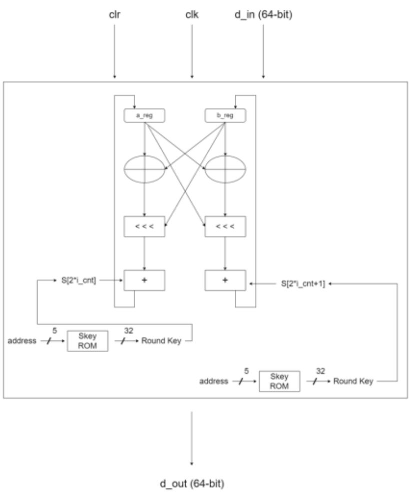
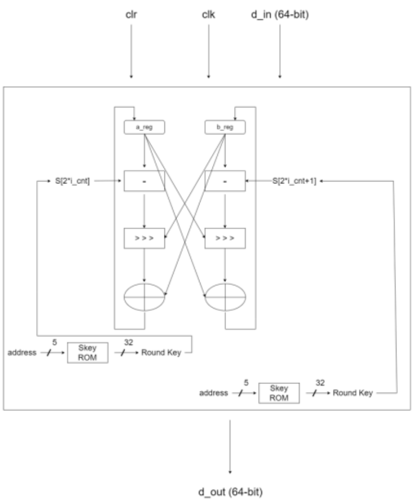
EL 6463 – Homework 4

Name: Xinran Tang **NYU ID Number**: N10257233 **Net ID**: xt2191

Link to the video:
https://drive.google.com/file/d/1VUlOp00zZv_frorL4VwqzWFLR2YRbbT5/view?usp=share_link

1. Datapath design





Since the mathematical equation for the "Simple Function" (RC5) is:

$$A = \big((A\ XOR\ B) <<< B\big) + S[2 * i]$$

$$B = \big((B\ XOR\ A) <<< A\big) + S[2 * i + 1]$$

The mathematical equation for the inverse "Simple Function" (RC5) is:

$$A = \big((A - S[2 * i]) >>> B\big)\ XOR\ B$$

$$B = \big((B - S[2 * i + 1]) >>> A\big)\ XOR\ A$$

As shown in the above image, the left Datapath is the datapath for the "Simple Function" (RC5), the right Datapath is the datapath for the inverse "Simple Function" (RC5).

2. Implement and simulate BOTH the ENCODE and the DECODE design

RC5 uses basic computer operations (addition, xor operation, shift, etc.) with variable number of rounds and variable number of key bits, thus greatly increasing flexibility. Applications requiring different security can set these values accordingly. another important feature of RC5 is that less memory is required for execution.

- **encoder**

In the one-time initial operation, the input is divided into two 32-bit blocks A and B. The rounds then begin, with each round completing the series of operations:

(1) xor operation
(2) left rotate
(3) addition with S[2*i_cnt] and S[2*i_cnt+1] respectively

- **decoder**

In the one-time initial operation, the input is divided into two 32-bit blocks A and B. The rounds then begin, with each round completing the series of operations:

(4) subtraction with S[2*i_cnt] and S[2*i_cnt+1] respectively
(5) right rotate

(6) xor operation

- **round key generation**

Two arrays are used to generate the round key: S_ARRAY and L_ARRAY.

- For the S_ARRAY, it is generated by the following logistic

  S[0] = 0xB7E15163(Pw)

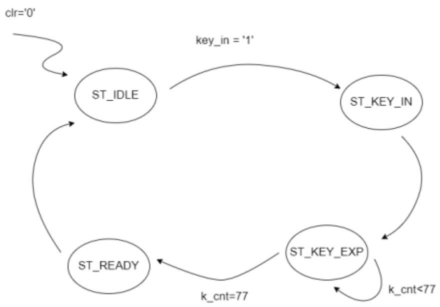
  for i=1 to 25 do S[i] = S[i-1] + 0x9E3779B9

- For the L_ARRAY, it is initialized with 0 and

  For i = b -1 downto 0 do

  L[i/u] = (L[i/u] <<< 8) + K[i]

- **State machine**

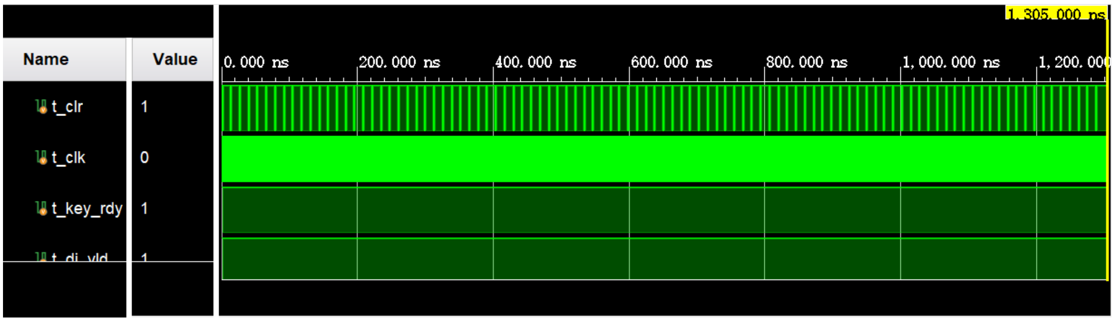


The state machine of this project is shown in the above image

- **Test**

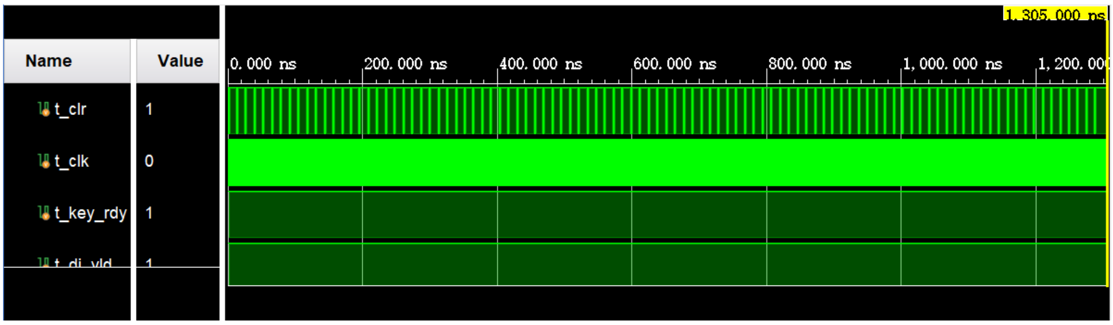
100 test cases are used to test for encode and decode function. The first row in the test cases file is the original input and the second row is the encoded output. For the encoder test, the first row is used as din and the second row is used as dout; for the decoder test, the second row is used as din and the first row is used as dout. The final result shows both encoder and decoder work.

- Test results for encoder:



Name	Value
t_clr	1
t_clk	0
t_key_rdy	1
t_di_vld	1

- Test results for decoder:



Name	Value
t_clr	1
t_clk	0
t_key_rdy	1
t_di_vld	1