Advance Encryption Standard (AES) core implemented in VHDL

# Introduction

This project consists of an AES encryption core that operates on a 128-bit keys and a 4 x 4 column-major order matrix of bytes termed the *state*. The implementation takes 10 clock cycles for a ciphered output to be generated.

# Specification

* Input:
  + 4 x 4 column-major order matrix *i\_state*
  + 4 x 4 column-major order key *i\_key*
  + Clock *clock*
  + Reset *reset*
* Output:
  + 4 x 4 encrypted column-major matrix *o\_state*
  + Valid encrypted output state *o\_valid*
* Toolset: Vivado 2018.1

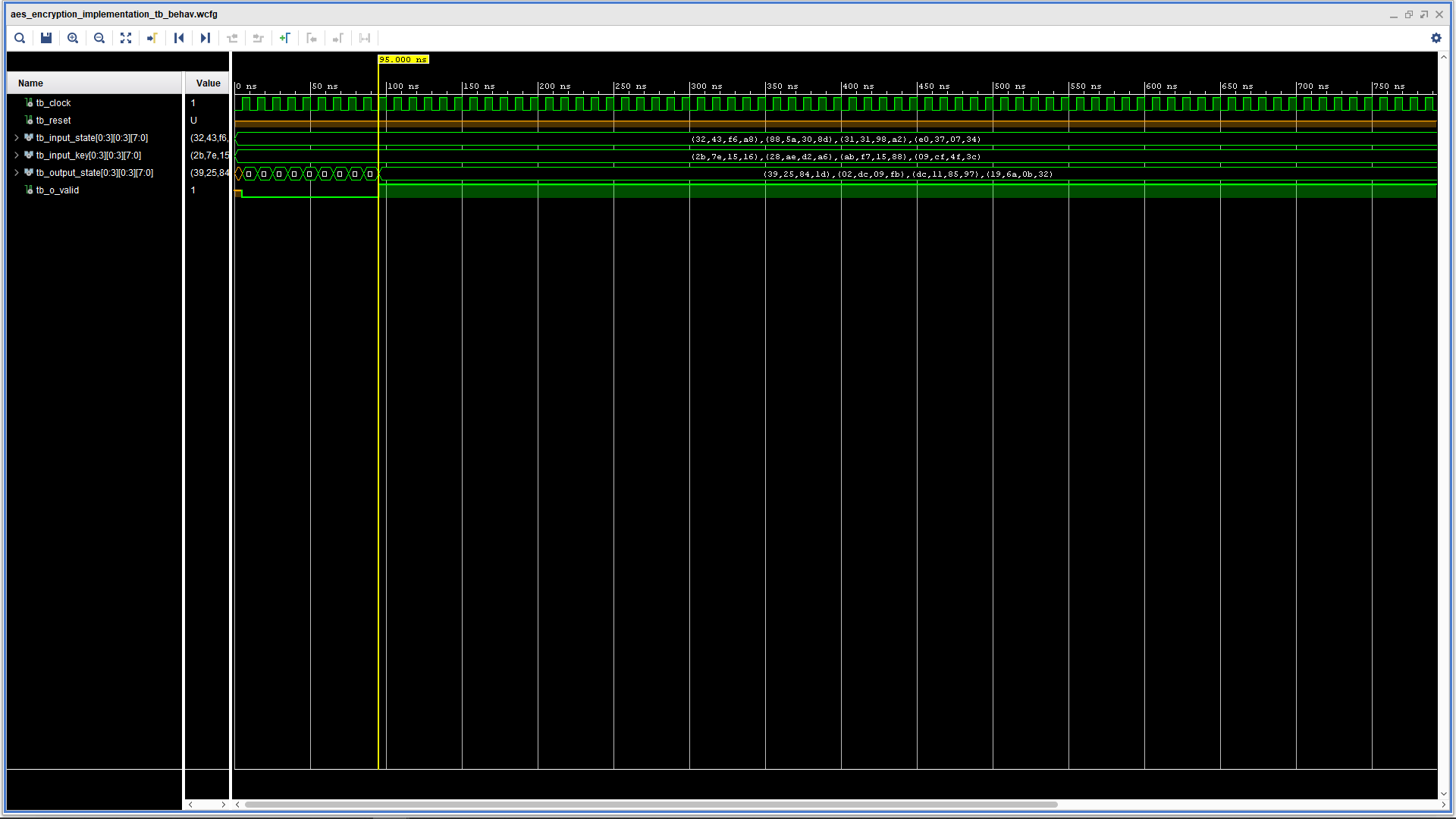
# Module Hierarchy

* **Aes\_encryption\_implementation** – top level with state machine
  + **Aes\_encryption\_key\_schedule** – generates the key schedule
    - **g\_function** – required for generating key schedule
      * **s\_box** – s-box substitution
  + **Aes\_encryption\_key\_addition** – first round addRoundkey implementation
  + **Aes\_encryption\_round**
    - **s\_box** – s-box substitution
    - **Aes\_encryption\_ShiftRows** – implements ShiftRows
    - **Aes\_encryption\_MixColumns** – implements mixColumns
    - **Aes\_encryption\_key\_addition** – implements addRoundKey
  + **Aes\_encryption\_last\_round**
    - **s\_box** – s-box substitution
    - **Aes\_encryption\_ShiftRows** – implements ShiftRows
    - **Aes\_encryption\_key\_addition** – implements addRoundKey

# Test bench

The project contains various testbenches for different modules that makes up the AES encryption core.

This includes the top-level testbench for the overall implementation. Below illustrates the waveform of the top-level waveform.

Running a testbench can be done by going into simulation sources in project manager, selecting the testbench as top then “run simulation” from the flow navigator.

# High Level Architecture

# References

Pub, N. F. (2001). 197: Advanced encryption standard (AES). *Federal information processing standards publication*, *197*(441), 0311.

Paar, C., & Pelzl, J. (2009). *Understanding cryptography: a textbook for students and practitioners*. Springer Science & Business Media.