Microprocessor-Based Systems (E155)

D. Harris and M. Spencer **Fall 2015**

Lab 7: Advanced Encryption Standard

Requirement

Construct a hardware accelerator to perform 128-bit AES encryption. Send a plaintext message and key from a Pi to the accelerator and verify that the cyphertext received back is correct. Displays the SPI communication on the logic analyzer.

Objectives of this lab are to learn to read and implement a complex specification, build a nontrivial system on an FPGA that requires thoughtful architecture to fit on the chip, interface between an FPGA and microprocessor, and gain experience with hardware accelerators.

Advanced Encryption Standard

The Advanced Encryption Standard is described in an unusually succinct and clear standard. Reading the standard carefully will save you time. See Appendix A-1 for an example of the key expansion during each round and Appendix B for an example of the intermediate results during each round.

Implementation

Download aes_starter.sv, sbox.hex, and lab7.c from the web page. aes_starter.sv contains the top-level module, an SPI interface, and a testbench that applies and checks the test vector described in Appendix A-1 and B. It also contains the mixcolumns logic that operates on a 128-bit intermediate state. The Galois field arithmetic for mixcolumns is more complicated than for the rest of AES, and the implementation is based on a paper cited in the code. The sbox module and sbox.hex lookup table perform the sbox substitution on a single byte. Lab7.c sends a key and plaintext message over SPI to the FPGA, then checks that the result is correct.

You will discover that the logic is too large to implement all the rounds as one giant block of combinational logic. Therefore, you will need to perform the rounds sequentially.

Turn in the usual report including design approach, code, schematics, results, and time spent.

This lab was developed in 2015 by Ben Chasnov.