10-25-2022

A 2D Chaotic Oscillator for Analog IC

Partha Sarathi Paul
University of Mississippi, ppaul@go.olemiss.edu

Parker Hardy
University of Mississippi

Maisha Sadia
University of Mississippi

Md Sakib Hasan
University of Mississippi, mhasan5@olemiss.edu

Recommended Citation

P. S. Paul, P. Hardy, M. Sadia and M. S. Hasan, "A 2D Chaotic Oscillator for Analog IC," in IEEE Open Journal of Circuits and Systems, vol. 3, pp. 263-273, 2022, doi: 10.1109/OJCAS.2022.3216780.

IEEE Open Journal of
Circuits and Systems

Received 5 August 2022; revised 4 October 2022; accepted 19 October 2022. Date of publication 25 October 2022; date of current version 31 October 2022.

Digital Object Identifier 10.1109/OJCAS.2022.3216780

A 2D Chaotic Oscillator for Analog IC

PARTHA SARATHI PAUL (Graduate Student Member, IEEE), PARKER HARDY (Member, IEEE), MAISHA SADIA (Graduate Student Member, IEEE), AND MD SAKIB HASAN (Member, IEEE)

Department of Electrical and Computer Engineering, University of Mississippi, Oxford, MS 38677, USA

This article was recommended by Associate Editor D. Linaro.

CORRESPONDING AUTHOR: P. S. PAUL (e-mail: parthapsp149@gmail.com)

ABSTRACT In this paper, we have proposed the design of an analog two-dimensional (2D) discrete-time chaotic oscillator. 2D chaotic systems are studied because of their more complex chaotic behavior compared to one-dimensional (1D) chaotic systems. The already published works on 2D chaotic systems are mainly focused either on the complex analytical combinations of familiar 1D chaotic maps such as Sine map, Logistic map, Tent map, and so on, or off-the-shelf component-based analog circuits. Due to complex hardware requirements, neither of them is feasible for hardware-efficient integrated circuit (IC) implementations. To the best of our knowledge, this proposed work is the first-ever report of an analog 2D discrete-time chaotic oscillator design that is suitable for hardware-constrained IC implementations. The chaotic performance of the proposed design is analyzed with bifurcation plots, the transient response, 2D Lyapunov exponent, and correlation coefficient measurements. It is demonstrated that the proposed design exhibits promising chaotic behavior with low hardware cost. The real-world application of the proposed 2D chaotic oscillator is presented in a random number generator (RNG) design. The applicability of the RNG in cryptography is verified by passing the generated random sequence through four standard statistical tests namely, NIST, FIPS, TestU01, and Diehard.

INDEX TERMS Discrete-time chaos, chaotic IC, chaotic oscillator, 2D chaotic system, random number generator.

I. INTRODUCTION

THE BEHAVIOR of a non-linear dynamic system is referred to as chaotic when the system responds aperiodically and shows extreme sensitivity to even an infinitesimal change in the initial state [1]. Unlike the random aperiodicity of stochastic systems, the aperiodicity of chaotic systems is deterministic, implying that, given the same system parameters, an identical aperiodic sequence is reproducible. The extreme sensitivity of a chaotic system to the initial state is also known as the butterfly effect, signifying the fact that, two initial states, even if they are very close, will result in a drastic difference in the response of a chaotic system. Thanks to this deterministic aperiodicity and initial state sensitivity, chaotic systems have attracted the attention of the security research for applications such as chaos-based logic generator [2], random number generation [3], physically unclonable systems [4], cryptography [5], and so on.

According to the nature of time evolution, chaotic systems are divided into two classes: (i) continuous-time, where the governing function contains the time derivative terms and time steps of the trajectory are continuous, (ii) discrete-time, where the trajectory evolves in discrete time steps and at every time step, a non-linear function, called a chaotic map, generates the next state output by using the output of the previous state as the input. In this paper, we will be limiting our discussion to discrete-time chaotic systems. The number of state variables involved in a chaotic system dictates the dimension of that system. An n-dimensional discrete-time chaotic system consists of n mutually dependent chaotic maps that define the discrete-time dynamics of n state variables. In a one-dimensional (1D) chaotic system, one mapping function, for example, Logistic map, Sine map, or Tent map, defines the dynamic behavior of one state variable. The structure of 1D chaotic systems are simple, and hence, they are easier to implement. However, some recent chaos-based hardware security research publications have proposed two-dimensional (2D) chaotic systems arguing that the chaotic orbits of 1D chaotic systems can be

too simple to ensure security against modern signal estimation techniques [5], [6], [7], [8]. All of the proposed multi-dimensional (2D or higher) chaotic systems, until now, can be divided into two groups. The first group consists of the systems that are generated from some kinds of analytical manipulation of traditional mathematical function-based chaotic maps such as Sine map, Logistic map, Tent map, and so on. These analytical function-based 2D chaotic systems are limited to either software-based encryption algorithms [9], or hardware implementations in a purely digital Field Programmable Gate Array (FPGA) domain [8], [10]. Because of the large area and high power demand, the digital hardware implementations of the chaotic systems are not suitable for Complementary Metal Oxide Semiconductor (CMOS)-based integrated (IC) implementations with critical chip area and power constraints. One example of this type of applications with a low area and power budget is hardware-based security protocol for edge devices like the Internet of Things (IoT). The analog CMOS-based implementations of classical chaotic maps including Logistic map [11], Sine map [12], and Tent map [13], have been reported. However, in the analog CMOS implementations as well, the circuits turned out to be too complex and hardware-hungry to be used in hardware-constrained IC applications. The second group of the proposed multi-dimensional chaotic circuits includes, the mathematical model of a memristor-based 5^{th} dimensional Chua's circuit [14], microcontroller-based digital realization of discrete memristor-based 2D maps [15], analog circuits using off-the-shelf components such as, operational amplifiers, multipliers, and so on [16], [17], [18], [19], [20]. Since these aforementioned circuits contain either analog or digital off-the-shelf components, they are not suitable to be used in area and power-constrained IC designs.

In this paper, we are introducing a novel CMOS-based design of an analog discrete-time 2D chaotic oscillator. The proposed 2D chaotic oscillator comprises CMOS-based chaotic maps and analog voltage transformation circuits. Both the chaotic maps and transformation circuits are designed with significantly low transistor-count circuits that have made our proposed 2D chaotic system suitable for hardware-efficient IC applications. We have demonstrated the application of the proposed 2D analog oscillator in a chaos-based random number generator (RNG) circuit and verified its cryptographic applicability with four standard statistical tests.

In the remaining portion of the paper, Section II presents the general design framework of the proposed 2D chaotic oscillator, the details of the oscillator design in a 45 nm CMOS process is discussed in Section III, Section IV presents the chaotic performance analysis of the proposed 2D chaotic oscillator, Section V demonstrates an application of the proposed scheme in a chaos-based RNG, Section VI presents some directions for future development, and Section VII gives the concluding remarks.

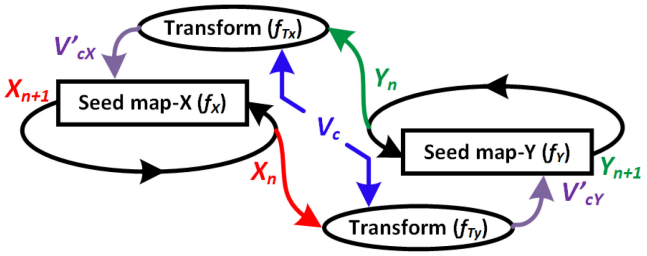


FIGURE 1. General framework of the 2D chaotic oscillator.

II. DESIGN FRAMEWORK

Equations (1) and (2) describe the scheme of the proposed 2D system. Here, there are two state variables, X and Y, involved. The functions, f_X and f_Y, denote two 1D non-linear mapping operations that depend on the control parameters, V'_{cX} and V'_{cY}, and the state variable value from the previous iteration, X_n and Y_n, respectively. The functions, f_{T_X} and f_{T_Y}, define two non-linear transformation operations that transform a global control variable, V_c, and the state variable of the second map (Y_n and X_n, respectively) to two new control variables, V'_{cX} and V'_{cY}, which are used in f_X and f_Y, respectively.

$$X_{n+1} = f_X\left(X_n, V'_{cX}\right);\ V'_{cX} = f_{T_X}(V_c, Y_n) \tag{1}$$

$$Y_{n+1} = f_Y\left(Y_n, V'_{cY}\right);\ V'_{cY} = f_{T_Y}(V_c, X_n) \tag{2}$$

The schematic of Figure 1 illustrates the general framework of the proposed 2D chaotic system. In the schematic, $Seedmap-X$ and $Seedmap-Y$ are two 1D chaotic map circuits with non-linear transfer characteristics. $Seedmap-X$ and $Seedmap-Y$ correspond to f_X and f_Y, respectively. Each chaotic map is a three-terminal circuit block containing an input terminal (X_n or Y_n), a control terminal (V'_{cX} or V'_{cY}), and the output terminal (X_{n+1} or Y_{n+1}). The voltage in the control terminal modulates the input versus output non-linearity of the 1D map circuit. The output of a 1D chaotic map is fed back to the same map's input to form a 1D chaotic oscillator. Here, the control parameter determines the chaotic property of the oscillator. As shown in Figure 1, the oscillating voltage of one 1D chaotic oscillator, for example, X_n, is passed through the transformation block (f_{T_X}) before being used as the control input, V'_{cY}, of the second 1D chaotic oscillator. Similarly, Y_n is transformed to generate V'_{cX}. The global control parameter, V_c, goes into both transformation blocks. Each transformation block couples both seed maps and ensures that both V'_{cX} and V'_{cY} are in a range of control input values for which the corresponding 1D chaotic oscillators are in the chaotic range. Consequently, the combined 2D oscillator also operates in the chaotic region across the whole range of V_c, resulting in a robust chaotic system.

III. DESIGN IMPLEMENTATION

A. 1D CHAOTIC OSCILLATOR

We have discussed in the previous section that a 2D chaotic oscillator consists of two 1D chaotic oscillators and the transformation blocks. In our design, we have implemented a 1D

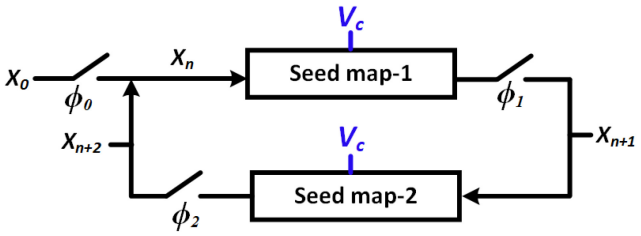


FIGURE 2. Schematic of a 1D chaotic oscillator.

chaotic oscillator as shown in Figure 2. According to the schematic, a 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 containing a seed map, *Seed map* -1, and we get the next state output, X_{n+1}. Generally, in the feedback path of a discrete-time oscillator, the voltage is sampled with switches, and the hold operation is performed with capacitors. We perform the sampling with two switches, ϕ_1 and ϕ_2, which are run by two non-overlapping clock pulses. To reduce the hardware cost in our design, the hold operation is performed with the parasitic capacitance of the transistors of a second seed map, *Seed map* -2. An iteration loop completes when the feedback path's output, X_{n+2}, is fed back to the forward path as the input for the next iteration. It is to be noted that, both *Seed map* -1 and *Seed map* -2 are implemented with two identical 1D chaotic maps. At each iteration, we sample out two analog voltages, X_{n+1}, and X_{n+2}. The discrete-time analog voltages are recorded for 15000 iteration loops. Then we get the steady-state output by discarding the first 1000 iterations. The steady-state discrete-time values are used for analyzing the chaotic performance.

B. 1D SEED MAP

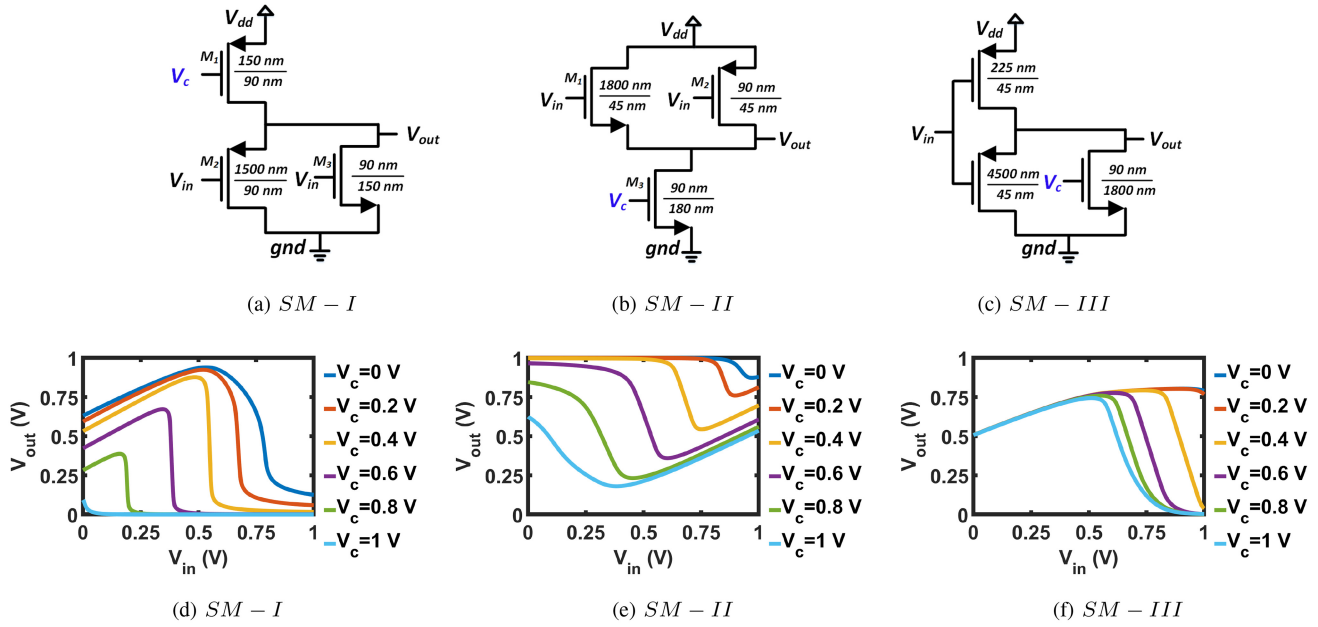
Figure 3 (a-c) shows the schematics of three chaotic maps that we have used as 1D seed maps (*SM*) to demonstrate the results of this paper. The seed maps perform the non-linear mapping operation of f_X and f_Y, as shown in (1) and (2). The 45 nm Cadence designs of the chaotic maps are done according to the topologies proposed in [1]. Figure 3 (d-f) shows the transfer characteristics of three seed maps at different control voltage (V_c) values. Two identical maps (for example, two $SM-I$) are used to form a 1D chaotic oscillator of Figure 2. Running the oscillator for 15000 iteration loops and discarding the first 1000, we get 14000 steady-state analog voltages (X_n), each time with different V_c. Figure 4(a-c) shows the plots of steady-state X_n with respect to corresponding V_c. These plots are called the bifurcation plots as they show how the chaotic behavior of an oscillator changes with the control voltage or bifurcation parameter, V_c. For example, Figure 4(a) corresponds to the 1D chaotic oscillator made with $SM-I$ which shows that the oscillator is chaotic for 0 V $< V_c <$ 0.25 V and then becomes periodic. On the other hand, Figure 4(c) enters into the chaotic region after $V_c \approx$ 0.6 V and Figure 4(b) is chaotic at the middle portion of the V_c range.

C. 2D CHAOTIC OSCILLATOR

The 2D chaotic oscillator of Figure 5 contains two 1D oscillators and four transformation blocks denoted with T_X and T_Y. The clocks are set up in a way so that the oscillating voltages of two 1D oscillators, X_{n+1}, X_{n+2}, Y_{n+1}, and Y_{n+2} are dynamically transformed during run-time by T_X and T_Y to generate the transformed control voltages (V'_{cX} or V'_{cY}) for each oscillator. The transformation blocks are designed in a way so that they can transform any combination of the oscillating voltages and the global control voltage, V_c, into a desirable range. The desirable range depends on a particular 1D chaotic oscillator; a range of control voltage across which the 1D oscillator is always chaotic. For example, the transformation block for $SM-I$ transforms any combination of V_c and X_n into 0 V to 0.25 V as, according to Figure 4(a), this is the chaotic region for $SM-I$.

D. TRANSFORMATION BLOCK

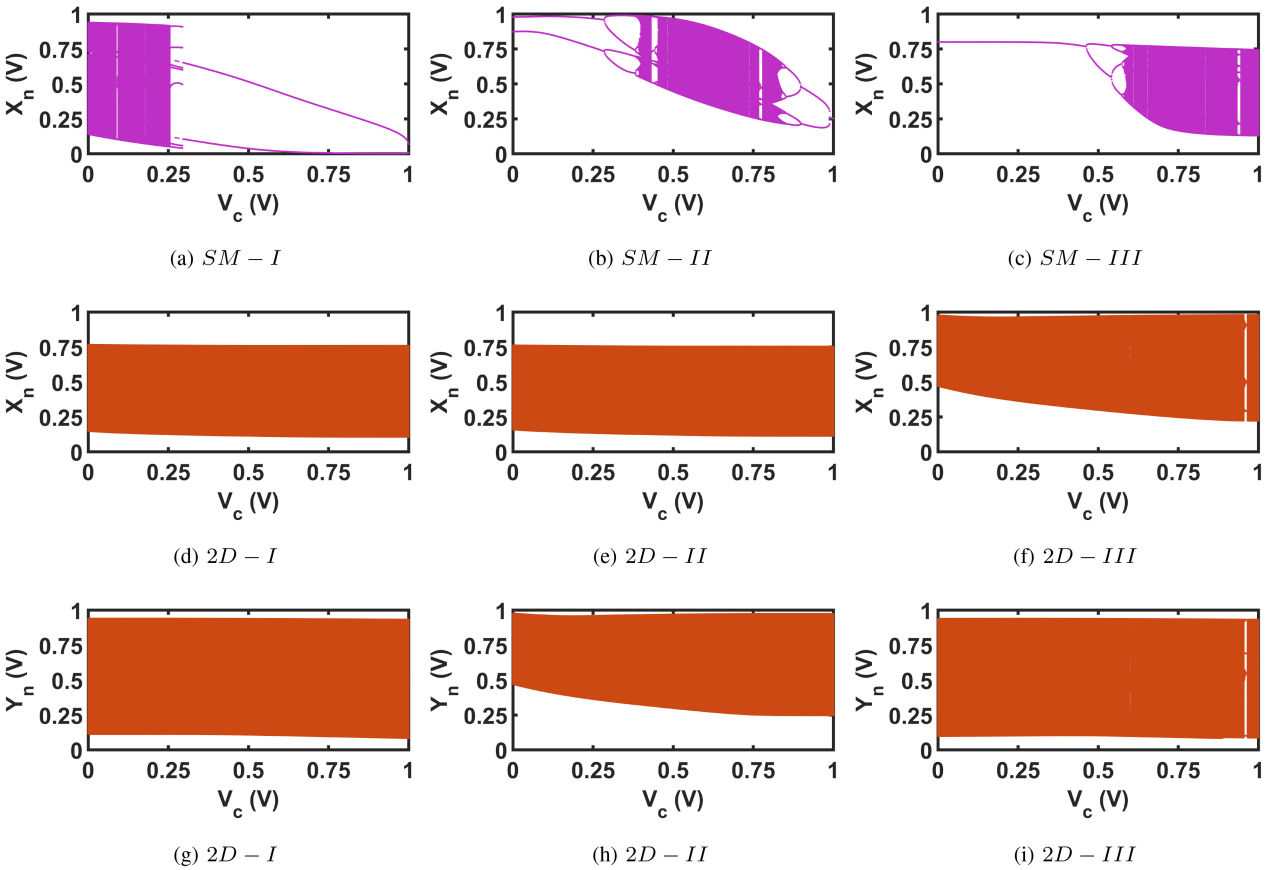
Figure 6(a-c) shows three topologies of transformation circuits. The design of a particular topology depends on the position of the chaotic region in the bifurcation plot of a 1D chaotic oscillator. For example, $T-I$ is suitable for transforming the output of a 1D chaotic oscillator where the chaotic region is positioned left to the middle (such as Figure 4(a)). Hence, each of the three transformation blocks corresponds to a particular seed map of our design: $T-I$ is for $SM-I$, $T-II$ is for $SM-II$, and $T-III$ is for $SM-III$. In the schematics of the transformation circuits, the input O_n denotes the oscillating voltage from the second 1D oscillator of the 2D chaotic oscillator, which can be X_n or Y_n, depending on which output is being transformed. We have kept two design variables for each circuit: the bias voltage, V_b, and the sizing parameter, W. The design variable W denotes the width of the V_b-gated transistor. We simulate for a range of V_b and W combinations to find for which combinations the transformed output (V'_{cX} or V'_{cY}) is in the chaotic range of a particular 1D chaotic oscillator. The green-marked regions of the plots of Figure 6(d-f) correspond to the desired combinations of V_b and W (denoted by the solution space, S). For example, as we can see in Figure 6(e), which corresponds to $S-II$, the coordinate point $W = 90$ nm and $V_b = 0$ V lies in the green solution space, and hence, we are using this values in our design. It is to mention that, although all the points in the green-marked regions are potential design choices, some combinations of V_b and W will result in more efficient designs than others. For example, $V_b = 1$ V or $V_b = 0$ V are particularly convenient design choices as we may directly use the supply voltage or the ground, respectively, which will save us from the need for an extra voltage regulator. In the case of choosing W, the closer the ratio, W/(90 nm) (the x-axis of Figure 6(d-f)), is to 1 the better as it will result in a more area-efficient design. The selected design choices are listed in the caption of Figure 6. Figure 6(g-i) shows the transfer characteristics of the transformation blocks for the selected design parameter values mentioned in the caption.



(a) $SM-I$ (b) $SM-II$ (c) $SM-III$

(d) $SM-I$ (e) $SM-II$ (f) $SM-III$

FIGURE 3. (a-c) Schematics and (d-f) transfer curves of 1D seed maps.



(a) $SM-I$ (b) $SM-II$ (c) $SM-III$

(d) $2D-I$ (e) $2D-II$ (f) $2D-III$

(g) $2D-I$ (h) $2D-II$ (i) $2D-III$

FIGURE 4. Bifurcation plots of: (a-c) 1D seed map oscillators, (d-f) *X* and (g-i) *Y* outputs of 2D oscillators.

IV. PERFORMANCE ANALYSIS

According to the above-mentioned design methodology in Section III, we have designed three 2D chaotic oscillators by combining two 1D chaotic oscillators each time from a pool of three: $2D-I$ is formed by combining $SM-III\&SM-I$, $2D-II$ is formed by combining $SM-III\&SM-II$,

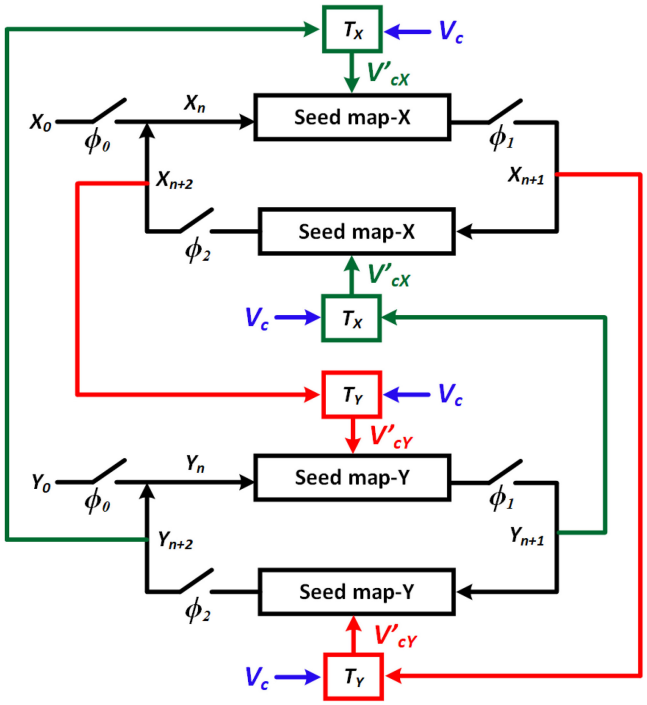


FIGURE 5. Schematic of 2D chaotic oscillator.

and $2D-III$ is formed by combining $SM-II\&SM-I$. The chip area of $2D-I$, $2D-II$, and $2D-III$ are 1.27 μm^2, 1.15 μm^2, and 0.74 μm^2, respectively. The chaotic performance of the 2D oscillators is analyzed based on the bifurcation plot, transient response, and two chaotic entropy metrics, Lyapunov Exponent and Correlation-coefficient.

A. BIFURCATION PLOT

Figure 4(d-i) presents the bifurcation plots of both voltage signals, X_n and Y_n, of the three 2D chaotic oscillators. As we can see, the chaotic regions of our 2D chaotic oscillators cover a wider range compared to the 1D chaotic oscillators. As a result, we are getting nearly uninterrupted chaotic regions across the whole design space from $V_c = 0$ V to $V_c = 1$ V, which is referred to as robust chaos [21]. Robust chaotic behavior is a desirable criterion of a chaotic system for multiple applications, including robust random number generation, chaos-based logic, and so on.

B. TRANSIENT BEHAVIOR

The transient behavior is an important aspect of chaotic oscillator design. To get a good throughput from the system we need to make sure that the time delay through each component is such that for a reasonable clock frequency the voltage at each node can be settled within the on-time of the clock period. Figure 7(a,c,e) shows the worst-case delay of the 2D oscillators for different V_c values. The maximum worst-case delay among all three delay profiles is close to 9 ns. Hence, we set the on-time of our clock pulse as 9 ns. Figure 8 shows the phases of the three clocks that are used to operate three types of switches on the oscillator, ϕ_0, ϕ_1, and ϕ_2. The clock period is 20 ns and the non-overlapping window between the switches, ϕ_1 and ϕ_2, is 1 ns. Figure 9 shows the transient responses of three 2D chaotic oscillators at $V_c = 0.6$ V. Each plot shows three traces for three very close initial states (denoted by X_0). We can see that initially, three traces follow each other until they diverge as a result of the initial state sensitivity or the butterfly effect. Figure 7(b,d,f) shows the power profile of three 2D chaotic oscillators. The power profile is generated by averaging the total power of 50 iteration cycles at different V_c values.

Algorithm 1 Algorithm for 2D LE Calculation

$sum \leftarrow 0$
$Q_0 \leftarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
for $i = 1 \rightarrow iterationcount$ **do**
  $J \leftarrow \begin{bmatrix} \frac{d}{dX}(f_X) & \frac{d}{dY}(f_X) \\ \frac{d}{dX}(f_Y) & \frac{d}{dY}(f_Y) \end{bmatrix}$
  $F \leftarrow J * Q_0$
  $[Q\ R] \leftarrow QRdecomposition(F)$
  if $i \geq Truncationamount$ **then**
    $Q_0 \leftarrow Q$
    $sum \leftarrow sum + log|diagonalelements(R)|$
  else
    $Q_0 \leftarrow \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
  end if
end for
$LE_1 \leftarrow max(Average(sum))$
$LE_2 \leftarrow min(Average(sum))$

C. LYAPUNOV EXPONENT

To quantify the initial state sensitivity of a chaotic system, the most widely accepted metric is the Lyapunov Exponent (LE). LE defines the average separation rate of two trajectories starting from two very close initial states where a positive LE value indicates chaotic behavior [22]. If a dynamical system has more than one positive LE, its trajectories will separate in several directions making the system hyperchaotic. The hyperchaotic behavior is more complex (hence, more secure) than the chaotic behavior [8], [15]. The analytical expression for LE of a 1D system is shown in (3) [23].

$$LE = \lim_{N\to\infty} \frac{1}{N} \sum_{i=0}^{N-1} ln \left| \frac{df_{1D}(X_n, V_c)}{dX} |_{X_i} \right| \tag{3}$$

Here, $f_{1D}(X_n, V_c)$ denotes the transfer function of a 1D map and N is the total iteration count. The LE of the 1D seed chaotic oscillators are calculated with 14000 steady-state discrete-time voltage values for each V_c and then plotted as shown in Figure 10(a-c).

To calculate LE for the 2D oscillator we have followed the algorithm presented in the MATLAB LE toolbox [24].

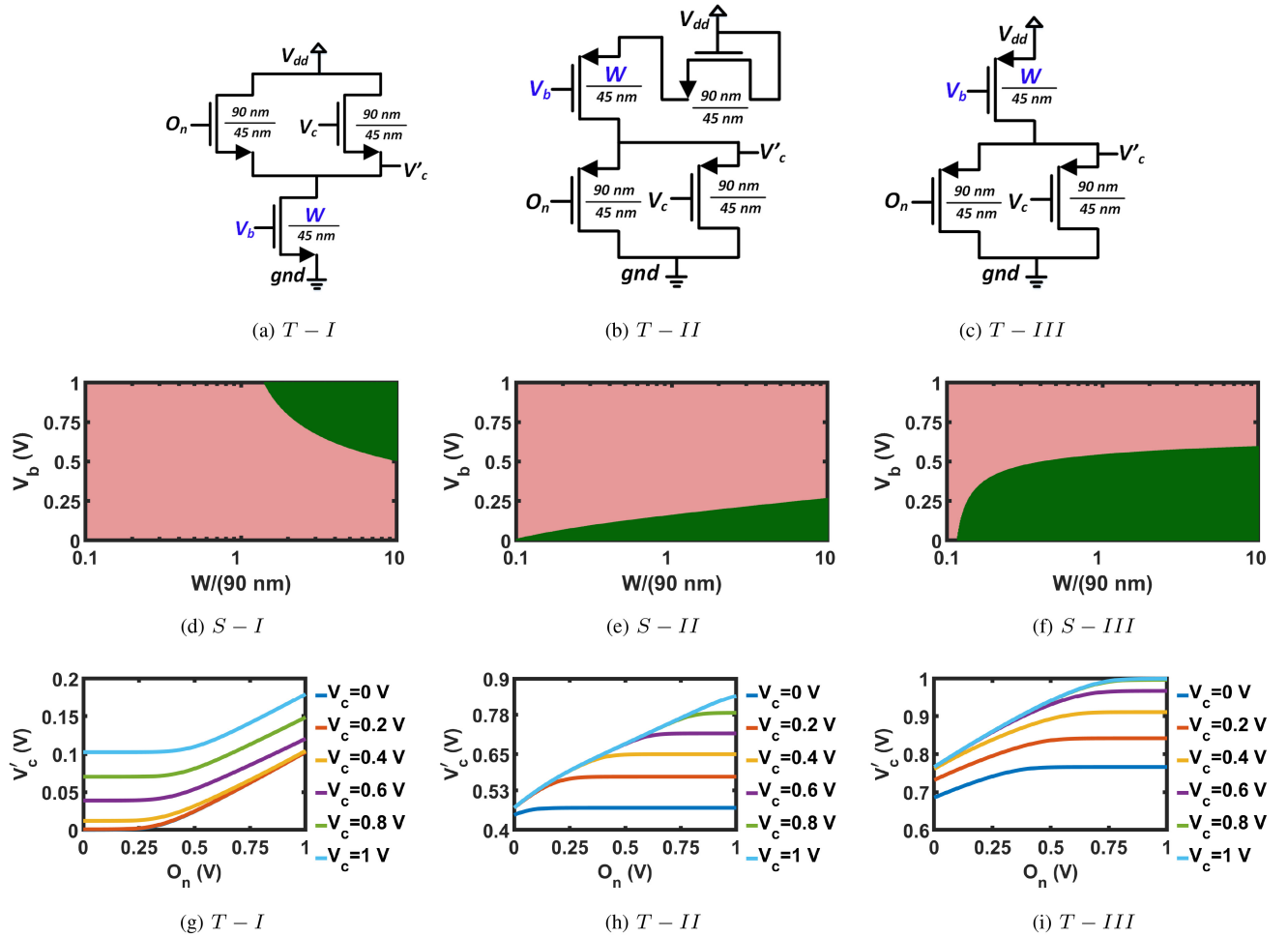


FIGURE 6. Transformation block (a-c) schematics, (d-f) plots of solution spaces, and (g-i) transfer curves. Corresponding design parameter values: $T-I$: $W = 200$ nm, $V_b = 1$ V, (b) $T-II$: $W = 90$ nm, $V_b = 0$ V; $T-III$: $W = 90$ nm, $V_b = 0$ V.

The MATLAB algorithm is developed for nonlinear mapping functions that can be expressed analytically. However, since our nonlinear mapping is done by three-transistor MOS circuits (as shown in Figure 3(a-c)), we do not have analytical expressions for the transfer function. Hence, we generated a very high-resolution look-up table by using Cadence simulation so that we can interpolate a transfer function for any given V_c. We have used this look-up table-based data set to calculate the 2D LE based on Algorithm 1.

Figure 10 (d-f) shows both LE values (LE_1 and LE_2) of the 2D chaotic oscillators where we can see there exists hyperchaotic behavior in all three oscillators.

D. CORRELATION-COEFFICIENT

The sensitive dependence on the initial state can be verified by correlation coefficient measurement, as well [25]. Equations (4) and (5) analytically express two schemes of our correlation coefficient measurements. In the equations, the operator 'E[.]' denotes the expectation function, μ and σ are the mean value and standard deviation, respectively. For each measurement, we generated two sets (X and X' in one scheme, while Y and Y' in the other one) of steady-state sequences by starting with two very close initial states which are only 1 nV apart. We varied the initial state (X_0) of only one 1D chaotic oscillator among the two in the 2D system. That means, starting with X_0, we generated X and Y, while starting with $X_0 + 1$ nV we get X' and Y'. Then we calculate the correlation coefficients between X and X' to get CCX_{X0} while the correlation coefficient between Y and Y' gives us CCY_{X0}. We repeated the same calculation at different V_c values and plotted as shown in Figure 11. The chaotic behavior results in significant divergence between the two sequences which results in the correlation coefficient values close to 0. To measure CCY_{X0}, as we are varying the initial state in one 1D oscillator and measuring the correlation from the other 1D oscillator's output, this experiment shows the strength of coupling between the two 1D oscillators in the 2D system, as well.

$$CCX_{X_o} = \frac{E\left[(X-\mu_X)(X'-\mu_{X'})\right]}{\sigma_X \sigma_{X'}} \tag{4}$$

$$CCY_{X_o} = \frac{E\left[(Y-\mu_Y)(Y'-\mu_{Y'})\right]}{\sigma_Y \sigma_{Y'}} \tag{5}$$

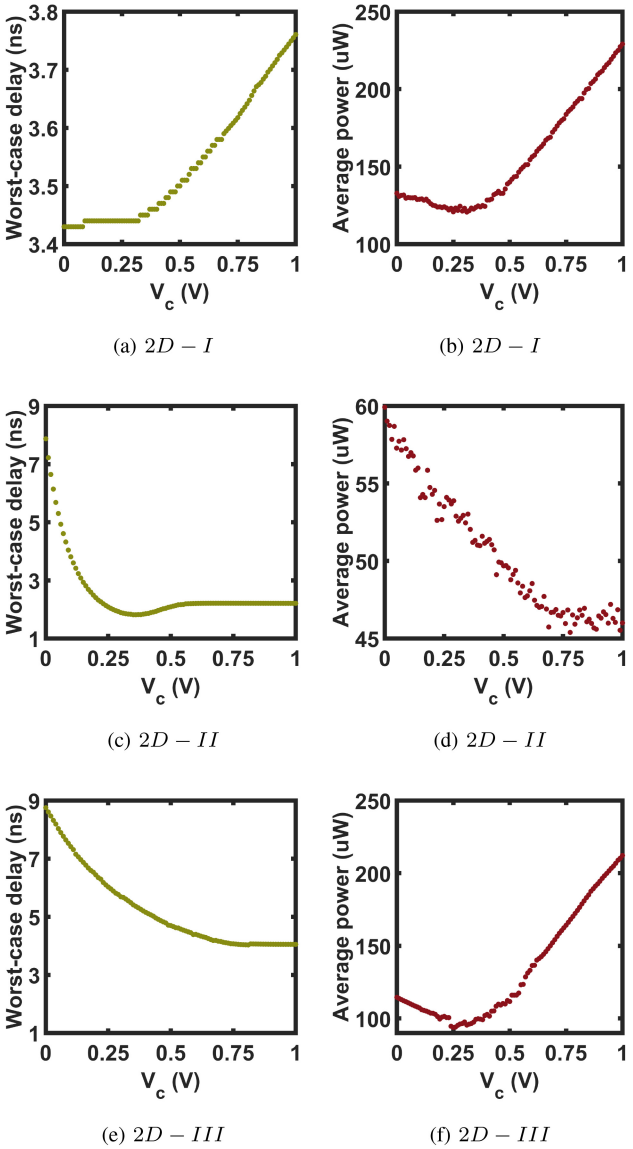


FIGURE 7. (a,c,e) The worst-case delay and (b,d,f) power profile of 2D oscillators.

V. APPLICATION

The proposed 2D chaotic oscillators show promising chaotic behavior including, hyper-chaos and wide chaotic window while offering a low area and power overhead with a reasonably small delay. Hence, this chaotic system can be useful in a number of hardware-based security protocols in the IC domain including, chaos-based logic generators for side-channel attack mitigation, physically unclonable systems, chaotic random number generation, and so on. In this paper, we are demonstrating the application of our proposed 2D system in a random number generator (RNG) circuit.

A. RNG STRUCTURE

Figure 12 shows the schematic of the RNG. The core architecture of this RNG was presented in [1]. Each of the four comparators in the RNG architecture compares between the outputs from two 2D chaotic oscillators. For example, $X-I$ comes from $2D-I$ and $CX-I$ comes from another $2D-I$ that is configured in a cascaded way, as shown in Figure 13. In the cascaded configuration, two copies of the same seed map are connected in series to harvest more chaotic entropy [1]. In the RNG architecture, $Y-I$ and $CY-I$ come from the Y-output of the same $2D-I$ and cascaded $2D-I$, respectively. Similarly, $X-II$, $CX-II$, $Y-II$, and $CY-II$ uses the $2D-II$ topology. Since the cascaded configuration has more delay compared to the regular one, we doubled the time period of the clocks shown in Figure 8 to run the RNG. V_c values of the four 2D oscillators used in RNG are set to the maximum LE_1 point for respective oscillators. The chip area of the RNG circuit combining all four 2D chaotic oscillators and the 4-input XOR gate is 449.5 μm^2. The average power consumption is 552.7 uW. We used 100 unique initial states and generated 1 million random bits (1s and 0s) for each state. The data set with that 100 million bits was used to perform four standard statistical tests to verify the randomness of the generated sequence. We have presented the results from each test as follows.

B. NIST

NIST SP 800-22 Test Suite from the National Institute of Standards and Technology (NIST) offers 15 statistical sub-tests to measure the randomness in a sequence [26]. We performed the test with a bit-stream length of 1 million and a significance level of 0.01. Hence, a sequence with 100 bit-streams (each bit-stream consists of 1 million binary bits) will pass a particular test if at least 96 out of the 100 bit-streams generate p-values greater than 0.01. The test suite allocates each one 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 is 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 are presented in Figure 14. The result shows that the generated sequence passes both the 96% threshold of the pass rate and 0.0001 $p-value_T$ threshold for all the 15 sub-tests.

C. FIPS

NIST developed the Federal Information Processing Standards Publications (FIPS PUB) 140-2 test suite [27]. FIPS verifies the randomness of a binary sequence by dividing the sequence into 20,000-bit blocks. As a result, for a test sequence with 100 million bits, there are 5,000 blocks in total. Each block is subjected to 4 sub-tests namely, Monobit, Poker, Runs, and Long run. The Monobit test counts the number of 1 in each 20,000-bit block. The number must be within the range of [9725, 10275] to pass the test. The Poker test is performed by dividing each 20,000-bit block into 5,000 successive 4-bit segments. Each 4-bit segment can have one of 16 possible values. This sub-test examines the uniformity of the 4-bit segment by counting and storing the occurrences of 16 values. In the Runs test, the maximum sequence of consecutive 1s or 0s in a 20,000-bit block are

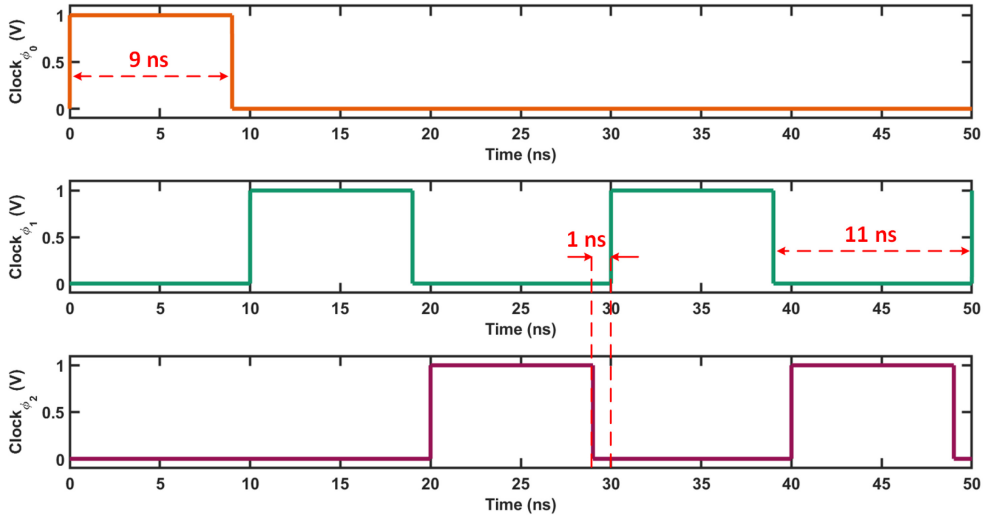


FIGURE 8. Phases of the three switches used in the oscillator.

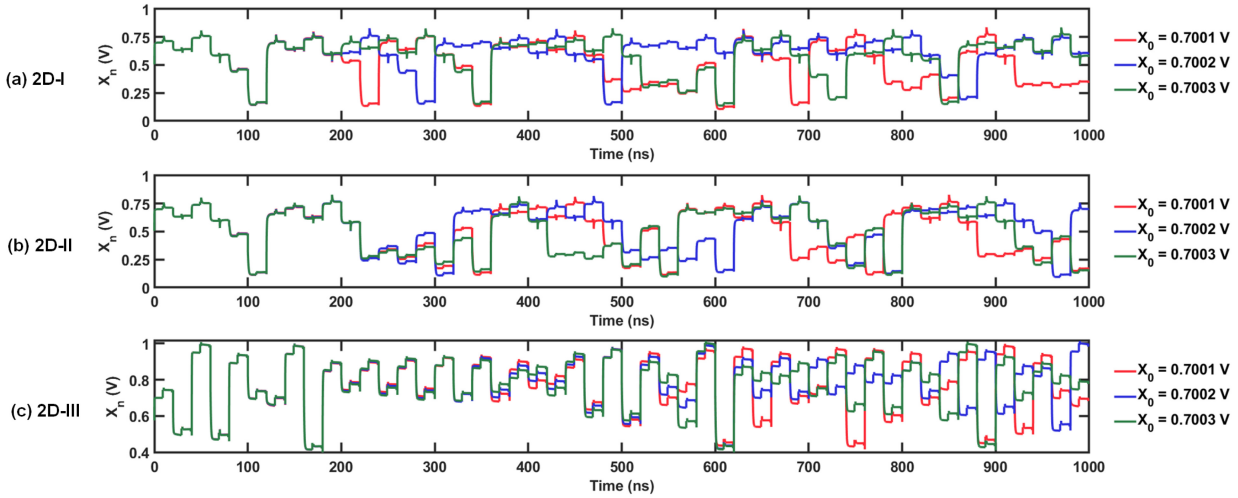


FIGURE 9. Transient response from 2D chaotic oscillators at V_C= 0.6 V.

TABLE 1. FIPS test results.

Total success	Monobit	Poker	Runs	Long run
4996	-	-	2	2

TABLE 2. TestU01 results.

Rabbit	*Alphabit*	*BlockAlphabit*
38/38	17/17	102/102

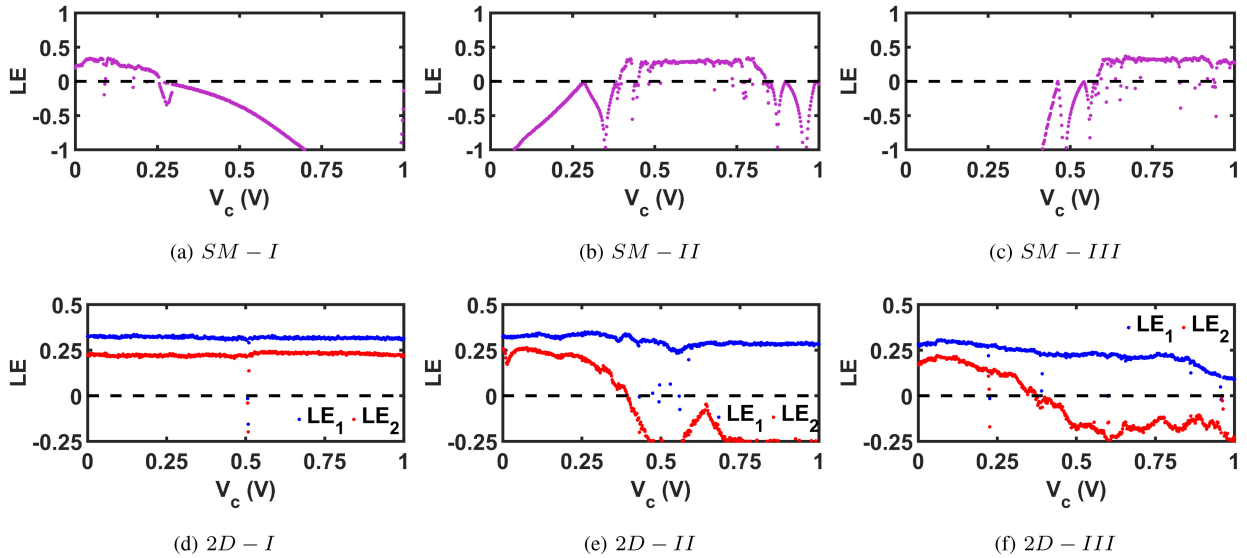
counted and stored. In the Long run test, a run of 26 or more of either 1s or 0s is defined as a Long run where the total number of Long runs in a 20,000-bit block is counted as the total failure. Table 1 shows the FIPS test result for the generated sequence. The first column (from the left) of Table 1 shows the total number of blocks passing the test and the last four columns show the number of failed blocks under each sub-test.

D. TESTU01

TestU01 comes as a software library generated in ANSI C language that offers a collection of utilities for empirical statistical testing [28]. We performed three test batteries namely, *Rabbit*, *Alphabit*, and *BlockAlphabit*. The test sequence for this test contains 2^{20} binary bits that was generated with one initial condition. Given 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 only if the generated p-value remains between 0.001 and 0.999. Table 2 presents the ratio between the number of passed test and the total number of sub-tests in each case.

E. DIEHARD

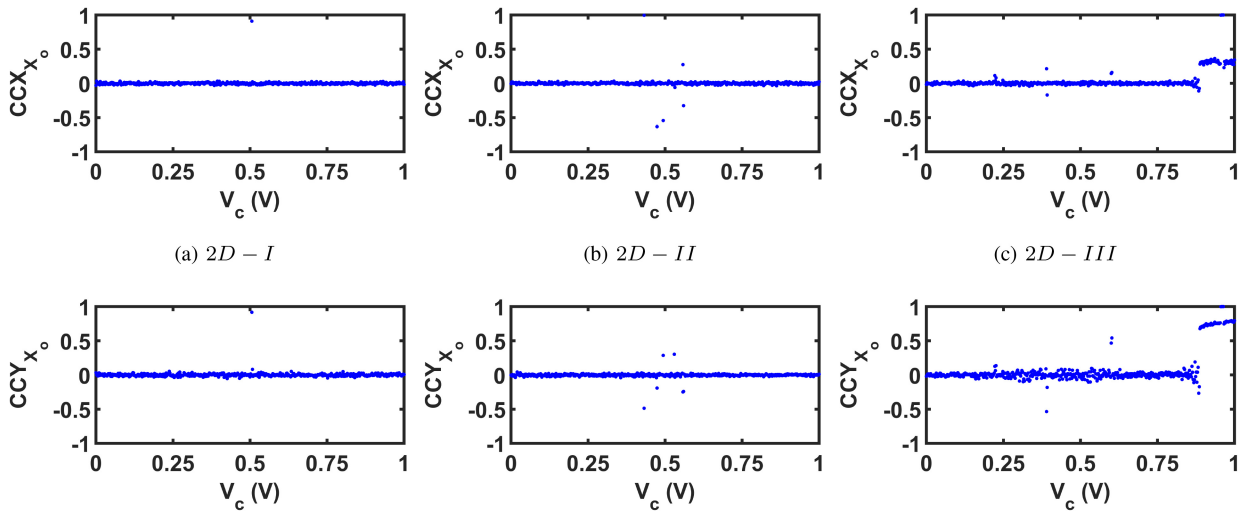
Diehard statistical test suite was developed by Marsaglia [29]. The suite generates 219 p-values under



(a) $SM-I$ (b) $SM-II$ (c) $SM-III$

(d) $2D-I$ (e) $2D-II$ (f) $2D-III$

FIGURE 10. *LE* plots of the 1D oscillators (a-c) and the 2D oscillators (d-f).



(a) $2D-I$ (b) $2D-II$ (c) $2D-III$

(d) $2D-I$ (e) $2D-II$ (f) $2D-III$

FIGURE 11. Correlation coefficient measurements for 2D oscillators.

15 sub-tests. A sequence is considered to be random if the generated p-values remain in the range [0,1). Conversely, if there are six or more (out of 219) p-values of either 0 or 1 then the sequence fails. Our test sequence contain 100,000,032 binary bits (a padding of 32 1s at the beginning). Figure 15 shows the plots of p-values, organized in ascending order. The linear fit in the plot shows a close conformity with the generated p-value trend, indicating the desirable randomness in the generated sequence.

VI. SCOPES FOR FUTURE RESEARCH

The proposed 2D chaotic oscillator scheme is very simple in the sense that the circuits, including the chaotic oscillator and non-linear transformation architecture, use very low transistor-count topologies. Moreover, the scheme is general as it can be adopted in a wide range of analog chaotic systems. In this paper, we are focusing on introducing the core concept of an IC-implementable 2D analog discrete-time chaotic oscillator and its applicability in real-world hardware security applications such as random number generation. The core idea demonstrated in this paper has opened up a wide window of scope for future research and development in the area of higher-dimensional chaotic system design. This scheme can be adopted to develop a 3D or even higher dimensional chaotic systems where there will be more than two chaotic oscillators and their transformation circuitry involved. The three-transistor 1D chaotic maps shown in this work can be further optimized or replaced by other topologies of 1D chaotic maps for achieving a higher chaotic complexity out of the 2D system. A library of improved 1D

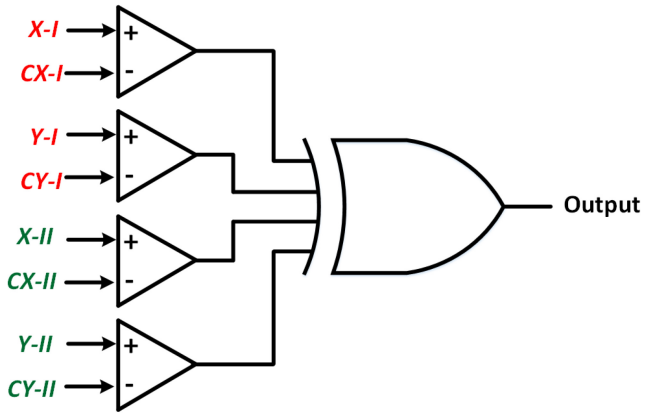


FIGURE 12. Schematic of the proposed RNG.

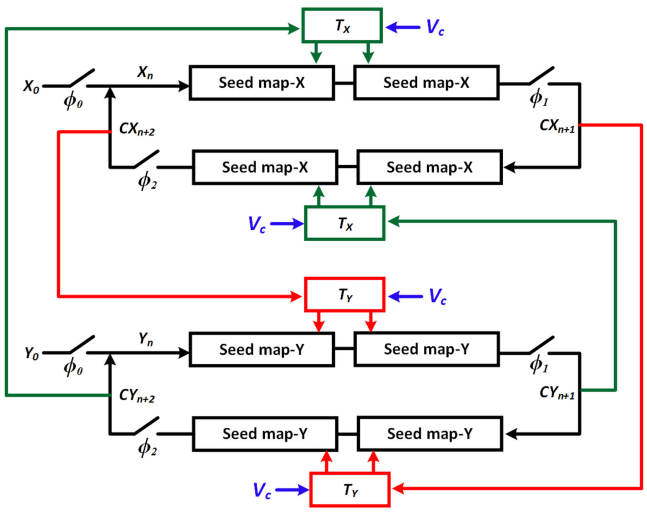


FIGURE 13. Cascaded configuration of the 2D chaotic oscillator.

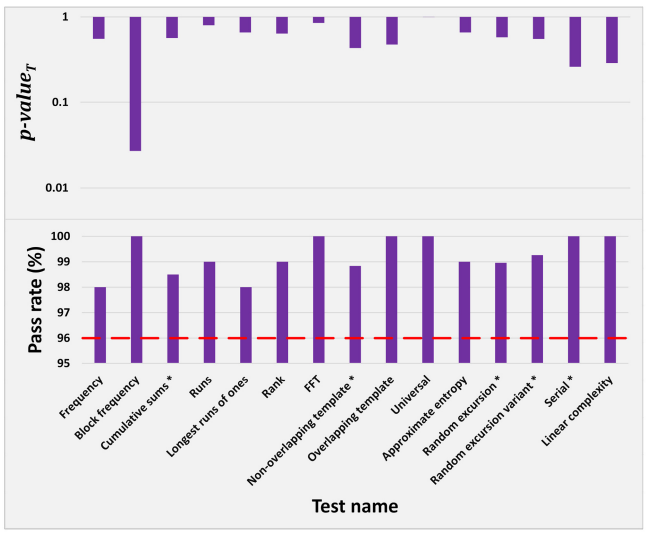


FIGURE 14. NIST results.

chaotic maps with a better chaotic entropy may lead to a more robust 2D (or higher dimensional) chaotic oscillator with a wider hyperchaotic window, higher *LE*, and as a result, a more area-efficient RNG or other hardware-security applications.

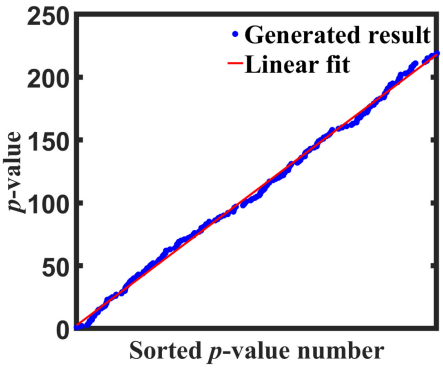


FIGURE 15. Diehard result.

VII. CONCLUSION

We have introduced the design of an analog 2D chaotic oscillator which is suitable for hardware-constrained IC implementation. The proposed 2D chaotic system comprises very low transistor-count 1D chaotic maps and transformation blocks, yet shows promising chaotic behavior. The proposed design framework of the 2D chaotic oscillator is general in the sense that it is applicable to a wide variety of 1D chaotic map circuits. The hyperchaotic behavior from this 2D chaotic oscillator and almost uninterrupted chaotic region across the whole design space can be very useful for designing robust and hard-to-break hardware-security applications. The applicability of the proposed 2D chaotic system is demonstrated in a RNG design. The randomness of the generated sequence from the RNG is verified through four established statistical tests. The sequence passes all of the tests justifying RNG's applicability in real-world hardware-based cryptographic applications. Future research scopes are discussed to point out the general adaptability of the proposed 2D scheme for a wide range of performance improvement explorations.

REFERENCES

[1] P. S. Paul, M. Sadia, M. R. Hossain, B. Muldrey, and M. S. Hasan, "Cascading CMOS-based chaotic maps for improved performance and its application in efficient RNG design," *IEEE Access*, vol. 10, pp. 33758–33770, 2022.

[2] 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*, 2021, pp. 1–7.

[3] 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.

[4] 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.

[5] Z. Hua, Y. Zhou, C.-M. Pun, and C. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.

[6] L. Moysis and A. T. Azar, "New discrete time 2D chaotic maps," *Int. J. Syst. Dyn. Appl.*, vol. 6, no. 1, pp. 77–104, 2017.

[7] H. Zhu, Y. Zhao, and Y. Song, "2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption," *IEEE Access*, vol. 7, pp. 14081–14098, 2019.
[8] Z. Hua, Y. Zhou, and B. Bao, "Two-dimensional sine chaotification system with hardware implementation," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 887–897, Feb. 2020.
[9] R. Kadir, R. Shahril, and M. A. Maarof, "A modified image encryption scheme based on 2D chaotic map," in *Proc. Int. Conf. Comput. Commun. Eng. (ICCCE)*, 2010, pp. 1–5.
[10] S. Chen, S. Yu, J. Lü, G. Chen, and J. He, "Design and FPGA-based realization of a chaotic secure video communication system," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 28, no. 9, pp. 2359–2371, Sep. 2018.
[11] 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.*, 2009, pp. 812–814.
[12] A. Farfan-Pelaez, E. Del-Moral-Hernández, J. Navarro, and W. Van Noije, "A CMOS implementation of the sine-circle map," in *Proc. 48th Midwest Symp. Circuits Syst.*, 2005, pp. 1502–1505.
[13] 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, 1997, pp. 781–784.
[14] Z. Wang, F. Min, and E. Wang, "A new hyperchaotic circuit with two memristors and its application in image encryption," *AIP Adv.*, vol. 6, no. 9, 2016, Art. no. 95316.
[15] H. Bao, Z. Hua, H. Li, M. Chen, and B. Bao, "Discrete memristor hyperchaotic maps," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 68, no. 11, pp. 4534–4544, Nov. 2021.
[16] W. Guang-Yi, B. Xu-Lei, and W. Zhong-Lin, "Design and FPGA implementation of a new hyperchaotic system," *Chin. Phys. B*, vol. 17, no. 10, p. 3596, 2008.
[17] C. Li, J. C. Sprott, W. Thio, and H. Zhu, "A new piecewise linear hyperchaotic circuit," *IEEE Trans. Circuits Syst. II, Exp. Briefs*, vol. 61, no. 12, pp. 977–981, Dec. 2014.
[18] C. Shen, S. Yu, J. Lü, and G. Chen, "A systematic methodology for constructing hyperchaotic systems with multiple positive Lyapunov exponents and circuit implementation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 61, no. 3, pp. 854–864, Mar. 2014.
[19] R. D. Méndez-Ramírez, A. Arellano-Delgado, M. A. Murillo-Escobar, and C. Cruz-Hernández, "A new 4D hyperchaotic system and its analog and digital implementation," *Electronics*, vol. 10, no. 15, p. 1793, 2021.
[20] W. Yu et al., "Design of a new seven-dimensional hyperchaotic circuit and its application in secure communication," *IEEE Access*, vol. 7, pp. 125586–125608, 2019.
[21] M. S. Hasan, P. S. Paul, M. Sadia, and M. R. Hossain, "Design of a weighted average chaotic system for robust chaotic operation," in *Proc. IEEE Int. Midwest Symp. Circuits Syst. (MWSCAS)*, 2021, pp. 954–957.
[22] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Physica D, Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.
[23] S. H. Strogatz, *Nonlinear Dynamics and Chaos: With Applications to Physics, Biology, Chemistry, and Engineering*. Boca Raton, FL, USA: CRC Press, 2018.
[24] S. Siu. "MATLAB Lyapunov exponents toolbox." 2022. [Online]. Available: https://www.mathworks.com/matlabcentral/fileexchange/233-let
[25] P. S. Paul, A. Dhungel, M. Sadia, M. R. Hossain, B. Muldrey, and M. S. Hasan, "Self-Parameterized chaotic map: A hardware-efficient scheme providing wide chaotic range," in *Proc. 28th IEEE Int. Conf. Electron., Circuits, Syst. (ICECS)*, 2021, pp. 1–5.
[26] 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 Hamilton, Inc., McLean, VA, USA, Rep. 800-22 Rev 1a, 2001.
[27] "Security requirements for cryptographic modules," Inf. Technol. Lab., Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. FIPS 140-2, 2001.
[28] 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.
[29] G. Marsaglia. "The marsaglia random number cdrom including the diehard battery of tests of randomness." 2014. [Online]. Available: https://web.archive.org/web/20160125103112/

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, University of Mississippi. His research area focuses on the mixed-signal circuit design for chaos-based hardware security applications.

PARKER HARDY (Member, IEEE) received the B.Sc. degree in electrical engineering from the University of Mississippi in May 2021, where he is currently pursuing the M.Sc. degree in electrical engineering. His interests include system design, mixed-signal circuit design, and software development, but mainly focuses on EDA tool-chain software development and VLSI design.

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

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, in 2017. He started as an Assistant Professor with the Department of Electrical and Computer Engineering, University of Mississippi in 2019. His research interests include semiconductor device modeling, VLSI design, secure nanoelectronic circuit design, and neuromorphic computing.