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

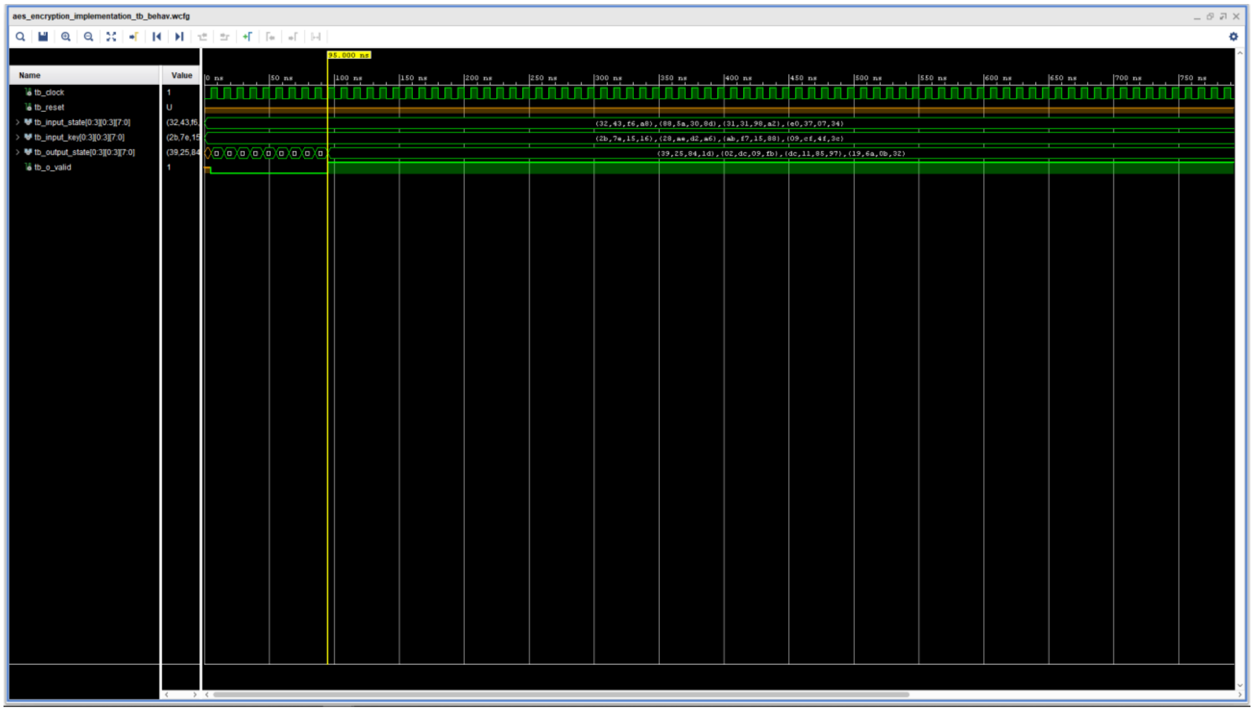
- **Aes_encryption_implementation** – top level with state machine
    - **Aes_encryption_key_schedule** – generates the key schedule
        - **g_function** – required for generating key schedule
            - **s_box** – s-box substitution
    - **Aes_encryption_key_addition** – first round addRoundkey 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.



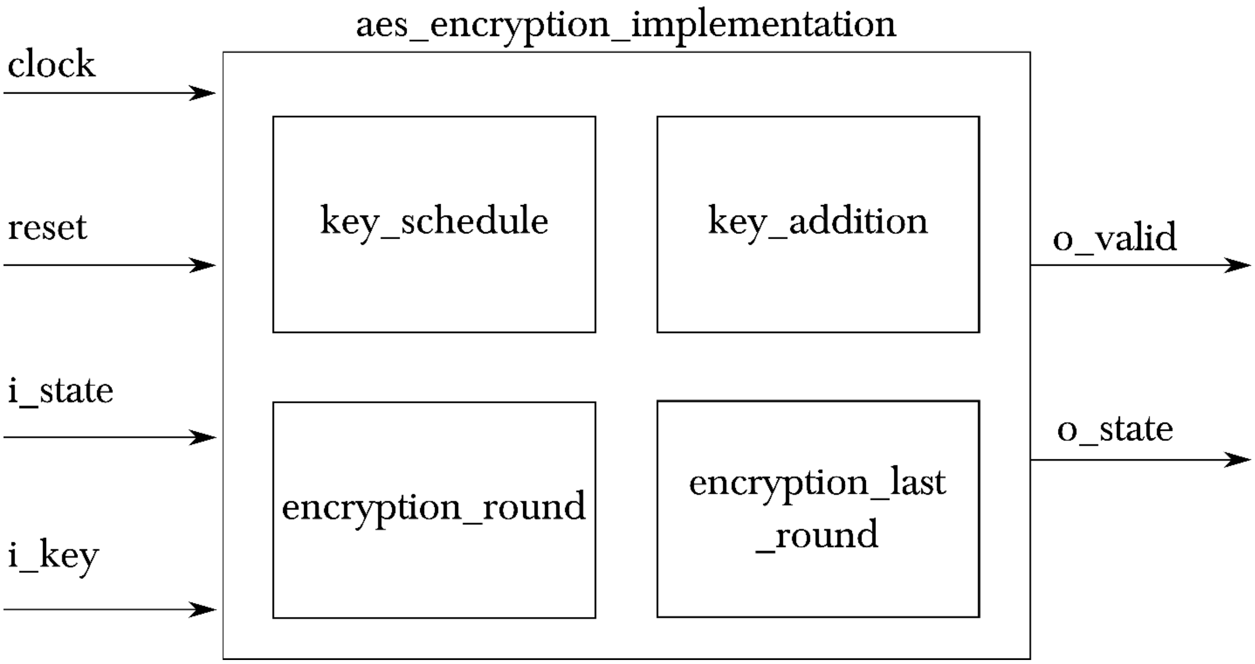
Name	Value
tb_clock	1
tb_reset	U
tb_input_state[0:3][0:3][7:0]	(32,43,f6,
tb_input_key[0:3][0:3][7:0]	(2b,7e,15
tb_output_state[0:3][0:3][7:0]	(39,25,84
tb_o_valid	1

(32,43,f6,a8),(88,5a,30,8d),(31,31,98,a2),(e0,37,07,34)

(2b,7e,15,16),(28,ae,d2,a6),(ab,f7,15,88),(09,cf,4f,3c)

(39,25,84,1d),(02,dc,09,fb),(dc,11,85,97),(19,6a,0b,32)

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.