# *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

**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.

As worded the question must be answered "Yes" as we cannot know what we do not know. Answering this question does not provide useful information. A better question would ask about specific discovered concerns or what specifically has been verified secure, etc.

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.

The feedback function defined by the LFSR structure can be expressed as a polynomial. Since the LFSR implements multiplication in a Galois Field mod the polynomial representation of the feedback function, this is also known as the **characteristic polynomial**. The last register and all other output registers tied to XOR gates logically contribute to the polynomial, which takes the form

$$P(x) = \sum_{i=0}^{n} c_i x^i = c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$$

Note that $c_n$ and $c_0$ are always equal to 1, so $P(x)$ can be rewritten as

$$P(x) = \sum_{i=0}^{n} c_i x^i = x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + 1$$

The polynomial is primitive, i.e., is a primitive polynomial if it is irreducible (i.e., cannot be evenly divided by any smaller polynomial where "even division" refers to division resulting in no remainder term) and provides full period (excluding the zero state, i.e., for an n-bit LFSR the period is $2^n - 1$).

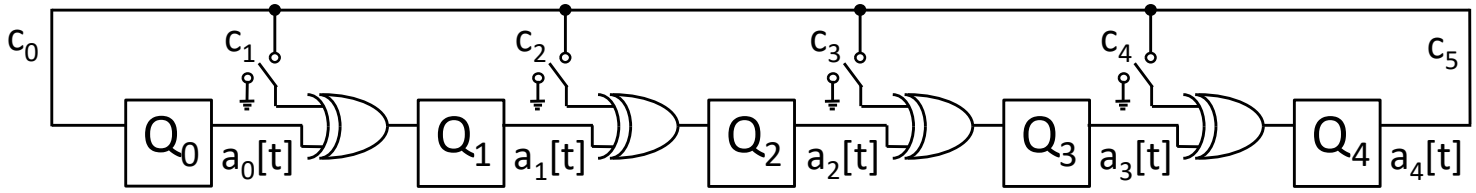
b. (5 pts.) Considering an n-bit LFSR, what is the length of the LFSR bit sequence if the feedback function implements a primitive polynomial and in the initial state of the LFSR is non-zero (i.e., the initial state is something other than all zero values)?

The n-bit LFSR with non-zero initialization and a feedback function implementing a primitive polynomial has a bit sequence length of $2^n$-1.

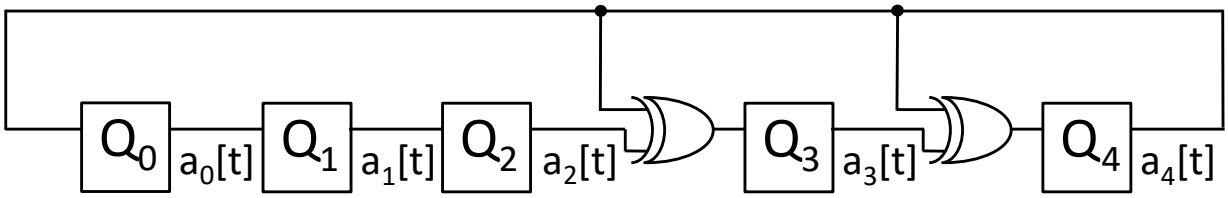
c. (5 pts.) Considering an n-bit LFSR, what is the length of the LFSR bit sequence if the feedback function implements a primitive polynomial and in the initial state of the LFSR is all zeros?

The length of the LFSR bit sequence is one (zero was also accepted, but formally speaking the sequence length is the number of elements in the sequence). The n-bit LFSR with all zero initialization has a trivial sequence. Regardless of the feedback function (i.e., the characteristic polynomial defining the feedback), the all-zero initialization will only result in 0's produced at the output, because 0 XOR 0 is 0.

**[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.



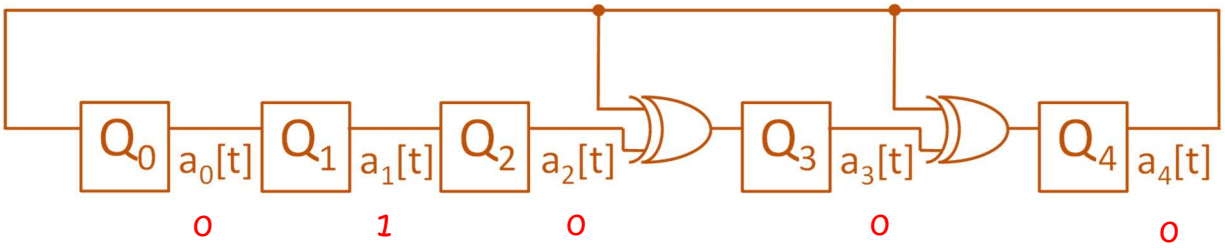

Note that the LFSR is a "Galois" or "internal-XOR" LFSR. Furthermore, the LFSR is autonomous (no external inputs).

This solution uses $c_4, c_3, c_2, c_1 = 1100$

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.

See LFSR above for 1100

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 $a_0$.

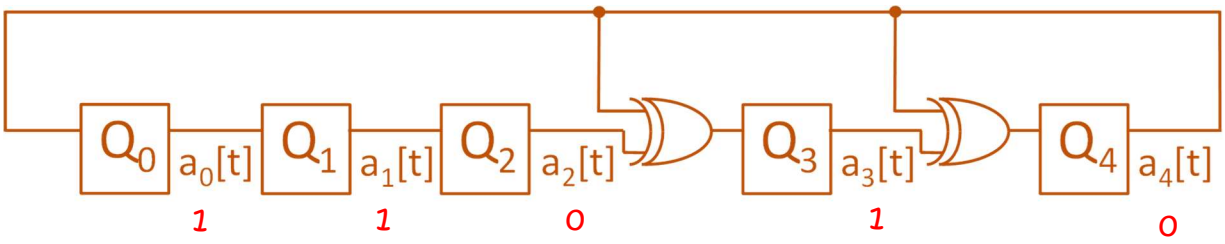



THIS ANSWER IS THE SAME FOR ALL CASES!!

After one clock cycle, the register state is

$$A(x)[1] =< a_4[1], a_3[1], a_2[1], a_1[1], a_0[1] >= 00010$$

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 $a_0$.




After six clock cycles, the register state is

$$A(x)[6] =< a_4[6], a_3[6], a_2[6], a_1[6], a_0[6] > = 01011$$

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

d. (15 pts.) Fill out the table below with the correct values for your LFSR.

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

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?

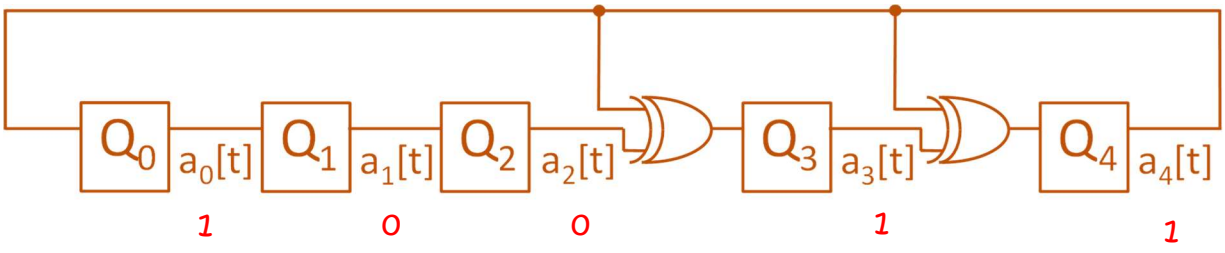
Yes, the bit pattern repeats with a period of 14 clock cycles

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.

See problem 3a.

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.



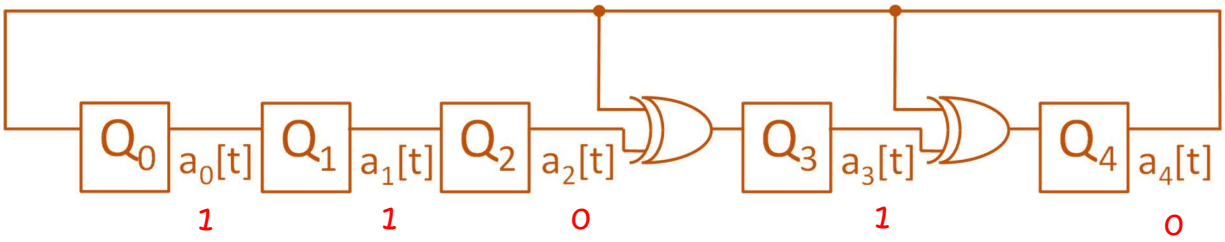

At five clock cycles, the register state is

$$A(x)[1] =< a_4[5], a_3[5], a_2[5], a_1[5], a_0[5] > = 11001$$

In polynomial form this is

$$A(x)[5] = x^4 + x^3 + 1$$

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).



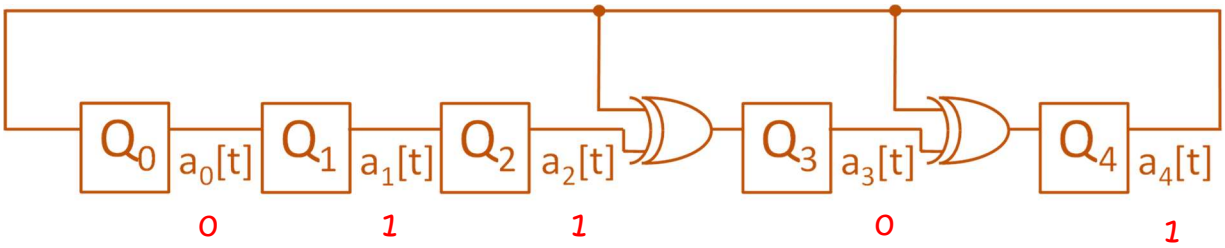

The feedback polynomial is

$$P(x) = x^5 + x^4 + x^3 + 1$$

In polynomial form this is

$$A(x)[6] = x * A(x)[5] \; mod \; P(x)$$
$$= x * (x^4 + x^3 + 1) \; mod \; (x^5 + x^4 + x^3 + 1)$$
$$= x^5 + x^4 + x \quad mod \; (x^5 + x^4 + x^3 + 1)$$
$$= x^3 + x + 1$$

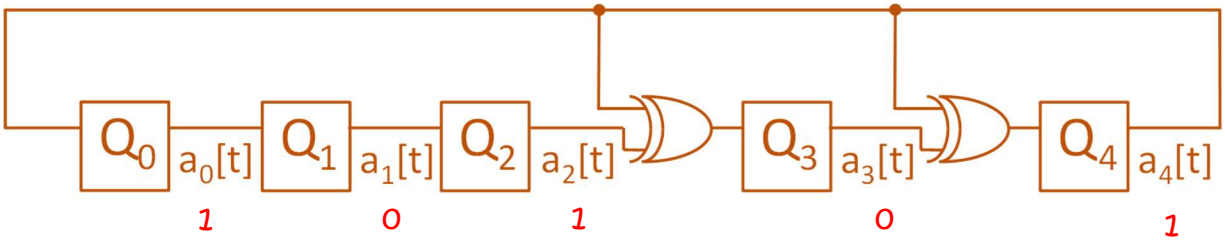
d. (10 pts.) Redraw your LFSR showing all FF inputs and outputs after one more clock cycle (i.e., go to time 7). Your new drawing should clearly label / indicate which are the values $a_4a_3a_2a_1a_0$. You are also required to calculate $a_4a_3a_2a_1a_0$ in the polynomial space and show all of your work.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




$$A(x)[7] = x * A(x)[6] \; mod \; P(x)$$
$$= x * (x^3 + x + 1) \; mod \; (x^5 + x^4 + x^3 + 1)$$
$$= x^4 + x^2 + x \quad mod \; (x^5 + x^4 + x^3 + 1)$$
$$= x^4 + x^2 + x$$

$$A(x)[7] =< a_4[7], a_3[7], a_2[7], a_1[7], a_0[7] > \; = 10110$$

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).




$$A(x)[8] = x * A(x)[7] \; mod \; P(x)$$
$$= x * (x^4 + x^2 + x) \; mod \; (x^5 + x^4 + x^3 + 1)$$
$$= x^5 + x^3 + x^2 \quad mod \; (x^5 + x^4 + x^3 + 1)$$
$$= x^4 + x^2 + 1$$

$$A(x)[8] =< a_4[8], a_3[8], a_2[8], a_1[8], a_0[8] > \; = 10101$$

**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!).**