Cryptography Homework

1. Build the 1 round and 64-bit block length versions of the BORON block cipher as given in Figure 2 in VHDL hardware. You do not need to implement key schedule at this step.

2. Verify the operation of the single round by feeding the plaintext and key values in the txt file and observing the output

    a. For example, Choose 0000 0000 0000 0000 to input to plaintext and master key. Produce first round output and check if it is same as `7777aaaa3333eeee`.
    b. Repeat the simulations using other test vectors given at the bottom of the paper.

3. Implement the Key Scheduler part in Figure 3, which generates the individual "roundkey"s for each round, using a Masterkey. Exact structure of the Key generator is explained in boron2.pdf.

4. Using the single round encryption and key generator circuits, design the complete circuit in Figure 3. Make sure the key generation is completely synchronous to the encryption algorithm, so that the it provides the correct roundkey for each round. The BORON algorithm has 25 rounds, so you should keep a counter and extract the output after the Substitution Permutation Network (Encryption algorithm box in Figure 3) is used 25 times.

    a. Use a signal to indicate when the algorithm is completed and the ciphertext is ready.
    b. A common mistake is to forget about the first or last XOR in the algorithm. See figure 1 in boron2.pdf, where the encryption algorithm is used 25 times, but the XOR is used 26 times in total.

-------ROUND = 0--------
Plaintext = 0
Masterkey = 00000000000000000000
-------ROUND = 1--------
Plaintext = 7777aaaa3333eeee
Masterkey = 0000000000000000000e
-------ROUND = 2--------
Plaintext = 29337c6644443822
Masterkey = 0000080000000001c00e
-------ROUND = 3--------
Plaintext = 4c9e24bdff548f8f
Masterkey = 0100100000003801c00e

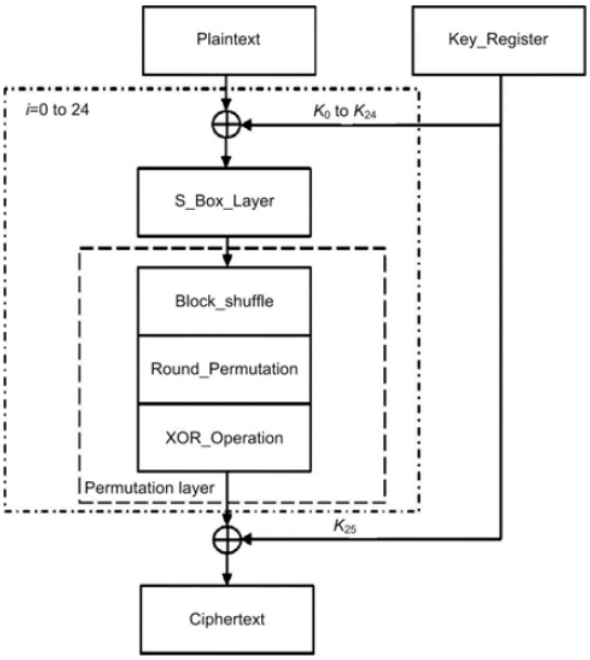

Figure 1: BORON cipher algortihm

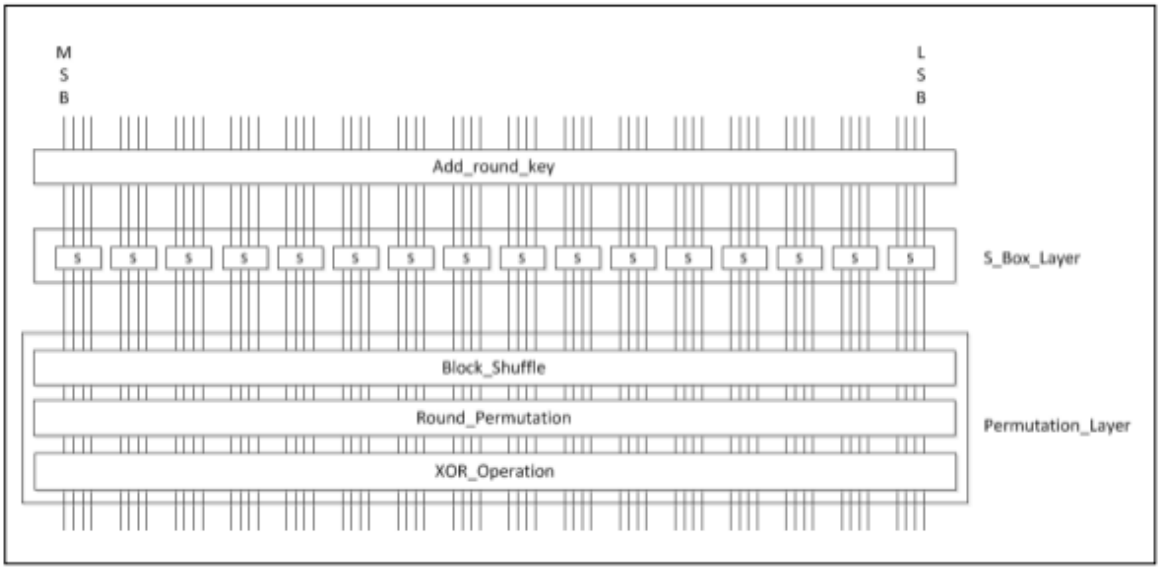

Figure 2: BORON round function

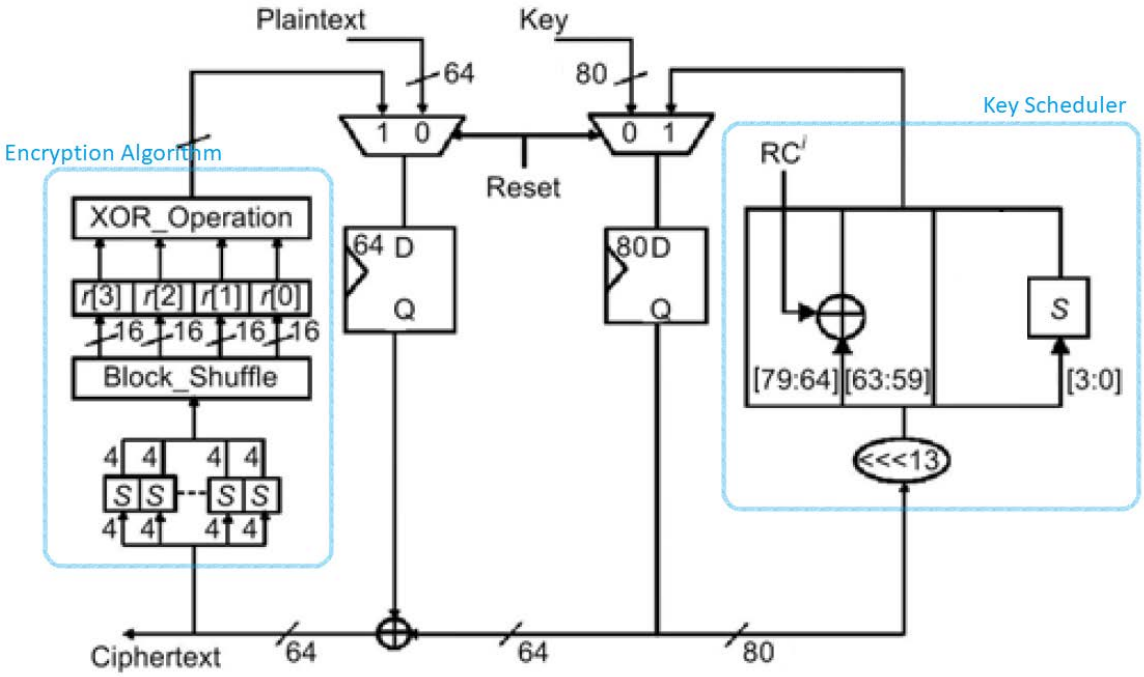

Figure 3: Complete datapath for the BORON cipher.

REFERENCES

[1] G. BANSOD, N. PISHAROTY, and A. PATIL. BORON: an ultra-lightweight and low power encryption design for pervasive computing. *Frontiers of Information Technology & Electronic Engineering*, 3:317 { 331, 2017.

[2] T. Okabe, ‘‘FPGA Implementation and Evaluation of lightweight block cipher – BORON’’, Tokyo Metropolitan Industrial Technology Research Institute, 2017

[3]http://web.itu.edu.tr/~orssi/thesis/2017/BurakAcar_bit.pdf