AHD - LAB 6

RC5 Key Expansion in HLS

Due 11/19/2018

Lab 6 RC5 Key Expansion

- Design RC5 Key Expansion that takes 128 bit key and 26 round keys (32-bit each).
- You can hardcode 96 bits and keep 32 bits of key as input.

- You can use a clk, clear, start and done signals .
- You may use either C or C++. Use xc7z010clg400-1 as device name. Set clock period as 10. Set uncertainty as 1.

Lab 6 – RC5 Key Expansion

- Please comment your code as much possible, for readability. There would be credits for well commented codes.
- You can hardcode the testbench inputs as of now. But, please clearly indicate the input variables. We will test with other random inputs while evaluating your code. You should create 3 solutions for your project. Name the project "RC5key". The three solutions should be named:
  1) least_area
  2) least_throughput
  3) least_latency
- The three solutions should correspond to minimal area, latency and throughput respectively. Please perform C simulation, synthesis, C/RTL co-simulation and Implementation of your design.

Lab 6 – RC5 Key Expansion

Things to submit:

1. Full project directory in a zip file. Please keep the source files in the same location as the project. The source C/C++ files should also be present.
2. A report indicating:
    a. Results of 10 different inputs you tried. (You can include screenshots if you want).
    b. Post-implementation resource usage for each of the solutions.
    c. Area of solution corresponding to least_area.
    d. Throughput of solution corresponding to least_throughput.
    e. Latency of solution corresponding to least_latency.
    f. Could you flatten/merge loops in the design? If yes, please indicate them in the report (from your code). If not, can you explain why you couldn't

⚠ 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.**