Homework 5 (5%) Due: 2:00 PM (NYC Time), November 12 2021

"Complete" RC5 Encrypt and Decrypt Designs

Overview

In this assignment, you will design and put together all the components required for RC5 encryption and decryption.

Task:

- Throughout the lectures you have been taught about the various building blocks of RC5 (a.k.a., the simple function, rotations, ROMs, etc.). In the previous HW you used these to build most of an RC5 system. Using your previous homework as a start point,
    - **Draw** the architecture diagram for a "**Complete**" (RC5) system capable of key derivation, encryption, and decryption
        - Use professional diagram software (e.g. https://draw.io)
        - The design should have the following I/O:
            - Input clk, input rst
            - Input user_key (128 bits), input start_generating_skey, output key_done
            - Input d_in (64 bits), input start_encryption, input start decryption, output d_out (64 bits), output done
    - **Implement** and **simulate** a single design that can BOTH ENCRYPT and DECRYPT
        - You must design a comprehensive testbench that includes file I/O (using Verilog's built-in functions or VHDL's textio packages) where you encrypt/decrypt at least 100 plaintext/ciphertext combinations
            - (Note: We will provide a script which encrypts inputs so that you can test your equivalences)
        - Your design should be a multi-cycle implementation
        - Your design will need to include a FSM to handle the different functionalities
        - Your design must be able to perform the key derivation algorithm from the user_key input
    - You may use either Verilog or VHDL
    - **Synthesize your design** so that you may discuss the resource utilization

- You might choose to refer to Rivest's original paper to help support your implementation: https://people.csail.mit.edu/rivest/Rivest-rc5.pdf

- **Write** a short (2 pages max.) report describing your design process. Justify your code and relate it to your datapath design. Justify your testbench, and describe how it covers all possible execution scenarios. You will also discuss the new features and the resource utilization.

Deliverables:

1. Submit a zip file of your complete Xilinx project which includes your VHDL or Verilog files,
2. and a PDF report :
    - Explaining and justifying the design and including your diagrams.
    - Discussing the new features as compared to the previous homework
    - Discussing the resource utilization from synthesis