Assignment No. 2

CS666: Hardware Security for Internet of Things

1 Questions

1. Design a Verilog module for AES-128 iterative architecture. The design should have two inputs: plaintext (128-bit), key (128-bit), and one output: ciphertext (128-bit). The key expansion utilized to generate the round keys using the master key and the AES round operation should run parallelly in a non-blocking manner. You can use the instantiation of given modules (subbyte, shiftrow, mixcolumn, sbox and key expansion) to design a 10-round iterative AES hardware. [Hint: Each round of AES would be executed in one clock cycle.]

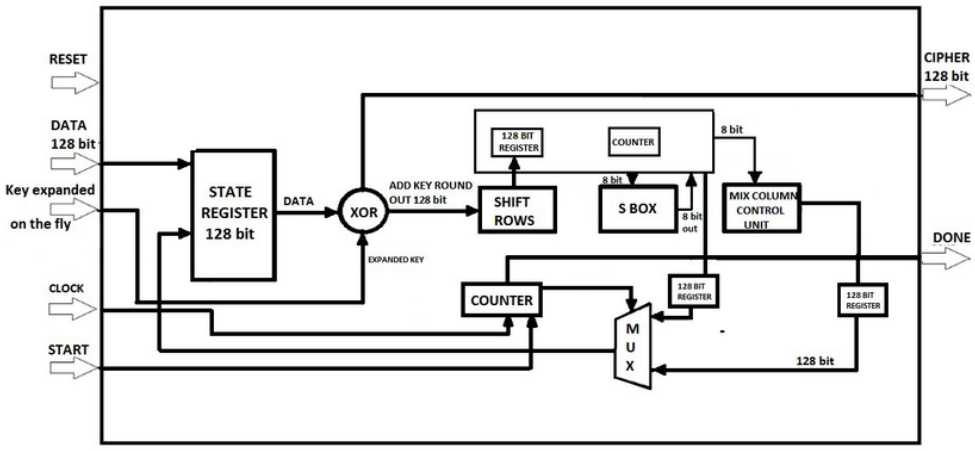

Figure 1: Iterative AES hardware