Midterm Exam ECE 448

Spring 2013

Wednesday Section (15 points)

Instructions:

Zip all your deliverables into an archive <last_name>.zip and submit it through Blackboard no later than Wednesday, March 20, 10:15 PM EDT.

Lab Midterm Exam

Introduction:

The described below circuit performs encryption of an N-bit message, using a simple algorithm based on addition and multiplication operations. Message is loaded in parallel, in blocks of 15 bits, and then it is serially sent out to the circuit one bit per clock cycle. The corresponding ciphertext bits leave the circuit in parallel, in blocks of 15 bits. The result of encryption depends on the MESSAGE and initialization vectors IV1, IV2 and IV3, which can be chosen at random on the sender's side and transmitted in clear to the receiver's side).

Interface:

Assume the following interface to your circuit.

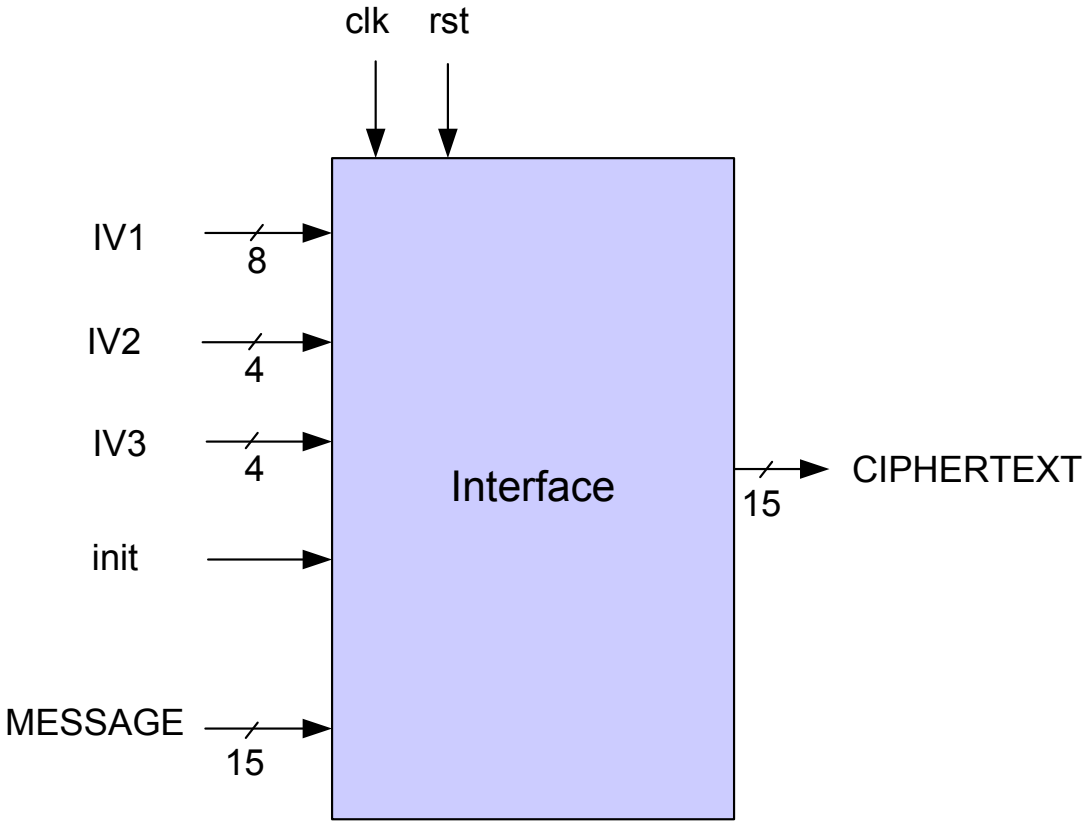
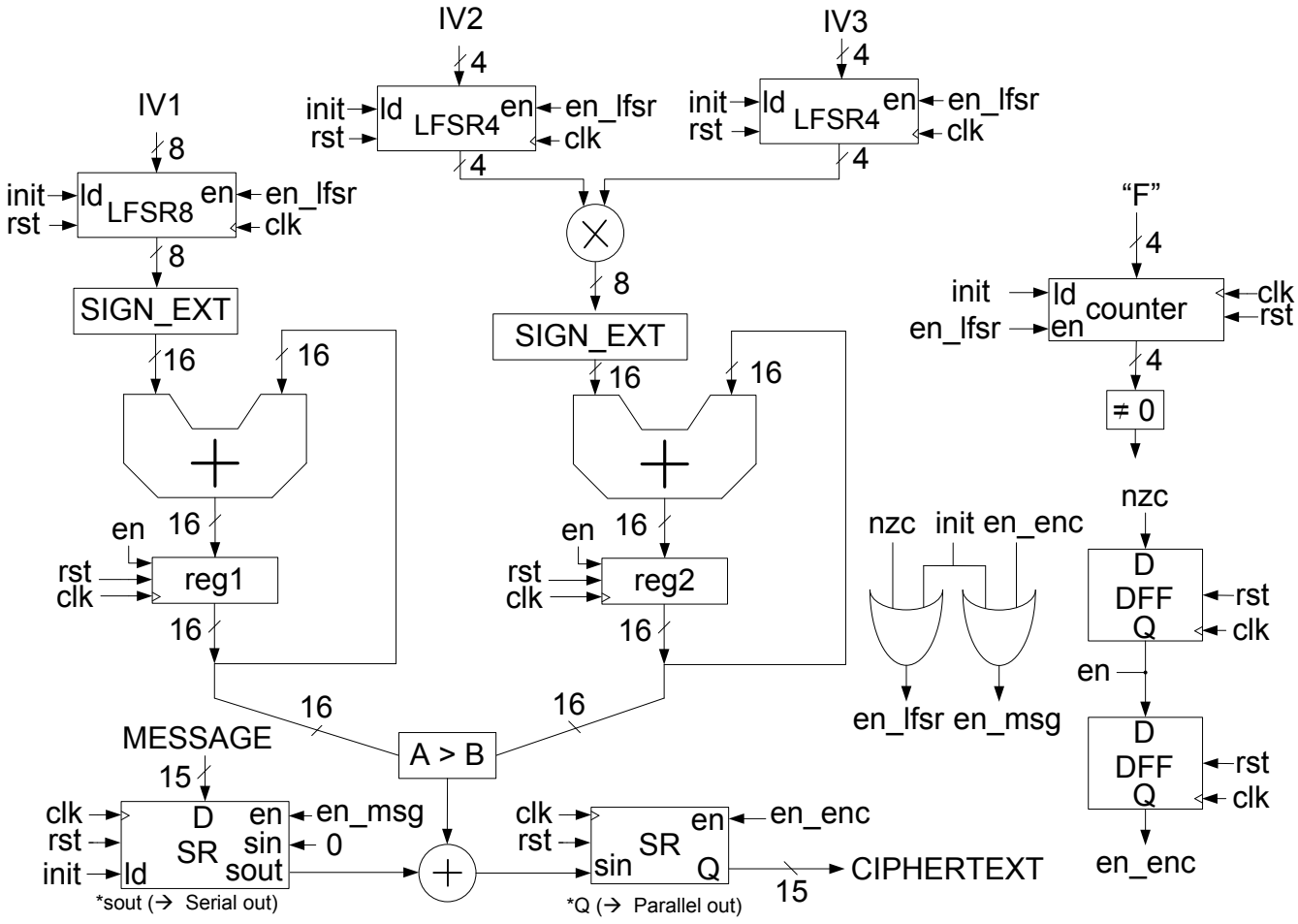


Table of input/output ports:

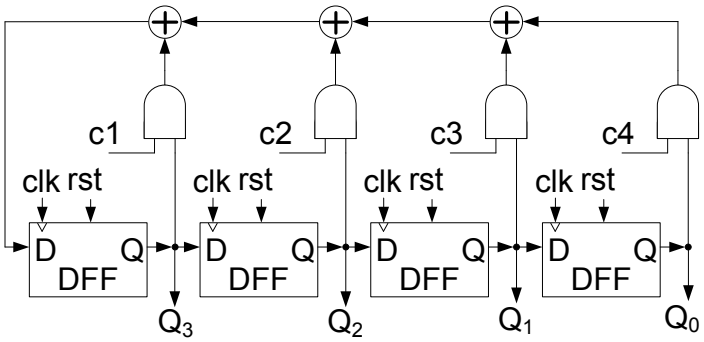
Port	width	Function
clk	1	System clock
rst	1	High at start for 50 ns
init	1	Active for one clock cycle to initialize encryption process
IV1	8	Initialization vector for LFSR 1
IV2	4	Initialization vector for LFSR 2
IV3	4	Initialization vector for LFSR 3
MESSAGE	15	Message block
CIPHERTEXT	15	Ciphertext block

Block diagram:

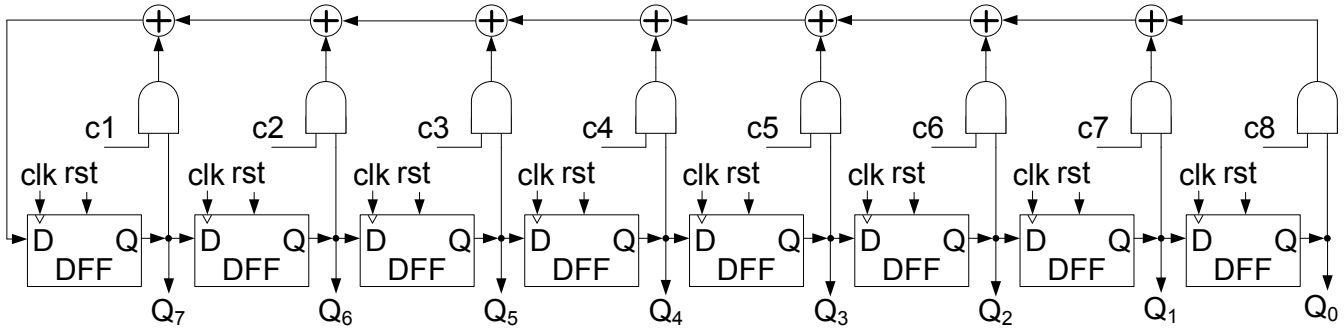


SIGN_EXT = Sign Extension from 8 to 16 bits; SR = Shift Register

LFSR4: 〈 4, 1+ D_3 + D_4 〉



LFSR8: 〈 8, 1+ D_4 + D_5+ D_6 + D_8 〉



Inputs, Outputs and Waveform:

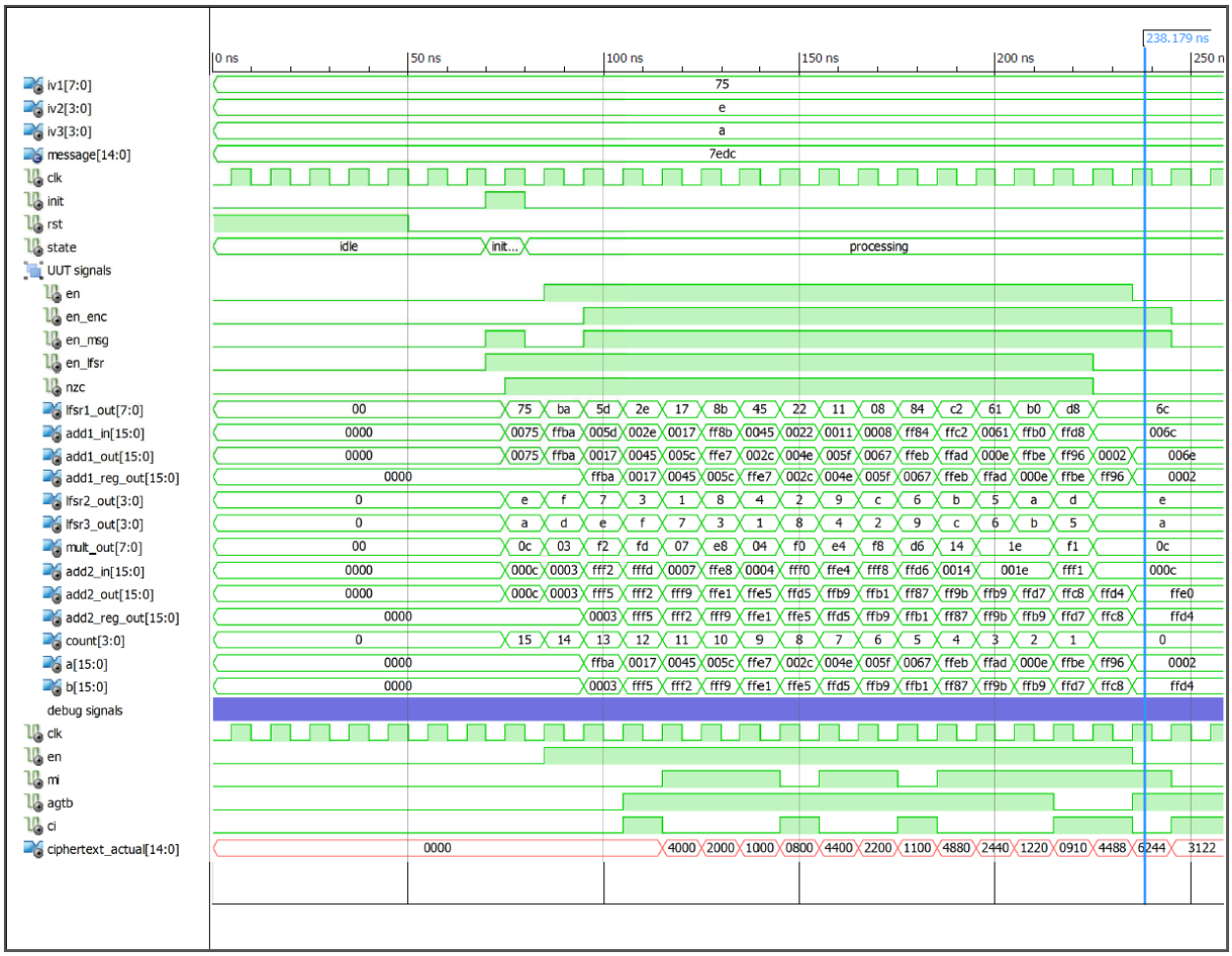
Inputs:

MESSAGE = "111111011011100" = x"7EDC
IV1 = x"75";
IV2 = x"E";
IV3 = x"A";

Output:

CIPHERTEXT ="110001001000100" = x"6244"

Functional Waveform:



Design Requirements:

The combinational portion of the circuit should be described using the dataflow VHDL code, and the sequential portion of the circuit should be described using the synthesizable behavioral code. Your code should infer a circuit that requires a minimum amount of FPGA resources. The target clock frequency should be **100 MHz**.

Tasks:

Perform the following tasks:

1. Write a synthesizable VHDL code representing encryption circuit (shown in the block diagram above).
2. Write a testbench verifying the operation of your encryption circuit.
3. Perform functional simulation of your circuit and use it to debug your VHDL code. Take a print out of the waveform showing the entire operation using default PDF conversion tool installed in the lab (Use the multiple page option in order to display necessary information on multiple pages, if required).
4. Synthesize your circuit.
5. Implement your circuit using
    a. FPGA family: Spartan 6
    b. Device: xc6slx16-3csg324
    c. Speed Grade: -3
6. Run the static timing analysis of your circuit.
7. Based on the circuit block diagram and the report from the static timing analysis, determine the most critical path in your circuit and the circuit maximum clock frequency.
8. Based on the implementation reports, determine the number of CLB slices, LUTs, flip-flops, and pins used by the circuit.
9. Perform the timing simulation of your circuit at the maximum clock frequency returned by the static timing analysis. Take a printout of the waveform showing the entire operation using default PDF conversion tool installed in the lab (Use the multiple page option in order to display necessary information on multiple pages, if required).

Deliverables:

1. VHDL code of your entire circuit **fulfilling the requirements** specified in the *Design Requirements* section above.
2. VHDL code of your testbench.
3. Timing waveforms from the functional and timing simulations demonstrating the correct operation of your circuit.
4. Description of the critical path in your circuit
5. FPGA resource utilization (as defined in Task 8 above).
6. Minimum clock period and maximum clock frequency of your circuit.