ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

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

Homework 8, 45 pts.

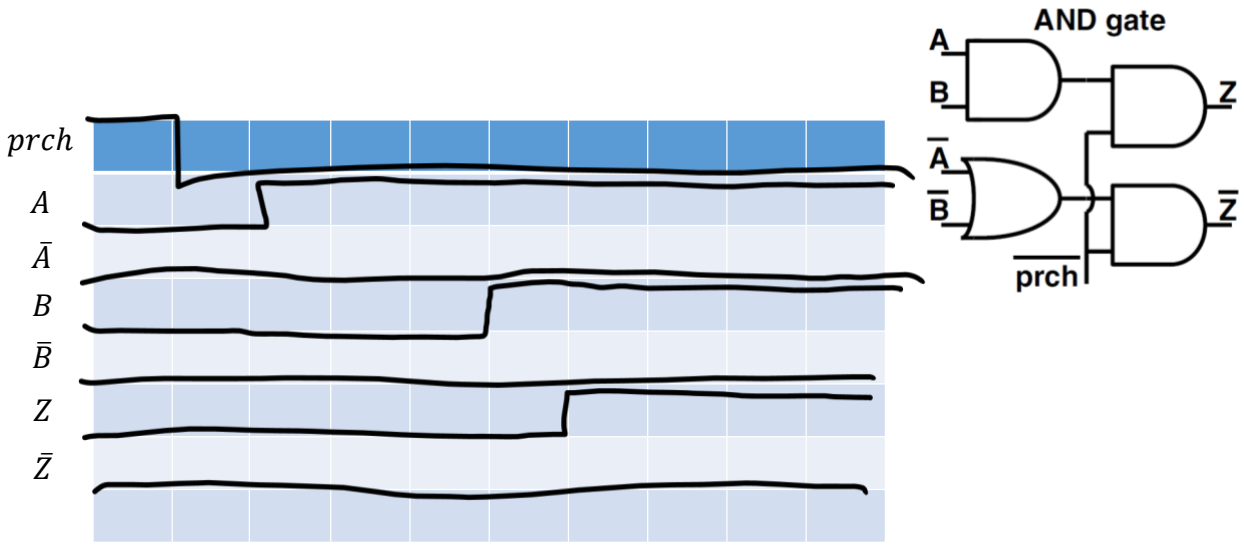
Due Friday Oct. 17 prior to 11:55pm

(please turn in homework electronically on Canvas)

As always this semester, you are required to solve this homework alone.

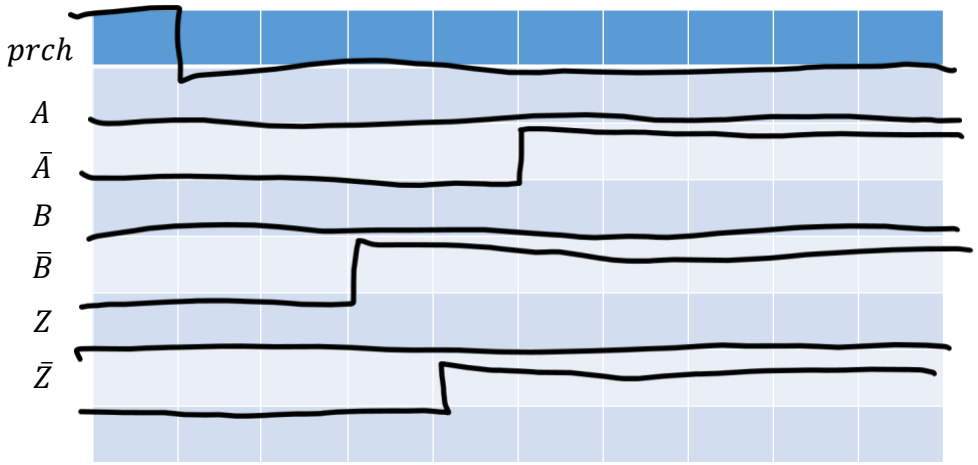
1) (15 pts.) In term of hiding (i.e., hiding data-dependent energy consumption from an attacker utilizing the power pins of a microchip as a side channel), what is the problem with SDDL? Please explain using your own words and without copying from any source, including the lecture notes or readings for this course.

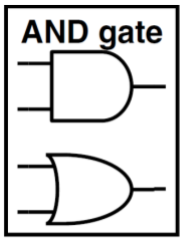
   The problem with SDDL lies in the dependence of the chip's power (energy consumption) on the chip's inputs and gate types. As a result, an attacker can deduce which operations the chip is performing by examining the chip's power traces.



2) (15 pts.) In class, the above figures were used to simulate / show the waveforms for SDDL. Now simulate / show the waveforms for A=1 and B=1. 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 SDDL, make sure to start your wave-forms 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 B rising to 1.

3) (15 pts.) In class, the figure below was used to simulate / show the waveforms for WDDL. Now simulate / show the waveforms for A=0 and B=0. 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 $\bar{B}$ rise to 1 prior to $\bar{A}$ rising to 1.





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!).