AHD - LAB 5

RC5 Encryption and Decryption using FSM

Due 11/5/2018

Lab 5 Implementing RC5 Encryption and Decryption

- Design and implement the following given function using **FSM**:
- The design should accept 64 bit input (Din) and the initial A=Din[63 downto 32], B=Din[31 downto 0]

Encryption

A = A + S[0];
B = B + S[1];
for i = 1 to 12 do
    A = ((A xor B) <<< B) + S[2×i];
    B = ((B xor A) <<< A) + S[2×i + 1];

Decryption

for i = 12 downto 1 do
    B = ((B - S[2×i +1]) >>> A) xor A;
    A = ((A - S[2×i]) >>> B) xor B;
B = B - S[1];
A = A - S[0];

'S' values are given in ne xt slide

- You can use a clk, clear, start and done signals .

Lab 5 – Implementing RC5 Encryption and Decryption

The S values are:

S = [x"00000000", x"00000000", x"46F8E8C5", x"460C6085", x"70F83B8A", x"284B8303", x"513E1454", x"F621ED22", x"3125065D", x"11A83A5D", x"D427686B", x"713AD82D", x"4B792F99", x"2799A4DD", x"A7901C49", x"DEDE871A", x"36C03196", x"A7EFC249", x"61A78BB8", x"3B0A1D2B", x"4DBFCA76", x"AE162167", x"30D76B0A", x"43192304", x"F6CC1431", x"65046380"]

Lab 5 – Implementing RC5 Encryption and Decryption

- Design and implement the given function
  - Simulate and analyze the designs
  - Perform functional and timing simulations
  - Calculate resource utilization (After synthesis and after Place-and-Route (PAR))
  - Demonstrate them on FPGA board.

• Lab 5 – Implementing RC5 Encryption and Decryption

- For each design the DELIVERABLES are:
  - VHDL code, Bit file, constraint files (Zip them as Lab5_vhd_<netID>.zip).
  - Don't include the report in the zip file, submit it as a separate pdf file (Lab5_report_<netID>.pdf). The report should include the following:
  - Draw the FSM
  - Test cases: 2 different values of "Din", hand calculation for first three rounds, you can use the test case from Lab 4.
  - Functional and Timing Simulation: Screen-shots of Isim/Modelsim wave window for all test cases.
  - Report the resource utilization (After synthesis and after Place-and-Route (PAR)).
  - Report the critical path delay, maximum clock frequency, and the latency (in number of clk cycles) of your design.
  - Demonstrate the design implementation on your FPGA board.
  - Include a 5 min video describing the FSM and demonstrating its implementation on the FPGA.

CAUTION – READ CAREFULLY

- **Important: We are using a Plagiarism checking service. Only one submission is available. You cannot resubmit/modify the report after submission. Please heed caution when submitting the report. Submit only the final version. Sending a modified report to TA/Professor is not allowed.**