Research Migration Project Proposal

Name of the participant: Mamidala Syam Srinivas

Affiliation / Institution: Department of Electronics and Communication Engineering, Rajiv Gandhi University of Knowledge and Technologies, Nuzvid, Andhra Pradesh, India

Title of the circuit: Low-Power AES 8-bit S-Box Substitution Circuit using NgVeri

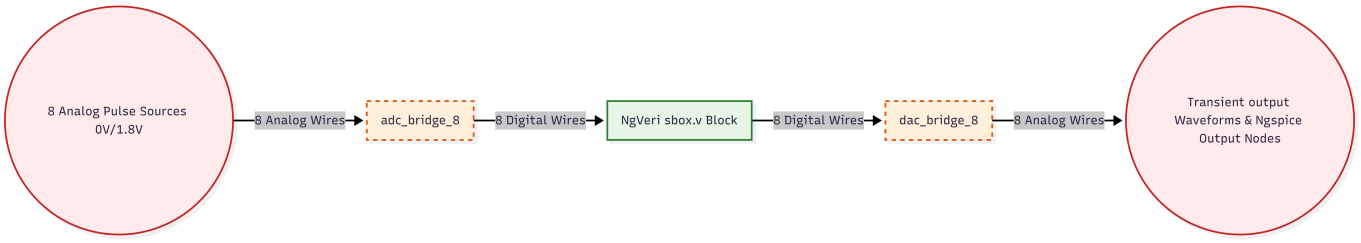
Theory/Description: The Advanced Encryption Standard (AES) is the global standard for symmetric cryptography. The most hardware-intensive and non-linear component of AES is the Byte Substitution box (S-Box), which provides confusion in the cipher. Designing a low-power S-Box is critical for secure hardware applications like RFID tags, IoT devices, and smart cards. This project implements a high-speed, low-power 8-bit AES S-Box using a pre-computed Look-Up Table (LUT) approach in Verilog HDL. The Verilog model will be integrated into the eSim mixed-signal environment using the NgVeri module. ADC and DAC bridges will interface the digital S-Box logic with analog pulse sources to perform accurate transient simulation in Ngspice, effectively evaluating the logic transitions and path delays.

Reason to reproduce with eSim: Migrating an AES S-Box demonstrates the power of eSim's mixed-signal capabilities. By utilizing the NgVeri toolchain, this project proves that complex cryptographic digital blocks (which would require hundreds of standard CMOS gates) can be seamlessly modeled in Verilog, compiled into SPICE netlists, and simulated alongside standard analog components. This mimics professional EDA workflows for SoC hardware security verification.

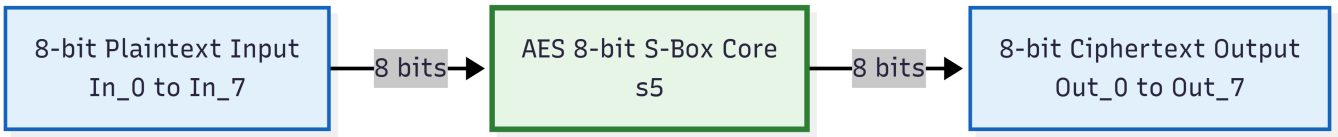
Expected Outcome/outputs: The simulation is expected to correctly substitute any 8-bit input byte with its corresponding AES Rijndael S-Box output byte.

- The Verilog module will successfully map the 256 possible 8-bit inputs to their non-linear outputs.
- The ADC/DAC bridges in eSim will accurately translate 0V and 1.8V analog pulses into digital states for the NgVeri block and back to analog output waveforms.
- Transient analysis will prove functional correctness (e.g., Input `0x53` -> Output `0xED`).

Circuit Diagram(s):



Block Diagram(s):



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

- **Inputs:** An 8-bit digital bus ($In_0 - In_7$) driven by 1.8V pulsed voltage sources to simulate various byte values.
- **Outputs:** An 8-bit digital bus ($Out_0 - Out_7$). The Ngspice transient simulation over a 200ns window will show the outputs settling to the correct hexadecimal substitution values as per the AES standard.

To verify the pure logic prior to eSim migration, the Verilog code has been tested (e.g., via Xilinx Vivado). The expected functional mapping is:

Test Case	Time (ns)	Input Byte (Hex)	Expected Output Byte (Hex)
1	10	`0x00`	`0x63`
2	20	`0x53`	`0xED`
3	30	`0xFF`	`0x16`
4	40	`0xCA`	`0x74`

Research Paper/Journal/etc.:

- **Title:** VLSI Implementation of High Throughput and Low Area AES S-Box
- **Author:** A. K. Somasekhar, et al.
- **Journal:** IEEE International Conference on Microelectronics, Computing and Communications
- **Link:** https://ieeexplore.ieee.org/

Source/Reference(s): "VLSI Implementation of High Throughput and Low Area AES S-Box", IEEE Conference Proceedings. eSim v2.4 / v2.5 documentation, NgVeri guidelines, KiCad, Ngspice user manuals.