardware utilization for the post-processor is  $\gamma$  2-input XOR gates and 1  $\gamma$ -bit register. For use with the chaos generator proposed in this paper, this circuit is replicated for each of the three outputs of the native chaotic system  $\{X, Y, Z\}$ , producing new post-processed outputs  $\{U, V, W\}$ .

## IV. Experiment Results

### 1. Output Characteristics

For the proposed chaotic generator, the defective bits in each native output  $\{X, Y, Z\}$  are verified through experiment to be  $\beta=14$ . The minimum random bits required for effective reduction of the bias is determined as  $\varepsilon=4$ . Statistical characteristics of the system output are enhanced after applying the post-processing technique. Figure 5 depicts the  $U$ - $V$ ,  $V$ - $W$ , and  $U$ - $W$  phase plots in which random values are seen to be uniformly distributed. The post-processing enables full coverage of the phase space, compared to the original attractors in Fig. 2, owing to the large

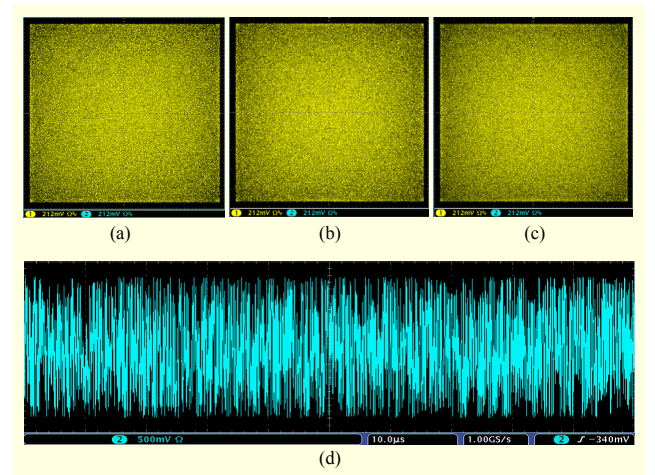


Fig. 5. Experimentally obtained attractors of (a)  $U$ - $V$ , (b)  $V$ - $W$ , and (c)  $U$ - $W$ , in addition to (d) time series output of  $U$  from the digitally implemented chaos generator. Results are drawn on oscilloscope from output of Xilinx Virtex 4 FPGA with  $\alpha=4$ .

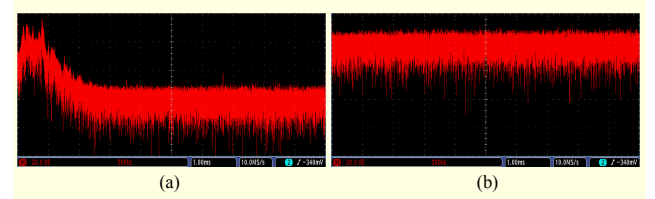


Fig. 6. Experimentally obtained FFT for (a) native  $X$  output and (b) post-processed  $U$  output with  $\alpha=4$ . Results are drawn on oscilloscope from output of Xilinx Virtex 4 FPGA.



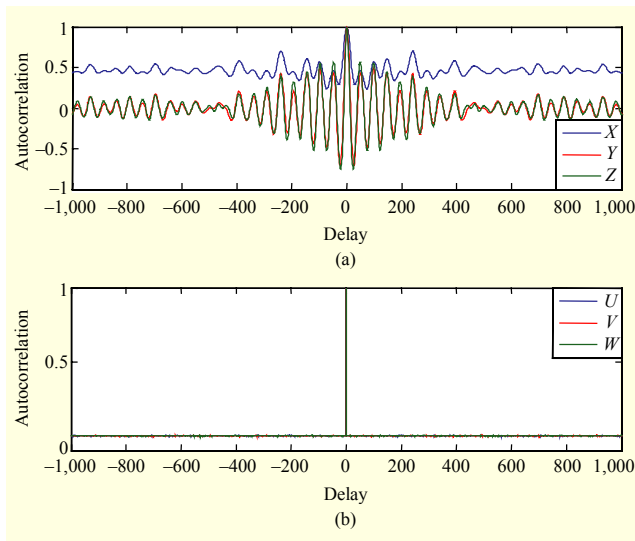


Fig. 7. Autocorrelations of (a)  $X$ ,  $Y$ , and  $Z$ , with (b)  $U$ ,  $V$ , and  $W$ .

Table 1. Crosscorrelation coefficients for original and post-processed outputs with  $\alpha=4$ .

Original			Post-processed		
$X$ - $Y$	$X$ - $Z$	$Y$ - $Z$	$U$ - $V$	$U$ - $W$	$V$ - $W$
-0.0461	-0.7479	-0.0613	-0.0006	-0.0008	0.0011

divergence in the trajectories. A comparison of the output time series of  $X$  in Fig. 2(d) and  $U$  in Fig. 5(d) reveals that short-term predictability is completely dissolved when observing the post-processed output. The FFT of the native output  $X$  and the corrected output  $U$  are shown in Fig. 6 for the complete spectrum range ( $f_s/2$ ). The figure shows that the post-processing is able to efficiently spread the signal power over the whole spectrum, giving the appearance of white noise, which is crucial for many security applications [33].

To quantitatively assess short-term predictability, the autocorrelations of  $\{X, Y, Z\}$  and  $\{U, V, W\}$  are shown in Figs. 7(a) and 7(b), respectively, with a sample size of 2,000,000. The outputs of the original chaotic system are highly correlated and therefore predictable, whereas the post-processed outputs have a favorable delta-like autocorrelation. The crosscorrelation coefficients are shown in Table 1, wherein post-processing suppresses the native crosscorrelations. These findings indicate that the proposed post-processing eliminates bias and suppresses short-term predictability, which are important characteristics for PRNGs.

## 2. Statistical Behavior

The quality of the distribution of random variables in the

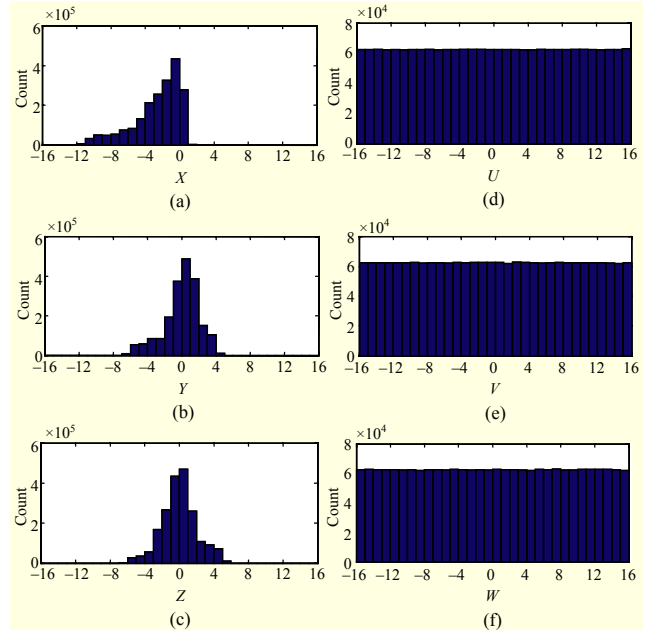


Fig. 8. Histogram of output symbols taken from (a)-(c),  $X$ ,  $Y$ ,  $Z$  native, respectively, and (d)-(f),  $U$ ,  $V$ ,  $W$  post-processed, respectively, with  $\alpha=4$ .

phase space is evaluated by analyzing the histogram of the output. Figure 8 compares the histograms of the native  $\{X, Y, Z\}$  and  $\{U, V, W\}$  outputs for 2,000,000 iterations and essentially approximates the probability density function of the respective outputs. Clearly, post-processing results in a desired uniform distribution, spreading the random values equally over the full range specified by the 5-bit integer width.

The NIST SP. 800-22 statistical test suite [32] is used to assess the properties of the system output using 2,000,000 iterations. Table 2 summarizes the NIST results for a 32-bit implementation of the original system and compares the performance of the proposed post-processing technique with Von Neumann post-processing [14], 2-bit simple XOR correction [16], and truncation of defective bits [10]. The outputs of the three states in every iteration are concatenated together into a single 96-bit sample. Results are represented by the proportion of passing sequences (PP) and the validity of the P-value distribution (PV).

Von Neumann correction examines successive non-overlapping pairs of bits from a single bitstream and produces the first bit only if the pair is different, giving a compression ratio of 4, on average. This technique has been applied through software in this paper and with variable-latency. In 2-bit simple XOR correction, pairs of bits are taken from the biased and unbiased sections of the  $N$ -bit bus (that is, bit  $N$  is compared with bit 1, bit  $N-1$  with bit 2, and so on) and XORed, giving a compression ratio of 2. Truncation simply eliminates statistically defective bits and thus does not require hardware.

**Table 2.** NIST SP. 800-22 test results and Xilinx Virtex 4 FPGA experiment results regarding area for original, Von Neumann, 2-bit XOR corrector, truncation, and proposed post-processing technique with  $\alpha=1, 2, 4, 8$ . Von Neumann implemented in software.

NIST SP. 800-22 results																
	Original		Von Neumann [14]		2-bit XOR [16]		Truncation [10]		Proposed post-processing							
									$\alpha=1$		$\alpha=2$		$\alpha=4$		$\alpha=8$	
	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP
Monobits	×	0.72	×	0.25	✓	1.00	✓	1.00	✓	1.00	✓	1.00	✓	0.99	✓	0.98
Block frequency	×	0.74	×	0.25	✓	1.00	✓	1.00	✗	0.94	✓	0.98	✓	0.96	✓	0.99
Cumulative sums	×	0.71	×	0.25	✓	0.99	✓	1.00	✓	1.00	✓	1.00	✓	0.99	✓	0.98
Runs	×	0.6	×	0.19	✓	1.00	✓	1.00	✓	1.00	✓	1.00	✓	1.00	✓	0.98
Longest run	×	0.69	×	0.25	✓	1.00	✓	0.98	✓	0.99	✓	0.99	✓	0.98	✓	0.98
Rank	×	0.85	×	0.38	✓	0.98	✓	1.00	✓	1.00	✓	0.98	✓	0.99	✓	1.00
Fast Fourier transform	×	0.72	×	0.31	✓	1.00	✓	0.98	✓	1.00	✓	0.99	✓	1.00	✓	1.00
Non-overlapping template	×	0.68	×	0.28	✓	0.99	✓	0.99	×	0.95	×	0.95	✓	0.99	✓	0.99
Overlapping template	×	0.69	×	0.23	✓	0.98	✓	1.00	✓	1.00	✓	1.00	✓	1.00	✓	0.98
Universal	×	0.71	×	0.29	✓	0.98	✓	0.98	✓	1.00	✓	0.99	✓	1.00	✓	0.98
Approximate entropy	×	0.56	×	0.23	✓	1.00	✓	0.96	✓	1.00	✓	1.00	✓	1.00	✓	0.99
Random excursion	×	0.99	✓	1.00	✓	0.99	✓	0.99	✓	0.99	✓	0.99	✓	0.99	✓	0.99
Random excursion variant	×	0.99	✓	1.00	✓	1.00	✓	1.00	✓	1.00	✓	1.00	✓	0.99	✓	0.99
Serial	×	0.57	×	0.26	✓	0.99	✓	0.99	✓	0.98	✓	0.98	✓	0.99	✓	0.99
Linear complexity	×	0.94	×	0.44	✓	1.00	✓	0.96	✓	1.00	✓	0.98	✓	1.00	✓	1.00
Final result	Fail		Fail		Pass		Pass		Fail		Fail		Pass		Pass	

XC4VVSX35-10FF668 FPGA (30,720 LUTs and 30,720 FFs) experiment results regarding area								
Total LUTs	193	193	241	193	238	241	247	259
Total flip-flops	96	96	96	96	141	144	150	162
Frequency (MHz)	160.8	160.8	160.8	160.8	160.8	160.8	160.8	160.8
Bits/cycle	96	approx. 24	48	54	96	96	96	96
Throughput (Gb/s)	15.44	3.86	7.72	8.68	15.44	15.44	15.44	15.44

The results in Table 2 show that the proposed post-processing technique provides full utilization of the entire bus width as a PRNG. In addition, the minimum value for efficient bias reduction of the statistically defective bits is verified as  $\varepsilon=\alpha=4$  with  $\beta=14$  in each of  $\{X, Y, Z\}$ .

Of particular interest is the information entropy associated with each output bit, a firm indicator of long-term unpredictability of bitstreams. For the implemented system, entropy is assessed for the entire 96-bit output for 1,000,000 iterations, using the mathematical formulation described in [32] with an order of 10. In base 2, the maximum entropy per bit is 1, for a fair coin toss. The results are shown in Fig. 9(a), wherein clearly the highly significant bits have very low entropy. In particular, the failures in the NIST tests are highlighted, indicating that a very high confidence in sufficient entropy is needed to pass the tests. Figure 9(b) shows the same

entropy graph after applying the proposed post-processing ( $\alpha=4$ ) on the original system. Entropy enhancement in highly significant bits is evident; all output bits are within 0.041% of the maximum value, and each bitstream passes the NIST tests. It is important to note that since the Von Neumann and 2-bit XOR correction techniques compress the output, only this technique allows full utilization of all output bits.

### 3. Application to Other Chaotic Oscillators

The performance of the proposed technique is evaluated for four different chaotic oscillators with different nonlinearities, that is, multiplication in Lorenz [34], modulus function in Chen [35], piecewise function in Elwakil and Kennedy [36], and the signum nonlinear function that was proposed simultaneously by Elawil and Kennedy [36] and Sprott [20]. All these systems

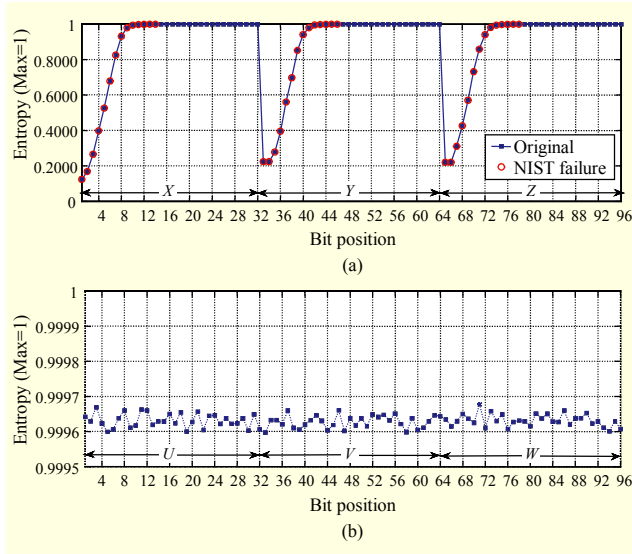


Fig. 9. Entropy of each output bitstream for (a) original system and (b) after applying proposed post-processing with  $\alpha=4$ .

were described digitally in [24], and Spratt [20] fully implemented them in [26]. Full descriptions of the tested systems along with the implementation parameters, that is, the bus width ( $N$ ), integer width ( $N_I$ ), fraction width ( $N_F$ ), Euler step size ( $h$ ), and post-processing parameters ( $\alpha$ ,  $\beta$ ), are provided in Table 3. In all cases,  $\alpha=\varepsilon$  such that hardware efficiency is maximized. Table 3 also summarizes the NIST results before and after applying the post-processing for each system. Clearly, the results verify the generalized behavior of the proposed circuit for different CB-PRNGs with randomness enhancement, full utilization of the bus width, and suppression of short-term predictability in each case.

#### 4. Area and Performance Analysis

The performance results from experiments conducted using a Xilinx Virtex 4 FPGA are provided in Table 2 for different post-processing techniques along with the original system to illustrate the hardware impact of post-processing. All systems show that logic utilization less than 0.84%, flip-flop utilization less than 0.53%, and throughput up to 15.44 Gbit/s in 32-bit implementations with the same clock frequency as post-processing is not a combinational bottleneck. To assess the scalability, a figure of merit (FOM) is devised as follows:

$$\text{FOM} = \frac{\text{Throughput}}{\text{Area}} = \frac{N_{\text{RNG}} \times f_{\text{CLK}}}{8 \times (\text{LUT} + \text{FF})}. \quad (8)$$

The numerator expresses the throughput, where  $f_{\text{CLK}}$  is the frequency of the system in MHz and  $N_{\text{RNG}}$  specifies the number of output bits per cycle utilized as RNG. The denominator approximates a gate count with LUT and FF

specifying the number of look-up tables and flip-flops used on the FPGA, respectively. The results for a range of bus widths from 24 to 64 are shown in Fig. 10. Clearly, the proposed technique is most effective if the number of overlap bits  $\alpha$  is kept to the minimum possible value (that is,  $\alpha=\varepsilon=4$  in this case). In particular, an optimal FOM of 4.86 is observed at a 32-bit implementation for  $\alpha=4$ . For very high bus widths, the FOM of the proposed post-processing becomes roughly similar to, but still greater than, the FOM of truncation. Nevertheless, post-processed systems would remain superior as they provide more throughputs in absolute terms. Critically, Von Neumann post-processing is insufficient to suppress all the bias in the system, indicated by NIST failures for all bus widths. Here, 2-bit simple XOR correction requires, at a minimum, that the number of statistically random bits be at least equal to the number of defective bits. Since  $\beta=14$  is known, 2-bit simple XOR correction only works for bus widths greater than 28, indicated by NIST failures at 16 bits, 20 bits, and 24 bits.

The FOM plots in Fig. 11 compare the bus widths from 32 to 96 for the different chaotic oscillators shown in Table 3 along with the system implemented in this paper with maximum function nonlinearity, again with  $\alpha=\varepsilon$  for hardware optimality. Clearly, the newly implemented system with maximum function nonlinearity shows the best performance while the Lorenz system shows the worst FOM, primarily due to the huge area requirement for the two  $32 \times 32$  bit multipliers. Furthermore, as the size of the system increases, the relative overhead of introducing post-processing also diminishes.

#### 5. Application in Chaos-Based Image Encryption

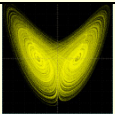
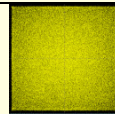
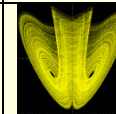

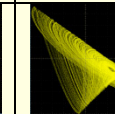
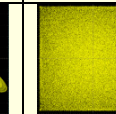
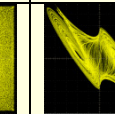
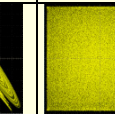
To demonstrate the effect of the quality of randomness in cryptographic applications, the generated key streams of both original and post-processed output are examined through a simple image encryption/decryption system. In general, images are prone to statistical cryptanalysis attacks due to the high correlation between adjacent pixels and the nonuniform histogram. The encryption adopted in this work is a simple encoder that directly XORs image pixels with the key stream bits generated by the chaotic oscillator. When received by the decoder, the ciphered pixels are XORed again with a key stream produced from a similar chaotic oscillator to reconstruct the original image. A grayscale image of  $1024 \times 1024$  pixels is used with a histogram, shown in Fig. 12(b). When the image is XORed with the original chaotic output, the resultant image is not effectively masked and suffers from statistical information leakage, as illustrated by the nonuniform histogram in Fig. 12(d). After applying the proposed post-processing technique, image pixels appear as noise with a uniform histogram, shown in Fig. 12(f).

**Table 3.** System descriptions, NIST SP. 800-22 results, FPGA implementation results, and oscilloscope snapshots of attractors for original output and output after proposed post-processing of Lorenz, Chen, Elwakil and Kennedy, and Sprott chaotic oscillators.

Chaotic generators				
	Lorenz [34]	Chen [35]	Elwakil and Kennedy [36]	Sprott [20]
Equations	$\dot{X} = (Y - X)$ $\dot{Y} = (2 - Z)X - Y$ $\dot{Z} = XY - 32Z$	$\dot{X} = (Y - X)$ $\dot{Y} = \text{sgn}(X)(1 - Z) + \frac{Y}{2}$ $\dot{Z} = Y - \frac{Z}{8}$	$\dot{X} = Y$ $\dot{Y} = Z$ $\dot{Z} = -Z - Y\phi(Y) - X$ $\phi(Y) = \begin{cases} 4, & Y \geq 1 \\ 0, & Y < 1 \end{cases}$	$\dot{X} = Y$ $\dot{Y} = Z$ $\dot{Z} = -\frac{Z}{2} - Y + G(X)$ $G(X) = -X - 2\text{sgn}(X)$
System nonlinearity	Multiplication	Sign, Modulus	Piecewise	Signum
$(N, N_i, N_E, h)$	$(32, 8, 24, 2^{-6})$	$(32, 5, 27, 2^{-6})$	$(32, 5, 27, 2^{-5})$	$(32, 5, 27, 2^{-5})$
Parameters $(b, \varepsilon, \alpha)$	$b = 14, \alpha = \varepsilon = 8$	$b = 20, \alpha = \varepsilon = 11$	$b = 20, \alpha = \varepsilon = 12$	$b = 24, \alpha = \varepsilon = 6$

	Native		Post-processed		Native		Post-processed		Native		Post-processed		Native		Post-processed	
	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP	PV	PP
Monobits	×	0.81	✓	1.00	×	0.67	✓	1.00	×	0.64	✓	0.99	×	0.72	✓	0.96
Block frequency	×	0.79	✓	0.97	×	0.60	✓	1.00	×	0.63	✓	0.99	×	0.64	✓	0.96
Cumulative sums	×	0.80	✓	1.00	×	0.67	✓	1.00	×	0.63	✓	0.99	×	0.72	✓	0.97
Runs	×	0.67	✓	0.97	×	0.46	✓	0.97	×	0.54	✓	0.96	×	0.51	✓	0.98
Longest run	×	0.65	✓	1.00	×	0.25	✓	1.00	×	0.43	✓	1.00	×	0.30	✓	0.96
Rank	×	0.81	✓	1.00	×	0.56	✓	1.00	×	0.67	✓	1.00	×	0.60	✓	0.98
FFT	×	0.73	✓	0.97	×	0.56	✓	0.96	×	0.63	✓	0.98	×	0.62	✓	0.97
Non-overlapping template	×	0.66	✓	0.98	×	0.19	✓	0.98	×	0.08	✓	0.98	×	0.40	✓	0.98
Overlapping template	×	0.64	✓	1.00	×	0.22	✓	0.99	×	0.40	✓	0.99	×	0.28	✓	0.98
Universal	×	0.68	✓	0.98	×	0.31	✓	0.99	×	0.45	✓	1.00	×	0.31	✓	0.98
Approximate entropy	×	0.58	✓	1.00	×	0.14	✓	0.97	×	0.37	✓	0.99	×	0.18	✓	0.97
Random excursion	✓	0.97	✓	0.98	×	-	✓	0.99	×	-	✓	0.99	✓	0.90	✓	0.99
Random excursion variant	✓	0.97	✓	0.98	×	-	✓	0.99	×	-	✓	0.99	✓	0.96	✓	0.99
Serial	×	0.57	✓	0.98	×	0.49	✓	0.98	×	0.38	✓	0.99	×	0.23	✓	0.97
Linear complexity	✓	0.92	✓	1.00	✓	0.99	✓	0.97	✓	0.96	✓	0.99	✓	0.72	✓	0.98
Final result	Fail		Pass		Fail		Pass		Fail		Pass		Fail		Pass	

XC4VSX35-10FF668 FPGA (30,720 LUTs and 30,720 FFs) experiment results regarding area

Total LUTs	2,711	2,783	315	409	215	311	185	275
Total flip-flops	96	168	96	189	96	192	96	186
1. Frequency (MHz)	56.92	56.92	130.71	130.71	146.56	146.56	162.42	162.42
Bits/cycle	96	96	96	96	96	96	96	96
2. Throughput (Gb/s)	5.46	5.46	12.55	12.55	14.07	14.07	15.59	15.59
Attractors ( $X$ - $Z$ , $U$ - $W$ )								



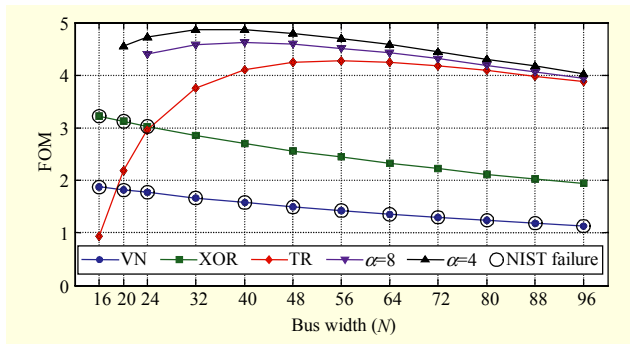


Fig. 10. Figure of merit results for Von Neumann (VN), 2-bit simple XOR (XOR), truncation of defective bits (TR), and proposed post-processing ( $\alpha=4$  and  $\alpha=8$ ) against bus width. NIST failures are highlighted.

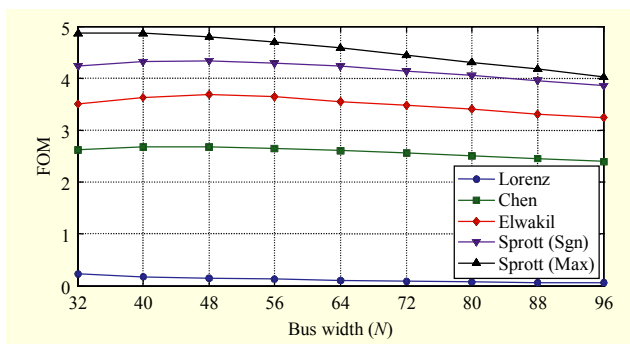


Fig. 11. Figure of merit results for proposed post-processing applied to digital implementations of Lorenz [34], Chen [35], Elwakil and Kennedy [36], Sprott (Sgn) [20], and Sprott (Max) [20] for various bus widths.

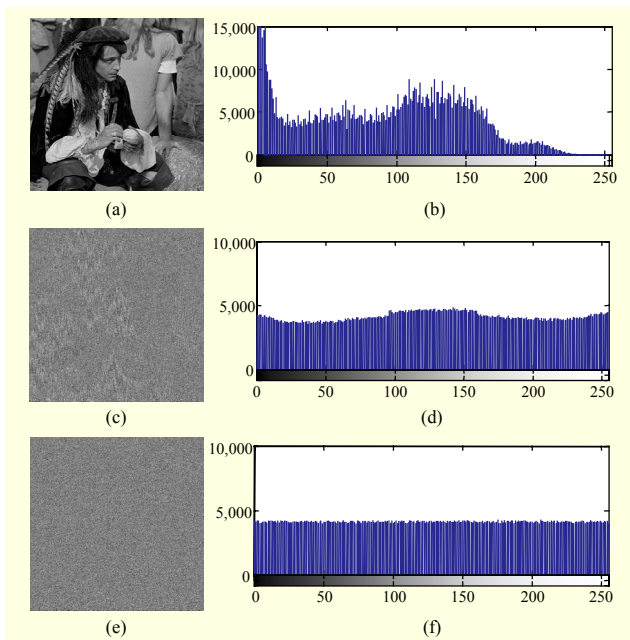


Fig. 12. Image and corresponding histogram of (a)-(b) plain image, (c)-(d) plain image encrypted with original chaotic output, and (e)-(f) plain image encrypted with post-processed chaotic output.

Table 4. Comparison with previously reported CB-PRNGs.

System		Area (Gc)	T <sub>put</sub> (Mb/s)	FOM	NIST
LFSR [5]		223	500	2.24	Fail
Addabbo, 2007 [7]	Rényi Map	3,988	200	0.05	Pass
Chen, 2010 [8]	Log. Map	9,622	200	0.02	Pass
Li, 2010 [37]	Log. Map	9,136	200	0.02	Fail
Chen, 2010 [6]	Log. Map	31,655	3,200	0.1	Pass
Zidan, 2011 [10]	ODE	2,464	1,180	0.47	Pass
Li, 2012 [5]	Log. Map	11,903	6,400	0.54	Pass
<b>This work (with post-processing)</b>					
Lorenz [34]	ODE	23,608	5,464	0.23	Pass
Chen [35]	ODE	4,784	12,548	2.62	Pass
Elwakil and Kennedy [36]	ODE	4024	14069	3.50	Pass
Sprott (Sgn) [20]	ODE	3,688	15,592	4.23	Pass
Sprott (Max) [20]	ODE	3,176	15,437	4.86	Pass

## V. Comparison to Previous Work

Different CB-PRNG systems reported in the literature are compared in Table 4 in terms of hardware efficiency with the proposed maximum function nonlinear CB-PRNG and the ODE-based CB-PRNGs from Table 3, all of 32-bit implementations, in addition to a linear feedback shift register (LFSR) for reference. In all cases of post-processing,  $\alpha=\epsilon$  is used. As this paper exhibits an FPGA implementation, the gate count is expressed as  $8 \times (\text{LUT} + \text{FF})$  to facilitate a basic area comparison, as with the FOM in (8). The proposed technique yields a higher FOM for each tested system when compared to several previous CB-PRNGs due to the increase in the throughput. In general, the logistic map occupies a disproportionately large area for a 1-D system due to the multiplier, as also reflected in the Lorenz system, which requires two multipliers. Implementation of discontinuous nonlinearities (signum, maximum, and modulus) is intrinsically easier in digital hardware and accounts for the significantly lower area of other systems shown. Higher throughputs in the ODEs arise from the use of the proposed post-processing and 3-D system outputs.

## VI. Conclusion

This paper presented a generalized post-processing technique to eliminate bias in CB-PRNGs using a nonlinear XOR-based operation with rotation and feedback. It was verified that this technique enhances the throughput with a minimal area penalty. The proposed technique can be applied

wherever there is a nonuniform distribution of randomness in a set of bitstreams. A third-order chaotic system with maximum function nonlinearity was implemented digitally for the first time, producing a positive MLE of 0.1362. After applying post-processing, the resulting CB-PRNG passed all NIST SP. 800-22 tests for all output bits, with a throughput surpassing other processing techniques. The proposed technique was shown to work effectively for other known chaotic systems, producing efficient PRNGs, and its generalized effect was verified. Furthermore, the proposed CB-PRNG after post-processing was tested in a basic image encryption system and proved to enhance the security performance. Results were experimentally tested on a Xilinx Virtex 4 FPGA with throughput up to 15.44 Gbit/s for 32-bit implementation of the maximum function nonlinear CB-PRNG

## Acknowledgement

The authors would like to thank Mr. M. Affan Zidan for his assistance with system design and valuable discussions.

## References

- [1] S.Y. Hwang et al., "Efficient Implementation of a Pseudorandom Sequence Generator for High-Speed Data Communications," *ETRI J.*, vol. 32, no. 2, Apr. 2010, pp. 222-229.
- [2] M. Asim and V. Jeoti, "Efficient and Simple Method for Designing Chaotic S-Boxes," *ETRI J.*, vol. 30, no. 1, Feb. 2008, pp. 170-172.
- [3] M.L. Barakat, A.G. Radwan, and K.N. Salama, "Hardware Realization of Chaos-Based Block Cipher for Image Encryption," *IEEE Int. Conf. Microelectron.*, 2011, pp. 1-5.
- [4] A. Kopp et al., "A Stochastic Differential Equation Code for Multidimensional Fokker-Planck Type Problems," *Comput. Physics Commun.*, vol. 183, no. 3, 2012, pp. 530-542.
- [5] C.-Y. Li et al., "Period Extension and Randomness Enhancement Using High-Throughput Reseeding-Mixing PRNG," *IEEE Trans. Very Large Scale Integ. Syst.*, vol. 20, no. 2, 2012, pp. 385-389.
- [6] S.-L. Chen et al., "A Fast Digital Chaotic Generator for Secure Communication," *Int. J. Bifurcation Chaos*, vol. 20, no. 12, 2010, pp. 3969-3987.
- [7] T. Addabbo et al., "A Class of Maximum-Period Nonlinear Congruential Generators Derived From the Rényi Chaotic Map," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 54, no. 4, 2007, pp. 816-828.
- [8] S.-L. Chen, T. Hwang, and W.-W. Lin, "Randomness Enhancement Using Digitalized Modified Logistic Map," *IEEE Trans. Circuits Syst. II: Exp. Briefs*, vol. 57, no. 12, 2010, pp. 996-1000.
- [9] M.A. Zidan, A.G. Radwan, and K.N. Salama, "Controllable V-Shape Multi-scroll Butterfly Attractor: System and Circuit Implementation," *Int. J. Bifurcation Chaos*, vol. 22, no. 6, 2012, pp. 1250143-1250156.
- [10] M.A. Zidan, A.G. Radwan, and K.N. Salama, "Random Number Generation Based on Digital Differential Chaos," *Int. Midwest Symp. Circuits Syst.*, 2011, pp. 1-4.
- [11] T. Addabbo et al., "Pseudochaotic Lossy Compressors for True Random Number Generation," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 58, no. 8, 2011, pp. 1897-1909.
- [12] G. Taylor and G. Cox, "Digital Randomness," *IEEE Spectrum*, vol. 48, no. 9, 2011, pp. 32-58.
- [13] S. Li, G. Chen, and X. Mou, "On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps," *Int. J. Bifurcation Chaos*, vol. 15, no. 10, 2005, pp. 3119-3152.
- [14] J.V. Neumann, "Various Techniques Used in Connection With Random Digits," *National Bureau of Standards Applied Mathematics Series 12*, 1951, pp. 36-38.
- [15] T. Stojanovski, J. Pihl, and L. Kocarev, "Chaos-Based Random Number Generators. Part II: Practical Realization," *IEEE Trans. Circuits Syst. I: Fundam. Theory Appl.*, vol. 48, no. 3, 2001, pp. 382-385.
- [16] V. Fischer and M. Drutarovský, "True Random Number Generator Embedded in Reconfigurable Hardware," *LNCS*, Berlin-Heidelberg: Springer, 2003.
- [17] B.-J. Wang et al., "Random Number Generator of BP Neural Network Based on SHA-2 (512)," *Int. Conf. Machine Learning Cybern.*, 2007, pp. 2708-2712.
- [18] P. Lacharme, "Analysis and Construction of Correctors," *IEEE Trans. Info. Theory*, vol. 55, no. 10, 2009, pp. 4742-4748.
- [19] Y.-S. Kim, J.-W. Jang, and D.-W. Lim, "Linear Corrector Overcoming Minimum Distance Limitation for Secure TRNG from (17, 9, 5) Quadratic Residue Code," *ETRI J.*, vol. 32, no. 1, Feb. 2010, pp. 93-101.
- [20] J.C. Sprott, "A New Class of Chaotic Circuit," *Physics Lett. A*, vol. 266, no. 1, 2000, pp. 19-23.
- [21] T. Addabbo et al., "Low Hardware Complexity PRBGs Based on a Piecewise-Linear Chaotic Map," *IEEE Trans. CAS - Part II*, vol. 53, no. 5, 2006, pp. 329-333.
- [22] T. Addabbo et al., "The Digital Tent Map: Performance Analysis and Optimized Design as a Source of Pseudo-Random Bits," *IEEE Trans. Instrum. Meas.*, vol. 55, no. 5, 2006, pp. 1451-1458.
- [23] J.C. Sprott, *Chaos and Time-Series Analysis*, Oxford, UK: Oxford University Press, 2003.
- [24] M.A. Zidan, A.G. Radwan, and K.N. Salama, "The Effect of Numerical Techniques on Differential Equation Based Chaotic Generators," *IEEE Int. Conf. Microelectron.*, 2011, pp. 1-4.
- [25] A.S. Mansingka, A.G. Radwan, and K.N. Salama, "Design, Implementation and Analysis of Fully Digital 1-D Controllable Multiscroll Chaos," *IEEE Int. Conf. Microelectron.*, 2011, pp. 1-5.
- [26] A.S. Mansingka et al., "Analysis of Bus Width and Delay on a Fully Digital Signum Nonlinearity Chaotic Oscillator," *Int. Midwest Symp. Circuits Syst.*, 2011, pp. 1-4.

- [27] R. Devaney, *An Introduction to Chaotic Dynamical System*, 2nd ed., Boulder, CO: Westview Press, 2003.
- [28] S. Kodba, M. Perc, and M. Marhl, "Detecting Chaos from a Time Series," *European J. Physics*, vol. 26, no. 1, 2005, pp. 205-215.
- [29] M.E. Yalcin, J.A.K. Suykens, and J. Vandewalle, "True Random Bit Generation from a Double-Scroll Attractor," *IEEE Trans. Circuits Syst. I: Reg. Papers*, vol. 51, no. 7, 2004, pp. 1395-1404.
- [30] R.B. Davies, "Exclusive OR (XOR) and Hardware Random Number Generators," 2002. <http://www.robertnz.net/pdf/xor2.pdf>
- [31] T. Addabbo et al., *Digitized Chaos for Pseudo-random Number Generation in Cryptography, Series: Studies on Computational Intelligence, Vol. 354*, L. Kocarev and S. Lian, Eds., Springer, 2011.
- [32] A. Rukhin et al., "A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications," *NIST Special Publication 800-22*, 2001.
- [33] H. Kim et al., "Efficient Masking Methods Appropriate for the Block Ciphers ARIA and AES," *ETRI J.*, vol. 32, no. 3, June 2010, pp. 370-379.
- [34] E. Lorenz, "Deterministic Nonperiodic Flow," *J. Atmospheric Sci.*, vol. 20, no. 2, 1963, pp. 130-141.
- [35] G.R. Chen and J.H. Lu, *Dynamics of the Lorenz System Family: Analysis, Control and Synchronization*, Beijing: Sci. Press, 2003.
- [36] A. Elwakil and M. Kennedy, "Construction of Classes of Circuit Independent Chaotic Oscillators Using Passive-Only Nonlinear Devices," *IEEE Trans. Circuits Syst. I: Fundam. Theory Appl.*, vol. 48, no. 3, 2001, pp. 289-307.
- [37] C.-Y. Li, T.-Y. Chang, and C.-C. Huang, "A Nonlinear PRNG Using Digitized Logistic Map with Self-Reseeding Method," *Int. Symp. VLSI Design Autom. Test (VLSI-DAT)*, 2010, pp. 108-111.



**Mohamed L. Barakat** received his BS (summa cum laude) in electronics engineering from the American University in Cairo (AUC), Cairo, Egypt, in 2010, where he was awarded an Academic Honor Certificate by the School of Science and Engineering (2008-2010) and was a recipient of the KAUST Discovery Scholarship (2008-2010). He received his MS in electrical engineering from the King Abdullah University of Science and Technology (KAUST), Thuwal, Saudi Arabia, in 2012, where he received the KAUST Provost's Award (2010-2011) for academic achievement. He is interested in VLSI design, system design, device modeling, and the study of cryptographic applications utilizing digital chaos.



**Abhinav S. Mansingka** received his BS (summa cum laude) in electrical and computer engineering from Cornell University, Ithaca, NY, USA, in 2010. He received his MS in electrical engineering at the King Abdullah University of Science and Technology (KAUST), Saudi Arabia, through a KAUST Fellowship (2010-2012) and was a recipient of the KAUST Provost's Award (2010-2011). His research interests include digital circuit design, VLSI, computer architecture, digital circuits, and, specifically, the fully digital implementation of chaotic systems.



**Ahmed G. Radwan** received his BS (with honors), MS, and PhD in electronics engineering from Cairo University, Egypt, in 1997, 2002, and 2006, respectively. He received the best thesis award from Cairo University in 2002. His main research interests are in the fields of nonlinear circuit analysis, chaotic systems, fractional order systems, and memristor-based circuits. He is an associate professor in the Engineering Mathematics Department and the director of the Technical Center for Job Creation (TCJC), Cairo University, Egypt. In addition, he is with the Nanoelectronics Integrated Systems Center (NISC), Nile University, Egypt. From 2008 to 2009, he was invited as a visiting professor with the Computational Electromagnetics Lab, ECE, McMaster University, Hamilton, Ontario, Canada. In 2010, he was recruited to be one of the pioneer researchers at King Abdullah University of Science and Technology (KAUST), Saudi Arabia, conducting research there through 2012. He introduced many generalized theorems applicable to fractional order circuits and electromagnetics. He is the co-author of more than 85 papers and five patents. He is a senior member of IEEE.



**Khaled N. Salama** received his MS and PhD from the Electrical Engineering Department at Stanford University, Stanford, CA, USA, in 2000 and 2005, respectively. He was an assistant professor at RPI between 2005 and 2008. He joined King Abdullah University of Science and Technology (KAUST) in January 2009 and was the electrical engineering founding program chair. His work on CMOS sensors for molecular detection was funded by the National Institute of Health (NIH) and the Defense Advanced Research Projects Agency (DARPA), earned him the Stanford-Berkeley Innovators Challenge Award in biological sciences, and was acquired by Illumina, Inc., San Diego, CA, USA, in 2008. He is the cofounder of Ultra Wave Labs, an AVC-funded biomedical imaging company. He is the co-author of over 100 papers and 10 patents on low-power mixed-signal circuits for intelligent fully integrated sensors and nonlinear electronics, especially memristor devices. He is a senior member of IEEE.