ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

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

Homework 7, 85 pts.

Due Friday Oct. 10 prior to 11:55pm

(please turn in homework electronically on Canvas)

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

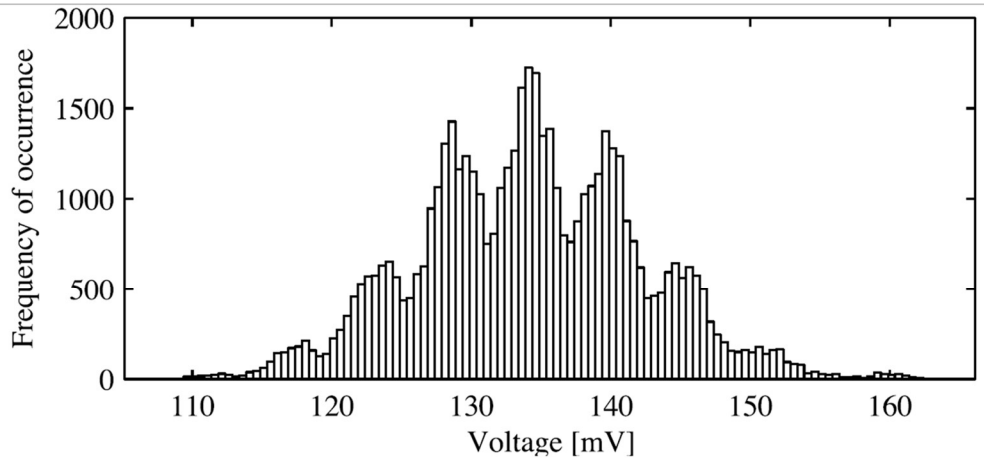

Figure 4.4. Histogram of the power consumption at 362 ns if different data values are transferred from the internal memory to a register.

1) (20 pts.) Explain using your own words what are the nine different Gaussian distributions which compose the energy consumption histogram above. Explain how and why the nine distributions are combined as well as the source of each Gaussian distribution. Include in your explanation the following terms and concepts: $\{D_i\} = D_0 \ldots D_{255}$ = 8-bit data values; HW = Hamming Weight (a.k.a. Hamming Distance from all zeros); μ = mean; and σ = standard deviation. Please define and explain any additional terms you utilize. You may refer to the figure on the next page, Figure 4.5, in your answer to explain the power histogram shown in Figure 4.4 above.

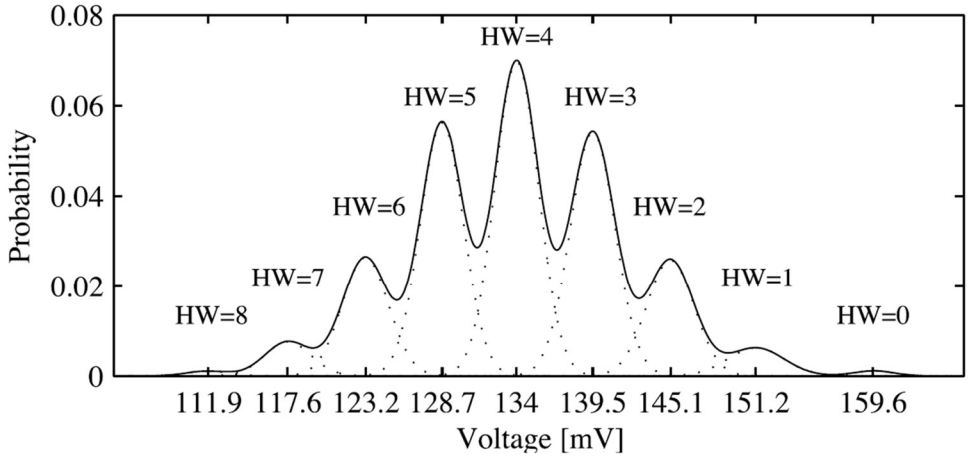

Figure 4.5. The distribution of the power consumption when the microcontroller transfers different data from the internal memory to a register.

2) (25 pts.) Consider Figures 4.1 and 4.2 from Chapter 4 of *Power Analysis Attacks: Revealing the Secrets of Smart Cards* by Mangard et al. The point of this question is qualitative, not quantitative.
   a. (5 pts.) Explain in your own words what the five power traces shown in Figure 4.1 indicate.
   b. (10 pts.) Use your own words to describe the experiment being carried out in Figure 4.2. Make sure that the following items appear in your answer: (i) $P_{el.\ noise}$, (ii) histogram and (iii) 10,000.
   c. (5 pts.) In your answer to the previous question, 2.b, you used the quantity 10,000. What if this quantity were changed to 100,000: would your answer to 2.b be the same or different? Why or why not? Please note that a correct "yes" or "no" answer without a proper reason will receive zero points.
   d. (5 pts.) In your answer to question 2.b, you used the quantity 10,000. What if this quantity were changed to 1,000: would your answer to 2.b be the same or different? Why or why not? Please note that a correct "yes" or "no" answer without a proper reason will receive zero points.

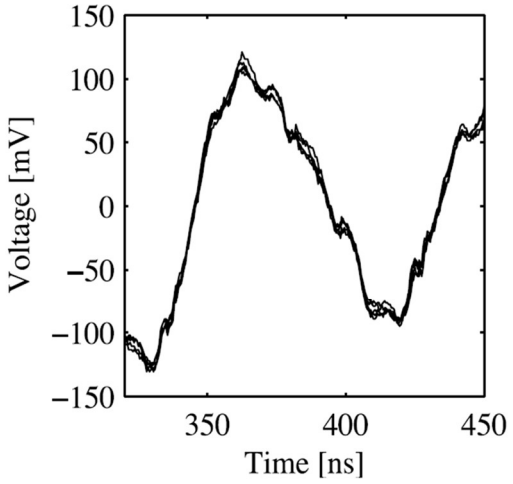

Figure 4.1. Power traces look very similar if the same data is processed.

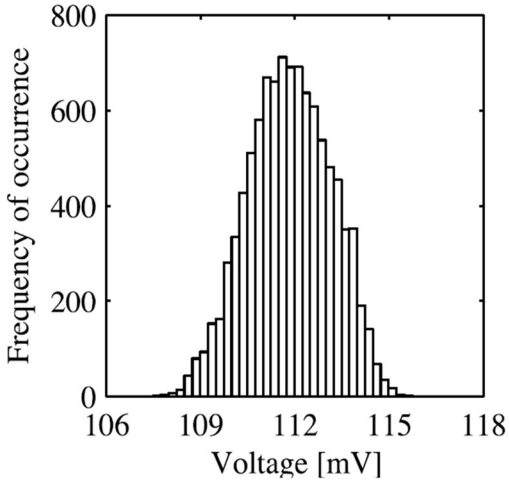

Figure 4.2. Histogram of the power consumption at 362 ns of Figure 4.1.

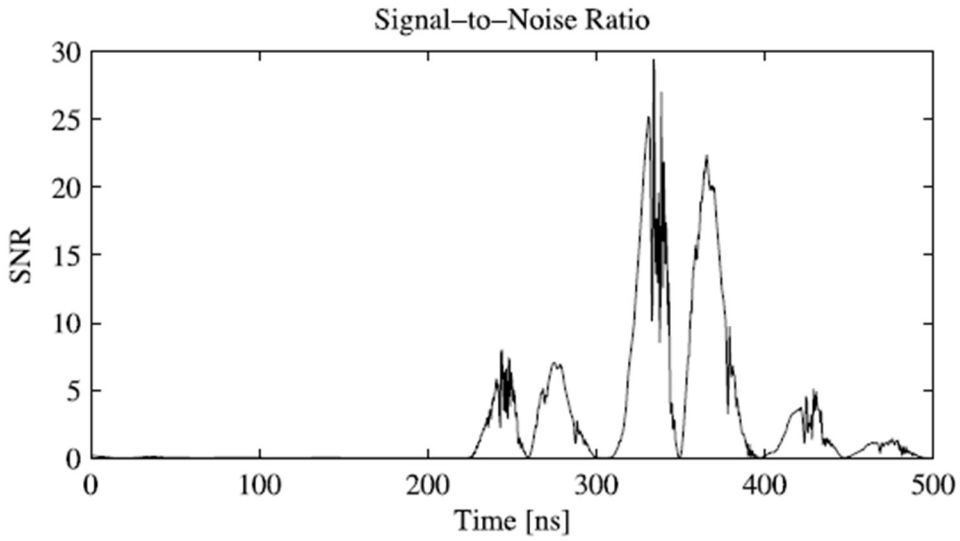

Figure 4.7. The signal levels, the standard deviation of the noise, and the SNR when attacking a uniformly distributed 8-bit data value on our microcontroller.

3) (25 pts.) Consider the third plot of Figure 4.7 from Chapter 4 of *Power Analysis Attacks: Revealing the Secrets of Smart Cards* by Mangard et al. The third plot of Fig. 4.7 shows the resulting Signal-to-Noise Ratio (SNR) for a uniformly distributed 8-bit data value used as a plaintext input to AES encryption with a secret key.

   a. (5 pts.) Write a proper expression for the Signal-to-Noise Ratio (SNR) calculation used to produce the y-axis in the third plot of Figure 4.7. Make sure that the following three variables appear in your answer: P_{exp}, $P_{switching}$ and $P_{el.\ noise}$.
   b. (5 pts.) Prior to 200 ns, the SNR in the third plot of Figure 4.7 has a value of approximately zero. Why is this the case and what does this SNR value of zero indicate?
   c. (15 pts.) In class it was stated that the two largest SNR values in the third plot of Figure 4.7 occur at 330 ns and 362 ns. For the purposes of using power as a side-channel attack, why are the measurements taken at 362 ns preferred over the even larger SNR measurements at 330 ns? You are required to answer this question in three parts as follows:
      i. (5 pts.) What is the goal of the attacker, i.e., what information is the attacker trying to gain?
      ii. (5 pts.) What assumption is made regarding attacker access to the microcontroller assembly code running AES, and why is this assumption reasonable? To receive full credit for this question, you must give at least one valid explanation for why this assumption is reasonable – but do please note that there are many such equally valid reasons; one good reason is enough for full credit.
      iii. (5 pts.) Now, in the context of your answers to 3.c.i and 3.c.ii above, explain why measurements taken at 362 ns are preferred for use by the attacker over the SNR measurements at 330 ns even though the measurements taken at 330 ns have a larger SNR for our quantities of interest (according to the answer to 3.a) as compared to the measurements taken at 362 ns.

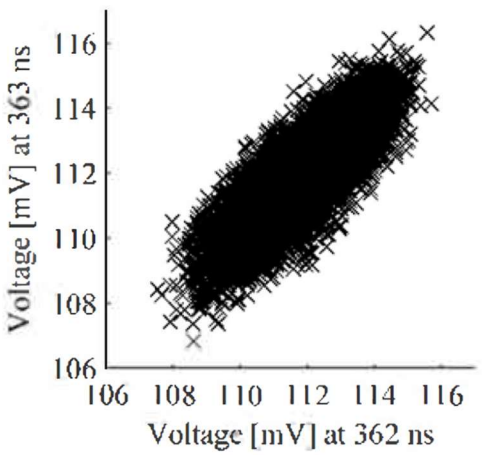

Figure 4.9. Scatter Plot: The power consumption at 362 ns is correlated to the power consumption at 363 ns. $r = 0.82$

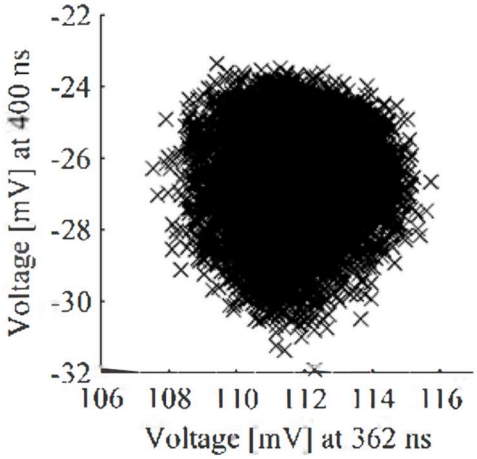

Figure 4.10. Scatter Plot: The power consumption at 362 ns is largely uncorrelated to the power consumption at 400 ns. $r = 0.12$

4) (15 pts.) Consider Figures 4.9 and 4.10 from Chapter 4 of *Power Analysis Attacks: Revealing the Secrets of Smart Cards* by Mangard et al. The point of this question is qualitative, not quantitative.

   a. (5 pts.) Explain the units used in the *x* and *y* axes of Figures 9 and 10. What do the millivolts represent and why is the representation valid?

   b. (10 pts.) Explain in your own words the difference between Figures 4.9 and 4.10 in terms of what the plots indicate about the relationship between the measurements at 362 ns as compared to 363 ns versus compared to 400 ns. In your answer, make sure to use the words "covariance" and "correlation" with their appropriate technical meanings clear from the context and usage.

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!).