1. Only the primary variant has been implemented. Primary variant SAEAES_128_64_128 parameters are (bits):
   key size (k) = 128
   bit length of associated data block (r1) = 64
   bit length of authentication tag (t) = 128

2. Remaining parameters are (bits):
   block length of underlying block cipher (n) = 128
   bit length of nonce (r2) = 120
   bit length of a plaintext/ciphertext block (r) = 64

3. When processing a nonce input, it is split into 2 blocks of 64 bits and 56 bits respectively. The 56-bit block is padded with LSB 0s to make it a 64-bit block.

4. The same initialization vector (IV) from encryption of a plaintext block is used for decryption of generated ciphertext block.

5. E_k is internally implemented using AES_Enc package of CERG lab.

6. For initial verification purpose, clock period duration has been taken from AES_Enc package's clock setting. In future, this is supposed to be replaced with minimum clock period obtained after placing and routing during synthesis and implementation phase.

7. Future work would include implementation of SIPO and PISO for integrating existing framework with GMU Hardware API's CryptoCore module.