1. Tools used for compiling and running your software implementations and generating test vectors

   Xilinx Vivado 2020.2

2. Strategy for verification:

   2.1 Order of tests and testbenches used:
   Testbench - EK_tb

   Steps
   Verify CT only for:
   2.1.1 Empty AD and PT
   2.1.2 2 blocks of AD and empty PT

   Verify CT and PT for:
   2.1.3 Empty AD and 2 blocks of PT
   2.1.4 2 blocks of AD and PT both

   2.2 Source and format of test vectors:

   2.2.1 SAEAES primary variant's Test Vector 1

   Nonce - 000102030405060708090A0B0C0D0E
   AD – (empty)
   Key - 000102030405060708090A0B0C0D0E0F
   PT – (empty)
   CT - 33F72C1AECA709664CABAA3D9EAE02D1

   2.2.2 SAEAES primary variant's Test Vector 17

   Nonce - 000102030405060708090A0B0C0D0E
   AD – 000102030405060708090A0B0C0D0E0F
   Key - 000102030405060708090A0B0C0D0E0F
   PT – (empty)
   CT – 1AD923A7B577F998CFDC6FACEAA9081D

   2.2.3 SAEAES primary variant's Test Vector 529

   Nonce - 000102030405060708090A0B0C0D0E
   AD – (empty)
   Key - 000102030405060708090A0B0C0D0E0F
   PT – 000102030405060708090A0B0C0D0E0F
   CT -
   593CB9748C9C3D15798CA8B952CC8DCBA575997A44F665A5CAF5713A1F5D13
   84

   2.2.4 SAEAES primary variant's Test Vector 545

Nonce - 000102030405060708090A0B0C0D0E
AD – 000102030405060708090A0B0C0D0E0F
Key - 000102030405060708090A0B0C0D0E0F
PT – 000102030405060708090A0B0C0D0E0F
CT –
60124944F0FAEAFDC38FE8BA5B48EE8C6A3117A9112807527D2B6D7CB0BC269A

2.3 Highest level entity verified for functional correctness and the results of its verification:

Test vectors 1, 17, 529 and 545 have been verified and results uploaded to 7_timing_analysis folder for comparing against expected results. Decryption of CT for test vector 529 and 545 has been verified as well.

From the Vivado console output, it can be seen that there is a significant latency in assigning output signal values to input signal values for verifying against expected results. Thus it takes first few simulations rounds to achieve **completely** successful result (all intermediate results passed) for a single test vector.

3. Verification of lower-level entities:

3.1 Name of entity – AES_Enc

3.2 Test vectors and their source (AES Specification)

Appendix C.1
PT - 00112233445566778899AABBCCDDEEFF
Key - 000102030405060708090A0B0C0D0E0F
CT - 69C4E0D86A7B0430D8CDB78070B4C55A

Appendix B
PT - 3243F6A8885A308D313198A2E0370734
Key - 2B7E151628AED2A6ABF7158809CF4F3C
CT - 3925841D02DC09FBDC118597196A0B32

3.3 Testbench used for verification – AES_Enc_tb

3.4 Result of verification, correct or incorrect behaviour – Correct

3.5 Possible sources of errors – NA