# *ECE 3170 Cryptographic Hardware for Embedded Systems*

Fall 2025

Assoc. Prof. Vincent John Mooney III
Georgia Institute of Technology

Homework 6, 100 pts.

Due Friday Oct. 3 prior to 11:55pm

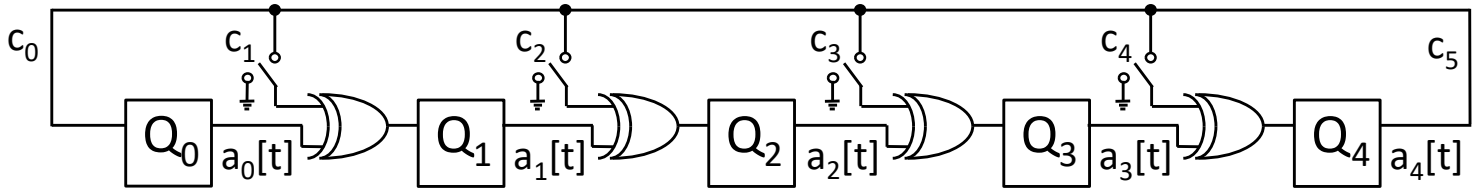
(please turn in homework electronically on Canvas)

**As always this semester, you are required to solve any and all homework questions alone.**

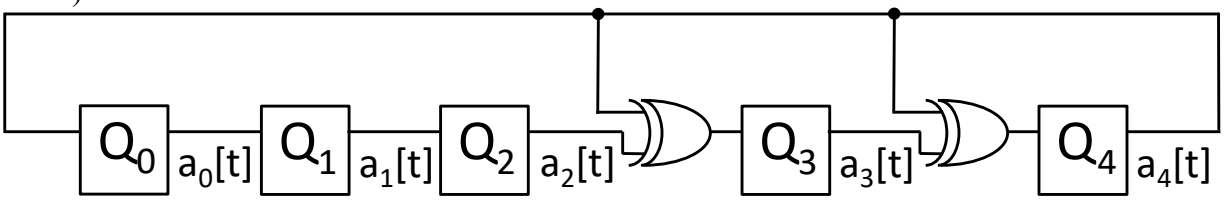
1) (5 pts.) Explain the problem with the following question: "Is it possible that the <one-way function under consideration> has a backdoor that we do not know about?" As a part of your explanation, please rewrite the question in your own words (do **not** copy from anywhere, including lecture!) in a way that is much more reasonable.

2) (15 pts.) Lecture 17 Cryptography XI covered Linear Feedback Shift Registers.
   a. (5 pts.) Use your own words to describe what is a primitive polynomial and how it is defined.
   b. (5 pts.) Considering an n-bit LFSR, what is the length of the LFSR bit sequence if the feedback function implements a primitive polynomial and in the initial state of the LFSR is non-zero (i.e., the initial state is something other than all zero values)?
   c. (5 pts.) Considering an n-bit LFSR, what is the length of the LFSR bit sequence if the feedback function implements a primitive polynomial and in the initial state of the LFSR is all zeros?

**[PLEASE TURN TO THE NEXT PAGE!]**




3) (40 pts.) For this problem, you are going to fill out a table for an LFSR with a feedback function you have been assigned where the assigned 4-bit binary number corresponds to $c_4c_3c_2c_1$ where the $c_i$ values correspond to the picture above. For example, 1100 means $c_4 = c_3 = 1$ while $c_2 = c_1 = 0$ which results in the LFSR shown below. Please see the course webpage for your assignment using the same name (first name then first initial of your last name) as was used in the RSA homework.




Note that the LFSR is a "Galois" or "internal-XOR" LFSR. Furthermore, the LFSR is autonomous (no external inputs).

a. (5 pts.) Draw the internal-XOR LFSR for your specific case with the values you have been given for $c_4c_3c_2c_1$. If an XOR gate has only one input which can possibly have value 1, please replace the XOR gate with a wire in your drawing.

b. (5 pts.) Assuming an initial state $a_4 = a_3 = a_2 = a_1 = 0$ and $a_0 = 1$, redraw your LFSR showing all FF inputs and outputs after one clock cycle. Your new drawing should clearly label / indicate which are the values of $a_4$, $a_3$, $a_2$, $a_1$ and $a_0$.

c. (5 pts.) Continuing from your answer to part b above, redraw your LFSR showing all FF inputs and outputs after six clock cycles. Your new drawing should clearly label / indicate which are the values of $a_4$, $a_3$, $a_2$, $a_1$ and $a_0$.

d. (15 pts.) Fill out the table below (see the next page of this homework) with the correct values for your LFSR.

e. (10 pts.) Now comment on the resulting bit patterns in your answer to part d. Considering $a_4a_3a_2a_1a_0$ as a group or number consisting of five bits – as shown in the table – does the bit pattern repeat? If yes (hint: the answer is **yes**), how often?

| Time | $a_4$ | $a_3$ | $a_2$ | $a_1$ | $a_0$ |
|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 1 |
| 1 | | | | | |
| 2 | | | | | |
| 3 | | | | | |
| 4 | | | | | |
| 5 | | | | | |
| 6 | | | | | |
| 7 | | | | | |
| 8 | | | | | |
| 9 | | | | | |
| 10 | | | | | |
| 11 | | | | | |
| 12 | | | | | |
| 13 | | | | | |
| 14 | | | | | |
| 15 | | | | | |
| 16 | | | | | |
| 17 | | | | | |
| 18 | | | | | |
| 19 | | | | | |
| 20 | | | | | |
| 21 | | | | | |
| 22 | | | | | |
| 23 | | | | | |
| 24 | | | | | |
| 25 | | | | | |
| 26 | | | | | |
| 27 | | | | | |
| 28 | | | | | |
| 29 | | | | | |
| 30 | | | | | |
| 31 | | | | | |
| 32 | | | | | |

**[PLEASE TURN TO THE NEXT PAGE!]**

4) (40 pts.) For this problem, you are going to use the LFSR with the same feedback function you used for the previous question but will add the appropriate representation of calculations in polynomial space.

   a. (5 pts.) Draw the internal-XOR LFSR for your specific case with the values you have been given for $c_4c_3c_2c_1$. If an XOR gate has only one input which can possibly have value 1, please replace the XOR gate with a wire in your drawing. You may copy from your answer to the previous problem since this problem (part a) is identical.

   b. (5 pts.) Please go to time 5 and redraw your internal-XOR LFSR for your specific case with this state. Please show all values $a_4a_3a_2a_1a_0$. You are also required to show the answer in a polynomial representation as explained in class. You may want to listen again to the example given in lecture on Thursday Oct. 3.

   c. (10 pts.) Redraw your LFSR showing all FF inputs and outputs after one clock cycle (i.e., go to time 6). Your new drawing should clearly label / indicate which are the values $a_4a_3a_2a_1a_0$. You are also required to calculate $a_4a_3a_2a_1a_0$ in the polynomial space and show all of your work. Specifically, calculate the unsimplified result as well as the result after modification with your feedback polynomial P(x).

   d. (10 pts.) Redraw your LFSR showing all FF inputs and outputs after one more clock cycle (i.e., go to time 7). Your new drawing should clearly label / indicate which are the values $a_4a_3a_2a_1a_0$. You are also required to calculate $a_4a_3a_2a_1a_0$ in the polynomial space and show all of your work. Specifically, calculate the unsimplified result as well as the result after modification with your feedback polynomial P(x).

   e. (10 pts.) Redraw your LFSR showing all FF inputs and outputs after one clock cycle (i.e., go to time 8). Your new drawing should clearly label / indicate which are the values $a_4a_3a_2a_1a_0$. You are also required to calculate $a_4a_3a_2a_1a_0$ in the polynomial space and show all of your work. Specifically, calculate the unsimplified result as well as the result after modification with your feedback polynomial P(x).

**YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES. ALL LABORATORY SUBMISSIONS MUST INCLUDE YOUR NAME, COURSE NUMBER, SECTION, AND THE HOMEWORK SET NUMBER. ALL SHEETS MUST BE STAPLED TOGETHER. ALL WRITING MUST BE EASY TO READ (FOR EXAMPLE, YOU MAY HAVE TO WRITE ONLY ON ONE SIDE OF EACH SHEET OF PAPER THAT YOU SUBMIT AND MAY NOT BE ABLE TO USE RECYCLED PAPER). FAILURE TO FOLLOW INSTRUCTIONS MAY RESULT IN ZERO POINTS. ALL WORK MUST BE YOUR OWN. NO PLAGIARISM IS ALLOWED, AND YOU MUST PROPERLY REFERENCE ALL SOURCES OF YOUR INFORMATION – ALTHOUGH YOU SHOULD NOT LOOK FOR AND MAY NOT CONSULT "SOLUTIONS" AVAILABLE FROM OTHER SOURCES (TO REPEAT, YOU MAY NOT CONSULT HOMEWORK SOLUTIONS OF THESE EXACT PROBLEMS FROM OTHER COURSES!).**