

ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

Assoc. Prof. Vincent John Mooney III

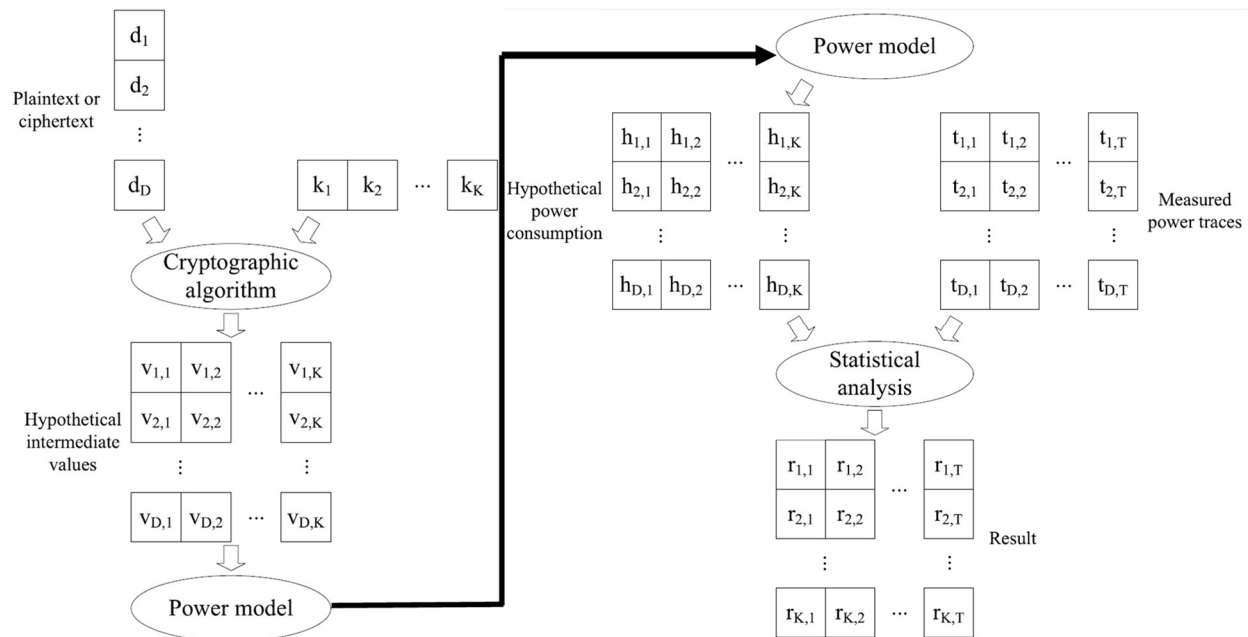
Georgia Institute of Technology

Homework 9, 35 pts.

Due Friday Oct. 24 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.) The figure above was described in lecture and is based on Figure 6.1 from Ch. 6 of *Power Analysis Attacks: Revealing the Secrets of Smart Cards* by Mangard et al. Please use your own words to provide answers to the following three aspects of the figure.
- (5 pts.) Describe what is going on in the first bubble of Figure 6.1 labeled "Cryptographic algorithm" including the inputs and outputs. Make sure to provide overall sizes of the data assuming that $D = 1000$ and $K = 256$.
 - (5 pts.) Describe what is going on in the second bubble of Figure 6.1 labeled "Power model" including the inputs and outputs. Make sure to provide overall sizes of the data assuming that $D = 1000$ and $K = 256$.
 - (5 pts.) Please describe at an abstract level what happens in the last bubble "Statistical analysis." Make sure to provide sizes of the inputs and outputs assuming that $D = 1000$, $T = 1000$ and $K = 256$.

2) (20 pts.) Consider Figure 6.2 from Ch. 6 of *Power Analysis Attacks: Revealing the Secrets of Smart Cards* by Mangard et al. (Please see the next page.) Please answer the following questions.

- (5 pts.) What does the graph show for key hypothesis = 223? In addition to the conclusion, i.e., stating what the graph shows, please also explain why with a few sentences. It is OK if this answer is similar to other answers.
- (5 pts.) What does the graph show for key hypothesis = 224? In addition to the conclusion, i.e., stating what the graph shows, please also explain why with a few sentences. It is OK if this answer is similar to other answers.
- (5 pts.) What does the graph show for key hypothesis = 225? In addition to the conclusion, i.e., stating what the graph shows, please also explain why with a few sentences. It is OK if this answer is similar to other answers.
- (5 pts.) What does the graph show for key hypothesis = 226? In addition to the conclusion, i.e., stating what the graph shows, please also explain why with a few sentences. It is OK if this answer is similar to other answers.

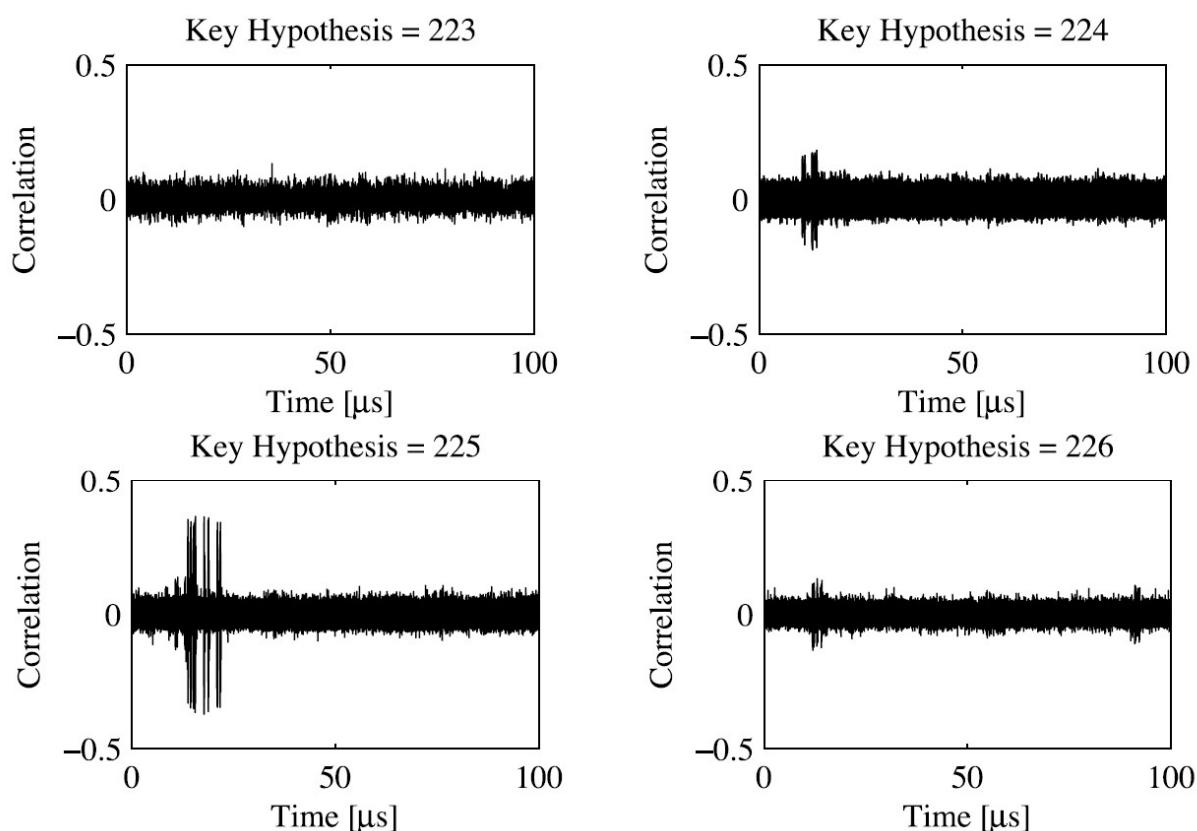


Figure 6.2. The rows of the matrix $\mathbf{R}$ that correspond to the key hypotheses 223, 224, 225, and 226.

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!).