Computer Department
Faculty of Engineering
Cairo University

CMPN111
Logic Design 2
Spring 2023

Project Document

Description:

The goal of the project is to use Verilog to design a circuit for a practical application. For this project, you will implement AES encryption and decryption. To understand the AES encryption and decryption procedure, refer to the attached document “NIST.FIPS.197” which defines the procedures in detail and provides step-by-step examples.

As you will notice, AES encrypts and decrypts blocks of 128 bits using a cryptographic key which can be 128, 192 or 256 bits long. In the project, both the encryption and decryption modules have to support all of the three key sizes. You can define the key size as a parameter provided to each module.

Another thing you will notice is that the number of inputs and outputs is huge. Therefore, each module has to be designed with a serial interface to read the inputs bit-by-bit over multiple clock cycles, and return the result bit-by-bit over multiple clock cycles. The interface should follow the SPI (Serial Peripheral Interface) specification. The SPI specification is explained in the attached document “introduction-to-spi-interface”. You only need to support SPI mode 0.

Finally, we need to test the project using simulation and on the DE1-SoC board. To test the design using simulation, you must write a testbench that tests the encryption and decryption modules together using multiple testcases. For each testcase, the input message and the key are supplied to the encryption module, then the encrypted message is received and compared with the expected result. Then the encrypted message and the key are supplied to the decryption module, then the decrypted message is received and compared with the original input. The testbench must be self-checking and it should print a message for each testcase to indicate if it has succeeded or not, then it should print the total number of successes and failures.

To test the design on the DE1-SoC board, you must write a test wrapper. The wrapper operates in a manner similar to the testbench, but instead of printing messages, it should show if the testcases have passed or not via a led (Turn the led on if the testcases have passed).

So as a summary, the requirements are:

- Implement two modules: AES encryption and decryption.
- The key size should not be fixed and can be changed without changing the code of the encryption and decryption modules.

- The encryption and decryption modules must have a serial interface that follows the SPI specification (mode 0) through which they receive the input message & key and send out the encrypted or decrypted message.
- Both modules must be able to receive and encrypt/decrypt a series of messages and keys without resetting between each pair of inputs. In other words, you should only use reset once at the start, then the modules should be operational for any number of testcases without resetting again.
- You should implement a self-checking testbench that tests the encryption and decryption modules using multiple testcases with different messages and keys. The testbench must show that the modules work at different key sizes. You can implement three testbenches (one for each key size) if you prefer to not write one that tests all the sizes together.
- You should implement a test wrapper that drives the inputs of the encryption and decryption modules on the DE1-SoC board, and it should automatically test their inputs and outputs and show an indicator if the test results were successful or not using a led.

Deliverables*:*

1. The Verilog files containing the following:
    a. AES encryption module.
    b. AES decryption module.
    c. The testbench(s).
    d. The test wrapper.
    e. Any extra modules that you created to reuse in the aforementioned modules.
2. A pdf report stating the workload distribution.

Team formation deadline: Wednesday April 19th, 2023, 23:59 pm.
Deadline: Wednesday May 17th, 2023, 13:30 pm.
Team size: 4 students.