ELL305 Computer Architecture Assignment 2

Submission by: Rahul Jain (2017EE10476)

Common to both ciphers

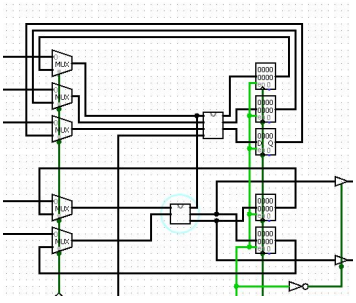
1. A delay circuit of 2 cycles is introduced. This is basically done to ensure that the main circuit starts after all the data is loaded in RAM. Delay is introduced with help of counter of 2 bits.
2. A controlled buffer is used just before the output which ensures that only the final output is printed. The controlled buffer is active at the 31st positive rising edge.
3. A MUX is used for loading the given input or the output from registers into the Key Schedule and Round Block .

Present Cipher

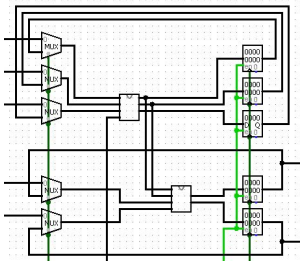
4. The boxes for Permutation, Substitution, Key Scheduling and Add Round Key are made separately and then assembled in main circuit. P-Box, Sbox and AddRoundKey are assembled into Round Block.
5. To implement 31 main rounds, a 5 bit counter is used. The register is enabled for counter values 0-30. As soon as all the bits become 1, the enable of register is made 0. The controlled buffer transfers the 64 bit output from registers to output pins.
6. The counter is set to stay at max value for max value 31.

ESF Cipher

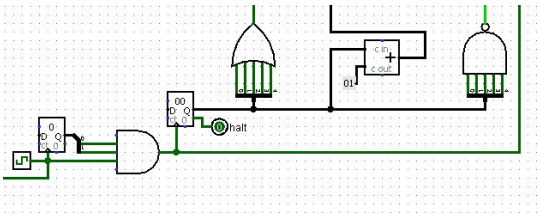
1. The boxes for F & Key Scheduling are made separately and then assembled in main circuit.
2. To implement 32 main rounds, a 5 bit counter is used. The register is enabled for counter values 0 31 (32 times). At the 31st cycle registers are disables and the controlled buffer is activated.
3. The ESF cipher round block halts at the count of 31st Postive Rising Edge.



ESF



PRESENT



Counter and Control Signals