Lab 7: The Advanced Encryption Standard

Learning Objectives

By the end of this lab you will have…

- Learned to read and implement a complex specification
- Built a nontrivial system on an FPGA that requires thoughtful architecture to fit on the chip
- Designed and implemented an interface to communicate between the FPGA and microprocessor on your MCU
- Learned how to use a logic analyzer to analyze and debug your system
- Gained experience with hardware accelerators

Requirements

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

The 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 the starter source code and libraries from the course website. The provided MCU libraries (included in the lib subdirectory of the project) support a number of peripherals on the MCU so that you can directly use them and do not need to write them yourself.

Examine aes_starter.sv, sbox.txt. aes_starter.sv contains the top-level module, an SPI interface, and two testbenches. The testbench module tests the entire system including the SPI link. The testbench_aes_core module is a separate testbench that tests only the aes_core module without the SPI link. It is suggested that you use testbench_aes_core first to check your core and then test the whole system including the SPI link with the full testbench. These testbenches apply and check the test vector described in Appendix A-1 and B.

The starter code 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.txt lookup table perform the sbox substitution on a single byte.

The MCU code lab7.c sends a key and plaintext message over SPI to the FPGA, then checks that the result is correct. Set up your Quartus project to target the FPGA on your board and develop the remaining modules necessary to implement AES. You will need to carefully read the specification to figure out what these are and how to connect them. Starting with a high-level block diagram of the system is a very helpful step to make sure that you are understanding the AES procedure correctly. The MCU starter code can be opened directly in SEGGER Embedded Studio and directly compiled and uploaded to the MCU and does not need any further modification.

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. You will also need to pay careful attention to the timing within each round since you need to allow for the one-cycle latency required to perform the sbox byte substitution which uses the synchronous RAM blocks.

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

Hints

Previous students have spent a highly variable amount of time on this lab. Here are some suggestions to make it go faster.

Start by thoroughly understanding the specification

In prior labs you may have gotten in the habit of thinking in code. Remember to go back to thinking about hardware rather than function calls. Draw a block diagram for your hardware using elements such as registers, multiplexers, FSMs, and blocks of combinational logic. Name all of the signals between blocks. Remember how the E85 multicycle processor had a datapath that required certain control signals such as mux selects, and a controller that generates the control signals at the appropriate times. You'll find a similar organization helpful. Write idiomatic Verilog code that exactly matches your block diagram.

Watch for warnings in synthesis and simulation, and correct these before moving ahead.

Get your design working in simulation first. When debugging, find the first place you can tell a signal is wrong. Add all the relevant inputs that influence that signal. If one of them is wrong, recursively work backward. When the inputs are good and the output is bad, you've isolated the bug and can look for it in that part of the code. Learn to do this systematically so you can find and solve each bug in minutes rather than hours.

If the design works in simulation but not on hardware, it is often a wiring error or a discrepancy between how you timed your control signals and what the C code expects. Make sure you've read the provided code carefully and are producing signals at the right times. Check that your FPGA and microcontroller are expecting the same polarity and phase for your SPI clock signal. Use the many channels of the logic analyzer to view all of the relevant signals at once and check them against your expectations. If you have a hard bug, it's helpful to tap out intermediate signals, such as the state of a FSM, onto FPGA pins so you can watch them on the logic analyzer.

Have fun! This is a sophisticated system and you should feel proud when you have built and debugged it!

What to Turn In

When you are done, have your lab checked off by the instructor. You should thoroughly understand how it works and what would happen if any changes were made. Turn in your lab writeup including the following information:

- Schematics of the breadboarded circuit.
- A screen capture (exported from the scope, not a photo captured using a camera) of an example SPI transaction captured on the oscilloscope/logic analyzer.
- Your source code.
- How many hours did you spend on the lab? This will not count toward your grade.

Credits

This lab was original developed in 2015 by Ben Chasnov '16, redesigned for the µMudd Mark 5.1 in 2019 by Caleb Norfleet '21, and revamped for the µMudd Mark 6 in 2021 by Prof. Josh Brake.