ECE 3170

Cryptographic Hardware for Embedded Systems

Midterm II

November 21, 2024

This test is open book for the Schneier textbook and the optional textbooks. This test is also open note. Calculators are permitted but no programs may be used. Open notes include electronic notes with any handwritten or typed information you may have added. For electronic notes, all wireless connectivity must be turned off, and cell phones are not allowed; in other words, no connection to any information source outside of the classroom is allowed during the exam. Open notes also include all course assignments (homeworks or labs) as well as solutions (including both your solution as well as official solutions posted on the course website or passed out for previous exams). All aspects of the Georgia Tech Honor Code apply. Please follow the instructions precisely. If you need to continue a problem, please use the back of the ***previous*** *page.* The meaning of each question should be clear, but please state any assumptions and ask for clarification if necessary.

Question	Score	Max
1		**15**
2		**10**
3		**10**
4		**15**
5		**10**
6		**10**
Total		**70**

You can do it!

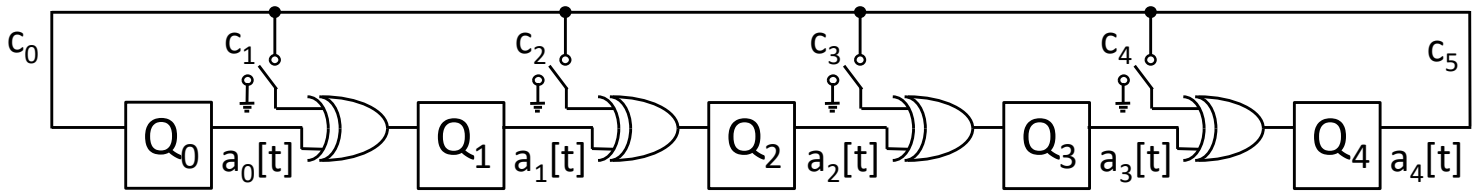
Name (Please print)_____

This test will be conducted according to the Georgia Tech Honor Code. I pledge to neither give nor receive unauthorized assistance on this exam and to abide by all provisions of the Honor Code.

Signed_____

1. **(15 pts.) Linear Feedback Shift Registers.**

Consider a 5-bit Linear Feedback Shift Register (LFSR) as follows:



(a) (5 pts.) For a 5-bit LFSR, what is the longest possible sequence of unique 5-bit states? (NOTE: the 5-bit "state" of an LFSR is $a_4[t]a_3[t]a_2[t]a_1[t]a_0[t]$ or $a_4a_3a_2a_1a_0$ at time t.)

(b) (5 pts.) What assumptions are necessary regarding the initial state and the feedback polynomial in order to achieve the longest possible state sequence? (NOTE: for the 5-bit LFSR pictured above, the values of $c_4c_3c_2c_1$ determine the feedback polynomial.)

(c) (5 pts.) Do all initial states for an LFSR achieve the same state sequence length for a given feedback polynomial? For full credit, please explain your reasoning.

2. **(10 pts.) Information Leakage through the Power Side-Channel.**

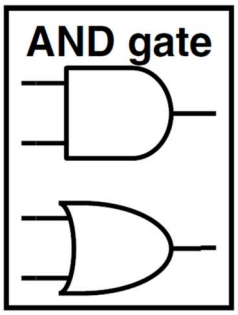
Assume you are a manager of a software development team. One of your team member wrote the following code to check passwords:

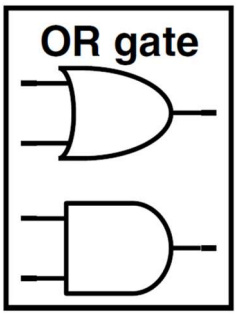
```
1  bool check_password(const char input[]){
2      const char correct_password[] = "I<3ECE3894";
3
4      if (strlen(input) != strlen(correct_password)) return false;
5
6      for (int i = 0; i < strlen(correct_password); i++){
7          if (input[i] != correct_password[i]) {
8              return false;
9          }
10     }
11
12     return true;
13 }
```

The above code is implemented on a small unpipelined single-issue microcontroller with the assembly code available to the adversary. Given your knowledge about power analysis, what information might the above code leak? Clearly explain **one** way in which the code above may leak information (HINT: there are at least two distinct ways!). For full credit, you are required to clearly explain your answer in 10 sentences or less and refer to specific lines of code in your answer.

3. **(10 pts.) WDDL.**

Consider implementing exclusive-or ($\oplus$) using WDDL. Legal WDDL gates are shown to the right, and you may redraw the gates you use in your answer but just place "WDDL AND" or "WDDL OR" in the middle to indicate which of the two WDDL gate types you are using. Each WDDL gate has four inputs and two outputs.





(a) (5 pts.) Draw an implementation of $A \oplus B$ using at most three WDDL gates. Please assume you have the following inputs available: A, $\bar{A}$, B and $\bar{B}$.

(b) (5 pts.) Simulate / show the waveforms for A=1 and B=0 for your implementation of $A \oplus B$ (i.e., your answer to the previous question). Please make sure to draw a waveform for the following signals: $prch, A, \bar{A}, B, \bar{B}, Z, and\ \bar{Z}$. As was shown in class for WDDL, make sure to start your waveforms with all of the signals equal to zero except for $prch$ which begins as value 1 but drops to 0 right away. In your waveforms, have A rise to 1 prior to $\bar{B}$ rising to 1.

$prch$									
A									
$\bar{A}$									
B									
$\bar{B}$									
Z									
$\bar{Z}$									

4. **(15 pts.) Mask Protection and Attacks on Masking.**

Consider protection afforded by masking against power analysis attacks.

(a) (5 pts.) Name at least one kind of attack which typically succeeds when cryptographic hardware is **not** protected by masking but which typically **fails** when masking is used. You do not have to "prove" beyond a doubt that the attack will fail when masking is used; you only need to explain why the attack is **likely** to fail. For full credit you must clearly describe the attack approach and when / why the attack succeeds or fails with or without masking. Please limit your answer to 10 sentences or less.

(b) (10 pts.) Name at least one kind of attack which has a reasonable chance of succeeding even when masking is used. Describe the conditions under which the attack is most likely to succeed. Please note that the majority of the points for this question will be awarded for correctly describing the conditions under which the attack is most likely to succeed. A correct name of the kind of attack which has a reasonable chance of succeeding against a masked implementation will, considered alone, earn less than half of the points for this question. Please limit your answer to 10 sentences or less.

5. **(10 pts.) The Padding Oracle Attack with (iii) Encrypt-then-authenticate.**

Consider the case of an adversary attempting to carry out the padding oracle attack when encrypt-then-authenticate is used. Please assume that two separate keys, K_E and K_{MAC}, have been exchanged securely prior to the adversary attempting to attack. Please further assume that the adversary cannot obtain or in any way discover K_E or K_{MAC}. Given that all decryption requests sent to the remote server must satisfy encrypt-then-authenticate, is it possible to carry out the padding oracle attack? Why or why not? Please limit your answer to 10 sentences or less (you may circle what you want to be graded). Please note that a correct "yes" or "no" answer with **no** correct reason(s) given will earn zero points. If multiple reasons are given some of which are correct and some of which are incorrect, partial credit will be earned. If at least one correct reason is given for the correct answer with no incorrect reason(s), full credit will be earned.

6. **(10 pts.) The Padding Oracle Attack with (ii) Authenticate-then-encrypt.**

Consider the case of an adversary attempting to carry out the padding oracle attack when authenticate-then-encrypt is used where the hash is calculated by SHA2. Please assume that an encryption key, K_E, has been exchanged securely prior to the adversary attempting to attack. Please further assume that the adversary cannot obtain or in any way discover K_E. Given that all decryption requests sent to the remote server must satisfy authenticate-then-encrypt, is it possible to carry out the padding oracle attack? Why or why not? Please limit your answer to 10 sentences or less (you may circle what you want to be graded). Please note that a correct "yes" or "no" answer with **no** correct reason(s) given will earn zero points. If multiple reasons are given some of which are correct and some of which are incorrect, partial credit will be earned. If at least one correct reason is given for the correct answer with no incorrect reason(s), full credit will be earned.

THIS IS THE LAST PAGE OF THE EXAM!