ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

Assoc. Prof. Vincent John Mooney III

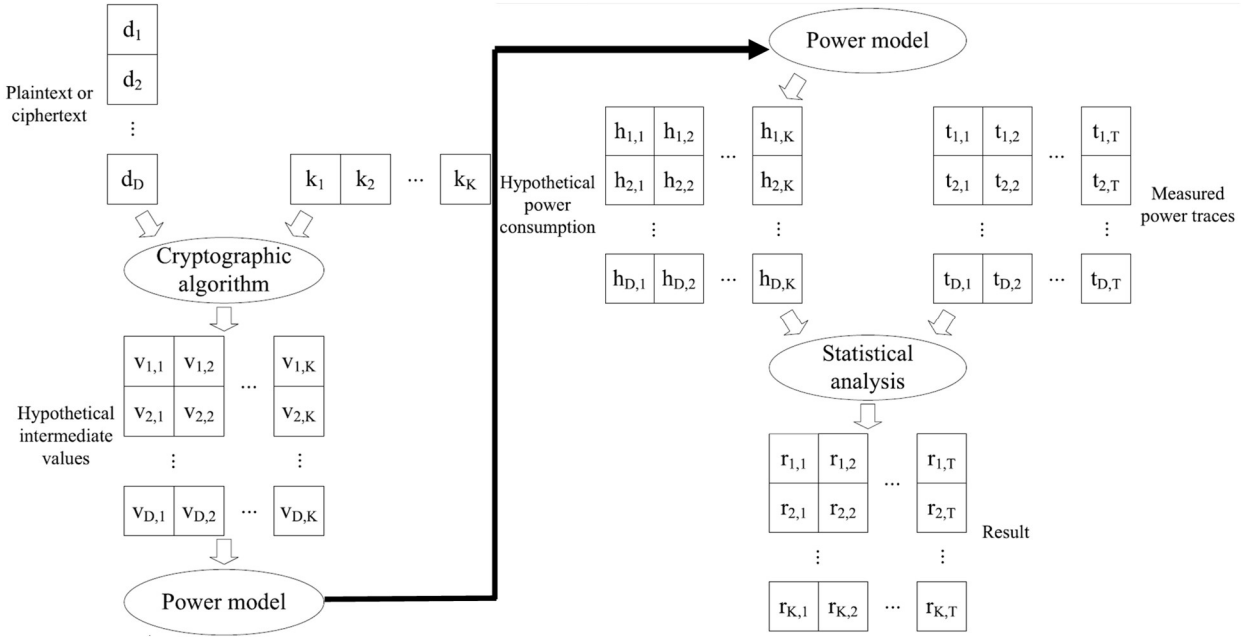
Georgia Institute of Technology

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.

   a. (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.

"Cryptographic algorithm" calculates hypothetical plaintext/ciphertext values given a specific algorithm such as DES, for possible key inputs and data inputs. In this case, eight bits of the key are used (for 256 combinations) with 1000 data samples (plaintext or ciphertext). This results in a matrix of size 1000 * 256 = 256,000.

b. (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.

Each of the hypothetical intermediate values from the matrix developed by the "Cryptographic algorithm" bubble is used to develop predicted energy consumption and power values. The output of the "Power model" bubble has the same size as the input matrix, which in this case is 1000 * 256 = 256,000.

c. (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.

1000 power measurements (each set of 1000 measurements is a "trace") are made for each of the plaintext or ciphertext inputs previously produced. This results in a matrix with size D * T, i.e., 1000 * 1000. This matrix is then correlated with the predicted power measurement values with each entry r_{ij} the result of comparing power consumption values for key i with measured trace j. This produces the result matrix with size K * T, i.e., 256 * 1000 = 256,000.

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.

a. (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.

For key hypothesis = 223, the graph shows little correlation between the hypothetical power consumption and the recorded power consumption of the microcontroller. This is due to no apparent high peaks existing in this plot.

b. (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.

For key hypothesis = 224, the graph shows weak correlation between the hypothetical power consumption and recorded power consumption of the microcontroller. The correlation is more significant than in a), owing to the more apparent peaks observed around the 10-microsecond mark.

c. (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.

For key hypothesis = 225, the graph shows strong correlation between the hypothetical power consumption and recorded power consumption of the microcontroller. This is because of the very high peaks observed around the 10-microsecond mark. A key takeaway from these peaks is that the first byte of the secret key for the microcontroller is 225.

d. (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.

For key hypothesis = 226, the plot is very similar to the plot in a), containing no high peaks. Therefore, the correlation between hypothetical and measured power consumption is incredibly weak as in part a) on the previous page.

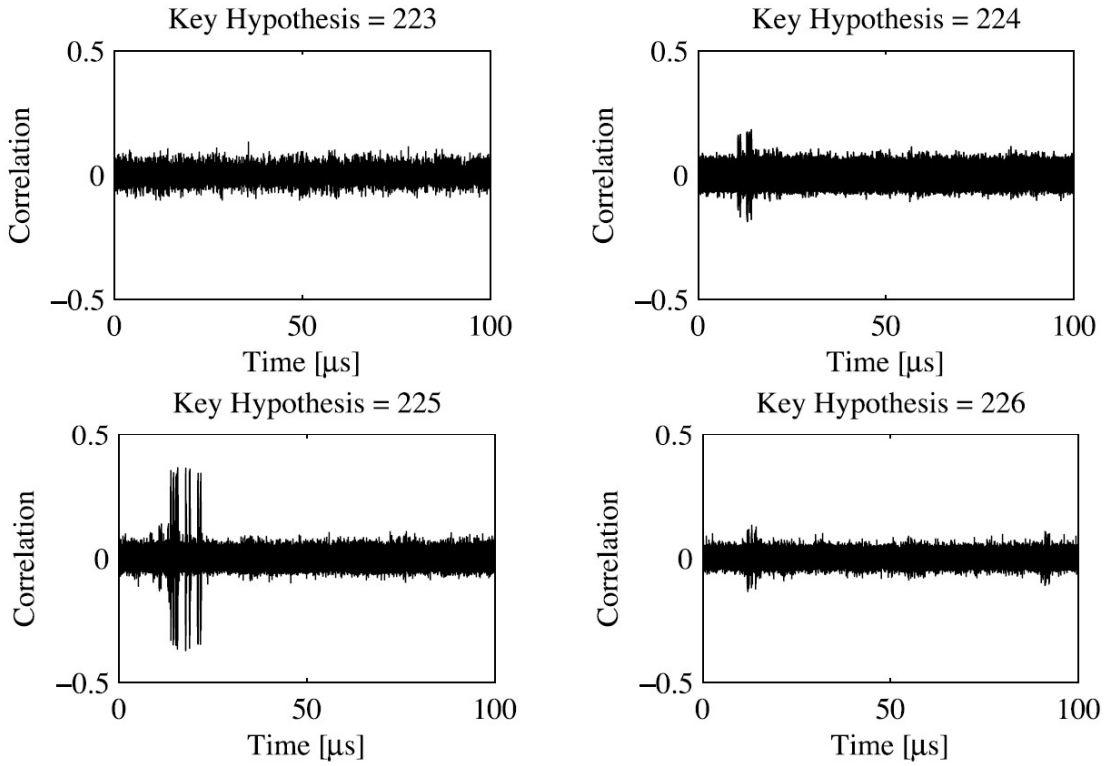


Figure 6.2. The rows of the matrix $\mathbf{R}$ that correspond to the key hypotheses 223, 224, 225, and 226.