IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received February 27, 2022, accepted March 16, 2022, date of publication March 28, 2022, date of current version April 1, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3162806

Cascading CMOS-Based Chaotic Maps for Improved Performance and Its Application in Efficient RNG Design

PARTHA SARATHI PAUL, (Graduate Student Member, IEEE),
MAISHA SADIA, (Graduate Student Member, IEEE),
MD RAZUAN HOSSAIN, (Graduate Student Member, IEEE),
BARRY MULDREY, (Member, IEEE), AND MD SAKIB HASAN, (Member, IEEE)
Department of Electrical and Computer Engineering, The University of Mississippi, Oxford, MS 38677, USA

Corresponding author: Partha Sarathi Paul (ppaul@go.olemiss.edu)

ABSTRACT We present a general framework for improving the chaotic properties of CMOS-based chaotic maps by cascading multiple maps in series. Along with two novel chaotic map topologies, we present the 45 *nm* designs for four CMOS-based discrete-time chaotic map topologies. With the help of the bifurcation plot and three established entropy measures, namely, Lyapunov exponent, Kolmogorov entropy, and correlation coefficient, we present an extensive chaotic performance analysis on eight unique map circuits (two under each topology) to show that under certain constraints, the cascading scheme can significantly elevate the chaotic performance. The improved chaotic entropy benefits many security applications and is demonstrated using a novel random number generator (RNG) design. Unlike conventional mathematical chaotic map-based digital pseudo-random number generators (PRNG), this proposed design is not completely deterministic due to the high susceptibility of the core analog circuit to inevitable noise that renders this design closer to a true random number generator (TRNG). By leveraging the improved chaotic performance of the transistor-level cascaded maps, significantly low area and power overhead are achieved in the RNG design. The cryptographic applicability of the RNG is verified as the generated random sequences pass four standard statistical tests namely, NIST, FIPS, Diehard, and TestU01.

INDEX TERMS Chaos, discrete-time chaos, chaotic map, PRNG, TRNG, CMOS, VLSI, hardware security, cryptography.

I. INTRODUCTION

The inception of chaos theory is marked by Henri Poincaré's observation on non-periodic orbits in his study on the three-body problem in the 1880s (translated in [1]). However, to see significant development in chaos theory, the world had to wait for the invention of digital computers that had made the repeated iterative computation easier, and eventually, resulted in Edward Lorenz's seminal 1963 publication [2] on an accidental discovery of chaos in his study on weather prediction [3]. Chaos occurs as a special condition in a nonlinear deterministic dynamic system [4]. Dynamic systems describe the time evolution of one or multiple points in a geometrical space. There are mainly two kinds of dynamic systems: (i) stochastic, when the trajectory of the point is random, and (ii) deterministic, when a mathematical function can exactly predict the future state after a certain time interval. Dynamic systems are called non-linear where the change in output is not proportional to the change in input. Generally, in a non-linear deterministic dynamic system, the time-trajectory of a point eventually reaches a periodic steady-state, after starting from any initial state. In this general case, two very close initial states result in an almost similar steady-state. However, when the parameters of a nonlinear deterministic dynamic system are tuned to its chaotic region then we can observe two special conditions: firstly, the time trajectory never reaches a periodic steady-state, secondly, two initial states – even if they are very close to each other–will eventually follow two very different time-trajectories [5]. The aperiodicity of a chaotic system is distinct from randomness since the time-trajectory is deterministic in the chaotic case where we can always reproduce the same trajectory starting from the same initial state. The initial state sensitivity is popularly known as the 'butterfly effect', after being coined

The associate editor coordinating the review of this manuscript and approving it for publication was Fabian Khateb.

by Lorenz in a lecture [6], as if a butterfly flapped its wings in Brazil a few weeks earlier and as a result, eventually, that minor perturbation has changed the nice sunny weather in Texas into a tornado. This deterministic aperiodicity and the sensitive dependence on the initial state of chaotic systems have proven their utility in numerous security applications such as data encryption [7], random number generation [8], [9], reconfigurable logic [10], [11], Physically Unclonable Function (PUF) [12], side-channel attack mitigation [13], secure communication [14], logic obfuscation [15] and so on.

Depending on the number of state variables involved, chaotic systems can be categorized into two groups: (i) one-dimensional (1-D) maps, where only one function describes the evolution of a single state variable. (ii) Multi-dimensional (multi-D) chaotic maps, where the time evolution of more than one state variable is described with the same number of functions. The nature of time-evolution divides the chaotic systems into two classes: (i) continuous time, where the governing function contains the time derivative terms and time steps of the trajectory is continuous, (ii) discrete-time, where the trajectory evolves in discrete time steps and any next state of the system is a direct function of the previous state. Familiar examples of 1-D discrete-time maps are sine map, tent map, logistic map, and so on. On the other hand, Henon map (discrete-time) and Lorenz system (continuous-time) are examples of multi-D maps. In this work, we focus on 1-D discrete-time chaotic maps.

Regarding security applications, multi-D chaotic maps, with their complex chaotic properties, provide higher security [16], however, they are expensive to implement in hardware. On the other hand, 1-D chaotic maps are simple to implement. One downside is this convenience in the implementation comes with a compromise in security since the output trend can be predictable with low computational cost [17]. Zhou *et al.* proposed a scheme where multiple 1-D chaotic maps are cascaded together in series to form the final map that shows improved chaotic properties relative to its constituent 1-D seed maps [18]. They have demonstrated superior chaotic performance from their proposed scheme by cascading multiple 1-D maps like sine, logistic, and tent maps. These mathematical maps are suitable for software-based applications like encryption algorithms, however, they are not suitable for CMOS (Complementary Metal Oxide Semiconductor) implementations in hardware for applications where there is high constraint in chip area and power. One example of this type of application can be a hardware-based security protocol for edge devices like IoT (Internet of Things). The reported CMOS implementations of classical mathematical maps, including logistic map [19], sine map [20], and tent map [21], are so hardware-hungry that they are not suitable for any low-overhead hardware-security applications. Instead of trying to mimic the characteristic curve of classical mathematical maps, some researchers have been leveraging the built-in non-linearity in MOS transistors and proposing simpler CMOS circuits, with characteristic curves similar enough to classical mathematical functions, which are capable of generating discrete-time chaotic sequences. Dudek *et al.* proposed the design of two discrete-time chaotic maps in a 600 *nm* CMOS process, in [22] and [23]. It was shown that, each of these two circuit topologies, with only three MOS transistors, demonstrated promising chaotic properties. In this paper, we present 45 *nm* designs of these two circuit topologies and propose two novel three-transistor discrete-time chaotic circuit topologies. With these four chaotic map topologies, we explore the application of the cascading scheme in CMOS-based chaotic circuits. The chaotic properties of the main four topologies and their cascaded combinations are analyzed with bifurcation plot, Lyapunov exponent, Kolmogorov entropy, and correlation coefficient. To demonstrate the application of cascading, we propose a novel CMOS-based chaotic random number generator (RNG) design with two additional alternative designs. The cryptographic performance of the proposed RNG is evaluated with four statistical tests.

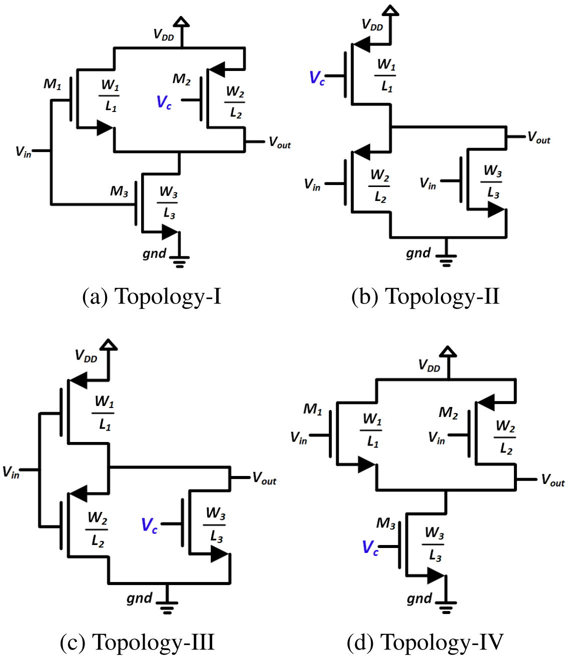
The rest of the paper is organized as follows: Section-II presents the four chaotic map topologies and the cascading scheme. The chaotic performance of the proposed chaotic maps and their cascades are analyzed in Section-III. The RNG design and performance evaluation of the RNG output are presented in section-IV. Section-V provides the concluding remarks.

II. CASCADED CHAOTIC MAP (CCM)

The building block of a discrete-time chaotic system is a function with non-linear transfer characteristics. Eq. (1) shows the general expression of a recursion relation where a non-liner function, $S(.)$, transforms any point, x_i from a closed interval $[L_1, L_2]$, into some other point, x_{i+1} in the same interval.

$$x_{i+1} = S(C, x_i) \tag{1}$$

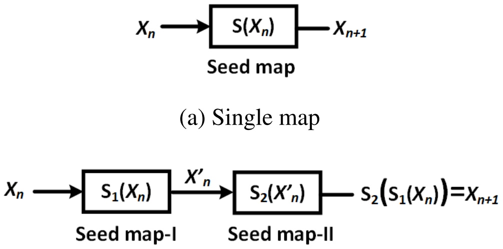
Here, C is a controlling parameter that governs the shape of the transfer characteristic and i denotes the discrete steps, $1, 2, 3, \ldots, n$. This is called a discrete-time map in the interval $[L_1, L_2]$. As we are dealing with CMOS implementations in this paper, this non-linear functionality will be provided by a CMOS circuit. We refer to this circuit as the seed map. FIGURE 1 shows the schematic of four topologies of seed maps where, V_c denotes the control parameter. As we have mentioned in section-I, the 600 *nm* CMOS designs of Topology-I (FIGURE 1(a)) and Topology-II (FIGURE 1(b)) were proposed in [22] and [23], respectively. We introduce two more three-transistor-based chaotic map topologies, namely, Topology-III (FIGURE 1(c)) and Topology-IV (FIGURE 1(d)) in this work. We have simulated these four chaotic map topologies (I-IV) using the Spectre simulator in Cadence, with a 45 *nm* CMOS process. In the simulation, we have experimented with the sizes of three MOS transistors and come up with different geometries that can generate discrete-time chaotic sequences. TABLE 1 shows the transistor sizing of two geometries (a, b) under each topology that we will be using to present all the results in this paper.



(a) Topology-I (b) Topology-II

(c) Topology-III (d) Topology-IV

FIGURE 1. Four topologies for three-transistor chaotic map.



(a) Single map

(b) Cascaded map

FIGURE 2. Schematic of the cascading scheme.

TABLE 1. Transistor sizing for different geometries.

Topology	Geometry	$\frac{W_1(nm)}{L_1(nm)}$	$\frac{W_2(nm)}{L_2(nm)}$	$\frac{W_3(nm)}{L_3(nm)}$
I	a	3000/45	112.5/45	112.5/45
	b	992/45	47/45	86/45
II	a	150/45	1500/45	45/150
	b	75/45	375/45	45/75
III	a	450/45	4500/45	45/450
	b	75/45	750/45	45/75
IV	a	450/45	45/45	450/90
	b	450/45	45/45	45/450

Generally, map circuits are designed to approximately imitate the unimodal transfer characteristics (for example, tent or 'V' shape for the tent map or inverse tent map, respectively) of one of the widely known chaos maps such as a logistic map, sine map or a tent map.

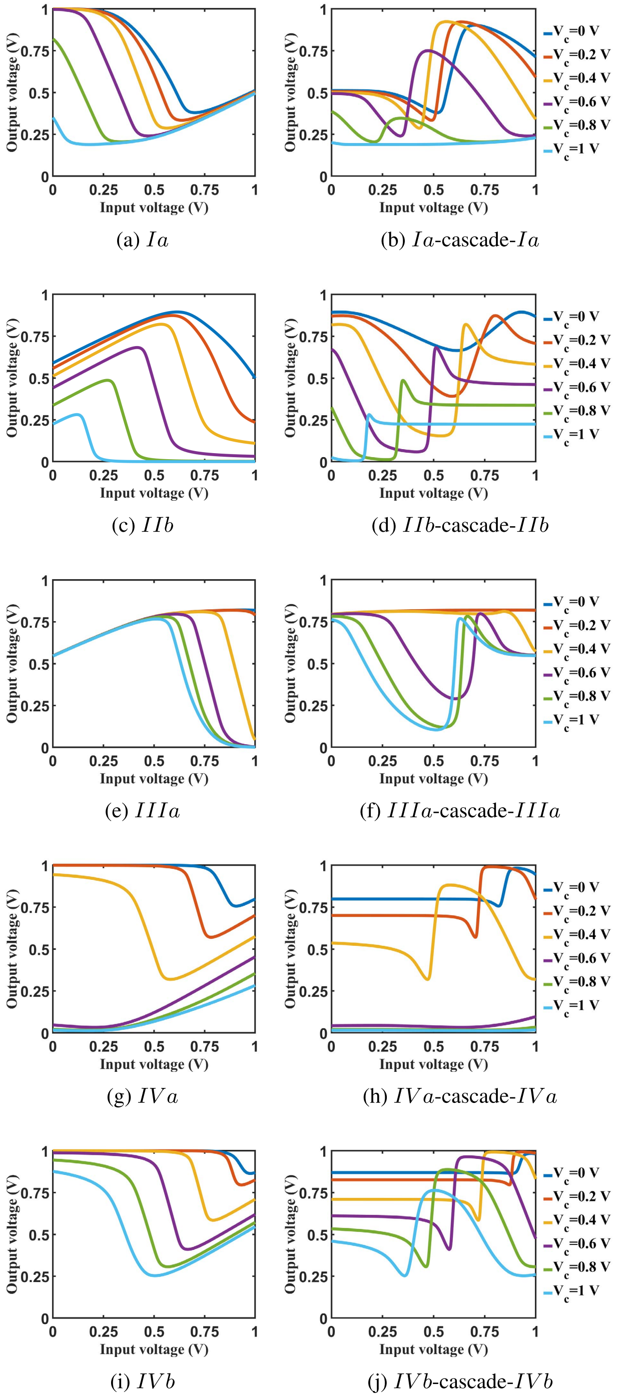
Although, in general, any number of seed maps can be connected in series to form CCM, in this paper, with the objective of overhead optimization in mind, we are limiting ourselves to a cascade of two seed maps. The schematic of the cascading scheme is shown in FIGURE 2. FIGURE 3 shows the transfer characteristics of seed maps and the cascaded pairs of the same maps. Comparing FIGURE 3(g) and 3(i), we can see how the shapes of the transfer curves vary with the choice of geometry in the same topology. The seed maps of $Topology - I$ and $Topology - IV$ generate approximate 'V-shaped' curves while we get approximate 'tent-shape' from $Topology-II$ and $Topology-III$. We know from Feigenbaum's work in [24] that differentiable uni-modal transfer characteristics have the potential to generate chaos. Hence, the transistor sizes of the seed maps are carefully chosen to get the unimodal transfer curve shapes (close to a 'V' or tent-shape). We are getting multi-modal transfer characteristics from cascaded maps which result in a much better chaotic properties compared to the unimodal characteristics of the seed maps.

III. PERFORMANCE ANALYSIS

The chaotic property of a discrete-time map is evaluated based on the discrete-time sequence generated from the map. For a particular value the control parameter, C, if we run the recursion relation of Eq. (1) in a loop where the output of one step will be fed back as the input for the next step, we get a sequence of discrete-time values. However, we do not have a simple closed-form analytical input-output relation for our CMOS-based seed maps. To generate discrete-time sequences from these map circuits, we use a feedback system called chaotic oscillator. FIGURE 4 shows the schematics of chaotic oscillators for a single seed map and cascade of two seed maps. In both oscillators, switch ϕ_0 is used to feed the initial state, X_0, to the system. At each iteration, an analog voltage, X_n, passes through the forward path ($Seed\ map - A$ in the single case, $Seed\ map - A$, and $Seed\ map - B$ in the cascaded case) and we get the first output, V_{out1}. In general, capacitors are used to sample and hold the voltage in the feedback path. In our design, we reduce the hardware cost by performing the sample and hold operation with two non-overlapping clock-run switches, ϕ_1 and ϕ_2, and the parasitic capacitance of the transistors of the seed map circuit. One iteration loop completes when the output of the feedback path, V_{out2}, is fed back to the forward path as an input for the next iteration. At each iteration, we sample out two analog voltages, V_{out1}, and V_{out2}. The discrete-time sequences are recorded for 15000 iteration loops. Then the first 1000 iterations are discarded to get steady-state values. The steady-state discrete-time values are used for chaotic performance analysis, with the help of bifurcation plot, and three chaotic entropy metrics: Lyapunov exponent, Kolmogorov entropy, and correlation coefficient measurement.

A. BIFURCATION PLOT

FIGURE 5 shows the bifurcation plots for single and cascaded maps of both geometries under each of the four topologies. In these plots, 14000 steady-state analog values are plotted for each control/bifurcation parameter (V_c).



(a) Ia

(b) Ia-cascade-Ia

(c) IIb

(d) IIb-cascade-IIb

(e) $IIIa$

(f) $IIIa$-cascade-$IIIa$

(g) IVa

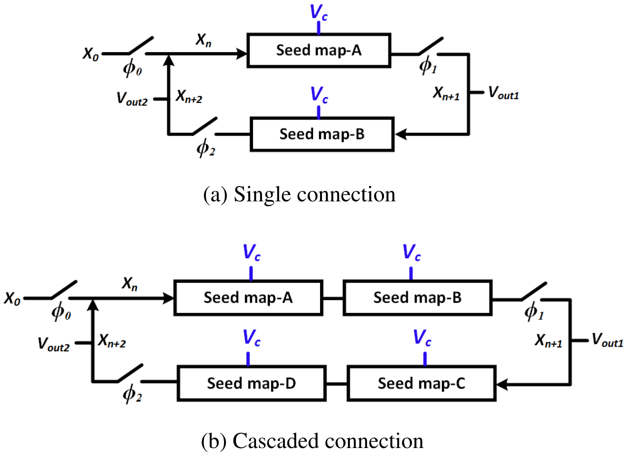
(h) IVa-cascade-IVa

(i) IVb

(j) IVb-cascade-IVb

FIGURE 3. Transfer curves of different seed maps and the cascade of two similar maps. Here, '*Ia*' denotes the *Geometry − a* of *Topology − I*.

The dark-colored regions of the plots indicate chaotic behaviour. In the remaining portions of the plots, the analog sequence either remains fixed to a single value (fixed point) or periodically fluctuates among a countable number of levels (periodic orbit). One distinction between the single and cascaded case is that the even periodic orbits are reduced by half in the cascaded case. For instance, $0\ V < V_c < 0.25\ V$ region in FIGURE 5(a) shows a period of two (two distinct output voltage levels for all the V_c values in this region), where the same region in Figure 5(e) shows just one level. The reduction of even periods by half comes from the fact that we are connecting two similar seed maps in series. A cascade of three similar maps would result in a reduction of the period-3 orbit region to a single level region.



(a) Single connection

(b) Cascaded connection

FIGURE 4. Schematic of the chaotic oscillator.

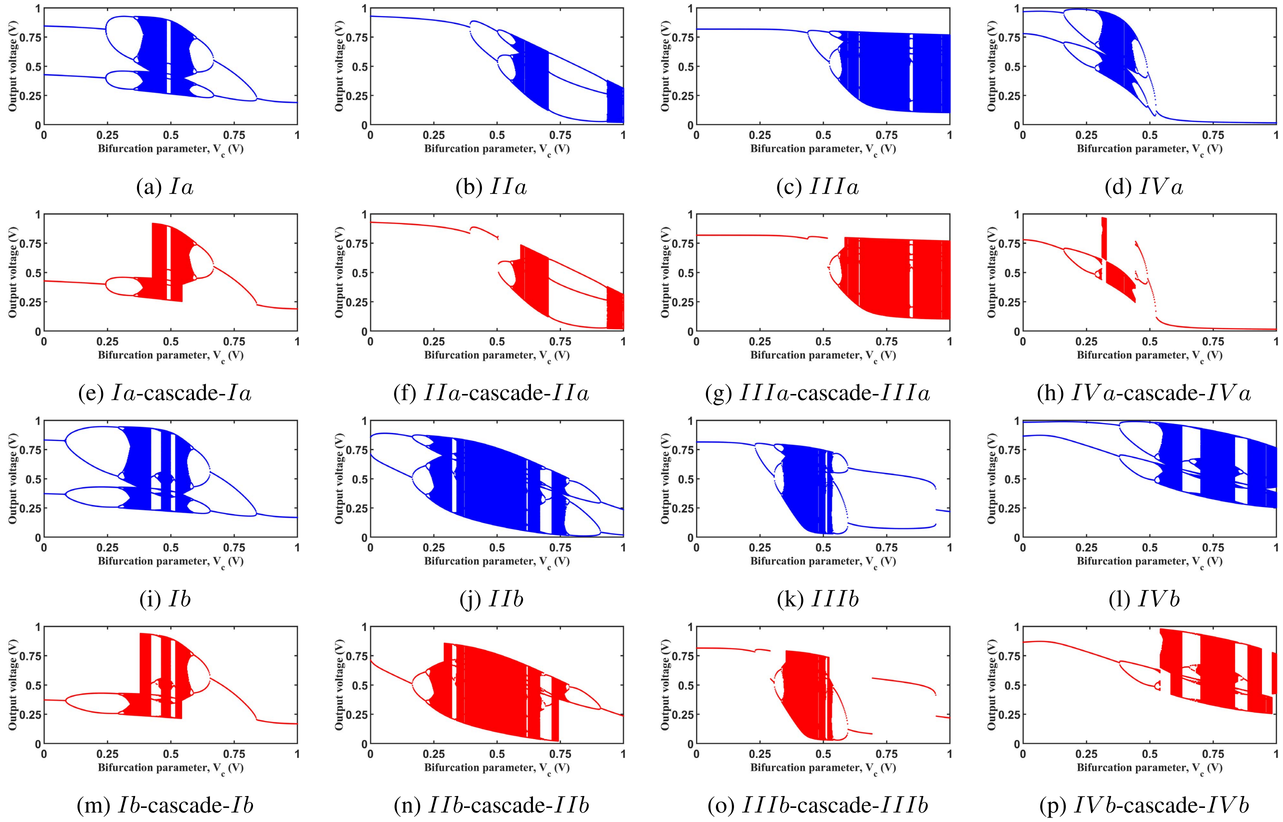
B. LYAPUNOV EXPONENT

The Lyapunov exponent (LE) is the most widely-used metric to quantify the sensitive dependence of a chaotic sequence on initial conditions. On average, two neighboring trajectories of a chaotic sequence, starting from slightly different initial conditions, diverge exponentially fast [5]. For a discrete-time chaotic system, as expressed in Eq. (1), LE (denoted by λ) can be expressed as shown in Eq. (2) [5], where, n denotes the number of iteration.

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} ln \left| \frac{dS}{dX}|_{X_i} \right| \tag{2}$$

A negative LE value indicates either a fixed point or a periodic orbit. On the other hand, a positive value of LE represents a chaotic attractor [5]. Faster divergence of the output trajectory of a chaotic oscillator corresponds to a larger positive LE value. Now, we want to derive the LE for a cascaded chaotic map. Let's consider two very close initial states, X_0^a and X_0^b, which are separately passing through a cascaded map as shown in FIGURE 2(b). After the first iteration, they result in two output states, X_1^a and X_1^b, respectively. We can express the difference between the two output states as shown in Eq. (3).

$$\begin{aligned} |X_1^a - X_1^b| &= |S_2\left(S_1(X_0^a)\right) - S_2\left(S_1(X_0^b)\right)| \\ &= \frac{|S_2\left(S_1(X_0^a)\right) - S_2\left(S_1(X_0^b)\right)|}{|S_1(X_0^a) - S_1(X_0^b)|} \\ &\quad \times \frac{|S_1(X_0^a) - S_1(X_0^b)|}{|X_0^a - X_0^b|} |X_0^a - X_0^b| \end{aligned} \tag{3}$$



(a) Ia (b) IIa (c) $IIIa$ (d) IVa

(e) Ia-cascade-Ia (f) IIa-cascade-IIa (g) $IIIa$-cascade-$IIIa$ (h) IVa-cascade-IVa

(i) Ib (j) IIb (k) $IIIb$ (l) IVb

(m) Ib-cascade-Ib (n) IIb-cascade-IIb (o) $IIIb$-cascade-$IIIb$ (p) IVb-cascade-IVb

FIGURE 5. Bifurcation plots for seed maps (a-d & i-l) and the cascade of two similar maps (e-h & m-p). Here, in the cascade, both maps use the same V_C.

The derivatives of two seed maps in the cascade combination can be considered separately as follows:

$$\left|\frac{dS_1}{dX}|_{X_0^a}\right| \approx \lim_{X_0^a \to X_0^b} \frac{|S_1(X_0^a) - S_1(X_0^b)|}{|X_0^a - X_0^b|}$$

$$\left|\frac{dS_2}{dX}|_{S_1(X_0^a)}\right| \approx \lim_{S_1(X_0^a) \to S_1(X_0^b)} \frac{|S_2\left(S_1(X_0^a)\right) - S_2\left(S_1(X_0^b)\right)|}{|S_1(X_0^a) - S_1(X_0^b)|}$$

Putting these derivative expressions in Eq. (3) we may get Eq. (4).

$$|X_1^a - X_1^b| = \left|\frac{dS_2}{dX}|_{S_1(X_0^a)}\right| \left|\frac{dS_1}{dX}|_{X_0^a}\right| |X_0^a - X_0^b| \qquad (4)$$

In the same way, after the 2nd iteration, the difference between two outputs can be expressed as shown in Eq. (5).

$$|X_2^a - X_2^b| = \left|\frac{dS_2}{dX}|_{S_1(X_1^a)}\right| \left|\frac{dS_1}{dX}|_{X_1^a}\right| \left|\frac{dS_2}{dX}|_{S_1(X_0^a)}\right| \times \left|\frac{dS_1}{dX}|_{X_0^a}\right| \times |X_0^a - X_0^b| \qquad (5)$$

The difference between two outputs after the n^{th} iteration can be expressed as shown in Eq. (6).

$$|X_n^a - X_n^b| \approx \left|\prod_{i=0}^{n-1} \frac{dS_2}{dX}|_{S_1(X_i^a)}\right| \left|\prod_{i=0}^{n-1} \frac{dS_1}{dX}|_{X_i^a}\right| |X_0^a - X_0^b| \qquad (6)$$

The average change per iteration that occurs to go from $|X_0^a - X_0^a|$ to $|X_n^a - X_n^a|$, can be expressed as shown in Eq. (7).

$$\Delta = \left\{ \left|\prod_{i=0}^{n-1} \frac{dS_2}{dX}|_{S_1(X_i^a)}\right| \left|\prod_{i=0}^{n-1} \frac{dS_1}{dX}|_{X_i^a}\right| \right\}^{1/n} \qquad (7)$$

According to the definition, LE for the cascaded map (λ_c) can be expressed as follows:

$$\begin{aligned} \lambda_c &= ln(\Delta) \\ &= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} ln \left|\frac{dS_2}{dX}|_{S_1(X_i^a)}\right| + \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} ln \left|\frac{dS_1}{dX}|_{X_i^a}\right| \\ &= \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} ln \left|\frac{dS_2}{dX}|_{S_1(X_i^a)}\right| \\ &\quad + \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} ln \left|\frac{dS_1}{dX}|_{S_2(S_1(X_{i-1}^a))}\right| \end{aligned} \qquad (8)$$

If the cascaded map uses two similar seed maps, i.e. when S_1 and S_2 are same, each of the two terms in Eq. (8) can be approximated as the LE of the seed map. In general case of the cascade of k similar maps, the LE of the cascaded map can be expressed as shown in Eq. (9).

$$\lambda_c = \lambda_s + \lambda_s + \cdots + \lambda_s = k \times \lambda_s \qquad (9)$$

FIGURE 6 shows the LE plots for seed map and their cascaded pair where both maps are the same. The cascaded maps show a clear improvement in the LE values from their constituent seed maps.

It should be noted that expressing the LE of cascaded maps as a sum of constituent seed maps (as shown in [18]) is not true in general. Eq. (9) holds only when the seed maps have identical or very similar trajectories. FIGURE 7 demonstrates this point by comparing the sum of the positive LE values of seed maps with the cascaded maps in two cases: (a-h) cascade of same seed maps (same topology, same geometry) and (i-l) cascade of different seed maps (same topology but different geometry). As we can see from FIGURE 7(a-h), Eq. (9) holds for same seed maps but does not necessarily hold in the general case with different seed maps (FIGURE 7(i-l)). Moreover, the bifurcation plots of FIGURE 7(o) and FIGURE 7(p) show that, the chaotic region is absent as a result of cascading two dissimilar maps where there is no overlap between their corresponding chaotic regions (as shown in FIGURE 5(c,k), and FIGURE 5(d,l)). Consequently, we get no positive LE value over the whole V_c range of FIGURE 7(k) and FIGURE 7(l). In all results up to this point, both maps of a cascade share the same V_c. However, it is possible to use any arbitrary combination of V_c values. FIGURE 8(a-c) shows the LE values using heat map for all possible combinations of V_c between two cascading maps. Here, we can see that, a cascade of two dissimilar topologies (FIGURE 8(c)) does not result in positive LE values for any combination of V_c. Hence, as a design guideline, we should keep in mind that the benefit of cascading can be leveraged most conveniently when we cascade two identical maps.

C. KOLMOGOROV ENTROPY

The Kolmogorov entropy (KE) measures the complexity in a sequence by capturing the generation rate of new information. To present an estimation method in [25], Grassberger *et al.* defined KE as follows: let's suppose, in a dynamic system, an F-dimensional phase space is partitioned to ϵ^{F}-sized boxes. We are measuring the state of a trajectory, $\vec{X}(t)$, in the time intervals τ. There is a probability measure, $p(i_1, i_2, \ldots, i_d)$, that defines the joint probability of $\vec{X}(t)$ being in the box i_1 at $t = \tau$, in i_2 at $t = 2\tau$, and so on. As a result, KE is defined as shown in Eq. (10) [25].

$$KE = -\lim_{\tau\to\infty}\lim_{\epsilon\to\infty}\lim_{d\to\infty}\frac{1}{n}\sum_{i_1,\ldots,i_d} p(i_1, i_2, \ldots., i_d) \times ln(p(i_1, i_2, \ldots., i_d)) \tag{10}$$

The value of KE is 0 for an ordered sequence, ∞ for a random sequence, and a nonzero constant for a chaotic sequence. FIGURE 9 shows a comparison of KE values between the seed map and it's cascaded pair where, the nonzero KE regions correspond to the respective chaotic regions. We can notice here as well that the cascading scheme substantially increases the entropy measure compared to the constituent seed map.

D. CORRELATION COEFFICIENT

The initial state sensitivity in chaotic and non-chaotic regions of a sequence can be measured using the correlation coefficient as well. The correlation coefficient between two sequences, X and Y, can be expressed as shown in Eq. (11) [26].

$$C_o = \frac{E[(X-\mu_X)(Y-\mu_Y)]}{\sigma_X\sigma_Y} \tag{11}$$

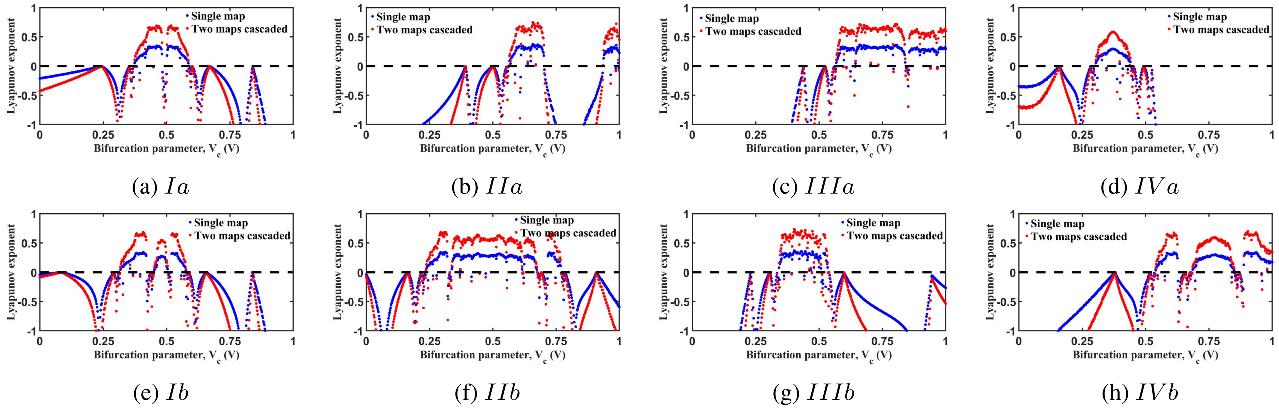
Here, in Eq. (11), the operator 'E[.]' denotes the expectation function, μ and σ are the mean value and standard deviation, respectively. The correlation value is close to $+1/-1$ if X and Y are highly correlated whereas, a 0 correlation coefficient value indicates an extremely low correlation between the two sequences. For each value of the bifurcation parameter, two sequences are generated, starting with two very close (1 nV apart) initial states. FIGURE 10 shows the calculated correlation coefficients for different values of bifurcation parameters, in both single and cascaded cases of different geometries. This same metric can also be used to see the sensitivity of the bifurcation parameter variation. For this purpose, another set of data is generated, with a 1 nV variation in the control parameter, while keeping the initial state fixed. FIGURE 11 shows the calculated correlation coefficients for the V_c variation scheme. Both figures depict that, in chaotic regions for both single and cascaded cases, even that tiny difference in the initial state or V_c leads to significant divergence between the two sequences which causes the correlation coefficient to become close to 0. However, in the non-chaotic regions, the tiny difference in initial condition eventually diminishes in steady-state output values and that results in a correlation coefficient of 1. Moreover, mainly at the edges of the chaotic regions, the cascaded maps show correlation coefficient values closer to 0 than the seed maps, which indicates stronger chaotic property from the cascaded maps.

IV. APPLICATION

It is clear from the entropy measurements that we are getting improved chaotic performance from cascaded maps. Hence, this topology can be a natural choice for applications like chaos-based random number generator (RNG) where a chaotic map with better chaotic properties is always desired for ensuring more secured cryptographic performance. In this section, we are presenting the design of an efficient RNG, based on a combination of single and cascaded maps. The applicability of the generated random sequence in cryptography is assessed with four established statistical randomness test suits and the overhead cost of the RNG is compared with other reported works.

A. RNG DESIGN

FIGURE 12 shows the schematic of the proposed RNG. One input of each comparator comes from a chaotic oscillator



(a) Ia

(b) IIa

(c) $IIIa$

(d) IVa

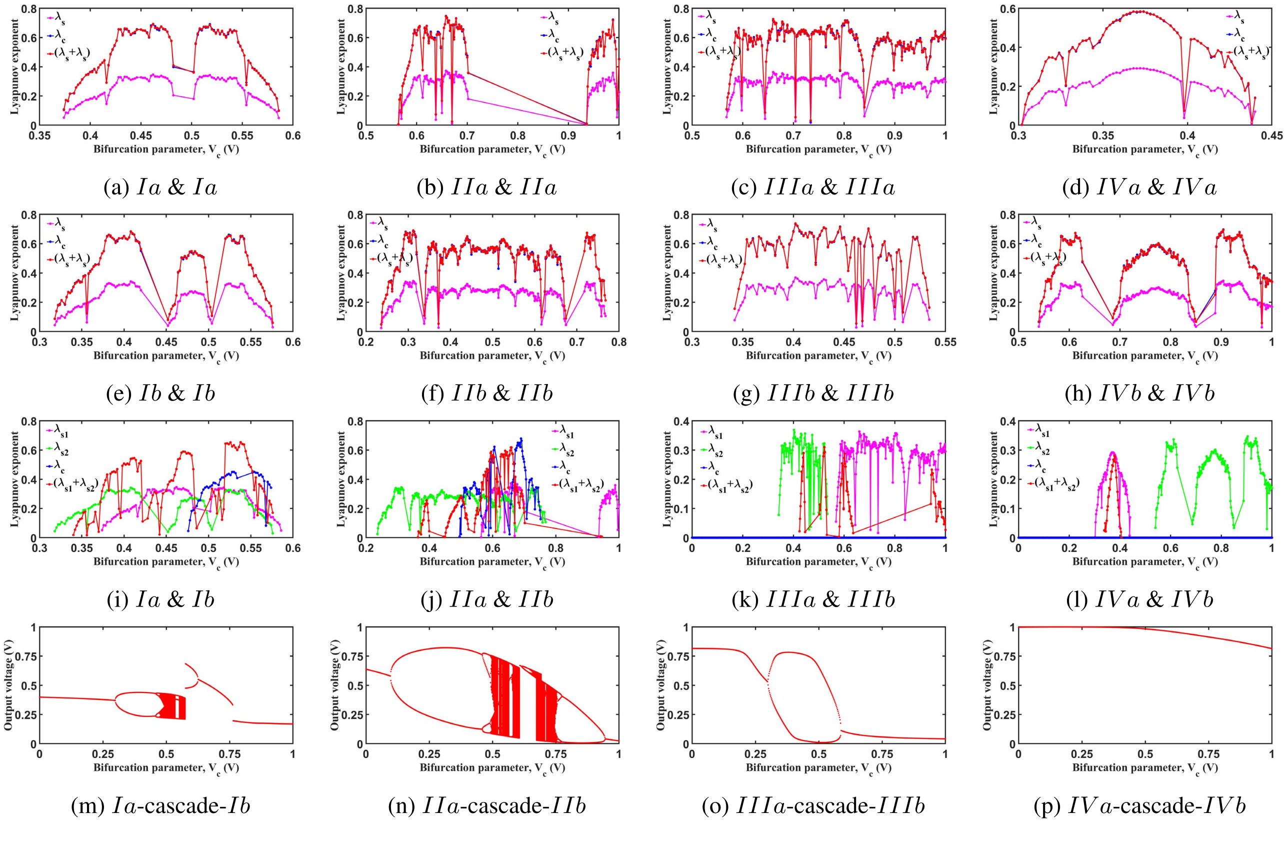
(e) Ib

(f) IIb

(g) $IIIb$

(h) IVb

FIGURE 6. The comparison of LE between seed maps and corresponding cascaded pair of the same seed maps. In the cascade, both maps use the same V_C. Here, for example, '*IIa*' denotes the *Geometry* − *a* of *Topology* − *II* which shows the comparison between the LE from the seed map, *IIa*, and the cascaded map, *IIa*-cascade-*IIa*.



(a) Ia & Ia

(b) IIa & IIa

(c) $IIIa$ & $IIIa$

(d) IVa & IVa

(e) Ib & Ib

(f) IIb & IIb

(g) $IIIb$ & $IIIb$

(h) IVb & IVb

(i) Ia & Ib

(j) IIa & IIb

(k) $IIIa$ & $IIIb$

(l) IVa & IVb

(m) Ia-cascade-Ib

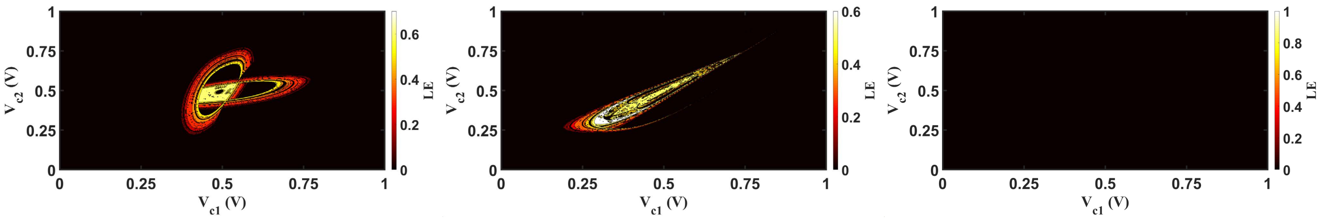
(n) IIa-cascade-IIb

(o) $IIIa$-cascade-$IIIb$

(p) IVa-cascade-IVb

FIGURE 7. LE comparison: (a-d) cascade of the same map using the first geometry for each topology, (e-h) cascade of the same map using the second geometry for each topology, (i-l) cascade of different geometries. (m-p) Bifurcation plot for the cascade of different geometries. Here, in the cascade, both maps use the same V_C.

as shown in FIGURE 4(a) (*Single map output*), while the other one comes from FIGURE 4(b) (*Cascaded map output*). The outputs of the three comparators are XOR-ed to increase the entropy in the generated sequence. For each comparator, we use the cascade of two identical maps and single output from the same map. We have experimentally come up with multiple combinations of maps to be used in three comparators of the RNG, that pass the statistical tests. Then we measured the worst-case delay of the cascaded oscillators (since the cascaded delay is higher than the single one and the higher delay component is the determining factor of the circuit). FIGURE 13 shows the delay with respect to V_c for different maps. We also have recorded the total power consumption of single and cascaded oscillators. The power

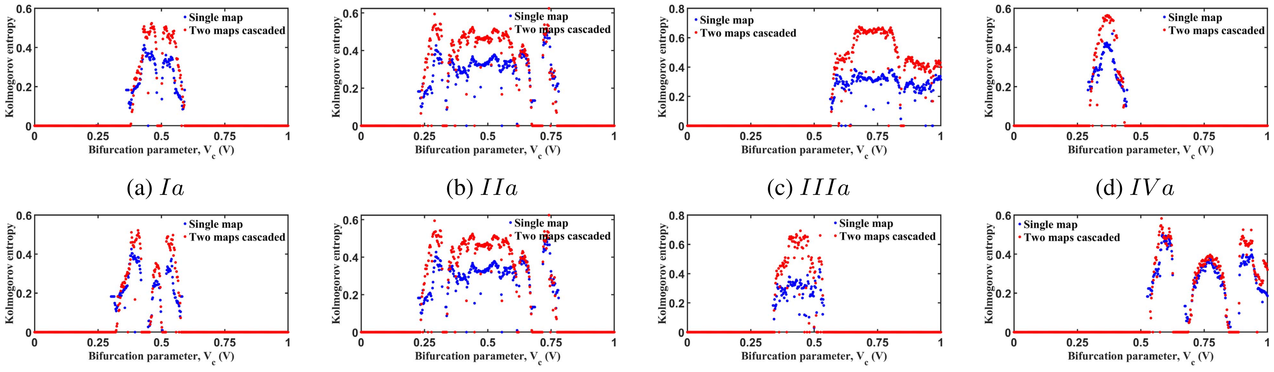


(a) Ia-cascade-Ia

(b) IIb-cascade-IIb

(c) Ia-cascade-IIb

FIGURE 8. LE plots in heat map showing all combinations of V_{c1} (Bifurcation parameter of the first map) and V_{c2} (Bifurcation parameter of the second map). Here, all negative LE values are suppressed to 0.



(a) Ia

(b) IIa

(c) $IIIa$

(d) IVa

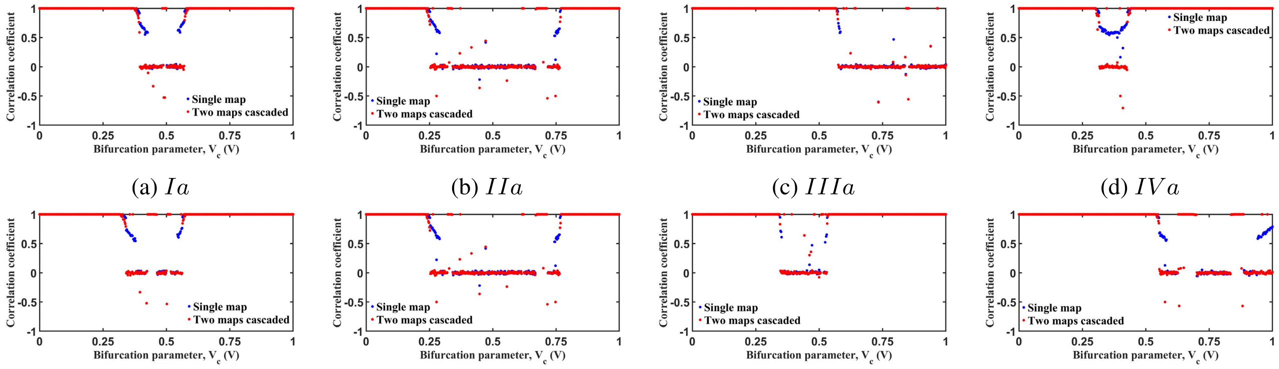
(e) Ib

(f) IIb

(g) $IIIb$

(h) IVb

FIGURE 9. The comparison of KE between seed maps and corresponding cascaded pair of the same seed maps. In the cascade, both maps use the same V_c.



(a) Ia

(b) IIa

(c) $IIIa$

(d) IVa

(e) Ib

(f) IIb

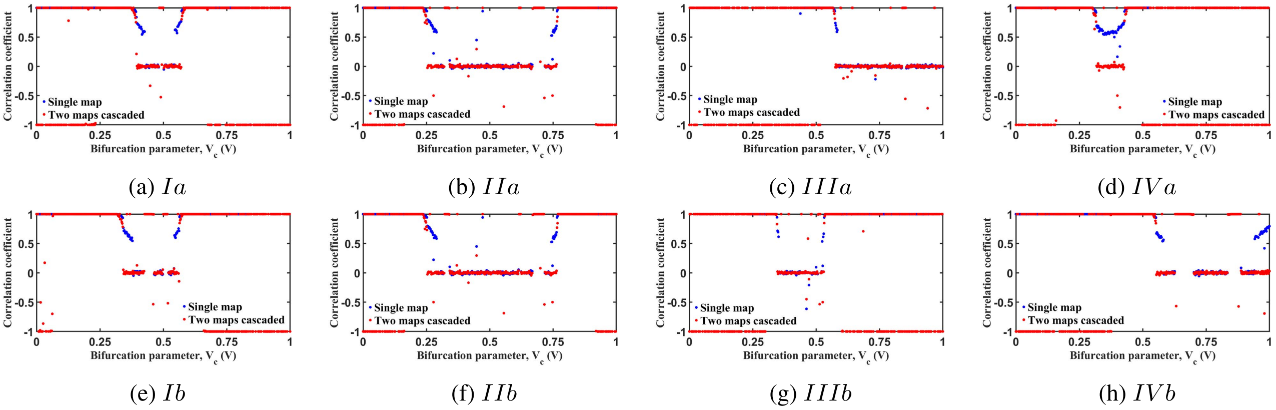
(g) $IIIb$

(h) IVb

FIGURE 10. The comparison of initial condition variation-based CC between seed maps and corresponding cascaded pair of the same seed maps. In the cascade, both maps use the same V_c.

is averaged over multiple oscillations in steady-state, starting from three different initial conditions. The average power with respect to V_c is shown in FIGURE 14. Considering the sizing of the transistors (shown in TABLE 1), the worst-case delay of the oscillators, and the average power consumed by the oscillators, we have nominated one combination to present the results where, $Comparator-I$, $Comparator-II$, and $Comparator-III$ use *Ib*, *IIIb*, and *IVb* maps, respectively. For each comparator, all the six maps from the single and cascaded oscillators run at one particular V_c. We wanted to make sure that the nominated combination would capture a low on-chip area, and the chosen V_c point for each oscillator is in a reasonable delay and power range while ensuring enough chaotic entropy to pass the statistical tests. In the presented RNG, $Comparator - I$, $Comparator - II$, and $Comparator - III$ use $V_c = 0.408\ V$, $0.474\ V$, and $0.904\ V$, respectively. For statistical tests, we generated 100 million binary bits, starting with 100 unique initial conditions where each initial voltage generates 1 million bits.

As mentioned earlier, the simulation is done in the SPICE (Simulation Program with Integrated Circuit Emphasis)-class circuit simulator of Cadence, called Spectre. We have not



(a) Ia (b) IIa (c) $IIIa$ (d) IVa

(e) Ib (f) IIb (g) $IIIb$ (h) IVb

FIGURE 11. The comparison of V_C variation-based CC between seed maps and corresponding cascaded pair of the same seed maps. In the cascade, both maps use the same V_C.

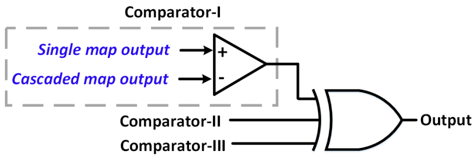


FIGURE 12. Schematic of the random number generator.

added any stochastic component in the simulations that are shown up to this point. Hence, the simulation results are purely deterministic. That means, with a specific V_c and initial condition, a chaotic oscillator made with two *IIa* maps, for example, will generate an identical chaotic sequence each time we run the simulation. As a result, the simulated number sequence from the proposed RNG is not truly random, since the simulation result is reproducible. This type of aperiodic but reproducible number sequence is called pseudo-random sequence and the circuit is called pseudo-random number generator (PRNG) [27]. Our proposed circuit acts as a PRNG in the simulation with no stochastic component added. However, in an integrated circuit (IC) chip, there will be inevitable cycle-to-cycle perturbations such as noise-driven drift of node voltages, power supply noise, temperature variation over the course of operation, and so on. These perturbations, even if they are small in amplitude, will eventually be amplified by the chaotic properties and the circuit will be close to a true-random number generator (TRNG) in practice [28]. To demonstrate the essence of this mechanism, we added normally distributed random noise (mean $= 0\ V$, standard deviation $= 0.1\ mV$) in the simulation. Two sets of 100 million data are generated from the TRNG, using the same set of 100 unique initial conditions in both cases. Then the correlation coefficient is calculated between these two sequences. A low correlation coefficient of 1.7×10^{-6} shows that the small noise perturbations got amplified by the chaotic nature of the circuit, satisfying the condition that the output of a truly random number generator is not reproducible.

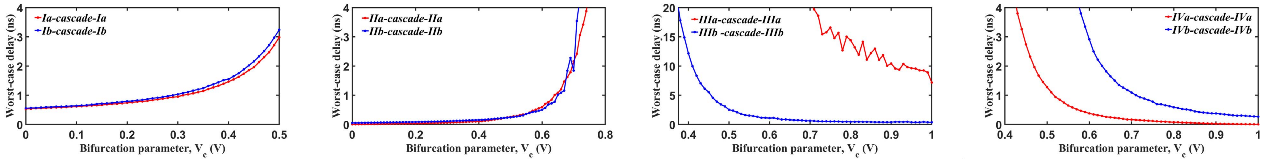
B. STATISTICAL TEST RESULTS

1) NIST SP 800-22 TEST SUITE

The test suite from the National Institute of Standards and Technology (NIST) offers 15 statistical sub-tests to measure the randomness in a sequence [29]. We ran the test with a bit-stream length of 1 million. The significance level was set to 0.01. Hence, a sequence with 100 million bits (containing 100 bit-streams) will pass a particular test if at least 96 out of the 100 bit-streams generate a p-values greater than 0.01. The test suite allocates each of the 100 generated p-values in 10 sub-intervals from 0 to 1 and evaluates the uniformity in the distribution with χ^2-test. The sequence under test can be considered uniform if the p-value generated from the χ^2-test (refers to $p-value_T$) is greater than or equal to 0.0001. NIST results, presented in FIGURE 15, show that both PRNG and TRNG sequences pass all requirements of 15 sub-tests.

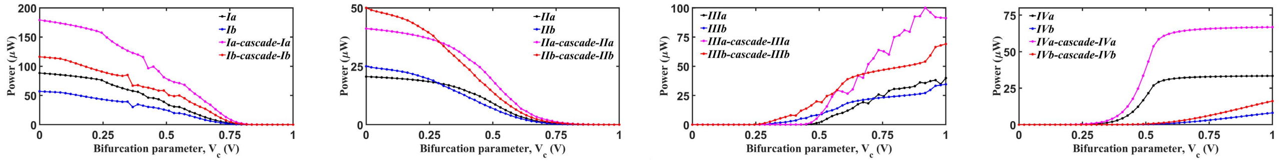
2) FIPS PUB 140-2

The Federal Information Processing Standards Publications (FIPS PUB) 140-2 test suite was developed by NIST [30]. FIPS tests the randomness of a binary sequence by dividing the sequence into 20,000-bit blocks. Hence, for a test sequence with 100 million bits, there will be 5000 blocks in total. The blocks are subjected to 4 sub-tests namely, Monobit, Poker, Runs, and Long run. The Monobit test counts the number of 1's in each 20,000-bit block. To pass the test, this number must be within the range of [9725, 10275]. The Poker test divides each 20,000-bit block into 5,000 successive 4-bit segments. The 4-bit segment can have 16 possible values. The occurrences of 16 values are counted and stored. This sub-test examines the uniformity of the 4-bit segment. Runs test counts and stores the maximum sequence of consecutive 1's or 0's in a 20,000-bit block. A run of 26 or more of either 1's or 0's is defined as a Long run. The total number of Long runs in a 20,000-bit block is counted as the total failure. TABLE 2 shows the FIPS test result for PRNG and TRNG sequences. The second column (from the left) of TABLE 2 shows the total number of blocks passing the test and the



(a) $Topology - I$ (b) $Topology - II$ (c) $Topology - III$ (d) $Topology - IV$

FIGURE 13. Worst-case delay of the chaotic oscillators. In the cascade, both maps use the same V_c.



(a) $Topology - I$ (b) $Topology - II$ (c) $Topology - III$ (d) $Topology - IV$

FIGURE 14. Power consumption of the chaotic oscillators. In the cascade, both maps use the same V_c.

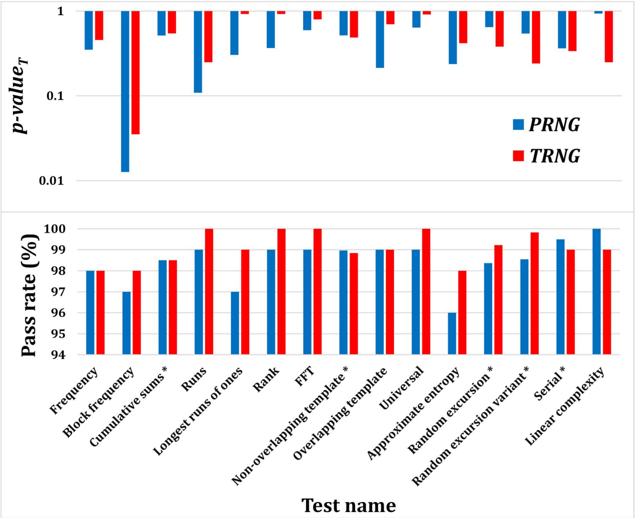


FIGURE 15. NIST results. Here, '*' marks the average of multiple tests.

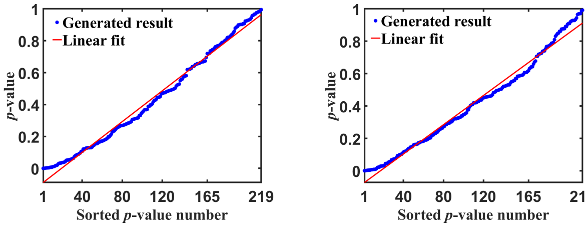
last four columns show the number of failed blocks under corresponding sub-tests.

3) DIEHARD STATISTICAL TEST SUITE

The Diehard statistical test suite was developed by George Marsaglia [31]. It generates 219 p-values under 15 sub-tests. A sequence is considered to be random if the generated p-values range between [0,1). On the other hand, if there are six or more (out of 219) p-values of either 0 or 1 then the sequence fails. Our test sequences contain 100,000,032 bits (with a padding of 32 1's at the beginning). FIGURE 16 shows the plots of p-values, organized in ascending order. The linear fits in both plots show close conformity with the generated p-value trends, indicating the desirable randomness in each sequence.

TABLE 2. FIPS test results.

PRNG	Total success	Monobit	Poker	Runs	Long run
PRNG	**4997**	-	1	1	1
TRNG	**4998**	-	1	1	-



(a) PRNG (b) TRNG

FIGURE 16. Diehard statistical test results.

TABLE 3. TestU01 results.

RNG	*Rabbit*	*Alphabit*	*BlockAlphabit*
PRNG	38/38	17/17	100/102
TRNG	38/38	17/17	99/102

4) TestU01

TestU01 offers a collection of utilities for the empirical statistical testing. This test suite comes as a software library generated in ANSI C language [32]. We ran three test batteries namely, *Rabbit*, *Alphabit*, and *BlockAlphabit*. The test sequence for this test contains 2^{20} bits, generated with one initial condition. Depending on this sequence size, the *Rabbit* test consists of 38 sub-tests whereas, *Alphabit* consists of 17 sub-tests and *BlockAlphabit* consists of 6 blocks of the same 17 sub-tests (102 tests in total). The sequence passes a sub-test if the generated p-value remains between

TABLE 4. Overhead comparison.

Parameter	Reported works						**Proposal**	**Alternative-I**	**Alternative-II**	
	[35]	[36]	[37]	[38]	[8]	[39]			**General**	n=25
Technology (nm)	180	180	180	65	65	45	**45**	**45**	**45**	**45**
Supply voltage (V)	1.8	1.8	1.8	1.2	1.2	1	**1**	**1**	**1**	**1**
Area ($10^3 \mu m^2$)	126	275	767	132	24	1.28	**0.33**	**0.11**	$n\times$**0.11**	**2.75**
Power ($10^2 \mu W$)	220	139	370	21.2	23.3	3.9	**1.43**	**1.41**	$n\times$**1.41**	**35.3**
Throughput (MS/s)	100	6400	120	100	200	270	**294**	**294**	$n\times$**294**	**7350**

0.001 and 0.999. TABLE 3 presents pass to the total number of sub-tests ratios in each case.

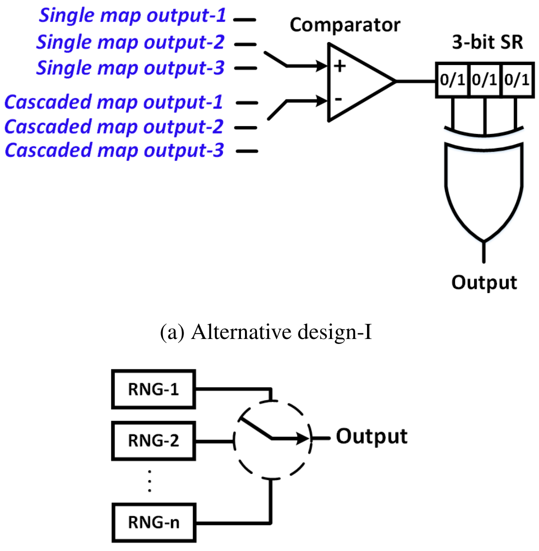
C. OVERHEAD ANALYSIS OF THE RNG

We have simulated our circuit in Cadence with 45 *nm* CMOS process and 1 V power supply. We analyzed the area, delay, and power profile of each of the components separately to optimize the whole RNG design. Considering two maps in the single oscillator (FIGURE 4(a)) and four maps in the cascaded oscillators (FIGURE 4(b)), we have a total of 18 maps from all six oscillators in the proposed three-comparator RNG design. The total area of six chaotic oscillators is 0.809 μm^2. The worst-case delay of the cascaded oscillators, at the chosen V_c points are 1.6 *ns*, 3.4 *ns*, and 0.36 *ns*. As the slowest oscillator governs the overall speed, the analog voltage generation rate from the oscillator portion of the circuit is 3.4 *ns*. The total power of six chaotic oscillators is 140.65 μW.

We have implemented the 45 *nm* design of a standard latch-type comparator, originally proposed by [33] in a larger technology node of 5 V power supply. We have verified that, in our supply voltage range of 1 V, the performance of this basic design is as good as a more advanced and complex (larger area) design proposed in [34]. The area of the comparator is 110.6 μm^2, the worst-case delay of the comparator is 0.4 *ns*, and the average power consumption is 1.9 μW. As a result, the overall area, power consumption, and bit generation rate of our proposed RNG design are 332.6 μm^2, 142.5 μW, and 294 MS/s.

D. PERFORMANCE IMPROVEMENT

We can accommodate additional design requirements by altering the proposed core RNG design. For example, the total area can be reduced by implementing an alternative design as presented in FIGURE 17(a). In this design, the added area and power overhead from the addition of a 3-bit shift register (SR) will be over-compensated by the deduction of two comparators. With an efficient setup of clocking for the selection mechanism at the comparator input and the 3-bit SR, we can ensure that the three bits from three pairs of single-cascade comparison will be ready for XORing within the worst-case delay of the slowest chaotic oscillator. As a result, the bit generation rate of the alternative design-I will be the same as the originally proposed design. This design can be useful where there is a tighter area constraint but slightly additional design complexity from the extra clocking for the selection mechanism is acceptable. On the other hand, if a design requires higher bit generation rate with a compromising area constraint then we may propose a design as shown in FIGURE 17(b). This design uses n copies of alternative design-I providing n-times more bit generation rate with respect to the alternative design-I. In this alternative design-II the area and power overhead will be increased by around n-times of the alternative design-I. We have verified that both of these alternative designs pass the statistical tests. TABLE 4 presents an overhead comparison between the proposed designs of this paper and some already reported designs. We can see that a significant improvement in the area and power overhead is achieved by the proposed designs.



(a) Alternative design-I

(b) Alternative design-II

FIGURE 17. Schematic of the alternative RNG designs.

V. CONCLUSION

We have demonstrated a hardware-efficient way of improving the chaotic performance of CMOS-based chaotic maps. The 45 *nm* designs of four chaotic map topologies are presented. With the help of eight unique chaotic maps, it is demonstrated that the cascade of multiple seed maps offers improved chaotic behavior over its constituent seed maps under certain constraints. This improved chaotic property of the cascading topology was utilized to propose a novel comparator-based RNG design that passes four standard statistical tests. Two alternatives of the proposed core design are presented to show the applicability in accommodating special design requirements. The proposed RNG designs have accomplished a significant reduction in area and power overhead compared to previous designs of similar kinds. The simple transistor-level seed maps along with the framework of cascading can be used to improve the chaotic performance and reduce the overhead cost of discrete-time chaotic systems. This work can be useful in different hardware security applications including side-channel attack mitigation by chaos-based reconfigurable logic and RNG-based data encryption.

REFERENCES

[1] H. Poincaré, *The Three-Body Problem and the Equations of Dynamics: Poincaré's Foundational Work on Dynamical Systems Theory*, vol. 443. Cham, Switzerland: Springer, 2017.

[2] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.

[3] B. Muthuswamy and S. Banerjee, *A Route to Chaos Using FPGAs*. Cham, Switzerland: Springer, 2015.

[4] M. W. Hirsch, S. Smale, and R. L. Devaney, *Differential Equations, Dynamical Systems, and an Introduction to Chaos*. New York, NY, USA: Academic, 2012.

[5] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Boca Raton, FL, USA: CRC Press, 2018.

[6] J. Gleick, *Chaos: Making a New Science*. Baltimore, MD, USA: Penguin, 2008.

[7] Y. Zhou, L. Bao, and C. P. Chen, "A new 1D chaotic system for image encryption," *Signal Process.*, vol. 97, no. 11, pp. 172–182, Apr. 2014.

[8] P. S. Paul, M. Sadia, and M. S. Hasan, "Design of a dynamic parameter-controlled chaotic-PRNG in a 65 nm CMOS process," in *Proc. IEEE 14th Dallas Circuits Syst. Conf. (DCAS)*, Nov. 2020, pp. 1–4.

[9] R. Agrawal, L. Bu, E. D. Rosario, and M. A. Kinsy, "Towards programmable all-digital true random number generator," in *Proc. Great Lakes Symp. VLSI*, Sep. 2020, pp. 53–58.

[10] M. S. Hasan, A. S. Shanta, P. S. Paul, M. Sadia, M. B. Majumder, and G. S. Rose, "Design of an enhanced reconfigurable chaotic oscillator using G4FET-NDR based discrete map," in *Proc. IEEE 14th Dallas Circuits Syst. Conf. (DCAS)*, Nov. 2020, pp. 1–5.

[11] M. Sadia, P. S. Paul, M. R. Hossain, and M. S. Hasan, "Design and analysis of a multi-parameter discrete chaotic map using only three SOI four-gate transistors," in *Proc. SoutheastCon*, Mar. 2021, pp. 1–7.

[12] K. Gołofit and P. Wieczorek, "Chaos-based physical unclonable functions," *Appl. Sci.*, vol. 9, no. 5, p. 991, Mar. 2019.

[13] M. S. Hasan, M. B. Majumder, A. S. Shanta, M. Uddin, and G. S. Rose, "A chaos-based complex micro-instruction set for mitigating instruction reverse engineering," *J. Hardw. Syst. Secur.*, vol. 4, no. 2, pp. 69–85, Jun. 2020.

[14] Z. Hua and Y. Zhou, "Exponential chaotic model for generating robust chaos," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 51, no. 6, pp. 3713–3724, Jun. 2021.

[15] A. S. Shanta, M. B. Majumder, M. S. Hasan, and G. S. Rose, "Physically unclonable and reconfigurable computing system (PURCS) for hardware security applications," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 40, no. 3, pp. 405–418, Mar. 2021.

[16] T. Gao and Z. Chen, "A new image encryption algorithm based on hyper-chaos," *Phys. Lett. A*, vol. 372, no. 4, pp. 394–400, 2008.

[17] D. Arroyo, R. Rhouma, G. Alvarez, S. Li, and V. Fernandez, "On the security of a new image encryption scheme based on chaotic map lattices," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 18, no. 3, Sep. 2008, Art. no. 033112.

[18] Y. Zhou, Z. Hua, C.-M. Pun, and C. L. P. Chen, "Cascade chaotic system with applications," *IEEE Trans. Cybern.*, vol. 45, no. 9, pp. 2001–2012, Sep. 2015.

[19] J. Lopez-Hernandez, A. Diaz-Mendez, R. Vazquez-Medina, and R. Alejos-Palomares, "Analog current-mode implementation of a logistic-map based chaos generator," in *Proc. 52nd IEEE Int. Midwest Symp. Circuits Syst.*, Aug. 2009, pp. 812–814.

[20] A. Farfan-Pelaez, E. Del-Moral-Hernandez, J. S. Navarro, and W. Van Noije, "A CMOS implementation of the sine-circle map," in *Proc. 48th Midwest Symp. Circuits Syst.*, Aug. 2005, pp. 1502–1505.

[21] S. Callegari, G. Setti, and P. J. Langlois, "A CMOS tailed tent map for the generation of uniformly distributed chaotic sequences," in *Proc. IEEE Int. Symp. Circuits Syst. (ISCAS)*, vol. 2, Jun. 1997, pp. 781–784.

[22] P. Dudek and V. D. Juncu, "Compact discrete-time chaos generator circuit," *Electron. Lett.*, vol. 39, no. 20, pp. 1431–1432, Oct. 2003.

[23] P. Dudek and V. D. Juncu, "An area and power efficient discrete-time chaos generator circuit," in *Proc. Eur. Conf. Circuit Theory Design*, Sep. 2005, p. 87.

[24] M. J. Feigenbaum, "Quantitative universality for a class of nonlinear transformations," *J. Statist. Phys.*, vol. 19, no. 1, pp. 25–52, 1978.

[25] P. Grassberger and I. Procaccia, "Estimation of the Kolmogorov entropy from a chaotic signal," *Phys. Rev. A, Gen. Phys.*, vol. 28, no. 4, p. 2591, 1983.

[26] Z. Hua and Y. Zhou, "Dynamic parameter-control chaotic system," *IEEE Trans. Cybern.*, vol. 46, no. 12, pp. 3330–3341, Dec. 2016.

[27] F. Yu, L. Li, Q. Tang, S. Cai, Y. Song, and Q. Xu, "A survey on true random number generators based on chaos," *Discrete Dyn. Nature Soc.*, vol. 2019, pp. 1–10, Dec. 2019.

[28] I. Çiçek, A. E. Pusane, and G. Dundar, "A novel design method for discrete time chaos based true random number generators," *Integr.*, vol. 47, no. 1, pp. 38–47, 2014.

[29] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Booz-Allen and Hamilton Inc., McLean, VA, USA, Tech. Rep. NIST Special Publication 800-22, May 2001. [Online]. Available: https://apps.dtic.mil/sti/citations/ADA393366

[30] *140-2: Security Requirements for Cryptographic Modules*, Information Technology Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, USA, 2001.

[31] G. Marsaglia. *The Marsaglia Random Number Cdrom Including the Diehard Battery of Tests of Randomness*. Accessed: Jan. 10, 2022. [Online]. Available: https://web.archive.org/web/20160125103112/http://stat.fsu.edu/pub/diehard/

[32] P. L'Ecuyer and R. Simard, "TestU01: AC library for empirical testing of random number generators," *ACM Trans. Math. Softw.*, vol. 33, no. 4, pp. 1–40, 2007.

[33] T. Kobayashi, K. Nogami, T. Shirotori, and Y. Fujimoto, "A current-controlled latch sense amplifier and a static power-saving input buffer for low-power architecture," *IEEE J. Solid-State Circuits*, vol. 76, no. 5, pp. 863–867, May 1993.

[34] B. Goll and H. Zimmerman, "A comparator with reduced delay time in 65-nm CMOS for supply voltages down to 0.65 V," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 56, no. 11, pp. 810–814, Nov. 2009.

[35] F. Pareschi, G. Setti, and R. Rovatti, "Implementation and testing of high-speed cmos true random number generators based on chaotic systems," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 57, no. 12, pp. 3124–3137, Aug. 2010.

[36] 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.*, vol. 20, no. 2, pp. 385–389, Feb. 2011.

[37] H.-T. Yang, J.-R. Huang, and T.-Y. Chang, "A chaos-based fully digital 120 MHz pseudo random number generator," in *Proc. IEEE Asia–Pacific Conf. Circuits Syst.*, vol. 1, Dec. 2004, pp. 357–360.

[38] A. S. Shanta, M. S. Hasan, M. B. Majumder, and G. S. Rose, "Design of a lightweight reconfigurable prng using three transistor chaotic map," in *Proc. IEEE 62nd Int. Midwest Symp. Circuits Syst. (MWSCAS)*, Aug. 2019, pp. 586–589.

[39] P. S. Paul, M. Sadia, M. R. Hossain, B. Muldrey, and M. S. Hasan, "Design of a low-overhead random number generator using cmos-based cascaded chaotic maps," in *Proc. Great Lakes Symp. VLSI*, 2021, pp. 109–114.

PARTHA SARATHI PAUL (Graduate Student Member, IEEE) received the B.Sc. degree in electrical and electronic engineering from the Bangladesh University of Engineering and Technology, in 2014, and the M.Sc. degree in electrical and computer engineering from Oregon State University, in 2017. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, The University of Mississippi. His research interests include mixed-signal circuit design for chaos-based hardware security applications, such as random number generator and reconfigurable logic.

MAISHA SADIA (Graduate Student Member, IEEE) received the B.Sc. and M.Sc. degrees in electrical engineering from The University of Mississippi, in 2017 and 2019, respectively, where she is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering. Her research interests include vehicular ad-hoc network and chaos-based hardware security applications.

MD RAZUAN HOSSAIN (Graduate Student Member, IEEE) received the B.Sc. (Eng.) degree from the Department of Electrical Electronic and Communication Engineering, Military Institute of Science and Technology, Bangladesh, in 2015, and the M.Sc. degree from the Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND, USA, in 2019. He is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering, The University of Mississippi. His M.Sc. research focused on nano material-based sensor devices. His current research interests include neuromorphic computing and non-linear dynamics.

BARRY MULDREY (Member, IEEE) received the B.Sc. degree in electrical engineering from The University of New Orleans, in 2009, and the master's and Ph.D. degrees from the Georgia Institute of Technology, in 2014 and 2019, respectively. In 2020, he joined the Department of Electrical and Computer Engineering, The University of Mississippi, as an Assistant Professor. His research interests include analog verification, artificial intelligence (active learning), and analog computing.

MD SAKIB HASAN (Member, IEEE) received the B.Sc. degree in electrical and electronic engineering from the Bangladesh University of Engineering and Technology, in 2009, and the Ph.D. degree in electrical engineering from The University of Tennessee, Knoxville, TN, USA, in 2017. In 2019, he joined the Department of Electrical and Computer Engineering, The University of Mississippi, as an Assistant Professor. His research interests include semiconductor device modeling, VLSI design, secure nanoelectronic circuit design, and neuromorphic computing.