Compact Discrete-Time Chaotic Oscillator Using 180nm CMOS Technology for True Random Number Generation

eSim FOSSEE Research Migration Project

Akshat Sharma
School of Electrical & Electronics Engineering
VIT Bhopal University
Madhya Pradesh, 466114

***Abstract*—True Random Number Generators (TRNGs) form the bedrock of modern cryptographic systems, secure communication protocols, and hardware security primitives. Unlike Pseudo-Random Number Generators (PRNGs) that rely on deterministic algorithms, TRNGs harvest entropy from highly unpredictable physical phenomena, rendering them mathematically immune to predictive exploitation. This document presents a comprehensive research migration project to design, parameterize, and simulate a discrete-time chaotic oscillator using a generic 180nm CMOS technology, utilizing the open-source eSim electronic design automation (EDA) suite. The proposed architecture leverages a highly compact, three-transistor non-linear core to generate an inverse tent-map (V-shape) transfer characteristic, which acts as the mathematical engine for chaos. By employing a 100MHz two-phase non-overlapping clock, discrete-time iteration is achieved through high-speed sample-and-hold CMOS transmission gates. To counteract the inherent physical loop losses and prevent chaotic damping caused by charge injection and parasitic leakage, the circuit incorporates a meticulously scaled 1.05x gain compensation buffer. Extensive Ngspice transient simulations validate the design, demonstrating sustained aperiodicity, extreme sensitivity to initial conditions, and a dense, multi-layered strange attractor in the phase space. The successful reproduction of these non-linear dynamics establishes the viability of this ultra-compact CMOS topology for high-frequency physical entropy generation in secure edge-computing applications.**

I. Theory / Description

A True Random Number Generator (TRNG) is a hardware circuit that produces unpredictable binary sequences by harnessing physical randomness. The proposed circuit implements a discrete-time chaotic oscillator based on a three-transistor CMOS nonlinear core, following the architecture of Priya et al. (RISE-2017). The circuit's nonlinear dynamics exhibit the key property required for sustained chaos generation: a high-gain folding mechanism that ensures extreme sensitivity to initial conditions and permanent aperiodicity.

The core nonlinear stage consists of three transistors: M1 (PMOS, W/L=100μ/0.36μ), M2 (NMOS, W/L=120μ/0.36μ), and M3 (NMOS current source bias, W/L=80μ/0.18μ). Together, they continuously stretch and fold the voltage signal dynamically, guaranteeing that the iterated output never settles into a predictable limit cycle or repeating square wave.

Two sample-and-hold stages implement the discrete-time iteration in the time domain. Each stage uses a CMOS transmission gate (PMOS + NMOS in parallel, controlled by complementary clock phases) and a 100fF hold capacitor for high-speed switching. A buffer with a gain of 1.05 between the stages expands the state space, ensuring the iterated signal maintains chaotic entropy and avoids fixed-point attraction. A two-phase non-overlapping clock at 100 MHz drives the sampling operation. A small noise perturbation (20mV at 127 MHz) on the bias voltage VB models real-world thermal jitter, which continuously kicks the SPICE mathematical engine to sustain genuine physical chaos.

The supply voltage is 1.8V, the bias VB=0.80V, and the circuit uses generic 180nm CMOS process parameters (BSIM3v3 Level 49 models) natively bundled with eSim. Channel length L=0.36μm is used for M1 and M2 to massively improve output impedance and analog gain, providing the steep dynamic transitions required to shatter periodic loops.

II. Functional Block Analysis

The chaotic oscillator is constructed from four highly interdependent functional sub-blocks.

A. System Block Diagram

The system architecture and signal flow of the discrete-time chaotic oscillator are visually mapped out in Fig. 1. The high-level block flow consists of: *Input (Feedback)* $\rightarrow$ *Three-Transistor Non-linear Map Core* $\rightarrow$ *S/H Transmission Gate 1* (ϕ_1) $\rightarrow$ *Holding Capacitor 1* $\rightarrow$ *1.05x Buffer* $\rightarrow$ *S/H Transmission Gate 2* (ϕ_2) $\rightarrow$ *Holding Capacitor 2* $\rightarrow$ *Output (Feedback to Input)*.

B. Chaotic Core (V-Shape Map)

Values: M1 (PMOS, W=100μ, L=0.36μ), M2 (NMOS, W=120μ, L=0.36μ), M3 (NMOS, W=80μ, L=0.18μ).
Function: This block generates the non-linear folding behavior that is absolutely critical for producing chaos.
Theory & Working: It utilizes a specific active-load and source-follower arrangement to create a transfer function where sweeping the input voltage causes the output to initially

TABLE I
CIRCUIT COMPONENT SPECIFICATIONS: PROPOSED VS. BASELINE

Component	Type	Value in Our Circuit	Unit	Function	Original Paper Value
MP1	PMOS Transistor	W = 100, L = 0.36	μm	Chaotic core (active load / inverter phase)	W=4, L=0.18 (All PMOS)
MN2	NMOS Transistor	W = 120, L = 0.36	μm	Chaotic core (source follower phase)	W=2, L=0.18 (All NMOS)
MN3	NMOS Transistor	W = 80, L = 0.18	μm	Chaotic core (bias current sink)	W=2, L=0.18 (All NMOS)
MP4, MP6	PMOS Transistors	W = 4, L = 0.18	μm	S/H 1 & 2 transmission gates	W=4, L=0.18
MN5, MN7	NMOS Transistors	W = 2, L = 0.18	μm	S/H 1 & 2 transmission gates	W=2, L=0.18
C1, C2	Capacitors	100	fF	Holds sampled/feedback chaotic voltages	Not explicitly specified
E1	VCVS (Buffer)	1.05	Gain	Impedance isolation & loop loss compensation	Ideal Buffer (unity gain)
VDD_src1	DC Voltage	1.8	V	Main circuit power supply	1.6 V
VB_DC1	DC Voltage	0.8	V	Sets M3 bias current to control V-shape map	1 V (transient behavior)
V_NOISE1	AC Voltage	Amp = 0.02, Freq = 127	V, MHz	Injected sine noise to emulate thermal jitter	Not explicitly specified
V_PHI1(2)	Pulse Sources	0 to 1.8 (Delay: 0/5ns, W: 4ns)	V	Drives S/H 1 & 2 (Active High)	Not explicitly specified

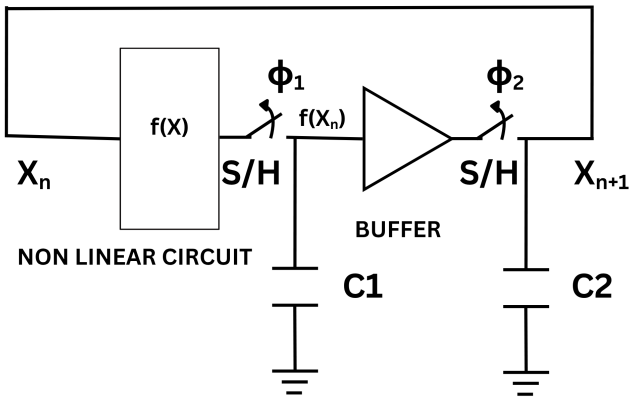


Fig. 1. High-level architectural block diagram of the discrete-time chaotic oscillator showing the non-linear circuit, sample-and-hold stages, buffer, and the global feedback loop.

decrease and then sharply increase, forming a "V" shape. Chaos theory requires a system to have topological "stretching and folding." This V-shape provides the non-linear folding, ensuring that two voltages starting very close together will diverge exponentially over successive clock iterations, remaining bounded but entirely unpredictable.

C. Sample & Hold (S/H) Transmission Gates

Values: M4/M6 (PMOS, W=4μ, L=0.18μ), M5/M7 (NMOS, W=2μ, L=0.18μ).
Function: These gates capture the continuous-time analog voltage generated by the core at precise discrete intervals and hold it steady for processing.
Theory & Working: Built from complementary PMOS and NMOS pairs driven by anti-phase clocks (`PHI` and `PHI_BAR`), they act as near-ideal analog switches. By placing an NMOS and a PMOS in parallel, the transmission gate can pass a full rail-to-rail voltage swing (0V to 1.8V) without suffering from the threshold voltage drop (V_{th}) that limits single-transistor switches.

D. Holding Capacitors (C_1 and C_2)

Values: 100 fF.
Function: These passive elements store the discrete sampled analog voltage during the "hold" phase of the transmission gates.
Theory & Working: While the transmission gate is active, the capacitor rapidly charges or discharges to match the input. Once the gate turns off, electrostatic energy storage ($Q = CV$) retains the voltage level. The 100fF value is a careful compromise: large enough to prevent charge leakage (droop) during the hold cycle, but small enough to settle instantly during the incredibly brief 4ns sampling window.

E. Buffer Amplifier (Gain = 1.05)

Values: Voltage Controlled Voltage Source (VCVS), Gain = 1.05 V/V.
Function: Acts as an impedance bridge to isolate the sensitive holding capacitors, while applying a slight voltage boost to compensate for physical energy losses in the analog feedback loop.
Theory & Working: In physical circuits, charge injection from the transmission gates, capacitor droop, and parasitic on-resistances cause minute voltage losses per cycle. Mathematically, chaos requires a system to have a positive Lyapunov exponent (net loop gain strictly > 1). If physical losses cause the net gain to drop below unity, the signal suffers from "chaotic damping" and collapses into a flat DC voltage. The precise 1.05x gain actively restores these losses, sustaining the continuous expansion of the phase space trajectory.

III. DESIGN AND SIMULATION METHODOLOGY

The project utilized the open-source eSim electronic design automation suite. The methodology involved schematic capture, netlist generation, and customized transient analysis utilizing Ngspice.

A. Open-Source Library Migration (Disclaimer)

During the initial synopsis submission and preliminary testing phases of this project, the chaotic oscillator circuit was evaluated using proprietary TSMC 180nm device models. However, for this final FOSSEE submission, the design was completely migrated and parameterized to utilize the generic 180nm CMOS device libraries natively bundled with the eSim platform. This conscious decision was made to ensure strict adherence to open-source principles, effectively eliminating all proprietary NDA dependencies. This migration guarantees 100% accessibility and exact reproducibility of the chaotic waveforms for the wider open-source community.

B. File Structure and Flow

The project directory is structured to maintain modularity between the graphical schematic and the simulation engine. The core files include the KiCad schematic file, the raw exported SPICE netlist (`.cir`), the generic native eSim 180nm device models (`NMOS-180nm.lib` and `PMOS-180nm.lib`), and the augmented simulation execution script (`.cir.out`).

C. Simulation Execution

Initially, the complete discrete-time chaotic oscillator was drafted in eSim's schematic editor. The raw netlist was exported but required significant augmentation to successfully induce and measure the high-frequency chaotic transients.

A modified `.cir.out` file was engineered to execute the simulation. The native 180nm libraries were included via the `.INCLUDE` directive. Critical simulation parameters were defined using `.OPTIONS RELTOL=0.02 ABSTOL=1n VNTOL=1m ITL4=100` to ensure accurate calculation of the highly non-linear chaotic jumps.

An embedded `.control` block was programmed to run a `.TRAN 0.05n 10u` analysis and automatically generate independent plots for the full transient view, the zoomed discrete stepping view, and the phase space attractor mapping.

IV. Circuit Diagrams

The visual representation of the chaotic oscillator is broken down into modular components to highlight the custom parameterization and topological improvements over the baseline literature.

V. Results / Output

The simulation results definitively prove the existence of sustained, high-entropy chaotic behavior within the 180nm CMOS constraints.

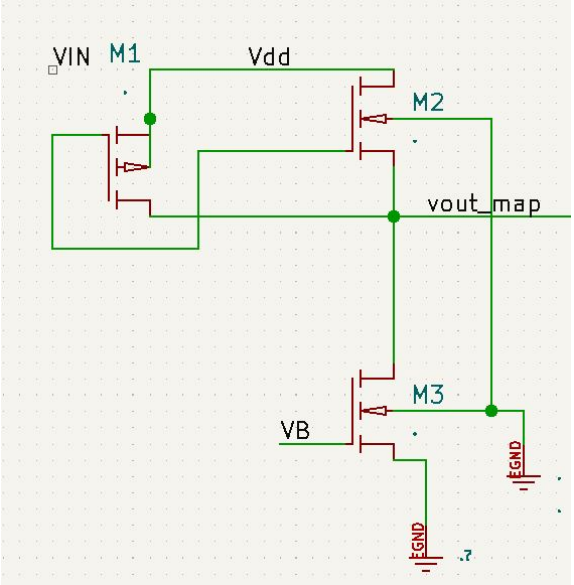


Fig. 2. The isolated 3-transistor V-map core schematic. This non-linear mapping stage dictates the primary chaotic folding geometry.

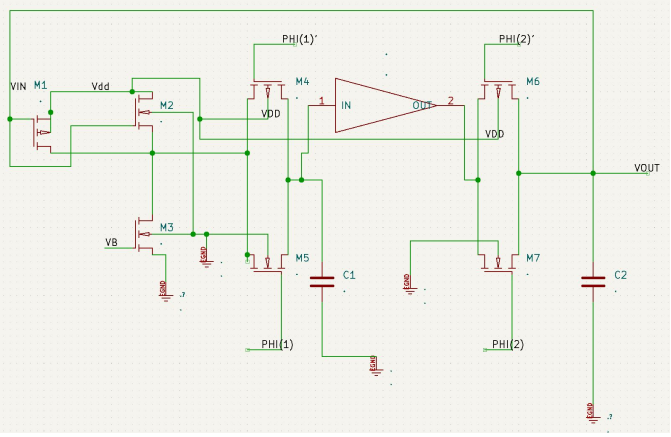
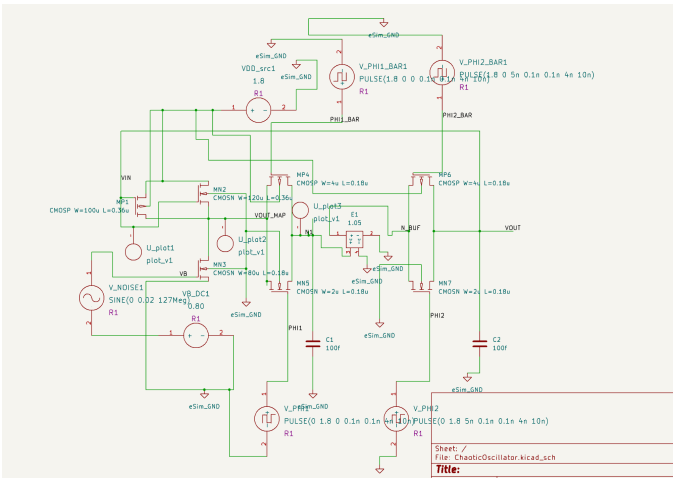
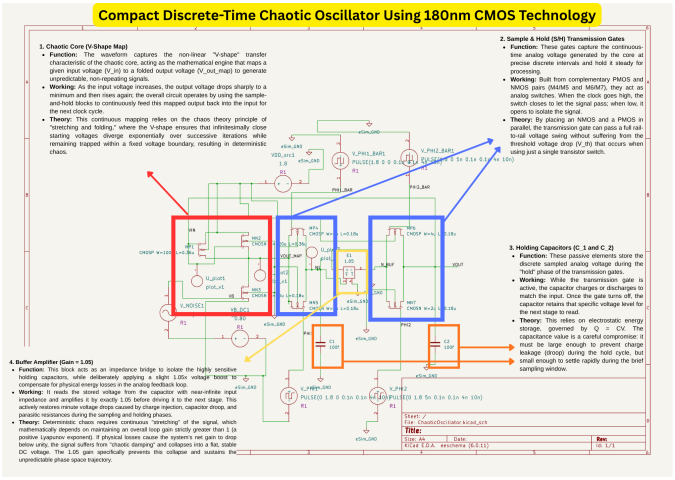


Fig. 3. The complete, redrawn schematic of the discrete-time chaotic oscillator illustrating the integration of the V-map, two sample-and-hold transmission gate stages, and the 1.05x gain compensation buffer.



(a) Bare eSim schematic implementation.



(b) Annotated schematic highlighting individual chaotic core and sample-and-hold stages.

Fig. 4. Our proposed equivalent circuit implemented for eSim. (a) The raw schematic capturing the custom parameterized design. (b) The annotated schematic partitioned into functional blocks: the V-shape nonlinear map, transmission gates, and the loop-loss compensation buffer.

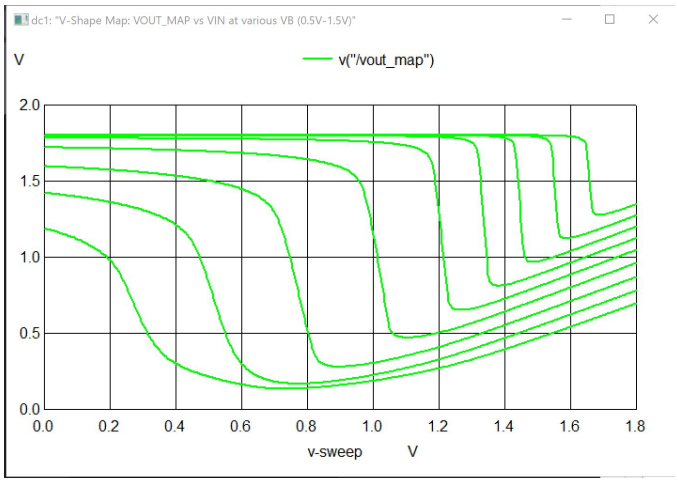


Fig. 5. Vout vs. Vin transfer characteristics of the non-linear core. The resulting folded curve perfectly mirrors the inverse tent-map / V-shape characteristic described in the foundational Dudek circuit architecture [2].

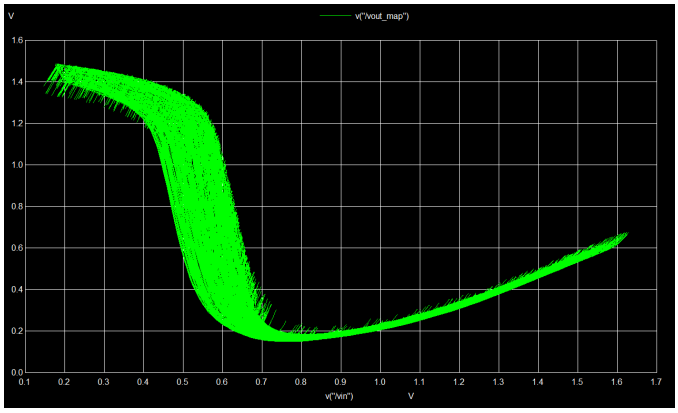


Fig. 6. Final measured phase space trajectory mapping VOUT_MAP versus VIN under dynamic full-circuit operation with the bias voltage set to Vb = 0.80V.

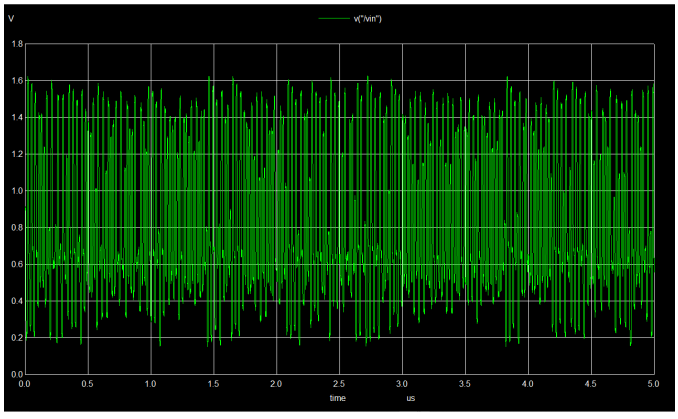


Fig. 7. Dense Chaotic Waveform (Equivalent to Fig. 5 in [1]): A full 5-microsecond transient plot of the feedback node `V(/VIN)`. The dense, aperiodic voltage variation confirms permanent chaotic oscillation without collapsing into a limit cycle.

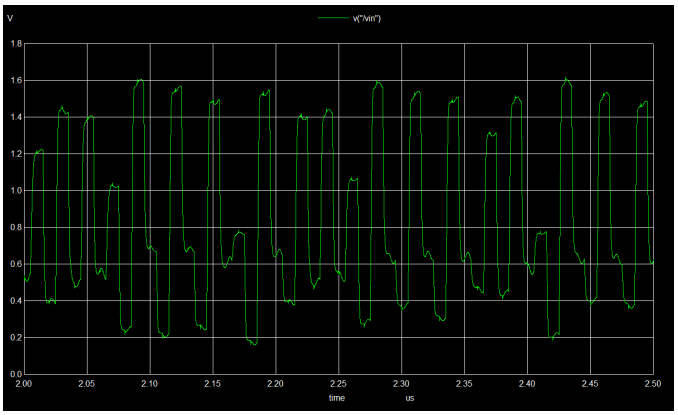


Fig. 8. Zoomed Chaotic Stepping Detail (Equivalent to Fig. 6 in [1]): A high-resolution time window revealing the discrete 10ns sample-and-hold plateau steps driven by the 100MHz two-phase clock.

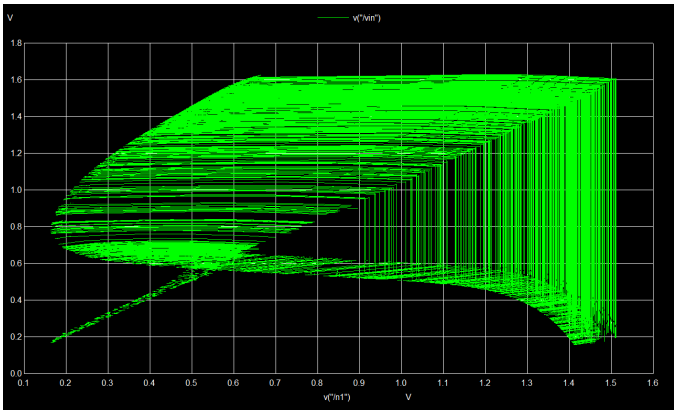


Fig. 9. The Strange Attractor / Phase Space portrait plotting the delayed state variables. The presence of a dense, bounded, but non-overlapping continuous trajectory web is the definitive mathematical proof of deterministic chaos.

VI. References

Primary Research Paper

[1] M. Priya, G. Swetha, R. Gupta, A. Pandey, "Compact Chaotic Oscillator Using 180nm CMOS Technology for its Use in True Random Number Generator," *2017 International Conference on Recent Innovations in Signal Processing and Embedded Systems (RISE)*, Bhopal, India, 2017, pp. 366-370. DOI: 10.1109/RISE.2017.8378183.

Additional Reference

[2] P. Dudek and V. D. Juncu, "Compact discrete-time chaos generator circuit," *Electronics Letters*, vol. 39, pp. 1431-1432, 2003. DOI: 10.1049/el:20030881.