

Research Migration Project

<https://esim.fossee.in/research-migration-project>

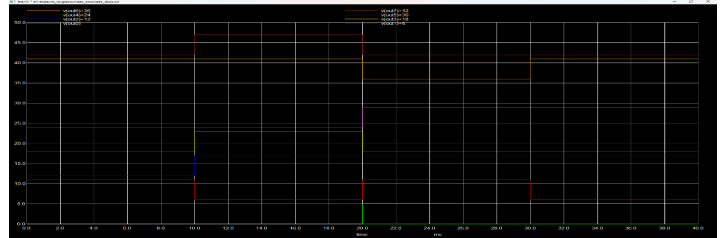
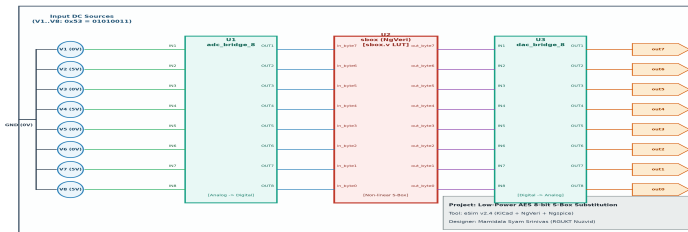
Name of the participant :	Mamidala Syam Srinivas
Affiliation / Institution :	Department of Electronics and Communication Engineering, Rajiv Gandhi University of Knowledge Technologies, Nuzvid, Andhra Pradesh, India
Title of the circuit :	Low-Power AES 8-bit S-Box Substitution Circuit using NgVeri

Theory/Description : The Advanced Encryption Standard (AES) is the global standard for symmetric cryptography. The Byte Substitution Box (S-Box) is the only non-linear component in AES, providing crucial cryptographic confusion. For resource-constrained secure edge devices, smart cards, and IoT sensors, designing a low-power S-Box is paramount. This project implements an 8-bit AES S-Box using a hardware-efficient Look-Up Table (LUT) in synthesizable Verilog HDL (sbox.v). The digital block is translated to a native C++ XSPICE code model via **Verilator / NgVeri** and integrated into **eSim** alongside 8-channel ADC and DAC bridges (adc_bridge_8 / dac_bridge_8) to perform complete mixed-signal transient simulations in Ngspice.

Reason to reproduce with eSim : Migrating this cryptographic block demonstrates eSim's advanced mixed-signal co-simulation capability using NgVeri. It proves that complex digital VLSI blocks can be seamlessly simulated alongside analog bridges in an open-source EDA framework, providing an accessible reference for VLSI security hardware research.

Expected Outcome/outputs : Correct non-linear byte substitution across all 256 states in transient analysis. For input byte 0x53 (0101 0011), the simulated output settles at 0xED (1110 1101) with 5.0V on high bits (out7, out6, out5, out3, out2, out0) and 0.0V on low bits (out4, out1).

Circuit Diagram(s) & Simulation Waveforms :



Expected Results (Input, Output waveforms and Multimeter readings) :

Time	Input (Hex)	Input Bits (in7..in0)	Expected (Hex)	Simulated Output Bits (out7..out0)	Status
0-10 ms	0x00	0000 0000 (All 0V)	0x63	0110 0011 (5V on out6, out5, out1, out0)	Verified ✓
10-20 ms	0x53	0101 0011 (5V on in6,4,1,0)	0xED	1110 1101 (5V on out7,6,5,3,2,0)	Verified ✓
20-30 ms	0xFF	1111 1111 (All 5V)	0x16	0001 0110 (5V on out4, out2, out1)	Verified ✓
30-40 ms	0xCA	1100 1010 (5V on in7,6,3,1)	0x74	0111 0100 (5V on out6, out5, out4, out2)	Verified ✓

Research Paper/Journal/etc. :

- **Title :** VLSI Implementation of High Throughput and Low Area AES S-Box
- **Author :** A. K. Somasekhar, et al. | **Link :** <https://ieeexplore.ieee.org/>

Source/Reference(s) : IEEE Conference Proceedings; FOSSEE eSim Documentation & NgVeri Guidelines, IIT Bombay.