ECE 3170 Cryptographic Hardware for Embedded Systems

Fall 2025

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

Homework 11, 50 pts.

Due Friday Nov. 7 prior to 11:55pm

(please turn in homework electronically on Canvas)

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

1) (5 pts.) Read the paper by T.S. Messerges, "Using Second-Order Power Analysis to Attack DPA Resistant Software," Cryptographic Hardware for Embedded Systems (CHES) conference, 2000. Please indicate that you have read the article by writing an appropriate sentence, e.g., "I hereby certify under the Georgia Tech Honor Code that I have read the CHES 2000 article assigned in this homework for problem 1."

2) (5 pts.) How can so-called "Zero-Value" or ZV 1st-order DPA attacks work against masked implementations of cryptographic calculations? Please provide a concrete example and explain using your own words.

The ZV 1st order DPA attack can work against a masked implementation if the output of the masked variable is independent of the mask when the variable has value zero. It is as if the mask was not there in the first place. For example, if $m = 0$, then $v_m = (v \oplus m) * m = 0$. Furthermore, if $v = 1$, *then* $v_m = (v \oplus m) * m = 0$ both when the mask $m = 0$ and when the mask $m=1$ since $(v \oplus m) * m = (1 \oplus 1) * 1 = 0 * 1 = 0$.

3) (10 pts.) Consider the following code where PTI stands for "Plain Text Input."

```
W1 (PTI)
{
   A: Result = PTI ⊕ SecretKey
```

Let there be N bits in the data types used in the instruction at position A, and let the i^{th} bit of PTI be p_i with the i^{th} bit of SecretKey represented as k_i. Assume that all bits (both key and plaintext bits) are random except for bit i. If the Result of the instruction at position A has Hamming Weight (HW) "d" then why do we know that the expected value of d, given that $k_i \oplus p_i$ is zero, is $\frac{N-1}{2}$? In other words, explain why the following is true: $E[d \mid k_i \oplus p_i = 0] = \frac{N-1}{2}$.

First, since $k_i \oplus p_i$ = 0 is given, then clearly the i^{th} bit of Result has an expected HW value of zero. That leaves N-1 bits each of which has an expected HW value of $\frac{1}{2}$. Therefore, the remaining N-1 bits of Result have an expected HW value of $\frac{N-1}{2}$.

4) (10 pts.) Consider the following code.

```
W2 (PTI)
{
B:  RandomMask = rand()
    mPTI = PTI ⊕ RandomMask
C:  Result = mPTI ⊕ SecretKey
```

Let there be N bits in the data types used in the instruction at position C, and let the i^{th} bit of RandomMask be r_i. Furthermore, let the i^{th} bit of PTI be p_i with the i^{th} bit of SecretKey represented as k_i. Assume that all bits (the key, the plaintext and the mask bits) are random except for bit i. If the Result of the instruction at position C has Hamming Weight (HW) "d_C" then why do we know that the expected value of d_C given that $r_i \oplus k_i \oplus p_i$ is one, is $\frac{N+1}{2}$? In other words, explain why the following is true: $E[d_C \mid r_i \oplus k_i \oplus p_i = 1] = \frac{N+1}{2}$.

First of all, since $r_i \oplus k_i \oplus p_i$ =1 is given, then clearly the i^{th} bit of mPTI⊕SecretKey = PTI⊕RandomMask⊕SecretKey has an expected HW value of one. That leaves N-1 bits each of which has an expected HW value of $\frac{1}{2}$. Therefore, the remaining N-1 bits of Result have an expected HW value of $\frac{N-1}{2}$. The total expected HW value is then $\frac{N-1}{2} + 1 = \frac{N-1}{2} + \frac{2}{2} = \frac{N+1}{2}$.

5) (20 pts.) Consider the following algorithm.

Proposition 2. When the W_2 algorithm is implemented in an N-bit processor, where there is a linear relationship between the instantaneous power consumption and the Hamming weight of the data being processed, the following second-order DPA attack is sound:

1. *Repeat for i equal to 0 through $N-1$ {*
2. *Repeat for $b = 0$ to 1 {*
3. *Calculate average statistic $\bar{S}_b = |P_B - P_C|$ by repeating the following:{*
4. *Set the ith bit of the PTI input to b.*
5. *Set the remaining PTI bits to random values.*
6. *Collect the algorithm's instantaneous power consumption as lines B and C. Call these values P_B and P_C, respectively. } }*
7. *Calculate the DPA bias statistic $T = \bar{S}_0 - \bar{S}_1$.*
8. *If $T > 0$ then the ith key bit is a one, otherwise it is a zero.*

The bias statistic $T = \bar{S_0} - \bar{S_1}$ is the focus of this question. We will start with $\bar{S_0}$ based on the following equation:

$$\bar{S}_0 = \frac{1}{2}\mathrm{E}\left[\varepsilon\left|d_B - d_C\right| \middle| r_i = k_i = p_i = 0\right] + \frac{1}{2}\mathrm{E}\left[\varepsilon\left|d_B - d_C\right| \middle| r_i = 1,\ k_i = p_i = 0\right] \quad (11)$$

$$= 0$$

Recall that in the paper from which the above equation is taken, p_i is the i^{th} bit of PTI, k_i is the i^{th} bit of the secret key, and r_i is the i^{th} bit of the mask.

a. (5 pts.) Explain why $\bar{S_0}$ claims that half of the time $r_i = 0$ and the other half of the time $r_i = 1$. What if the sample size is very small, is this claim always true?

GRADED ON AN EFFORT / NO EFFORT BASIS

The mask is supposed to be from a random number generator, therefore bit i of the mask, i.e., r_i, should have the statistical behavior of an unbiased, fair coin toss. This is true even if the sample size is small because even a pseudo random number generator will behave like a true random number generator given a small sample size.

Some students pointed out that even an unbiased, fair coin toss will vary from 50%. For example, suppose the sample size is an odd number, then it is not possible for $r_i = 0$ 50% of the time. This is true. The statistical behavior when concretized to a specific number of samples will have a possibility of not having $r_i = 0$ 50% of the time. However, each sample of r_i still has a 50% chance of being a 1 or a 0 .

b. (5 pts.) Give the value of $E[\varepsilon d_C \mid r_i=1, k_i = p_i = 0]$ and explain why your answer is correct (i.e., give reasons for your answer).

Given that r_i=1, k_i =p_i =0, then $r_i \oplus k_i \oplus p_i$ = 1. We know that $E[d_c \mid r_i \oplus k_i \oplus p_i=1] = \frac{N+1}{2}$. Therefore, $E[\varepsilon d_c \mid r_i \oplus k_i \oplus p_i=1] = \varepsilon\frac{N+1}{2}$.

Next we will consider $\bar{S}_1$ based on the following equation:

$$\bar{S}_1 = \frac{1}{2}\mathrm{E}\left[\varepsilon\left|d_B - d_C\right| \middle| p_i = 1, r_i = k_i = 0\right] + \frac{1}{2}\mathrm{E}\left[\varepsilon\left|d_B - d_C\right| \middle| r_i = p_i = 1, k_i = 0\right] \quad (12)$$
$$= \varepsilon$$

c. (5 pts.) Give the value of $E[\varepsilon d_B \mid p_i=1, k_i = r_i = 0]$ and explain why your answer is correct (i.e., give reasons for your answer).

Given that p_i= 1, k_i= r_i = 0, then r_i = 0. The instruction at location B is the generation of the random mask value which determines the value of r_i. But we already know that r_i = 0. Therefore there are N-1 bits remaining which have an expected HW value of $\frac{N-1}{2}$. Thus, $E[d_B \mid p_i= 1, k_i= r_i = 0] = \frac{N-1}{2}$. Therefore, $E[\varepsilon d_B \mid p_i= 1, k_i= r_i = 0] = \varepsilon\frac{N-1}{2}$.

d. (5 pts.) Give the value of $E[\varepsilon|d_B - d_C| \mid r_i = p_i = 1, k_i = 0]$ and explain why your answer is correct (i.e., give reasons for your answer).

Given that p_i = r_i = 1, k_i = 0, then r_i = 1. The instruction at location B is the generation of the random mask value which determines the value of r_i. But we already know that r_i = 1. Therefore, there are N-1 bits remaining which have an expected HW value of $\frac{N-1}{2}$. Thus, $E[d_B \mid p_i = r_i = 1, k_i=0] = \frac{N-1}{2} + 1 = \frac{N-1}{2} + \frac{2}{2} = \frac{N+1}{2}$.

Now for d_c. Given that p_i = r_i = 1, k_i = 0, then $r_i \oplus k_i \oplus p_i$ = 0. Thus, $E[d_c \mid p_i = r_i = 1, k_i=0] = \frac{N-1}{2}$.
Therefore, $E[|d_B - d_c| \mid p_i = r_i = 1, k_i=0] = E[|\frac{N+1}{2} - \frac{N-1}{2}|] = 1$.

Finally, $E[\varepsilon|d_B - d_c| \mid p_i = r_i = 1, k_i=0] = \varepsilon$.